OPSWAT.



MetaDefender™ for Secure Storage

MetaDefender Storage Security

4.5.x

Table of Contents

Introduction 10
- Overview 11
- Architecture & Components 12
- Planning your Deployment 14
- Sizing Guide 17
- General System Requirements 20
  - Unix deployment 22
  - Windows deployment 23
- Licensing Model 25
- MetaDefender Storage Security Documentation 26
- Choosing your deployment model 27
  - Basic Deployment 27
  - Basic Deployment with Self-Hosted Shared Services 28
  - Basic Deployment with Managed Services 29
  - Advanced Deployment with Managed Services 31
  - Advanced Deployment with Self-Hosted Shared Services 32
  - Cloud Deployment with Kubernetes (k8s) 34

Installation 36
- Types of deployment 37
- Deploy to cloud service providers 38
  - CSP Deployment Overview 38
  - Architecture Examples in CSPs 38
  - General Cloud Considerations 45
  - Using OPSWAT´s image from CSPs Marketplace 46
  - AWS Deployment 47
  - Azure Deployment 62
  - GCP Deployment 77
  - External Services Configuration 92
- ON-PREMISE DEPLOYMENT 104
  - On-Premise Deployment Overview 104
  - Production Considerations 104
  - Installation Methods 113
  - Upgrade MDSS 130
  - Uninstall 136
  - Troubleshooting On-Premise 137

containerized deployments 139
Containerized Deployment Overview 139
Kubernetes Deployment 139
Portable Package 152

Integrations 153

Integrations 154
Add An Amazon S3 Storage 156
How to Enable Inline Scanning? 165
How to verify if tagging functionality is supported? 165
How to Enable Autodiscovery 166
Add A Cubbit Storage 173
Add An Oracle Cloud Storage 175
Add An Oracle SDK Storage 180
Add A Wasabi Storage 183
Add a Cloudian Storage 187
Add a MinIO Storage 190
Add an OneDrive Storage 192
Add a SharePoint Online Storage 200
How to Enable Autodiscovery 209
Add a Microsoft Teams Storage 216
Add a SharePoint On-Premise Storage 218
Configuring Error Handling and Retry Mechanisms for SharePoint On-Premise 219
Add a Box Storage 224
Add an Azure Files Storage 234
Add an Azure Blob Storage 236
How to Enable Autodiscovery 244
Add an Alibaba Cloud Storage 251
Add a Google Cloud Storage 253
How to Enable Autodiscovery 256
Add an OPSWAT MFT Storage 263
Add an NFS Storage 268
[Linux] How to add an NFS storage unit 269
[Windows] How to add an NFS storage unit 274
How to add an Amazon EFS as an NFS storage unit 279
[Windows] How to Expose an SMB Share as an NFS Storage Unit 282
How to Enable NFS scanning on a Kubernetes Cluster 286
What is User Squashing for Network File System [NFS] 287
Add an NFS with SISL Storage 289

Add an SMB-Compatible Storage 291
How to scan Windows client SMB shares? 291
Recommended approach when adding SMB units on Linux deployments 292
Add an SMB-Compatible unit in Windows deployments 293
Add an SMB-Compatible unit in Linux deployments 296
Add a NetApp ONTAP Storage 301
Vscan | How to enable 303
Vscan | Best practices 317
Vscan | Scalability 318
AWS FSx for NetApp ONTAP 321
Vscan | How to connect multiple SVMs 323
Vscan | Configuration 328
ONTAP Connector Configuration file 330
Add an SFTP Storage 341
Add a Dell EMC Isilon Storage 345
Add an FTP Storage 347
Configuring a Windows IIS FTP Server for MDSS Scanning 349
Add a Scality RING Storage 355

Operations 360
Onboarding 361
Dashboard 367
Scanning 372
Password Protected Files and Encrypted Archives 381
Reprocess files 383
Identity Scanning 387
Reports 393
Settings 395
Importing/Exporting a configuration 396
Scan Pools 401
Workflows 402
Autodiscovery 412
Inventory 418
Cross-Domain Transfer (Data Diode) 427

Configuration and Management 430
Custom configuration 431
Web interface port 433
Real Time Processing configuration for NAS 434

Temporary local files created during remediation 436
Performance Tuning Guide 439
Configuring HTTPS 443
Custom CA certificates 446
Enable Real-Time Processing (RTP) 448
Polling handling 450
Event-based handling 451
Event-Based request format 452
Event-Based Real-Time Cloud Functions Examples 455
Event-based handling for Box 457
Event-based handling for SharePoint Online 460
Event-Based Real-Time handling for AWS 468
Event-Based Real-Time handling for Azure 476
Event-Based Real-Time handling for OracleSDK 479
Workflows 485
File Tagging 485
Deep Content Disarm and Reconstruction (Deep CDR) 490
Keep, Copy, Move or Delete Files 493
Delete Empty Folders 504
Remediation Process Retries 507
File Definition 507
Technologies 508
Scan File Versions 511
User Management 515
Reset/forgot password 520
Change your account information 526
Generate an API Key 527
SMTP 530
License 533
Notifications 534
Email reports 535
User registration request notifications 539
Blocked file notifications 543
Scan completed notifications 544
File scanned notifications 547
File scanned RabbitMQ notifications 551
External Loggers Configuration 556
Kafka External Logger 557
Syslog UDP External Logger 560

Syslog TCP External Logger 563
AWS CloudWatch External Logger 567
Syslog Message Reference — One Sample per Event Type 570
Single Sign On 610
AD FS Specific Configuration 610
Okta Specific Configuration 618
Azure AD Specific Configuration 628
PingFederate Specific Configuration 641
AD FS SAML2 Specific Configuration 649
Database procedures 658
AWS RDS with PostgreSQL 658
Exporting database 662
Upgrade Guide to PostgreSQL [MDSS v4.0.0] 663
Database Vacuum 669
Database Retention 671
File Discovery Debounce 672
Active-Active configuration 674
Security & Encryption Keys 676
My OPSWAT Central Management 678
Enrolling the product to Central Management 678
Telemetry 686
Automatic Scaling [Autoscaler] 687
Automatic scaling settings 695

Knowledge Base 706

The MDSS API Gateway - What It Is and Which Port It Uses 707
External Loggers — Streaming the MDSS Audit Trail to a SIEM 711
CONFIGURATION _ SETUP 735
Is there a limitation on importing configuration to MetaDefender Storage Security? 735
[Linux] What are MDSS-related resources and how to perform disk cleanup? 735
How to Enable Specific Modules in the Configuration? 737
Which API endpoints from MD Core does MDSS utilize? 739
Advanced File API Filtering and Sorting 739
Is SNMP monitoring supported for MetaDefender Storage Security? 741
[Linux] How to download docker images from alternate location? 741
[Windows] How to create a persistent mount for SMB and NFS? 741
[K8s] How to enable Horizontal Pod Autoscaling based on RabbitMQ queue metrics 746
How to Configure and Use Syslog and Serilog Sinks? 751
Does MetaDefender Storage Security support symlinks scanning? 754

Does a CVE affect MetaDefender Storage Security? 755
How do I Check Port 80 and 443 Usage Before Installing MDSS on Windows and Linux? 756
What's the Best Practice for Managing Logs and Data Retention in MDSS? 759
How to disable the Local PostgreSQL when using an external Database? 761
Why remediation actions are not working? 762
What is the expected MetaDefender Storage Security Remediation Behavior Behind F5 Load Balance? 764
Why connection to SMB share cannot be established? 765
What permissions are needed for the user of the storage of Google Cloud? 766
How to Integrate Cerberus SFTP with MDSS? 768
How to Handle SSL/TLS Issues with OPSWAT MetaDefender Core Webhook Callback? 782
Why does MetaDefender Storage Security reset the RTP StartTime every day? 783
How to Exclude the OPSWAT Folder from Windows Defender? 784
What are the Syslog Facilities and Levels in MetaDefender Storage Security? 787
How to protect the customer.env file in MetaDefender Storage Security? 789
How Can I Improve Folder Discovery and Scanning Performance in MetaDefender Storage Security? 789
How to create a PostgreSQL Database in AWS? 791
How to set up Active Active configuration? 796
AWS Lambda with S3 Trigger for MDSS Real-Time Processing 798
How to configure SMTP server on MetaDefender Storage Security to send notification to Gmail mailbox? 804
What are the Maximum and Minimum Data Retention Periods for MetaDefender Storage Security? 806
How to change PostgreSQL DB port used by MDSS 807
What is the latest MetaDefender Storage Security version? 809
Why is the Discovery Service becoming unresponsive due to RabbitMQ connection issues? 811
Changing the Authority URL in SSO will redirect to initial one 811
Scan Priorities & Throughput Tuning 813
Service Instance Scaling on Linux 819
How to move the location of the MetaDefender Storage Security services_logs folder? 824
Errors and Troubleshooting 826
Why does MetaDefender Storage Security get stuck in a remediation loop, causing inaccessibility? 826
How to fix 'Name does not resolve' error in RHEL / Rocky Linux 8 with Podman 827
Why is my MetaDefender Storage Security account disabled due to too many failed login attempts? 829
Troubleshooting errors when configuring HTTPS communication for webserver 830
Why does a report fail to load with error "API took too long to respond"? 832
Why am I receiving the error "PostgreSQL migrations did not finish" when installing MetaDefender Storage Security? 834

Why am I getting a "stat /etc/mdss/docker-compose.onedrive.yml: no such file or directory" error when upgrading MetaDefender Storage Security from 3.6.1 to 4.1.0? 836
Why is RabbitMQ consuming excessive memory in MetaDefender Secure Storage (MDSS) Kubernetes deployment? 838
Is the Scheduled Scan in MetaDefender Storage Security Based on OS Time or an Internal Timer? 839
Why does MDSS installation might fail with “net/http: TLS handshake timeout” when pulling Docker containers? 840
How to resolve "Remediation Reached the Configured Timeout" for SMB Storage 842
How to troubleshoot slow historical data retrieval from the AVEVA PI Server? 844

Troubleshooting Guide 848

Diagnostic 849
Logs location 849
How to read the logs 849
How to generate a support package 851
How to Enable Extra Logging in the Configuration? 857
Enable debug logs for script commands 861
Resolving error code 1722 when OPSWAT ONTAP Connector tries to connect to ONTAP AV Connector 861
INSTALLATION 868
Unable to remove docker network 868
Running behind a proxy 868
Why I am getting error "No available rule is present for scanning" 870
Why am I getting the 'Configured user limit on inotify instances has been reached' error in MDSS on Linux/Kubernetes? 873
How to handle empty objects in Discovery? 875
Permission denied while uninstalling on Linux 875
Portable package and offline docker toolkit are not starting due to RabbitMQ deprecated feature not being permitted? 876
INTEGRATIONS 878
NFS storage unit is not detecting any files 878
Why my files are not moving on SharePoint On-Prem with MDSS, despite UI confirmation? 879
Scan stuck in the "processing" state on the SMB Service 879

Release Notes 881

Release notes 882
Changelog 886

MetaDefender Storage Security API 912

Introduction

Overview

MetaDefender Storage Security offers a robust solution for protecting enterprise data stored in various on-premises, cloud, and hybrid environments. It is designed to prevent data breaches, downtime, and compliance violations by scanning files for malware, vulnerabilities, and sensitive data.

A crucial aspect of MetaDefender Storage Security's operation is its **exclusive bundling and integration with MetaDefender Core and its associated engine packages.**

MetaDefender Storage Security itself does not perform the deep file analysis. Instead, it acts as a component that connects to various storage solutions (Amazon S3, Azure Blob, network-attached storage, etc.) and orchestrates the scanning process by sending files to a MetaDefender Core instance.

MetaDefender Core is the underlying analysis engine that utilizes multiple proprietary OPSWAT technologies, including:

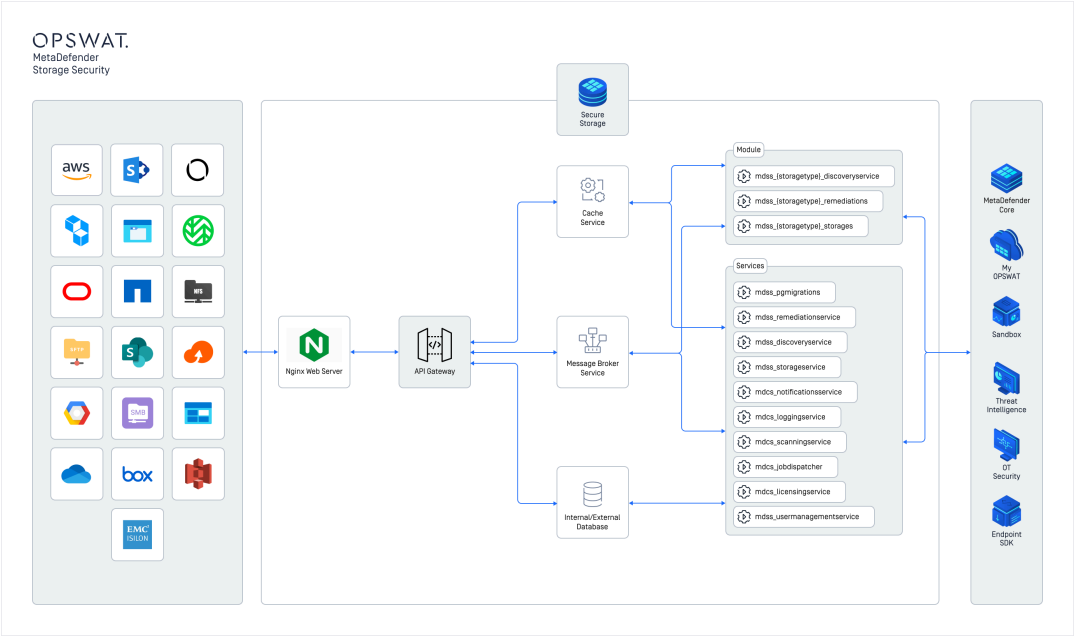
- Multiscanning leverages multiple anti-malware engines to detect a broad range of known threats.
- Deep CDR (Content Disarm and Reconstruction) sanitizes files by removing potentially malicious content and reconstructing safe, usable versions, effectively preventing zero-day attacks.
- Proactive DLP (Data Loss Prevention) identifies and redacts or blocks sensitive information within files to help meet compliance requirements. **NOTE:** MetaDefender Storage Security does not process the redacted file; it only displays the detected sensitive data in a file.
- File-Based Vulnerability Assessment detects known vulnerabilities within software components.

MetaDefender Storage Security functions as the layer that integrates with your storage systems and manages the file processing workflow, while MetaDefender Core, with its various licensed engine packages, performs the actual threat detection, sanitization, and data protection tasks.

This architecture ensures that files are thoroughly inspected before they are stored or accessed, providing a comprehensive security layer for enterprise data. Deployment options may involve a self-hosted MetaDefender Core, a cloud-based MetaDefender Cloud instance (which includes Core functionalities as a service), or MetaDefender Core deployed via AMIs or containers.

Architecture & Components

MetaDefender Storage Security (MDSS) is built for flexibility. It uses containers, which let you customize and adapt your development to match your specific needs. Getting the sizing right is crucial for performance and reliability as your workload directly impacts sizing. Proper sizing ensures smooth operation. This guide will help you understand the key components and make informed decisions.



Shared Services

MDSS depends on the following stateful services to ensure high performance and data consistency:

- **PostgreSQL (Database)** – Stores configuration, job metadata, and system state. Proper sizing ensures transactional integrity and I/O performance at scale.
- **RabbitMQ (Message Broker)** – Coordinates communication across system components. It must be horizontally scalable to handle high volumes of concurrent file scan tasks.
- **Redis (Cache)** Provides low-latency access to ephemeral data and scan results. Effective caching reduces load on other components and speeds up workflow processing.

Why These Services Matter:

- **Scalability** – Each service must scale independently to accommodate varying workloads.

- **Reliability** – As stateful services, downtime or data loss can impact the entire system's operation.
- **Performance** – Throughput and responsiveness of the system depend on proper resource allocation for these services.

Planning your Deployment

MetaDefender Storage Security (MDSS) offers versatile deployment options to align with your organization's specific infrastructure and security requirements. This includes support for air-gapped environments. Understanding the different deployment models will help you choose the most suitable approach.

Regardless of the deployment type, make sure you have reviewed the **recommended system requirements** for MetaDefender Storage Security.

MetaDefender Storage Security can be deployed across various platforms:

- **Physical Servers** for direct hardware installations.
- **Virtualization Platforms** compatible with popular platforms like VMware, Hyper-V, and XenServer.
- Can be deployed on **Infrastructure as a Service** from major cloud providers such as AWS, Azure, and GCP.
- Supports containerized deployments in **Kubernetes** clusters.

The Basic and Advanced Deployment types can be broadly categorized based on how the shared services (database, message broker, and cache) are managed:

Deployments with Self-Hosted Shared Services

- Usage Cases
  - Shared services are segregated from the main MetaDefender Storage Security instance, often onto a single dedicated VM (Linux is preferred). This is suitable for allocating dedicated resources to these services. (Basic Deployment)
  - Each shared service is installed on separate instances to enhance reliability, scalability, and high availability, crucial for managing larger workloads. The key difference from the basic setup is the implementation of high availability for one or more services and potentially more advanced scalability features like database clustering (sharding) if required. (Advanced Deployment)
- High-Level Steps
  1. Prepare the system(s) by updating packages
  2. Deploy PostgreSQL (Database)
  3. Deploy RabbitMQ (Message Broker)
  4. Deploy Redis (Cache)
  5. Configure MetaDefender Storage Security to connect to these self-hosted shared services
  6. Start MetaDefender Storage Security

7. (For advanced deployments) Implement and configure scalability and high availability for the shared services

Deployments with Managed Shared Services

This model leverages cloud-provider-managed services for the database, message broker, and cache, reducing the operational overhead of managing these components yourself.

- Usage Scenarios
  - A single MetaDefender Storage Security instance utilizes managed cloud services for its shared components (Basic Deployment)
  - Multiple MetaDefender Storage Security instances are deployed, all connecting to the same managed cloud services. This enhances capacity, reliability, and high availability (Advanced Deployment)
- Characteristics
  - Easily deploy multiple MetaDefender Storage Security instances. Each new instance is configured to use the same managed shared services.
  - For deployments with multiple instances, a **load balancer** is recommended, especially for event-based, real-time scanning, to ensure high availability and distribute traffic.
    - Cloud - use the cloud provider's load balancing services.
    - On-Premises - manually deploy load balancers like NGINX, HAProxy, or Traefik.
  - Managed services are configured within MetaDefender Storage Security similarly to self-hosted ones, though specific terminology might vary by cloud provider.
  - Examples of Managed Services:
    - Database (PostgreSQL alternatives): Amazon RDS, Azure Database for PostgreSQL, Google Cloud SQL
    - Cache (Redis alternatives): AWS ElastiCache for Redis, Azure Cache for Redis
    - Message Broker (RabbitMQ alternatives): AWS Amazon MQ, Azure MP Cloud AMQP and Bitnami package for RabbitMQ in Azure MP.

Kubernetes Deployment

This approach involves deploying MetaDefender Storage Security within a Kubernetes cluster using a Helm chart.

- Prerequisites
  - An existing Kubernetes cluster (Managed Kubernetes Services like EKS, AKS, GKE are common for production, while self-managed Kubernetes offers more control

but requires more maintenance).

- For deployments using the OPSWAT-provided convenience script (`metadefenderk8s.sh`):
  - Familiarity with the chosen Cloud Service Provider (AWS or Azure)
  - An account with the CSP to create the necessary resources
  - Linux shell environment
  - Tools: Terraform, Helm, AWS-CLI (for AWS), Kubectl

- Deployment Method
  - The OPSWAT **convenience script** (`metadefenderk8s.sh`) is the simplest way to provision a Kubernetes cluster (if needed) and install MetaDefender Storage Security. It guides users through the required steps.

Choosing the right deployment type depends on your existing infrastructure, technical expertise, scalability needs, and budget.

Carefully evaluate these factors and the prerequisites for each model before proceeding with your MetaDefender Storage Security installation.

Sizing Guide

This table summarizes the various deployment options available for MDSS. It helps you understand the differences between each option and choose the one that best fits your needs.

		Small scale deployments	
Feature	**Basic Deployment (Single Instance)**	**Basic Deployment with Self-Hosted Shared Services**	**Basic Deployment with Managed Services**
Best for	*Small and predictable workloads*	*Small workloads, some flexibility, HA desired*	*Small workloads, with managed services*
Scalability	NO	NO	NO
High Availability	NO	NO	PARTIAL
Auto-Scale Ready	NO	NO	NO
Files / hour (Objects / hour)	**5,000** (125,000)	**20,000** (500,000)	**50,000** (1,250,000)
Recommended MD Core #	2-4	4 or more	4 or more
Recommended MDSS #	1	1	1
Infrastructure complexity	1/5	4/5	3/5

	Medium scale deployments		Large scale deployments	
Feature	**Advanced Deployment with Self-Hosted Shared Services**	**Advanced Deployment with Managed Services**	**Cloud Deployment with Kubernetes (k8s)**	**MDSS Cloud (SaaS)**
Best for	*Medium workloads, manual scaling*	*Medium to Large workloads, no auto-scaling*	*Large workloads, dynamic scaling, cost-optimized*	Scalable, secure, efficient cloud-based storage security solution
Scalability	YES	YES	YES	YES
High Availability	YES	YES	YES	YES
Auto-Scale Ready	NO	NO	YES	YES
Files / hour (Objects / hour)	**100,000** (2,500,000)	**100,000** (2,500,000)	**100,000** or more	**500,000** or more
Recommended MD Core #	4 or more	4 or more	Tailored per customer	Tailored per customer
Recommended MDSS #	2 or more	2 or more	Tailored per customer	Tailored per customer
Infrastructure complexity	5/5	4/5	1/5	1/5

How we tested and what it means

We tested MDSS with a mix of everyday files, like documents, images, and videos, to get realistic performance numbers. We started small and then scaled up to see how it handled larger workloads. However, remember that these are just guidelines. Your actual performance will depend on your files, network, and hardware. For critical systems, it's always best to test it out yourself.

The numbers in the deployment table are based on rigorous testing using a diverse set of real-world files. We didn't just use one type of file; we included a mix of:

- **Documents** - PDFs, Word files (DOC/X), Excel files (XLS/X), PowerPoint files (PPT/X)
- **Executables** - EXEs, MSIs (installation files)
- **Images -** BMP, JPG, PNG
- **Media** - MP3, MP4 (audio and video)

- **Text and Archives** - various text files and compressed archives

The Numbers Explained

- **our starting point was 5,000 files**, totaling 7,728.5 MB. The average file size was 1.55 MB.
- to see how MDSS handles **bigger workloads**, we replicated this dataset to create scenarios with 50,000 files and over 100,000 files. This helped us understand performance scaling.

The numbers in the table are meant to be *guidelines*. Real-world performance can vary due to:

- **File Type Variations** - some file types are processed faster than others.
- **Network Speed** - a slow network can impact throughput.
- **Hardware Specs** - the performance of your servers matters.

For mission-critical applications we strongly recommend running your own performance tests (benchmarks) in your specific environment *before* deploying MDSS in production. This will give you the most accurate picture of how MDSS will perform with your unique setup.

General System Requirements

This page outlines the necessary prerequisites for deploying MetaDefender Storage Security (MDSS), covering supported operating systems, system requirements, and specific details for Unix and Windows deployments.

Operating system-specific system requirements are available at:

- Unix deployment
- Windows deployment

Prerequisites

Hardware Configurations

Depending on your deployment type, please ensure your hardware meets the following minimum requirements:

Basic Deployment (Minimum System Requirements)

Hardware	MDSS Dedicated Instance	MDSS + MD Core Shared Instance
CPU	16 cores (vCPUs)	32 cores (vCPUs)
RAM	32 GB	64 GB
Free Disk Space	500 GB*	900 GB*

Advanced Deployment (Minimum System Requirements)

For advanced usage, particularly when you intend to process a very large number of files, it is not recommended to run MD Core on the same machine as MDSS.

Hardware	MDSS Dedicated Instance	PostgreSQL Database Instance
CPU	16 cores (vCPUs)	16 cores (vCPUs)
RAM	32 GB	32 GB
Free Disk Space	150 GB*	380 GB*

*** Disk Space Planning (applicable to all deployments)**

> **Info**

> Please note that the database disk space requirements outlined in this document are calculated based on processing **10 million files***.
>
> **Important:** If you anticipate discovering and processing more than 10 million files, you will need to allocate additional disk space for the database proportionally.
>
> The disk space requirements for the application and logs remain constant regardless of the number of files processed.
>
> If you need assistance calculating the appropriate database disk size for your specific file volume, please don't hesitate to reach out.
>
> *Each file discovery creates a separate database entry, even if it's the same file.

Careful disk space planning is crucial for the optimal performance and reliability of the MetaDefender Storage Security platform.

- Base Installation (database excluded):
  - MDSS Application: **20 GB**
  - Default install path:
    - Windows: `C:\Program Files\OPSWAT\MetaDefender Storage Security`
    - Linux: `/etc/mdss`
- Operational Requirements
  - A minimum of **100 GB** is recommended for **log retention and analysis**
    - Default install path:
      - Windows:
        - `C:\Program Files\OPSWAT\MetaDefender Storage Security\logs`
        - `C:\Windows\System32\opswat.mdss.windows.service`
        - Installer logs: `C:\Users\<user>\AppData\Local\Temp\`
      - Linux: `/var/log/mdss` and `/etc/mdss/sevices_logs`
  - For the various MDSS services (database included), an additional **380 GB** is required
    - Default install path:
      - Windows: `C:\Program Files\OPSWAT\MetaDefender Storage Security\services`
      - Linux: `/etc/mdss`
- This heavily depends on the actual dataset and configuration in a production environment.
- More details on the exact logging paths can be found at Logs location

Note: Insufficient disk space may negatively impact system performance and reliability, particularly during high-volume remediation operations. Regular monitoring of disk usage

is strongly advised to ensure optimal system performance.

Unix deployment

Supported Operating Systems

Distribution	Supported versions	Architecture
CentOS Stream	9-x, 10-x (latest)	x86_64 (64-bit)
Red Hat Enterprise Linux **(podman only)**	7.x, 8.x, 9.x (latest)	x86_64 (64-bit)
Rocky Linux **(podman only)**	9.x, 10.x (latest)	x86_64 (64-bit)
Debian	10.x, 11.x, 12.x (latest)	x86_64 (64-bit)
Ubuntu	18.x, 19.x, 20.x, 21.x, 22.x, 23.x, 24.x (latest)	x86_64 (64-bit)
Amazon Linux	2	x86_64 (64-bit)

Installation details

The default installation path for MetaDefender Storage Security resources is the `/etc/mdss` folder.

The installation package will automatically install the following dependencies if they are not already present on the system:

Debian / Ubuntu	Red Hat Enterprise / CentOS
- `curl` - `openssl` (uses the default version on the host) - `openssl` (the container uses version 3.2.0) - `ca-certificates` - `sudo` - `jq` - `iproute2` - `apt-utils` - `gnupg-agent` - `apt-transport-https` - `software-properties-common`	- `curl` - `openssl` (uses the default version on the host) - `openssl` (the container uses version 3.2.0) - `ca-certificates` - `sudo` - `jq` - `iproute` - `yum-utils` - `gnupg2` - `wget` - `device-mapper-persistent-data` - `lvm2`

Installation components

MetaDefender Storage Security automatically deploys the following components:

Name	Version	Type
Docker Engine	system defined*	Containerization technology
Docker Compose	system defined*	Container orchestration
PostgreSQL	v17.0	Database
RabbitMQ	v4.3.0	Message broker
NGINX	v1.29.2	Web server
Redis	v8.6.0-alpine	Data Cache

Our system uses the existing Docker version if available. If not, it automatically downloads the latest stable version using the docker-install script.

Windows deployment

Supported Operating Systems

OS	Version	Architecture
Windows Server	2019, 2022, 2025 (latest)	64-bit

Operating System Requirements and Licensing Considerations

Microsoft's licensing terms prohibit the use of Windows Desktop operating systems in server environments. As a result, MetaDefender Storage Security is not compatible with Windows Desktop editions.

For organizations concerned about Windows Server licensing costs, we recommend deploying on Unix-based systems instead. Unix platforms deliver enterprise-level reliability and performance without additional licensing fees.

Port Requirements

The following ports must be available for our services to listen on.

Please ensure that no other services are using these ports before starting the installation. NGINX port can be customized during the installation process.

> For the MDSS Windows deployment, every port in the below table is **TCP**, and the rule you need is an **inbound "Allow" rule** for each so the components can talk to each other and clients can reach the services. Open these before installing:

Component	Port
PostgreSQL	5432
RabbitMQ	5672
NGINX	80 (and 443 if SSL enabled)
API Gateway	8005
Licensing Service	5001
SMB Service	6002, 6003, 6004, 6005, 6006, 7002, 7003, 7004, 7005, 7006
SFTP Service	5003
NFS Service	5004

Installation components

MetaDefender Storage Security automatically deploys the following components:

Name	Version	Type
PostgreSQL	v17.0	Database
RabbitMQ	v4.3.0	Message Broker
NGINX	v1.29.2	Web Server
Garnet	v1.1.8	Data Cache (Redis compatible)

Licensing Model

Licensing for MetaDefender Storage Security is directly integrated with MetaDefender Core, as both solutions are delivered together. The licensing framework includes several key elements:

Licenses are provided through a subscription model, with agreements structured for annual or multi-year terms.

Pricing details, entitlements, and usage terms are outlined in a formal agreement with OPSWAT. For enterprise-level implementations, tailored quotes are provided to align with organisational requirements.

Activation is managed via a license key linked to a unique deployment ID generated by the associated MetaDefender Core instance. Both online and offline activation options are available.

A valid and appropriately tiered MetaDefender Core license is required to support MetaDefender Storage Security. This includes coverage for necessary engine packages such as anti-malware engines, Deep CDR, and Proactive DLP to meet the intended security standards.

A Bring Your Own License (BYOL) model is supported for deployments using cloud marketplaces like AWS Marketplace. In this scenario, customers acquire the license directly from OPSWAT and apply it within the cloud platform.

Organizations planning to implement MetaDefender Storage Security must consult OPSWAT or their sales representatives to receive personalized pricing and licensing guidance based on deployment size, security objectives, and selected engine packages.

MetaDefender Storage Security Documentation

MetaDefender Storage Security (MDSS) protects your storage against malware, zero-day threats, and hidden sensitive data. It scans files at rest and in real time across cloud and on-premises storage, using multiscanning with 30+ anti-malware engines, Deep CDR (Content Disarm and Reconstruction), Proactive DLP, and vulnerability assessment.

Use this documentation to plan, deploy, size, license, and operate MDSS across supported storage targets including Amazon S3, Azure Blob, Dell EMC Isilon, NetApp, SMB/CIFS and NFS shares, and Kubernetes-based cloud deployments.

What you'll find here

- Overview and how MDSS fits into an OPSWAT MetaDefender deployment
- Architecture and components, including MD Core scanning backend and shared services
- Planning your deployment and choosing a deployment model (basic, advanced, managed, self-hosted, or cloud/Kubernetes)
- Sizing guide for on-demand and real-time scanning, instance counts, and machine specs
- General system requirements and supported storage integrations
- Licensing model

Choosing your deployment model

MDSS supports basic and advanced deployments, with either managed or self-hosted shared services, plus a Kubernetes (k8s) option for cloud. Pick the model that matches your scale, storage type, and operational preferences. See the deployment sections in the left menu for step-by-step guidance.

Download the full manual

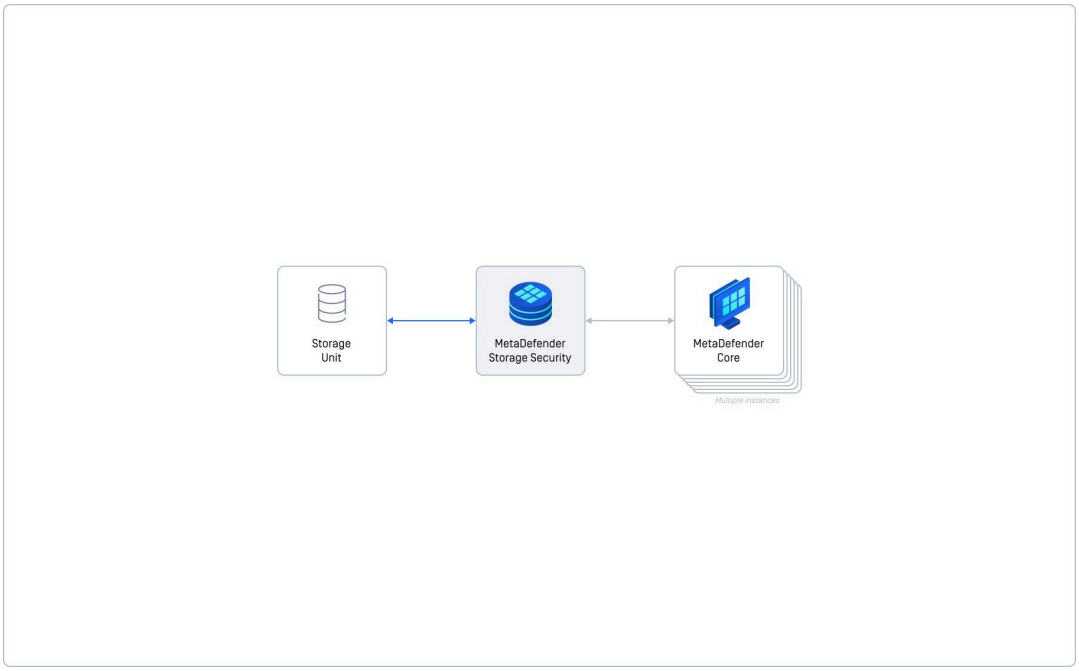
Prefer a single file? Download link for the complete guide in PDF format for OPSWAT MetaDefender Storage Security (MDSS) 4.5.x Documentation

Choosing your deployment model

Basic Deployment

The basic deployment is the fastest way to get **MetaDefender Storage Security (MDSS)** up and running. All system components — MDSS, Metadefender Core, and shared services — are installed on a single machine.

Imagine running MDSS on a single computer. It's fast to set up and good for small tasks. But if you need to handle a lot of work or can't afford any downtime, this isn't the right choice.



Suitable For

- Small workloads (perfect for testing or light usage)
- Quick setup with minimal configuration

Key Points

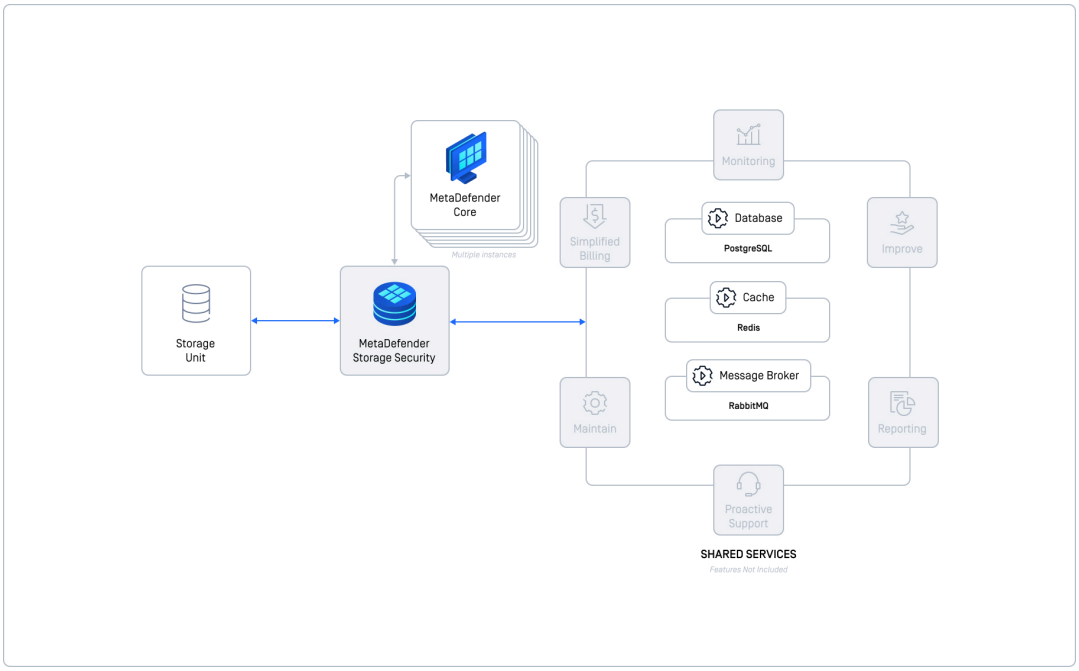
- All components run on one server.
- You can't add more servers to handle more load.
- If the server goes down, MDSS goes down.
- You can still reconfigure or upgrade MDSS on this setup.

Important Considerations

- Performance will vary depending on your server and file types.
- This setup is *not recommended* for live, critical systems where you need high availability or the ability to handle a lot of data.
- You get simplicity, but you lose the ability to scale and ensure continuous operation.

Basic Deployment with Self-Hosted Shared Services

This deployment takes the basic setup a step further by separating the core services (database, cache, and message broker) from the main MDSS instance. This gives you more control and improves performance, but adds complexity.



Instead of running everything on one machine, you're now running the database, memory cache, and communication hub on separate machines. This gives you more control and better performance, but you're also responsible for setting everything up and keeping it running smoothly.

Suitable For

- **Small to Medium Workloads** as it can handle up to 20,000 files per hour with proper resources.
- **Organizations with IT Expertise** as it requires in-house expertise to manage the infrastructure.

Key Components & Their Roles

- PostgreSQL (Database) stores data.
- Redis (Cache) speeds up data access.
- RabbitMQ (Message Broker) manages communication between components.

Key Points

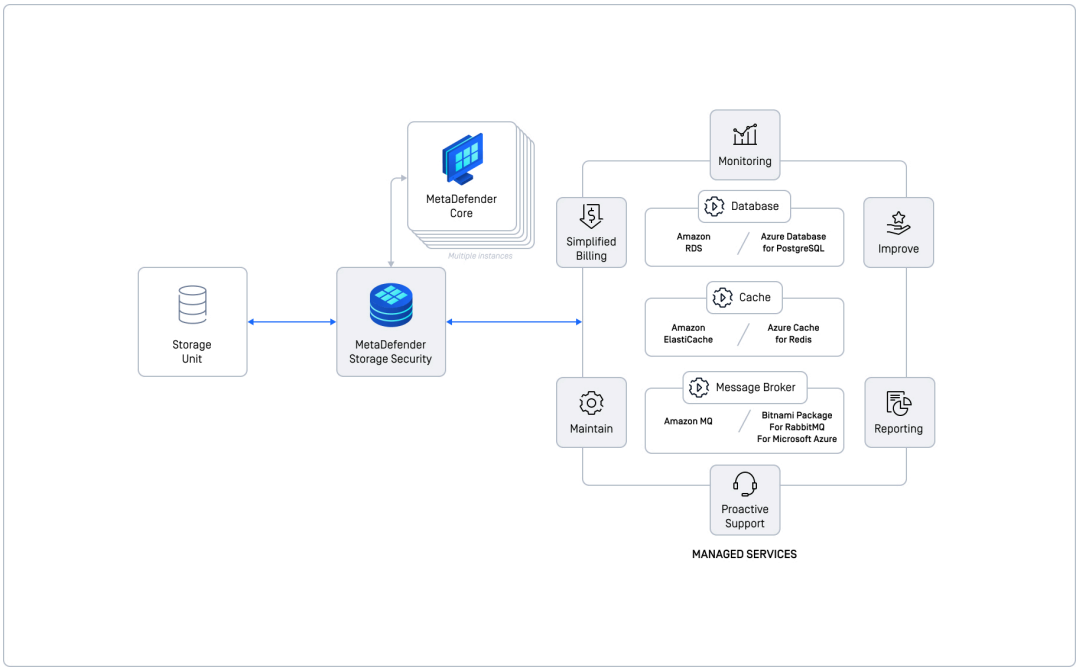
- Each shared service runs on its own server/VM.
- You are responsible for installing, configuring, and maintaining these services.
- Requires more technical knowledge and effort.
- Can handle larger workloads compared to a single instance.
- You can scale individual services, but it's not as seamless as a fully cloud-native setup.

Important Considerations

- You need to configure replication for high availability.
- Make sure sufficient resources are allocated to each shared service.
- Running all shared services on a single VM defeats the purpose of this setup and impacts performance.
- While better than a single instance, it's still possible to have single points of failure if not configured correctly.

Basic Deployment with Managed Services

Instead of managing the database, cache, and message broker yourself, you let the cloud provider handle it. You focus on setting up and scaling MDSS, while the cloud takes care of the underlying infrastructure. Think of it as renting managed services instead of buying and maintaining them yourself.



This deployment builds on the basic model by using *managed cloud services* for the shared components (database, cache, message broker). This means you leverage the cloud provider's expertise to handle the infrastructure, simplifying your setup.

Suitable For

- Cloud-First Organizations, organizations heavily reliant on cloud infrastructure.
- Organizations Seeking Simplicity as it reduces the burden of managing infrastructure.
- Workloads up to 50,000 Files/Hour - achievable with sufficient cloud resources and MDSS and MD Core instances.

Key Advantages

- Cloud provider handles maintenance, monitoring, and scaling of shared services.
- Ideal for organizations already using cloud services like AWS, Azure, or Google Cloud.
- Reduces operational overhead compared to self-hosting.
- Benefits from cloud-provided features like enhanced monitoring, reporting, and proactive support.

Example: Amazon AWS Integration

- Database - use Amazon RDS.
- Cache - use Amazon ElastiCache for Redis.
- Message Broker - use Amazon MQ.

Adaptable to Other Clouds

This approach can be adapted to Azure and Google Cloud, using their respective managed services. Please follow this article for more information regarding integrating with various cloud providers.

Key Points

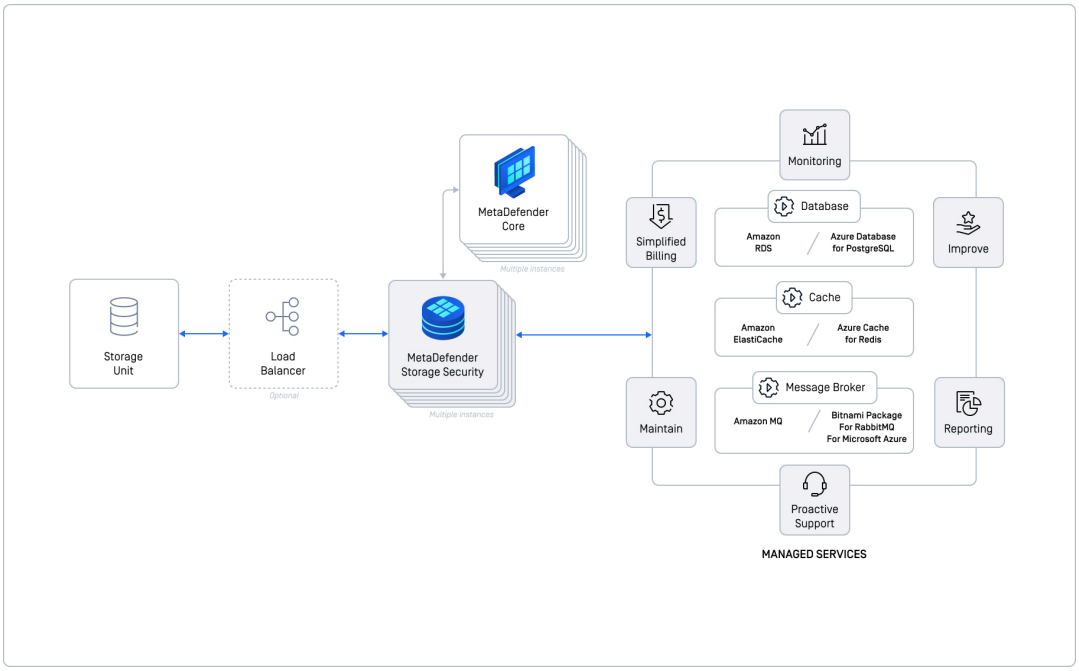
- You don't manage the shared services directly.
- Your primary focus is on configuring and scaling MDSS itself.
- Leverage the cloud provider's scalability for shared services.
- Benefit from the cloud provider's redundancy and reliability.

Important Considerations

- Managed services have associated cloud costs, which need to be factored in.
- Requires understanding cloud service integrations and their complexity

Advanced Deployment with Managed Services

This setup uses **multiple** MetaDefender Storage Security (MDSS) instances and leverages your cloud provider's managed services for the database, cache, and message broker. It's designed for high throughput and simplifies management.



Imagine having a team of experts (your cloud provider) handle the backend infrastructure, allowing you to focus on scaling and managing your MDSS instances. This setup is powerful and efficient for high-volume workloads.

Suitable For

- Organizations processing a lot of files.
- Cloud-Centric Businesses who already leveraging cloud infrastructure.

Why It's Powerful

- Multiple MDSS instances handle large workloads efficiently.
- Your cloud provider handles the underlying infrastructure (database, etc.).
- Ideal if you're already using cloud services.
- Get monitoring, reporting, and proactive support from your cloud provider.

Example (AWS)

- Database: use Amazon RDS
- Cache: use Amazon ElastiCache
- Message Broker: use Amazon MQ

Adaptable to Azure & Google Cloud: You can use similar services from those providers. For more information on integrating with various cloud providers, please follow this page: CSP Deployment Overview.

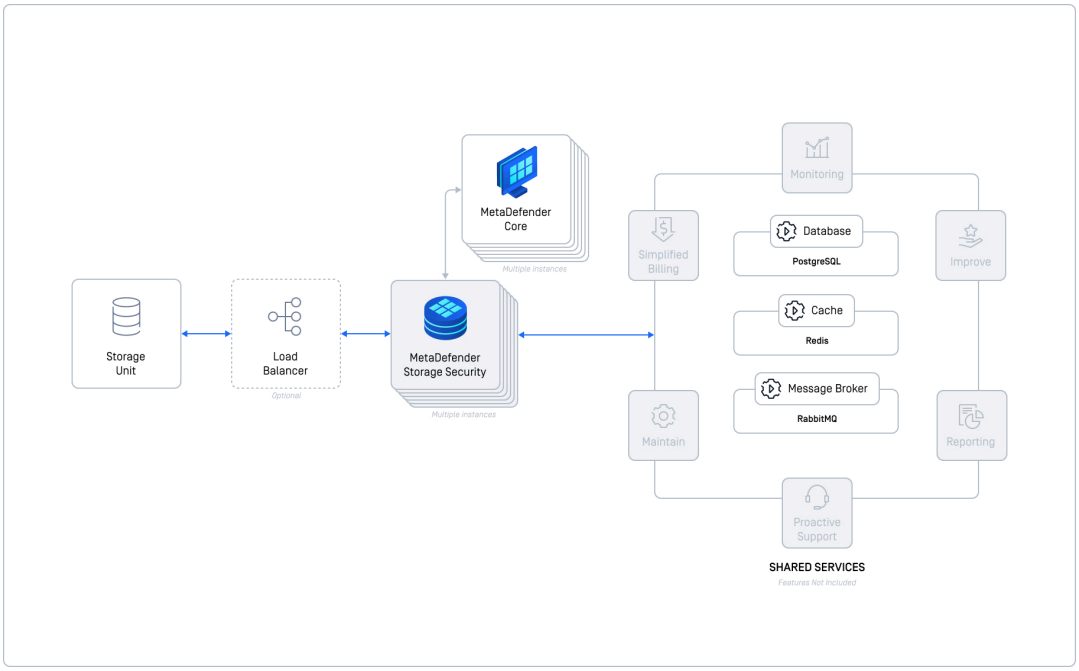
Key Benefits

- You manage the MDSS instances, not the database, cache, etc.
- Cloud providers ensure redundancy and availability.
- Tested to handle 100,000 files/hour (with 2+ MDSS and 4+ MDSS Core instances).

Important Note: Cloud managed services have associated costs.

Advanced Deployment with Self-Hosted Shared Services

This deployment is for high-performance needs, using multiple MDSS and MD Core instances and self-hosted shared services (database, cache, message broker). It's significantly more complex than the basic setups but offers superior performance and reliability.



This setup is like building a powerful engine. You're running multiple MDSS and MD Cores and managing the database, cache, and communication hub yourself. This gives you high performance, but it's also more complex to set up and maintain.

Suitable For

- High-Throughput Environments, organizations processing large volumes of files.
- Organizations with Strong IT Infrastructure as it requires in-house expertise to manage the complexity.

Key Components & Their Roles

- Multiple MDSS Core Instances - allows parallel processing for higher throughput.
- PostgreSQL (Database) - stores data.
- Redis (Cache) - speeds up data access.
- RabbitMQ (Message Broker) - manages communication between components.

Key Points

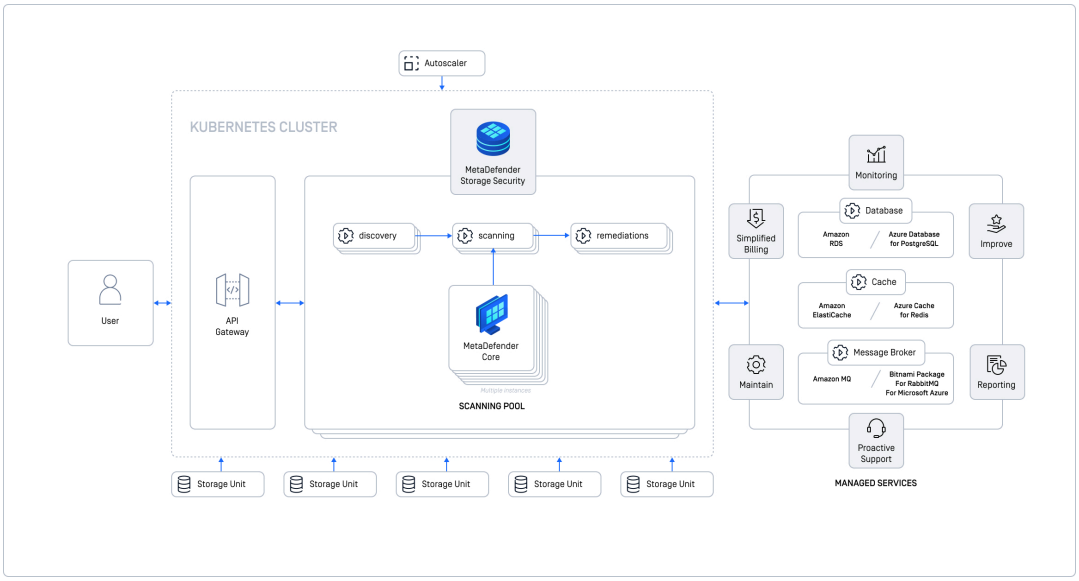
- Requires more planning and technical expertise.
- Can handle up to 100,000 files per hour with sufficient resources.
- You are responsible for installing, configuring, and maintaining all components.
- Allows scaling through multiple MDSS Core instances and shared services.
- Achieved through database replication and careful configuration.

Important Considerations

- Requires significant hardware resources for all components.
- Effective monitoring is essential due to the increased complexity.
- While better than basic setups, careful planning is needed to avoid single points of failure.
- Our testing showed 2 MDSS instances with 4 MDSS Core instances yielded substantial performance improvements.
- Once all services are deployed and ready to be used, please follow Installation Methods to connect MDSS to them.

Cloud Deployment with Kubernetes (k8s)

This is our recommended option for maximum scalability, high availability, and handling large volumes of data. It uses Kubernetes to automate deployment, scaling, and management of MDSS in a cloud environment.



Kubernetes is like an automated control system for your cloud deployment. It lets you scale MDSS easily, ensures it stays running, and optimizes resource usage. If you need high performance and availability, this is the way to go.

Suitable For

- Organizations handling massive amounts of data.
- Organizations Prioritizing High Availability, needing minimal downtime.
- Cloud-Savvy Teams familiar with Kubernetes.

Why Use Kubernetes?

- Dynamically adjust resources based on workload.
- Distributes MDSS across multiple nodes to minimize downtime.
- Optimize resource allocation for each component.
- Kubernetes handles load balancing, autoscaling, and more.

Key Components & Cloud Integration

- Kubernetes (k8s) orchestrates the deployment.
- Managed Cloud Services for database, cache, message broker (e.g., AWS EKS, Azure AKS, Google GKE).

Examples

- For AWS - use Amazon RDS, Amazon ElastiCache, Amazon MQ
- Users of Azure or Google Cloud can adapt this model to employ their respective managed services with Azure Kubernetes Service (AKS) or Google Kubernetes Engine (GKE). For detailed guidance on integrating with various cloud providers, please follow:
  - Azure AKS
  - Azure Database for PostgreSQL
  - Azure Cache for Redis
  - Google Kubernetes Engine (GKE)

Key Points

- Kubernetes automates many deployment tasks.
- Easily scale up or down as needed.
- Kubernetes ensures high availability.
- Integrates with cloud monitoring, reporting, etc.

Important Considerations

- Requires understanding Kubernetes concepts.
- You need a Kubernetes cluster set up before deploying MDSS.
- MDSS is deployed using a Helm chart available on GitHub.

Installation

Types of deployment

Whether you require the rapid scalability of the cloud, the control of on-premises infrastructure, or the simplicity of SaaS, MetaDefender Storage Security ensures seamless integration and robust protection across all platforms.

Pre-Deployment Checklist

Before continue with the deployment of MetaDefender Storage Security

1. Verify prerequisites met (System, Network, Database).
2. Gather necessary credentials and OPSWAT license (Service accounts, API keys).
3. Confirm chosen deployment architecture.

Deployment Options

Aiming to facilitate the deployments of the OPSWAT´s products to different environments, there are documented examples of architectures and how to deploy them for the following options.

- Deploy using Cloud Service Providers services
- Deploy to your On-Premise Deployment Overview
- Deploy using containerized technologies in all environments

Deploy to cloud service providers

CSP Deployment Overview

This section explains the various deployment options for MetaDefender Storage Security using services from Cloud Service Providers (CSPs) such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).

Before consulting the documentation specific to each CSP, please review the following general documents:

- Architecture Examples in CSPs illustrate different deployment options within each CSP.
- General Cloud Considerations cover access and configuration considerations applicable to cloud environments.
- Using OPSWAT´s image from CSPs Marketplace, detail using the pre-configured image designed to facilitate Proof of Concepts (POCs).

This guide also includes dedicated sections for the main Cloud Service Providers:

- AWS Deployment
- Azure Deployment

Architecture Examples in CSPs

This page outlines the recommended architecture for running MetaDefender Storage Security (MDSS) with any Cloud Service Provider (CSP).

We provide diagrams for AWS, Azure, and GCP, where our product is available in their respective marketplaces. However, our products are cloud-agnostic and can be deployed to any CSP.

Infrastructure Options for MetaDefender Storage Security using Compute Services

The appropriate infrastructure will vary depending on the number of instances where MetaDefender Storage Security will be installed.

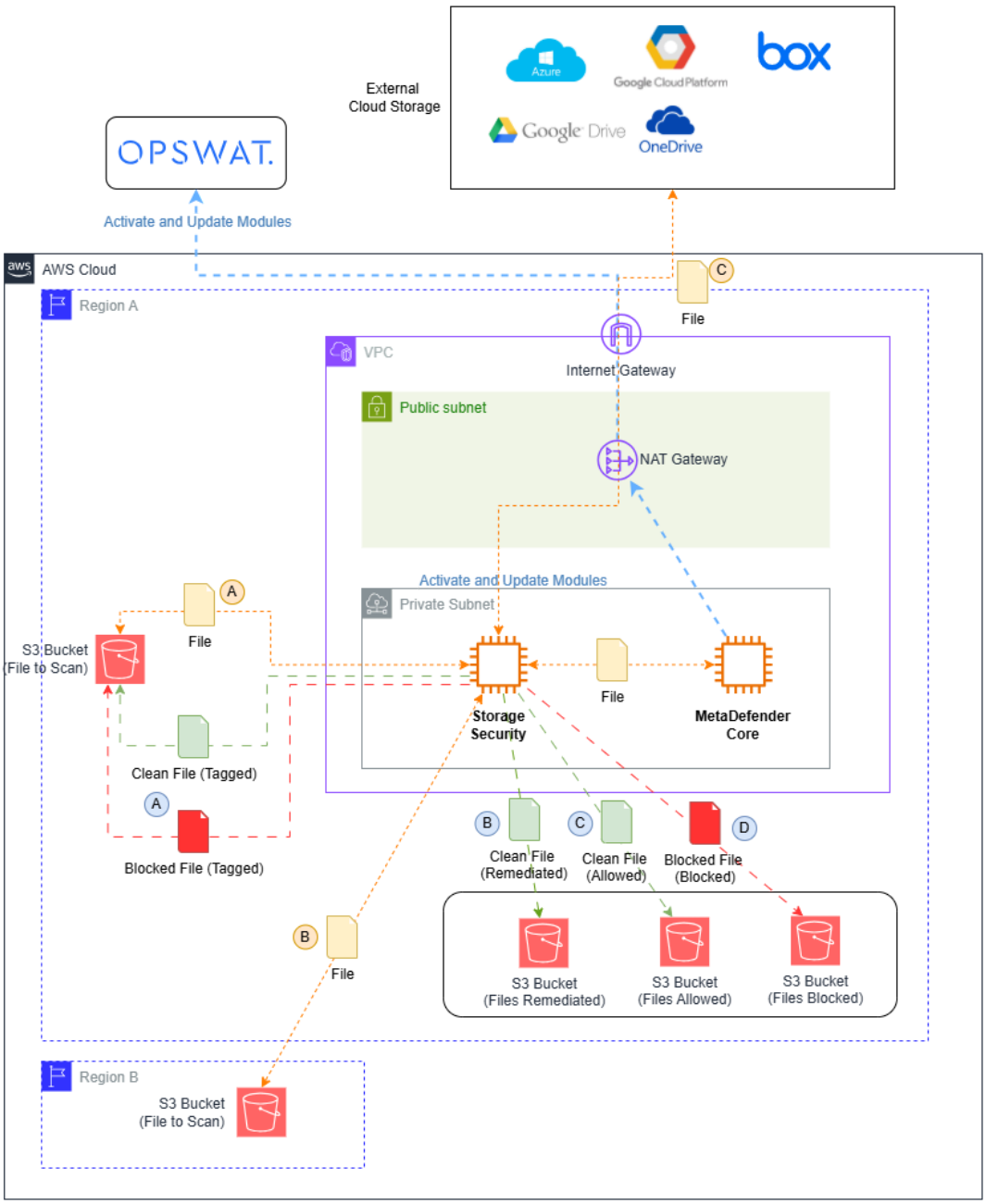
Options:

1. Single Instance
2. Multi-Instance with Autoscaling

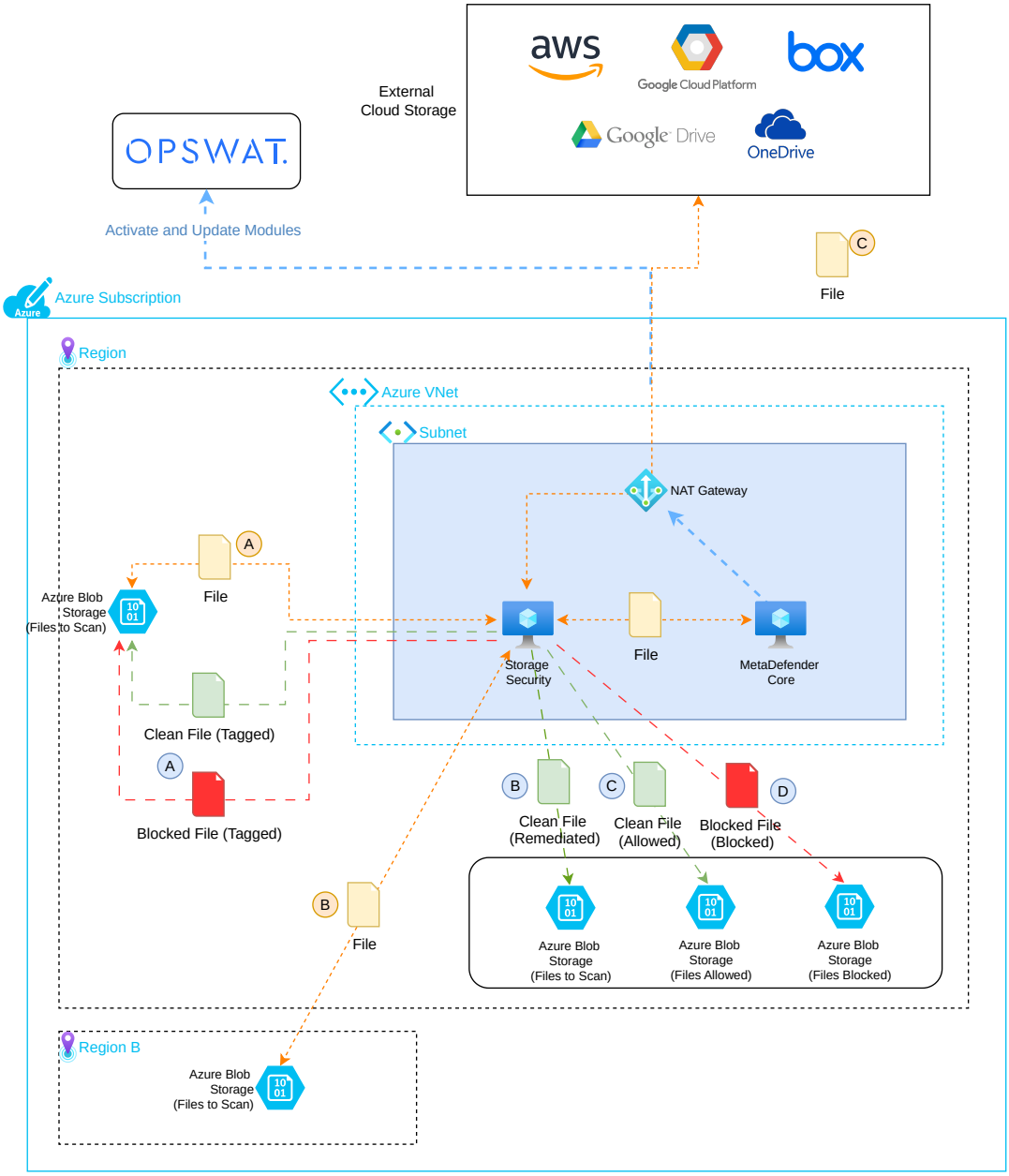
Single Instance

To proceed, select the tab corresponding to the CSP where you intend to deploy MetaDefender Storage Security.

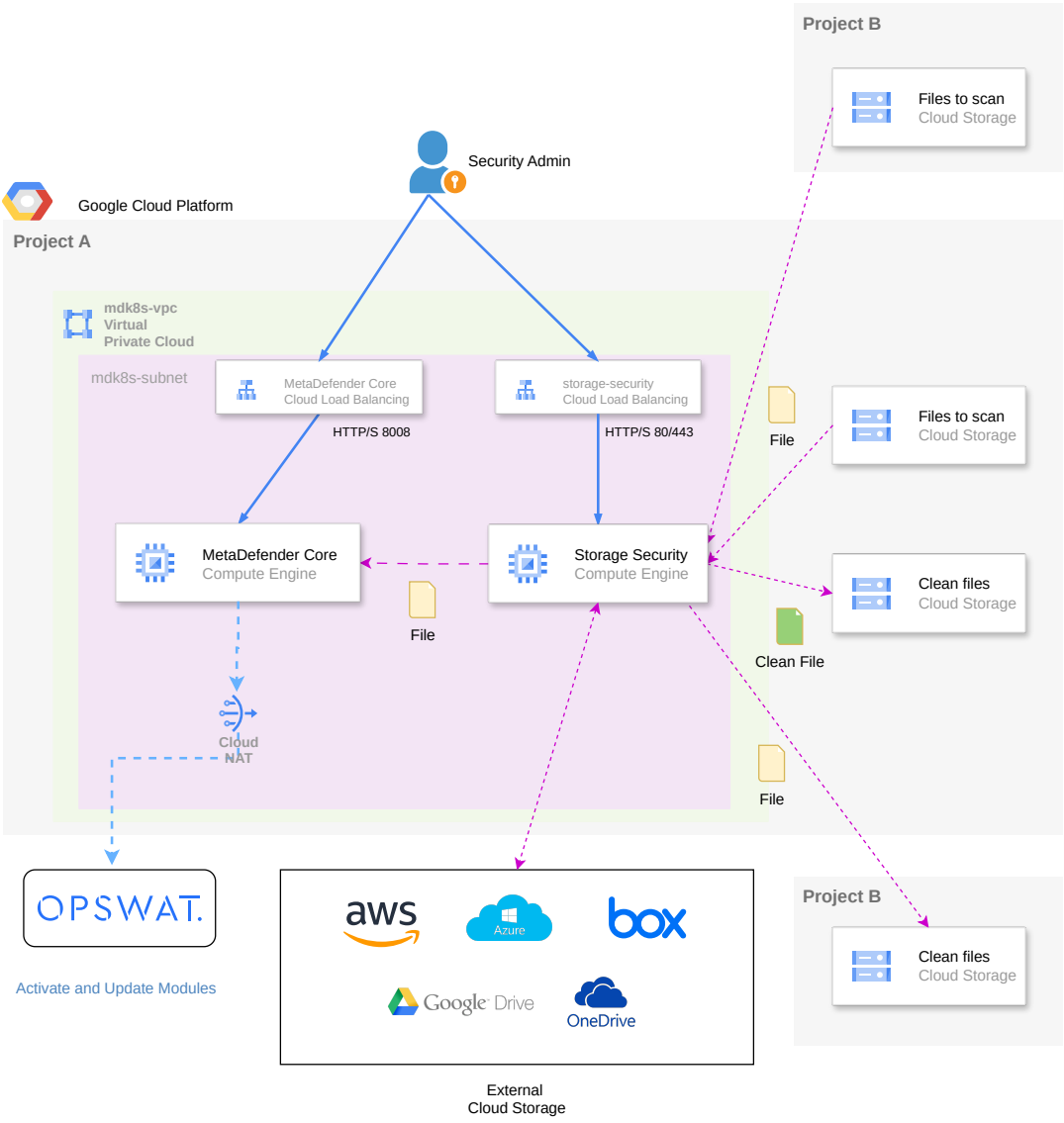
AWS



Azure


External
Cloud Storage
aws
Google Cloud Platform
box
Google Drive
OneDrive
OPSWAT.
Activate and Update Modules
C
File
Azure Subscription
Region
Azure VNet
Subnet
NAT Gateway
A
File
Azure Blob
Storage
(Files to Scan)
Storage
Security
File
MetaDefender
Core
Clean File (Tagged)
A
Blocked File (Tagged)
B
Clean File
(Remediated)
C
Clean File
(Allowed)
Blocked File
(Blocked)
D
B
File
Azure Blob
Storage
(Files to Scan)
Azure Blob
Storage
(Files Allowed)
Azure Blob
Storage
(Files Blocked)
Region B
Azure Blob
Storage
(Files to Scan)

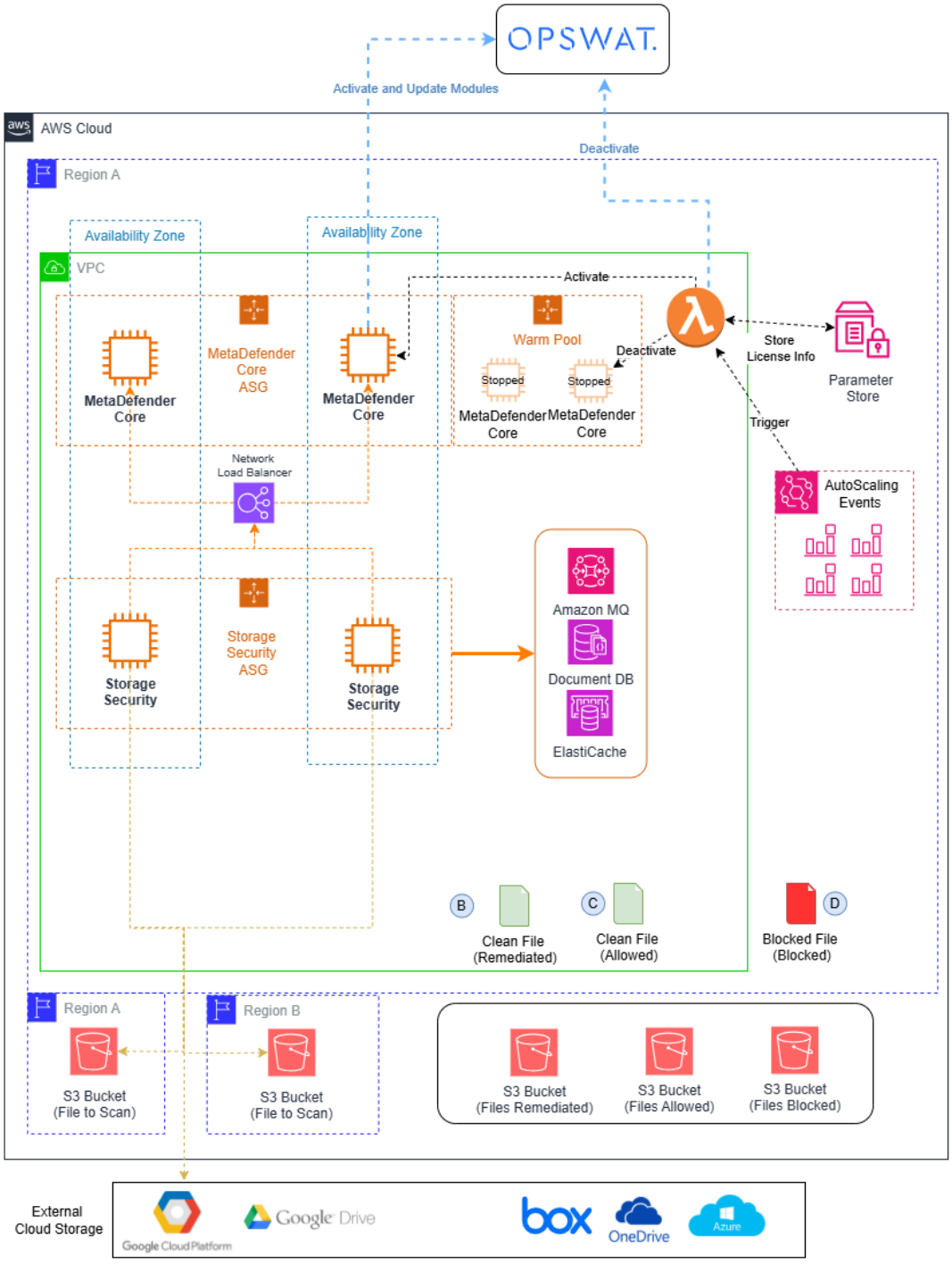
GCP



Multi-Instance with Autoscaling

Select the tab for the CSP where you want to deploy MetaDefender Storage Security.

AWS



Infrastructure Options for MetaDefender Storage Security using Container Services

The possible infrastructure **varies** depending on the Cloud services used for hosting MetaDefender Storage Security and how the **required third-party tools** are provisioned.

Options:

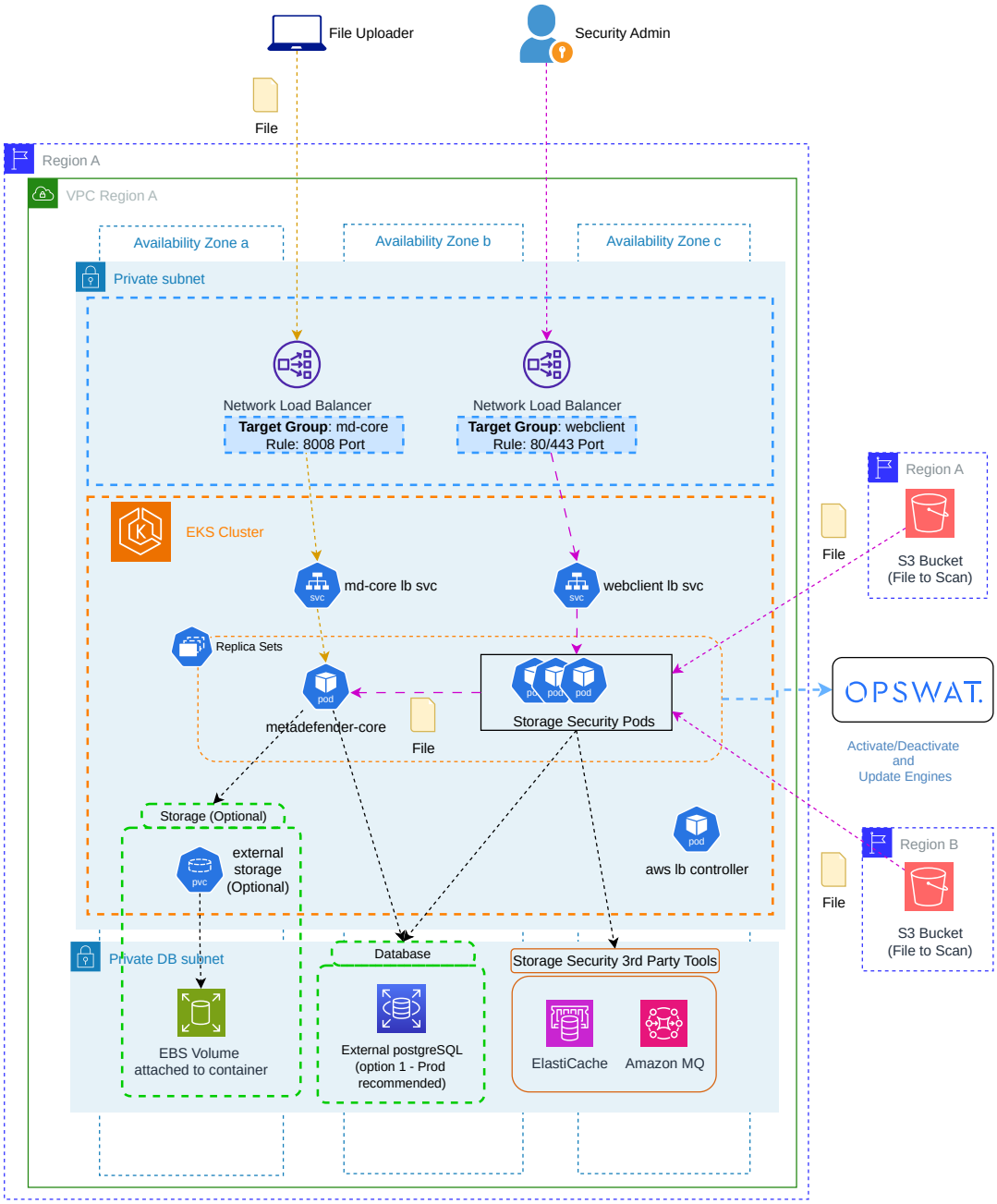
1. Kubernetes Cluster with **Customer-Managed** Worker Nodes, utilizing either a Cloud PostgreSQL Service or **third-party tools as Pods**.
2. Kubernetes Cluster with **CSP-Managed** Worker Nodes, utilizing a Cloud PostgreSQL Service

Customer Managed Worker Nodes

Select the **tab** for the CSP where you want to deploy MetaDefender Storage Security.

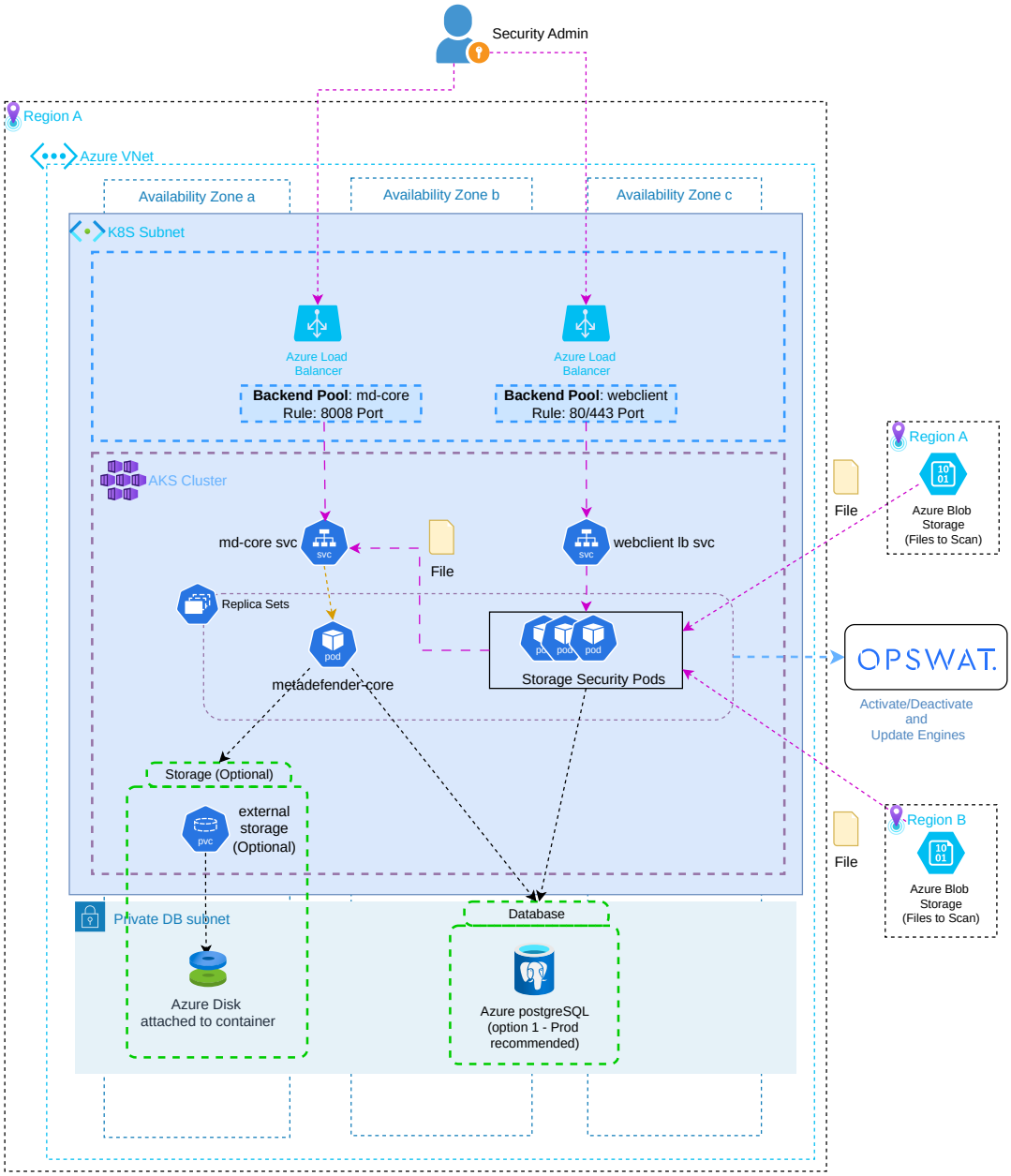
AWS

EC2 Instances + AWS Document DB or 3rd Party tools as Pod



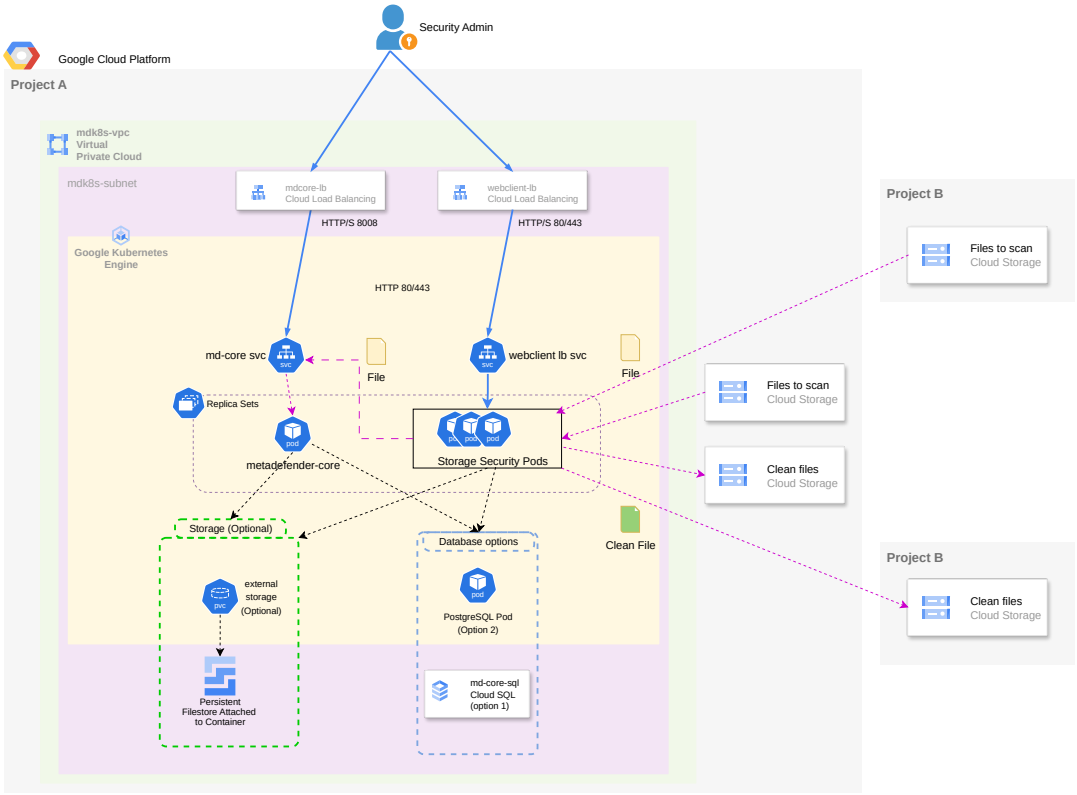
Azure

Azure VM (Worker Nodes) + Azure PostgreSQL DB Service or 3rd Party tools as Pod



GCP

Google Compute Engines Instances (Worker Nodes) + Google Cloud SQL or 3rd Party tools as Pod



CSP-Managed Worker Nodes

Above examples include **AWS Fargate or Azure Container Apps options for computing.**

These are serverless compute engines for containers that allow you to run containerized applications without managing the underlying infrastructure.

These services run containers with certain **limitations**, such as CPU limits per instance or ephemeral storage, which may be required for some Linux packages.

Please check the **system requirements** before choosing this architecture.

> **IMPORTANT
>
> We recommend deploying a database service from your Cloud Service Provider (CSP) for MetaDefender Core and MetaDefender Storage Security.**

General Cloud Considerations

When deploying to any Cloud Service Provider (CSP), consider these general recommendations:

Roles/Permissions

The Principle of Least Privilege (PoLP) is a foundational cybersecurity concept. It entails granting users, applications, and systems only the minimum access necessary to perform their tasks.

This approach minimizes the potential attack surface, mitigates risks associated with insider threats, and helps prevent privilege creep. When deploying OPSWAT products, **OPSWAT recommends** adhering to this principle.

Regarding access to applications or API endpoints, generate **strong passwords** for UI access.

Store the **API keys** required to access the API endpoints of the various products in a secure secrets manager.

VPC/Networking

OPSWAT recommends following networking best practices when deploying products:

- Multi-AZ Deployment
  - Distribute resources across multiple Availability Zones (AZs) to enhance fault tolerance and availability. OPSWAT products are designed to run in different AZs simultaneously.
- Security Groups
  - These act as virtual firewalls to control inbound and outbound traffic. Follow the system requirements for each OPSWAT product to open the necessary ports.
- IP Address Planning
  - Allocate CIDR blocks thoughtfully to avoid overlaps, especially when integrating with on-premises networks.
- Subnet Segmentation
  - Use distinct subnets to separate public-facing resources (MDSS UI) from private resources (MDSS PostgreSql database server).

Using OPSWAT´s image from CSPs Marketplace

Usage of image published in CSPs Marketplaces

OPSWAT has published images of MetaDefender Storage Security in **AWS, Azure and GCP** only **Linux OS**. OPSWAT provides a sample AMI (updated on a regular cadence).

> **Info**

> It is recommended for the customer to **run only POCs** as it is configured with the default options.

For production cases it is recommended to generate an image, after following the installation steps as in On-Premise Deployment. This process is always good to get familiar with the product and configure it to be adapted to the customer use case.

> **Info**
>
> In case the image published to the marketplace with the default configuration works for the customer, the overall and ongoing responsibility of the OS security patch status for that AMI is with the customer.

CSPs Marketplace Images

AWS

- MetaDefender Storage Security on Linux

Azure

- MetaDefender Storage Security on Linux

Google Cloud

- MetaDefender Storage Security – Marketplace – OPSWAT Public – Google Cloud console

AWS Deployment

This Deployment Guide provides step-by-step instructions for deploying MetaDefender Storage Security on Amazon Web Services (AWS) infrastructure.

This guide is intended for IT infrastructure architects, administrators, and DevOps professionals seeking to prevent malicious traffic from entering their AWS Cloud environment. It outlines how MetaDefender Core enhances threat prevention by inspecting uploaded productivity files and identifying known vulnerabilities in running services, applications, and unpatched operating systems deployed within AWS.

MetaDefender is provided in the following formats:

- An Amazon Machine Image (AMI) available through the AWS Marketplace (MetaDefender products) (Recommended for PoC)
- A packaged installer available for download from the My OPSWAT portal.

- Helm charts for MetaDefender products on GitHub with corresponding container images accessible from the OPSWAT Docker Hub Repository

Currently, there are no restrictions on the AWS regions where MetaDefender can be deployed, with the exception that MetaDefender is not available in AWS GovCloud at this time.

For installing our solution, please review the guidelines listed below to deploy the different infrastructure needed to install the product:

- Deploy using EC2 Instances
- Deployment on EKS

Database Configuration

MetaDefender Storage Security currently supports AWS RDS, an AWS-managed service compatible with PostgreSQL.

EC2 Key Management

An EC2 key pair is used exclusively for SSH or RDP access to an EC2 instance, a scenario typically reserved for debugging.

You can either create a new key pair or use an existing one.

Deploy using EC2 Instances

The deployment options vary depending on what are the number of instances where MetaDefender Storage Security will be installed.

Options:

1. **Single Instance** deployment of MetaDefender Core and MetaDefender Storage Security
2. **Multi-Instance** with Autoscaling for MetaDefender Core and single instance of MetaDefender Storage Security.

OPSWAT provides a terraform project to deploy MetaDefender Storage Security and MetaDefender Core in different instances using AWS services.

Prerequisites

AWS knowledge: This guide assumes familiarity with AWS Services

AWS account: needs permission to create AWS Services depending on the examples listed in Architecture Examples in CSPs

Tools installation: Terraform, AWS CLI

Single Instance Deployment

Deploy using Terraform

OPSWAT provides a terraform project to create the infrastructure needed to deploy the Architecture Examples in CSPs

- Locally clone the metadefender-csp repository and go to AWS/single-ec2

```
git clone git@github.com:OPSWAT/metadefender-csp.git
cd AWS/single-ec2
```

- Modify terraform.tfvars with the desired options
  - LICENSE_KEY required if wanted to have the MetaDefender Core instance activated automatically
  - APIKEY_GENERATION=true to have the apikey generated by terraform
  - There is one general section and one section for each product that is supported using this Terraform project

```
# General variables

MD_ENV_NAME             = "metadefender" # Prefix to add to all the
resources
MD_REGION               = "eu-central-1" # Region for all the resources
EC2_KEY_NAME            = "" # Key pair to attach to EC2 instances
(Optional)
#ACCESS_KEY_ID          = "<ACCESS_KEY_ID>"
#SECRET_ACCESS_KEY      = "<SECRET_ACCESS_KEY>"  # To give access to
terraform (Optional, can use other ways to authenticate)
PUBLIC_ENVIRONMENT      = true
APIKEY_GENERATION       = true

# MetaDefender Core variables

DEPLOY_CORE             = true
MD_VPC_CIDR             = "192.168.0.0/16"  # VPC CIDR where to create
the MetaDefender products
CORE_PRODUCT_ID            = "ani6v4vb5z4t87cymrfg3m451" #MetaDefender
Core ID in AWS Marketplace || For Windows it is
"9s8powksm1cj7fuafdnv0sfj9"
CORE_INSTANCE_TYPE      = "c5.2xlarge"   # Instance type for
MetaDefender Core
LICENSE_KEY_CORE        = ""
```

- To deploy MetaDefender Storage Security, modify the section for Storage Security

```
# MetaDefender Storage Security variables

DEPLOY_MDSS             = true               # true to deploy
MetaDefender Storage Security together with Core
MDSS_PRODUCT_ID         = "3mup1qubt6hwmup405eljau0k" # MetaDefender
Storage Security LINUX ID in AWS Marketplace
MDSS_INSTANCE_TYPE      = "c5.2xlarge"    # Instance type for
MetaDefender Storage Security

DEPLOY_MDSS_ELASTICACHE = true  # true to deploy  MetaDefender Storage
Security with a managed instance of Elasticache Redis
MDSS_ELASTICACHE_NODE_TYPE = "cache.m5.large"
```

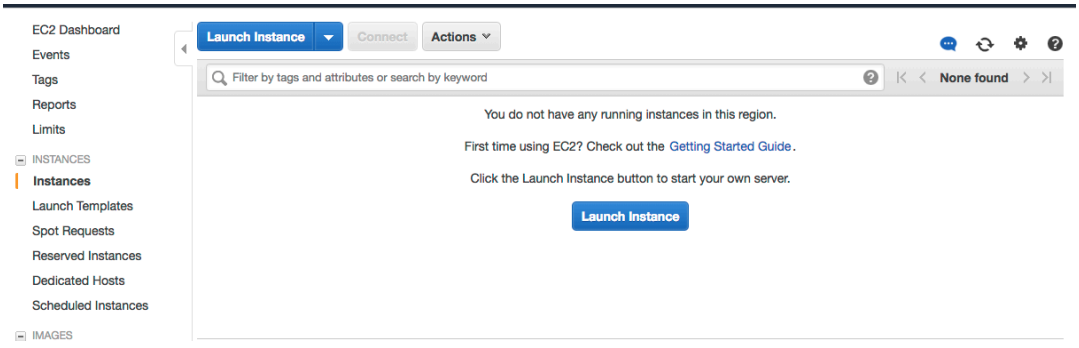
- Run terraform init and apply. Check the resource to be created, after that enter “y”

```
terraform init
terraform apply
```

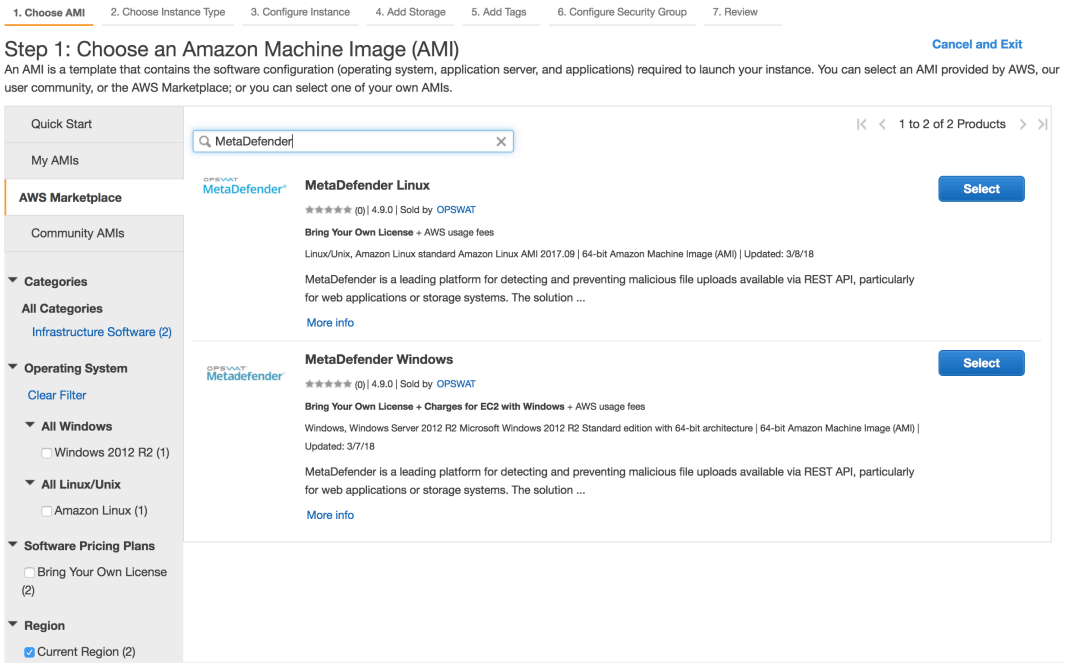
Deploy using AWS Console

Select MetaDefender Storage Security AMI

- Go to the EC2 Management Console in AWS and select Launch Instance

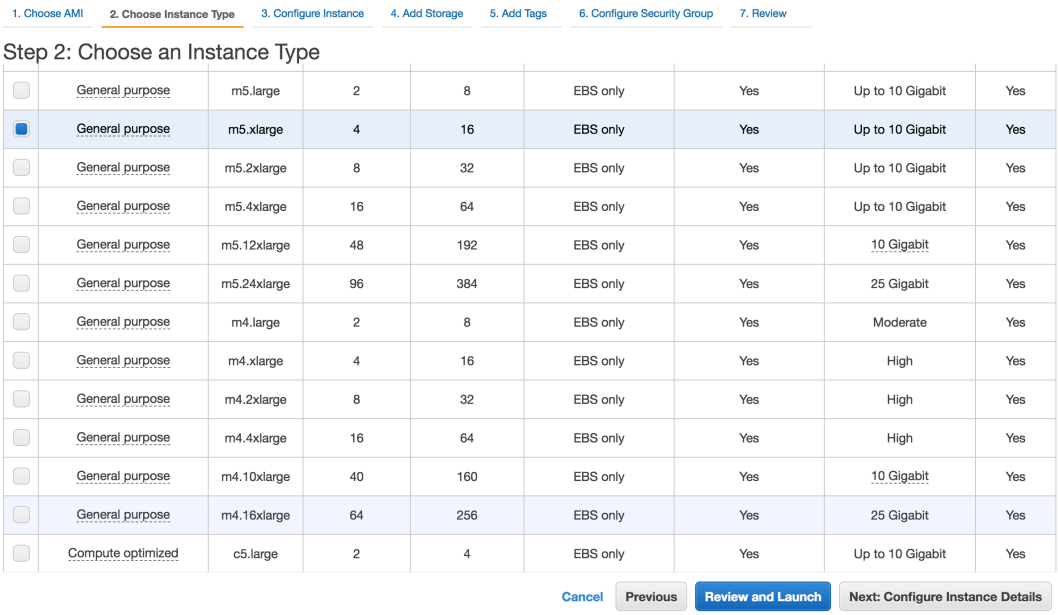


- Select the desired MetaDefender Storage Security, based on the OS support:



- Choose the Instance type

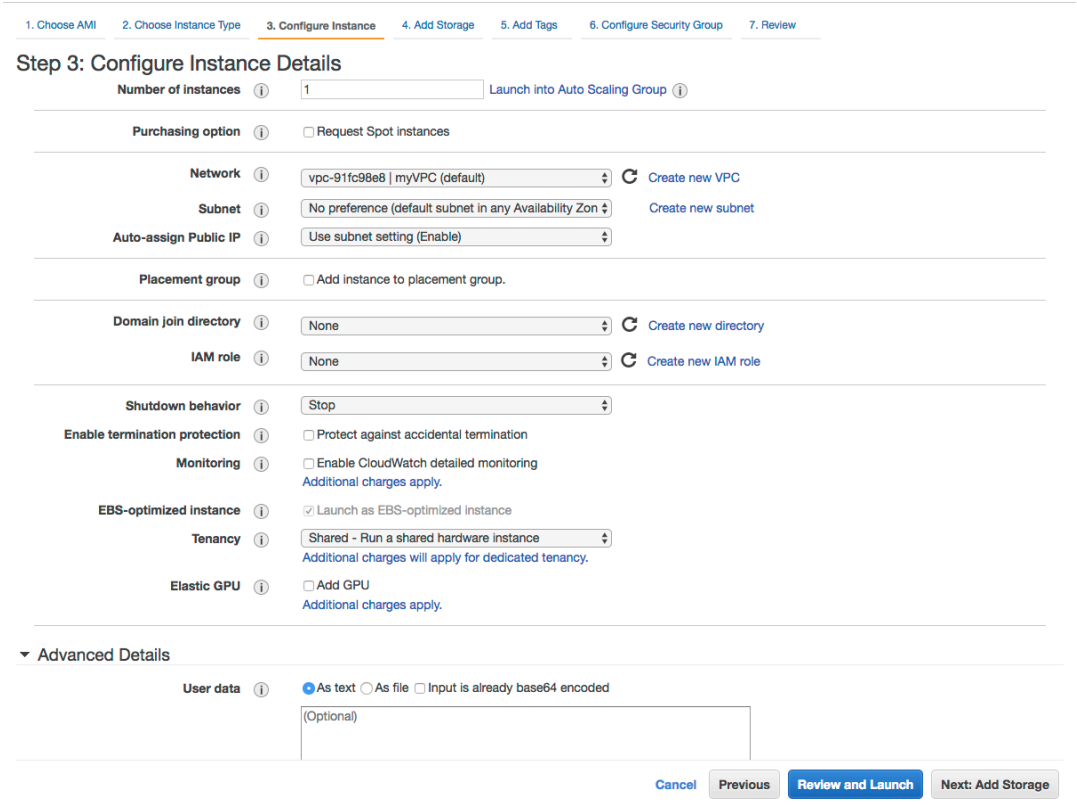
Please review MetaDefender Storage Security's general system requirements before choosing the desired AMI and instance type.



☐	General purpose	m5.large	2	8	EBS only	Yes	Up to 10 Gigabit	Yes
☑	General purpose	m5.xlarge	4	16	EBS only	Yes	Up to 10 Gigabit	Yes
☐	General purpose	m5.2xlarge	8	32	EBS only	Yes	Up to 10 Gigabit	Yes
☐	General purpose	m5.4xlarge	16	64	EBS only	Yes	Up to 10 Gigabit	Yes
☐	General purpose	m5.12xlarge	48	192	EBS only	Yes	10 Gigabit	Yes
☐	General purpose	m5.24xlarge	96	384	EBS only	Yes	25 Gigabit	Yes
☐	General purpose	m4.large	2	8	EBS only	Yes	Moderate	Yes
☐	General purpose	m4.xlarge	4	16	EBS only	Yes	High	Yes
☐	General purpose	m4.2xlarge	8	32	EBS only	Yes	High	Yes
☐	General purpose	m4.4xlarge	16	64	EBS only	Yes	High	Yes
☐	General purpose	m4.10xlarge	40	160	EBS only	Yes	10 Gigabit	Yes
☐	General purpose	m4.16xlarge	64	256	EBS only	Yes	25 Gigabit	Yes
☐	Compute optimized	c5.large	2	4	EBS only	Yes	Up to 10 Gigabit	Yes

Networking for EC2

- Select the desired VPC and subnet you would like to have MetaDefender Storage Security deployed.



Depending on the deployment model, the recommendation would be to deploy MetaDefender Storage Security in a private subnet.

Storage configuration

Storage step can be skipped

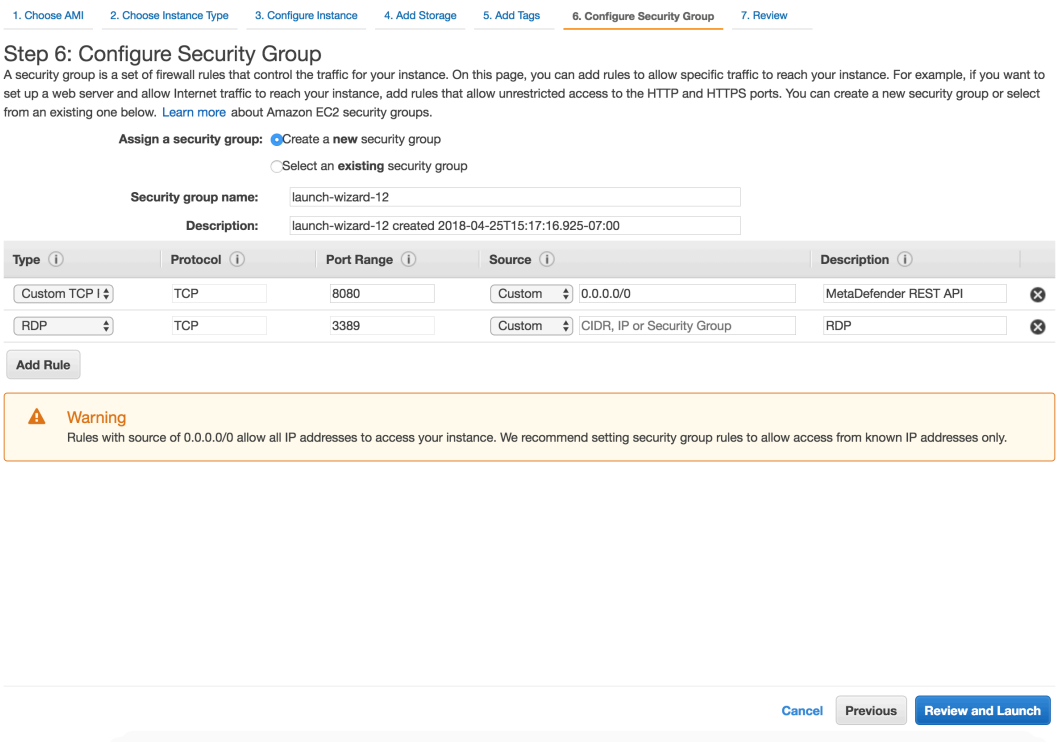
In general there's no need for additional storage by MetaDefender Storage Security. Follow the system requirements for Storage.

Security Groups configuration

There are 2 rules that are needed to be opened during the installation phase, after which only one rule should remain:

- Custom TCP: 80/443
  - MetaDefender Storage Security exposes the web UI by default to port 80 and 443 with SSL. However this port can be changed during the installation phase or updated during it's lifetime.
- RDP / SSH
  - In order to install MetaDefender Storage Security on Windows add access for RDP and for Linux add support for SSH

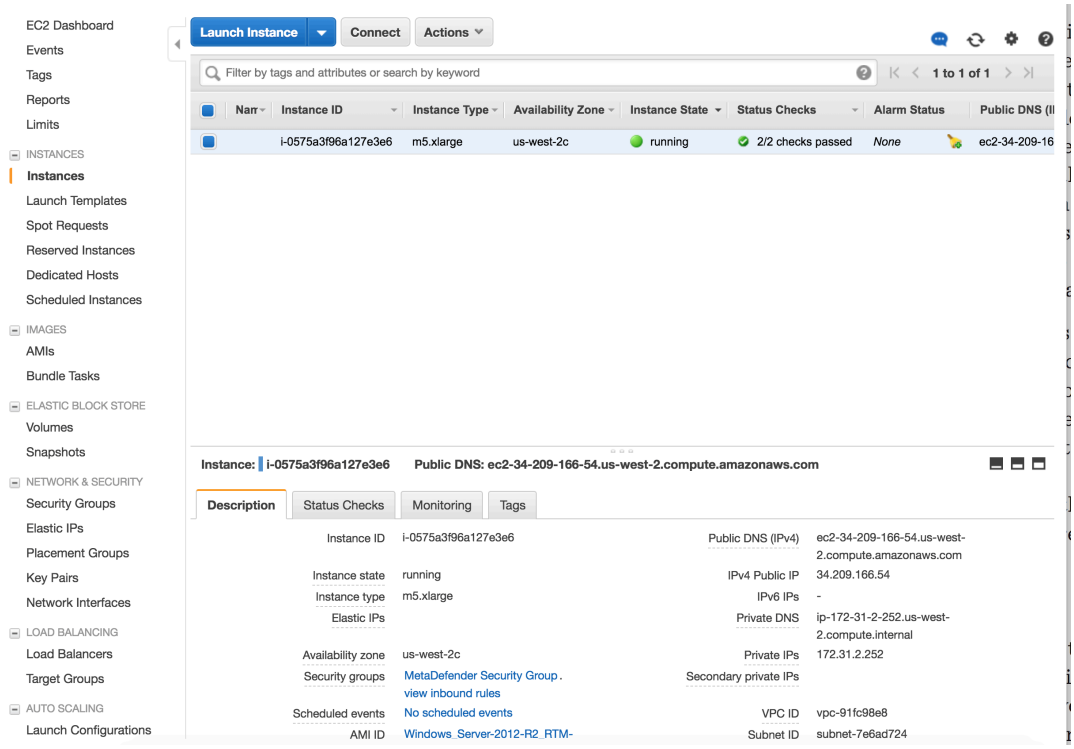
- Highly recommended would be not to allow traffic to RDP or SSH from anywhere, but to limit to your IP address



> **Warning**
>
> *After the installation remove RDP or SSH from this Security Group!*

Launch the instance

After you review the settings, hit Launch. In a few minutes the instance should become available



Multi-Instance Deployment

Deploy using Terraform

OPSWAT provides a terraform project to create the infrastructure needed to deploy the Architecture Examples in CSPs

- Locally clone the metadefender-csp repository and go to AWS/autoscaling-group

```
git clone git@github.com:OPSWAT/metadefender-csp.git
cd AWS/autoscaling-group
```

- Modify terraform.tfvars with the desired options

```
# General variables

MD_ENV_NAME             = "metadefender"
MD_REGION               = "eu-central-1"
#ACCESS_KEY_ID          = "<ACCESS_KEY_ID>"
#SECRET_ACCESS_KEY      = "<SECRET_ACCESS_KEY>"
MD_VPC_CIDR             = "192.168.0.0/16"
PUBLIC_ENVIRONMENT      = true
WARM_POOL_ENABLED       = true

# MetaDefender Core variables

DEPLOY_CORE             = "false"
CORE_PRODUCT_ID            = "ani6v4vb5z4t87cymrfg3m451" # For Windows
it is "9s8powksm1cj7fuafdnv0sfj9"
CORE_INSTANCE_TYPE      = "c5.2xlarge"
LICENSE_KEY_CORE        = ""
CORE_PWD                = "admin"
CORE_PORT               = 8008

# MetaDefender Storage Security variables

DEPLOY_MDSS             = true               # true to deploy
MetaDefender Storage Security together with Core
MDSS_PRODUCT_ID         = "3mup1qubt6hwmup405eljau0k" # MetaDefender
Storage Security LINUX ID in AWS Marketplace
MDSS_INSTANCE_TYPE      = "c5.2xlarge"    # Instance type for
MetaDefender Storage Security

DEPLOY_MDSS_DOCUMENTDB  = true  # true to deploy  MetaDefender Storage
Security with a managed instance of Amazon DocumentDB
MDSS_DOCUMENTDB_INSTANCE_CLASS = "db.r5.large"
DEPLOY_MDSS_ELASTICACHE = true  # true to deploy  MetaDefender Storage
Security with a managed instance of Elasticache Redis
MDSS_ELASTICACHE_NODE_TYPE = "cache.m5.large"
```

- Run terraform apply and check the resource to be create, after that enter “y”

```
terraform apply
```

Deployment on EKS

This guide explains how to use the provisioning tools provided by OPSWAT to create an AWS EKS and generate all the Kubernetes components needed to run MetaDefender Core and MetaDefender Storage Security.

> **Info**

> In case of having the K8S cluster already created, please check the Containerized Deployment Overview
>
> This page is purely for provisioning the EKS cluster and install the products at the same time with tools that OPSWAT has prepared.

Deploy using Terraform

- Locally clone the metadefender-k8s repository and go to terraform folder

```
git clone git@github.com:OPSWAT/metadefender-k8s.git
cd terraform/aws/
```

- Modify variables/variables.tfvars file
  - PERSISTENT_DEPLOYMENT=true -> To create K8S cluster with EC2 Worker Nodes
  - DEPLOY_FARGATE_NODES=false -> To true if wanted to create a Fargate profile
  - DEPLOY_RDS_POSTGRES_DB=true -> To create RDS instance for PostgreSQL server
  - POSTGRES_USERNAME -> if DEPLOY_RDS_POSTGRES_DB=true, set up admin database username
  - POSTGRES_PASSWORD -> if DEPLOY_RDS_POSTGRES_DB=true, set up admin database password
  - MQ_USERNAME -> if DEPLOY_RABBITMQ=true
  - MQ_PASSWORD -> if DEPLOY_RABBITMQ=true

```
MD_CLUSTER_NAME         = "md-k8s"
MD_CLUSTER_REGION       = "eu-central-1"
ACCESS_KEY_ID           = "<ACCESS_KEY_ID>"
SECRET_ACCESS_KEY       = "<SECRET_ACCESS_KEY>"
PERSISTENT_DEPLOYMENT   = true
DEPLOY_FARGATE_NODES    = false
DEPLOY_RDS_POSTGRES_DB  = true
POSTGRES_USERNAME       = "<POSTGRES_USERNAME>"
POSTGRES_PASSWORD       = "<POSTGRES_PASSWORD>"

DEPLOY_REDIS            = true
DEPLOY_RABBITMQ         = true
MQ_PASSWORD             = "<MQ_USERNAME>"
MQ_USERNAME             = "<MQ_PASSWORD>"
```

- Run terraform init and apply. Check the resource to be created, after that enter “y”

```
terraform init
terraform apply
```

MetaDefenderK8S script details

- Script path: %provisioning_script_path%
- **Programming Language:** Bash
- Installation Pre-requisites for provisioning:
  - Terraform
  - Helm
  - AWS CLI
  - Kubectl
  - eksctl (When using the lb controller script)
- AWS Credentials
  - Set in your local environment credentials the IAM user credentials under ***AWS_ACCESS_KEY_ID*** & ***AWS_SECRET_ACCESS_KEY***
- MetaDefender Core License Key (Required with --mdcore parameter)
  - Set it in your local environment credentials under ***MDCORE_LICENSE_KEY***

> **Warning**
>
> As security measure do not use the root user for any deployment or operation. Follow the principle of least privilege for all access granted. Keep in mind the resources listed in this page for your option selected: EKS Cluster Architecture

How to run the script

```
./metadefenderk8s.sh provision -l AWS --mdcore --mdss
```

Script Parameters

Parameter	Flags	Options	Default	Description	Required/Optional
Action		- provision - install		Action to indicate the script if we want to provision (Create resources + install Core) or install (Install Core)	**Required**
Location	-l or --location	- AWS - Azure - GCP		Where is going to be the K8S cluster	**Required**
MetaDefender Flag Installation	Combination of - --mdcore - --mdss - --icap		-	Install MetaDefender Core in the cluster provisioned	**Required**
Image Version	–image	- latest -	latest	MetaDefender Core image version to install	Optional
Region	–region	AWS Regions	eu-central-1	AWS region where all the resources will be provisioned	Optional
Cluster Name	–name	Not uppercase allowed	md-k8s	Name of the cluster that will be used for naming all the resources	Optional
Number of Replicas	–replicas	[0-9]*	1	Number of replicas for MetaDefender Core service	Optional
Namespace	–namespace	[A-Za-z]{1,10}		Namespace where MetaDefender products will be installed in the K8S Cluster	Optional Max Characters: 10

Limitations using parameters

- When using Fargate
  - the pods should be installed in the default namespace.
  - if using AWS Load Balancer controllers need a worker node to be installed in.

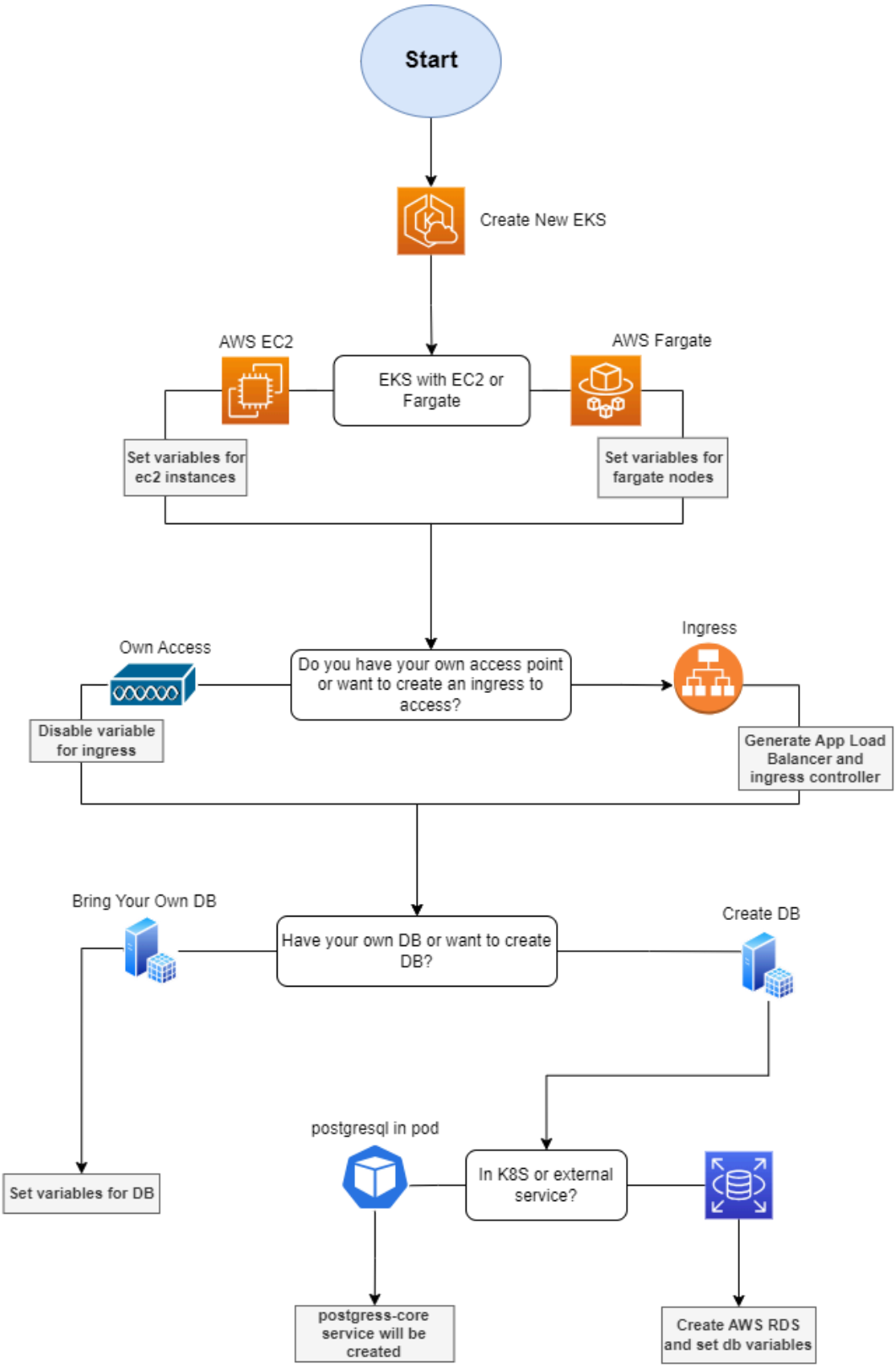
> **Info**
>
> The script will deploy a single Worker Node for the cluster with enough space for 1 replica of MD Core. AWS EC2 Instance size is **c5.2xlarge (8 vCPU & 16 GiB Memory).** Each pod would request 7 vCPU and 8 GiB Memory. To change the request to adapt each pod to the specific case go to values.yml To change the node group go to the terraform file terraform/aws/eks_cluster_module

MetaDefender Core Flowchart Provisioning in AWS

The following flowchart represents how the provisioning script will configure the environment based on the options selected for provisioning AWS EKS.

Summary options to be selected

1. EKS with **EC2** or **Fargate**
2. Access to the K8S cluster. Generate **Ingress** or provide **own** access.
   1. **An Ingress** will be create per each product flag added as parameter to the script
   2. **Own Access**, you decide how to access to the cluster so it won't generate any load balancer for accessing
3. Have your **own database** or create **new database**
   1. **Own database,** will be asked if you want the script to set up the credentials and database host url for you or the script will just indicate the secrets to edit, later on by you, for connecting the MetaDefender Core with your database.
   2. Create new **DB in K8S** or **external DB** that for AWS we will provision a ***RDS instance***


Start
Create New EKS
AWS EC2
EKS with EC2 or Fargate
AWS Fargate
Set variables for ec2 instances
Set variables for fargate nodes
Own Access
Do you have your own access point or want to create an ingress to access?
Ingress
Disable variable for ingress
Generate App Load Balancer and ingress controller
Bring Your Own DB
Have your own DB or want to create DB?
Create DB
postgresql in pod
In K8S or external service?
Set variables for DB
postgress-core service will be created
Create AWS RDS and set db variables

OPSWAT Licensing on AWS

To activate the instances where the MetaDefender products are running, it is needed to activate these products providing the LICENSE_KEY.

> **Info**
>
> LICENSE_KEY needs to be requested to Sales before starting to install the product.

MetaDefender Storage Security ask for the LICENSE_KEY when doing the on-boarding process. It is needed to assure the persistence of the database, not to have to reactivate the product on every restart.

> **Info**
>
> MetaDefender Storage Security works together with MetaDefender Core, to see how works the licensing for MetaDefender Core check this page

Azure Deployment

Introduction

This Deployment Guide provides step-by-step instructions for deploying MetaDefender Storage Security on Azure Cloud Services infrastructure.

This guide is for IT infrastructure architects, administrators and DevOps professionals who are seeking to prevent potential malicious traffic being allowed in their Azure Cloud deployment. Threat Prevention is ensured for both productivity files that might be uploaded and for known vulnerabilities that can be identified for all running services/applications deployed in Azure. The vulnerability scanning is checking known vulnerabilities for unpatched OS and running applications.

MetaDefender is provided as:

- AMI through the Azure Marketplace [MetaDefender products]
- A packaged installer available for download from the My OPSWAT portal.
- Helm charts for MetaDefender products on GitHub with corresponding container images accessible from the OPSWAT Docker Hub Repository

There are currently no restrictions on Azure regions in which you can deploy MetaDefender. The only restriction is that MetaDefender is not available Azure for Government at this time.

For deploying our solution in Azure, please review the guideline listed below:

- Deploy using Azure VMs
- Deployment on AKS

Private Key Management

The Private key pair is only used to SSH or RDP to the Azure VM. This is a very uncommon scenario, used primarily for debugging. You can create a new key pair, or use an existing pair.

Deploy using Azure VMs

The deployment options vary depending on what are the number of instances where MetaDefender Storage Security will be installed.

Options:

1. **Single Instance** deployment of MetaDefender Core and MetaDefender Storage Security
2. **Multi-Instance** with Autoscaling for MetaDefender Core and single instance of MetaDefender Storage Security.

OPSWAT provides a terraform project to deploy MetaDefender Storage Security and MetaDefender Core in different instances using Azure services.

> **Warning**
>
> MetaDefender Storage Security running in VMs only supports single instance as the 3rd party tools cannot be all exported with Azure services. However, in case of using VMs separately for these 3rd party tools then MDSS can be replicated multiple times.

Prerequisites and Requirements

Azure knowledge: This guide assumes familiarity with Azure Services

Azure account: needs permission to create Azure Services listed in Architecture Examples in CSPs for Azure.

Tools installation: Terraform

Single Instance Deployment

For a single deployment of MetaDefender Core in Azure you can use this example to test this deployment type, besides the MetaDefender VM instance, additional resources are being generated and set up.

Deploy using Terraform

OPSWAT provides a terraform project to create the infrastructure needed to deploy the Architecture Examples in CSPs

- Locally clone the metadefender-csp repository and go to Azure/single-vm-deployment

```
git clone git@github.com:OPSWAT/metadefender-csp.git
cd Azure/single-vm-deployment
```

Modify terraform.tfvars with the desired options

- LICENSE__KEY_CORE_ required if wanted to have the MetaDefender Core instance activated automatically
- APIKEY_GENERATION=true to have the apikey generated by terraform
- There is one general section and one section for each product that is supported using this Terraform project

```
# General variables

RG_NAME                 = "metadefender" # Prefix to add to all the
resources
MD_REGION               = "eastus" # Region for all the resources
MD_VNET_CIDR            = "192.168.0.0/16"  # VPC CIDR where to create
the MetaDefender products
PUBLIC_ENVIRONMENT      = true
APIKEY_GENERATION       = true
IMPORT_RG               = false
VM_PWD                  = "<SET_UP_VM_PWD>"

# MetaDefender Core variables

DEPLOY_CORE             = true
CORE_INSTANCE_TYPE      = "Standard_D8s_v5"   # Instance type for
MetaDefender Core
LICENSE_KEY_CORE        = ""
OFFER_PRODUCT_CORE      = "opswat-mdcore-linux"  # Windows opswat-
mdcore-windows
SKU_CORE                = "opswat-mdcore-linux"  # Windows opswat-
mdcore-windows


# MetaDefender Storage Security variables

DEPLOY_MDSS             = true                          # true to deploy
MetaDefender Storage Security together with Core
MDSS_INSTANCE_TYPE      = "Standard_D8s_v5"   # Instance type for
MetaDefender Storage Security
OFFER_PRODUCT_MDSS      = "opswat-mdss-ubuntu"
SKU_MDSS                = "opswatmdssubuntu"
DEPLOY_MDSS_COSMOSDB     = false
```

- Run terraform init and apply. Check the resource to be created, after that enter “y”

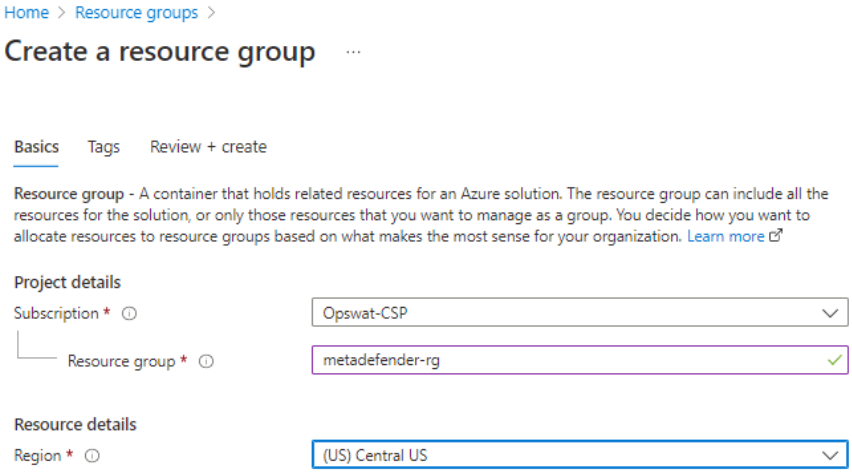
```
terraform init
terraform apply
```

Deploy using Azure portal

For having MetaDefender Core in a Single Azure VM as showed in Single Instance VM Architecture for Azure, it is needed to follow the next steps:

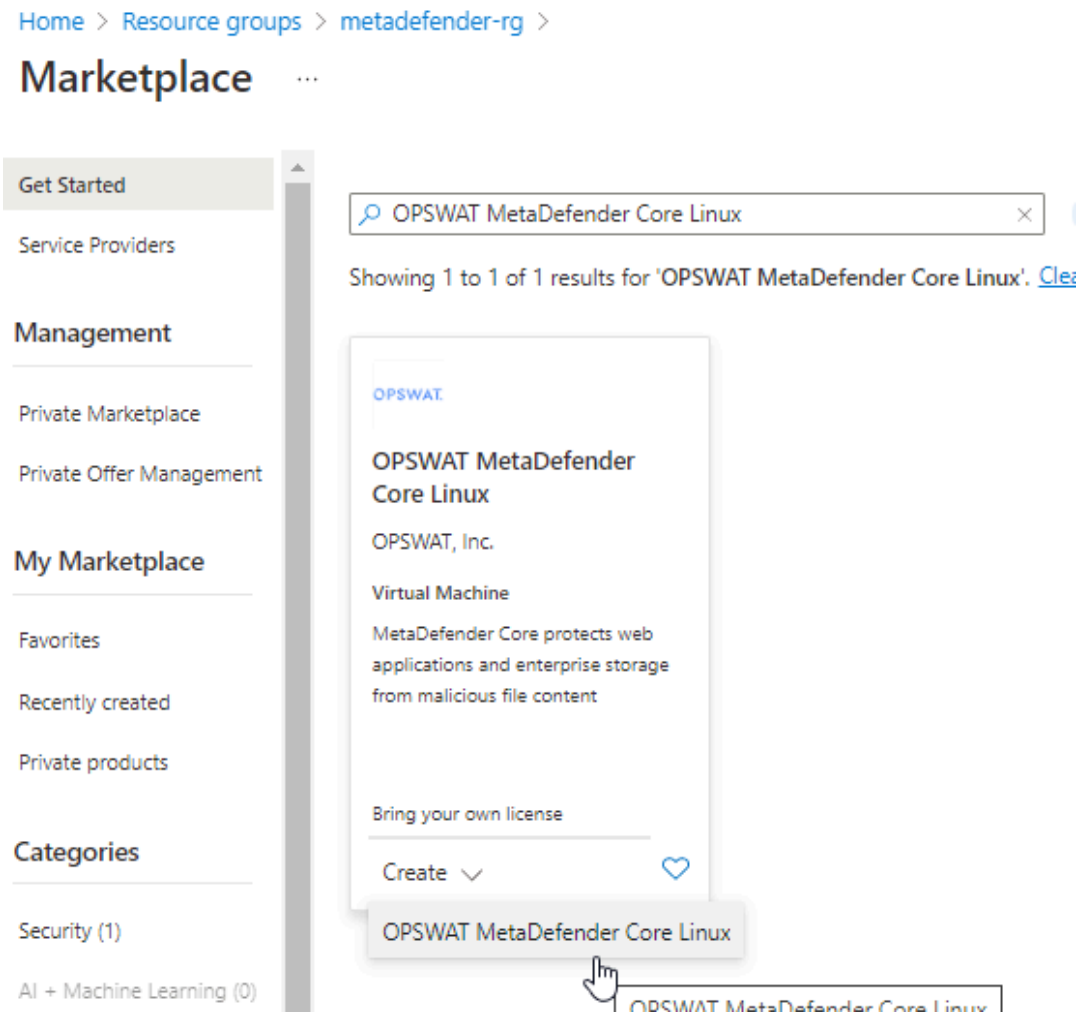
1. Create Resource Group

- Go to you Azure account and create a new resource group (we will refer to it as “metadefender-rg”)

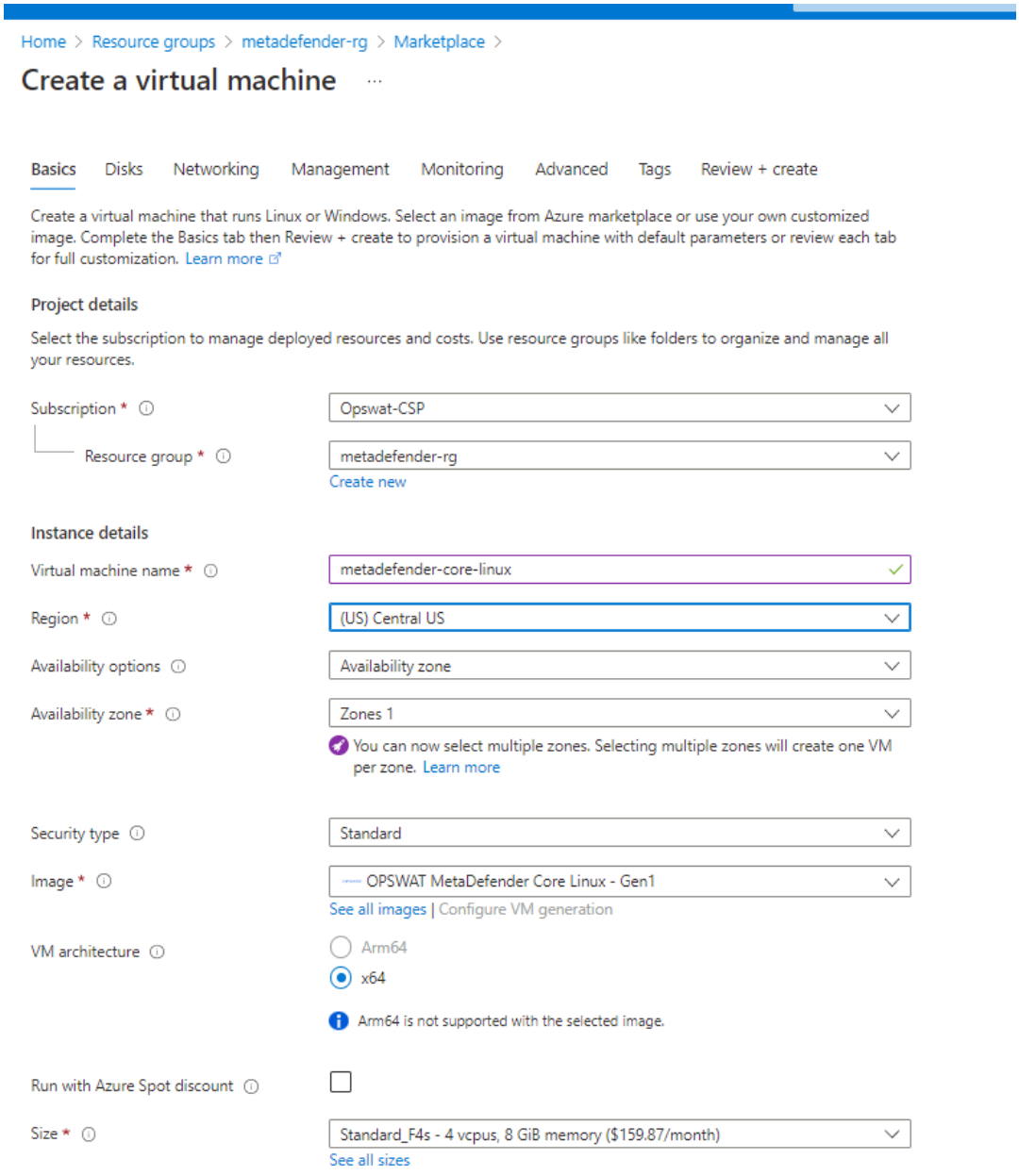


2. Create Azure VM

- Inside the resource group click on create resource and search for ***"OPSWAT MetaDefender Core Linux"***



- Input the vm name and select the size based on General System Requirements
- Under Administrator Account section select the desired way to access to the VM. For this guideline we will generate a public key to access to it



3. Storage Configuration

Storage step can be skipped.

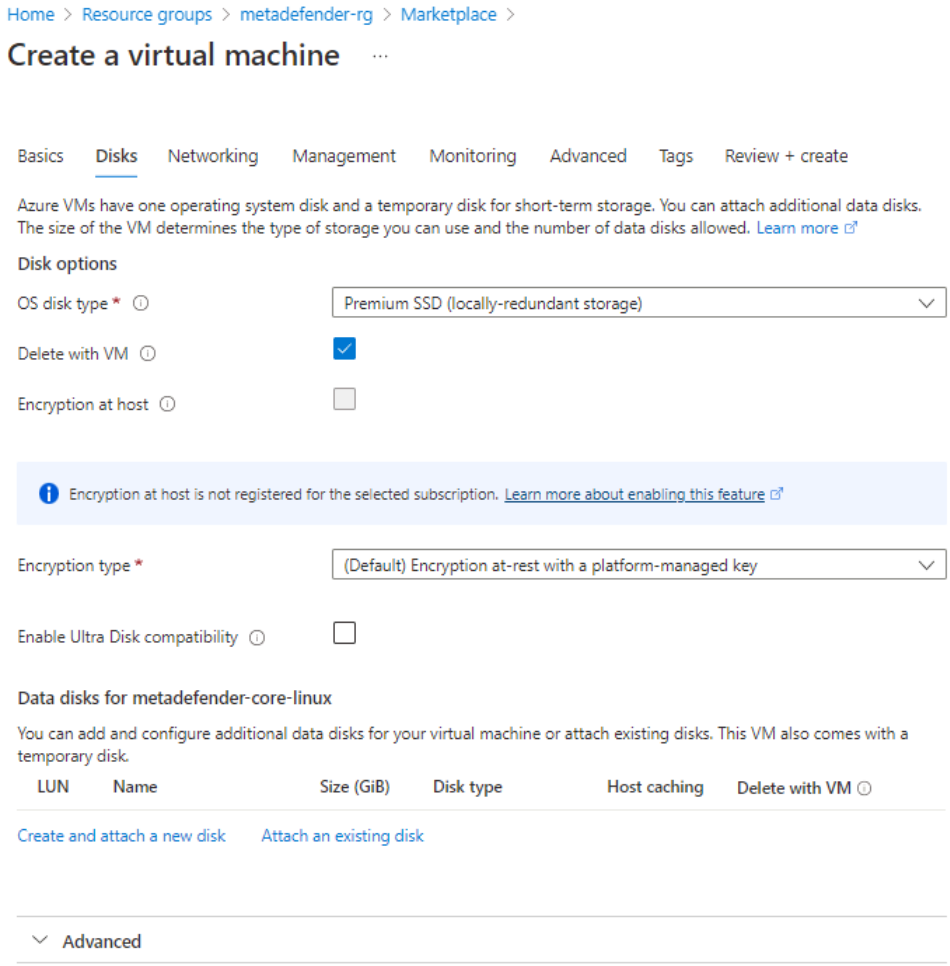
In general there's no need for additional storage by MetaDefender. However, there are 2 situations where additional local storage might be required:

- MetaDefender will process large files or a high volume of files which submitted in MetaDefender's queue will need over 10GB files storage

- MetaDefender is configured to store files in the Quarantine section which will eventually fill the entire root volume.

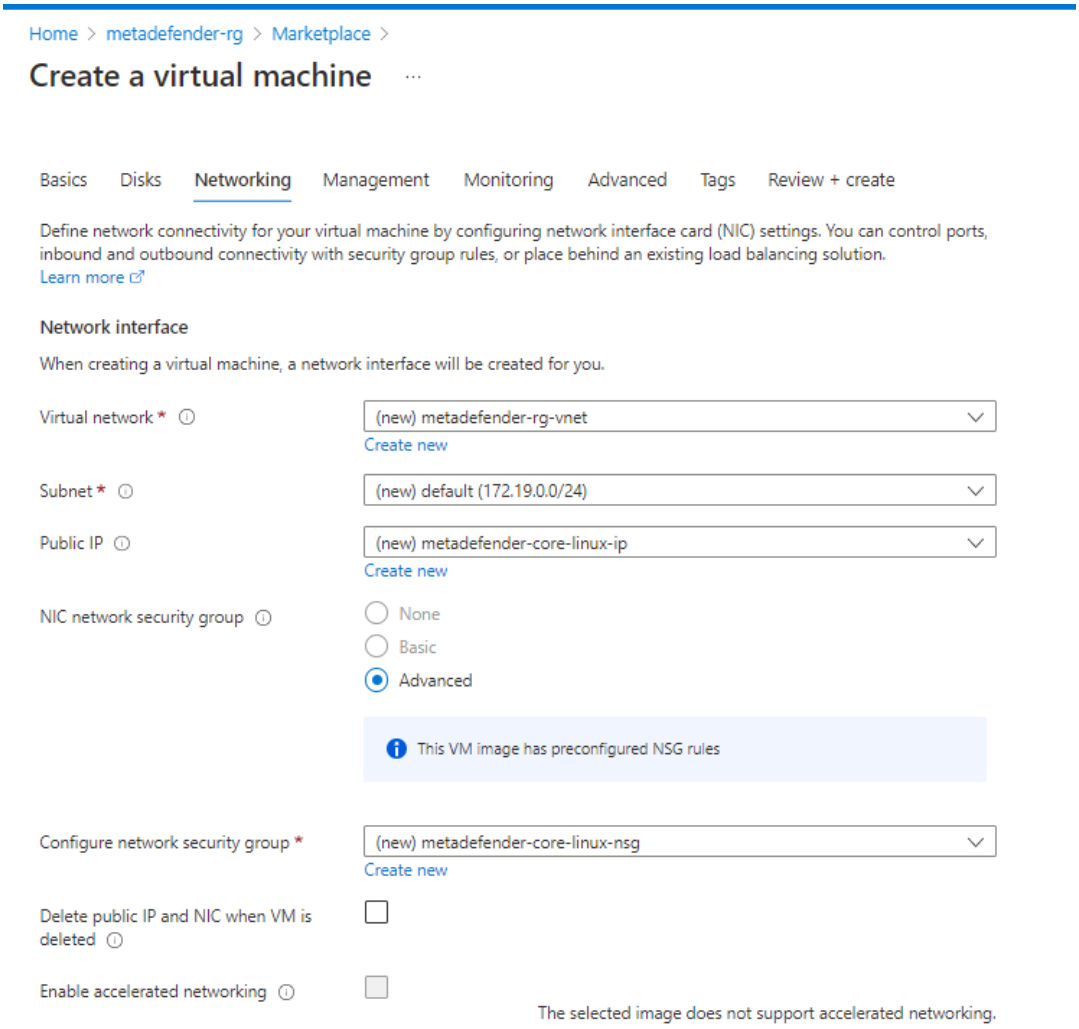
In case quarantining the files in the MetaDefender instance or analyzing high volumes of files is a requirement, please consider adding an additional Azure Managed Disk

- Premium SSD is recommended for having the best performance

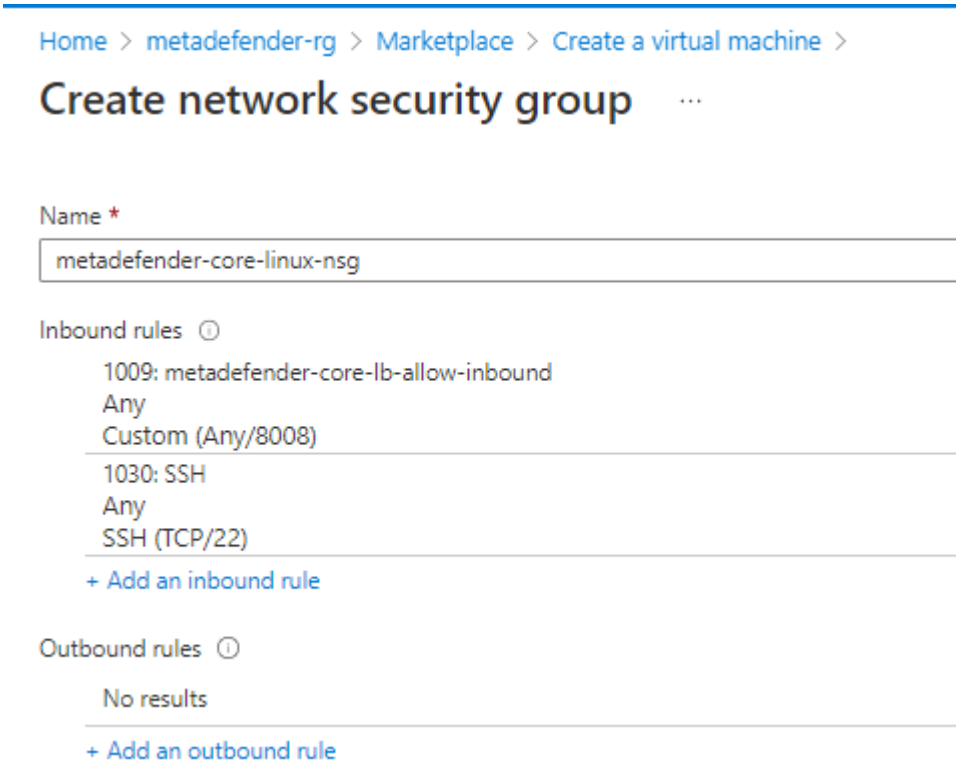


4. Network Configuration

- Change public IP to None in case you do not want to access from internet.
- Select the Virtual network and Subnet in case you already have them created, if not leave it to create them



- Create Security Group adding rules for 8008 and SSH



- Under Load Balancing section as it is a single vm it is not really needed but it can be used to set up a health check using the /readyz endpoint

5. Review & Create the VM

- Under Management, Monitoring, Advanced and Tags there are not any configuration different from the default ones that are needed to be selected. So customize it as it is needed for each use case.
- After creating it will show you a window to download the private key to access to the VM in case that option was selected for accessing

Deployment on AKS

This guide explains how to use the provisioning tools provided by OPSWAT to create an Azure AKS and generate all the Kubernetes components needed to run MetaDefender Core and MetaDefender Storage Security.

> **Info**
>
> In case of having the K8S cluster already created, please check the Containerized Deployment Overview

> This page is purely for provisioning the AKS cluster and install the products at the same time with tools that OPSWAT has prepared.

Deploy using Terraform

- Locally clone the metadefender-k8s repository and go to terraform folder

```
git clone git@github.com:OPSWAT/metadefender-k8s.git#OPTIONAL, IT CAN
BE SET UP WITH ENV VARIABLES
cd terraform/azure/
```

- Modify variables/variables.tfvars file
  - PERSISTENT_DEPLOYMENT=true -> To create K8S cluster with EC2 Worker Nodes
  - DEPLOY_FARGATE_NODES=false -> To true if wanted to create a Fargate profile
  - DEPLOY_RDS_POSTGRES_DB=true -> To create RDS instance for PostgreSQL server
  - POSTGRES_USERNAME -> if DEPLOY_RDS_POSTGRES_DB=true, set up admin database username
  - POSTGRES_PASSWORD -> if DEPLOY_RDS_POSTGRES_DB=true, set up admin database password`

```
aks_service_principal_app_id = "" #OPTIONAL, IT CAN BE SET UP WITH ENV
VARIABLES
aks_service_principal_client_secret = "" #OPTIONAL, IT CAN BE SET UP
WITH ENV VARIABLES
aks_service_principal_object_id = "" #OPTIONAL, IT CAN BE SET UP WITH
ENV VARIABLES

postgres_admin = ""
postgres_password = ""
```

- Run terraform init and apply. Check the resource to be created, after that enter “y”

```
terraform init
terraform apply

# IF Variables are not setup you can use this command
terraform apply \
  -var="aks_service_principal_app_id=$ARM_CLIENT_ID" \
  -var="aks_service_principal_client_secret=$ARM_CLIENT_SECRET"
```

MetaDefenderK8S Script Details

- **GitHub Project** metadefender-k8s --> **Script path**: ./metadefenderk8s.sh
- **Programming Language:** Bash

- Installation **Pre-requisites** for provisioning:
  - Terraform
  - Helm
  - AZ CLI
  - Kubectl
- **Azure Credentials**
  - Set in your local environment variables the credentials of the IAM user under
    - **ARM_CLIENT_ID**
    - **ARM_CLIENT_SECRET**
    - **ARM_SUBSCRIPTION_ID**
    - **ARM_TENANT_ID**
  - ssh public key to used to access the cluster with kubectl. Default [~/.ssh/id_rsa.pub]. Change from here
  - az login before running the script for the step of downloading the kubeconfig file for you
- MetaDefender **Core License Key** [Required with --mdcore parameter]
  - Set it in your local environment variables the credentials under ***MDCORE_LICENSE_KEY***

How to run the script

```
./metadefenderk8s.sh provision -l Azure --mdcore
```

```
./metadefenderk8s.sh provision -l Azure --mdcore --mdss
```

```
./metadefenderk8s.sh provision -l Azure --mdcore --icap
```

> **Info**
>
> The script will deploy a single Worker Node for the cluster with enough space for 1 replica of MD Core. Azure VM size is **Standard_F8s_v2 [8 vCPU & 16 GiB Memory].** Each pod would need a minimum of 4 vCPU and 8 GiB Memory. To change the request to adapt each pod to the specific case go to values.yml To change the size of the node pool for having more MD Core replicas or install additional MetaDefender products go to terraform file terraform/azure/main.tf

Script Parameters

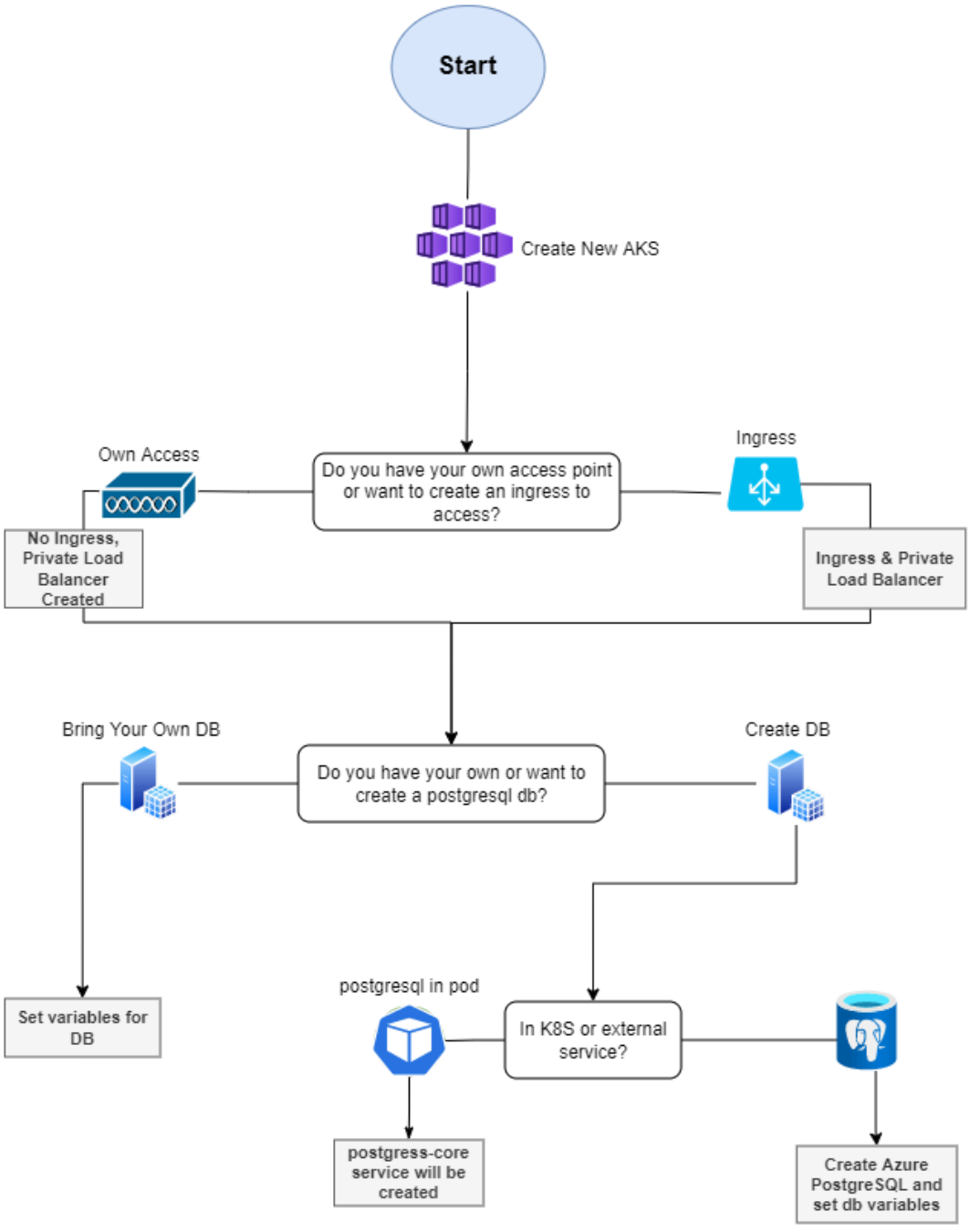
Parameter	Flags	Options	Default	Description	Required/Optional
Action		- provision - install		Action to indicate the script if we want to provision (Create resources + install Core) or install (Install Core)	**Required**
Location	-l or --location	- AWS - Azure - GCP		Where is going to be the K8S cluster	**Required**
MetaDefender Flag Installation	Combination of - --mdcore - --mdss - --icap		-	Install MetaDefender Core in the cluster provisioned	**Required**
Image Version	–image	latest 5.0.1	latest	MetaDefender Core image version to install	Optional
Region	–region	Azure Regions	centralus	AWS region where all the resources will be provisioned	Optional
Cluster Name	–name		md-k8s	Name of the cluster that will be used for naming all the resources	Optional
Number of Replicas	–replicas	[0-9]*	1	Number of replicas for MetaDefender Core service	Optional
Namespace	–namespace	[A-Za-z] {1,10}		Namespace where MetaDefender products will be installed in the K8S Cluster	Optional Max Characters: 10

MetaDefender Core Flowchart Provisioning in Azure

The following flowchart represents how the provisioning script will configure the environment based on the options selected for provisioning Azure AKS.

Summary options to be selected

1. Access to the K8S cluster. Generate **Ingress** or provide **own** access.
    1. **An Ingress** and an internal load balancer will be created per each product flag added as parameter to the script
    2. **Own Access**, you decide how to access to the cluster so it won't generate any ingress but will still create the internal load balancer for the product service deployed
2. Have your **own database** or create **new database**
    1. **Own database,** will be asked if you want the script to set up the credentials and database host url for you or the script will just indicate the secrets to edit, later on by you, for connecting the MetaDefender Core with your database.
    2. Create new **DB in K8S** or **external DB** that for Azure we will provision a **Azure *PostgreSQL Flexible Server***_ **** ___ _ ******._



OPSWAT Licensing on Azure

All the AMI published in the Azure Marketplace are Bring Your Own License, that need to be provided by an OPSWAT Sales representative.

To activate the instances where the MetaDefender products are running, it is needed to activate these products providing the LICENSE_KEY.

> **Info**

> LICENSE_KEY needs to be requested to Sales before starting to install the product.

MetaDefender Storage Security ask for the LICENSE_KEY when doing the on-boarding process. It is needed to assure the persistence of the database, not to have to reactivate the product on every restart.

> **Info**
>
> MetaDefender Storage Security works together with MetaDefender Core, to see how works the licensing for MetaDefender Core check this page

GCP Deployment

Introduction

This Deployment Guide provides step-by-step instructions for deploying MetaDefender Storage Security on Google Cloud Services infrastructure.

This guide is for IT infrastructure architects, administrators and DevOps professionals who are seeking to prevent potential malicious traffic being allowed in their Google Cloud deployment. Threat Prevention is ensured for both productivity files that might be uploaded and for known vulnerabilities that can be identified for all running services/applications deployed in Google. The vulnerability scanning is checking known vulnerabilities for unpatched OS and running applications.

MetaDefender is provided as:

- A packaged installer available for download from the My OPSWAT portal.
- Helm charts for MetaDefender products on GitHub with corresponding container images accessible from the OPSWAT Docker Hub Repository
- AMI through the Google Marketplace [**On Roadmap for Storage Security, for MetaDefender Core it is available**]

There are currently no restrictions on Google regions in which you can deploy MetaDefender.

For deploying our solution in Google, please review the guideline listed below:

- Deploy using Google Compute Engines
- Deployment on GKE

Deploy using Google Compute Engines

The deployment options vary depending on what are the number of instances where MetaDefender Storage Security will be installed.

Options:

1. **Single Instance** deployment of MetaDefender Core and MetaDefender Storage Security
2. **Multi-Instances** with Autoscaling for MetaDefender Core and MetaDefender Storage Security.

OPSWAT provides a terraform project as example to deploy MetaDefender Storage Security and MetaDefender Core in different instances using Google services.

> **Warning**
>
> MetaDefender Storage Security running on Compute Engine only supports multiple instances if the third-party tools are externalized from the Storage Security instance. Google Cloud provides managed services for PostgreSQL and Redis Cache, but not for RabbitMQ. If RabbitMQ is deployed externally on a separate Compute Engine instance, then a multi-instance deployment is supported.

Prerequisites and Requirements

Google knowledge: This guide assumes familiarity with Google Services

Google project: needs permission to create Google Services listed in Architecture Examples in CSPs for Google.

Tools installation: Terraform

Single Instance Deployment

For a single deployment of MetaDefender Core in Google you can use this example to test this deployment type, besides the MetaDefender VM instance, additional resources are being generated and set up.

Deploy using Terraform

OPSWAT provides a terraform project to create the infrastructure needed to deploy the Architecture Examples in CSPs

- Locally clone the metadefender-csp repository and go to GCP/single-vm-deployment

```
git clone git@github.com:OPSWAT/metadefender-csp.git
cd GCP/single-compute-engine-deployment
```

Modify terraform.tfvars with the desired options

- LICENSE__KEY_CORE_ required if wanted to have the MetaDefender Core instance activated automatically
- APIKEY_GENERATION=true to have the apikey generated by terraform
- There is one general section and one section for each product that is supported using this Terraform project

```
# General variables

RG_NAME                 = "metadefender" # Prefix to add to all the
resources
MD_REGION               = "eastus" # Region for all the resources
MD_VNET_CIDR            = "192.168.0.0/16"  # VPC CIDR where to create
the MetaDefender products
PUBLIC_ENVIRONMENT      = true
APIKEY_GENERATION       = true
IMPORT_RG               = false
VM_PWD                  = "<SET_UP_VM_PWD>"

# MetaDefender Core variables

DEPLOY_CORE             = true
CORE_INSTANCE_TYPE      = "Standard_D8s_v5"   # Instance type for
MetaDefender Core
LICENSE_KEY_CORE        = ""
OFFER_PRODUCT_CORE      = "opswat-mdcore-linux"  # Windows opswat-
mdcore-windows
SKU_CORE                = "opswat-mdcore-linux"  # Windows opswat-
mdcore-windows


# MetaDefender Storage Security variables

DEPLOY_MDSS             = true                          # true to deploy
MetaDefender Storage Security together with Core
MDSS_INSTANCE_TYPE      = "Standard_D8s_v5"   # Instance type for
MetaDefender Storage Security
OFFER_PRODUCT_MDSS      = "opswat-mdss-ubuntu"
SKU_MDSS                = "opswatmdssubuntu"
DEPLOY_MDSS_COSMOSDB     = false
```

- Run terraform init and apply. Check the resource to be created, after that enter “y”

```
terraform init
terraform apply
```

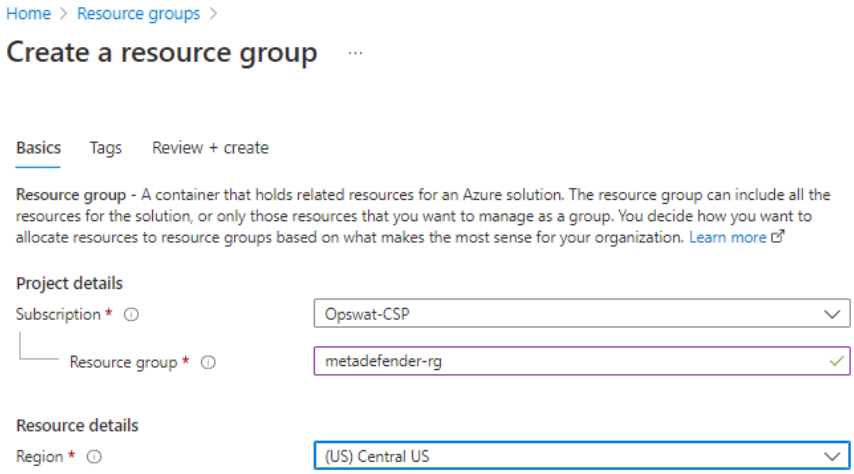
Deploy using Google Cloud Console

Before starting with the installation, Storage Security needs that MetaDefender Core is installed, if you haven´t already installed it please follow this page

For having MetaDefender Storage Security in a Single Compute Engine VM as showed in Single Instance VM Architecture for GCP, it is needed to follow the next steps:

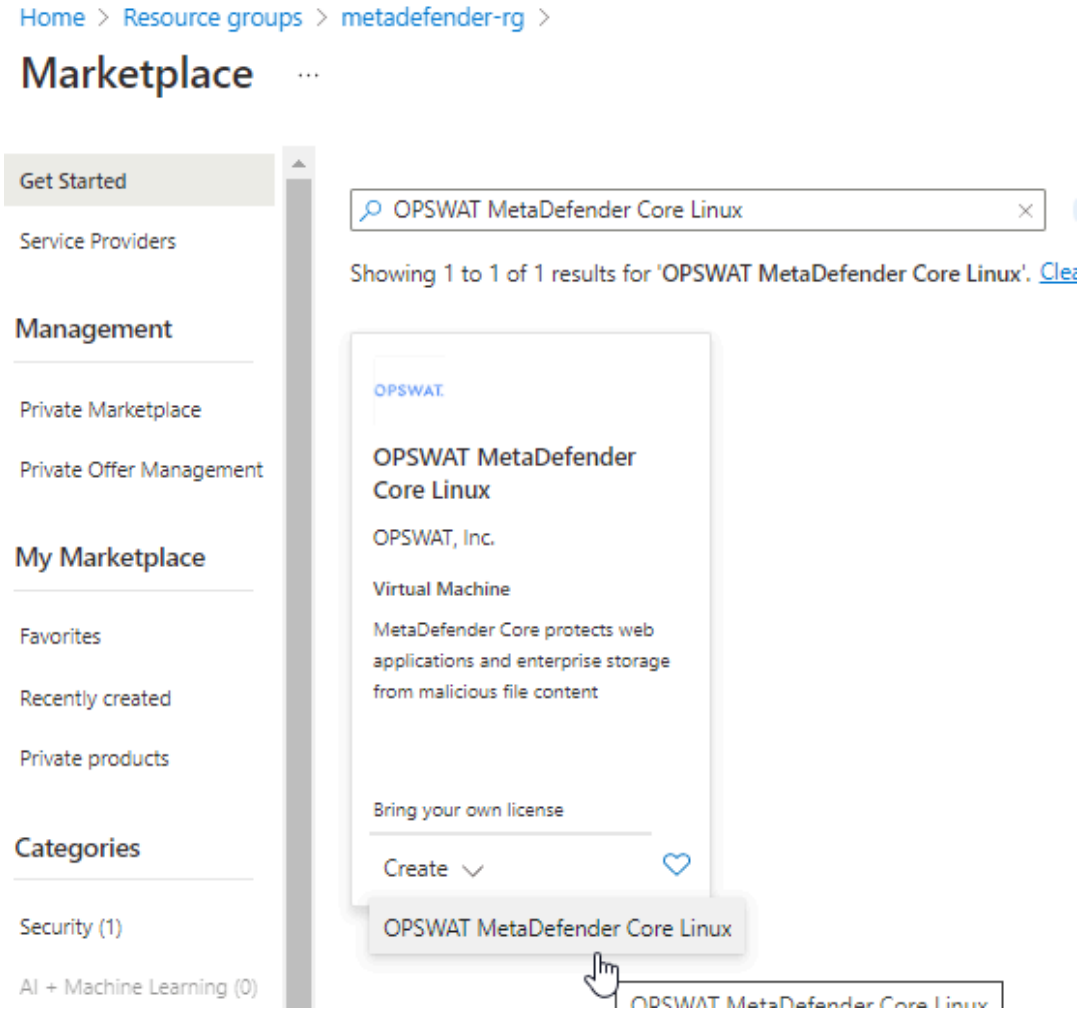
1. Create Resource Group

- Go to you Azure account and create a new resource group (we will refer to it as "metadefender-rg")

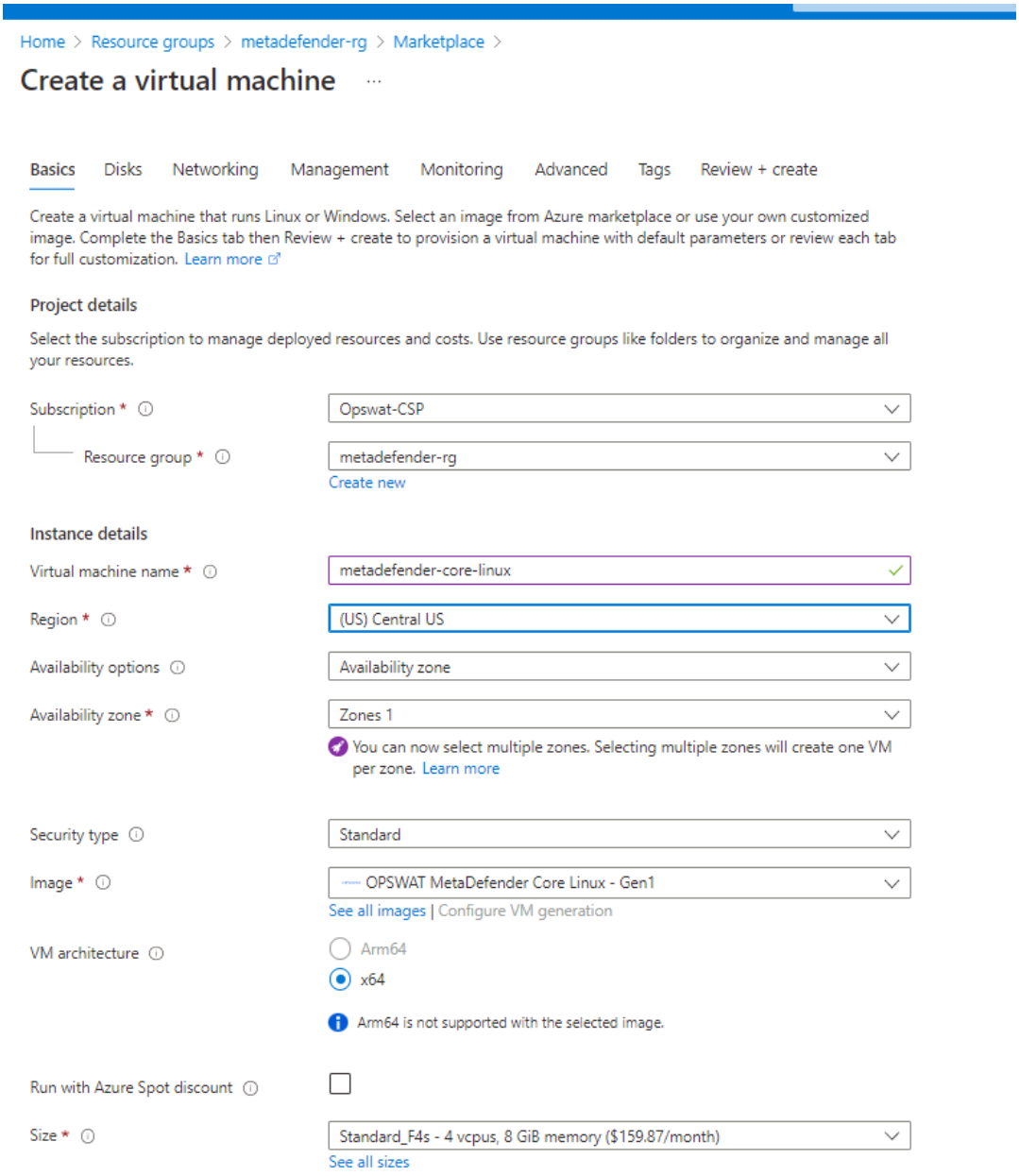


2. Create Azure VM

- Inside the resource group click on create resource and search for ***"OPSWAT MetaDefender Core Linux"***



- Input the vm name and select the size based on General System Requirements
- Under Administrator Account section select the desired way to access to the VM. For this guideline we will generate a public key to access to it



3. Storage Configuration

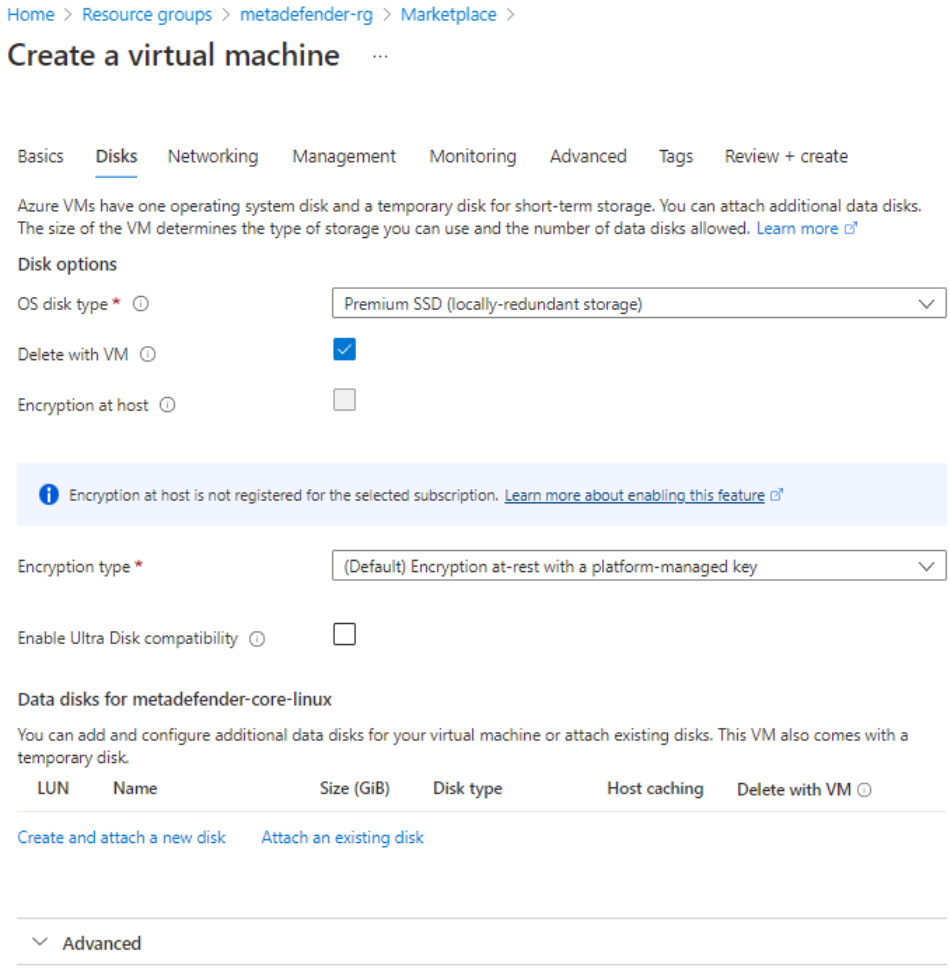
Storage step can be skipped.

In general there's no need for additional storage by MetaDefender. However, there are 2 situations where additional local storage might be required:

- MetaDefender will process large files or a high volume of files which submitted in MetaDefender's queue will need over 10GB files storage
- MetaDefender is configured to store files in the Quarantine section which will eventually fill the entire root volume.

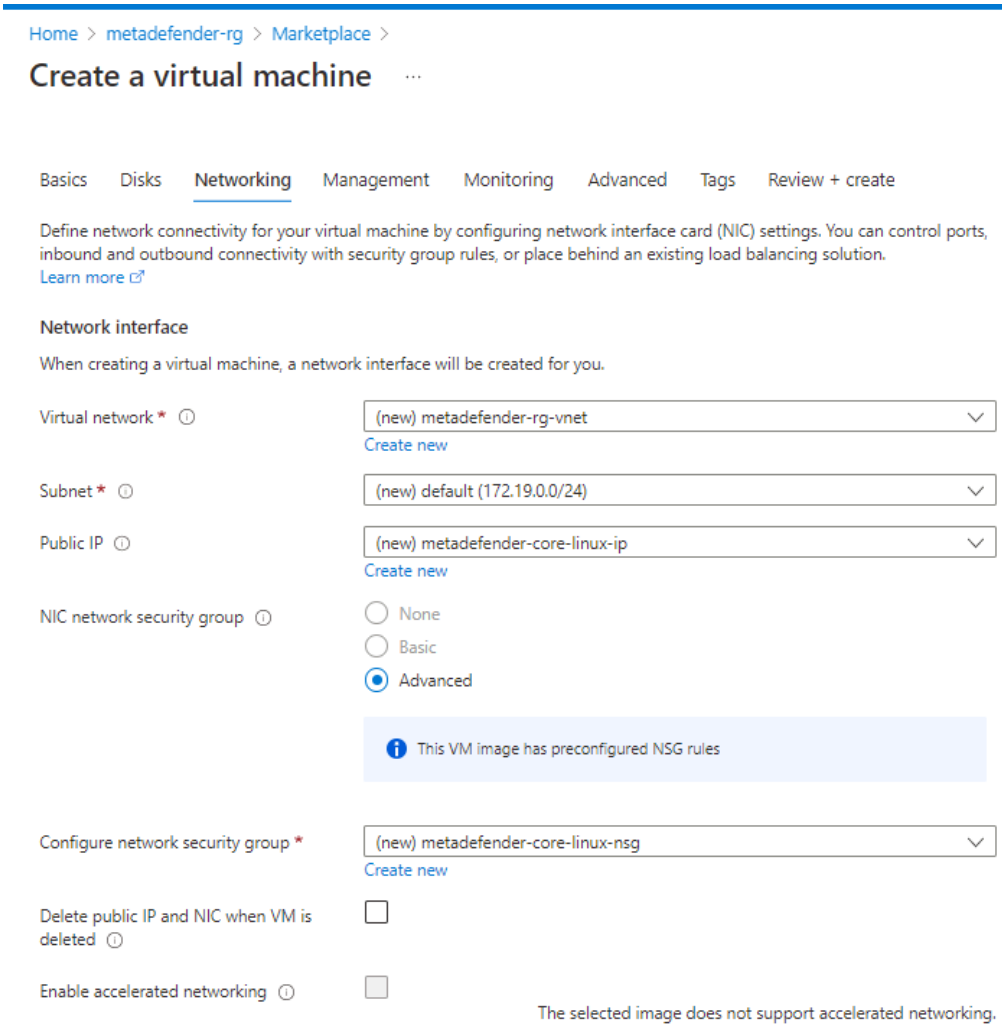
In case quarantining the files in the MetaDefender instance or analyzing high volumes of files is a requirement, please consider adding an additional Azure Managed Disk

- Premium SSD is recommended for having the best performance

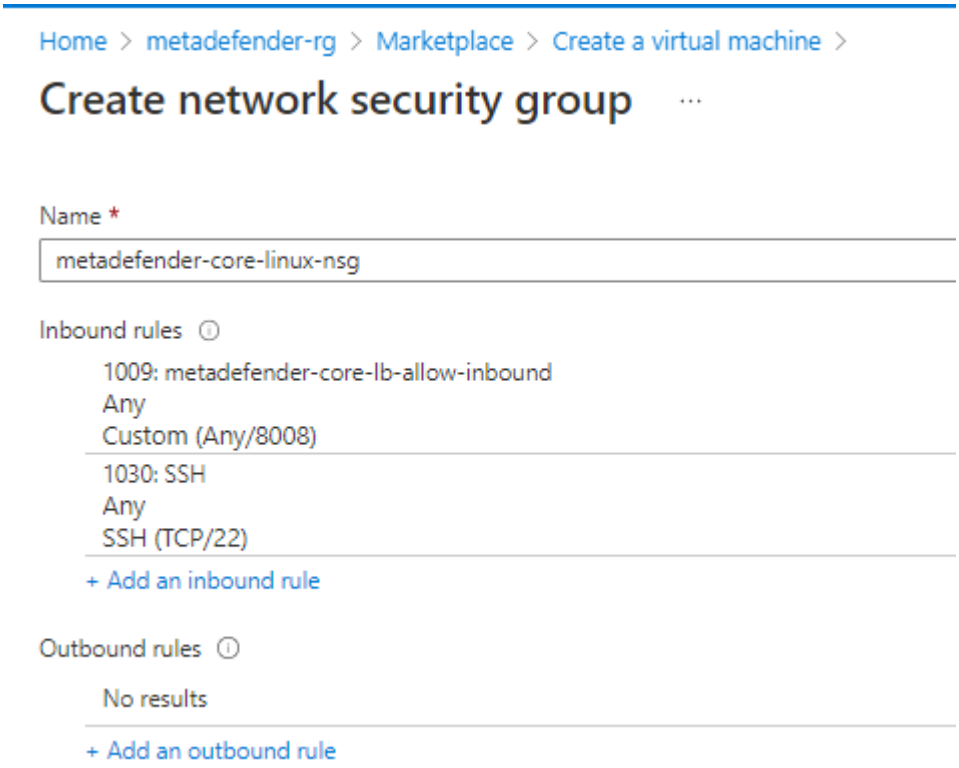


4. Network Configuration

- Change public IP to None in case you do not want to access from internet.
- Select the Virtual network and Subnet in case you already have them created, if not leave it to create them



- Create Security Group adding rules for 8008 and SSH



- Under Load Balancing section as it is a single vm it is not really needed but it can be used to set up a health check using the /readyz endpoint

5. Review & Create the VM

- Under Management, Monitoring, Advanced and Tags there are not any configuration different from the default ones that are needed to be selected. So customize it as it is needed for each use case.
- After creating it will show you a window to download the private key to access to the VM in case that option was selected for accessing

Deployment on GKE

This guide explains how to use the provisioning tools provided by OPSWAT to create an AWS GKE and generate all the Kubernetes components needed to run MetaDefender Core and MetaDefender Storage Security.

> **Info**
>
> In case of having the K8S cluster already created, please check the Deployment Using Helm page

> This page is purely for provisioning the EKS cluster and install the products at the same time with the tools that OPSWAT has prepared.

Deploy using Terraform

- Locally clone the metadefender-k8s repository and go to terraform folder

```
git clone git@github.com:OPSWAT/metadefender-k8s.git
cd terraform/gcloud/
```

- Modify terraform.tfvars file
  - PERSISTENT_DEPLOYMENT=true -> To create K8S cluster with EC2 Worker Nodes
  - DEPLOY_FARGATE_NODES=false -> To true if wanted to create a Fargate profile
  - DEPLOY_RDS_POSTGRES_DB=true -> To create RDS instance for PostgreSQL server
  - POSTGRES_USERNAME -> if DEPLOY_RDS_POSTGRES_DB=true, set up admin database username
  - POSTGRES_PASSWORD -> if DEPLOY_RDS_POSTGRES_DB=true, set up admin database password
  - MQ_USERNAME -> if DEPLOY_RABBITMQ=true
  - MQ_PASSWORD -> if DEPLOY_RABBITMQ=true

```
# project_id = "<ADD_YOUR_PROJECT_ID>"
# region = "europe-central2"
# cluster_location = "europe-central2"
gcloud_json_key_path = "/path/to/json"
# node_count = "1"
# machine_type = "e2-standard-8"
deploy_cloud_sql = true
AUTOPILOT_GKE = false
# private_ip_cloud_sql = true
# cloud_sql_user = postgres
# cloud_sql_password = <ADD_YOUR_POSTGRES_PASS>
```

- Run terraform init and apply. Check the resource to be created, after that enter “y”

```
terraform init
terraform apply
```

MetaDefenderK8S script details

- Script path: %provisioning_script_path%
- **Programming Language:** Bash

- Installation Pre-requisites for provisioning:
  - Terraform
  - Helm
  - AWS CLI
  - Kubectl
  - eksctl (When using the lb controller script)
- AWS Credentials
  - Set in your local environment credentials the IAM user credentials under ***AWS_ACCESS_KEY_ID*** & ***AWS_SECRET_ACCESS_KEY***
- MetaDefender Core License Key (Required with --mdcore parameter)
  - Set it in your local environment credentials under ***MDCORE_LICENSE_KEY***

> **Warning**
>
> As security measure do not use the root user for any deployment or operation. Follow the principle of least privilege for all access granted. Keep in mind the resources listed in this page for your option selected: EKS Cluster Architecture

How to run the script

```
./metadefenderk8s.sh provision -l AWS --mdcore --mdss
```

Script Parameters

Parameter	Flags	Options	Default	Description	Required/Optional
Action		- provision - install		Action to indicate the script if we want to provision (Create resources + install Core) or install (Install Core)	**Required**
Location	-l or --location	- AWS - Azure - GCP		Where is going to be the K8S cluster	**Required**
MetaDefender Flag Installation	Combination of - --mdcore - --mdss - --icap		-	Install MetaDefender Core in the cluster provisioned	**Required**
Image Version	–image	- latest -	latest	MetaDefender Core image version to install	Optional
Region	–region	AWS Regions	eu-central-1	AWS region where all the resources will be provisioned	Optional
Cluster Name	–name	Not uppercase allowed	md-k8s	Name of the cluster that will be used for naming all the resources	Optional
Number of Replicas	–replicas	[0-9]*	1	Number of replicas for MetaDefender Core service	Optional
Namespace	–namespace	[A-Za-z]{1,10}		Namespace where MetaDefender products will be installed in the K8S Cluster	Optional Max Characters: 10

Limitations using parameters

- When using Fargate
  - the pods should be installed in the default namespace.
  - if using AWS Load Balancer controllers need a worker node to be installed in.

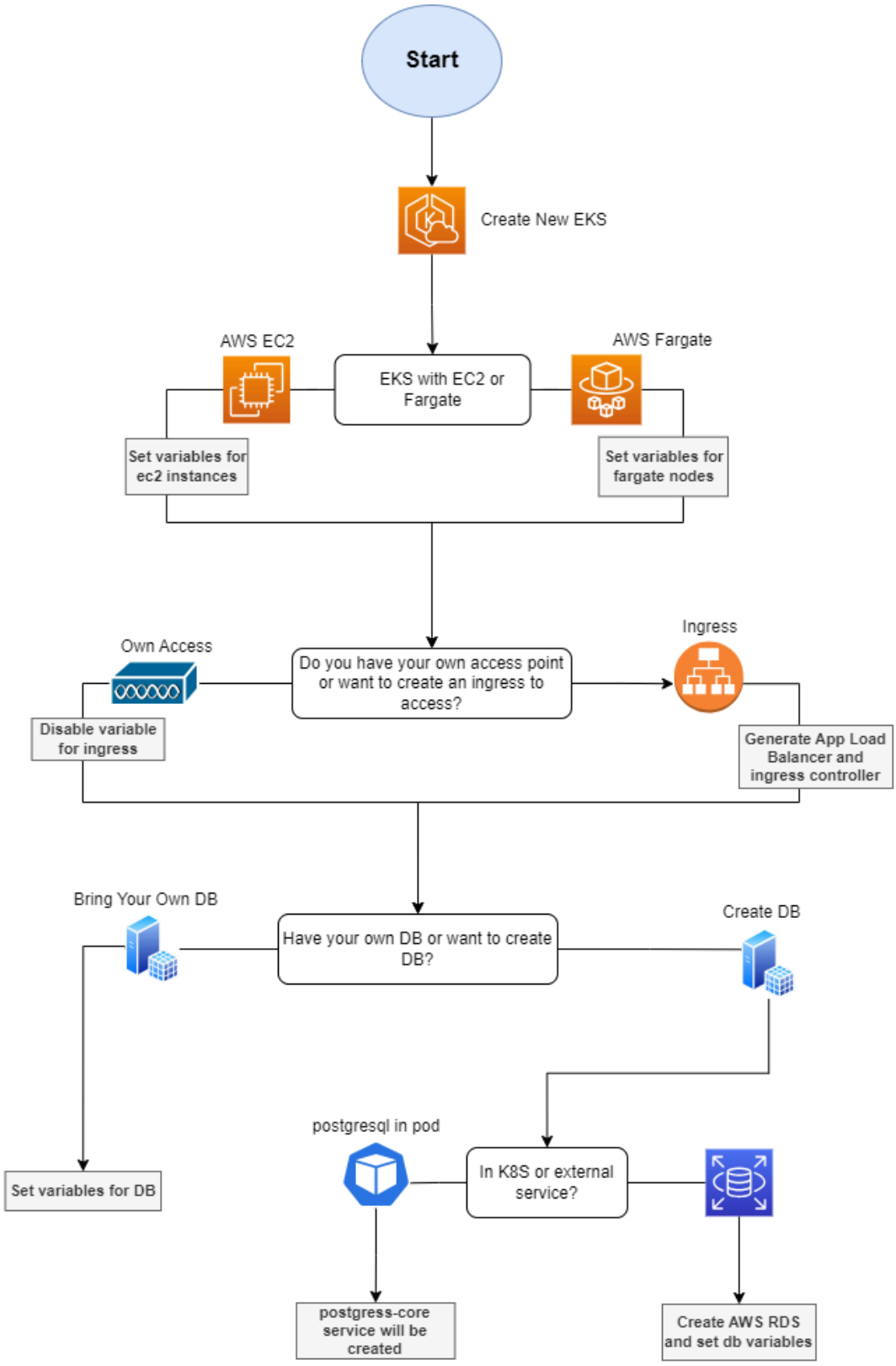
> **Info**
>
> The script will deploy a single Worker Node for the cluster with enough space for 1 replica of MD Core. AWS EC2 Instance size is **c5.2xlarge (8 vCPU & 16 GiB Memory).** Each pod would request 7 vCPU and 8 GiB Memory. To change the request to adapt each pod to the specific case go to values.yml To change the node group go to the terraform file terraform/aws/eks_cluster_module

MetaDefender Core Flowchart Provisioning in AWS

The following flowchart represents how the provisioning script will configure the environment based on the options selected for provisioning AWS EKS.

Summary options to be selected

1. EKS with **EC2** or **Fargate**
2. Access to the K8S cluster. Generate **Ingress** or provide **own** access.
   1. **An Ingress** will be create per each product flag added as parameter to the script
   2. **Own Access**, you decide how to access to the cluster so it won't generate any load balancer for accessing
3. Have your **own database** or create **new database**
   1. **Own database,** will be asked if you want the script to set up the credentials and database host url for you or the script will just indicate the secrets to edit, later on by you, for connecting the MetaDefender Core with your database.
   2. Create new **DB in K8S** or **external DB** that for AWS we will provision a ***RDS instance***


Start
Create New EKS
AWS EC2
EKS with EC2 or Fargate
AWS Fargate
Set variables for ec2 instances
Set variables for fargate nodes
Own Access
Do you have your own access point or want to create an ingress to access?
Ingress
Disable variable for ingress
Generate App Load Balancer and ingress controller
Bring Your Own DB
Have your own DB or want to create DB?
Create DB
postgresql in pod
In K8S or external service?
Set variables for DB
postgress-core service will be created
Create AWS RDS and set db variables

OPSWAT Licensing in GCP

All the AMI published in the GCP Marketplace are Bring Your Own License, that need to be provided by an OPSWAT Sales representative.

To activate the instances where the MetaDefender products are running, it is needed to activate these products providing the LICENSE_KEY.

> **Info**
>
> LICENSE_KEY needs to be requested to Sales before starting to install the product.

MetaDefender Storage Security ask for the LICENSE_KEY when doing the on-boarding process. It is needed to assure the persistence of the database, not to have to reactivate the product on every restart.

> **Info**
>
> MetaDefender Storage Security works together with MetaDefender Core, to see how works the licensing for MetaDefender Core check this page

External Services Configuration

While this documentation focuses on self-managed, locally deployed services for maximum control and customization, MDSS supports any compatible external services — whether self-managed on your own VMs or consumed as managed services from a Cloud Service Provider (CSP).

Protocol Compatibility

MDSS communicates with its external stateful dependencies using **standard open-source protocols only**:

- **PostgreSQL:** standard PostgreSQL wire protocol
- **RabbitMQ:** AMQP 0-9-1 (the standard RabbitMQ protocol)
- **Redis:** standard Redis protocol (RESP)

Any service — managed or self-deployed — that exposes these standard protocols is compatible with MDSS. This is why managed services not explicitly listed in this guide (for example, managed PostgreSQL on Oracle Cloud) also work without compatibility issues. Conversely, managed services that only expose proprietary or different protocols (for example, **Azure Service Bus**, which does not implement AMQP 0-9-1 semantics compatible with RabbitMQ clients) are **not** compatible.

If your cloud provider does not offer a protocol-compatible managed service for a given component, either:

- **Self-deploy the service on a Linux VM** in your cloud environment, following the External Components Setup instructions below, or
- **Use a CSP marketplace alternative** — for example, CloudAMQP provides managed RabbitMQ available through the Azure Marketplace and Google Cloud Marketplace, and can be recommended across any CSP.

The configuration principles outlined in this guide remain the same regardless of whether you choose self-managed or cloud-managed services — simply update the connection URLs and credentials in your `customer.env` file to point to your chosen service endpoints.

Supported Managed Services by Cloud Provider

Component	AWS	Azure	Google Cloud
PostgreSQL	Amazon RDS for PostgreSQL	Azure Database for PostgreSQL	Cloud SQL for PostgreSQL
RabbitMQ	Amazon MQ for RabbitMQ	No native compatible managed service — use CloudAMQP (Azure Marketplace) or self-deploy on a Linux VM	No native compatible managed service — use CloudAMQP (Google Cloud Marketplace) or self-deploy on a Linux VM
Redis	Amazon ElastiCache for Redis	Azure Cache for Redis	Memorystore for Redis

PostgreSQL

Amazon RDS for PostgreSQL

1. In the AWS Console, create an **RDS for PostgreSQL** instance, choosing an instance class that meets the recommended specs.
2. Deploy it in the same VPC as your MDSS hosts and configure the security group to allow inbound traffic on port `5432` from the MDSS hosts only.
3. Connect with the master user and create the `mdss` user, the `MDSS` database, and grants as described in PostgreSQL Configuration (steps 1–2).
4. Copy the instance endpoint into `POSTGRESQL_URL` in `customer.env` on the MDSS host and disable the embedded PostgreSQL container (`DISABLED_SERVICES=postgres`).

Reference: Creating and connecting to a PostgreSQL DB instance (AWS)

Azure Database for PostgreSQL

1. In the Azure Portal, create an **Azure Database for PostgreSQL – Flexible Server** instance sized per the recommended specs.
2. Use private access (VNet integration) or configure firewall rules so only MDSS hosts can reach port `5432`.
3. Connect with the admin user and create the `mdss` user, the `MDSS` database, and grants as described in PostgreSQL Configuration (steps 1–2).
4. Copy the server FQDN into `POSTGRESQL_URL` in `customer.env` and disable the embedded PostgreSQL container (`DISABLED_SERVICES=postgres`).

Reference: Create an Azure Database for PostgreSQL flexible server (Microsoft)

Google Cloud SQL for PostgreSQL

1. In the Google Cloud Console, create a **Cloud SQL for PostgreSQL** instance sized per the recommended specs.
2. Enable a private IP on the VPC shared with your MDSS hosts (or use authorized networks) so only MDSS hosts can reach port `5432`.
3. Connect with the default `postgres` user and create the `mdss` user, the `MDSS` database, and grants as described in PostgreSQL Configuration (steps 1–2).
4. Copy the instance IP into `POSTGRESQL_URL` in `customer.env` and disable the embedded PostgreSQL container (`DISABLED_SERVICES=postgres`).

Reference: Create a Cloud SQL for PostgreSQL instance (Google)

RabbitMQ

Amazon MQ for RabbitMQ (AWS)

1. In the AWS Console, create an **Amazon MQ** broker with the **RabbitMQ** engine type, deployed in the same VPC as your MDSS hosts.
2. Configure the broker's security group to allow inbound traffic on port `5671` (AMQPS) from the MDSS hosts.
3. Create the broker admin credentials and note the AMQPS endpoint.
4. Set `RABBITMQ_URI` (using the `amqps://` scheme), `RABBITMQ_HOST`, `RABBITMQ_PORT`, `RABBITMQ_DEFAULT_USER`, and `RABBITMQ_DEFAULT_PASS` in `customer.env`, and disable the embedded RabbitMQ container (`DISABLED_SERVICES=rabbitmq`).
5. Review the broker's consumer timeout configuration — MDSS long-running scan consumers require the consumer timeout to be disabled or increased, as described in RabbitMQ Configuration.

Reference: Getting started with Amazon MQ for RabbitMQ (AWS)

CloudAMQP (Azure and Google Cloud)

Azure and Google Cloud do not offer a native managed service compatible with the standard RabbitMQ (AMQP 0-9-1) protocol — Azure Service Bus is **not** RabbitMQ-compatible. For these providers, use **CloudAMQP** (managed RabbitMQ available via the CSP marketplaces) or self-deploy RabbitMQ on a Linux VM as described in RabbitMQ Configuration.

1. Subscribe to CloudAMQP through the Azure Marketplace or Google Cloud Marketplace, or sign up directly at cloudamqp.com.
2. Create an instance in the same cloud region as your MDSS deployment; for production, choose a dedicated plan and enable VPC peering to keep traffic private.
3. From the instance details page, copy the AMQPS URL and credentials.
4. Set `RABBITMQ_URI` (using the `amqps://` scheme, including the vhost from the CloudAMQP URL), `RABBITMQ_HOST`, `RABBITMQ_PORT`, `RABBITMQ_DEFAULT_USER`, and `RABBITMQ_DEFAULT_PASS` in `customer.env`, and disable the embedded RabbitMQ container (`DISABLED_SERVICES=rabbitmq`).
5. Disable the consumer timeout for the instance (configurable via the CloudAMQP console) as described in RabbitMQ Configuration.

Reference: CloudAMQP documentation

Self-deployed RabbitMQ on a CSP Linux VM (any provider)

If a marketplace service is not an option, provision a Linux VM (e.g., Azure Virtual Machines, Google Compute Engine, Amazon EC2) in the same network as your MDSS hosts and follow the RabbitMQ Configuration instructions below.

Redis

Amazon ElastiCache for Redis (AWS)

1. In the AWS Console, create an **ElastiCache for Redis** cluster in the same VPC as your MDSS hosts.
2. Configure the security group to allow inbound traffic on port `6379` from the MDSS hosts.
3. Enable authentication (Redis AUTH) and, for production, in-transit encryption (TLS).
4. Copy the primary endpoint into `CACHE_SERVICE_URI`, `CACHE_SERVICE_URL`, and `CACHE_SERVICE_PORT` in `customer.env`, and disable the embedded Redis container (`DISABLED_SERVICES=redis`).

Reference: Getting started with Amazon ElastiCache (AWS)

Azure Cache for Redis

1. In the Azure Portal, create an **Azure Cache for Redis** instance in the same region as your MDSS deployment.
2. Use private endpoint / VNet integration or firewall rules so only MDSS hosts can reach the cache.
3. From **Access keys**, copy the host name, port, and access key.
4. Set `CACHE_SERVICE_URI` (host, port, and the access key as the password), `CACHE_SERVICE_URL`, and `CACHE_SERVICE_PORT` in `customer.env`, and disable the embedded Redis container (`DISABLED_SERVICES=redis`).

Reference: Create an Azure Cache for Redis instance (Microsoft)

Google Cloud Memorystore for Redis

1. In the Google Cloud Console, create a **Memorystore for Redis** instance on the VPC shared with your MDSS hosts.
2. Enable AUTH and, for production, in-transit encryption (TLS).
3. Note the instance IP address, port, and AUTH string.
4. Set `CACHE_SERVICE_URI`, `CACHE_SERVICE_URL`, and `CACHE_SERVICE_PORT` in `customer.env` accordingly, and disable the embedded Redis container (`DISABLED_SERVICES=redis`).

Reference: Create a Memorystore for Redis instance (Google)

Prerequisites

- Multiple VMs in the same network for MDSS deployment
- Separate VMs or managed services for external components
- Administrative access to all systems

Recommended specs:

- PostgreSQL: minimum 8 CPU and 16GB of RAM for the average workload
- RabbitMQ: RabbitMQ System Requirements
- Redis: Redis System Requirements
- MDSS VM: General System Requirements

1. External Components Setup

RabbitMQ Configuration

Installation: Follow the official RabbitMQ installation guide for your distribution.

Configure credentials for remote access:

```
sudo rabbitmqctl add_user <username> <password>
sudo rabbitmqctl set_permissions -p / <username> ".*" ".*" ".*"
sudo rabbitmqctl set_user_tags <username> administrator
```

Enable management interface for monitoring:

```
sudo rabbitmq-plugins enable rabbitmq_management
```

Disable consumer timeout (important for long processing consumers)

Edit RabbitMQ config:

```
sudo nano /etc/rabbitmq/rabbitmq.conf
```

Add:

```
consumer_timeout = undefined
```

Restart RabbitMQ

```
sudo systemctl restart rabbitmq-server
```

PostgreSQL Configuration

Installation: Follow the PostgreSQL installation guide.

Configure for remote access:

1. **Create the Database User and Database**

Connect to PostgreSQL as a superuser and run:

```
-- Create the MDSS user (replace <your_password> with a strong
password)
CREATE ROLE mdss LOGIN PASSWORD '<your_password>';

-- Create the database
CREATE DATABASE "MDSS" OWNER mdss;
```

2. ** Grant Required Permissions

**

Still connected as superuser, switch to the `MDSS` database and run:

```
\c "MDSS"

-- Database connection
GRANT CONNECT ON DATABASE "MDSS" TO mdss;

-- Schema permissions (required for migrations to create tables)
GRANT CREATE, USAGE ON SCHEMA public TO mdss;

-- Full privileges on existing objects
GRANT ALL PRIVILEGES ON ALL TABLES    IN SCHEMA public TO mdss;
GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA public TO mdss;
GRANT ALL PRIVILEGES ON ALL FUNCTIONS IN SCHEMA public TO mdss;
GRANT ALL PRIVILEGES ON ALL PROCEDURES IN SCHEMA public TO mdss;

-- Default privileges for new objects created by migrations
ALTER DEFAULT PRIVILEGES IN SCHEMA public
    GRANT ALL PRIVILEGES ON TABLES    TO mdss;
ALTER DEFAULT PRIVILEGES IN SCHEMA public
    GRANT ALL PRIVILEGES ON SEQUENCES TO mdss;
ALTER DEFAULT PRIVILEGES IN SCHEMA public
    GRANT ALL PRIVILEGES ON FUNCTIONS TO mdss;

-- pg_catalog access (For encryption extensions if needed)
GRANT USAGE ON SCHEMA pg_catalog TO mdss;
```

3. **Configure postgresql.conf:**

```
listen_addresses = '*'

# PostgreSQL Performance Configuration
max_connections = 1000

# Memory settings for optimal database performance
shared_buffers = 16GB
work_mem = 256MB
temp_buffers = 64MB
maintenance_work_mem = 2GB
effective_cache_size = 24GB

# WAL (Write-Ahead Logging) configuration
wal_level = minimal
max_wal_senders = 0
max_replication_slots = 0
max_wal_size = 2GB
min_wal_size = 160MB
```

4. **Increase file limits in sysctl.conf:**

```
fs.file-max = 50000
```

5. Update systemd service file `/usr/lib/systemd/system/postgresql.service` to increase file limits for PostgreSQL user.
6. Restart PostgreSQL:

```
sudo systemctl daemon-reload && sudo systemctl restart
postgresql.service
```

7. **Configure customer.env on the MDSS Host**

On the MDSS host, edit /etc/mdss/customer.env (in your MDSS installation directory) and add:

```
POSTGRESQL_URL=Host=<pg-host-ip>;Port=5432;Username=mdss;Password=
<your_password>;Database=MDSS;Timeout=60;CommandTimeout=60
```

Replace with the IP or hostname of your PostgreSQL server and <your_password> with the password you set in Step 1.

8. **Disable the Embedded PostgreSQL Container**

Add the following to customer.env:

```
DISABLED_SERVICES=postgres
```

Redis Configuration

> **Note:** Use external Redis only when deploying MDSS services on multiple nodes. For single-node deployments, the local Redis instance provides better latency.

Installation: Follow the Redis installation guide.

Configure password and remote access in `/etc/redis/redis.conf`:

```
requirepass your_password_here
bind 0.0.0.0
```

2. MDSS Configuration

Configure External Services

Edit `customer.env` file with your external service configurations:

```
# Configure external RabbitMQ
RABBITMQ_URI=amqp://mdss:mdss@<rabbitmq-host>:5672
RABBITMQ_HOST=<rabbitmq-host>
RABBITMQ_PORT=5672
RABBITMQ_DEFAULT_PASS=mdss
RABBITMQ_DEFAULT_USER=mdss

# Optional: Configure external Redis instance
CACHE_SERVICE_URI=<redis-
host>:6379,user=default,password=mdss,syncTimeout=10000
CACHE_SERVICE_URL=<redis-host>
CACHE_SERVICE_PORT=6379

# Configure external database
POSTGRESQL_URL=Host=<pg-host-ip>;Port=5432;Username=mdss;Password=
<your_password>;Database=MDSS;Timeout=60;CommandTimeout=60

# Disable all the local services
DISABLED_SERVICES=postgres,redis,rabbitmq

# Example performance tuning parameters for higher workloads
RABBITMQ_SCANNING_PREFETCH_COUNT=5
RABBITMQ_LOAD_BALANCER_PREFETCH_COUNT=60
RABBITMQ_NFS_DISCOVERY_PREFETCH_COUNT=60
RABBITMQ_DISCOVERY_PREFETCH_COUNT=40
DISCOVERY_THROTTLER_MAX_PENDING_FILES=10000
```

3. Performance Monitoring

Monitor RabbitMQ Queues

Access the RabbitMQ management interface at `http://<rabbitmq-host>:15672` to monitor queue sizes.

Key queue to monitor:

- `object_ready_for_scan_queue`: Shows files waiting to be scanned

If this queue accumulates messages, consider increasing the number of scanning services.

Prefetch Count Optimization

When running multiple scanning services, decrease the scanning prefetch count to distribute load more evenly: RABBITMQ_SCANNING_PREFETCH_COUNT=5

Adjust other prefetch counts based on your queue sizes and performance requirements.

5. Best Practices

1. **Resource Allocation:** Ensure adequate CPU and memory for both MDSS and external service VMs
2. **Network Latency:** Keep all components in the same network to minimize latency
3. **Monitoring:** Regularly monitor RabbitMQ queues and system resources
4. **Scaling:** Start with fewer MDSS instances and scale up based on queue monitoring
5. **Engine Selection:** Use minimal engines required for your use case to improve performance

Troubleshooting

Common Issues:

- **High queue buildup:** Increase scanning service containers or optimize prefetch counts
- **External service timeouts:** Check network connectivity and service configuration
- **Resource exhaustion:** Monitor CPU/memory usage and scale resources accordingly

Log Locations:

- MDSS logs: `/etc/mdss/services_logs/`

This configuration enables horizontal scaling of MDSS deployments while maintaining shared state through external services, providing improved performance for high-volume scanning workloads.

Production Considerations

Security

Encrypted Connections: Always use secure connection protocols (TLS/SSL) for all communications between MDSS instances and external services. Configure RabbitMQ with AMQPS, and Redis with TLS encryption.

Network Security: Implement network-level security by restricting access to external services only from authorized MDSS hosts using firewalls, VPCs, or security groups. Deploy services in private subnets when possible.

Authentication & Authorization: Create dedicated service accounts with minimal required privileges for MDSS access.

High Availability

Configure external services for high availability using their native clustering or replication features:

- **PostgreSQL**: Use replication to a secondary database
- **RabbitMQ:** Configure clustering with HA policies
- **Redis:** Use Redis Sentinel or Redis Cluster

For managed cloud services, enable multi-AZ deployments and automatic failover capabilities provided by your cloud provider.

Monitoring & Alerting

Implement comprehensive monitoring for:

- Service availability and response times
- Resource utilization (CPU, memory, disk, network)
- Queue depths and processing rates
- Connection pool health
- Error rates and failed operations

Set up alerting for critical thresholds that could impact MDSS performance.

Backup & Disaster Recovery

Establish regular backup procedures and test recovery processes for all external services. For managed services, configure automated backups with appropriate retention policies.

Performance Optimization

- Configure connection pooling based on your concurrent load requirements
- Set appropriate resource limits and file descriptors
- Monitor and tune service-specific performance parameters
- Plan capacity based on expected MDSS throughput

Documentation References

For detailed configuration guidance, refer to the official production documentation:

- PostgreSQL Documentation
- RabbitMQ Production Checklist
- Redis Security Guidelines

For managed cloud services, consult your cloud provider's best practices documentation for the specific services you're using.

ON-PREMISE DEPLOYMENT

On-Premise Deployment Overview

Before installation

Before you begin the installation, ensure that your On-premise environment meet the system requirements. If you are installing MetaDefender Storage Security on the same server as MetaDefender Core, the server must meet the cumulative system requirements of all the products.

Installation General Steps

1. Download the package of your choice from the My OPSWAT
2. Check the Production Considerations
3. Install the package on your computer based on Installation Methods
4. Open a web browser and point to http:// [by default, port 80 is used]
5. Complete the installation and proceed with the onboarding

Installation notes

- **Internet Connectivity:** The installation requires internet access to download packages from the container registry
- **.NET Framework:** On Windows, the installer will download and apply .NET Framework 4.8 if it is not already installed
- **Support:** If you encounter issues, open a support case and include the "Metadefender*" files located in `C:\Users\<user>\AppData\Local\Temp`

Offline Installation

If you need to perform an offline installation, please refer to the Linux Offline Installation for detailed instructions on how to install MetaDefender Storage Security without an active internet connection. This guide includes steps for preparing necessary dependencies.

Production Considerations

This section of the user guide focuses on essential production considerations. When deploying in a production environment, it is recommended to follow this guide to ensure optimal security and reliability. Key steps include:

1. **Setting up HTTPS**: Ensure that HTTPS is configured to secure communication between clients and servers.
2. **Using an External Database**: Instead of the built-in database, configure an external database to handle your data for better performance and scalability.
3. **OS-Specific Tasks**: Perform operating system-specific tasks that enhance the security and reliability of your system.

Following these guidelines will help you maintain a secure and efficient production environment.

Depending on your deployment type, please choose between:

- Production considerations for Unix-based deployments
- Production considerations for Windows-based deployments

Windows Deployments

This page describes in detail how you can achieve the following tasks:

- Use an external PostgreSQL server instead of the built-in database
- Configure HTTPS communication for the web server

Use an external database

Production deployments of MetaDefender Storage Security should ensure high availability and/or load-balancing at the database level by using an external PostgreSQL (or any compatible service) instead of the built-in database that is included with the basic installation.

> **Info**
>
> We recommend using a version of PostgreSQL that is the same as the built-in database version from the requirements page.

How to setup an external PostgreSQL in MetaDefender Storage Security

> **Info**
>
> These steps should be performed immediately after the installation (before completing the onboarding or any other UI configuration) because any existing data will be lost.

1. Ensure that your external PostgreSQL is properly configured and ready to accept remote connections

Note: it is recommended to setup access control for your external database as well as taking the necessary network security measures to ensure that only the server running MetaDefender Storage Security can access the database.

1. Locate the configuration file `customer.env` created by the installer (by default it is located at *C:\Program Files\OPSWAT\MetaDefender Storage Security\config*)
2. Add the following configuration line:

```
POSTGRES_USER=user
POSTGRES_PASSWORD=password
POSTGRES_DB=dbName
POSTGRESQL_URL=Host=postgres;Port=5432;Username=user;Password=password;
Database=dbName
```

4. Please check the connection string documentation for more information. Make sure you add “mdss” as the target database as shown in the example above.
5. Save the file.
6. Reinstall the internal components by running the following PowerShell command

```
PS> .\mdss.ps1 -c refresh
```

7. Continue to the onboarding process.

PostgreSQL SSL Configuration

To enable SSL/TLS certificate validation for the PostgreSQL connection, update the `POSTGRESQL_URL` variable in the `customer.env` file.

File Location

By default, the `customer.env` file is located at:

C:\Program Files\OPSWAT\MetaDefender Storage Security\config

The installer creates this file automatically.

Configuring POSTGRESQL_URL

The `POSTGRESQL_URL` variable can include additional parameters for SSL/TLS. By default SSL Mode is set to “prefer”.

```
POSTGRESQL_URL=Host=postgres;Port=5432;Username=user;Password=password;
Database=dbName;SSL Mode=VerifyFull;Root Certificate=<path to root CA
certificate>
```

SSL Mode Options

- **prefer** (default): Attempts to connect using SSL. If SSL fails, falls back to unencrypted. **No certificate validation.**
- **require**: Requires SSL encryption. **Certificate validation is skipped** — allows self-signed, expired, or otherwise invalid certifications.
- **verify-full**: Requires SSL and performs **full certificate validation**, including hostname match and trusted CA.

Important Notes

- If **certificate validation is required**, use `verify-full` and provide a valid CA-signed certificate via the `Root Certificate` parameter.
- If using a **self-signed or otherwise invalid certificate**, use `require`, which skips validation but still encrypts the connection.
- The `Root Certificate` must point to the CA file if using `verify-ca` or `verify-full`.

How to modify it

Set the parameter in your **customer.env** file. Please find here more details on how to update the configuration file.

PostgreSQL advanced setup

For special use cases you may need to backup your database or restore it. MetaDefender Storage Security allows you to do this by using the following commands

```
PS> .\mdss.ps1 -u export_db
```

Running this command will create a dump file in the install directory. This file can be use afterwards as a restore file using the import command:

```
PS> .\mdss.ps1 -u import_db
```

> **Info**

> The import_db utility will use the latest file as restore point

> **CRITICAL: Stop MDSS Service Before Database Import**
>
> Data corruption may occur if the MDSS service is running during database import.
>
> Follow these steps:
>
> **1.** Stop the service: mdss -c stop **2.** Verify it's stopped: mdss -c status **3.** Import your database **4.** Restart the service: mdss -c start
>
> **Allow 30 seconds between stop and start commands.**
>
> Failure to follow this procedure may result in data loss.

Configure HTTPS communication for the web server

Production deployments should ensure that any HTTP traffic between clients (browsers or other API client) and MetaDefender Storage Security is encrypted using HTTPS.

Click here for detailed instructions on how to setup a certificate for NGINX web server.

Linux Deployments

This page describes in detail how you can achieve the following tasks:

- Use an external PostgreSQL server instead of the built-in database
- Configure HTTPS communication for the web server
- Install MetaDefender Storage Security on a different disk

Use an external database

Production deployments of MetaDefender Storage Security should ensure high availability and/or load-balancing at the database level by using an external PostgreSQL (or any compatible service) instead of the built-in database that is included with the basic installation.

> **Info**
>
> We recommend using a version of PostgreSQL that is the same as the built-in database version from this page.

How to setup an external PostgreSQL in MetaDefender Storage Security

The following steps should be performed before initializing MetaDefender Storage Security for the first time (i.e before the **mdss -u init** command from the Installation Methods).

> **Info**
>
> These steps can be performed after the installation or at any other time but the existing data (if any) will be lost. In this case, the last step should be replaced with a restart instead of a start command.

1. Ensure that your external PostgreSQL is properly configured and ready to accept remote connections

Note: it is recommended to setup access control for your external database as well as taking the necessary network security measures to ensure that only the server running MetaDefender Storage Security can access the database.

2. Locate the configuration file created by the installer in **/etc/mdss/customer.env**
3. Add the following configuration line:

```
POSTGRES_USER=user
POSTGRES_PASSWORD=password
POSTGRES_DB=dbName
POSTGRESQL_URL=Host=postgres;Port=5432;Username=user;Password=password;
Database=dbName
```

4. Please check the connection string documentation for more information. Make sure you add “mdss” as the target database as shown in the example above.
5. Save the file.
6. Initialize MetaDefender Storage Security by running the following command:

```
sudo mdss -u init
```

7. Return to the steps in Installation Methods and continue the installation.

PostgreSQL SSL Configuration

To enable SSL/TLS certificate validation for the PostgreSQL connection, update the `POSTGRESQL_URL` variable in the `customer.env` file.

File Location

By default, the `customer.env` file is located at:

C:\Program Files\OPSWAT\MetaDefender Storage Security\config

The installer creates this file automatically.

Configuring POSTGRESQL_URL

The `POSTGRESQL_URL` variable can include additional parameters for SSL/TLS. By default SSL Mode is set to “prefer”.

```
POSTGRESQL_URL=Host=postgres;Port=5432;Username=user;Password=password;
Database=dbName;SSL Mode=VerifyFull;Root Certificate=<path to root CA
certificate>
```

SSL Mode Options

- **prefer** [default]: Attempts to connect using SSL. If SSL fails, falls back to unencrypted. **No certificate validation.**
- **require**: Requires SSL encryption. **Certificate validation is skipped** — allows self-signed, expired, or otherwise invalid certifications.
- **verify-full**: Requires SSL and performs **full certificate validation**, including hostname match and trusted CA.

Important Notes

- If **certificate validation is required**, use `verify-full` and provide a valid CA-signed certificate via the `Root Certificate` parameter.
- If using a **self-signed or otherwise invalid certificate**, use `require`, which skips validation but still encrypts the connection.
- The `Root Certificate` must point to the CA file if using `verify-ca` or `verify-full`.

How to modify it

Set the parameter in your **customer.env** file. Please find here more details on how to update the configuration file.

PostgreSQL advanced setup

For special use cases you may need to backup your database or restore it. MetaDefender Storage Security allows you to do this by using the following commands

```
sudo mdss -u export_db
```

Running this command will create a dump file in `/etc/mdss/db_[...].tar` this file can be use afterwards as a restore file using the import command:

```
sudo mdss -u import_db
```

> **Info**
>
> Product versions 3.4.2 and above do not support importing databases from earlier versions (less than 3.4.2). When using the `import_db` utility on these versions, it will automatically restore the database from the most recent backup file named `db_[...].tar`.

> **CRITICAL: Stop MDSS Service Before Database Import**
>
> > Data corruption may occur if the MDSS service is running during database import.
> >
> > Follow these steps:
> >
> > **1.** Stop the service: mdss -c stop **2.** Verify it's stopped: mdss -c status **3.** Import your database **4.** Restart the service: mdss -c start
> >
> > **Allow 30 seconds between stop and start commands.**
> >
> > Failure to follow this procedure may result in data loss.

Configure HTTPS communication for the web server

Production deployments should ensure that any HTTP traffic between clients (browsers or other API client) and MetaDefender Storage Security is encrypted using HTTPS.

Click here for detailed instructions on how to setup a certificate for NGINX web server.

Install MetaDefender Storage Security on a different disk

The following steps should be performed before initializing MetaDefender Storage Security for the first time (i.e before the **mdss -u init** command from the Linux Installation).

> **Info**
>
> These steps should be performed right after the installation of Docker so that no data is lost.

1. First make sure Docker is not running and the default directory is clean
2. Remove existing images and volumes

```
sudo docker rm -f $(docker ps -aq); docker rmi -f $(docker images -q)
```

3. Stop Docker

```
sudo systemctl stop docker
```

4. Remove the default Docker location

```
sudo rm -rf /var/lib/docker
```

5. Create a new empty directory in the default location

```
sudo mkdir /var/lib/docker
```

6. Create a new empty directory on the new partition

```
sudo mkdir /<PATH_TO_NEW_LOCATION>
```

7. Mount the new location in the default directory

```
sudo mount --rbind //<PATH_TO_NEW_LOCATION> /var/lib/docker
```

8. Start back the docker service

```
sudo systemctl start docker
```

9. Initialize MetaDefender Storage Security by running the following command:

```
sudo mdss -u init
```

Installation Methods

The different installation methods depend by the OS and if they are installed using the command line, the wizard or the offline option.

- Deploy to a Windows server
- Deploy to a Linux Server
- Deploy to a Linux Server offline

Windows Installation

Windows package using Command Line (.msi)

From the command line interface, it is possible to install the product by executing this PowerShell command in an **Administrator** session:

```
PS>msiexec /i metadefender-storage-security.msi
```

where the possible keys and their default values are the following:

Key	Description
/quiet or /passive	Suppress the installation wizard
–% INSTALLFOLDER	Customize the installation directory
WEB__CLIENT__PORT	80 (Web client (UI) port)
API__GATEWAY__PORT	8005
LICENSING__SERVICE__PORT	5001
POSTGRESQL_PORT	5432
SMB__PORT__RANGE_START	6002(SMB starting port. Reserves 10 ports total: 5 consecutive from this value and 5 more offset by 1000)
SFTP__SERVICE__PORT	5003
NFS__SERVICE__PORT	5004
PG__ADMIN__PASSWORD	PostgreSQL superuser password
MODULE__AMAZON__S3	Enable Amazon S3 module (1=enabled, 0=disabled)
MODULE__AZURE__BLOB	Enable Azure Blob module (1=enabled, 0=disabled)
MODULE__AZURE_FILES_	Enable Azure Files module (1=enabled, 0=disabled)
MODULE__GOOGLE__CLOUD	Enable Google Cloud module (1=enabled, 0=disabled)
MODULE__ALIBABA__CLOUD	Enable Alibaba Cloud module (1=enabled, 0=disabled)
MODULE_SMB	Enable SMB module (1=enabled, 0=disabled)
MODULE_BOX	Enable Box module (1=enabled, 0=disabled)
MODULE__ONEDRIVE_SHAREPOINT_	Enable OneDrive / SharePoint Online module (1=enabled, 0=disabled)
MODULE_SFTP	Enable SFTP module (1=enabled, 0=disabled)
MODULE_NFS	Enable NFS module (1=enabled, 0=disabled)
MODULE_FTP	Enable FTP module (1=enabled, 0=disabled)
MODULE__OPSWAT__MFT	Enable Oracle SDK module (1=enabled, 0=disabled)
MODULE__ORACLE__SDK	Enable OPSWAT MFT module (1=enabled, 0=disabled)
MODULE__SHAREPOINT__ONPREM	Enable SharePoint On-Prem module (1=enabled, 0=disabled)

Step by step using Install Wizard

The Install Wizard is only for the Windows installer (.msi file).

Before you begin, please make sure to read the following pages in order to install the necessary requirements for each system.

1. Navigate to MetaDefender Storage Security installer location
2. Run it with Administrator privileges.

Important: If a local antivirus or endpoint protection solution is active, you must configure an exclusion for the MetaDefender Storage Security installation directory before running the installer. Failure to do so may result in blocked components, incomplete installation, or unstable runtime behavior. Refer to How to Exclude the OPSWAT Folder from Windows Defender? for exclusion instructions.

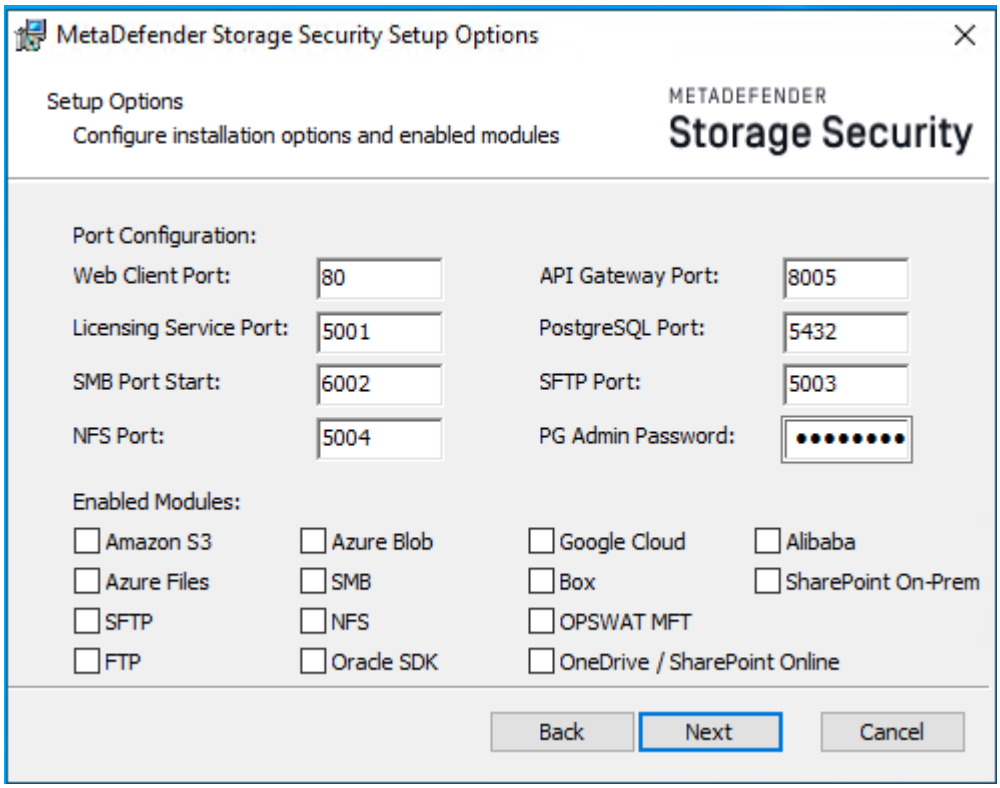
2. To proceed with the installation, read the License Agreement and check **I accept the terms in the License Agreement** if you accept it.



3. (Optional) **Configure Installation Options**
    1. Review the installation options presented in the setup wizard.
    2. Configure the **Port Configuration** section:
        1. Web Client Port: Default is 80
        2. API Gateway Port: Default is 8005

3. Licensing Service Port: Default is 5001
4. PostgreSQL Port: Default is 5432
5. SMB Port Range Start: Default is 6002. This is the starting port of a range. When set, 10 ports will be reserved: 5 consecutive ports starting from this value (e.g., 6002-6006) and another 5 consecutive ports offset by 1000 (e.g., 7002-7006).
6. SFTP Service Port: Default is 5003
7. NFS Service Port: Default is 5004

3. When installing MetaDefender Storage Security, you can choose which storage connection modules to enable. Each module allows integration with different storages. Select the desired **Enabled Modules** by checking the corresponding boxes
4. Click Next to proceed with the installation

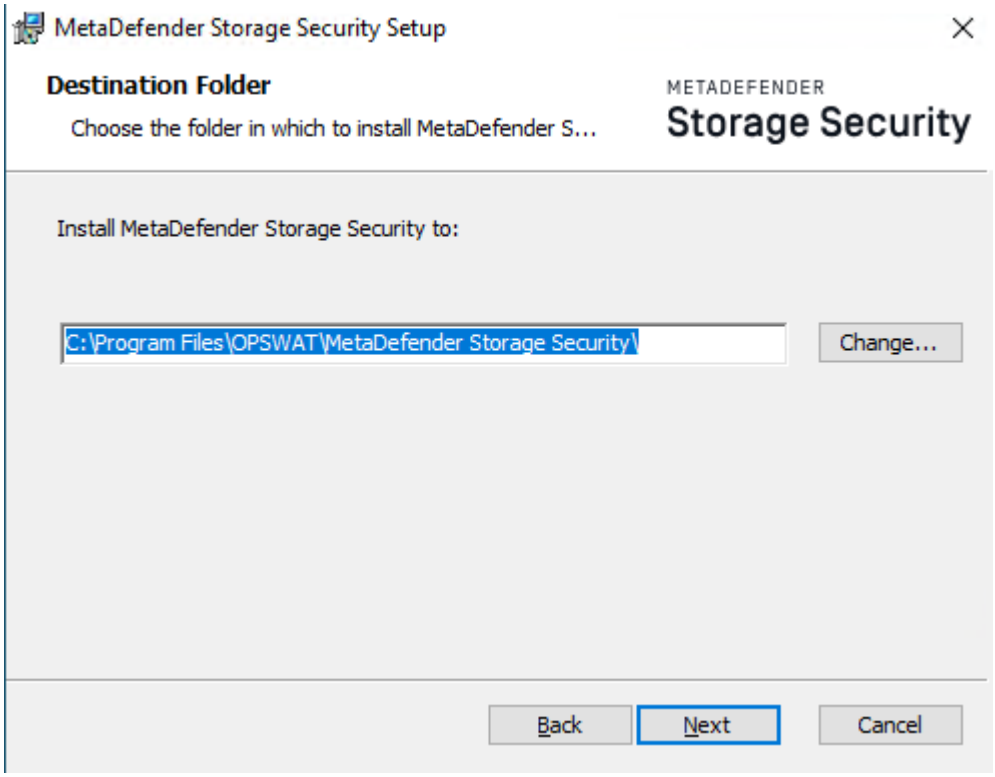


Info — SharePoint On-Prem Module

Enabling this module requires the installation of additional SharePoint Client Components. These will be installed automatically on the next system reboot, or immediately by running the following command from a PowerShell session with Administrator privileges, from the scripts folder, once the main installation has completed: `.\mdss.ps1 -c refresh`

Info

> Port configuration and additional modules can be added later by modifying the customer.env file. See: Custom configuration

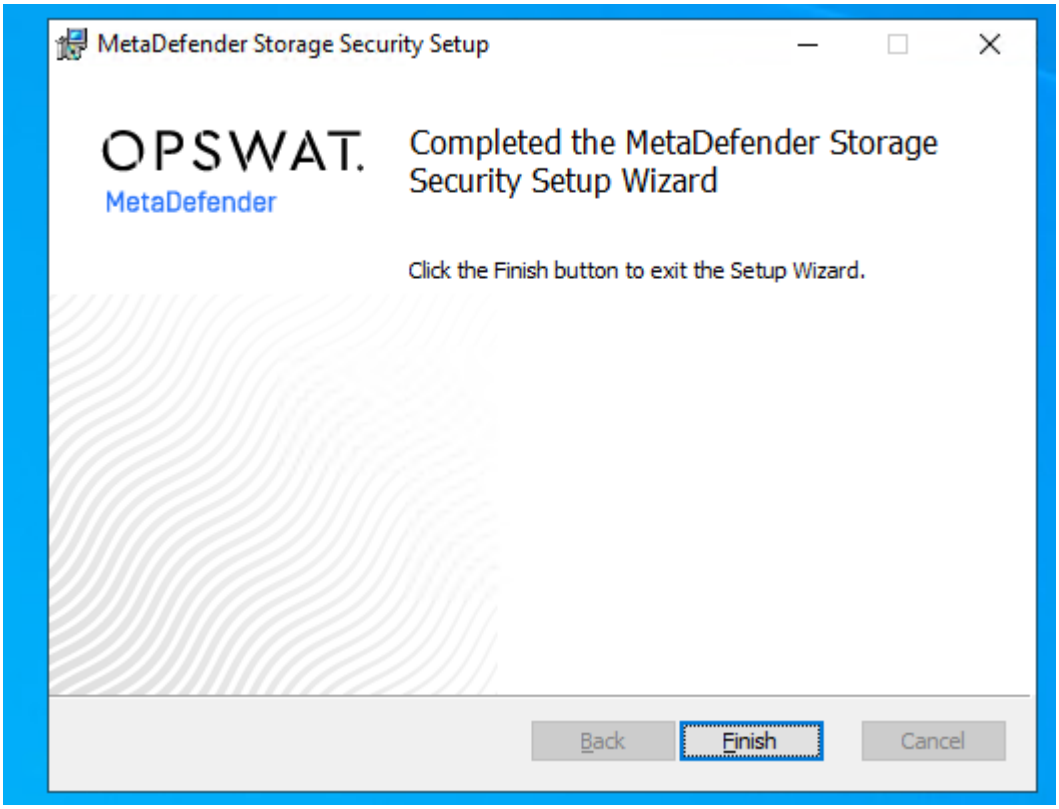


4. To choose another installation path click **Change** and then **Browse** to the desired location. Confirm the new location by clicking **OK**.
5. Click **Next**.
6. Click **Install**.
7. Please wait while the product is being configured.

Note: this operation may take more than 15 minutes to complete



8. Installation completed successfully.



9. Press **Finish.**

Next steps

Production deployments should follow the Production Considerations in order to set up a remote PostgreSql database and enable HTTPS.

After that, please follow the setup in the newly opened browser window in order to create a local administrator and complete the installation.

Please see the onboarding page for more details.

Linux Installation

Preliminary notes

Before you begin the installation, please ensure that the system requirements are met.

If the MetaDefender Storage Security installer package dependencies are not installed on your system the installer will attempt to automatically download them over the internet.

Acquire the package

In order to acquire the package please visit https://www.opswat.com/solution

> **Info**
>
> To limit the required resources, use the `ENABLED_MODULES` and the `DISABLED_SERVICES` environment variables in the `customer.env` file to select which modules to install when deploying MetaDefender Storage Security, you can follow these steps:
>
> 1. Locate the `customer.env` file in your MetaDefender Storage Security deployment. This file contains environment variables used for customization.
> 2. Open the `customer.env` file in a text editor.
> 3. Add the `ENABLED_MODULES` environment variable to the file. The variable should be in the format `ENABLED_MODULES=<module_list>`, where `<module_list>` is a comma-separated list of the modules you want to enable. For example, if you want to enable modules Amazon S3, Google Cloud, and Azure Blob storage units, your `customer.env` file should include the following line: ENABLED_MODULES=azureblob,amazonsdk,googlecloud
> 4. Save the `customer.env` file.
> 5. Proceed with the deployment of MetaDefender Storage Security.
>
> Recommended Article: How to Enable Specific Modules in the Configuration?

Please note that an online installation involves downloading the required `docker` images from Docker Hub. If image pulls fail, you may have reached Docker Hub's rate limits, especially when multiple services pull from the same IP address.

To address this, please consider one of the following solutions:

- Use `docker login` to increase your pull limit
- Implement image caching or registry proxies
- Stagger deployments to avoid concurrent pulls

Advanced installation

We recommend that production deployments use an external database and ensure that web traffic is encrypted. For detailed information on how to configure an external database or HTTPS see advanced installation section:

- Production Consideration Linux Deployments
- Production Considerations Windows Deployments

Debian / Ubuntu package (.deb)

1. Update your packages

```
sudo apt update
```

2. Install the necessary package dependencies

```
sudo apt install jq curl gnupg-agent software-properties-common
```

3. Move to the folder containing the installer and install it

```
sudo dpkg -i <name of the file>.deb
```

4. After the installation is completed, check if everything went fine

```
man mdss
```

or using the help menu

```
sudo mdss -h
```

5. Run the following command in order to initialize MetaDefender Storage Security

```
sudo mdss -u init
```

6. Start the service

```
sudo mdss -c start
```

7. Optionally, you can check the status using the following command:

```
sudo mdss -c status
```

8. Open a browser and navigate to the web interface http:// to configure your deployment.

Red Hat Enterprise Linux / CentOS / Rocky package (.rpm)

> **Info**
>
> Please note that Docker Engine is officially supported only on RHEL s390x architecture, but you may be able to install it manually following the CentOS installation steps: https://docs.docker.com/engine/install/centos/
>
> On Rocky Linux, it is recommended to use Podman , as Podman is officially supported by Red Hat.

> **Info**
>
> On RHEL 8, the default iptables FORWARD chain policy is set to DROP. Podman's CNI networking does not automatically add forwarding rules for external interface to bridge traffic, which will cause the web interface to be unreachable from outside the host even if the correct ports are open in the firewall or security group.

In case the FORWARD chain policy is set to DROP, here are the commands to switch it to ACCEPT:

```
# External → container (new connections)
iptables -I FORWARD -i eth0 -o cni-podman1 -j ACCEPT

# Container → external (return traffic for established connections)
iptables -I FORWARD -i cni-podman1 -o eth0 -m state --state
RELATED,ESTABLISHED -j ACCEPT
```

1. Update your packages

```
sudo yum -y update
```

2. Move to the folder containing the installer and install it

```
sudo yum install -y <name of the file>.rpm
```

3. After the installation is completed, check if everything went fine

```
sudo man mdss
```

or using the help menu

```
sudo mdss -h
```

4. Run the following command in order to initialize MetaDefender Storage Security

```
sudo mdss -u init
```

Note: If you don't have docker already installed, the installer will do that for you, but you will be prompted to sign out and sign back in. This is necessary because your current user needs to be added to the docker group.

5. Start the service

```
sudo mdss -c start
```

6. Optionally, you can check the status using the following command:

```
sudo mdss -c status
```

7. Open a browser and navigate to the web interface http:// to configure your deployment.
8. If you are using firewall (on CentOS8 and RHEL 8) you may need to update it's policies:

```
# Check what interface docker is using, e.g. 'docker0'
ip link show

# Check available firewalld zones, e.g. 'public'
sudo firewall-cmd --get-active-zones

# Check what zone the docker interface it bound to, most likely 'no
zone' yet
sudo firewall-cmd --get-zone-of-interface=docker0

# So add the 'docker0' interface to the 'public' zone. Changes will be
visible only after firewalld reload
sudo nmcli connection modify docker0 connection.zone public

# Masquerading allows for docker ingress and egress (this is the juicy
bit)
sudo firewall-cmd --zone=public --add-masquerade --permanent
# Optional open required incomming ports (wasn't required in my tests)
# sudo firewall-cmd --zone=public --add-port=443/tcp
# Reload firewalld
sudo firewall-cmd --reload
# Reload dockerd
sudo systemctl restart docker
```

Podman Configuration

MDSS can also run using the Podman container engine instead of the default Docker one on RHEL operating systems. `Podman`, `podman-docker` and `docker-compose` need to be installed and running before installing MDSS.

```
# stop MDSS if is already installed
sudo mdss -c stop

# install podman, podman-docker and docker-compose
sudo yum install podman
sudo yum install podman-docker
sudo curl -SL
https://github.com/docker/compose/releases/download/v2.15.1/docker-
compose-linux-x86_64 -o /usr/local/bin/docker-compose
sudo chmod +x /usr/local/bin/docker-compose

sudo systemctl enable podman.socket
sudo systemctl start podman.socket

# to disable selinux permanetly 'SELINUX=disabled' needs to be set in
the following config file
sudo vim /etc/selinux/config

# reboot machine for changes take effect
sudo reboot
```

Once the Podman and Docker components are installed, proceed with the installation of MetaDefender Storage Security (MDSS). You can skip the installation if MDSS is already installed.

After installation, MDSS must be configured to skip the default Docker engine checks. This is achieved by setting `SKIP_DOCKER_CHECKS=yes` in the `/etc/mdss/customer.env` configuration file.

```
# install additional MDSS dependencies (skip this if MDSS is already
installed)
sudo subscription-manager repos --enable codeready-builder-for-rhel-
8-$(arch)-rpms
sudo yum -y install https://dl.fedoraproject.org/pub/epel/epel-release-
latest-8.noarch.rpm
sudo yum install lvm2
sudo yum install wget

# install MDSS (skip this if MDSS is already installed)
sudo rpm -i mdss-x.x.x-1.noarch.rpm

# edit customer.env and add SKIP_DOCKER_CHECKS=yes
sudo vim /etc/mdss/customer.env

# start MDSS
sudo mdss -c start
```

Configure Automatic Service Startup at Boot on RHEL and Rocky Linux with Podman

Due to a technical limitation, on **RHEL and Rocky Linux**, MDSS will not start automatically after machine restarts. To enable this option, please follow these steps:

1. Create a service file

```
sudo vi /etc/systemd/system/mdss.service
```

2. Paste the following content

```
[Unit]
    Description=MDSS Stack
    After=network-online.target
    Wants=network-online.target

    [Service]
    Type=oneshot
    RemainAfterExit=yes
    ExecStart=mdss -c start

    [Install]
    WantedBy=multi-user.target
```

3. Save and exit the file (Esc + :wq!)
4. Enable the service

```
sudo systemctl daemon-reload
sudo systemctl enable mdss.service
```

That's it. To confirm the changes were applied successfully, please restart your VM and then run **sudo mdss -c status** to make sure MDSS is up and running after reboot.

Linux Offline Installation

This guide provides detailed instructions for installing MetaDefender Storage Security and its dependencies on machines with limited or no internet connectivity. A machine connected to the internet will be needed to download the dependencies manually and copy them to the offline machine.

Installing Binary Packages

You will need to download and install the following binary packages for your respective operating system:

Debian/Ubuntu

```
curl, openssl, sudo, apt-utils, ca-certificates, jq, gnupg-agent,
iproute2, apt-transport-https,  software-properties-common
```

RedHat/CentOS

```
curl, openssl, sudo, yum-utils, ca-certificates, jq, gnupg2, iproute,
lvm2, wget, device-mapper-persistent-data
```

> **Info**
>
> **Note:** For detailed instructions, refer to the guide for Debian/Ubuntu or CentOS/RHEL

Option 1: Using installers

This option uses the the official installation methods for docker and docker-compose to create an offline docker environment where the MDSS installer from the MyOPSWAT portal can be used to deploy MDSS containers. If for some reason this method cannot be used on the target deployment machine then skip to **Option 2** below.

Installing Docker and Docker Compose

To be able to install the dependencies offline, you need a machine connected to the internet to download the required packages. Later, the packages will be copied to the offline machine.

To download the dependencies, follow the official guide for Docker Engine and Docker Compose

The compose plugin for docker can be installed only manually when in an offline environment using the following commands (also available in the official instructions in the link above):

```
mkdir -p /usr/local/lib/docker/cli-plugins/
curl -SL
https://github.com/docker/compose/releases/download/v2.28.0/docker-
compose-linux-x86_64 -o /usr/local/lib/docker/cli-plugins/docker-
compose

sudo chmod +x /usr/local/lib/docker/cli-plugins/docker-compose
```

Installing MetaDefender Storage Security package

After the prerequisites above have been set up, you can run the MetaDefender Storage Security installer to setup the compose files and the mdss command line.

Debian/Ubuntu

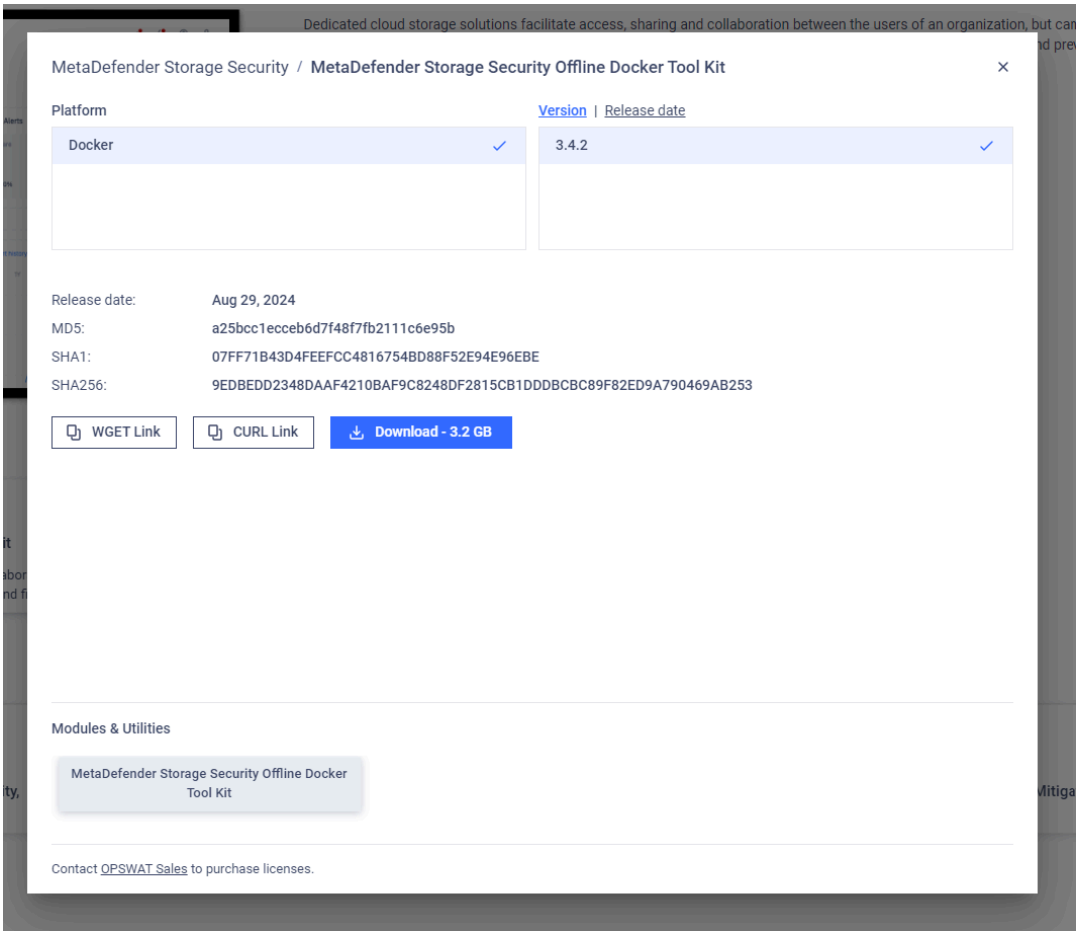
```
sudo dpkg -i <name of the file>.deb || sudo apt-get install -f
```

RedHat/CentOS

```
sudo yum install -y <name of the file>.rpm
```

Loading Docker images

MetaDefender Storage Security is composed of several Docker images that need to be pulled from an online repository. For offline installations, these images are available on the MyOPSWAT portal under **MetaDefender Storage Security** in the **MetaDefender Storage Security Offline Docker Toolkit** section:



Next, you need to extract the `mdss.tar` archive and transfer it to the offline machine. Once the file is on the offline machine, use the following command to load the Docker images:

```
docker load -i <archive_path>\mdss.tar
```

Starting MetaDefender Storage Security

Finally, MDSS can be started using the regular startup command:

```
sudo mdss -c start
```

Option 2: using bundled binaries

Using this method you will only need to download the same MetaDefender Storage Security Offline Docker Toolkit as above without needing to pre-install docker and docker-compose or use the MDSS installer. It's still recommended to have all prerequisites installed before continuing.

Download and extract the offline toolkit

The offline toolkit is available on the **MyOPSWAT** portal under **MetaDefender Storage Security** in the **MetaDefender Storage Security Offline Docker Toolkit** section. The package needs to be extracted to the desired path on the target offline machine and the following steps should all be performed from the same path where the package is extracted on the offline machine.

Load docker images

To load the MDSS docker images run the following command from the same path where the offline package is extracted:

```
sudo ./mdss.sh -u load_images
```

Starting MetaDefender Storage Security

Finally, MDSS can be started using the regular startup command but specifying the local path to the `mdss.sh` script from the offline package:

```
sudo ./mdss.sh -c start
```

Using this method, all mdss commands (start, stop etc.) will need to be executed from the same path where the package is extracted.

Updating MetaDefender Storage Security Offline

> **Info**
>
> To update MetaDefender Storage Security while in offline mode the same steps can be followed but with the latest installer and offline package, detailed instructions are outlined in the Offline Update Guide

Portable Package

This guide provides instructions on how to deploy MetaDefender Storage Security docker images without using the the installer. This method is intended for deployment scenarios where installing docker and docker-compose is not possible using official installation methods.

> **Info**

> It's recommended to have the same dependencies as the ones required for the offline installation preinstalled on the target host machine.

Downloading the portable toolkit

The toolkit is available on the **MyOPSWAT** portal under **MetaDefender Storage Security** in the **MetaDefender Storage Security Portable Toolkit** section. The package needs to be extracted to the desired path on the target machine and the following steps should all be performed from the same path where the package is extracted on the target machine.

Starting MetaDefender Storage Security

From the path where the portable package is extracted, MDSS can be started using the regular startup command but specifying the local path to the `mdss.sh` script:

```
sudo ./mdss.sh -c start
```

Using this method, all mdss commands (start, stop etc.) will need to be executed from the same path where the package is extracted.

> **Info**
>
> When running in portable mode, the `mdss.sh` script detects if docker is already installed or if the bundled docker binaries should be used in which case the following should be taken into consideration:
>
> - Docker commands will not work from the command line by default unless using the docker binarys directly from the bundled `docker` folder.
> - The bundled docker binary is not running as a service, the `dockerd` process is started automatically when running `mdss` commands.
> - Since docker is not running as a service it does not automatically start at boot

Upgrade MDSS

> **Warning**
>
> Before proceeding with the upgrade process, it's highly recommended that a backup is performed of the original deployment in order for recovery purposes.

> The contents of the `customer.env` file (contains credentials and custom settings) and the PostgreSQL database files (contain all MDSS data) are critical in order to prevent any data loss.

Upgrading is typically a two-step process:

1. Upgrade the **mdss** package by installing the newer version.
2. Update the codebase by downloading and applying new container images.

> **NOTE**
>
> > The behavior of the update process depends on the current version:
>
> - **Before v3.5.3:** Can only upgrade to v3.5.3
> - **From v3.5.3:** Can upgrade to version **v3.6.0** for database validation
> - **From v3.6.0**: Can upgrade to the latest compatible version
>
> > ⚠️ MDSS v3.6.0+ requires **MongoDB 6.0 or higher**
> >
> > ⚠️ MDSS v4.0.0+ requires **PostgreSQL 16.0 or higher**

Upgrading to version 4.0.0 or newer

Starting with version 4.0.0 of MDSS the database will be migrated from MongoDB to PostgreSQL. Please follow the Upgrade Guide to PostgreSQL to ensure the upgrade completes successfully and all data is migrated.

> ## Unix-Based Systems
>
> ### Step 1: Download the Installer
>
> Visit My OPSWAT to download the latest `.deb` or `.rpm` package.

> **Offline Deployments**
>
> In case of an offline deployment, the offline steps need to be followed: Offline Upgrade

Debian / Ubuntu package (.deb)

1. Update your packages

```
sudo apt-get update
```

2. Move to the folder containing the installer and install it

```
sudo dpkg -i <name of the file>.deb || sudo apt-get install -f
```

3. Start the service

```
sudo mdss -u update
```

4. Optionally, you can check the status using the following command:

```
sudo mdss -c status
```

5. Open a browser and navigate to the web interface: **http://** to configure your deployment.

Red Hat Enterprise Linux / CentOS package (.rpm)

1. Update your packages

```
sudo yum -y update
```

2. Move to the folder containing the installer and install it

```
sudo yum upgrade <name of the file>.rpm
```

3. Start the service

```
sudo mdss -u update
```

4. Optionally, you can check the status using the following command:

```
sudo mdss -c status
```

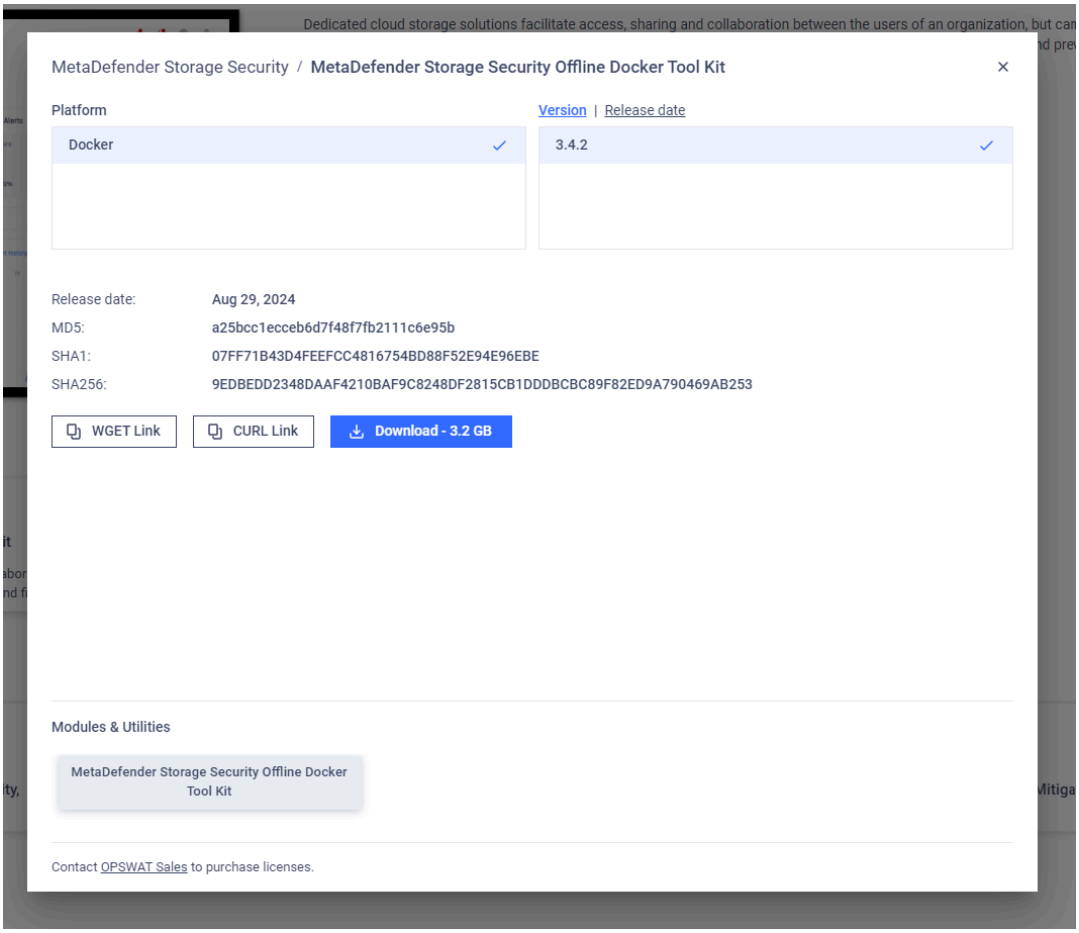
5. Open a browser and navigate to the web interface: http:// to configure your deployment.

Offline Upgrade

> **Warning**
>
> The following steps only apply when MDSS is installed using the official installer (.deb/.rpm). For any other deployment methods like when using the portable package, bundled binaries or the helm chart, then you should consider a clean deployment and migrating the original data if necessary.

> **Info**
>
> Instructions to be followed for upgrading after installing the product using the Installing Offline on Linux documentation

1. Download the latest MetaDefender Storage Security **Installation Package** from My OPSWAT portal.
2. Download the latest MetaDefender Storage Security **Offline Docker Tool Kit** from My OPSWAT portal.



3. Stop the service

```
sudo mdss -c stop
```

4. Run the installation script

```
sudo dpkg -i <name of the file>.deb
```

```
sudo yum install -y <name of the file>.rpm
```

5. Extract deployment.zip folder and load the container images

```
unzip deployment.zip -d <extracting_path>/
cd <extracting_path>/
sudo docker load -i ./mdcs.tar
```

6. Start the service

```
sudo mdss -c start
```

Upgrading from a previous version on Windows-based deployments

Upgrading from v3.4.0 or newer

To upgrade from a previous version, running the new installer is enough. The installer will walk you through the Windows Installation Wizard Section

Upgrading from v3.3.4 or earlier to v3.4.0 or newer

Upgrading to v.3.4.0 from an older version requires a special procedure due to major architectural changes. If a clean install with configuration import is not possible, please see the steps below.

Caution: This operation modifies a live database. Errors may cause irreversible data loss. Proceed with caution and ensure adequate backups. We advise on performing this operation only if absolutely necessary.

All commands should be run in a PowerShell terminal.

1. Update MDSS to the latest version

```
.\mdss.ps1 -u update
```

2. Edit the following file: C:\Program Files\OPSWAT\MetaDefender Storage Security\docker\docker-compose.main.linux.yml
3. Under the mongodb container modify the image to use version 6.0. It should look like this:

```
version: '3'
services:
    mongodb:
        platform: linux/amd64
        image: "mongo:6.0"
        volumes:
            - mongo_db:/data/db
```

4. Repeat procedure for C:\Program Files\OPSWAT\MetaDefender Storage Security\docker\docker-compose.main.all.linux.yml
5. Run the upgrade command from the installation directory [C:\Program Files\OPSWAT\MetaDefender Storage Security\docker]:

```
.\mdss.ps1 -u upgrade_db
```

Depending on your DB size, this operation may take more than 30 minutes

6. After upgrade is finished, export the DB

```
.\mdss.ps1 -u export_db
```

7. Copy the exported DB archive to a different location, e.g.: C:\temp
8. In that different location, extract the archive

```
tar -xf .\db_{timestamp}.tar
```

9. Compress the files in a zip format

```
Compress-Archive .\dump\  db_{timestamp}.zip
```

10. Uninstall MetaDefender Storage Security 3.3.4 as documented Uninstall.
11. Run the latest installer for MetaDefender Storage Security as documented Installation Methods
12. Run the stop command from the installation directory [C:\Program Files\OPSWAT\MetaDefender Storage Security\scripts]

```
.\mdss.ps1 -c stop
```

13. Copy the .zip file you created earlier (db__{timestamp}_.zip) to the installation directory (by default, (C:\Program Files\OPSWAT\MetaDefender Storage Security)
14. Import the DB

```
.\mdss.ps1 -u import_db
```

15. Run the start command:

```
.\mdss.ps1 -c start
```

Uninstall

> **NOTE**
>
> If the current MetaDefender Storage Security (MDSS) deployment (4.0.0 or later) was upgraded from 3.6.1 or earlier, any existing MongoDB backups will be deleted during uninstallation. Manually back up the data beforehand if it's still needed.

Uninstall via Command Line

Debian / Ubuntu (.deb package)

To remove all files installed by MetaDefender Storage Security:

```
sudo mdss -u clean
```

To remove the `mdss` package from the system:

```
sudo apt-get remove mdss
```

Red Hat Enterprise Linux / CentOS (.rpm package)

To remove all files installed by MetaDefender Storage Security

```
sudo mdss -u clean
```

To remove the `mdss` package from the system:

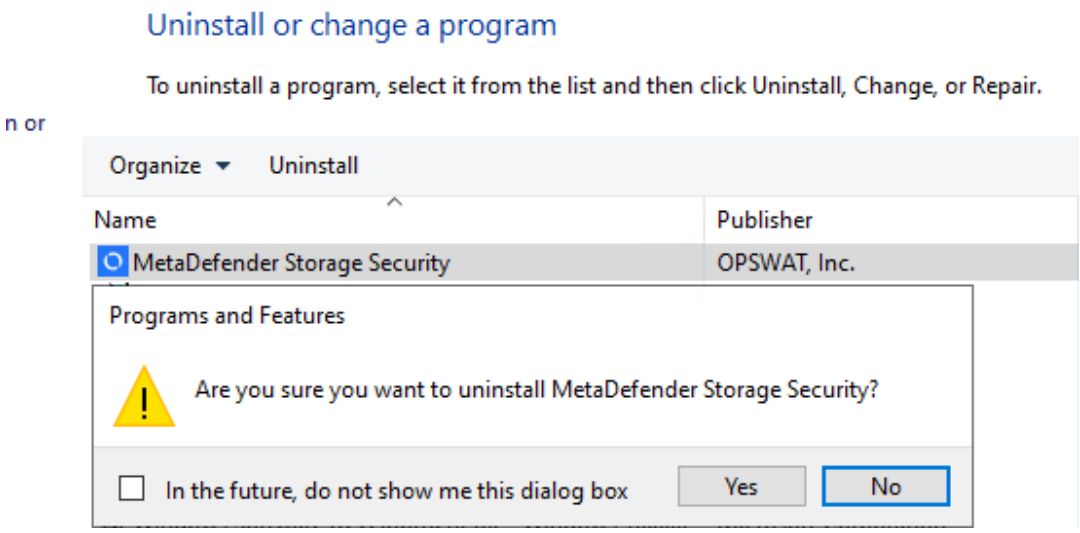
```
sudo yum remove mdss
```

Uninstall via Uninstall Wizard (Windows only)

> **NOTE**
>
> The Uninstall Wizard is available only for the Windows installer (`.msi`).

Step-by-Step Instructions

1. Open **Start** → **Control Panel** → **Uninstall a program**
2. Locate **MetaDefender Storage Security** in the list
3. Double-click the entry
4. Click **Uninstall and Yes** to begin the process



n or

5. Wait for the uninstallation to complete
6. Click **Finish** to finish.

Troubleshooting On-Premise

To troubleshoot when deploying to your On-Premise environment we have created a specific section, where we have divided the articles in:

- Diagnostic
- Deployment

- Integration

containerized deployments

Containerized Deployment Overview

This section provides comprehensive guides for deploying and managing MetaDefender Storage Security in both Docker and Kubernetes environments. Containerization offers significant advantages for flexibility, scalability, and efficiency in managing your security infrastructure.

Docker

Deploying MetaDefender Storage Security with Docker provides a lightweight and portable solution. This guide covers:

- Overview of the MetaDefender Storage Security Docker images published on OPSWAT Docker Hub.

Kubernetes

Leveraging Kubernetes for deploying MetaDefender Storage Security offers enhanced scalability, high availability, and simplified management. This guide covers essential aspects, including:

- Overview of Kubernetes components and their roles in the deployment.
- Upgrade and deployment strategies for seamless transitions and updates.
- Step-by-step instructions for installing MetaDefender Storage Security within your Kubernetes cluster.
- Licensing information specific to Kubernetes deployments.
- Storage configuration options to optimize performance and data management.
- High availability configurations for ensuring continuous operation.
- Guidance on scaling your Kubernetes cluster to adapt to changing demands.
- Troubleshooting tips for common issues and challenges.
- Release information and updates for MetaDefender Storage Security on Kubernetes.

By following these guides, you can effectively deploy and manage MetaDefender Storage Security in containerized environments, enhancing your security posture and ensuring the protection of your critical data.

Kubernetes Deployment

This Installation Guide provides step-by-step instructions for installing MetaDefender Storage Security (MDSS) in your own Kubernetes cluster in whatever environment you have

it deployed.

This guide is for IT infrastructure architects, administrators and DevOps professionals who are seeking to prevent potential malicious traffic being allowed in their environments. Threat Prevention is ensured for both productivity files that might be uploaded and for known vulnerabilities that can be identified for all running services/applications. The vulnerability scanning is checking known vulnerabilities for unpatched OS and running applications.

Using Kubernetes technology provides us with some features that distinct it from other type of deployments. These are the main features:

- **Service discovery and load balancing.**
- **Storage orchestration.** Allows you to automatically mount a storage system.
- **Automated rollouts and rollbacks.**
- **Automatic bin packing.** You tell Kubernetes how much CPU and memory (RAM) each container needs.
- **Self-healing.** Kubernetes restarts containers that fail, replaces containers, kills containers that don't respond to your user-defined health check, and doesn't advertise them to clients until they are ready to serve.
- **Secret and configuration management.** Kubernetes lets you store and manage sensitive information.
- Scale your application up and down

There are recommended configuration for each of the features to use by default when deploying MetaDefender Core in a Kubernetes cluster.

Kubernetes Guide Structure

1. Deployment Using Helm
2. Replication & High Availability on K8S
3. Custom certificates on K8S
4. OpenShift Considerations

Deployment Using Helm

The Kubernetes deployment for MetaDefender Storage Security can be performed directly using the provided Helm chart, which is available in our public GitHub repository here.

Example configuration files for different environments are provided in the `helm_charts` directory within the repository.

Using the helm repository

The GitHub repository can be used directly as a Helm repository:

```
helm repo add mdk8s https://opswat.github.io/metadefender-k8s/
helm repo update mdk8s

#Example installation command
helm install mdss mdk8s/metadefender_storage_security -f
<CUSTOM_VALUES_FILE.yml>
```

Alternatively, the repository can be cloned locally:

```
git clone https://github.com/OPSWAT/metadefender-k8s.git metadefender
cd metadefender/helm_carts

#Example installation command
helm install mdss ./mdss -f <CUSTOM_VALUES_FILE.yml>
```

Storage

MDSS containers are stateless and do not require persistent storage.

However, if deploying the PostgreSQL database within the cluster, it is recommended to use persistent storage managed by your cloud provider.

An external database can be configured using the following values:

```
mdss-common-environment:
  POSTGRESQL_URL:
"Host=postgres;Port=5432;Username=user;Password=password;Database=dbNam
e"
```

When using an external database not deployed via the MDSS chart, the `deploy_with_mdss_db` value must be set to `false` to prevent the chart from deploying an additional database.

Exposing MDSS

By default, the Helm chart deploys a `ClusterIP` service for the MDSS deployment.

This can be changed to any service type supported by your Kubernetes cluster.

For example, to create a `LoadBalancer` service, overwrite the `service_type` value in the `webclient` component:

```
mdss_components:
  webclient:
    service_type: LoadBalancer
```

MDSS can also be exposed using an Ingress:

```
mdss_ingress:
  host: <APP_NAMESPACE>-mdss.k8s  # Hostname for the publicly
accessible ingress, the `<APP_NAMESPACE>` string will be replaced with
the namespace where the chart is deployed
  enabled: true                   # Enable or disable the ingress
creation
  class: nginx                    # Sets the ingress class depending
on the installed ingress controller
```

Flexible deployment

By default, the Helm chart deploys MDSS with support for the following storage units: `azureblob`, `amazonsdk`, `googlecloud`, `alibabacloud`, `azurefiles`, and `box`.

For more efficient resource utilization, you can specify only the required storage units by modifying the `ENABLED_MODULES` value.

For instance, to enable support for only Azure, AWS, and GCP:

```
mdss-common-environment:
  ENABLED_MODULES: "azureblob,azurefiles,amazonsdk,googlecloud"
```

Supported modules

Currently supported modules include:

- `azureblob`
- `amazonsdk`
- `googlecloud`
- `alibabacloud`
- `azurefiles`
- `smb`
- `box`
- `graph`

Replication & High Availability on K8S

When installing MetaDefender Storage Security in Kubernetes as this technology provide the system with its self-healing feature, it might not be strictly necessary to set it up with at least 2 replicas for each of the pods in case of wanting to have **High Availability,** but it is always a best practice to have 2 replicas of each pod running in different worker nodes. For those components that could not be running within the cluster, we will provide different solutions that are supported by our application.

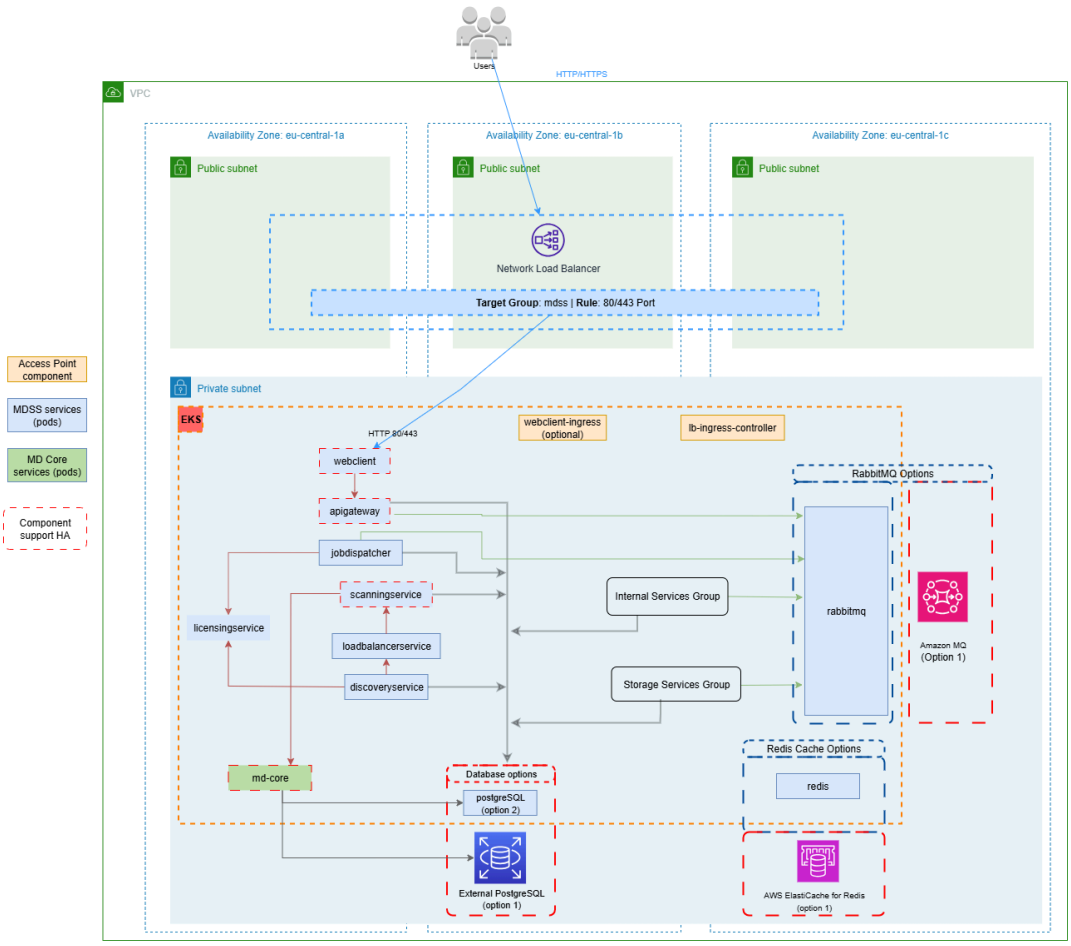
However, there are a few components that may incur in high load in some situations, so for those components it is recommended to have more than 1 replica. These components are the following.

MDSS services

- `Web Client` -> to provide high availability to outside requests
- `API Gateway` -> to provide high availability to outside requests
- `Scanning Service` -> to provide high availability when having to handle big number of files to scan

3rd Party components

- `Database` -> Deploy an external service for PostgreSQL with HA or PostgreSQL operator running on K8S cluster
- `RabbitMQ` -> Use external service for RabbitMQ with HA
- `Redis Cache` -> Use external service for Redis cache with HA



HA solutions for PostgreSQL

For CSPs provided service it has been tested and is supported by the following:

- Amazon RDS
- Azure Database for PostgreSQL

If a highly available database is required inside the k8s cluster, then there are publicly available solutions that can deploy a PostgreSQL Replica Set. For a k8s cluster, Zalando provides an operator for deploying a Replica Set: https://github.com/zalando/postgres-operator/blob/master/docs/quickstart.md

HA Solution for Redis Cache

OPSWAT have tested the following services to provided HA to a redis service.

- AWS ElasticCache for Redis
- Azure Cache for Redis

HA Solution for RabbitMQ

OPSWAT have tested the following services to provided high availability to a RabbitMQ service.

- Amazon MQ for RabbitMQ
- Bitnami package for RabbitMQ in Azure MP

RabbitMQ Cluster Operator

1. Install Cert-Manager (required for operator webhooks)

```
kubectl apply -f https://github.com/cert-manager/cert-
manager/releases/download/v1.13.3/cert-manager.yaml
```

2. Install RabbitMQ Cluster Operator:

You can download the file using this link: RabbitMQ Cluster Operator

```
kubectl apply -f <path-to-cluster-operator.yml>
```

3. Install RabbitMQ Messaging Topology Operator:

You can download the file using this link: RabbitMQ Messaging Topology Operator

```
kubectl apply -f <path-to-messaging-topology-operator-with-
certmanager.yaml>
```

Update your Helm values to enable the operator:

```
rabbitmq-cluster-operator:
  enabled: true
  replicas: 3
  resources:
    requests:
      cpu: "250m"
      memory: "512Mi"
```

The operator will automatically create a 3-node RabbitMQ cluster with quorum-based HA. During node failures, the cluster continues operating and services automatically reconnect to healthy nodes.

HA deployment for MDSS

MDSS containers can be scaled independently depending on the availability and performance requirements. For example, just the `webclient`and `apigateway` pods can be replicated to provide high availability to outside requests and for the web interface.

```
mdss_components:
  webclient:
    replicas: 3
  apigateway:
    replicas: 3
```

The `mongomigrations`service is used to migrate the data from older versions of MDSS at startup if required and provides no benefits if replicated .

Create environment with HA components

For deploying all the components that provide a high availability, OPSWAT have prepared a terraform module to deploy all the 3rd parties applications (Redis, RabbitMQ & PostgreSQL DB).

There are 2 ways of using that terraform module

- Applying changes directly using the terraform project
- Using the metadefenderk8s.sh to deploy MDSS with it.

Automatic replicas using horizontal pod autoscaling (HPA)

The HPA can be enabled on all MDSS services from the values:

```
hpa:
  enabled: true
  minReplicas: 2
  maxReplicas: 3
  cpuTargetUtilization: 85
```

In the example above the number of replicas are adjusted within the specified limits depending on the measured CPU usage. The HPA is applied for all MDSS services, for a more granular autoscaling it's recommended to manually create a HPA separately from the helm deployment just for the desired services.

Custom certificates on K8S

Custom certificates need to be loaded in MDSS when connecting to services that use a private TLS/SSL certificate like MD Core, storage units, external databases etc. These certificates need to be loaded into the K8S cluster as a secret which can be mounted into the appropriate services by adding the following section to the values file:

```
mdss_components:
  <SERVICE_NAME>:
    update_ca: true
    customMounts:
      - mountPath: "/usr/local/share/ca-certificates/my-custom-
cert.crt"
        name: my-cert
        subPath: cert-data
    customVolumes:
      - name: my-cert
        secret:
          secretName: my-custom-cert
```

An example values file where certificates are loaded into multiple MDSS services can be found on our GitHub repo here: https://github.com/OPSWAT/metadefender-k8s/blob/main/helm_charts/mdss-custom-certs-example.yml

OpenShift Considerations

Introduction

This guide explains how to deploy MetaDefender Storage Security (MDSS) on OpenShift using Helm with the required OpenShift-specific configuration.

Prerequisites

- Access to OpenShift cluster with admin privileges
- Helm 3.x installed
- oc command-line tool configured
- Ability to grant privileged SCC permissions

Deployment Steps

1. Login to OpenShift

```
oc login --token=<your_token> --server=<cluster_url>
```

2. Create Project

```
oc new-project mdss
```

3. Create Service Account and Grant Permissions

The MDSS components require privileged access to function properly on OpenShift:

```
# Create a service account for MDSS
oc create sa mdss -n mdss

# Grant privileged security context constraints to the service account
oc adm policy add-scc-to-user privileged -z mdss -n mdss
```

Important: The privileged SCC is necessary because several MDSS components require elevated permissions.

4. Add Helm Repository

```
helm repo add mdk8s <https://opswat.github.io/metadefender-k8s/>
helm repo update mdk8s
```

5. Prepare OpenShift Values File

Create a file named `mdss-openshift.yml` with the OpenShift-specific configuration:

```
# Download the OpenShift values file directly from GitHub # Run this
command to fetch the file:
curl -O <https://raw.githubusercontent.com/OPSWAT/metadefender-
k8s/refs/heads/main/helm_charts/mdss-openshift.yml
```

6. Deploy the MDSS Helm Chart

```
helm install mdss mdk8s/metadefender_storage_security -f mdss-
openshift.yml
```

Note: The OpenShift values file configures the SecurityContext to run as user 0 (root), assigns the mdss service account to pods, and adjusts command arguments for

compatibility.

7. Verify Deployment

```
oc get pods -n mdss
oc get services -n mdss
```

Wait until all pods are in Running state. This may take a few minutes as containers initialize.

Post-Deployment Configuration

Access MDSS Console

```
# Create a route to access the MDSS web interface
oc expose svc/webclient -n mdss
# Get the route URL
oc get route webclient -n mdss
```

Access the web interface using the hostname provided by the route.

Maintenance

Upgrading MDSS

```
helm repo update mdk8s helm upgrade mdss
mdk8s/metadefender_storage_security -f mdss-openshift.yml
```

Uninstalling MDSS

```
helm uninstall mdss oc delete project mdss
```

Upgrade/Deployment Strategy on K8S

The helm upgrade command can be used to upgrade the mdss services using the latest helm chart:

```
helm upgrade my_mdss <path_to_chart>
```

General recommendations

Before performing any upgrade, review the following best practices:

- **Back up the database**: Always take a full backup of your PostgreSQL database before upgrading. For in-cluster deployments this means snapshotting the persistent volume; for externally managed databases use the provider's native backup/snapshot mechanism. Keep the backup until the new version has been validated in production.
- **Read the release notes**: Check for any breaking changes or required configuration updates in the target release before upgrading.
- **Blue-green deployment**: For production environments where rollback safety is critical, consider a blue-green upgrade strategy:
  1. Clone your existing PostgreSQL database to a separate instance (e.g. a snapshot-restored replica or a managed DB clone).
  2. Deploy the new chart version into a separate namespace (e.g. `mdss-green`), pointing it at the cloned database:`helm install my_mdss_green path_to_new_chart --namespace mdss-green --set POSTGRESQL_URL="connection_string_to_cloned_db"`
  3. Validate functionality of the new deployment against the cloned data without affecting production traffic.
  4. Switch ingress or DNS to the new namespace once satisfied.
  5. If issues arise, revert by routing traffic back to the original namespace — the original database remains untouched.
  6. Decommission the old deployment and cloned database after a suitable validation period.

Database upgrades

This step is not required when using an external, managed database

The helm chart is configured by default to use the latest compatible version of PostgreSQL. Before upgrading an existing deployment with a persistent in-cluster database, make sure the database version matches the version required by the corresponding release:

- MDSS (latest) - PostgreSQL 17

Upgrading from MongoDB (versions prior to v4.0.0)

Starting with MDSS v4.0.0, PostgreSQL replaces MongoDB as the primary database backend. If upgrading from an older MongoDB-based deployment, follow the official Upgrade Guide to PostgreSQL which covers three upgrade options:

- **Option 1 – Standard upgrade with migration**: Recommended for small to medium deployments where historical data is required. Data is migrated automatically; no extra configuration needed. Note that migration takes approximately 2–3 hours per 1 million files.
- **Option 2 – Skip data migration**: Recommended for large deployments or when historical data is not critical. The chart sets `SKIP_MONGO_TO_PG: "yes"` by default, so migration is skipped unless explicitly removed from the values. This provides immediate availability of the new version without waiting for data migration.
- **Option 3 – Blue-green deployment**: Recommended for production environments requiring zero downtime. Deploy v4.0.0 in parallel, test it, then cut over storage processing with easy rollback capability.

Schema migrations

Database schema migrations are handled automatically by the `pgmigrations` pod, which runs as an init step before any other MDSS containers start up. No manual migration steps are required — ensure the `pgmigrations` pod completes successfully before troubleshooting other service startup issues.

Upgrading with an externally managed database

When using an external (managed) database, the database itself holds all persistent state. In this case it is **strongly recommended to perform a clean reinstall** rather than a rolling upgrade, to avoid schema or configuration conflicts:

```
helm delete my_mdss
helm install my_mdss <path_to_chart>
```

The following components are non-persistent and can be updated to the latest compatible version by setting the respective image tag:

- RabbitMQ: `rabbitmq:4.1.0-alpine`
- Redis Cache: `redis:7.4.1-alpine`

Operational Notes

The entire deployment can be customized by overwriting the chart's default configuration values. Here are a few point to look out for when changing these values:

- By default, a PostgreSQL 17 database is deployed alongside the MDSS deployment
- In a production environment it's recommended to use an external service for the database and set `deploy_with_mdss_db` to false in order to not deploy an in-cluster database

- When using an external database, prefer a clean reinstall (`helm delete` / `helm install`) over `helm upgrade`, since the database holds all persistent state and a clean install avoids potential schema or configuration conflicts

Portable Package

This guide provides instructions on how to deploy MetaDefender Storage Security docker images without using the the installer. This method is intended for deployment scenarios where installing docker and docker-compose is not possible using official installation methods.

> **Info**
>
> It's recommended to have the same dependencies as the ones required for the offline installation preinstalled on the target host machine.

Downloading the portable toolkit

The toolkit is available on the **MyOPSWAT** portal under **MetaDefender Storage Security** in the **MetaDefender Storage Security Portable Toolkit** section. The package needs to be extracted to the desired path on the target machine and the following steps should all be performed from the same path where the package is extracted on the target machine.

Starting MetaDefender Storage Security

From the path where the portable package is extracted, MDSS can be started using the regular startup command but specifying the local path to the `mdss.sh` script:

```
sudo ./mdss.sh -c start
```

Using this method, all mdss commands (start, stop etc.) will need to be executed from the same path where the package is extracted.

Integrations

Integrations

MetaDefender Storage Security integrates with various cloud and on-premises storage solutions, represented as **storage units**.

We provide a list (see table below) of officially supported integrations that are continuously tested for full functionality.

> **IMPORTANT
>
> Please get in touch with us if your specific storage provider isn't shown.**
>
> We likely already support storage systems that use S3-compatible interfaces or standard protocols such as SMB, NFS, or SFTP.

Cloud Object Storages

Storage Name	Integration Type	Tagging	Event-Based	Metadata * Copy
Amazon S3	Native	Yes	Yes	Yes
Wasabi	S3 Compatible	Yes	Yes	No
Cloudian®	S3 Compatible	Yes	Yes	No
Oracle Cloud	S3 Compatible	Yes	Yes	No
Oracle Cloud	Native	No	Yes	Yes
MinIO	S3 Compatible	Yes	Yes	No
Cubbit	S3 Compatible	Yes	Yes	No
Azure Blob	Native	No	Yes	No
Google Cloud	Native	Yes	Yes	No
Alibaba Cloud	Native	No	Yes	No

File Storages

Storage Name	Integration Type	Event-Based
Box	Native	Yes
OneDrive	Native	No
SharePoint Online	Native	Yes
Microsoft Teams	Native	No
SharePoint On-Premise	Native	No
Azure Files	Native	Yes
OPSWAT Managed File Transfer (MFT)	Native	No

Network Attached Storages (NAS)

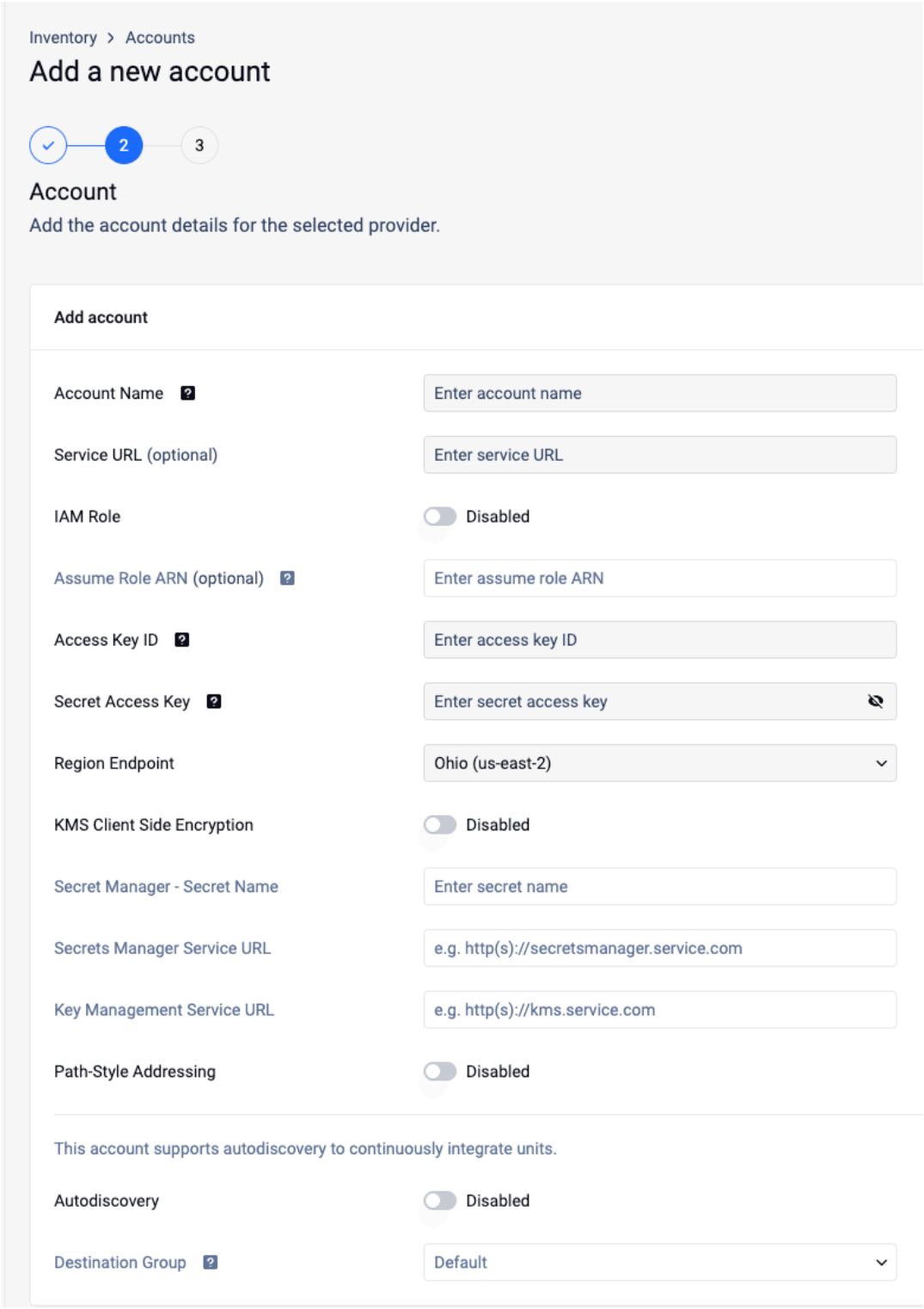
Storage Name	Integration Type	Event-Based	Delete empty folders
NFS	Native	Yes	Yes
SMB	NFS (recommended) Native	Yes	Yes
NetApp ONTAP	SMB / NFS	Yes	Yes
Amazon EFS	NFS	Yes	Yes
Dell Isilon	SMB / NFS	Yes	Yes
SFTP	Native	Yes	Yes
FTP	Native	Yes	No

*** Tags and checksum information**

Add An Amazon S3 Storage

Enabling this option may hinder product performance due to the increased number of actions required when communicating with the S3 server. In order to integrate Amazon S3 with MetaDefender Storage Security please follow these steps:

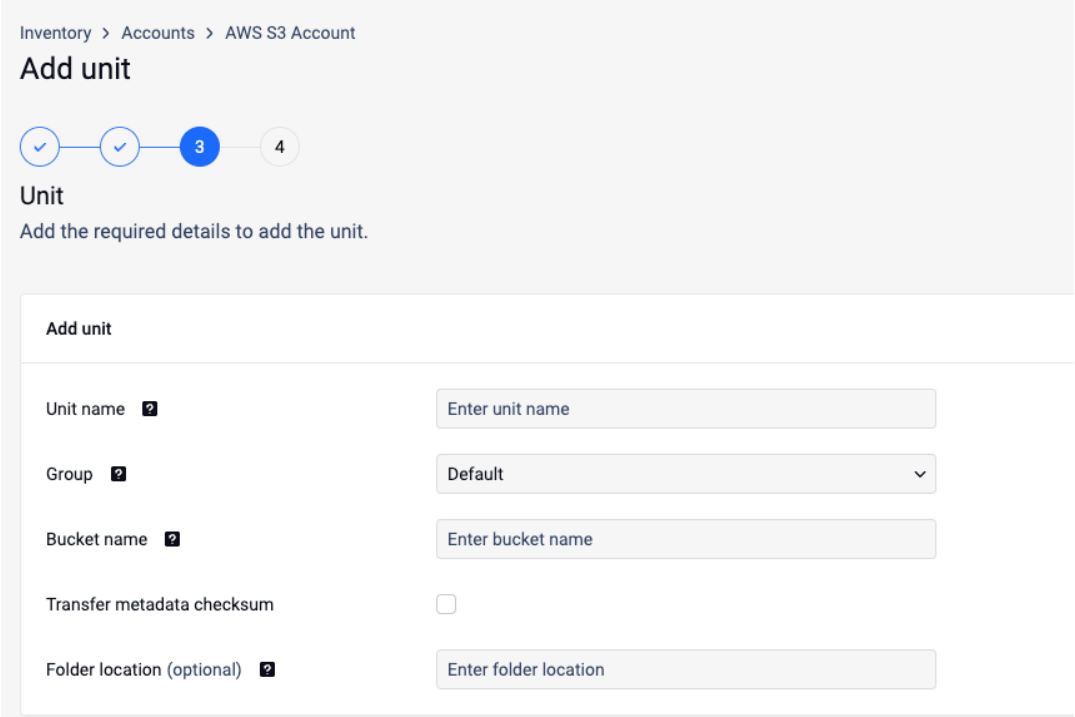
1. Navigate to **Inventory** tab -> **Add ** -> **Account -> Amazon S3**



2. Give your account a name so you can easily identify it later
3. Optionally, add a custom **Service URL** for your S3 Service, if you have one configured.
4. There are two ways to connect:

- **via the IAM role from the EC2 instance (skip to step 7)**
- **using security credentials**

5. Enter your **Access Key ID**. Scroll to the end of this page for more details.
6. Enter your **Secret Access Key.** Scroll to the end of this page for more details.
7. Choose the **Region endpoint** where your S3 endpoint is located.
8. If you want to enable **client-side encryption**, please read the below section named *Using client-side encryption*
9. *Enable Path-Style Addressing if needed.*
10. *Enable AutoDiscovery if needed*
11. *Choose the destination Group*
12. *Once the account is added successfully, proceed with adding the storage unit by navigating to ***Inventory** tab -> **Add New** -> **Unit -> Choose account previously created**



13. Give your storage a unique name so you can easily identify it later.
14. Assign a Group to your storage unit
15. Enter a valid S3 Bucket name
16. Enable Transfer metadata checksum if needed.
17. Add folder location (optional).
18. Complete the changes and add your storage unit.

Where can I find the Access Key ID and Secret Access Key?

To generate an Access Key ID / Secret Access Key pair please follow these steps:

1. Log in to **IAM Console** and go to **Users**

2. In the **Details** pane, click the appropriate IAM user or create one if none exists
3. From the **Security Credentials,** tab click **Create Access Key**

> **Info**
>
> If you already have a maximum of two access keys—active or inactive—you must delete one first before proceeding. If you need more than two root access keys, IAM users (each of whom can be assigned their own access keys) would probably better suit your requirements.

Using IAM role for Amazon S3 integration

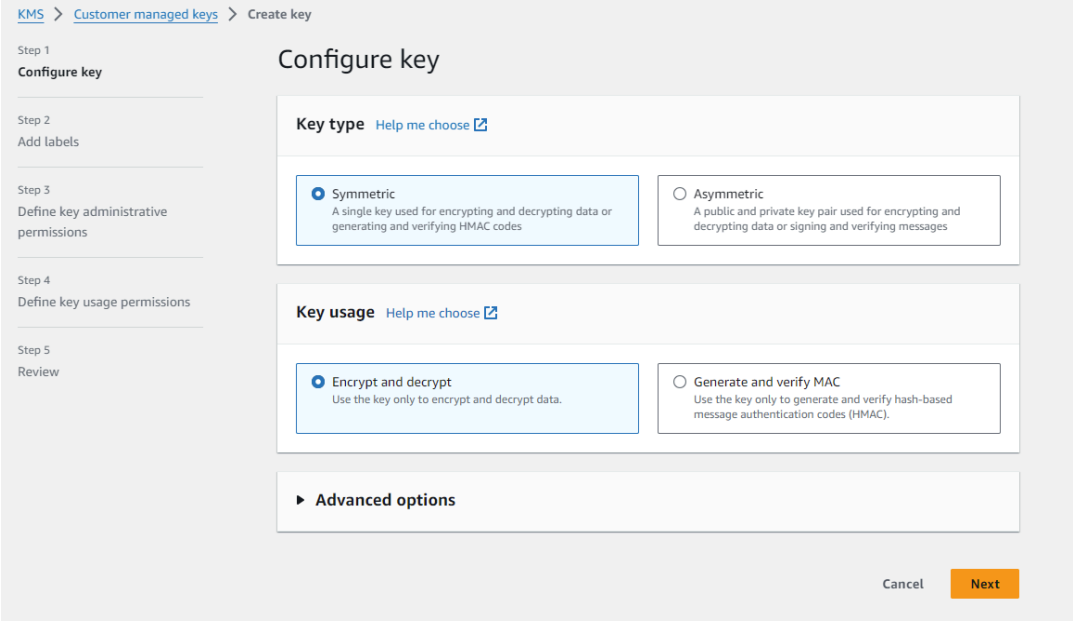
On S3 integration with IAM, the role configured on the EC2 machine will be used to authenticate.

With the optional field of Assume Role ARN, MetaDefender Storage Security allows integration with other buckets that are in different accounts from the current AWS account. This is possible by configuring Assume Role ARN field, with the ARN of the role that has access to the other account's S3 bucket.

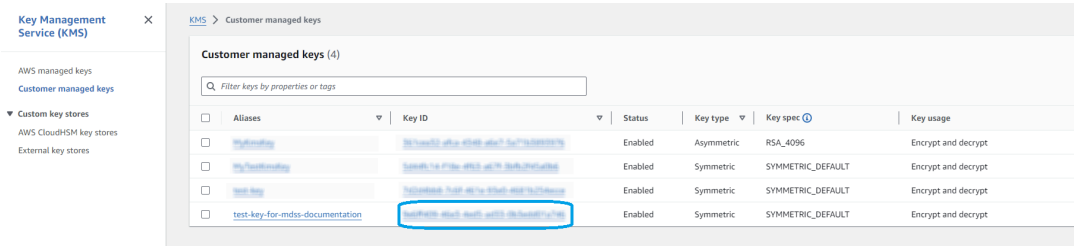
> **Using IAM Role: Modifying the default hop limit**
>
> If you are deploying MetaDefender Storage Security on an EC2 instance you will need to run the following AWS CLI command in order to increase the default `hop-limit`
>
> ```
> aws ec2 modify-instance-metadata-options --instance-id <INSTANCE_ID> --http-put-response-hop-limit 3 --http-endpoint enabled
> ```
>
> This is **required** because our services run within Docker and IMDSv2 restricts the number of "hops" each request to the metadata service can make.

Using client-side encryption

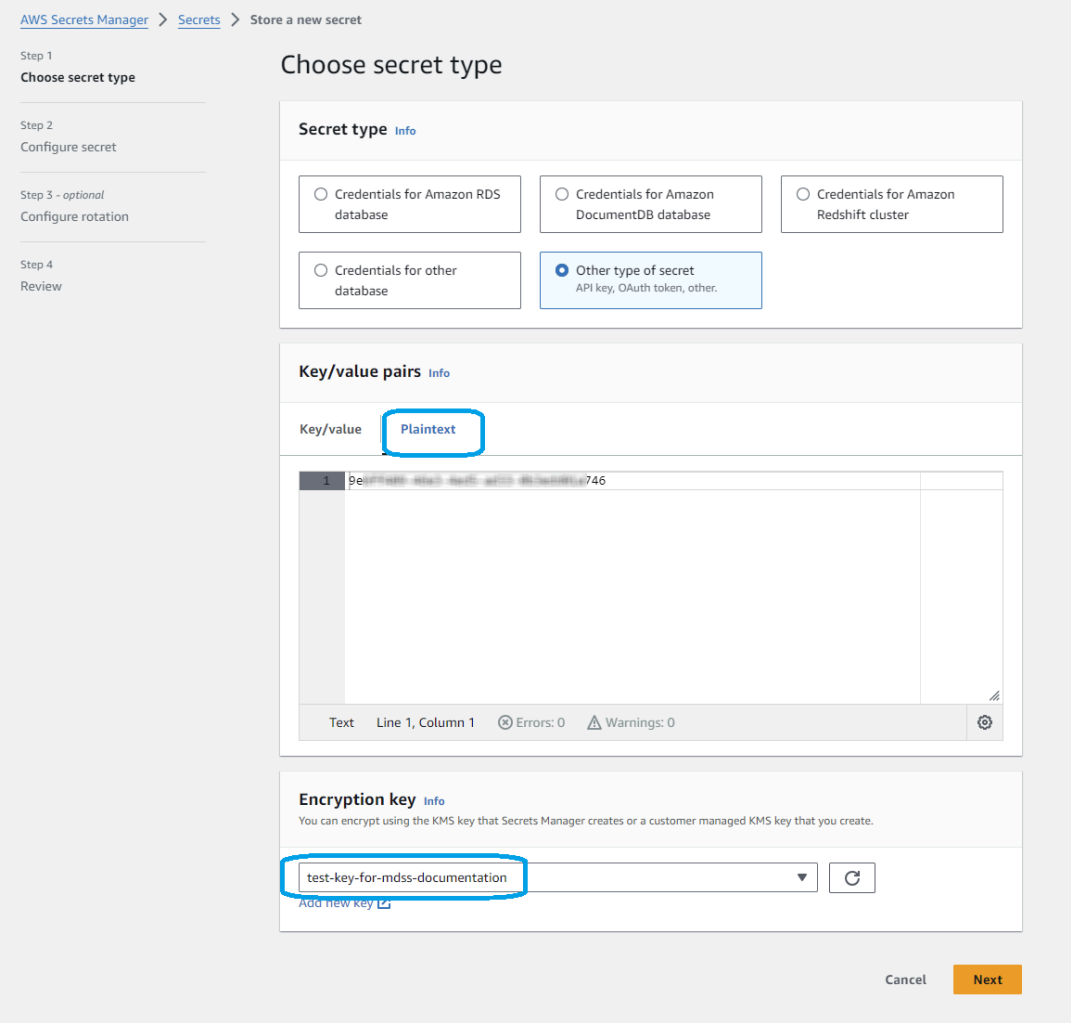
To use client-side encryption, you will need to do the following. From AWS Console, navigate to Key Management Service (KMS) and click on **Create a key.** The key should be a symmetric key and used to encrypt and decrypt.



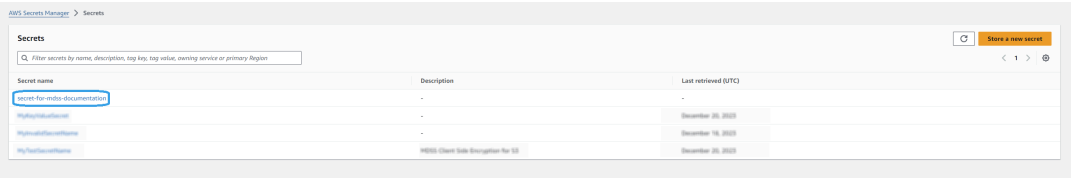
Click **Next,** give a name (Alias) to the key and finish the creation process. Once complete, the key should look like this:



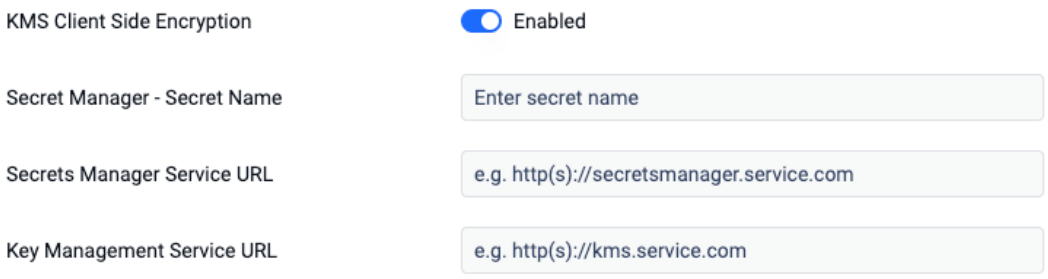
From AWS Console, navigate to Secrets Manager and click on **Store a new secret**. Secret type should be Other type of secret and Encryption key should be the name of the key from step 2. The Secret value needs to be in plain text and should be the ID of the key created at step 1. Please note that we do not support **Key/value**.



Click **Next,** give a name to the secret and finish the process. Once complete, the Secret should look like this:



Navigate to MetaDefender Storage Security UI and introduce the name of the secret created at step 4. If your Secret name is not valid or its value does not point to a valid key ID in Key Management Service, an error will be displayed on top of the UI. Also, optionally, you can add a custom **Service URL** for your Secrets Manager Service, if you have one configured.



Necessary AWS policies

These are the necessary AWS policies required in order to add an Amazon S3 Storage:

- `s3:GetObject`
- `s3:PutObject`
- `s3:GetObjectVersion`
- `s3:ListBucket`
- `s3:ListBucketVersions`
- `s3:GetObjectTagging`
- `s3:GetObjectVersionTagging`
- `s3:PutObjectTagging`
- `s3:PutObjectVersionTagging`
- `s3:DeleteObject`
- `s3:DeleteObjectVersion`

To be able to use client side encryption, additional AWS policies are required:

- `secretsmanager:GetSecretValue`
- `kms:DescribeKey`
- `kms:Decrypt`

To be able to use **server-side encryption with AWS Key Management Service (SSE-KMS)**, additional AWS policies are required:

- `kms:GenerateDataKey`
- `kms:DescribeKey`
- `kms:Decrypt`

To be able to use **autodiscovery**, additional AWS policies are required:

- s3:ListAllMyBuckets

S3 Compatible integrations

In order to use an S3 compatible storage unit the following requirements should be met:

- A valid TLS endpoint. since we are enforcing HTTPS for all S3 integrations. A valid certificate is also required. Please note that there is an option to add a custom certificate
- The storage should be configured to use or support the *virtual-hosted* addressing model, not path based.

The following object storage providers have been validated but any provider that meets the requirements and implements the S3 compatible open standard will work with MDSS:

- MinIO Object Storage
- Ceph Object Gateway

Configure UserAgent

In order to have a good tracking in AWS of every requests that MDSS does, a environment variable can be set that will be used to configure user agent.

Parameter	Value
MDSS_LOG_IDENTIFIER	string

By default this is not configured and the dotnet SDK value is used.

Transfer file metadata and checksum on created or moved files

> **Warning**
>
> MDSS does not support checksums CRC32C and CRC64NVME for any kind of operation.

This option enables the storage functionality to retrieve the metadata and checksum of files, and upon moving, copying or sanitizing them, the information is kept in the destination bucket for the files if it supports metadata or file checksum.

It can be enabled by checking the "**Transfer file metadata and checksum on created files**" and saving the storage. This also performs a test on the storage to verify if both functionalities are supported. If either of them is not supported either by the storage or due to permissions, the option cannot be enabled and saved.

If this option is enabled, the **File API** will provide information about the Checksum and Metadata of a file on the **ObjectStorageMetadata** field.

Files resulting from **DeepCDR** and **Encrypted Files** will have checksums recalculated if this option is enabled. At the same time these files will have the same metadata as the original file.

If a file has an unsupported checksum algorithm, or it does not have a checksum at all, the default **CRC32** algorithm will be used to compute a checksum for data integrity **by default**. This is the case only if the transfer option is enabled.

Checksum algorithm	Transfer support in MDSS
CRC-32 (used by default)	✅
SHA-1	✅
SHA-256	✅
CRC-32C	❌
CRC-64NVME	❌

> **Warning**
>
> If this option is enabled scanning performance may be reduced as more queries are performed to AWS services, and also the checksum needs to be recalculated during scanning in certain scenarios which also involves a performance penalty.

> **Warning**
>
> To move checksum and metadata to storages created in versions prior to v3.5.3, these need to be retested for this functionality. This can be done with a simple **Edit** action on the storage, with no changed fields.

Server-Side Encryption Override

How to enable: Set the environment variable **AMAZONSDK_USE _AWS _MANAGED _SSE** to **true**. When set, all S3 uploads send the *x-amz-server-side-encryption: aws:kms* header, so S3 uses the AWS-managed KMS key (aws/s3) instead of the bucket's default KMS key.

When to use: Enable this when S3 buckets are configured with SSE-KMS encryption using a KMS key that is not accessible to the service (e.g., cross-account keys, deleted keys, or keys without the required kms:GenerateDataKey permission). This is commonly needed in multi-account setups where the destination bucket's KMS key belongs to a different AWS account.

Note: Objects are encrypted with the AWS-managed key, not the bucket's customer-managed key. This can affect key rotation and compliance that rely on a specific KMS key.

How to Enable Inline Scanning?

In order to prevent access to files on AWS S3 that have not been scanned yet, a bucket policy can be used in combination with the file tagging feature in MDSS to only allow get requests on files with the “No Threat Detected” tag.

For example, a bucket policy allowing full access just to scanned files would look like this:

```
{
  "Effect": "Allow",
  "Principal": "*",
  "Action": [
    "s3:*"
  ],
  "Resource": [
    "arn:aws:s3:::<BUCKET_NAME>/*",
    "arn:aws:s3:::<BUCKET_NAME>"
  ],
  "Condition": {
    "StringEquals": {
      "s3:ExistingObjectTag/MetaDefenderResult": "No Threat Detected"
    }
  }
}
```

In the above example `<BUCKET_NAME>` should be replaced with the S3 bucket name configured in MDSS or with the corresponding folder path that is subject to scanning.

The “Action” list from the example above can also be customized to only allow specific actions on the objects in question. To allow just get operations on scanned objects the `s3:GetObject` action can be used instead of `s3:*`.

This approach is particularly useful when using event-based real time scanning as it prevents any uploaded file from being accessed while it’s still processing in MDSS.

How to verify if tagging functionality is supported?

Object tagging functionality is supported for AWS S3 and other S3-compatible storage providers. This document explains the permission requirements and troubleshooting steps for tagging functionality.

MDSS verifies the following permissions during storage integration or modification:

```
"s3:GetObject",
"s3:PutObject",
"s3:DeleteObject"
"s3:PutObjectTagging",
"s3:GetObjectTagging",
```

Status Conditions

Disabled Tagging Functionality

Tagging functionality may be unavailable due to:

1. Missing core permissions (`s3:GetObject`, `s3:PutObject`, `s3:DeleteObject`)
   - When these are missing, tagging functionality cannot be tested and will be disabled
2. Missing tagging permissions (`s3:PutObjectTagging`, `s3:GetObjectTagging`)
   - When these are missing, tagging functionality will not be supported
3. Storage provider limitations
   - If the S3-compatible storage does not support object tagging

Verification Process

Permission verification occurs:

- When storage is first integrated with MDSS
- When storage configuration is edited

Troubleshooting

If tagging functionality is disabled but required permissions have been added:

1. Edit the storage configuration in MDSS
2. Save changes without modifying any settings

This action will trigger a re-verification of permissions and enable tagging functionality if all requirements are met.

How to Enable Autodiscovery

This guide provides step-by-step instructions for enabling Autodiscovery for Amazon S3 storage in MetaDefender Storage Security.

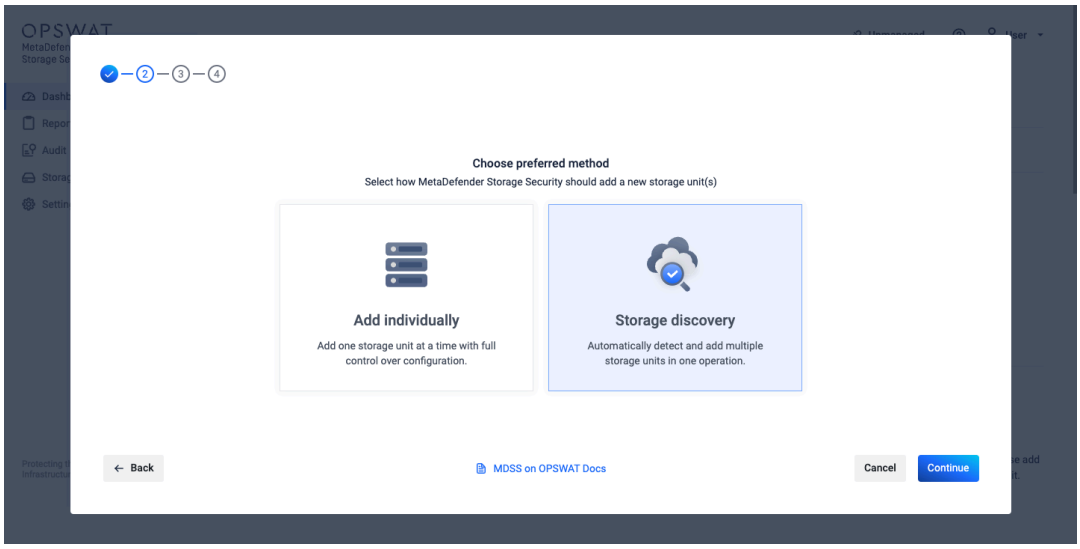
Autodiscovery automatically detects and adds S3 buckets as storage units, saving time and reducing configuration errors.

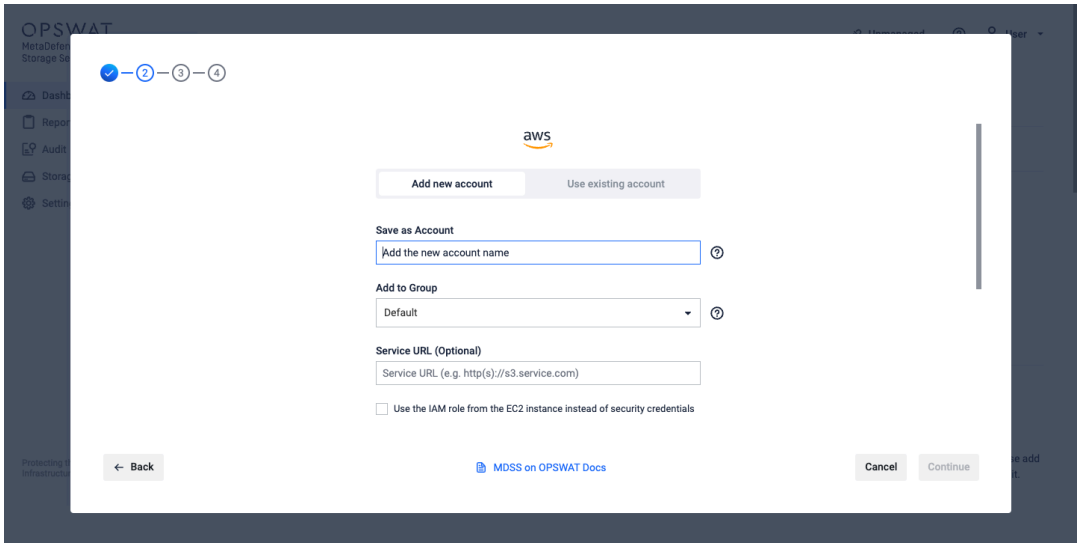
Prerequisites

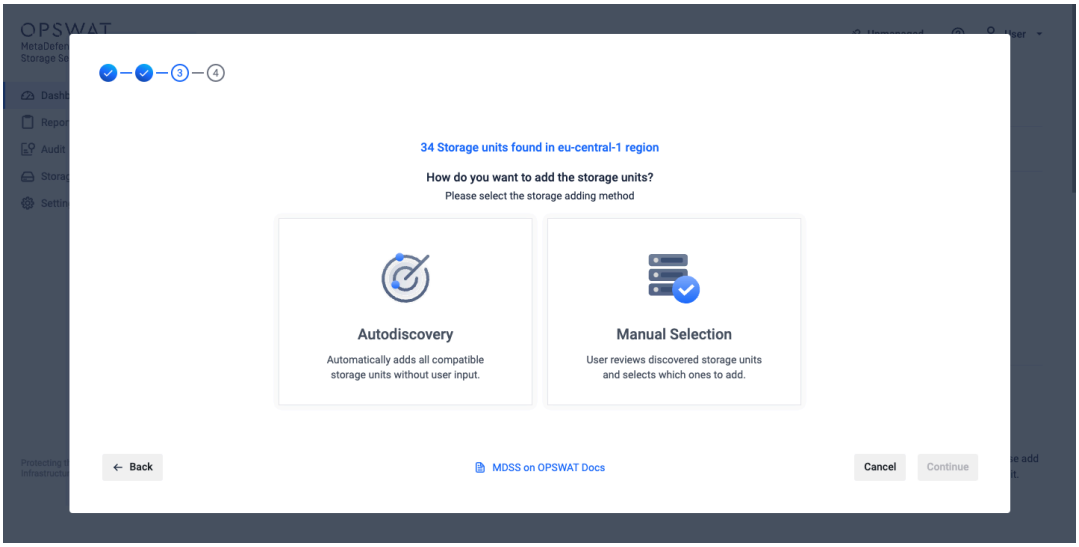
Before enabling Autodiscovery, ensure you have:

1. Valid AWS access key ID and secret access key with sufficient permissions
2. Permissions as stated in Add An Amazon S3 Storage

Method 1: Enable Autodiscovery During Storage Unit Addition







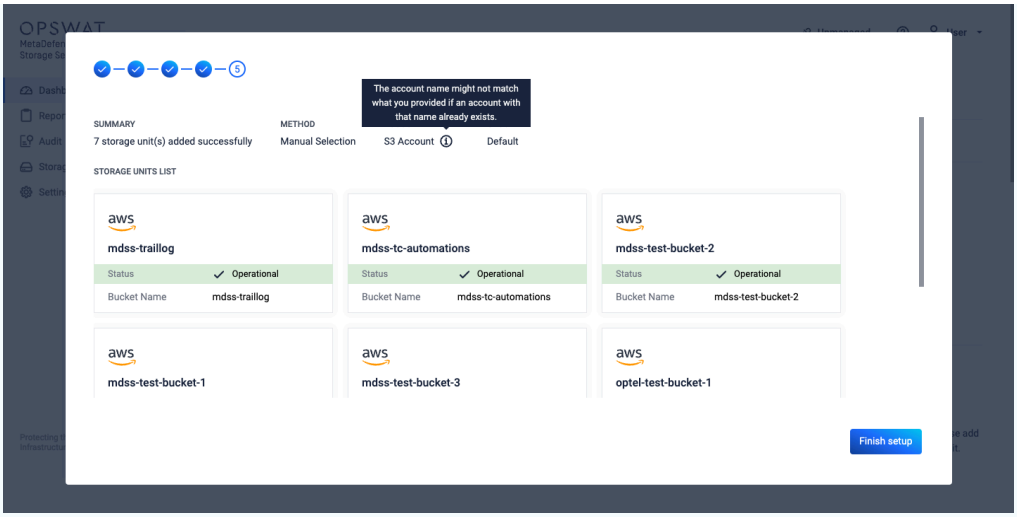
- Navigate to **Storage Units** page
- Click **Add Storage Unit** button
- Select **Amazon S3** Storage Type
- Select **Storage Discovery** and click **Continue**
- Fill out the form with valid Amazon S3 credentials and click **Continue**

REGION-SPECIFIC ENDPOINTS

Only the storages from the selected region endpoint will be discovered in the next steps.

ACCOUNT ALREADY EXISTS

If an account with the same credentials already exists, it will just use the existing account; this means at the final step, you will see the original account name [which might differ than the one you provided at this step].

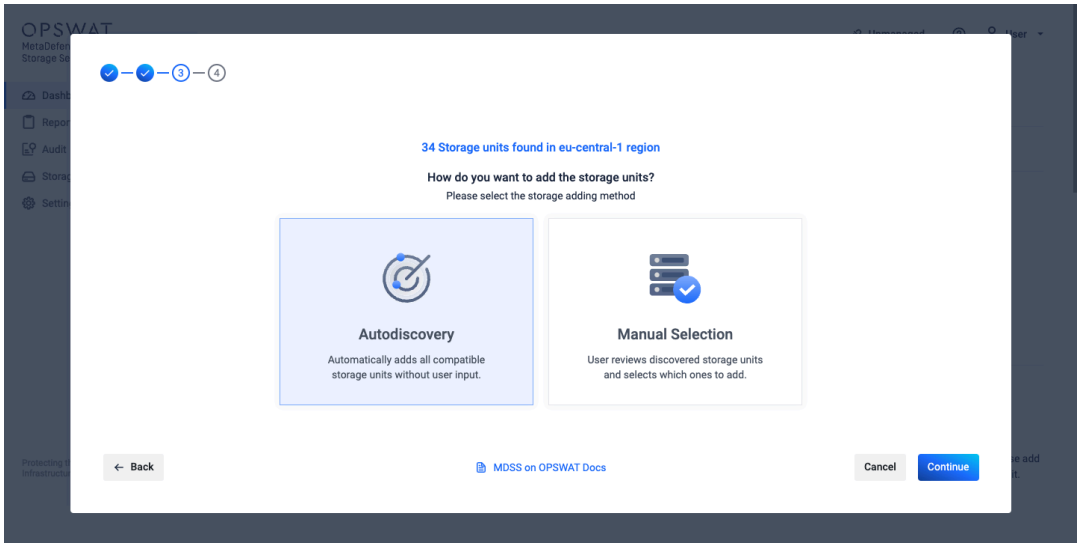


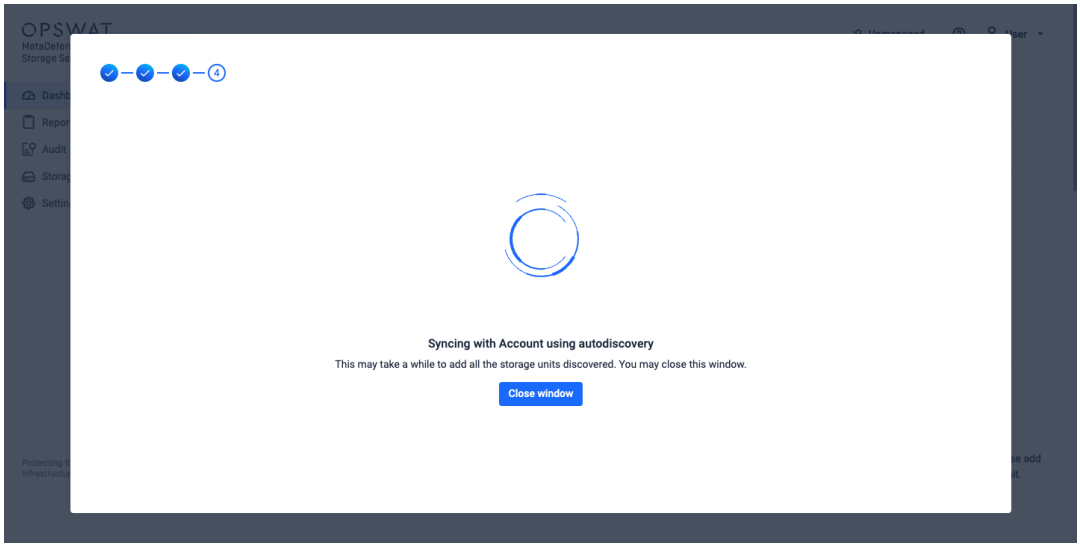
- In the next step, select your integration method. You have two choices: Autodiscovery and Manual Selection.
  - **Autodiscovery** for convenience, this option automatically adds all the buckets MDSS finds
  - **Manual Selection** for precise control, this option lets users choose specific buckets from the discovered list to integrate.

To learn more about each integration type, please consult the Autodiscovery documentation.

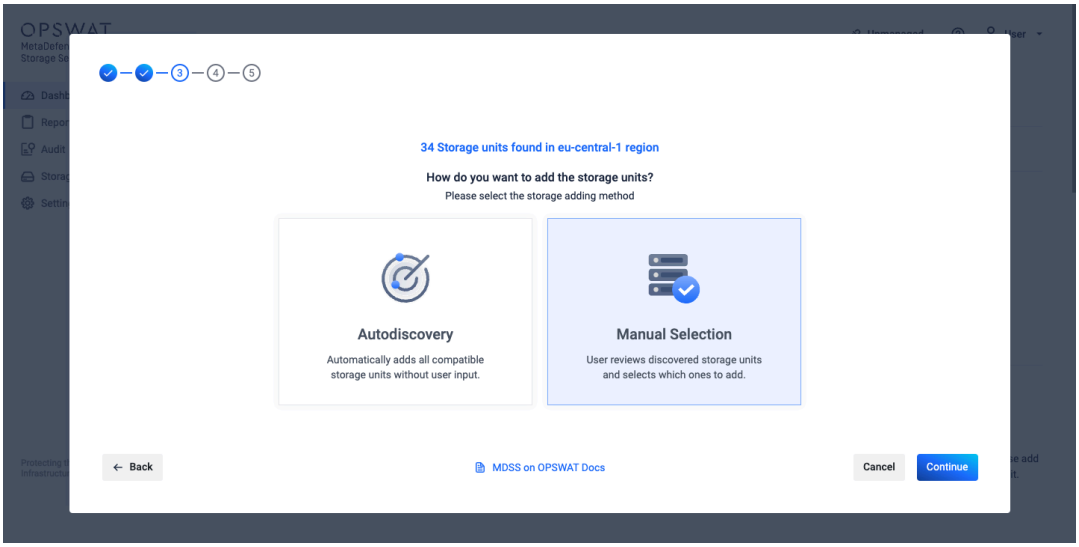
> **NO BUCKETS FOUND FOR THE SPECIFIC REGION**
>
> If there were no buckets found for the specific region, you will be presented with a third option - **Add Individually** - which will reveal the credentials form to manually add the storage by using the bucket name.

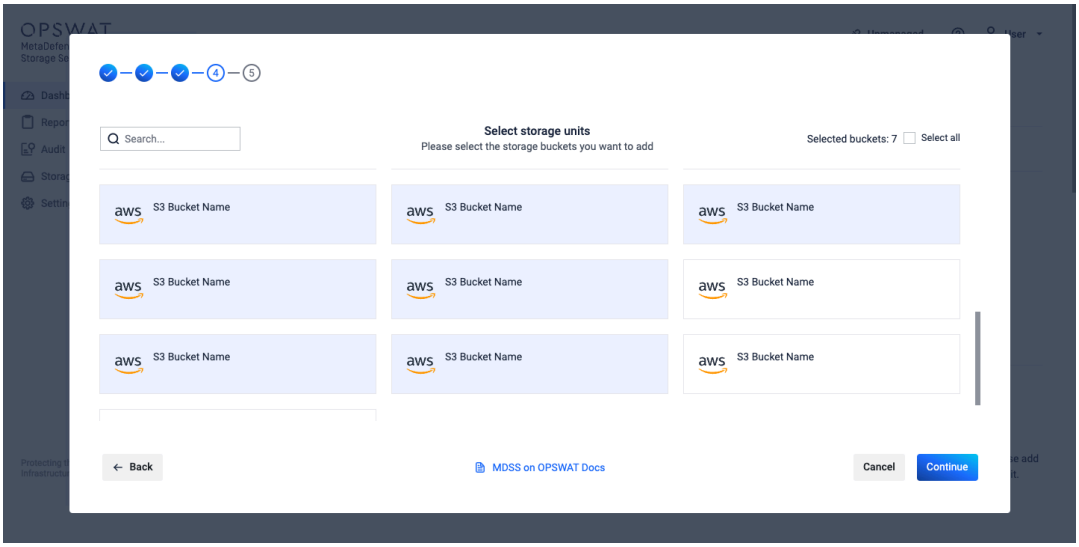
- If selecting **Autodiscovery** option:
  - Click **Continue** and an informative message will be displayed that the autodiscovery process has started in the background. You can safely close the modal and the storages will be added in background to the Storage Units page

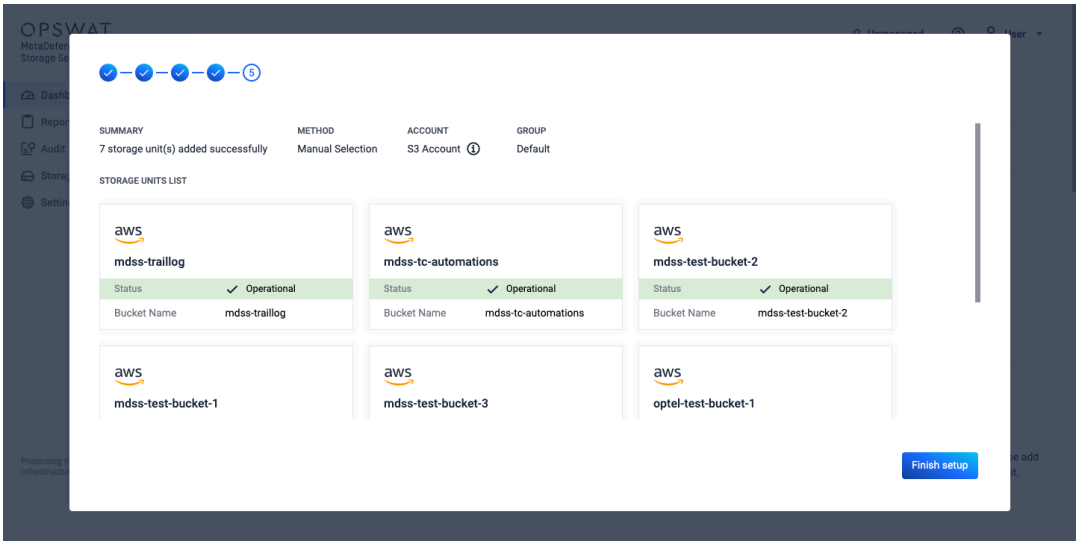




- If selecting **Manual Selection** option:
  - Click **Continue**
  - Select the buckets you want to add from the discovered list
  - Click **Continue**
  - The system will show a syncing message indicating buckets are being added; You can choose to stay on this page in order to see the storages that were successfully added and also to see if there were any errors while trying to add specific storages.





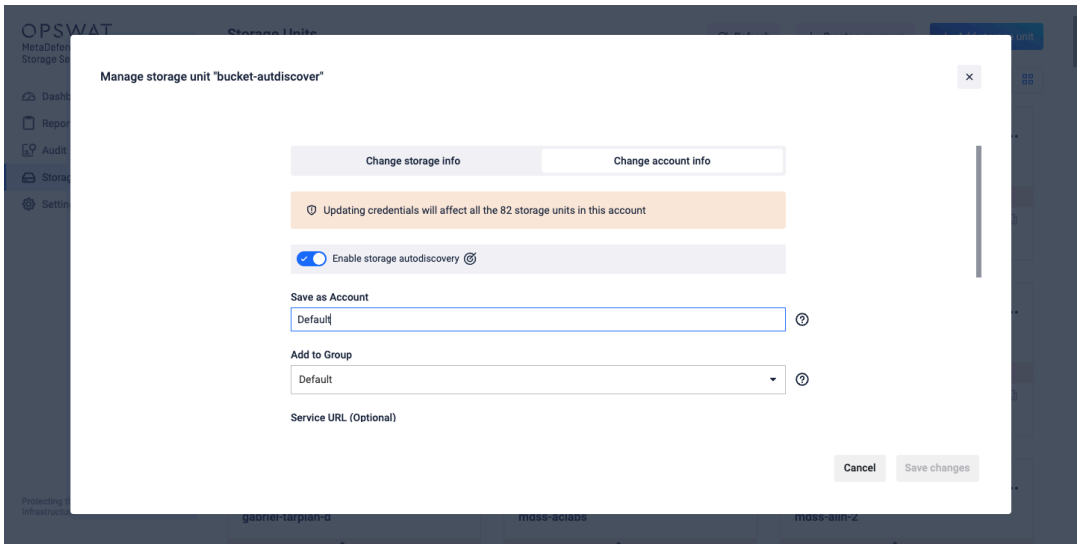


ERROR ADDING A STORAGE THAT WAS SELECTED DURING MANUAL SELECTION

> In case there was an error while trying to add your storage, you will see the error message in the Storage card while hovering over the (i) icon.

Method 2: Enable Autodiscovery for an Existing Account

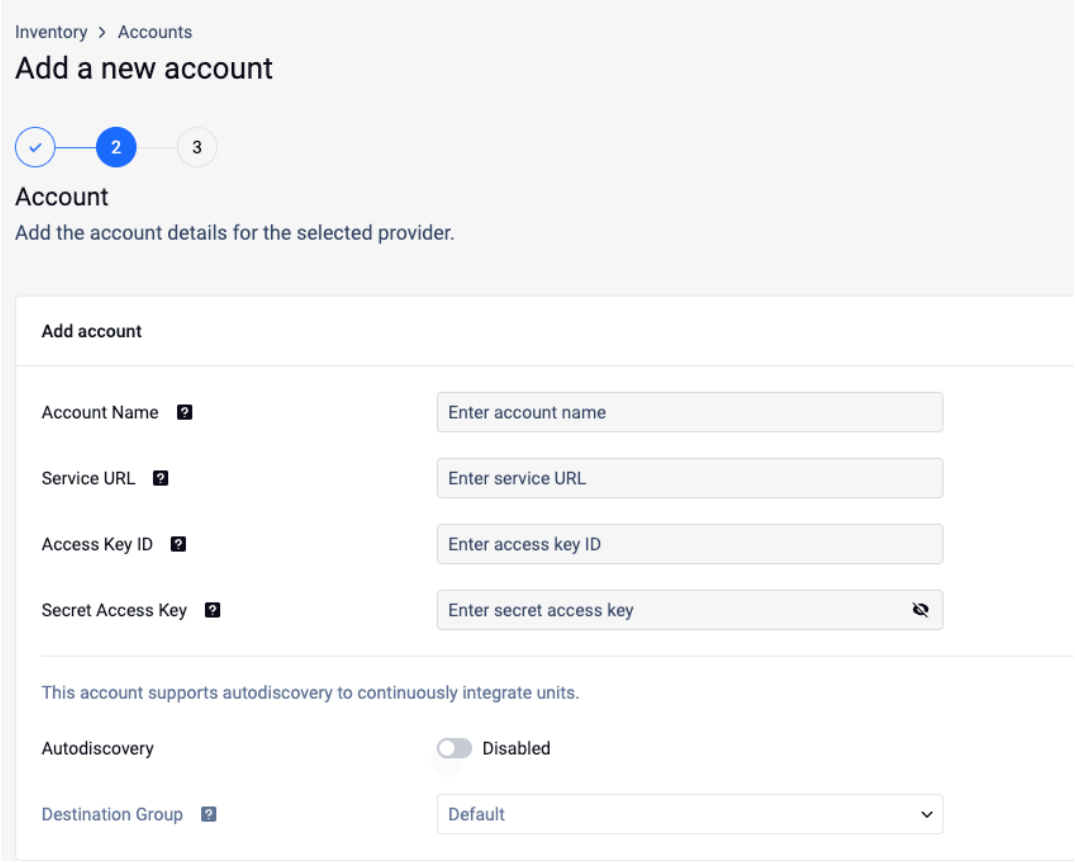
- Navigate to **Storage Units** page
- Identify a storage that's using the account you want to start autodiscovery for
- Click on the 3-dots button from the storage's card and select **Manage Storage Unit**
- From the top toggle, select **Change account info**
- Turn on autodiscovery by toggling the **Enable storage autodiscovery** switch



Add A Cubbit Storage

1. Prerequisites

In order to Add a **Cubbit** storage in MDSS, you will need the **Cubbit Service URL, Access Key Id, Secret Access Key** and the **bucket name**.



2. Obtaining the Service URL

1. Enter **s3.cubbit.eu** as the REST Endpoint or if you have a custom tenant **s3.[your-tenant].cubbit.eu.**

3. Obtaining Access Keys

1. **Access Console:** Go to the Cubbit console dashboard.
2. **Find Access Keys:** Look for **API keys** in the side menu
3. **Generate Keys:** Create a new set of keys, following any provided guidelines.
4. **Record Keys:** Securely note down your **Access Key ID** and **Secret Access Key**.

4. Obtaining the bucket name

1. **Login:** Sign into Cubbit and navigate to the dashboard.
2. **Identify Bucket:** Find your bucket in the list and note its name.

5. Adding Cubbit storage in MDSS

Once you have the details above, go to your MDSS web page, **Storage Units** page, click **Add storage unit**, choose **Cubbit** and fill the form.

6. Limitations

> **Bucket Versioning not supported**
>
> Due to a known issue with the Cubbit, any action that MDSS does to delete a version of the file will not work as expected. This will not affect in any way a user that doesn't use bucket versioning

Add An Oracle Cloud Storage

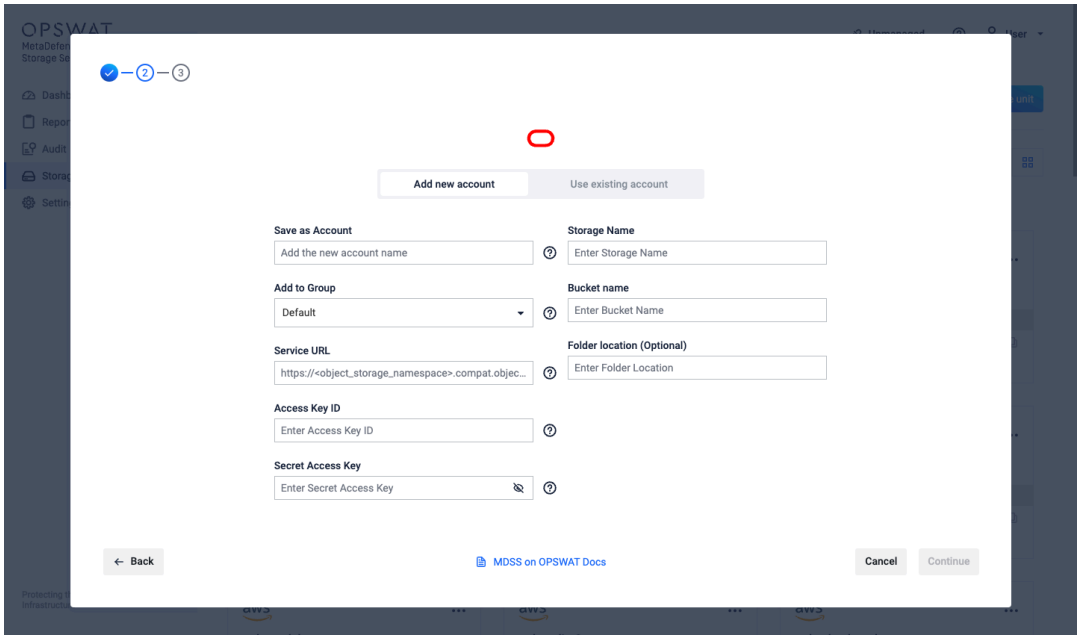
Oracle Cloud Storage can be integrated into MetaDefender Storage Security (MDSS) in **two different ways**:

1. **Using the S3-Compatible API** – This method allows MDSS to connect to Oracle Object Storage using S3-style access credentials (Access Key and Secret Key).
2. **Using the Oracle Native SDK (OCI SDK)** – This method uses Oracle's native authentication system with API keys or IAM roles for a more direct and secure integration.

Integration via S3-Compatible

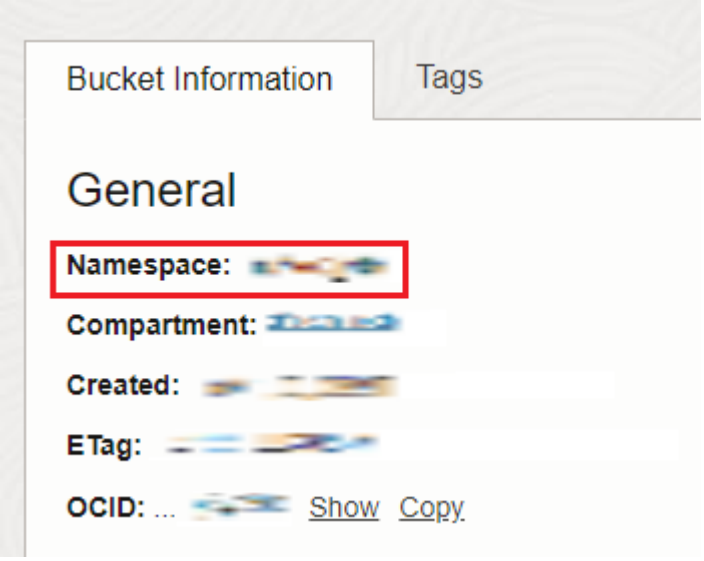
1. Prerequisites

In order to Add an Oracle Cloud storage in MDSS, you will need the **Oracle Cloud Service URL**, **Access Key Id / Secret Access Key** and the **bucket name**.



2. Obtaining the Service URL

1. To construct the URL, you will need to have you bucket's object storage namespace and region. The namespace can be found the navigating to one of your existing buckets and opening it. Afterwards, construct the URL like this: **https://<your_object_storage_namespace>.compat.objectstorage.<your_region>.oraclecloud.com**



3. Obtaining Access Key ID

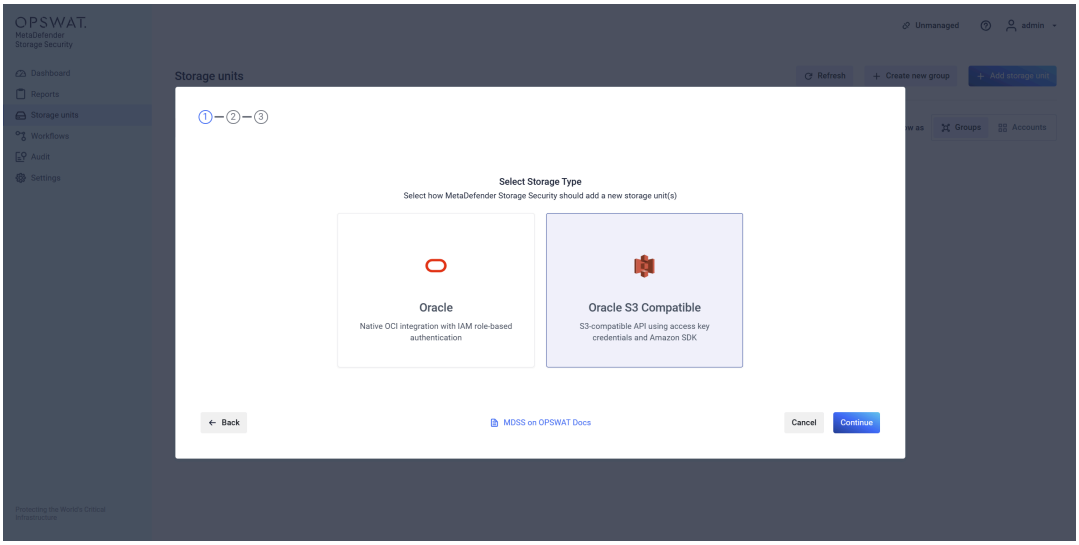
1. Log in to your Oracle Cloud dashboard at **cloud.oracle.com**
2. In the top-right corner, open the **Profile** menu by clicking on your profile icon and afterwards, click on **My profile**
3. From the **Resources** tab**,** navigate to **Customer secret keys** and either click **Generate secret key** or copy an existing one from the list

4. Obtaining Secret Access Key

1. Log in to your Oracle Cloud dashboard at **cloud.oracle.com**
2. In the top-right corner, open the **Profile** menu by clicking on your profile icon and afterwards, click on **My profile**
3. Click **Generate secret key** and give the key any name you like
4. Save the generated key secret somewhere safe. You can only see it at creation

5. Adding the Oracle Cloud storage in MDSS as an S3 Compatible

Once you have the details above, go to your MDSS web page, **Storage Units** page, click **Add storage unit**, click **Oracle,** choose **Oracle S3 Compatible** and fill the form.

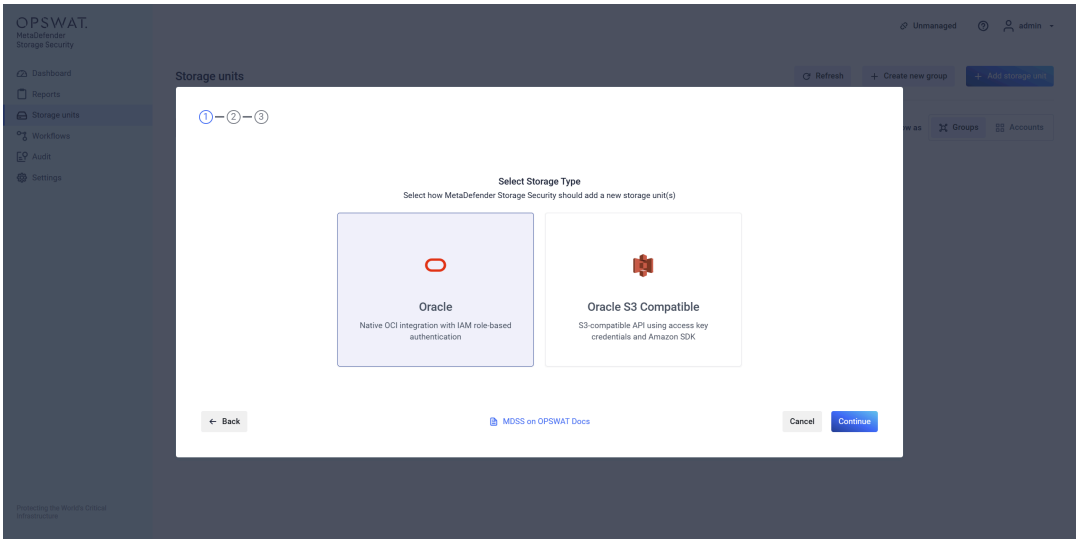


Integration via Oracle Native SDK (OCI SDK)

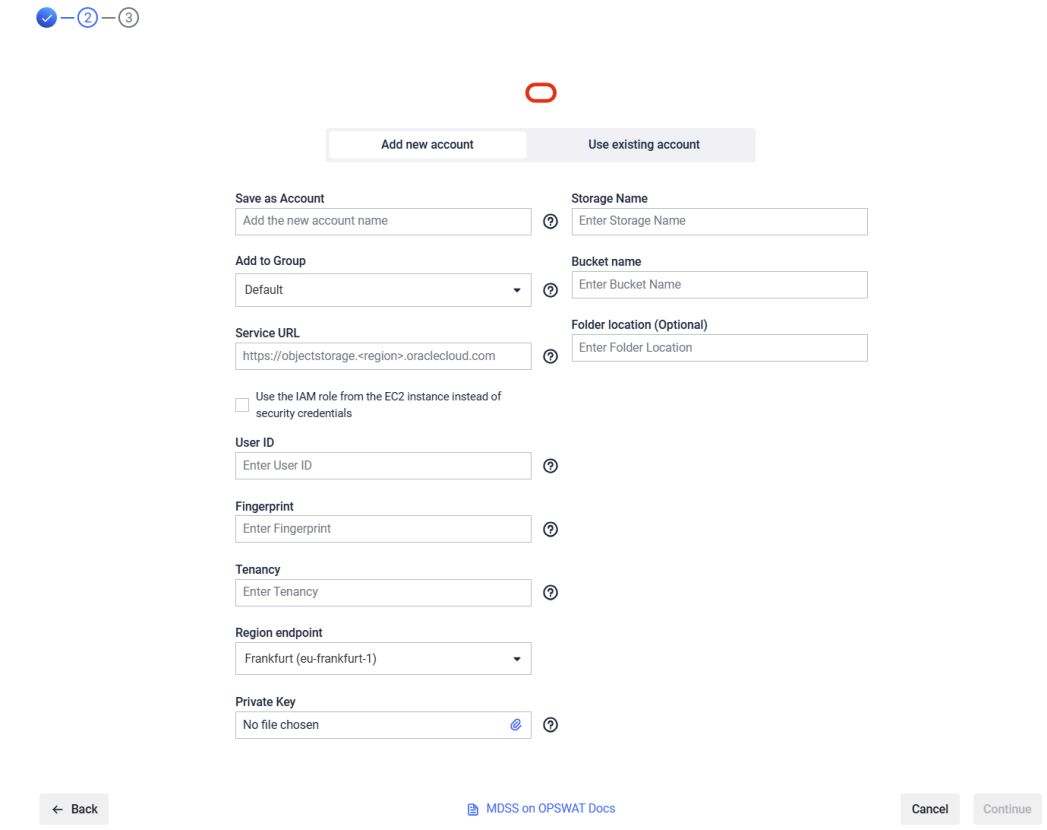
1. Prerequisites

In order to Add an Oracle SDK storage in MDSS, you will need an **Oracle API Key including UserId, Fingerprint, Tenancy, Region and Private Key, and the bucket name**

1. From the left side menu, navigate to **Storage units**, click on **Add Storage** Unit and choose **Oracle**



2. Choose the **Oracle** option



3. Give your storage a name so you can easily identify it later
4. There are two ways to connect:
   - **via the IAM role from the instance:** please skip to using IAM Role for authentication
   - **using security credentials**
5. Enter your **User Id**, **Fingerprint**, **Tenancy**, **Region** and **Private Key**
6. Enter the **name of the bucket** you wish to process with **MetaDefender Storage Security**.
7. If you wish to only process a particular folder enter the name or path of the folder in the **Folder location** field. Leave this field empty if you wish to process the entire bucket.
8. Select **Continue** in order to finish the process.

Where can I find the Credentials?

To generate the required credentials please follow these steps:

1. Log in to Oracle Console and go to **My Profile** in the top right
2. From there go to **Token and Keys** tab
3. Click **Add API Key**
4. Download the **Private Key** and Click **Add**

5. After that all the required credentials will be generated and can be copied into **MetaDefender Storage Security**

Using IAM Role for authentication

Allow your **MetaDefender Storage Security** instance to use the **Instance Principals** to access Object Storage (buckets and objects) securely without embedding credentials.

1. Create a **Dynamic Group** with at least the following matching rule `instance.id = <your instance id>`
2. Create an **IAM Policy** with the following statements
    1. Allow dynamic-group to manage buckets in tenancy
    2. Allow dynamic-group to manage objects in tenancy

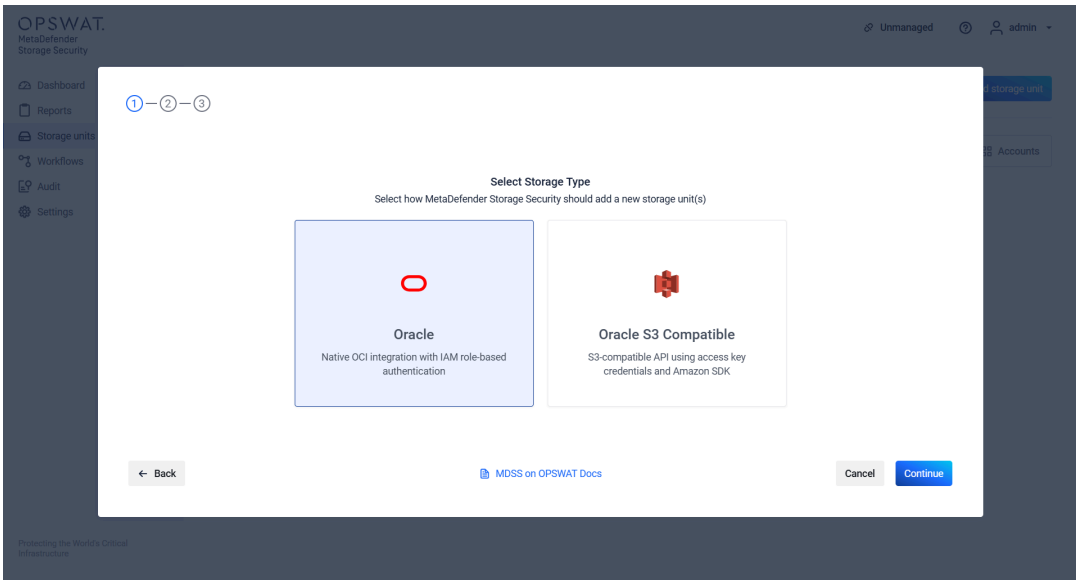
This setup allows your MDSS instance to securely access Oracle Object Storage using Oracle Cloud's native identity management system.

Add An Oracle SDK Storage

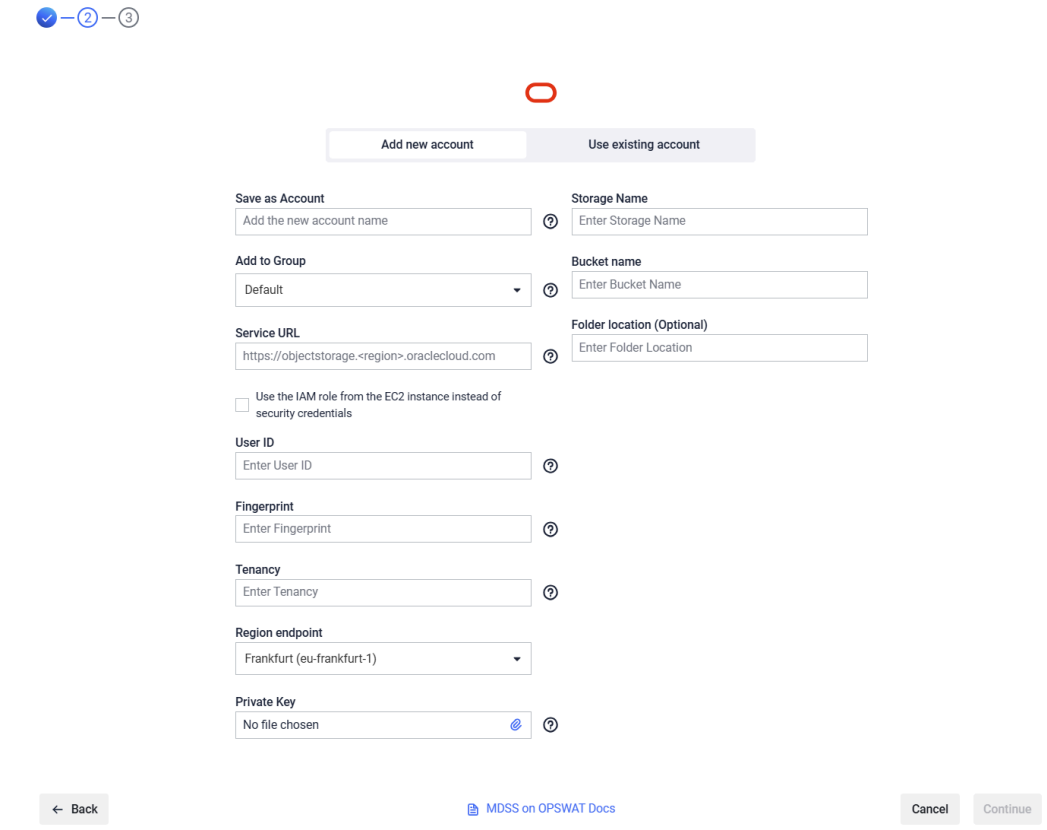
1. Prerequisites

In order to Add an Oracle SDK storage in MDSS, you will need an **Oracle API Key including UserId, Fingerprint, Tenancy, Region and Private Key, and the bucket name**

1. From the left side menu, navigate to **Storage units**, click on **Add Storage** Unit and choose **Oracle**



2. Choose the **Oracle** option



3. Give your storage a name so you can easily identify it later
4. There are two ways to connect:
   - **via the IAM role from the instance:** please skip to using IAM Role for authentification
   - **using security credentials**
5. Enter your **User Id**, **Fingerprint**, **Tenancy**, **Region** and **Private Key**
6. Enter the **name of the bucket** you wish to process with **MetaDefender Storage Security**.
7. If you wish to only process a particular folder enter the name or path of the folder in the **Folder location** field. Leave this field empty if you wish to process the entire bucket.
8. Select **Continue** in order to finish the process.

Where can I find the Credentials?

To generate the required credentials please follow these steps:

1. Log in to Oracle Console and go to **My Profile** in the top right
2. From there go to **Token and Keys** tab
3. Click **Add API Key**

4. Download the **Private Key** and Click **Add**
5. After that all the required credentials will be generated and can be copied into **MetaDefender Storage Security**

Using IAM Role for authentication

Allow your **MetaDefender Storage Security** instance to use the **Instance Principals** to access Object Storage (buckets and objects) securely without embedding credentials.

1. Create a **Dynamic Group** with at least the following matching rule `instance.id = <your instance id>`
2. Create an **IAM Policy** with the following statements
    1. Allow dynamic-group to manage buckets in tenancy
    2. Allow dynamic-group to manage objects in tenancy

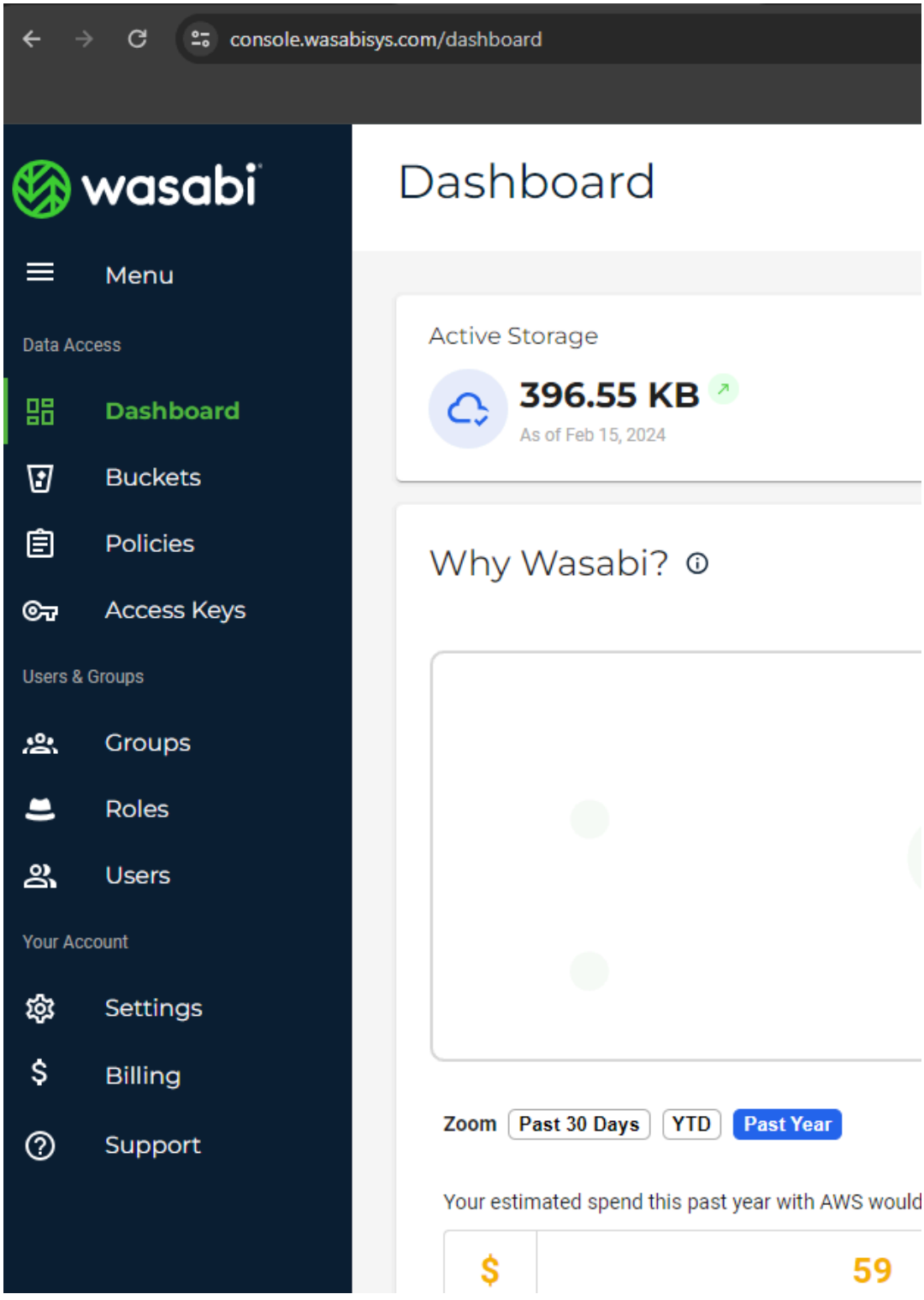
Add A Wasabi Storage

1. Prerequisites

In order to Add a **Wasabi** storage in MDSS, you will need the **Wasabi Service URL**, **Access Key Id / Secret Access Key** and the **bucket name**. If you want to enable **path style addressing** for the bucket, tick the checkbox.

2. Obtaining the Service URL

1. **Login:** Sign into your Wasabi account at https://console.wasabisys.com/
2. **Find Bucket Region:** In the bucket management section, note your bucket's region.
3. **Construct URL:** Format your service URL as `https://s3.<bucket-region>.wasabisys.com`, replacing `<bucket-region>` with your bucket's actual region.
4. Wasabi service URL docs



3. Obtaining Access Keys

1. **Access Console:** Go to the Wasabi console dashboard.
2. **Find Access Keys:** Look for “Access Keys” in the main menu [https://console.wasabisys.com/access_keys/]
3. **Generate Keys:** Create a new set of keys, following any provided guidelines.

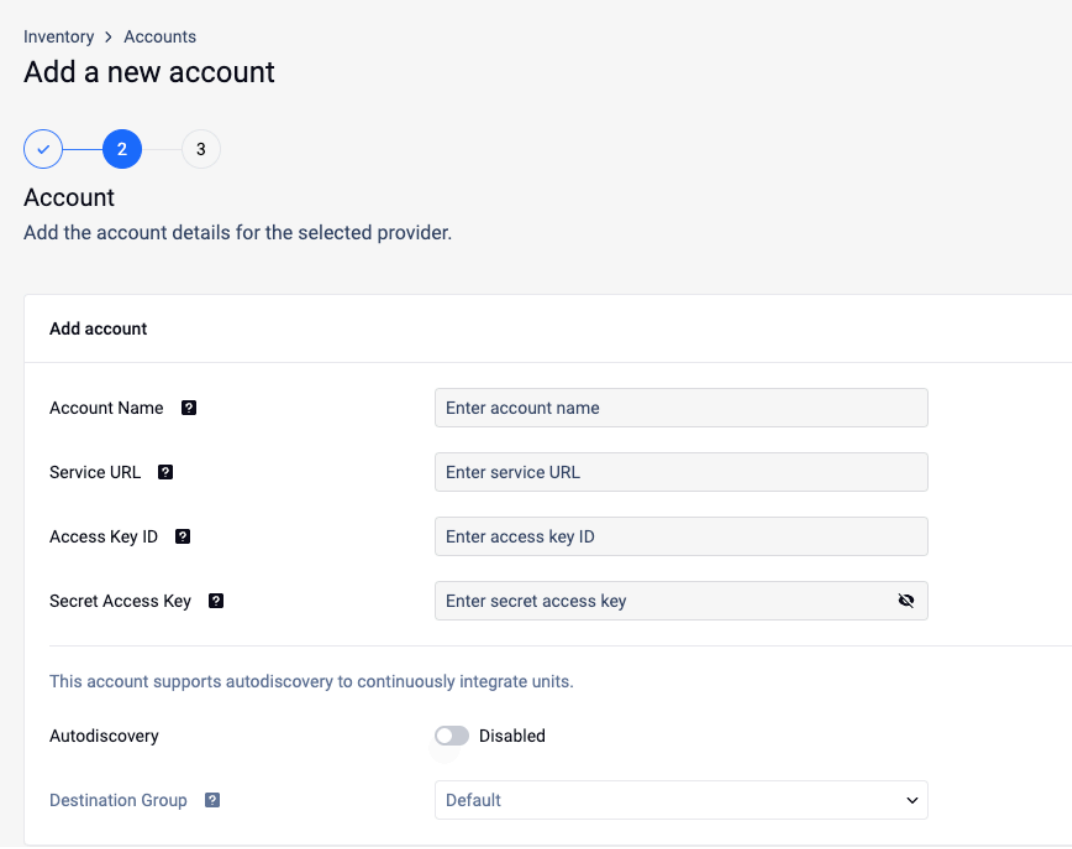
4. **Record Keys:** Securely note down your Access Key ID and Secret Access Key.

4. Obtaining the bucket name

1. **Login:** Sign into Wasabi and navigate to the dashboard.
2. **Go to Buckets:** Locate the “Buckets” section [https://console.wasabisys.com/file_manager/]
3. **Identify Bucket:** Find your bucket in the list and note its name.

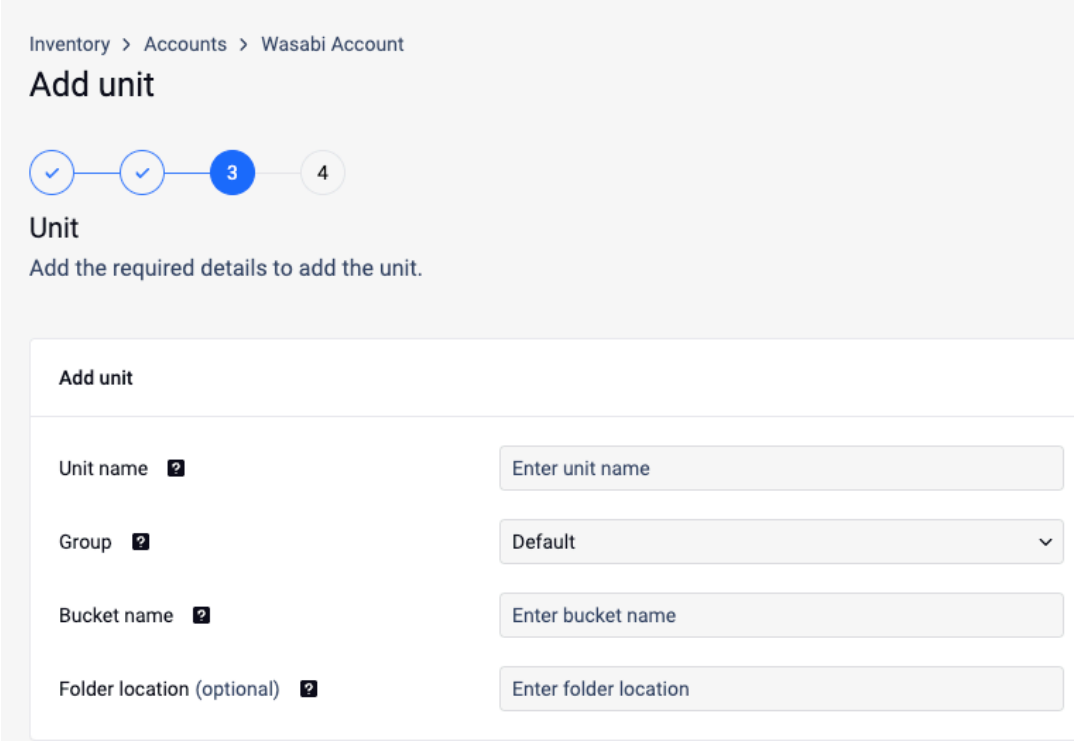
5. Adding Wasabi storage in MDSS

Once you have the details above, go to your MDSS web page, **Inventory** tab, click **Add account **choose **Wasabi** and fill the form.



Once the account is successfully added, please add the storage unit. Navigate to Inventory -> Add Unit -> Choose previously created Wasabi account:

1. Give your storage unit an unique name
2. Choose the group
3. Enter a valid bucket name
4. Enter folder location (optional)



Info

Supports both virtual-host and path-based style addressing

6. Limitations

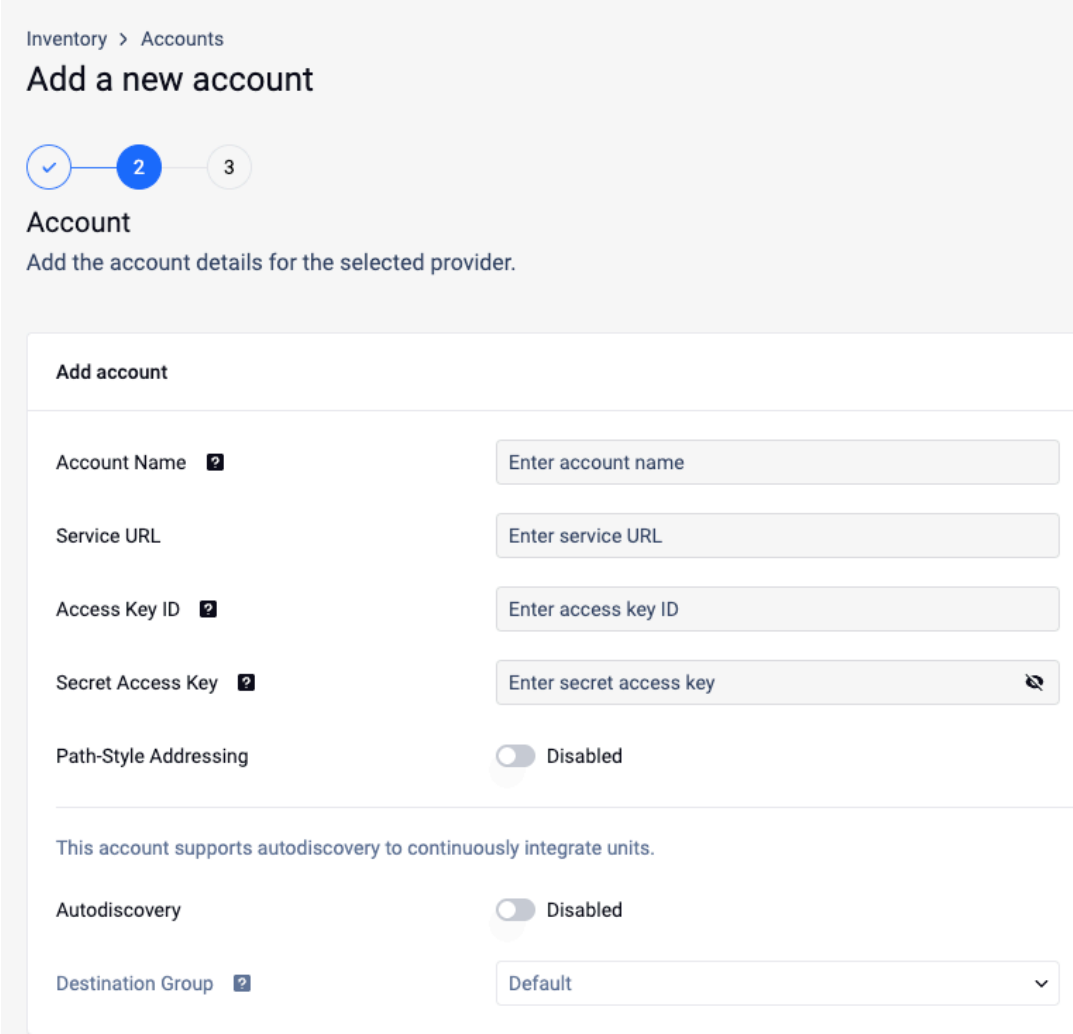
Real-Time Scans and File Renaming in Wasabi Storage

Due to a known issue with the Wasabi web interface, renaming a file does not change its “Last Modified” field. Consequently, MDSS cannot initiate real-time scans when files are renamed within Wasabi storage. This limitation stems from MDSS’s reliance on detecting changes to the “Last Modified” field to trigger scans, which does not occur in this specific scenario with Wasabi storage.

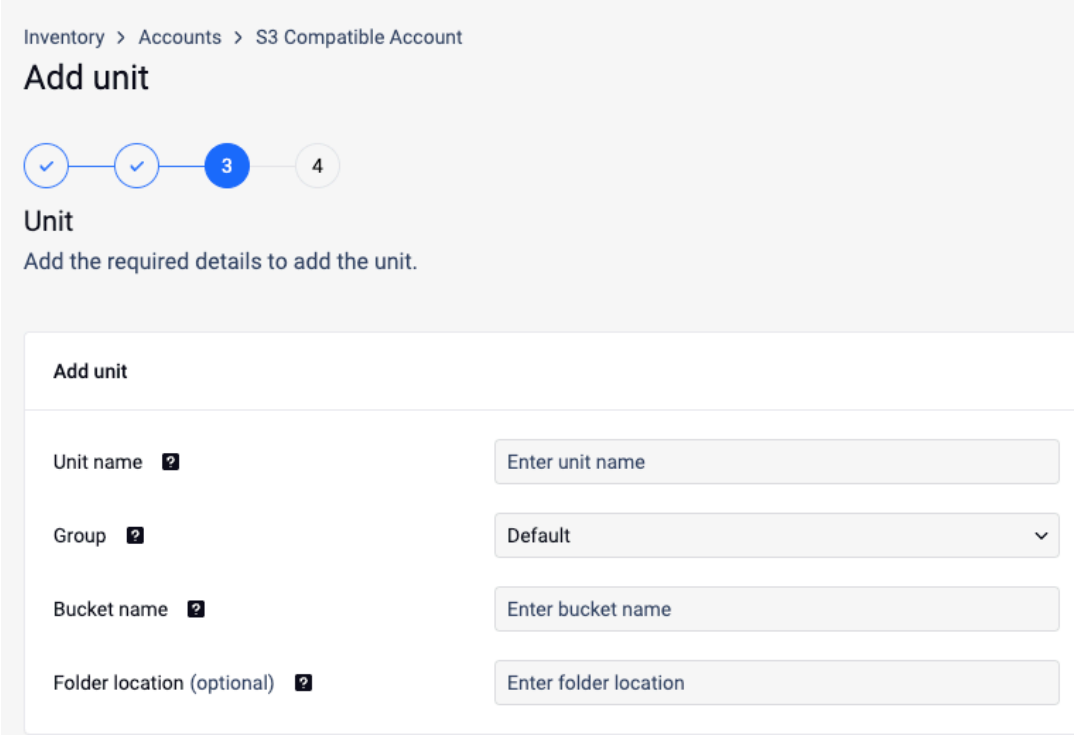
Add a Cloudian Storage

In order to integrate Cloudian On-Premises with MetaDefender Storage Security please follow these steps:

1. From the left side menu, navigate to **Inventory,** click on **Add Account **and choose **S3 Compatible**



2. Give your account a name so you can easily identify it later
3. Enter the Service URL for your Cloudian endpoint
4. Enter your **Access Key ID**. Scroll to the end of this page for more details.
5. Enter your **Secret Access Key.** Scroll to the end of this page for more details.
6. If you want to enable **path style addressing** for the bucket, tick the checkbox.
7. (Optional) Enable Autodiscovery
8. Once the account is successfully added, navigate to Inventory -> Add Unit -> Choose the account

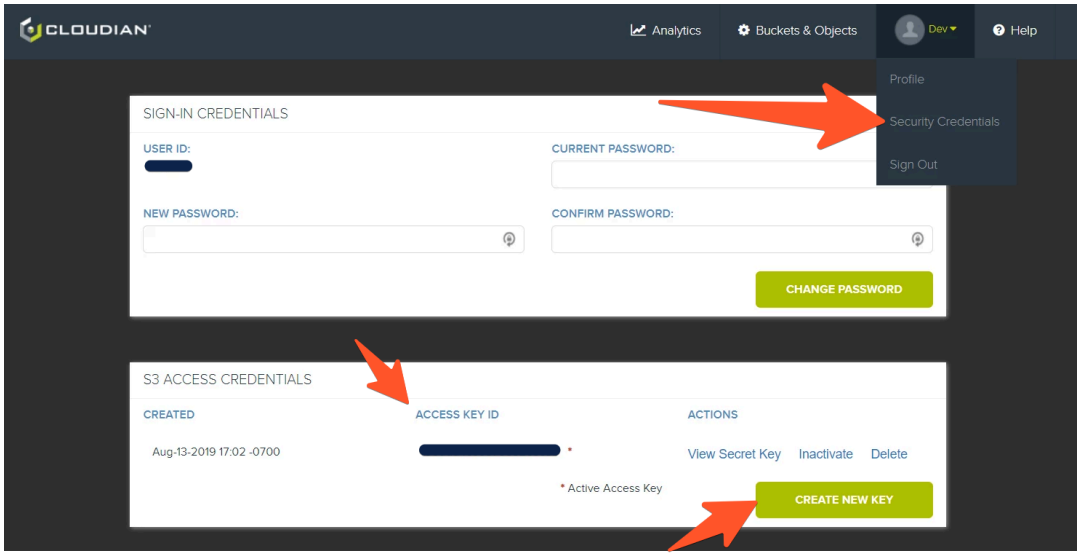


9. Give your unit an unique name
10. Choose Group
11. Enter a valid bucket name
12. Enter a Folder location (optional)

Where can I find the Access Key ID and Secret Access Key

To generate an Access Key ID / Secret Access Key pair please follow these steps:

1. Log in to **Cloudian Console** and go to **Security Credentials**
2. From the S3 Access Credentials zone, copy an existing Access Key ID and Secret Key or generate a new one by clicking **Create New Key.**

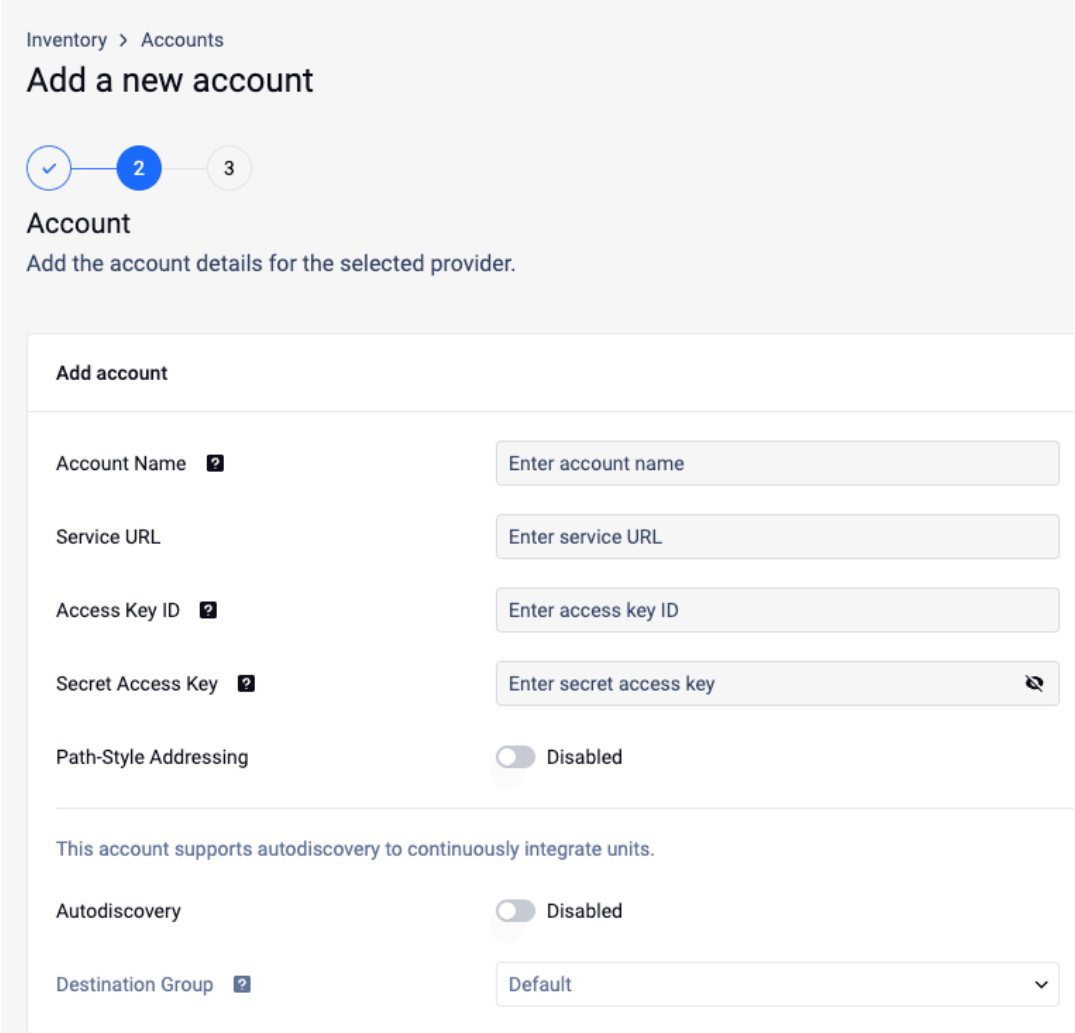

CLOUDIAN
Analytics
Buckets & Objects
Dev
Help
Profile
Security Credentials
Sign Out
SIGN-IN CREDENTIALS
USER ID:
CURRENT PASSWORD:
NEW PASSWORD:
CONFIRM PASSWORD:
CHANGE PASSWORD
S3 ACCESS CREDENTIALS
CREATED
ACCESS KEY ID
ACTIONS
Aug-13-2019 17:02 -0700
View Secret Key
Inactivate
Delete
* Active Access Key
CREATE NEW KEY

Add a MinIO Storage

> **Info**
>
> The minimum supported MinIO version is **RELEASE.2020-09-10T22-05-01Z**.

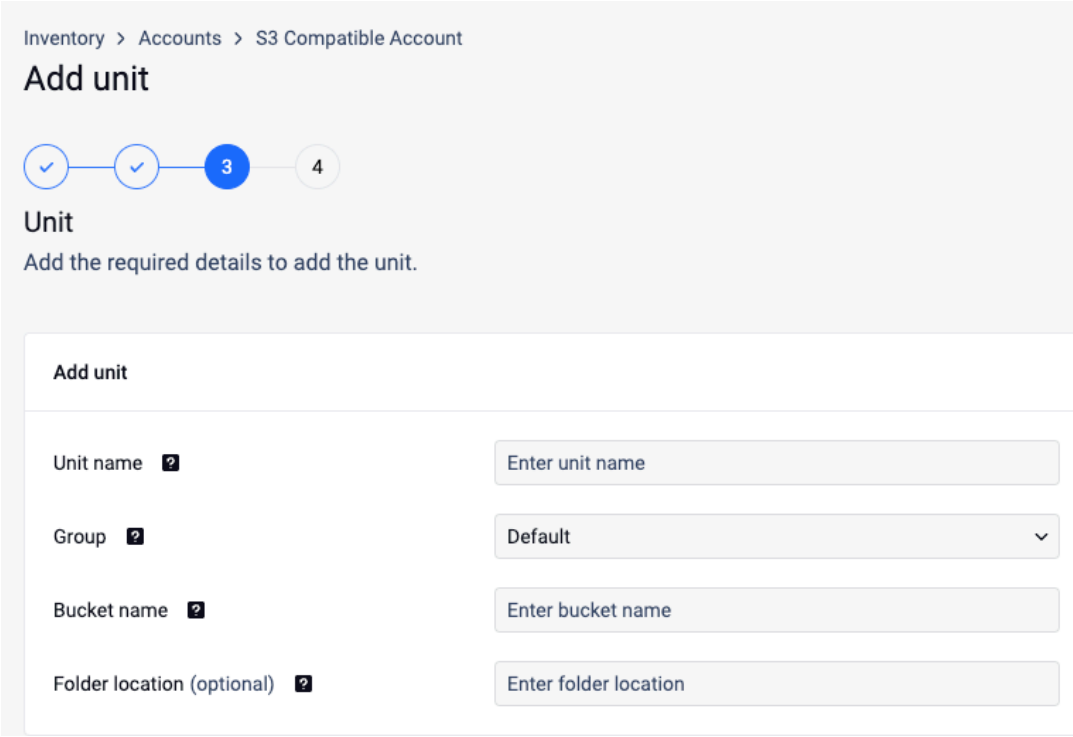
In order to integrate MinIO with MetaDefender Storage Security please follow these steps:

1. From the left side menu, navigate to **Inventory,** click on **Add Account **and choose **S3 Compatible**



2. Give your account a name so you can easily identify it later
3. Enter the Service URL for your MinIO endpoint
4. Enter your **Access Key ID**. Scroll to the end of this page for more details.
5. Enter your **Secret Access Key.** Scroll to the end of this page for more details.
6. If you want to enable **path style addressing** for the bucket, tick the checkbox.
7. (Optional) Enable Autodiscovery

8. Once the account is successfully added, navigate to Inventory -> Add Unit -> Choose the account

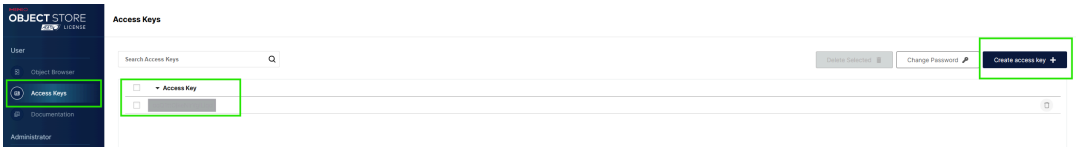


9. Give your unit an unique name
10. Choose Group
11. Enter a valid bucket name
12. Enter a Folder location (optional)

Where can I find the Access Key ID and Secret Access Key

To generate an Access Key ID / Secret Access Key pair please follow these steps:

1. Log in to **MinIO Console** and go to **Access Keys**
2. Copy an existing Access Key ID and Secret Key or generate a new one by clicking **Create New Key.**

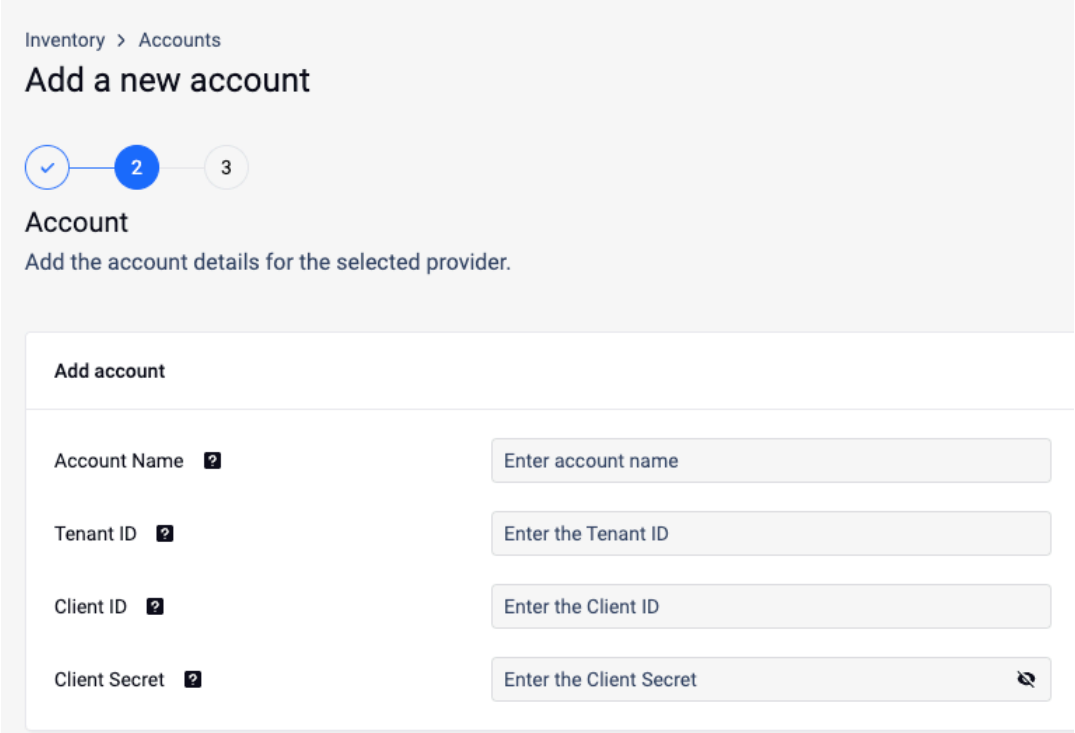


Add an OneDrive Storage

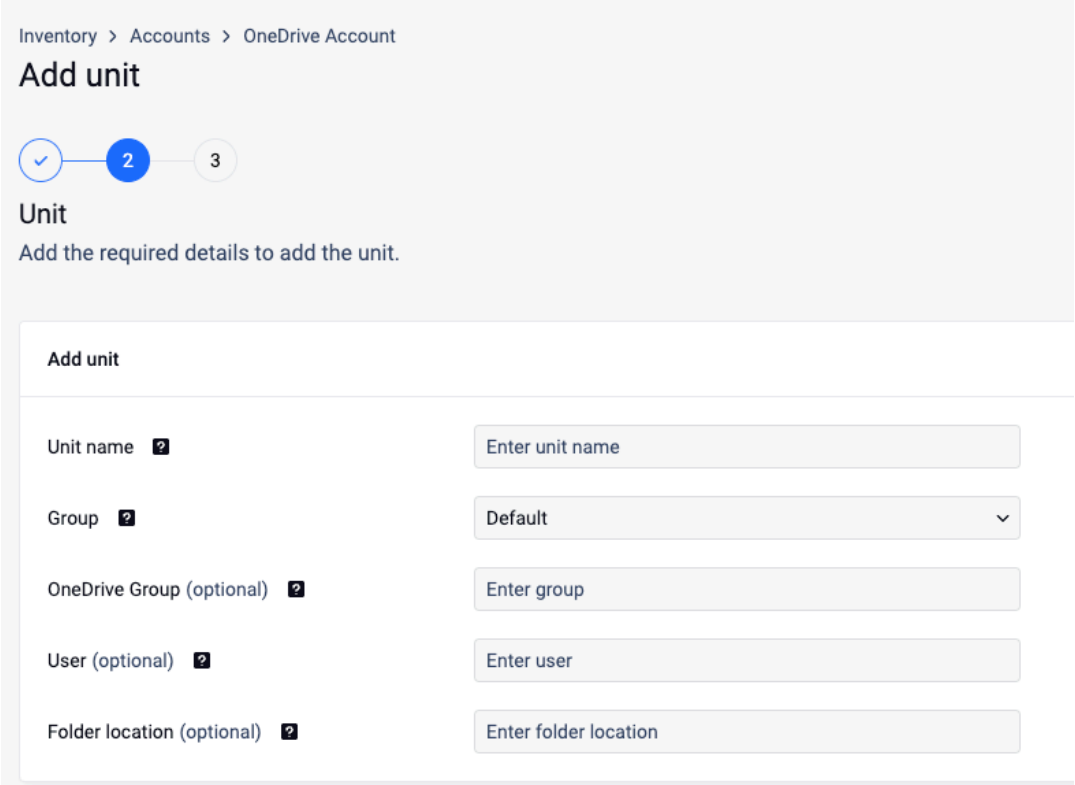
In order to integrate Microsoft OneDrive service with MetaDefender Storage Security you will be required to create an application registration, assign the necessary permissions and then generate a secret key. Please follow these steps:

> **Info**
>
> When the upload process takes more than a few seconds, OneDrive creates a temporary file having the same name as your uploading file and the size of 0 bytes. By default, we will discover that file and show it into the list of discovered files. Once the upload is complete, we will discover the original uploaded file and process it accordingly. To skip the discovery of the temporary empty file created, please follow these instructions: How to handle empty objects in Discovery?

1. From the left side menu, navigate to **Inventory,** click on **Add Account** and choose **OneDrive**



2. Give your account a name so you can easily identify it later
3. Enter your **Tenant ID**. Scroll to the end of this page for more details.
4. Enter your **Client ID.** Scroll to the end of this page for more details.
5. Enter your **Client Secret.** Scroll to the end of this page for more details.
6. Once the account is added, proceed with adding the unit

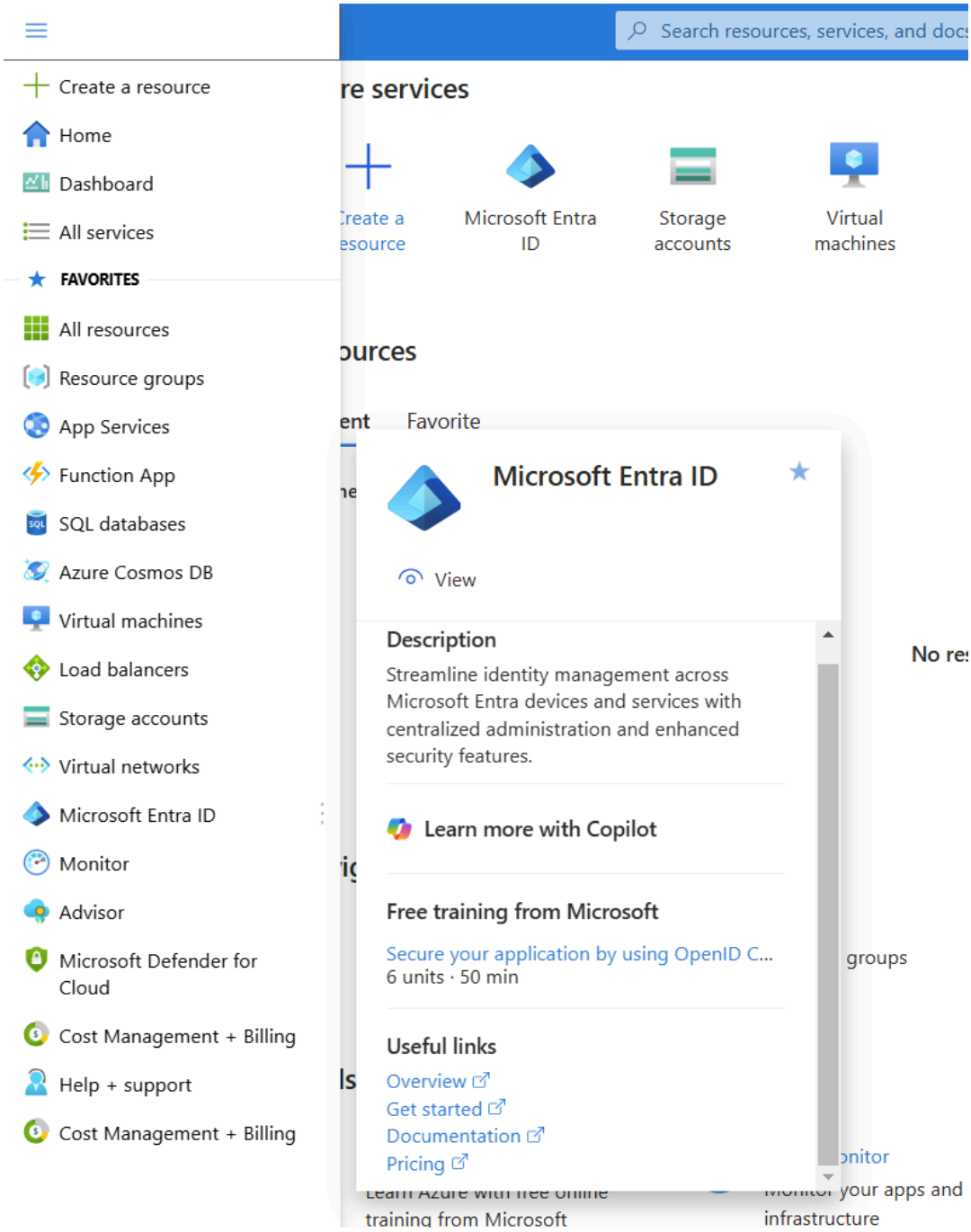


6. Enter an unique name for your unit
7. Assign the unit to a Group
8. Optionally, enter the name of a OneDrive Group that you want to protect
9. Optionally, enter the **UPN** of a user from the selected group if you wish to only process files from that specific user.
10. Optionally, enter the **name of a folder** from the user's files if you wish to only process files from that folder. This field will appear only if there is a value inputted in the **User** field.
11. Select **Continue** in order to finish the process.

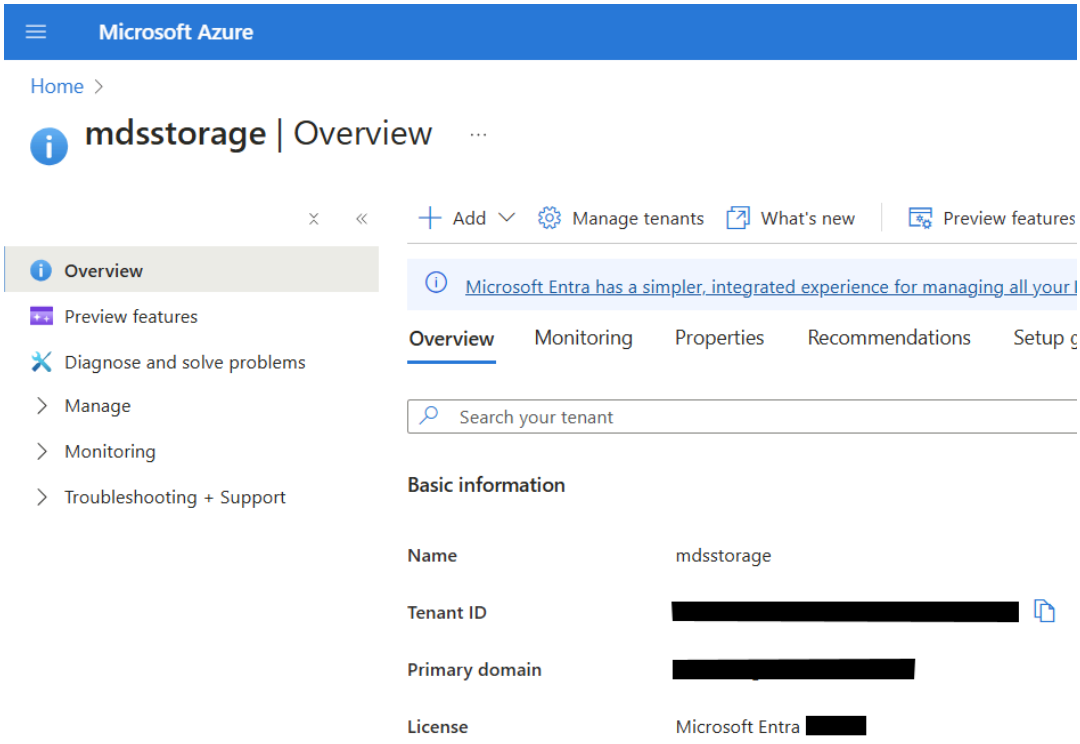
How to create a OneDrive application

In order to process your OneDrive files and folders with MetaDefender Storage Security you will be required to add a new app registration in your Microsoft Entra ID Azure Portal.

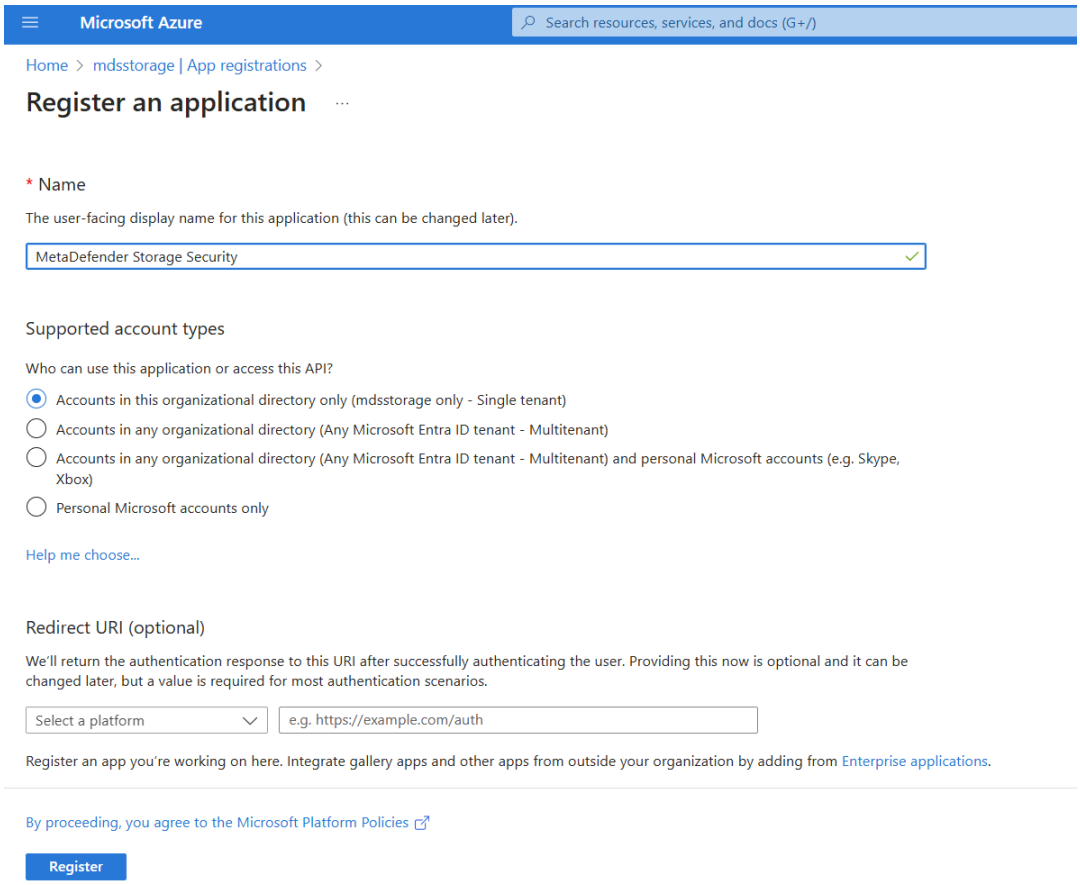
1. Log in to Azure Portal and from the left navigation menu choose **Microsoft Entra ID**



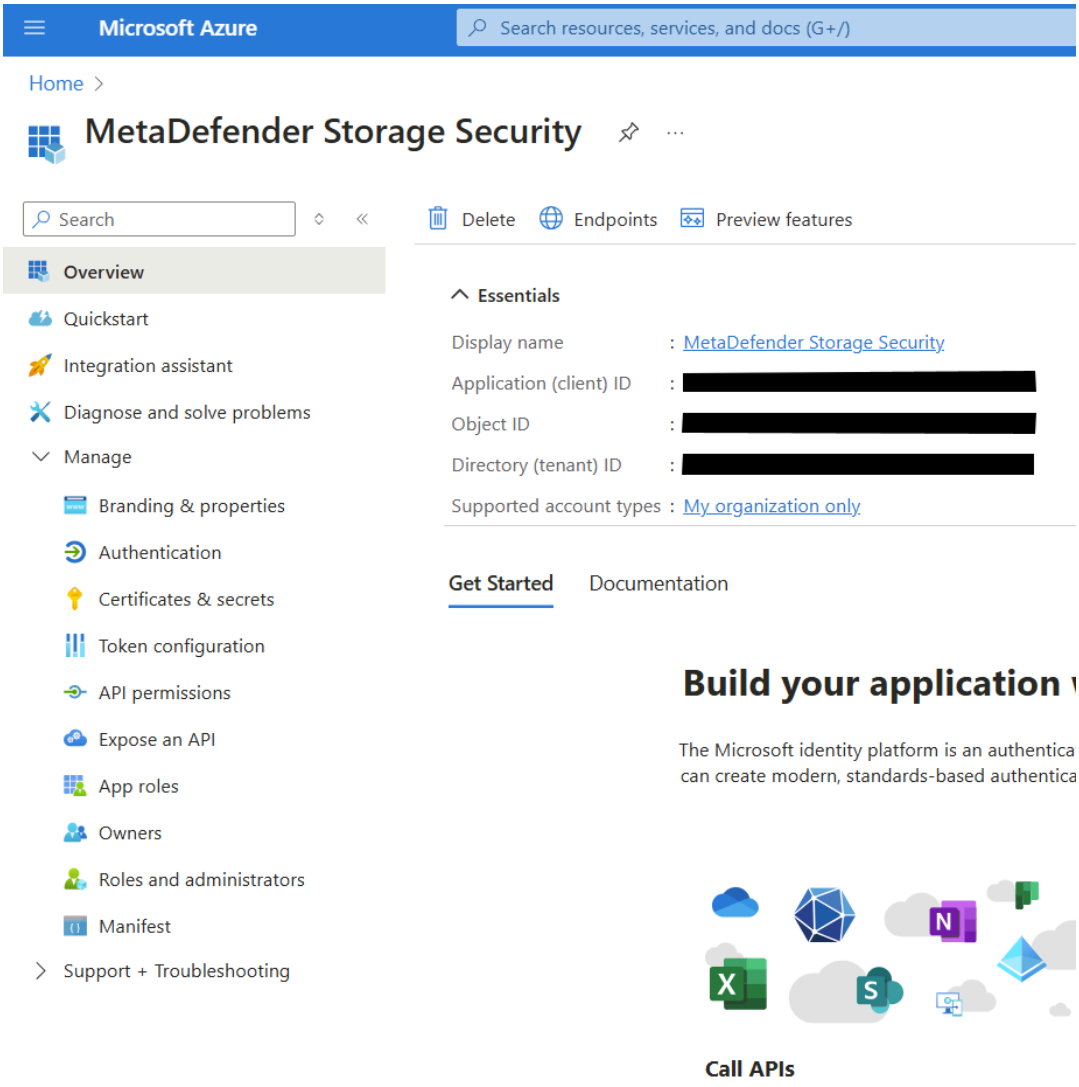
2. Make a copy of the **Tenant ID** from the overview page



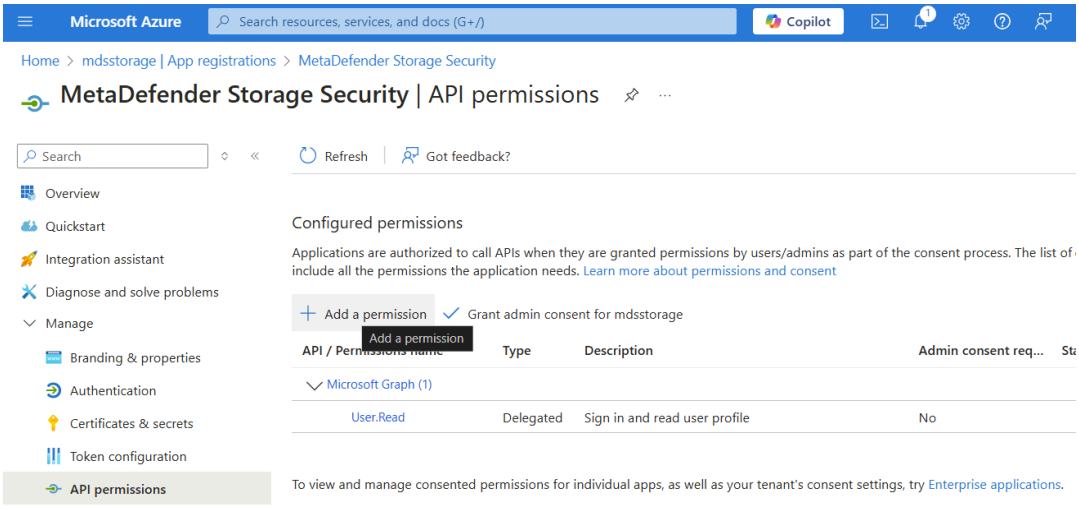
3. From the left side menu, choose **App registrations**
4. Click **New registration**
5. Give your app a name so you can easily identify it



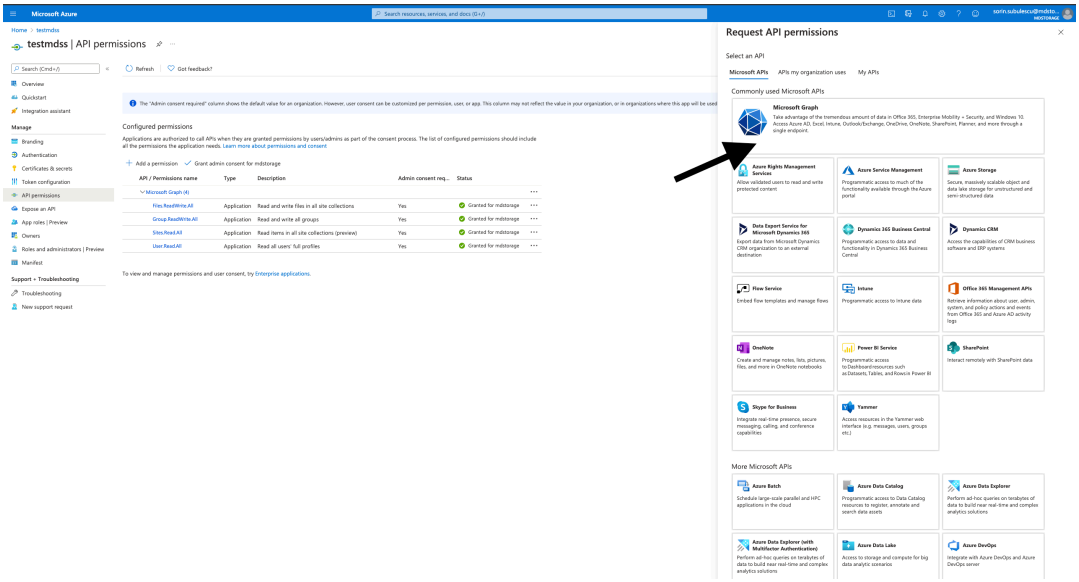
6. There is no need to modify the other properties. When ready, please click **Register**
7. From the **Overview** page of your newly created application, make a copy of **Application (client) ID**



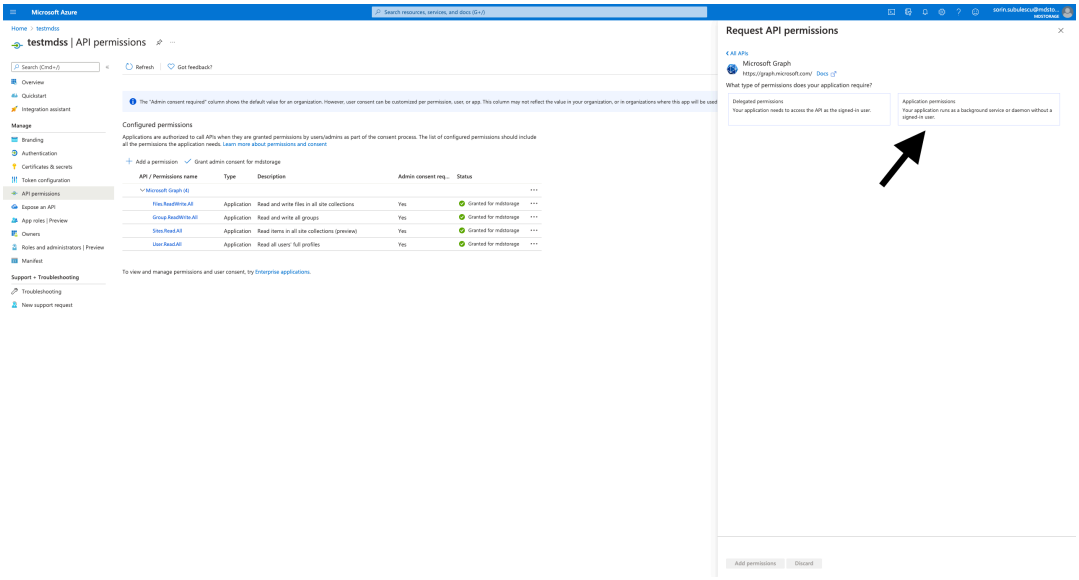
8. You now need to specify which permissions should the application have. To do this, please navigate to **API permissions** from the left-side menu
9. Click **Add a permission**



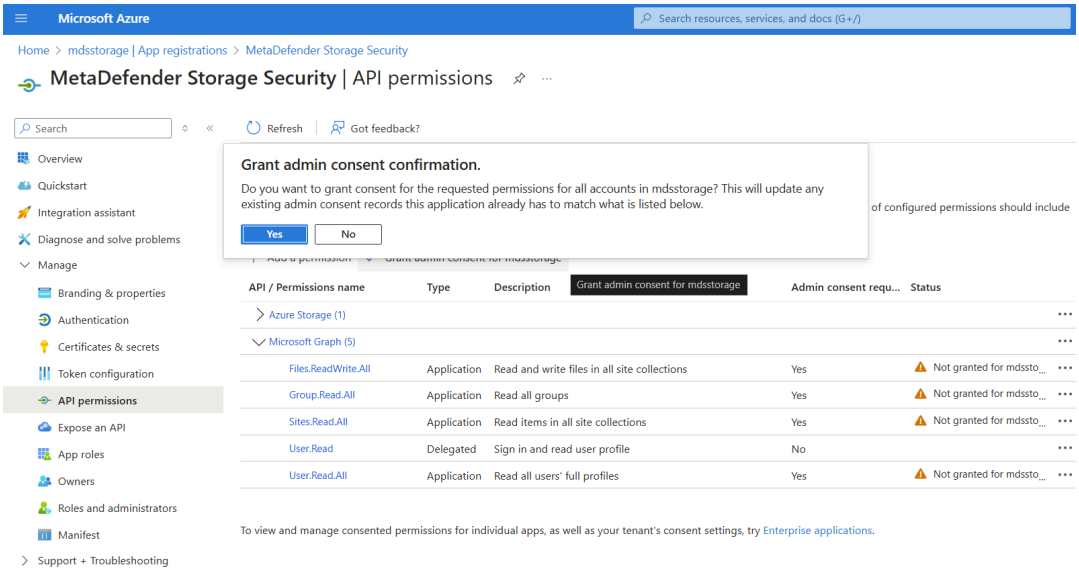
10. Select **Microsoft Graph** from the right-side menu



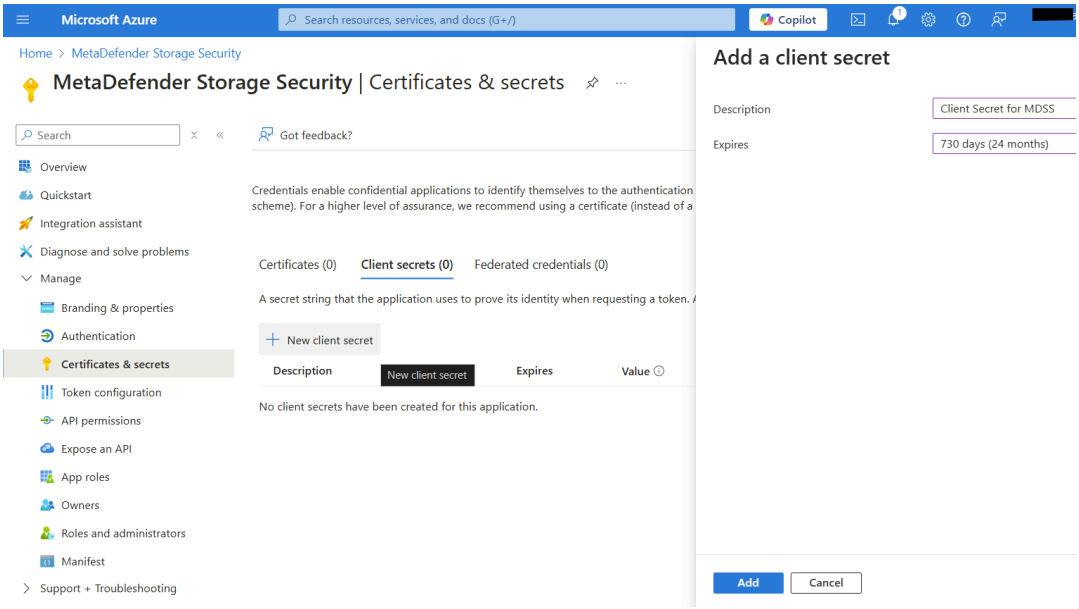
11. Select **Application permissions**



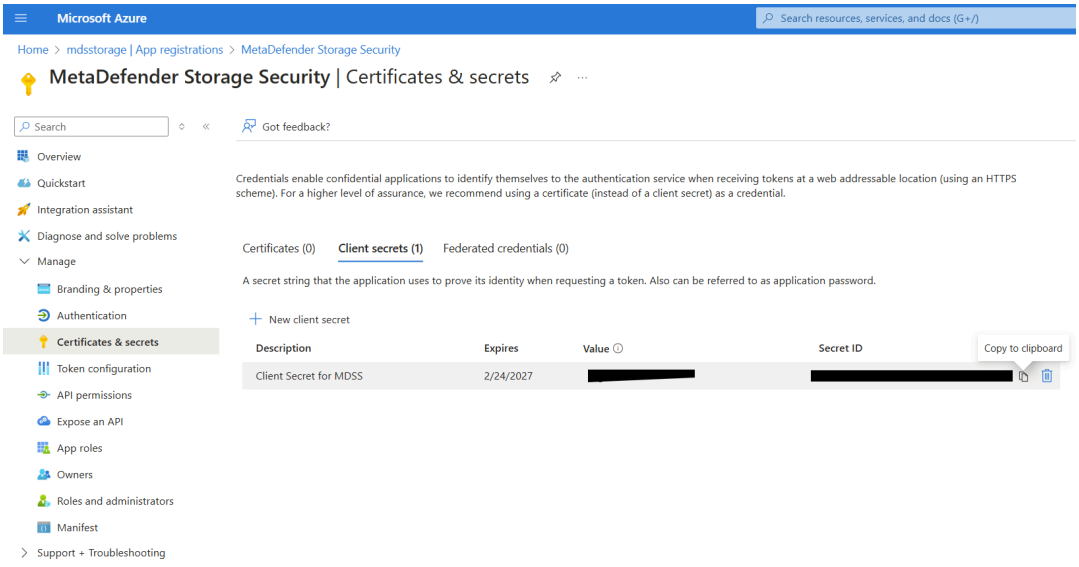
12. In order for MetaDefender Storage Security to correctly work please add the following permissions:
    1. Files.ReadWrite.All
    2. Group.Read.All
    3. Sites.Read.All
    4. User.Read.All
13. When ready, click **Add permissions**
14. We need to grant admin consent for the added permissions



15. Now that the required permissions are in place, you are ready for the final step. Please navigate to **Certificates & secrets** from the left-side menu
16. Click **New client secret** and choose Expires in 24 months



17. Click **Add** and then your will need to make a copy of the generated **secret key** because it will not be available later
18. Now that you have the **Tenant ID,** the **Client ID** and the **Client Secret Key** you can go back in **MetaDefender Storage Security** and finish the OneDrive integration. Congratulations!



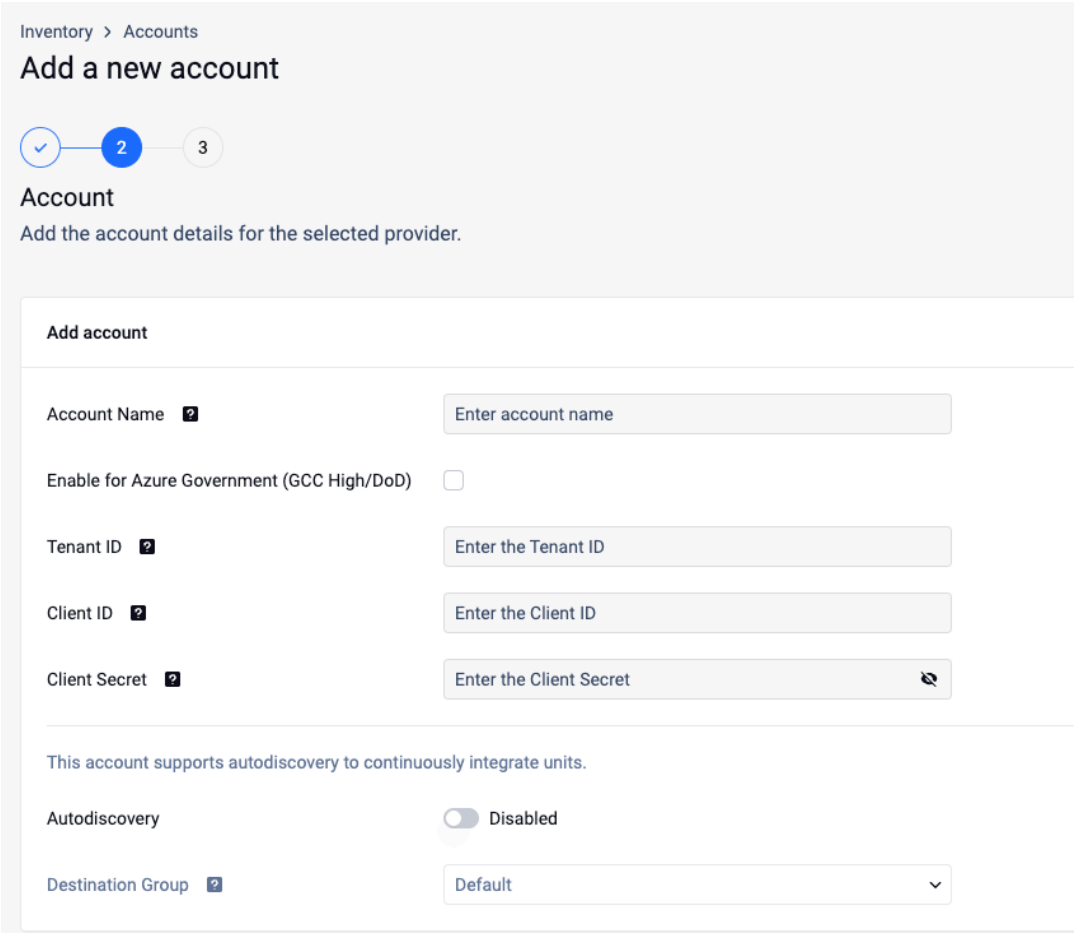
Add a SharePoint Online Storage

In order to integrate Microsoft SharePoint service with MetaDefender for Secure Storage you will be required to create an application registration, assign the necessary permissions and then generate a secret key. Please follow these steps:

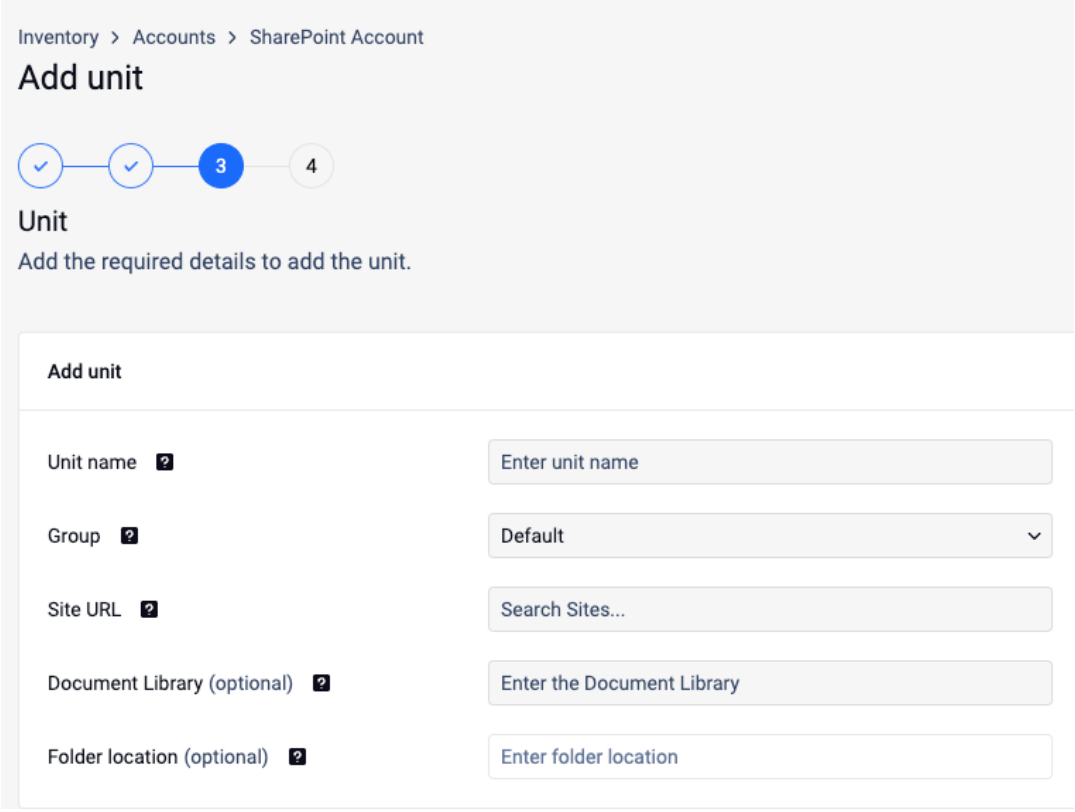
> **Info**
>
> Please note this page is **applicable only for SharePoint Online** and not applicable for SharePoint On Premise. For a guide to integrating a Sharepoint On-Premise deployment, consult this page: Add a SharePoint On-Premise Storage.

> **Info**
>
> When the upload process takes more than a few seconds, SharePoint creates a temporary file having the same name as your uploading file and the size of 0 bytes. By default, we will discover that file and show it into the list of discovered files. Once the upload is complete, we will discover the original uploaded file and process it accordingly. To skip the discovery of the temporary empty file created, please follow these instructions: How to handle empty objects in Discovery?

1. From the left side menu, navigate to **Inventory -> Add account -> Choose SharePoint**



2. Give your account a name so you can easily identify it later
3. Check **Enable for Azure Government (GCC High/DoD)** only if your organization uses Microsoft 365 GCC High or DoD environments. Leave unchecked for commercial or standard GCC environments.
4. Enter your **Tenant ID**. Scroll to the end of this page for more details.
5. Enter your **Client ID.** Scroll to the end of this page for more details.
6. Enter your **Client Secret.** Scroll to the end of this page for more details.
7. Click Next, finish adding the account and then add a new unit to this account

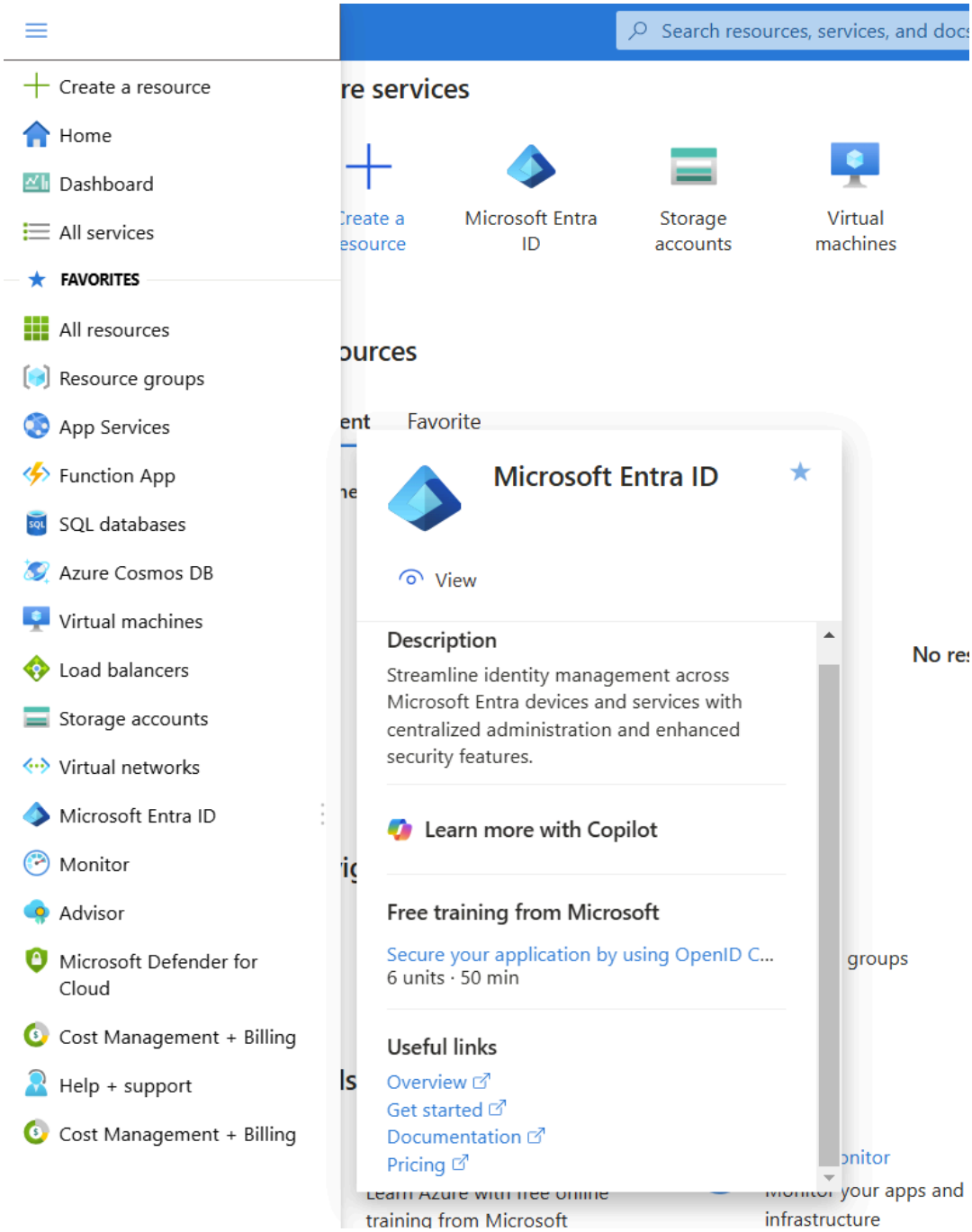


8. Give your unit an unique name
9. Assign your unit to a Group
10. Enter the **URL of a site** you wish to process files and folders.
11. Enter the **name of a Document Library** from the Site URL if you wish to process files and folders from a specific Document Library. This is optional. In case is not provided, we will process the files and folders from all the **Public Document Libraries** (we do not scan the private ones) that belong to the Site provided at step 10.
12. Enter the **name of a Folder** if you wish to process files and folders only from a specific folder, inside a specific Document Library. To be able to add a folder location, you need to provide a Document Library (11).
13. Select **Continue** in order to finish the process. If the data you entered is valid, a new SharePoint storage will be created. If is not valid, a specific error message will inform you.

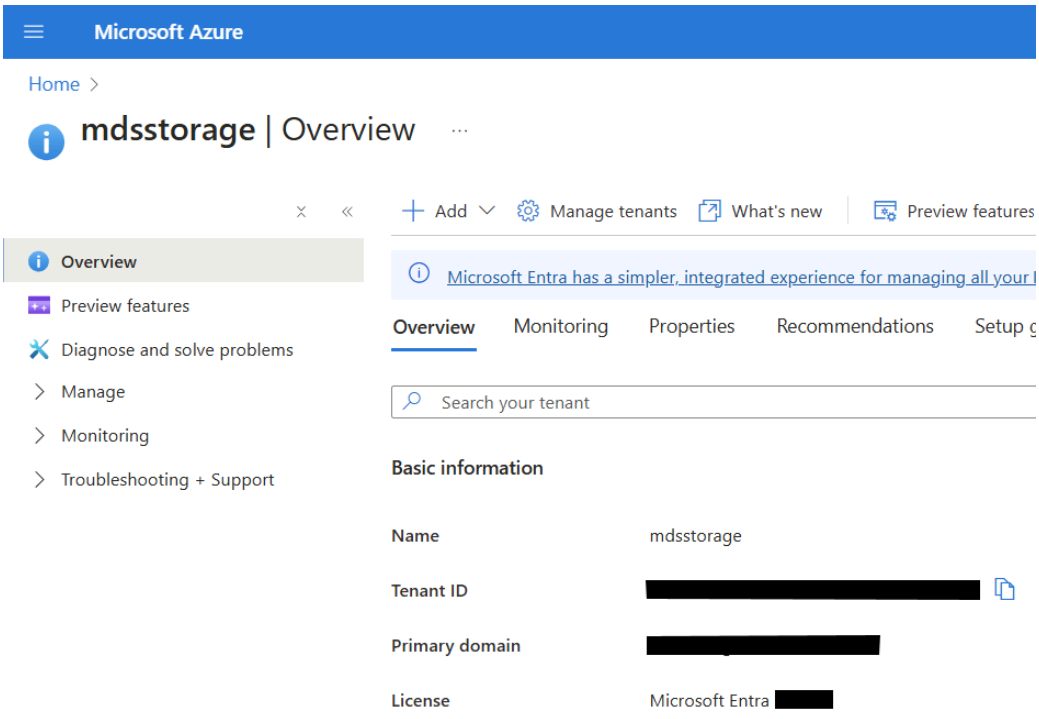
How to create a SharePoint application

In order to process our SharePoint files and folders with MetaDefender for Secure Storage you will be required to add a new app registration in your Microsoft Entra ID Azure Portal

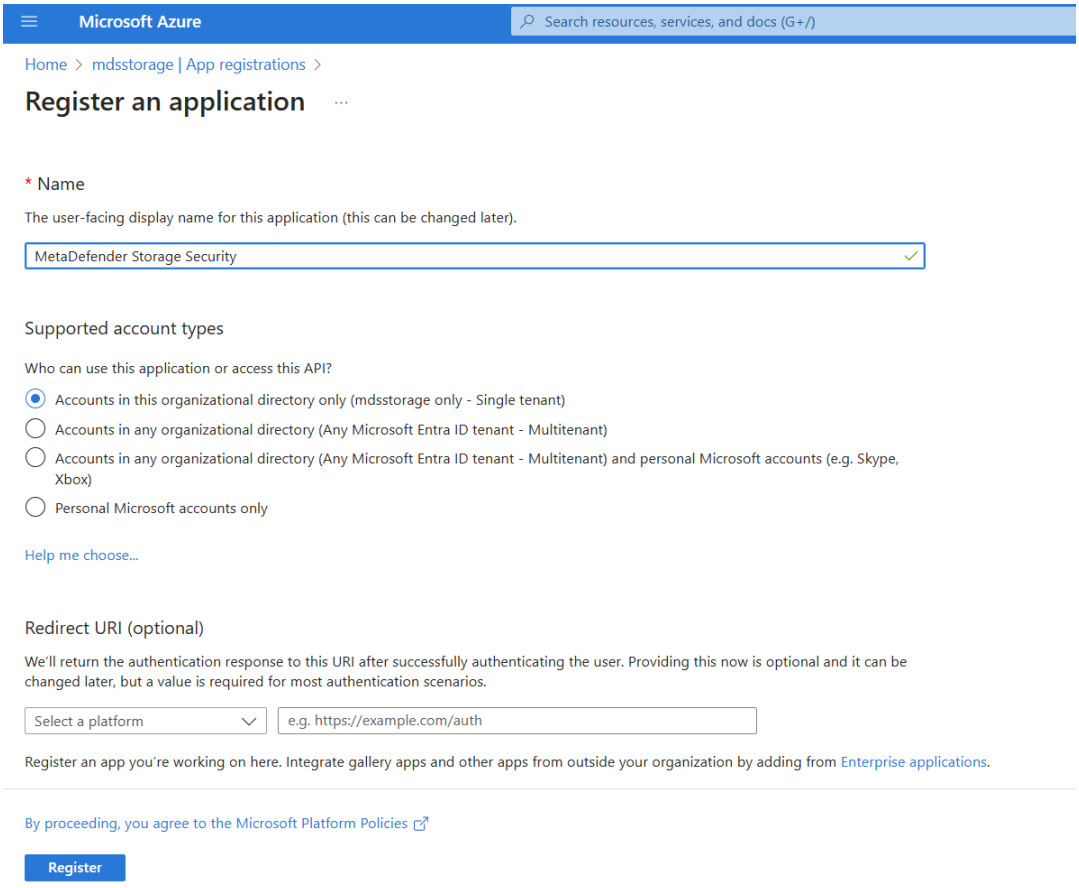
1. Log in to Azure Portal and from the left navigation menu choose **Microsoft Entra ID**


Search resources, services, and docs
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
App Services
Function App
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Microsoft Entra ID
Monitor
Advisor
Microsoft Defender for Cloud
Cost Management + Billing
Help + support
Cost Management + Billing
re services
Create a resource
Microsoft Entra ID
Storage accounts
Virtual machines
ources
ent
Favorite
Microsoft Entra ID
View
Description
Streamline identity management across Microsoft Entra devices and services with centralized administration and enhanced security features.
Learn more with Copilot
Free training from Microsoft
Secure your application by using OpenID C...
6 units · 50 min
Useful links
Overview
Get started
Documentation
Pricing
No res
groups
onitor
your apps and infrastructure
training from Microsoft

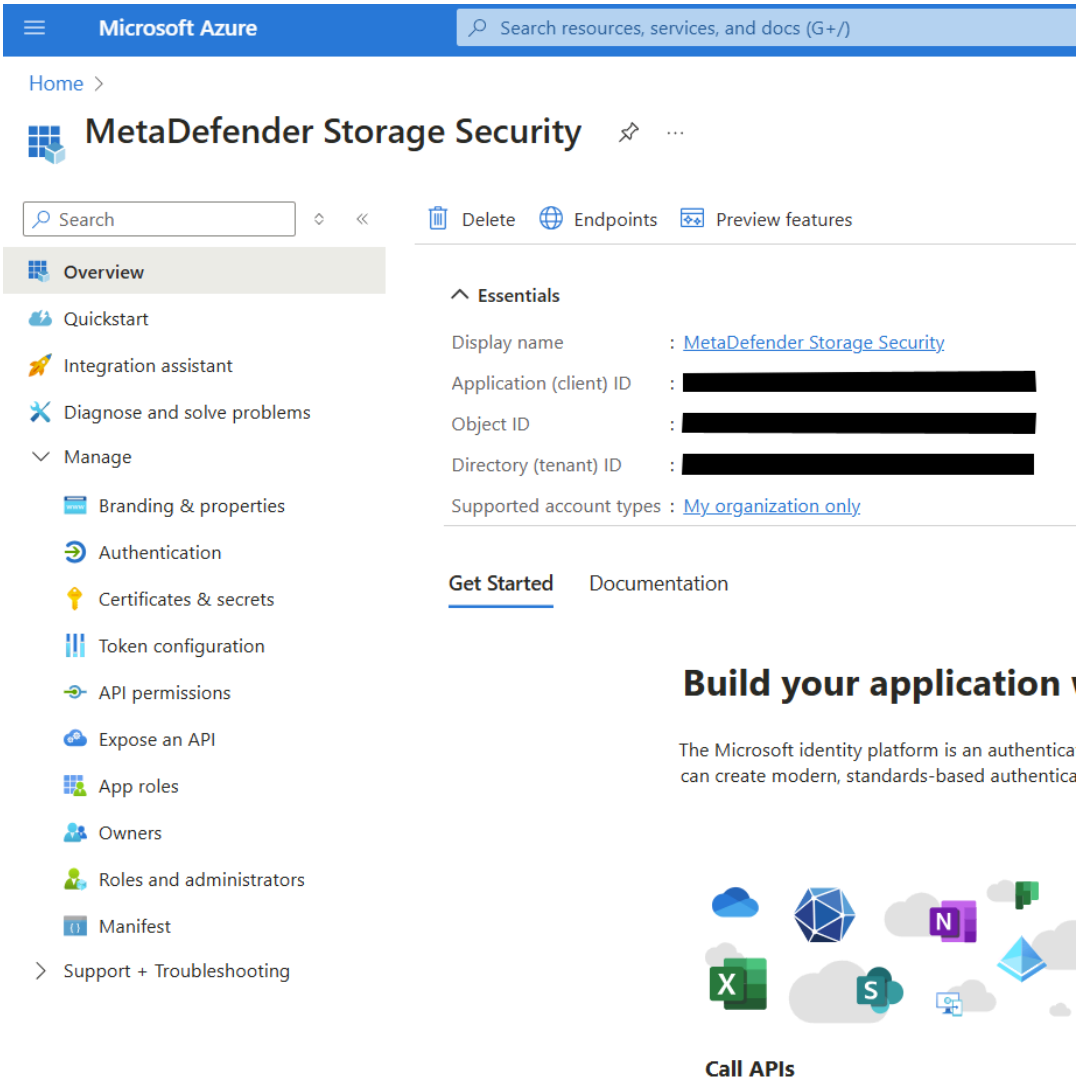
2. Make a copy of the **Tenant ID** from the overview page



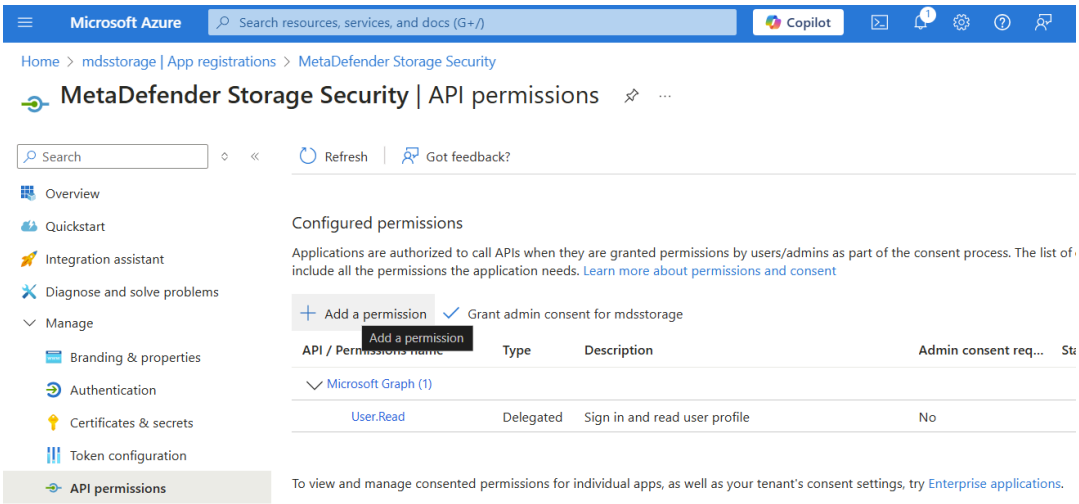
3. From the left side menu choose **App registrations**
4. Click **New registration**
5. Give your app a name so you can easily identify it



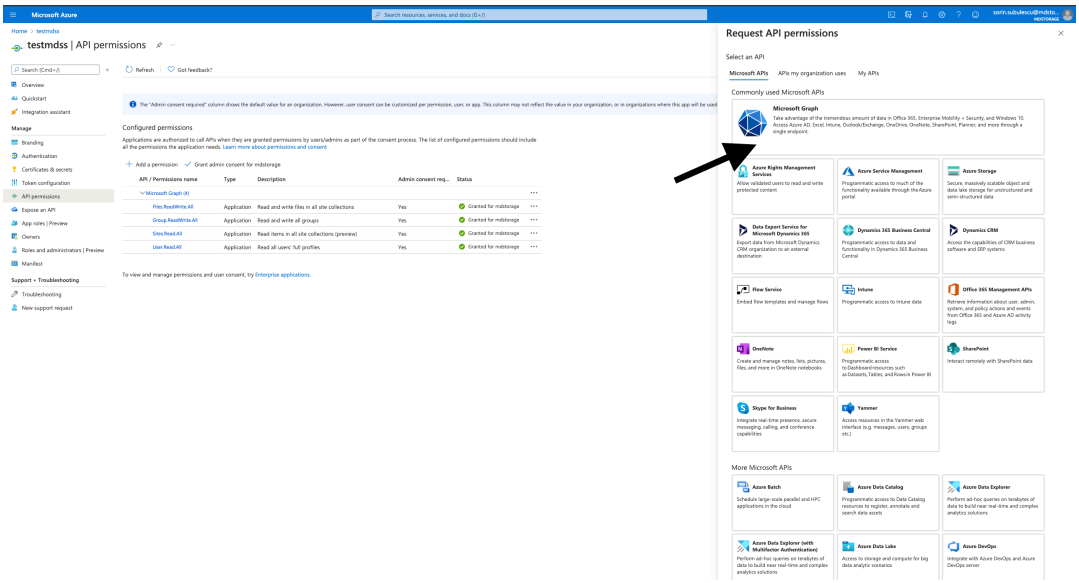
6. There is no need to modify the other properties. When ready, please click **Register**
7. From the **Overview** page of your newly created application, make a copy of **Application (client) ID **



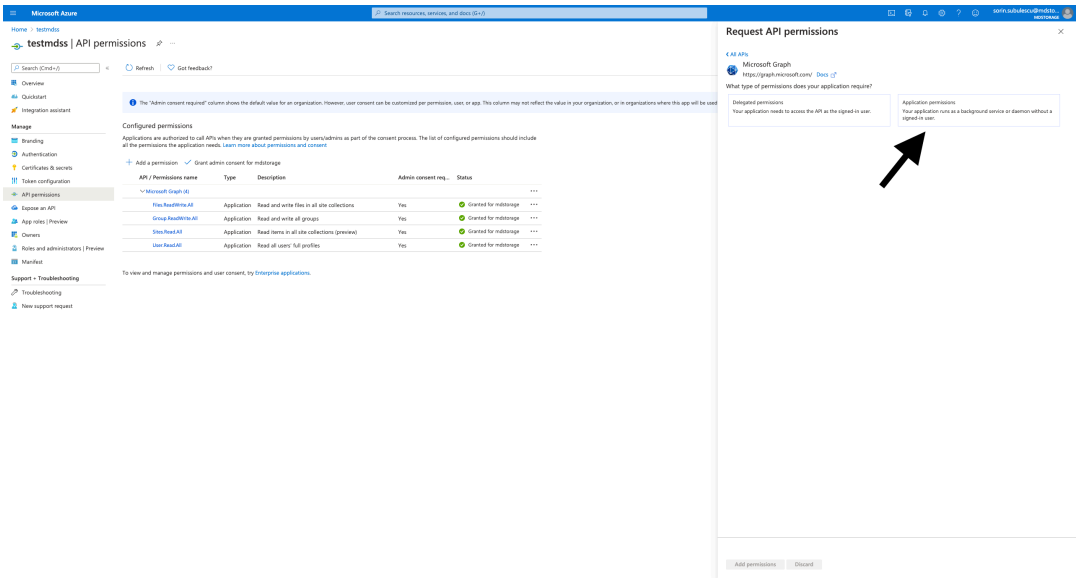
8. You now need to specify which permissions should the application have. To do this, please navigate to **API permissions** from the left-side menu
9. Click **Add a permission **



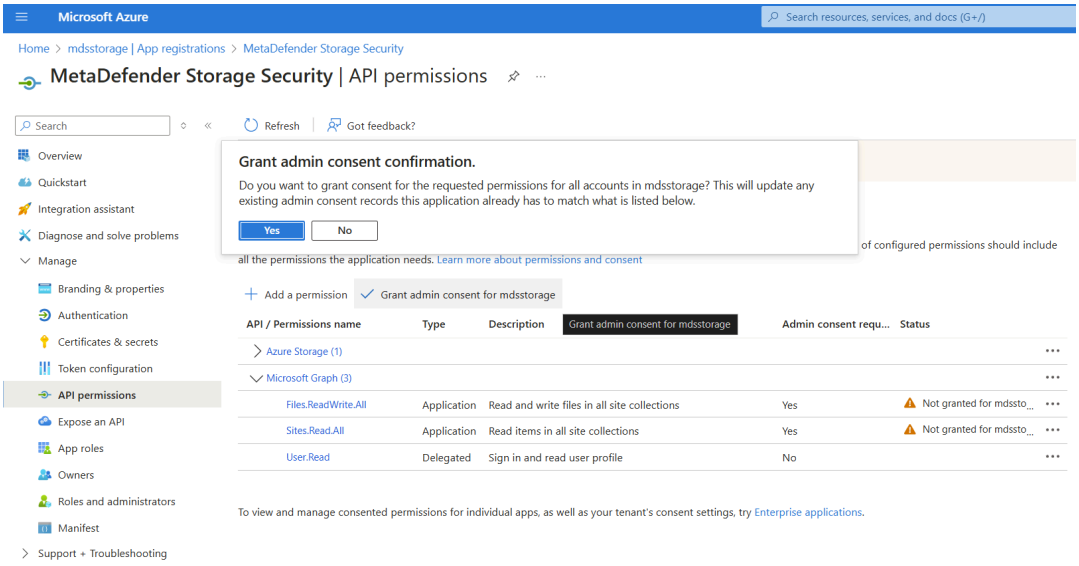
10. Select **Microsoft Graph** from the right-side menu



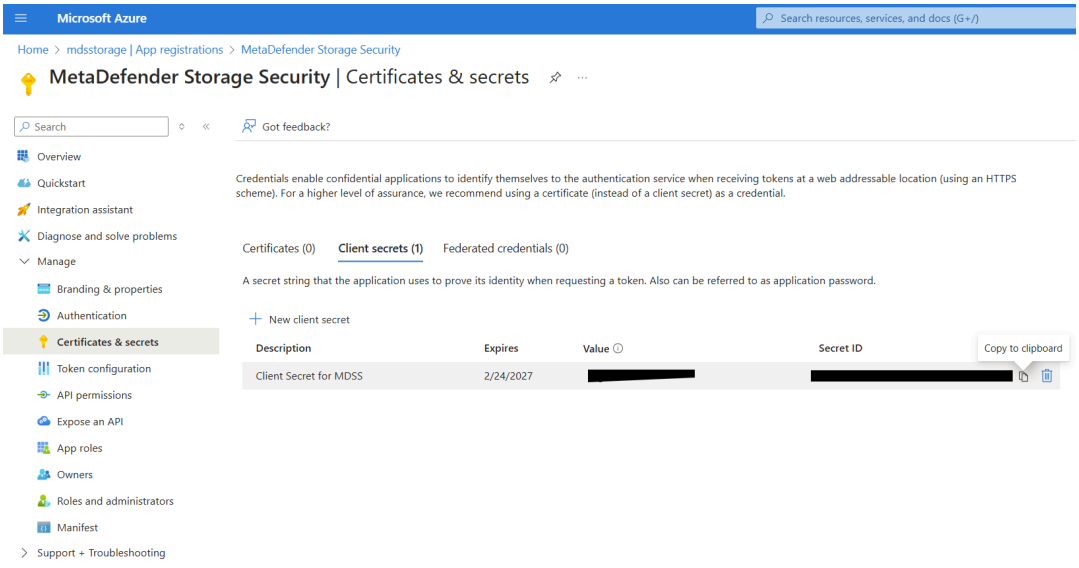
11. Select **Application permissions **



12. In order for MetaDefender Storage Security to correctly work please add the following permissions:
    1. Files.ReadWrite.All
    2. Sites.Read.All
13. When ready, click **Add permissions**
14. We need to grant admin consent for the added permissions



15. Now that the required permissions are in place, you are ready for the final step. Please navigate to **Certificates & secrets** from the left-side menu
16. Click **New client secret** and make sure that it **will not expire** as long as MetaDefender Storage Security is using it
17. Click **Add** and then you will need to make a copy of the generated **secret key** because it will not be available later



18. Now that you have the **Tenant ID,** the **Client ID** and the **Client Secret Key** you can go back in **MetaDefender Storage Security** and finish the SharePoint integration. Congratulations!

How to Enable Autodiscovery

This guide provides step-by-step instructions for enabling Autodiscovery for SharePoint Online in MetaDefender Storage Security.

Autodiscovery automatically detects and adds SharePoint Online sites as storage units, saving time and reducing configuration errors.

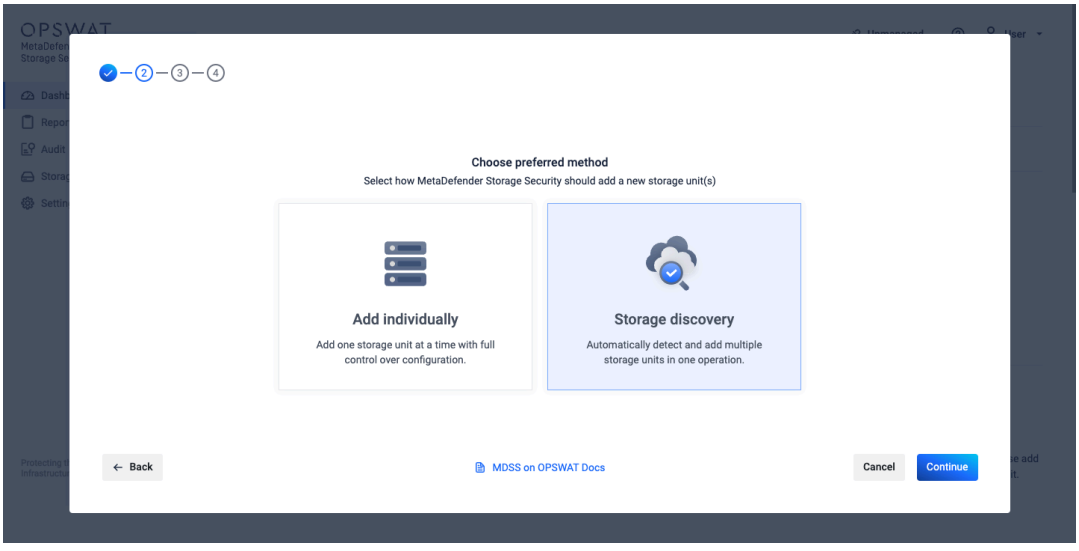
Prerequisites

Before enabling Autodiscovery, ensure you have:

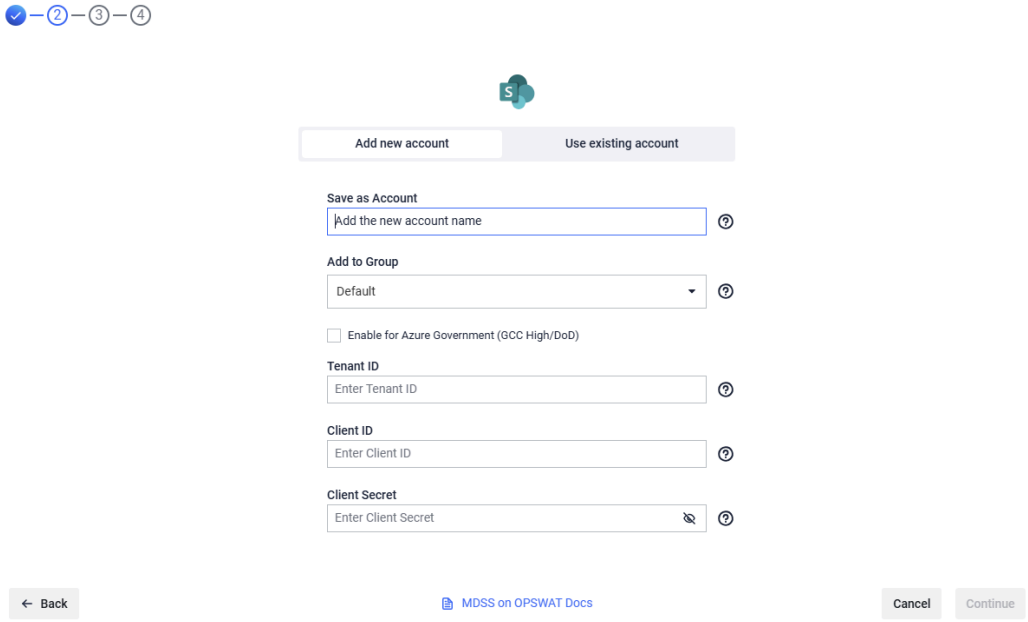
1. Valid SharePoint Online credentials with sufficient permissions
2. Permissions as stated in Add a SharePoint Online Storage

Method 1: Enable Autodiscovery During Storage Unit Addition

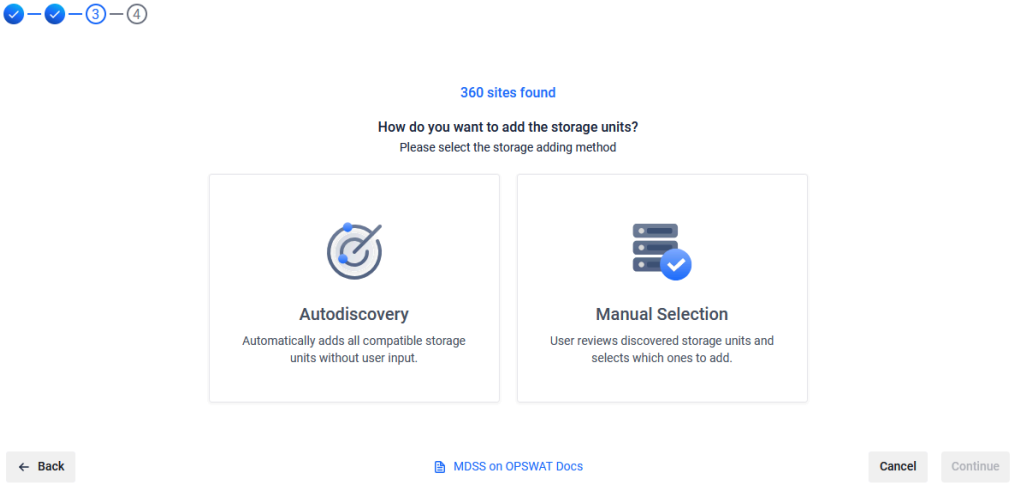
- Navigate to **Storage Units** page
- Click **Add Storage Unit** button
- Select **SharePoint Online** Storage Type
- Select **Storage Discovery** and click **Continue**



- Fill out the form with valid SharePoint Online credentials and click **Continue**



- In the next step, select your integration method. You have two choices: Autodiscovery and Manual Selection.
  - **Autodiscovery** for convenience, this option automatically adds all the sites MDSS finds
  - **Manual Selection** for precise control, this option lets users choose specific sites from the discovered list to integrate.

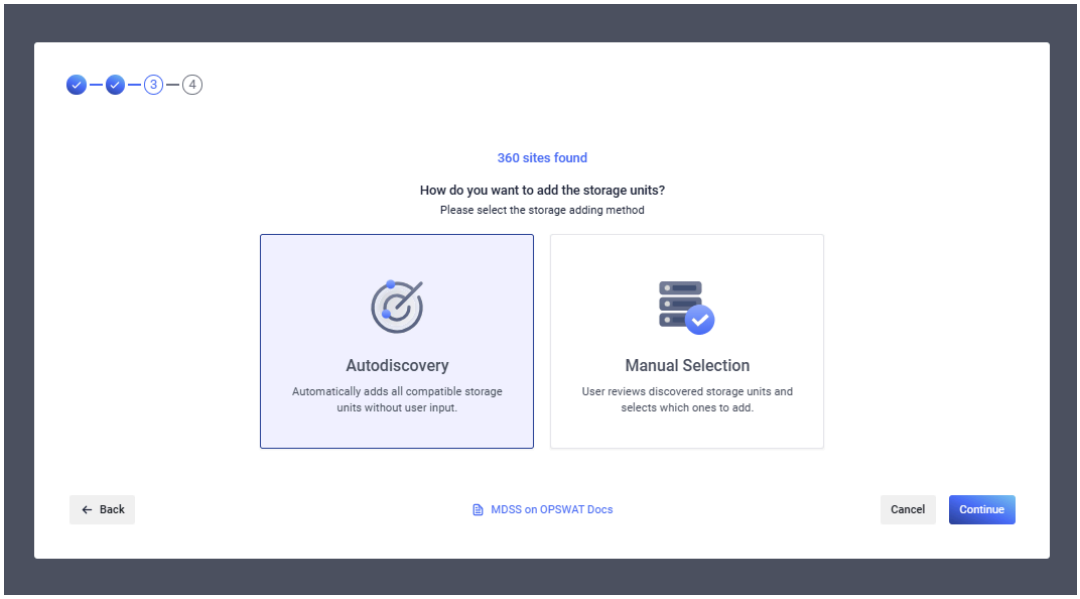


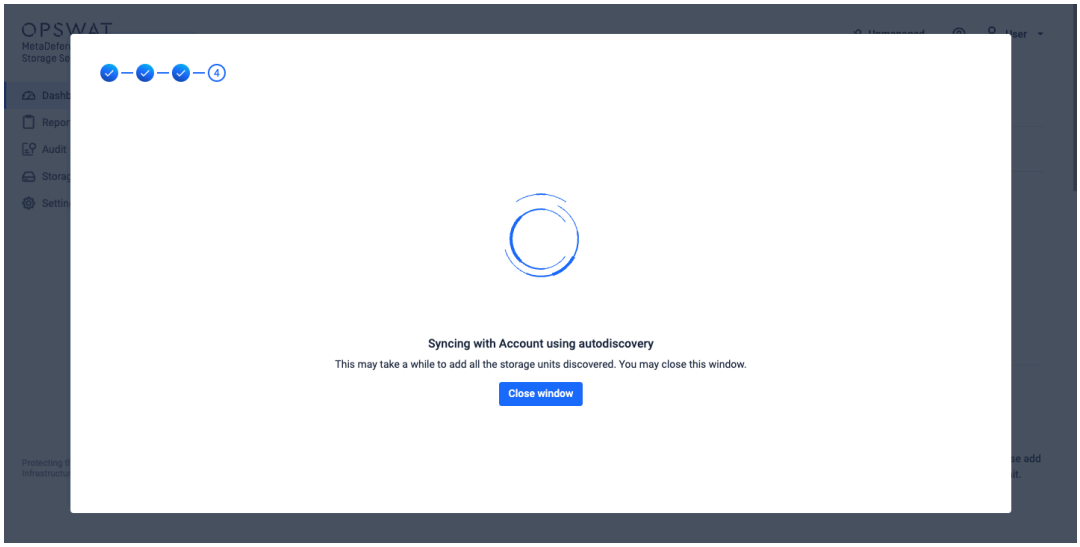
To learn more about each integration type, please consult the Autodiscovery documentation.

NO SITES FOUND

> If there were no sites found, you will be presented with a third option - **Add Individually** - which will reveal the credentials form to manually add the storage by using the site name.

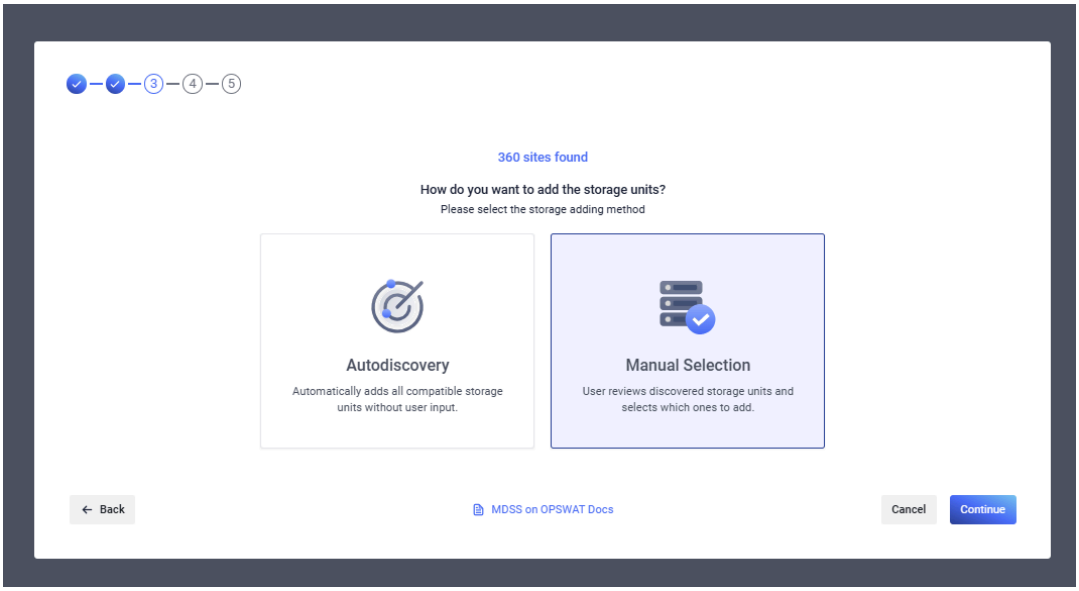
- If selecting **Autodiscovery** option:
  - Click **Continue** and an informative message will be displayed that the autodiscovery process has started in the background. You can safely close the modal and the storages will be added in background to the Storage Units page

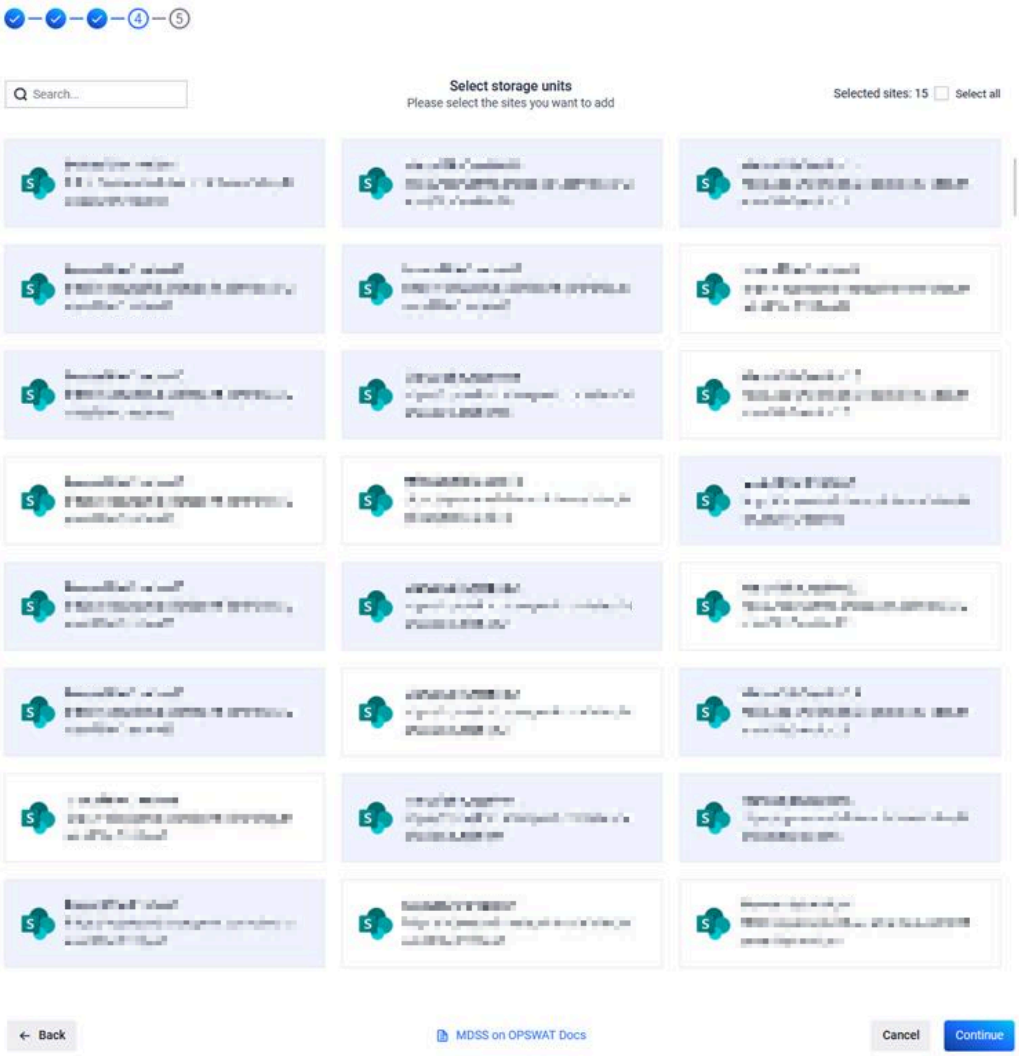


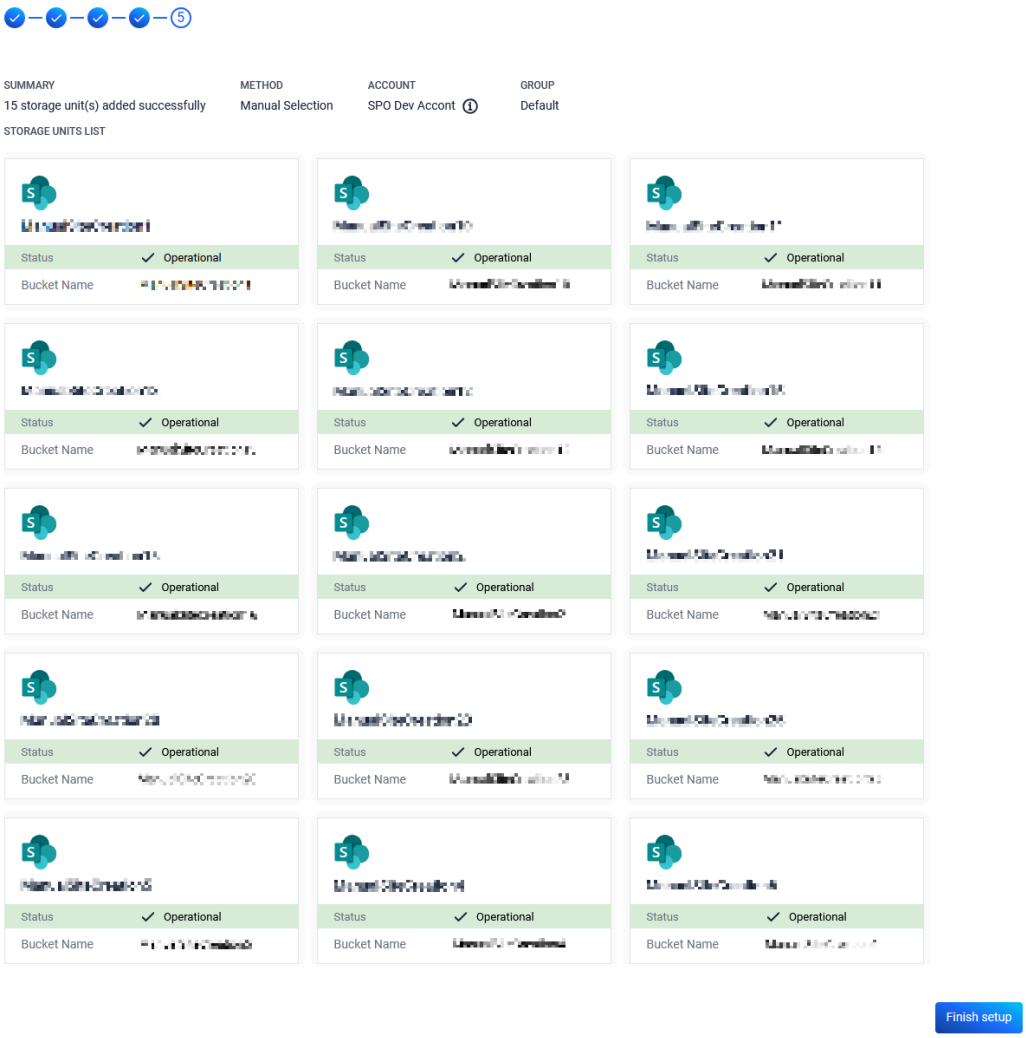


- If selecting **Manual Selection** option:
  - Click **Continue**
  - Select the sites you want to add from the discovered list
  - Click **Continue**

- The system will show a syncing message indicating sites are being added; You can choose to stay on this page in order to see the storages that were successfully added and also to see if there were any errors while trying to add specific storages.




Search...
Select storage units
Please select the sites you want to add
Selected sites: 15
Select all
Back
MDSS on OPSWAT Docs
Cancel
Continue

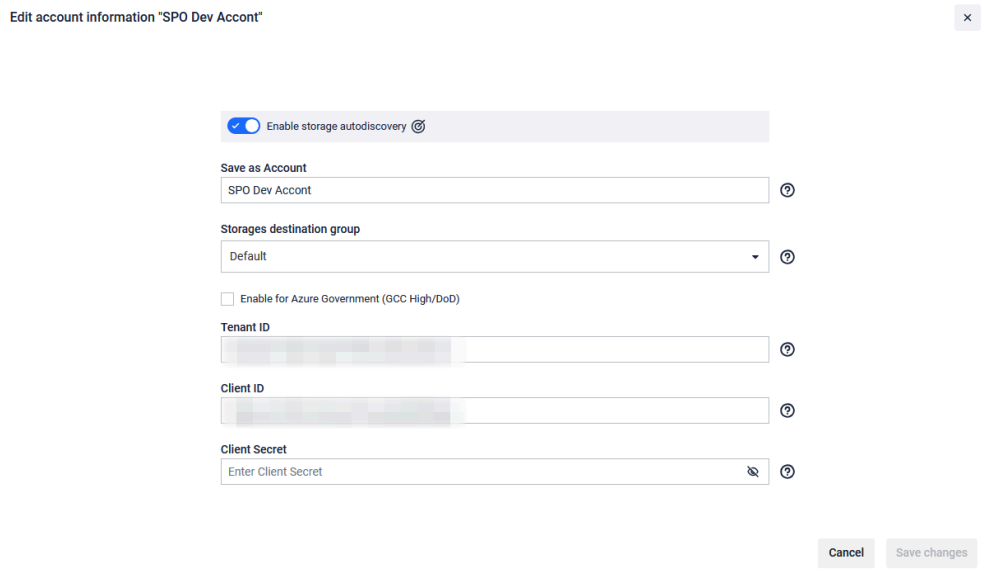


> **ERROR ADDING A STORAGE THAT WAS SELECTED DURING MANUAL SELECTION**
>
> In case there was an error while trying to add your storage, you will see the error message in the Storage card while hovering over the (i) icon.

Method 2: Enable Autodiscovery for an Existing Account

- Navigate to **Storage Units** page
- Identify a storage that's using the account you want to start autodiscovery for
- Click on the 3-dots button from the storage's card and select **Manage Storage Unit**
- From the top toggle, select **Change account info**

- Turn on autodiscovery by toggling the **Enable storage auto discovery** switch



Add a Microsoft Teams Storage

MetaDefender Storage Security supports scanning files shared through **Microsoft Teams** by integrating with the underlying Microsoft storage services used by Teams: **OneDrive** and **SharePoint**.

How Teams Stores Files

Teams Chat (1:1 and Group Chats → OneDrive)

When a user sends a file in a Teams chat, the file is uploaded to the sender's OneDrive

These files are stored in a folder named **Microsoft Teams Chat Files**

- Only files sent by that user appear in their OneDrive folder
- Other chat participants see read-only references to the file, but the actual file remains in the sender's OneDrive

Teams Channels (Channels → SharePoint)

- Files sent in a Teams channel are stored in the team's SharePoint site
- They appear under the Documents library, inside a folder named after the channel

Integrating OneDrive

In order to add a OneDrive storage in MetaDefender Storage Security, follow the documentation.

Recommended Configuration for Teams Chat

For scanning files sent in Teams chats, we recommend adding the user and the folder location **Microsoft Teams Chat Files.**

This configuration ensures that only files sent by that user in Teams chats are scanned.

Integrating SharePoint

In order to add a **SharePoint** storage in MetaDefender Storage Security, follow the documentation.

Recommended Configuration for Teams Channels

For scanning files shared in Teams channels, we recommend integrating with the **channel folder** inside the SharePoint site's *Documents* library

This configuration ensures that only files shared in the selected Teams channel are scanned.

Scanning with Deep CDR

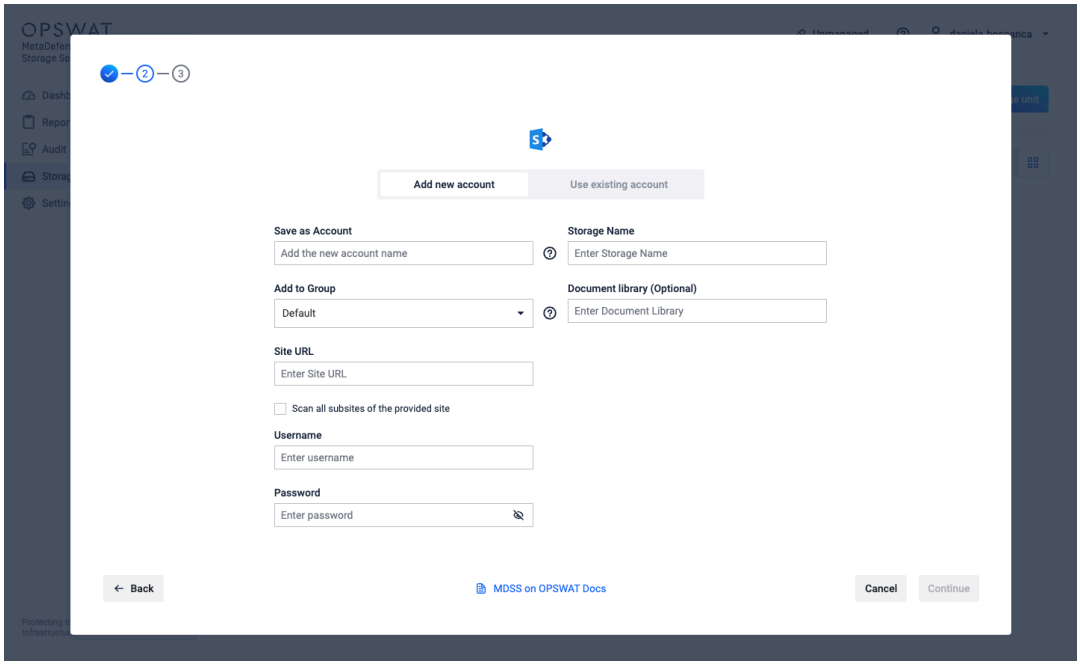
When using Deep CDR, the sanitized file will not be accessible in Teams by default.

To ensure Teams users can access the sanitized file, you must enable the **"Replace Original File"** feature, following the documentation.

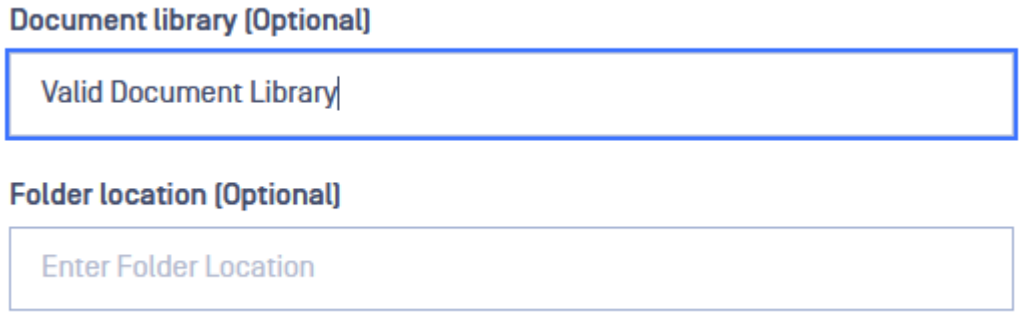
This replaces the original Teams file with the sanitized version, meaning Teams users will always access the sanitized file in their chat or channel.

Add a SharePoint On-Premise Storage

> **Info**
>
> Please note this page is **applicable only for SharePoint On-Premise** and not applicable for SharePoint Online. For a guide to integrating a Sharepoint Online deployment, consult this page Add a SharePoint Online Storage. Moreover, the SharePoint On-Premise integration is available **only on Windows MetaDefender Storage Security Deployments.**



1. Give your storage a name so you can easily identify it later.
2. Enter the **Site URL** associated with the Site you want to integrate from you Sharepoint Server.
3. Enter the **domain** and **username** of the user you want to log in as. This should be in the form **DOMAIN/USERNAME.** The user must have at least **Contribute** permissions on the site.
4. Enter the **password** associated with the user account you are logging in as.
5. Optionally, enter the name of a **Document Library** from the site URL. If this field contains a valid value, then only the files from this specific document library will be processed. If no value is entered here, files from all public document libraries belonging to the site will be processed.
6. If the **Document Library** field has a value, the **Folder Location** field will appear. Optionally, you can enter the name of a **Folder** that is part of the input document library. If this field contains a valid value, then only the files from this folder inside the document library will be processed.



7. The **Scan all subsites of the provided site** checkbox enables you to optionally explore the entire subsite hierarchy of the integrated site, allowing for the processing of files from all document libraries within the subsites. This option is applicable only when a **Site URL** is entered without specifying a **Document Library**. If you do select one, the integration will be restricted to that particular library within the site.

> **Warning**
>
> Known Limitation: there is a heavy limitation in regards to the number of concurrent requests a user can make to the SharePoint Server. Thus, when doing remediation actions with a large number of files, the heavy throttling will cause the operations to have to wait for the SharePoint Server to free up resources and will result in a considerably long scanning time. For more information, you can access this article:
>
> To customize the values used in the error handling and retry mechanism to better suit your deployment, please visit this page for more information.

Configuring Error Handling and Retry Mechanisms for SharePoint On-Premise

This guide is for administrators and users managing the MetaDefender Storage Security integration with SharePoint On-Prem. It details crucial environment variables that control error handling, request retries, connection management, and batch processing. Properly tuning these settings is essential for maximizing your deployment's performance and reliability. Fine-tuning helps prevent SharePoint server throttling, which can occur under heavy load, ensuring smoother operations and minimizing disruptions.

Key Configuration Settings (Environment Variables)

Below are the environment variables you can configure to optimize communication with your SharePoint On-Prem server.

SHAREPOINT_ON_PREM_MAX_CONNECTIONS sets the maximum number of simultaneous connections to SharePoint On-Prem that can be held in the connection pool. Requests

exceeding this limit will wait for an existing connection to become available.

Impact

- Higher Value
  - Can lead to faster processing of requests to the same site and better performance during high-demand periods by allowing more concurrent operations.
  - Increases the risk of hitting the SharePoint server's own simultaneous connection limits, potentially causing throttling, slower responses, and service disruptions.
- Lower Value
  - Enhances connection reusability, leading to more reliable and stable request management.
  - May reduce processing speed, as fewer simultaneous connections can lead to longer wait times for requests, especially during peak usage.
- Default is set to 5 maximum connections for every pool
- Units measured in number of connections

SHAREPOINT*ON* PREM_MAX_QUERY_RETRIES controls how many times a failed SharePoint On-Prem query will be automatically retried. Retries use an exponential backoff strategy (increasing delays between attempts) to avoid overwhelming a struggling server

Impact

- Higher Value
  - Increases the chance of a query succeeding during temporary server issues.
  - Can lead to longer overall operation times if failures are frequent or persistent.
- Lower Value
  - Reduces time spent retrying, leading to quicker finalization of operations (either success or failure)
  - May result in a higher rate of failed operations if transient issues are common, as the system gives up sooner.
- Default is set to 5 retries per query
- Configurable Range goes from 0 to 8 (MetaDefender Storage Security enforces a hard upper limit of 8 retries)
- Units measured in number of retries

SHAREPOINT_ON_PREM_CIRCUIT_BREAKER_THRESHOLD defines the number of consecutive connection failures to SharePoint that must occur before the circuit breaker "opens." Once open, connection attempts are temporarily halted to prevent overwhelming an unhealthy SharePoint server.

Impact

- Higher Value
  - Makes the system more tolerant of repeated transient issues before halting requests
  - Risks overwhelming an unhealthy SharePoint server for a longer duration, potentially worsening performance issues and recovery times.
- Lower Value
  - Reacts more quickly to potential SharePoint server issues, helping to prevent server overload and allowing for faster recovery.
  - May lead to more frequent (though temporary) interruptions in service if transient issues are common.
- Default is set to 5 consecutive failed requests
- Units measured in number of failures

SHAREPOINT_ON_PREM_CIRCUIT_BREAKER_DURATION_SECS specifies how long (in seconds) the circuit breaker remains open after tripping. During this "cooldown" period, all requests to SharePoint are automatically rejected. After the duration, the circuit enters a "half-open" state to test if the SharePoint server has recovered.

Impact

- Higher Value
  - Provides a longer recovery window for a significantly troubled SharePoint server before new connection attempts are made
  - Results in a longer period of unavailability for users trying to access SharePoint resources.
- Lower Value
  - Reduces downtime by attempting to reconnect to SharePoint sooner.
  - Risks repeatedly tripping the circuit breaker if the server hasn't fully recovered, potentially increasing load on an unstable server.
- Default is set to 30 seconds

SHAREPOINT_MAX_CONCURRENT_REQUESTS controls the maximum number of SharePoint requests that MetaDefender Storage Security will process simultaneously. This helps prevent overwhelming the SharePoint server.

Impact

- Higher Value
  - Allows more requests to be processed at once, potentially improving throughput and performance during high demand.
  - Increases the risk of overwhelming the SharePoint server, which can lead to throttling or degraded performance.

- Lower Value
  - Helps prevent server overload and ensures more stable performance, especially during peak usage.
  - May result in slower overall processing times and longer wait times for users, as requests are queued.
- Default is set to 5 concurrent requests
- Units: Number of concurrent requests

`SHAREPOINT_BATCH_SIZE` specifies the maximum number of SharePoint requests to be processed in a single batch operation. Batching optimizes performance by reducing round-trips but needs to be balanced against server resource capacity

Impact

- Higher Value
  - Can improve efficiency and performance by processing more requests in each interaction with SharePoint.
  - Larger batches consume more resources and increase the risk of overwhelming the SharePoint server, potentially leading to throttling.
- Lower Value
  - Helps maintain stability and prevent resource saturation on the SharePoint server.
  - May lead to increased overall processing times due to a higher number of smaller batch operations.
- Default is set to 10 requests per batch.

SHAREPOINT_BATCH_INTERVAL_MS defines the time interval in milliseconds between the processing of SharePoint request batches. This determines how frequently the system checks for and processes queued requests.

Impact

- Higher Value
  - Reduces the frequency of batch processing, which can lessen the load on the SharePoint server, especially during peak times.
  - May lead to increased wait times for users as requests are queued for longer before being processed.
- Lower Value
  - Improves responsiveness and user experience by processing queued requests more frequently.
  - Increases the load on the SharePoint server due to more frequent processing cycles, potentially leading to resource saturation or throttling if the interval is too short.

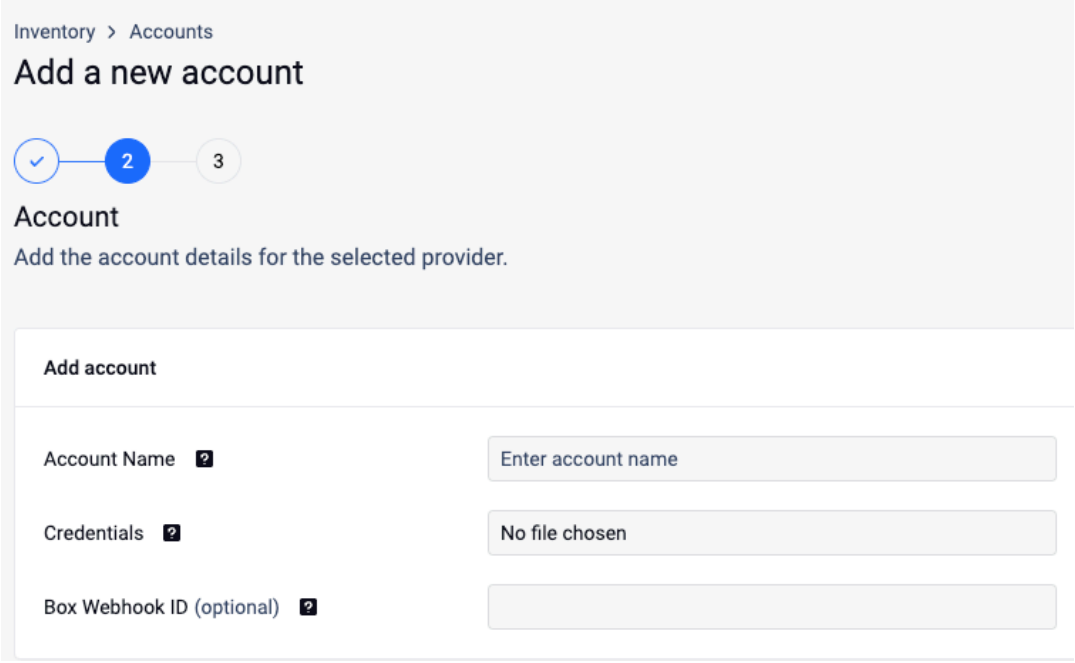
- Default is set to 1000 milliseconds (1 second)

Add a Box Storage

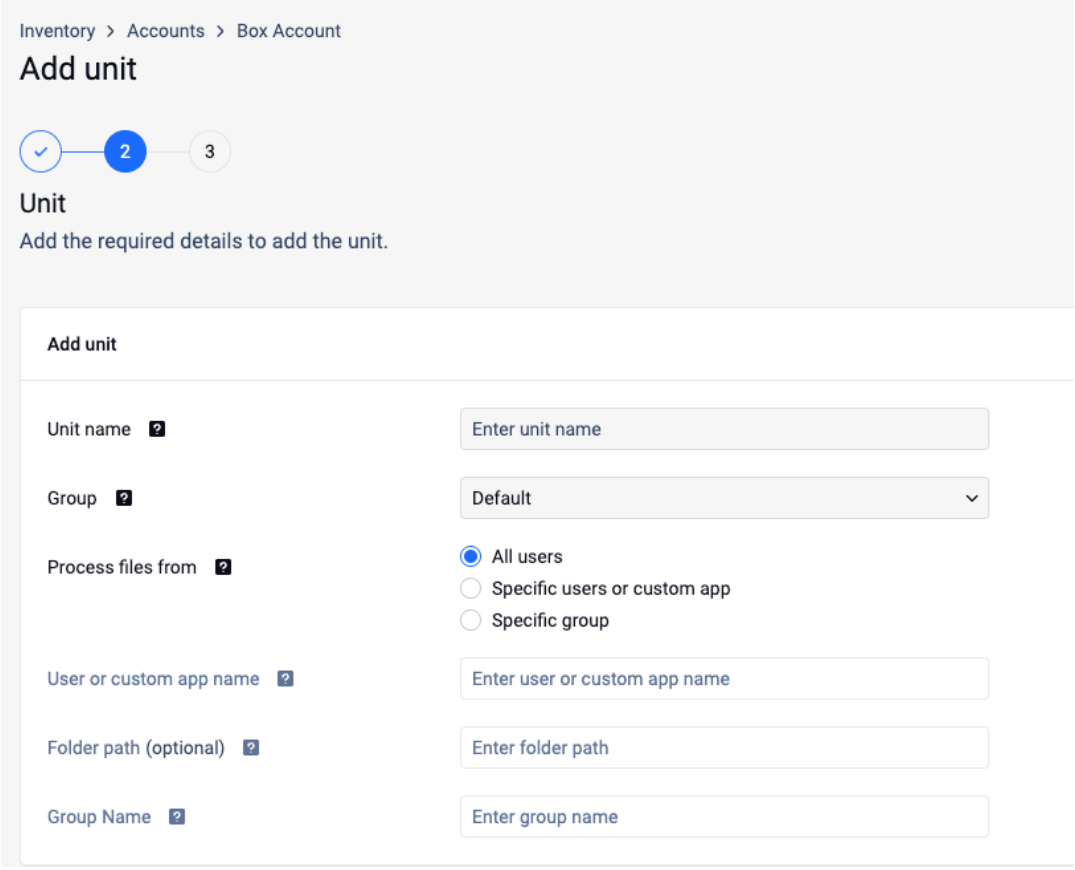
In order to integrate Box with MetaDefender Storage Security please follow these steps:

> **Info**
>
> Steps 4 and 5 are optional. Perform them in order to set up a specific location for file processing.

1. From the left side menu, navigate to **Inventory**, click on **Add unit** and choose **Box**



2. Give your account a name so you can easily identify it later
3. Upload your **Credentials** file. Scroll down for more details.
4. (Optional) Enter the Webhook ID, you can find more details in this page Event-based handling for Box
5. Click Next and after account is successfully created, please add a unit to it



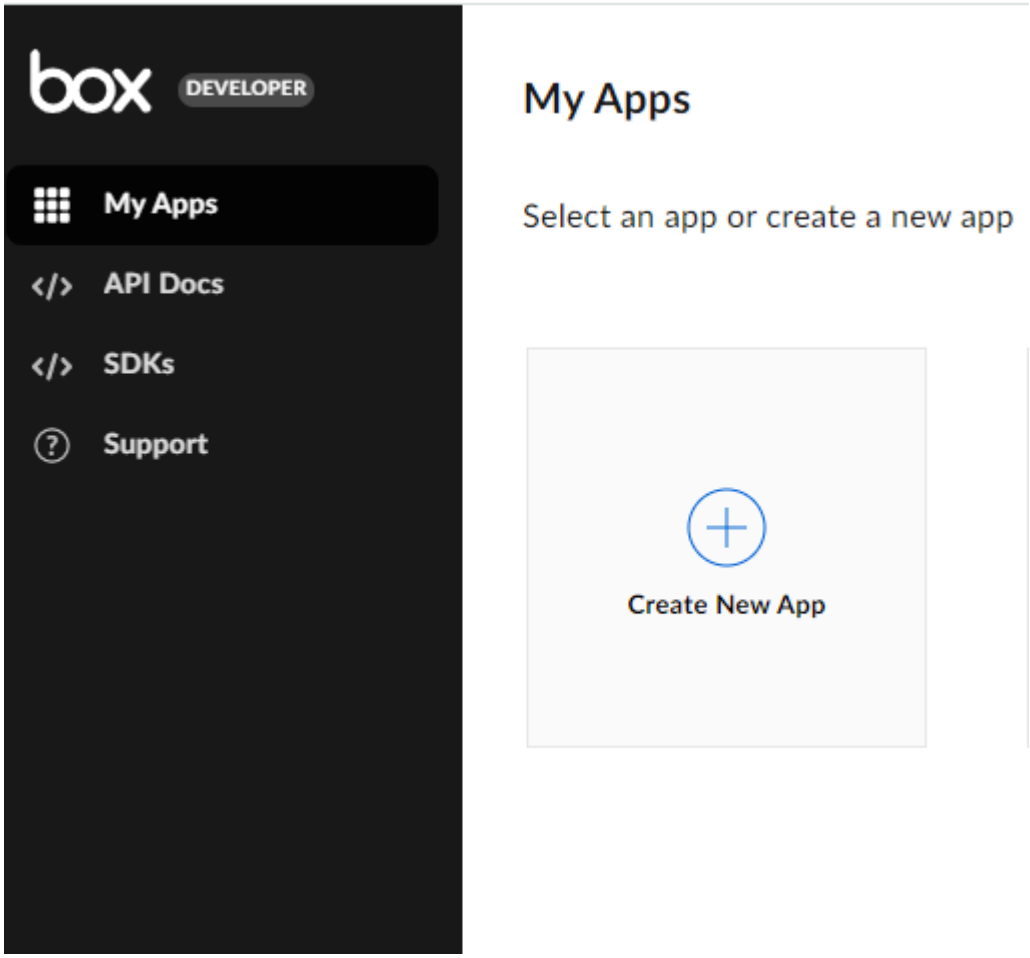
5. Enter an unique name for your unit.
6. Assign the unit to a Group.
7. Set up a specific location as a source of files that should be processed By MetaDefender Storage Security
    1. **All Users** - process files from all users created by the custom application, from the application itself and also from all the Enterprise users, depending on the Application Access provided
    2. **A specific user or custom app** - process only the files from a specific user/custom app. Additionally you can set up a location as a source of files, by filling in the full path of the folder. Make sure it's a valid path corresponding to the User or Custom App name you previously added. Note that it could take up to 10-15 minutes for newly added folders to be discovered.
    3. **A specific group***-* process only the files from a group of users
8. Select **Add** in order to finish the process.

> **Info**
>
> For most Box applications "All Files" is considered the root of the folder structure. To be able to scan entire structure of folders from a user or custom application, Folder Path field should remain empty.

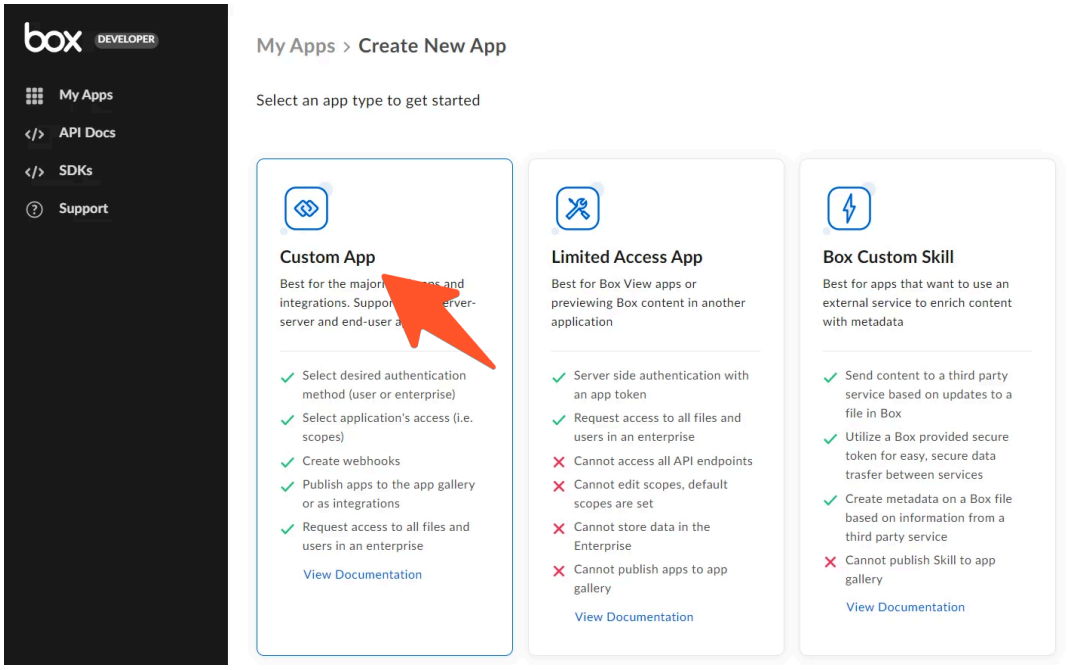
How can I generate a Public / Private key pair

To generate a file that contains all the necessary information to connect MetaDefender Storage Security to your Box storage please follow these steps:

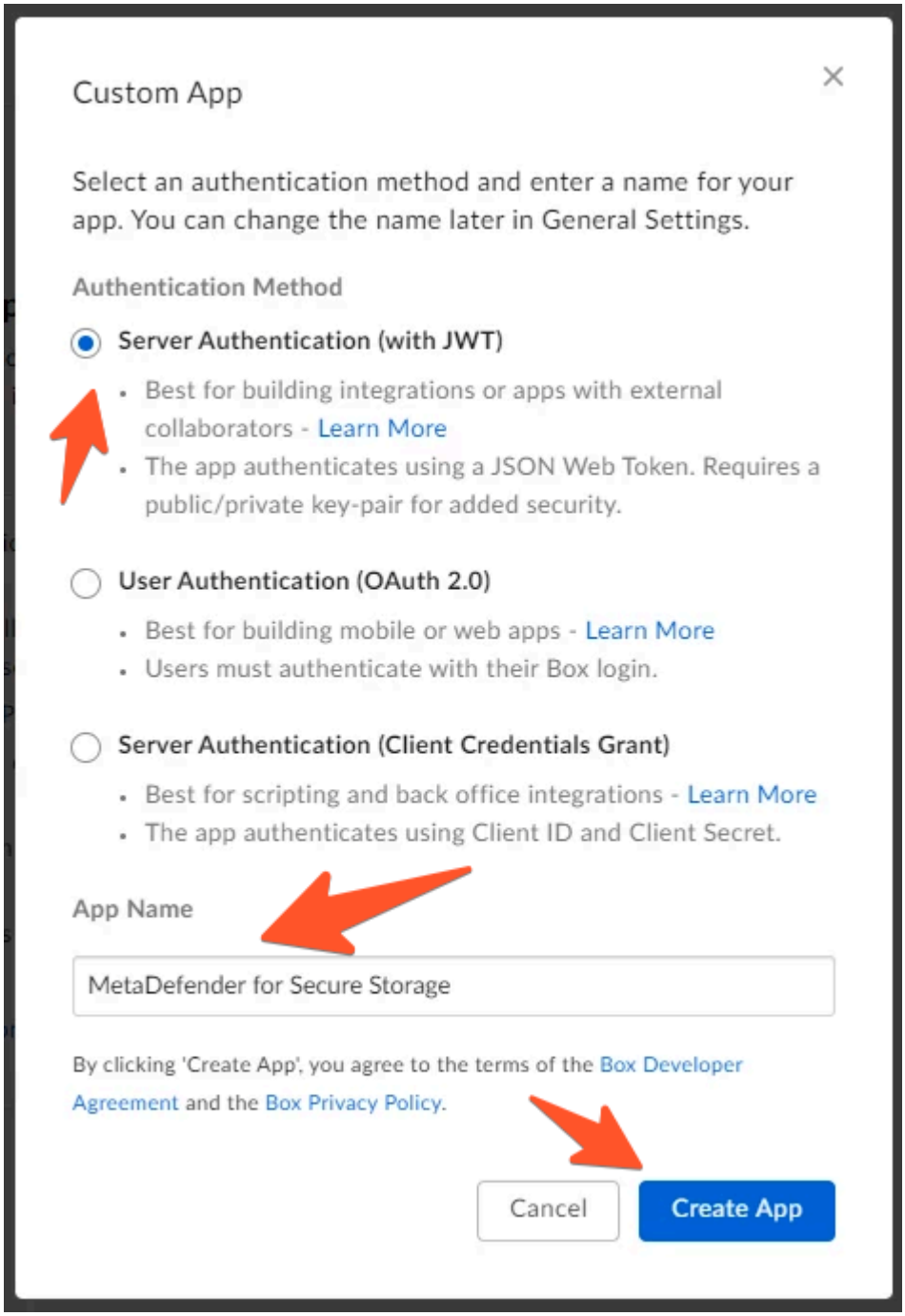
1. Log in to **Box** and then go to Dev Console
2. From the console, choose **Create New App**



3. Select **Custom App** and click **Next**

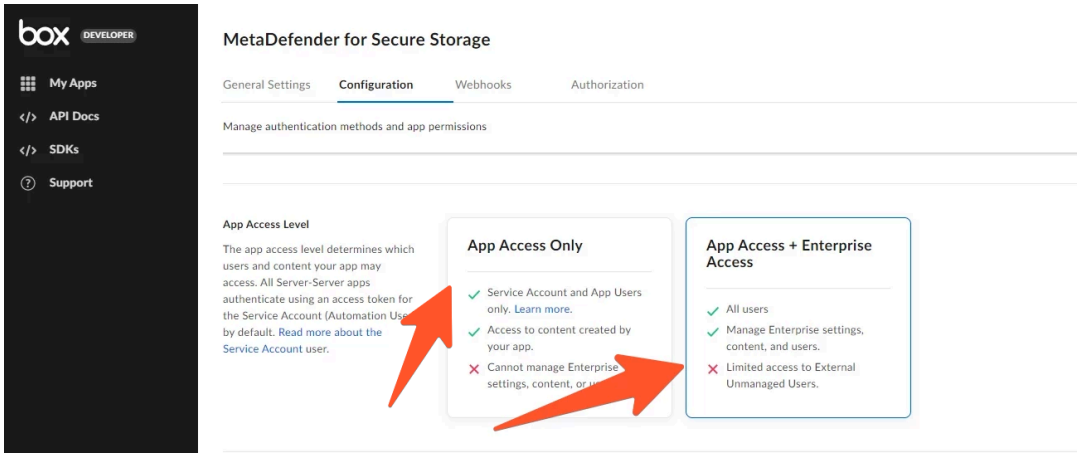


4. Choose **OAuth 2.0 with JWT (Server Authentication)** as the authentication method and give your app a name, for example **MetaDefender Storage Security** and then click **Create App**

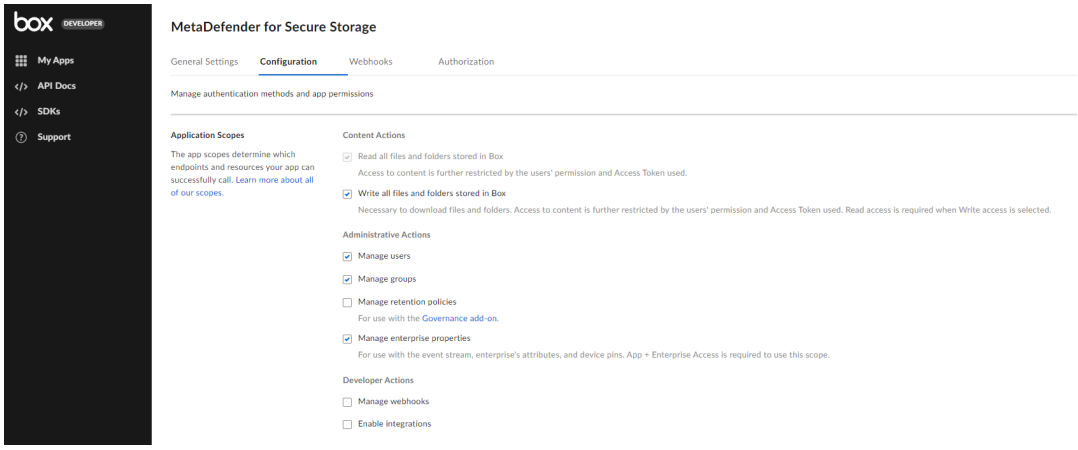


5. You will receive a message saying that your app has been successfully created. Click **View Your App**.
6. You will be redirected to the app **General Settings** page, switch to **Configuration**.
7. Scroll down to the **Application Access** section and choose **App Access Only** or **App Access + Enterprise Access**. Selecting **App Access only** will allow MetaDefender Storage Security to be able to process files from the users created by the custom application and also from the application itself. Selecting **App Access + Enterprise Access** will allow MetaDefender Storage Security to be able to process files from the

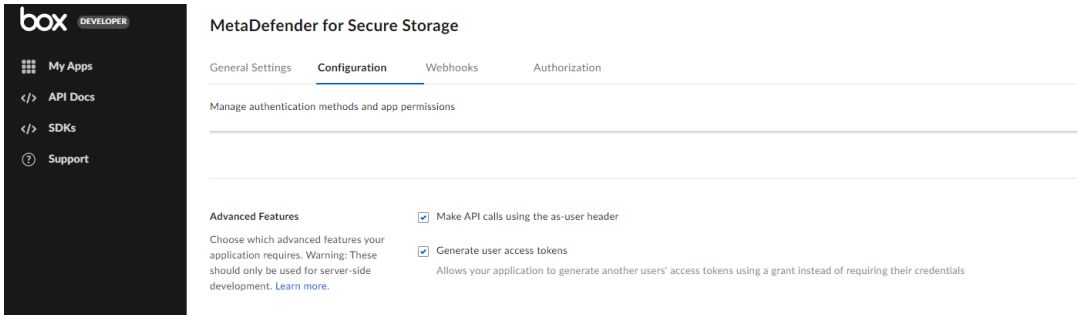
users created by the custom application, from the application itself and also from the Enterprise users.



8. Scroll down to the **Application Scopes** section and make sure that the following permissions are checked:
    1. Read all files and folders stored in Box
    2. Read and write all files and folders stored in Box
    3. Manage users
    4. Manage groups

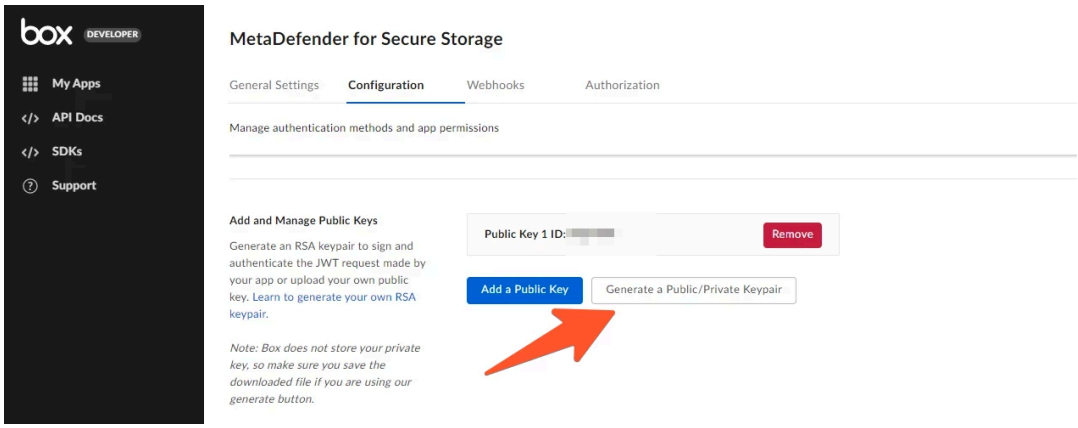


9. Next, please scroll down to the **Advanced Features** section and make sure that both **Perform Actions as Users** and **Generate Users Access Tokens** are enabled

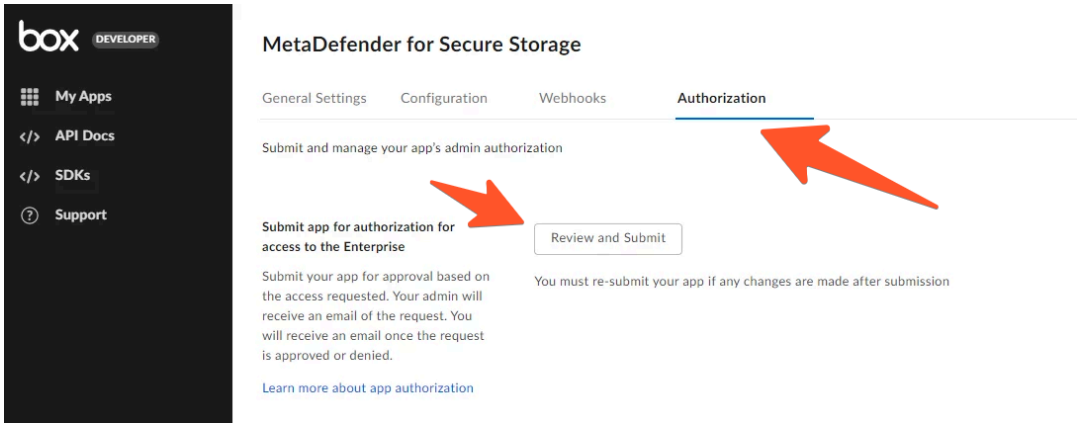


10. Make sure you **save your changes.**
11. The next step will be to generate a Public/Private Keypair

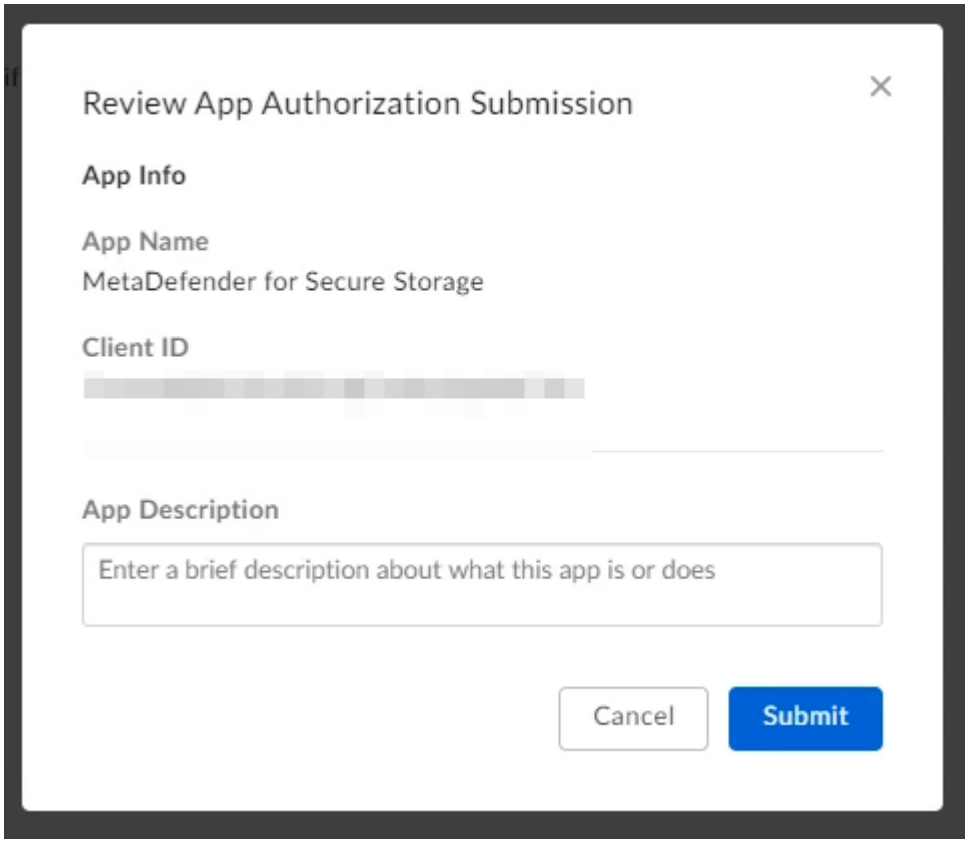
Note: When performing this action you may be required to re-authenticate using a two-factor authentication method. If this happens, after re-authenticating, please go back and click **Generate Public/Private Keypair** again



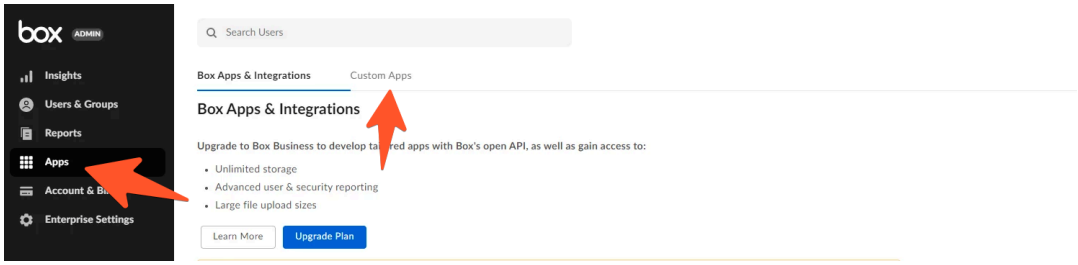
12. A configuration file with all of your app settings will be downloaded. Please store it securely as you will need it a bit later
13. Click to **Authorization** menu.



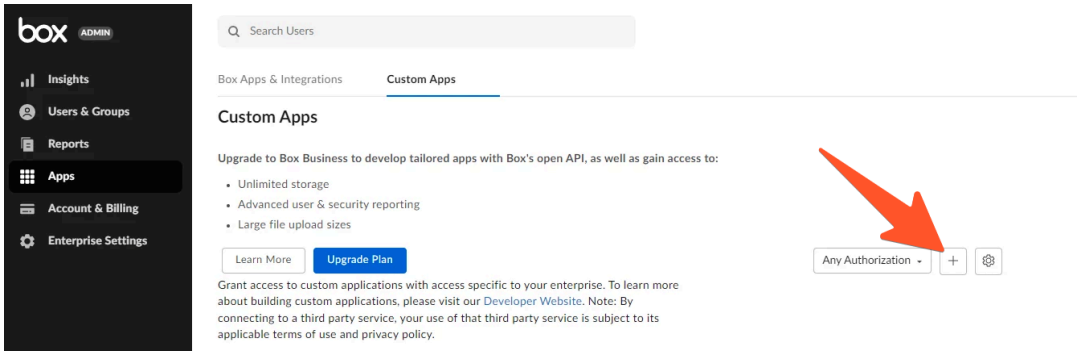
14. Click **Review and Submit**. From the popup that will appear, please make a copy of the **Client ID**

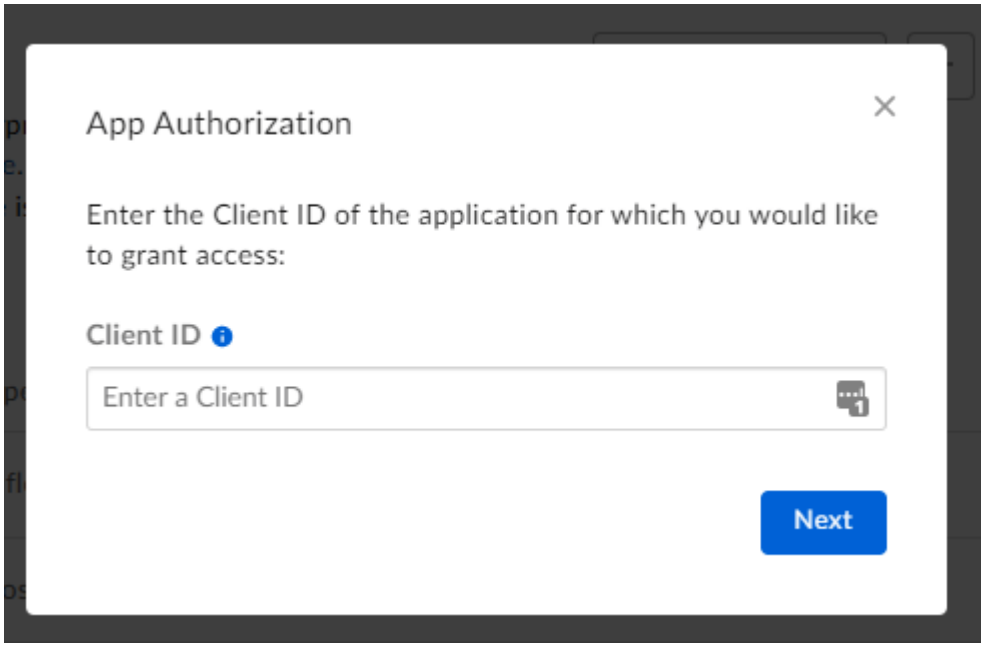


15. Click **Submit**
16. From the left-side menu, please press **Back to My Account** and switch to **Admin Console**.
17. Using the Admin Console left-side menu, navigate to **Apps** and then **Custom Apps**

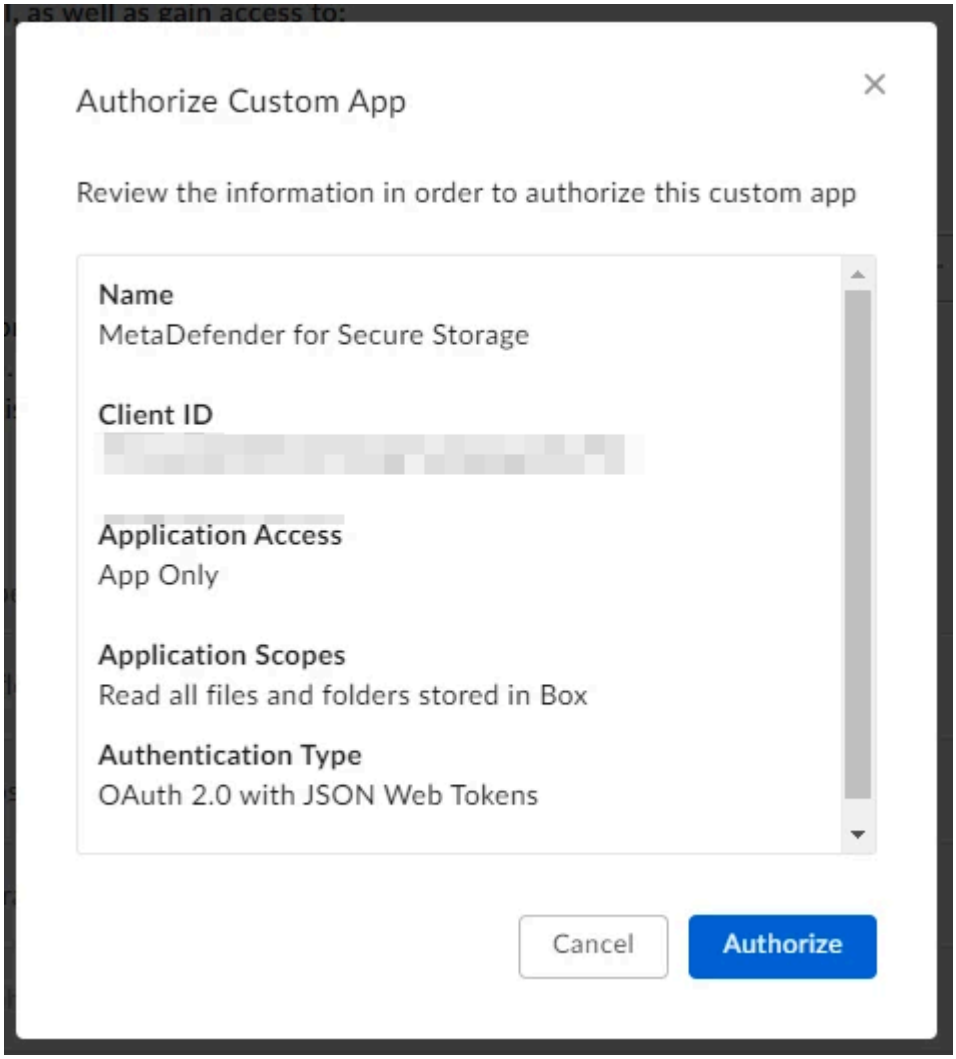


18. Click "**+**" and paste the previously copied **Client ID** and then click **Next**





19. Review the application permissions once again and then click **Authorize**



20. Almost done! All you need to do is go back to the MetaDefender Storage Security web interface and upload the **Public/Private Keypair** that you generated earlier in the **Credentials** field.

How my metadata is managed

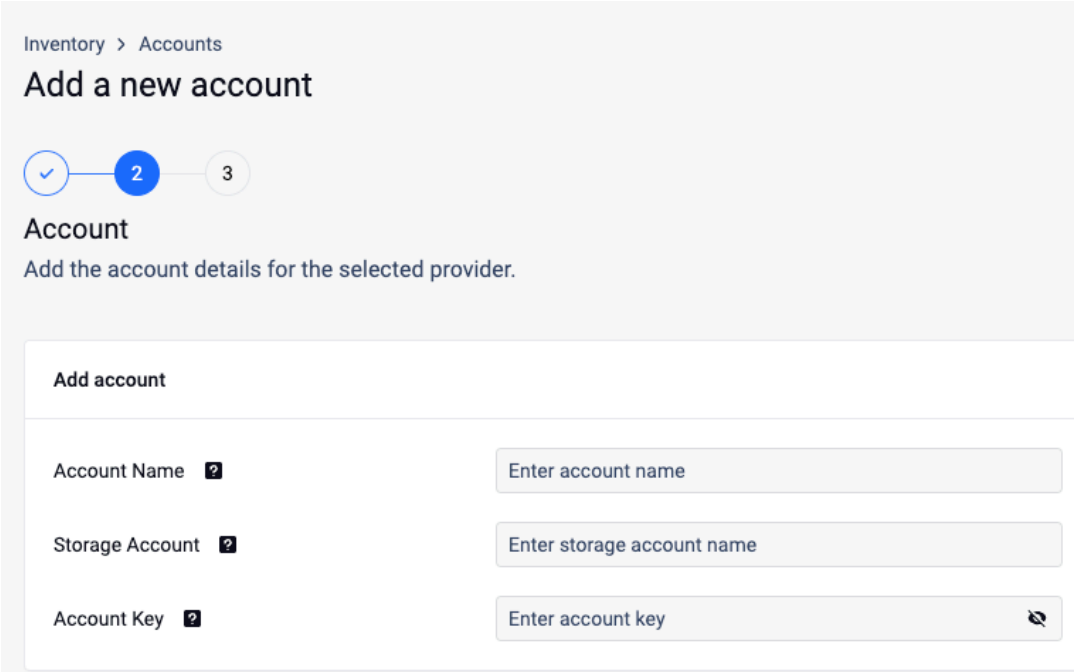
> **Warning**
>
> In Box, we support metadata, but with some limitations:
>
> 1. If the remediation actions are enabled and the file needs to be moved between accounts of the same enterprise, the metadata will be fully transferred.
> 2. If the remediation actions are enabled and the file needs to be moved between accounts of different enterprises, the metadata and its fields must be the same in these accounts in order to match. Otherwise, the metadata that does not match will be lost.

Add an Azure Files Storage

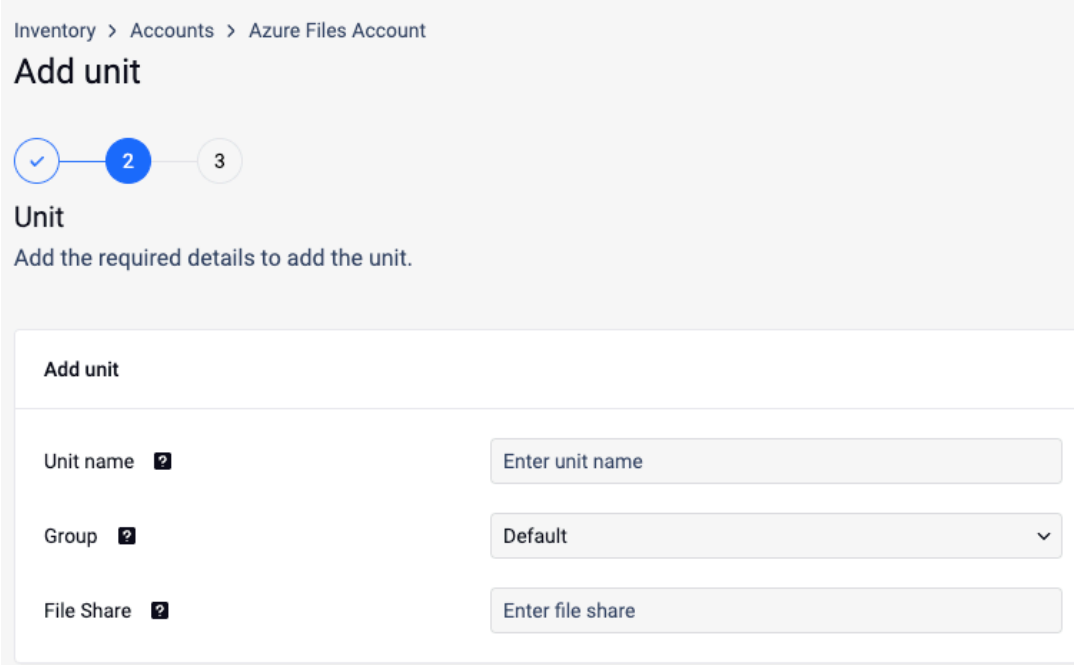
> **Warning**
>
> **Limitation :** Due to an Azure Files restriction, uploading 0-byte files is not supported. If a remediation action attempts to upload an empty file, the operation will fail.

In order to integrate Azure Files with MetaDefender Storage Security please follow these steps:

1. From the left side menu, navigate to **Inventory **, click on **Add account** and choose **Azure Files**



2. Give your account a name so you can easily identify it later
3. Enter the **Account Name**.
4. Enter your Azure **Storage Account**
5. Enter your **Account Key**. Scroll to the end of this page for more details.
6. Click next and finish the process
7. Add a new unit for the previously created account



7. Give your unit an unique name
8. Assign your unit to a Group
9. Enter the **name of the share** you wish to process with MetaDefender Storage Security.
10. Click **Next** in order to finish the process.

Where can I find the Access Key?

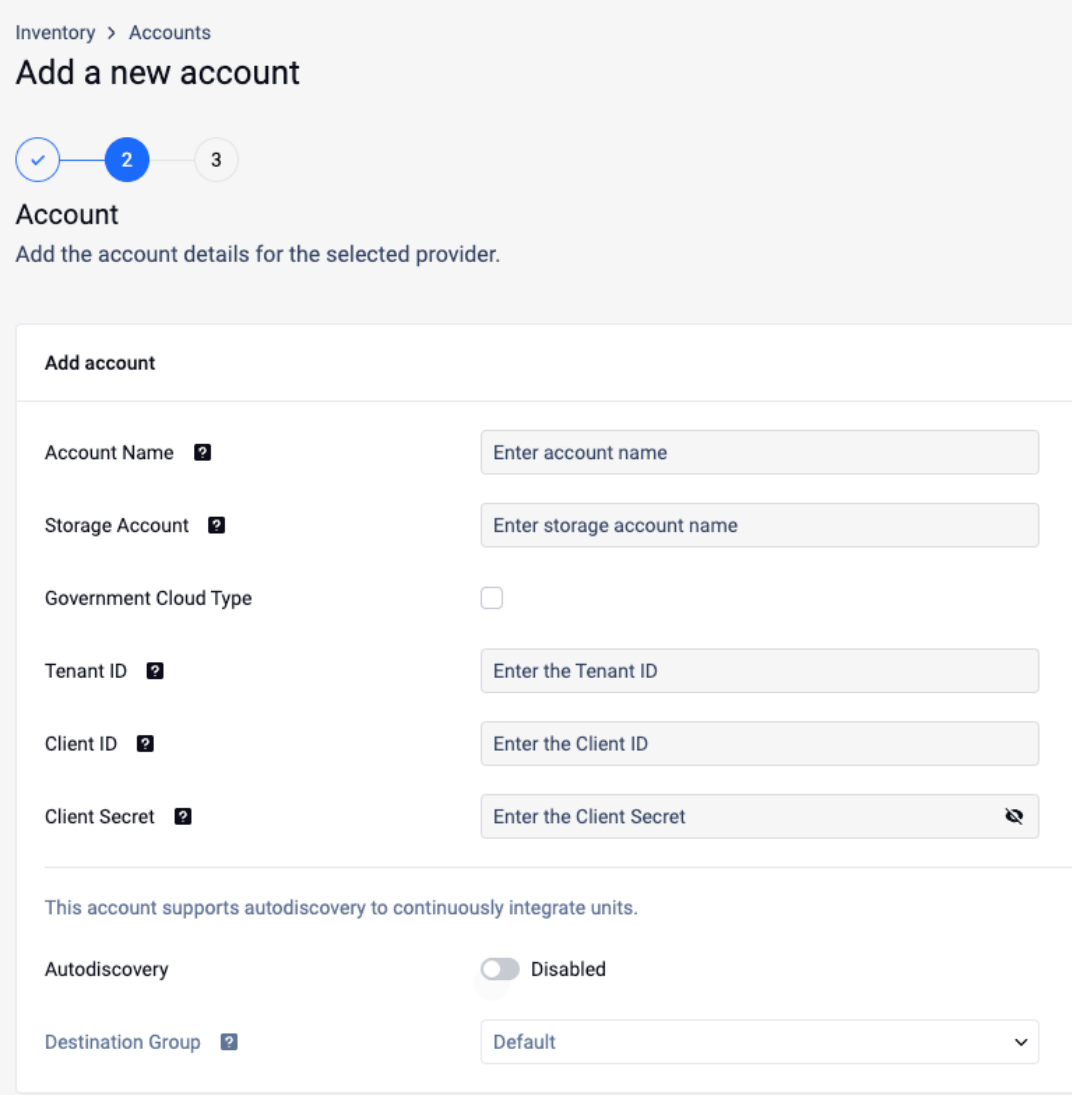
To find the Account Key, please follow these steps:

https://learn.microsoft.com/en-us/azure/storage/common/storage-account-keys-manage?tabs=azure-portal

Add an Azure Blob Storage

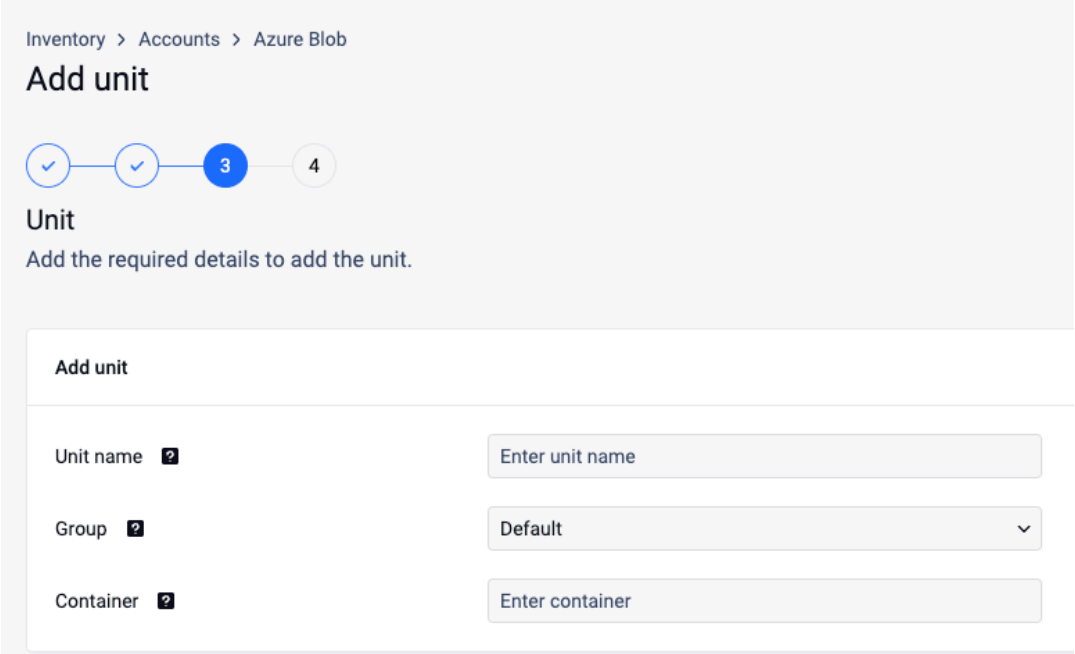
In order to integrate Azure Blob with MetaDefender Storage Security you will be required to create an application registration, assign the necessary permissions and roles, and then generate a secret key. Please follow these steps:

1. From the left side menu, navigate to **Inventory**, click on **Add account** and choose **Azure Blob**



2. Give your account a name so you can easily identify it later
3. Enter the Azure **Storage Account** name.
4. Select **Government Cloud type** if the storage belongs to Azure US Government Cloud.
5. Enter your **Tenant ID**. Scroll to the end of this page for more details.
6. Enter your **Client ID.** Scroll to the end of this page for more details.
7. Enter your **Client Secret.** Scroll to the end of this page for more details.
8. Click Next to finish the process.

9. Add a new unit for the created account

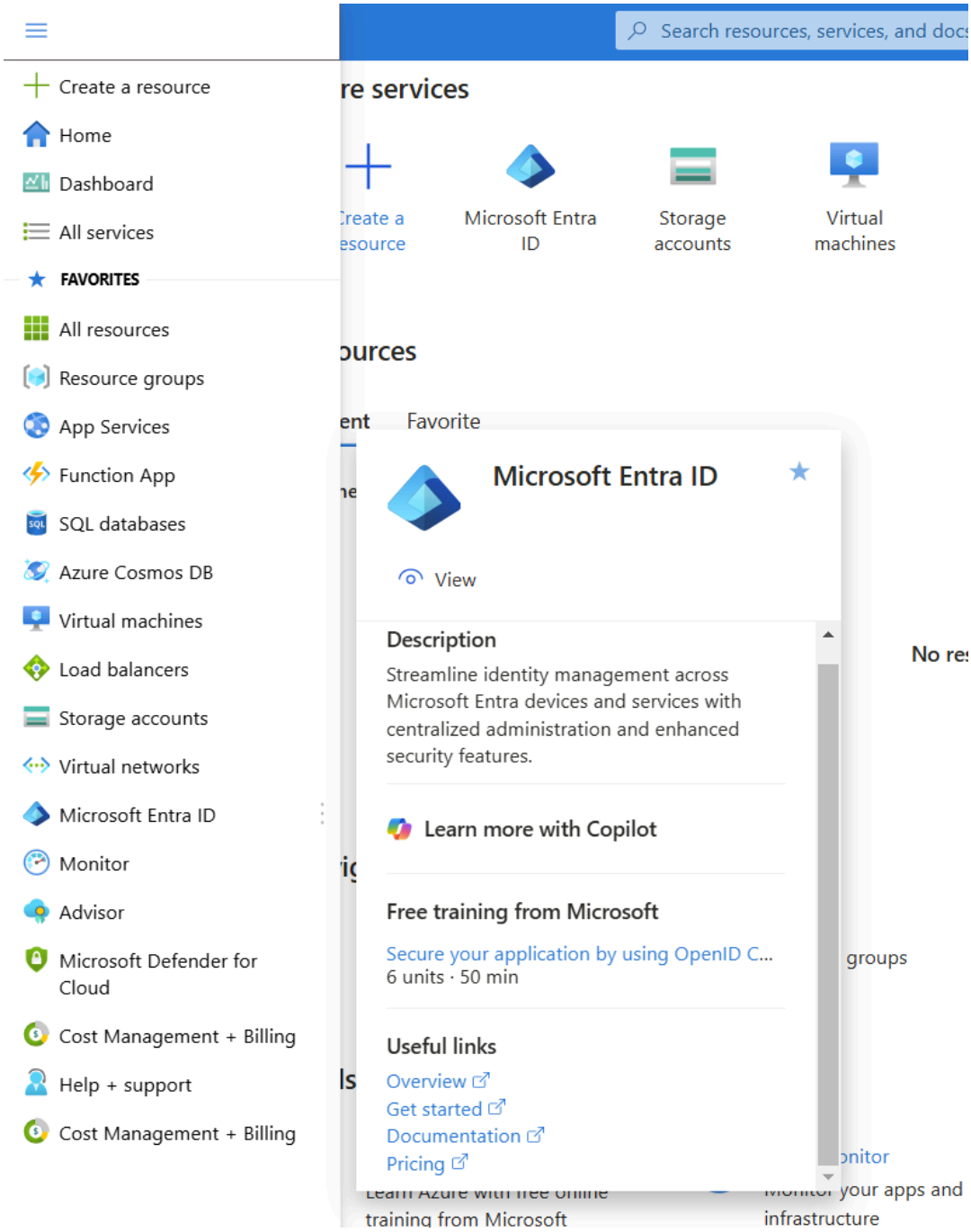


10. Enter an unique name for your unit.
11. Assing your unit to a Group
12. Enter the **name of a container** to process objects from a particular container.
13. Select **Next** in order to finish the process.

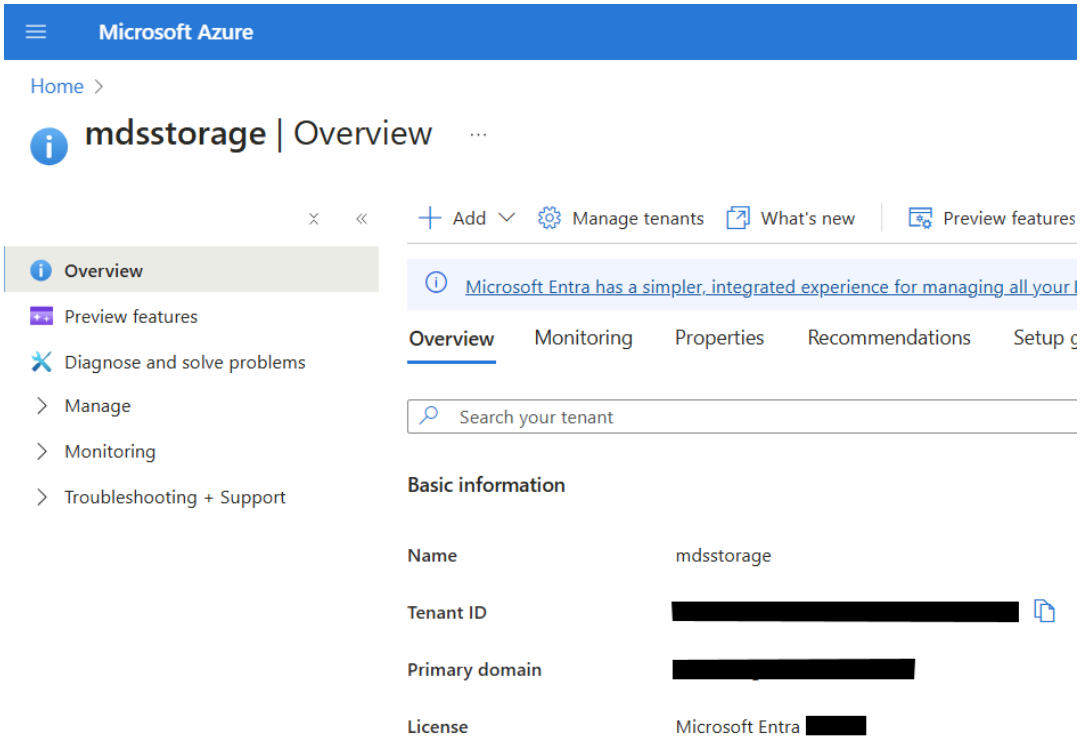
How to create an Azure Blob application?

In order to process your Azure Blob objects with MetaDefender Storage Security you will be required to add a new app registration in your Microsoft Entra ID Azure Portal.

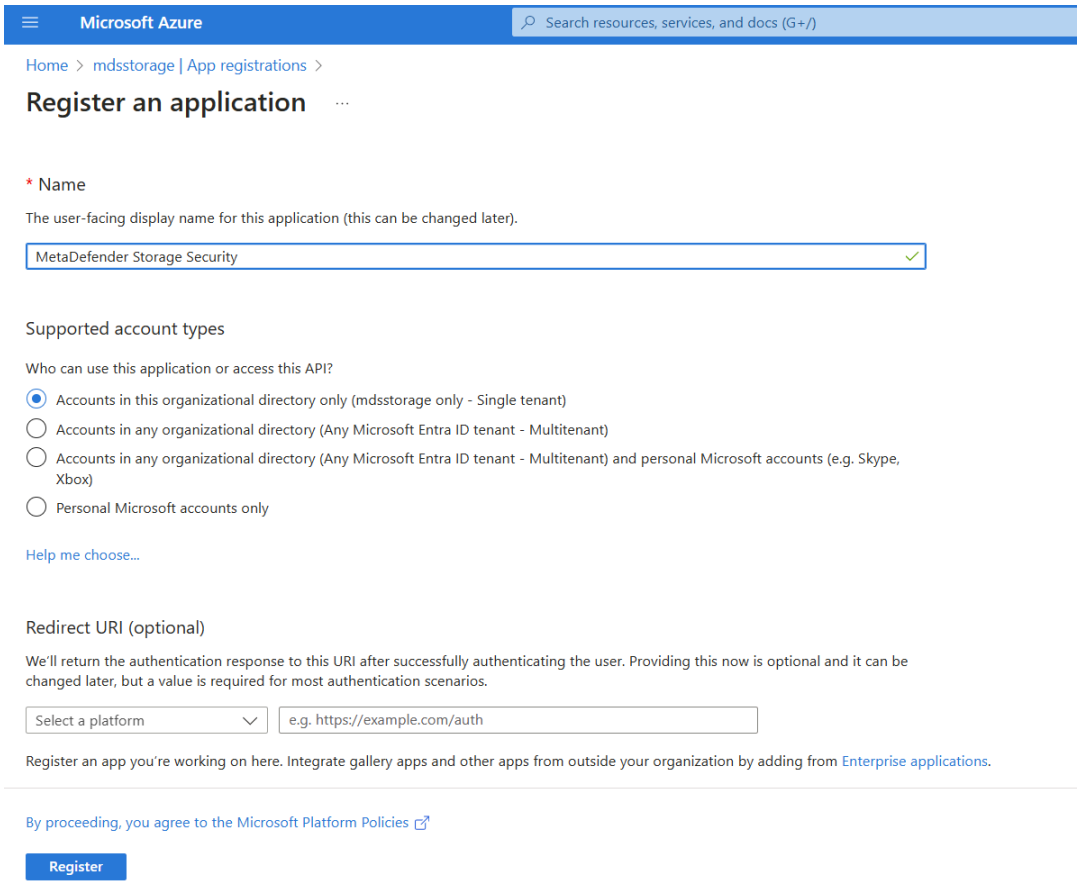
1. Log in to Azure Portal and from the left navigation menu choose **Microsoft Entra ID**



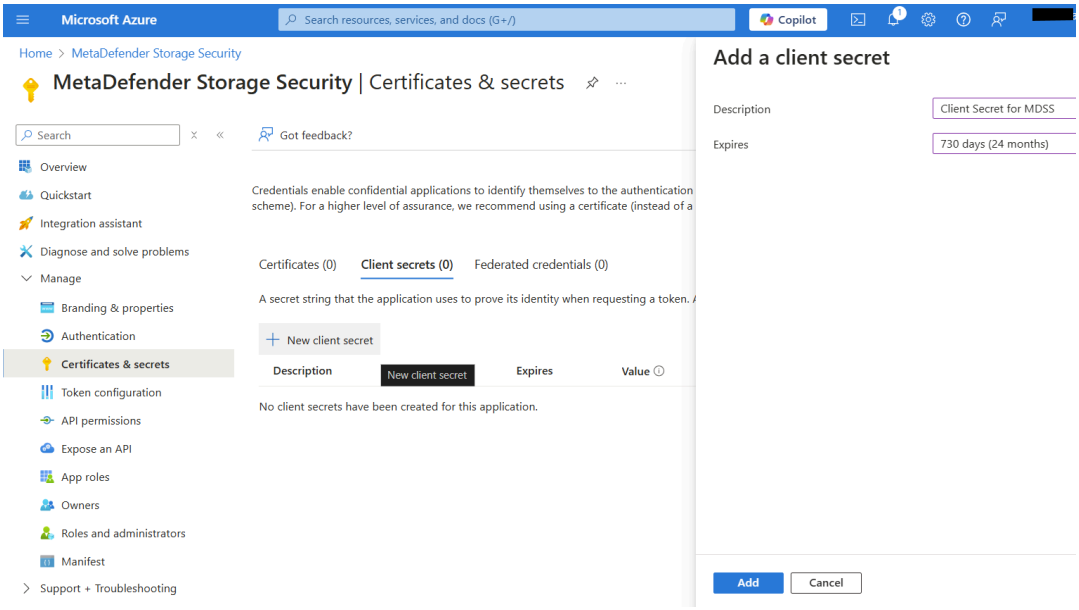
2. Make a copy of the **Tenant ID** from the overview page



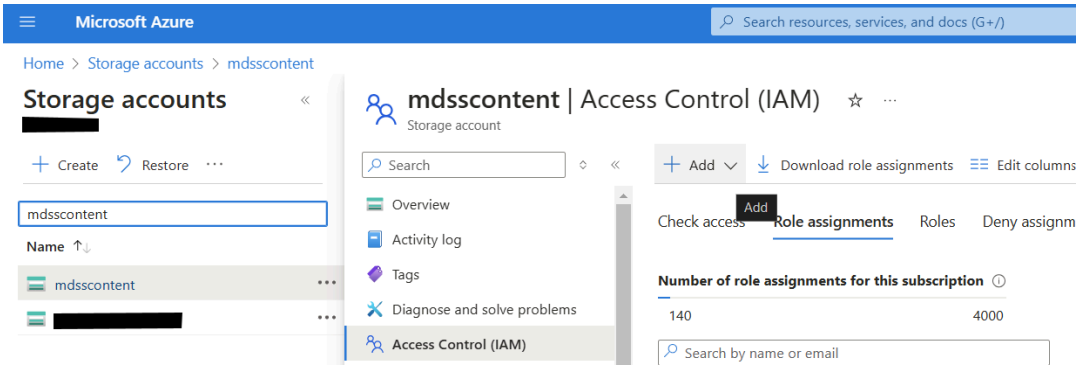
3. From the left side menu, choose **App registrations**
4. Click **New registration**
5. Give your app a name so you can easily identify it



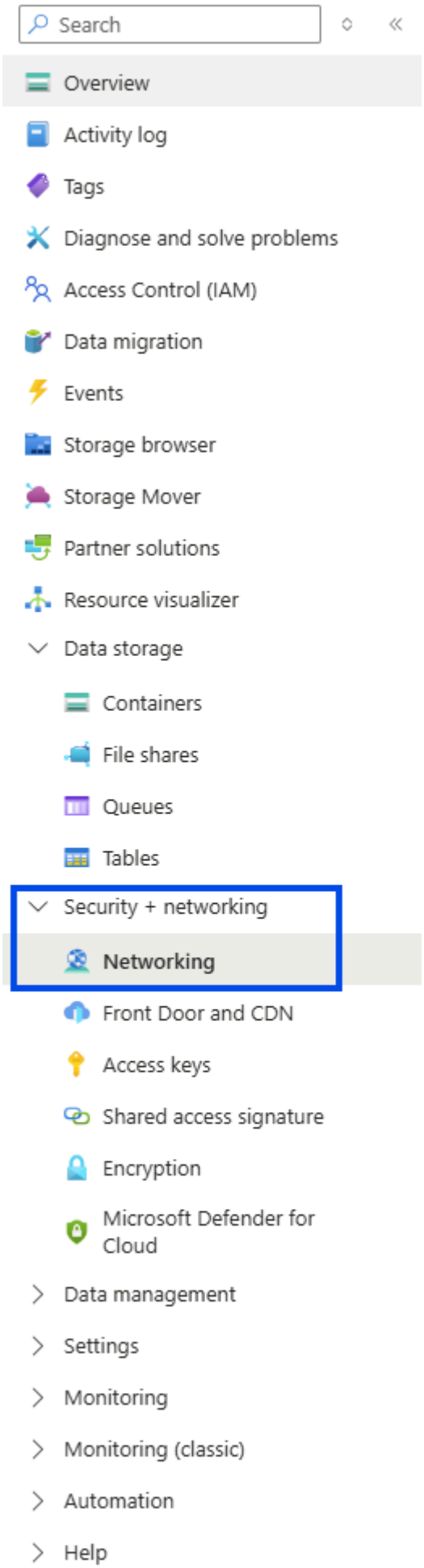
6. There is no need to modify the other properties. When ready, please click **Register**
7. From the **Overview** page of your newly created application, make a copy of **Application (client) ID**
8. Navigate to **Certificates & Secrets** from the left-side menu
9. Click **New client secret** and choose Expires in 24 months



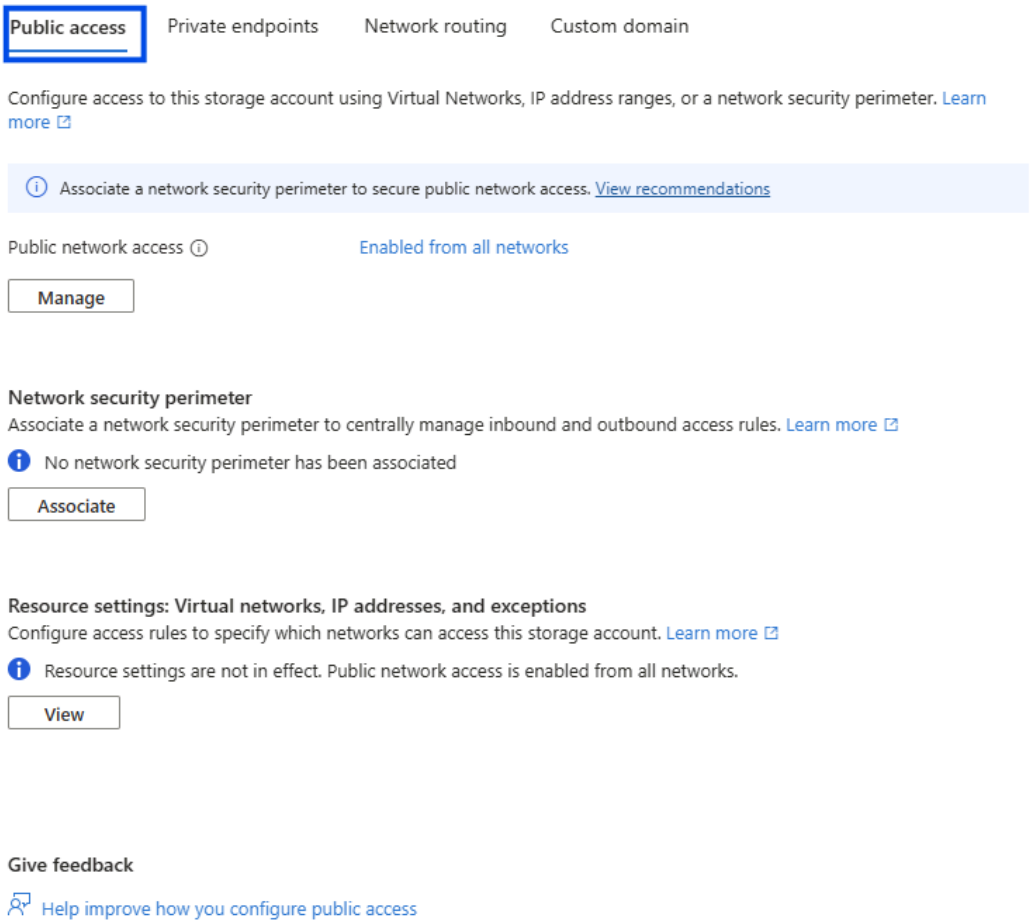
10. Click Add and then you will need to make a copy of the generated secret key because it will not be available later
11. Navigate to your **Storage Account** and select the **Access Control (IAM)** menu
12. Select the **Role assignments** tab, then select the **Add role assignment** option from the **Add** dropdown.



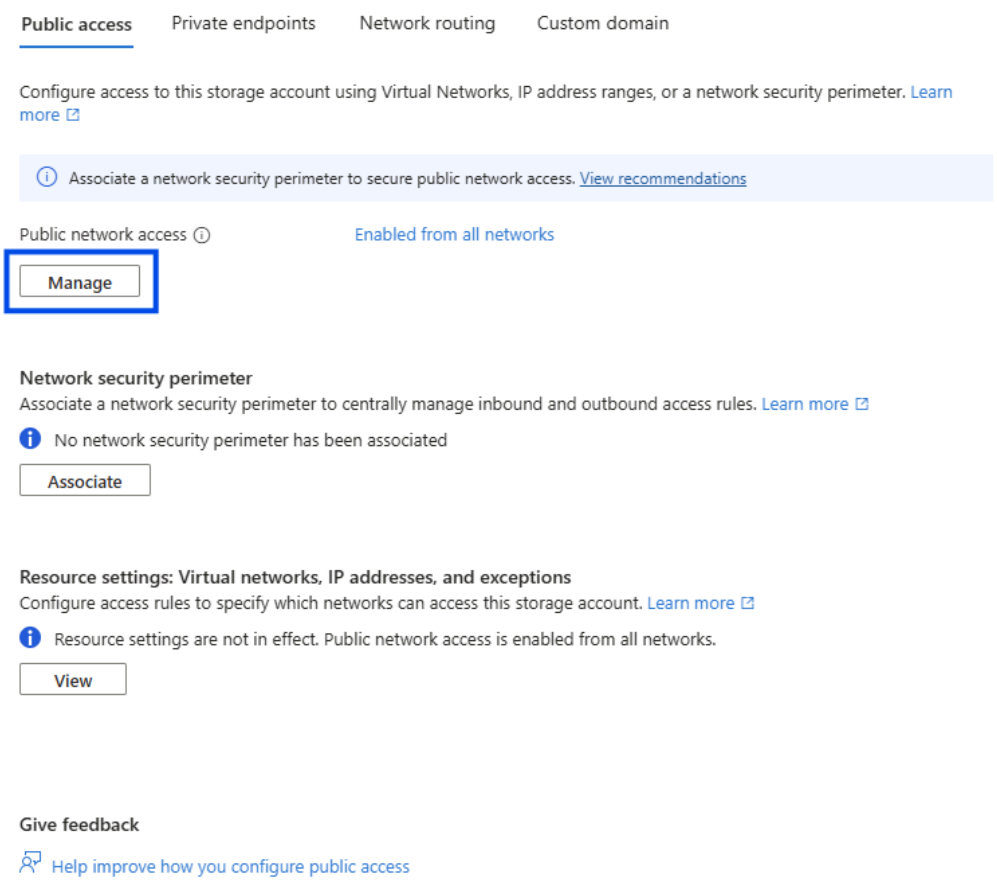
13. Assign the following roles to the **Client Application** you previously registered:
    1. Storage Blob Data Contributor
    2. Reader
14. Navigate back to your **Storage Account** and from **Security + networking** menu, select **Networking**


Search
Overview
Activity log
Tags
Diagnose and solve problems
Access Control (IAM)
Data migration
Events
Storage browser
Storage Mover
Partner solutions
Resource visualizer
Data storage
Containers
File shares
Queues
Tables
Security + networking
Networking
Front Door and CDN
Access keys
Shared access signature
Encryption
Microsoft Defender for Cloud
Data management
Settings
Monitoring
Monitoring (classic)
Automation
Help

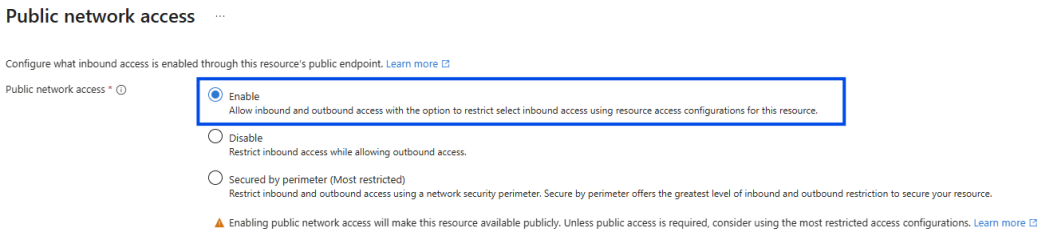
15. Navigate to **Public access** tab (the first and default one)



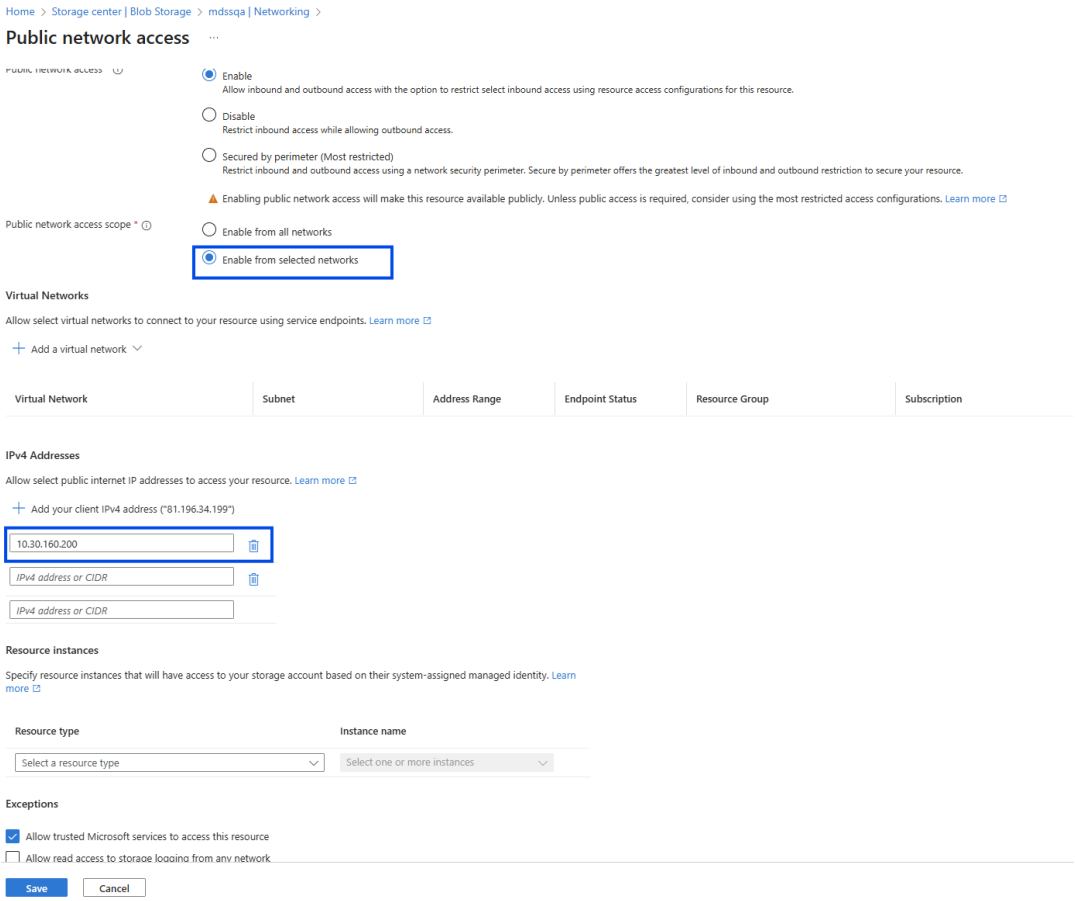
16. Click Manage on the Public network access section



17. Enable **Public network access**



18. From the **Public network access scope**, you have two options:
    1. Enable from all networks: this is less restrictive and will allow any applications to try to establish a successful connection to your storage account.
    2. Enable from selected networks: this will restrict access only to specific IPv4 addresses. If you enable this option, please add the IP address of the machine where MetaDefender Storage Security instance is running. If is running on Kubernetes, please add the IP addresses of the following pods: storagesservice-azureblob, discoveryazureblobservice, remediationsservice-azureblob, scanningservice. If you are moving file from Azure Blob to another type of storage unit, please add its remediationsservice-{storageType} pod to this list.



19. Now that you have the **Tenant ID**, **Client ID** and the **Client Secret Key**, you can go back in **MetaDefender Storage Security** and finish the Azure Blob integration. Congratulations!

For additional configuration of how MetaDefender Storage Security handles blobs please check custom configuration.

How to Enable Autodiscovery

This guide provides step-by-step instructions for enabling Autodiscovery for Azure Blob storage in MetaDefender Storage Security.

Autodiscovery automatically detects and adds Azure Blob containers as storage units, saving time and reducing configuration errors.

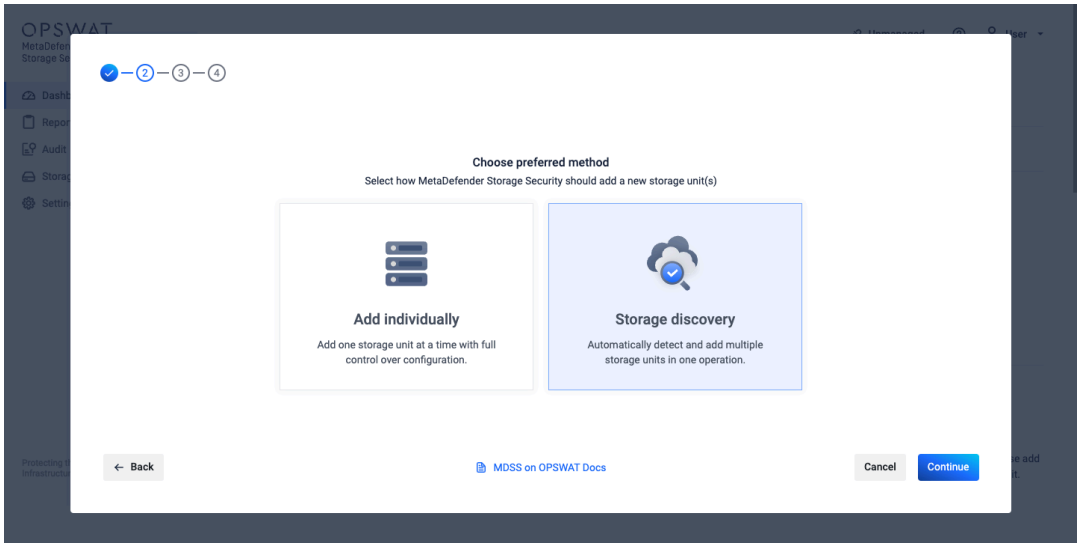
Prerequisites

Before enabling Autodiscovery, ensure you have:

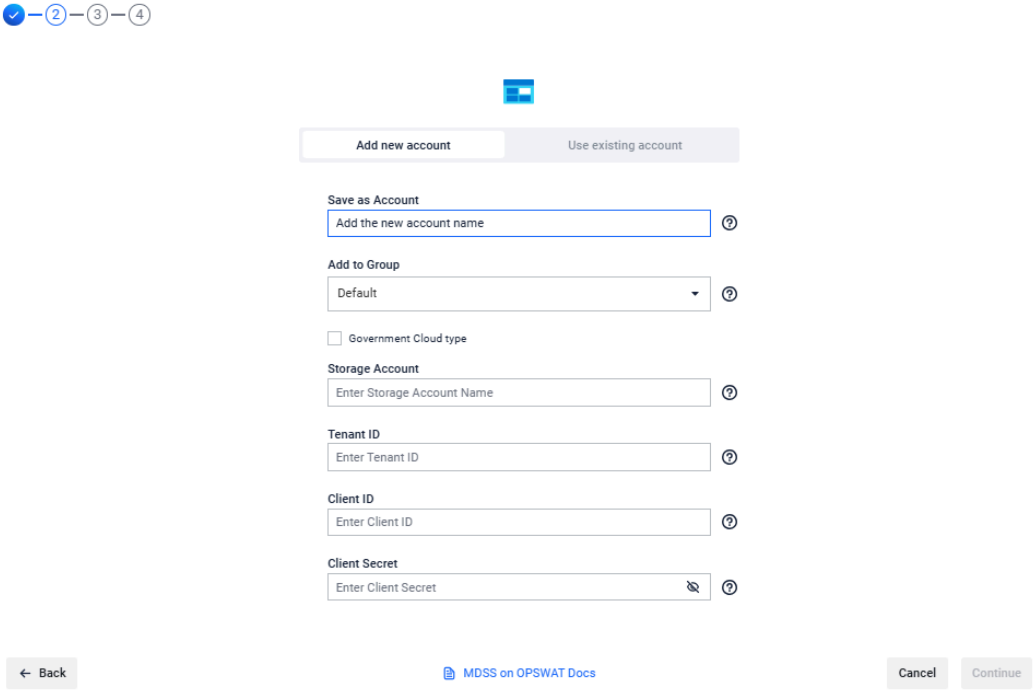
1. Valid Azure Blob credentials with sufficient permissions
2. Permissions as stated in Add an Azure Blob storage

Method 1: Enable Autodiscovery During Storage Unit Addition

- Navigate to **Storage Units** page
- Click **Add Storage Unit** button
- Select **Azure Blob** Storage Type
- Select **Storage Discovery** and click **Continue**

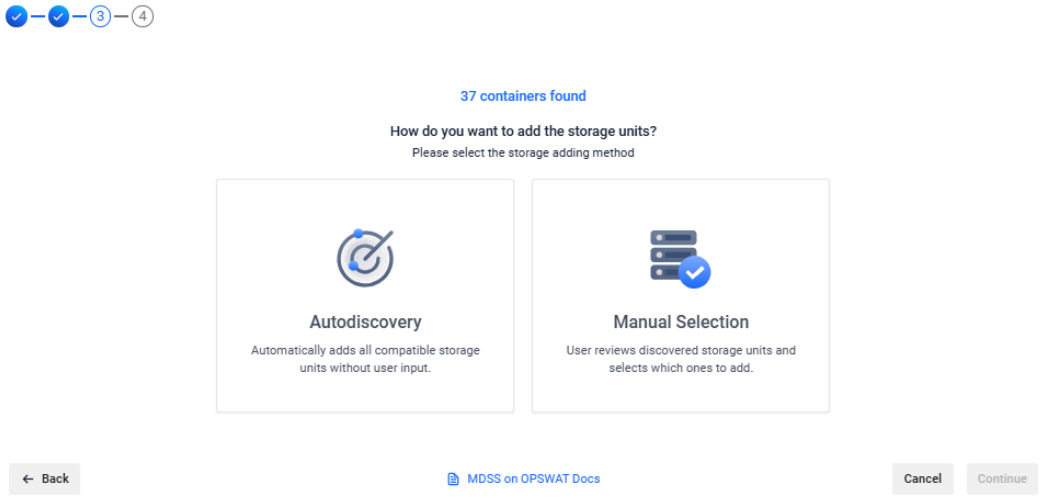


- Fill out the form with valid Azure Blob credentials and click **Continue**



- In the next step, select your integration method. You have two choices: Autodiscovery and Manual Selection.

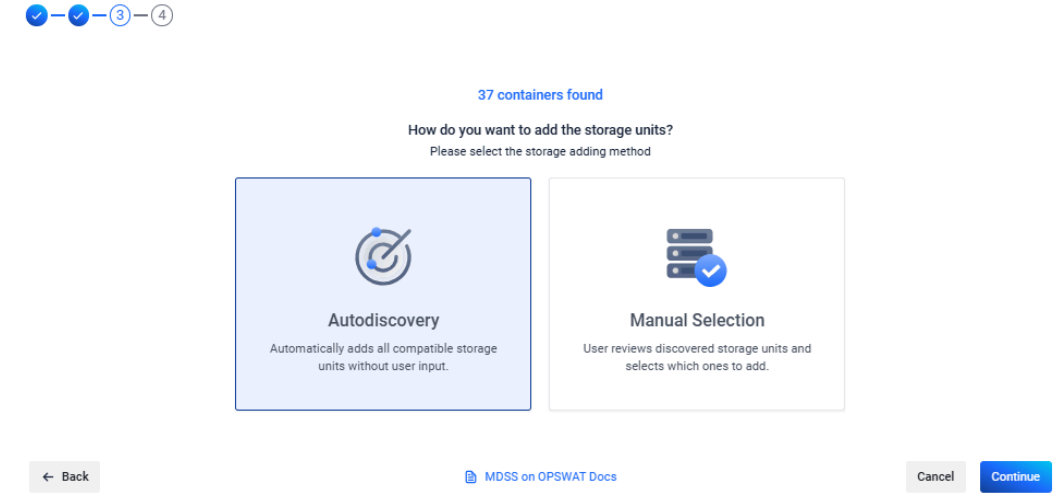
- **Autodiscovery** for convenience, this option automatically adds all the containers that MDSS finds
- **Manual Selection** for precise control, this option lets users choose specific containers from the discovered list to integrate.

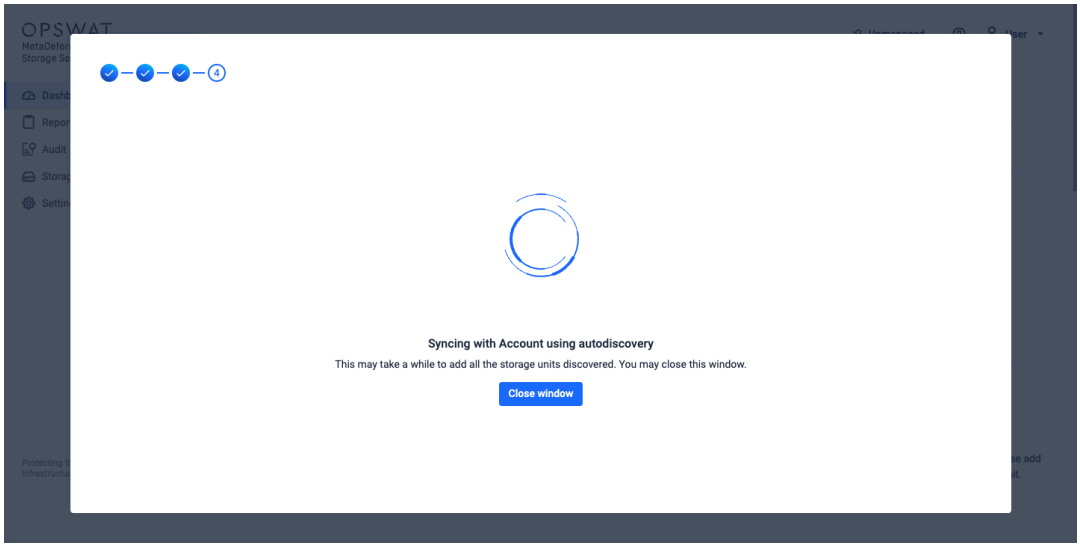


To learn more about each integration type, please consult the Autodiscovery documentation.

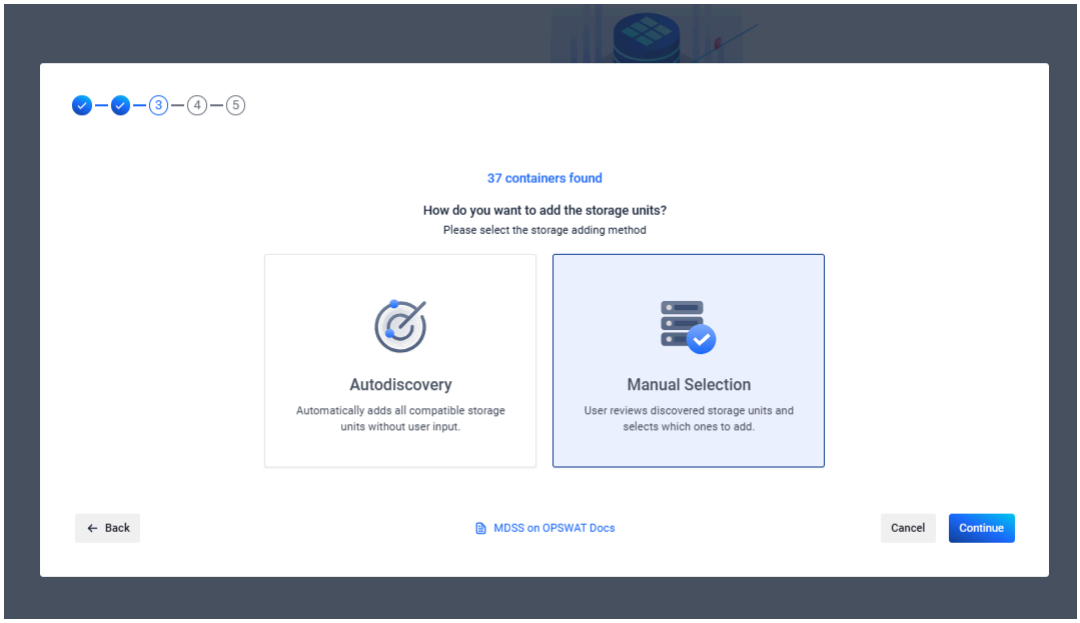
> **NO CONTAINERS FOUND**
>
> If there were no containers found, you will be presented with a third option - **Add Individually** - which will reveal the credentials form to manually add the storage by using the site name.

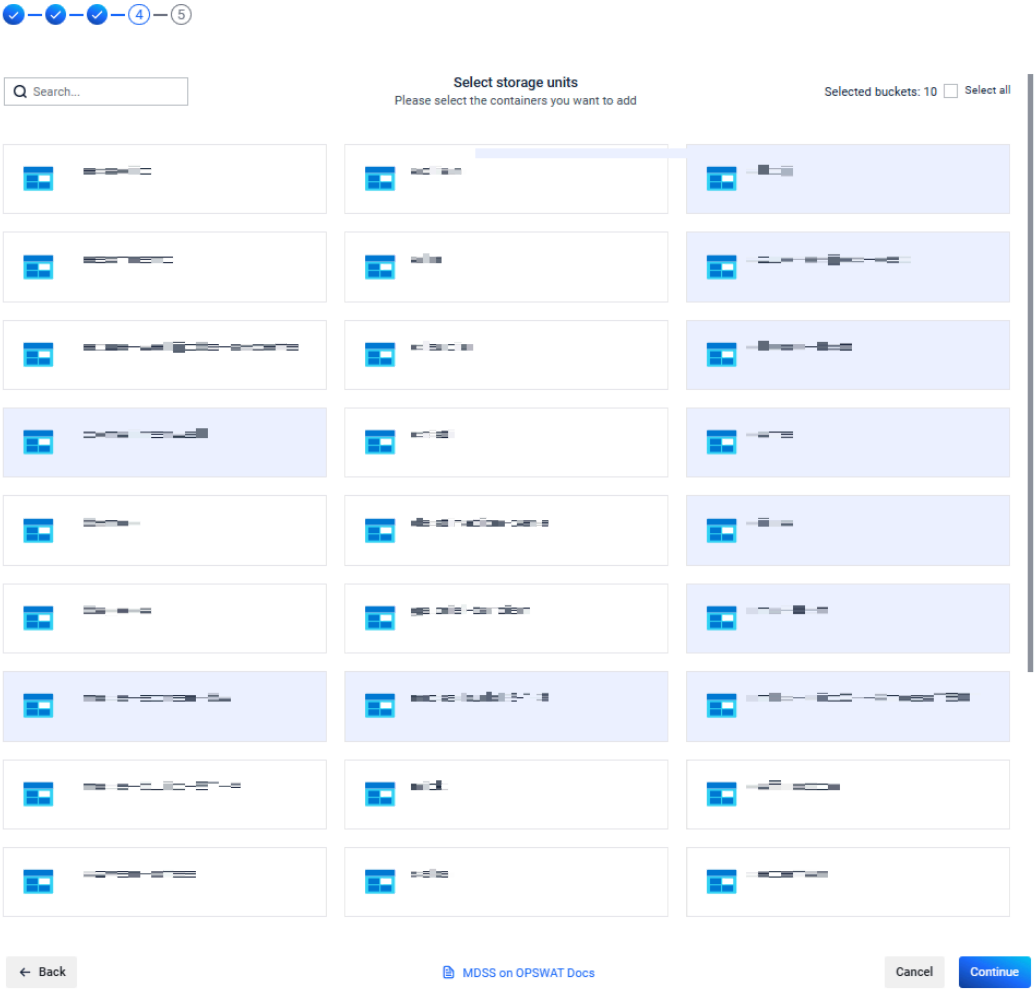
- If selecting the **Autodiscovery** option:
  - Click **Continue,** and an informative message will be displayed that the autodiscovery process has started in the background. You can safely close the modal, and the storage units will be added in the background to the Storage Units page

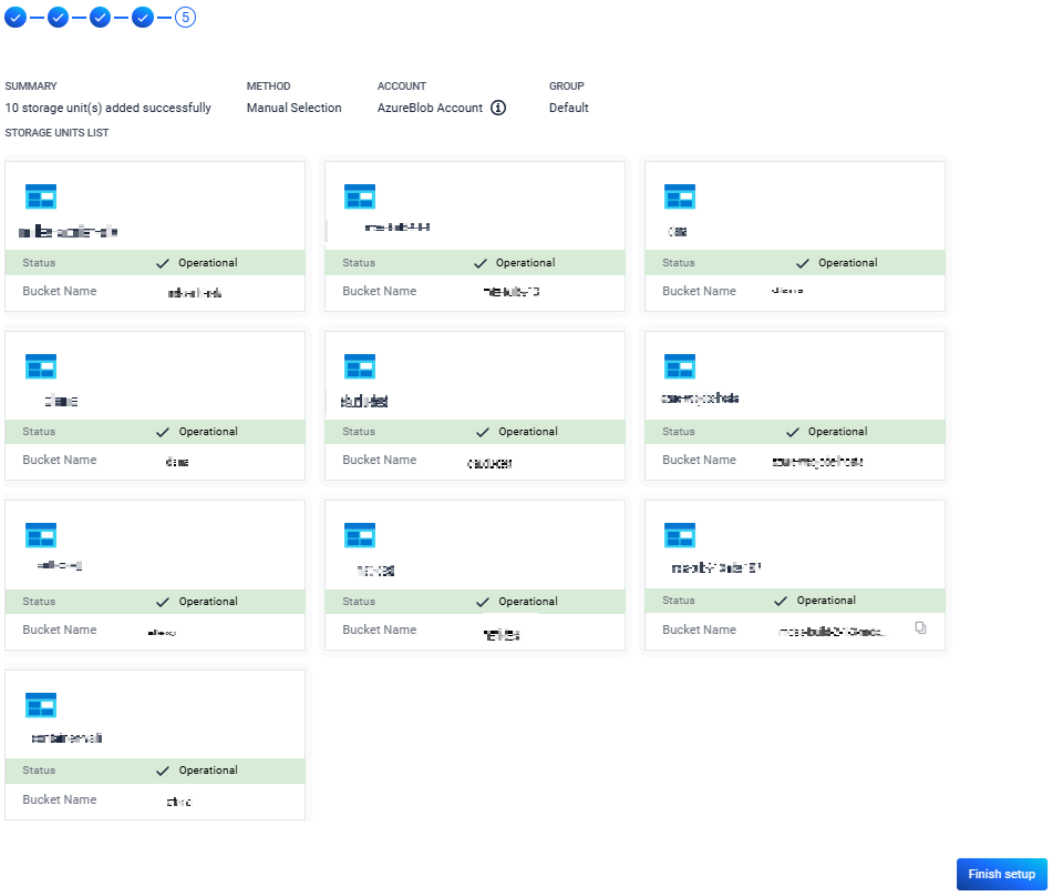




- If selecting **Manual Selection** option:
  - Click **Continue**
  - Select the containers you want to add from the discovered list
  - Click **Continue**
  - The system will show a syncing message indicating containers are being added. You can choose to stay on this page in order to see the storage units that were successfully added and also to see if there were any errors while trying to add specific storage units.


37 containers found
How do you want to add the storage units?
Please select the storage adding method
Autodiscovery
Automatically adds all compatible storage units without user input.
Manual Selection
User reviews discovered storage units and selects which ones to add.
Back
MDSS on OPSWAT Docs
Cancel
Continue

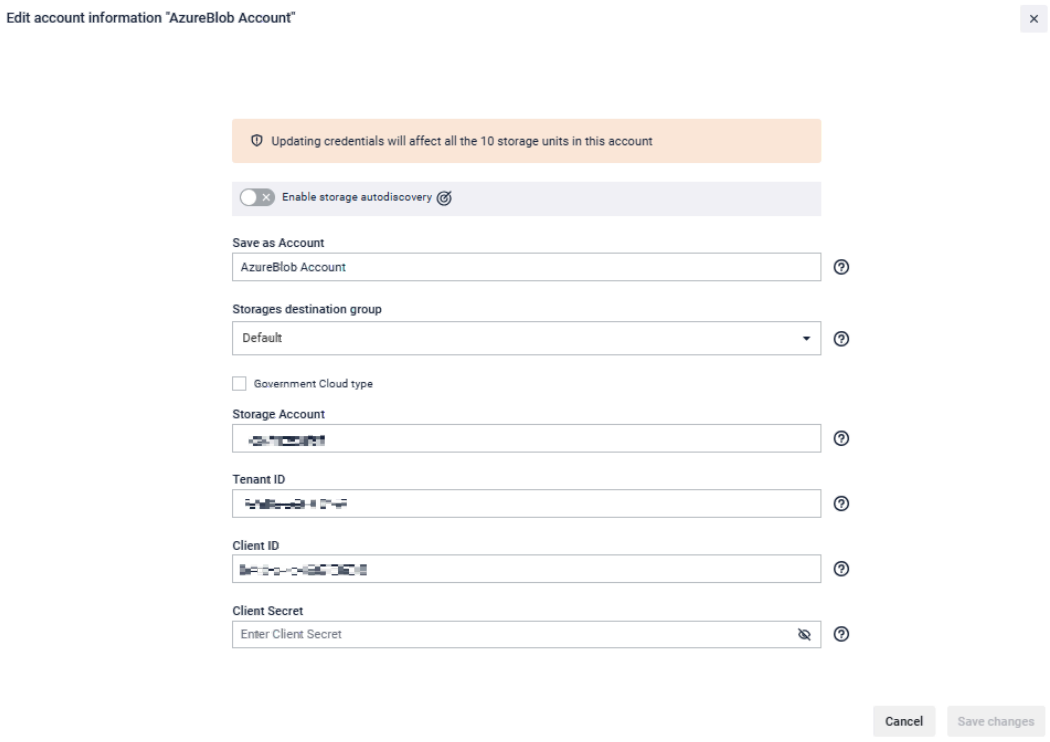

Search...
Select storage units
Please select the containers you want to add
Selected buckets: 10
Select all
Back
MDSS on OPSWAT Docs
Cancel
Continue



> **ERROR ADDING A STORAGE THAT WAS SELECTED DURING MANUAL SELECTION**
>
> In case there was an error while trying to add your storage, you will see the error message in the Storage card while hovering over the (i) icon.

Method 2: Enable Autodiscovery for an Existing Account

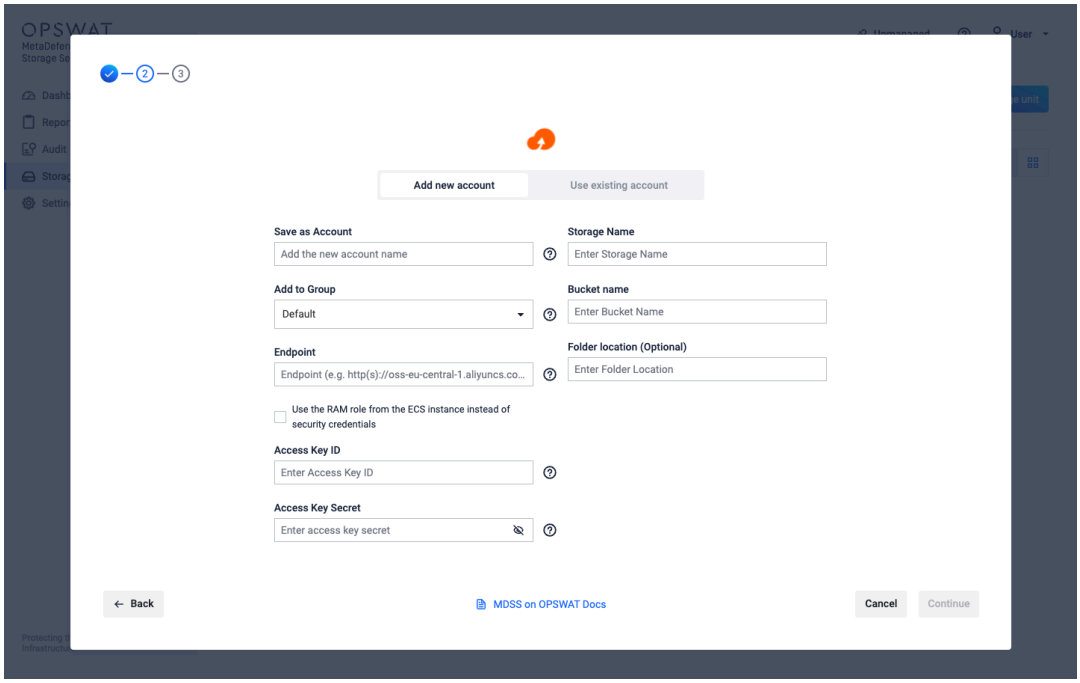
- Navigate to the **Storage Units** page
- Identify a storage that's using the account you want to start autodiscovery for
- Click on the 3-dots button from the storage card and select **Manage Storage Unit**
- From the top toggle, select **Change account info**
- Turn on autodiscovery by toggling the **Enable storage auto discovery** switch


Edit account information "AzureBlob Account"
Updating credentials will affect all the 10 storage units in this account
Enable storage autodiscovery
Save as Account
AzureBlob Account
Storages destination group
Default
Government Cloud type
Storage Account
Tenant ID
Client ID
Client Secret
Enter Client Secret
Cancel
Save changes

Add an Alibaba Cloud Storage

In order to integrate Alibaba Cloud with MetaDefender Storage Security please follow these steps:

1. From the left side menu, navigate to **Storage units**, click on **Add storage unit** and choose **Alibaba Cloud**



2. Give your account a name so you can easily identify it later
3. Give your storage a name so you can easily identify it later
4. Enter the **Endpoint** URL for *Access Over Internet*. Scroll to the end of this page for more details.
5. There are two ways to connect:
   - **via the RAM role from the ECS instance** [If you choose this option, skip the following two steps and continue from step 7]
   - **using security credentials**
6. Enter your **Access Key ID**. Scroll to the end of this page for more details.
7. Enter your **Access Key Secret .** Scroll to the end of this page for more details.
8. Enter the **name of the bucket** you wish to process with MetaDefender Storage Security.
9. If you wish to only process a particular folder enter the name or path of the folder in the **Folder location** field. Leave this field empty if you wish to process the entire bucket.
10. Select **Continue** in order to finish the process.

Where can I find the Endpoint URL?

The endpoint URL can be found in the following list of the official documentation of Alibaba Cloud.

https://www.alibabacloud.com/help/en/object-storage-service/latest/regions-and-endpoints

Where can I find the Access Key ID and Access Key Secret?

To generate an Access Key ID / Access Key Secret pair please follow these steps, explained in the official documentation of Alibaba Cloud.

https://www.alibabacloud.com/help/en/basics-for-beginners/latest/obtain-an-accesskey-pair

Using RAM role for Alibaba Cloud integration

On Alibaba Cloud integration with RAM, the role configured on the ECS instance will be used to authenticate.

Please use the following links to configure and attach a RAM role to the ESC instance:

https://www.alibabacloud.com/help/en/ram/product-overview/best-practices-for-identity-and-access-control

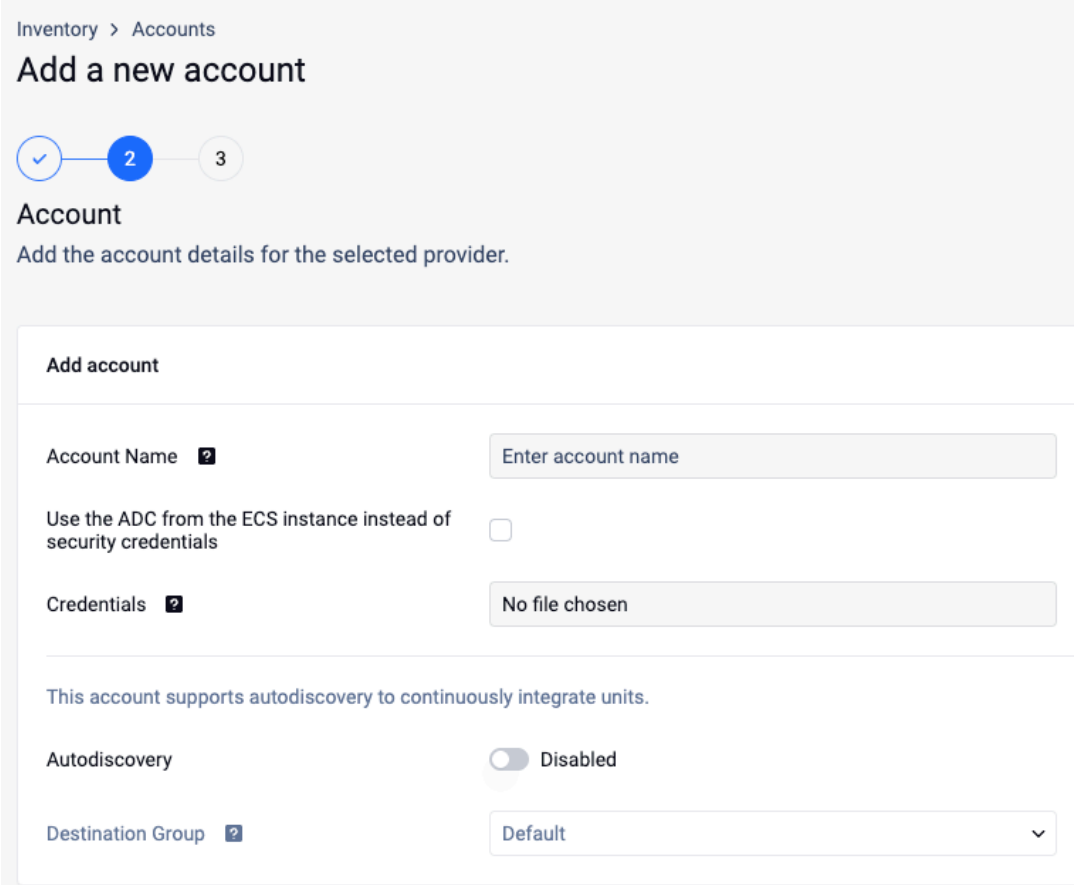
https://www.alibabacloud.com/help/en/elastic-compute-service/latest/use-ram-roles-to-access-other-alibaba-cloud-services

https://www.alibabacloud.com/help/en/elastic-compute-service/latest/attach-an-instance-ram-role

Add a Google Cloud Storage

In order to integrate Google Cloud with MetaDefender Storage Security please follow these steps:

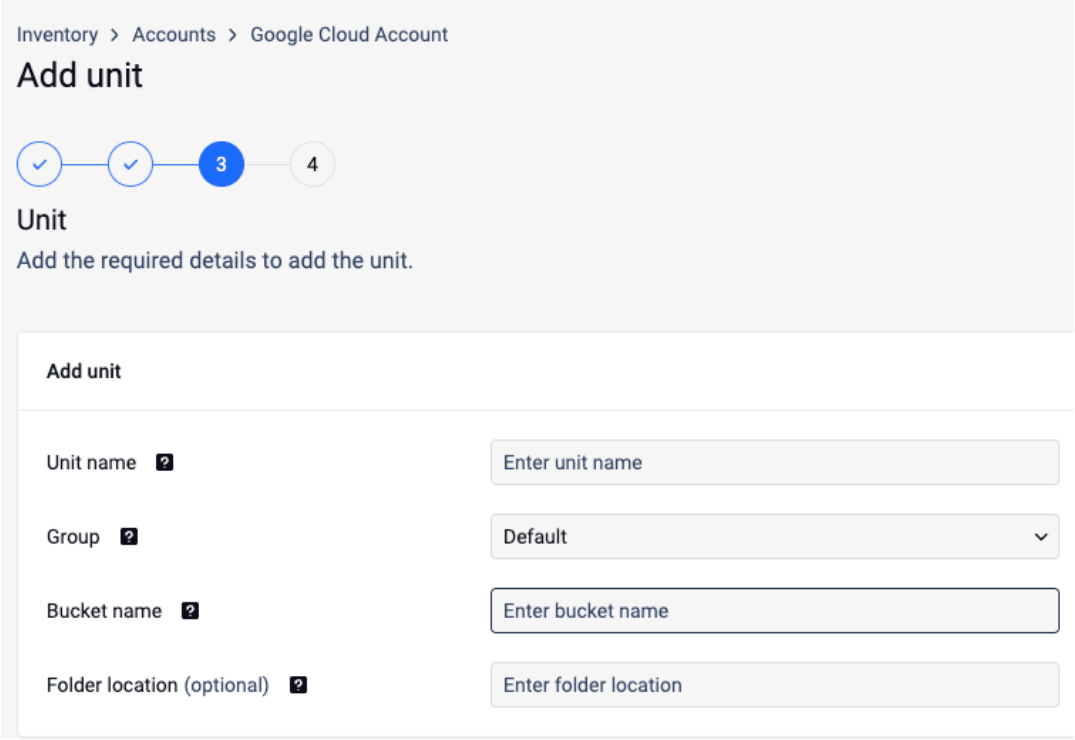
1. From the left side menu, navigate to **Inventory**, click on **Add account** and choose **Google Cloud**



2. Give your account a name so you can easily identify it later
3. There are two ways to connect:

- **via the ADC from the ECS instance** (If you choose this option, skip the following step and continue from step 5)
- **using security credentials**

4. Upload your **Credentials** file. Scroll down for more details.
5. Click Next in order to finish the process
6. Add an unit for the created account



7. Give your unit an unique name
8. Assign your unit to a Group
9. Enter the **name of the bucket** you wish to process with MetaDefender Storage Security.
10. If you wish to only process a particular folder enter the name or path of the folder in the **Folder location** field. Leave this field empty if you wish to process the entire bucket.
11. Select **Next** in order to finish the process.

> **Info**
>
> To be able to use **autodiscovery**, the credentials should have at minimum the **Storage Legacy Bucket Reader** [**roles/storage.legacyBucketReader**] role

Where can I generate the Credentials file?

To generate a credentials file, please follow these steps, explained in the official documentation of Google Cloud.

https://developers.google.com/workspace/guides/create-credentials#service-account

Using ADC for Google Cloud integration

On Google Cloud integration with ADC, the default credentials configured on the ECS instance will be used to authenticate.

Please use the following links to attach application default credentials to the ESC instance:

https://cloud.google.com/docs/authentication/application-default-credentials

https://cloud.google.com/iam/docs/impersonating-service-accounts#attaching-to-resources

> **Warning**
>
> If the google credentials are **not** set in the **GOOGLE_APPLICATION_CREDENTIALS** variable, then the service account assigned to the VM instance requires the **iam.serviceAccounts.signBlob** permission (included in the **Service Account Token Creator** role) and the `https://www.googleapis.com/auth/iam` OAuth access scope (or the broader `https://www.googleapis.com/auth/cloud-platform` scope).

Using GCP Buckets With Hierarchical Namespace (HNS)

We recommend enabling **Hierarchical Namespace (HNS)** on your Google Cloud Storage buckets. When HNS is enabled, folder paths behave as true directories, allowing MetaDefender Storage Security to correctly validate and process **empty folders** and **folders containing only subfolders**.

With HNS enabled:

- Empty folders can be added as destinations
- Folder existence is reliably detected

Without HNS:

- Empty folders may be rejected as “non-existent”
- Hidden system objects may affect folder validation

Learn more in Google’s official documentation:
https://docs.cloud.google.com/storage/docs/folders-overview

Google Cloud: Handling Rate Limiting

For transient errors on Google Cloud requests a retry with exponential backoff can be configured to adjust the required needs. The HTTP error codes covered are the `TooManyRequests`, `RequestTimeout`and `ServiceUnavailable`.

The retry policy can be customized using the following environment variables:

Parameters	Value
GCP_MAX_RETRY_ATTEMPTS	10
GCP_MAX RETRY_DELAY	120 (seconds)

The retry policy implements exponential backoff, starting with a 200-millisecond delay between retries and capping at a maximum delay of 120 seconds after 10 retries.

How to Enable Autodiscovery

This guide provides step-by-step instructions for enabling Autodiscovery for Google Cloud storage in MetaDefender Storage Security.

Autodiscovery automatically detects and adds GCP buckets as storage units, saving time and reducing configuration errors.

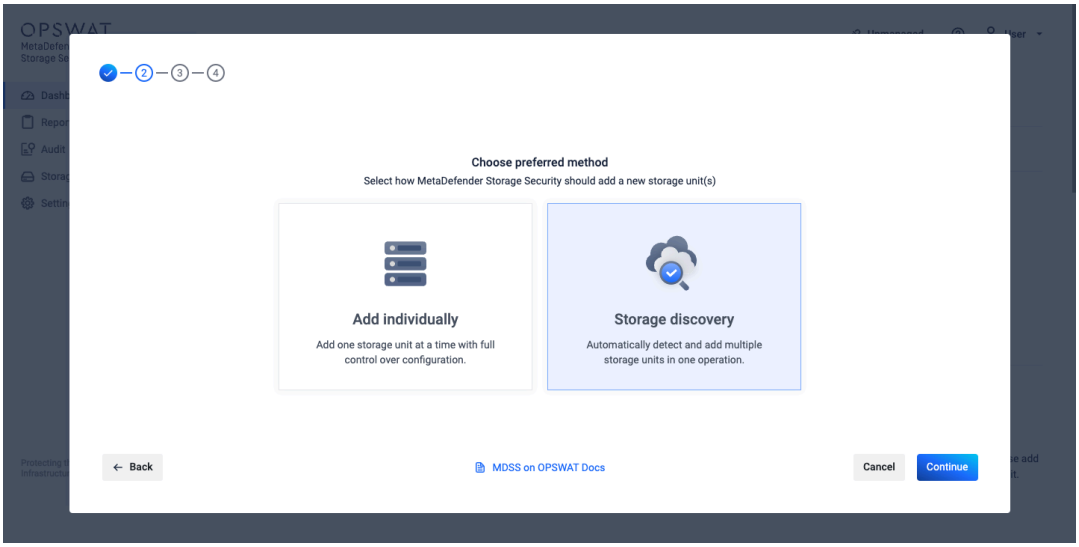
Prerequisites

Before enabling Autodiscovery, ensure you have:

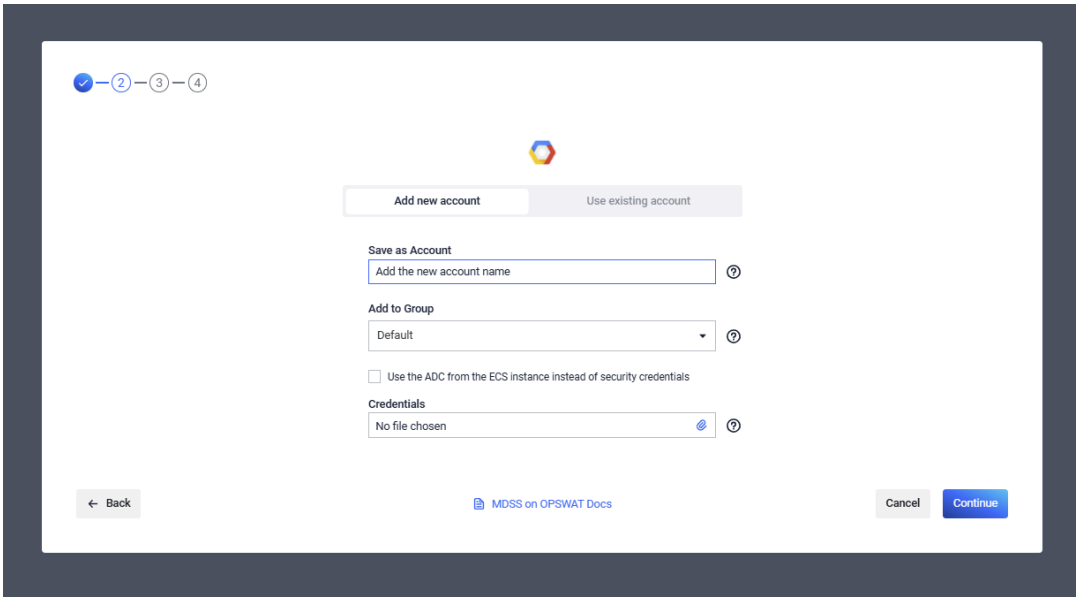
1. Valid GCP credentials file with sufficient permissions
2. Permissions as stated in Add a Google Cloud Storage

Method 1: Enable Autodiscovery During Storage Unit Addition

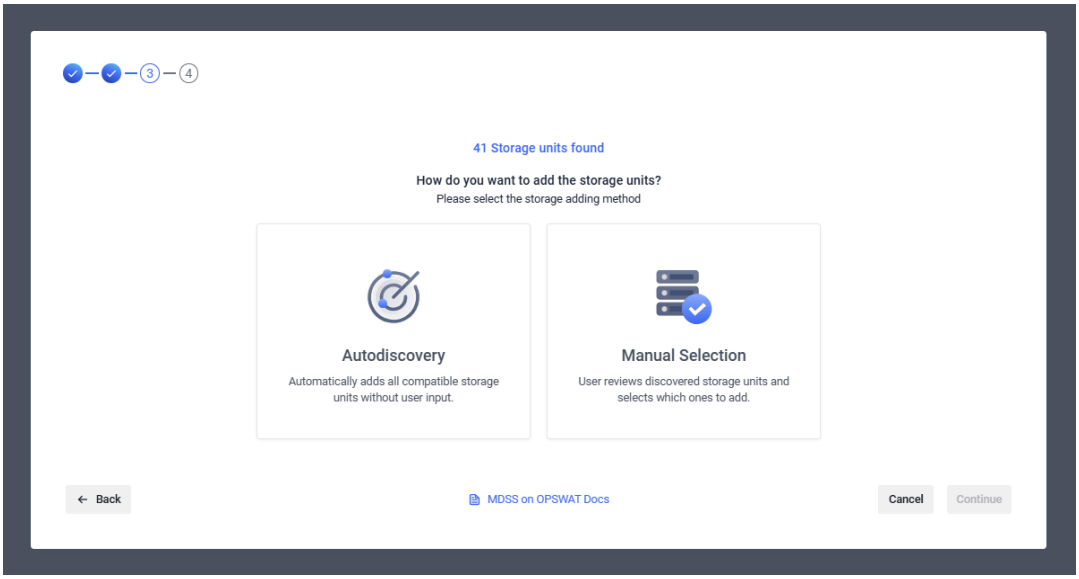
- Navigate to **Storage Units** page
- Click **Add Storage Unit** button
- Select **Google Cloud** Storage Type
- Select **Storage Discovery** and click **Continue**



- Fill out the form with valid GCP credentials and click **Continue**



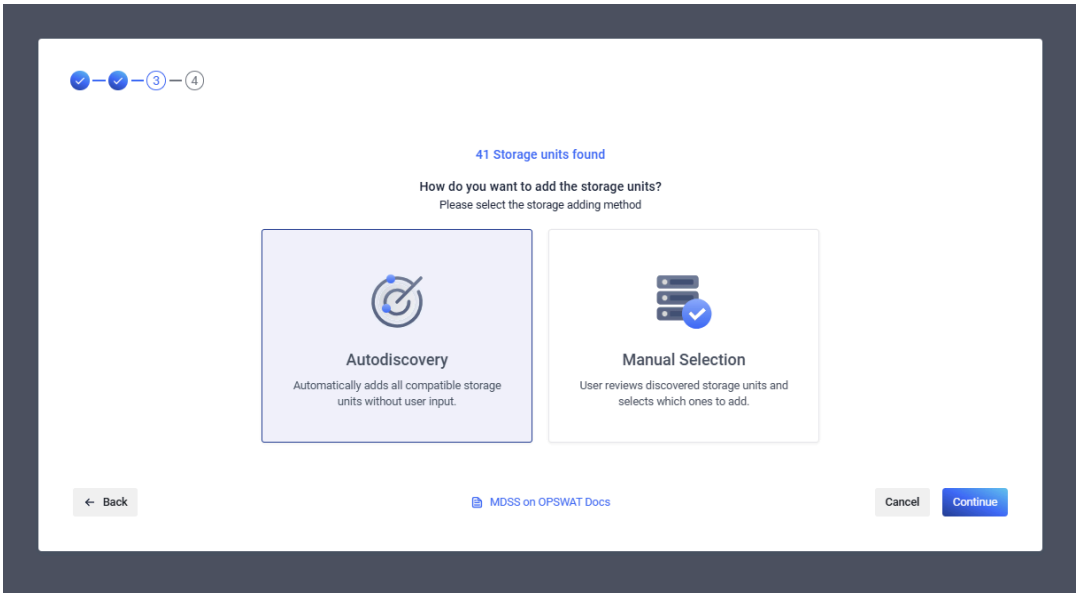
- In the next step, select your integration method. You have two choices: Autodiscovery and Manual Selection.
  - **Autodiscovery** for convenience, this option automatically adds all the buckets MDSS finds
  - **Manual Selection** for precise control, this option lets users choose specific buckets from the discovered list to integrate.

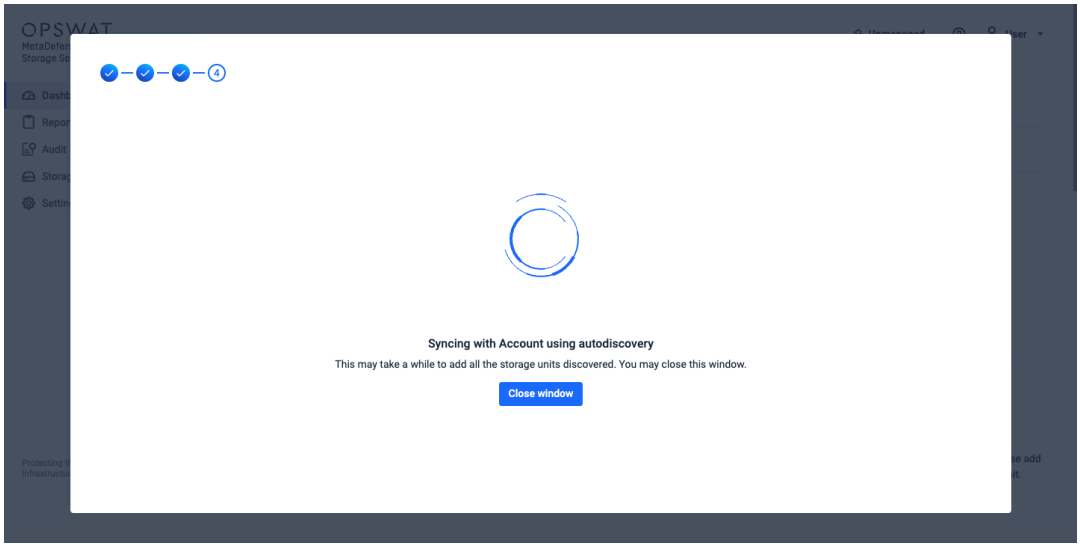


To learn more about each integration type, please consult the Autodiscovery documentation.

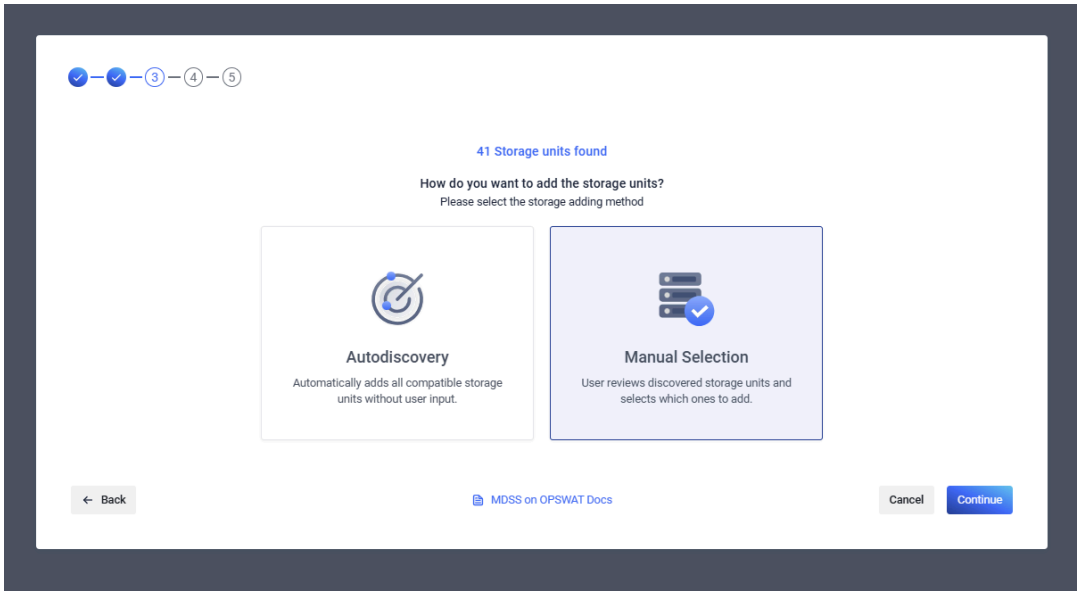
> **NO BUCKETS FOUND**
>
> If there were no buckets found, you will be presented with a third option - **Add Individually** - which will reveal the credentials form to manually add the storage by using the bucket name.

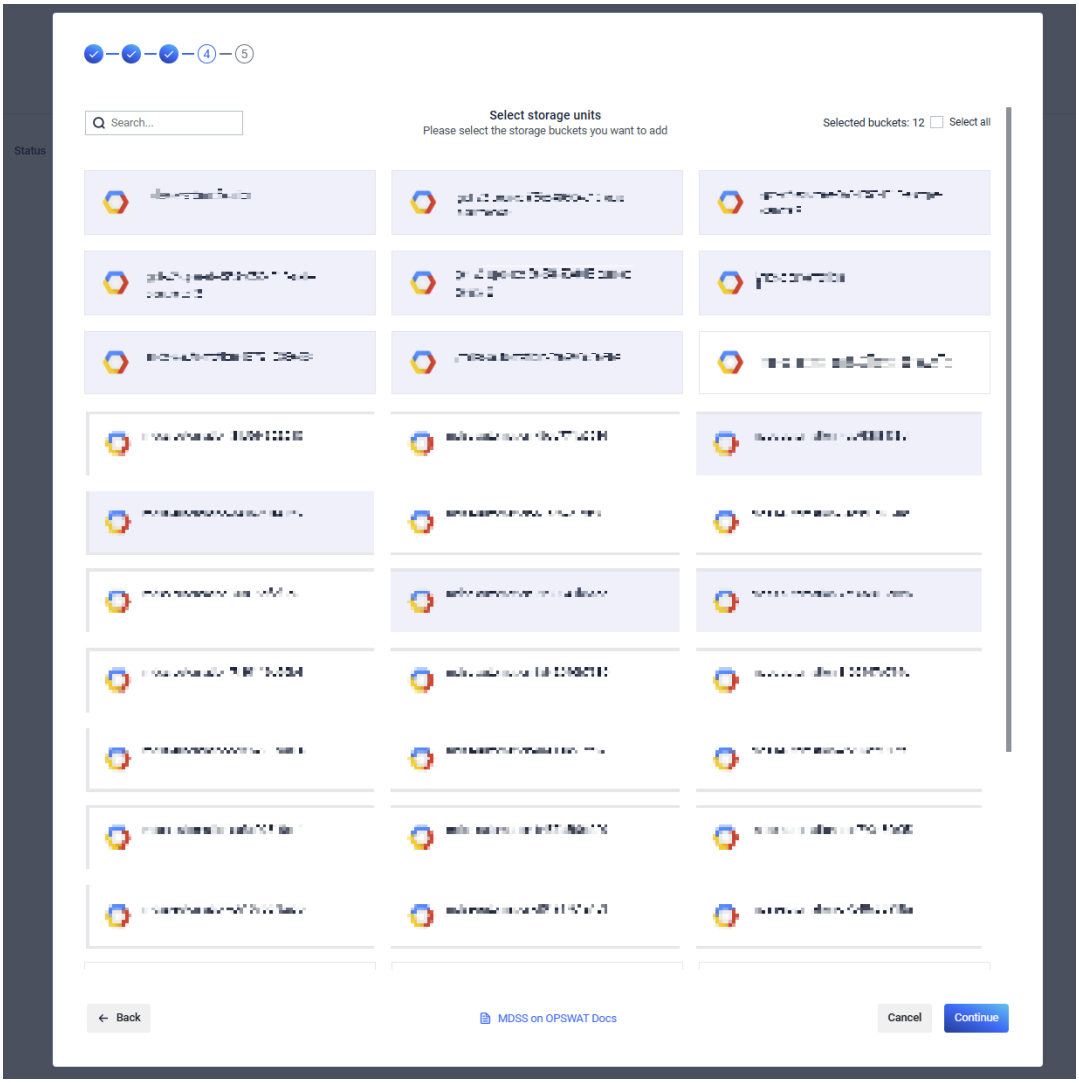
- If selecting **Autodiscovery** option:
  - Click **Continue** and an informative message will be displayed that the autodiscovery process has started in the background. You can safely close the modal and the storages will be added in background to the Storage Units page

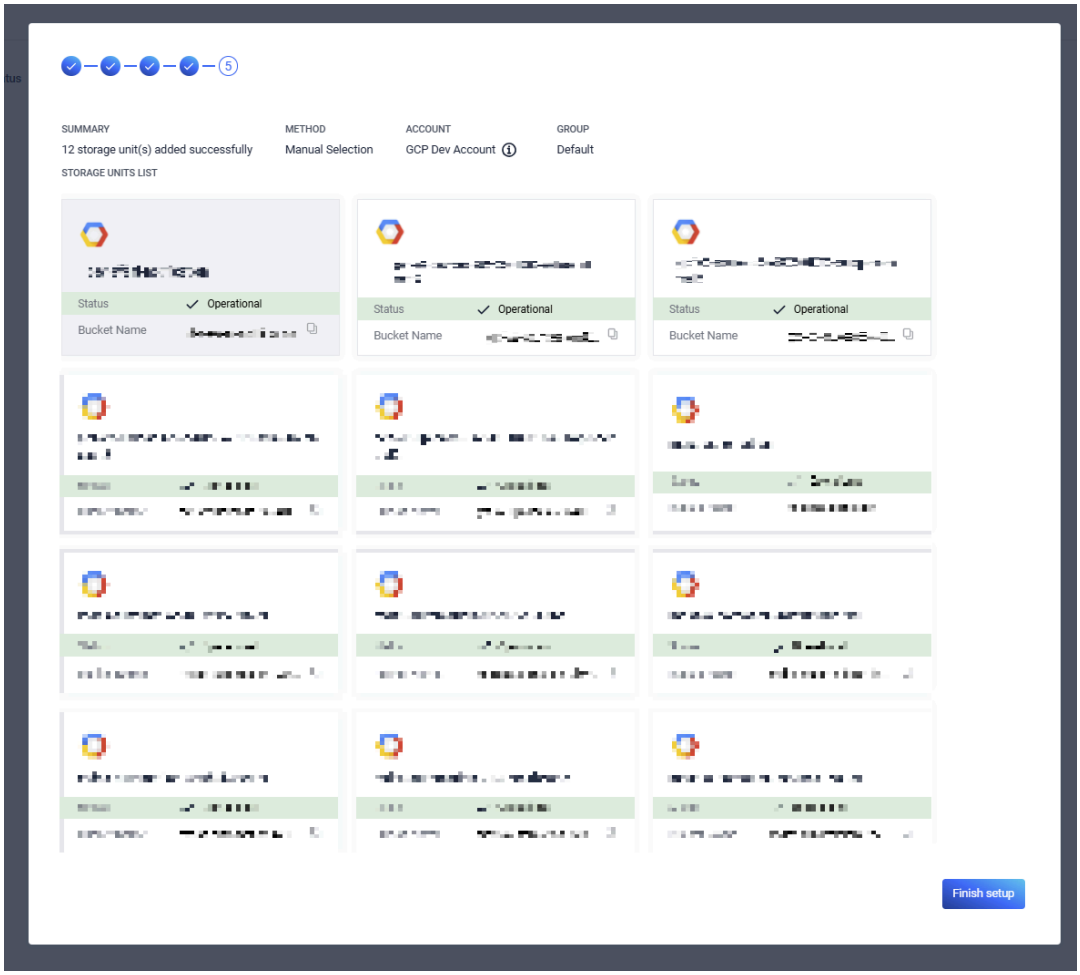




- If selecting **Manual Selection** option:
  - Click **Continue**
  - Select the buckets you want to add from the discovered list
  - Click **Continue**
  - The system will show a syncing message indicating buckets are being added; You can choose to stay on this page in order to see the storages that were successfully added and also to see if there were any errors while trying to add specific storages.



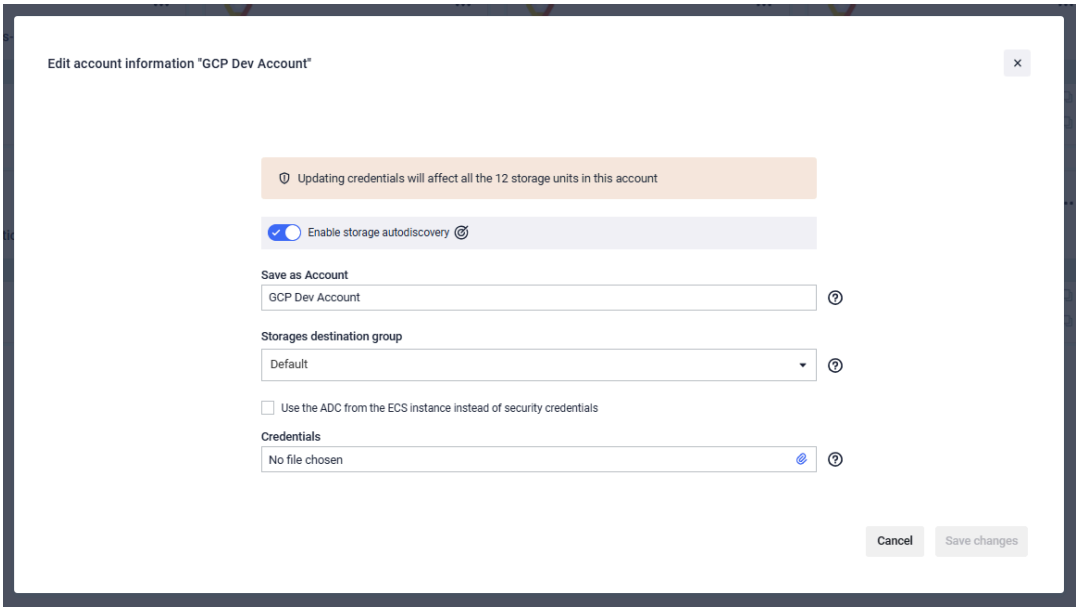

Status
Search...
Select storage units
Please select the storage buckets you want to add
Selected buckets: 12
Select all
Back
MDSS on OPSWAT Docs
Cancel
Continue



> **ERROR ADDING A STORAGE THAT WAS SELECTED DURING MANUAL SELECTION**
>
> In case there was an error while trying to add your storage, you will see the error message in the Storage card while hovering over the (i) icon.

Method 2: Enable Autodiscovery for an Existing Account

- Navigate to **Storage Units** page
- Identify a storage that's using the account you want to start autodiscovery for
- Click on the 3-dots button from the storage's card and select **Manage Storage Unit**
- From the top toggle, select **Change account info**
- Turn on autodiscovery by toggling the **Enable storage autodiscovery** switch


Edit account information "GCP Dev Account"
Updating credentials will affect all the 12 storage units in this account
Enable storage autodiscovery
Save as Account
GCP Dev Account
Storages destination group
Default
Use the ADC from the ECS instance instead of security credentials
Credentials
No file chosen
Cancel
Save changes

Add an OPSWAT MFT Storage

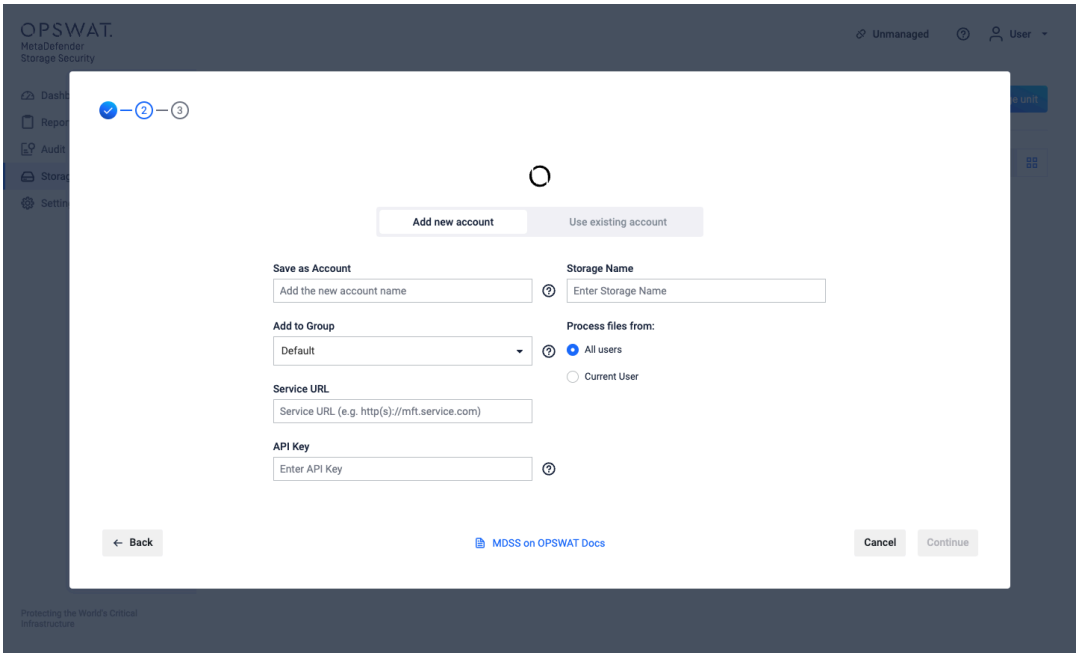
This guide outlines the necessary steps to integrate an OPSWAT Managed File Transfer (MFT) storage solution with your OPSWAT MetaDefender Storage Security (MDSS) instance.

> **LIMITATION**
>
> The MFT integration does not currently support the “Shared Space” feature within Custom Groups. Consequently, while files in a Custom Group’s Shared Space will be discovered during a scan using the “All users” storage option, any attempts to apply remediation actions to these files will fail.

1. Prerequisites

Before you begin adding an MFT storage unit in MDSS, make sure you have the following:

- an **MFT Service URL** - this is the base web address used to access your OPSWAT MFT provider
- an **API Key** required for MDSS to authenticate and interact with your MFT service
- You will need **administrator privileges** for both your MFT dashboard and your MDSS web page.



2. Obtaining the Service URL

The MFT Service URL is the primary address for your MFT provider.

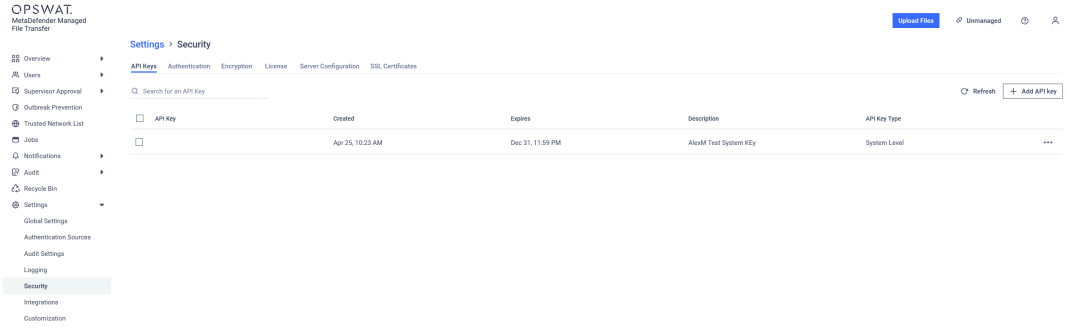
- Determine the complete base URL where your MFT service is hosted.

- Make sure the URL includes the correct protocol, either `http://` or `https://`.
  - Example: `https://mft.yourcompany.com` or `http://mft.internal.net`

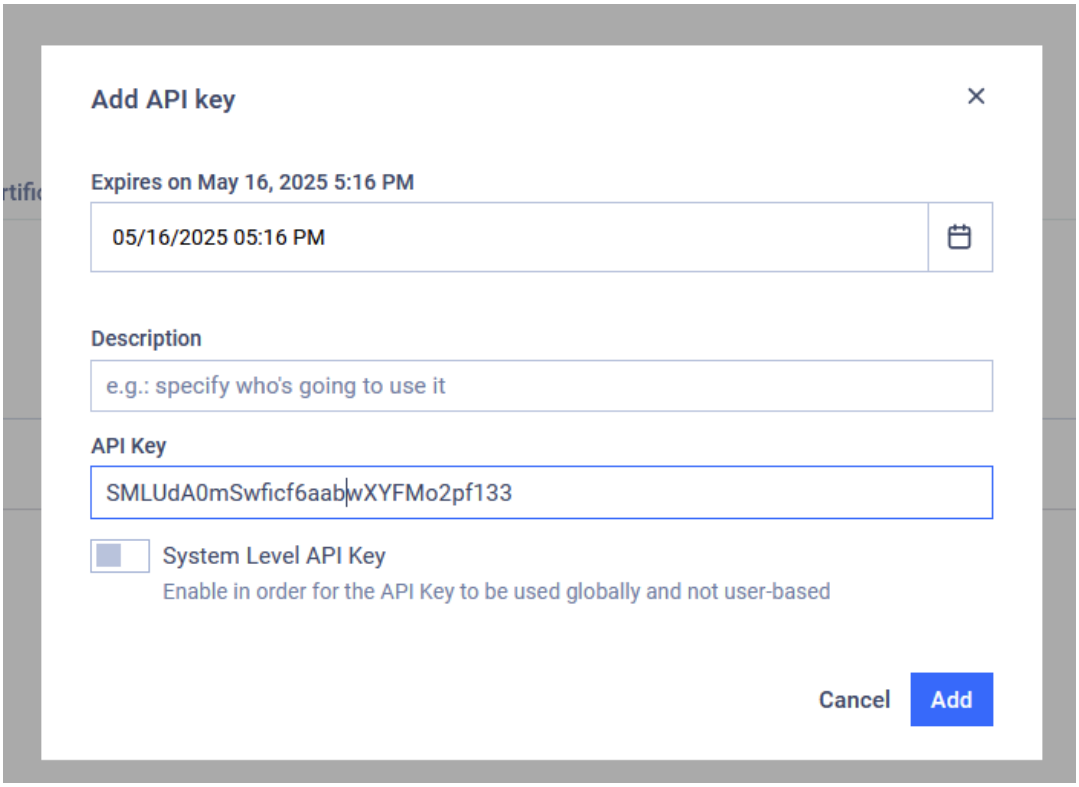
3. Generating Your MFT API Key

An API key is essential for secure communication between MDSS and your MFT service.

- Log in to your MFT dashboard with administrator credentials and navigate to the **Settings** page.
- Within the Settings menu, find and select the **Security** section. This is often located in a side navigation panel.
- Within the Security section, select the **API Keys** tab.



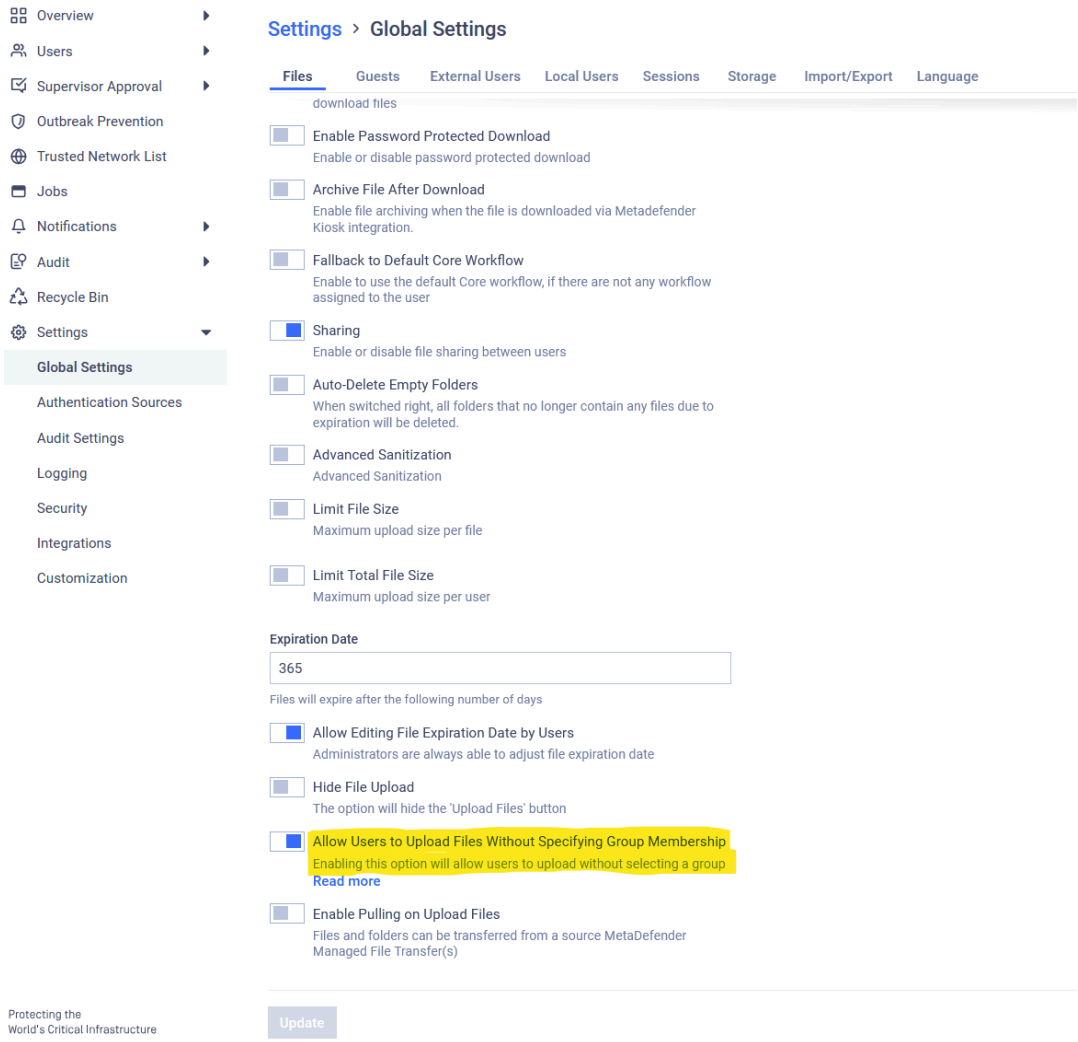
- Click on the **Add API key** button (or a similarly named option like “Generate New Key”).
- Set an appropriate expiration date for the API key to enhance security. Consider your organization’s security policies.
- Once generated, the API key will be displayed. **Immediately and securely copy and store this key.** For security reasons, treat this key like a password.



4. Configuring MFT File Upload Settings

To ensure MDSS can successfully upload files, a specific MFT setting needs to be enabled. This allows MDSS to upload files on behalf of users, even if those users are part of a group and the group membership isn't explicitly specified during the upload.

- As an administrator, navigate to the **Settings** page on your MFT dashboard
- Under the **Global Settings** section, locate and select the **Files** tab
- Make sure that the option labeled **"Allow Users to Upload Files Without Specifying Group Membership"** is **checked (enabled)**
- If you've made any modifications to this setting, ensure you save them



5. Adding the MFT Storage Unit in MDSS

With the MFT Service URL and API key obtained, and the necessary MFT setting configured, you can now add the MFT storage to MDSS. [**Note**: The latest supported version of MFT Storage is **3.9.4**]

- Log in to your MDSS web interface.
- Go to the **Storage Units** page. This is typically found in the main navigation menu.
- Click on the **"Add storage unit"** button.
- From the available storage unit types, choose **"OPSWAT MFT"**
- Fill in the required fields in the form, which will include:
  - **MFT Service URL** - enter the URL obtained in Step 2.
  - **API Key** - enter the API key generated and saved in Step 3.
  - Complete any other specific configuration options presented in the MDSS form for MFT integration.

- Save the configuration. It is highly recommended to test the integration by uploading or scanning a file to ensure the MFT storage is working correctly with MDSS.

> **IMPORTANT**
>
> MDSS will not discover or process files that OPSWAT MFT has already blocked and made unavailable for download.

Add an NFS Storage

Network File System (NFS) is a popular distributed file system protocol that allows a user on a client computer to access files over a network in a manner similar to how local storage is accessed. This document guides you through the process of integrating NFS storage with MetaDefender Storage Security.

1. Understanding NFS Server and Client

In a NFS setup, there are two primary components:

1. **NFS Server**: This is the machine where your files are stored. It must be configured to share files using the NFS protocol.
2. **NFS Client**: This is the machine where MetaDefender Storage Security is installed. It accesses the files stored on the NFS Server.

2. Setting up the NFS Server machine

Please make sure your files are shared via NFS protocol.

To enable remediations capabilities of MetaDefender Storage Security (sanitization, file moving / deleting), we need to have write access to your shared folder. To allow write access, please choose the appropriate configuration for your server. More details in this article.

The next steps are tailored to your deployment type, please choose yours:

- Windows deployment
- Linux deployment

> **Info**
>
> **Symlink Support:** MetaDefender Storage Security is able to follow all types of symbolic links (symlinks) and process the files they point to when integrating with NFS storage on both Linux and Windows deployments. This includes:
>
> - **Soft links (symbolic links)**
> - **Hard links**
> - **Junction points (on Windows)**
>
> For more details on this functionality, follow this link.

[Linux] How to add an NFS storage unit

> **Info**
>
> For steps 1 and 2, please see this page

3. Setting up the NFS Client machine

Before integrating NFS storage with MetaDefender Storage Security, a mount needs to be created from the NFS Client machine to the NFS Server. Follow these steps **on the NFS Client machine**:

1. Install NFS:
   - For Debian-based distributions, install `nfs-common`.
   - For Fedora-based distributions, install `nfs-utils`.
   - Our product is not bound to a specific NFS version. It should work as expected with the version provided by the above package.
2. Prepare the Mount Directory:
   - The default directory for all mounts is `/mnt/mdss/nfs`. Within this directory, create a new folder, for example, `company-files`, where the NFS mount will be performed

> **Info**
>
> /mnt/mdss/nfs is the default mount directory. This can be changed a custom location by setting *NFS_MOUNT_LOCATION=/path/to/your/location* in customer.env. Information on how to modify customer.env: Custom configuration

All new files and folders created by MetaDefender Storage Security (during Sanitization, Remediations) will adopt the same read, write and execute permissions as the parent directory. This means you need to set the appropriate permissions to the `company-files` folder in order new items to be accessible for the desired audience.

1. Perform the NFS Mount:
   - Execute the following command: **sudo mount -t nfs -o rw,hard,intr,nolock {nfs-server-ip}:/srv/company-shared-files /mnt/mdss/nfs/company-shared-files/**
   - This command mounts the shared files from the NFS Server to the `company-files` directory on the NFS Client.
   - It is required the `mount`command to have the `nolock` flag as some older NFS servers are locking the file when opened by another application. Apart from `nolock` , we do not require any specific flags. As long as the mount command is working as expected and we have permissions to the mount directory, should be enough. READ

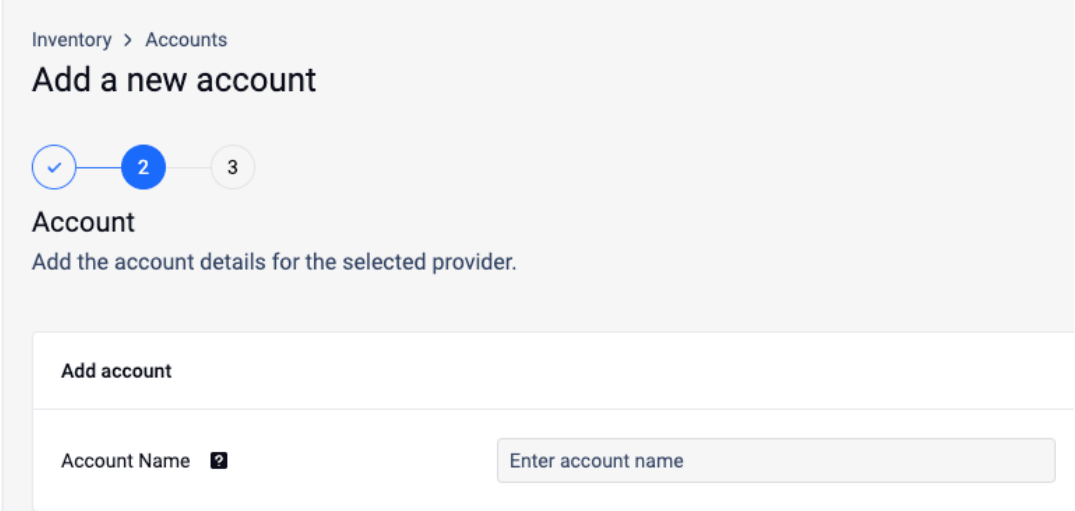
permissions are required for scanning, WRITE permissions are required for remediation operations that implies writing to the storage.

2. Ensure Persistent Mounting:
   - To maintain the mount across reboots, add the following entry to the `/etc/fstab` file: `{nfs_server_ip}:/srv/company-shared-files /mnt/mdss/nfs/company-files nfs rw,hard,intr,nolock 0 0`
   - Without this step, the mount will be lost when the NFS Client machine is restarted.

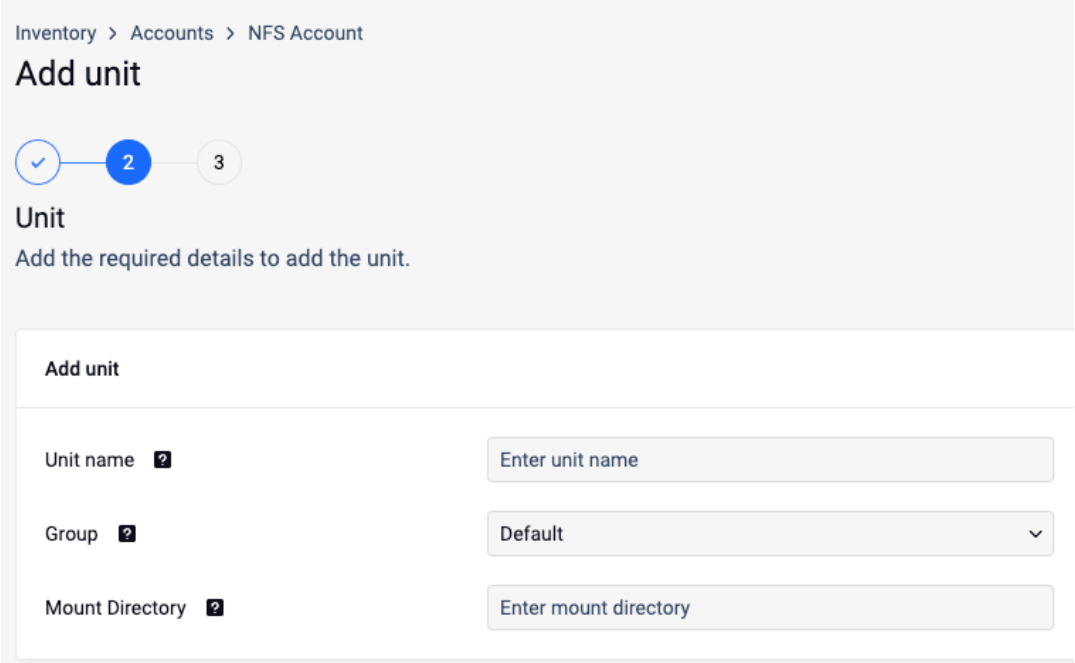
4. Adding an NFS storage in MDSS

In order to integrate NFS with MetaDefender Storage Security, please follow these steps:

1. As NFS is not using any credentials, you can have only one NFS account in MDSS. If you already have one, please go to step 4
2. From the left side menu, navigate to **Inventory,** click on **Add account** and choose **NFS**.
3. Give your account a name so you can easily identify it later



4. From the left side menu, navigate to **Inventory,** click on **Add unit** and choose the previously created account.



5. Give your unit an unique name so you can easily identify it later
6. Assign your unit to a Group
7. Input the mount directory where your NFS shared files are mounted on the MetaDefender Storage Security machine. For instance, if your files are mounted at `/mnt/mdss/nfs/company-files`, simply enter `company-files` in the text box.
8. Click **Next** in order to finish the process.

> **Warning**
>
> Absolute paths (e.g. `/home`) are not functional in versions prior to 4.4.0. Paths configured this way must be manually reconfigured using relative paths — there is no automatic migration.
>
> Starting in 4.4.0, path normalization (`/home` → `home`) is supported for newly created storage.

5. Additional NFS Configuration

NFS offers a wide range of configurations to suit different needs. For more detailed information on NFS configurations, please refer to the following resources based on your operating system:

- NFS Server and NFS Client configuration on Fedora
- NFS Server and NFS Client configuration on Ubuntu

—published

> **Info**
>
> For steps 1 and 2, please see this page

3. Setting up the NFS Client machine

Before integrating NFS storage with MetaDefender Storage Security, a mount needs to be created from the NFS Client machine to the NFS Server. Follow these steps **on the NFS Client machine**:

1. Install NFS:
   - For Debian-based distributions, install `nfs-common`.
   - For Fedora-based distributions, install `nfs-utils`.
   - Our product is not bound to a specific NFS version. It should work as expected with the version provided by the above package.
2. Prepare the Mount Directory:
   - The default directory for all mounts is `/mnt/mdss/nfs`. Within this directory, create a new folder, for example, `company-files`, where the NFS mount will be performed

> **Info**
>
> /mnt/mdss/nfs is the default mount directory. This can be changed a custom location by setting *NFS_MOUNT_LOCATION=/path/to/your/location* in customer.env. Information on how to modify customer.env: Custom configuration

All new files and folders created by MetaDefender Storage Security (during Sanitization, Remediations) will adopt the same read, write and execute permissions as the parent directory. This means you need to set the appropriate permissions to the `company-files` folder in order new items to be accessible for the desired audience.

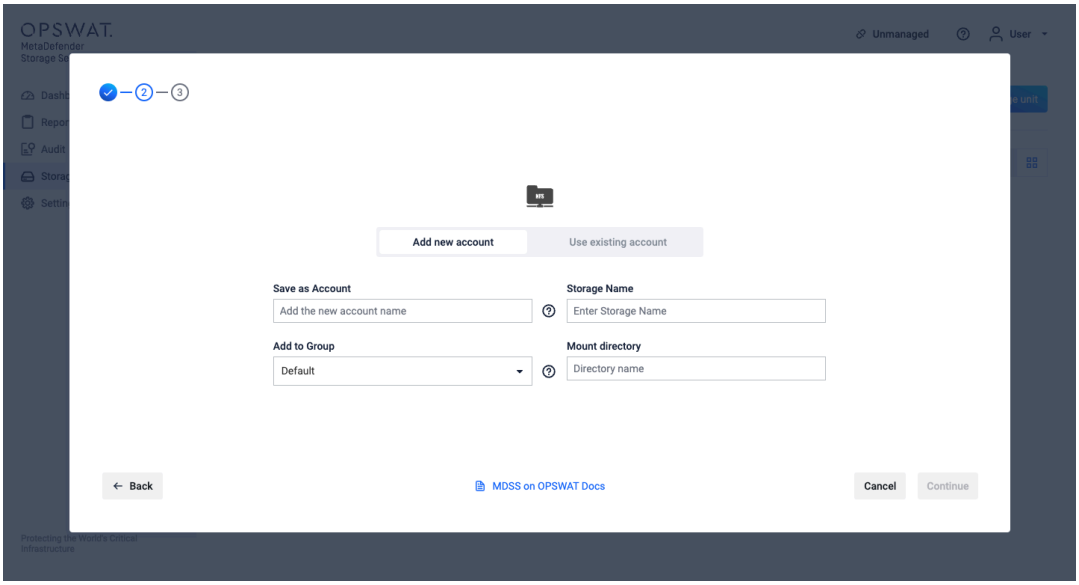
1. Perform the NFS Mount:
   - Execute the following command: **sudo mount -t nfs -o rw,hard,intr,nolock {nfs-server-ip}:/srv/company-shared-files /mnt/mdss/nfs/company-shared-files/**
   - This command mounts the shared files from the NFS Server to the `company-files` directory on the NFS Client.
   - It is required the `mount`command to have the `nolock` flag as some older NFS servers are locking the file when opened by another application. Apart from `nolock` , we do not require any specific flags. As long as the mount command is working as expected and we have permissions to the mount directory, should be enough. READ permissions are required for scanning, WRITE permissions are required for remediation operations that implies writing to the storage.

2. Ensure Persistent Mounting:
    - To maintain the mount across reboots, add the following entry to the `/etc/fstab` file: `{nfs_server_ip}:/srv/company-shared-files /mnt/mdss/nfs/company-files nfs rw,hard,intr,nolock 0 0`
    - Without this step, the mount will be lost when the NFS Client machine is restarted.

4. Adding an NFS storage in MDSS

In order to integrate NFS with MetaDefender Storage Security, please follow these steps:

1. From the left side menu, navigate to **Storage units,** click on **Add storage unit** and choose **NFS**



2. Give your account a name so you can easily identify it later
3. Assign a meaningful name to your NFS storage for easy identification later.
4. Input the mount directory where your NFS shared files are mounted on the MetaDefender Storage Security machine. For instance, if your files are mounted at `/mnt/mdss/nfs/company-files`, simply enter `company-files` in the text box.
5. Click **Add** in order to finish the process.

> **Warning**
>
> Absolute paths (e.g. `/home`) are not functional in versions prior to 4.4.0. Paths configured this way must be manually reconfigured using relative paths — there is no automatic migration.
>
> Starting in 4.4.0, path normalization (`/home` → `home`) is supported for newly created storage.

5. Additional NFS Configuration

NFS offers a wide range of configurations to suit different needs. For more detailed information on NFS configurations, please refer to the following resources based on your operating system:

- NFS Server and NFS Client configuration on Fedora
- NFS Server and NFS Client configuration on Ubuntu

[Windows] How to add an NFS storage unit

> **Info**
>
> For steps 1 and 2, please see this page

> **Limitation**
>
> NFS shares originating from **Dell OneFS PowerScale** are incompatible with MDSS deployments on Windows. A Linux-based MDSS deployment is required to scan these shares.
>
> To add NFS share on Linux deployment, please follow this article.

3. Setting up the NFS Client machine

On the same machine where MetaDefender Storage Security is installed, run this powershell command from an admin console:

```
Install-WindowsFeature NFS-Client
```

With the default options, a user has read permissions when mounting an NFS share using the anonymous user. We can give the anonymous user write permissions by changing the UID and GID that it uses to mount the share.

To change the UID and GID we must make a simple change to the Windows registry by performing the following steps:

- Open regedit by typing it in the search box end pressing Enter.
- Browse to `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ClientForNFS\CurrentVersion\Default`.
- Create a new New DWORD (32-bit) Value inside the Default folder named `AnonymousUid` and assign the UID 0

- Create a new New DWORD (32-bit) Value inside the Default folder named `AnonymousGid` and assign the GID 0
- Reboot the machine to apply the changes.

4. Mount the NFS share

The below command needs to be run as NTSYSTEM user because NFS service is running as NTSYSTEM user.

To run terminal as NTSYSTEM, please do the following:

- download and extract PsTools
- Open an Administrator console
- cd to PsTools folder
- run `.\PsExec.exe -i -s cmd.exe`. It will open another terminal as a NTSYSTEM user

In the above-opened terminal, run the following command:

```
mount -o "nolock,sec=sys" {nfs-server-ip}:{nfs-share-location}
{mounted-drive}
```

For example, the NFS share will be mounted in the Y drive:

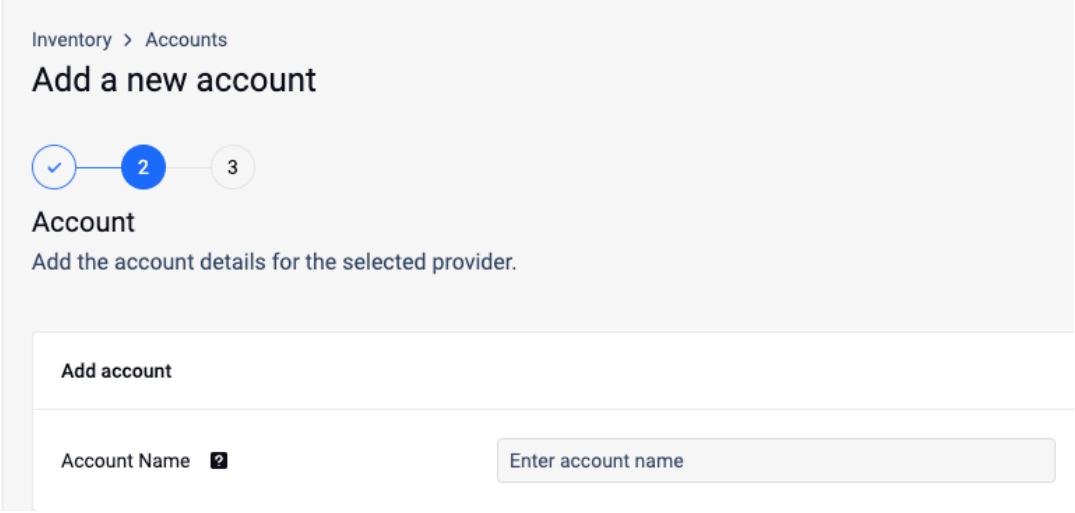
```
mount -o "nolock,sec=sys" 192.168.207.139:/srv/company-public-files/ Y:
```

To make the mount persistent, please follow this article.

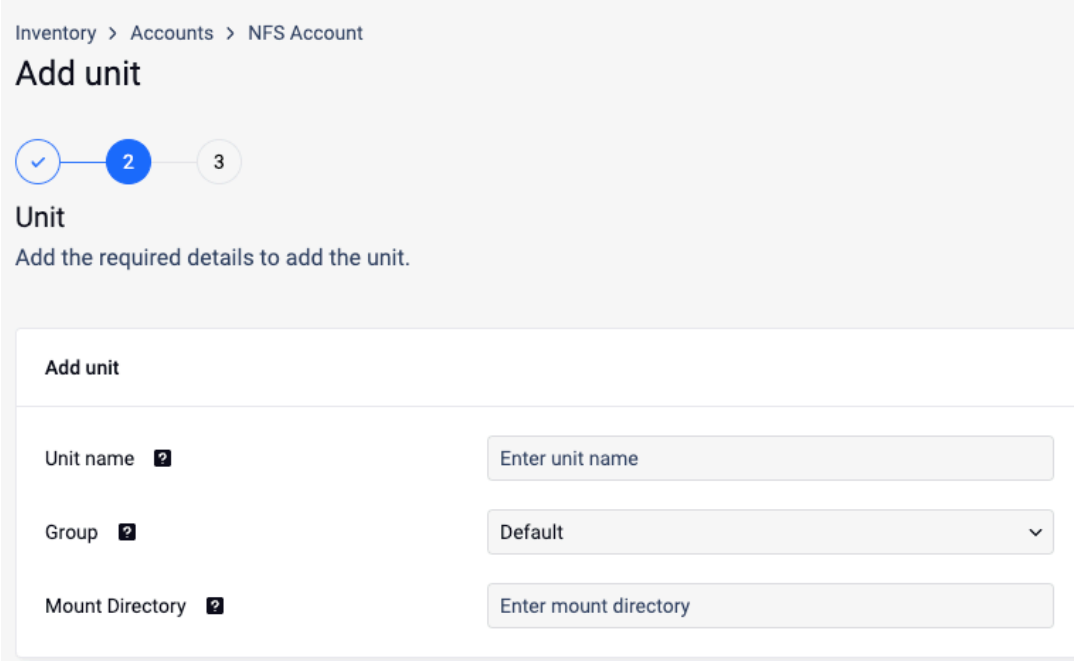
5. Add the NFS share in MDSS UI

In order to integrate NFS with MetaDefender Storage Security, please follow these steps:

1. As NFS is not using any credentials, you can have only one NFS account in MDSS. If you already have one, please go to step 4
2. From the left side menu, navigate to **Inventory,** click on **Add account** and choose **NFS**.
3. Give your account a name so you can easily identify it later



4. From the left side menu, navigate to **Inventory,** click on **Add unit** and choose the previously created account.



5. Give your unit an unique name so you can easily identify it later
6. Assign your unit to a Group
7. Input the mount drive used at step 4. In this example, should be `Y:\`
8. Click **Next** in order to finish the process.

> **Info**
>
> Please follow the Microsoft recommendations for file and directory names.

—published

> **Info**
>
> For steps 1 and 2, please see this page

> **Limitation**
>
> NFS shares originating from **Dell OneFS PowerScale** are incompatible with MDSS deployments on Windows. A Linux-based MDSS deployment is required to scan these shares.
>
> To add NFS share on Linux deployment, please follow this article.

3. Setting up the NFS Client machine

On the same machine where MetaDefender Storage Security is installed, run this powershell command from an admin console:

```
Install-WindowsFeature NFS-Client
```

With the default options, a user has read permissions when mounting an NFS share using the anonymous user. We can give the anonymous user write permissions by changing the UID and GID that it uses to mount the share.

To change the UID and GID we must make a simple change to the Windows registry by performing the following steps:

- Open regedit by typing it in the search box end pressing Enter.
- Browse to `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ClientForNFS\CurrentVersion\Default`.
- Create a new New DWORD (32-bit) Value inside the Default folder named `AnonymousUid` and assign the UID 0
- Create a new New DWORD (32-bit) Value inside the Default folder named `AnonymousGid` and assign the GID 0
- Reboot the machine to apply the changes.

4. Mount the NFS share

The below command needs to be run as NTSYSTEM user because NFS service is running as NTSYSTEM user.

To run terminal as NTSYSTEM, please do the following:

- download and extract PsTools

- Open an Administrator console
- cd to PsTools folder
- run `.\PsExec.exe -i -s cmd.exe`. It will open another terminal as a NTSYSTEM user

In the above-opened terminal, run the following command:

```
mount -o "nolock,sec=sys" {nfs-server-ip}:{nfs-share-location}
{mounted-drive}
```

For example, the NFS share will be mounted in the Y drive:

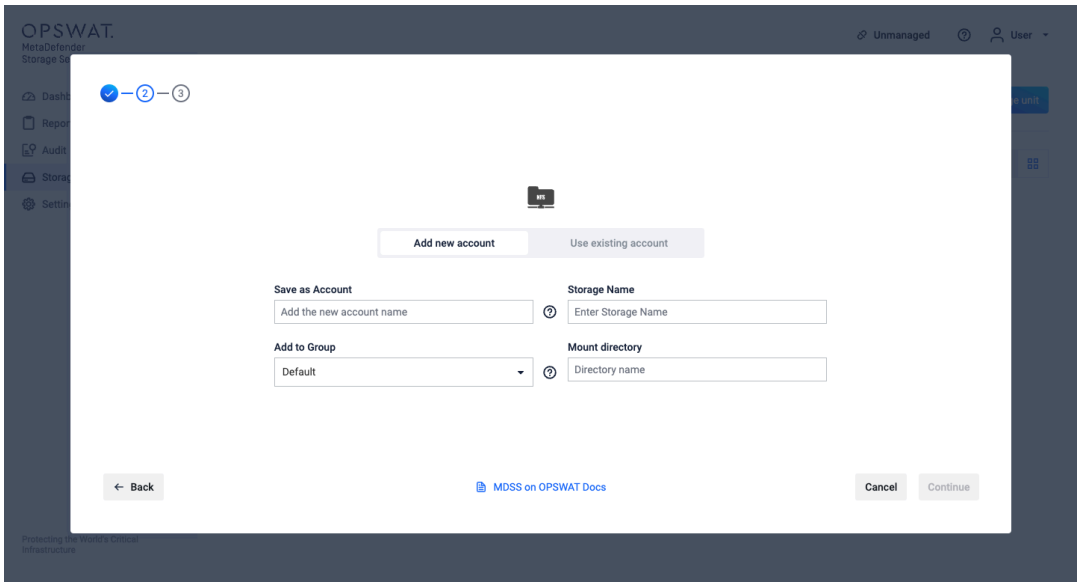
```
mount -o "nolock,sec=sys" 192.168.207.139:/srv/company-public-files/ Y:
```

To make the mount persistent, please follow this article.

5. Add the NFS share in MDSS UI

In order to integrate NFS with MetaDefender Storage Security, please follow these steps:

1. From the left side menu, navigate to **Storage units,** click on **Add storage unit** and choose **NFS**



2. Give your accounts a name so you can easily identify it later
3. Assign a meaningful name to your NFS storage for easy identification later.
4. Input the mount drive used at step 4. In this example, should be `Y:\`
5. Click **Add** in order to finish the process.

> **Info**

> Please follow the Microsoft recommendations for file and directory names.

How to add an Amazon EFS as an NFS storage unit

Prerequisites:

1. an Amazon EFS file storage.
2. a Linux machine where MDSS is installed. This machine needs to be inside AWS and to have access to file storage from 1

Step 1:

On MDSS machine, please install the **cifs-utils** package

Step 2:

On machine where MetaDefender Storage Security is installed, create a new folder at the following path **/mnt/mdss/nfs/{my-new-folder}**

Step 3:

On machine where MetaDefender Storage Security is installed, mount the Amazon EFS file storage in the folder created at step 1. In our testing, we have used the following command, provided by Amazon:

```
sudo mount -t nfs4 -o
nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresv
port fs-42f1fa845a1b23ece.efs.eu-central-1.amazonaws.com:/
/mnt/mdss/nfs/{my-new-folder}
```

Please note the mount command has multiple parameters that can be configured in many ways. Feel free to adapt it to your needs. Any configuration works with our product, as long as the Amazon EFS file storage is mounted successfully and we have, at least, read access to it (to benefit from our remediation capabilities, we will need write access).

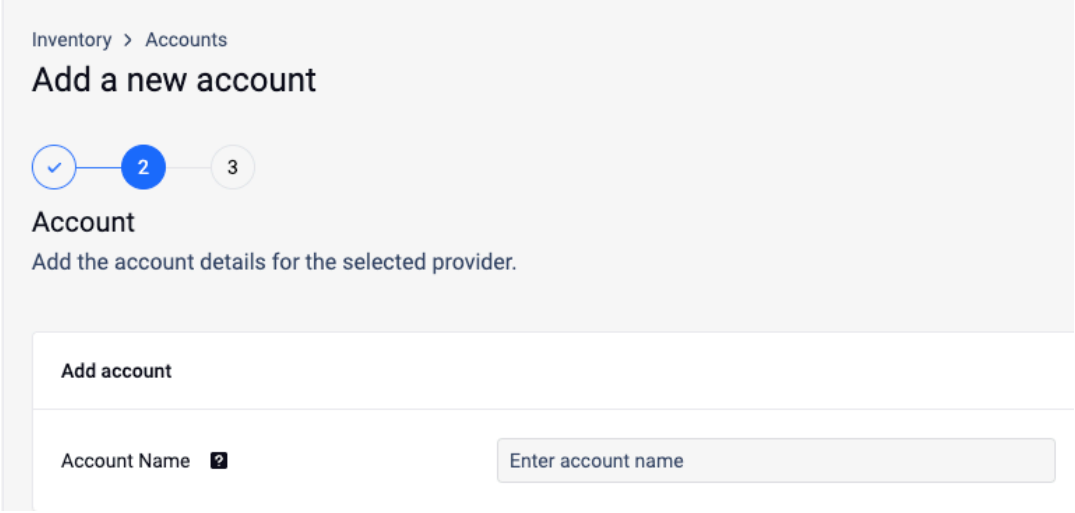
Step 4:

To ensure the mount is persistent, please add it in **/etc/fstab .** Otherwise, the mount will be lost when machine restarts.

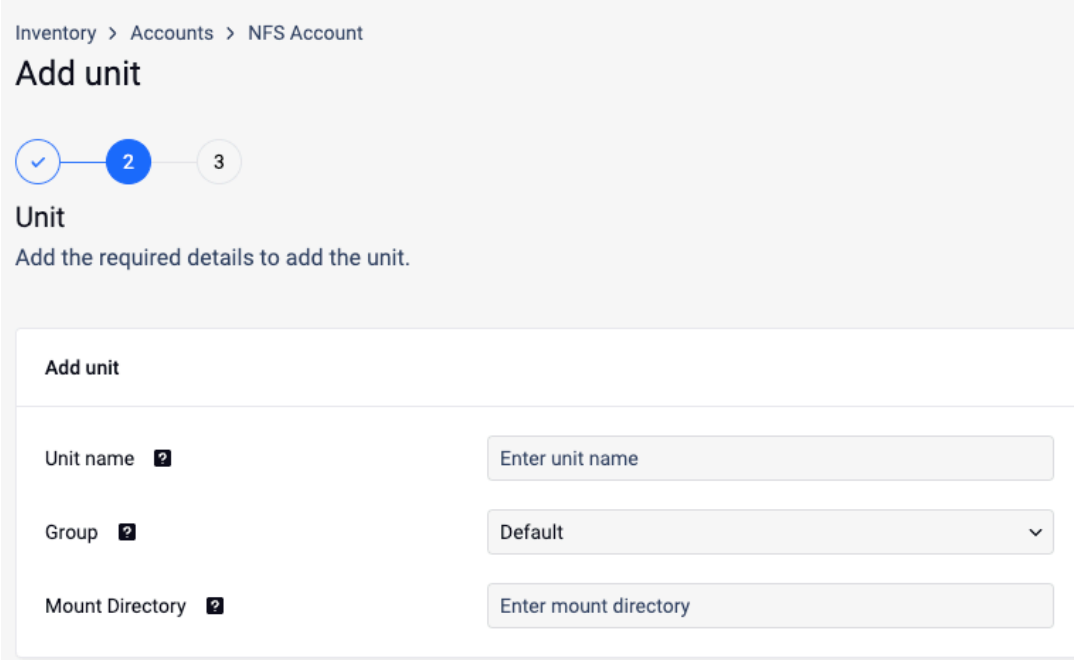
Step 5:

In order to integrate Amazon EFS with MetaDefender Storage Security, please follow these steps:

1. As NFS is not using any credentials, you can have only one NFS account in MDSS. If you already have one, please go to step 4
2. From the left side menu, navigate to **Inventory,** click on **Add account** and choose **NFS**.
3. Give your account a name so you can easily identify it later



4. From the left side menu, navigate to **Inventory,** click on **Add unit** and choose the previously created account.



5. Give your unit an unique name so you can easily identify it later
6. Assign your unit to a Group
7. Input the mount directory where your Amazon EFS shared files are mounted on the MetaDefender Storage Security machine. For instance, if your files are mounted at `/mnt/mdss/nfs/efs`, simply enter `efs` in the text box.
8. Click **Next** in order to finish the process.

—published

Prerequisites:

1. an Amazon EFS file storage.
2. a Linux machine where MDSS is installed. This machine needs to be inside AWS and to have access to file storage from 1

Step 1:

On MDSS machine, please install the **cifs-utils** package

Step 2:

On machine where MetaDefender Storage Security is installed, create a new folder at the following path **/mnt/mdss/nfs/{my-new-folder}**

Step 3:

On machine where MetaDefender Storage Security is installed, mount the Amazon EFS file storage in the folder created at step 1. In our testing, we have used the following command, provided by Amazon:

```
sudo mount -t nfs4 -o
nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresv
port fs-42f1fa845a1b23ece.efs.eu-central-1.amazonaws.com:/
/mnt/mdss/nfs/{my-new-folder}
```

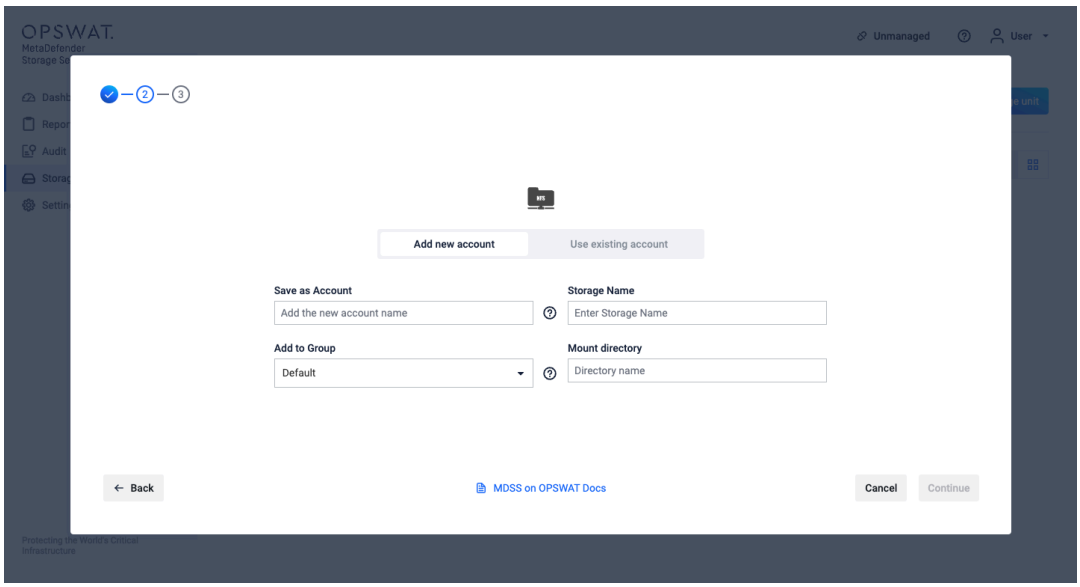
Please note the mount command has multiple parameters that can be configured in many ways. Feel free to adapt it to your needs. Any configuration works with our product, as long as the Amazon EFS file storage is mounted successfully and we have, at least, read access to it (to benefit from our remediation capabilities, we will need write access).

Step 4:

To ensure the mount is persistent, please add it in **/etc/fstab .** Otherwise, the mount will be lost when machine restarts.

Step 5:

From MetaDefender Storage Security user interface, add a NFS storage unit having the **Mount directory** the folder created at step 1.



[Windows] How to Expose an SMB Share as an NFS Storage Unit

> This guide uses the **SMB/CIFS protocol** exclusively for all storage operations. Despite references to "NFS storage" in MDSS terminology, no NFS (Network File System) protocol is involved. The term "NFS storage" refers to MDSS's storage subsystem name that is using the local file system API, not the NFS network protocol. **All connections use SMB/CIFS (Common Internet File System).**

1. Map SMB share as a drive

The below command needs to be run as NTSYSTEM user because our internal NFS service is running as NTSYSTEM user.

To run terminal as NTSYSTEM, please do the following (on the same machine where MetaDefender Storage Security is installed):

- download and extract PsTools
- Open an Administrator console
- cd to PsTools folder
- run `.\PsExec.exe -i -s cmd.exe`. It will open another terminal as a NTSYSTEM user

In the above-opened terminal, run the following command:

```
net use {drive-letter} {smb-share-path} /user:{DOMAIN\username}
{password} /persistent:yes
```

Alternatively, if supported, you can map the drive using QUIC transport:

```
net use {drive-letter} {smb-share-path} /user:{DOMAIN\username}
{password} /persistent:yes /TRANSPORT:QUIC
```

For example, this SMB share is mapped to drive G:

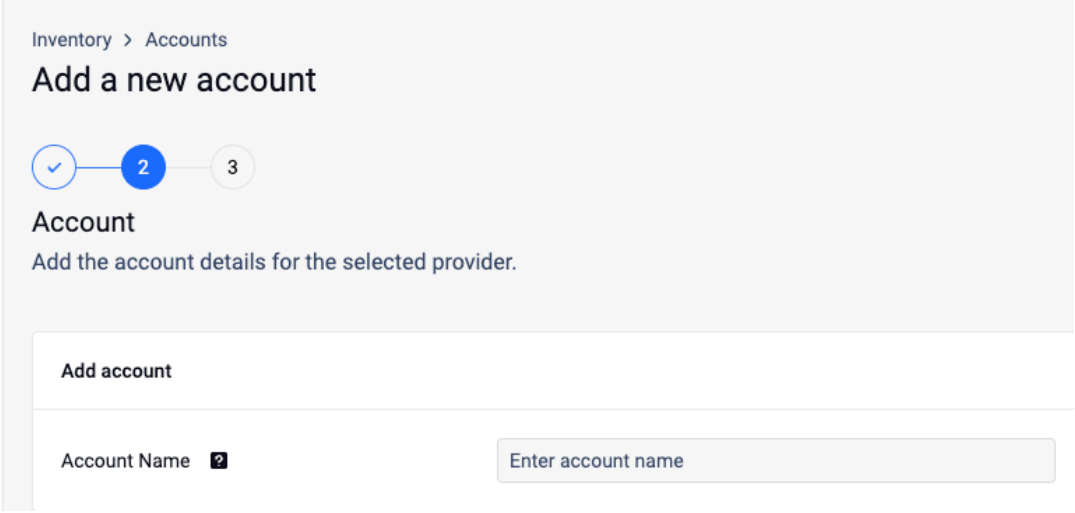
```
net use G: \\152.168.212.101\smb-share /user:OPSWAT\smbuser
smbpassword1234 /persistent:yes
```

> **Warning**
>
> The SMB share mapping configured using this method is temporary and will not survive system reboots. **The mapping will be automatically removed when the machine is restarted.**
>
> **To create a persistent mapping** please refer to this article..

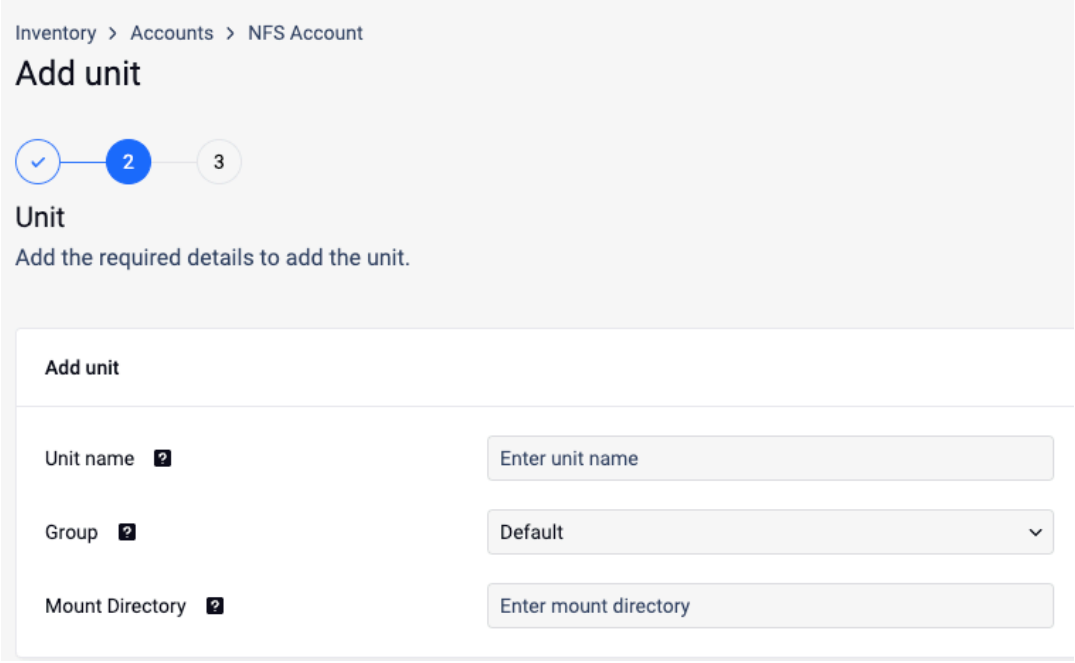
2. Add the SMB share as NFS storage in MDSS UI

In order to integrate SMB share as NFS unit with MetaDefender Storage Security, please follow these steps:

1. As NFS is not using any credentials, you can have only one NFS account in MDSS. If you already have one, please go to step 4
2. From the left side menu, navigate to **Inventory,** click on **Add account** and choose **NFS**.
3. Give your account a name so you can easily identify it later



4. From the left side menu, navigate to **Inventory,** click on **Add unit** and choose the previously created account.



5. Give your unit an unique name so you can easily identify it later
6. Assign your unit to a Group
7. Input the mount drive used at step 1. In this example, should be `G:\`
8. Click **Next** in order to finish the process.

> **Info**
>
> Please follow the Microsoft recommendation for file and directory names.

—published

> This guide uses the **SMB/CIFS protocol** exclusively for all storage operations. Despite references to "NFS storage" in MDSS terminology, no NFS (Network File System) protocol is involved. The term "NFS storage" refers to MDSS's storage subsystem name that is using the local file system API, not the NFS network protocol. **All connections use SMB/CIFS (Common Internet File System).**

1. Map SMB share as a drive

The below command needs to be run as NTSYSTEM user because our internal NFS service is running as NTSYSTEM user.

To run terminal as NTSYSTEM, please do the following (on the same machine where MetaDefender Storage Security is installed):

- download and extract PsTools
- Open an Administrator console
- cd to PsTools folder
- run `.\PsExec.exe -i -s cmd.exe`. It will open another terminal as a NTSYSTEM user

In the above-opened terminal, run the following command:

```
net use {drive-letter} {smb-share-path} /user:{DOMAIN\username}
{password} /persistent:yes
```

Alternatively, if supported, you can map the drive using QUIC transport:

```
net use {drive-letter} {smb-share-path} /user:{DOMAIN\username}
{password} /persistent:yes /TRANSPORT:QUIC
```

For example, this SMB share is mapped to drive G:

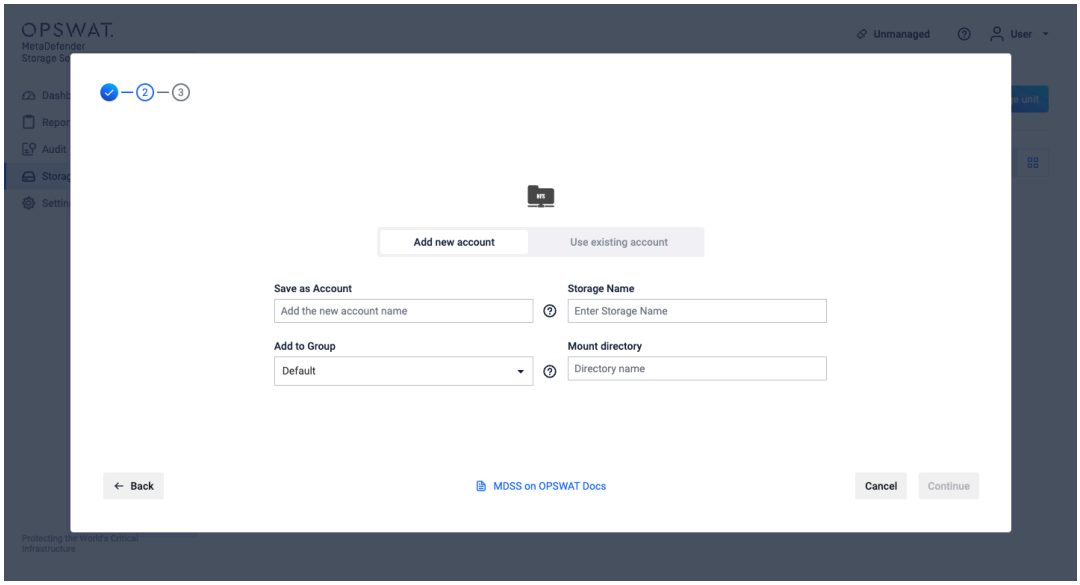
```
net use G: \\152.168.212.101\smb-share /user:OPSWAT\smbuser
smbpassword1234 /persistent:yes
```

> **Warning**
>
> The SMB share mapping configured using this method is temporary and will not survive system reboots. **The mapping will be automatically removed when the machine is restarted.**
>
> **To create a persistent mapping** please refer to this article..

2. Add the SMB share as NFS storage in MDSS UI

In order to integrate NFS with MetaDefender Storage Security, please follow these steps:

1. From the left side menu, navigate to **Storage units** and choose **+ Add Storage Unit** and then select **NFS:**



2. Assign a meaningful name to your NFS storage for easy identification later.
3. Input the mount drive used at step 1. In this example, should be `G:\`
4. Click **Add** in order to finish the process.

> **Info**
>
> Please follow the Microsoft recommendation for file and directory names.

How to Enable NFS scanning on a Kubernetes Cluster

In order to scan an NFS share when having MDSS deployed in a Kubernetes cluster, the share location has to be mounted in the `nfsservice` container as a directory in the following path: `/opt/mdss/nfs/` . For example, the following values file can be applied when deploying MDSS using the helm chart.

```
mdss_components:
  nfsservice:
    extraVolumes:
      nfsTest:
        name: nfs-storage-unit
        nfs:
          server: <NFS_SERVER_IP>
          path: <PATH_EXPORTED_ON_SERVER>
          readOnly: no
    extraVolumeMounts:
      - name: nfs-storage-unit
        mountPath: /opt/mdss/nfs/<MOUNT_DIRECTORY>
        subPath: <SUBPATH_TO_SCAN>
```

This example file can also be found on our GitHub repo for k8s deployments here

After replacing the placeholders, these values can be applied when deploying MDSS:

```
helm install mdss <PATH_TO_HELM_CHART> -f mdss-nfs-example.yml
```

Notes:

- Any storage unit that can be mounted as a Persistent Volume in the container can also have it's contents scanned using the NFS module
- Make sure that the share is mounted with the appropriate permissions, for example, whenever remediations or CDR are configured write permissions are also required

What is User Squashing for Network File System (NFS)

In NFS (Network File System), **user squashing** is a security mechanism that controls how user IDs (UIDs) are mapped between the client and server machines. It helps protect the server from potential security risks when users connect with elevated privileges.

Here's a breakdown of different concepts, containing an example of how the `/etc/exports` file look like:

1. Root Squashing:

- By default, root squashing is enabled. This means when a user with root privileges (UID 0) on the client attempts to access the NFS share, their UID is mapped to a specific user on the server, typically "nobody" (UID 65534). This user typically has limited permissions, preventing the client root user from performing actions that could compromise the server.

2. All Squashing:

- This option maps all client user IDs to a single user on the server, usually “nobody.” This provides minimal permissions to all users accessing the share, regardless of their privileges on the client machine. Use this cautiously as it can severely limit functionality.

```
/shared/data *(rw,sync,nfsvers=4,all_squash)
```

- There is also the option to map all client user IDs to a specific user. You will need to create the dedicated user, set permissions and assign it to a group. Here is an example of how `/etc/exports` file looks

```
/path/to/shared/folder *(rw,sync,root_squash,usermapping=
(to="dedicated_user", squash))
```

3. No_root_squash:

- This option disables user squashing altogether. It allows client users, including root, to retain their original UIDs on the server. This can be risky as it grants potentially harmful permissions to users, especially root. Only use this in trusted environments and with explicit security measures.

```
/shared/data *(rw,sync,nfsvers=4,no_root_squash)
```

You can find more details on the official documentation of the NFS protocol: https://docs.kernel.org/admin-guide/nfs/index.html

Add an NFS with SISL Storage

Simple Information Serialization Language (SISL) is a simple structured text format designed for use in the NCSC Safely Importing Data Pattern. MDSS provides the functionality to wrap and unwrap files with an XOR scrambling technique using the following algorithm pySISL.

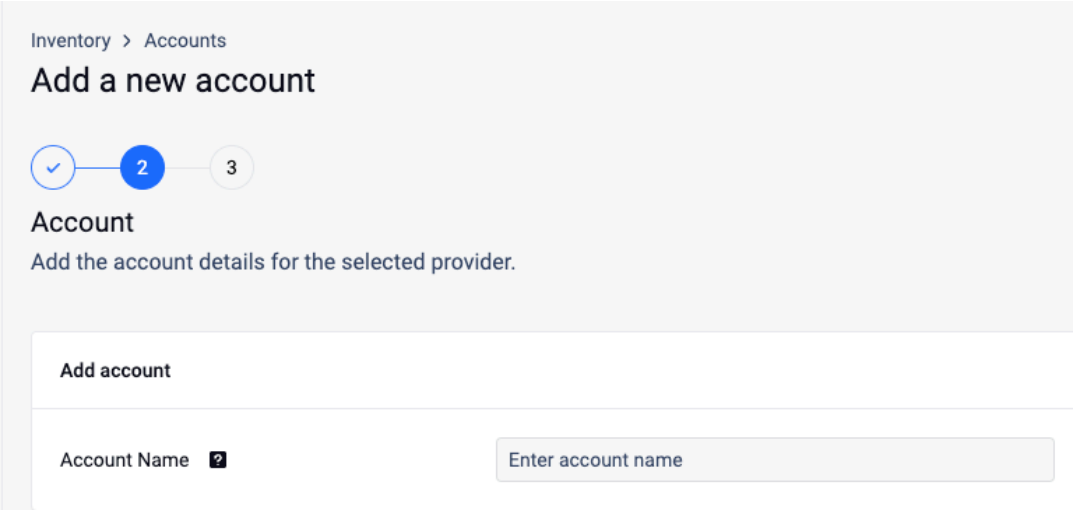
Step 1:

To scan a storage that contains wrapped files, you have to integrate it as an NFS storage unit. Please see this page.

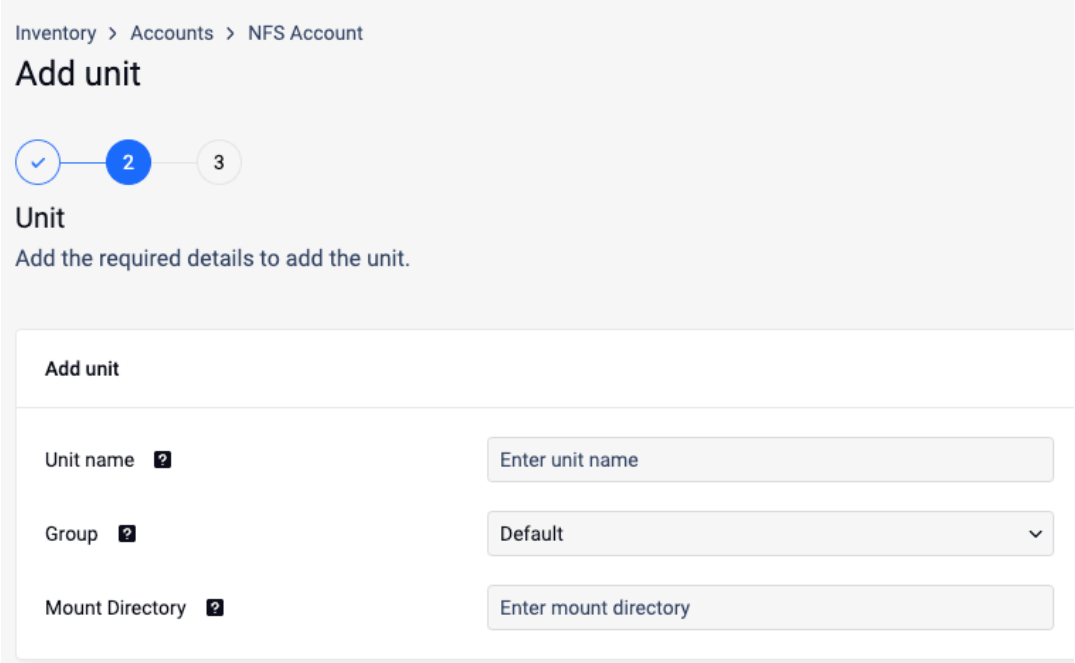
Step 2:

In order to integrate NFS with SSL with MetaDefender Storage Security, please follow these steps:

1. As NFS with SISL is not using any credentials, you can have only one NFS with SISL account in MDSS. If you already have one, please go to step 4
2. From the left side menu, navigate to **Inventory,** click on **Add account** and choose **NFS with SISL**.
3. Give your account a name so you can easily identify it later



4. From the left side menu, navigate to **Inventory,** click on **Add unit** and choose the previously created account.



5. Give your unit an unique name so you can easily identify it later
6. Assign your unit to a Group
7. Input the mount directory to the folder created at Step 1.
8. Click **Next** in order to finish the process.

> **Info**
>
> Remediation behavior is as follows:
>
> - Files moved between NFS with SISL storage units remain unchanged
> - Files moved from NFS with SISL to another storage type (such as Amazon S3) are unwrapped during the move
> - Files moved from another storage type (such as Amazon S3) to NFS with SISL are wrapped during the move

> **Warning**
>
> The wrap/unwrap action is not configurable.

Add an SMB-Compatible Storage

Product Specification Requirements	Version
Service Message Block (SMB) protocol	SMB 3.1.1 (or SMB3) SMB 2.0.2 (or SMB2)

> **Info**
>
> Integration with SMB Compatible Storage is currently accomplished via the Service Message Block (SMB) TCP protocol. Before you begin, you should ensure that this protocol is enabled on your computer.

Please choose your deployment type:

- Add an SMB-Compatible unit in Windows deployments
- Add an SMB-Compatible unit in Linux deployments

How to scan Windows client SMB shares?

> **Info**
>
> Windows client shares are **not officially supported**. This document is intended solely for demonstration, testing, and proof-of-concept (PoC) purposes to help you learn how to scan them. It is not suitable for use in production environments.

Symptoms

When the connection limit is reached, the following error will appear in SMB service logs:

```
No more connections can be made to this remote computer at this time
because the computer has already accepted the maximum number of
connections. (3221225680) STATUS_REQUEST_NOT_ACCEPTED: 0xc00000d0
```

Solution

When SMB shares are configured on a Windows client (Windows 10, Windows 11) there is a limit of connections that the SMB server allows. By default the limit is a total of 20 connections.

The default configuration of MetaDefender Storage Security (MDSS) requires a minimum of 50 connections to ensure optimal performance. However, it is possible to adjust certain

configurations on the MDSS side to accommodate scenarios where fewer connections are necessary.

First, we should check how many connections are used excluding the 50 connections required by MDSS. You can check this using the following command that should be executed on the SMB Server with Administrative privileges

```
Get-SMBSession
```

It will return a list of open sessions connections. Based on the number of connections you can adjust the custom configuration using an environment variable called **SMBSERVICE_SESSIONS_ON_STORAGE** not have more than 20 connections used on the SMB Server.

> **Info**
>
> There are a total of 5 SMB services and each will use a number of **SMBSERVICE__*SESSIONS* ON_STORAGE** equal to 10 which results in 50 connections.
>
> For Windows clients SMB shares, the recommendation is to configure **SMBSERVICE_SESSIONS_ON_STORAGE** to 2 or 3, but it depends of the number of connections already present.

Recommended approach when adding SMB units on Linux deployments

> This article is **applicable only for MetaDefender Storage Security deployed on Linux**. If your deployment is on **Windows**, please follow this article.

For production environments, we recommend using **OS-level SMB/CIFS mounts** instead of application-level connections.

This approach provides:

- Better stability under high load
- Improved file descriptor management
- Enhanced performance
- More reliable connections

> **Success**
>
> Many of our enterprise customers have already migrated to OS-level SMB mounts and are experiencing significantly improved stability and performance in their production environments.

Why We Recommend This Approach

Through extensive testing and production deployments, we've identified challenges with the **3rd-party SMB client library** that we are using when handling:

- **High concurrent workloads**: connection drops intermittently
- **Large file descriptor usage**: the SMB client library may open excessive file descriptors, leading to system resource exhaustion
- **Connection stability**: Network interruptions can cause SMB connections created from the SMB client library to become stale or unresponsive

Technical Background

OS-level mounts leverage the operating system's native **SMB/CIFS client**, which:

- **Handles connection pooling automatically**: The OS manages connection lifecycle and recovery
- **Manages file descriptors more efficiently**: Kernel-level implementation prevents descriptor leaks
- **Provides better fault tolerance**: Built-in retry logic and connection recovery
- **Reduces application-level overhead**: Direct kernel I/O without library abstraction layers

This configuration has been validated across multiple production deployments with varying workloads and is now our recommended best practice for enterprise installations.

Choose Your Platform

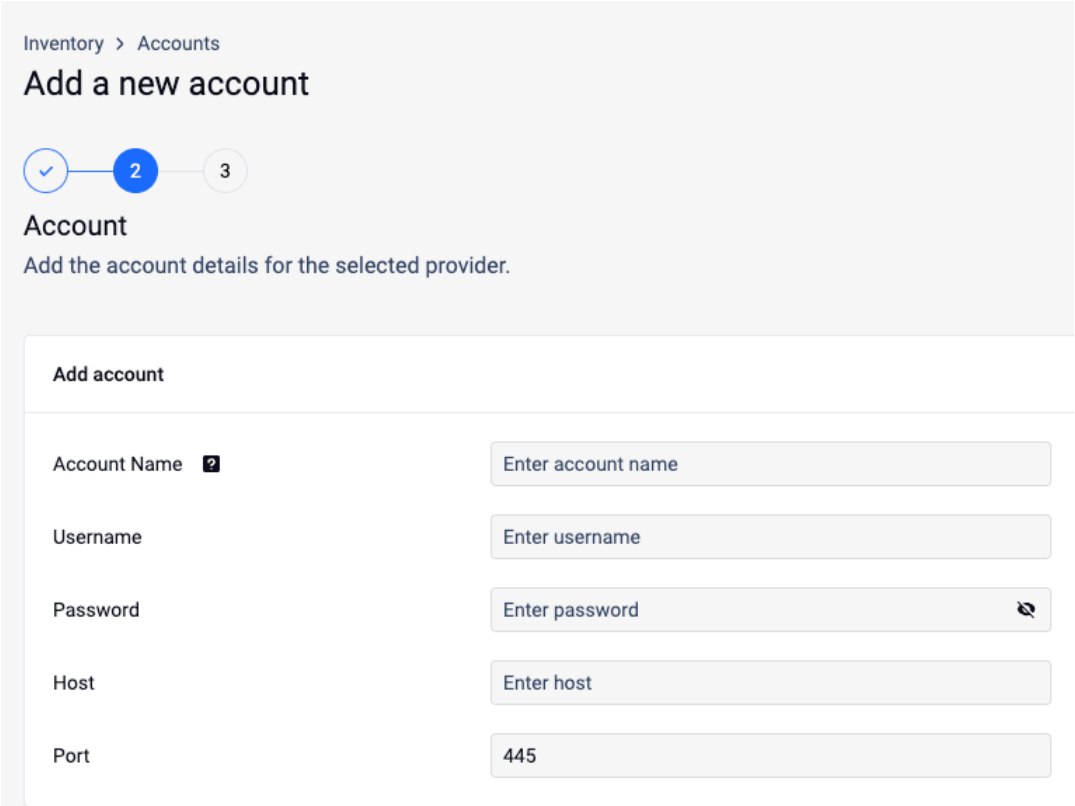
- **Linux Deployment**: [Linux] How to Expose an SMB Share as an NFS Storage Unit

Add an SMB-Compatible unit in Windows deployments

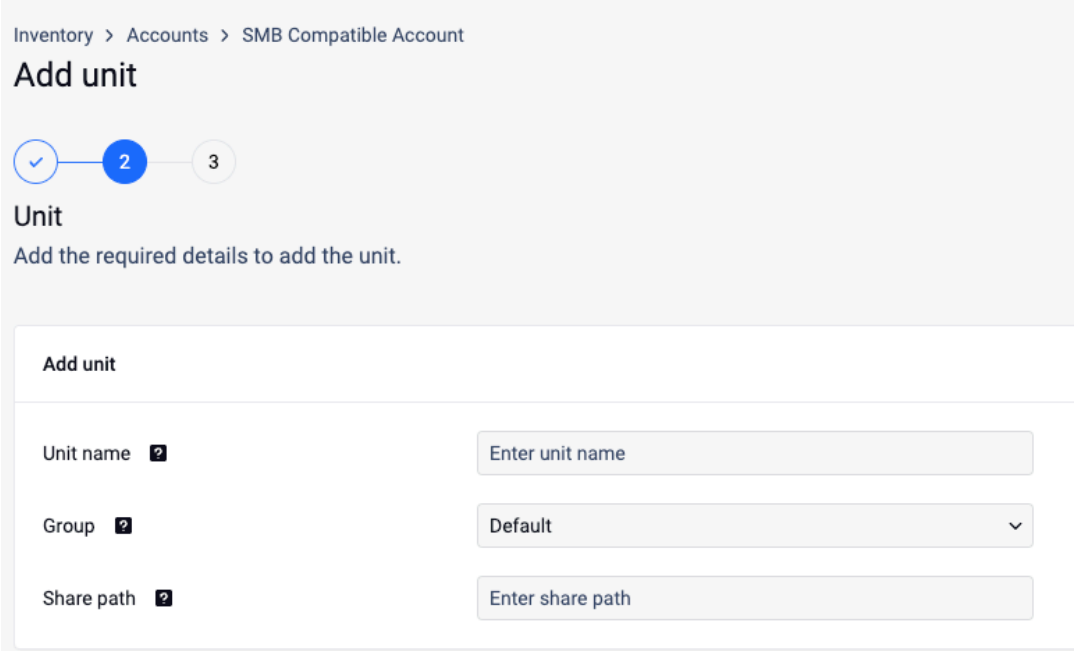
> This article is **applicable only for MetaDefender Storage Security deployed on Windows Server**.
>
> If your MetaDefender Storage Security is deployed on **Linux** based distributions, please follow this article.

In order to integrate SMB Compatible Storage with MetaDefender Storage Security please follow these steps:

1. From the left side menu, navigate to **Inventory**, click on **Add -> Account** -> **SMB Compatible**



2. Give your account a name so you can easily identify it later
3. Enter the name of the user that will be used to access the SMB share
4. Enter the password of the above user.
5. Enter the IP address of the SMB server you wish to connect to.
6. Specify the port number used for the SMB connection, **445** being the default SMB port
7. Click on Next to finish the process.
8. From the left side menu, navigate to **Inventory**, click on **Add -> Unit -> **Choose the previously created account



9. Give your unit a unique name so you can identify it later.
10. Assign your unit to a Group
11. Indicate the specific share path on the SMB server from which you want to access files .
12. Click **Next** in order to finish the process.

> **Info**
>
> To avoid authentication issues the Username should have one of the following formats:
>
> - local users should be .\username (for example: .\Administrator)
> - domain users should be username@domain or domain\username

> **Info**
>
> A Samba file server needs to be enabled in order to connect to a Unix-based system **SharePath.** Since Samba doesn't use the system account password, it needs to be set up using the *sudo smbpasswd -a username* command.

> **Info**
>
> If you use a hostname in the host portion of IPv4/v6 socket address, the program may show a non-deterministic behavior. The socket address will be resolved differently into an actual IPv4/v6 address, depending on the results from DNS

resolution and/or the host configuration. For deterministic behavior use a numeric address in host portion.

Info

Windows client shares have a default configuration of 20 connections in the same time. Our default configuration will require 50 connections. To adjust this SMBSERVICE_SESSIONS_ON_STORAGE should be set to a value lower than 4

Info

Please note that SMB over QUIC is not supported at this time - only traditional SMB over TCP connections are compatible with this integration. See [Windows] How to Expose an SMB Share as an NFS Storage Unit for more details.

Add an SMB-Compatible unit in Linux deployments

This guide uses the **SMB/CIFS protocol** exclusively for all storage operations. Despite references to "NFS storage" in MDSS terminology, no NFS (Network File System) protocol is involved. The term "NFS storage" refers to MDSS's storage subsystem name that is using the local file system API, not the NFS network protocol. **All connections use SMB/CIFS (Common Internet File System).**

This article is **applicable only for MetaDefender Storage Security deployed on Linux distributions**.

If your MetaDefender Storage Security is deployed on **Windows Server**, please follow this article.

Prerequisites

1. A Linux machine where MetaDefender Storage Security is installed (let's call it MDSS machine)
2. An SMB share from a Linux or Windows machine

Step-by-Step Guide

Follow these steps to configure the SMB share as an NFS storage unit in MDSS:

Step 1: Install cifs-utils

On the MDSS machine, you will need the **cifs-utils** package to enable mounting of SMB shares.

Install it using your distribution's package manager.

Step 2: Create new mounting directory

Create a dedicated directory on the MDSS machine where the SMB share will be mounted.

The new directory must be at the following path **/mnt/mdss/nfs/{my-new-folder}** where **{my-new-folder}** is a name you choose for your share.

Step 3: Perform the mount

This step involves preparing credentials and then executing the mount command.

3.1 Create a credentials file containing the SMB server credentials

Create a file, for instance at **/etc/smb-credentials**, to store the SMB server login details. The file should contain:

```
username={username}
password={password}
domain={domain} # optional
```

Replace **{username}, {password}** and [if needed] **{domain}** with the actual credentials for the SMB share.

> **Security Recommendation**
>
> It's recommended to use separate credential files for different shares

3.2 Secure the credentials file

To protect the sensitive information in the credentials file, restrict its permissions and ownership:

- set permissions so only the owner can read and write:

```
sudo chmod 600 /etc/smb-credentials
```

- set ownership to root:

```
sudo chown root:root /etc/smb-credentials
```

3.3 Perform the mount

Execute the mount command to connect the SMB share to the directory you created. The command format is:

```
sudo mount -t cifs //server/share /mnt/mdss/nfs/{my-new-folder} -o
credentials=/etc/smb-
credentials,uid=0,gid=0,file_mode=0655,dir_mode=0755
```

- replace `//server/share` with the actual path to your SMB share
- replace `/mnt/mdss/nfs/{my-new-folder}` with the mount directory you created.
- ensure the path to your credentials file is correct

> **Info**
>
> The mount command offers various configurable parameters. You can adapt these to your specific requirements.
>
> MDSS will work with any configuration as long as the SMB share is mounted successfully and MDSS has at least read access. For remediation capabilities, write access will be necessary.

Step 4: Ensure mount is persistent

To make sure the SMB share automatically mounts after the MDSS machine restarts, add an entry to the `/etc/fstab` file. Without this, the mount will be lost upon reboot.

An example entry in `/etc/fstab` might look like this (adapt it to your specific paths and options):

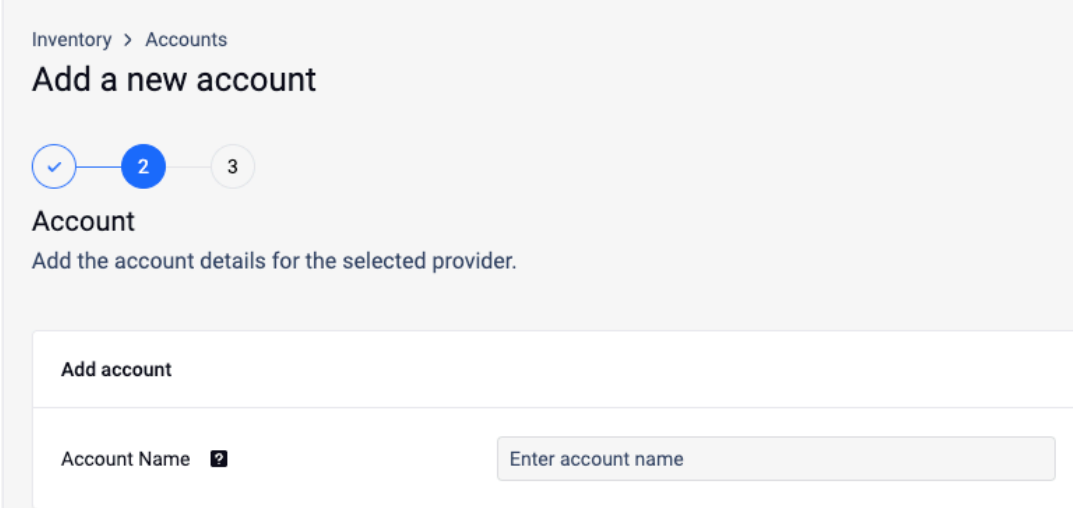
```
//server/share   /mnt/mdss/nfs/{my-new-folder}   cifs
credentials=/etc/smb-
credentials,uid=0,gid=0,file_mode=0655,dir_mode=0755   0   0
```

You may need to adjust options like **uid** and **gid** to ensure proper file permissions for MDSS.

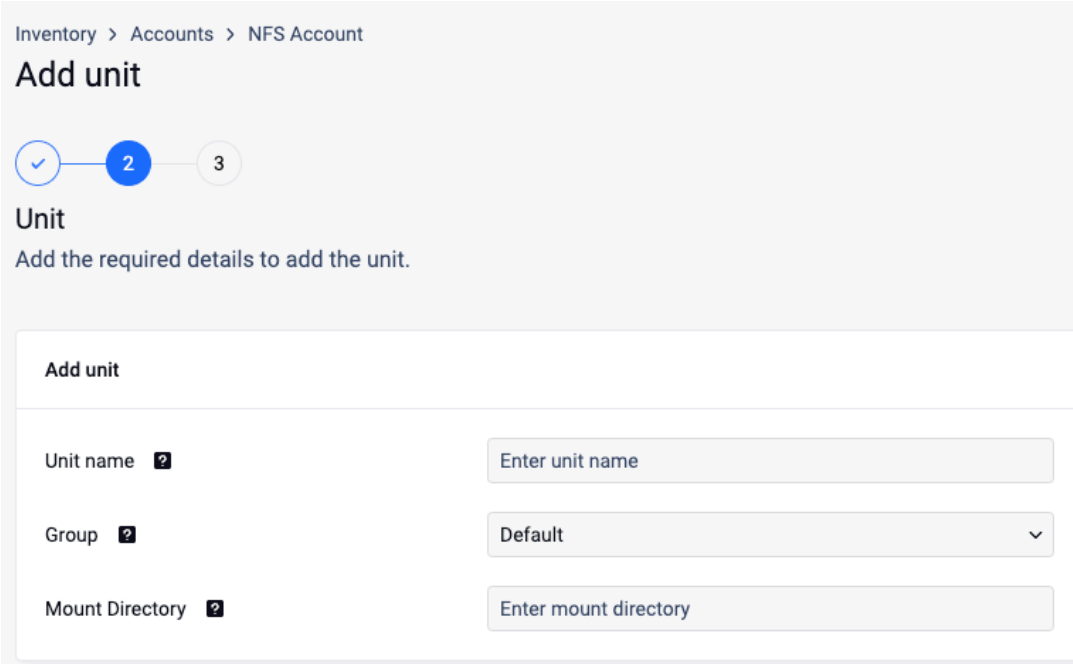
Step 5: Add the mounted directory in MDSS

In order to integrate SMB share as NFS unit with MetaDefender Storage Security, please follow these steps:

1. As NFS is not using any credentials, you can have only one NFS account in MDSS. If you already have one, please go to step 4
2. From the left side menu, navigate to **Inventory,** click on **Add account** and choose **NFS**.
3. Give your account a name so you can easily identify it later



4. From the left side menu, navigate to **Inventory,** click on **Add unit** and choose the previously created account.



5. Give your unit an unique name so you can easily identify it later
6. Assign your unit to a Group
7. Specify the **Mount directory** as the folder you created and used in Step 2 [**{my-new-folder}**]
8. Click **Next** in order to finish the process.

Info

To avoid authentication issues the Username should have one of the following formats:

- local users should be .\username (for example: .\Administrator)
- domain users should be username@domain or domain\username

Info

A Samba file server needs to be enabled in order to connect to a Unix-based system **SharePath.** Since Samba doesn't use the system account password, it needs to be set up using the *sudo smbpasswd -a username* command.

Info

If you use a hostname in the host portion of IPv4/v6 socket address, the program may show a non-deterministic behavior. The socket address will be resolved differently into an actual IPv4/v6 address, depending on the results from DNS resolution and/or the host configuration. For deterministic behavior use a numeric address in host portion.

Info

Windows client shares have a default configuration of 20 connections in the same time. Our default configuration will require 50 connections. To adjust this SMBSERVICE_SESSIONS_ON_STORAGE should be set to a value lower than 4

Info

Please note that SMB over QUIC is not supported at this time - only traditional SMB over TCP connections are compatible with this integration. See [Windows] How to Expose an SMB Share as an NFS Storage Unit for more details.

Add a NetApp ONTAP Storage

NetApp ONTAP is a powerful data management software that provides unified storage for various protocols, including NFS, SMB/CIFS, iSCSI, and Fibre Channel.

It offers features like high availability, data protection, and storage efficiency, making it a popular choice for enterprise storage needs.

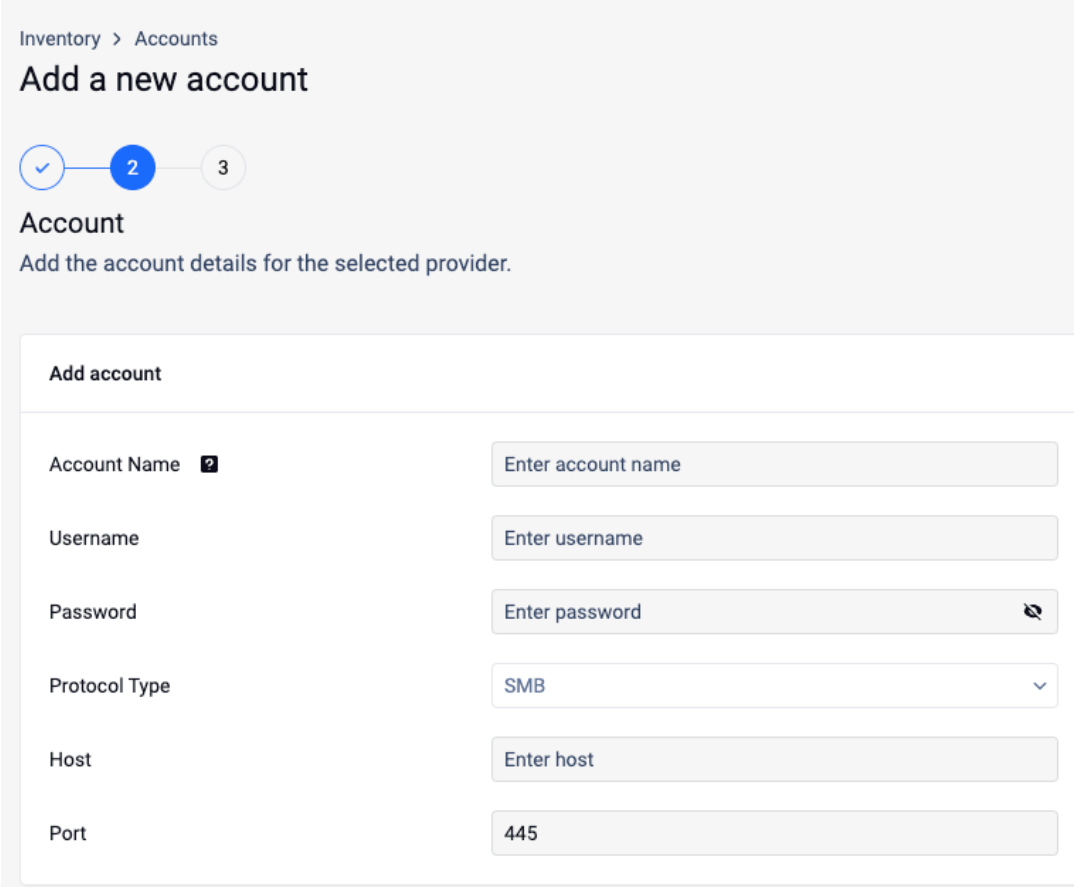
> **Key information:**
>
> To connect with your NetApp ONTAP storage, we rely on the Service Message Block (SMB) protocol. **Please enable SMB on your storage system beforehand for seamless integration.**

Product Specification Requirements	Version
Service Message Block (SMB) protocol	SMB 3.1.1 (or SMB3)

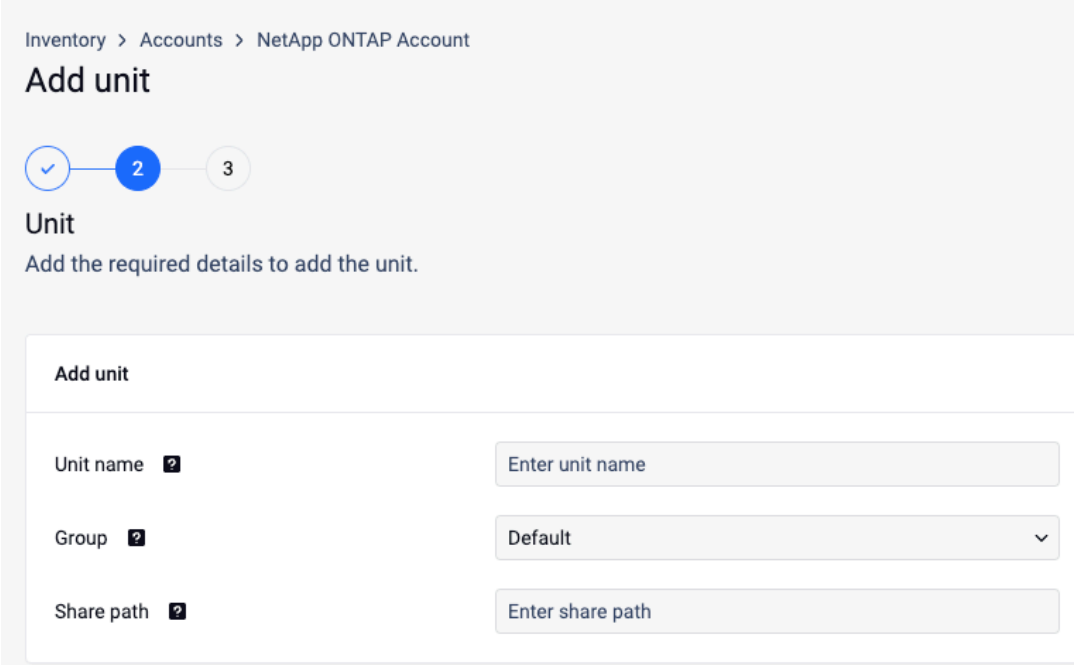
> **Key Information:**
>
> To use the virus scanning features (VSCAN) of your NetApp ONTAP storage with MetaDefender Storage Security **on your Windows deployment**, check out this article for detailed instructions.

To integrate your NetApp ONTAP storage with this system, follow these simple steps:

1. From the left side menu, navigate to **Inventory** -> **Add** -> **Account** -> Choose **NetApp**



3. **Provide an Account Name:** Give your account a name so you can easily identify it later
4. **Enter User Credentials**:
    1. Provide the username of an account with at least read and write permissions to the desired share.
    2. For Deep CDR & Remediations capabilities, the user needs modify permissions as well.
    3. Enter the password for the specified user.
5. Enter the IP address of the SMB server you wish to connect to.
6. Specify the port number used for the SMB connection, **445** being the default SMB port
7. Click on **Next** to finish the process.
8. From the left side menu, navigate to **Inventory** -> **Add** -> **Unit** -> Choose the previously created account



8. Give your unit an unique name so you can easily identify it later
9. Assign your unit to a Group
10. **Specify the Share Path.** Enter the path to your network share using one of the supported formats:
    1. file://servername/pathToShare
    2. \servername\pathToShare
    3. //servername/pathToShare
    4. smb://servername/pathToShare
11. **Complete the Process:** Click **Next** to finish integrating your NetApp ONTAP storage

Once added, you can use this storage within the system for various functionalities, leveraging the capabilities of NetApp ONTAP for data management and access.

Vscan | How to enable

Step 1: Understanding Vscan

What is Vscan?

Vscan is an antivirus scanning solution developed by NetApp that allows customers to protect their data from being compromised by viruses or other malicious code. It combines partner-provided antivirus software with ONTAP features to give customers the flexibility they need to manage file scanning.

Major components

- **Vscanner** or **Vscan Server**) - This is a Microsoft Windows server used for antivirus (AV) scanning.
- **Vscan engine** - This is the partner-supplied antivirus (AV) software that runs on Vscanner(s).
- **ONTAP Antivirus Connector** - This is NetApp-provided software that runs on Vscan Server
- **LIF (logical interface)** - This is the IP address used to access a cluster
  - To send files for virus scanning, you must configure ONTAP Antivirus Connector to connect to one or more SVMs by entering the Data ONTAP management LIF, the poll information, and the account credentials.
  - The management LIF is polled to retrieve the list of data LIFs
- **Storage Virtual Machine (SVM)** or **virtual storage server (Vserver)** - this is the logical storage object in NetApp ONTAP software
  - Vscan configuration is defined at the SVM level. The scope of the configuration is the SVM, and it only operates on SVM resources.

Vscan configurable components

- **Scanner pool** - This component defines the Vscanners and privileged users that can connect to SVMs. It also defines a scan request timeout period, after which the scan request is sent to an alternative Vscanner, if one is available.
- **Privileged user** - This component is a domain user account that a Vscanner uses to connect to the SVM. The account must exist in the list of privileged users in the scanner pool
- **Scanner policy** - This component determines whether a scanner pool is active. Scanner policies are system-defined, so you cannot create custom scanner policies. Only these three policies are available
  - **Primary** specifies that the scanner pool is active
  - **Secondary** specifies that the scanner pool is active, only when none of the Vscanners in the primary scanner pool are connected
  - **Idle** specifies that the scanner pool is inactive
- **On-Access Policy** - This component defines the scope of an on-access scan
  - You can specify the maximum file size to scan, file extensions and paths to scan, and file extensions and paths to exclude from the scan
  - By default, **only read-write** volumes are scanned. You can specify filters that enable scanning of read-only volumes or that restrict scanning to files opened with

execute access:

- `scan-ro-volume` enables scanning of read-only volumes
- `scan-execute-access` restricts scanning to files opened with execute access. Note: “Execute access” is different from “execute permission.” A given client will have “execute access” on an executable file only if the file was opened with “execute intent.”

- Within on-access mode you can choose from these two mutually-exclusive options
  - **Mandatory**: With this option, Vscan tries to deliver the scan request to the server until the timeout period expires. If the scan request is not accepted by the server, then the client access request is denied
  - **Non-Mandatory**: With this option, Vscan always allows client access, whether or not a Vscanner was available for virus scanning

- **On-demand task** - This component defines the scope of an on-demand scan
  - You can specify the maximum file size to scan, file extensions and paths to scan, and file extensions and paths to exclude from the scan. Files in subdirectories are scanned by default.
  - You use a cron schedule to specify when a task runs

- **Vscan file-operations profile (on-access scanning only)** - The vscan-fileop-profile parameter for the `vserver cifs share create` command defines which SMB file operations trigger virus scanning. By default, the parameter is set to **standard**. File operations are suspended until the external server reports the scan status of the file. If the file has already been scanned, ONTAP allows the file operation. Otherwise, it requests a scan from the server. You can adjust this parameter as necessary when you create or modify an SMB share:
  - **no-scan** specifies that virus scans are never triggered for the share
  - **standard** specifies that virus scans are triggered by open, close, and rename operations
  - **strict** specifies that virus scans are triggered by open, read, close, and rename operations
    - The strict profile provides enhanced security for situations in which multiple clients access a file simultaneously. If one client closes a file after writing a virus to it, and the same file remains open on a second client, strict ensures that a read operation on the second client triggers a scan before the file is closed
    - You should be careful to restrict the strict profile to shares containing files that you anticipate will be accessed simultaneously. Since this profile generates more scan requests, it may impact performance

- **writes-only** specifies that virus scans are triggered only when modified (or newly added) files are closed
  - Because writes-only generates fewer scan requests, it typically improves performance.
  - If you use this profile, the scanner must be configured to delete or quarantine unrepairable infected files, so they cannot be accessed. If, for example, a client closes a file after writing a virus to it, and the file is not repaired, deleted, or quarantined, any client that accesses the file without writing to it will be infected
- **On-access scanning is not supported for NFS**

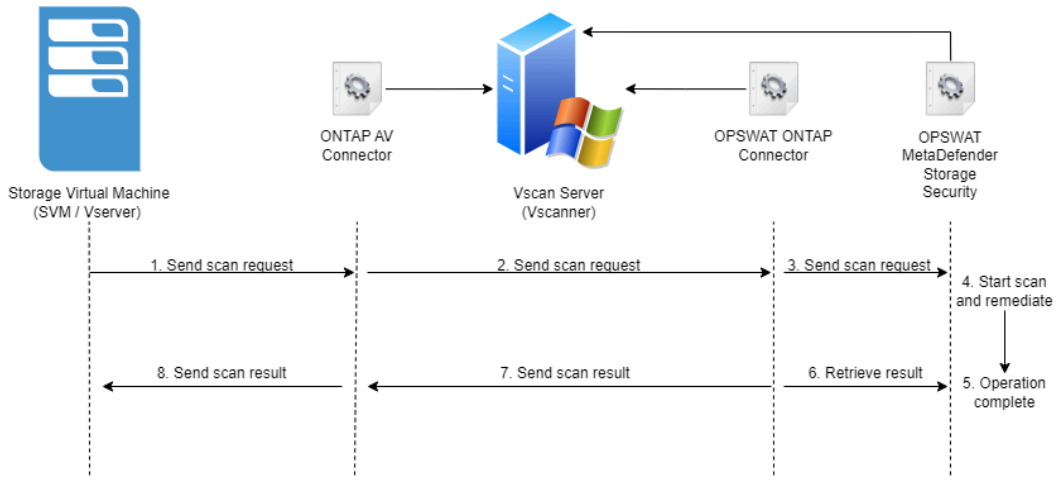
> **Important information**
>
> Currently, MetaDefender Storage Security supports only **on-access** scanning with profile type set to **writes-only** as a configuration from ONTAP**.** This means only the newly added or modified files will be sent by ONTAP to MetaDefender Storage Security for scanning. In the future, we will add support for **standard** and **strict** profile types too. For more details about file operations profile types please read this article provided by NetApp team.
>
> For **on-demand task** (immediately or on a schedule), use this feature directly from MetaDefender Storage Security.

How virus scanning works

Storage systems offload scanning operations to external servers hosting antivirus software from third-party vendors.

Based on the active scanning mode (Vscan file-operations profile), ONTAP sends scan requests when clients access files over SMB (on-access).

The ONTAP Antivirus Connector, provided by NetApp and installed on the external server, handles communication between the storage system and the antivirus software.



Step 2: Prerequisites

1. **Windows Server machine (minimum required version is 2019)**. This will be the Vscan Server where the following components will be installed:
    1. NetApp ONTAP Antivirus Connector
    2. OPSWAT ONTAP Antivirus Connector
2. Windows or Linux machine where MDSS is installed. **For best performances, we recommend installing MetaDefender Storage Security on the same machine from step 1**
3. One or multiple SVMs created from NetApp ONTAP that contain ore or multiple SMB shares.
4. An AD user that will be logged in on the Vscan Server. This user will become the privileged user for your SVMs / SMB shares and will be used later to add the SVMs / SMB shares to MetaDefender Storage Security.
5. **Read the best practices recommended by NetApp team here.**

Step 3: Enable Vscan from ONTAP

Assuming you have already created an SVM / SMB share and a Vserver, please execute the below commands from ONTAP CLI.

Step 3.1: Create scanner pool

```
vserver vscan scanner-pool create -vserver {your-vserver} -scanner-pool
{scanner-pool-name} -hostnames {IP-of-Vscan-Server} -privileged-users
{AD-Privileged-User}
```

> **Attention**

> If MetaDefender Storage Security is **running on a different machine than Vscan server**, the IP address of that machine needs to be added to this scanner pool. Example below:

```
vserver vscan scanner-pool servers add -vserver {your-vserver} -
scanner-pool {scanner-pool-name} -hostnames {IP-of-MDSS-machine}
```

For more details about creating a scanner pool, please read this article.

Step 3.2: Apply policy to your scanner pool

```
vserver vscan scanner-pool apply-policy -vserver {your-vserver} -
scanner-pool {scanner-pool-name} -scanner-policy primary
```

For more details about applying a policy to your scanner pool, please read this article.

Step 3.3: Create on-access policy to receive scan requests

```
vserver vscan on-access-policy create -vserver {vserver-name} -policy-
name {policy-name} -protocol CIFS
```

For more details about creating an on-access-policy, please read this article.

Step 3.4: Modify file operations profile to writes_only(will trigger a file scanning, when the file will be Closed, only for newly created or modified files)

```
vserver cifs share modify -share-name {cifs-share-name} -vscan-fileop-
profile writes-only
```

For more details about modifying a CIFS share, please read this article.

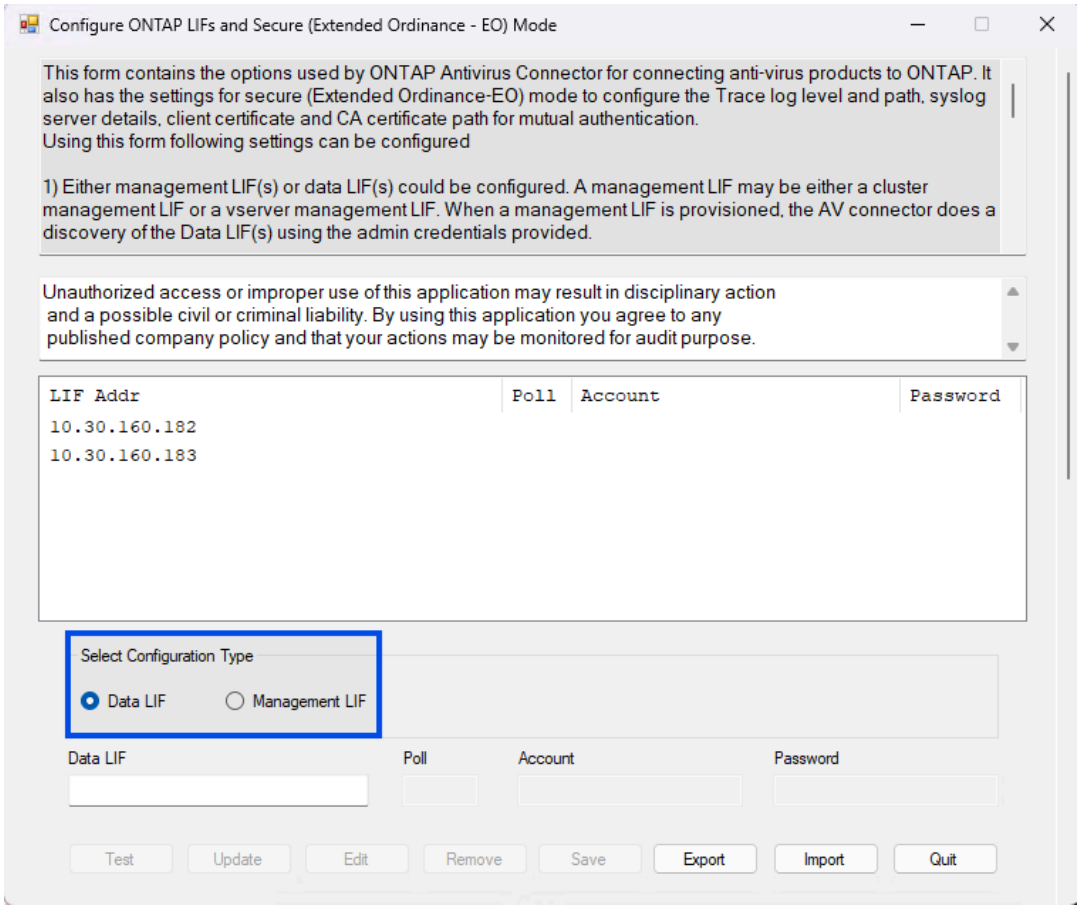
Step 3.5: Enable Vscan

```
vserver vscan enable -vserver {vserver-name}
```

Step 4: Install NetApp ONTAP AV Connector on the Vscan Server machine

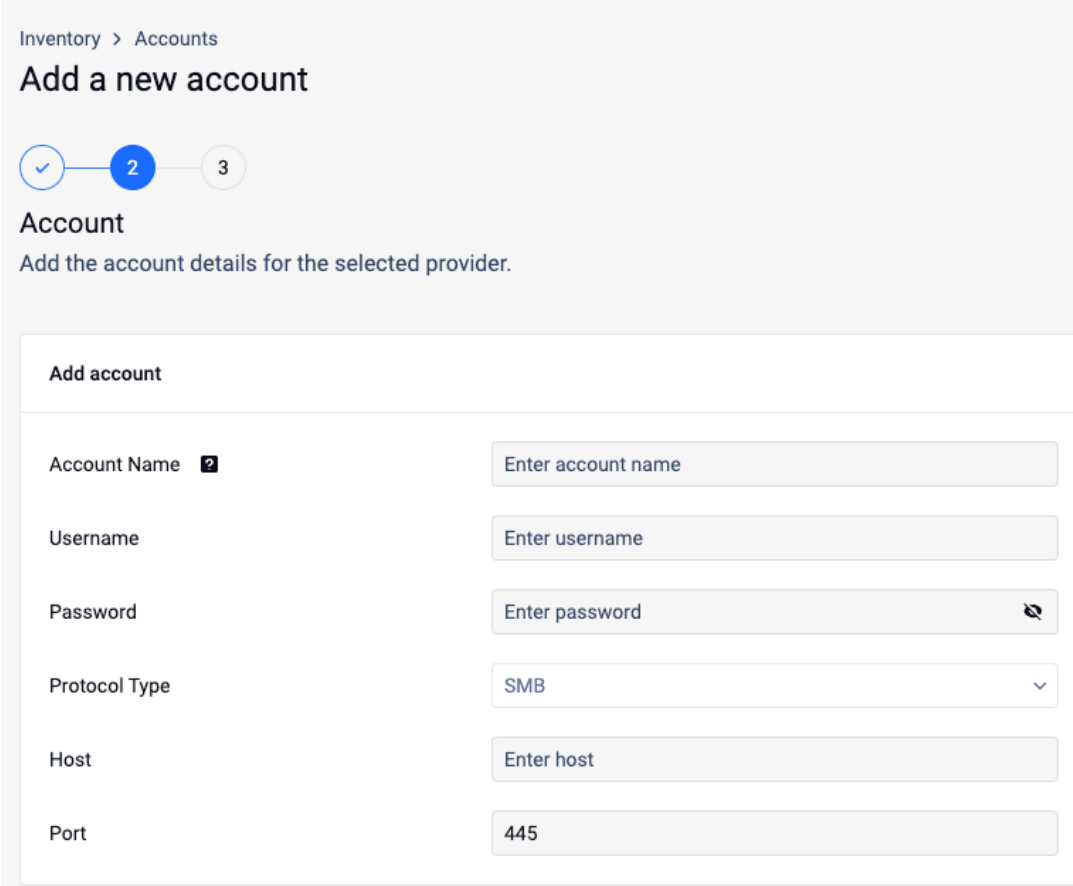
Please download the installer from here and follow the guidelines from NetApp team. The ONTAP AV Connector should be installed under the privileged user configured at step 3.1.

Both configuration types are supported from our side: **Data LIF** and **Management LIF**

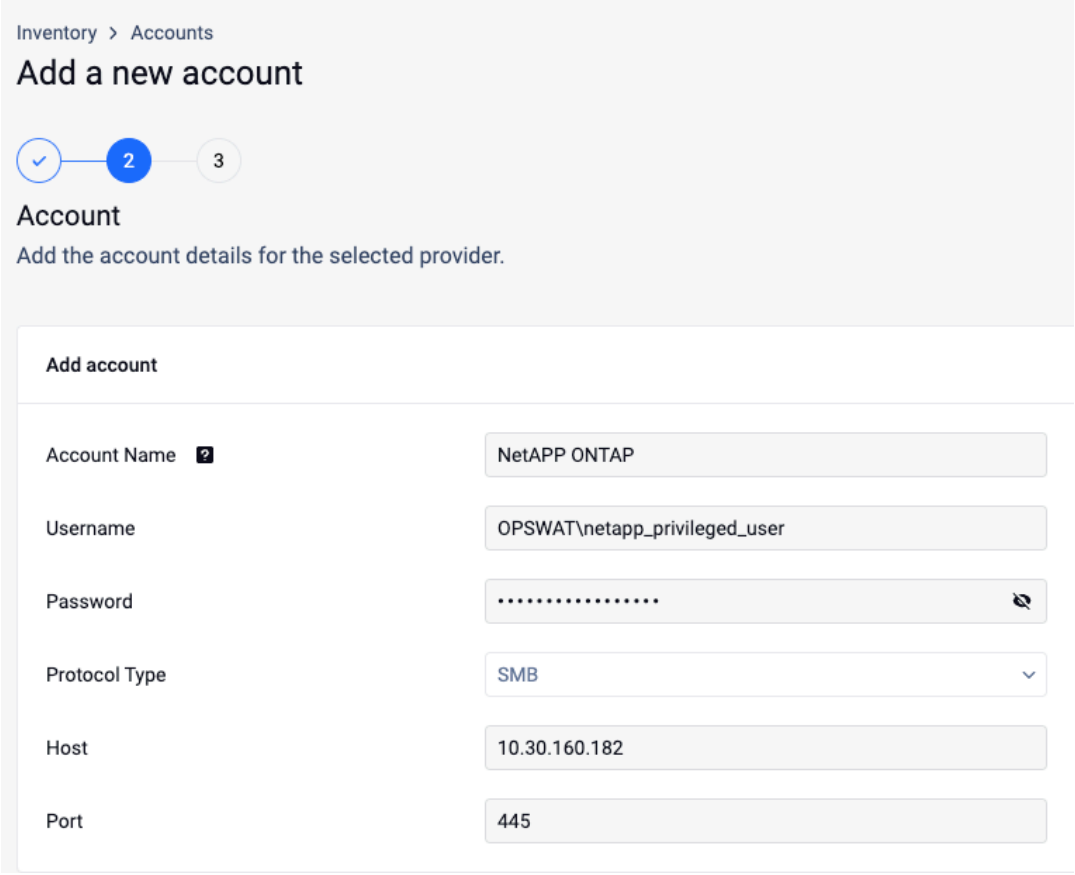


Step 5: Add the SVM in MetaDefender Storage Security

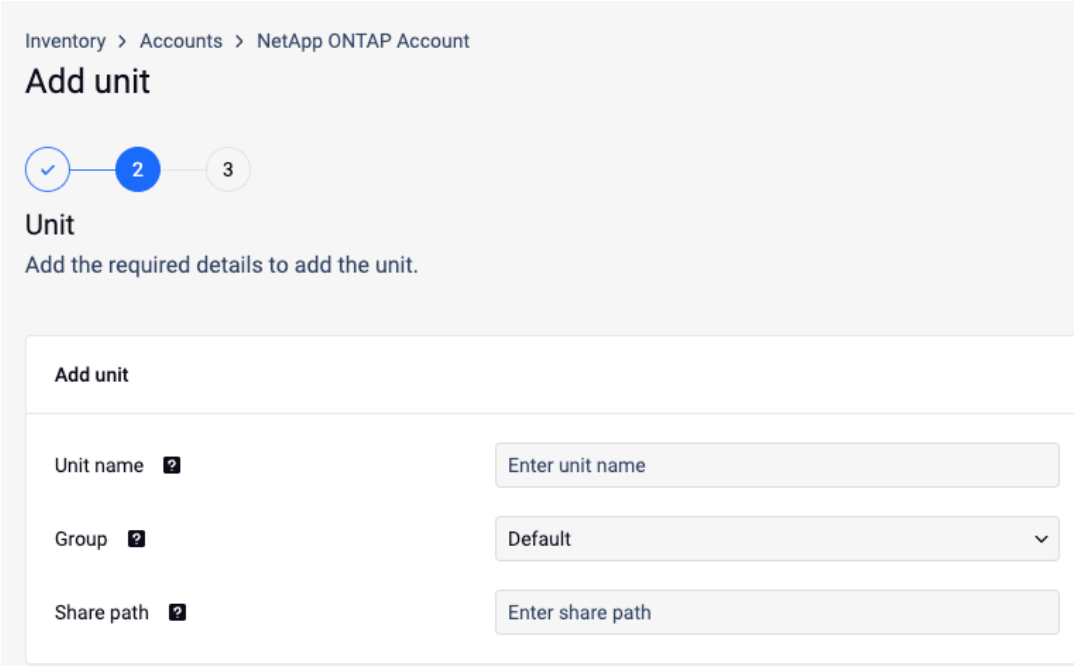
1. From Vscan server machine navigate to MDSS UI (localhost or remote machine)
2. Navigate to **Inventory** -> **Add** -> **Account** -> Choose **NetApp**



3. Give your account an unique name so you can easily identify it later
4. **Username**: Enter the privileged user configured at step 3.1. The following format is required: DOMAIN\Username
5. **Password**: Enter the password of the privileged user.
6. **Host**: Enter the IP address of the SVM
7. **Port**: Enter the port where the SMB server can be reached (default is 445)
8. Here is an example of how this should look like:

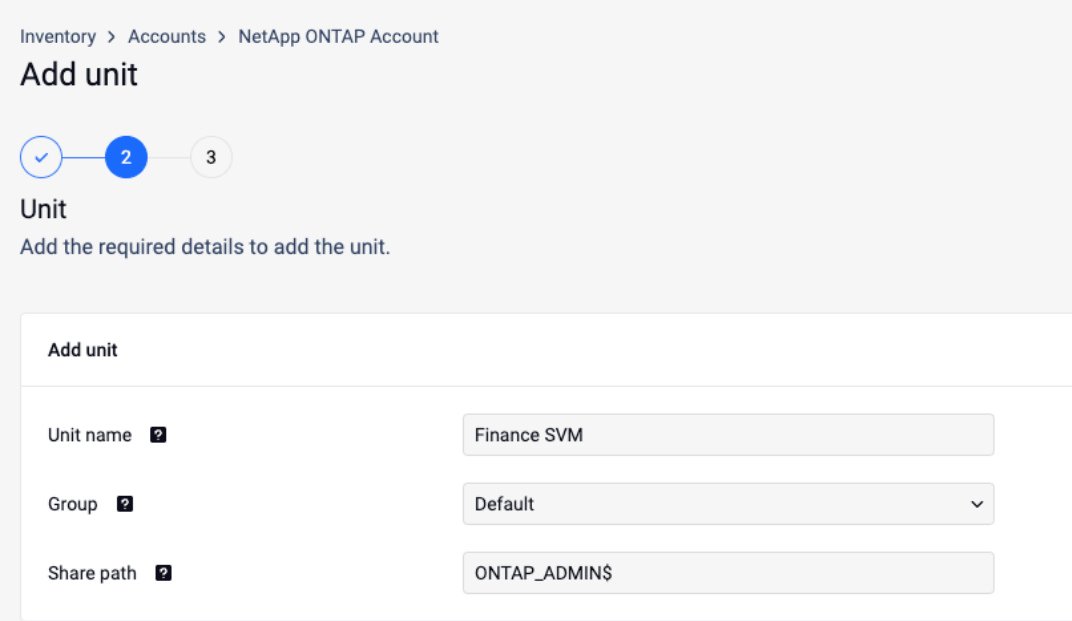


9. Click **Next** in order to finish the process of adding the account.
10. From left side pane, navigate to **Inventory** -> **Add** -> **Unit** -> Choose the previously created account



11. Give your unit an unique name so you can easily identify it later.

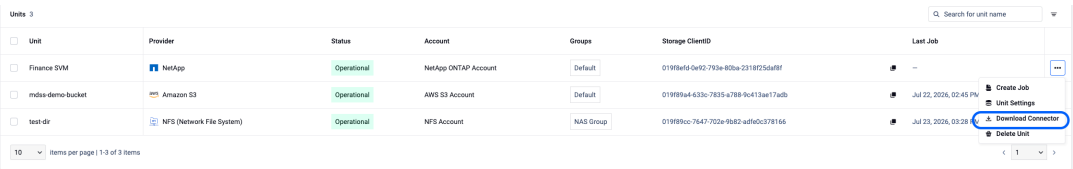
12. Assign your unit to a Group
13. **SharePath** should be **ONTAP_ADMIN$ **to protect all volumes on the SVM. ONTAP_ADMIN$ is a privileged path created by ONTAP when Vscan is enabled. This path is available only for the privileged user and from the privileged machine configure on the SVM' scanner pool from ONTAP.
14. Here is an example of how adding the unit should look like



7. Click **Next** in order to finish the process.

Step 6: Install OPSWAT ONTAP Connector on the Vscan Server machine

1. From MetaDefender Storage Security, navigate to Inventory -> Units -> Click on the three dots from your NetApp ONTAP Storage -> Click **Download Connector**



2. Unzip the downloaded archive
3. Open a console with admin privileges at the same path where the archive was unzipped
4. Run the following command line instruction

```
.\OPSWAT-ONTAP-Connector.exe --install
```

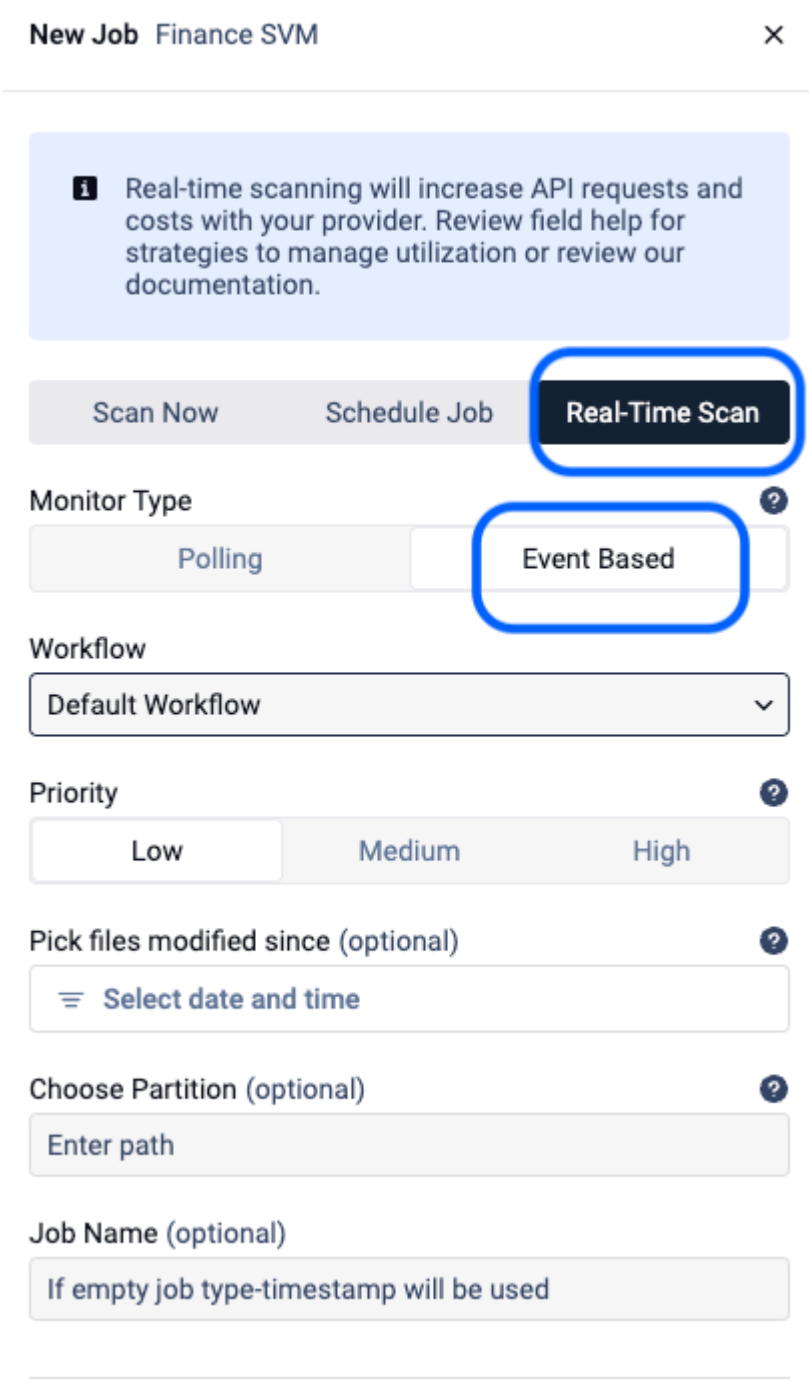
5. You will be asked if you want to install the OPSWAT ONTAP Connector under the Local System Account. In our testing, we have used this user and everything worked as expected. However, NetApp team recommends to install it under the same privileged user configured at step 3.1. To do that, close the current installation and run again with following parameters:

```
.\OPSWAT-ONTAP-Connector.exe --install /user DOMAIN\privilegeduser
/password your-password
```

6. A confirmation message should be received once the installation is complete.

Step 7: Test the integration

1. From MetaDefender Storage Security UI, navigate to Inventory -> Units -> Click on the three dots from the end of the row -> Create Job
2. Select Real-Time Scan and Event-Based and start the job



2. Copy a new file to one of the SVM volumes
3. From MetaDefender Storage Security UI, navigate to Dashboard -> Choose your NetApp ONTAP Storage -> Click on **View running jobs** -> Click on the previously started RTP scan
4. The newly uploaded file should be detected and scanned by MetaDefender Storage Security
5. Open the file and modify its content, then save it.

6. The modified file should be detected and scanned by MetaDefender Storage Security. If it's not the case, please see the below section named `Troubleshooting` .

> **Info**
>
> For different ways to enhance your scanning experience, please read this article.

Troubleshooting

Step 1 - Check if the file is received by NetApp ONTAP AV Connector

1. Enable verbose logging on ONTAP AV Connector by following the recommendations from this article.
2. Put a new file in the SMB share and then check the log file configured at previous step. If you see similar logs like this, it means the file is received by the ONTAP AV Connector and sent to our ONTAP Connector

```
2025-01-10T07:45:39.000564Z [pipe: 10.40.160.140]Server: Received 1152 bytes, ofsPartReq: [0]
2025-01-10T07:45:39.000564Z
[Pipe: 10.40.160.140]
       magic_num    : [4e74417041760003]
       session_id   : [cf99361b6bb7374d]
       len          : [1152]
       reqId        : [5]
       type         : [15, req_SCAN_EXTENDED]

[dump_mem] len: 66
 5c  0 6d  0 79  0 76  0   6f  0 6c  0 5c  0 75  0    [\ m y v o l \ u ]
 70  0 6c  0 6f  0 61  0   64  0 2d  0 62  0 79  0    [p l o a d - b y ]
 2d  0 67  0 61  0 62  0   72  0 69  0 65  0 6c  0    [- g a b r i e l ]
 2d  0 76  0 31  0 33  0   2e  0 74  0 78  0 74  0    [- v 1 3 . t x t ]
  0  0                                                [   ]
2025-01-10T07:45:39.000567Z Sending id 1 (rsrv-id: 0) for \\?\UNC\10.40.160.140\ontap_admin$\myvol\upload-by-gabriel-v13.txt
2025-01-10T07:45:39.000567Z Sent!
```

3. If the file is not received by NetApp ONTAP AV Connector, it means there is a misconfiguration in your side and needs to be fixed. You can start from section `Step 3: Enable Vscan from ONTAP`, located above in this page.

Step 2 - Check if the file is received by OPSWAT ONTAP Connector

1. Navigate to `C:\ProgramData\OPSWAT-ONTAP-Connector\logs`
2. Open the log file from today and search for your file name. You should see a message like this if your file was sent by ONTAP AV Connector and received by OPSWAT ONTAP Connector:

```
[{Time}] [Information] VS_ScanRequest received. Id: {sca-id}. File path
: \\?\UNC\{IP-of-smb-share}\ontap_admin$\{volume-name}\{file-name-and-
extension}
```

```
[2024-10-21 15:33:40] [Information] VS_ScanRequest received. Id: 3.
File path : \\?\UNC\160.160.160.160\ontap_admin$\myvolume\test-file.txt
```

3. If file is not received by our ONTAP Connector, there is a misconfiguration somewhere. Please check:
    1. privileged user from ONTAP to be the same as NetApp ONTAP user from storage unit from MDSS UI
    2. ONTAP AV Connector connected to management LIF that has the cluster IP address
4. You can also enable logging for ONTAP AV Connector by following this guideline

Step 3 - Check if the file is sent by OPSWAT ONTAP Connector to MetaDefender Storage Security

1. In the logs from step 1.2, search for your file name. You should see a log containing the following text: `File successfully sent for scanning`
2. If file is not sent to MDSS for scanning, please check the following:
    1. Real Time Processing with Event-Based to be enabled for your NetApp ONTAP storage unit
    2. `Apikey`and `StorageClientId` from config file `C:\ProgramData\OPSWAT-ONTAP-Connector\config.ini` to be the same as their values from MDSS UI.

Step 3 - Check if file is discovered by MetaDefender Storage Security

1. In MDSS UI, navigate to `Dashboard -> NetApp ONTAP -> Choose your storage unit -> Real-Time Processing [Event Based] -> View Report`
2. Check if the file appears in the table
3. If not, something happened with our SMB service. You can check the logs from `C:\Program Files\OPSWAT\MetaDefender Storage Security\services\opswat.mdcs.smbservice\logs\600x` to see if you spot anything. Please check in each of the 600x folders. If you need guidance from us, please generate a support package and send it to our support team.

Uninstall

To uninstall OPSWAT-ONTAP-Connector, run the following command line in an admin console

```
.\OPSWAT-ONTAP-Connector.exe --uninstall
```

A confirmation message will be received.

If you run the command with the executable from `C:\ProgramData\OPSWAT-ONTAP-Connector\OPSWAT-ONTAP-Connector.exe`, the service will be uninstalled but the

executable file will not be deleted because is in use. Finish the uninstallation process and then remove the folder manually.

Vscan | Best practices

Privileged User

- Restrict privileged users to virus-scanning operations. Normal users should be discouraged from using privileged user credentials. This restriction can be achieved by turning off login rights for privileged users on Active Directory.
- Privileged users are not required to be part of any user group that has a large number of rights in the domain, such as the administrators group or the backup operators group
- Privileged users must be validated only by the storage system so that they are allowed to create Vscanner connections and access files for virus scanning.

Vscanner

- Use the computers running Vscanners only for virus-scanning purposes. To discourage general use, disable the Windows terminal services and other remote access provisions on these machines and grant the right to install new software on these machines only to administrators.
- Dedicate Vscanners to virus scanning and do not use them for other operations, such as backups. You might decide to run the Vscanner as a virtual machine (VM). If this is the case, ensure that the resources allocated to the VM are not shared and are sufficient to perform virus scanning.
- Provide adequate CPU, memory, and disk capacity to the Vscanner to avoid resource bottlenecks. Most Vscanners are designed to use multiple CPU core servers and to distribute the load across the CPUs.
- For remote sites and branch offices, NetApp recommends using a local Vscanner rather than a remote Vscanner because the former is a perfect candidate for high latency. If cost is a factor, use a laptop or PC (as a Vscanner) for moderate virus protection.

Vscanner Networking

- Connect the NetApp storage system and the Vscanner by using at least a 1GbE network.
- For an environment with multiple Vscanners, connect all servers that have similar high-performing network connections. Connecting the Vscanners improves performance by allowing load sharing.

- NetApp recommends using a dedicated network with a private VLAN for the connection from the SVM to the Vscanner so that the scan traffic is not affected by other client network traffic. Create a separate NIC that is dedicated to the antivirus VLAN on the Vscanner and to the data LIF on the SVM. This step simplifies administration and troubleshooting if network issues arise.
- The AV traffic should be segregated using a private network. The AV server should be configured to communicate with domain controller (DC) and clustered Data ONTAP in one of the following ways:
  - The DC should communicate to the AV servers through the private network that is used to segregate the traffic.
  - The DC and AV server should communicate through a different network (not the private network mentioned previously), which is not the same as the CIFS client network. Private Network is optional.
- For Kerberos authentication to work for the AV communication, create a DNS entry for the private LIFs and a service principal name on the DC corresponding to the DNS entry created for the private LIF. Use this name when adding a LIF to the Antivirus Connector. The DNS should be able to return a unique name for each private LIF.

Node Failover

If the LIF for Vscan traffic is configured on a different port than the LIF for client traffic, the Vscan LIF might fail over to another node in case of a port failure. The change will make the Vscanner not reachable from the new node and the scan notifications for file operations on the node will fail.

> **Info**
>
> For more details about this type of storage please read the official ONTAP Documentation

Vscan | Scalability

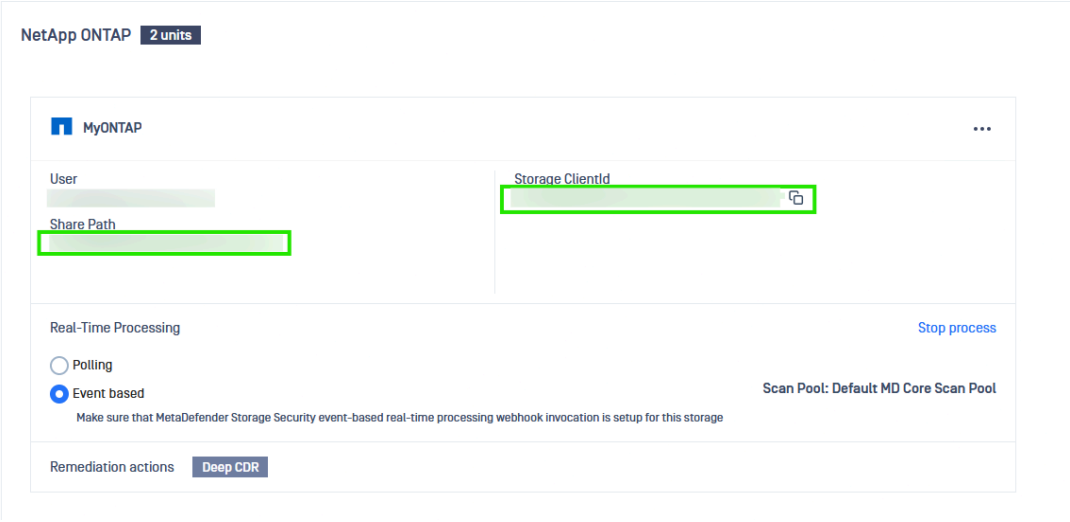
Our recommendation is to start with the basic use case, monitor the performance and, depending your business needs, scale the system accordingly.

Description	Use case	Solution
Small scale deployments with one SMB share	0 - 20,000 files per hour* 1 x SMB share	1 x Vscan Server
Small scale deployments with multiple SMB shares	0 - 20,000 files per hour* 2 or more SMB shares	1. Connect multiple SMB shares to the same OPSWAT-ONTAP-Connector 2. Connect each SMB share to a separate MDSS instance. You will need a Vscan Server for each MDSS instance
Medium to Large scale deployments	20,000 + files per hour *	1. Configure multiple Vscan Servers to support your SMB share. 2. Split your data in multiple SMB shares each one being connected to a separate Vscan Server having separate MDSS instances.

*** The data presented in the table was derived from our sizing guide. These results are intended as guidelines rather than precise performance guarantees due to the multitude of variables that can impact performance, such as file types, network configurations, and hardware specifications. For critical throughput requirements, OPSWAT recommends conducting site-specific benchmarks prior to deploying a production solution.

How to connect multiple SMB shares to the same OPSWAT-ONTAP-Connector

1. Add your SMB share to MetaDefender Storage Security following this article
2. Copy your `StorageClientId`and `SharePath`for your new storage



3. Navigate to `C:\ProgramData\OPSWAT-ONTAP-Connector\config.ini`
4. Open the file in text editor (requires admin privileges) and modify the number of storage units: `StorageUnits=2`
5. Add details about the second storage unit:

```
[Storage Unit 2]
ClientId={StorageClientId}
SharePath={SharePath}
```

6. Restart the service with name`opswat-ontap-connector` in order changes to take effect

How to configure multiple Vscan Servers

1. You need to have a new Windows Server machine and another AD user (privileged user). For each scan server you will need to have a separate Windows Server machine because **only one ONTAP Connector can be installed on the same Windows Server machine**
2. From ONTAP CLI, add the new IP of the Vscan Server and the new privileged user to scanner pool

```
vserver vscan scanner-pool modify -vserver {your-vserver} -scanner-pool
{scanner-pool-name} -hostnames {list-of-host-names} -privileged-users
{list-of-privileged-users}
```

```
vserver vscan scanner-pool modify -vserver opswat-vserver -scanner-pool
opswat-scanner-pool -hostnames 10.30.160.180,10.30.160.181 -privileged-
users TestAD\privilegeduser1,TESTAD\privilegeduser2
```

For more information about `vserver vscan scanner-pool modify` command, please read this article

3. Install ONTAP AV Connector and OPSWAT ONTAP Connector on the new Windows Server machine. Follow this guidance. To install OPSWAT ONTAP Connector, please copy the zip from first Vscan Server and install from there.
4. Navigate to `C:\ProgramData\OPSWAT-ONTAP-Connector\config.ini` , open it in a text editor with admin privileges
5. Modify the IP of the MetaDefender Storage Security from `127.0.0.1` with the IP of the first Vscan Server, where your MDSS instance is installed (**Note**: Please be aware that the IP displayed or assigned may differ if a proxy or VPN is being used. To ensure accurate IP information, verify if any proxy or VPN is active)
6. Restart service with name `opswat-ontap-connector` in order changes to take effect
7. Now you should have two scanning servers connected to the same SMB share and same MDSS instance.
8. If you want to add more scan servers, please repeat the process.

> **Info**

> When multiple scan servers are utilized, files are distributed to the scan servers using a round-robin method.

AWS FSx for NetApp ONTAP

Metadefender Storage Security is fully compatible with AWS FSx for NetApp ONTAP, leveraging NetApp's Vscan feature for seamless integration. This allows MDSS to scan files stored on your FSxN volumes for threats, helping to ensure the integrity and security of your data.

Before you begin, make sure you have:

- An operational AWS FSx for NetApp ONTAP file system.
- A Windows Server machine designated to run Metadefender Storage Security.
- Appropriate licenses for both AWS FSx for NetApp ONTAP and Metadefender Storage Security.
- Administrative access to both your AWS environment and your NetApp ONTAP configuration.

Setup and Configuration

Follow these steps to integrate MDSS with your FSxN instance:

1. Set Up AWS FSx for NetApp ONTAP (if not already deployed)
    - Follow the official AWS documentation to create and configure your FSx for NetApp ONTAP file system:
        - AWS FSx for ONTAP Setup Guide: Amazon FSx for NetApp ONTAP User Guide
2. Configure Vscan for MDSS Integration
    - Vscan enables communication between your NetApp ONTAP system and external virus scanning servers, such as your MDSS instance.
    - Detailed instructions for enabling and configuring Vscan can be found in the NetApp and AWS documentation. Refer to the following resources, starting with **step 3** of the OPSWAT Vscan guide which typically outlines the ONTAP-side configuration:
        - OPSWAT Vscan Integration Guide (refer to ONTAP configuration steps): MetaDefender Storage Security - Add A NetApp ONTAP Storage (This page also contains instructions for adding NetApp ONTAP as a storage unit in MDSS).
        - AWS Guide for Vscan with FSx for ONTAP: Use NetApp ONTAP Vscan with FSx for ONTAP
        - NetApp ONTAP Vscan Enablement (CLI reference): vserver vscan enable - NetApp ONTAP CLI

3. Domain Membership - CRITICAL for proper authentication and Vscan communication
    - The Windows Server machine running Metadefender Storage Security **must** be a member of the same Active Directory domain as the AWS FSx for NetApp ONTAP SVM (Storage Virtual Machine) that you intend to scan.
4. Install and Configure Metadefender Storage Security
    - Install MDSS on your designated Windows Server.
    - During the MDSS configuration, add your FSxN SVM as a NetApp ONTAP storage unit, providing the necessary credentials and connection details as prompted by the MDSS interface. Refer to the MetaDefender Storage Security documentation for specific instructions on adding storage units.

Troubleshooting

If you encounter issues during or after the integration, use the following NetApp ONTAP CLI commands on your FSxN instance for diagnostics:

- `event log show` this command displays the event log, which may contain error messages related to Vscan or authentication. Filter for Vscan-related events for more targeted information.
    - Example: `event log show -message-name *vscan*`
- `vserver vscan connection-status show-all` this command shows the status of Vscan connections from the SVM to the scanning servers (your MDSS instances). This helps verify if the MDSS server is successfully connected.
- `vserver vscan show` this command displays the Vscan configuration for a specified SVM, allowing you to verify settings like active scanners and policies.

Additional Troubleshooting Tips

- Make sure there are no firewall rules (either on the MDSS server, AWS Security Groups, or network ACLs) blocking the necessary Vscan communication ports between the FSxN SVM and the MDSS server. (Default Vscan port is 139/445 for SMB).
- Verify that the service account used by MDSS for Vscan has the appropriate permissions on the NetApp SVM and the shares being scanned.
- Confirm that the MDSS server and the FSxN SVM can resolve each other's hostnames via DNS.
- Make sure that the MDSS server and the FSxN instance (and domain controllers) have their time synchronized. Significant time skew can cause authentication issues.
- Check the Metadefender Storage Security logs on the Windows server for any specific error messages related to the NetApp integration.

Performance Testing

The validation was performed using the basic deployment infrastructure model:

- **Windows Server**: 1 x MDSS instance and 1 x OPSWAT ONTAP Connector instance
- **Linux**: 1 MetaDefender Core instance

The performance metrics obtained from this configuration aligned with the specifications outlined in our sizing guide. The test successfully validated the expected performance parameters for this particular deployment architecture.

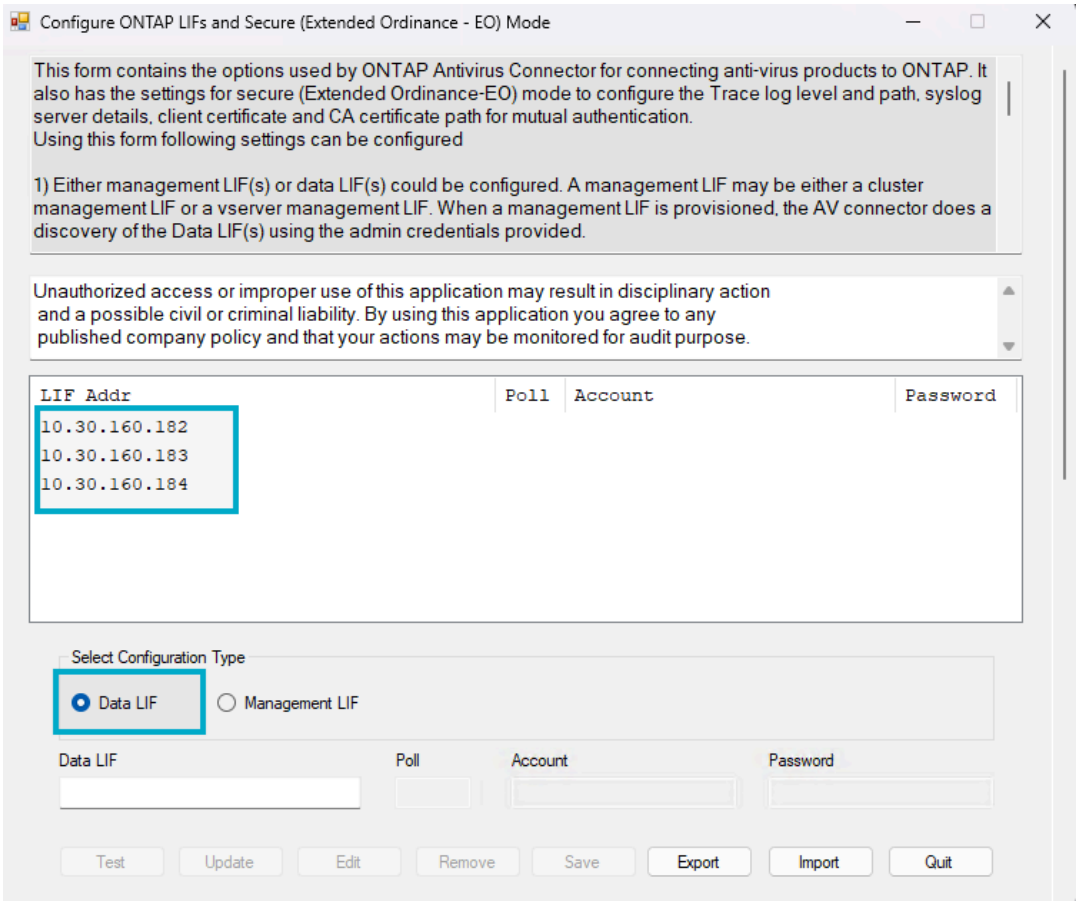
> **Note:** For detailed performance metrics and specific hardware recommendations, please refer to the official sizing guide.

Vscan | How to connect multiple SVMs

When Vscan is enabled, **multiple SVMs** can be connected to the same MDSS instance.

Step 1: Add the SVM on ONTAP AV Connector

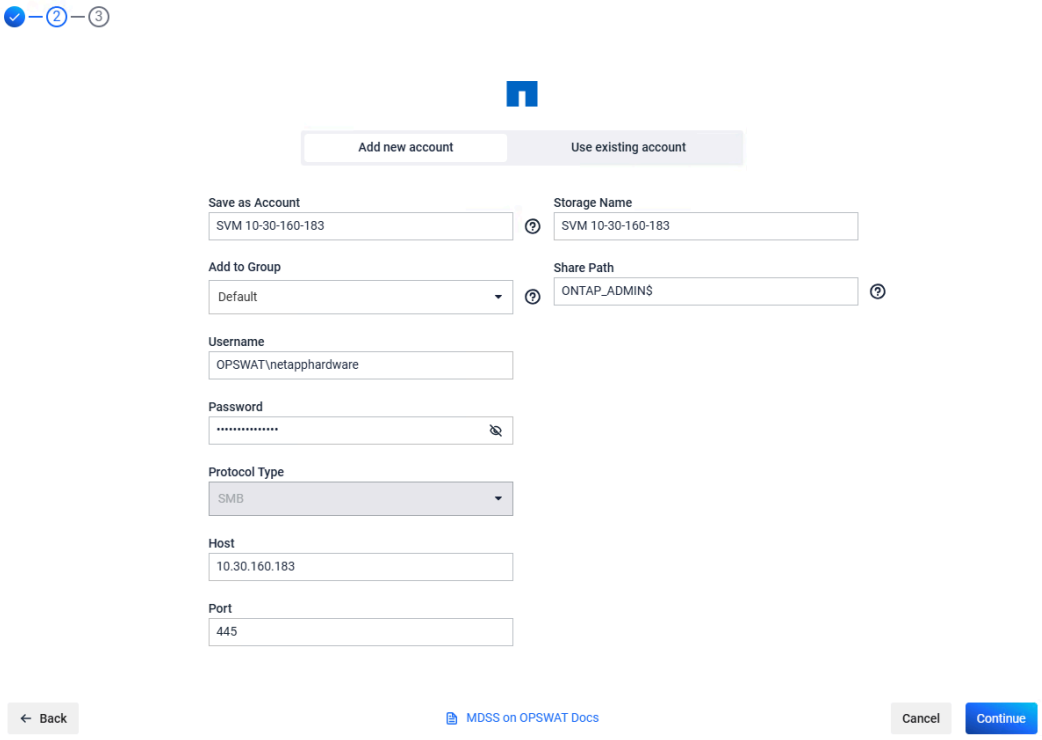
1. From MDSS machine, open the **Configure ONTAP LIFs** app provided by NetApp and available with the ONTAP AV Connector installation.
2. Add the additional SVMs (can be either data LIF or management LIF). In our example, we have used Data LIF as does not require authentication



3. Once all the SVMs are added, save and quit.

Step 2: Add each SVM as a different storage unit in MDSS

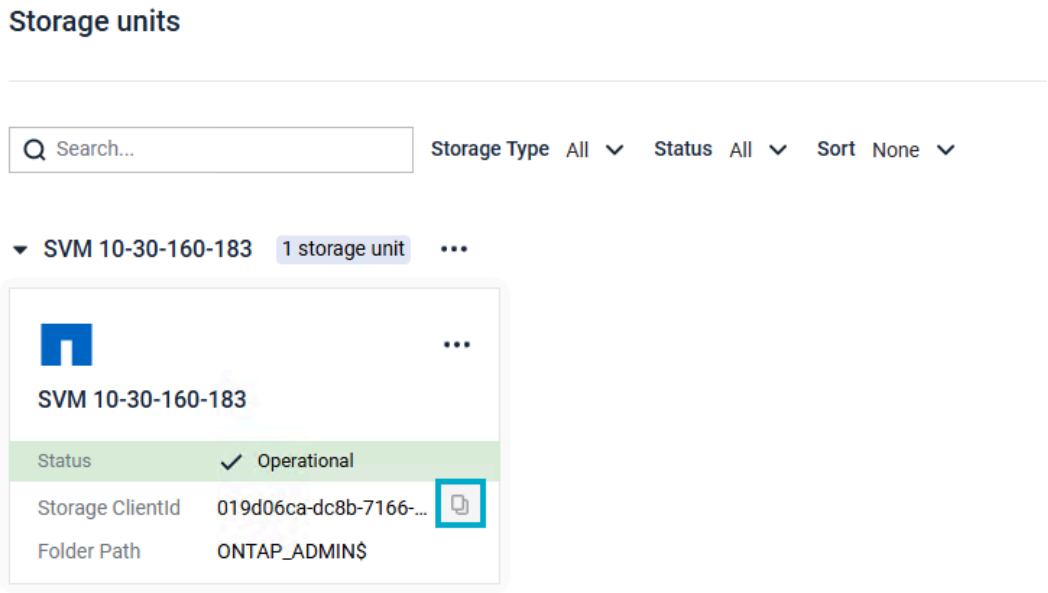
1. Navigate to MetaDefender Storage Security UI
2. Go to Storage Units -> Add new storage unit -> Choose NetApp -> Add new Account
3. For the Account, input:
    1. name
    2. username and password of the privileged user configured on ONTAP
    3. Host (IP) of the SVM
4. For the Storage, input:
    1. name
    2. Share Path. In case you want to add all the SMB shares created under the SVM, input **ONTAP_ADMIN$** (privileged path created by ONTAP) that is available only for the privileged user.
5. Here is an example of how the form should look like



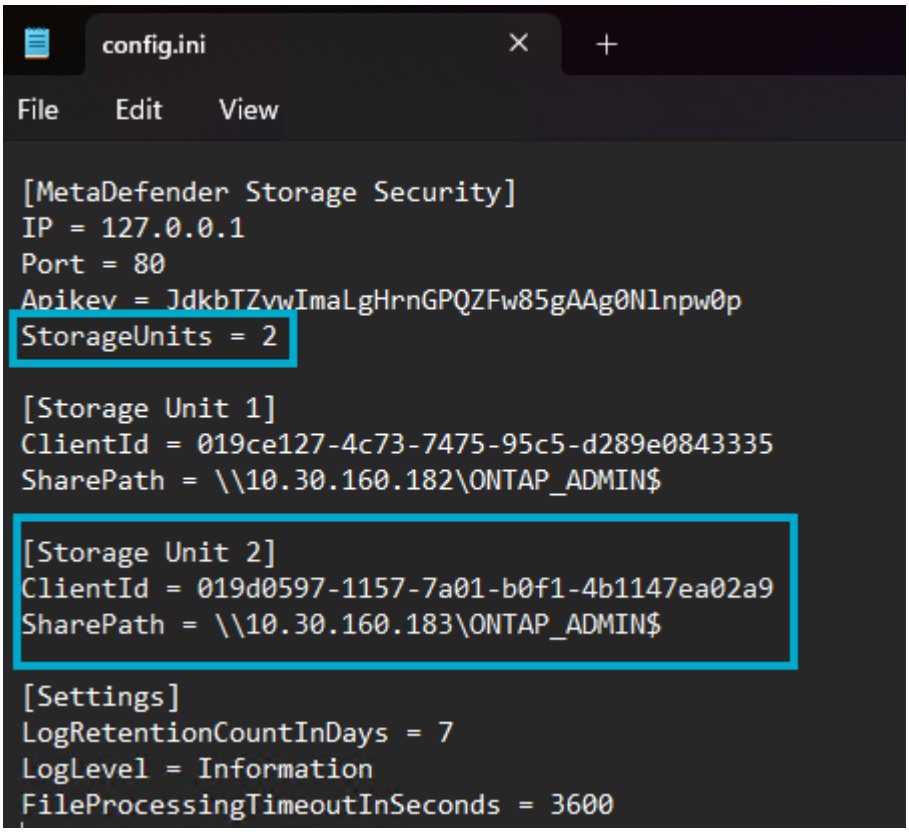
6. Click Continue and wait for the storage to be added.
7. If **OPSWAT ONTAP Connector** is installed, do not download or install it.
8. Repeat the steps with all the SVMs you want to add

Step 3: Add each SVM in the OPSWAT ONTAP Connector config file

1. From MDSS machine, navigate to **C:\ProgramData\OPSWAT-ONTAP-Connector**
2. Open **config.ini** file
3. Set **Storage Units** to the number of SVMs you have added in MDSS
4. Add each Storage Unit and its corresponding details.
    1. **ClientId** can be copied from MDSS UI by Navigating to Storage Units -> Your storage unit card and click the copy button

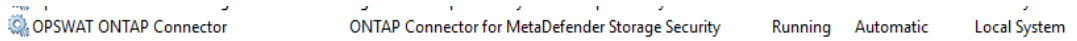


5. Here is an example of how the config file should look like:



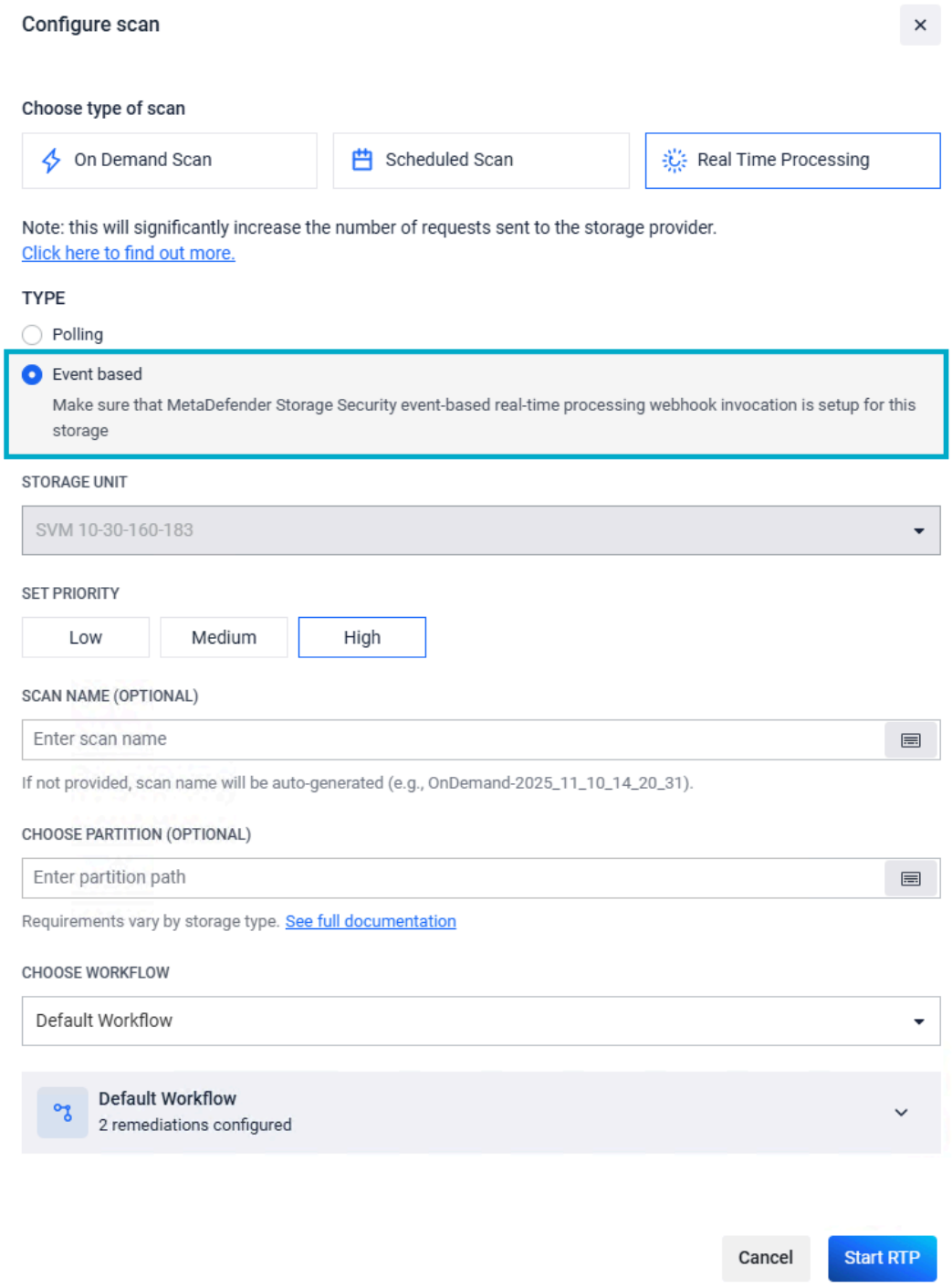
Step 4: Restart OPSWAT ONTAP Connector service

This service needs to be restarted for the changes to take effect



Step 5: Enable RTP with Event-Based

One last step is to enable Real Time scan with Event-Based for all the storage units corresponding to your SVMs, so that MDSS can processed the new files



Vscan | Configuration

The OPSWAT connector for NetApp ONTAP is configured through a **config.ini** file. This page documents the settings available in that file, grouped by section. If a setting is left empty or omitted, its default value is used (if there is one). If a setting contains a value outside its allowed range or of the wrong type, the connector will not start and will report the invalid setting.

Example

```
[MetaDefender Storage Security]
IP=127.0.0.1
Port=80
Apikey=
StorageUnits=1

[Storage Unit 1]
ClientId=
SharePath=

[Settings]
LogRetentionCountInDays=7
LogLevel=Information
FileProcessingTimeoutInSeconds=3600
RpcLocalPipeHost=127.0.0.1
ZoneIdentifierFiles=0
```

[MetaDefender Storage Security] section

Defines how the connector reaches the MetaDefender Storage Security instance.

Setting	Type	Default	Description
IP	Text (IPv4 address)	127.0.0.1	IP address of the MetaDefender Storage Security instance.
Port	Integer	80	Network port of the MetaDefender Storage Security instance.
Apikey	Text		API key used to authenticate with MetaDefender Storage Security.
StorageUnits	Integer	1	Number of configured storage units

[Storage Unit N] sections

One section per configured storage unit, numbered sequentially (**[Storage Unit 1]**, **[Storage Unit 2]**, and so on). The number of these sections should match the **StorageUnits** value above. If the value of the **StorageUnits** variable is less than the number of **Storage Unit** sections in the file, only the first N storage units will be checked. If the value is greater, all storage units will be checked and the extra amount of the value will be silently ignored. If there is any storage unit section that is missing (e.g. **StorageUnits=3**, **[Storage Unit 1] **and** [Storage Unit 3] **are present but **[Storage Unit 2]** is missing), the connector will fail.

Setting	Type	Default	Description
ClientId	Text		Identifier of the storage unit generated by MetaDefender Storage Security
SharePath	Text		Path of the share to protect as it is integrated in MetaDefender Storage Security

[Settings] section

General connector behavior.

Setting	Type	Default	Description
LogRetentionCountInDays	Integer (1-30)	7	Number of days log files are retained
LogLevel	Text	Information	Logging verbosity. One of: Debug, Information, Warning, Error, Fatal
FileProcessingTimeoutInSeconds	Integer	3600	Maximum time allowed to process a single file before it times out
RpcLocalPipeHost	Text	127.0.0.1	Local host address used for the connector's internal communication
ZoneIdentifierFiles	Integer (0-3)	0	Handling mode for Windows *Zone.Identifier* files (see below).

ZoneIdentifierFiles values

Zone.Identifier files are small metadata streams Windows attaches to files downloaded from the internet. They hold no user content, so scanning them is usually unnecessary. This setting selects how the connector handles them; all other files always go through the normal scanning pipeline regardless of this value.

Value	Mode	Behavior
0	Skip (default)	Zone.Identifier files are ignored, not scanned and no verdict is returned
1	Scan	Zone.Identifier files are sent to MetaDefender Storage Security and scanned like any other file
2	Allow	Zone.Identifier files are immediately allowed without scanning
3	Block	Zone.Identifier files are immediately blocked without scanning

ONTAP Connector Configuration file

The OPSWAT ONTAP Connector is the Windows service (`opswat-ontap-connector`) that sits between a NetApp ONTAP Vscan (AV) connector and a MetaDefender Storage Security (MDSS) instance. It receives scan requests from ONTAP over MSRPC named pipes, forwards each file to MDSS for real-time processing, and returns the verdict back to ONTAP.

All of its behaviour is driven by a single `config.ini` file. This page documents every section, key, accepted value and default.

File location and load behaviour

File name	`config.ini`
Location	The folder containing `OPSWAT-ONTAP-Connector.exe`
Installed location	`C:\ProgramData\OPSWAT-ONTAP-Connector\config.ini`
When it is read	Once, at process start, before any other initialization
Applying a change	**Restart the opswat-ontap-connector service.** The file is never re-read at runtime.

`config.ini` is copied from the executable folder into the installation folder by `--install` and `--upgrade`, so edit the *installed* copy when tuning a deployed connector.

If the file cannot be read, or any value fails validation, the connector logs `Error when reading config.ini file` at `Fatal` level and exits without starting.

Format rules

Standard INI semantics apply:

- Sections are declared as `[Section Name]`; section and key names are matched case-insensitively by Windows.
- Entries are `Key=Value`. Whitespace around the `=` is trimmed.
- Lines beginning with `;` are comments.
- Do **not** quote values — quotes become part of the value.
- A single value is limited to 254 characters; anything longer is truncated.

Section `[MetaDefender Storage Security]`

Identifies the MDSS instance the connector talks to.

Key	Required	Type	Default	Accepted values
`IP`	Yes	IPv4 address	—	Dotted-quad IPv4 only, e.g. `10.0.0.15`
`Port`	Yes	Integer	—	MDSS HTTP port, e.g. `80`, `8008`
`PortSsl`	No	Integer	`443`	MDSS HTTPS port
`IgnoreCertErrors`	No	Integer	`0`	`0` or `1`
`Apikey`	Yes	String	—	MDSS API key
`StorageUnits`	Yes	Integer	—	1 or greater

`IP`

The address of the MDSS instance. **Validated against an IPv4 regular expression — hostnames. FQDNs and IPv6 addresses are rejected** and cause a fatal configuration error at startup.

`Port` and `PortSsl`

The connector does not require you to declare whether MDSS is served over HTTP or HTTPS. It starts every session on plain HTTP against `Port`, and switches transport automatically:

1. A request fails with a transport-level WinHTTP error — TLS handshake failure (`12175`), connection reset (`12030`), an invalid server response (`12152`), or the port refusing connections (`12029`).
2. The connector flips its transport mode (HTTP ⟷ HTTPS) and retries the request once on the other port.

3. The new mode is kept for subsequent requests, and the switch is logged at `Warning` level (`MDSS request failed with a transport error. Switched transport to …`).

The switch is bidirectional and self-healing, so an MDSS instance that moves from HTTP to HTTPS (or back) is picked up without restarting the connector. Automatic switching is only attempted when `PortSsl` is greater than `0`; setting `PortSsl=0` pins the connector to plain HTTP on `Port`.

The connector negotiates TLS 1.2 and, where the build environment supports it, TLS 1.3.

`IgnoreCertErrors`

Value	Behaviour
`0` (default)	Full TLS certificate validation. A certificate MDSS cannot prove is trusted fails the request.
`1`	Certificate errors are ignored on HTTPS requests: unknown CA, wrong certificate usage, host-name mismatch, and expired/not-yet-valid dates.

Set this to `1` when MDSS is serving its default self-signed certificate. Any other value (for example `2`) is a fatal configuration error. The setting has no effect on plain HTTP requests.

> Security note: `IgnoreCertErrors=1` disables certificate validation entirely and leaves the channel open to an on-path attacker. Use it only on trusted management networks, or install a certificate the connector's host trusts.

`Apikey`

The MDSS API key, sent as the `Apikey` HTTP header on every call the connector makes (`POST /api/webhook/realtime`, `GET /api/file/{correlationId}`, `GET /api/health`).

This will be automatically added when you download and install the OPSWAT ONTAP Connector from MDSS.

`StorageUnits`

The number of `[Storage Unit N]` sections that follow. Must be an integer of at least `1`; `0`, a negative number or a non-numeric value is a fatal configuration error.

The connector reads exactly the sections `[Storage Unit 1]` … `[Storage Unit <StorageUnits>]`. **Numbering must be consecutive and start at 1** — a gap causes the missing section's read to fail. Sections beyond the declared count are ignored.

Section `[Storage Unit N]`

One section per storage unit, numbered `1` to `StorageUnits`. Both keys are required in every section.

Key	Required	Type	Default	Description
`ClientId`	Yes	String	—	The MDSS storage client id
`SharePath`	Yes	String	—	ONTAP-side path prefix for this storage unit

`ClientId`

The client id of the storage configured in MDSS. It is sent as `storageClientId` in the real-time webhook payload and tells MDSS which storage the file belongs to. Copy it from the storage's configuration in MDSS.

`SharePath`

The ONTAP path prefix that identifies files belonging to this storage unit, for example `svm1\share1`. The value is used twice on each incoming scan request:

1. **Storage-unit selection.** The connector takes the path ONTAP sent and finds the first storage unit whose `SharePath` appears in it. The match is a case-insensitive substring search. If no unit matches, the file is dropped with `Failed to find a MDSS storage unit for file …` at `Error` level and ONTAP never receives a verdict for it.
2. **Computing the MDSS-relative path.** ONTAP paths arrive as `\\?\UNC\<path>`. The connector strips the 8-character `\\?\UNC\` prefix, then strips `SharePath` plus one separator from the front of what remains. The result is the relative path sent to MDSS as the file's `name`.

Because step 2 removes a fixed number of characters, `SharePath` must be **the exact leading portion of the ONTAP path after \?\UNC** — not merely a substring that happens to appear somewhere in it. A value that is too short or too long produces a wrong relative path and MDSS will not find the file.

Leading backslashes are stripped when the value is read, so `\svm1\share1` and `svm1\share1` are equivalent. Do not add a trailing separator.

When several storage units are configured, order matters: the first match wins, so avoid share paths where one is a prefix of another, or list the most specific first.

Section `[Settings]`

Every key in this section is optional. A missing or empty key falls back to its default; a present but invalid value is a fatal configuration error.

Key	Type	Default	Range / accepted values
`LogRetentionCountInDays`	Integer	`7`	`1` – `30`
`LogLevel`	String	`Information`	`Verbose`, `Debug`, `Information`, `Warning`, `Error`, `Fatal`
`FileProcessingTimeoutInSeconds`	Integer	`3600`	Any integer
`RpcLocalPipeHost`	String	`127.0.0.1`	An address, or the literal `NULL`
`ZoneIdentifierFiles`	Integer	`0`	`0` – `3`
`TimeoutResponse`	Integer	`4`	`0` – `5`

`LogRetentionCountInDays`

How many log files to keep. The connector writes one file per day to a `logs` folder next to the executable, named `YYYYMMDD.log`. A rotation thread runs every 10 seconds; it rolls over to a new file when the date changes and deletes the oldest files until only `LogRetentionCountInDays` remain.

Values outside `1` – `30` are rejected with `Value not in range [1,30]`.

`LogLevel`

The minimum severity written to the log. Messages below the configured level are discarded.

Value	Use
`Verbose`	Everything, including per-file ONTAP verdict mapping
`Debug`	Full HTTP request and response bodies exchanged with MDSS — the level to use when troubleshooting MDSS connectivity
`Information` (default)	Lifecycle events, per-file progress, configuration dump at startup
`Warning`	Transport switches, ONTAP service not yet available, non-fatal failures
`Error`	Failed operations
`Fatal`	Startup-blocking failures only

The value is compared case-sensitively, so it must be spelled exactly as listed — `information` is rejected with `Invalid LogLevel value ...`.

Note that the level only takes effect once the service main thread starts; configuration parsing itself is logged at `Verbose`, which is why the startup banner and the configuration dump always appear.

When the executable is run interactively (`--install`, `--uninstall`, `--upgrade`) output goes to the console instead of a file. File logging is used for `--service` and `--debug`.

`FileProcessingTimeoutInSeconds`

How long a single file may stay in the connector's pipeline, measured from the moment ONTAP's scan request was received. When the timeout is exceeded and MDSS has still not returned a final verdict — or the connector cannot reach MDSS or ONTAP at all — the connector gives up on the file: it sends the verdict configured in `TimeoutResponse` to ONTAP and removes the file from its tracking list. Exactly one timeout verdict is sent per file.

The default `3600` (one hour) is deliberately generous: it must accommodate the slowest case MDSS can produce, including large archives and Deep CDR. Lowering it makes the connector give up sooner on files MDSS is still working on. No range validation is applied to this key.

Files still in flight are persisted to `data.json` next to the executable every 3 seconds, so a connector restart does not lose pending work; the timeout continues to be measured from the original request time.

`RpcLocalPipeHost`

The network address the connector uses when binding to the NetApp registration pipe (`\pipe\ntapvscp`) exposed by the ONTAP AV connector service (`ontapavc`) on the same machine.

Value	Behaviour
`127.0.0.1` (default)	Binds the named pipe using the loopback address
Any other address	Binds using that address as the network address
`NULL` (the literal four-character string)	Binds with a null network address — the local machine, with no explicit host

Use `NULL` when the loopback binding is refused by the local RPC configuration. The connector retries the binding and the ONTAP registration every 3 seconds until both succeed, so a wrong value shows up as a repeating `RpcConnectionThread: Failed to create connection` or `Failed to register to RPC server` in the log.

`ZoneIdentifierFiles`

Controls how `:Zone.Identifier` alternate-data-stream files are handled. Windows creates these tiny metadata streams alongside downloaded files, and ONTAP submits them for scanning like any other file — which can double the request volume for no security benefit.

Value	Mode	Behaviour
`0`	Skip (default)	The request is logged and dropped. No scan, and **no verdict is returned to ONTAP** — ONTAP applies its own scan-request timeout policy.
1	Scan	Treated as a normal file and sent to MDSS through the usual pipeline.
2	Allow	An immediate allow verdict (`VSENGINE_NO_ERROR`) is returned without scanning.
3	Block	An immediate block verdict (`VSENGINE_INFECTED`) is returned without scanning.

Values outside `0` – `3` are rejected with `Value not in range [0,3]`.

Prefer `2` (Allow) over `0` (Skip) if ONTAP clients are seeing access delays on downloaded files: it settles the request immediately instead of leaving ONTAP waiting for its own timeout.

`TimeoutResponse`

The verdict sent to ONTAP when a file hits `FileProcessingTimeoutInSeconds`. Each value maps to a NetApp Vscan engine status, and it is ONTAP — not the connector — that decides what the client sees based on that status and the share's `scan-mandatory` setting.

Value	Mode	ONTAP status	Effect
`0`	Allow	`VSENGINE_NO_ERROR`	Access is allowed. The file is treated as clean.
1	TimeoutNoBlock	`VSENGINE_INTERNAL_TIMEOUT_NOBLOCK`	Access is allowed, but recorded as a scanner timeout.
2	InfectedBlock	`VSENGINE_INFECTED`	Access is always blocked and the file is reported as infected.
3	TimeoutBlock	`VSENGINE_INTERNAL_TIMEOUT_BLOCK`	Access is always blocked, with a timeout reason.
4	Timeout (default)	`VSENGINE_INTERNAL_TIMEOUT`	Blocked only where scanning is mandatory; allowed otherwise.
5	EngineBusyRetryLater	`VSENGINE_BUSY_TRY_AGAIN_LATER`	Reported as scanner busy so ONTAP can retry or hand the request to another scanner.

Values outside `0` – `5` are rejected with `Value not in range [0,5]`. Use `0` or `1` for availability-first deployments, `2` or `3` for security-first, and `5` when several scanners serve the same ONTAP cluster and another one should get a chance at the file.

Complete example

```
[MetaDefender Storage Security]
IP=10.0.0.15
Port=8008
PortSsl=8443
IgnoreCertErrors=1
Apikey=b1946ac92492d2347c6235b4d2611184
StorageUnits=2

[Storage Unit 1]
ClientId=6f1c2f7a-6c1e-4f9a-9c0e-3ac0d1f2b111
SharePath=ONTAP_ADMIN$

[Storage Unit 2]
ClientId=9d4b8e01-11aa-42cc-8e77-5b6c9d0e2222
SharePath=ONTAP_ADMIN$

[Settings]
LogRetentionCountInDays=14
LogLevel=Debug
FileProcessingTimeoutInSeconds=1800
RpcLocalPipeHost=127.0.0.1
ZoneIdentifierFiles=2
TimeoutResponse=4
```

The shipped template, with every optional key at its default:

```
[MetaDefender Storage Security]
IP=127.0.0.1
Port=80
PortSsl=443
IgnoreCertErrors=0
Apikey=
StorageUnits=1

[Storage Unit 1]
ClientId=
SharePath=

[Settings]
LogRetentionCountInDays=7
LogLevel=Information
FileProcessingTimeoutInSeconds=3600
RpcLocalPipeHost=127.0.0.1
ZoneIdentifierFiles=0
TimeoutResponse=4
```

Validation and troubleshooting

What the connector logs at startup

After parsing succeeds, the connector dumps the effective configuration at `Information` level — the resolved values, with defaults already applied. Three lines are written, one per section:

```
MetaDefender Storage Security <IP: 10.0.0.15. Port: 8008. PortSsl:
8443. IgnoreCertErrors: 1. Apikey: …>
Settings <LogRetentionCountInDays: 14. LogLevel: Debug.
FileProcessingTimeoutInSeconds: 1800. RpcLocalPipeHost: 127.0.0.1.
ZoneIdentifierFiles: 2. TimeoutResponse: 4>
Storage Unit <ClientId: 6f1c2f7a-…. SharePath: svm1\finance_share>
```

This is the fastest way to confirm the connector is reading the file you think it is, and that your edits took effect.

Error messages and their causes

Log message	Cause
`Failed to read from .ini file at location …`	The file is missing from the executable's folder, or a required key is absent
`Invalid format for key IP`	`IP` is empty, a hostname, or not a valid IPv4 address
`Invalid value (must be integer). Key: …`	A numeric key contains a non-numeric value
`Invalid value (must be 0 or 1). Key: IgnoreCertErrors`	`IgnoreCertErrors` is set to something other than `0` or `1`
`Value must be greater than 0. Key: StorageUnits`	`StorageUnits` is `0` or negative
`Value not in range [1,30] for key LogRetentionCountInDays`	Retention outside the supported range
`Value not in range [0,3] for key ZoneIdentifierFiles`	Unsupported Zone.Identifier mode
`Value not in range [0,5] for key TimeoutResponse`	Unsupported timeout response mode
`Invalid LogLevel value '…'`	Misspelled or wrongly-cased log level
`Invalid configuration inside config.ini file`	Summary line written after any of the above; the service does not start
`Failed to find a MDSS storage unit for file …`	No `SharePath` matches the path ONTAP submitted

Add an SFTP Storage

Product Specification Requirements	Version
Secure File Transfer Protocol (SFTP)	OpenSSH_for Windows_8.1p1 OpenSSH_7.9p1 Debian-10+deb10u2 OpenSSL 1.1.1(for Linux)

IMPORTANT

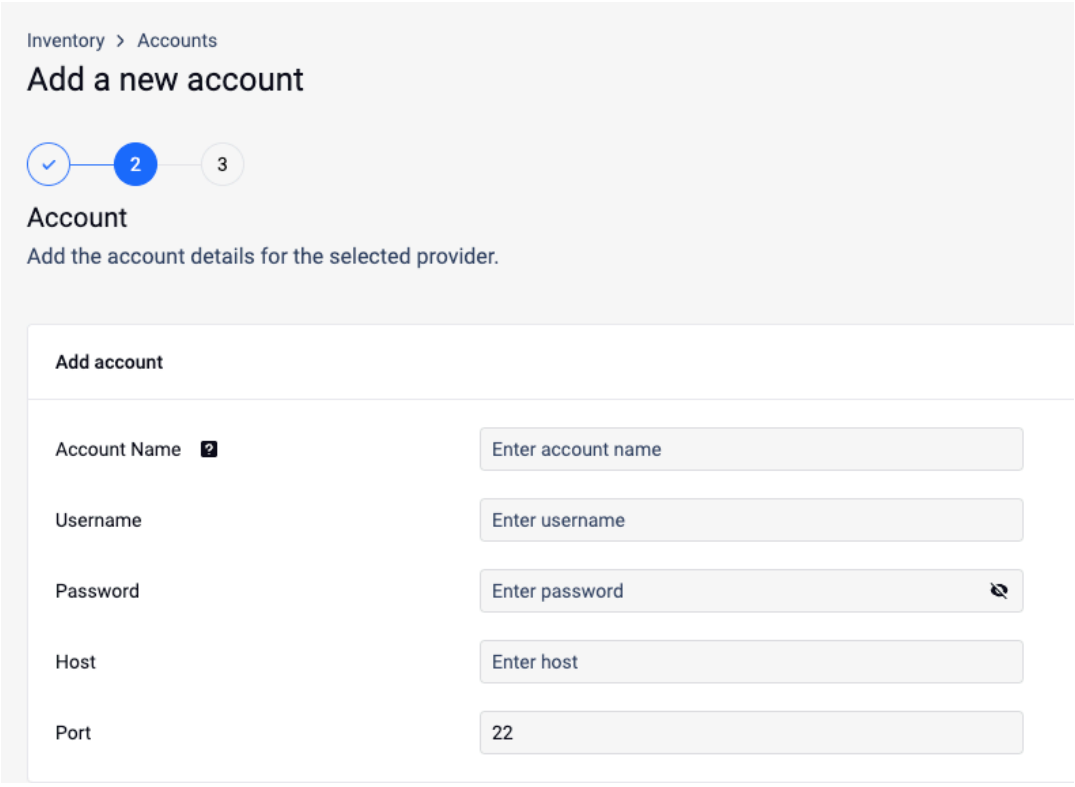
Integration with SFTP storage is achieved through the SSH File Transfer Protocol (SFTP). Before proceeding, please ensure that this protocol is enabled on your system. Our application is compatible with SFTP servers that adhere to the standard SSH File Transfer Protocol, including Cerberus SFTP for Windows and the OpenSSH SFTP subsystem, which is typically included with Linux and Unix SSH servers.

Info

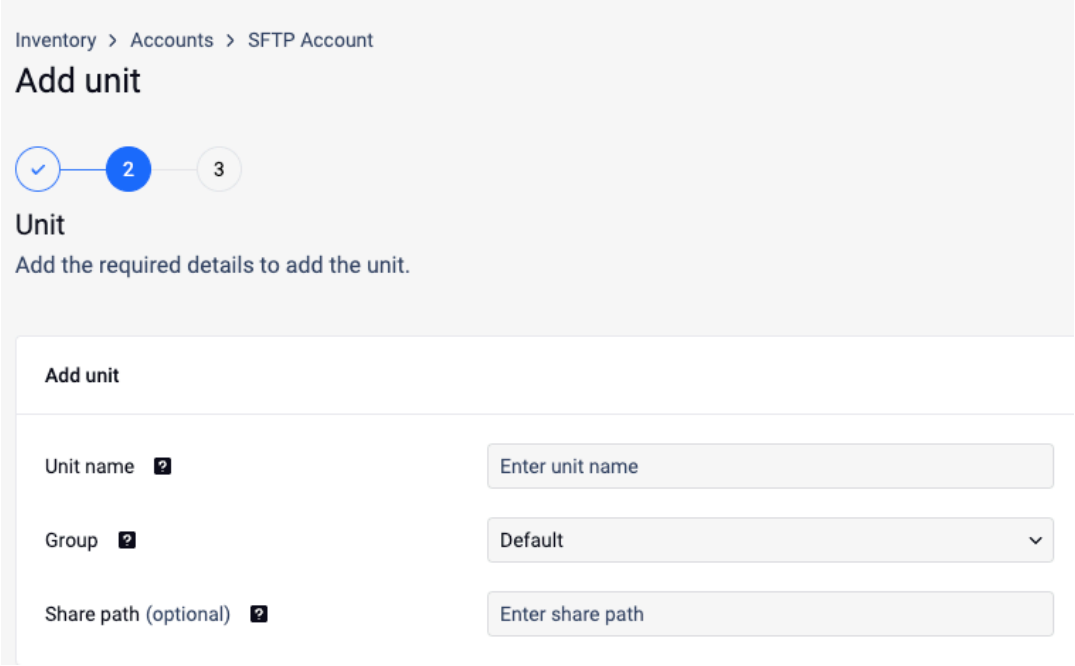
We recommend increasing the maximum number of concurrent connections allowed by your SFTP server from its default setting. This helps improve performance and prevent connection bottlenecks during high-load operations. After that, make sure to set the **SFTP_CONNECTION_POOL_MAX** environment variable in MDSS, which is at 100 by default.

In order to integrate SFTP with MetaDefender Storage Security please follow these steps:

1. From the left side menu, navigate to **Inventory**, click on **Add -> Account** and choose **SFTP**



2. Give your account a name so you can easily identify it later
3. Input the **Username** required to authenticate your access to the SFTP server. (The user should have at least read and write security permissions)
4. Provide the **Password** associated with the username provided at step 3.
5. **Host:** Enter the IP address of the SFTP server you wish to connect to.
6. **Port**: Specify the port number used for the SFTP connection, typically **22** for standard SFTP
7. Click **Next** in order to finish the process of adding the account
8. From the left side menu, navigate to **Inventory**, click on **Add -> Unit** and choose the previously created account



9. Give your unit an unique name so you can easily identify it later.
10. Assign your unit to a Group
11. (Optional) Indicate the specific directory path on the SFTP server from which you want to access files.

> **Info**
>
> The folder path should start from the root of the shared directory, not the absolute path of the server. For example, if the shared directory is `/shared_files` and you want to access a folder named `documents` within it, you would enter `documents` as the folder path, rather than the full path like `/home/user/shared_files/documents`

9. Click **Next** in order to finish the process.

> **Info**
>
> A SSH connection is required to be enabled in order to connect to a Unix-based system **SharePath.** If the SSH is not installed please run the following commands:
>
> ```
> sudo apt-get update
> ```
>
> ```
> sudo apt-get upgrade
> ```
>
> ```
> sudo apt-get install openssh-client
> ```

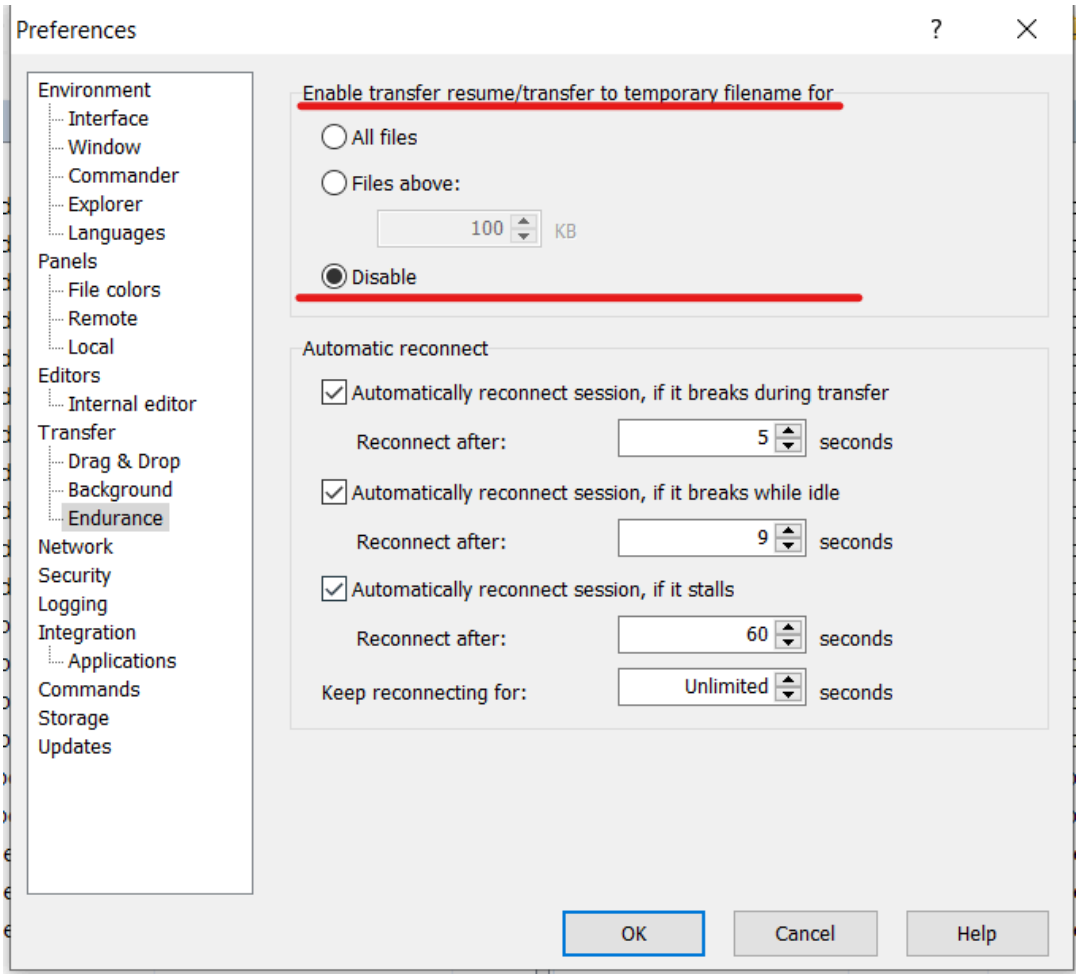
> **Info**

If you use a hostname in the host portion of IPv4/v6 socket address, the program may show a non-deterministic behavior. The socket address will be resolved differently into an actual IPv4/v6 address, depending on the results from DNS resolution and/or the host configuration. For deterministic behavior use a numeric address in host portion.

Warning

Please make sure that **Enable transfer resume/transfer to temporary filename** option is set on **Disable** if **using 3rd party SFTP clients** (if it allows this feature).

See the image below for **WinSCP client**.



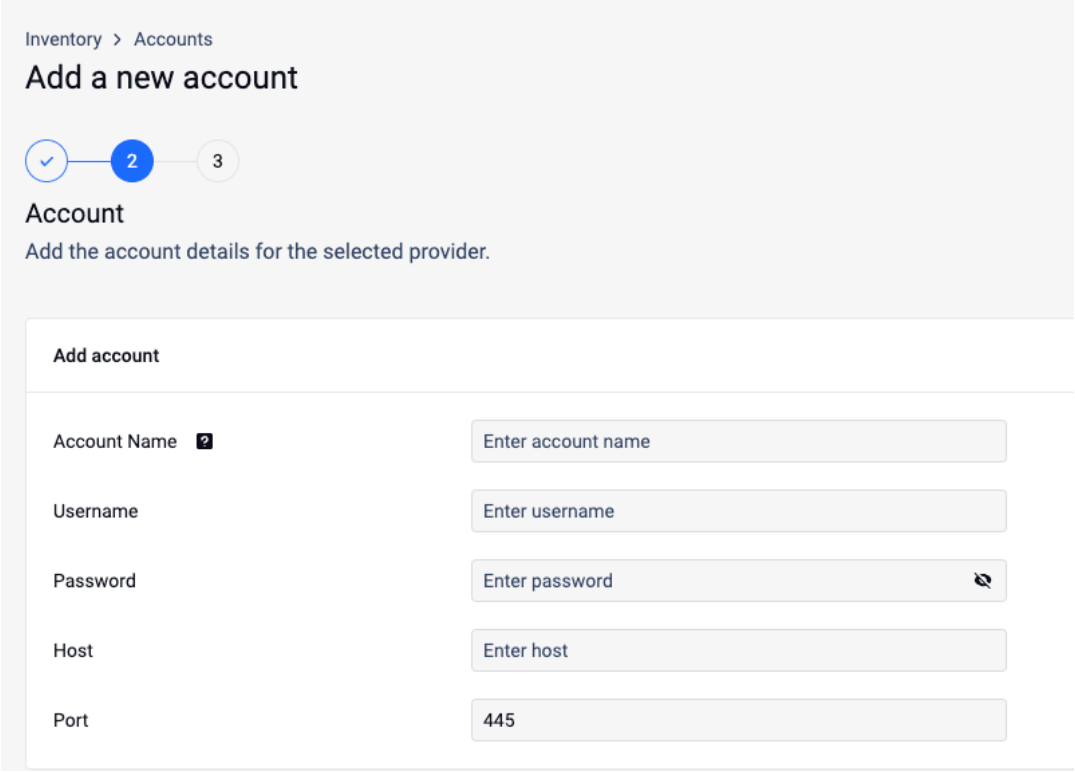
Add a Dell EMC Isilon Storage

Product Specification Requirements	Version
Dell EMC OneFS	Version 8.x
Service Message Block (SMB) protocol	SMB 3.1.1 (or SMB3)

> **Info**
>
> Integration with Dell Isilon is currently accomplished via the Service Message Block (SMB) protocol. Before you begin, you should ensure that this protocol is enabled in your Dell Isilon configuration.

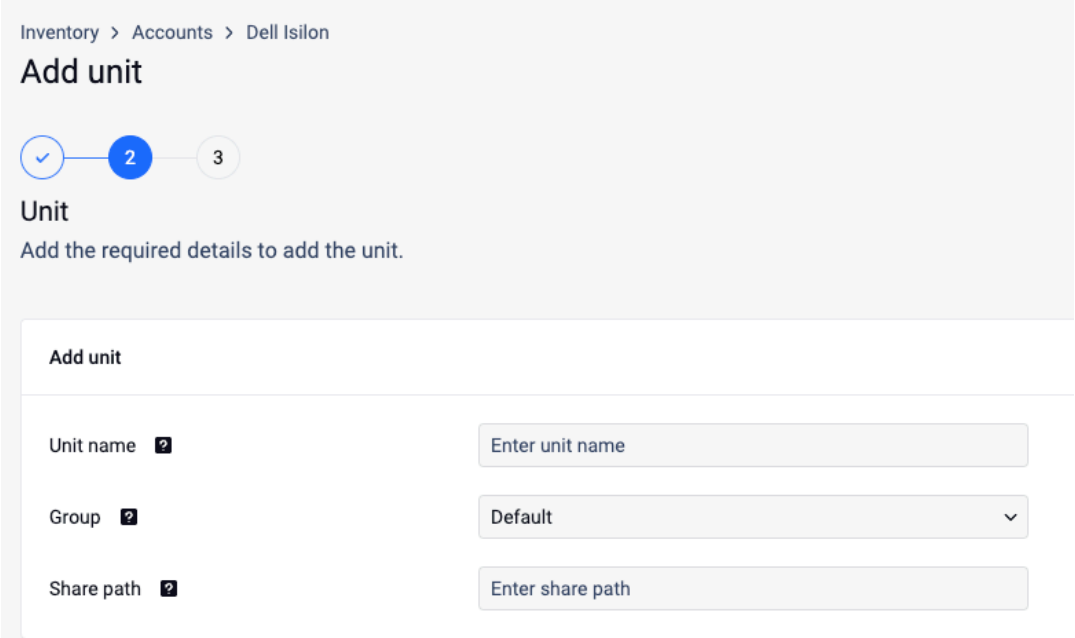
In order to integrate Dell Isilon with MetaDefender Storage Security please follow these steps:

1. From the left side menu, navigate to **Inventory -> Add -> Account -> Choose Dell Isilon**



2. Give your account a name so you can easily identify it later
3. Input the **Username** required to authenticate your access to the server. (The user should have at least read and write security permissions)
4. Provide the **Password** associated with the username from step 3.

5. **Host:** Enter the IP address of the server you wish to connect to.
6. **Port**: Specify the port number used for the connection, **445** being the default port
7. Click **Next** in order to finish the process
8. From the left side menu, navigate to **Inventory -> Add -> Unit -> **Choose the previously created account



9. Give your unit an unique name so you can easily identify it later
10. Assign your unit to a Group
11. Indicate the specific directory path on the server from which you want to access files
12. Click **Next** in order to finish the process.

Info

To avoid authentication issues the Username should have one of the following formats:

- local users should be .\username (for example: .\Administrator)
- domain users should be username@domain or domain\username

Info

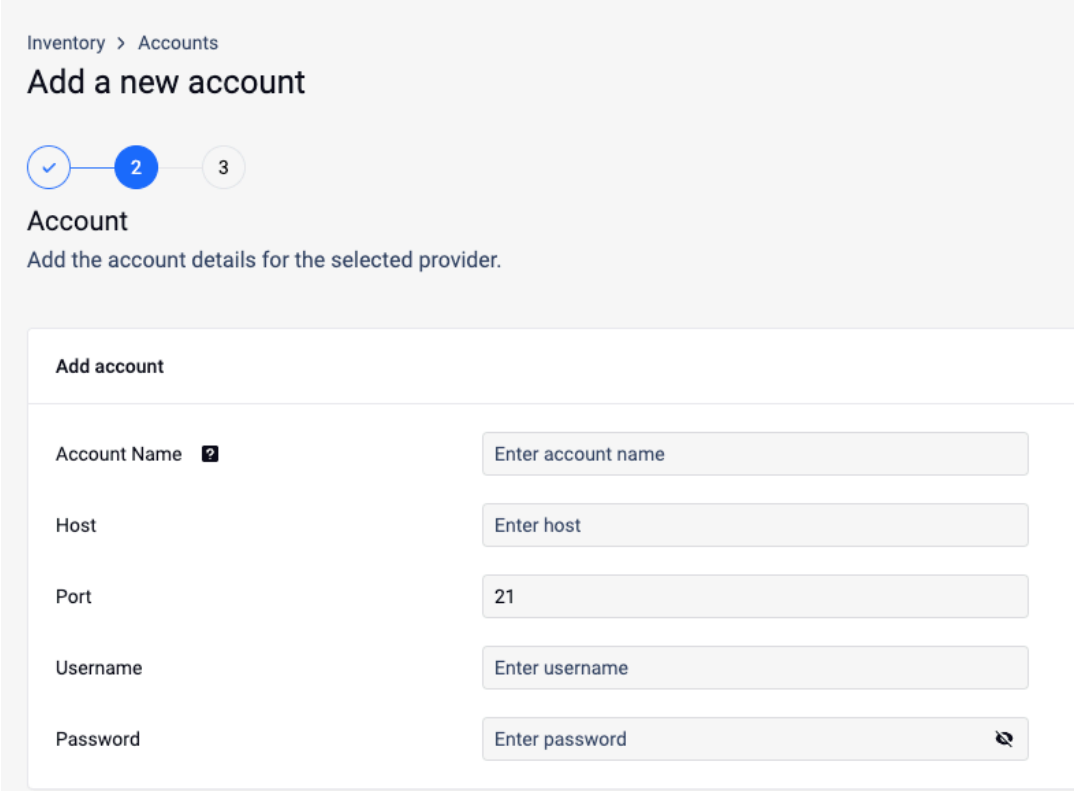
If you use a hostname in the host portion of IPv4/v6 socket address, the program may show a non-deterministic behavior. The socket address will be resolved differently into an actual IPv4/v6 address, depending on the results from DNS resolution and/or the host configuration. For deterministic behavior use a numeric address in host portion.

Add an FTP Storage

> **Info**
>
> We recommend increasing the maximum number of concurrent connections allowed by your FTP server from its default setting. This helps improve performance and prevent connection bottlenecks during high-load operations. After that, make sure to set the **FTP_MAX_CONNECTIONS** environment variable in MDSS

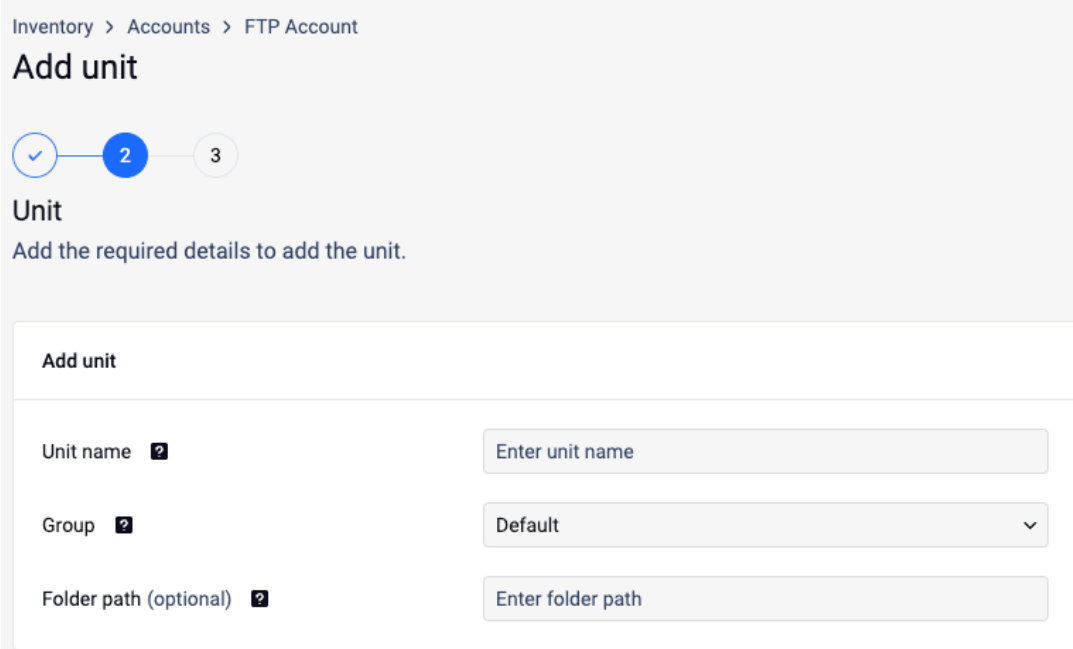
In order to integrate FTP with MetaDefender Storage Security please follow these steps:

1. From the left side menu, navigate to **Inventory**, click on **Add -> Account** and choose **FTP**



2. Give your account a name so you can easily identify it later
3. **Host:** Enter the IP address of the FTP server you wish to connect to.
4. **Port**: Specify the port number used for the FTP connection, typically **21** for standard FTP
5. Input the **Username** required to authenticate your access to the FTP server. (The user should have at least read and write security permissions)
6. Provide the **Password** associated with the username provided at step 4.

7. Click **Next** to finish the process
8. From the left side menu, navigate to **Inventory**, click on **Add -> Account ** and choose the previously created account.



8. Give your unit an unique name so you can identify it later
9. Assign your unit to a Group
10. Indicate the specific directory path on the FTP server from which you want to access files .
11. Click **Next** to finish the process

> **Info**
>
> The folder path should start from the root of the shared directory, not the absolute path of the server. For example, if the shared directory is `/shared_files` and you want to access a folder named `documents` within it, you would enter `documents` as the folder path, rather than the full path like `/home/user/shared_files/documents`

6. Click **Continue** in order to finish the process.

> **Info**
>
> If you use a hostname in the host portion of IPv4/v6 socket address, the program may show a non-deterministic behavior. The socket address will be resolved differently into an actual IPv4/v6 address, depending on the results from DNS resolution and/or the host configuration. For deterministic behavior use a numeric address in host portion.

Configuring a Windows IIS FTP Server for MDSS Scanning

Applies to: Microsoft IIS FTP on Windows Server · All MetaDefender Storage Security (MDSS) versions

MDSS scans FTP storage by opening a new passive data connection for every folder listing and every file it reads. One IIS setting governs how many of those connections the server can sustain — and its default is far too small for a scan. This page covers that setting, the connection limits that go with it, and how to verify the result.

---

1. Settings at a glance

Four server-side settings matter. Only the first one commonly breaks scans; the rest are usually already correct and just need confirming.

Setting	Recommended	IIS default	Priority
Data Channel Port Range	`10000-20000`	`0-0` (ephemeral)	**Must set**
Firewall rule for that range	Inbound TCP allow	none	**Must set**
Server Listen Backlog	`500`	`60`	Confirm
Max Connections	unlimited, or >= 200	`4294967295`	Confirm

> **Read this first**
>
> When an FTP scan fails, **Max Connections and Server Listen Backlog are the settings everyone checks, and they are almost never the cause** — IIS ships with Max Connections effectively unlimited. The setting that actually stops scans is the passive **Data Channel Port Range**, because it is consumed by connection turnover rather than by how many clients are connected. Check it first.

---

2. Set the data channel port range

Every listing and every file transfer takes one port from this range. When the transfer finishes, Windows holds that port in `TIME_WAIT` for 120 seconds before it can be reused. A range of a handful of ports therefore supports only a handful of operations every two minutes, which a scan exhausts in seconds.

This range is server-wide — one range covers every FTP site on the machine. Run all commands in an **elevated** PowerShell session on the FTP server.

```
& "$env:windir\system32\inetsrv\appcmd.exe" set config -
section:system.ftpServer/firewallSupport `
  /lowDataChannelPort:10000 /highDataChannelPort:20000
```

Choosing your own numbers is fine, as long as they satisfy all four constraints:

- **At least 1000 ports** — see How many ports you need.
- **Within 1025-65535** — IIS rejects anything lower.
- **Below 49152**, so the range never overlaps the Windows dynamic port range. Confirm your own with `netsh int ipv4 show dynamicport tcp`.
- **Clear of reserved and in-use ports.** Hyper-V, Docker and WinNAT silently reserve large blocks; a range overlapping one will fail to bind.

Check the range you picked is free:

```
netsh int ipv4 show excludedportrange protocol=tcp

Get-NetTCPConnection -State Listen |
  Where-Object { $_.LocalPort -ge 10000 -and $_.LocalPort -le 20000 } |
  Select-Object LocalPort, @{n='Process';e={(Get-Process -Id
$_.OwningProcess).ProcessName}}
```

No overlapping exclusions and no listeners returned means the range is yours to use.

---

3. Allow the range through the firewall

Widening the range achieves nothing if the firewall still blocks it. Scope the rule to the MDSS host so you are not opening 10,000 ports to the whole network.

```
New-NetFirewallRule -DisplayName "IIS FTP Passive Data Channel 10000-
20000 (MDSS)" `
  -Direction Inbound -Action Allow -Protocol TCP -LocalPort 10000-20000
`
  -RemoteAddress 10.0.0.50 -Profile Any
```

> **Use the MDSS host address, not the container address**
>
> The MDSS FTP services run in Docker, and their outbound traffic is source-NAT'd to the Docker host. The address to allow is the **MDSS host** IP — never the internal `172.x.x.x` container address.

To read the address the FTP server actually sees, run this while a scan or a storage **Test connection** is in progress:

```
Get-NetTCPConnection -LocalPort 21 -State Established |
  Select-Object -ExpandProperty RemoteAddress -Unique
```

If the MDSS host uses DHCP, give it a static address or a reservation first — otherwise the rule silently stops matching the next time the lease changes.

For multiple MDSS hosts, `-RemoteAddress` accepts a list `[@('10.0.0.50','10.0.0.51')]` or a subnet `['10.0.0.0/24']`. Scope the existing port 21 rule the same way — there is little point restricting the data channel while the control channel accepts connections from anywhere.

---

4. Confirm the connection limits

These two settings live on the FTP site rather than the server. Max Connections caps how many clients may be connected at once; Server Listen Backlog caps how many connection attempts can queue while the service is busy. MDSS connects in bursts, so a small backlog causes intermittent failures under load.

Substitute your own FTP site name:

```
$site = "Your FTP Site Name"

& "$env:windir\system32\inetsrv\appcmd.exe" set site /site.name:"$site"
`
  /ftpServer.connections.maxConnections:4294967295 `
  /ftpServer.connections.serverListenBacklog:500
```

`4294967295` is the IIS value for unlimited and is the default, so in most cases this command changes nothing but is harmless to run. Set it explicitly if a previous administrator lowered it. If your policy requires a real cap, size it to at least **200**: MDSS runs three services that each maintain their own connection pool, and a single host can hold up to 48 sessions before you account for retries or a second MDSS instance.

If `appcmd` rejects the syntax on your IIS version, set the same two values through **IIS Manager → select the FTP site → Advanced Settings → ftpServer → connections**.

If the FTP server is behind NAT

The server tells the client which address to open the data connection on. Behind NAT it will advertise its private address unless you tell it otherwise, and every data connection will fail.

```
& "$env:windir\system32\inetsrv\appcmd.exe" set config -
section:system.applicationHost/sites/siteDefaults `
  /ftpServer.firewallSupport.externalIp4Address:"203.0.113.10"
```

Use the address MDSS connects to. Any intervening firewall must also forward the same data channel port range.

---

5. Restart and verify

IIS only picks up a changed data channel range when the FTP service restarts. This drops any FTP session in progress, so do it outside a scan window.

```
net stop ftpsvc
net start ftpsvc

Get-Service ftpsvc | Select-Object Name, Status

Select-String -Path
"$env:windir\system32\inetsrv\config\applicationHost.config" `
  -Pattern
'firewallSupport|maxConnections|serverListenBacklog|externalIp'
```

The service should report `Running`, and the configuration should show your new `lowDataChannelPort` and `highDataChannelPort`.

Now start a scan from MDSS and, while it runs, confirm data connections are landing in the new range:

```
Get-NetTCPConnection | Where-Object { $_.LocalPort -ge 10000 -and
$_.LocalPort -le 20000 } |
  Group-Object State | Format-Table Name, Count
```

A healthy result shows a handful of `Established` connections and a larger, **stable** count of `TimeWait` entries. Stable is the important word: a count that plateaus means ports are being recycled as fast as they are consumed. A count that climbs steadily toward the size of your range means the range is too small — widen it.

---

6. How many ports you need

Port demand is driven by connection turnover, not by how many files the storage holds:

```
ports needed  ~=  new data connections per second  x  120
```

The 120 is the Windows `TIME_WAIT` delay in seconds. A production MDSS scan measured roughly six new data connections per second, which held about 750 ports in use at steady state — against an IIS default that often leaves only a handful available.

Deployment	Range	Ports
Single MDSS host, light scanning	`10000-11000`	1001
Standard — recommended default	`10000-20000`	10001
Multiple MDSS hosts, or real-time plus on-demand	`10000-20000` with a shorter `TIME_WAIT`	10001

A bigger range costs nothing — IIS does not reserve the ports, it just draws from the range on demand.

For the heaviest workloads you can instead attack the other half of the formula and shorten `TIME_WAIT`, which multiplies the capacity of whatever range you chose:

```
New-ItemProperty -Path
'HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters' `
  -Name 'TcpTimedWaitDelay' -PropertyType DWord -Value 30 -Force
```

Valid values are 30-300 seconds. Going from 120 to 30 quadruples effective capacity. Unlike the other changes on this page, this one needs a full reboot rather than an FTP service restart.

---

7. If scans still fail

A misconfigured data channel produces this error in the MDSS FTP discovery log, usually preceded by several `Transient FTP error detected, retrying with fresh client` warnings a few seconds apart:

```
System.IO.IOException: FTP passive data-channel connection to the
server failed.
 ---> System.NullReferenceException: Object reference not set to an
instance of an object.
   at FluentFTP.AsyncFtpClient.OpenDataStreamAsync(...)
```

The signature to recognise: logins succeed and the control channel works, but every data connection fails immediately. Work through these in order.

1. **Is the port range wide enough?** Run `appcmd list config -section:system.ftpServer/firewallSupport`. Anything under a few hundred ports is the cause.

2. **Did the FTP service restart** after the range changed? Without it, IIS is still using the old range.
3. **Does the firewall rule match the new range exactly,** and is it scoped to the right source address? A rule left pointing at an old narrow range fails identically.
4. **Watch the drops directly.** Enable logging, reproduce, then read it — dropped entries name the exact ports being refused.

```
Set-NetFirewallProfile -All -LogBlocked True

# reproduce the failure, then:
Get-Content "$env:systemroot\system32\LogFiles\Firewall\pfirewall.log"
-Tail 200 |
  Select-String 'DROP'

# turn logging back off when finished
Set-NetFirewallProfile -All -LogBlocked False
```

If the range and the firewall both check out, look at what the server advertises in its passive reply — a private or unexpected address there points back to the NAT setting in section 4. The IIS FTP logs under `%SystemDrive%\inetpub\logs\LogFiles\FTPSVC<n>` record every command, and the `sc-win32-status` column on failing `LIST` entries gives the underlying Windows error.

---

8. MDSS-side settings

Both of these are optional and read from the MDSS `.env` file. Neither is a substitute for the server configuration above, and both need `docker compose restart ftp-services` to take effect.

Variable	Default	Guidance
`FTP_MAX_CONNECTIONS`	unset	Unset, each service starts at 3 connections and grows to a maximum of 16. Set it only when the FTP server genuinely limits concurrent sessions; lowering it does not relieve data channel port exhaustion.
`FTP_LIST_USE_STAT`	`false`	Leave off for IIS. It moves listings onto the control channel, but returns zero items against IIS FTP — discovery appears to succeed while finding nothing.

Every command on this page runs in an elevated PowerShell session on the FTP server

Add a Scality RING Storage

1. Prerequisites

In order to Add a **Scality RING** storage in MDSS, you will need the **Service URL**, **Access Key Id / Secret Access Key** and the **bucket name**.

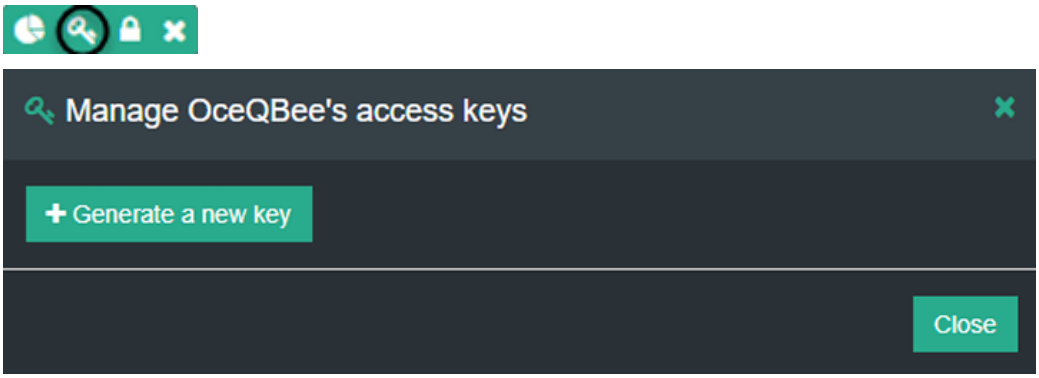
2. Obtaining the Service URL

The Service URL is the S3 endpoint URL of your Scality RING, used to access the S3 services on the RING. It is typically available via the **Supervisor interface** under **S3 Services**.

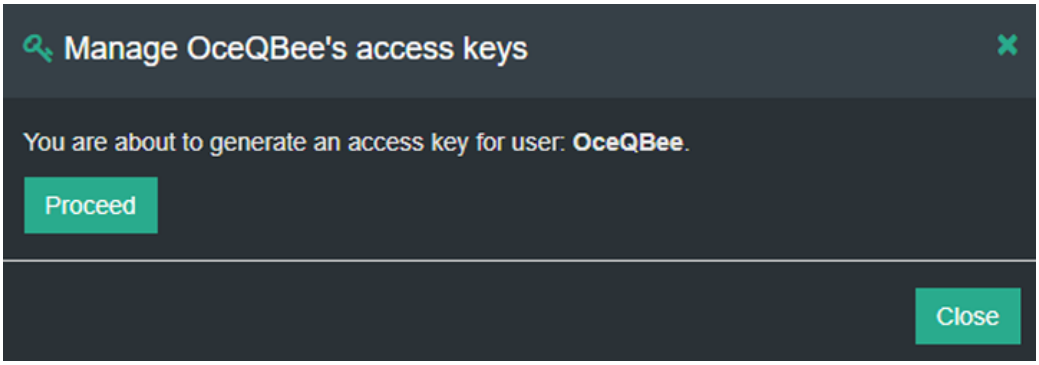
3. Obtaining Access Keys

Access keys are managed through the Scality RING Supervisor's S3 Console.

1. Click the target account's Actions Key icon to call the Manage access keys dialog.

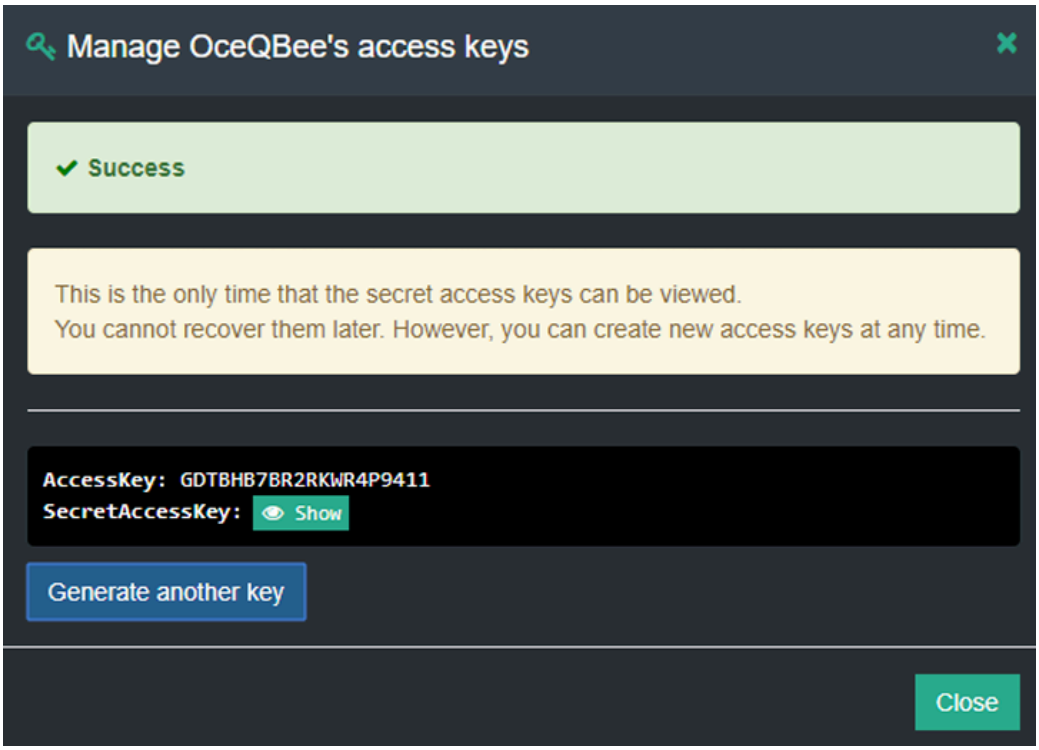


2. Click Generate a new key. A confirmation dialog will display.



3. Click Proceed to trigger account access key creation. The dialog will indicate the success of the operation, as well the AccessKey (click Show to view the

SecretAccessKey).



> **Warning**
>
> Copy and save SecretAccessKey to a secure location. It is not shown again and cannot be recovered later.

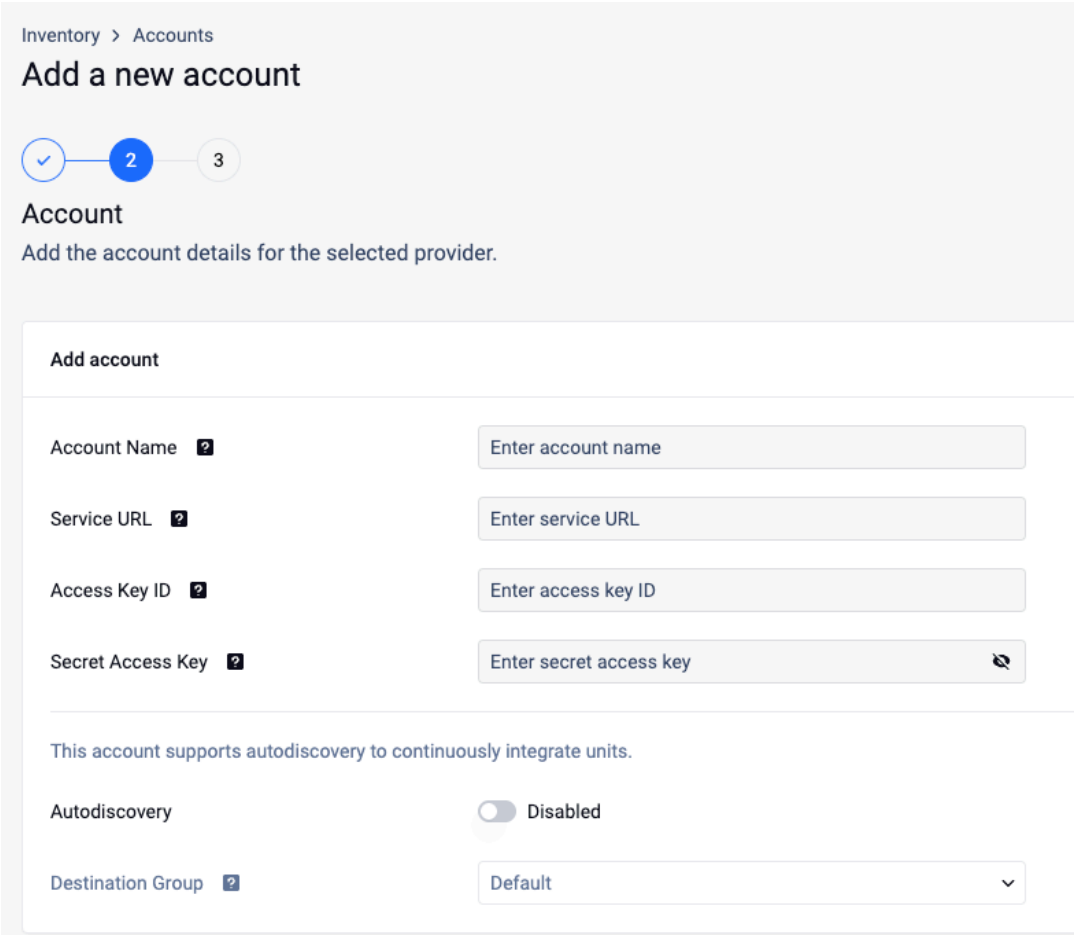
4. Obtaining the bucket name

1. **Go to Buckets:** Locate the “Buckets” section
2. **Identify Bucket:** Find your bucket in the list and note its name.

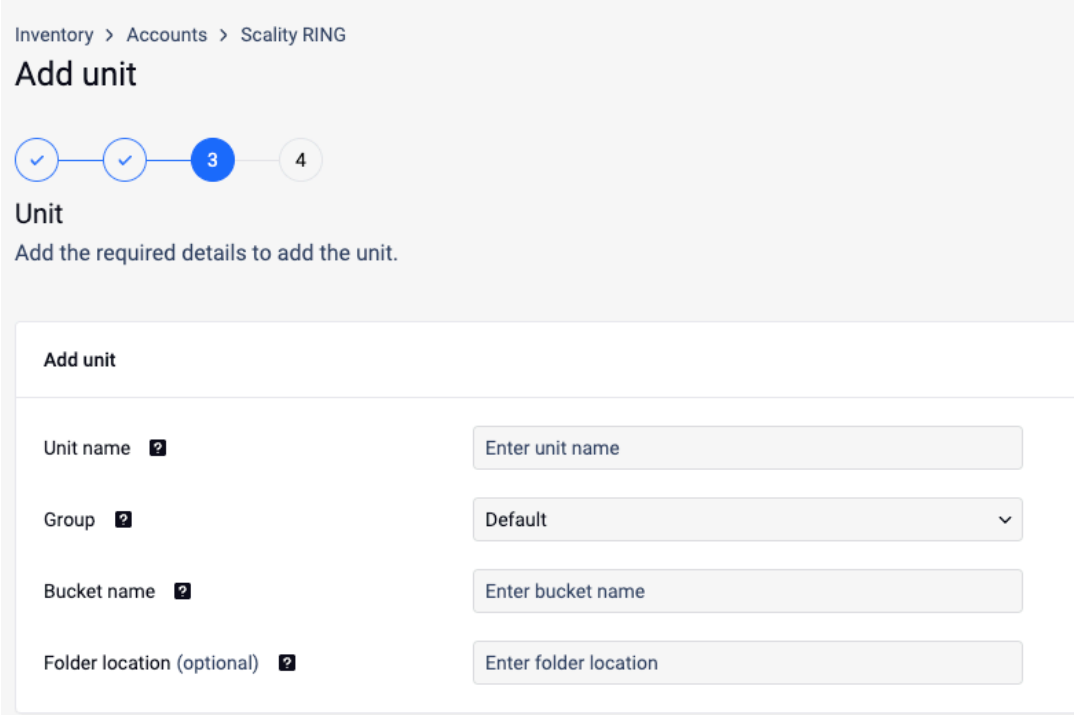
5. Adding Scality RING storage in MDSS

In order to integrate Scality RING with MetaDefender Storage Security please follow these steps:

1. From the left side menu, navigate to **Inventory,** click on **Add -> Account **and choose **Scality RING**



2. Give your account a name so you can easily identify it later
3. Enter the Service URL for your Scality RING endpoint
4. Enter your **Access Key ID**. Scroll to the end of this page for more details.
5. Enter your **Secret Access Key.** Scroll to the end of this page for more details.
6. (Optional) Enable Autodiscovery
7. Once the account is successfully added, navigate to Inventory -> Add Unit -> Choose the previously created account



9. Give your unit an unique name
10. Choose Group
11. Enter a valid bucket name
12. Enter a Folder location (optional)
13.

Necessary policies

These are the necessary policies required in order to add a Scality RING Storage:

- `s3:GetObject`
- `s3:PutObject`
- `s3:GetObjectVersion`
- `s3:ListBucket`
- `s3:ListBucketVersions`
- `s3:GetObjectTagging`
- `s3:GetObjectVersionTagging`
- `s3:PutObjectTagging`
- `s3:PutObjectVersionTagging`
- `s3:DeleteObject`
- `s3:DeleteObjectVersion`

To be able to use client side encryption, additional AWS policies are required:

- `secretsmanager:GetSecretValue`

- `kms:DescribeKey`
- `kms:Decrypt`

To be able to use **server-side encryption with AWS Key Management Service (SSE-KMS)**, additional AWS policies are required:

- `kms:GenerateDataKey`
- `kms:DescribeKey`
- `kms:Decrypt`

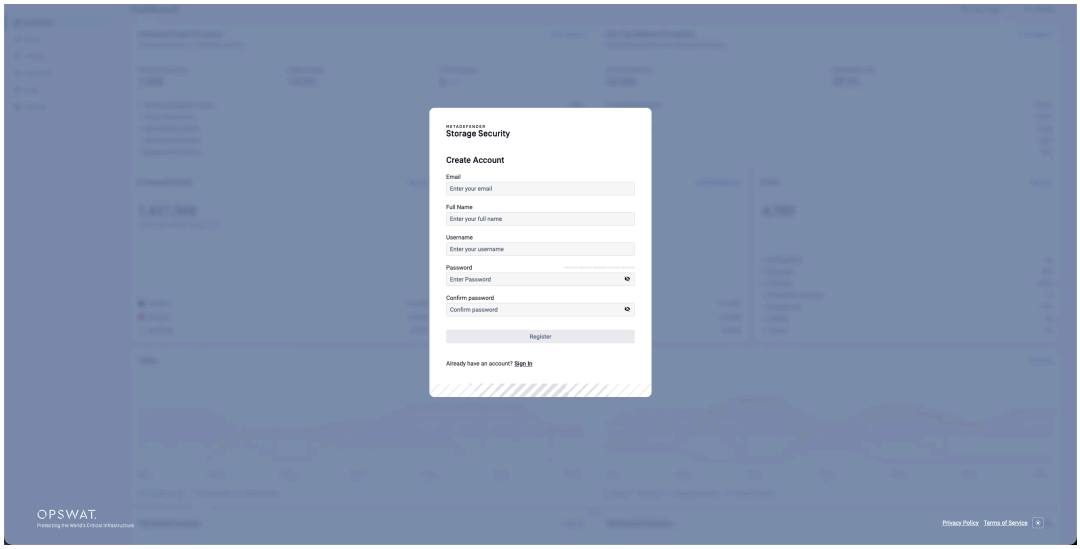
To be able to use **autodiscovery**, additional AWS policies are required:

- s3:ListAllMyBuckets

Operations

Onboarding

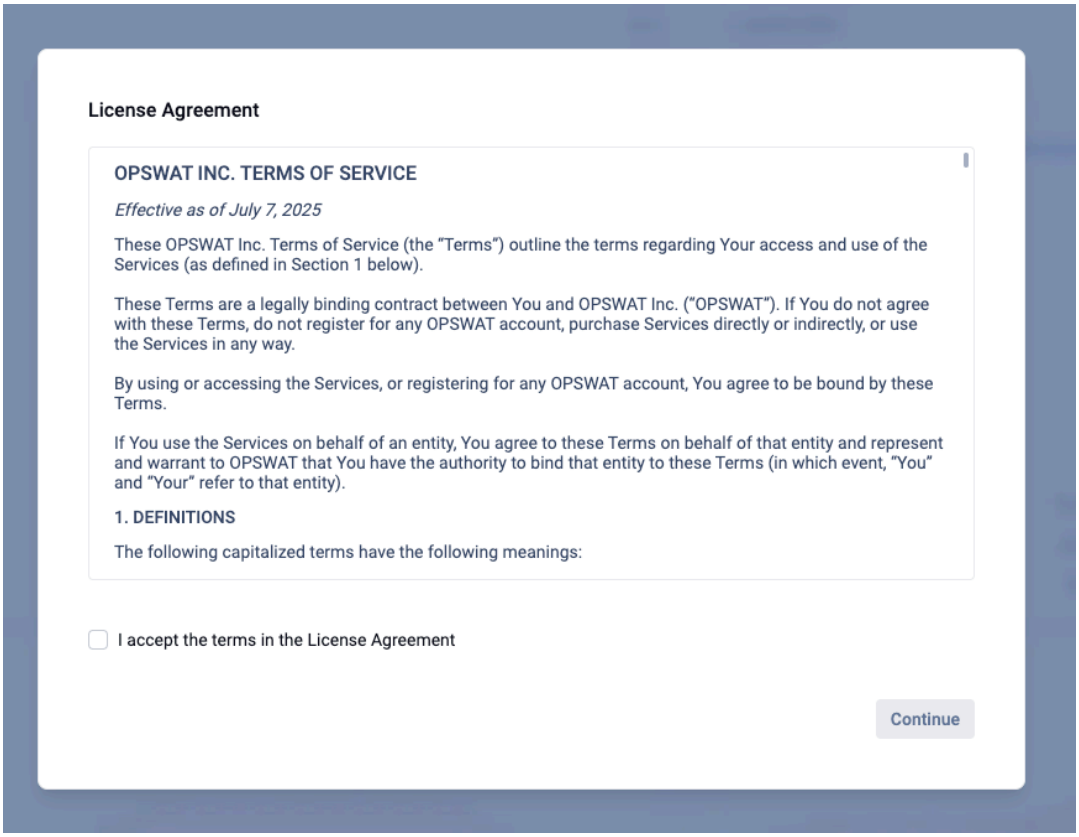
Once you've completed the installation you are ready to configure MetaDefender Storage Security. To begin, please navigate using your preffered browser to the MetaDefender Storage Security web interface which is located by default at http://:80. You will see the following screen:



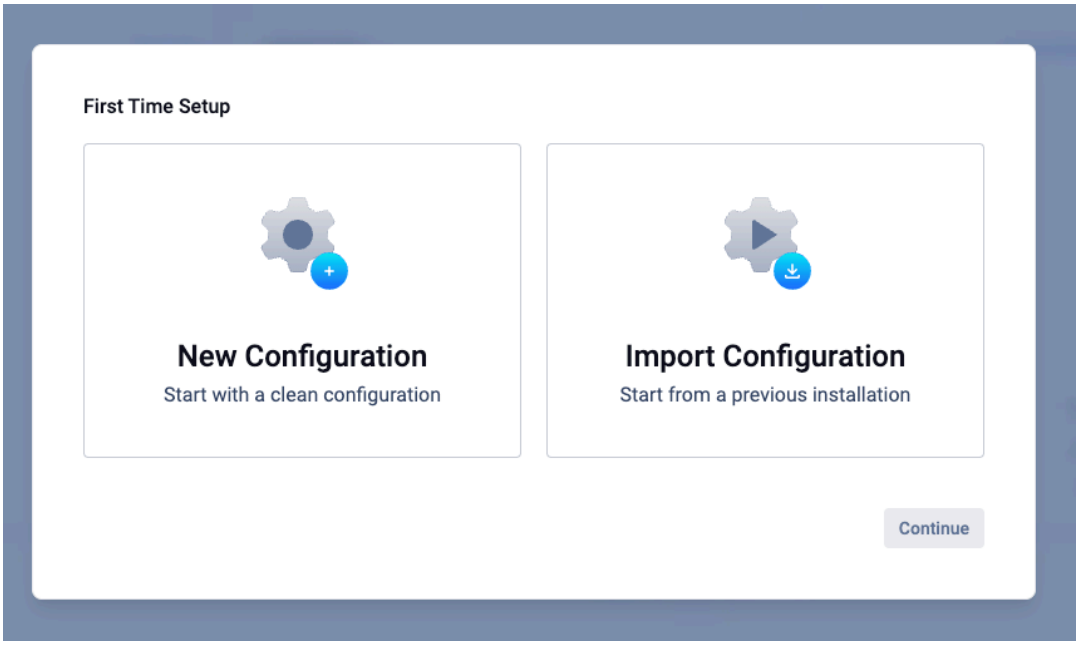
Create your account by filling the necessary information.

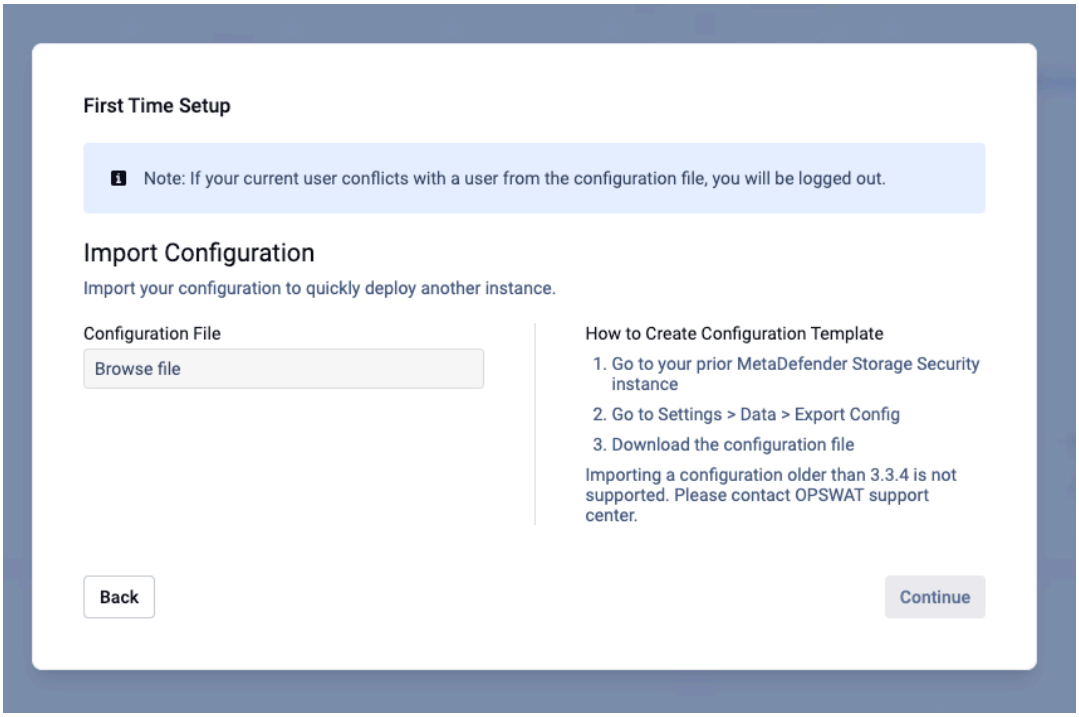
When you are ready, click **Register**. And then login using your newly created account. You are now ready to begin the initial configuration wizard.

Before starting the process, please accept our Licensing Terms of Service.

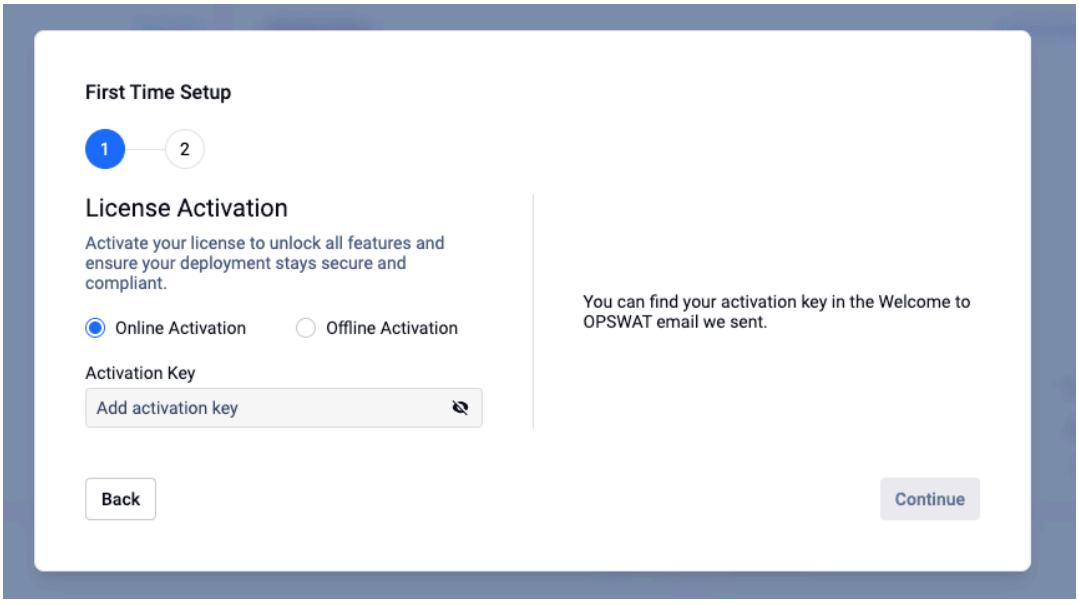


In this step, you can start with a new configuration, or import an existing configuration so that all your saved settings are restored.





The next step is to apply a license:



Choose between the following options:

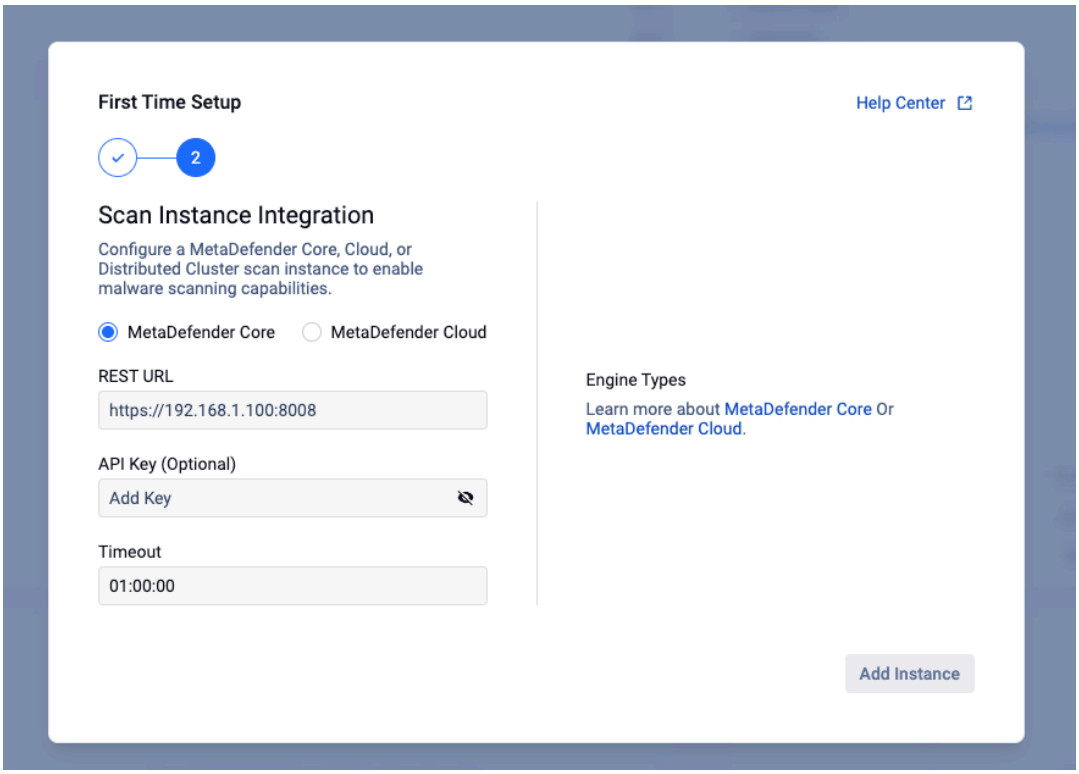
- Online activation: your license will be online validated against OPSWAT's activation server.
- Offline activation: you will upload a file that you previously generated from My OPSWAT
- Trial: if you don't have a license, please contact OPSWAT in order to receive one.

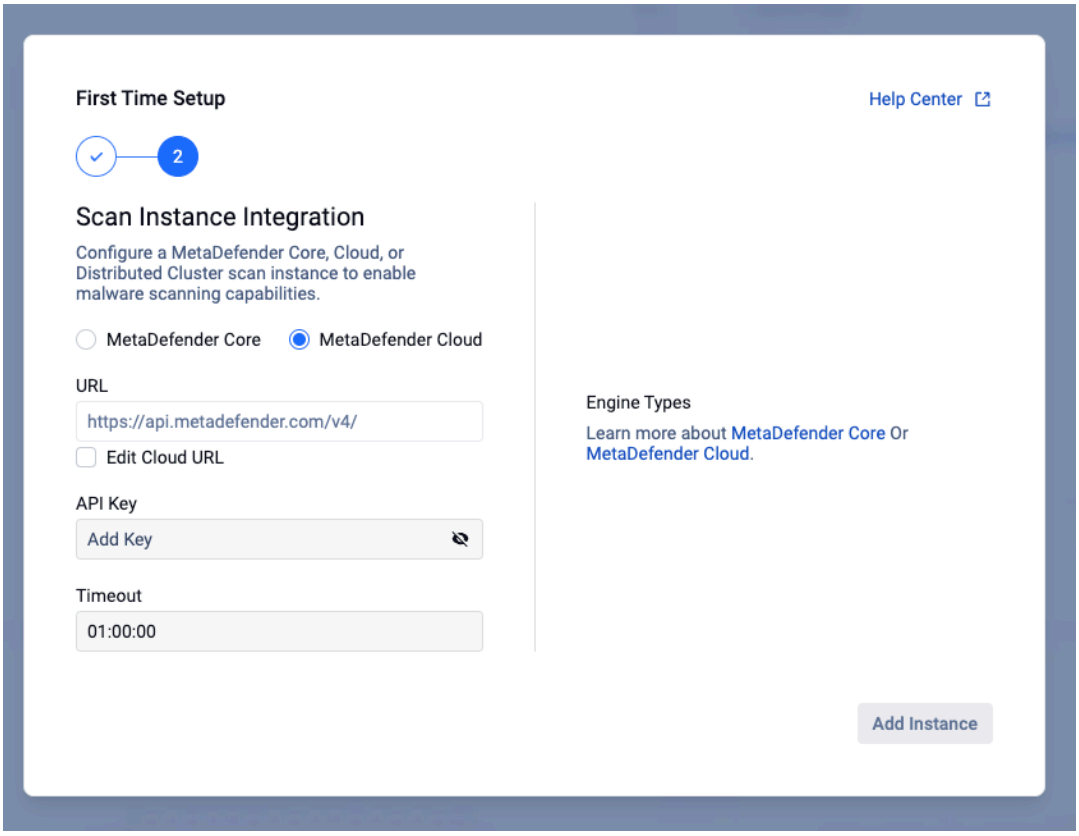
Once your instance of MetaDefender Storage Security is activated you can proceed to the next step.

In the next step, you'll be integrating MetaDefender Storage Security with MetaDefender Core or MetaDefender Cloud.

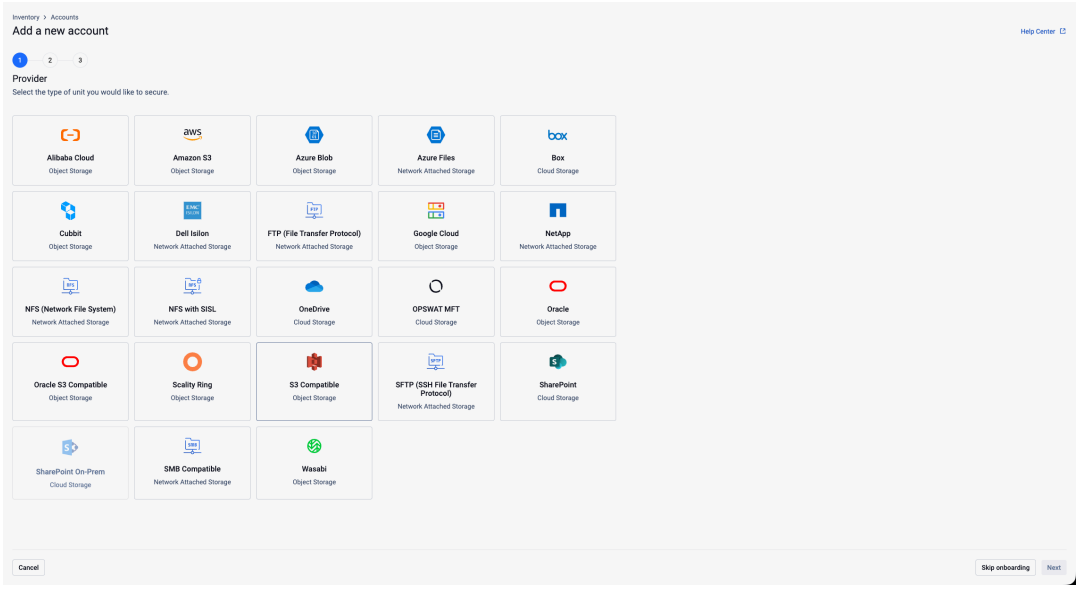
MetaDefender Core is an advanced malware protection and detection system that offers high-speed multi-scanning, deep content disarm and reconstruction (Deep CDR), and file-based vulnerability assessment technologies, preventing zero-day attacks and unknown threats as well as providing close to 100% known threat detection, without affecting performance. Click here to learn more about MetaDefender Core.

After choosing between MetaDefender Core or MetaDefender Cloud, you will be prompted with a form to complete the integration.





After MetaDefender Core/Cloud integration is done, you can start configuring an account or skipping the onboarding:



For a detailed tutorial on how to integrate a specific account and storage unit, please visit the Integrations section.

Browser Requirements for the Web Console

The following browsers are suggested to view the MetaDefender for Secure Storage Web Console:

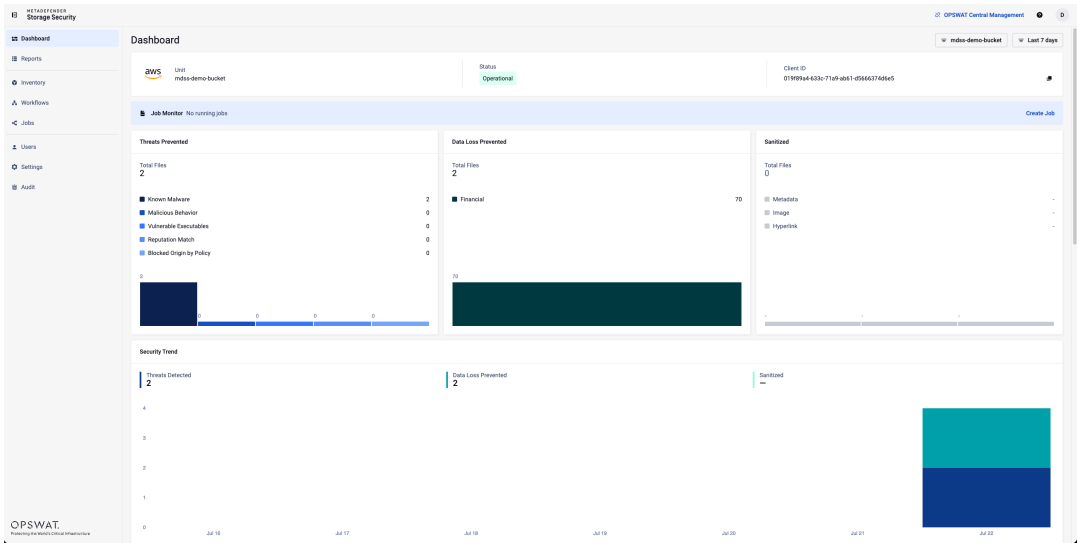
- Microsoft Edge
- Chrome
- Firefox
- Safari

Chrome, Firefox, Safari, and Edge browsers are tested with the latest available version at the time of release.

> **IMPORTANT**
>
> Note that Internet Explorer is no longer supported. Please upgrade to another supported browser (listed in the **Installation** section) to access the MetaDefender Storage Security web interface.

Dashboard

The MetaDefender Storage Security dashboard is the page where you can see an overview of your storage and find information about file processing and usage statistics as well as details about currently running processes or upcoming ones.



Key Features at a Glance

- The dashboard begins with a dynamic activity feed, displaying the most recent scan results, file processing statuses, and any detected threats. This immediate visibility allows you to quickly assess the current state of your storage security.
- Quick access to essential configuration settings, user management, and other key sections of MetaDefender Storage Security is available through the navigation menu on the right. Customize your setup, manage users, and fine-tune your security policies directly from this central location.
- Gain a quick understanding of your system's performance with key statistics displayed prominently in the center. See the total number of files processed, detected threats, and other critical metrics at a glance.
- Dive deeper into file processing details with a breakdown of processed, sanitized, and blocked files. Understand the efficiency of your security measures and identify any potential bottlenecks.
- Monitor threat detection effectiveness with clear visualizations of potentially malicious files, permanently unavailable files, and possible threats.
- Track system performance over time with an interactive graph. Analyze file processing trends and identify any performance anomalies.
- Access in-depth analysis of individual files, including threat assessment results and remediation actions. This granular view allows you to understand the specific threats detected and take appropriate action.

Why the Dashboard Matters

The MetaDefender Storage Security dashboard is designed to be your primary point of interaction with the system. It provides the essential information you need to:

- Stay informed about the real-time security status of your storage.
- Understand system efficiency and identify areas for optimization.
- Customize settings and policies to meet your specific security requirements.
- Quickly address detected threats and mitigate potential risks.

Dashboard Counters

Previously, the MetaDefender Storage Security dashboard provided a consolidated view of compliance and security metrics, offering insights into potential violations and threats. While these metrics remain critical for understanding your security posture, they are now presented in more detail within their respective technology sections: Multiscanning, Content Disarm and Reconstruction (CDR), and Data Loss Prevention (DLP).

Key Compliance and Security Metrics (Now Found in Dedicated Sections)

These categories, though no longer directly visible on the main dashboard, are still essential for comprehensive security analysis and are now located within the dedicated sections for each technology:

- Compliance Violations (DLP Section):
  - PCI-DSS (Payment Card Industry Data Security Standard): Tracks files containing Credit Card Numbers (CCN).
  - HIPAA (Health Insurance Portability and Accountability Act): Identifies files containing protected health information (e.g., full name, address, date of birth, phone number, email, SSN, bank account, passport).
  - GDPR (General Data Protection Regulation): Monitors files with personally identifiable information (PII) as defined by GDPR (e.g., full name, address, date of birth, phone number, email, bank account, passport).
- Security Alerts (Multiscanning and Vulnerability Assessment Sections):
  - Malware: Displays the number of potentially dangerous files detected by our multi-scanning technology.
  - Vulnerabilities: Shows the number of files with known vulnerabilities identified by our File-Based Vulnerability Assessment engine.
- PII Data (DLP Section) tracks files containing personally identifiable information (e.g., full name, bank account, passport, email, SSN).

Why These Metrics Still Matter

- Demonstrating adherence to industry regulations.
- Identifying potential malware and vulnerabilities.
- Protecting sensitive information from unauthorized access.

Where to Find These Metrics Now:

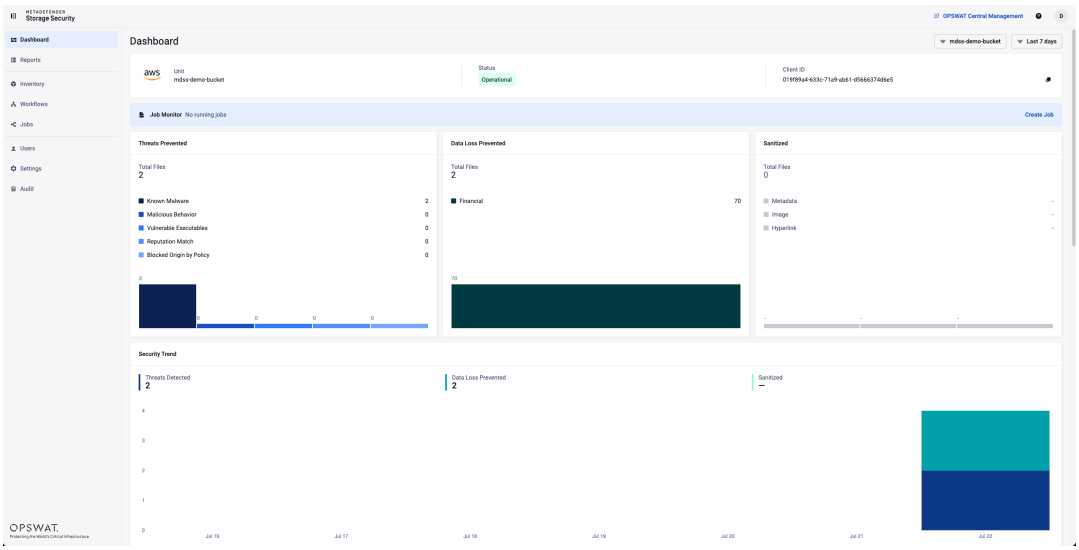
For detailed information on these metrics, please click on each dedicated sections for: Multiscanning, CDR and DLP.

> **Info**
>
> Please check the MetaDefender Core sample regular expression page for a list of rules that are being used to match full names, US addresses, birth dates, etc.

> **Info**
>
> The small arrows below each category shows you a percentage increase or decrease based on the previous scan.

Processing Overview

You can select to view data for the last week, month or even the last year. The height of the bar represents the volume of files processed by MetaDefender Storage Security. Hover over it to see more details:



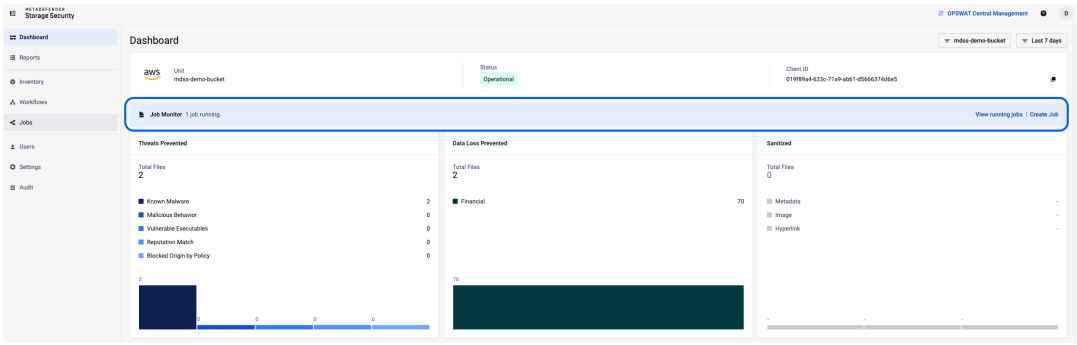
The processed quantity field represents the total amount of data processed with MetaDefender Storage Security. This quantity will exceed your actual storage data if you have triggered more than one process in the defined time unit (day or month). That is

because every time you process a file this quantity will be increased even if you've processed the same file multiple times.

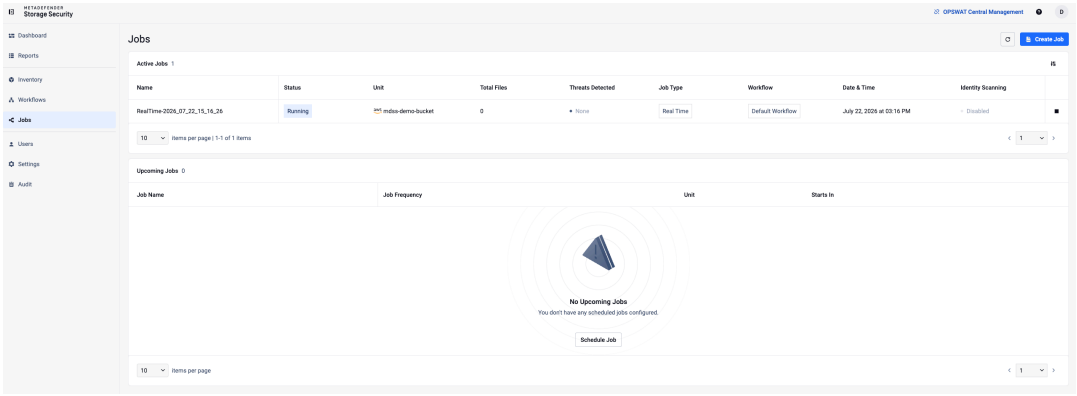
The number of suspicious files, as well as the counters on the top of the page, represent unique files. If the hash of the file has not changed, MetaDefender Storage Security will only count it once.

Active jobs

The dashboard displays an overview of all active jobs. To see them in detail, click **View Running Jobs**.

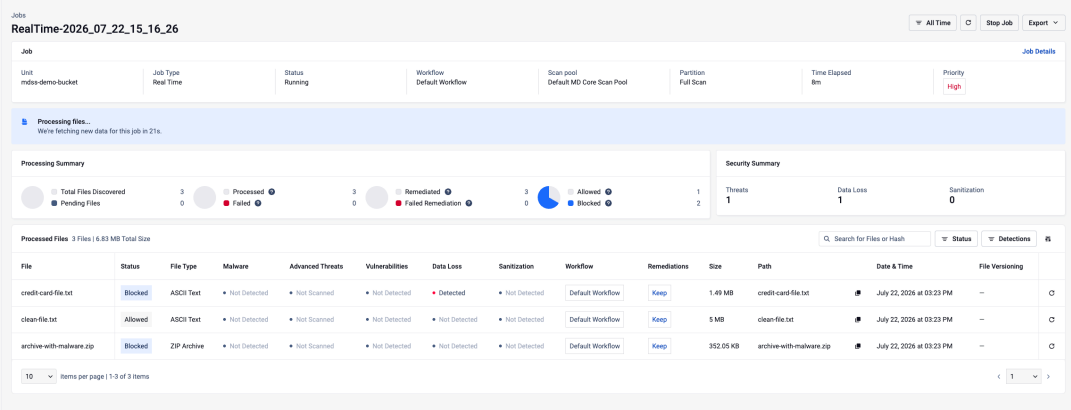


By clicking on **View Running Jobs**, you will be redirected to a page that contains the following information:



Ongoing Jobs details

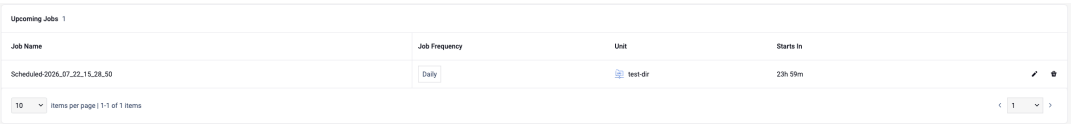
When clicking on the job you will be redirected to the ongoing job page:



Here you can find the information we previously mentioned as well as the time elapsed since this job was started. Click back if you want to go back to the dashboard.

Real time processing and upcoming processes

On the dashboard page, if you scroll down, you will find more information about real time processing and upcoming scheduled processes. This area, like the whole page, is updated in real time so you can always know what's happening.



Info

Real time processing requires a lot of internal communication. This could impact the performance of other scans

Warning

Starting real time processing and other type of scans in parallel with remediations that modify the files in storage could trigger a loop scanning.

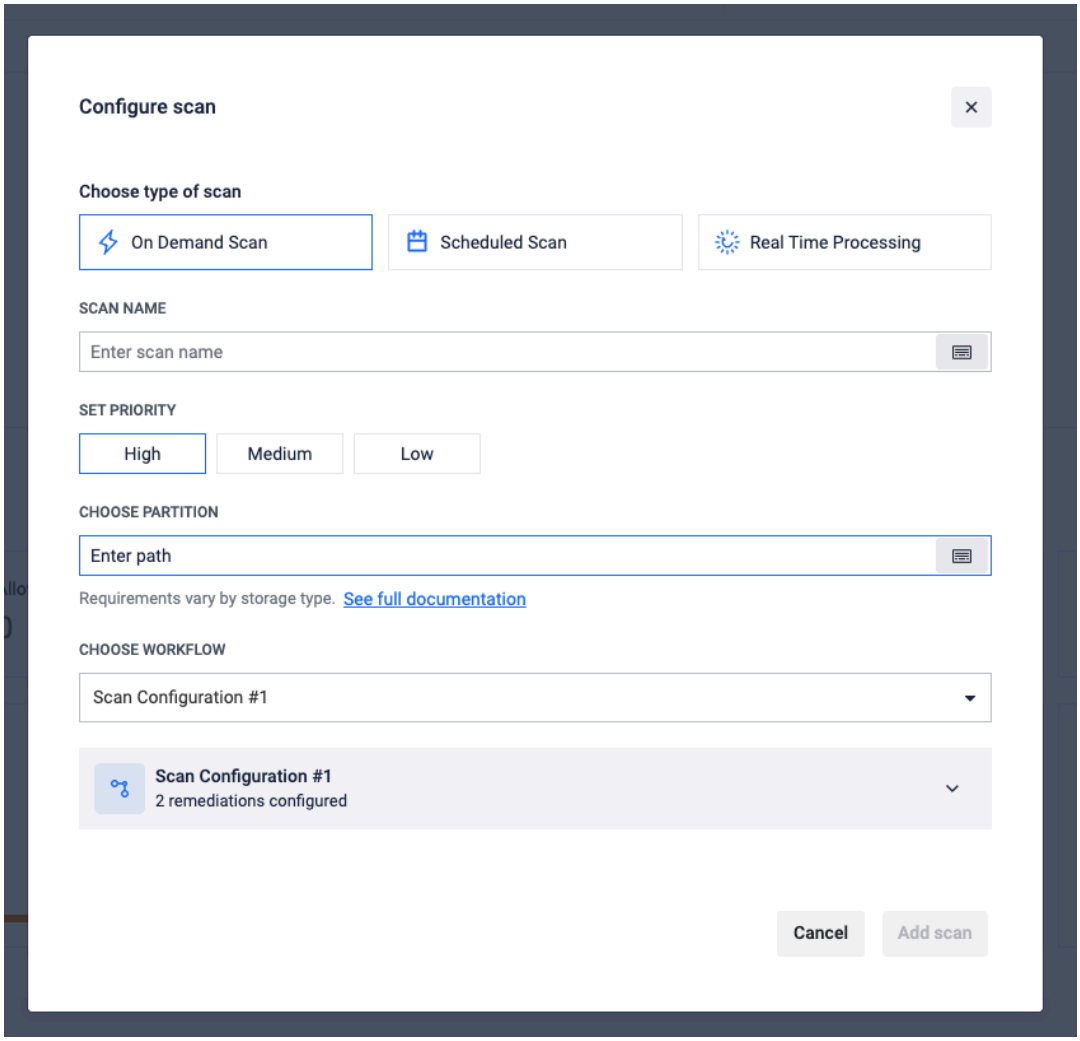
Scanning

This page explains how to configure scans in MetaDefender Storage Security (MDSS) and highlights its unique features.

Types of scanning

MetaDefender Storage Security offers three distinct types of scanning to meet your needs: **On-Demand Scan**, **Scheduled Scan**, and **Real-Time Processing**. Each type offers distinct configurations and capabilities to ensure effective file management.

1. On-Demand Scan

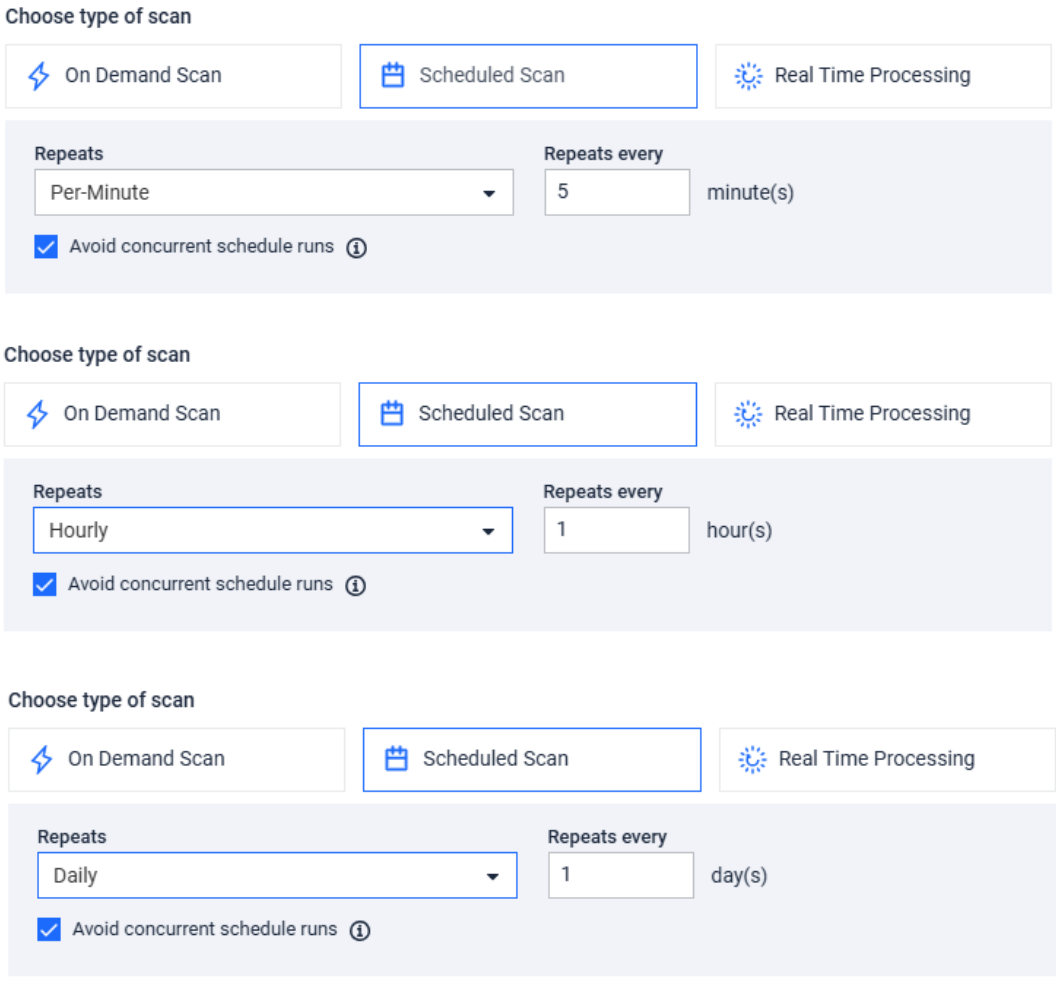


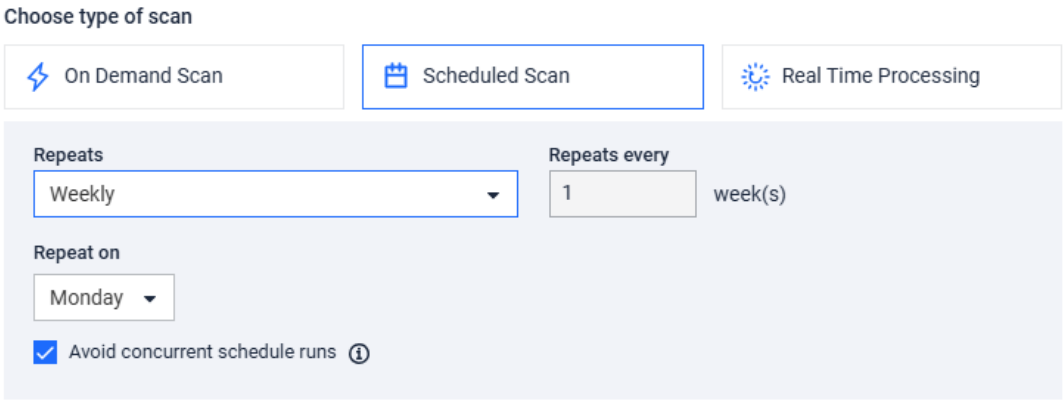
The On-Demand Scan allows you to initiate an instant scan of your selected storage. Here's how it works:

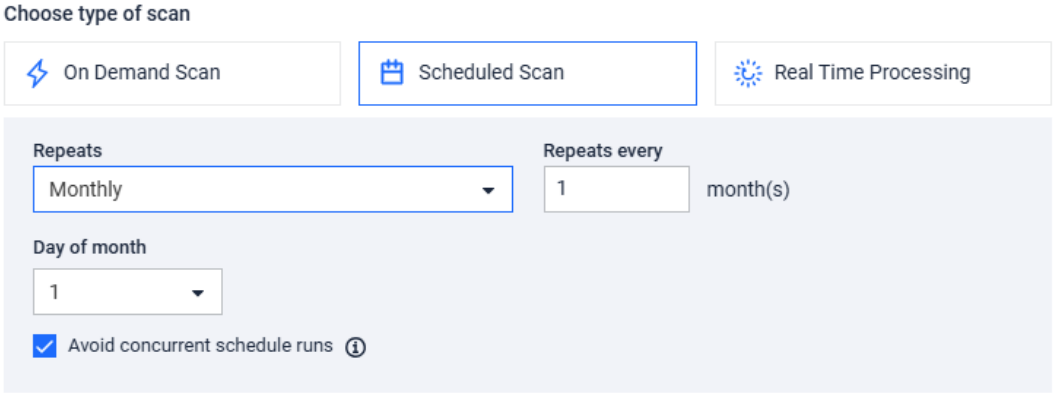
- **Input Scan Name**: Provide a name for your scan.

- **Set Priority**: Choose the priority level for the scan.
- **Choose partition** (optional): Specify a path from the storage root to scan instead of the integrated folder path.
- **Select Workflow**: Choose your preferred workflow (you can preview it's configuration).
- **Start the Scan**: Click "Add Scan" to begin processing all files in your storage integration immediately.

2. Scheduled Scan







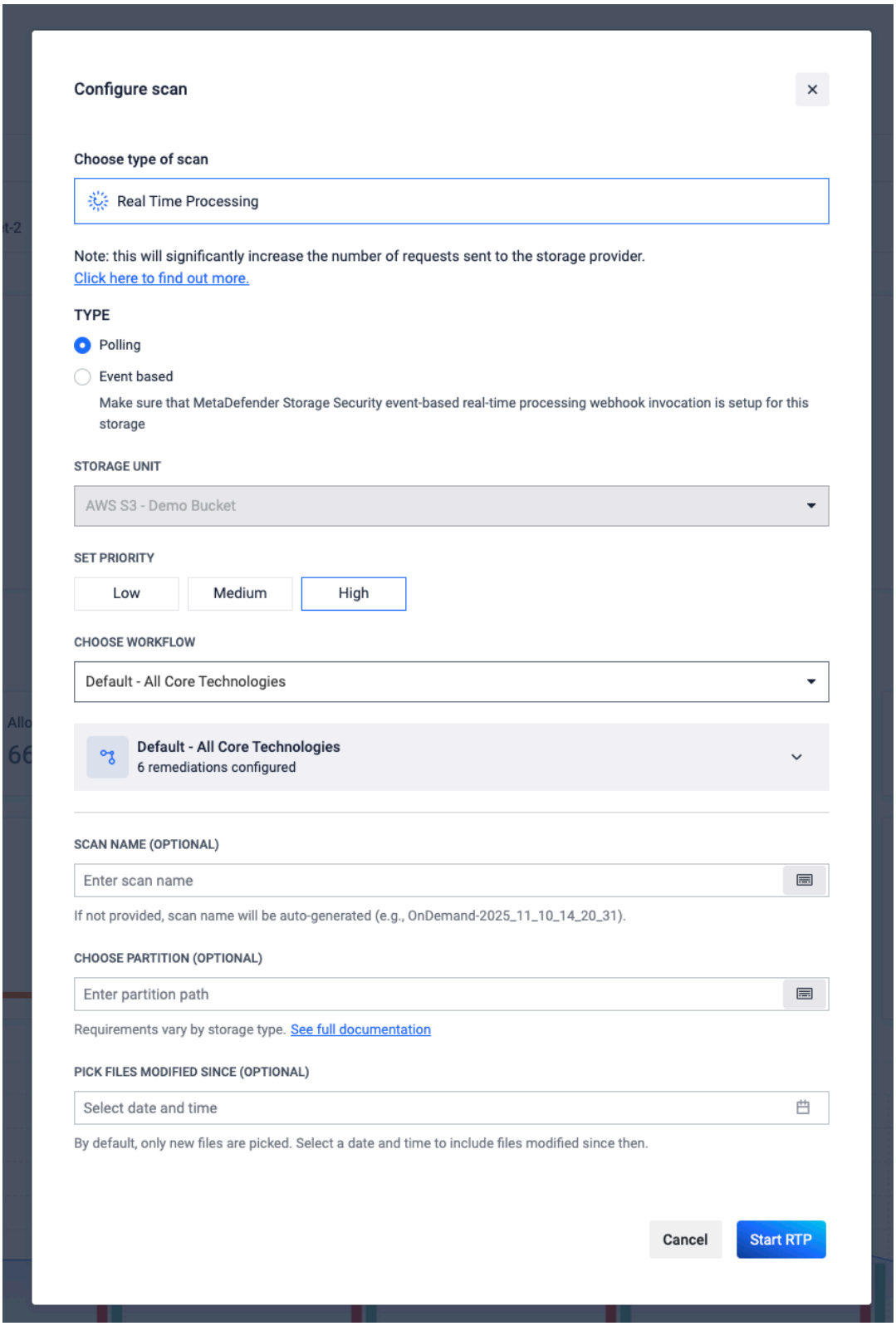
The Scheduled Scan enables you to set up recurring scans at specified intervals. You can configure the scan with the following options:

- **Input Scan Name**: Provide a name for your scan.
- **Set Priority**: Choose the priority level for the scan.
- **Choose partition** (optional): Specify a path from the storage root to scan instead of the integrated folder path.
- **Select Workflow**: Choose your preferred workflow.
- **Recurrence Options:** You can configure the scan to recur in one of four ways:
  - **Per-minute**: Set the scan to trigger every specified number of hours. The scheduling begins immediately upon clicking “Schedule Scan.”
  - **Daily**: Configure the scan to recur every specified number of days, starting from the moment you click “Schedule Scan.”
  - **Hourly**: Set the scan to trigger every specified number of hours. The scheduling begins immediately upon clicking “Schedule Scan.”
  - **Daily**: Configure the scan to recur every specified number of days, starting from the moment you click “Schedule Scan.”
  - **Weekly**: Set the scan to run every specified number of weeks, with the option to select the specific day of the week. The scan will commence at the time you click the button.

  - **Monthly**: Choose the frequency in months for the scan to repeat, along with the specific day of the month it will run.

- **Avoid concurrent schedule runs -** When enabled, the system will skip a scheduled scan run if the previous run is still in progress. This prevents multiple scans from running simultaneously.

3. Real-Time Processing



Real-Time Processing continuously monitors your storage integration for any new or modified files after the scan has started. This option includes:

- **Input Scan Name**: Provide a name for your scan.
- **Set Priority**: Choose the priority level for the scan.
- **Choose partition** (optional): Specify a path from the storage root to scan instead of the integrated folder path. Only one single Real-Time Processing scan is allowed per partition.
- **Choose monitoring date** (optional): By default only new files are picked starting from the moment real time processing is enabled. You can select a date from which the monitoring will start
- **Select Workflow**: Choose your preferred workflow.
- **Processing Methods**: You can select from two methods of Real-Time Processing:
  - **Polling Method**: This method checks for new files at specified intervals in the order of seconds.
  - **Event-Based Mode**: Available for certain storage integrations, this method allows you to configure a function that sends notifications to MetaDefender Storage Security via a generic webhook endpoint whenever a file is added to your storage For more information, check out this page Event-based handling.

Monitoring starting date

This feature will allow users to set a specific date in the past to start a real time processing.

> **Info**
>
> Retention configuration will alter this configuration on runtime to not process the same files after were removed from the report

Partition scanning

Partitions replace the integrated folder path for that scan only. Any folder path configured during storage integration will be ignored. The partition path takes full effect instead. Partitions are defined relative to the root of the storage source, and this behavior is consistent across all supported storage types.

For example, if your integrated storage is `my-bucket/` and you want to scan only `my-bucket/folder/subfolder/`, your partition should be set to `folder/subfolder/`.

> **Info**

> For **OPSWAT MFT, OneDrive, SharePoint, Box and SharePoint OnPrem**: If no specific users or document libraries are selected, the integration applies to **all users/doc libraries**, and **every one of them must contain the specified folder** or the partition scan will fail.

Priority scanning

MetaDefender Storage Security features a **Priority Scanning** system that allows you to assign priority levels to your scans, ensuring that critical tasks are processed more efficiently. This feature is available for all scan types, including On-Demand, Scheduled, and Real-Time Processing.

Priority Scanning Behavior:

While you can assign priority levels to any type of scan—On-Demand, Scheduled, or Real-Time Processing—it's important to understand that these priorities do not influence the execution order of scans. Here's how it works:

- **Same Priority, Same Type**: If you have two On-Demand scans with the same priority, they will run concurrently without any prioritization.
- **Different Priorities, Same Type**: When two scans of the same type are initiated with different priorities, the scan with the higher priority will be processed faster, but they will still run concurrently.
- **Different Types, Different Priorities**: For scans of different types, such as a Real-Time scan with Low priority and a Scheduled scan with High priority, the priority level will still be respected. The Scheduled scan will be processed faster than the Real-Time scan, regardless of their types.

Key Features of Priority Scanning:

- **Priority Levels**: You can choose from three priority options—**High**, **Medium**, and **Low**—when initiating any scan.
- **Efficient Processing**: Scans with higher priority levels are processed faster than those with lower priority levels, allowing you to manage your resources effectively and address urgent tasks promptly.
- **Concurrent Scanning**: Multiple scans can run simultaneously at the same priority level, ensuring flexibility in your scanning operations.

By leveraging the Priority Scanning feature, you can enhance your file management processes and ensure that your most critical scans are prioritized effectively. This not only improves overall performance but also enhances the efficiency of your scanning

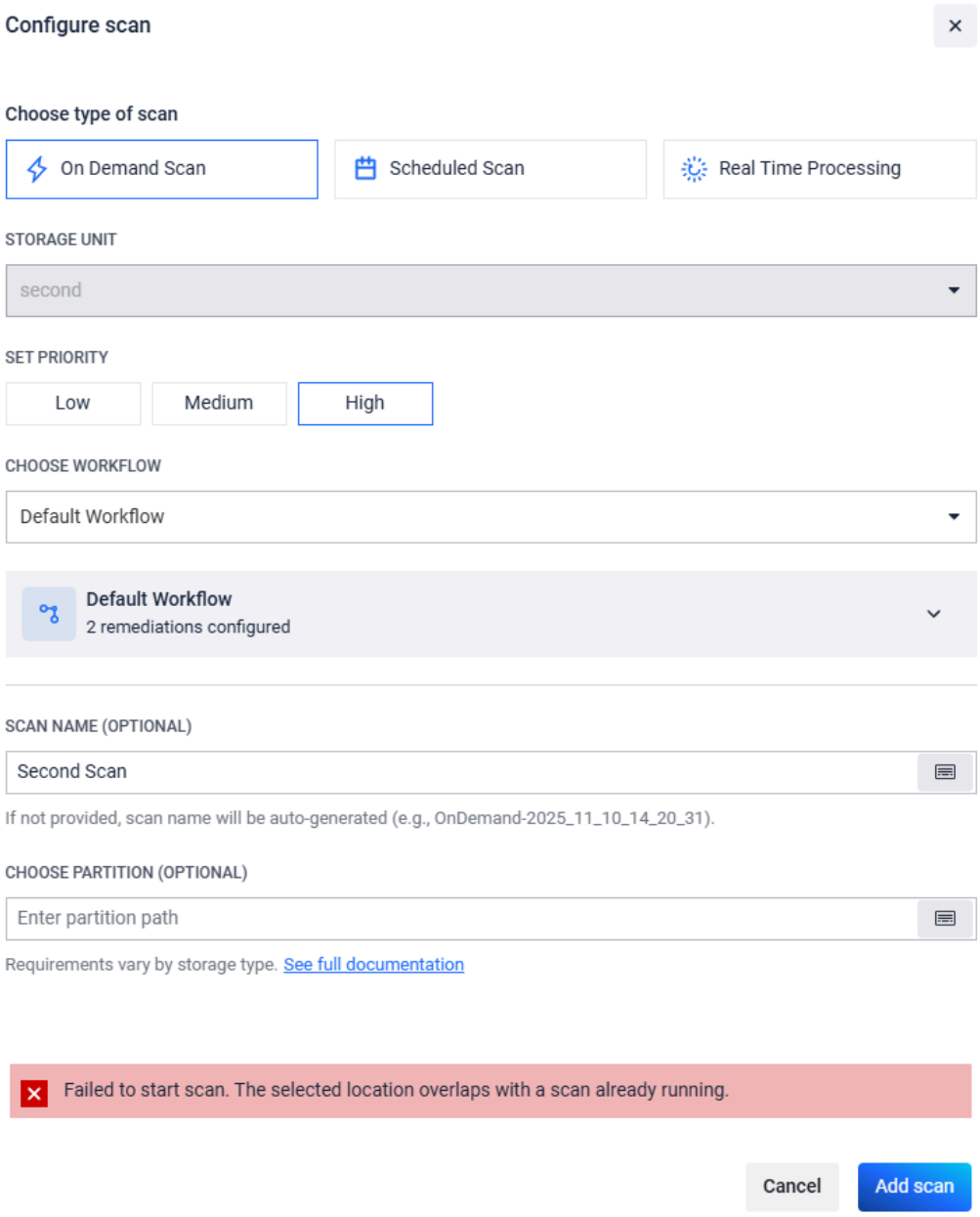
operations. For more ways to fine-tune performance and customize your deployment for speed, please check out this page: Performance Tuning Guide.

Scan Overlap Protection

MetaDefender Storage Security prevents two scans from running at the same time over the same physical storage location. The same location, regardless if it's a bucket, share, site, or folder, can be added to the product more than once (for example, a bucket root and a sub-folder within it, or the same location added twice with different credentials). Scanning both at once wastes resources by re-processing the same files and, when a tagging or remediation workflow is enabled, can create a repeating loop or unexpected behavior in general.

Behavior

This check takes place before starting any type of scan (**On-Demand**, **Real-Time Processing** or **Scheduled**) and will check if the storage location you are trying to start a scan for overlaps with a storage location from any other running scan. If it does overlap, you will receive this error:



Currently, this overlap detection compares locations within the same storage protocol type. It does not detect overlap between two different protocols pointing at the same physical storage (for example, the same NAS accessed over two different protocols). Path comparison is also case-sensitive, so locations that differ only in letter case will not be recognized as overlapping.

Skipping the scan overlap check

Some environments intentionally rely on running scans over overlapping locations and may need to preserve that behavior. For these cases, the overlap check can be disabled using the environment variable:

- **Variable**: SKIP_SCAN_OVERLAP_CHECK

- **Values**: *true* / *false*
- **Default**: *false*
- **Effect**: When *false*, overlap protection is active and overlapping scans are blocked. When *true*, the overlap check is skipped entirely and all scans are allowed to start regardless of overlap.

Password Protected Files and Encrypted Archives

Overview

Password-protected or **encrypted files**, such as Word documents, archives, and PDFs, cannot be scanned without providing the appropriate password to the scanner instance. To address this limitation, MetaDefender Storage Security offers several features, which we will detail below.

Password Storage

One option is to utilize the **Password Storage** feature from MetaDefender Core as explained here.

This feature enables you to define and manage a list of static passwords used for file decryption, making it particularly useful for automated workflow scenarios. When this feature is enabled, the scanner can decrypt and scan the file seamlessly, meaning it will not appear as password-protected in Storage Security.

Unlocking Encrypted Files within Storage Security using the GUI

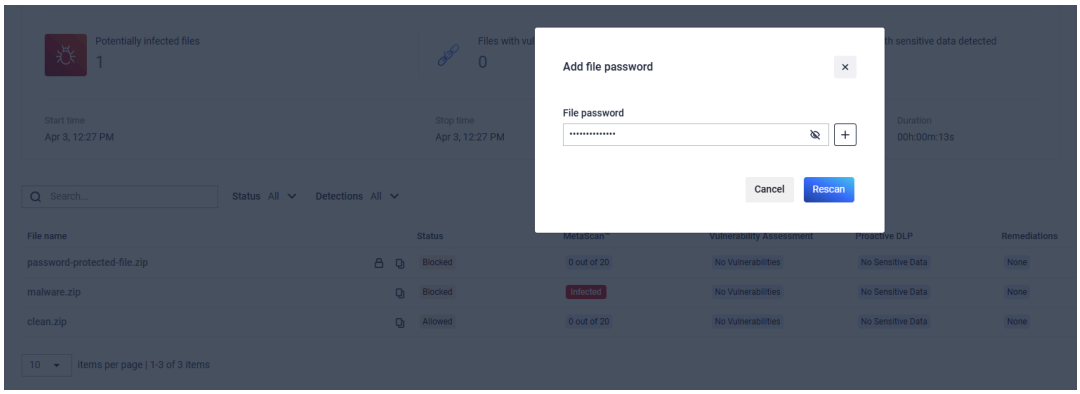
This feature empowers you to take control of sensitive data by enabling immediate scans of encrypted files. Simply provide the necessary passwords through the intuitive user interface and Storage Security will analyze the files, ensuring comprehensive protection against hidden threats.

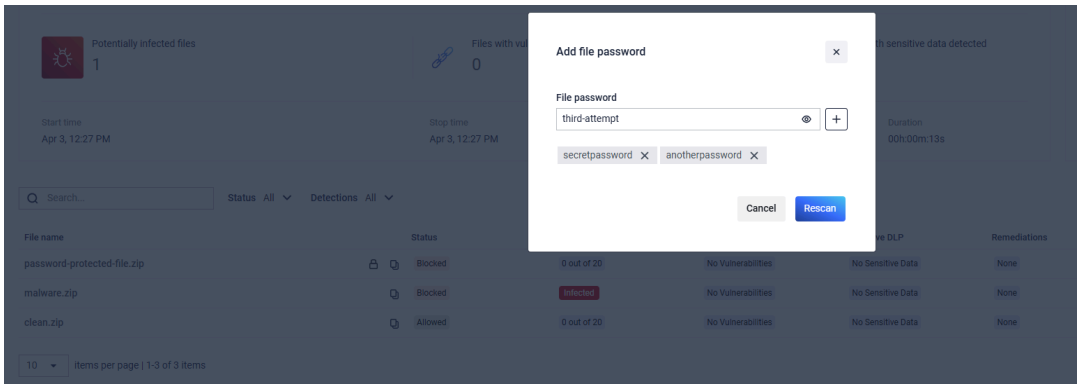
Unlocking Encrypted Files within MetaDefender Storage Security is simple **for users who prefer the GUI**:

1. Identify Encrypted Files: In the Reports page, look for files marked with a lock icon, indicating an “Encrypted” verdict. These files are automatically blocked to ensure security.



2. Provide Passwords: Click the lock icon to open a window where you can securely enter potential passwords. Need to try multiple passwords? Easily add more with the “plus” symbol. You can also visualize your entered passwords using the “eye” icon.
3. Initiate Rescan: Click the rescan icon to begin the decryption process. MDSS will attempt to decrypt the file using each password provided.





Currently, you can rescan one encrypted file at a time. We are actively working to enhance this feature, allowing you to provide passwords for multiple encrypted files simultaneously in future releases.

Unlocking Encrypted Files within Storage Security using the API

For **users who prefer the API integration**, MetaDefender Storage Security offers a flexible approach to On-Demand Scanning of encrypted archives:

The dedicated API endpoint allows you to initiate rescans of encrypted files programmatically. This means you can trigger a rescan at any time, regardless of whether you have passwords to provide.

If passwords are available, simply include them in your API request. MDSS will attempt decryption using the provided passwords and return the scan results. This enables

seamless integration of encrypted archive scanning into your automated workflows and security processes.

This API-driven approach provides advanced users with the control and flexibility they need to manage encrypted archives effectively within their existing systems. Full API documentation is available to guide your implementation.

Request Body:

```
{

        "fileId": "{string}",
        "scanId": "{string}",
        "storageProtocolType": "{int32}",
        "passwords": ["{array[string]...}"]
}
```

Reprocess files

MetaDefender Storage Security allows users to manually initiate a new scan for files. This feature provides control and flexibility, enabling rescans for the following scenarios:

- Investigating potential false positives
- Re-evaluating a file after anti-malware definition updates
- Re-processing a file after a policy configuration change
- Attempting to scan an encrypted file by providing the correct password(s)

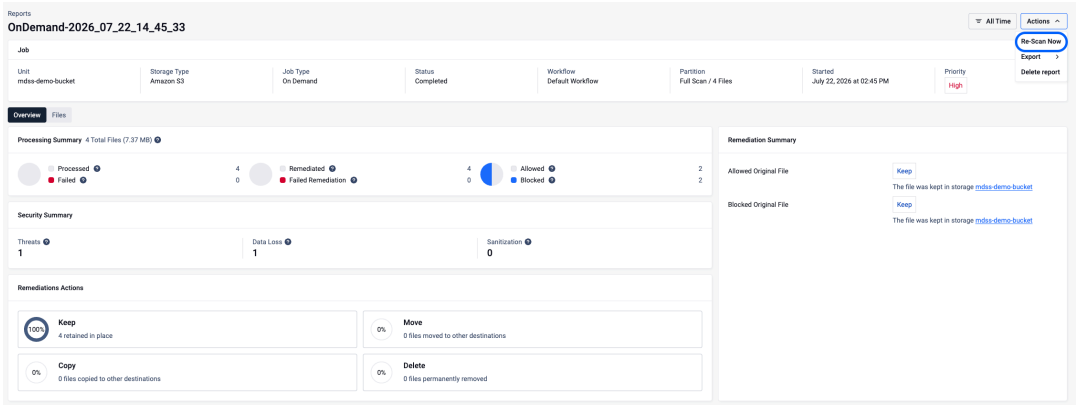
Files can be rescanned using either the **graphical user interface (GUI)** or the **Application Programming Interface (API)**.

> **Info**
>
> Reprocess actions have been designed for finished scans and are not applicable to running scans or active Real-Time Processing (RTP) scans.

Using the Report Reprocess Flow

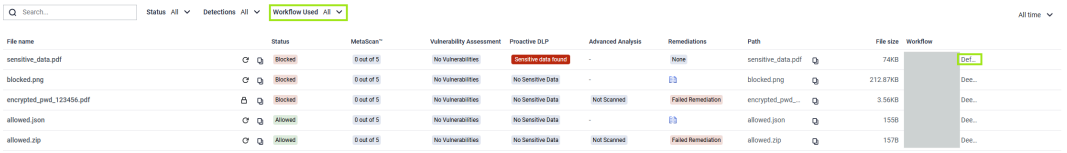
You can initiate a batch rescan directly from the MetaDefender Storage Security web interface:

1. From the scan report, go to **Actions -> Re-Scan Now**



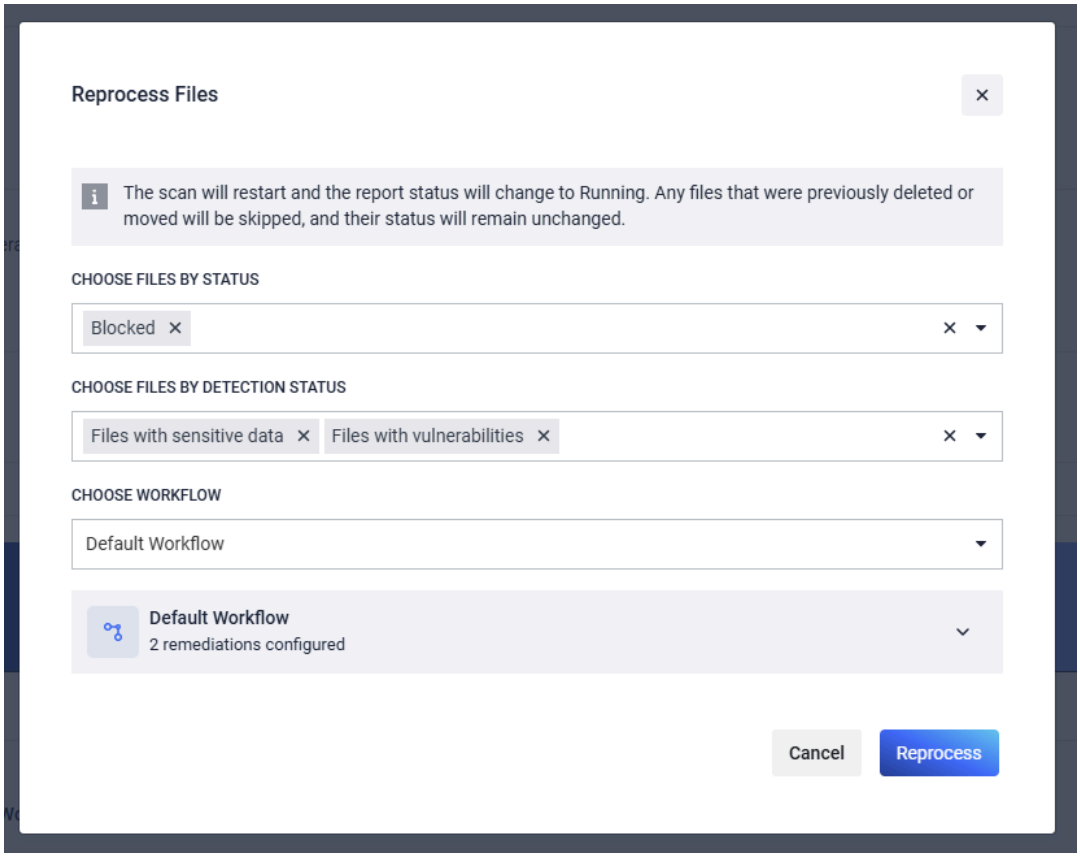
2. Configure the reprocess filters with the desired **Status**, **Detection**, and **Workflow** to be used by the rescan action.

3. After a batch rescan, the files of the report can be filtered by the Workflow and Date of the rescan action.



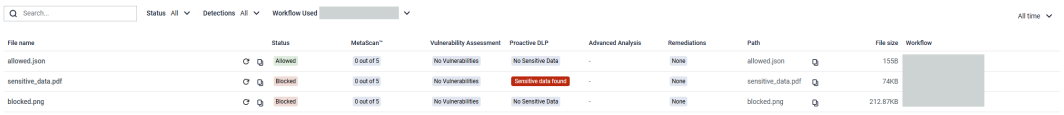
> **Info**
>
> The rescan process will filter for files that match both the STATUS and the DETECTION filters.
>
> Adding multiple DETECTION filters will scan will filter for files that match ALL DETECTIONS and not at least one of them.

Rescanning for **Blocked** files with **Sensitive Data - AND - Vulnerabilities** will not rescan any files because no files have triggered both **DLP** and **Vulnerability** detection flags in the scenario above.



Info

Reprocessing for Allowed and Blocked files will reprocess all files with Allowed and Blocked files but not any with Failed Remediations or other results.

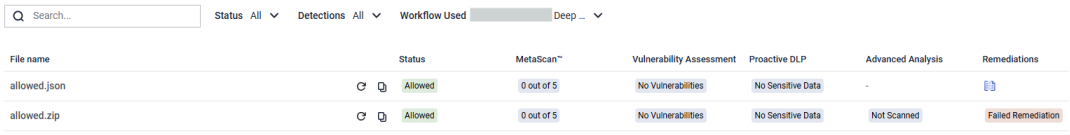


Warning

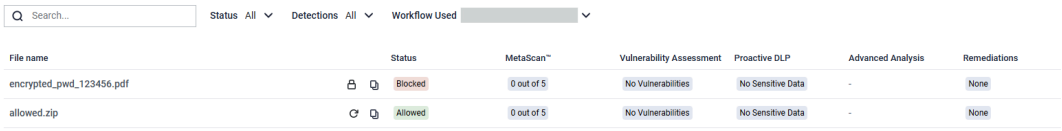
Allowed and Blocked file results are 1 tier above Failed, Failed Remediations, and Canceled file results.

Reprocessing for Allowed and Failed Remediations Files will NOT rescan Blocked files with Failed Remediation results because the rescan did not target Blocked files. Only Allowed files, with or without Failed Remediations, will be reprocessed.

File name	Status	MetaScan™	Vulnerability Assessment	Proactive DLP	Advanced Analysis	Remediations
allowed.json	Allowed	0 out of 5	No Vulnerabilities	No Sensitive Data	-	
allowed.zip	Allowed	0 out of 5	No Vulnerabilities	No Sensitive Data	Not Scanned	Failed Remediation
encrypted_pwd_123456.pdf	Blocked	0 out of 5	No Vulnerabilities	No Sensitive Data	Not Scanned	Failed Remediation
blocked.png	Blocked	0 out of 5	No Vulnerabilities	No Sensitive Data	-	
sensitive_data.pdf	Blocked	0 out of 5	No Vulnerabilities	Sensitive data found	-	



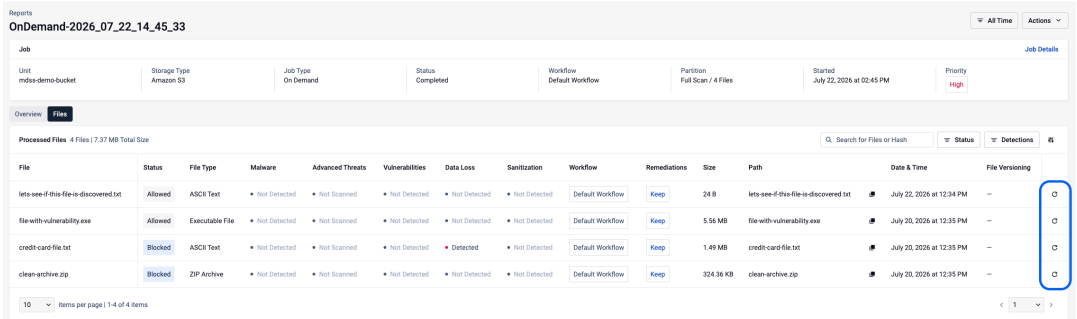
> **Info**
>
> Reprocessing for ONLY Failed Remediation files will reprocess both Allowed and Blocked files that have Failed Remediations



Using the Reports GUI

You can initiate a single file rescan directly from the MetaDefender Storage Security web interface:

1. Navigate to the **Active Scans** page or the **Reports** page.
2. Locate the specific file you wish to rescan within the list (status is indicated by icons or labels).
3. Click the **Reprocess File** button in the actions column for the blocked or failed file. For encrypted files, click the lock icon, enter the passwords, and click the rescan icon.
4. The file will be re-queued for processing using the currently applicable workflow.
5. Monitor the scan progress and final result on the Reports page.



Using the API

1. Files can be programmatically submitted for rescan using this API from the MetaDefender Storage Security API. This is useful for automation or integration with other systems.

2. You will need the unique identifier (`fileId`) of the blocked file you wish to rescan. This ID can typically be retrieved from scan reports or event logs associated with the initial block action.
3. **Missing Information :** the specific endpoint for triggering a rescan of any blocked file in MDSS based on `fileId` should be documented here / link to it
4. Send an API request (POST) to the determined endpoint. The request body should be in JSON format (below)
5. The API should return a response indicating whether the rescan request was successfully submitted (a success message, perhaps a new `data_id` or task ID for tracking or whatever it is). The actual scan results will be available asynchronously and can be retrieved via subsequent API calls or viewed in the GUI.

For standard rescan

```
{
        "fileId": "{string}",
        "scanId": "{string}",
        "storageProtocolType": "{int32}",
}
```

For encrypted blocked files

```
{
        "fileId": "{string}",
        "scanId": "{string}",
        "storageProtocolType": "{int32}",
        "passwords": ["password_1","password_2"]
}
```

Full API documentation is available to guide your implementation.

Identity Scanning

Identity Scanning speeds up file processing by identifying files that have already been scanned in previous runs. When MDSS (MetaDefender Storage Security) detects that a file hasn't changed since the last scan, it reuses the existing scan results instead of re-scanning the file.

This feature is useful for backup datasets where many files stay the same across multiple scan cycles, and for recurring scans of the same dataset.

Benefits

- Improves performance for backup datasets and recurring scans
- Reduces scanning time by skipping unchanged files
- Keeps complete reporting while avoiding redundant work

- Maintains security with customizable rescan intervals

How it works

Identity Scanning uses file metadata to check whether files have been scanned before. Here's what happens:

1. Mount backup repositories as NFS/SMB file shares to MDSS
2. Enable Identity Scanning in your workflow and set a scan interval (for example, 3 days)
3. First scan: All files are scanned (no stored results exist yet)
4. Later scans: Only new or changed files are scanned; unchanged files use cached results
5. You get better performance while keeping full security coverage

Rescan interval

To maintain security, Identity Scanning includes a rescan interval. Even files that haven't changed get rescanned after the time period you configure. This ensures nothing slips through the cracks.

> **IMPORTANT**
>
> Deep CDR and Real-Time Processing are currently not supported by Identity Scanning.

Things to know

- Identity Scanning works with On-Demand and Scheduled scans only
- You cannot start Real-Time Processing with Identity Scanning enabled
- The feature checks file metadata to identify files accurately

Configuration

Setting up identity scanning

Configure Identity Scanning from the Discovery tile in your workflow:

1. Create or edit a Standard Workflow with scanning enabled
2. Turn on "Enable Identity Scanning"
3. Set the "Scan Interval (Days)" value
4. Save your changes

Scan interval

Choose how often MDSS will rescan files to check for changes. For example, if you enter "3", MDSS will scan every 3 days to verify files that haven't changed.

Reading scan results

What happens during scans

First Scan

- All files in storage are scanned
- No identity matches exist in the database yet
- All files show as "Scanned"

Later Scans

- New or changed files are scanned
- Unchanged files use stored results and show as "Stored"
- Reports show all files, whether scanned or stored

What the labels mean

Identity: Scanned

- Files that were scanned in this run
- Includes new files and files changed since the last scan

Identity: Stored

- Files that were skipped during scanning
- These files haven't changed since the last scan
- Results come from stored data

Using Reports

Dashboard

When a scan with Identity Scanning runs, you'll see an "Identity Scan" indicator on the scan card.

Report list

Reports that used Identity Scanning show an icon next to the report name.

Report details

Inside a report, you'll find:

Summary Cards

- Identity Scanned - the number of files scanned in this run
- Identity Stored - the number of files that used stored results

Filters and Columns

- Filter by "Identity Status" to see only "Scanned" or "Stored" files
- Each file shows its status in the table

Active Scans

- See Identity Scanned and Identity Stored counts in real-time
- Filter the file table by Identity Status while scans run

Special cases

Files that are always scanned

Even with Identity Scanning turned on, some files always get scanned:

- Manual reprocessing - if you manually reprocess a file, it gets scanned regardless of identity status
- Different Scan Instance - if a file was scanned with a Scan Instance that's not in your current Workflow's Scan Pool, it gets scanned again

After the interval expires

When you run a scan after your configured interval (like 3 days), all files get scanned again even if they haven't changed. This keeps your security coverage complete.

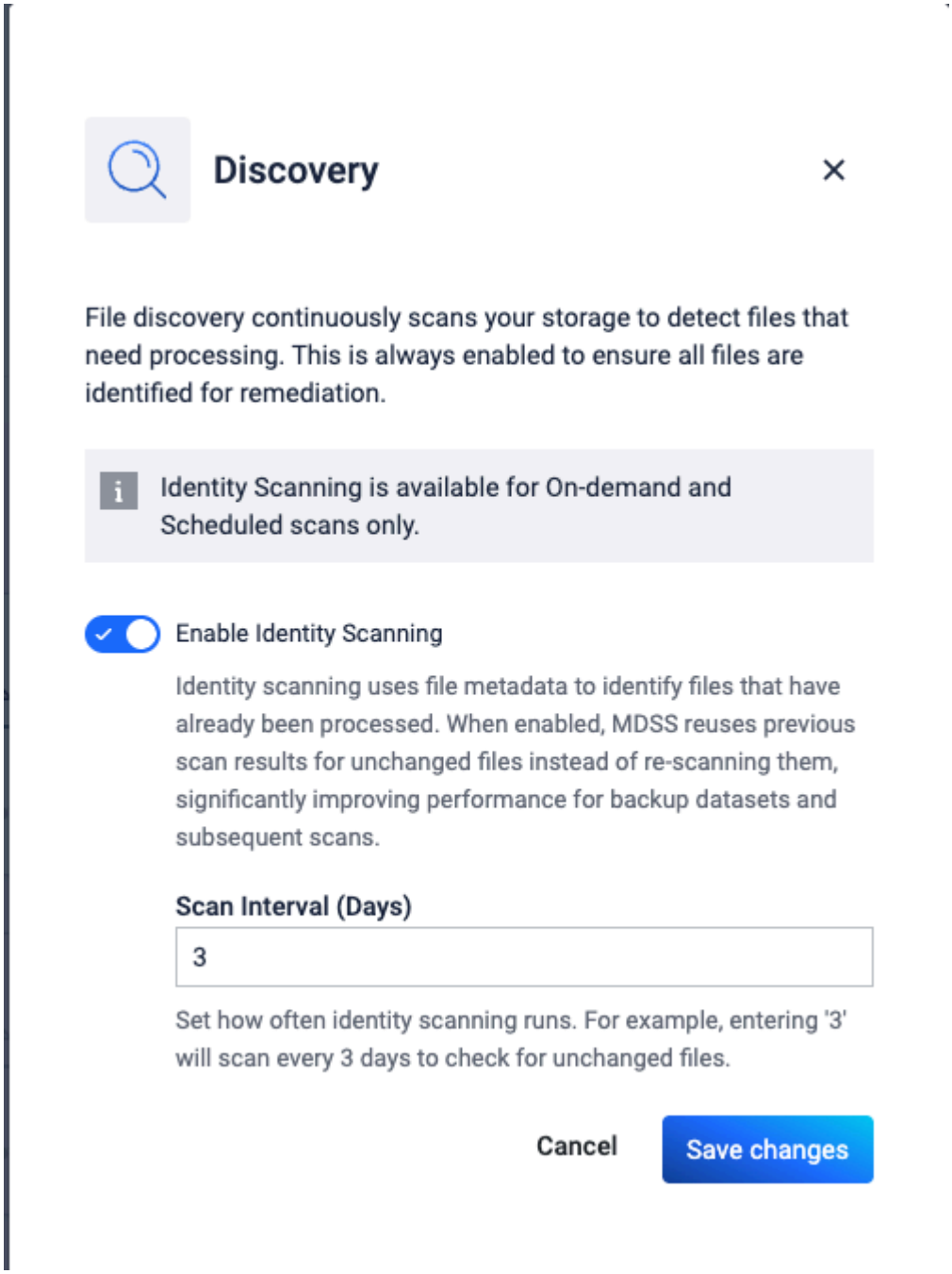
Example workflow

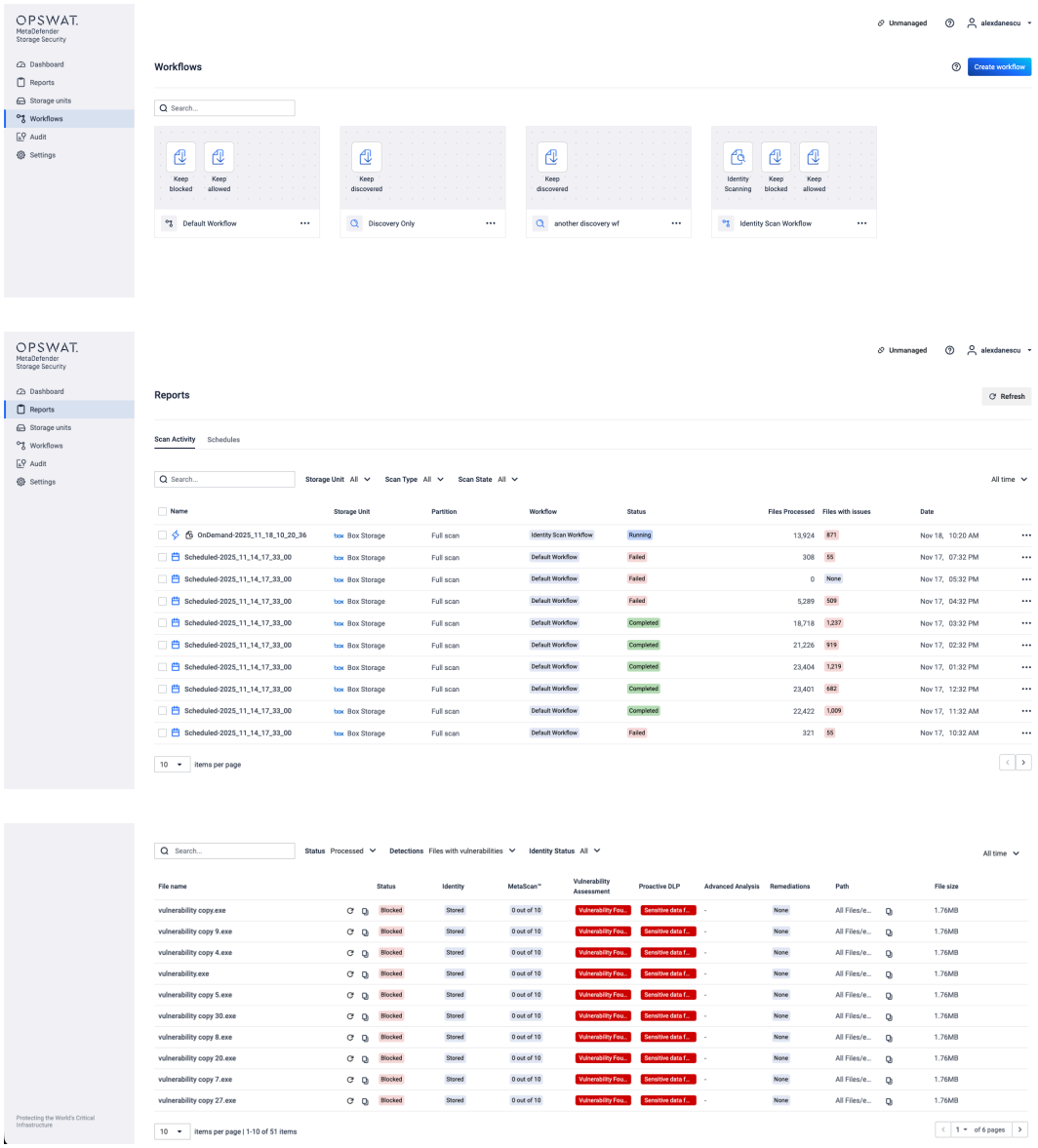
Here's how Identity Scanning works in practice:

1. Create a workflow with Identity Scanning turned on and a 3-day interval
2. Run the first scan
    - All files are scanned
    - Report shows all files as "Identity: Scanned"
3. Run a second scan (within 3 days)

- Unchanged files show as “Stored”
- Only new or changed files actually get scanned

4. Run a third scan (after 3 days)
   - All files get scanned again, whether they changed or not
   - This keeps your security coverage up to date





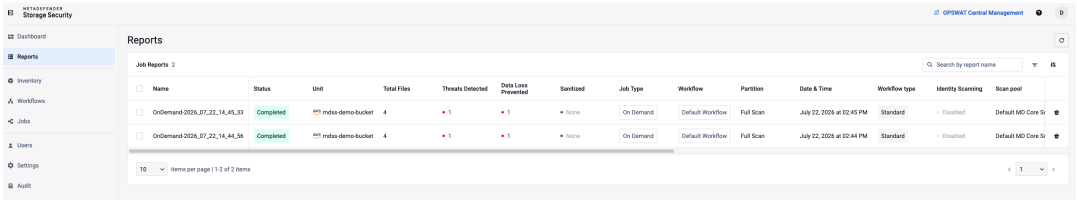
Tips for Using Identity Scanning

- Identity Scanning works well for **backup datasets** where most files stay the same
- Pick a scan interval that balances security needs with performance
- Look at Identity Scanned vs. Identity Stored numbers to see how your files change over time
- Use Identity Scanning with scheduled scans for automated security coverage

Reports

After a process is finished a report is produced for you by MetaDefender Storage Security. This report has information about the overall scan of your storage (i.e. the number of detected issues) as well as individual file analysis details.

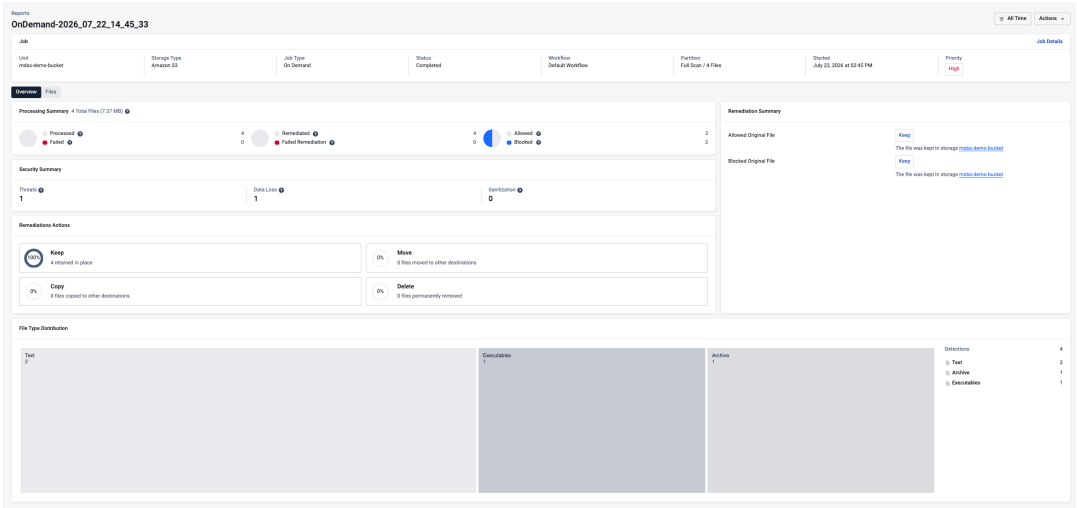
You can access all the reports generated for a specific storage by navigating from the left menu:



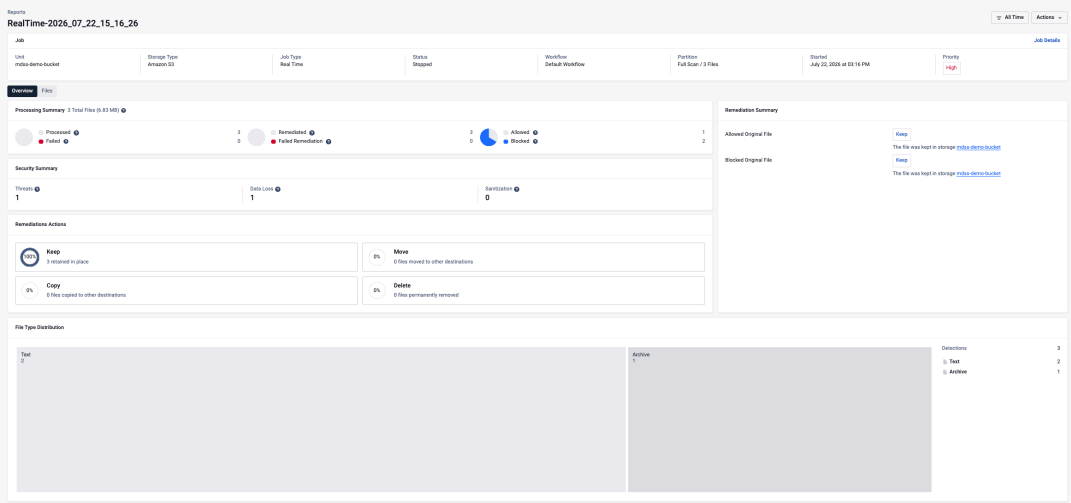
Here are some actions that are available for you:

- Search for a report or filters report based on type or a specific time range
- Click on a report in order to see more details and you will be redirected to the report page
- Delete a report using the three dots menu from the last column

Scan Report



Real Time Processing Report



Info

Cleaning a RTP report will not reprocess existing files.

In case one of the following, on cleaning the RTP report only the files that were not processed will be handled.

DISCOVERY_SERVICE _SMB_RTP_HANDLING=1

DISCOVERY_SERVICE_SFTP_RTP_HANDLING=1

DISCOVERY_SERVICE_NFS_RTP_HANDLING=1

DISCOVERY_SERVICE_FTP_RTP_HANDLING=1

Settings

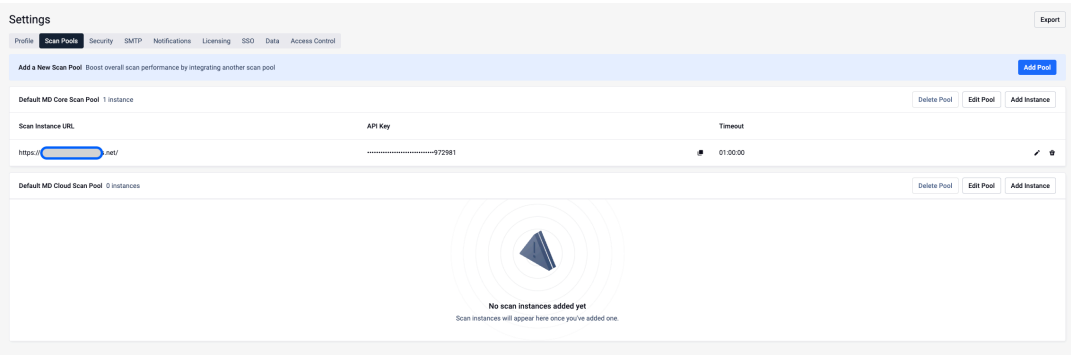
The “Settings” section of MetaDefender Storage Security provides a centralized location for configuring various aspects of the system to meet your specific security and operational needs.

Each tab provides a clear interface for configuring the corresponding settings. Make sure to review the specific documentation for each tab to fully understand the available options and their impact on your system.

The Settings page is organized into the following sections:



- Scan Pools
  - This tab allows you to manage and configure scan pools, which define the resources used for scanning files. You can add, edit, and delete scan pools, as well as specify the number of integrated scan instances for each pool. *[Referencing the image: this tab is currently selected in the screenshot.]*



- Export
  - This tab allows you to configure how scan results and other data are exported from MetaDefender Storage Security. You can specify export formats, destinations, and other export-related settings. You can find more information on this page.
- SMTP
  - This tab is used to configure SMTP settings for email notifications. You can specify the SMTP server, authentication details, and other email-related parameters to

ensure seamless delivery of notifications.

- Notifications
  - This tab allows you to configure various types of notifications, such as alerts for detected threats, scan completion notifications, and other system events. You can customize the content and delivery method for each notification type.
- License
  - This tab provides information about your MetaDefender Storage Security license, including expiration dates and feature availability. You can also use this tab to manage and update your license.
- Users
  - This tab allows you to manage user accounts and permissions within MetaDefender Storage Security. You can add, edit, and delete users, as well as assign roles and permissions to control access to different features.
- Data Retention
  - This tab allows you to configure data retention policies, specifying how long scan results and other data are stored in the system. You can define retention periods based on your organization's compliance requirements.
- External Loggers
  - This tab allows you to configure external loggers, such as syslog servers, to forward system logs for centralized logging and analysis.
- Single Sign On (SSO)
  - This tab allows you to configure Single Sign-On (SSO) integration with your organization's identity provider. You can enable SSO and specify the necessary settings to allow users to authenticate using their existing credentials.
- Security
  - This tab allows you to generate a new master encryption key that will re-encrypt all sensitive data. You can find more information on this page.
- Access Control
  - This tab allows you to view the roles defined in your system and the permissions associated with each. You can browse all roles, inspect their Read, Write, and Delete permissions per resource, and use the search bar to locate a specific role by name quickly

Importing/Exporting a configuration

> **Warning**

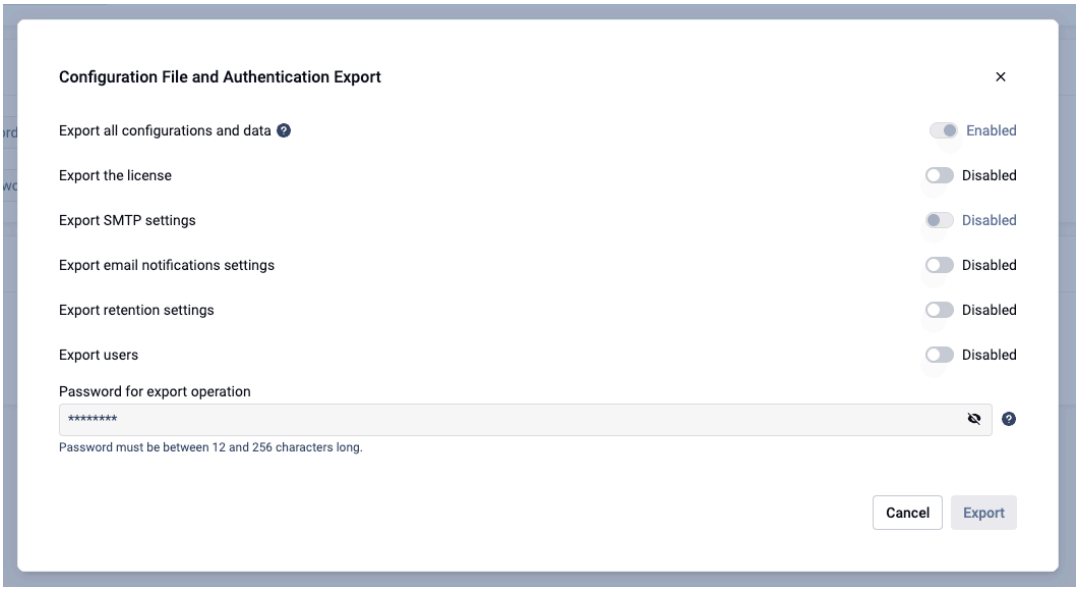
> Importing a configuration file from a version greater than 4.0.0 that includes SSO settings will require reconfiguring SSO, as it was not properly exported.

MetaDefender Storage Security allows administrators to export and import system configuration files. This feature is useful for backup, migration, or replicating settings across environments.

Exporting the Configuration File

Navigate to **Settings **page, click on **Export** button. The export includes all system settings such as accounts, groups, storage units, scan pools, workflows, and more.





Steps to Export

1. Choose which parts of the configuration you want to export (License, SMTP settings, email notifications, retention settings).
2. In the Export Authentication section, you must set a password for the export operation. This password will be required to import the configuration file later. Please store it

securely, as it cannot be recovered.

3. Click Export Configuration to download the configuration file. The file will be encrypted using the password you provided.

Export File Information

1. Configurations from version 4.0.0 and newer are exported as ZIP files. Older versions use JSON format.
2. Export files typically range from 10MB for basic setups to 100MB+ for complex configurations.
3. Store export files in secure locations with appropriate access controls.

Importing a Configuration File

On a fresh install of MetaDefender Storage Security, after creating the first user account and logging in, you can choose to import an existing configuration.

Version Compatibility

- **JSON files** for configurations older than version 4.0.0
- **ZIP files** for configurations from version 4.0.0 or newer
- **Cross-version imports** for importing older configurations into newer versions - has limited compatibility and may require manual review

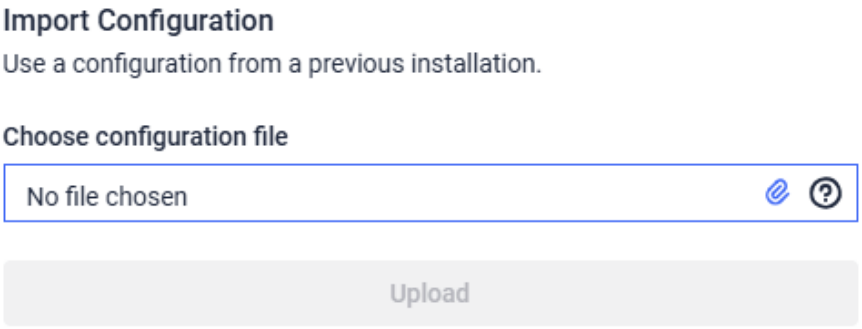
Steps to Import

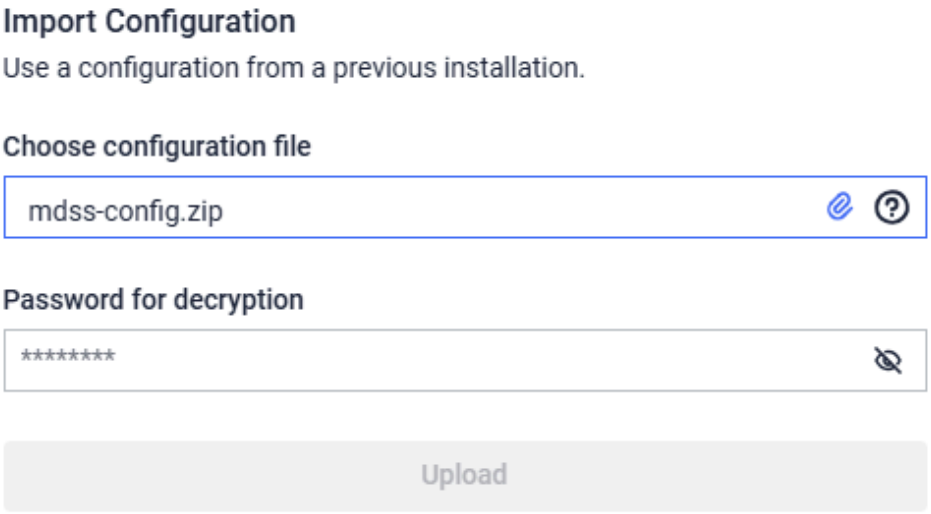
In the Import Configuration screen, you can click on the input field, browse and select a file to Import. The input will accept either a JSON file (if the configuration is older than 4.0.0) or a .ZIP file (if the configuration is 4.0.0 or newer).

If the file is password-protected, you will be prompted to enter the password that was set during export. Afterwards, click on the Upload button and the configuration import procedure will start.

Import timing

The import process typically takes 30 seconds to 2 minutes, depending on configuration size. If license transfer is enabled, allow additional time for online activation.





Post-Import Requirements

Important: After importing a configuration that contains advanced settings (such as HTTPS configurations, SSL certificates, or custom integrations), you must restart the following Windows services:

- MetaDefender Storage Security Service
- MetaDefender Storage Security Web Service

- MetaDefender Storage Security Scanning Service

Note: Service restart is only required if the imported configuration contains advanced settings. Basic configurations typically do not require a service restart.

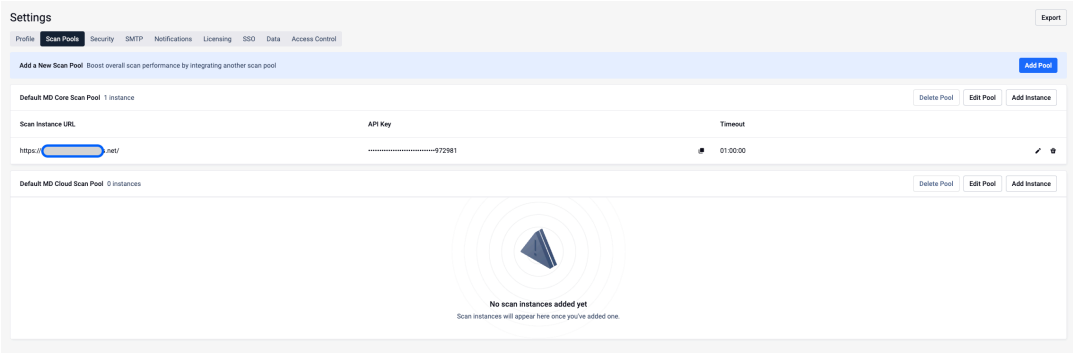
Verification Steps

After import completion, verify the following:

- All services are running properly
- License is activated (if applicable)
- Storage units are accessible
- User accounts function correctly
- Email notifications work (if configured)

Scan Pools

MetaDefender Storage Security uses scan pools to group instances of MetaDefender Core or MetaDefender Cloud.



These two types of scan pools can be used to balance the load of scan requests.

MD Core API Endpoints and Permissions

To learn more about the required permissions and the endpoints used by MDSS for MD Core, please read the following KB article: Which API endpoints from MD Core does MDSS utilize?

MD Cloud Private Processing

MD Cloud instances use private processing by default to ensure maximum data privacy and security. Therefore, a non-Community API key must be used when integrating in MDSS. With private processing:

- All submitted files are automatically deleted immediately after analysis completion
- Scan results are only accessible to the original API key owner

Workflows

Each workflow consists of the following configurations:

- File discovery
- Scan pool
- File tagging
- Deep CDR
- File remediations
- Other remediations

> **Configurations limitations**
>
> The available configurations are tied to the MetaDefender Cloud/Core available technologies. Providing an API Key when setting up the Scan Pools will list all the available technologies that are configured in MetaDefender Cloud/Core so that configurations can be successfully applied.

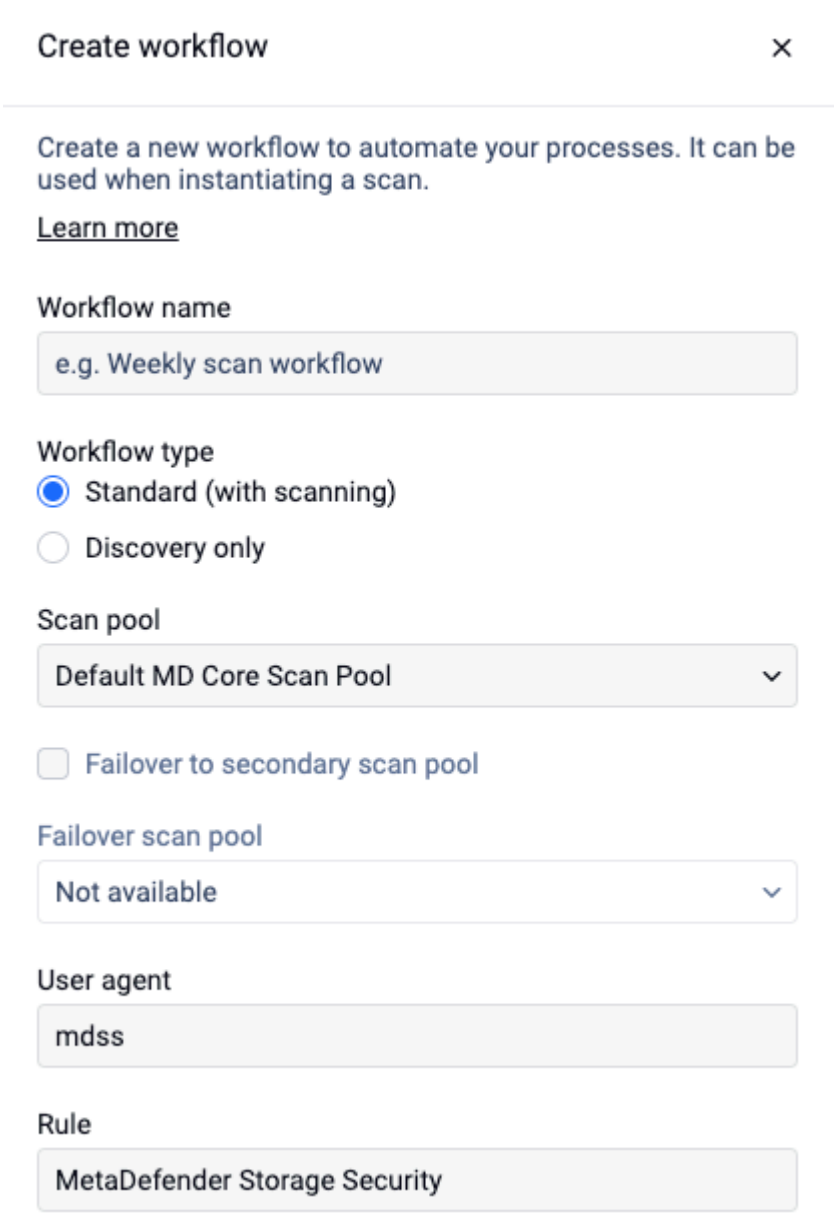
> **Prerequisites**
>
> In order to be able to create a workflow, a scan pool is required.

Creating a Workflow

As a first time user, there is a default workflow that is created during the onboarding process. There can be created as many workflows as required for different use-cases.

> **Default workflow**
>
> The default workflow can't be deleted. There must always be a default workflow configured in the system.

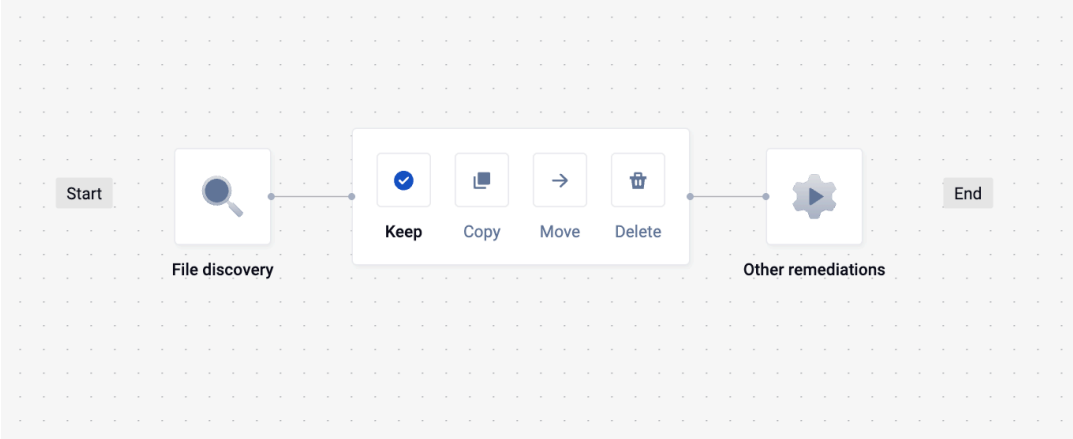
A workflow can be created by navigating to the Workflows page and clicking the "Add new workflow" button. This will reveal a dialog box where the new workflow name must be set and also the type of the workflow.



Once a name is given to the new workflow it will require to choose the type of workflow, afterwards the system will mark it as a draft.

Discovery only

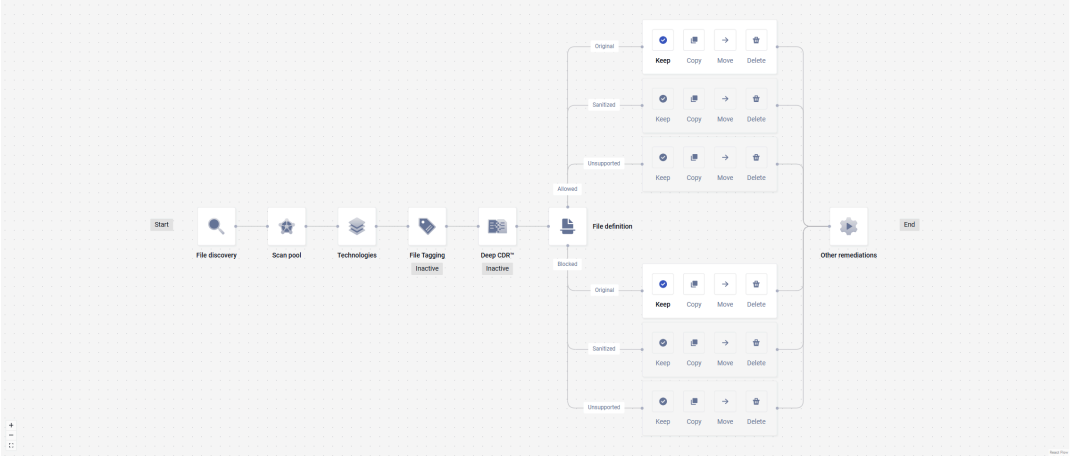
The Discovery only workflow will be created with the default settings after pressing Create button.



This type of workflow it is used for storage interaction without scanning the file. This allows a more limited number of remediations and focus only on discovering folder structure and managing it

Standard

The standard workflow is saved in the system only after the “Scan pool” is properly configured. While in draft mode, all the other settings nodes are inaccessible until the Scan pool is successfully configured.



Once the Scan pool is successfully configured, the other settings can be updated by clicking on each one individually. The workflow is updated instantly once the “Save changes” button is clicked for each of the settings nodes.

Scan pool

Each workflow must have a scan pool node that determines which scan pool is used for scanning. It connects to an existing scan pool - such as MetaDefender Core, MetaDefender Distributed Cluster, or MetaDefender Cloud - and allows you to specify a user agent and a workflow rule to control how scanning is performed. A failover scan pool

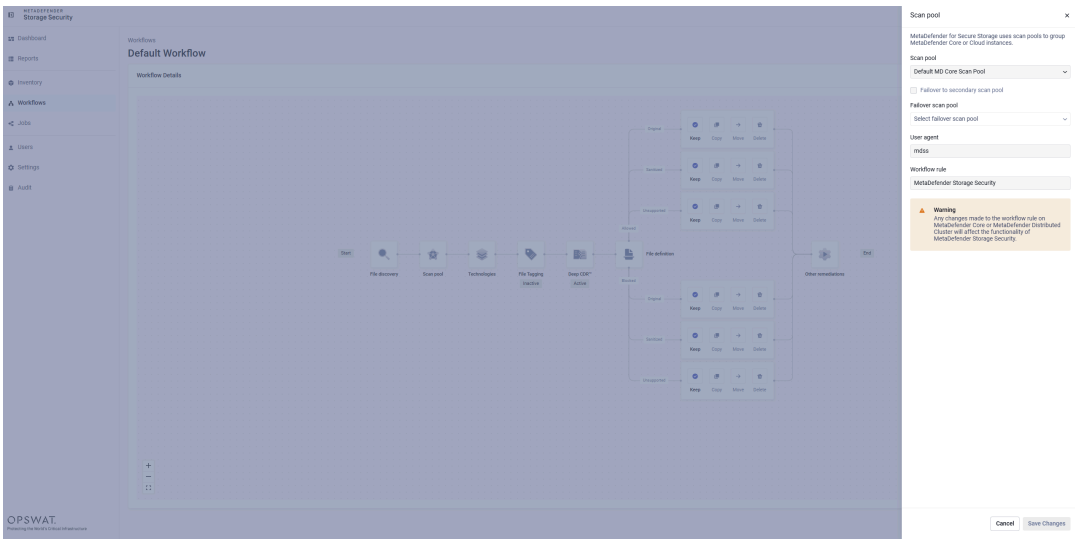
can also be designated to provide an alternative scanning resource when the primary pool is unavailable or unresponsive.

MetaDefender Storage Security uses scan pools to provide a flexible way to initiate scanning processes, leveraging scanning services from MetaDefender Core, MetaDefender Distributed Cluster, or MetaDefender Cloud based on the configured workflow rule.

Each scan pool configuration is tied to a specific scan pool and workflow rule, ensuring consistent scanning behavior across MetaDefender Core, MetaDefender Distributed Cluster, and MetaDefender Cloud instances.

> **IMPORTANT**
>
> The default workflow rule for MetaDefender Core/Distributed Cluster is 'MetaDefender Storage Security'.
>
> For MetaDefender Cloud default rules are 'multiscan' and 'unarchive', please check the following documentation.

When configuring the scan pool step in a workflow, you can select a scan pool, optionally enable failover to a secondary scan pool for cases where all scan instances from the primary pool are unavailable or unresponsive, and specify the user agent and workflow rule to apply during scanning.



Technologies

This lists all technologies available in the connected MetaDefender Core/Cloud/Distributed Cluster instance configured in the scan pool step. If settings have changed on the MetaDefender Core/Cloud/Distributed Cluster side, use the **Refresh technologies** button to load the latest available technologies



File Tagging

When enabled, File Tagging labels processed files with their security status (clean, sanitized, blocked) to support compliance and audit requirements. You can configure which tags are applied, including the MetaDefender result, file ID, and analysis timestamp and customize the tag name for each. Tags can be reset to their default values at any time using the **Reset tags to default** button.

For instructions on setting up the feature, refer to the Configure File Tagging.



Deep CDR

Applies OPSWAT's Deep CDR (file sanitization) technology to files.

Enabling the File Sanitization feature creates a secure version of a file by removing potentially harmful content. This process utilizes OPSWAT's Deep Content Disarm and

Reconstruction (Deep CDR) technology.

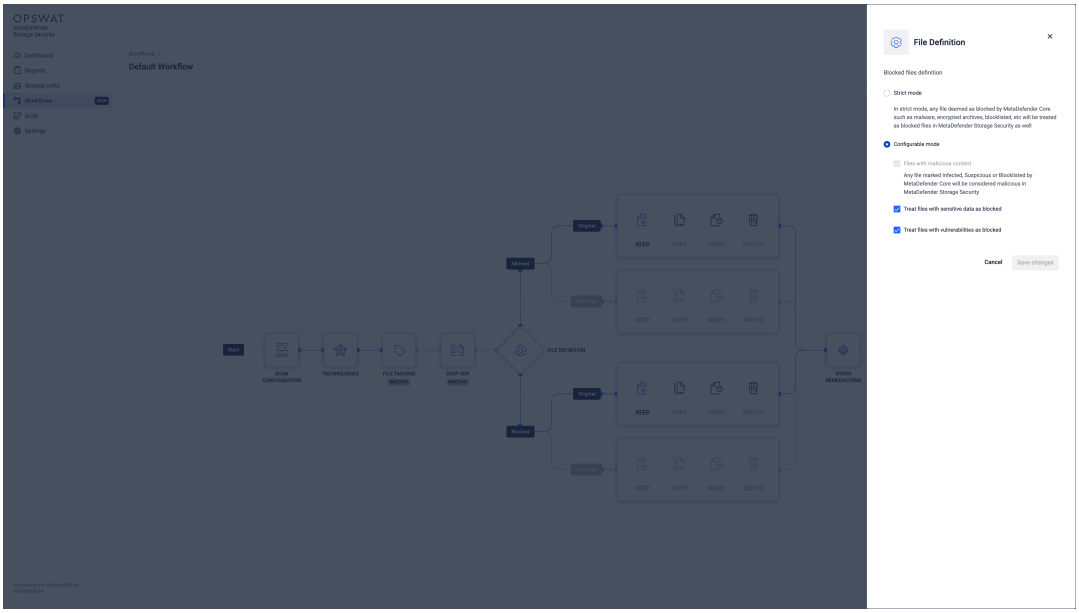
For detailed instructions on configuring this feature, refer to the Deep CDR user guide and Deep Content Disarm and Reconstruction (Deep CDR).



File Definition

What was previously known as Remediation Actions is now called File Definition, which dictates the outcome for each file based on its scan results. Files can be designated as Allowed (approved), Sanitized (cleaned), or Blocked (quarantined).

For detailed setup instructions, refer to the Configure File Definition.



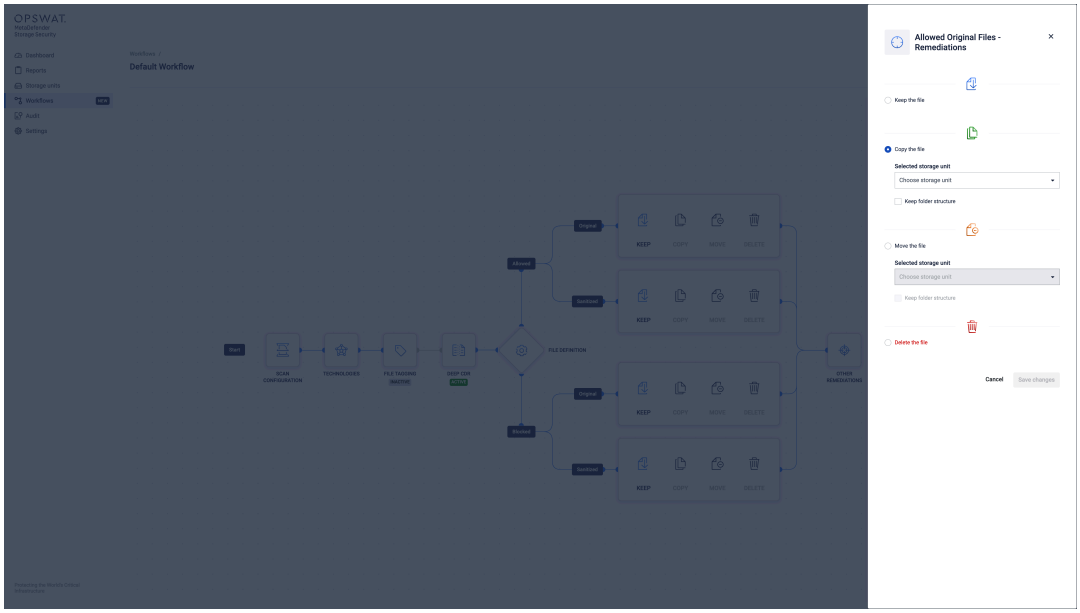
File Remediations

File remediation actions are automated post-processing tasks performed on files after they have been scanned. The following remediation options are currently available: Keep, Copy, Move, Delete.

For more information on setting up the feature, refer to the Keep, Copy, Move or Delete Files.

Important Considerations

- Make sure that the destination buckets for moved or copied files are properly configured and accessible within your environment (in this case Amazon S3)
- Carefully consider your organization's risk tolerance when configuring deletion actions. Implement safeguards like versioning or backups to prevent accidental data loss.
- Develop a clear tagging strategy to facilitate efficient file management and consistency.
- Regularly review and update your remediation actions and tagging configurations to align with your organizational evolving security needs and policies.



Other Remediations

Delete Empty Folders

Delete a directory if it is empty after remediation (does not delete if the folder was empty to begin with).

For detailed setup instructions, refer to the Delete Empty Folders.

> **Dependency**
>
> The delete empty folders remediation can be active only if there is at least one of another remediations configured with “Move the file” or “Delete the file”.

Scan File Versions

> This remediation type is only supported by the SharePoint On-Prem storage unit type.

Retrieve & process all past versions of a file. This comes with a performance cost, as all versions will be scanned like normal files.

For more details about this feature, refer to Scan File Versions.


Other remediations
Delete Directories
If it is empty after remediation (does not delete if the folder was empty to begin with) delete it.
Disabled
Depth
1
How does depth work?
Scan File Versions
File versioning is only supported by the following storage types: SharePoint On-Prem
Enabled
End

Error Handling

The remediation process includes automatic retry functionality to handle transient failures.

For detailed configuration steps, refer to the Remediation Process Retries.

Autodiscovery

Autodiscovery is a powerful feature in MetaDefender Storage Security designed to **simplify and accelerate the integration of your cloud storage**.

It automatically detects and adds storage units from supported cloud storage services, eliminating the need to manually configure each one.

This significantly streamlines the process of onboarding multiple storage units, saving valuable administrative time and reducing the potential for configuration errors.

Supported Storage Types

> **Info**
>
> Currently, Autodiscovery functionality is available for the following cloud storage service:
>
> - **Amazon S3**
> - **Google Cloud**
> - **SharePoint Cloud**

Note: MetaDefender Storage Security is continuously evolving. Support for additional cloud storage services may be introduced in future releases. Please refer to the latest release notes for the most up-to-date information.

How Autodiscovery Works

The Autodiscovery process involves several key stages:

1. **Prerequisites**
    - Before initiating autodiscovery, ensure the credentials you provide for your cloud storage service (for example AWS IAM user or role for Amazon S3) have the necessary permissions to list all available storage units (`s3:ListAllMyBuckets` permission for S3). Without these permissions, MetaDefender Storage Security cannot detect your storage units.
    - Familiarize yourself with how accounts and groups are managed within MetaDefender Storage Security. This will help you understand how autodiscovered storage units are organized post-discovery. For comprehensive details, please review the Accounts & Groups documentation below.
2.

Initiating Storage Discovery

- You provide valid credentials for a supported cloud storage service through the MDSS interface.

3. **Scanning and Detection**

- MDSS uses the provided credentials to securely connect to your cloud storage account
- It then scans the account to detect all available storage units (e.g. S3 buckets associated with the AWS account).

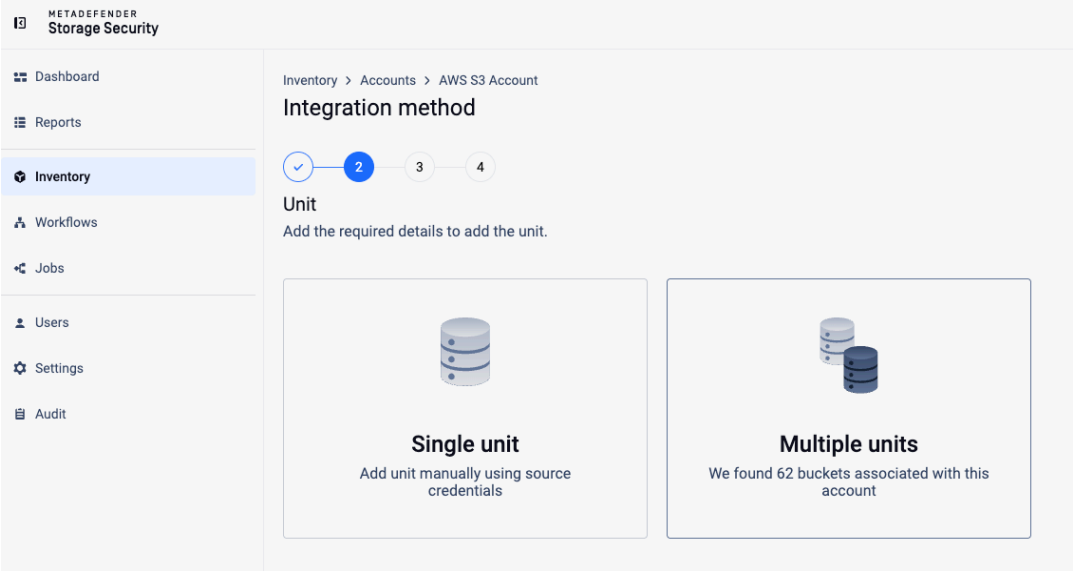
4. **Automated Integration & Configuration**

- Successfully detected storage units are automatically added to MetaDefender Storage Security.
- These autodiscovered storage units will typically be associated with a specific account and group within MetaDefender Storage Security, often based on the context of the autodiscovery setup.

> **LIMITATION**
>
> **All units discovered in a single operation will share the same initial account and group configuration.**

The Autodiscovery feature works by:

- **Storage Discovery**: When provided with valid credentials for a supported cloud storage service, the system scans the associated account to detect all available storage units (such as S3 buckets).



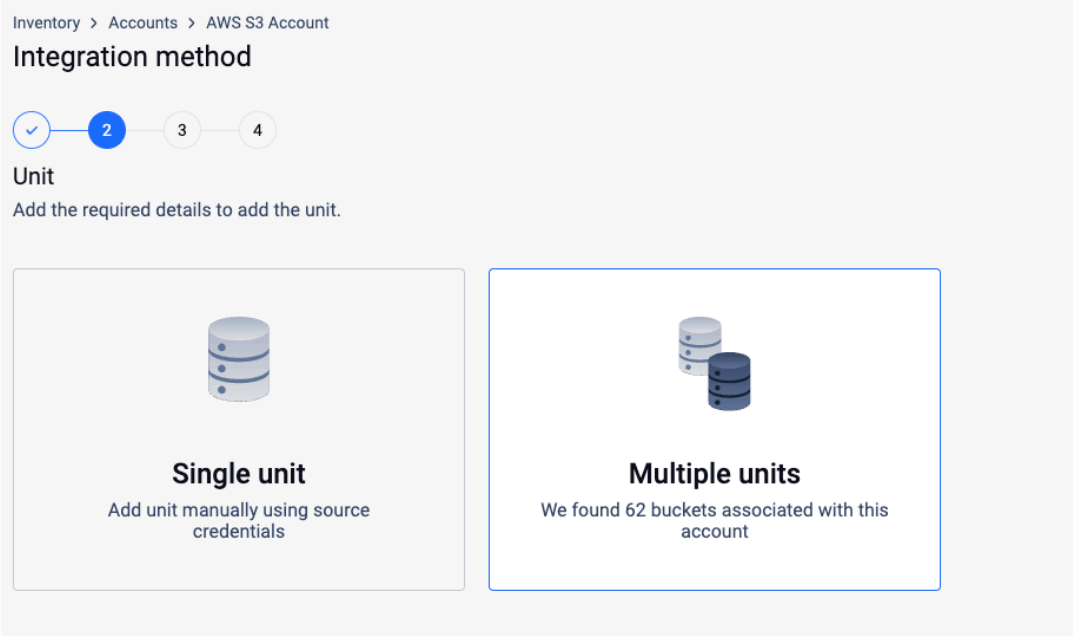
- **Automated Addition**: Depending on the chosen method, the system can either:
  - Automatically add all discovered storage units
  - Present a list of discovered storage units for manual selection
  - Allow individual adding of storage units
- **Periodic Synchronization**: For accounts with Autodiscovery enabled, the system periodically checks for new storage units and automatically adds them to MetaDefender Storage Security.

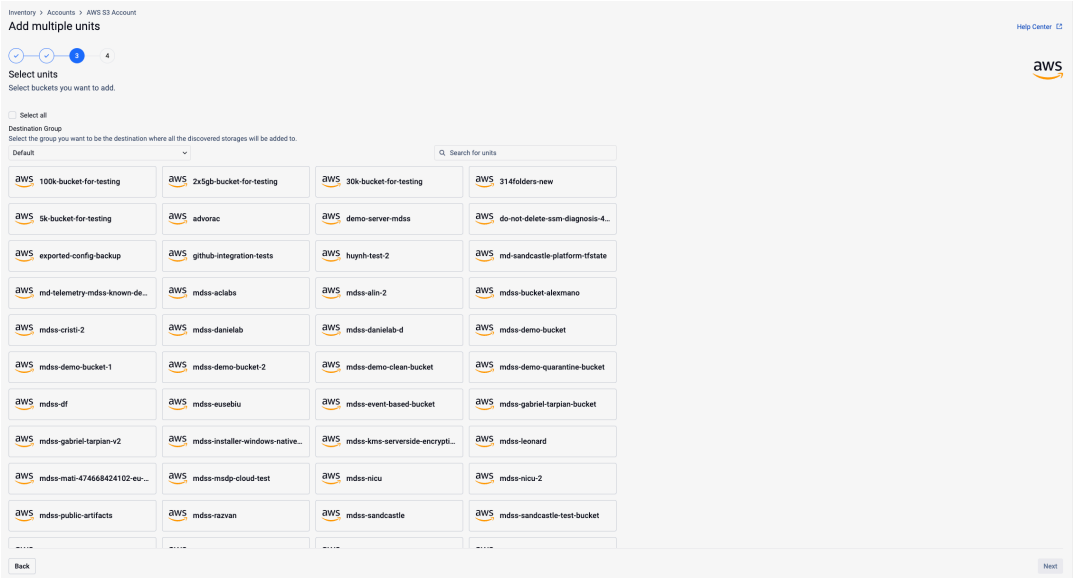
Using Autodiscovery

Method 1: During Storage Unit Addition

1. From the Storage Units page, click “Add Storage Unit”
2. Select a supported storage type (Amazon S3, Google Cloud)
3. You’ll be presented with two options:
    1. Add one storage unit with full configuration control
    2. Use Autodiscovery to add multiple storage units
4. If you select “Storage Discovery”, you’ll need to:
    1. Provide account credentials
    2. Select a region (if applicable)
    3. The system will then discover available storage units
5. After discovery completes, you’ll have two options:
    1. Automatically add all discovered storage units (Autodiscovery)
    2. Select which specific units to add (Manual Selection)

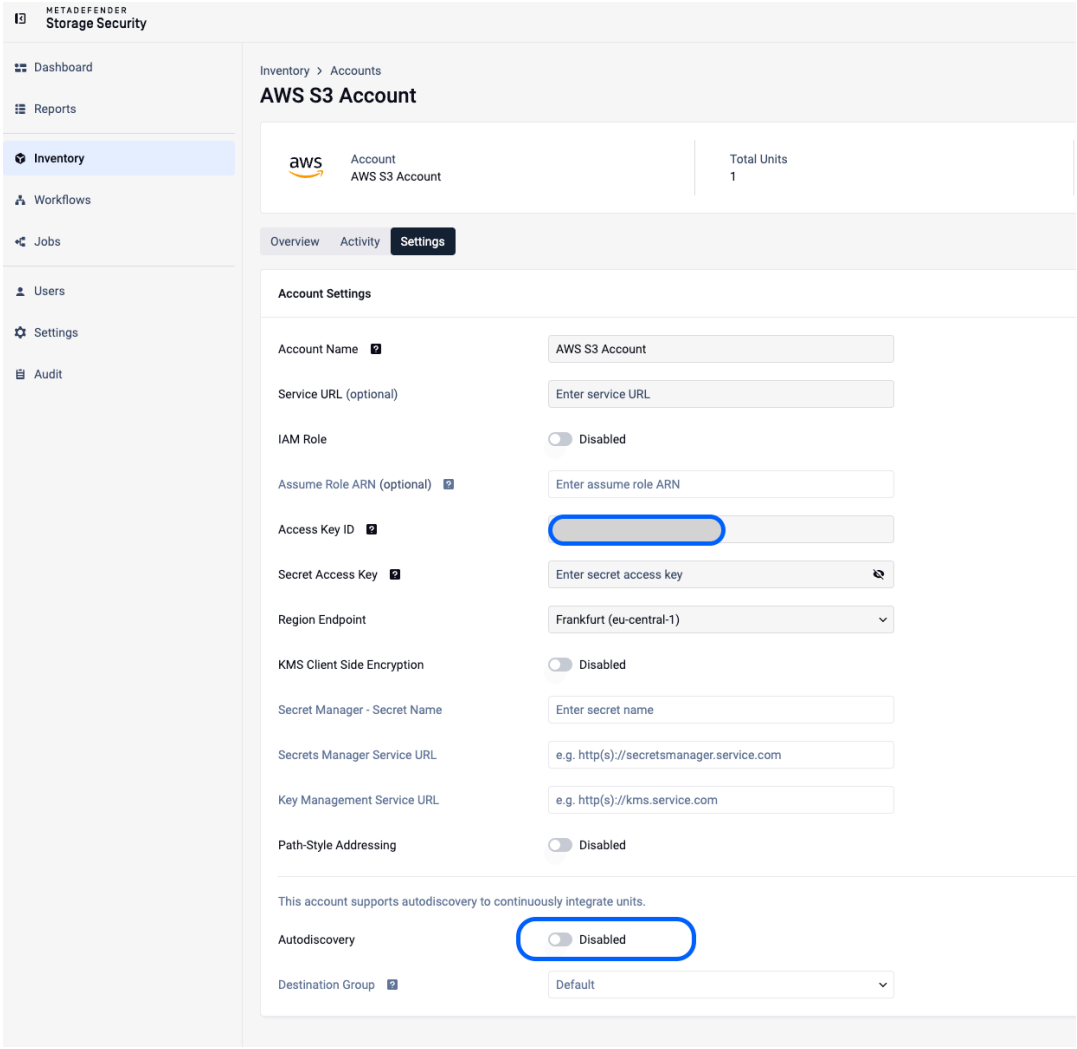
6. Complete the process by clicking “Continue” and confirming your choices





Method 2: Enabling Autodiscovery for an Existing Account

1. From the Storage Units page, click on the 3-dots menu of a supported storage type card (e.g., Amazon S3) and select “Manage Storage Unit”
2. You’ll be presented with two options:
    1. Update just the storage information (not the credentials of the account)
    2. Update the account’s credentials
3. If you select “Change Account Info”, you’ll be able to toggle the Autodiscovery on or off
4. Input the secret key and complete the process by clicking “Save changes”



Common Issues

1. **No storage units discovered**
    1. Verify the credentials have sufficient permissions
    2. Check that the selected region is correct
    3. Confirm that the account contains storage units of the supported type
2. **Autodiscovery not working periodically**
    1. Verify the account's Autodiscovery setting is enabled
    2. Check system logs (e.g., Audit page) for any authentication or connection errors
3. **Storages not appearing in Storage Units page**
    1. If the used option was "Storage Discovery" + "Manual Selection", in the Summary view of adding the storage unit, a list of the storages that weren't added successfully will be visible, including the error why it wasn't added.

LIMITATIONS

When storage units are autodiscovered, they will all be set up in the system sharing the same account and group details provided during the autodiscovery configuration.

For autodiscovery to successfully identify your storage units, the credentials used must possess the necessary permissions to list all accessible buckets.

Inventory

The **Inventory** page is where you view and manage all the storage resources that MetaDefender Storage Security (MDSS) protects. From here you can see every storage unit registered for scanning, the groups they are organized into, and the accounts used to connect to your storage providers.

Access: Select **Inventory** in the left navigation menu.

Tabs

The page is organized into three tabs:

- **Units** — Individual storage locations registered for scanning (for example, an Amazon S3 bucket or an NFS share).
- **Groups** — Logical collections of units, used to apply shared settings and workflows.
- **Accounts** — The connections and credentials MDSS uses to reach each storage provider.

Units

Individual storage locations registered for scanning (for example, an Amazon S3 bucket or an NFS share).

To add a new storage unit, please follow the Integrations page.

Accounts

What are Accounts?

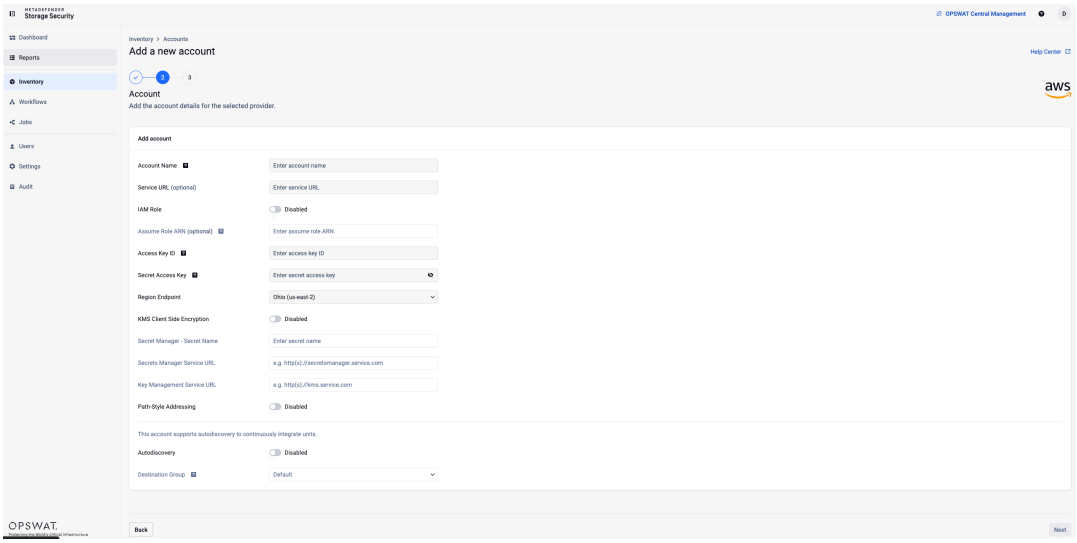
Accounts in MetaDefender Storage Security allow you to:

- Store and manage access credentials for storage services in one centralized location (credentials are encrypted and stored securely in the database)
- Associate multiple storage units with a single account for simplified management
- Enable automatic discovery of new storage units for supported services (currently Amazon S3)
- Organize storage resources within groups for better administration

> **Security Note**
>
> Role-based access control governs all account operations - Administrator, SSO Administrator, and Tenant Administrator roles have full permissions to create, modify,

> and delete accounts, while Read-Only Administrator and SSO Read-Only Administrator roles cannot perform these actions.

Creating a New Account



Accounts can be created during Storage Unit addition:

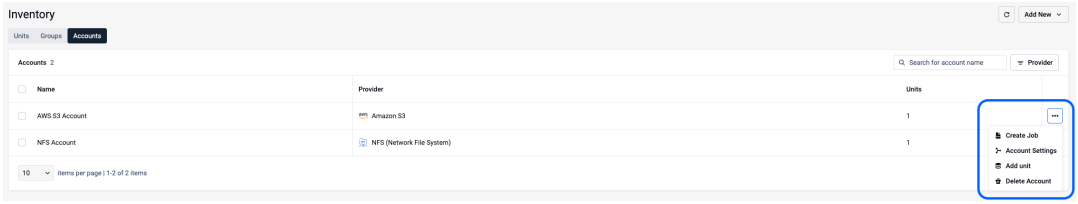
1. Navigate to the Storage Units page and click on "**Add storage unit**" button
2. Select the service you want to integrate
3. From the top toggle, select "**Add new account**"
4. Fill out the required account's credentials and the storage's specific fields
5. Click "Continue" to create both the account and storage unit

> **Note**
>
> There are no limits on the number of accounts that can be created.

Managing Existing Accounts

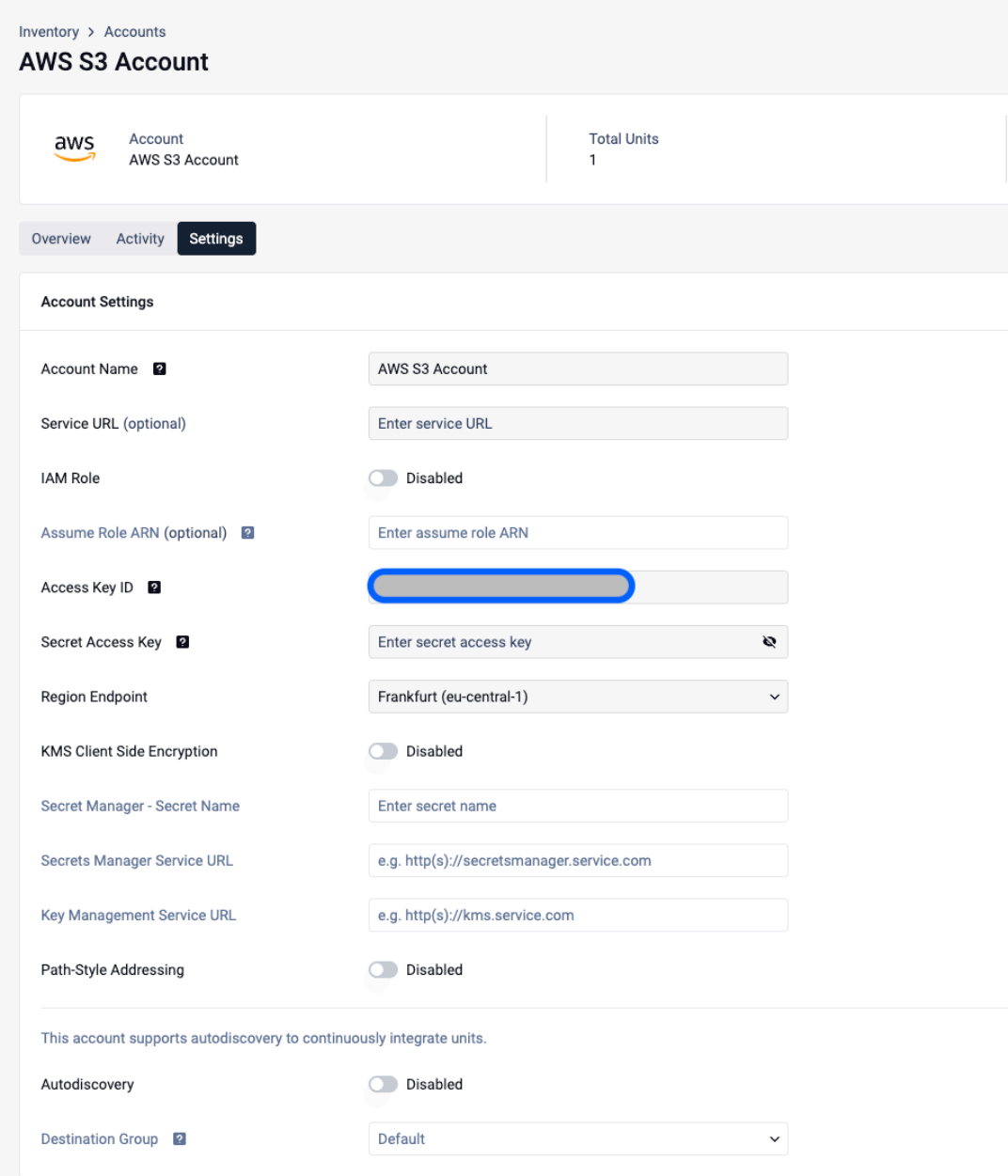
1. Navigate to the Storage Units page
2. Switch to **"Accounts"** view using the toggle in the top-right
3. Locate the account you want to manage
4. Click the **three-dot menu** next to the account name

Available Account Actions



- **Create Job - **Starts instant scans for all storage units under the account. These scans can be monitored through the ongoing scans interface. If individual scans fail, they are handled independently without affecting other scans in the batch.
- **Account Settings** - Opens modal to modify account credentials
- **Add unit** - Add a new storage unit in this account
- **Delete Account** - Removes the account

Edit Account Information



1. From the account's three-dot menu, select **"Edit Account Information"**
2. The modal opens pre-populated with current account details
3. You'll be required to input credentials or credentials file to validate changes
4. Click **"Save changes"** to update the account

Delete Account

1. From the account's three-dot menu, select **"Delete Account"**

2. **Accounts with storage units:** Cannot be deleted - you'll see a warning message with the count of associated storage units
3. **Empty accounts:** Can be deleted after explicit confirmation
4. Confirm the deletion when prompted

> **IMPORTANT**
>
> When accounts are deleted, all associated reports and historical scan data are permanently removed and cannot be exported - there are currently no data export capabilities for this purpose.

Groups

What are Groups?

Groups in MetaDefender Storage Security provide an organizational structure for managing storage units and accounts. They enable logical grouping of related storage resources, simplifying administration and enhancing visibility across the system.

Key Features include ways to:

- Organize storage units and accounts in logical collections
- Perform actions on multiple storage units at once
- Clear visual separation of resources in the user interface

> **IMPORTANT**
>
> MDSS groups operate as a single-level organization system without nesting capabilities, and storage units cannot belong to multiple groups simultaneously. All storage units are mandatory to be assigned to a group.

Default Group

The system includes a default group. This ensures that all storage units and accounts always have a group assignment, even if a custom group is deleted.

- Storage units or accounts can be moved to the default group if their assigned group is deleted
- The default group has a predefined ID and name but can have its description modified

Creating and Managing Groups

Creating a New Group

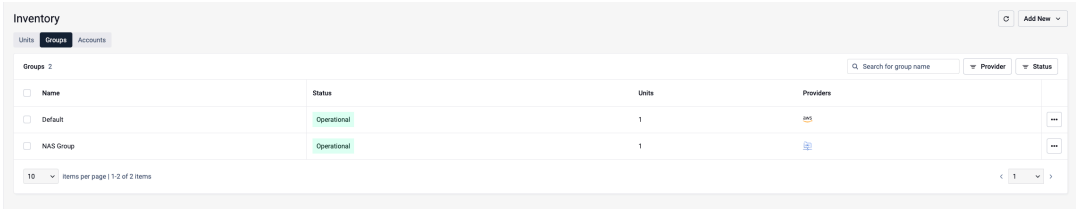


Groups can be created from the Storage Units and Dashboard View

- Click the **“Create New Group”** button in the header actions
- Enter a **group name** (required field)
- Optionally **select existing storage units** to include in the group
- Click **“Create Group”** to finalize

> **Note**
>
> During storage unit creation, the first available group is pre-selected by default. There are no limits on the number of groups that can be created.

Managing Existing Groups



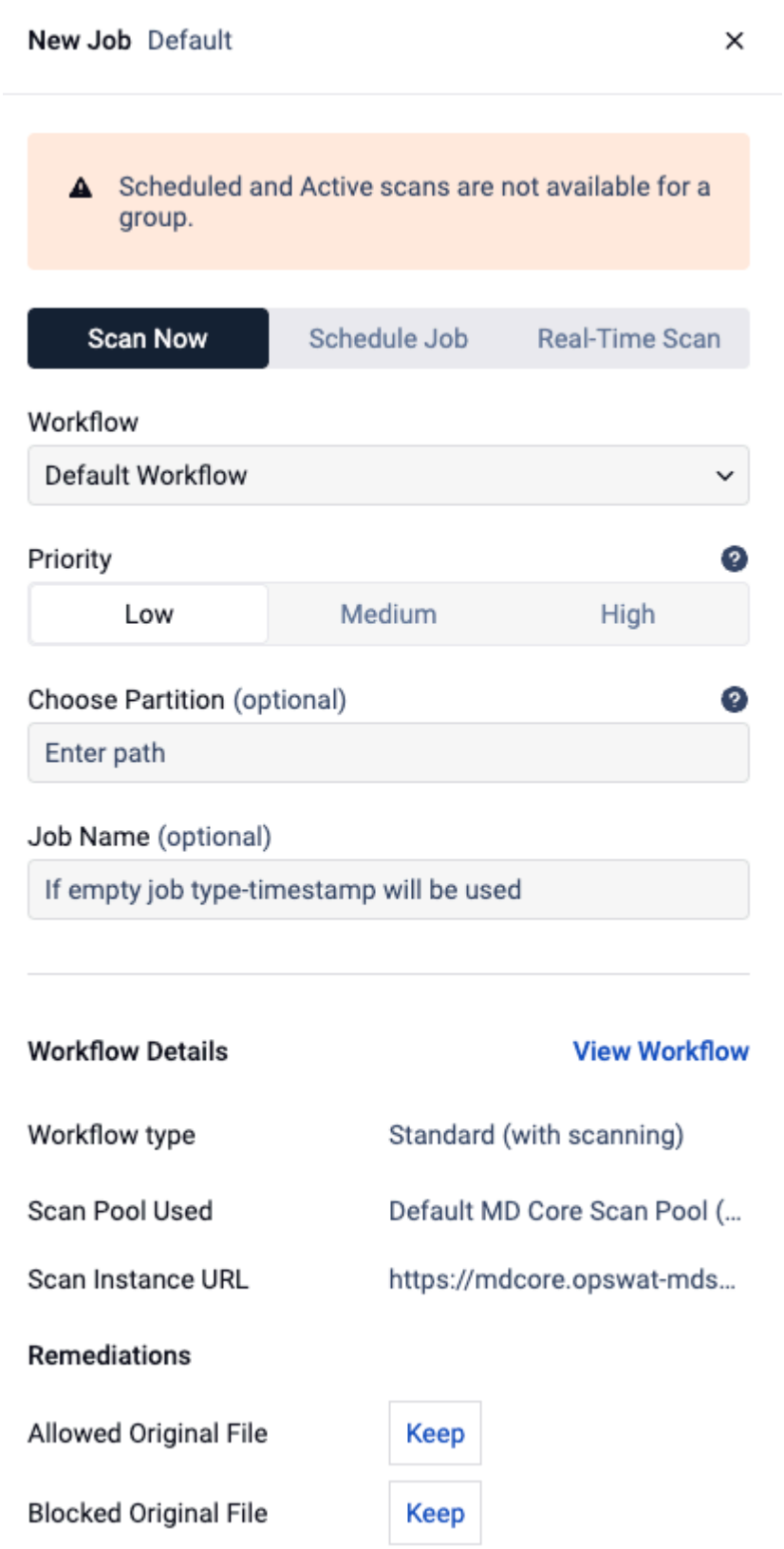
1. Navigate to the Storage Units page (Groups view)
2. Locate the group you want to manage
3. Click the **three-dot menu** next to the group name

> **Security Note**

> Role-based access control governs all group operations - Administrator, SSO Administrator, and Tenant Administrator roles have full permissions to create, modify, and delete groups, while Read-Only Administrator and SSO Read-Only Administrator roles cannot perform these actions.

Available Group Actions

Scan All Group Items



- Starts instant scans for all storage units under the group. These scans can be monitored through the ongoing scans interface. If individual scans fail, they are

handled independently without affecting other scans in the batch.

Group Status Information

Storage Count Badge

- Shows the total number of storage units in each group with format: “X storage units”

Status Badges

Visual indicators showing:

- **Error Count** - Badge showing storage units with errors
- **Testing/Untested Count** - Badge showing storage units being tested or untested
- **Success State** - No badges when all storage units are operational

Moving Storage Units Between Groups

1. From any storage unit’s management options(three-dots), select **“Move to Group”**
2. Choose the destination group from the dropdown
3. Confirm the move to complete the transfer

Cross-Domain Transfer (Data Diode)

Move files across a one-way security boundary using MetaDefender Storage Security on both sides of an OPSWAT NetWall diode. The diode transfers files over SMB; MDSS accesses each SMB share by mounting it as an NFS storage unit.

Overview

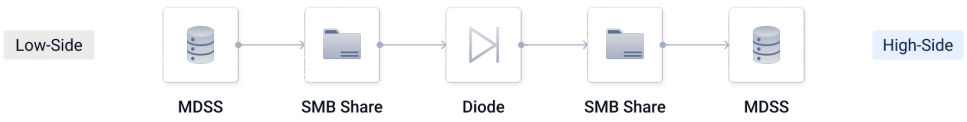
A data diode enforces one-way data flow: traffic goes from the low side (source) to the high side (destination) and never back. This physical isolation is why diodes protect critical environments — there is no return path, and no delivery acknowledgement.

How It Works (Concepts & Architecture)

The architecture is symmetric. The diode owns the cross-boundary mechanics over SMB; MDSS reads and writes its share through an NFS mount of that same SMB share. Complete flow:

1. Low-side MDSS pulls from a source storage (SharePoint, S3, or any integrated storage), scans/remediates, and writes approved files to the low-side share.
2. The NetWall diode polls that share over SMB, transmits each file across the optical link, and writes it to the high-side share.
3. High-side MDSS reads the high-side share, scans/remediates, and forwards files to the destination.

The diode is the SMB client on both sides and owns all cross-boundary mechanics: polling, transfer, and cleanup. MDSS only writes to the low-side share and reads from the high-side share, treating each as an ordinary NFS storage unit.



SMB vs FTP

SMB is recommended. It multiplexes transfers, sustains higher bandwidth, and has sub-second timestamps that MDSS uses to detect when a file is fully written. NetWall's native FTP transport is supported but under increased concurrent load the FTP channel resets without self-recovery.

Requirements

- An OPSWAT NetWall diode configured for native SMB file transfer. Set up the share on the diode per the NetWall Windows file share guide.
- Two SMB shares, one per side, reachable by the diode and the local MDSS host. Any standards-compliant SMB server works (e.g. Samba).
- Two MDSS instances, one per side, see Planning your deployment. Low-side MDSS reaches the source storage; high-side MDSS reaches the destination.

The diode speaks SMB, but MDSS connects to each share as an NFS storage unit: mount the SMB share on the MDSS host, then add it to MDSS as NFS. Do this on both sides:

- Add an SMB share as an NFS storage unit (Windows deployment)
- Add an SMB share as an NFS storage

Throughput is bounded by the diode license tier (e.g. 100 Mbps; gigabit raises file transfer to 500 Mbps) and by disk I/O on the shares.

Set Up the Low Side (Sender)

1. Mount the SMB share into low-side MDSS and add it as a NFS storage unit (see Requirements).
2. Create a workflow whose copy or move destination is that storage unit.
3. Start a scan on the desired storage unit with that workflow. Files are written to the share, and the diode polls them automatically.

Set Up the High Side (Receiver)

1. Mount the SMB share into high-side MDSS as an NFS storage unit (see Requirements).
2. Set the discovery debounce environment variable so MDSS never scans a file the diode is still writing; it skips any file modified within the window:`NFS_DISCOVERY_DEBOUNCE_TIME_SECONDS=30` 30s suits typical files; raise it for large files that take longer to cross the link.
3. Create a workflow whose copy or move destination is your target storage (e.g. SharePoint)
4. Start a real-time (RTP) scan on the storage unit with that workflow. As the diode writes files in, MDSS discovers, scans, and forwards them.

Monitor

- MDSS surfaces progress only for running scans, the low-side scans and the high-side RTP scan, from the UI.
- Use the diode's own monitoring for transfer status, queue depth, and channel health across the link.
- There is no delivery acknowledgement back to the low side. End-to-end reconciliation means comparing source vs. destination inventories.

Troubleshooting

Files get scanned mid-write, or scans come back partial. MDSS picked up a file before the diode finished writing it. Bump `NFS_DISCOVERY_DEBOUNCE_TIME_SECONDS` past how long your biggest file takes to cross.

Transfers die after the first 10–15 files. This shows up on old SMB servers (Samba 4.12.x). Upgrade to a modern version, if it is not an option, turning off oplocks and leases helps but the real fix is the newer server.

Low-side share keeps filling up. The diode is supposed to delete each file once it's across. If files pile up, check that its account can actually delete on the share and that it's still polling.

Files vanish under heavy load. When the destination can't keep up with the incoming rate, the high-side diode buffers to disk. Once that buffer is full, new files are dropped — silently, because a diode has no way to tell the sender to slow down. Give the destination enough headroom, cap per-file size, and split very large files on the source side.

Limitations

- **No delivery confirmation.** A diode has no return channel, so a full high-side buffer drops files silently. Size the destination and diode disk for peak load.
- **Retransmit on HA failover.** NetWall supports active/standby HA, but if the active high-side node fails with files still buffered, those files are lost and must be re-sent from the source today a manual reprocess. Plan source-side retention.
- **FTP is supported but not recommended.** channel resets under concurrent load and timestamps are minute-resolution. Use SMB.

Configuration and Management

Custom configuration

How to edit the configuration file on Linux

Custom application configuration can be achieved by editing the *customer.env* environment file.

The following steps are required to change different parameters in this file:

- Navigate to */etc/mdss/customer.env* and open the file
- If the parameter that needs to be changed is not present, add the new parameter with the desired value. If it already exists, just edit the value.

```
CONFIGURATION_PROPERTY_NAME=VALUE
```

- Save the file
- In order for the changes to apply, please restart the application by running the following command:

```
sudo mdss -c restart
```

How to edit the configuration file on Windows

Custom application configuration can be achieved by editing the *customer.env* environment file.

The following steps are required to change different parameters in this file:

- By default the file is located in C:\Program Files\OPSWAT\MetaDefender Storage Security\config\cutomer.env
- If the parameter that needs to be changed is not present, add the new parameter with the desired value. If it already exists, just edit the value

```
CONFIGURATION_PROPERTY_NAME=VALUE
```

- Save the file
- In order for the changes to apply, please restart the application by running the following command:

```
mdss.ps1 -c refresh
```

Increase the number of concurrent scans

To be able to scan multiple files at the same time, the event bus needs to be configured accordingly. Please add the following environment variable in your *customer.env* file (as described above):

Environment Variable	Default Value	Maximum Value	Description
RABBITMQ_SCANNING_PREFETCH_COUNT	20	200	Allow up to 50 files to be scanned at the same time.

Certificate validation for MetaDefender Core connection

This environment variable controls certificate validation for MetaDefender Core integration during HTTP(S) requests. It is useful when MetaDefender Storage Security needs to accept a partially valid certificate chain or a self-signed certificate.

Environment Variable	Default Value	Possible Values
MD_CORE_CERTIFICATE_VALIDATION	0	0 - Use the built-in validation (recommended) 1 - Ignore certificate chain errors 2 - Ignore all certificate errors

Description

- 0 → A MetaDefender Core server with invalid certificate can't be integrated
- 1 → A MetaDefender Core server with certificate chain errors can be integrated
- 2 → A MetaDefender Core server with invalid certificate can be integrated

MetaDefender Core unavailability period

Configure the period of time a MetaDefender Core server is considered unavailable when a scan failure occurs.

Environment Variable	Default Value	Description
LOAD_BALANCER_MD_CORE_UNAVAILABLE_TIME	5	When a scan fails, the respective MetaDefender Core server will be unavailable for this period of time (in minutes). The load balancer cannot choose it for another file during this time period.

Azure Blobs

Configure the number of blobs read in one request

Environment Variable	Default Value	Max Value	Description
AZURE_BLOB_PAGE_SIZE	100	5000	Number of blobs discovered in container in a single request.

Amazon S3

Configure the validity duration of presigned URL used for download files from storage

Environment Variable	Default Value	Min Value	Description
PRESIGNED_URL_EXPIRATION_SECONDS	259200	30	Value is defined in seconds

Web interface port

MetaDefender Storage Security's web interface normally uses port 80 (for regular web access) and port 443 (for secure web access). If you need to use different ports, follow these steps:

For Linux Users:

1. Open the Configuration File:
   - Having elevated privileges, use a text editor to open the file located at `/etc/mdss/customer.env`.
2. Change the Port Numbers:
   - Find or add these lines:
     - `WEB_PORT = 80`

    - `WEB_PORT_SSL = 443`
  - Replace `80` and `443` with the new port numbers you want to use.
3. Save the Changes:
  - Save the `customer.env` file.
4. Restart MetaDefender Storage Security:
  - Open a terminal and run this command: `sudo mdss -c restart`

For Windows Users:

Setting up a custom Web interface port can be done either during the installation process [Windows Installation] or after the installation by following the steps below:

1. Open the Configuration File:
2. - Having elevated privileges, open the file `C:\Program Files\OPSWAT\MetaDefender Storage Security\config\customer.env` using a text editor like Notepad.
3. Change the Port Numbers:
  - Find or add these lines:
    - `WEB_PORT = 80`
  - [Optional] If running on HTTPS
    - `WEB_PORT_SSL = 443`
  - Replace `80` and `443` with the new port numbers.
4. Save the Changes:
  - Save the `customer.env` file.
5. Apply the Changes and Restart:
  - Open powershell.
  - Run these commands:
    - `cd "C:\Program Files\OPSWAT\MetaDefender Storage Security\scripts"`
    - `.\mdss.ps1 -c refresh`
    - This command will refresh the environment variables and restart MetaDefender Storage Security.

Real Time Processing configuration for NAS

> **Info**

> This is applicable only to **NFS**, **SMB**, **SFTP, FTP**, **NetApp ONTAP** and **Dell Isilon** storage units.

When activating Real-Time Processing (RTP) for your storage resources, please note the following operational characteristics:

Scope of Detection

Real-Time Processing monitors and detects only files that are newly created or modified subsequent to scan initiation. The system does not retroactively process pre-existing files that were present in your storage prior to enabling RTP.

Comprehensive File Assessment

To ensure complete analysis of your storage repository, including all pre-existing files, we recommend implementing either:

- Scheduled scans - Configured at predetermined intervals
- On-demand scans - Initiated manually as needed

These comprehensive scan types will process the entirety of your storage contents, including files that predate your RTP implementation. This differentiated approach allows for both continuous monitoring of new content and periodic comprehensive assessment of your complete data repository.

Timestamp Behavior and Detection Implications

When using certain file transfer tools such as WinSCP and similar GUI-based applications, the original file's **LastModifiedDate** is typically preserved during the copy operation. This behavior means:

- Files copied via WinSCP to SMB/NFS/SFTP/FTP shares will retain their original modification dates
- A file last modified in January 2023 and copied in June 2024 will still display January 2023 as its modification date

As a result, Real-Time Processing (RTP) may not detect these files if their modification timestamps predate the RTP scan initialization. For example, if a file with a modification date of "January 2023" is copied to your storage in "June 2024" after RTP has been activated, standard detection mechanisms will not identify this file as newly added content.

Advanced Configuration for Comprehensive Detection

To ensure all newly copied files are properly detected regardless of their modification timestamps, we have implemented enhanced detection capabilities through the following configuration parameters:

DISCOVERY_SERVICE_SMB_RTP_HANDLING=1

DISCOVERY_SERVICE_SFTP_RTP_HANDLING=1

DISCOVERY_SERVICE_NFS_RTP_HANDLING=1

DISCOVERY_SERVICE_FTP_RTP_HANDLING=1

Implementation Procedure

To activate enhanced file detection, add the appropriate parameter (following this guide) in your **customer.env** file and then restart our product for changes to apply.

Once implemented, these configuration options ensure that all files added to your storage will be detected during Real-Time Processing, irrespective of their modification timestamps.

Temporary local files created during remediation

Overview

MDSS creates temporary files during specific remediation operations to ensure reliable data processing. These temporary files are generated during:

- File transfers between storage units
- File sanitization operations using our DeepCDR technology

To assist with troubleshooting and compliance auditing, MDSS provides configurable logging of these temporary file operations.

Temporary File Locations

Linux deployments

Each storage integration runs as a single Docker container named mdintegrations_ (for example mdintegrations_nfs), which hosts the Discovery, Storage, and Remediation services for that storage type. Temporary files are created inside the container of the destination storage type, in the standard Linux temporary directory** /tmp/**.

Operation	Container location
Moving from any storage to NFS	**mdintegrations_nfs**
Moving from any storage to SMB	**mdintegrations_smb**
Sanitization with DeepCDR	Container of the source storage[**mdintegrations_nfs **for NFS files]

Windows deployments

All temporary files will be created in the standard Windows temporary directory **C:\Windows\Temp**

Configuration

The temporary file logging feature can be enabled or disabled by setting the **LOG_CREATION_OF_TEMP_FILES** variable in your **customer.env** file:

- 0: logging disabled (default value)
- 1: logging enabled

To update your **customer.env** file, please follow this guide.

Example:

```
LOG_CREATION_OF_TEMP_FILES=1
```

```
[2025-03-13 14:44:40Z] [Information] remediations.nfs.service: Local
temporary file created. Path: C:\Windows\Temp\4mn110iw.gzn. Size:
1048624. Reason: Upload non-seekable stream. AutoDelete: True.
Destination: credit-card-file-
v2_sanitized_by_OPSWAT_MetaDefender_9619874ae98542129d386871a8cb0268.tx
t
```

Log file locations

Linux deployments: **/etc/mdss/services_logs/**

Windows deployments**:** **{InstallDir}\services**

Frequently Asked Questions

Are my files safe during this process?

Yes. Temporary files exist only within isolated Docker containers (Linux deployment) or in locations accessible only by administrators (Windows). Access to these files is restricted to MDSS processes.

Does this affect performance?

The impact is minimal. Our system is optimized to handle temporary files efficiently and clean them up promptly.

Can I disable temporary file creation?

No. Temporary files are essential for reliable data transfer between microservices in the MDSS architecture.

What happens if a container crashes?

Temporary files exist only within the container's filesystem. If a container crashes or restarts, the temporary files are automatically deleted as part of Docker's container lifecycle.

Are the temporary files using additional storage beyond what is already allocated?

No. The temporary files are created within the allocated storage for your Docker containers. They do not consume additional storage beyond what is already allocated to your deployment.

Best Practices

For optimal performance and security:

1. Ensure your Docker containers have adequate storage allocation. Please follow our guide to properly allocate disk space
2. Monitor container resource usage during large data transfers

Performance Tuning Guide

About This Guide

This guide is designed to assist you in fine-tuning various configuration settings to achieve desired throughput and performance levels. By default, MetaDefender Storage Security operates in a balanced mode, optimizing both speed and functionality for maximum value. However, in scenarios where certain features may be unnecessary and system throughput is paramount, this guide will provide you with the necessary steps to adjust your settings for optimal performance outcomes.

Scanning Performance

The throughput of the system largely depends on the speed of the scan instance. If you are using MetaDefender Cloud, our SaaS offering, you are automatically benefiting from optimal performance. For users of MetaDefender Core, we recommend visiting the MetaDefender Core Performance Tuning Guide to explore ways to reduce the response time of your scan instance.

Increasing the number of concurrent file scans

A critical configuration parameter in MetaDefender Storage Security that significantly affects throughput is the number of concurrent scan requests sent to the scan instance. By default, the system processes 20 files simultaneously. As each file completes scanning, another is promptly queued. If your scan instance has additional capacity, we recommend gradually increasing this count to optimize throughput until you reach the desired performance level.

> **IMPORTANT**
>
> When adjusting the number of parallel scan requests, it's important to monitor the scan instance queue closely. An excessive number of messages in the queue indicates that the setting is too high, which can lead to performance degradation due to overloading the scan instance. Please adjust accordingly to maintain optimal performance.

To adjust this setting please modify the **`RABBITMQ_SCANNING_PREFETCH_COUNT`**environment variable as described in: Custom Configuration | Increase the number of concurrent scans.

Discovery Performance

Discovery Throttling

In scenarios where system load is exceptionally high, you may encounter a notification that discovery has been temporarily throttled. This measure halts the discovery of new files when the queue already contains a large volume of pending files. It is designed to optimize system resources and prevent excessive RAM usage. By setting this limit, we ensure efficient processing and reduce the risk of an endlessly growing queue, which can occur if the rate of file discovery exceeds the scanning capacity.

The threshold for maximum pending files is controlled by two environment variables:

- `DISCOVERY_THROTTLER_MAX_PENDING_FILES` , which defaults to 5000 for workflows with scanning
- `DISCOVERY_THROTTLER_NOT_SCANNED_MAX_PENDING_FILES` , which default to 50000 for discovery-only workflows

These values can be adjusted up or down based on your system's specifications to optimize memory usage.

When the system is throttled, it does not stop indefinitely - it waits a moment, then checks whether it is ready to continue. Two settings let you control how long it keeps trying before moving on:

- `DISCOVERY_THROTTLER_MAX_RETRY_ATTEMPTS` - the number of times the system will check before resuming discovery. Defaults to `10`.
- `DISCOVERY_THROTTLER_MAX_DELAY_MINUTES` - the maximum wait time between each check, in minutes. Defaults to `10`.

You can raise these values if you want the system to wait longer during periods of high load, or lower them if you prefer it to resume sooner.

Performance Mode

Several configuration options are available that can accelerate system performance while slightly reducing functionality. When certain features are not required, enabling **Performance Mode** can be an effective way to enhance speed.

To activate Performance Mode, modify the environment variable `PERFORMANCE_MODE`as outlined in Custom configuration and set the value to `PERFORMANCE_MODE=true` .

Functionality Impacted with Performance Mode Activated

Before enabling Performance Mode, please review the table below, which details all areas that will be impacted. This information will help you make an informed decision about whether the trade-offs in functionality are acceptable for your needs.

Functionality	Details
Amazon S3	Tags are not being retrieved automatically for all files which means they are not available on the response of `/api/file/{fileId}` and `/api/file/{scanId}/{startIndex}/{count}` APIs.
Core max file size validation	The WorkflowRules Job which updates cache with the max file size configured on each Core Instance will not run, and files which are bigger than this limit will be sent for scanning and fail

Rabbitmq configuration

One of the key ways to adjust MetaDefender Storage Security performance is by changing default configuration of Rabbitmq. The following are three environment variables that can help increase performance

`RABBITMQ_CONSUMER_MULTIPLIER`

Controls how many RabbitMQ consumers are created per standard (non-RPC) subscribe queue. The value is applied per priority tier with built-in multipliers:

- Low = N
- Medium = N × 3
- High = N × 6

When to increase:

When a service's standard queues show growing message backlogs and the service has spare CPU headroom. Each additional consumer adds a concurrent message-processing goroutine per priority channel.

Recommended values (16 CPU / 32 GB RAM VM): 1–3.

Valid range: 1–10. Default: 1.

`RABBITMQ_RPC_CONSUMER_MULTIPLIER`

Controls how many RabbitMQ consumers are created per RPC (request/reply) subscribe queue. RPC consumers handle synchronous-style calls from the API Gateway and other services, so they typically need higher concurrency than fire-and-forget consumers.

Valid range: 1–50. Default: 10.

Recommended values (16 CPU / 32 GB RAM VM): 10–20.

When to increase:

When RPC calls time out under load due to all consumers being busy, not because of slow downstream processing. Check RabbitMQ management for consumer utilization on RPC queues before raising this

`RABBITMQ_CONNECTION_CONSUMER_CONCURRENCY`

Sets **ConsumerDispatchConcurrency** on the RabbitMQ connection, which controls the maximum number of messages the client dispatches concurrently to consume callbacks on a single connection. This is a connection-level cap — it limits the total in-flight message processing across ALL channels and consumers on the connection.

Default: 50.

When to increase:

When the service has many queues/consumers (especially after raising ConsumerMultiplier or RpcConsumerMultiplier) and you observe that throughput plateaus while CPU is not used at full capacity. A low concurrency cap starves consumers even when there are messages ready.

Recommended values (16 CPU / 32 GB RAM VM): 50–100.

Configuring HTTPS

MetaDefender Storage Security can be configured to support HTTPS communication when accessing the Web UI and REST API.

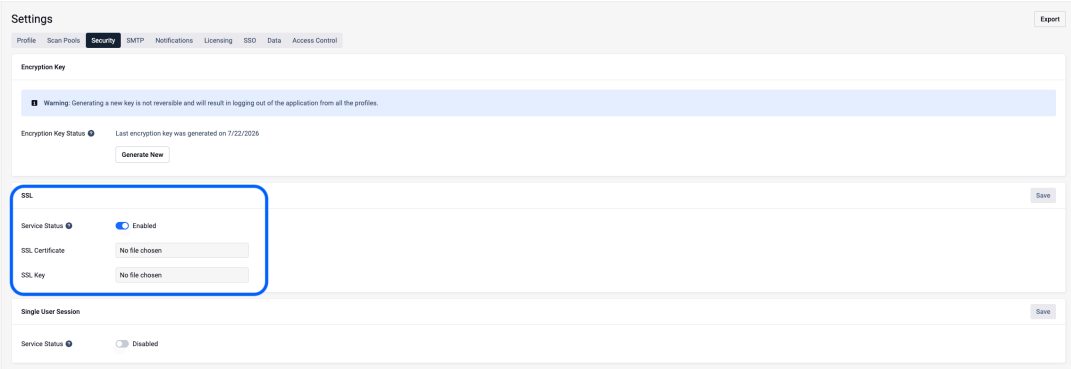
Which method applies to your deployment?

Deployment type	Method
Linux (Docker-based)	CLI — `mdss -u enable_https`
Windows (native services)	CLI — `mdss.ps1 -u enable_https`
Any (non-Kubernetes)	UI — Settings → Security tab
Kubernetes	See the Kubernetes deployment guide

Enabling HTTPS from the UI

Enabling HTTPS from the UI is now available for non Kubernetes deployments. On the Settings page, under the Security tab, you can enable HTTPS directly from the UI by entering the certificate file and the key file. The certificate must be a `.crt` file while the key must be a `.key` file.

After configuring HTTPS from UI, for the configuration to apply, restarting MDSS manually is required using the `mdss` command on Linux or the `mdss.ps1` script on Windows.




```
sudo mdss -c restart
```

```
.\mdss.ps1 -c restart
```

Enabling HTTPS from the Command Line

Prerequisites (both platforms)

- Certificate and private key must be in **PEM format** (`.crt` or `.pem` for the cert, `.key` for the key).
- If your certificate chain includes intermediate certificates, concatenate them into the `.crt` file (server cert first, then intermediates).
- Only one `.crt`/`.pem` and one `.key` file may be present in the certificate directory at a time.
- If no certificate is available, skip the certificate placement steps — the script will auto-generate a self-signed certificate (Linux only; Windows requires a certificate to be provided).

> **Info**
>
> **Self-signed certificates**: Browsers will show a trust warning for self-signed certificates. This is expected in lab or internal environments. To suppress the warning, add the certificate to your browser's or OS's trust store.

Enable HTTPS on Windows-based deployments

In order to setup HTTPS communication please follow these steps:

1. Place your certificate (`.crt` or `.pem`) and key (`.key`) files in: `C:\Program Files\OPSWAT\MetaDefender Storage Security\config\nginx\certificates` The files can have any name — the script renames them to `ssl.crt` and `ssl.key` automatically.
2. Navigate to the scripts folder: `C:\Program Files\OPSWAT\MetaDefender Storage Security\scripts`
3. Open a PowerShell prompt and run:

```
PS> .\mdss.ps1 -u enable_https
```

4. The script restarts the services automatically. Verify HTTPS is working by navigating to `https://<your-host>:443` (or the port configured in `WEB_PORT_SSL` in your .env file).
5. Verify that HTTPS is configured correctly by navigating with your browser.

Disable HTTPS on Windows-based deployments

For disabling HTTPS communication please follow these steps:

1. Navigate to the *scripts* folder (by default, in *C:\Program Files\OPSWAT\MetaDefender Storage Security\scripts)*
2. Run the following command in PowerShell:

```
PS> .\mdss.ps1 -u disable_https
```

3. The script patches the nginx configuration and restarts services automatically. The certificate files remain in `config\nginx\certificates` — they are not deleted.

Enable HTTPS on Unix-based deployments

In order to setup HTTPS communication please follow these steps:

1. Place your certificate (`.crt` or `.pem`) and key (`.key`) files in `/etc/mdss/webclient/` The files can have any name — the script renames them to `ssl.crt` and `ssl.key` automatically.
2. Run:

```
sudo mdss -u enable_https
```

3. The script reloads nginx automatically — **no MDSS restart is required**. Verify HTTPS is working by navigating to `https://<your-host>:443` (or the port configured in `WEB_PORT_SSL` in your .env file)
4. Verify that HTTPS is configured correctly by navigating with your browser.

Disable HTTPS on Unix-based deployments

> **Info**
>
> **Note:** Disabling HTTPS on Linux removes the certificate files from `/etc/mdss/webclient/`. Back up your certificates beforehand if needed.

For disabling HTTPS communication, run the following command:

```
sudo mdss -u disable_https
```

The script reloads nginx automatically — no restart required.

Port configuration

By default, MDSS listens on:

- **HTTP**: port `80`

- **HTTPS**: port 443

If ports 80 or 443 are unavailable, you can change them in your .env file:

```
WEB_PORT=8080
WEB_PORT_SSL=8443
```

Custom CA certificates

Custom certificates can be loaded in each MDSS container by placing them in the appropriate configuration directory depending on the host OS. If the directory does not exist, an empty one is created at startup. Any number of certificates can be placed in the directory and they will be loaded into MDSS.

Configuring custom certificates on Linux

Certificates are loaded from the following path:

```
/etc/mdss/ca_certificates/
```

Notes:

- All certificates should be in .crt format
- The full SSL certificate chain should be loaded in MDSS, especially if the certificate wasn't issued by a trusted CA
- Root CAs and intermediate CAs can be loaded using the same procedure

Configuring custom certificates on Windows

Certificates are loaded from the host certificate store. In order to add new CA certificates you'll need to do the following:

- Obtain the CA Certificate: Get the root CA certificate file (usually a .cer or .crt file) from your CA administrator.
- Open Certificate Manager:
- Press the Windows Key + R, type certlm.msc, and press Enter. (This opens the local machine certificate store)
- Import the Certificate:
- Expand the Trusted Root Certification Authorities folder.
- Right-click on Certificates.
- Select All Tasks -> Import.

- Follow the Certificate Import Wizard, browsing to the CA certificate file. Make sure to place the certificate in the Trusted Root Certification Authorities store

Enable Real-Time Processing (RTP)

Real-Time Processing is a scan type that processes files immediately upon upload.

This scan mode offers two file discovery methods:

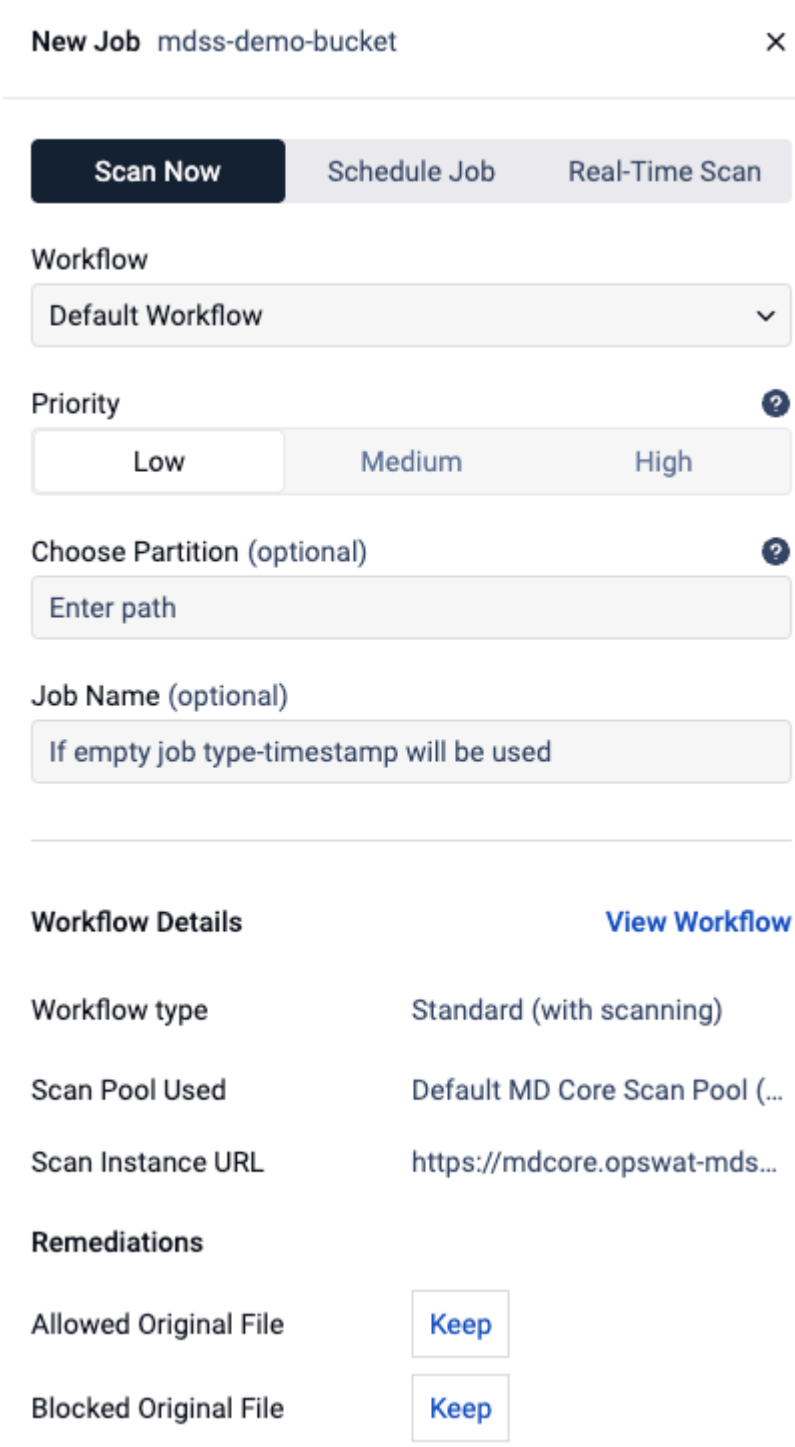
- Polling
- Event-Based

This feature is disabled by default. To enable it:

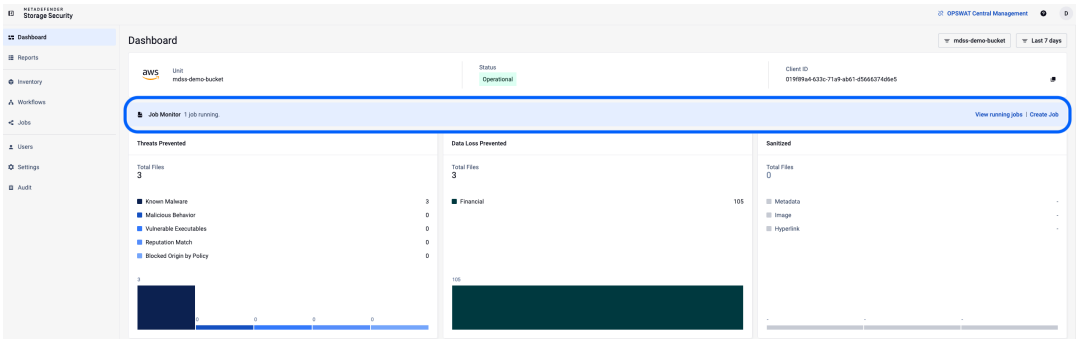
1. In the MetaDefender Storage Security web interface, navigate to "**Storage Units**."
2. Select the desired storage unit and click the "More Options" button (represented by three dots) to choose "**Add New Scan**."

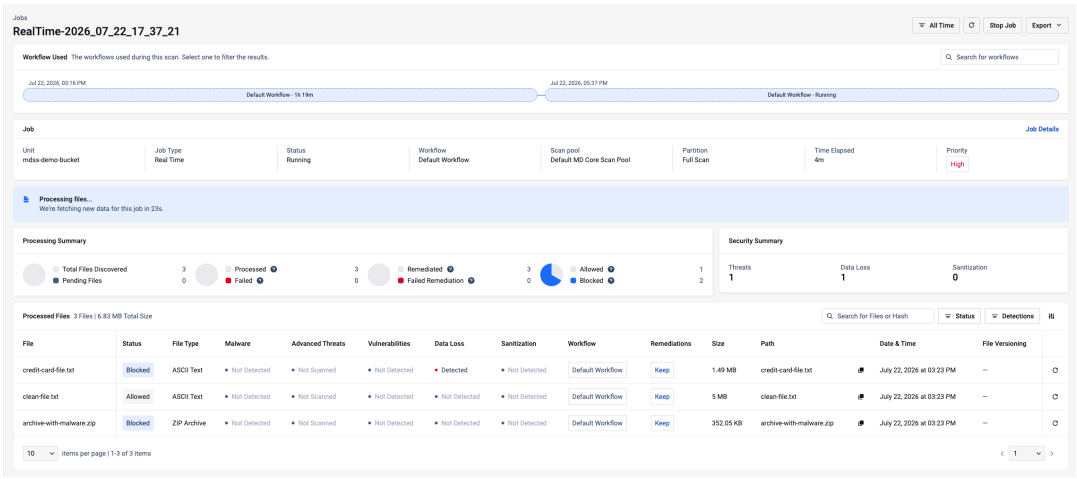
3. Select "Real-Time Processing" and choose the file discovery method (Polling or Event-Based, if the storage supports event-based real-time processing webhook invocation).

> **Info**
>
> Pick files modified since (Optional) field is a date/time picker that defines a cutoff point for file discovery; by default, only new files are picked up, but selecting a date causes the scan to also include files that were modified on or after that date and time.
>
> The field is **disabled** in the following cases:
>
> - `DISCOVERY_SERVICE_<PROTOCOL>_RTP_HANDLING = 1` (for SMB, SFTP, NFS or FTP)
> - **Event-based RTP**: event-based processing handles all incoming events regardless of file modification date, so this filter is not applicable.



To monitor active processes, go to the “Dashboard”, select your storage unit and click the “Active Process” card. This will open the scan details page, providing an overview of scan settings, discovery, and options to stop the scan, view, export, or clear the scan report from the audit log.





> **Info**
>
> Starting a second RTP scan on the same storage partition will update the existing scan and not start one more. Each storage supports multiple RTP scans, but only one RTP scan for each defined partition.

Polling handling

The **Polling file discovery method** retrieves and processes new or modified files directly from the storage.

Key characteristics include:

- Each identified file is processed independently.
- Files are processed only once, preventing redundant scans.
- The storage is checked for updates **every 10 seconds**, or immediately after a complete storage discovery cycle.

> **Note:**
>
> Using the **Polling** method significantly increases the number of requests to the storage system, ensuring timely detection of file changes.

Special considerations for Dell Isilon / SMB Compatible Storage

Dell Isillon / Smb Compatible

Real-time processing for Dell Isilon and SMB-compatible storage units employs a distinct approach compared to other storage types.

The behavior of this processing mode is governed by environment variables.

Refer to the the custom configuration page for detailed information on these settings.

Event-based handling

> **Event-Based File Discovery**
>
> Event-based real-time processing triggers scans immediately upon file creation or modification notifications.
>
> This method is supported for the following storage units: **Amazon S3**, **S3 Compatible**, **Azure Blob**, **Alibaba Cloud**, **Google Cloud**, **Box**, **SMB Compatible**, **NFS**, **SFTP, FTP**, **SharePoint Online** and **NetApp ONTAP**.

Generic Webhook Endpoint

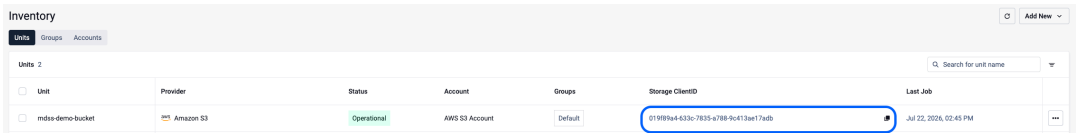
MetaDefender Storage Security provides a generic webhook endpoint **http[s]://{baseurl}/api/webhook/realtime** for integration with serverless functions from AWS, Azure, Alibaba Cloud, and Google Cloud Platform.

> **Important Note for BOX Integration**
>
> For Box, the API endpoint is `https://{baseurl}/api/webhook/realtime/public/{storageClientId}`. The generic webhook endpoint is **NOT** compatible with BOX. Refer to the Event-based handling for Box documentation for specific instructions.

Integrating Cloud Provider Event Notifications

To integrate event notifications from AWS, Azure, Alibaba Cloud, and Google Cloud Platform with MetaDefender Storage Security's real-time processing, the following parameters must be included as request headers in the event payload:

- `storageclientid` - Obtain this value from the Dashboard, once you select the Storage Unit desired



- `apikey`- Generate an API key for authentication in MetaDefender Storage Security under “Settings” -> “Users” -> “User (More Options).” Refer to the “Generate an API Key” documentation for detailed instructions.
- `apiendpoint`- Use the generic real-time webhook endpoint: `http(s)://{baseurl}/api/webhook/realtime`

For examples of the request format, please visit this page.

For detailed configuration instructions, please consult the Event-Based Real-Time Cloud Functions Examples documentation.

Event-Based request format

Overview

This document describes the real-time webhook API endpoint that external integrators can use to notify the system about file events. The endpoint accepts different payload formats depending on the storage type.

Endpoint Information

URL: `https://{baseurl}/api/webhook/realtime`

Method: POST

Content-Type: application/json

> **Important note for Box integration**
>
> For Box, the API endpoint is **https://{baseurl}/api/webhook/realtime/public/{storageClientId}.** Please refer to this article for specific instructions.

Request Format (with examples)

The request body differs based on storage type. Below are the specifications for each supported storage:

Amazon S3 and S3 Compatible

```
{
    "metadata": "{\"s3\": { \"object\": {\"key\": \"{Object Path}\"
}}}",
    "storageClientId": "{Storage Client Id}"
}
```

```
{
    "storageClientId": "0c5454e3-d576-44c5-8ce4-cdc078011d0b",
    "metadata": "{\"s3\": { \"object\": {\"key\": \"test-file.txt\"
}}}"
}
```

```
{
    "storageClientId": "0c5454e3-d576-44c5-8ce4-cdc078011d0b",
    "metadata": "{\"s3\": { \"object\": {\"key\":
\"folder1/folder2/test-file.txt\" }}}"
}
```

Alibaba Cloud

```
{
    "metadata": "{\"oss\": {\"object\": {\"key\": \"{Object
Path}\"}}}",
    "storageClientId": "{Storage Client ID}"
}
```

```
{
    "metadata": "{\"oss\": {\"object\": {\"key\": \"test-
file.pdf\"}}}",
    "storageClientId": "0c5454e3-d576-44c5-8ce4-cdc078011d0b"
}
```

```
{
    "metadata": "{\"oss\": {\"object\": {\"key\":
\"folder1/folder2/test-file.pdf\"}}}",
    "storageClientId": "0c5454e3-d576-44c5-8ce4-cdc078011d0b"
}
```

Google Cloud, OracleSdk, Azure Blob, SMB Compatible, NFS, SFTP, FTP and NetApp ONTAP

```
{
    "metadata": "{\"Name\": \"{Object Path}\" }",
    "storageClientId": \"{Storage Client ID}\"
}
```

```
{
    "metadata": "{\"Name\": \"test-file.exe\" }",
    "storageClientId": "0c5454e3-d576-44c5-8ce4-cdc078011d0b"
}
```

```
{
    "metadata": "{\"Name\": \"folder1/folder2/test-file.exe\" }",
    "storageClientId": \"0c5454e3-d576-44c5-8ce4-cdc078011d0b\"
}
```

Scanning with a partition

If you have one or more partition Event-Based scans active, a new parameter called `scanId` is required with every request and the format will become:

```
{
    "metadata": "{Metadata format specific for every storage}",
    "storageClientId": \"{Storage Client ID}\",
    "scanId": "Scan Id for the scan with partition"
}
```

Response Formats

Success

When a webhook is successfully processed, the system returns:

```
{
    "correlationId": "67ea85a36f2f5732a82834d0"
}
```

Field	Description
correlationId	A unique identifier that references the submitted file in our database. You can use this ID for tracking the file's processing status or for future API calls related to this file.

Error

When an error occurs during processing, the system returns:

```
{
    "responseKey": "REST_API_MSG_FAILED_STORAGE_RTP_NOT_ENABLED",
    "responseMessage": "Real-Time Process is not enabled."
}
```

Field	Description
responseKey	Machine-readable error code that identifies the specific error condition.
responseMessage	Human-readable explanation of the error.

Common error responses

Response Message	Description	Recommended Action
The storage could not be found	The specified storage client ID does not exist in the system.	Verify the storageClientId is correct and the storage has been properly configured in the system.
Real-Time Process is not enabled.	Real-time processing has not been activated for this storage client.	Enable real-time processing for the storage client in your account settings.
Real-Time Process is enabled, but it is not set to Event Based.	The storage is configured for real-time processing, but is using polling rather than event-based processing.	Stop the current RTP scan and start another one using Event-Based

Event-Based Real-Time Cloud Functions Examples

Google Cloud Function Setup

1. Configure the Cloud Run with the `google.cloud.storage.object.v1.finalizedtrigger` to process newly added objects.
2. Python Function Example:

```
import functions_framework
import json
import requests
import os

@functions_framework.cloud_event
def hello_gcs(cloud_event):
    try:
        name = cloud_event.data['protoPayload']['request']
['insertObjectSpec']['resource']['name']
    except KeyError as e:
        print(f"Missing key in event data: {e}")
        return

    request_body = {
        'storageClientId': os.getenv('STORAGECLIENTID'),
        'metadata': json.dumps({'name': name})
    }

    requests.post(
        os.getenv('APIENDPOINT'),
        headers={'ApiKey': os.getenv('APIKEY')},
        json=request_body
    )
```

3. Requirements.txt example:

```
functions-framework==3.*
requests
```

Alibaba Cloud Function Setup

1. Follow the official Alibaba Cloud documentation to create a compute function with an OSS trigger: https://www.alibabacloud.com/help/en/function-compute/latest/configure-an-oss-trigger
2. Specify the bucket to monitor and subscribe to the `oss:ObjectCreated:*` event.
3. Python Function Example:

```
import oss2, json, os
import requests

def handler(event, context):
    for eventRecord in json.loads(event)['events']:
        requests.post(os.getenv('APIENDPOINT', ""), headers=
{'ApiKey':os.getenv('APIKEY', "")}, json = {'metadata':
json.dumps(eventRecord), 'storageClientId':
os.getenv('STORAGECLIENTID', "") })
```

Wasabi Function Setup

1. Follow the official Wasabi documentation to create an event notification: https://docs.wasabi.com/v1/docs/event-notifications-bucket
2. Establish a connection with a service capable of sending requests to MetaDefender Storage Security (MDSS).
3. The Wasabi documentation example uses AWS SNS, which can be integrated with AWS Lambda (see Amazon S3 Lambda Function Setup: How do I configure Event Notifications on my Wasabi bucket using AWS SNS?

S3 Compatible function setup

- Event-based real-time processing configuration varies for different S3-compatible services.
- Most S3-compatible services offer event notification similar to Wasabi.
- The service must send a request to the MDSS endpoint: `http(s)://{baseurl}/api/webhook/realtime` with the appropriate request body:

```
{
    "storageClientId": [Storage Client Id],
    "metadata": "{'s3': { 'object': {'key': [Object Path] }}}"
}
```

Event-based handling for Box

MetaDefender Storage Security has a generic webhook endpoint that can be invoked through the Box Webhooks. These monitor Box content for events and notify you whenever an event occurs. There are two types of Box Webhooks: V1 and V2, but only V2 is supported by MetaDefender Storage Security

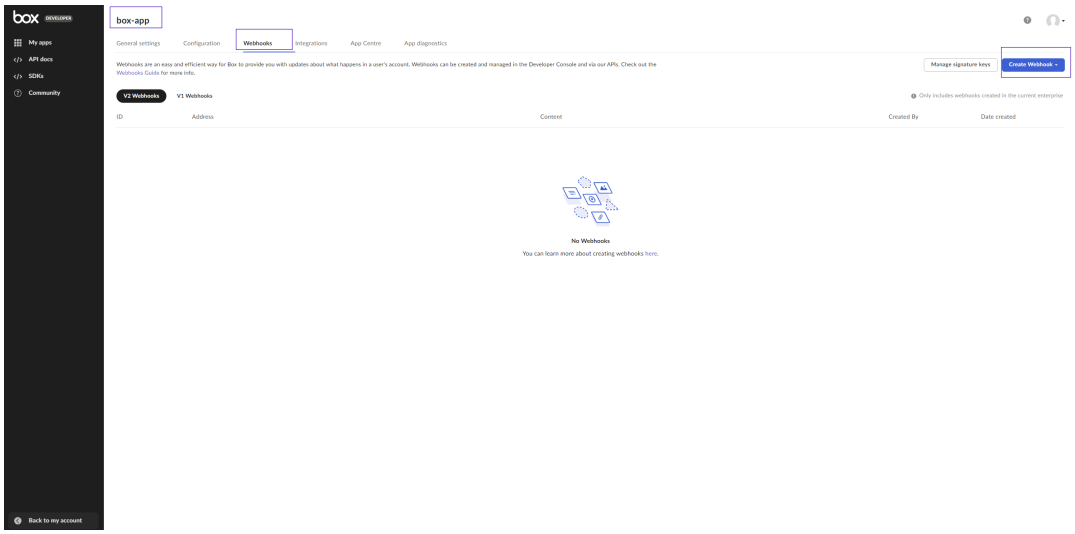
How to create Box Webhooks

1. Log in to Box and then go to Developer Console
2. If you do not have an existing app, create a new one (Please check How can I generate a public/private key pair)

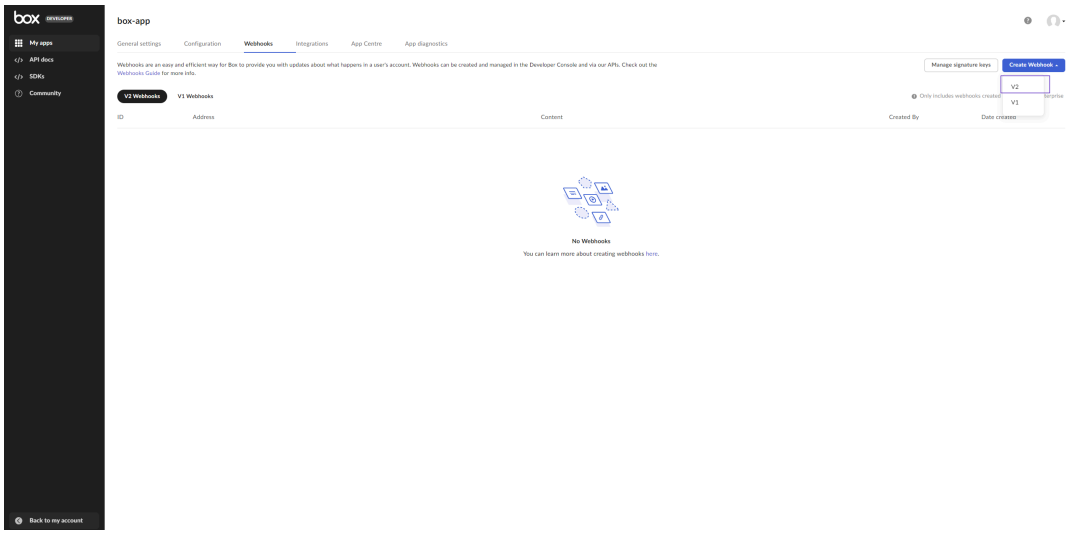
> **WARNING**
>
> Box V2 Webhooks can only be created when the scope Manage Webhooks is selected and the application has been authorized

3. Navigate to your application

4. Select the **Webhooks** tab
5. Click the **Create webhook** button

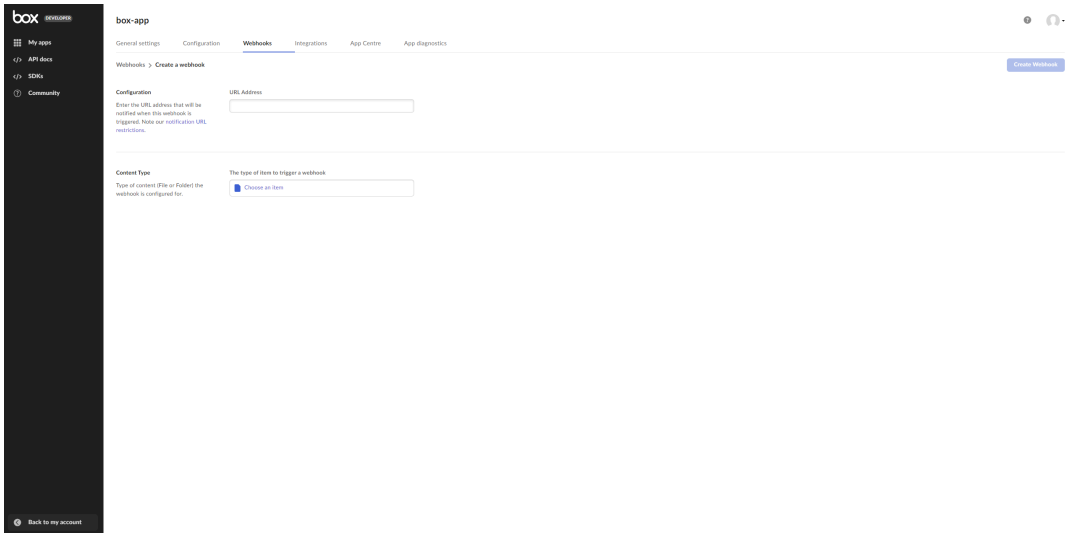


6. Select **V2** from the drop-down list



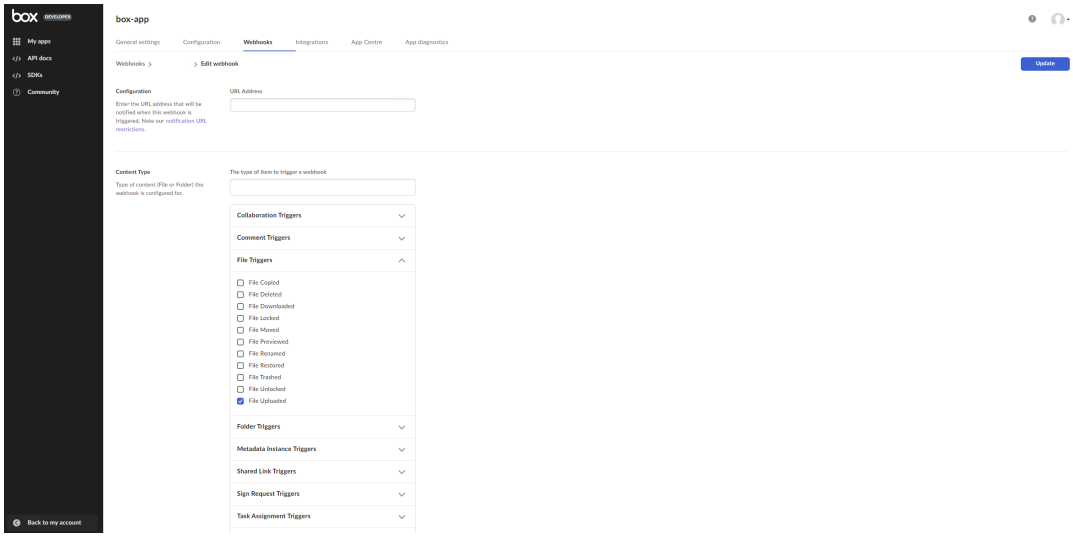
7. Fill in the form:
    1. Enter the **URL address** that will be notified when the webhook is triggered (the address where MetaDefender Storage Security is hosted)

> **WARNING**
>
> URL Address must have a secure URL (HTTPS)

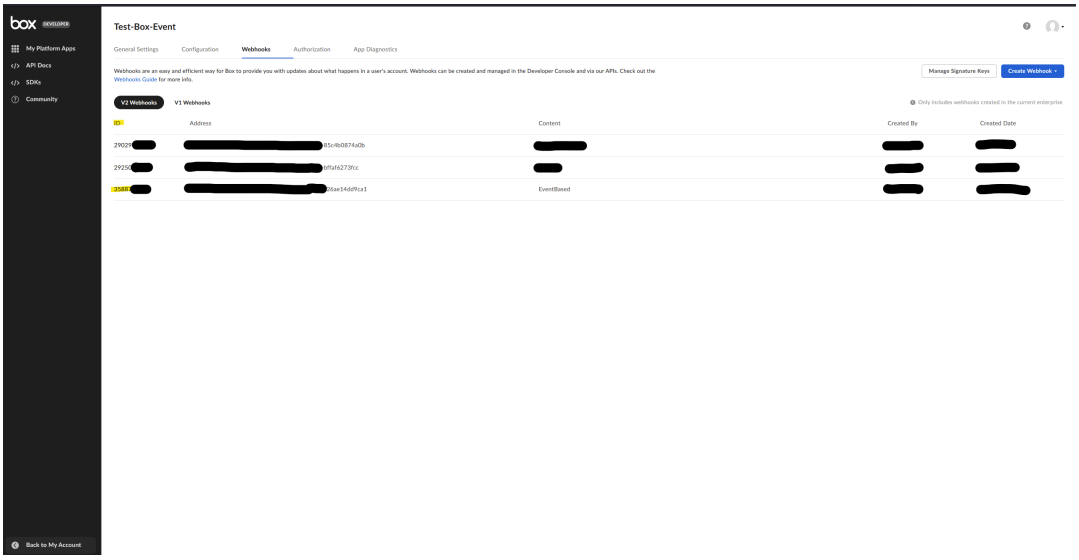


b. Select the folder that you have set in MetaDefender Storage Security as the element that triggers the webhook

c. Choose **File Uploaded** as the trigger for the selected folder



8. Click the Create webhook button to save your changes
9. **Copy the ID** of the generated webhook to enter into MDSS



10. Enter the copied webhook ID into the edit storage form for your Box storage

Event-based handling for SharePoint Online

MetaDefender Storage Security supports event-based handling for SharePoint Online, enabling real-time scanning of content as it is added.

Unlike other storage providers, **MDSS automates the setup of the Microsoft Graph subscriptions** needed for monitoring SharePoint events. This makes the configuration process simpler and faster for SharePoint Online users.

Advantages

- MDSS automatically creates, renews, and manages all necessary Microsoft Graph API subscriptions. **No manual intervention is required for this critical infrastructure**
- Get real-time scanning up and running faster, without the complexities of manual Graph API configuration
- Files are scanned immediately upon upload or modification in SharePoint Online, providing continuous security

How it works

MDSS leverages Microsoft Graph API webhooks to receive notifications from SharePoint Online whenever content is added or modified. MDSS handles the entire lifecycle of these webhook subscriptions on your behalf. For this to work correctly, your MDSS instance must be reachable from the internet to receive these notifications from Microsoft.

Prerequisites

Before MDSS can automatically configure event-based handling, your environment must meet the following crucial prerequisites:

1. MDSS Hosted and Accessible via HTTPS
    - SharePoint Online sends event notifications (webhooks) to your MDSS instance. These notifications require a secure HTTPS connection to a trusted endpoint
    - Your MDSS instance must be served over HTTPS
    - The machine running MDSS needs a valid SSL certificate from a trusted Certificate Authority. While self-signed certificates can technically work, they are **strongly discouraged** as they require complex trust configurations within your SharePoint environment and can lead to notification failures if not managed perfectly
2. Publicly Accessible MDSS Port
    - Microsoft Graph API needs to send event notifications directly from Microsoft's cloud services to your MDSS instance. If MDSS is not publicly accessible, these critical notifications cannot be delivered
    - The HTTPS port used by MDSS (default is 443) must be open and reachable from the public internet
    - Configure your firewall, router, load balancers, and any other network security infrastructure to allow incoming HTTPS traffic on this port, directing it to the MDSS host machine
3. Configured SharePoint Online Connection in MDSS
    - MDSS needs to authenticate with your SharePoint Online environment to register the webhooks for event notifications and access file content for scanning
    - Your SharePoint Online storage must be successfully added and properly configured within MDSS.
    - Make sure that MDSS has the necessary permissions to access your SharePoint site(s). These permissions are typically granted via OAuth during the initial storage addition process and must include the ability to manage Graph API subscriptions for the targeted resources

> **Warning**
>
> The document library's display name must match its name in the web address (URL). For example, if the URL is `.../sites/[SiteName]/[LibraryName]/`, the name should also be **[LibraryName]**. If they differ, SharePoint event-based handling will not work, and MDSS won't process file events for that library.

Once these prerequisites are met, MDSS will automatically handle the setup and ongoing management of event-based scanning for your configured SharePoint Online storage

Unsupported SharePoint Content Types

Certain SharePoint content types fall outside the scope of items protected by our solution. Administrators should be aware of the following exclusions when reviewing coverage of their SharePoint environments.

Form Templates Library

The **Form Templates** library that appears under a SharePoint site's contents is a hidden system library automatically provisioned by SharePoint on every site. Despite its visibility in the site contents view, it is not a standard document library and is not backed by a Drive resource in Microsoft Graph. As a result, this library is **not protected** by our solution.

Lists

SharePoint items of type **List** (for example, custom lists, task lists, and contact lists) are not backed by a Drive resource in Microsoft Graph and are therefore **not protected** by our solution.

Site Pages and Other Page Libraries

Content stored in libraries of type **Page Library** (such as the default *Site Pages* library) is **not protected** by our solution. These libraries host SharePoint pages rather than user documents and are managed through SharePoint's page infrastructure rather than as standard document storage.

Content Type	Microsoft Graph Drive	Protected
Document Library	Yes	Yes
Form Templates (system library)	No	No
List	No	No
Page Library (e.g., Site Pages)	No	No

How Microsoft delivers the file-changed notifications

Purpose

This page explains how Microsoft delivers change notifications to MetaDefender Storage Security (MDSS) when Event-Based Real-Time Protection (RTP) is enabled for a SharePoint

Cloud site, and what timing to expect.

It answers the most common question we receive:

> A user made several edits to a document in quick succession, and each one was saved. Why did MDSS receive only one notification instead of one per edit?

Short answer: this is Microsoft's documented behaviour, not a loss of coverage. Microsoft deliberately groups changes together, and a notification is only a signal that *something* changed — MDSS then queries Microsoft for the full list of changes and scans the file in its current state. No change is skipped.

The remainder of this page provides the detail, with references to the official Microsoft documentation for every statement.

---

1. How MDSS subscribes

When you enable Event-Based RTP on a SharePoint Cloud site, MDSS creates one Microsoft Graph subscription **per document library** in that site.

Each subscription is created against the Microsoft Graph `list` resource:

```
POST https://graph.microsoft.com/v1.0/subscriptions

{
  "changeType": "updated",
  "notificationUrl": "https://<your-mdss-
host>/api/webhook/realtime/graph/...",
  "resource": "sites/{siteId}/lists/{listId}",
  "expirationDateTime": "<29 days from creation>",
  "clientState": "<secret generated by MDSS>"
}
```

This is the resource path Microsoft documents for SharePoint document libraries — see the *Supported resources* table in Set up notifications for changes in resource data, which lists:

> **list** under a SharePoint **site** — Changes to content within the *list*: `/sites/{site-id}/lists/{list-id}`

MDSS renews each subscription automatically before it expires. Microsoft caps SharePoint `list` subscriptions at 42,300 minutes (just under 30 days), per the *Subscription lifetime* table on the same page.

---

2. How Microsoft delivers the notifications

Three separate Microsoft mechanisms sit between a user's edit and the notification MDSS receives. Each one groups changes together.

Layer 1 — Office for the web saves periodically, not per keystroke

When a document is edited in the browser, the "Saved" indicator means the change was committed to the Office co-authoring session. The file itself is written back to SharePoint on a timer.

From Co-author using Microsoft 365 for the web, section *Word for the web co-authoring behavior*:

> **Auto-save frequency**: Every 30 seconds if document is updated. In other words, if users are actively editing a document, PutFile is called every 30 seconds. But if users stop editing for a period of time, Word for the web doesn't call PutFile until document changes are made again.

The same page's Table 1 documents all three applications:

Application	Auto-save frequency
Word for the web	Every 30 seconds if document is updated
PowerPoint for the web	Every 60 seconds if document is updated
Excel for the web	Every two minutes

Consequence: several edits made within the same interval result in **one** file write to SharePoint, not one per edit.

Layer 2 — SharePoint batches notifications and sends them once a minute

SharePoint does not notify subscribers at the moment a change occurs. From SharePoint webhooks sample reference implementation, section *Grab the changes your service needs to act upon*:

> SharePoint does not call your service in real-time: when a change happens on a list that has a webhook, SharePoint queues a webhook callout. Once each minute, this queue is read and the appropriate service endpoints are called. This batching of

> requests is important. For example, if a bulk upload of 1000 records occurred at once, batching prevents SharePoint from calling your endpoint 1000 times.

And from Overview of SharePoint webhooks, section *Receiving notifications*:

> Multiple notifications to your application may be batched together into a single request if multiple changes occurred in the resource within the same time period.

Layer 3 — The notification does not contain the changes

This is the most important point for understanding why grouping is safe. From Overview of SharePoint webhooks, section *Receiving notifications*:

> The notification doesn't include any information about the changes that triggered it. Your application is expected to use the GetChanges API on the list to query the collection of changes from the change log and store the change token value for any subsequent calls when the application is notified.

A notification is a signal, not a payload. It identifies the *document library* that changed — never the file.

A notification looks like this (identifiers replaced with placeholders):

```
{
  "value": [
    {
      "subscriptionId": "00000000-0000-0000-0000-000000000000",
      "clientState": "<secret generated by MDSS>",
      "resource": "sites/{tenant}.sharepoint.com,{siteId},
{webId}/lists/{listId}",
      "tenantId": "00000000-0000-0000-0000-000000000000",
      "resourceData": { "@odata.type": "#Microsoft.Graph.ListItem" },
      "subscriptionExpirationDateTime": "2026-09-08T11:45:26Z",
      "changeType": "updated"
    }
  ]
}
```

Note that `resourceData` contains only a type marker — there is no file name, file ID, or change detail.

---

3. What MDSS does when a notification arrives

1. Receives the notification and identifies which document library it refers to.

2. Calls Microsoft Graph's delta query for that library, resuming from the point the previous query finished.
3. Receives the complete list of everything that changed since then — however many changes accumulated.
4. Submits each changed file for scanning.

Because step 2 always resumes from where the previous query stopped, **grouping cannot cause a change to be skipped**. If Microsoft groups ten edits into one notification, the delta query returns all ten. This is the pattern Microsoft prescribes in the documentation quoted in Layer 3 above.

It also means a file is scanned in its **current** state rather than once per intermediate save — which is the desired outcome, since intermediate drafts are superseded before a scan of them would finish.

---

4. Expected timing

Published Microsoft figures for a SharePoint document library:

Stage	Documented timing	Source
Browser edit written to SharePoint	Every 30s while actively editing (Word)	Co-authoring behaviour
SharePoint webhook queue drained	Once each minute	Reference implementation
Graph notification latency (`list`)	Average under 1 minute, maximum 6 hours	Latency table

The 6-hour figure is Microsoft's stated maximum for the `list` resource and represents the worst case under service degradation. Typical delivery is under a minute.

Observed example

In a customer environment, a single document was edited continuously in the browser for roughly 13 minutes. MDSS received 9 notifications for that document library. The shortest interval between any two notifications was **36 seconds**.

That matches the documented behaviour precisely: a 30-second save cadence feeding a queue drained once a minute cannot produce notifications closer together than roughly half a minute, regardless of how many keystrokes occur.

---

5. Frequently asked questions

A user saved five times in five seconds but MDSS received one notification. Was anything missed? No. Five saves within five seconds produce approximately one file write to SharePoint (Layer 1), and any changes within the same batching window are grouped into one notification (Layer 2). The delta query returns the file in its latest state, so it is scanned.

Can MDSS receive a notification per individual edit? No. This is controlled entirely by Microsoft and is not configurable. The notification carries no file-level information, so a per-edit notification would contain nothing to distinguish it.

What happens if hundreds of files change at once — for example a bulk upload? Microsoft sends a small number of notifications rather than one per file, exactly as described in the 1,000-record example quoted in Layer 2. The delta query returns all the changed files, and MDSS scans each one.

What is the maximum delay before a new or modified file is scanned? Under normal conditions, typically under a minute plus scan time. Microsoft's documented maximum notification latency for a SharePoint list is 6 hours — see the Latency table.

Does anything need to be configured to make notifications arrive faster? No. The intervals are Microsoft service behaviour and cannot be changed by MDSS or by tenant configuration.

Is Event-Based RTP the right choice for files edited continuously in the browser? Yes. Event-Based RTP scans the file as it reaches its saved state in SharePoint. For workloads where you want a guaranteed sweep independent of notification delivery, combine it with a scheduled on-demand scan.

6. Microsoft reference documentation

Topic	Link
Change notifications overview, supported resources, subscription lifetime, latency SLA	https://learn.microsoft.com/en-us/graph/change-notifications-overview
Receiving change notifications through webhooks (delivery, retries, clientState)	https://learn.microsoft.com/en-us/graph/change-notifications-delivery-webhooks
Overview of SharePoint webhooks (batching, notification contents, error handling)	https://learn.microsoft.com/en-us/sharepoint/dev/apis/webhooks/overview-sharepoint-webhooks
SharePoint list webhooks (supported list event types)	https://learn.microsoft.com/en-us/sharepoint/dev/apis/webhooks/lists/overview-sharepoint-list-webhooks
SharePoint webhooks reference implementation (queue drained once a minute, batching rationale)	https://learn.microsoft.com/en-us/sharepoint/dev/apis/webhooks/webhooks-reference-implementation
Co-authoring in Microsoft 365 for the web (auto-save frequency per application)	https://learn.microsoft.com/en-us/microsoft-365/cloud-storage-partner-program/online/scenarios/coauth
Change tracking / delta query overview	https://learn.microsoft.com/en-us/graph/delta-query-overview

Event-Based Real-Time handling for AWS

AWS Lambda Function with S3 Trigger Setup Guide

Before proceeding with the setup, ensure the following requirements are met:

1. IAM User Permissions

- Your IAM user must have the necessary permissions to:
  - Create Lambda functions
  - Assign IAM roles
  - Configure S3 triggers
  - Access the target S3 buckets

2. Account-Level Verification

- Confirm there are no account-level naming restrictions that would prevent your chosen Lambda function name
- Verify your AWS account has sufficient permissions and service quotas to create new Lambda functions in the desired region
- Ensure you have access to the target AWS region where the Lambda function will be deployed

3. S3 Bucket Configuration

- Verify that S3 bucket policies are configured to allow access from the Lambda function's execution role
- Required S3 permissions may include:
  - `s3:GetObject` - to read objects from the bucket
  - `s3:PutObject` - to write objects to the bucket (if applicable)
  - `s3:DeleteObject` - to delete objects from the bucket (if applicable)

4. IAM Execution Role

- Ensure you have a pre-configured IAM role with:
  - Lambda execution permissions
  - S3 access permissions for your target bucket(s)
  - CloudWatch Logs permissions for function monitoring

Step 1: Creating the Lambda Function

1.1 Navigate to Lambda Service

1. Open the AWS Management Console
2. Navigate to the **Lambda** service

1.2 Initialize Function Creation

1. Click **"Create function"**
2. Select **"Author from scratch"**

1.3 Configure Basic Settings

1. **Function name**: Enter a descriptive name for your Lambda function

- Example: `MetaDefenderStorageSecurityProcessor`
- Ensure the name complies with AWS naming conventions and any account-specific policies

2. **Runtime**: Select **Python** (choose the latest compatible version)

1.4 Configure Permissions

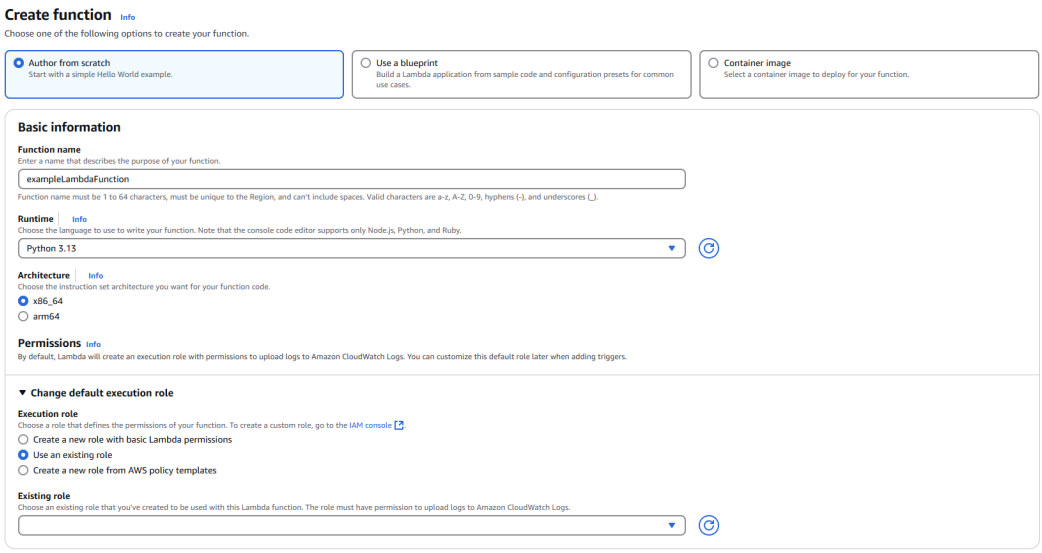
1. Under **"Change default execution role"**, select **"Use an existing role"**
2. From the **"Existing role"** dropdown, choose your pre-configured IAM role
3. **Verify role permissions**:
   - Navigate to the IAM console and review the selected role
   - Confirm **Permission policies** include necessary access to S3, CloudWatch Logs, and other required services
   - Verify **Trust relationships** allow the Lambda service (`lambda.amazonaws.com`) to assume the role

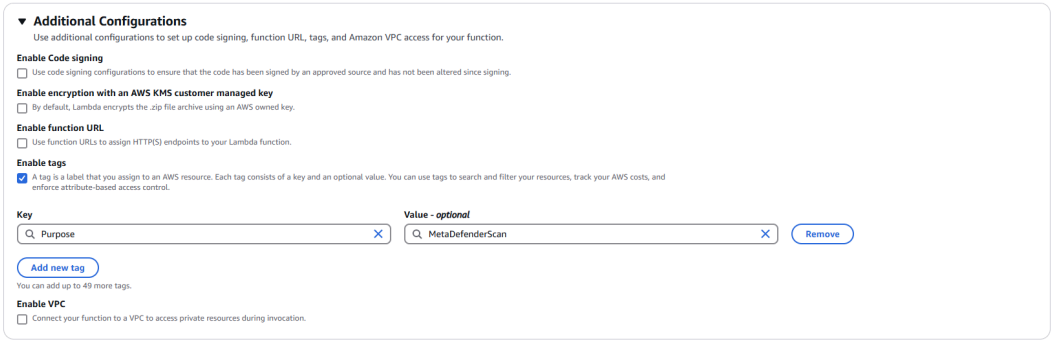
1.5 Configure Advanced Settings (Optional but Recommended)

1. Expand **"Advanced configuration"**
2. Enable **"Tags"**
3. Add relevant tags for resource organization:
   - **Key**: `Purpose` | **Value**: `MetaDefenderScan`
   - **Key**: `Environment` | **Value**: `Production/Development`
   - **Key**: `Owner` | **Value**: `[Your Team/Department]`

1.6 Create the Function

1. Click **"Create function"**
2. Wait for the function to be successfully created





Step 2: Adding S3 Trigger

2.1 Add Trigger Configuration

1. In your newly created Lambda function, click **“Add trigger”**
2. Select **“S3”** as the trigger source

2.2 Configure S3 Trigger Settings

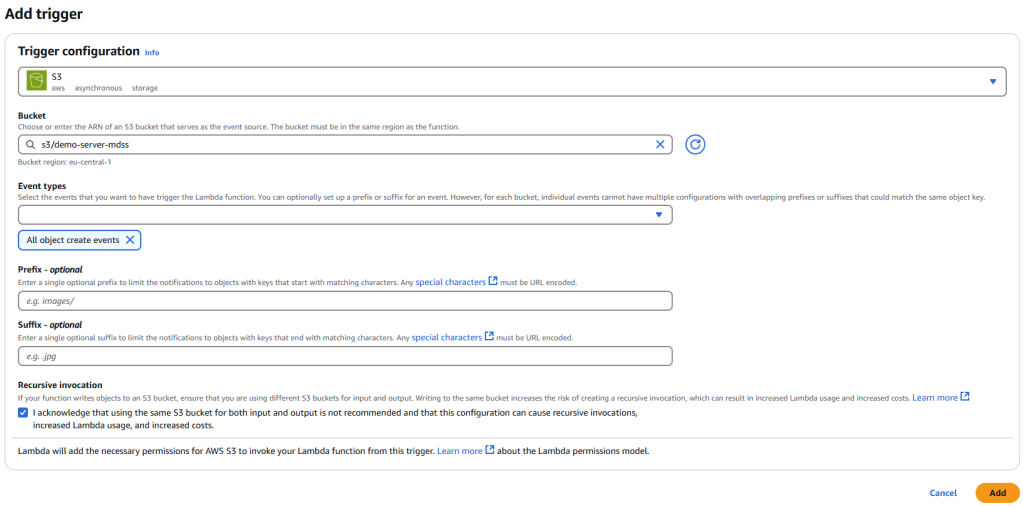
1. **Bucket**: Select your target S3 bucket from the dropdown menu
2. **Event types**: Choose the appropriate event type
   - Default: **“All object create events”**
   - Alternative options: Object create, delete, or restore events based on your requirements
3. **Prefix** (Optional): Specify a prefix to filter objects by path
   - Example: `uploads/` to only trigger on objects in the uploads folder
4. **Suffix** (Optional): Specify a suffix to filter objects by file extension

- Example: `.pdf` to only trigger on PDF files

5. **Recursive invocation**: Check this option to acknowledge potential recursive invocations

2.3 Finalize Trigger Setup

1. Review your trigger configuration
2. Click **“Add”** to create the S3 trigger



3.1 Navigate to Code Section

1. In your Lambda function console, navigate to the **“Code”** tab
2. Replace the default code with the following implementation:

```
import os
import json
import urllib.request
from urllib.parse import unquote

def lambda_handler(event, context):
    for eventRecord in event['Records']:
        eventRecord['s3']['object']['key'] = unquote(eventRecord['s3']
['object']['key'].replace("+", " "))

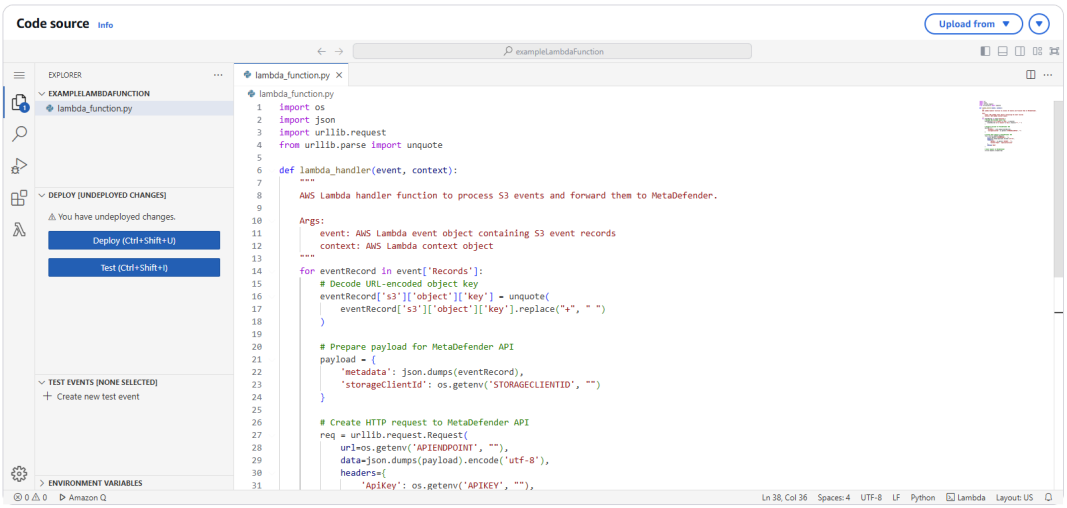
        payload = {
            'metadata': json.dumps(eventRecord),
            'storageClientId': os.getenv('STORAGECLIENTID', "")
        }

        req = urllib.request.Request(
            url=os.getenv('APIENDPOINT', ""),
            data=json.dumps(payload).encode('utf-8'),
            headers={
                'ApiKey': os.getenv('APIKEY', ""),
                'Content-Type': 'application/json'
            },
            method='POST'
        )

        urllib.request.urlopen(req)
```

3.2 Deploy the Code

1. Click **“Deploy”** to save and deploy your function code



Request Format (with examples)

The request body differs based on storage type. Below are the specifications for each supported storage:

Amazon S3 and S3 Compatible

```
{
    "storageClientId": '{Storage Client Id}',
    "metadata": "{'s3': { 'object': {'key': '{Object Path}' }}}"
}
```

```
{
    "storageClientId": "0c5454e3-d576-44c5-8ce4-cdc078011d0b",
    "metadata": "{'s3': { 'object': {'key': 'test-file.txt' }}}"
}
```

```
{
    "storageClientId": "0c5454e3-d576-44c5-8ce4-cdc078011d0b",
    "metadata": "{'s3': { 'object': {'key': 'folder1/folder2/test-
file.txt' }}}"
}
```

Response Formats

Success

When a webhook is successfully processed, the system returns:

```
{
    "correlationId": "67ea85a36f2f5732a82834d0"
}
```

Field	Description
correlationId	A unique identifier that references the submitted file in our database. You can use this ID for tracking the file's processing status or for future API calls related to this file.

Error

When an error occurs during processing, the system returns:

```
{
    "responseKey": "REST_API_MSG_FAILED_STORAGE_RTP_NOT_ENABLED",
    "responseMessage": "Real-Time Process is not enabled."
}
```

Field	Description
responseKey	Machine-readable error code that identifies the specific error condition.
responseMessage	Human-readable explanation of the error.

Common error responses

Response Message	Description	Recommended Action
The storage could not be found	The specified storage client ID does not exist in the system.	Verify the storageClientId is correct and the storage has been properly configured in the system.
Real-Time Process is not enabled.	Real-time processing has not been activated for this storage client.	Enable real-time processing for the storage client in your account settings.
Real-Time Process is enabled, but it is not set to Event Based.	The storage is configured for real-time processing, but is using polling rather than event-based processing.	Stop the current RTP scan and start another one using Event-Based

Step 4: Configuring Environment Variables

4.1 Navigate to Configuration

1. In your Lambda function console, click on the **“Configuration”** tab
2. Select **“Environment variables”** from the left sidebar

4.2 Add Required Environment Variables

Click **“Edit”** and add the following environment variables:

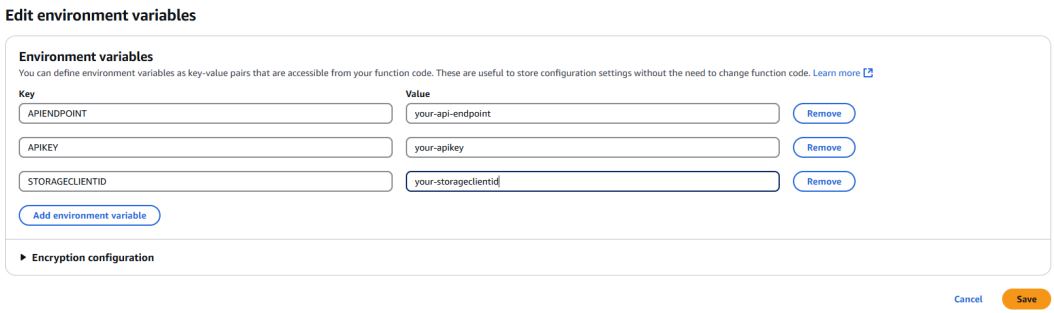
1. **APIENDPOINT**
   - **Key**: `APIENDPOINT`
   - **Value**: Your MDSS URL + `/api/webhook/realtime`
   - **Example**: `https://mdss-example.com/api/webhook/realtime`
2. **APIKEY**

- **Key**: `APIKEY`
- **Value**: Your MDSS user API key
- **Note**: Ensure this key has appropriate permissions for webhook operations

3. **STORAGECLIENTID**
   - **Key**: `STORAGECLIENTID`
   - **Value**: Your storage client ID from MDSS
   - **To obtain**: Navigate to your desired storage configuration and copy the `storageClientId`

4.3 Save Configuration

1. Click **"Save"** to apply the environment variable changes



Step 5: Testing and Validation

5.1 Test the Function

1. Upload a test file to your configured S3 bucket
2. Monitor the Lambda function's execution in the **"Monitor"** tab
3. Check CloudWatch Logs for any execution errors or successful processing

5.2 Verify Integration

1. Confirm that file events are being sent to your MDSS instance
2. Verify that scans are initiated as expected
3. Review MDSS logs for successful webhook reception

Event-Based Real-Time handling for Azure

Azure Blob function app setup

1. Deploy the Azure function app using the Terraform script: https://github.com/OPSWAT/metadefender-k8s/tree/main/terraform/azure-function-docker
2. Configure `STORAGECLIENTID`, `APIKEY`, and `APIENDPOINT` variables in the `.tvars` file:

```
resource_group_name = "" #The name of the resource group in which the
function app will be created."
service_plan_name = "" #The name of the app service plan
storage_account_name = "" #The name of the storage account to be
created
docker_registry_server_url = ""
docker_registry_server_username = "" #optional
docker_registry_server_password = "" #optional
docker_image_name = ""
docker_image_tag = ""
AzureWebJobsBlobTrigger = "" #The storage account connection string
that triggers the function
CONTAINERNAME = "" #The blob container that needs to be scanned
fn_name_prefix = "" #function name
location = "" #azure region
STORAGECLIENTID  = ""
APIKEY = ""
APIENDPOINT = ""
```

Request Format (with examples)

The request body differs based on storage type. Below are the specifications for each supported storage:

Amazon S3 and S3 Compatible

```
{
    "storageClientId": '{Storage Client Id}',
    "metadata": "{'s3': { 'object': {'key': '{Object Path}' }}}"
}
```

```
{
    "storageClientId": "0c5454e3-d576-44c5-8ce4-cdc078011d0b",
    "metadata": "{'s3': { 'object': {'key': 'test-file.txt' }}}"
}
```

```
{
    "storageClientId": "0c5454e3-d576-44c5-8ce4-cdc078011d0b",
    "metadata": "{'s3': { 'object': {'key': 'folder1/folder2/test-
file.txt' }}}"
}
```

Response Formats

Success

When a webhook is successfully processed, the system returns:

```
{
    "correlationId": "67ea85a36f2f5732a82834d0"
}
```

Field	Description
correlationId	A unique identifier that references the submitted file in our database. You can use this ID for tracking the file's processing status or for future API calls related to this file.

Error

When an error occurs during processing, the system returns:

```
{
    "responseKey": "REST_API_MSG_FAILED_STORAGE_RTP_NOT_ENABLED",
    "responseMessage": "Real-Time Process is not enabled."
}
```

Field	Description
responseKey	Machine-readable error code that identifies the specific error condition.
responseMessage	Human-readable explanation of the error.

Common error responses

Response Message	Description	Recommended Action
The storage could not be found	The specified storage client ID does not exist in the system.	Verify the storageClientId is correct and the storage has been properly configured in the system.
Real-Time Process is not enabled.	Real-time processing has not been activated for this storage client.	Enable real-time processing for the storage client in your account settings.
Real-Time Process is enabled, but it is not set to Event Based.	The storage is configured for real-time processing, but is using polling rather than event-based processing.	Stop the current RTP scan and start another one using Event-Based

Azure Blob Event Grid RTP configuration

Refer to the example for detailed configuration: https://github.com/OPSWAT/metadefender-k8s/tree/main/terraform/CloudFunctions/Azure/webhook-notification

> **WARNING**
>
> Event Notifications for Page and Append blob are **NOT** supported.
>
> Events for these blob types are triggered upon the first block commit, potentially before the upload is complete.

Event-Based Real-Time handling for OracleSDK

Oracle Rule with custom Function trigger Setup Guide

This guide explains how to configure **Oracle Cloud Functions** and **Object Storage Events** to enable **real-time event-based processing** in MetaDefender Storage Security (MDSS) when using the **Oracle Native SDK** integration.

Prerequisites

Before proceeding with the setup, ensure the following requirements are met.

1. Required Permissions

Your Oracle Cloud Infrastructure (OCI) environment only needs the following **IAM permissions if you plan to deploy the function from an OCI repository**. Deploying from the repository is optional; these permissions are **not required** if you use other deployment methods.

Dynamic Group Permissions
Allow dynamic-group <your_dynamic_ group> to to read repos in tenancy
Allow dynamic-group <your_dynamic_ group> to use repos in tenancy

These permissions enable your function to **read and execute code from the OCI repository**.

2. Network and Access Requirements

- The function's subnet must allow outbound access to the public MDSS domain. No specific protocol (HTTP/HTTPS) is enforced by MDSS.
- Ensure your **Object Storage bucket** is in the same **tenancy and region** as your Function Application (recommended for lower latency).
- Verify that your **Object Storage bucket emits object events** (see Step 5).

Step 1: Create an Application and Function

1. In the Oracle Cloud Console, navigate to **Developer Services → Functions → Applications**.
2. Click **Create Application** and provide:
   - **Name**: e.g. `MetaDefenderStorageProcessorApp`
   - **VCN/Subnet**: Select a subnet with outbound internet access.
3. Once created, open your application and click **Create Function**.
4. Set:
   - **Function Name**: `MetaDefenderStorageSecurityProcessor`
   - **Runtime**: **Python**
   - **Entry Point**: `handler`

You can create and deploy your function either from the **OCI Console Code Editor** or using the **OCI CLI / Fn Project CLI**.

Step 2: Implement Function Code

Use the following Python function implementation. This code listens to Object Storage create events and sends real-time metadata to your MDSS instance for processing.

```
import io
import os
import json
import urllib.request
from urllib.parse import unquote
from fdk import response

def handler(ctx, data: io.BytesIO = None):
    event_body = json.loads(data.getvalue())
    object_key = event_body.get('data', {}).get('resourceName', '')
    object_key = unquote(object_key.replace("+", " "))

    payload = {
        "metadata": json.dumps({"Name": object_key}),
        "storageClientId": os.getenv("STORAGECLIENTID", "")
    }

    req = urllib.request.Request(
        url=os.getenv("APIENDPOINT", ""),
        data=json.dumps(payload).encode("utf-8"),
        headers={
            "ApiKey": os.getenv("APIKEY", ""),
            "Content-Type": "application/json"
        },
        method="POST"
    )

    urllib.request.urlopen(req, timeout=5)

    return response.Response(
        ctx,
        response_data=json.dumps({"status": "ok"}),
        headers={"Content-Type": "application/json"}
    )
```

Step 3: Configure Function Environment Variables

1. Open your **Function details** page in the Oracle Cloud Console.
2. Click **Configuration → Environment Variables → Edit**.
3. Add the following key-value pairs:

Key	Value	Description
APIENDPOINT	Your MDSS URL + `/api/webhook/realtime`	The MDSS real-time processing API endpoint
APIKEY	Your MDSS user API key	Your MDSS API key with webhook permissions
STORAGECLIENTID	Your storage client ID from MDSS	Navigate to your desired storage configuration and copy the `storageClientId` in order to obtain

4. Click **Save Changes**.

Step 4: Deploy the Function

If you are using the Code Editor in the OCI Console, click **Deploy**.

If you are using the CLI:

```
fn deploy --app MetaDefenderStorageProcessorApp
```

Once deployment completes, confirm your function appears in the **Functions** list and has an active **endpoint**.

Step 5: Create Object Storage Rule and Enable Event Emission

You will now link your Object Storage bucket to your Oracle Function so that MDSS receives file events in real time.

5.1 Create a Rule

1. In the OCI Console, navigate to **Observability & Management → Events Service → Rules**.
2. Click **Create Rule** and configure:
   - **Name**: `ObjectCreateTriggerRule`
   - **Condition**:
     - **Service**: *Object Storage*
     - **Event Type**: *Object - Create*
   - **Actions**:

- Select **Functions** and choose your **MetaDefenderStorageSecurityProcessor** function.

3. Click **Create Rule**.

This ensures that every time a new object is created in your bucket, an event triggers the Function.

5.2 Enable Object Event Emission on the Bucket

1. Navigate to **Object Storage → Buckets → [Your Bucket Name]**.
2. Under **Events**, click **Emit Object Events** → **Enable**.
3. Save your configuration.

Step 6: Testing and Validation

1. Upload a new file to your configured **Object Storage bucket**.
2. Open the **Functions → Metrics & Logs** tab to confirm the function execution was triggered.
3. Check the **MDSS instance** to verify the event was received and the file processing started.
4. If successful, the MDSS dashboard should show the new file scan in progress.

Request and Response Format

Request Body (Example)

```
{
    "storageClientId": "{Storage Client Id}",
    "metadata": "{'Name': 'uploads/sample.pdf'}"
}
```

Successful Response Example

```
{
    "correlationId": "67ea85a36f2f5732a82834d0"
}
```

Field	Description
correlationId	A unique identifier that references the submitted file in our database. You can use this ID for tracking the file's processing status or for future API calls related to this file.

Error

When an error occurs during processing, the system returns:

```
{
    "responseKey": "REST_API_MSG_FAILED_STORAGE_RTP_NOT_ENABLED",
    "responseMessage": "Real-Time Process is not enabled."
}
```

Field	Description
responseKey	Machine-readable error code that identifies the specific error condition.
responseMessage	Human-readable explanation of the error.

Common error responses

Response Message	Description	Recommended Action
The storage could not be found	The specified storage client ID does not exist in the system.	Verify the storageClientId is correct and the storage has been properly configured in the system.
Real-Time Process is not enabled.	Real-time processing has not been activated for this storage client.	Enable real-time processing for the storage client in your account settings.
Real-Time Process is enabled, but it is not set to Event Based.	The storage is configured for real-time processing, but is using polling rather than event-based processing.	Stop the current RTP scan and start another one using Event-Based

Summary

After completing this setup:

- Oracle **Object Storage** emits events on object creation.
- **Oracle Cloud Function** receives the event and forwards it to **MDSS** via webhook.
- **MDSS** immediately begins scanning the uploaded object in real time.

This configuration enables secure, low-latency, event-driven protection for files stored in Oracle Object Storage.

Workflows

Workflows are configurable processing pipelines that define how files should be scanned, analyzed, and remediated. A workflow is required to be able to start a new scan with a specified set of rules. Each workflow consists of a set of remediation actions.

Remediation actions are automated post-processing tasks performed on files after they have been scanned. The following remediation options are currently available:

Name	Description	Documentation
File Tagging	Adds metadata tags to files in S3-like storage units, providing processing information.	File Tagging
Deep CDR	Applies OPSWAT's Deep CDR (file sanitization) technology to files.	Deep Content Disarm and Reconstruction (Deep CDR)
Keep, copy, move or delete	Keeps, copies, moves or deletes files based on configured rules, such as blocked or sanitized status.	Keep, Copy, Move or Delete Files
Other remediations	Delete a directory if it is empty after remediation (does not delete if the folder was empty to begin with).	Delete Empty Folders

REMEDIATION ACTION PROCESSING ORDER

The following order is used when applying remediation actions:

1. File Tagging
2. Sanitized Files (Deep CDR, Move or Delete)
3. Blocked Files (Keep, Copy, Move or Delete)
4. Allowed Files (Keep, Copy, Move or Delete)

NOTE

If you require a post-processing action not listed above, please let us know.

We may be able to add it in a future update.

File Tagging

IMPORTANT

File Tagging is only available for Amazon S3, S3-compatible storage units (where supported) and Google Cloud Platform.

Info

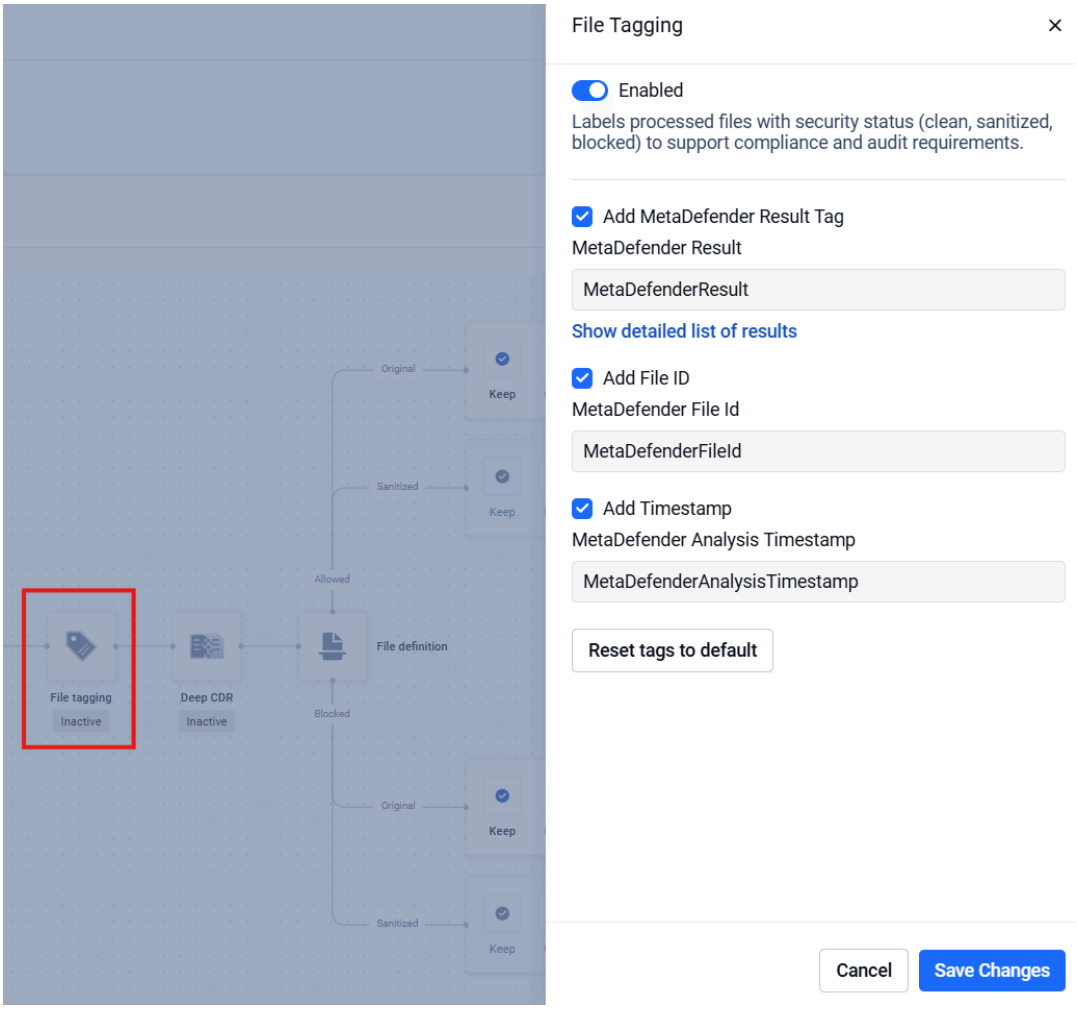
Google Cloud does not support applying tags directly to files; however, it does support metadata. Therefore, we treat metadata as tags and apply them in the same way as we apply tags in Amazon S3 and S3-compatible.

Warning

Metadata is preserved only when moving files between Google Cloud storage units.

Configuring File Tagging

- From the left-side navigation menu, go to **Workflows**
- Select the workflow for which you wish to configure **File Tagging** post action
- Select which tags to be added by checking/unchecking the boxes. (**Note:** at least one tag should be enabled if File Tagging is on)

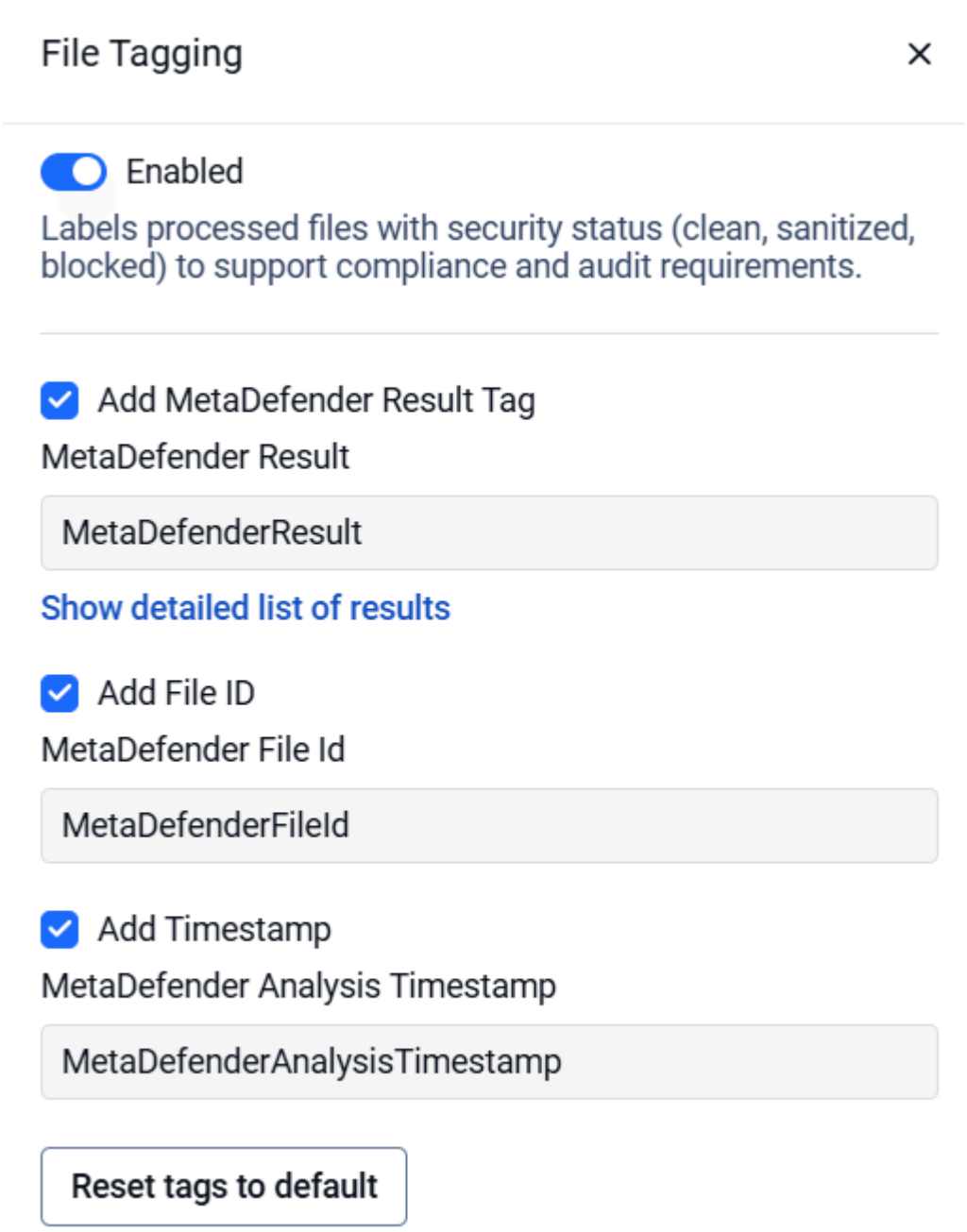


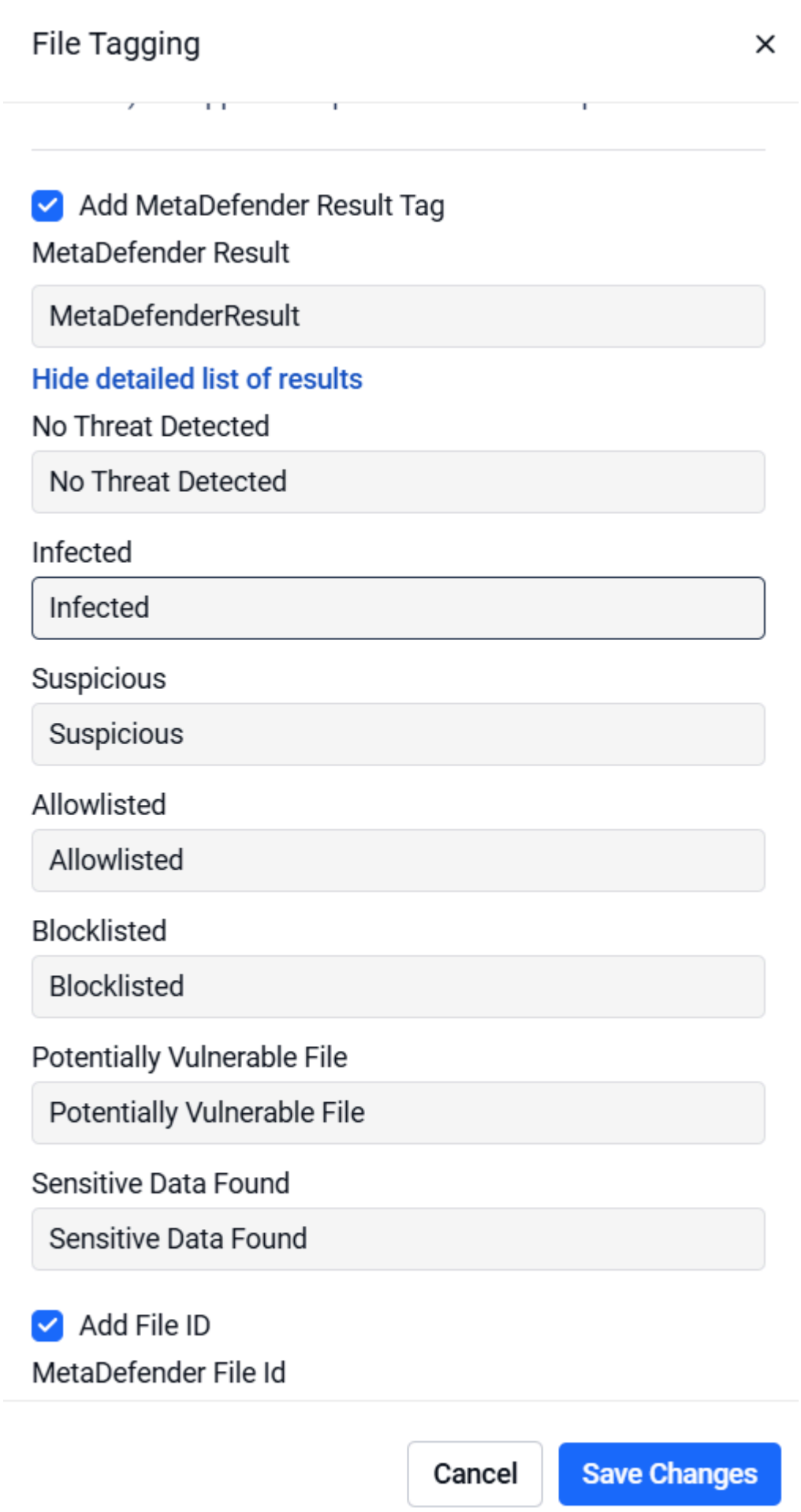
Customize file tags

There are three tags which can be customized and added to the file:

1. **MetaDefenderResult**
2. **MetaDefenderFileId**
3. **MetaDefenderAnalysisTimestamp**

To customize the **key** of a tag, please modify the values and if you want to keep it as a default value, click on the reset tags to default button.


File Tagging
Enabled
Labels processed files with security status (clean, sanitized, blocked) to support compliance and audit requirements.
Add MetaDefender Result Tag
MetaDefender Result
MetaDefenderResult
Show detailed list of results
Add File ID
MetaDefender File Id
MetaDefenderFileId
Add Timestamp
MetaDefender Analysis Timestamp
MetaDefenderAnalysisTimestamp
Reset tags to default


File Tagging
Add MetaDefender Result Tag
MetaDefender Result
MetaDefenderResult
Hide detailed list of results
No Threat Detected
No Threat Detected
Infected
Infected
Suspicious
Suspicious
Allowlisted
Allowlisted
Blocklisted
Blocklisted
Potentially Vulnerable File
Potentially Vulnerable File
Sensitive Data Found
Sensitive Data Found
Add File ID
MetaDefender File Id
Cancel
Save Changes

For the MetaDefender Result you can view the detailed list of customizable values. Below are some examples for the keys and the values of the tags.

Name	Value	Description
MetaDefenderResult (or the customized key associated with this name)	No Threat Detected / Infected etc (or the customized value associated with each result)	The final result of the processing
MetaDefenderFileId (or the customized key associated with this name)	5e7e15f132efdd0006b0e132	A unique file identifier that can be used for further REST API queries
MetaDefenderAnalysisTimestamp (or the customized key associated with this name)	2020-03-28T21:43:40.1500000Z	Date and time in UTC format when file processing has started

Deep Content Disarm and Reconstruction (Deep CDR)

Enabling the File Sanitization feature creates a secure version of a file by removing potentially harmful content. This process utilizes OPSWAT's Deep Content Disarm and Reconstruction (Deep CDR) technology.

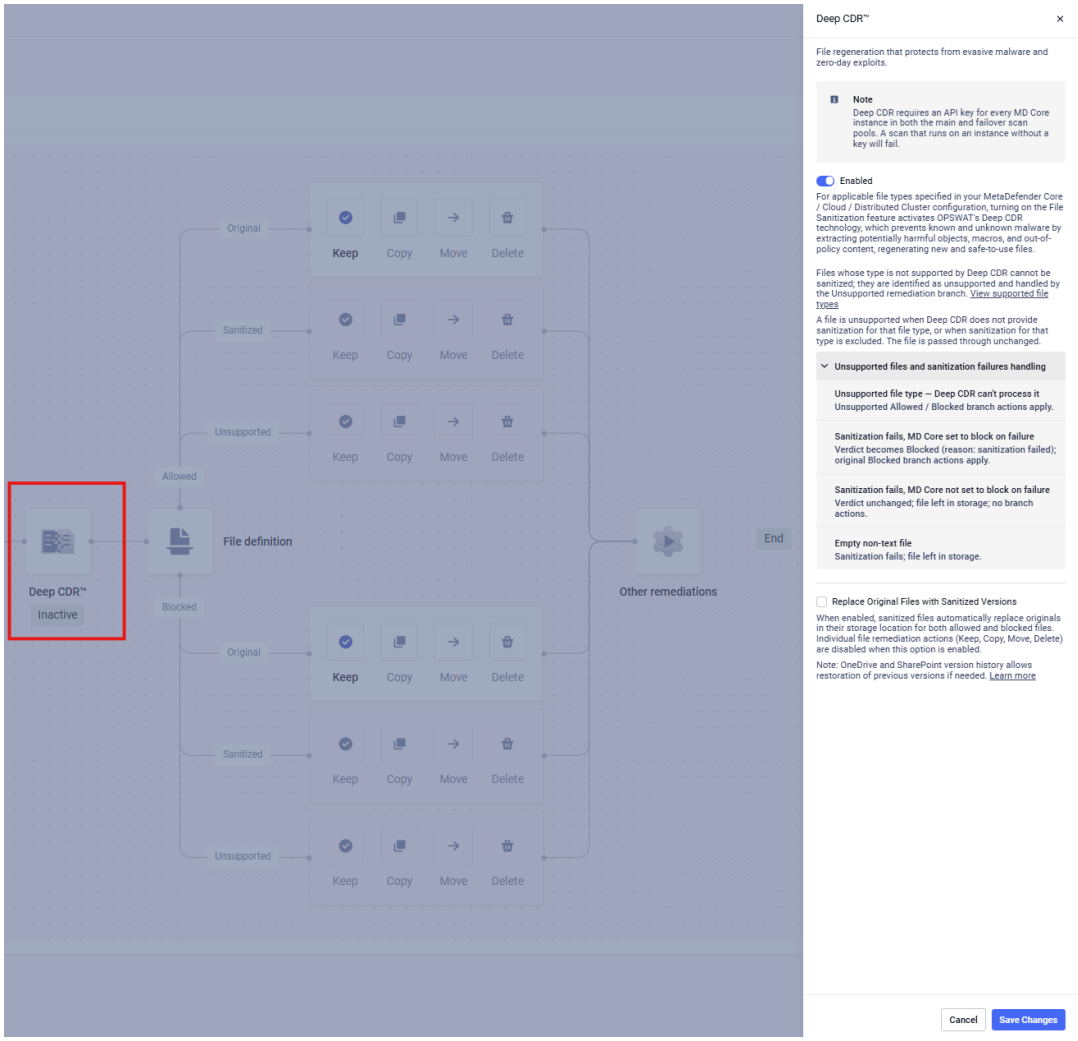
For detailed configuration instructions, refer to the Deep CDR user guide.

Learn more about OPSWAT's Deep CDR technology:
https://www.opswat.com/technologies/data-sanitization

Enabling Deep CDR

> **Dependency**
>
> In order to be able to use the Deep CDR functionality, Deep CDR must be active in MetaDefender Core instance or Metadefender Cloud and each scan instance both in the main and failover scan pools must have an API key.

1. Navigate to **Workflows** from the left-side navigation menu.
2. Select the workflow for which you want to enable Deep CDR.
3. In the **Workflow Diagram**, click on the "**Deep CDR**" node
4. In the modal window that's opened, select the **Deep CDR** tab and toggle **Active** to enable File Sanitization



> **Info**
>
> Enabling Deep CDR, also enables the configuration nodes for sanitized files that were allowed or blocked, which define what will happen with the sanitized file. It also enables the configuration nodes for files that are not supported by Deep CDR technology. Disabling Deep CDR disables the four nodes.

Unsupported branches

Files whose type is not supported by Deep CDR cannot be sanitized; they are identified as **Unsupported **and handled by the **Unsupported **remediation branch. For the list of supported file types, refer to the Deep CDR supported file types.

A file is considered unsupported when Deep CDR has no sanitization support for that file type, or when sanitization for that type has been disabled in the MetaDefender configuration. Unsupported files are not processed by Deep CDR and are left in their original state.

Unsupported files and sanitization failures handling

1. Unsupported file type - Deep CDR does not support this file type and cannot process it. The file is routed through the Unsupported branch, where the configured Allowed or Blocked actions apply.
2. Sanitization fails, and scan instance is configured to block the file on failure - The file verdict is set to Blocked with “Sanitization failed” as the reason. The original file is handled by the Blocked branch actions (move, copy, delete, or keep).
3. Sanitization fails, and scan instance is not configured to block the file on failure - The original file verdict is preserved. The file stays in its original location. No branch actions are applied.
4. For empty non-text files, sanitization fails - Sanitization cannot be applied to empty non-text files. The original file verdict is preserved and it is marked with a “Sanitization failed” remediations status. The file is left in its original location.

Replace Original Files with Sanitized Versions

Info

This is currently only supported for **OneDrive** and **SharePoint** storage types.

Overview

This feature enables **true in-place replacement** of original files with their sanitized counterparts produced by Deep CDR.

Previously, when Deep CDR was configured to *keep the sanitized version* and *delete the original*, the system performed these actions as two separate steps:

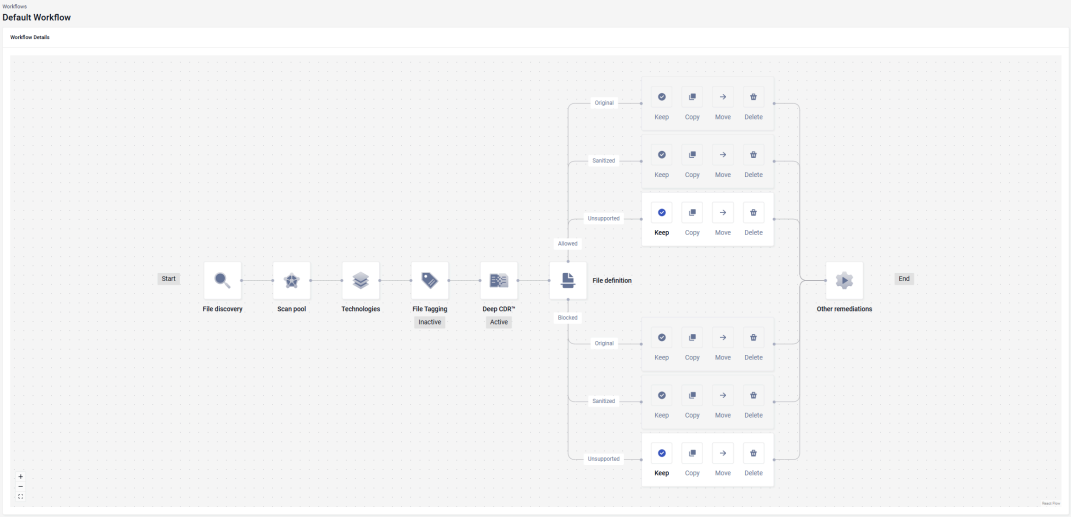
- A **new sanitized file** was uploaded
- The **original file** was deleted

With Replace Original Files enabled, the original file is **replaced directly** with the sanitized content, preserving file continuity by creating a new version of the same file rather than a new file.

How to Enable

1. Enable Deep CDR in the MetaDefender Storage Security Workflow
2. Check **“Replace Original Files with Sanitized Versions”**
3. Click Save Changes

When Replace Original Files with Sanitized Versions is enabled, all other **file remediation options are disabled and locked**. The only enabled options are those for files that are unsupported by Deep CDR.



File Version Cleanup (Optional)

By default, when Deep CDR replaces an original file with its sanitized version, the previous file version is retained in the storage unit's version history. This applies to **OneDrive** and **SharePoint Online**, which maintain automatic version histories for all files. To automatically delete the older version after replacement, set the following environment variable in the customer.env file:

```
DELETE_FILE_VERSIONS_AFTER_REPLACE=1
```

This setting is disabled by default (`0`). When enabled, the pre-sanitization version is removed from the version history after a successful replacement, keeping storage clean. If sanitization fails, the original file is left unchanged and no version deletion occurs.

Keep, Copy, Move or Delete Files

Configuring Keep/Copy/Move/Delete Remediation Actions

- Navigate to **Workflows** from the left-side navigation menu.
- Select the workflow for which you want to configure these remediation actions.
- Select the node for which you want to configure these remediation actions (Allowed Original, Allowed Sanitized, Blocked Original, Blocked Sanitized)
- Click on the box of the specific node.

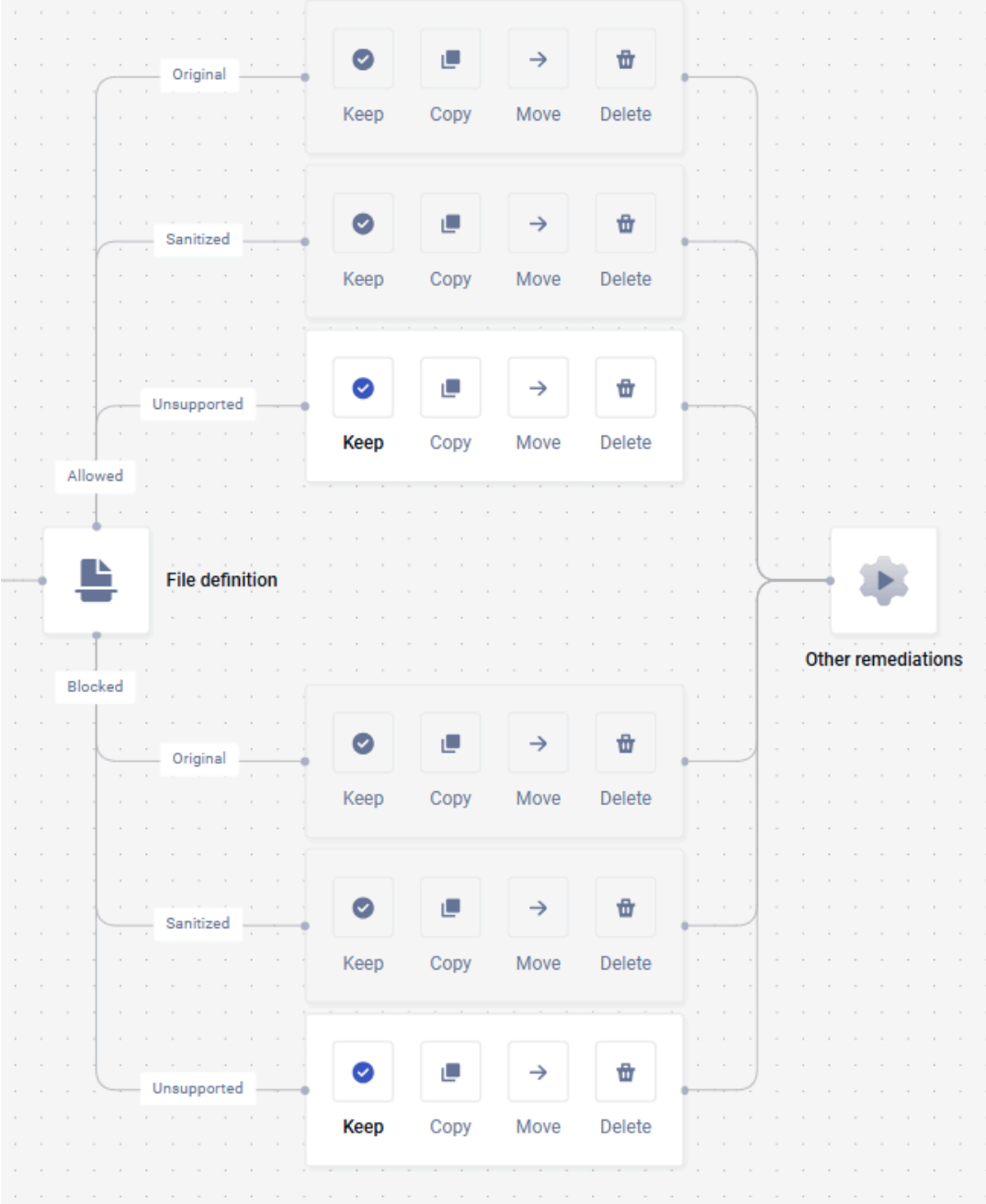
> **Note**

1. Sanitization fails, and MD Core is configured to block the file on failure - The file verdict becomes Blocked with Sanitization failed as the reason; in this case, the original Blocked branch actions apply
2. Sanitization fails, and MD Core is not configured to block the file on failure - The file verdict remains unchanged; the file is left in the storage unit, no branch actions are applied

Move operations are performed as a copy-then-delete sequence rather than a native move; if the upload step fails, the source file is left unchanged and the deletion is not attempted.

Technical Considerations

- Move and Re-processing **->** when a sanitized file is moved from Storage A to Storage B, it will not be re-sanitized on Storage B, even if Deep CDR is enabled there.
  - Similarly, if Real-Time Processing is enabled on Storage B, the moved file will not be processed again.
- File Overwriting **->** moving a file with the same name and path as an existing file on the destination storage will overwrite the existing file.
- By default, “Keep” is the selected option -> which will keep the file as is.
- For the sanitized versions (Allowed Sanitized, Blocked Sanitized), Copy and Delete options are unavailable.



Keeping/Moving Sanitized Files

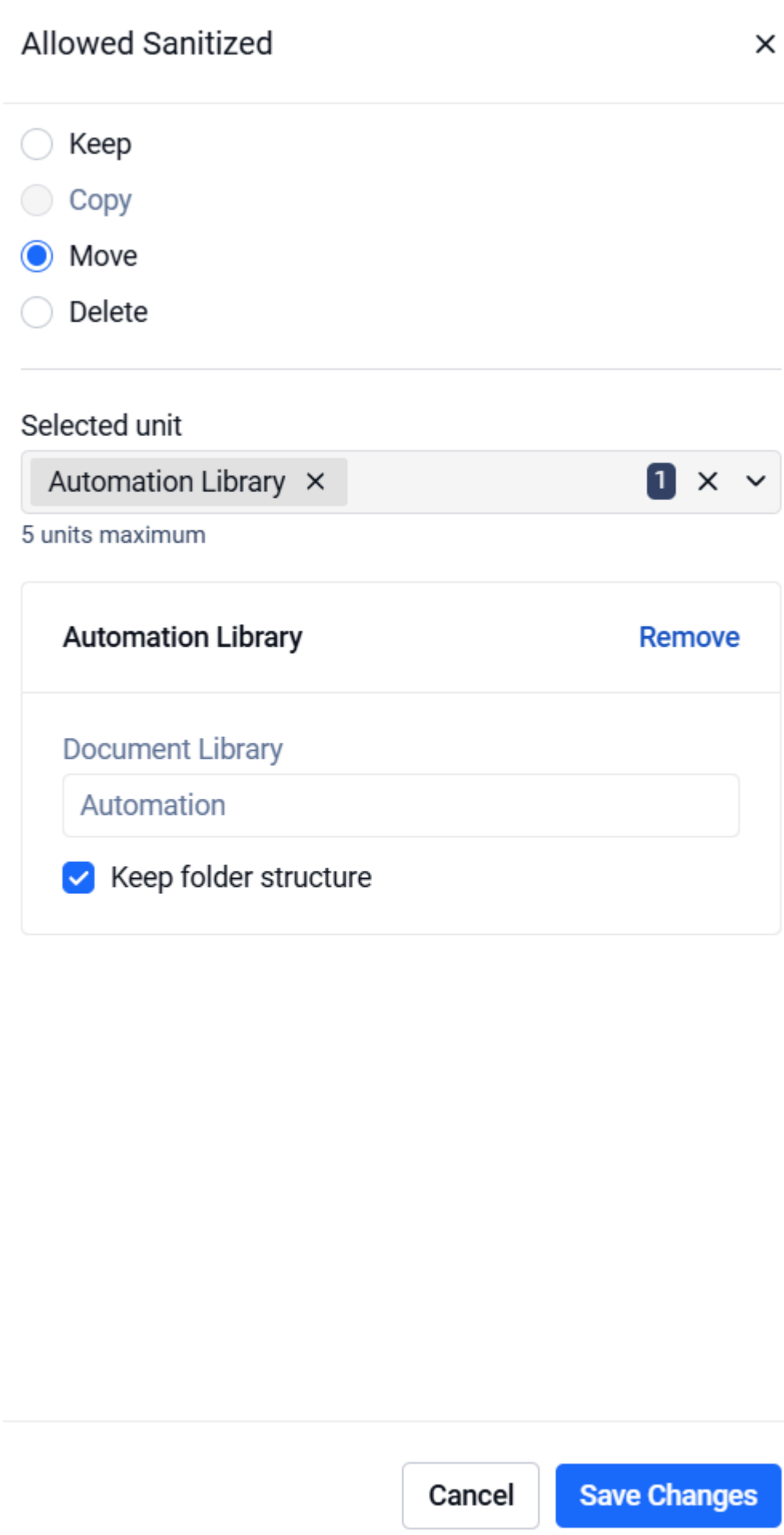
Sanitized files, created by OPSWAT's Deep CDR, can be moved to one or more storage units (up to a maximum of 5 destinations per remediation type).

Note: The File Sanitization feature must be enabled to configure this action - see Enabling Deep CDR: Deep Content Disarm and Reconstruction (Deep CDR)

1. Click on the **Sanitized Remediation (Allowed Sanitized or Blocked Sanitized)** node to open the modal window
2. Choose the action:

1. **“Keep the file”** -> the sanitized file is kept in the source storage location
2. “**Move the file**” -> the sanitized file is moved to another storage unit (or units). Configure the destination storage(s) as described below.

3. Configure the **destination storage** (only for option b):
   - Select one or multiple storage unit destinations out of the dropdown list
     - Additionally, narrow down the destination for certain types of storages (SharePoint Cloud, OneDrive, Box, SharePoint On-Premises), depending on how they are integrated
   - Note: A valid connection with the destination storage(s) is required.
   - Select **Keep folder structure** to maintain the source’s structure.

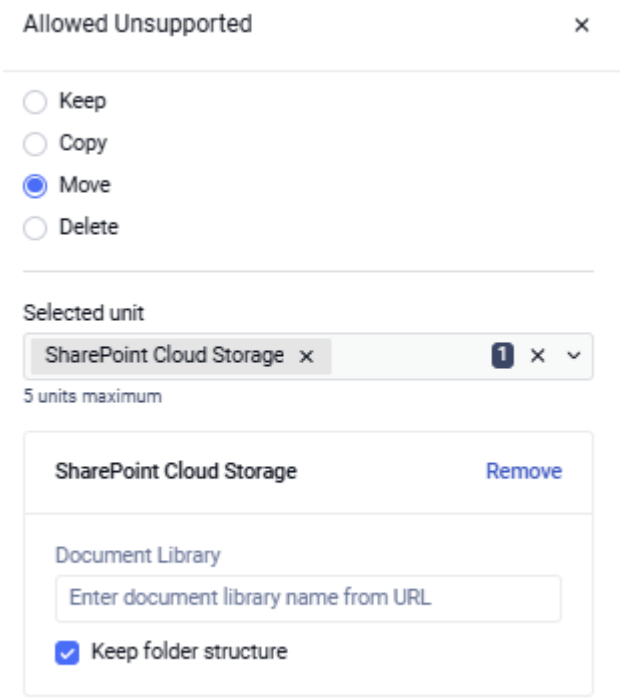

Allowed Sanitized
Keep
Copy
Move
Delete
Selected unit
Automation Library
1
5 units maximum
Automation Library
Remove
Document Library
Automation
Keep folder structure
Cancel
Save Changes

Keeping/Copying/Moving/Deleting Files that are Unsupported by Deep CDR

Deep CDR does not support all file types. Unsupported files can be kept, deleted, moved or copied to one or more storage units (up to a maximum of 5 destinations per remediation type).

Note: The File Sanitization feature must be enabled to configure this action - see Enabling Deep CDR: Deep Content Disarm and Reconstruction (Deep CDR)

1. Click on the **Unsupported Remediation (Allowed Unsupported or Blocked Unsupported)** node to open the modal window
2. Choose the action:
    1. **"Keep the file"** -> the file is kept in the source storage location
    2. **"Copy the file"** -> the file is copied to another storage unit (or units). Configure the destination storage unit(s) as described below
    3. "**Move the file**" -> the file is moved to another storage unit (or units). Configure the destination storage unit(s) as described below
    4. **"Delete the file"** -> the file is deleted
3. Configure the **destination storage** (only for options b and c):
    - Select one or multiple storage unit destinations out of the dropdown list
        - Additionally, narrow down the destination for certain types of storages (SharePoint Cloud, OneDrive, Box, SharePoint On-Premises), depending on how they are integrated
    - Note: A valid connection with the destination storage(s) is required.
    - Select **Keep folder structure** to maintain the source's structure.



Keeping/Copying/Moving/Deleting Allowed Original Files

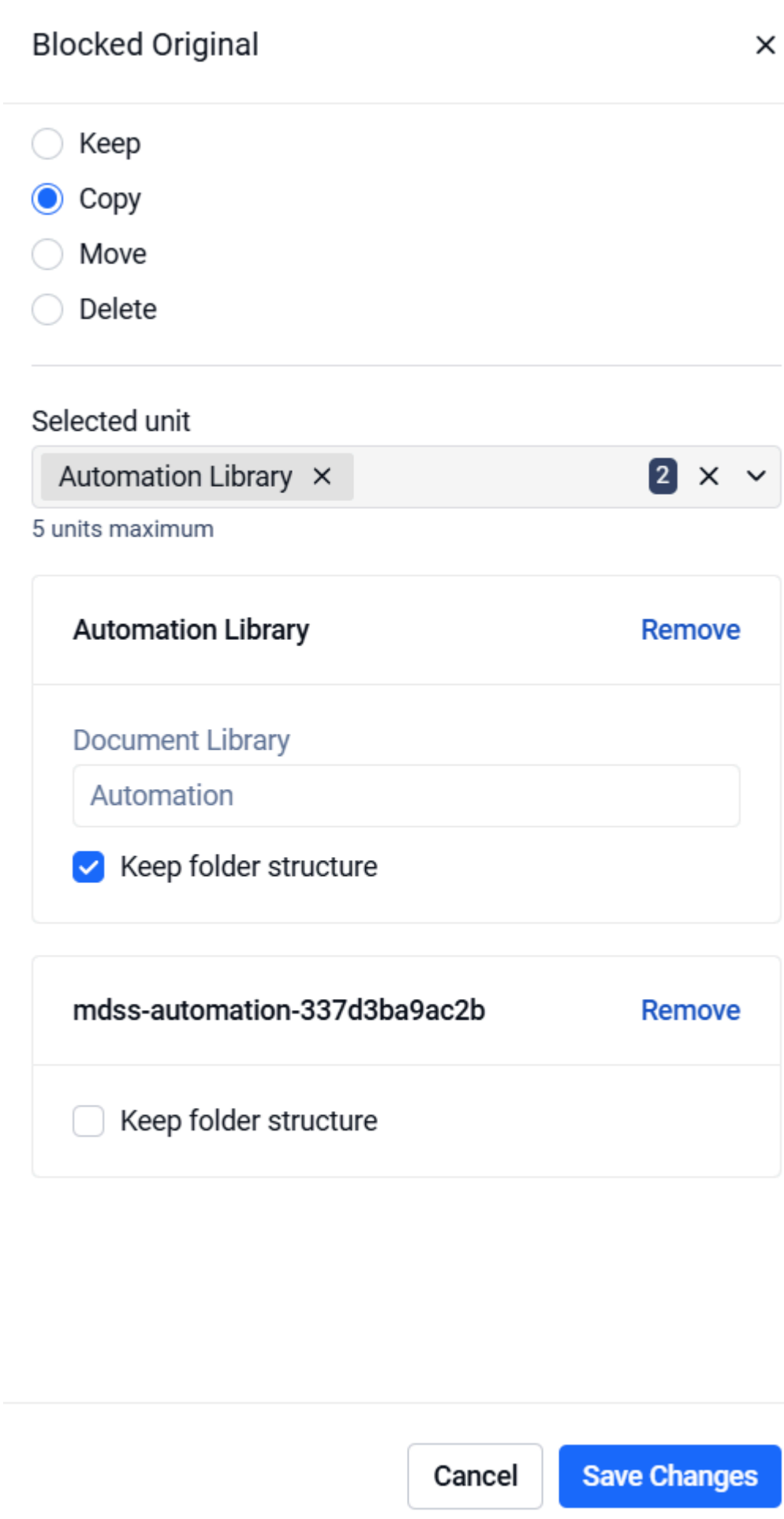
Files marked as **allowed** during processing can be deleted, copied or moved to one or more storage units (up to a maximum of 5 destinations per remediation type).

1. Click on the **Allowed Original Remediation** node to open the modal window
2. Choose the action:
    1. **Keep the file** -> the allowed file is kept in the same location
    2. **Copy the file** -> the allowed file is copied to another storage unit (or units). Configure the destination storage(s) as described below.
    3. **Move the file** -> the allowed file is moved to another storage unit (or units). Configure the destination storage(s) as described below.
    4. **Delete the file** -> the allowed file is deleted.
3. Configure the destination storage (only for options b and c):
    - Select one or multiple storage unit destinations out of the dropdown list
        - Additionally, narrow down the destination for certain types of storages (SharePoint Cloud, OneDrive, Box, SharePoint On-Premises), depending on how they are integrated
    - Note: A valid connection with the destination storage(s) is required
    - Select **Keep folder structure** to maintain the source's structure.

Keeping/Copying/Moving/Deleting Blocked Original Files

Files marked as **blocked** during processing can be deleted, copied or moved to one or more storage units (up to a maximum of 5 destinations per remediation type).

1. Click on the **Blocked Original Remediation** node to open the modal window
2. Choose the action:
    1. **Keep the file** -> the blocked file is kept in the same location
    2. **Copy the file** -> the blocked file is copied to another storage unit (or units). Configure the destination storage(s) as described below.
    3. **Move the file** -> the blocked file is moved to another storage unit (or units). Configure the destination storage(s) as described below.
    4. **Delete the file** -> the blocked file is deleted.
3. Configure the destination storage:
    - Select one or multiple storage unit destinations out of the dropdown list
        - Additionally, narrow down the destination for certain types of storages (SharePoint Cloud, OneDrive, Box, SharePoint On-Premises), depending on how they are integrated
    - Note: A valid connection with the destination storage(s) is required
    - Select **Keep folder structure** to maintain the source's structure.


Blocked Original
Keep
Copy
Move
Delete
Selected unit
Automation Library
2
5 units maximum
Automation Library
Remove
Document Library
Automation
Keep folder structure
mdss-automation-337d3ba9ac2b
Remove
Keep folder structure
Cancel
Save Changes

Storage types with additional configuration needed

INFO

For a number of the possible storage integrations - SharePoint Cloud, OneDrive, Box, SharePoint On-Premises - extra specifications may be necessary when selecting them as destinations as follows:

- If the **SharePoint Cloud** integration only has the **Site** specified, you will be asked to enter the name of the **Document Library** to which the files should be moved/copied
- If the **OneDrive** integration only has the **Group** specified, you will be asked to enter the name or email of the **User** to which the files should be moved/copied
- If the **SharePoint On-Premises integration** only has the **Site URL** specified, you will be asked to enter the name of the **Document Library** to which the files should be moved/copied
- If the **Box** integration has the **All Users** or **A specific group** selected, you will be asked to enter the name or email of the **User** to which the files should be moved/copied

Restrictions

Destination storage restrictions

Marking a storage as a destination for a remediation restricts certain actions on that storage such as deleting it, or altering its configuration in a way that makes the remediation invalid (in the case of destination storages that support users or libraries as a remediation configuration).

Scan restrictions

Starting a scan requires a valid workflow configuration.

The configuration can become invalid if one of the technologies that was enabled and used on the workflow is no longer available on the configured Scan Pool.

Handling Remediation Issues

When remediation actions are configured in a workflow and a user initiates a scan using that workflow, there is a possibility that some files may be discovered and scanned by the

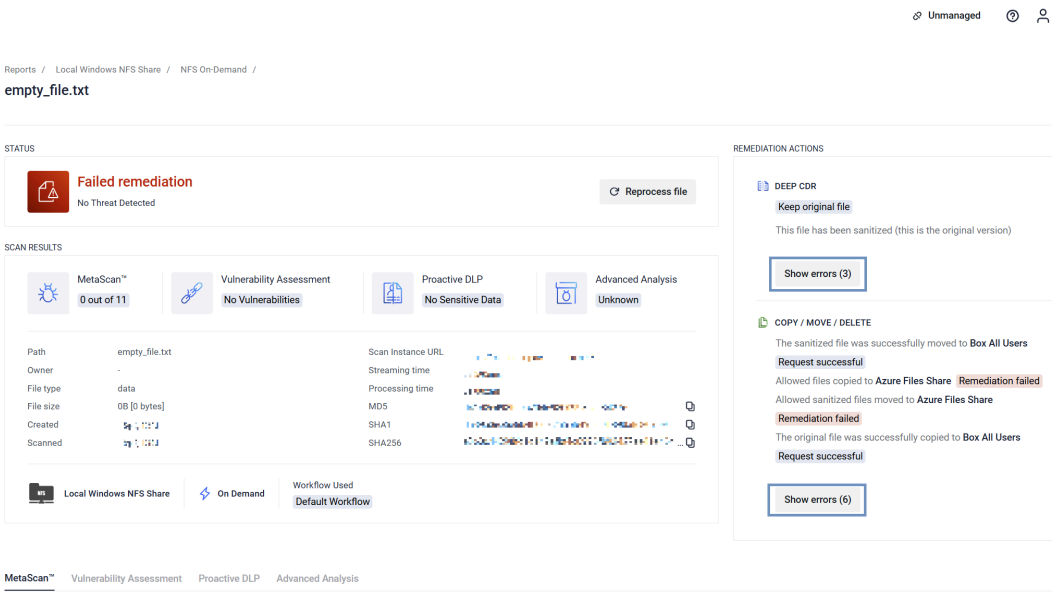
Scan Instance but fail during the application of remediation actions.

In such cases, the scan report will indicate a **Remediation Failed** status.

File name	Status	MetaScan™	Vulnerability Assessment	Proactive DLP	Advanced Analysis	Remediations	Path
presentation.pptx	Allowed	0 out of 11	No Vulnerabilities	No Sensitive Data	Unknown		presentation...
alireza.txt	Allowed	0 out of 11	No Vulnerabilities	No Sensitive Data	Unknown		alireza.txt
empty_file.txt	Failed	0 out of 11	No Vulnerabilities	No Sensitive Data	Unknown	Failed remediation	empty_file.txt
receipts.csv	Allowed	0 out of 11	No Vulnerabilities	No Sensitive Data	Unknown		receipts.csv

To obtain further details about this issue, users can filter the files marked as **Remediation Failed** and click on individual files to access their specific reports.

On the right side of the report, the **Remediation Actions** tab will display all remediation actions taken on the file, including their success or failure.



To diagnose the cause of the failure, users can click on the failed remediation to view the specific exception that led to the failure.

Typically, for Move or Copy remediation actions, the issue is related to the destination storage. If sanitization has failed, refer to the Unsupported files and sanitization failures handling section for details on which branch actions apply.

Troubleshooting Reference

Issue	Common causes	First steps
Copy/Move failures	Storage permissions, network connectivity, disk space	Check storage health, verify credentials
Sanitization failures	File type not enabled, sanitized version upload issue	Check Scan Instance configuration
Performance issues	Multiple destinations, large files, network latency	Review remediation complexity, optimize storage placement
Configuration Errors	Invalid storage selections, missing permissions	Validate workflow configuration, test connections

Integration considerations

Storage requirements

- Make sure the destination storages have sufficient capacity (recommend 2x source storage size)
- Verify network bandwidth between source and destination storages

Security Best Practices

- Use service accounts with minimum required permissions
- Enable encryption for sensitive file transfers
- Regular security audits of remediation workflows

Next steps after configuring remediation actions:

Test Workflows -> run test scans with sample files to verify remediation behavior

Plan scaling -> consider future storage and performance requirements

Delete Empty Folders

Automatic Empty Folder Deletion After Remediation

The **Delete Empty Folders** feature automatically removes directories that become empty following remediation actions. This feature helps maintain a clean and organized file system by eliminating unnecessary empty folders.

> **SUPPORTED STORAGE TYPES**
>
> NFS, SMB and SFTP

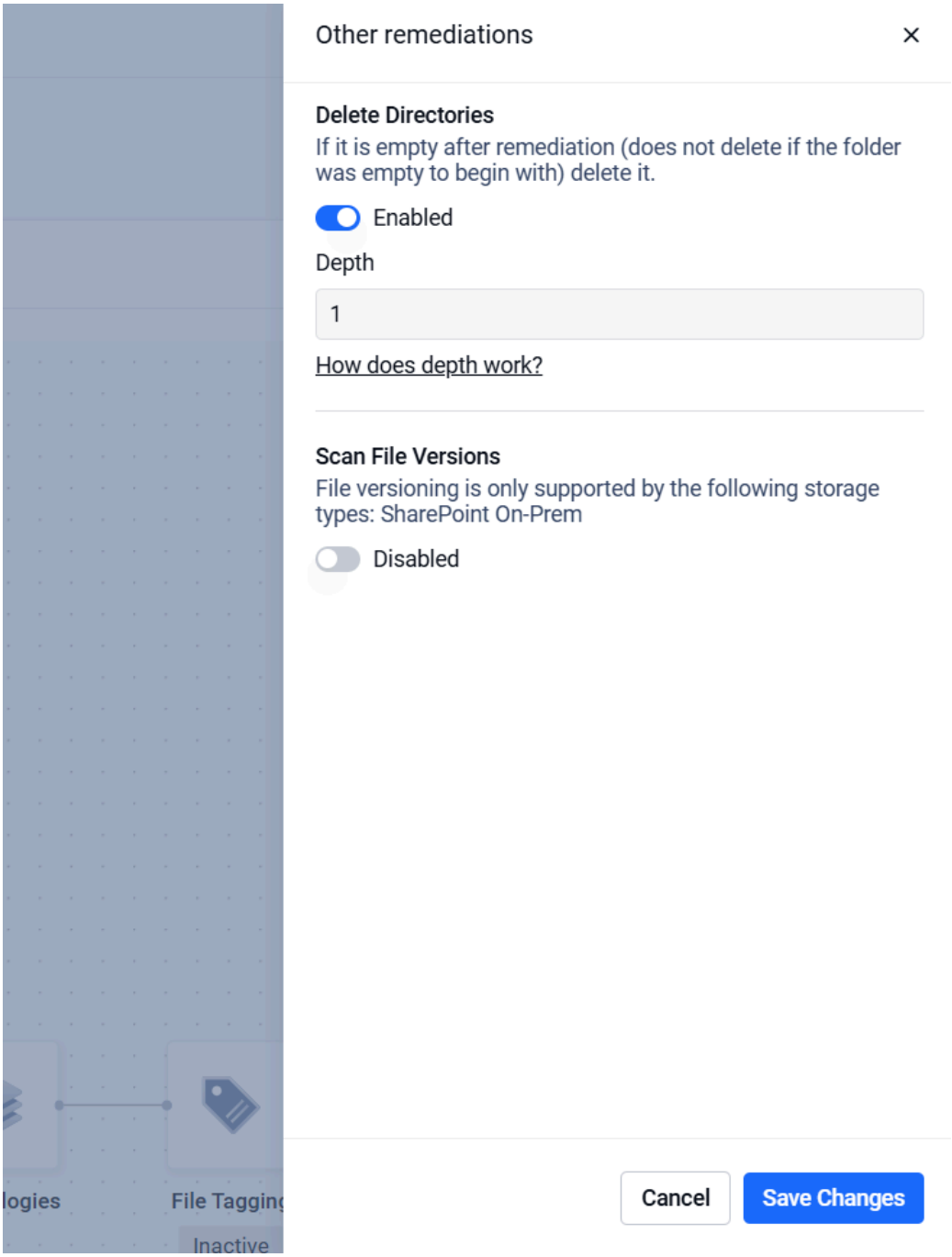
Deletion Behavior

1. Empty folder deletion occurs after a scan completes and then every 10 minutes.
2. A folder will **NOT** be deleted if it contains any files or folders after the remediation.
3. A folder will **NOT** be deleted if it was empty before the remediation.

Configuring Empty Folder Deletion

> **Limitations**
>
> The node is disabled if there is no prior remediation configured with Move/Delete. If Delete Empty Folders is enabled, and there is only one remediation configured with Move/Delete, that remediation cannot be changed to Keep/Copy.

- Navigate to **Workflows** from the left-side navigation menu
- Select the workflow for which you want to configure empty folder deletion
- Click the **Other remediations** node
- In the modal window opened, toggle the “Delete a directory if it is empty after remediation” option
- Enable the option: **Delete a directory if it is empty after remediation** - this does not delete if the folder was empty to begin with.

- 

Depth Parameter

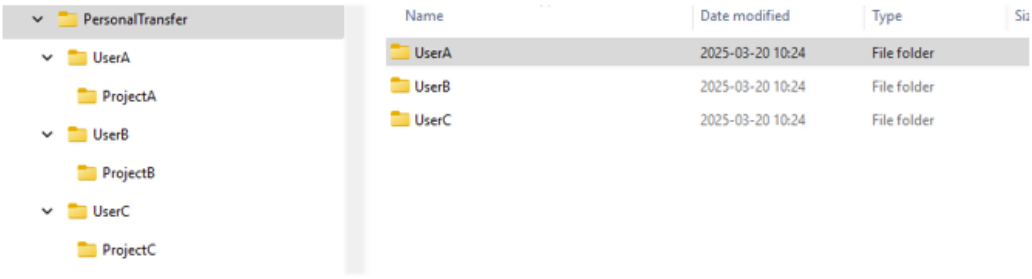
The depth parameter is used to determine where deletion of empty folders starts. It is a value in the range 1-10000

For example in the picture below we have a folder structure. Let's say that there is an nfs storage that has the sharePath PersonalTransfer.

Default - Depth = 1 -> PersonalTransfer Folder (which is also root) is kept, the rest of the empty folders are deleted

Depth = 2 -> UserA, UserB and UserC are kept, the rest of the empty folders are deleted

Depth = 3 -> UserA, UserB, UserC, ProjectA, ProjectB and ProjectC are kept, the rest of the empty folders are deleted



Remediation Process Retries

The remediation process includes automatic retry functionality to handle transient failures. When processing each file, the system will attempt up to **3 retries** if the initial remediation attempt fails. There is a **30-second interval** between each retry attempt to allow for temporary issues to resolve.

The retry interval is configurable through the `POLLY_POST_ACTION_RETRY_TIME` environment variable, allowing you to adjust the timing based on your specific requirements and infrastructure constraints.

Configuration Example

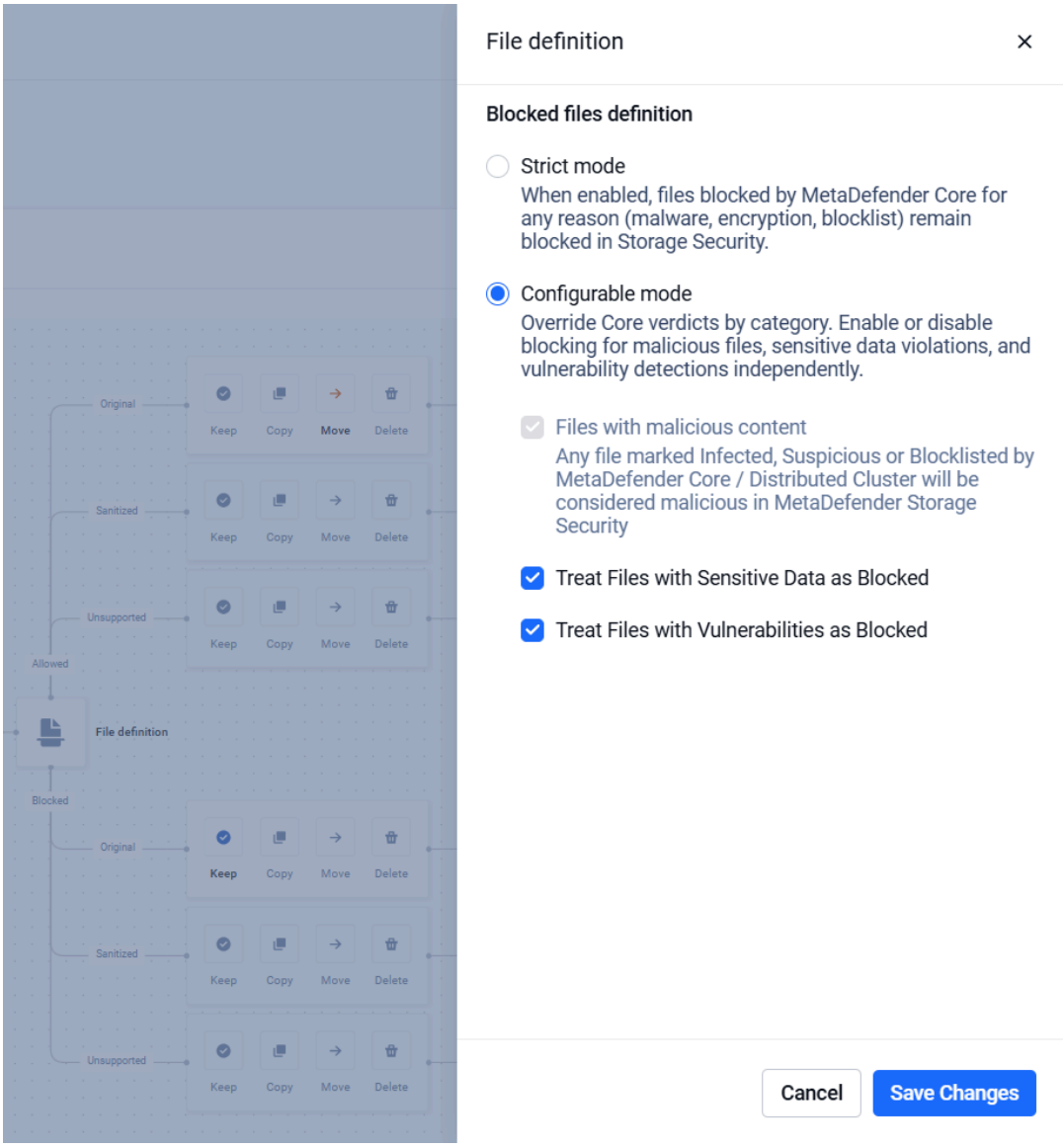
To extend the retry interval to 60 seconds, add the following to your `customer.env` file (instructions here):

```
POLLY_POST_ACTION_RETRY_TIME=60
```

File Definition

Blocked File Treatment Options

1. **Strict** - all files blocked by MetaDefender Core (e.g., malware, encrypted archives, blocklisted files) are treated as blocked
2. **Configurable -** allows selecting additional file types to treat as blocked.
   - **Files with malicious content** - always enabled (Infected, Suspicious, Blocklisted).
   - **Files with sensitive data -** enabled if checked.
   - **Files with vulnerabilities** - enabled if checked.



Technologies

MDSS monitors the status of the following technologies from MetaDefender Core:

- Data Loss Prevention
- Deep CDR
- Sandbox
- Metascan

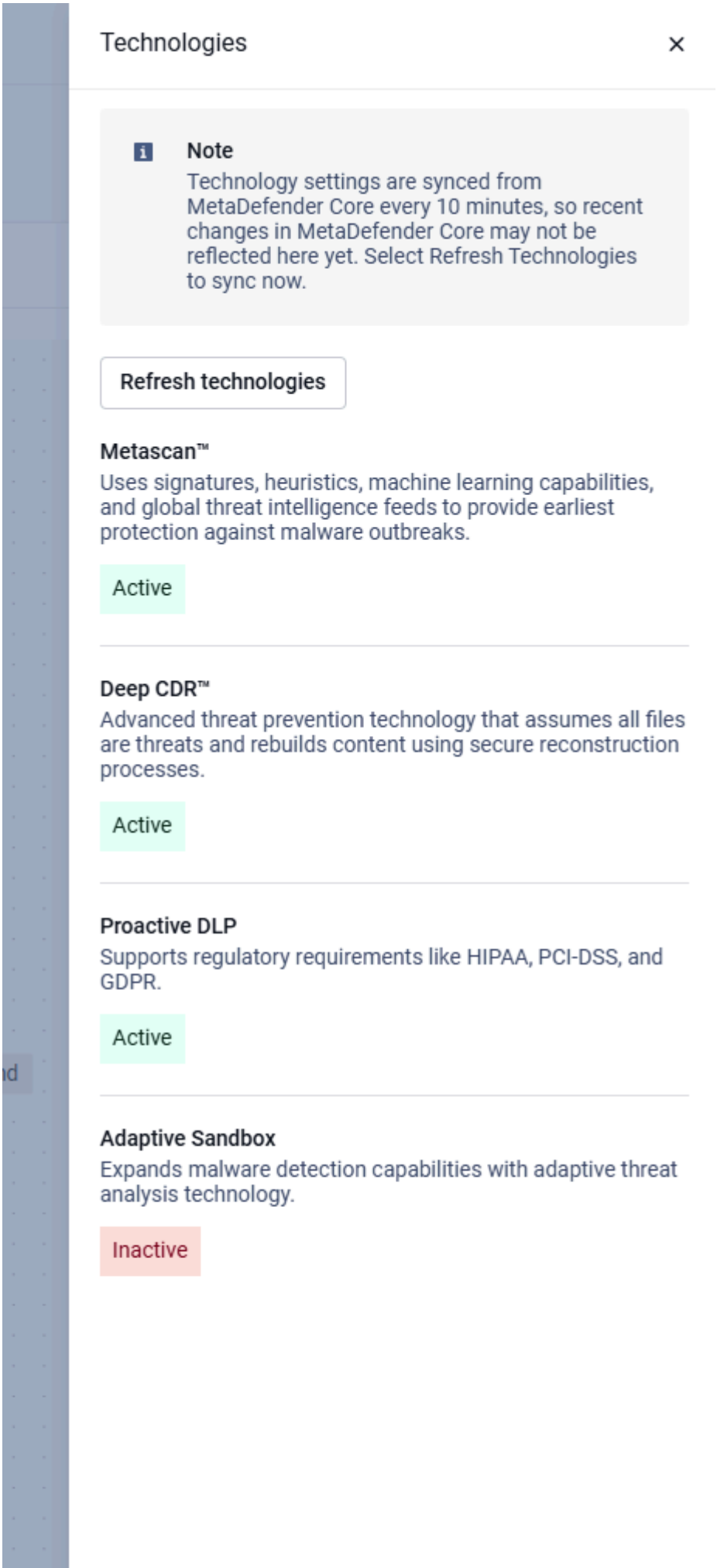
These monitoring is done every 5 minutes to see what changes are done on MetaDefender Core for these technologies. A manual refresh is available as well to have this check done on demand

This is not available on MetaDefender Cloud

Technology Status

There are three statuses for the technologies:

- **Enabled**
  - A valid ApiKey was provided for the scan pool and the technology is **available** in the MetaDefender Core instance.
- **Disabled**
  - A valid ApiKey was provided for the scan pool and the technology is **unavailable** in the MetaDefender Core instance.
  - This will prevent allowing to set up actions that are not available in the MetaDefender Core instance.
- **Unknown**
  - No ApiKey was provided for the scan pool. The status of the technology from MetaDefender Core instance is unknown.


Technologies
Note
Technology settings are synced from MetaDefender Core every 10 minutes, so recent changes in MetaDefender Core may not be reflected here yet. Select Refresh Technologies to sync now.
Refresh technologies
Metascan™
Uses signatures, heuristics, machine learning capabilities, and global threat intelligence feeds to provide earliest protection against malware outbreaks.
Active
Deep CDR™
Advanced threat prevention technology that assumes all files are threats and rebuilds content using secure reconstruction processes.
Active
Proactive DLP
Supports regulatory requirements like HIPAA, PCI-DSS, and GDPR.
Active
Adaptive Sandbox
Expands malware detection capabilities with adaptive threat analysis technology.
Inactive

Scan File Versions

Overview

The File Version Scanning remediation capability enables MDSS to locate and examine **every version of a file** that exists during scanning operations. This functionality helps users more effectively pinpoint problematic or restricted file versions.

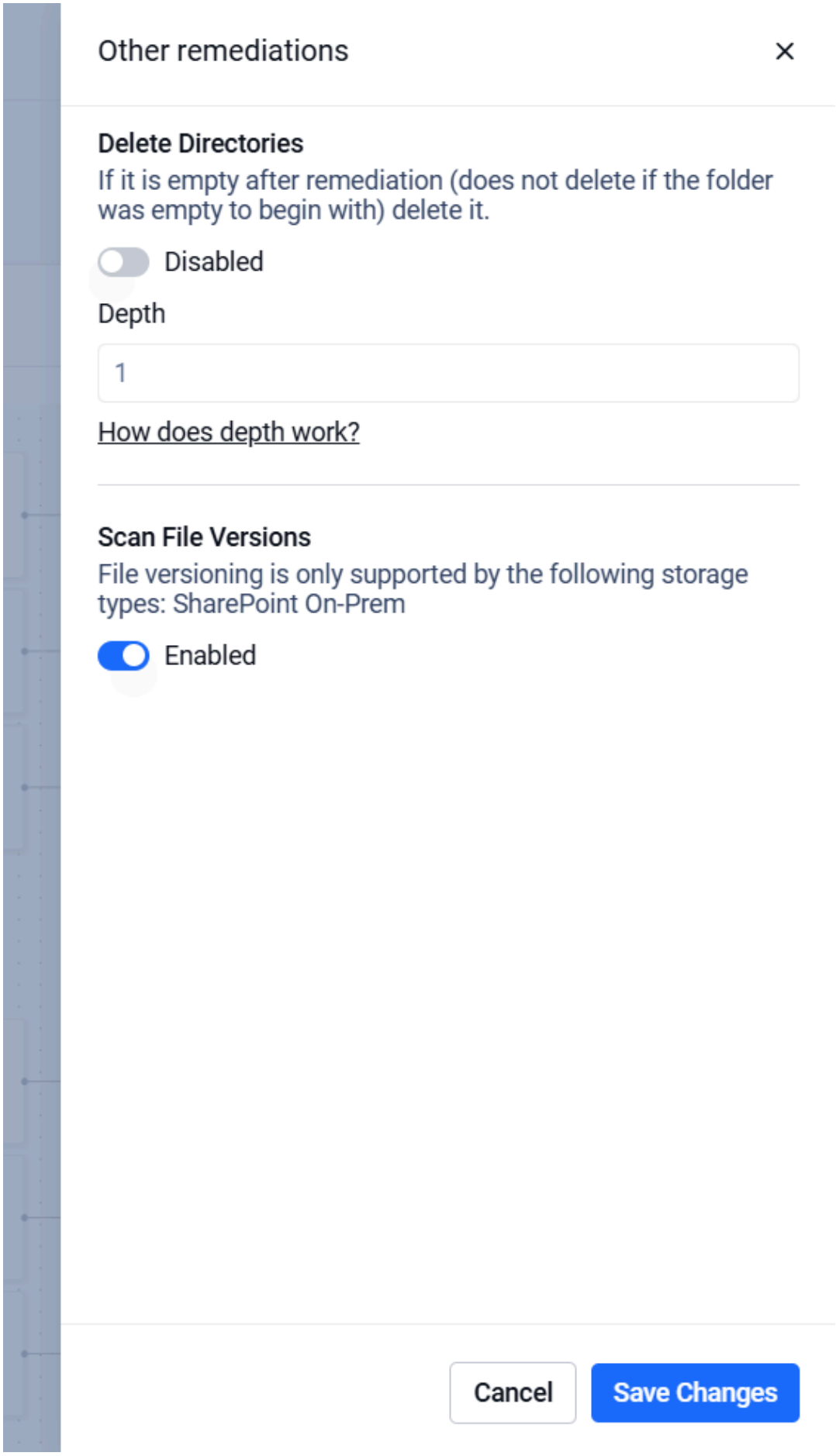
Requirements

File versioning must be activated on your SharePoint On-Premises environment before utilizing this feature. The scanning process cannot identify and report on multiple file versions without versioning being enabled.

> **Compatible Storage Systems/Storage Unit**
>
> SharePoint On-Premises

Configuration

1. Navigate to **Workflows** from the left-side navigation menu.
2. Select the workflow you want to configure scan file versions.
3. Click the **Other Remediations** node.
4. In the modal window that opens, toggle the **Scan File Versions** option.
5. Click **Save Changes** to apply the changes.


Other remediations
Delete Directories
If it is empty after remediation (does not delete if the folder was empty to begin with) delete it.
Disabled
Depth
1
How does depth work?
Scan File Versions
File versioning is only supported by the following storage types: SharePoint On-Prem
Enabled
Cancel
Save Changes

Use Case

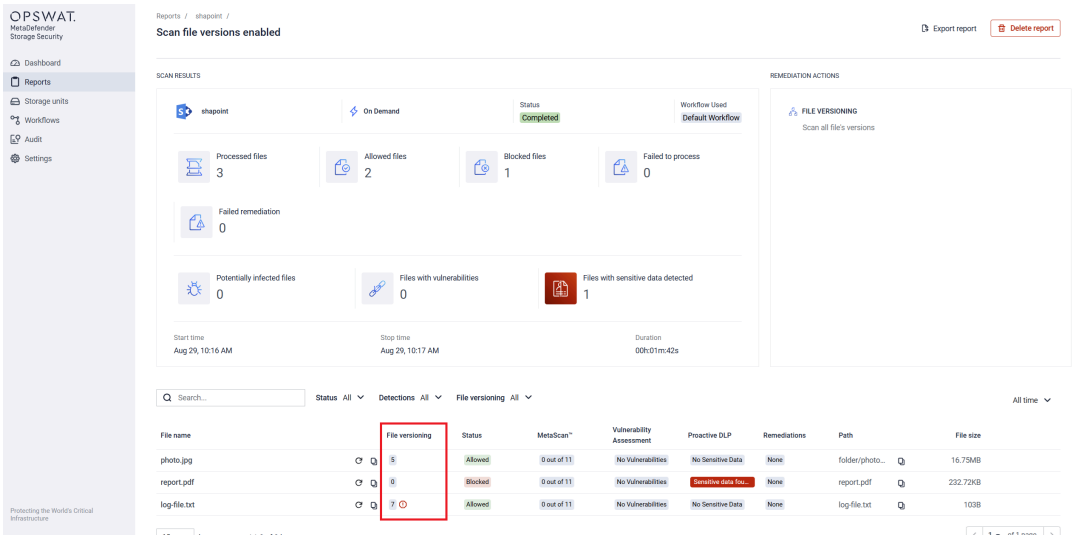
This remediation type is particularly useful when:

- Multiple versions of the same file may exist across different environments.
- You need to ensure that all versions comply with security and compliance requirements.
- You want quick visibility into which versions are safe and which are blocked.

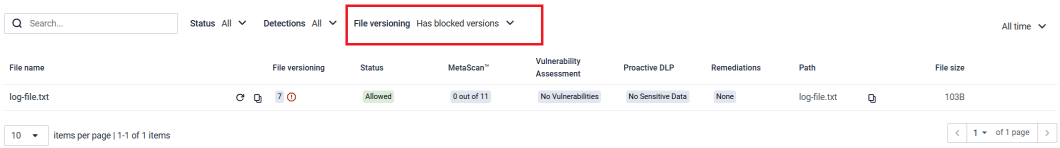
Reporting

During or after a scan with **Scan File Versions** enabled, the report provides additional insights:

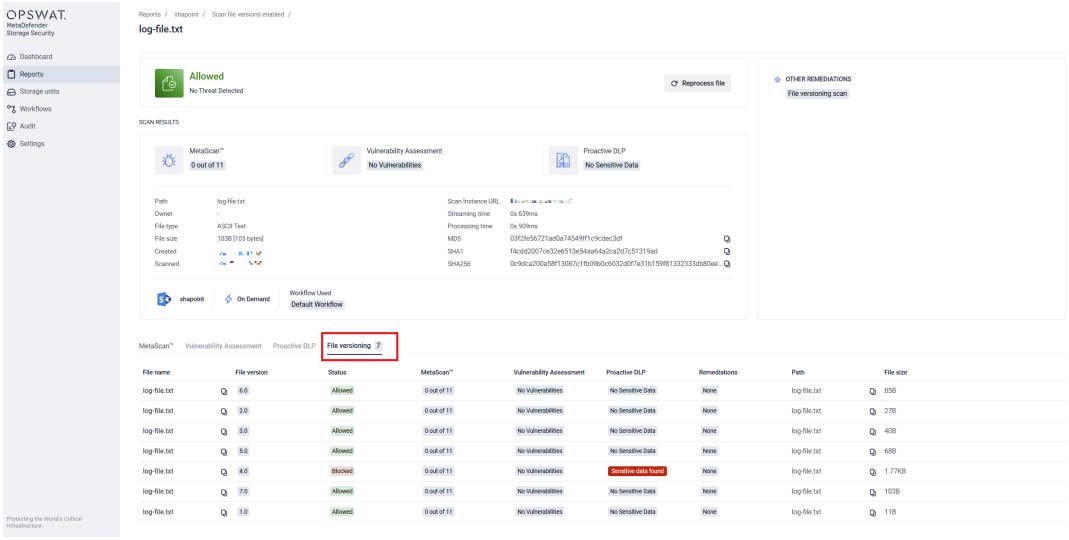
- **New Column – File Versioning**: A dedicated column displays the number of detected versions for each file and indicates if any of those versions are blocked.

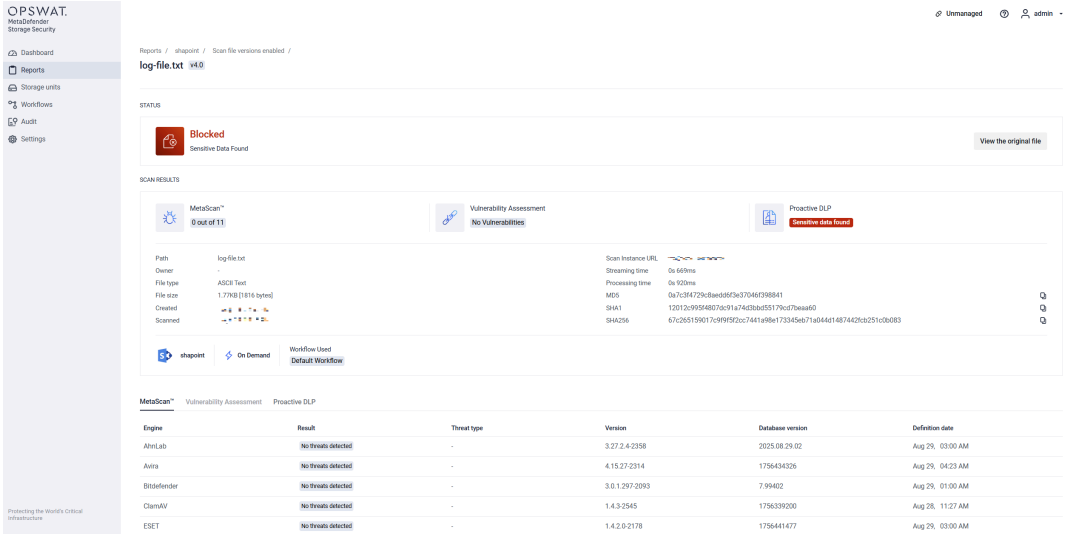


- **Filtering**: The report includes a filter to show only files that contain blocked versions.



- **Individual File Report**: Within a file's detailed report, a new column lists all discovered versions. Clicking on a version displays its scan result.


OPSWAT.
MetaDefender
Storage Security
Dashboard
Reports
Storage units
Workflows
Audit
Settings
Reports / shapoint / Scan file versions enabled /
log-file.txt
Allowed
No Threat Detected
Reprocess file
OTHER REMEDIATIONS
File versioning scan
SCAN RESULTS
MetaScan™
0 out of 11
Vulnerability Assessment
No Vulnerabilities
Proactive DLP
No Sensitive Data
Path log-file.txt
Owner -
File type ASCII Text
File size 103B [103 bytes]
Created
Scanned
Scan Instance URL
Streaming time 0s 639ms
Processing time 0s 909ms
MD5 03f2fe56721ad0a74549ff1c9cdec3df
SHA1 14cdd2007ce32fe6513e54ab64a2ca267c51319ad
SHA256 0c9dca200a58f13087c1fb09b0c6032d0f7e31b159f81332333db80ee...
shapoint
On Demand
Workflow Used
Default Workflow
MetaScan™
Vulnerability Assessment
Proactive DLP
File versioning 7
File name
File version
Status
MetaScan™
Vulnerability Assessment
Proactive DLP
Remediations
Path
File size
log-file.txt 6.0 Allowed 0 out of 11 No Vulnerabilities No Sensitive Data None log-file.txt 85B
log-file.txt 2.0 Allowed 0 out of 11 No Vulnerabilities No Sensitive Data None log-file.txt 27B
log-file.txt 3.0 Allowed 0 out of 11 No Vulnerabilities No Sensitive Data None log-file.txt 40B
log-file.txt 5.0 Allowed 0 out of 11 No Vulnerabilities No Sensitive Data None log-file.txt 68B
log-file.txt 4.0 Blocked 0 out of 11 No Vulnerabilities Sensitive data found None log-file.txt 1.77KB
log-file.txt 7.0 Allowed 0 out of 11 No Vulnerabilities No Sensitive Data None log-file.txt 103B
log-file.txt 1.0 Allowed 0 out of 11 No Vulnerabilities No Sensitive Data None log-file.txt 11B
Protecting the World's Critical Infrastructure


OPSWAT.
MetaDefender
Storage Security
Dashboard
Reports
Storage units
Workflows
Audit
Settings
Unmanaged
admin
Reports / shapoint / Scan file versions enabled /
log-file.txt v4.0
STATUS
Blocked
Sensitive Data Found
View the original file
SCAN RESULTS
MetaScan™
0 out of 11
Vulnerability Assessment
No Vulnerabilities
Proactive DLP
Sensitive data found
Path log-file.txt
Owner -
File type ASCII Text
File size 1.77KB [1816 bytes]
Created
Scanned
Scan Instance URL
Streaming time 0s 669ms
Processing time 0s 920ms
MD5 0a7c3f4729c8eedd6f3e37046f398841
SHA1 12012c995f4807dc91a74d3bbd55179cd7beaa60
SHA256 67c265159017c9f9f5f2cc7441a98e173345eb71a044d1487442fcb251c0b083
shapoint
On Demand
Workflow Used
Default Workflow
MetaScan™
Vulnerability Assessment
Proactive DLP
Engine
Result
Threat type
Version
Database version
Definition date
AhnLab No threats detected - 3.27.2.4-2358 2025.08.29.02 Aug 29, 03:00 AM
Avira No threats detected - 4.15.27-2314 1756434326 Aug 29, 04:23 AM
Bitdefender No threats detected - 3.0.1.297-2093 7.99402 Aug 29, 01:00 AM
ClamAV No threats detected - 1.4.3-2545 1756339200 Aug 28, 11:27 AM
ESET No threats detected - 1.4.2.0-2178 1756441477 Aug 29, 03:00 AM
Protecting the World's Critical Infrastructure

User Management

> **IMPORTANT**
>
> Sharing administrative accounts is strongly discouraged.
>
> For users who only need to review reports, assign read-only permissions.

For organizations requiring multiple individuals to access MetaDefender Storage Security or MetaDefender Storage Security Cloud for report review or storage integration, you can create individual user accounts.

MetaDefender Storage Security supports various user roles with different permission levels.

Local Administrator

- Accounts with administrative privileges have full control over each available configuration and all features
- Exclusive to one individual per deployment
- Hidden from other users in the system
- Configure and set up the MDSS deployment with all necessary parameters
- Modify any settings related to the deployment as required
- Facilitate the creation and management of additional user roles for customer use

Permissions

- Add, delete, or modify scan instances, scan pools, and workflows
- Manage the product license settings
- Configure data retention settings
- Configure the possibility of external logging (to Kafka)
- Modify the SSO configuration if any alterations are necessary
- Access user management-related settings
- View the settings related to Workflows
- View the status of scan pools and individual scan instances
- View the configuration of data retention policies
- Set up and manage webhook notification settings to facilitate external integrations
- Add, delete, or modify storage units and remediation actions
- Initiate instant, scheduled, or real-time scans on specific storage units
- Access and review generated reports for insights into scan results
- View the audit page to track changes and activities within the system

- Monitor the dashboard for an overview of storage activity and key metrics

Tenant Administrator

- Available only on MDSS Cloud
- Highest privilege role available to standard users of MDSS Cloud
- Multiple users can hold this role simultaneously
- Utilize the MDSS features and functionalities without altering the overall configuration
- Manage common operations and user interactions within the application

Permissions

- Access user management-related settings
- View the settings related to Workflows
- Set up and manage webhook notification settings to facilitate external integrations
- Add, delete, or modify storage units and remediation actions
- Initiate instant, scheduled, or real-time scans on specific storage units
- Access and review generated reports for insights into scan results
- View the audit page to track changes and activities within the system
- Monitor the dashboard for an overview of storage activity and key metrics

Read-Only

- designed for users with minimal access privileges
- Multiple users can hold this role simultaneously
- Use the MDSS functionality without the ability to make any modifications or changes to MDSS
- Provides basic monitoring and visibility into system operations

SSO Read-Only

- Designed for users with minimal access privileges
- Multiple users can hold this role simultaneously
- This role can be used when logging in via SSO

Permissions

- View the audit page to track changes and activities within the system
- Monitor the dashboard for an overview of storage activity and key metrics

SSO Administrator

- Designed for users with minimal access privileges who need scan capabilities
- Multiple users can hold this role simultaneously
- This role can be used when logging in via SSO

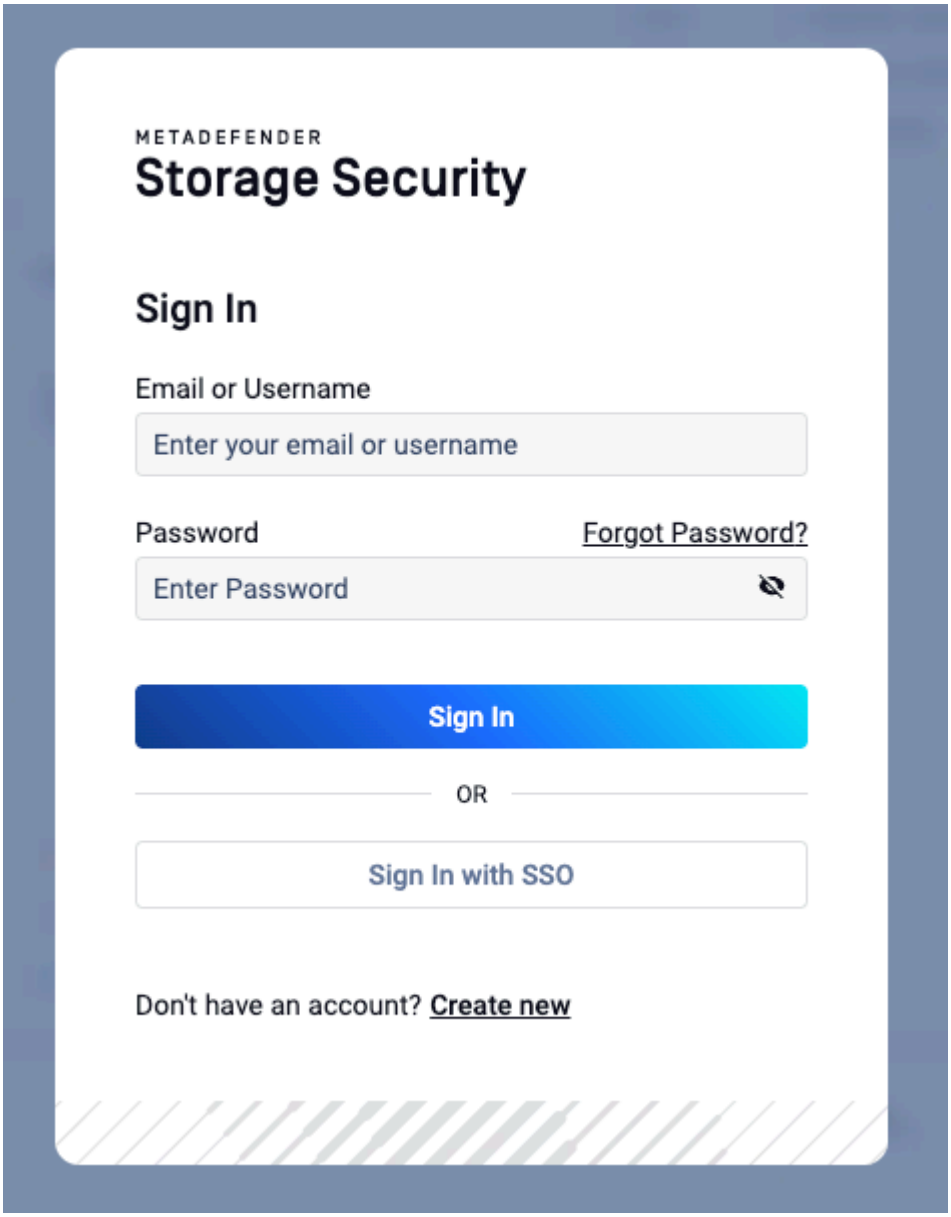
Permissions

- Add, delete, or modify Workflows
- Manage the product license settings
- Configure data retention settings
- Configure the possibility of external logging (to Kafka)
- Initiate instant, scheduled, or real-time scans on specific storage units
- Access and review generated reports for insights into scan results

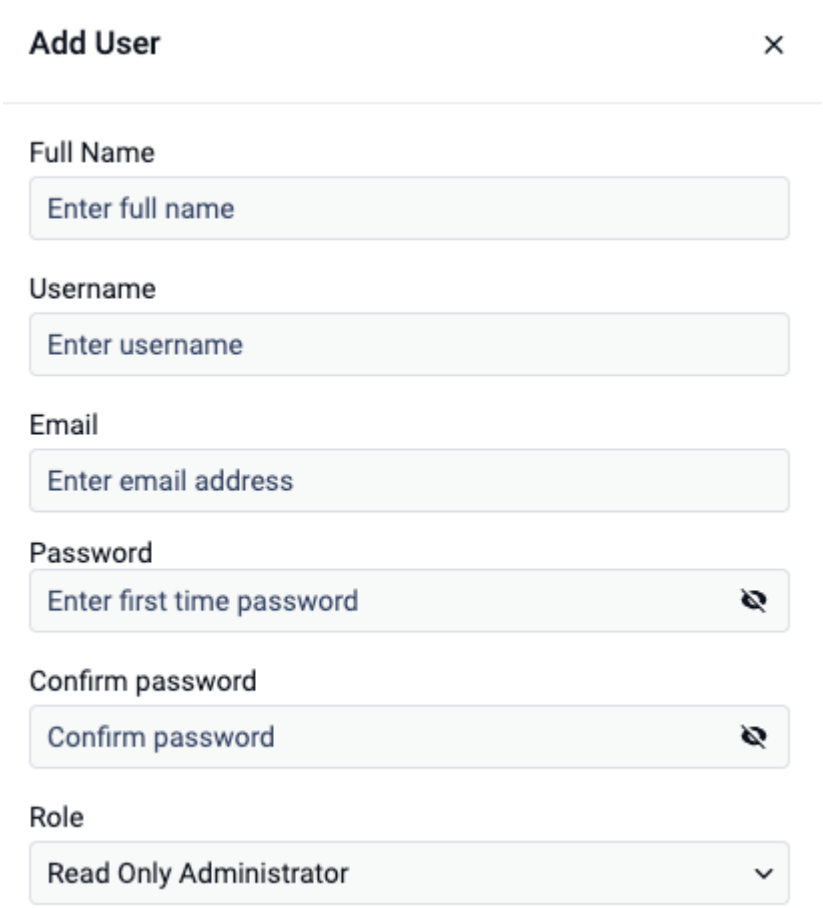
Creating New User Accounts

There are two methods to create user accounts:

- **User Self-Registration** - users can create their own accounts by clicking **Sign Up** on the web interface login page.



- **Administrator Creation** - administrators can create accounts through **Settings/Users** by clicking **Add new user** by clicking **Add new user**

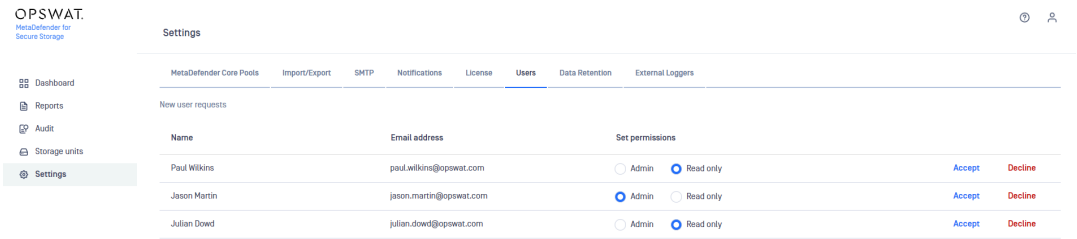


Approving or Denying User Registration Requests

When a user registers via the login page, their account is created but initially inactive. Administrators must approve these requests to grant access.

To manage registration requests:

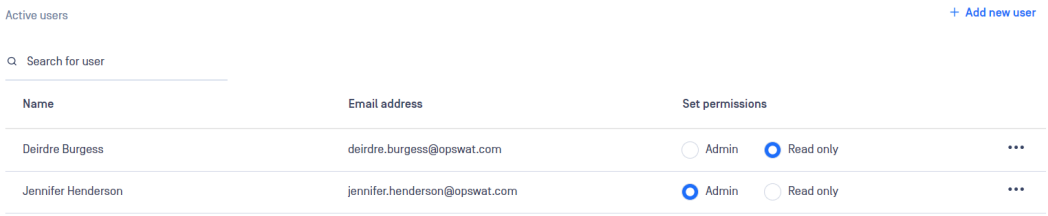
1. Navigate to Settings / Users.
2. Select the user request.
3. Choose the desired permissions for the account.
4. Click **Accept** to activate the account or **Decline** to deny access.



Modifying Permissions for Existing Users

To change the permissions of an existing user:

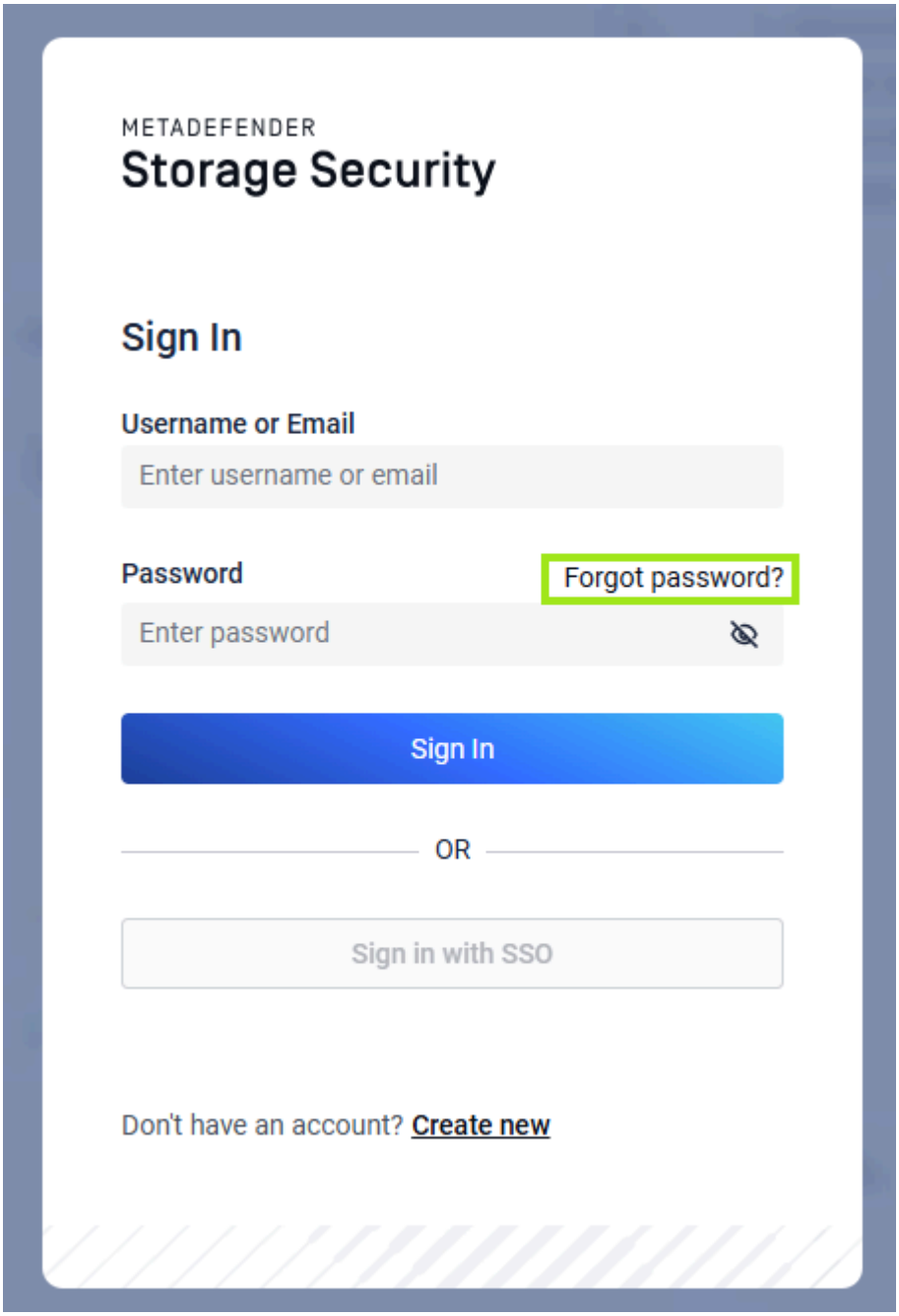
1. Navigate to Settings/Users.
2. Select the user account.
3. Choose the new permission level.



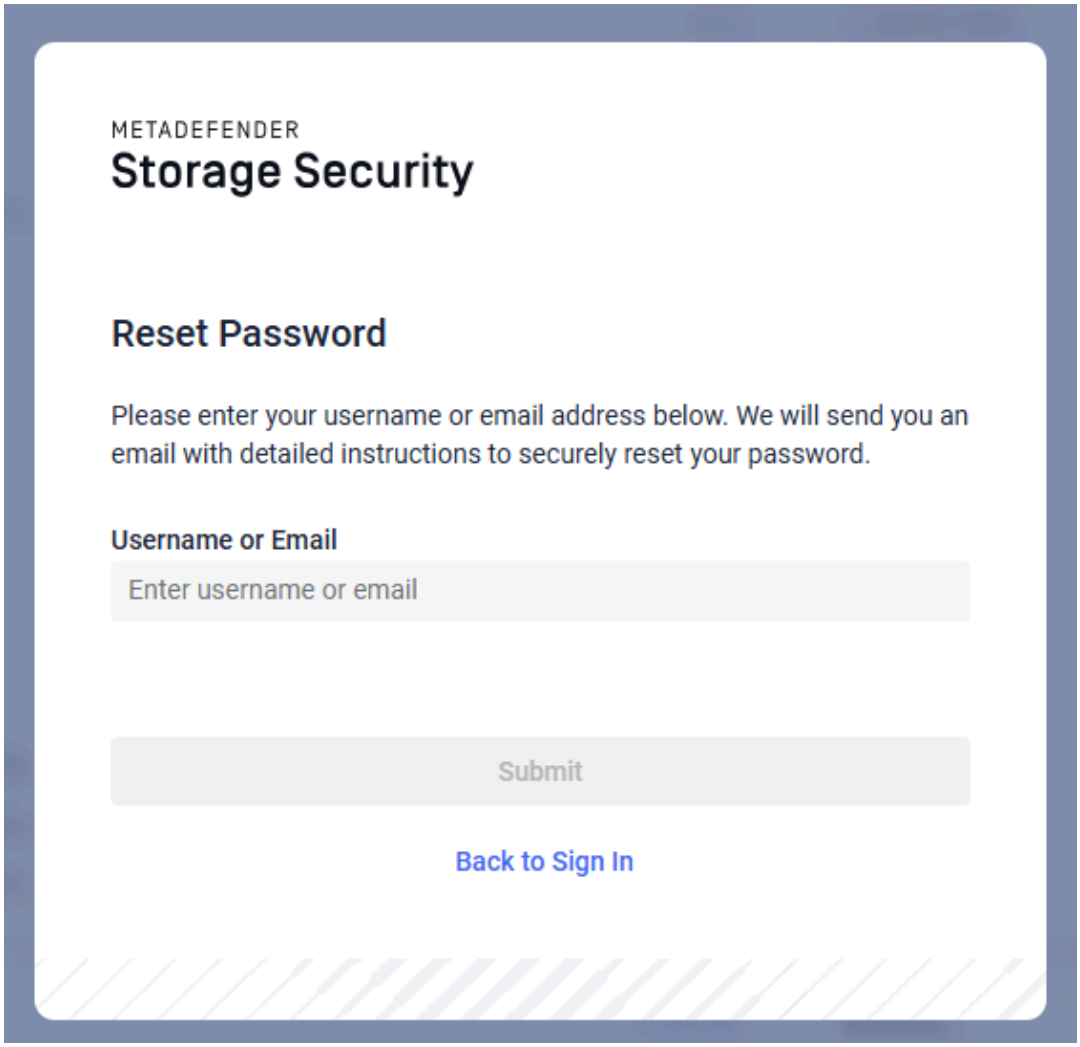
Reset/forgot password

> **INFORMATION**
>
> This functionality is available only when SMTP is configured and enabled. How to configure SMTP here

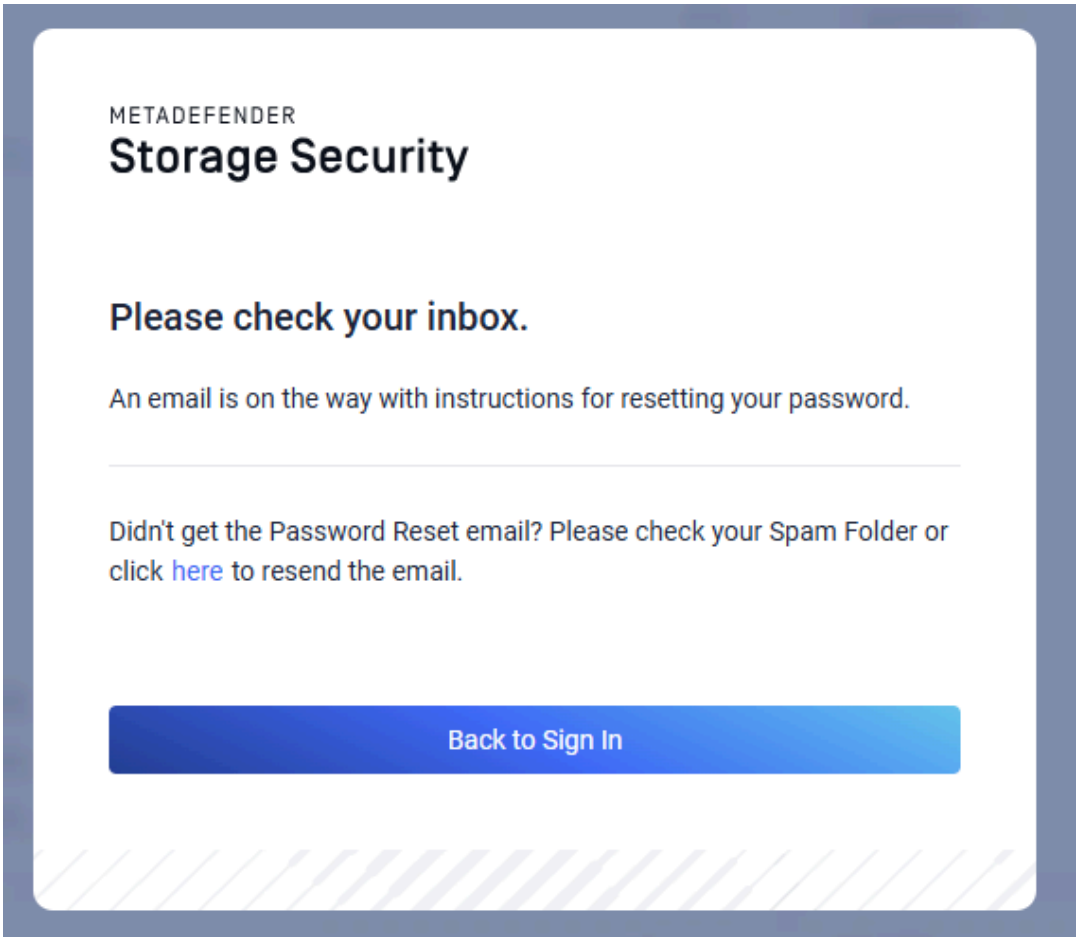
1. From the Sign in page, click on **Forgot password?**



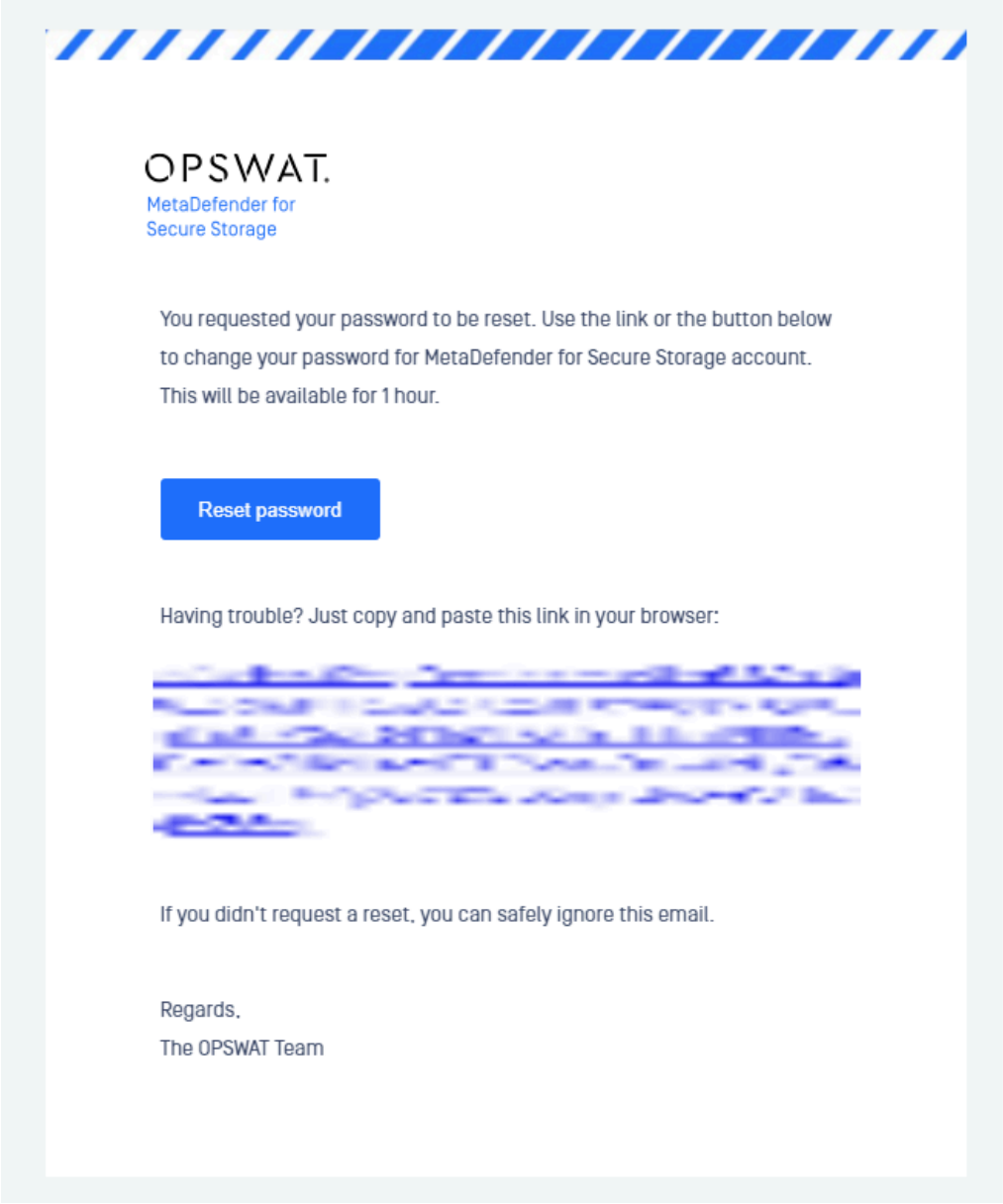
2. This will redirect you to a page where you can provide either the **username** or the **email address** associated with the account you want to change the password for. To continue, please click **Submit**.



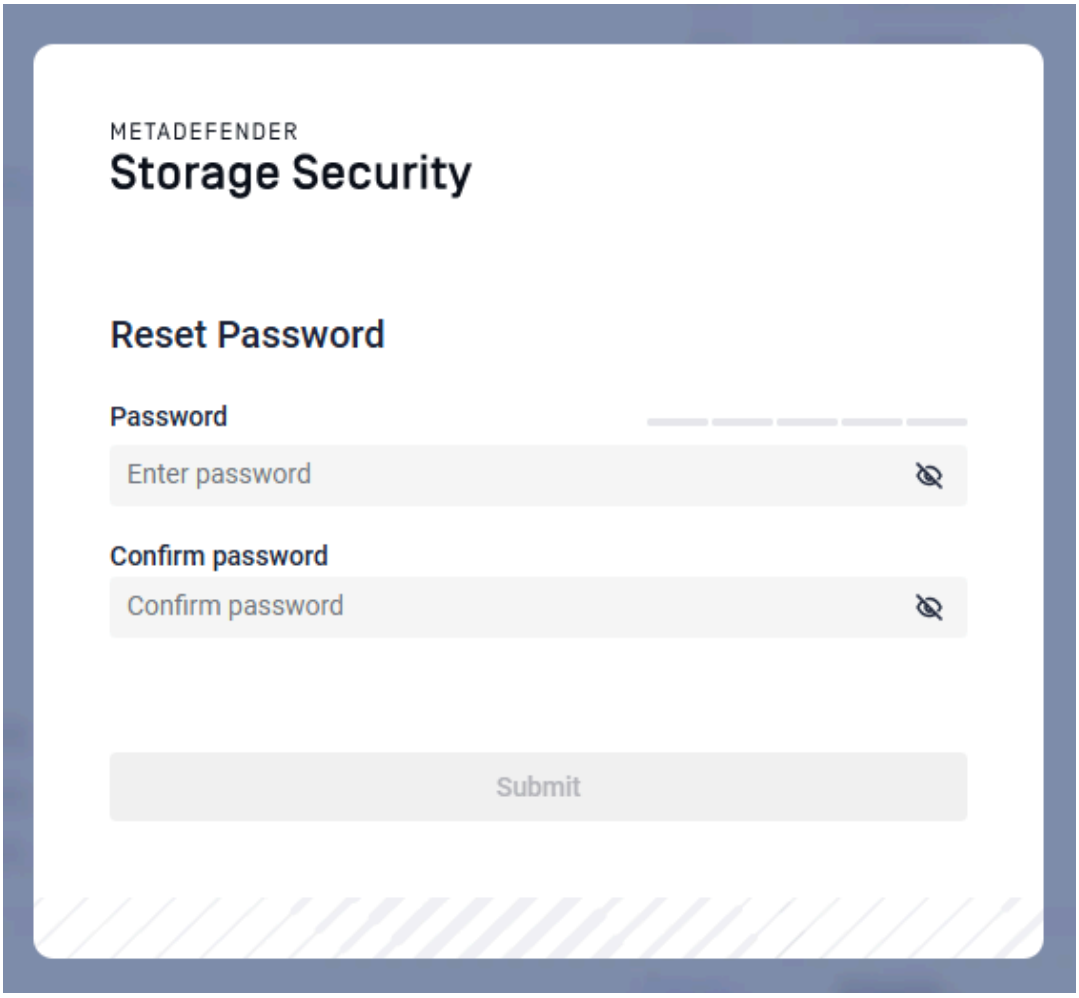
3. If the request is successful, an informative message will appear on the screen.



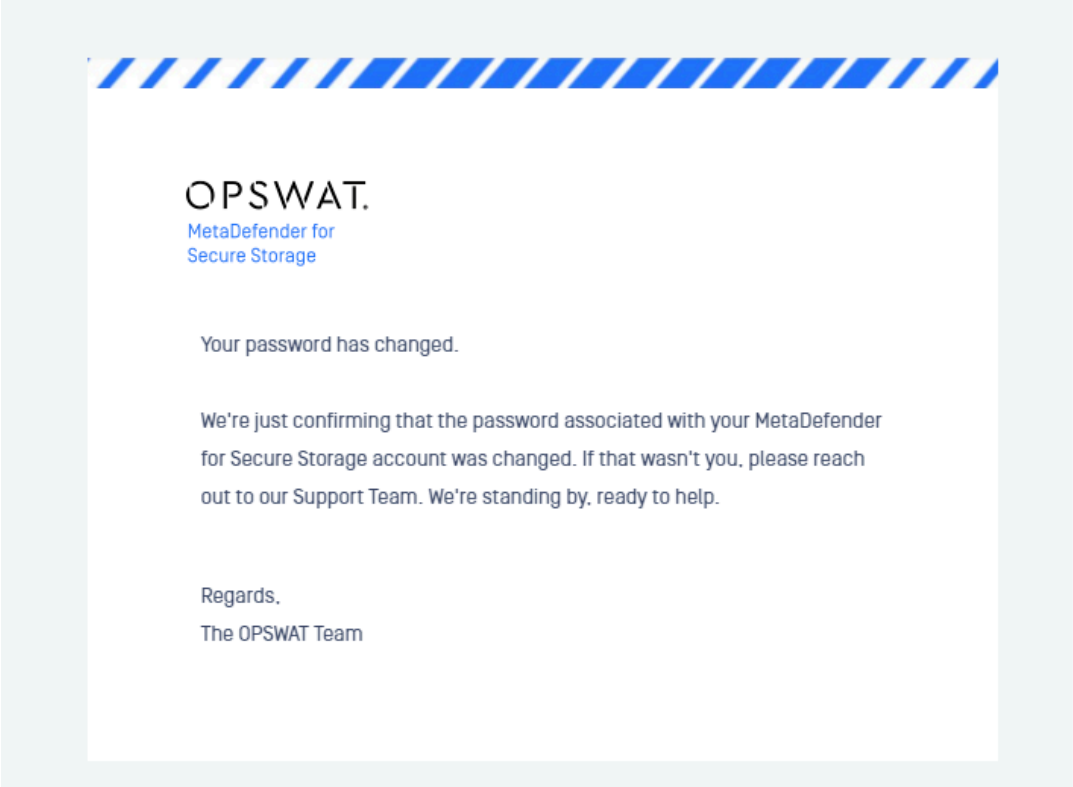
4. An email will be sent to the email address associated with the account. By clicking on the **Reset password** button or directly on the link, you will be redirected to a new tab in browser to continue with the password reset.



5. In the new tab, you are asked to provide the new password and to confirm it. Please click on **Submit** to finish the password reset.

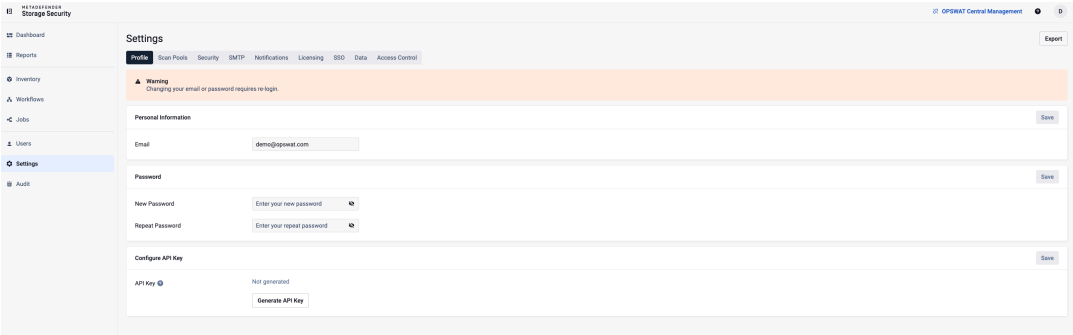


6. After resetting the password, you will be redirected to the login page and a confirmation email will be sent to your email address.



Change your account information

Navigate to **Settings** tab -> **Profile**.



Change password

1. Please enter the current password associated with the account.
2. After validating it, you will be allowed to provide the new password and to confirm it.
3. To finish changing the password, please click on **Update password**.

Change email

1. Please enter the current password associated with the account.
2. After validating it, you will be allowed to provide a new email address.

3. To finish changing the email, please click on **Update email**.

Change full name

1. Provide the new full name you wish to use for the account.
2. To finish changing the full name, please click on **Update full name**.

Generate API Key

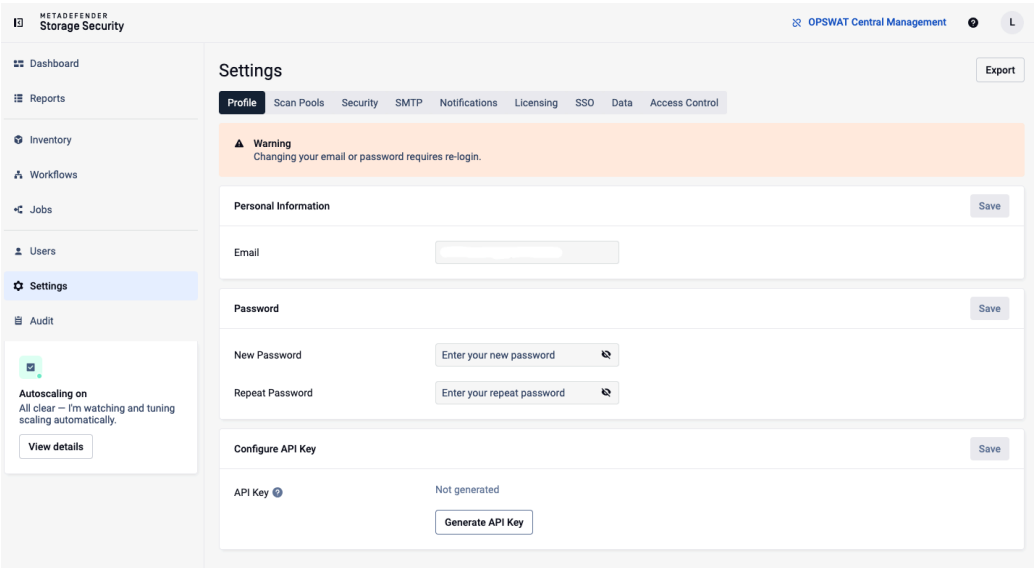
1. Click on **Generate API Key** button
2. Copy the generated API Key
3. Click on **Save** button

Generate an API Key

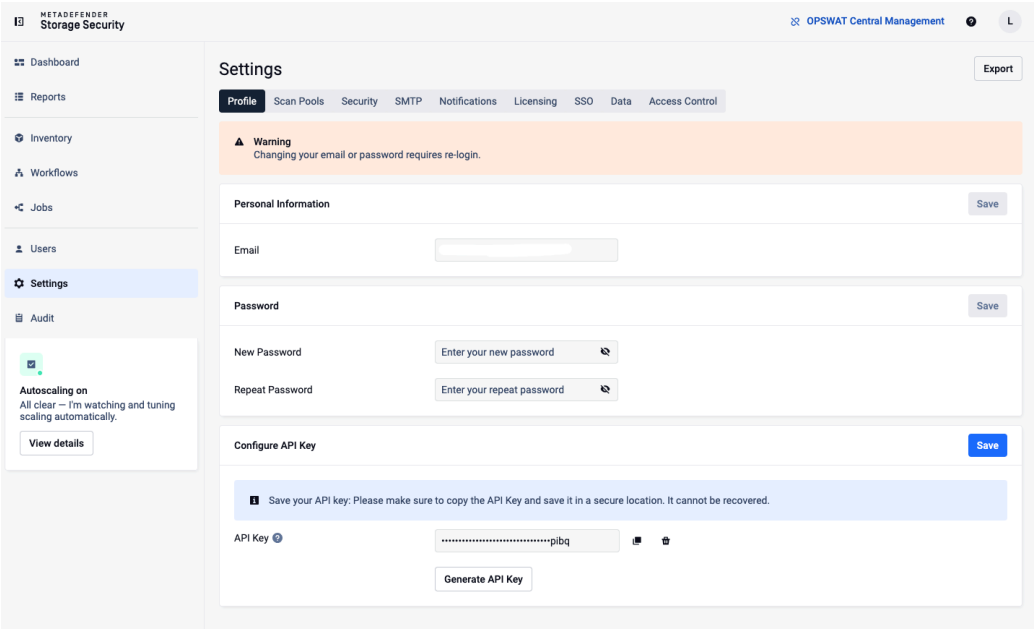
MetaDefender Storage Security users can generate **one API Key** for their user account. This key can be used as an alternative method to authenticate REST API requests to MetaDefender Storage Security — with the exception of user and API key management operations.

To generate an API key, follow these steps:

1. Navigate to **Settings** tab -> **Profile**

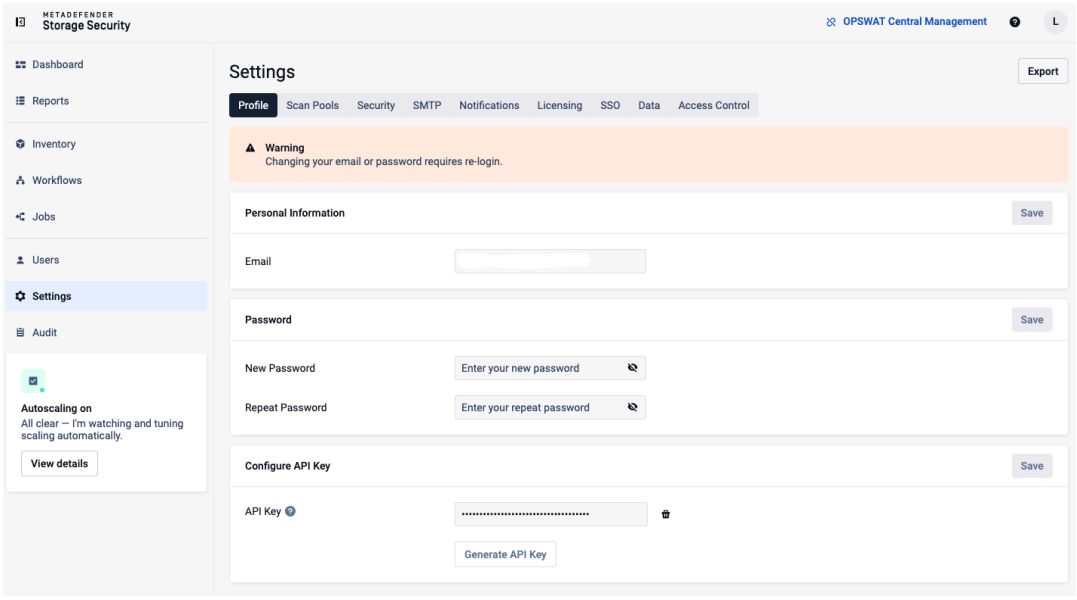


2. Select **Generate API Key**



3. Click the copy button and store your API Key somewhere secure. Afterwards, click on **Save**.

> **Information**
>
> The API key can be copied only at this step and is saved only after clicking the save changes button. If an API Key already exists, it can be deleted or updated to a freshly generated one.



> **Warning**
>
> API keys of a user are invalidated on a password change or reset operation.

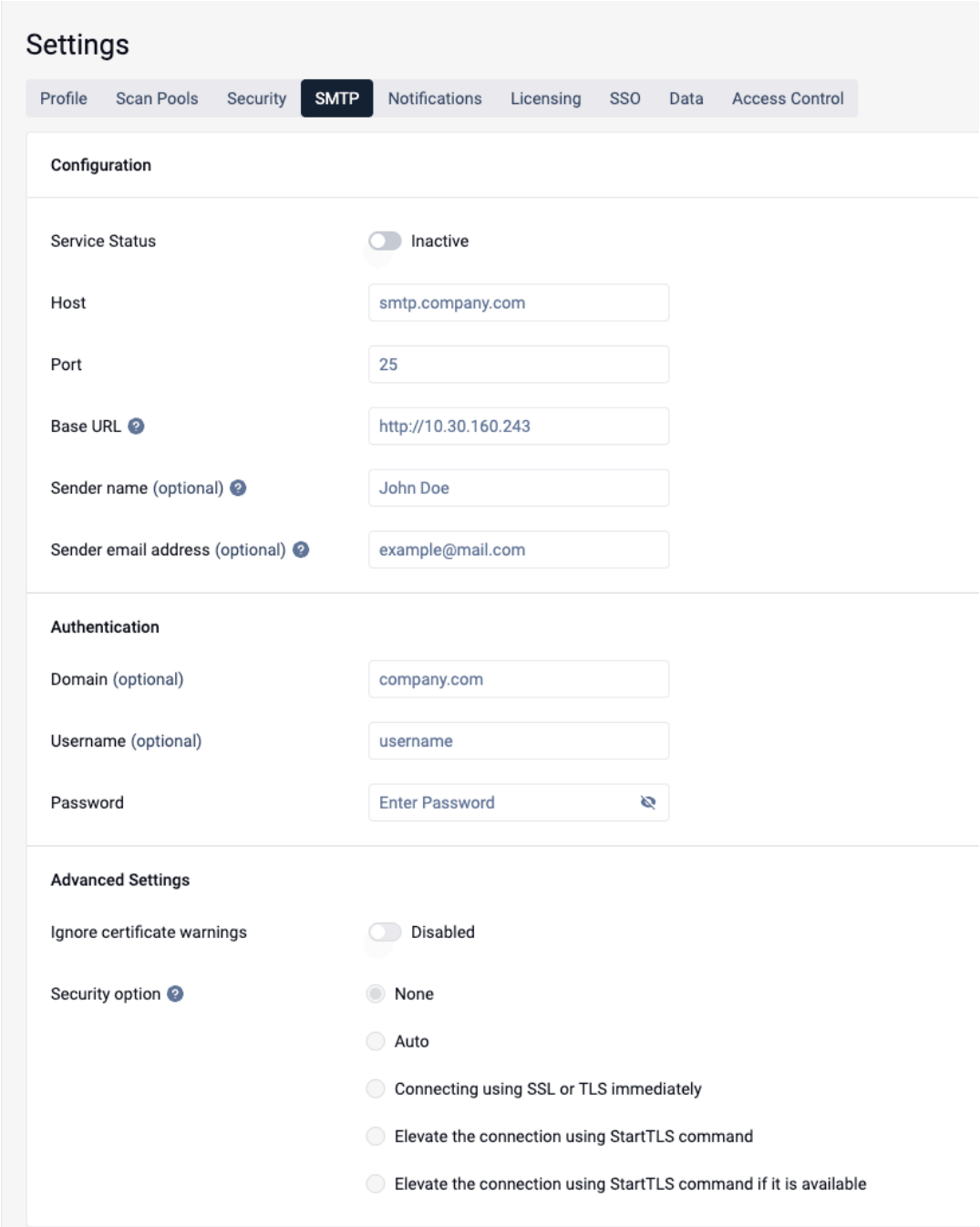
Warning

The following operations are not allowed using an API key:

- Generate an API key: **GET /api/apikey/generate**
- Retrieve an API key: **GET /api/apikey**
- Add an API key: **POST /api/apikey**
- Update an API key: **PUT /api/apikey**
- Delete an API key: **DELETE /api/apikey/{id}**
- Enumerate active users: **GET /api/user/active/{startIndex}/{count}**
- Create an user: **POST /api/user/create**
- Update user role: **PUT /api/user/role**
- Enumerate user requests: **GET /api/user/requests**
- Remove a user: **DELETE /api/user/{userId}**
- Update user: **PUT /api/user**
- Validate password: **POST /api/user/validation**

SMTP

In order to generate email reports, MetaDefender Storage Security needs to connect to an SMTP server. To configure this integration, please go to **Settings → SMTP**.



Setup the integration

1. Enable SMTP by clicking the toggle
2. Input the **Host** address of your SMTP server (i.e smtp.company.com)

3. Input the **Port** of your SMTP server
4. **Base URL**: the address to use in the email for links; this address should point to the MetaDefender Storage Security web interface
5. **Sender Email Address:** email address to be used as *From:* field when sending notifications (**Note:** if left empty, we will use the default email address: *mdss@opswat.com*)
6. **Sender Name**: display name to be used as *From Name:* field when sending notifications (**Note:** if left empty, we will use the default sender name: *MetaDefender Storage Security*)
7. (Optionally) Input a **domain, username,** and **password** if your SMTP requires authentication
    1. You can leave these fields empty if your SMTP server does not require authentication
    2. You can leave the domain empty if your SMTP provider requires only a username and a password
8. Advanced Settings
    1. **Security option:** provides a way of specifying the SSL and/or TLS encryption that should be used for a connection. Please select one of the following options (**Note:** default option is None)
        1. **None:** No SSL or TLS encryption should be used
        2. **Auto:** Allow the system to decide which SSL or TLS options to use (default). If the server does not support SSL or TLS, then the connection will continue without any encryption
        3. **Connect using SSL or TLS immediately:** The connection should use SSL or TLS encryption immediately
        4. **Elevate the connection using StartTLS command:** Elevates the connection to use TLS encryption immediately after reading the greeting and capabilities of the server. If the server does not support the STARTTLS extension, then the connection will fail
        5. **Elevate the connection using StartTLS command if it is available:** Elevates the connection to use TLS encryption immediately after reading the greeting and capabilities of the server, but only if the server supports the STARTTLS extension
    2. **Ignore Certificate Warnings:** select this option if your SMTP does not have a valid certificate but wish to use SSL
9. **Save** your settings when you are done.

> **Info**

> In order to test the configuration, MetaDefender Storage Security will attempt to send a test email using the email address of the currently logged-in user. Please make sure that your account has a valid email configured.

License

A MetaDefender Storage Security license contains the following fields

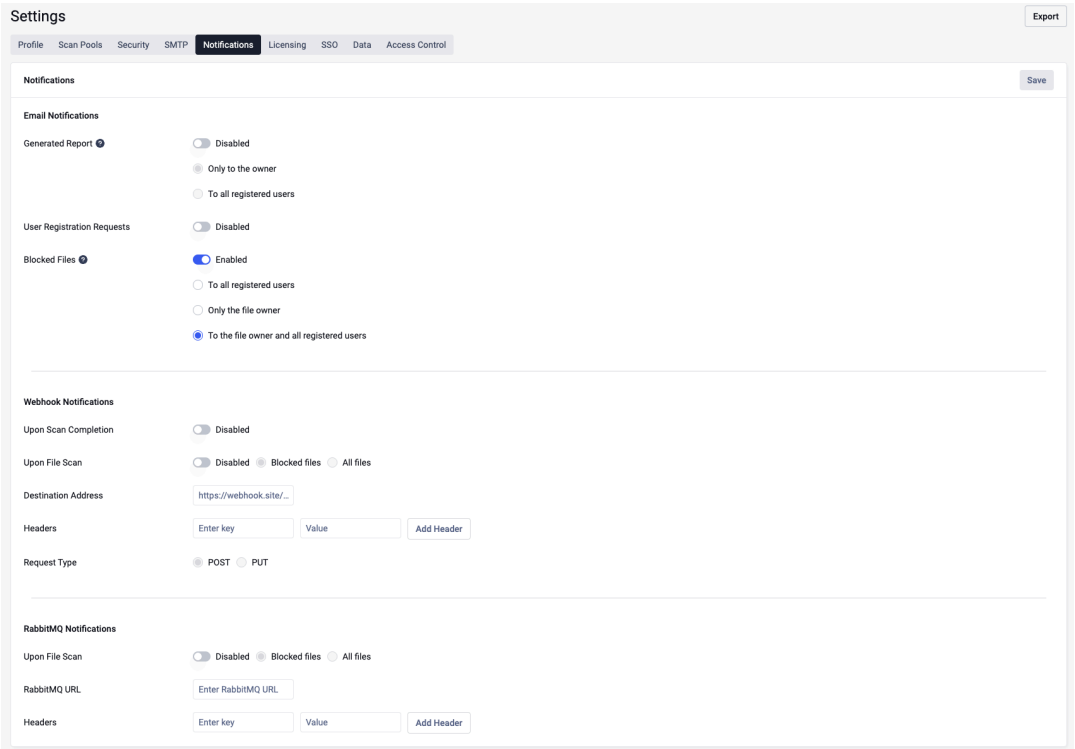
Field	Description
Deployment ID	A uniquely generated value that identifies your deployment.
Product ID	A unique product identifier
Expiration Date	The date until your license is valid
Name	The name of the license
Activation Key	The key with which the license is activated

Notifications

> **Info**
>
> In order to send email notifications, make sure that an SMTP server is available. Please see SMTP for more details.

To enable notifications follow these steps:

1. Navigate to **Settings -> Notifications**
2. Choose the event for which you wish to receive notifications. There are two types of notifications, each having different possible configurations:
    1. Email notifications, which can be sent:
        1. When a report is generated. Please see Email reports.
        2. When a user registration request is pending an administrator approval
        3. When a file is blocked while processing a storage. Please see Blocked file notifications.
    2. Webhook notifications, which can be sent:
        1. When a scan is completed. Please see Scan completed Notifications
        2. When a file is completed. Please see File scanned Notifications
    3. RabbitMQ notification which can be sent when a file is completed. Please see File scanned RabbitMQ Notifications

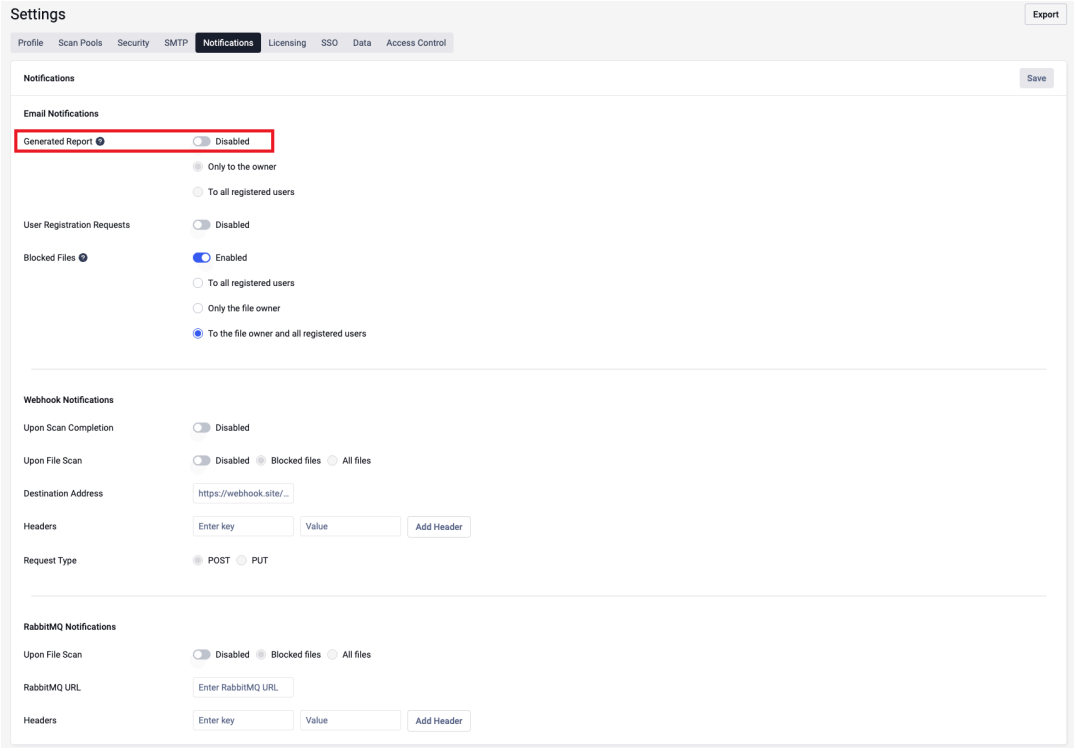


Email reports

Email reports can be generated after a storage process completes. The report contains vital information about multi-scanning results, potential compliance violations as well as detected vulnerabilities or other issues.

You can choose to send the email report:

- Only to the owner - the user that started the process
- All registered users - all MetaDefender Storage Security users



An email report contains the following information:

- A list of Top Risk Files
- An overview of the report
- Engine versions for Deep CDR and Vulnerability engine
- Details engine information for multi-scanning engines

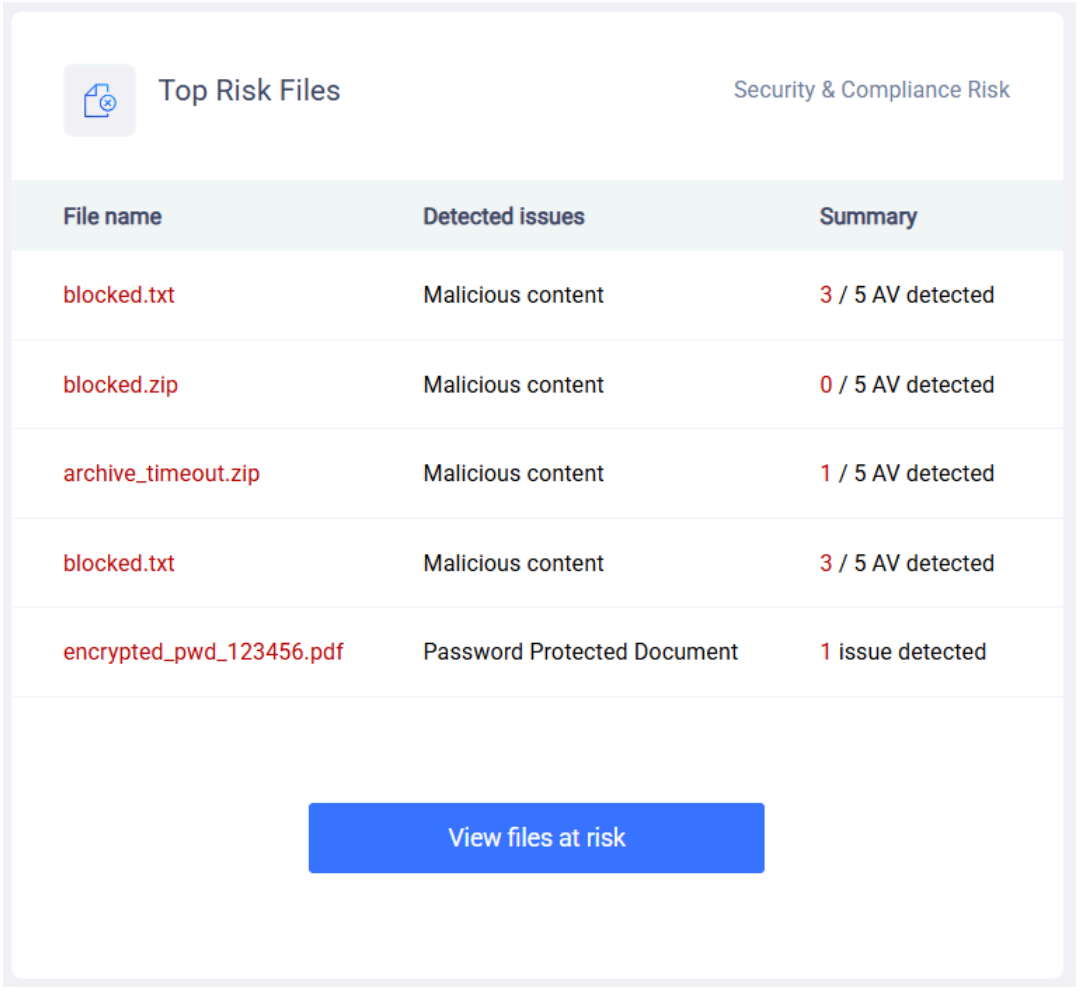
OPSWAT.
MetaDefender
Storage Security

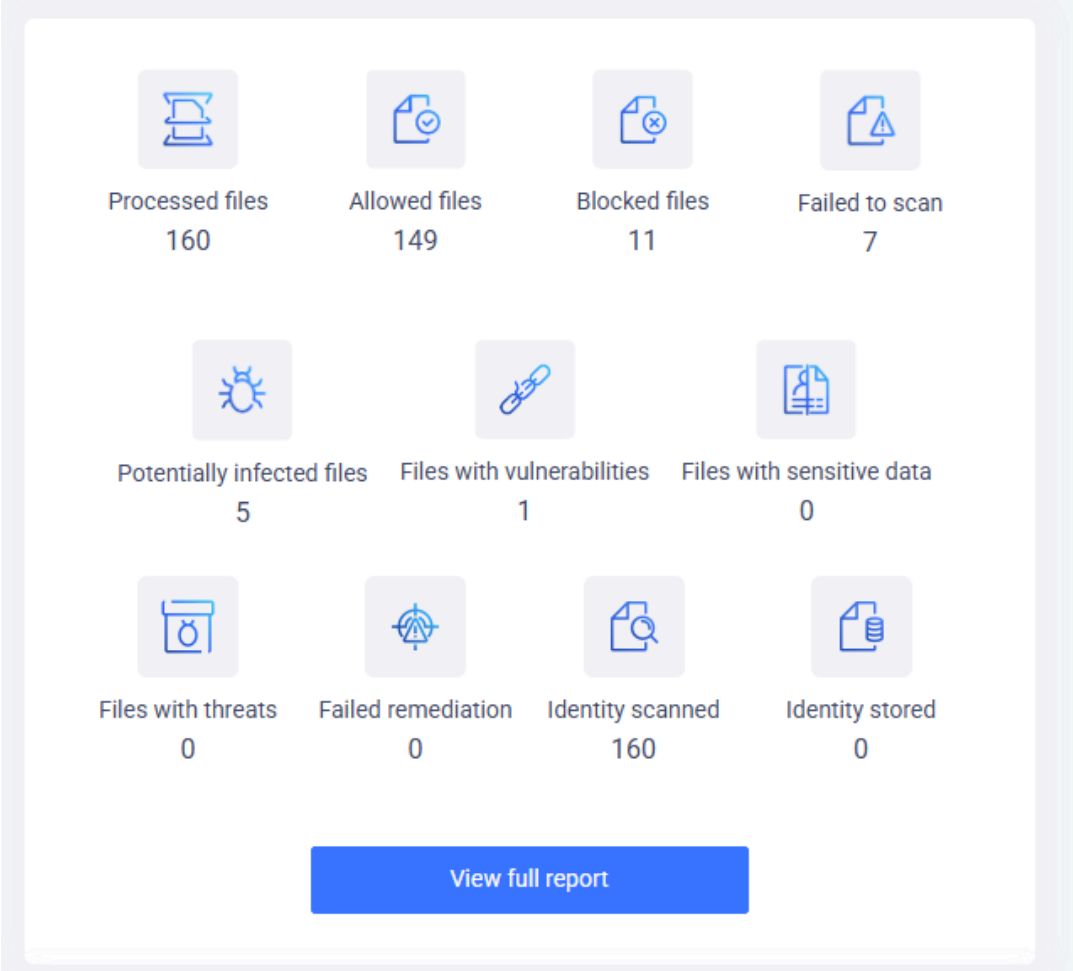
Report generated
Aug 5, 2026 10:48 UTC

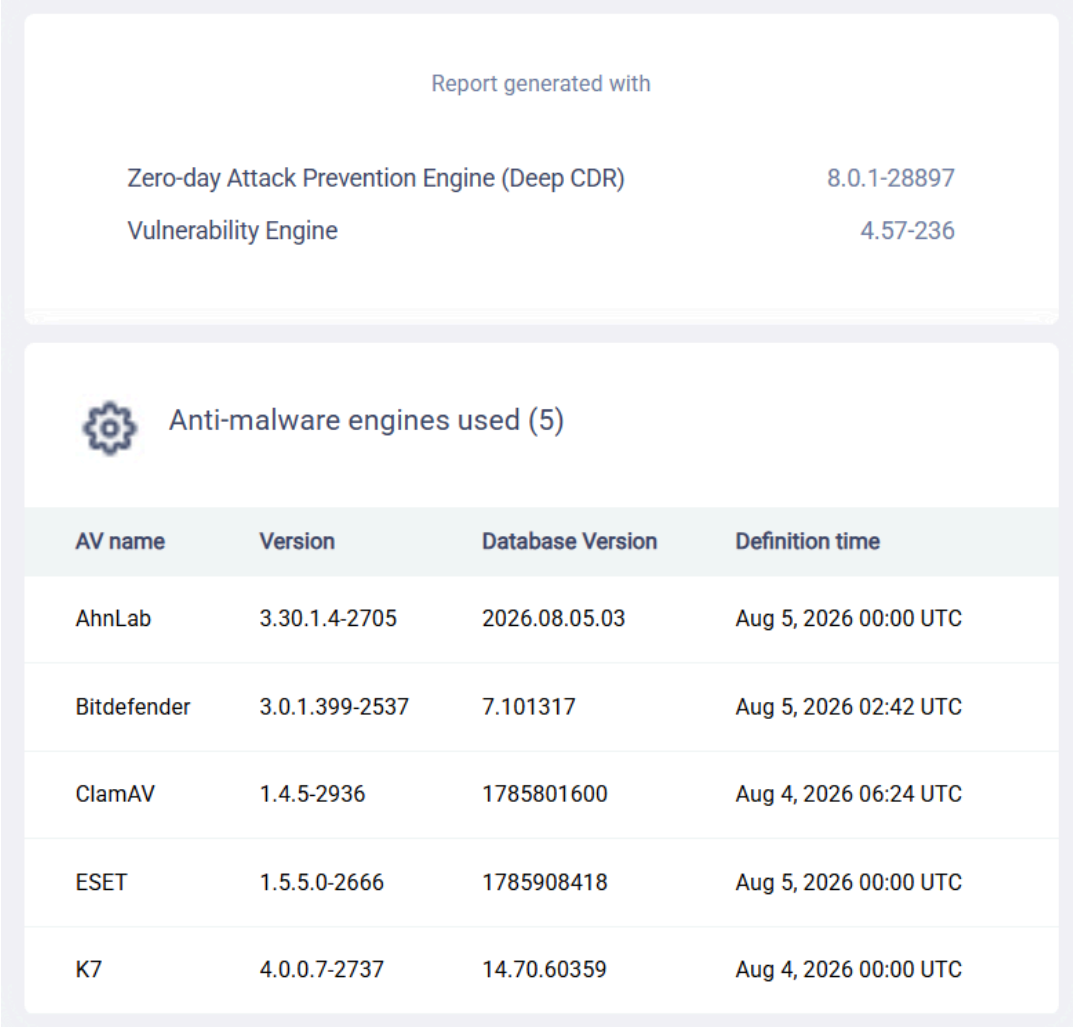
Protecting storage **Automation Library**
Scan name **OnDemand-2026_08_05_13_47_30**
Workflow Used **Default Workflow**

Type	Status
Instant	Completed

Start Time	Stop Time	Duration
Aug 5, 2026 10:47 UTC	Aug 5, 2026 10:48 UTC	0d 00h 00m 44s


Top Risk Files
Security & Compliance Risk
File name
Detected issues
Summary
blocked.txt
Malicious content
3 / 5 AV detected
blocked.zip
Malicious content
0 / 5 AV detected
archive_timeout.zip
Malicious content
1 / 5 AV detected
blocked.txt
Malicious content
3 / 5 AV detected
encrypted_pwd_123456.pdf
Password Protected Document
1 issue detected
View files at risk


Processed files
160
Allowed files
149
Blocked files
11
Failed to scan
7
Potentially infected files
5
Files with vulnerabilities
1
Files with sensitive data
0
Files with threats
0
Failed remediation
0
Identity scanned
160
Identity stored
0
View full report



Report generated with

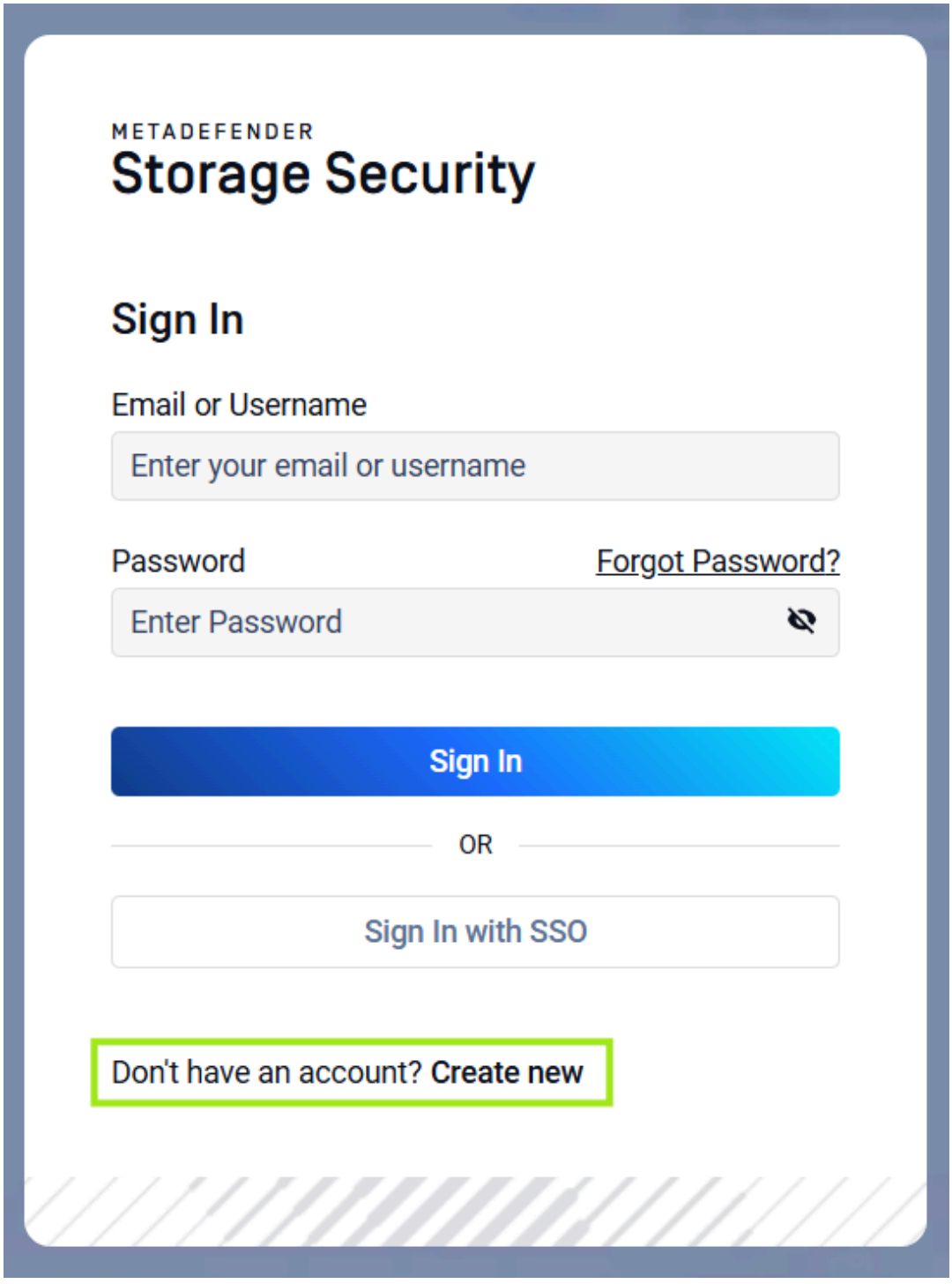
Zero-day Attack Prevention Engine (Deep CDR)	8.0.1-28897
Vulnerability Engine	4.57-236

Anti-malware engines used (5)

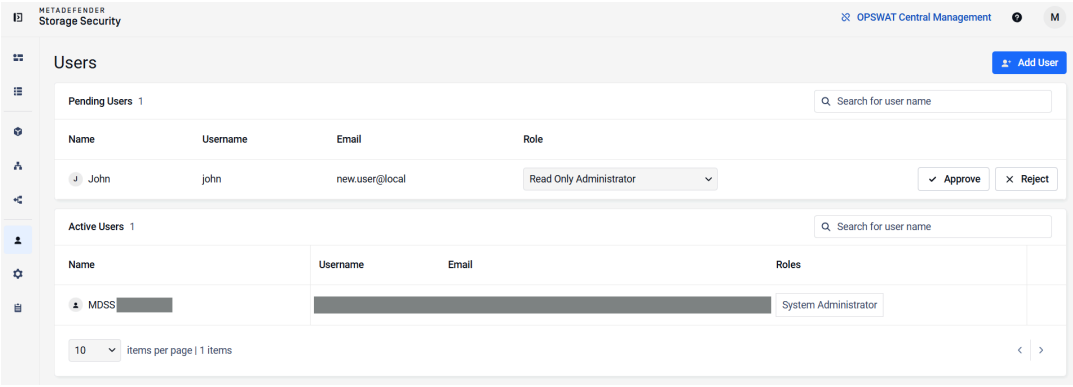
AV name	Version	Database Version	Definition time
AhnLab	3.30.1.4-2705	2026.08.05.03	Aug 5, 2026 00:00 UTC
Bitdefender	3.0.1.399-2537	7.101317	Aug 5, 2026 02:42 UTC
ClamAV	1.4.5-2936	1785801600	Aug 4, 2026 06:24 UTC
ESET	1.5.5.0-2666	1785908418	Aug 5, 2026 00:00 UTC
K7	4.0.0.7-2737	14.70.60359	Aug 4, 2026 00:00 UTC

User registration request notifications

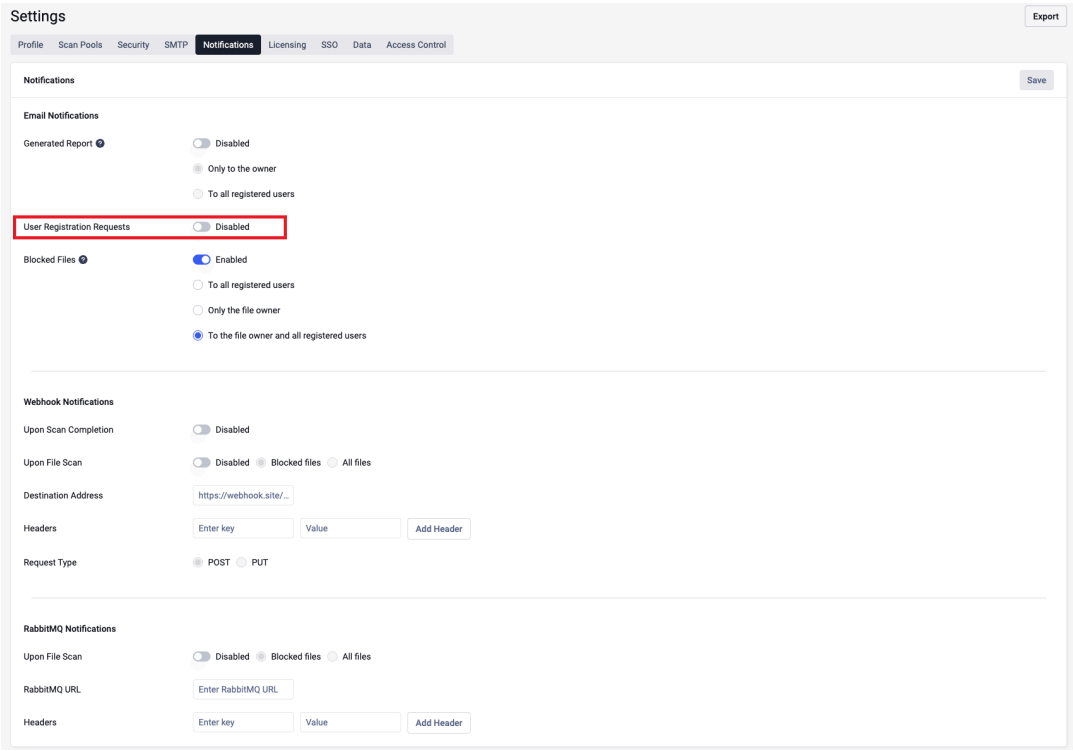
New users can attempt to register accounts from the login page:



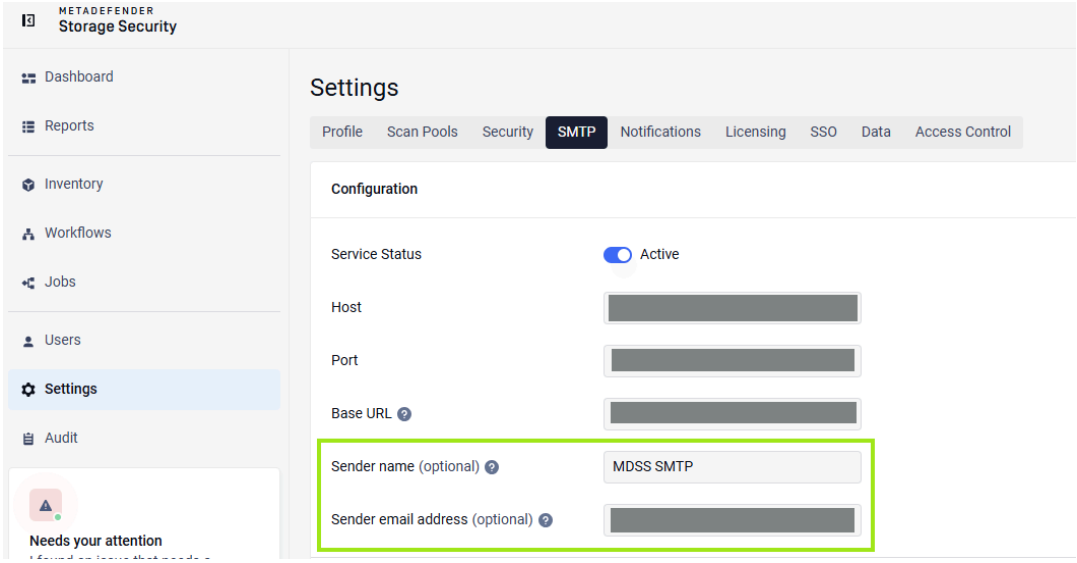
These registration requests need to be verified and approve by MDSS System Administrators.



To enable notifications for user registration requests, please select the **User Registration Requests** option from the **Email Notifications** section:

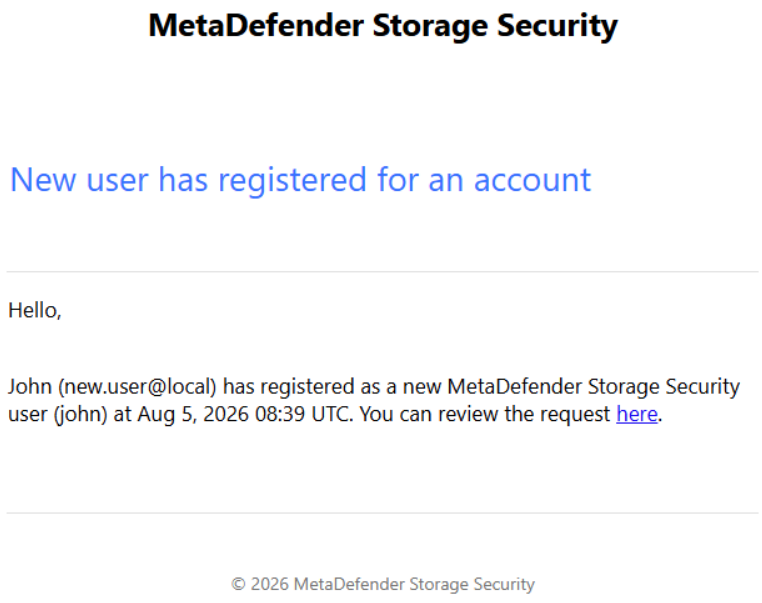


> Always triple check the sender of the email before trusting ANY links.



The email contains the following information:

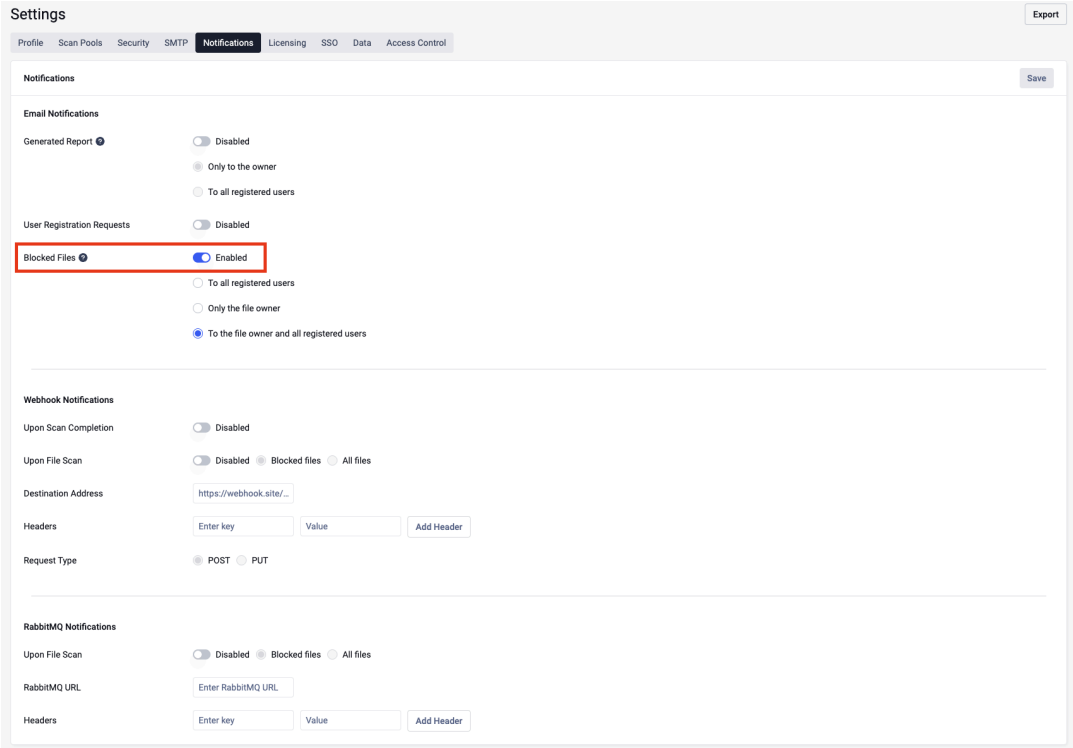
- Full Name of of registered user
- Email address of registered user
- Date of registration
- Link to the MDSS instance's Users tab



Blocked file notifications

Blocked files notifications are sent for each blocked file that is found during an Instant, Scheduled or Real-Time processing.

To enable notifications for blocked file, select the option to **Blocked Files** from the **Email Notifications **section:



You can choose to send this email to:

- All MetaDefender Storage Security registered users
- Only to the file owner
- To the file owner and all MetaDefender Storage Security registered users

> **Info**
>
> Please note that the notification to the file owner could be sent only for OneDrive, Box and MFT integrations.

The email contains the following information:

- File name
- File path
- Storage unit type and name
- The reason why the file is blocked

- Remediation actions details (delete/move blocked files), when these are configured for the storage that is processed



OPSWAT.
MetaDefender for
Secure Storage

Hello,

The file [redacted] has been blocked while scanning the S3 Compatible storage (Storage Name [redacted]), for the following reason: Sensitive Data Found.

The file has been moved due to remediation configured for the S3 Compatible storage (Storage Name: [redacted]) to: Box storage (Storage Name: [redacted]).

Regards,
The OPSWAT Team

Scan completed notifications

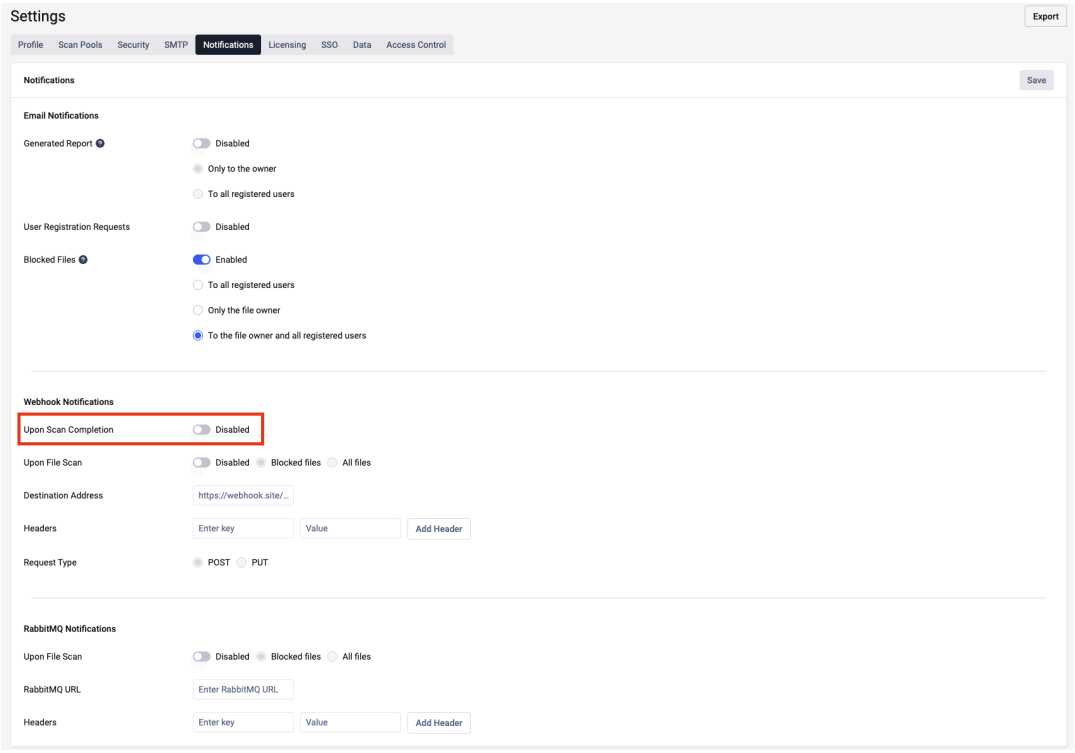
Overview

Scan Completed webhook notifications allow you to receive real-time alerts whenever an Instant or Scheduled scan has finished running in MetaDefender Storage Security. This feature is useful if you need to:

- Track the completion status of scans for auditing and compliance.
- Monitor whether scans succeed, fail, or are cancelled.
- Integrate scan lifecycle events into external systems (e.g., scheduling dashboards, reporting tools, SIEM).
- Trigger automated follow-up processes once a scan has completed.

Setup

1. Go to **Settings > Notifications** in the MetaDefender Storage Security console.
2. Select **Upon Scan Completion** under the **Webhook Notifications** section.
3. Enter the **Destination Address** (your endpoint).
4. Select the **Request Type** (**POST** or **PUT**).
5. (Optional) Add any custom **HTTP headers**.
6. Save the configuration.



Configuration Details

- **Destination address** – The URL of the receiving system (must accept HTTP requests).
- **Request type** – Either `POST` or `PUT`.
- **Headers** – Optional key-value pairs (e.g., `Authorization: Bearer <token>`).

Webhook Payload

When triggered, the webhook sends a JSON request body to your configured endpoint.

```
{
   "ScanId":"01987f90-870a-7826-9115-18d96a1a4ae0",
   "ScanName":"second-scan",
   "StartTime":"2025-08-06T13:27:14.953181Z",
   "StopTime":"2025-08-06T13:27:20.12684Z",
   "Status":"Completed",
   "WebhookNotificationType": "ScanCompleted"
}
```


Field Reference

Field	Type	Example Value	Description
`ScanId`	string(UUID)	`01987f90-870a-7826-9115-18d96a1a4ae0`	Unique identifier of the scan.
`ScanName`	string	`second-scan`	Name of the scan as configured.
`StartTime`	datetime (UTC)	`2025-08-06T13:27:14.953181Z`	Time the scan started.
`StopTime`	datetime (UTC)	`2025-08-06T13:27:20.12684Z`	Time the scan finished.
`Status`	string	`Completed` /`Cancelled` /`Failed`	Final status of the scan.
`WebhookNotificationType`	string	`ScanCompleted`	Identifies the notification type.

Delivery Behavior

- Webhooks are delivered as standard HTTP requests.
- Delivery is **best-effort** → if the destination is invalid, the request is logged in the **Audit page**, but no retries are performed.
- Payload size is small (JSON only, no scan contents).

Security Considerations

- Configure HTTPS endpoints to ensure data is transmitted securely.
- Use authentication headers (e.g., API tokens) to protect your webhook endpoint.

- Ensure your endpoint validates payloads before processing.

Troubleshooting

- **No webhook received** → Verify the endpoint URL and request type (POST/PUT).
- **Audit shows delivery failed** → Endpoint is invalid or unreachable. Fix and test again.
- **Authentication errors** → Confirm your endpoint accepts the headers you configured.

File scanned notifications

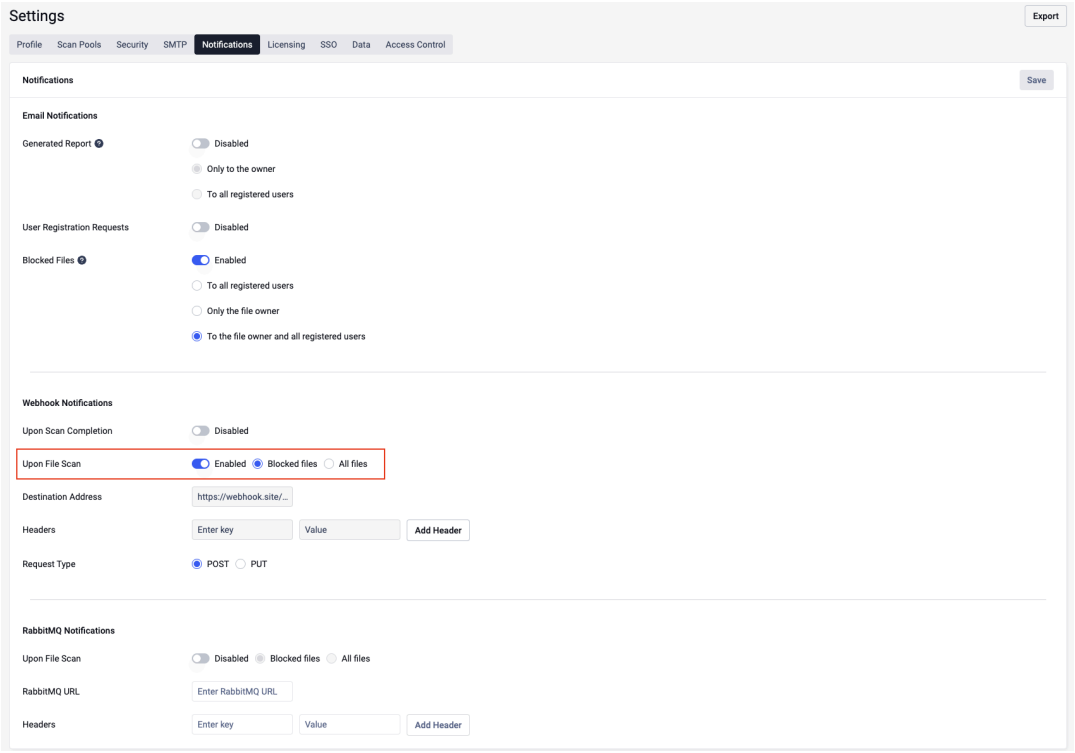
Overview

File Scanned webhook notifications allow you to receive real-time alerts whenever a file has been scanned by MetaDefender Storage Security. This feature is useful if you need to:

- Track the outcome of file scans for auditing or compliance.
- Integrate scan results into external systems (e.g., ticketing, alerting, SIEM).
- Trigger automated workflows based on file status (e.g., quarantine, user notification).

Setup

1. Go to **Settings > Notifications** in the MetaDefender Storage Security console.
2. Select **Upon File Scan** under the **Webhook Notifications** section
3. Choose whether you want to receive notifications for **all scanned files** or **only blocked files**.
4. Enter the **Destination Address** (your endpoint).
5. Select the **Request Type** (**POST** or **PUT**).
6. (Optional) Add any custom **HTTP headers**.
7. Save the configuration.



Configuration Details

- **Destination address** – The URL of the receiving system (must accept HTTP requests).
- **Request type** – Either `POST` or `PUT`.
- **Headers** – Optional key-value pairs (e.g., `Authorization: Bearer <token>`).
- **Notification scope** – Choose between:
  - **All scanned files** → You will receive a notification for every file scanned.
  - **Blocked only** → You will only receive notifications when a file is marked as blocked in MetaDefender Storage Security (see File Definition)

Webhook Payload

When triggered, the webhook sends a JSON request body to your configured endpoint.

```
{
  "FileId": "0198f02f-ed4d-7c0d-8668-1036d322209c",
  "FileName": "file.txt",
  "FilePath": "folder/file.txt",
  "FileStatus": "Allowed",
  "CoreScanResult": "No Threat Detected",
  "FileState": "Available",
  "RemediationResult": [
    "AllowedKept: Applied"
  ],
  "ScanCompletedTimeStamp": "2025-08-28T10:20:24.974998Z",
  "WorkflowName": "Default Workflow",
  "Rules": [
    "MetaDefender Storage Security"
  ],
  "ExceptionDetails": "",
  "RemediationErrors": [],
  "WebhookNotificationType": "FileScanned"
}
```

Field Reference

Field	Type	Example Value	Description
`FileId`	string (UUID)	`0198f02f-ed4d-7c0d-8668-1036d322209c`	Unique identifier of the file.
`FileName`	string	`file.txt`	Original file name.
`FilePath`	string	`folder/file.txt`	File's relative path.
`FileStatus`	string	`Allowed/Blocked`	File status based on MDSS file definitions
`CoreScanResult`	string	`No Threat Detected`	Result from Scan instance.
`FileState`	string	`Failed/Canceled/FailedRemediation/Available`	File status in MDSS.
`RemediationResult`	array[string]	`["AllowedKept:Applied"]`	Array of remediations applied and their result
`ScanCompletedTimeStamp`	datetime (UTC)	`2025-08-28T10:20:24.974998Z`	Time when scan completed.
`WorkflowName`	string	`Default Workflow`	Name of the workflow used.
`Rules`	array[string]	`["MetaDefender Storage Security"]`	Workflow rules applied.
`ExceptionDetails`	string	""	Details of any exceptions during scan.
`RemediationErrors`	array[string]	`[]`	Errors during remediation, if any.
`WebhookNotificationType`	string	`FileScanned`	Identifies the notification type.

Delivery Behavior

- Webhooks are delivered as standard HTTP requests.
- Delivery is **best-effort** → if the destination is invalid, the request is logged in the **Audit page**, but **no retries** are performed.
- Payload size is typically small (JSON only, no file contents).

Security Considerations

- Configure HTTPS endpoints to ensure data is transmitted securely.
- Use authentication headers (e.g., API tokens) to protect your webhook endpoint.
- Ensure your endpoint validates payloads before processing.

Troubleshooting

- **No webhook received** → Verify the endpoint URL and request type (POST/PUT).
- **Audit shows delivery failed** → Endpoint is invalid. Fix and test again.
- **Authentication errors** → Confirm your endpoint accepts the headers you configured.

File scanned RabbitMQ notifications

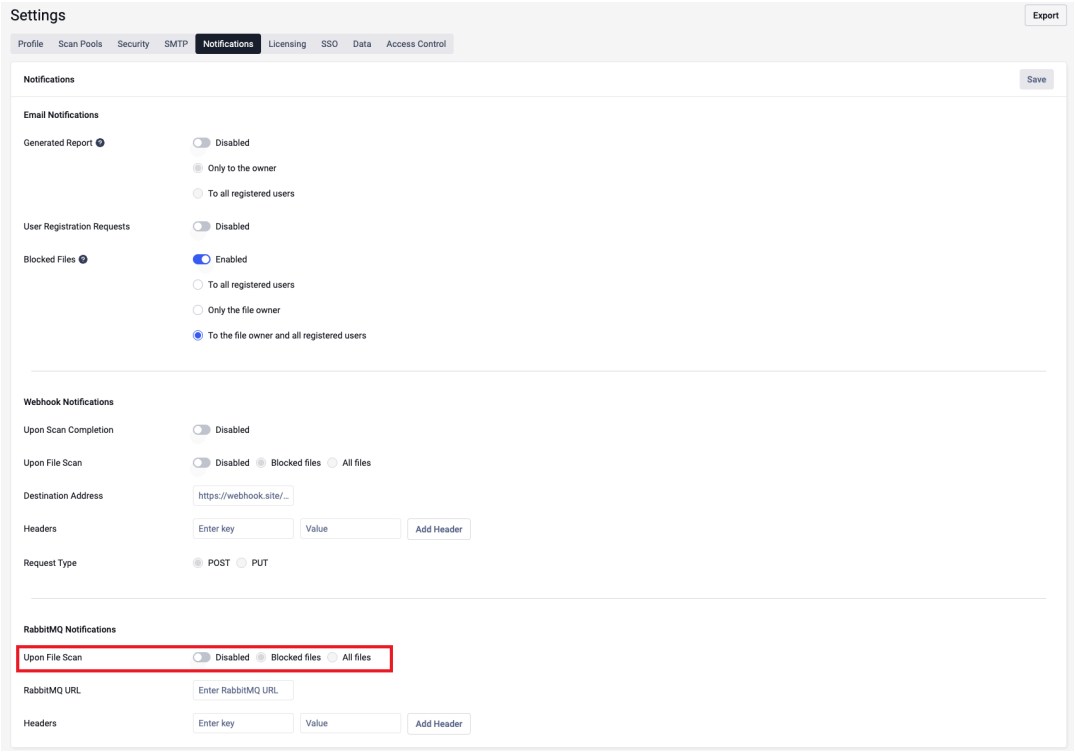
Overview

File Scanned RabbitMQ notifications allow you to receive real-time alerts whenever a file has been scanned by MetaDefender Storage Security. This feature is useful if you need to:

- Enable cross-MDSS instance scanning where one MDSS instance publishes scan results and another automatically rescans the file

Setup

1. Go to **Settings > Notifications** in the MetaDefender Storage Security console.
2. Select **Upon File Scan** from the **RabbitMQ Notifications **section.
3. Choose whether you want to receive notifications for **all scanned files** or **only blocked files**.
4. Enter the **RabbitMQ URL** (your endpoint).
5. (Optional) Add any custom **headers**.
6. Save the configuration.



Configuration Details

- **RabbitMQ URL** – The URL of the receiving system (ex: amqp://username:passowrd@localhost:27049).
- **Headers** – Optional key-value pairs (e.g., `StorageClientId: string; ScanId: string`).
  - StorageClientId - destination storage client Id
  - ScanId - destination scanId
- **Notification scope** – Choose between:
  - **All scanned files** → You will receive a notification for every file scanned.
  - **Blocked only** → You will only receive notifications when a file is marked as blocked in MetaDefender Storage Security (see File Definition)

RabbitMQ Payload

When triggered, the RabbitMQ sends a JSON request body to your configured endpoint.

```
{
  "isPublicWebhook": false,
  "metadata": {
    "serializedEventMetadata": ""
  },
  "metadataToBuild": {
    "serializedEventMetadata": "{\"FileId\":\"019a0b68-1c71-7b7b-ac39-
8357658c3220\",\"FileName\":\"text1.txt\",\"FilePath\":\"folder1/text1.
txt\",\"FileStatus\":\"Allowed\",\"CoreScanResult\":\"No Threat
Detected\",\"FileState\":\"Available\",\"RemediationResult\":
[],\"ScanCompletedTimeStamp\":\"2025-10-
22T10:12:49.647929Z\",\"WorkflowName\":\"Default Workflow\",\"Rules\":
[\"MetaDefender Storage
Security\"],\"ExceptionDetails\":\"System.ObjectDisposedException: The
CancellationTokenSource has been disposed.\\r\\n   at
System.Threading.CancellationTokenSource.get_Token()\\r\\n   at
opswat.mdcs.scanning.service.ScanningService.HandleScanResults(IPipelin
e`2 getScanResultsQueryPipeline, IMediator mediator,
ObjectReadyForScanEvent message, ScanningData scanningData,
CancellationTokenSource cts, InitiateScanCommandResponse
initiateScanCommandResponse) in C:\\\\Projects\\\\md-cloud-
services\\\\Backend\\\\src\\\\opswat.mdcs.scanning.service\\\\Services\
\\\Classes\\\\ScanningService.cs:line 427\\r\\n   at
opswat.mdcs.scanning.service.ScanningService.ObjectReadyForScanEventHan
dler(ObjectReadyForScanEvent message, CancellationToken
cancellationToken) in C:\\\\Projects\\\\md-cloud-
services\\\\Backend\\\\src\\\\opswat.mdcs.scanning.service\\\\Services\
\\\Classes\\\\ScanningService.cs:line 357\",\"RemediationErrors\":
[],\"WebhookNotificationType\":\"FileScanned\"}"
  },
  "scanId": "01985f77-2bf6-7895-bf6f-ceced4c95a87",
  "storageClientId": "01985f77-2b01-764a-bc6e-6cc3e38f3761"
}
```

```
{
  "FileId": "0198f02f-ed4d-7c0d-8668-1036d322209c",
  "FileName": "file.txt",
  "FilePath": "folder/file.txt",
  "FileStatus": "Allowed",
  "CoreScanResult": "No Threat Detected",
  "FileState": "Available",
  "RemediationResult": [
    "AllowedKept: Applied"
  ],
  "ScanCompletedTimeStamp": "2025-08-28T10:20:24.974998Z",
  "WorkflowName": "Default Workflow",
  "Rules": [
    "MetaDefender Storage Security"
  ],
  "ExceptionDetails": "",
  "RemediationErrors": [],
  "WebhookNotificationType": "FileScanned"
}
```


Field Reference

Field	Type	Example Value	Description
`ScanId`	string (UUID)	`01985f77-2b01-764a-bc6e-6cc3e38f3761`	Unique identifier of the destination scan.
`StorageClientId`	string	`01985f77-2b01-764a-bc6e-6cc3e38f3761`	Unique identifier of the destination storage client.
`IsPublicWebhook`	bool	`false`	Used only for webhook
`Metadata`	WebHookMetadataRtp	""	Empty for RabbitMQ notification
`MetadataToBuild`	WebHookMetadataRtp	`Serialized FileScannedNotificationDetails`	Populated with FileScannedNotificationDet

Delivery Behavior

- Cross-MDSS Instance Scanning: When MDSS Instance A completes a scan and publishes to RabbitMQ, Instance B consumes the notification and automatically triggers an Event-Based RTP scan for the same file.
- Delivery is **best-effort** → if the destination is invalid, the request is logged in the **Audit page**, but **no retries** are performed.

Security Considerations

- The RabbitMQ URL is stored encrypted

Troubleshooting

- **No RabbitMQ message received** → Verify the endpoint URL and headers you configured.
- **Audit shows delivery failed** → Endpoint is invalid. Fix and test again.

External Loggers Configuration

This feature allows you to forward event logs from MetaDefender Storage Security to an external system.

This is essential for centralized monitoring, security analysis, and integrating with a SIEM (Security Information and Event Management) platform, such as Splunk.

Supported Platforms and Formats

- **Syslog** uses the UDP protocol and requires the RFC5424 format
- **Kafka** connects directly to an Apache Kafkla cluster.

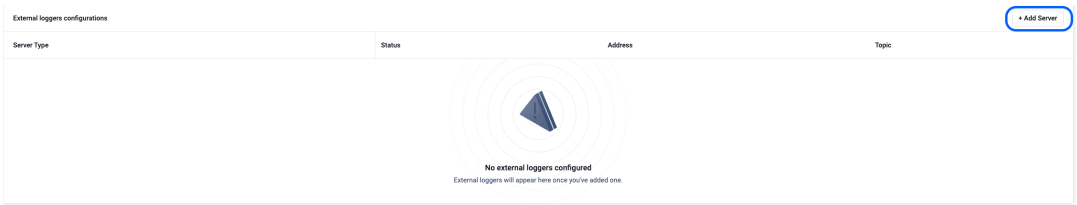
Before You Begin

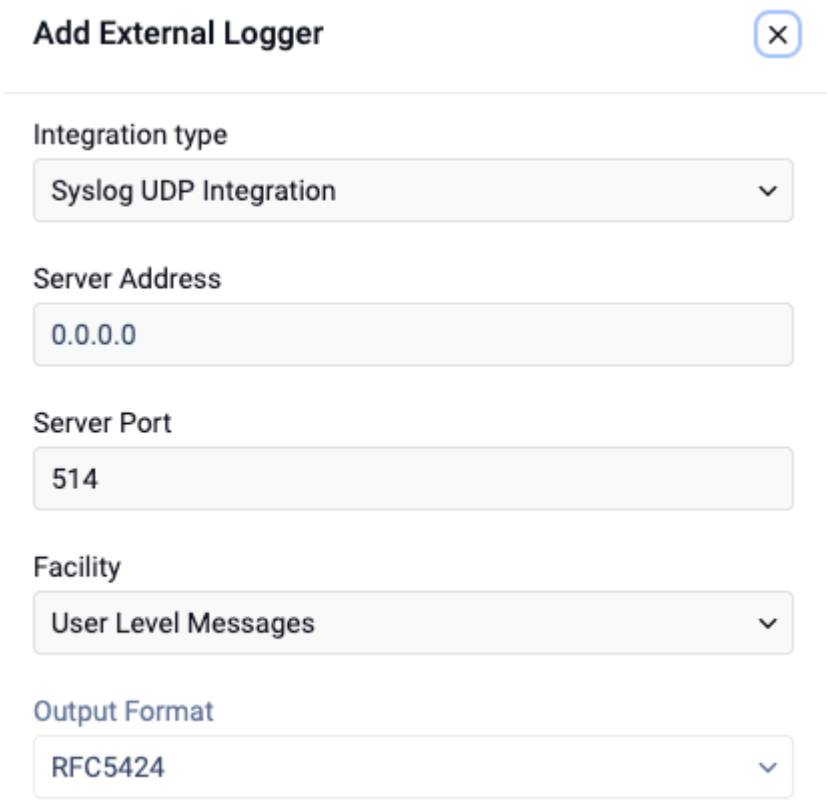
Before adding a configuration, ensure that your external logging server is already deployed and accessible from your MetaDefender Storage Security instance. You will need:

- A Syslog server ready to accept UDP traffic.
- Or, an Apache Kafka cluster with a designated topic.

How to Configure an External Logger

1. In the MetaDefender Storage Security interface, go to **Settings** > **External Loggers**.
2. Click the **+ Add new server** button to open the configuration panel.
3. Fill in the required server details, such as the server type, network address (IP or hostname), and port.
4. Enable the configuration using the toggle switch and save your changes.





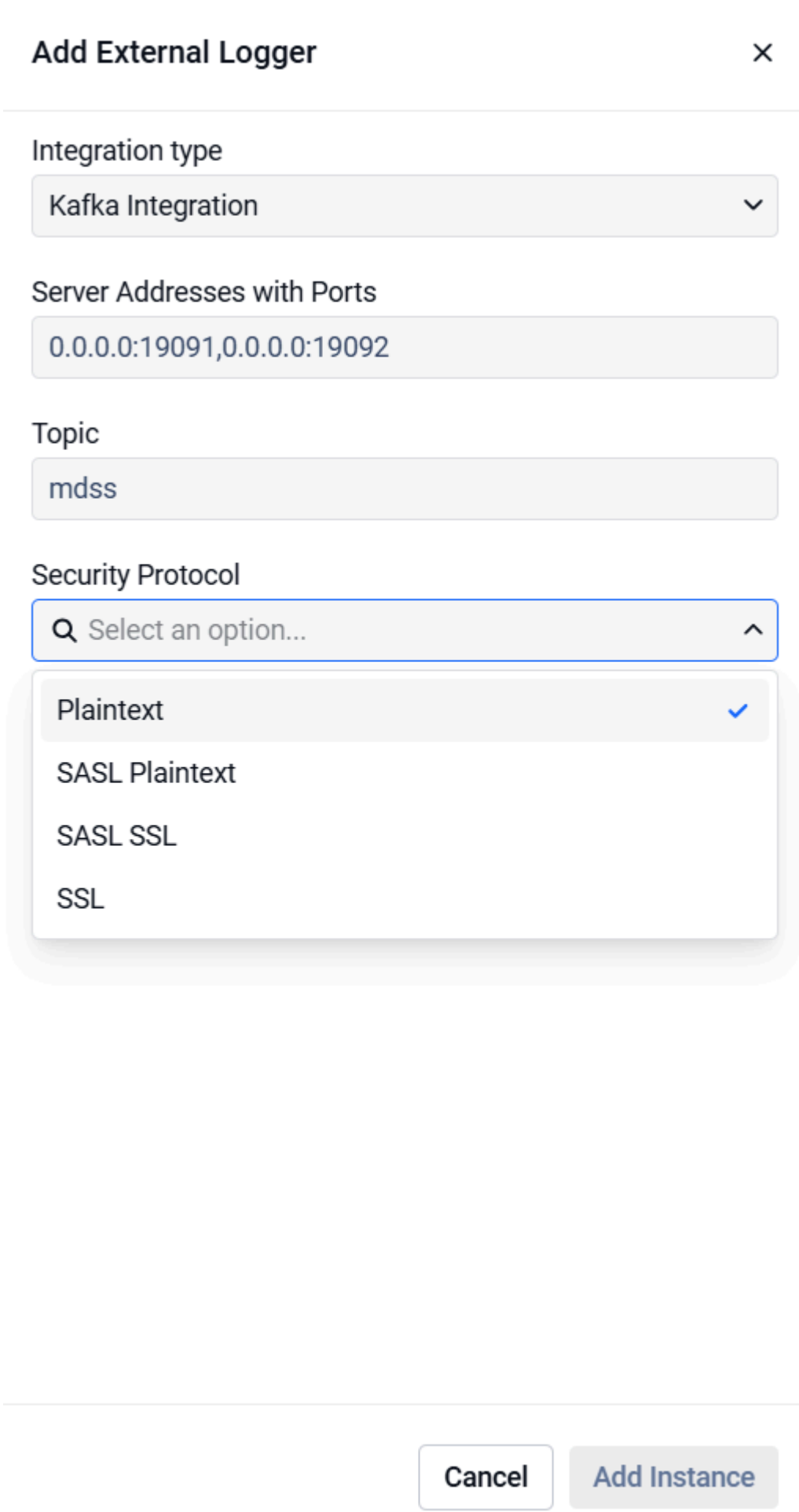
Kafka External Logger

For adding a new Kafka external logger configuration, you will need to enter the following details on the **Add External Logger window:**

- **Integration type**: Select **Kafka Integration**
- **Server addresses with ports** - Ipv4, Ipv6 and Host Name formats are supported with the port specified for each of them (multiple addresses can be separated with a comma)
- **Topic**: The Kafka topic where the logs will be sent
- **Security Protocol**: Select the desired protocol from Plaintext, SASL Plaintext, SASL SSL or SSL

For SASL Plaintext and SASL SSL security protocols, the following fields are also required:

- **SASL mechanism**: Select the desired mechanism from Plain, SCRAM SHA 256 and SCRAM SHA 512
- **SASL username**: The SASL username
- **SASL password**: The SASL password


Add External Logger
Integration type
Kafka Integration
Server Addresses with Ports
0.0.0.0:19091,0.0.0.0:19092
Topic
mdss
Security Protocol
Select an option...
Plaintext
SASL Plaintext
SASL SSL
SSL
Cancel
Add Instance

Kafka message format:

The log messages sent are sent as JSON, and contain information such as the timestamp, log type, level and the log message.


```
{
        "Timestamp": "2024-11-18T09:13:43.4018931+00:00",
        "Level": "Information",
        "MessageTemplate": "{User} logged in.",
        "RenderedMessage": "\"User (John Doe)\" logged in.",
        "Properties": {
                "User": "User(John Doe)",
                "Namespace": "ExternalLogger",
                "EventTimestamp": "2024-11-18 09:13:43",
                "UserName": "User",
                "UserId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx",
                "Category": 3,
                "LogType": 600
        }
}
```


Logging non-audit MDSS messages to Kafka:

For logging other log messages produced by MDSS the appsettings.json can be modified to include a configuration to write to Kafka such as:

```
{
  "Serilog": {
    "MinimumLevel": {
      "Default": "Information",
      "Override": {
        "Microsoft": "Warning",
        "System": "Warning",
        "Microsoft.Hosting.Lifetime": "Information"

      }
    },
    "Enrich": [ "FromLogContext", "WithMachineName", "WithProcessId",
"WithProcessName", "WithThreadId" ],
    "WriteTo": [
      {
        "Name": "Kafka",
        "Args": {
          "bootstrapServers":
"kafkaServerAddress1:kafkaport1,kafkaServerAddress2:kafkaport2",
          "securityProtocol": "Plaintext",
          "topic": "mdss",
          "messageKey": "EventTimestamp"
        }
      }
    ]
  }
}
```

For "**securityProtocol"** values can be Plaintext, SaslSsl, SaslPlaintext or Ssl. For using SASL, the "**saslMechanism"** can be specified with values such as Plain, ScramSha512 or ScramSha256. For example, to use SASL with a Plain mechanism with username and password, the following values can be added to the Args key in the appsettings Kafka configuration.

```
{
          "saslMechanism": "Plain",
          "saslUsername": "username",
          "saslPassword": "password",
}
```

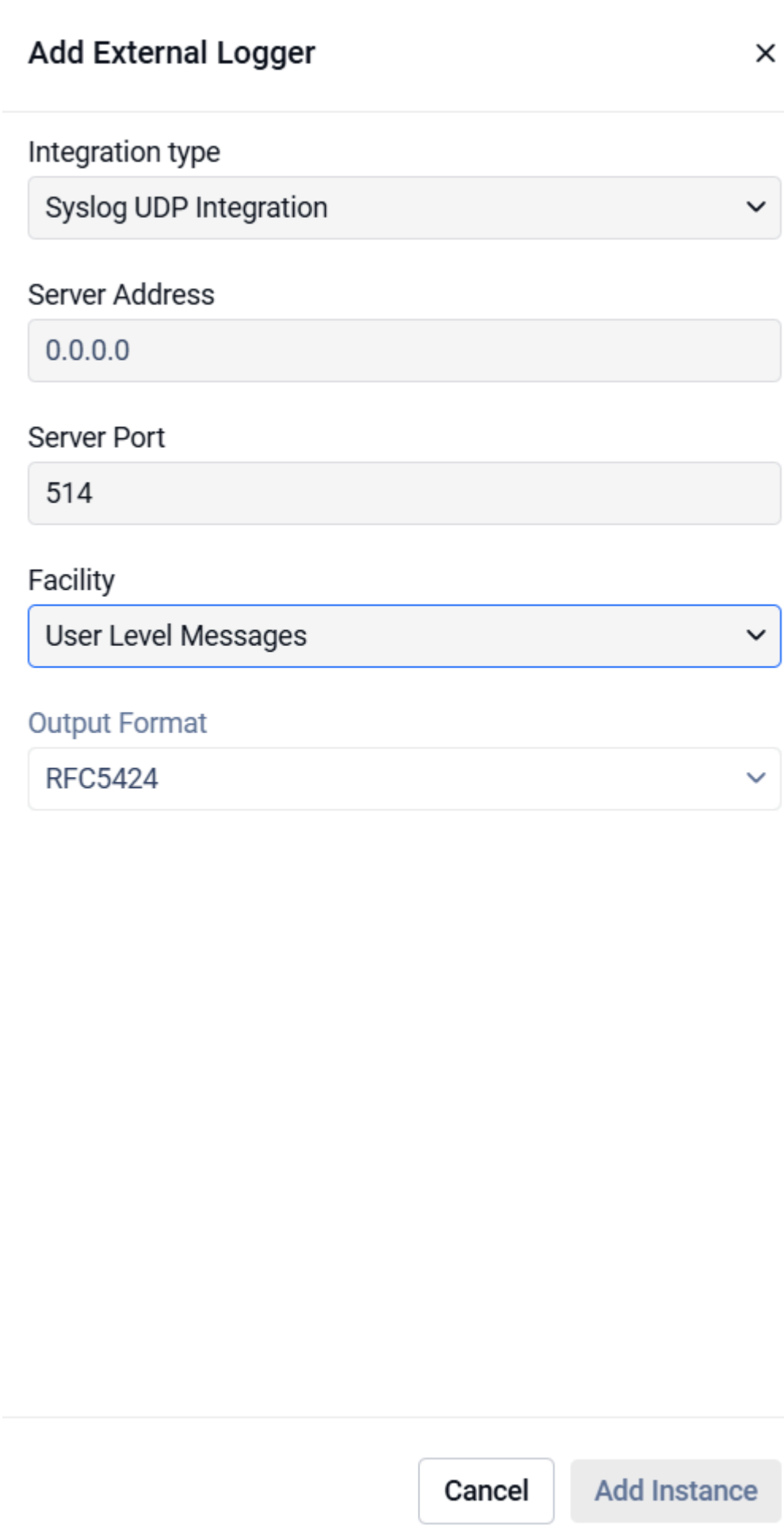
Syslog UDP External Logger

> **Info**
>
> Currently we support Syslog (UDP) using **only** the **RFC 5424** Output format as external logger configuration.

In order to visualize MetaDefender Storage Security audit logs in a centralized dashboard, integration with a Syslog (UDP) server is possible.

For adding a new Syslog configuration, you will need to enter the following details on the **Add External Logger window:**

- Server address - Ipv4, Ipv6 and Host Name formats are supported
- Port
- Syslog Facility
- Output format - RFC5424 format is supported


Add External Logger
Integration type
Syslog UDP Integration
Server Address
0.0.0.0
Server Port
514
Facility
User Level Messages
Output Format
RFC5424
Cancel
Add Instance

> **Info**
>
> Up to 5 different external loggers configurations of each type are supported.

Syslog message format

We support format **RFC5424**. You can find more details about this format here.

```
<PRI>VERSION TIMESTAMP HOSTNAME APP-NAME PROCID MSGID STRUCTURED-DATA
MSG
```

Prefix Field (click for more info)	Description
PRI	Priority value
VERSION	The version of the syslog protocol specification
TIMESTAMP	A formalized timestamp
HOSTNAME	The machine that originally sent the syslog message
APP-NAME	The device or application that originated the message
PROCID	Process name or ID associated with a syslog system
MSGID	Type of the message
STRUCTURED-DATA	A mechanism to express information in an easily parsable and interpretable data format
MSG	Free-form message that provides information about the event

```
<110>1 2024-03-26T12:27:58.276724+02:00 LP10-D8569
MetaDefenderStorageSecurity 36800 - [meta UserName="jdavis"
UserId="e69e8c2d-4dcc-4489-8f40-0df84199de52"
EventTimestamp="03/26/2024 10:27:58" Category="3" LogType="600"] John
Davis (jdavis) logged in.
```

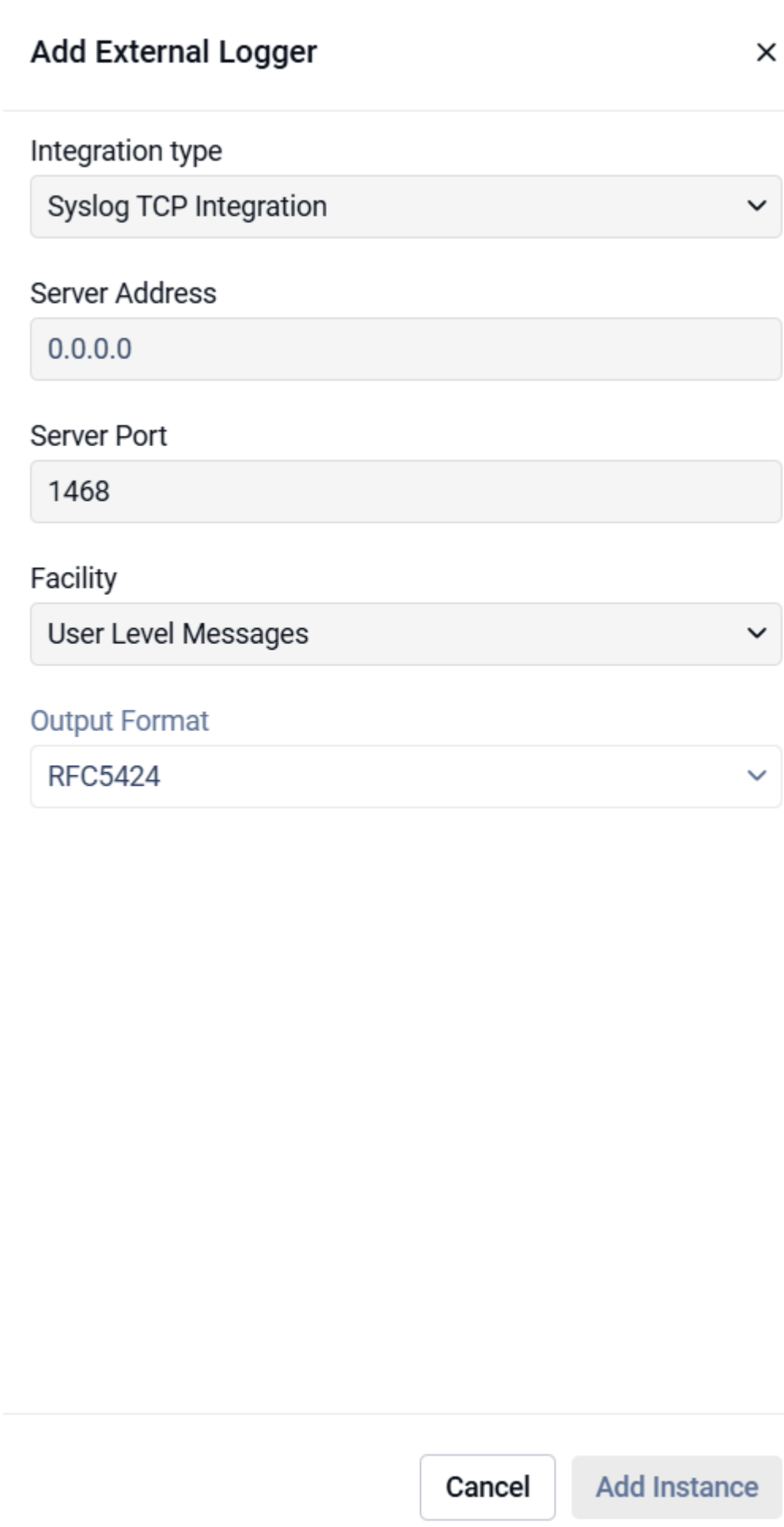
Syslog TCP External Logger

> **Info**
>
> Currently we support Syslog (TCP) using **only** the **RFC 5424** Output format as external logger configuration.

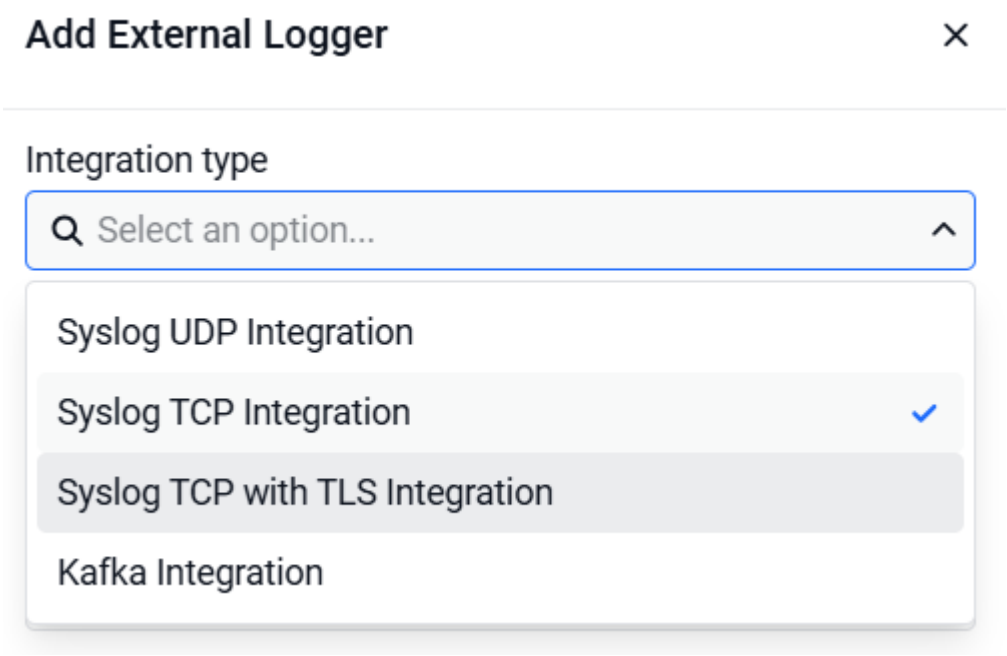
In order to visualize MetaDefender Storage Security audit logs in a centralized dashboard, integration with a Syslog (TCP) server is possible.

For adding a new Syslog configuration, you will need to enter the following details on the **Add External Logger window:**

- Server address - Ipv4, Ipv6 and Host Name formats are supported
- Port
- Syslog Facility
- Output format - RFC5424 format is supported


Add External Logger
Integration type
Syslog TCP Integration
Server Address
0.0.0.0
Server Port
1468
Facility
User Level Messages
Output Format
RFC5424
Cancel
Add Instance

The Syslog TCP integration also supports TLS certificates. MDSS might request CA certificates for the Syslog server.



> **Info**
>
> Up to 5 different external loggers configurations of each type are supported.

Syslog message format

We support format **RFC5424**. You can find more details about this format here.

```
<PRI>VERSION TIMESTAMP HOSTNAME APP-NAME PROCID MSGID STRUCTURED-DATA
MSG
```

Prefix Field (click for more info)	Description
PRI	Priority value
VERSION	The version of the syslog protocol specification
TIMESTAMP	A formalized timestamp
HOSTNAME	The machine that originally sent the syslog message
APP-NAME	The device or application that originated the message
PROCID	Process name or ID associated with a syslog system
MSGID	Type of the message
STRUCTURED-DATA	A mechanism to express information in an easily parsable and interpretable data format
MSG	Free-form message that provides information about the event

```
<110>1 2024-03-26T12:27:58.276724+02:00 LP10-D8569
MetaDefenderStorageSecurity 36800 - [meta UserName="jdavis"
UserId="e69e8c2d-4dcc-4489-8f40-0df84199de52"
EventTimestamp="03/26/2024 10:27:58" Category="3" LogType="600"] John
Davis (jdavis) logged in.
```

AWS CloudWatch External Logger

To use the AWS CloudWatch logging service, the following conditions must be met:

- AWS SSM agent installed, up to date and active on the EC2 instance (more info here)
- These IAM permissions allocated to the instance
  - AmazonSSMManagedInstanceCore
  - CloudWatchAgentServerPolicy
- AWS CloudWatch agent installed, up to date and active on the EC2 instance (more info here)

If the above conditions are met, the CloudWatch agent can be configured either through editing its configuration file or from the EC2 web UI for your instance.

When configuring the log collection section, you can set specific paths and filenames or, alternatively, you can use wildcard characters (*) to cover multiple folders and/or files. If you want to collect logs from exact paths or specific files, one separate entry needs to be created for each folder or file.

You also have the option to group logs from multiple locations into one or several log groups and streams which will then be visible in AWS CloudWatch. A log group can contain one or multiple log streams, and each log stream can be set to collect logs from one or multiple log files.

> **Info**
>
> If you group logs from multiple files into the same log stream they will be combined and displayed in chronological order, there will be no separation based on the source log files.

An example configuration to collect CPU, RAM and disk storage metrics from a Linux installation every 5 seconds as well as to pull all MetaDefender Storage Security logs using wildcards would look like this:

> **Note**
>
> The example below will collect **all logs** from MetaDefender Storage Security.
>
> If you would like to customize which logs are collected, please configure the paths according to the documented locations here.

```
{
    "agent": {
        "metrics_collection_interval": 60
    },
    "metrics": {
        "namespace": "CWAgent",
        "append_dimensions": {
            "InstanceId": "${aws:InstanceId}"
        },
        "metrics_collected": {
            "mem": {
                "measurement": [
                    "used_percent"
                ]
            },
            "cpu": {
                "measurement": [
                    "usage_active"
                ]
            },
            "disk": {
                "measurement": [
                    "used_percent"
                ]
            }
        }
    },
    "logs": {
        "logs_collected": {
            "files": {
                "collect_list": [
                    {
                        "file_path": "/var/log/mdss/*.log",
                        "filters": [],
                        "log_group_name": "mdss-logs",
                        "log_stream_name": "applogs"
                    },
                    {
                        "file_path": "/etc/mdss/services_logs/*/*.txt",
                        "filters": [],
                        "log_group_name": "mdss-logs",
                        "log_stream_name": "applogs"
                    }
                ]
            }
        },
        "log_stream_name": "mdss-logging"
    }
}
```

Syslog Message Reference — One Sample per Event Type

This page lists a sample Syslog message for every event type MDSS can emit to an external logger. Use it to build parsers, field extractions and detection rules without having to generate each event first.

MDSS emits 98 distinct event types across 12 categories. Each is listed below with its `LogType` value, the fields it carries, and a complete sample message.

For how to configure a Syslog destination, see **External Loggers — Streaming the MDSS Audit Trail to a SIEM**.

---

1. Message anatomy

Every message is a standard RFC 5424 line with five parts:

```
<110>1 2026-08-13T12:15:42.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta ...] Message text
└─┘└┘ └──────────────────────────┘ └──────┘ └──────┘
└──────────┘ └─┘ └─┘ └──────┘ └──────┘
  |  |          |          |          |          |
|   |    |      |
 PRI |        timestamp          hostname      app-name
proc-id |  structured  message
   version
msg-id   data
```

Part	Notes
PRI	`facility × 8 + severity`. With the default `LogAudit` facility (13): `110` for informational, `108` for warning, `107` for error. Change the facility in the destination configuration and every PRI shifts accordingly.
Timestamp	Local time of the MDSS host, with UTC offset.
Hostname	The MDSS host that emitted the event.
App-name	Always `MetaDefenderStorageSecurity`.
Proc-id	Process id of the MDSS logging service. Not stable across restarts.
Msg-id	Always `-` (not used).
Structured data	A single `[meta ...]` element containing every field as a quoted key–value pair.
Message	Human-readable text. Field values are substituted inline.

What is inside `[meta ...]`

Two groups of fields, in one element:

1. **Message fields** — one pair for every placeholder in the message text. These vary by event type and are listed per event below.
2. **Envelope fields** — present on every event: `TenantId`, `UserName`, `UserId`, `EventTimestamp`, `Category`, `LogType`, `Namespace`, `Id`.

> **Key on names, not position**
>
> Field order inside `[meta ...]` is not part of the contract and may change between releases. Always parse by key name. Likewise, treat message fields as optional — the same event type carries different fields depending on what MDSS knows at the time.

Two conventions to note

All values are quoted strings. RFC 5424 structured data has no types, so `fileSize="48213"` is a string even though it is a number. Cast in your parser.

String values are quoted in the message text too. The message reads `... fileName: "invoice.docx" ...`, with the quotes present. Numeric values appear unquoted. This affects regular expressions written against the message body — prefer the structured data.

A complete example

The most detailed event in the product, with nothing elided — a blocked file, `LogType 1`:

```
<110>1 2026-08-13T12:15:42.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta fileName="invoice.docx"
filePath="/finance/2026/invoice.docx"
fileHash="5d41402abc4b2a76b9719d911017c592" fileSize="48213"
fileId="0199c0de-7a1e-7000-8000-0000000000ab"
dataId="bzIxMDgwOU5xTFZ2b2E"
sha256="e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b85
5" result="Blocked" blockedReason="Infected"
numberOfInfectedEngines="3" AVCount="32" threatFound="Ahnlab:
Trojan/Win32.Agent" storageName="Finance-SMB" storageType="Category:
FileShare, Protocol: Smb, Vendor: Generic" storageId="7f3a9c14-2b8e-
4d51-9a06-c1e5b48f2d73" scanId="e1b6d842-0f37-4c9b-8a15-63d0947fe2ba"
scanName="Nightly Finance" scanType="Scheduled Process"
Workflow="Default workflow" TenantId="default" UserName="system"
UserId="system" EventTimestamp="2026-08-13 10:15:42" Category="0"
LogType="1" Namespace="ExternalLogger" Id="0199c0de-7a1e-7000-8000-
000000000001"] File (fileName: "invoice.docx"; filePath:
"/finance/2026/invoice.docx"; fileHash:
"5d41402abc4b2a76b9719d911017c592"; fileSize: 48213; fileId: "0199c0de-
7a1e-7000-8000-0000000000ab"; dataId: "bzIxMDgwOU5xTFZ2b2E";
sha256:"e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b85
5"; result: "Blocked"; blockedReason: "Infected";
numberOfInfectedEngines: 3; AVCount: 32; threatFound:"Ahnlab:
Trojan/Win32.Agent") from storage (name: "Finance-SMB"; "Category:
FileShare, Protocol: Smb, Vendor: Generic"; ID: "7f3a9c14-2b8e-4d51-
9a06-c1e5b48f2d73") was successfully scanned by scan (ID: "e1b6d842-
0f37-4c9b-8a15-63d0947fe2ba", name: "Nightly Finance", type: "Scheduled
Process") with the following configuration "Default workflow".
```

For readability, the samples in sections 3 to 14 show the message text and the message fields, with the eight envelope fields abbreviated to . Substitute the envelope from the example above; only `Category`, `LogType`, `UserName` and `UserId` change between event types, and those are stated in each entry.

Sample environment

All samples use one consistent fictional deployment:

Item	Value
Host	`mdss-prod-01`
Administrator	`John Davis (jdavis)`, id `e69e8c2d-4dcc-4489-8f40-0df84199de52`
Storage	`Finance-SMB`, id `7f3a9c14-2b8e-4d51-9a06-c1e5b48f2d73`, SMB file share
Scan	`Nightly Finance`, id `e1b6d842-0f37-4c9b-8a15-63d0947fe2ba`, scheduled
Workflow	`Default workflow`, id `9d4e1f60-3a72-4b85-8c19-f2073be5a1c8`
File	`invoice.docx` at `/finance/2026/invoice.docx`
Tenant	`default`

---

2. Reading the actor fields

`UserName` and `UserId` identify who caused the event.

- For an administrator action, both carry that account's values — `UserName="jdavis"`.
- For anything MDSS does on its own — discovery, scanning, remediation, notification delivery — both carry the literal string `system`.

This is the fastest way to separate operator activity from automated processing: filter on `UserName="system"`.

---

3. Category 0 — Scan activities

`Category="0"`. File discovery and scanning, scan process lifecycle, and scan and schedule configuration changes.

LogType 0 — File discovered

A file was found in storage and registered. `UserName="system"`.

Message fields: `fileName`, `filePath`, `fileHash`, `fileSize`, `fileId`, `lastModified`, `storageName`, `storageType`, `storageId`, `scanId`, `scanName`, `scanType`.

```
<110>1 2026-08-13T12:15:42.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta fileName="invoice.docx"
filePath="/finance/2026/invoice.docx"
fileHash="5d41402abc4b2a76b9719d911017c592" fileSize="48213"
fileId="0199c0de-7a1e-7000-8000-0000000000ab" lastModified="08/12/2026
16:40:11" storageName="Finance-SMB" storageType="Category: FileShare,
Protocol: Smb, Vendor: Generic" storageId="7f3a9c14-2b8e-4d51-9a06-
c1e5b48f2d73" scanId="e1b6d842-0f37-4c9b-8a15-63d0947fe2ba"
scanName="Nightly Finance" scanType="Scheduled Process" <envelope
Category="0" LogType="0" UserName="system">] File(fileName:
"invoice.docx"; filePath: "/finance/2026/invoice.docx"; fileHash:
"5d41402abc4b2a76b9719d911017c592"; fileSize: 48213; fileId: "0199c0de-
7a1e-7000-8000-0000000000ab"; lastModified: 08/12/2026 16:40:11) from
storage (name: "Finance-SMB"; "Category: FileShare, Protocol: Smb,
Vendor: Generic"; ID: "7f3a9c14-2b8e-4d51-9a06-c1e5b48f2d73") was
discovered by scan (ID: "e1b6d842-0f37-4c9b-8a15-63d0947fe2ba", name:
"Nightly Finance", type: "Scheduled Process")
```

Real-time variant. When the scan is real-time, the message gains a discovery mode and a `HandlingType` field:

```
... was discovered by scan (ID: "5a20c7e9-8b41-4f63-9d28-1e7c05ab3f94",
name: "Real Time Process", type: "Real Time Process")  (Discovery mode:
"EventBased")
```

LogType 1 — File scanned

The verdict for a file. `UserName="system"`. See the complete example in section 1.

Field composition depends on the outcome:

Outcome	Message fields
Allowed	`fileName`, `filePath`, `fileHash`, `sha256`, `fileSize`, `fileId`, `dataId`, `result`, `AVCount`, plus storage, scan and `Workflow`
Blocked	The above plus `blockedReason`, `numberOfInfectedEngines`, `threatFound`
Not yet scanned	Identity only — `fileName`, `filePath`, `fileHash`, `fileSize`, `fileId`, `lastModified`

Allowed file:

```
<110>1 2026-08-13T12:15:44.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta fileName="policy.pdf"
filePath="/finance/2026/policy.pdf"
fileHash="8b1a9953c4611296a827abf8c47804d7"
sha256="9f86d081884c7d659a2feaa0c55ad015a3bf4f1b2b0b822cd15d6c15b0f00a0
8" fileSize="120344" fileId="0199c0de-7a1e-7000-8000-0000000000ac"
dataId="bzIxMDgwOVJrTXBXcWI" result="Allowed" AVCount="32"
storageName="Finance-SMB" storageType="Category: FileShare, Protocol:
Smb, Vendor: Generic" storageId="7f3a9c14-2b8e-4d51-9a06-c1e5b48f2d73"
scanId="e1b6d842-0f37-4c9b-8a15-63d0947fe2ba" scanName="Nightly
Finance" scanType="Scheduled Process" Workflow="Default workflow"
<envelope Category="0" LogType="1" UserName="system">] File (fileName:
"policy.pdf"; filePath: "/finance/2026/policy.pdf"; fileHash:
"8b1a9953c4611296a827abf8c47804d7";
sha256:"9f86d081884c7d659a2feaa0c55ad015a3bf4f1b2b0b822cd15d6c15b0f00a0
8"; fileSize: 120344; fileId: "0199c0de-7a1e-7000-8000-0000000000ac";
dataId: "bzIxMDgwOVJrTXBXcWI"; result: "Allowed";  AVCount: 32 ) from
storage (name: "Finance-SMB"; "Category: FileShare, Protocol: Smb,
Vendor: Generic"; ID: "7f3a9c14-2b8e-4d51-9a06-c1e5b48f2d73") was
successfully scanned by scan (ID: "e1b6d842-0f37-4c9b-8a15-
63d0947fe2ba", name: "Nightly Finance", type: "Scheduled Process") with
the following configuration "Default workflow".
```

Scan failure — emitted at error severity, PRI `<107>`, with a different message and no verdict fields:

```
<107>1 2026-08-13T12:15:46.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta fileName="archive.zip"
filePath="/finance/2026/archive.zip"
fileHash="c4ca4238a0b923820dcc509a6f75849b" fileSize="9812443"
fileId="0199c0de-7a1e-7000-8000-0000000000ad" lastModified="08/12/2026
09:02:55" storageName="Finance-SMB" storageType="Category: FileShare,
Protocol: Smb, Vendor: Generic" storageId="7f3a9c14-2b8e-4d51-9a06-
c1e5b48f2d73" scanId="e1b6d842-0f37-4c9b-8a15-63d0947fe2ba"
scanName="Nightly Finance" scanType="Scheduled Process" <envelope
Category="0" LogType="1" UserName="system">] Unable to scan file
(fileName: "archive.zip"; filePath: "/finance/2026/archive.zip";
fileHash: "c4ca4238a0b923820dcc509a6f75849b"; fileSize: 9812443;
fileId: "0199c0de-7a1e-7000-8000-0000000000ad"; lastModified:
08/12/2026 09:02:55) from storage (name: "Finance-SMB"; "Category:
FileShare, Protocol: Smb, Vendor: Generic"; ID: "7f3a9c14-2b8e-4d51-
9a06-c1e5b48f2d73") by scan (ID: "e1b6d842-0f37-4c9b-8a15-
63d0947fe2ba", name: "Nightly Finance", type: "Scheduled Process")
```

Scanned with identity. When MDSS reuses a previous result instead of rescanning, the text reads `was successfully scanned with identity` in place of `was successfully scanned`.

File version variant. On storages that keep versions, the label becomes `File version` and the fields are `fileVersionName`, `fileId`, `fileVersionPath`, `fileVersionHash`,

`fileVersionSize`, `fileVersionId`, `createdAt`.

LogType 2 — File discovery failed

Discovery could not complete for one file. Emitted at error severity, PRI `<107>`. `UserName="system"`.

Message fields: `ObjectId`, `objectPath`, storage, scan, `FailureReason`.

```
<107>1 2026-08-13T12:15:48.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta ObjectId="0199c0de-7a1e-7000-
8000-0000000000ae" objectPath="/finance/2026/locked.xlsx"
storageName="Finance-SMB" storageType="Category: FileShare, Protocol:
Smb, Vendor: Generic" storageId="7f3a9c14-2b8e-4d51-9a06-c1e5b48f2d73"
scanId="e1b6d842-0f37-4c9b-8a15-63d0947fe2ba" scanName="Nightly
Finance" scanType="Scheduled Process" FailureReason="Access denied"
<envelope Category="0" LogType="2" UserName="system">] Unable to
discover file with ID "0199c0de-7a1e-7000-8000-0000000000ae" with path
"/finance/2026/locked.xlsx" from storage (name: "Finance-SMB";
"Category: FileShare, Protocol: Smb, Vendor: Generic"; ID: "7f3a9c14-
2b8e-4d51-9a06-c1e5b48f2d73") by scan (ID: "e1b6d842-0f37-4c9b-8a15-
63d0947fe2ba", name: "Nightly Finance", type: "Scheduled Process").
Reason: "Access denied"
```

> **File skipped uses this same event type**
>
> When a file is skipped rather than failed — excluded by a filter, for example — MDSS emits `LogType="2"` at **warning** severity, PRI `<108>`, with the same message shape and the skip reason in `FailureReason`. Distinguish the two by severity, not by event type.

LogType 3 — File cancelled

A user cancelled processing for a file. Carries that user's identity, not `system`.

Message fields: file identity fields.

```
<110>1 2026-08-13T12:16:02.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta fileName="invoice.docx"
filePath="/finance/2026/invoice.docx"
fileHash="5d41402abc4b2a76b9719d911017c592" fileSize="48213"
fileId="0199c0de-7a1e-7000-8000-0000000000ab" lastModified="08/12/2026
16:40:11" <envelope Category="0" LogType="3" UserName="jdavis">] File
(fileName: "invoice.docx"; filePath: "/finance/2026/invoice.docx";
fileHash: "5d41402abc4b2a76b9719d911017c592"; fileSize: 48213; fileId:
"0199c0de-7a1e-7000-8000-0000000000ab"; lastModified: 08/12/2026
16:40:11) has been cancelled
```

LogType 100 to 103 — Scan process lifecycle

One event per scan run and storage. `UserName="system"`. The `ScanType` field holds the lifecycle action, lower-cased.

LogType	Action	Severity
100	started	informational, <110>
101	completed	informational, <110>
102	cancelled	informational, <110>
103	failed	error, <107>

```
<110>1 2026-08-13T12:15:40.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta scanId="e1b6d842-0f37-4c9b-
8a15-63d0947fe2ba" scanName="Nightly Finance" scanType="Scheduled
Process" ScanType="started" storageName="Finance-SMB"
storageType="Category: FileShare, Protocol: Smb, Vendor: Generic"
storageId="7f3a9c14-2b8e-4d51-9a06-c1e5b48f2d73" <envelope Category="0"
LogType="100" UserName="system">] Scan (ID: "e1b6d842-0f37-4c9b-8a15-
63d0947fe2ba", name: "Nightly Finance", type: "Scheduled Process")
"started" for storage (name: "Finance-SMB"; "Category: FileShare,
Protocol: Smb, Vendor: Generic"; ID: "7f3a9c14-2b8e-4d51-9a06-
c1e5b48f2d73")
```

Substitute `ScanType="completed"` with `LogType="101"`, `ScanType="cancelled"` with `LogType="102"`, and `ScanType="failed"` with `LogType="103"` and PRI <107>.

> **Two fields named for the scan type**
>
> `scanType` (lower case s) is the kind of scan — `Scheduled Process`, `Real Time Process` or `Instant Process`. `ScanType` (upper case S) is the lifecycle action on these four event types. They are different fields.

LogType 1500 to 1503 — Scan configuration changed

An administrator added, updated, deleted or imported a scan.

LogType	Action
1500	added
1501	updated
1502	deleted
1503	imported

Message fields: `Scan`, `Type`, `Action`, `User`. Add and update also carry `WorkflowName`, `UserAgent`, `WorkflowRule`, `ScanPoolName`, `ScanInstances`. Add, update and delete also carry the storage fields.

```
<110>1 2026-08-13T09:22:10.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta Scan="Nightly Finance"
Type="Scheduled" Action="added" User="jdavis" WorkflowName="Default
workflow" UserAgent="" WorkflowRule="" ScanPoolName="Primary pool"
ScanInstances="https://core-01:8008" storageName="Finance-SMB"
storageType="Category: FileShare, Protocol: Smb, Vendor: Generic"
storageId="7f3a9c14-2b8e-4d51-9a06-c1e5b48f2d73" <envelope Category="0"
LogType="1500" UserName="jdavis">] Scan "Nightly Finance", type:
"Scheduled" was "added" by "jdavis". Workflow: name - "Default
workflow", user agent - "", workflow rule - "". Scan pool: name -
"Primary pool", scan instances - "https://core-01:8008". Storage (name:
"Finance-SMB"; "Category: FileShare, Protocol: Smb, Vendor: Generic";
ID: "7f3a9c14-2b8e-4d51-9a06-c1e5b48f2d73")
```

Failure variant — error severity, PRI `<107>`, fields `User`, `Action`, `Scan`, `ResponseMessage`:

```
<107>1 2026-08-13T09:22:12.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta User="jdavis" Action="add"
Scan="Nightly Finance" ResponseMessage="A scan with this name already
exists" <envelope Category="0" LogType="1500" UserName="jdavis">] User
"jdavis" was unable to "add" scan "Nightly Finance". Response message:
"A scan with this name already exists".
```

LogType 1900 to 1904 — Scan schedule changed

LogType	Action
1900	added
1901	updated
1902	deleted
1903	imported
1904	skipped

Message fields: `scanName`, `scanId`, `Action`, `User`, storage fields, `WorkflowId`, `WorkflowName`.

```
<110>1 2026-08-13T09:25:00.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta scanName="Nightly Finance"
scanId="b83f27a5-14c9-4e06-9f7b-2d58e0ca934f" Action="added"
User="jdavis" storageName="Finance-SMB" storageType="Category:
FileShare, Protocol: Smb, Vendor: Generic" storageId="7f3a9c14-2b8e-
4d51-9a06-c1e5b48f2d73" WorkflowId="9d4e1f60-3a72-4b85-8c19-
f2073be5a1c8" WorkflowName="Default workflow" <envelope Category="0"
LogType="1900" UserName="jdavis">] Scan schedule (Name: "Nightly
Finance"; ID: "b83f27a5-14c9-4e06-9f7b-2d58e0ca934f";)  was "added" by
"jdavis" for storage (name: "Finance-SMB"; "Category: FileShare,
Protocol: Smb, Vendor: Generic"; ID: "7f3a9c14-2b8e-4d51-9a06-
c1e5b48f2d73") with Workflow (Id: "9d4e1f60-3a72-4b85-8c19-
f2073be5a1c8"; Name: "Default workflow")
```

`LogType="1904"` uses `Action="skipped"` and is emitted by the system when a scheduled run is skipped, so `UserName="system"`.

Failure variant — error severity, PRI `<107>`:

```
<107>1 2026-08-13T09:25:04.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta User="jdavis" Action="add"
scanName="Nightly Finance" scanId="b83f27a5-14c9-4e06-9f7b-
2d58e0ca934f" storageName="Finance-SMB" storageType="Category:
FileShare, Protocol: Smb, Vendor: Generic" storageId="7f3a9c14-2b8e-
4d51-9a06-c1e5b48f2d73" <envelope Category="0" LogType="1900"
UserName="jdavis">] User "jdavis" was unable to "add" scan schedule
(Name: "Nightly Finance"; ID: "b83f27a5-14c9-4e06-9f7b-2d58e0ca934f";)
(name: "Finance-SMB"; "Category: FileShare, Protocol: Smb, Vendor:
Generic"; ID: "7f3a9c14-2b8e-4d51-9a06-c1e5b48f2d73")
```

4. Category 1 — Post actions

`Category="1"`. What MDSS did about each file after scanning. All are emitted by the system, so `UserName="system"`.

Every post-action event shares one message shape:

```
{PostAction} applied to file {file fields} from storage {storage
fields} by scan {scan fields}. {outcome sentence}
```

`PostAction` holds one of: `Tagging`, `Blocked file remediation`, `Allowed file remediation`, `Discovered file remediation`, `Scan file versions`.

LogType 200 — File tagged

Message fields: `PostAction`, file identity, storage, scan.

```
<110>1 2026-08-13T12:15:50.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta PostAction="Tagging"
fileName="invoice.docx" filePath="/finance/2026/invoice.docx"
fileHash="5d41402abc4b2a76b9719d911017c592" fileSize="48213"
fileId="0199c0de-7a1e-7000-8000-0000000000ab" lastModified="08/12/2026
16:40:11" storageName="Finance-SMB" storageType="Category: FileShare,
Protocol: Smb, Vendor: Generic" storageId="7f3a9c14-2b8e-4d51-9a06-
c1e5b48f2d73" scanId="e1b6d842-0f37-4c9b-8a15-63d0947fe2ba"
scanName="Nightly Finance" scanType="Scheduled Process" <envelope
Category="1" LogType="200" UserName="system">] "Tagging" applied to
file (fileName: "invoice.docx"; filePath: "/finance/2026/invoice.docx";
fileHash: "5d41402abc4b2a76b9719d911017c592"; fileSize: 48213; fileId:
"0199c0de-7a1e-7000-8000-0000000000ab"; lastModified: 08/12/2026
16:40:11) from storage (name: "Finance-SMB"; "Category: FileShare,
Protocol: Smb, Vendor: Generic"; ID: "7f3a9c14-2b8e-4d51-9a06-
c1e5b48f2d73") by scan (ID: "e1b6d842-0f37-4c9b-8a15-63d0947fe2ba",
name: "Nightly Finance", type: "Scheduled Process").
```

LogType 205 — Blocked file moved

Move and copy actions add three destination fields: `destinationStorageName`, `destinationStorageType`, `destinationStorageId`, and `RelativeObjectName` for the path written at the destination.

```
<110>1 2026-08-13T12:15:52.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta PostAction="Blocked file
remediation" fileName="invoice.docx"
filePath="/finance/2026/invoice.docx"
fileHash="5d41402abc4b2a76b9719d911017c592" fileSize="48213"
fileId="0199c0de-7a1e-7000-8000-0000000000ab" lastModified="08/12/2026
16:40:11" storageName="Finance-SMB" storageType="Category: FileShare,
Protocol: Smb, Vendor: Generic" storageId="7f3a9c14-2b8e-4d51-9a06-
c1e5b48f2d73" scanId="e1b6d842-0f37-4c9b-8a15-63d0947fe2ba"
scanName="Nightly Finance" scanType="Scheduled Process"
destinationStorageName="Quarantine-SMB"
destinationStorageType="Category: FileShare, Protocol: Smb, Vendor:
Generic" destinationStorageId="2c94f0b7-6d13-4e8a-b5f2-90a7cd31e648"
RelativeObjectName="/quarantine/2026-08-13/invoice.docx" <envelope
Category="1" LogType="205" UserName="system">] "Blocked file
remediation" applied to file (fileName: "invoice.docx"; filePath:
"/finance/2026/invoice.docx"; fileHash:
"5d41402abc4b2a76b9719d911017c592"; fileSize: 48213; fileId: "0199c0de-
7a1e-7000-8000-0000000000ab"; lastModified: 08/12/2026 16:40:11) from
storage (name: "Finance-SMB"; "Category: FileShare, Protocol: Smb,
Vendor: Generic"; ID: "7f3a9c14-2b8e-4d51-9a06-c1e5b48f2d73") by scan
(ID: "e1b6d842-0f37-4c9b-8a15-63d0947fe2ba", name: "Nightly Finance",
type: "Scheduled Process"). The blocked file was moved to storage
(name: "Quarantine-SMB"; "Category: FileShare, Protocol: Smb, Vendor:
Generic"; ID: "2c94f0b7-6d13-4e8a-b5f2-90a7cd31e648") Destination
objectPath: "/quarantine/2026-08-13/invoice.docx"
```

LogType 206 — Blocked file deleted

No destination fields. Outcome sentence: `The blocked file was deleted.`

```
<110>1 2026-08-13T12:15:53.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta PostAction="Blocked file
remediation" fileName="invoice.docx"
filePath="/finance/2026/invoice.docx"
fileHash="5d41402abc4b2a76b9719d911017c592" fileSize="48213"
fileId="0199c0de-7a1e-7000-8000-0000000000ab" lastModified="08/12/2026
16:40:11" storageName="Finance-SMB" storageType="Category: FileShare,
Protocol: Smb, Vendor: Generic" storageId="7f3a9c14-2b8e-4d51-9a06-
c1e5b48f2d73" scanId="e1b6d842-0f37-4c9b-8a15-63d0947fe2ba"
scanName="Nightly Finance" scanType="Scheduled Process" <envelope
Category="1" LogType="206" UserName="system">] "Blocked file
remediation" applied to file (fileName: "invoice.docx"; ...) from
storage (name: "Finance-SMB"; ...) by scan (ID: "e1b6d842-0f37-4c9b-
8a15-63d0947fe2ba", ...). The blocked file was deleted.
```

LogType 207 to 215 — Remaining move, copy, delete and keep actions

All share the shape above. The differences are `PostAction`, `LogType`, and the outcome sentence.

LogType	Event	PostAction	Outcome sentence	Destination fields
207	Sanitized file moved	`Allowed file remediation`	`The sanitized file was moved to storage ...`	yes
208	Allowed file moved	`Allowed file remediation`	`The allowed file was moved to storage ...`	yes
209	Blocked file copied	`Blocked file remediation`	`The blocked file was copied to storage ...`	yes
210	Sanitized file copied	`Allowed file remediation`	`The sanitized file was copied to storage ...`	yes
211	Allowed file copied	`Allowed file remediation`	`The allowed file was copied to storage ...`	yes
212	Blocked file kept	`Blocked file remediation`	`The blocked file was kept.`	no
213	Allowed file kept	`Allowed file remediation`	`The allowed file was kept.`	no
214	Sanitized file kept	`Allowed file remediation`	`The sanitized file was kept on storage ...`	yes
215	Allowed file deleted	`Allowed file remediation`	`The allowed file was deleted from storage.`	no
221	Sanitized file deleted	`Allowed file remediation`	`The sanitized file was deleted from storage ...`	yes

PostAction does not distinguish sanitised from allowed

Sanitised-file remediations report `PostAction="Allowed file remediation"`. Use `LogType` to identify the specific action, not the `PostAction` text.

LogType 216 — File versions scanned

`PostAction="Scan file versions"`, no destination fields, no outcome sentence beyond the base text.

```
<110>1 2026-08-13T12:15:55.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta PostAction="Scan file
versions" fileName="invoice.docx" filePath="/finance/2026/invoice.docx"
fileHash="5d41402abc4b2a76b9719d911017c592" fileSize="48213"
fileId="0199c0de-7a1e-7000-8000-0000000000ab" lastModified="08/12/2026
16:40:11" storageName="Finance-SMB" storageType="Category: FileShare,
Protocol: Smb, Vendor: Generic" storageId="7f3a9c14-2b8e-4d51-9a06-
c1e5b48f2d73" scanId="e1b6d842-0f37-4c9b-8a15-63d0947fe2ba"
scanName="Nightly Finance" scanType="Scheduled Process" <envelope
Category="1" LogType="216" UserName="system">] "Scan file versions"
applied to file (fileName: "invoice.docx"; ...) from storage (name:
"Finance-SMB"; ...) by scan (ID: "e1b6d842-0f37-4c9b-8a15-
63d0947fe2ba", ...).
```

LogType 217 to 220 — Discovered file actions

Applied without scanning, by a discovery-only workflow. `PostAction="Discovered file remediation"`.

LogType	Event	Outcome sentence	Destination fields
217	Discovered file deleted	`The discovered file was deleted from storage.`	no
218	Discovered file moved	`The discovered file was moved to storage ...`	yes
219	Discovered file copied	`The discovered file was copied to storage ...`	yes
220	Discovered file kept	`The discovered file was kept.`	no

```
<110>1 2026-08-13T12:15:57.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta PostAction="Discovered file
remediation" fileName="old-report.xls" filePath="/finance/archive/old-
report.xls" fileHash="a87ff679a2f3e71d9181a67b7542122c"
fileSize="22100" fileId="0199c0de-7a1e-7000-8000-0000000000af"
lastModified="03/02/2024 11:20:00" storageName="Finance-SMB"
storageType="Category: FileShare, Protocol: Smb, Vendor: Generic"
storageId="7f3a9c14-2b8e-4d51-9a06-c1e5b48f2d73" scanId="e1b6d842-0f37-
4c9b-8a15-63d0947fe2ba" scanName="Nightly Finance" scanType="Scheduled
Process" <envelope Category="1" LogType="217" UserName="system">]
"Discovered file remediation" applied to file (fileName: "old-
report.xls"; filePath: "/finance/archive/old-report.xls"; fileHash:
"a87ff679a2f3e71d9181a67b7542122c"; fileSize: 22100; fileId: "0199c0de-
7a1e-7000-8000-0000000000af"; lastModified: 03/02/2024 11:20:00) from
storage (name: "Finance-SMB"; ...) by scan (ID: "e1b6d842-0f37-4c9b-
8a15-63d0947fe2ba", ...). The discovered file was deleted from storage.
```

Post-action failure

Any post action that fails is emitted at error severity, PRI `<107>`, with the same `LogType` and a different message:

```
<107>1 2026-08-13T12:15:58.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta PostAction="Blocked file
remediation" fileName="invoice.docx"
filePath="/finance/2026/invoice.docx"
fileHash="5d41402abc4b2a76b9719d911017c592" fileSize="48213"
fileId="0199c0de-7a1e-7000-8000-0000000000ab" lastModified="08/12/2026
16:40:11" storageName="Finance-SMB" storageType="Category: FileShare,
Protocol: Smb, Vendor: Generic" storageId="7f3a9c14-2b8e-4d51-9a06-
c1e5b48f2d73" scanId="e1b6d842-0f37-4c9b-8a15-63d0947fe2ba"
scanName="Nightly Finance" scanType="Scheduled Process" <envelope
Category="1" LogType="205" UserName="system">] "Blocked file
remediation" failed for file (fileName: "invoice.docx"; ...) from
storage (name: "Finance-SMB"; ...) by scan (ID: "e1b6d842-0f37-4c9b-
8a15-63d0947fe2ba", ...)
```

LogType 419 — Empty folders deleted

Folder paths are embedded directly in the message text, not as a field.

```
<110>1 2026-08-13T12:16:10.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta storageName="Finance-SMB"
storageType="Category: FileShare, Protocol: Smb, Vendor: Generic"
storageId="7f3a9c14-2b8e-4d51-9a06-c1e5b48f2d73" scanId="e1b6d842-0f37-
4c9b-8a15-63d0947fe2ba" scanName="Nightly Finance" scanType="Scheduled
Process" <envelope Category="1" LogType="419" UserName="system">] The
following empty folders have been deleted: [/finance/2026/tmp,
/finance/2026/old] from storage (name: "Finance-SMB"; "Category:
FileShare, Protocol: Smb, Vendor: Generic"; ID: "7f3a9c14-2b8e-4d51-
9a06-c1e5b48f2d73") by scan (ID: "e1b6d842-0f37-4c9b-8a15-
63d0947fe2ba", name: "Nightly Finance", type: "Scheduled Process") .
```

---

5. Category 2 — Storage units

`Category="2"`.

LogType 300 to 302 — Storage added, updated, removed

LogType	Action
300	added
301	updated
302	removed

Message fields: `storageName`, `storageType`, `storageId`, `Action`, `User`.

```
<110>1 2026-08-13T09:10:22.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta storageName="Finance-SMB"
storageType="Category: FileShare, Protocol: Smb, Vendor: Generic"
storageId="7f3a9c14-2b8e-4d51-9a06-c1e5b48f2d73" Action="added"
User="jdavis" <envelope Category="2" LogType="300" UserName="jdavis">]
Storage (name: "Finance-SMB"; "Category: FileShare, Protocol: Smb,
Vendor: Generic"; ID: "7f3a9c14-2b8e-4d51-9a06-c1e5b48f2d73") was
"added" by "jdavis".
```

Failure variant — error severity, PRI `<107>`. `was` becomes `could not be`:

```
... Storage (name: "Finance-SMB"; ...) could not be "added" by
"jdavis".
```

LogType 400 — Real-time processing changed

Real-time protection enabled, disabled or reconfigured on a storage.

Enabled, with a backfill start date:

```
<110>1 2026-08-13T09:12:00.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta Action="enabled"
User="jdavis" storageName="Finance-SMB" storageType="Category:
FileShare, Protocol: Smb, Vendor: Generic" storageId="7f3a9c14-2b8e-
4d51-9a06-c1e5b48f2d73" RealTimeStartDate="2026-08-13T00:00:00.000Z"
<envelope Category="2" LogType="400" UserName="jdavis">] Real Time
Process was "enabled" by "jdavis" for storage (name: "Finance-SMB";
"Category: FileShare, Protocol: Smb, Vendor: Generic"; ID: "7f3a9c14-
2b8e-4d51-9a06-c1e5b48f2d73") discovering files modified since "2026-
08-13T00:00:00.000Z"
```

Disabled — same shape with `Action="disabled"` and no `RealTimeStartDate`.

Handling type changed — a different message and a `NewHandlingType` field:

```
<110>1 2026-08-13T09:13:30.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta NewHandlingType="EventBased"
User="jdavis" storageName="Finance-SMB" storageType="Category:
FileShare, Protocol: Smb, Vendor: Generic" storageId="7f3a9c14-2b8e-
4d51-9a06-c1e5b48f2d73" <envelope Category="2" LogType="400"
UserName="jdavis">] Real Time Process handling type was changed to
"EventBased" by "jdavis" for storage (name: "Finance-SMB"; "Category:
FileShare, Protocol: Smb, Vendor: Generic"; ID: "7f3a9c14-2b8e-4d51-
9a06-c1e5b48f2d73")
```

Failure variant — error severity, PRI `<107>`, `was` becomes `could not be`.

---

6. Category 3 — Authentication

`Category="3"`.

LogType 600 — Signed in

Message field: `User`, the account's full name and user name.

```
<110>1 2026-08-13T12:15:42.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta User="John Davis (jdavis)"
<envelope Category="3" LogType="600" UserName="jdavis">] "John Davis
(jdavis)" logged in.
```

> **Failed sign-ins are not emitted**
>
> MDSS 4.5 emits this event only on a successful sign-in. There is no event for a rejected sign-in attempt, so this feed cannot be used for brute-force detection.

> Where MDSS runs behind SSO, the identity provider's own logs carry authentication failures.

LogType 601 — Signed out

```
<110>1 2026-08-13T13:02:19.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta User="John Davis (jdavis)"
<envelope Category="3" LogType="601" UserName="jdavis">] "John Davis
(jdavis)" logged out.
```

A sign-out that does not complete cleanly is emitted at warning severity, PRI `<108>`, with the text `"John Davis (jdavis)" encountered an issue while logging out.`

---

7. Category 4 — Settings

`Category="4"`. Configuration changes across the product.

LogType 700 to 703 — Scan engine instance changed

Message fields: `ScanInstance` (the engine URL), `Action`.

LogType	Action
700	added
701	updated
702	deleted
703	imported

```
<110>1 2026-08-13T08:40:05.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta ScanInstance="https://core-
01:8008" Action="added" <envelope Category="4" LogType="700"
UserName="jdavis">] Scan Instance "https://core-01:8008" was "added" by
"jdavis".
```

Failure variant — error severity, PRI `<107>`, with `ResponseMessage`:

```
<107>1 ... [meta Action="add" ScanInstance="https://core-01:8008"
ResponseMessage="Connection refused" <envelope Category="4"
LogType="700" UserName="jdavis">] Unable to "add" Scan Instance
"https://core-01:8008". Response message: "Connection refused".
```

LogType 750 to 753 — Scan pool changed

Message fields: `ScanPool` (the pool name), `Action`. Same actions and failure shape as scan instances.

```
<110>1 2026-08-13T08:42:11.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta ScanPool="Primary pool"
Action="added" <envelope Category="4" LogType="750" UserName="jdavis">]
Scan Pool "Primary pool" was "added" by "jdavis".
```

LogType 800 to 802 — Licence activation

Message fields: `Action`, `User`.

LogType	Action
800	online activated
801	offline activated
802	deactivated

```
<110>1 2026-08-13T08:05:00.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta Action="online activated "
User="jdavis" <envelope Category="4" LogType="800" UserName="jdavis">]
License was "online activated " by "jdavis".
```

Failure variant — error severity, PRI `<107>`. `was` becomes `failed to be`.

LogType 900 — Configuration imported

Message fields: `Action`, `User`. The inclusion summary is part of the message text.

```
<110>1 2026-08-13T08:12:44.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta Action="imported"
User="jdavis" <envelope Category="4" LogType="900" UserName="jdavis">]
Configuration was "imported" by "jdavis". License was included. SMTP
configuration was included. Retention configuration was not included.
Notifications configuration was partially included. Users were included
```

Failure variant — error severity, PRI `<107>`, with `FailureReason`:

```
<107>1 ... [meta Action="imported" User="jdavis" FailureReason="the
provided password is incorrect" <envelope Category="4" LogType="900"
UserName="jdavis">] Configuration failed to be "imported" by "jdavis"
because "the provided password is incorrect".
```

Other failure reasons: `the configuration file could not be upgraded`, `the configuration file is empty`, `the license could not be activated`, `the deserialization of the configuration file has failed`, `the provided configuration file version is not supported`, `the configuration file has an invalid structure`.

LogType 901 — Configuration exported

Identical shape with `Action="exported"`.

```
<110>1 2026-08-13T08:14:02.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta Action="exported"
User="jdavis" <envelope Category="4" LogType="901" UserName="jdavis">]
Configuration was "exported" by "jdavis". License was included. SMTP
configuration was included. Retention configuration was included.
Notifications configuration was included. Users were not included
```

LogType 950 — Notification settings changed

Message fields: `NotificationType`, `Action`, `User`.

```
<110>1 2026-08-13T08:30:10.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta NotificationType="Blocked
file notifications" Action="enabled" User="jdavis" <envelope
Category="4" LogType="950" UserName="jdavis">] "Blocked file
notifications" were "enabled" by "jdavis".
```

`NotificationType` is one of: `Email notifications for scan reports`, `Email notifications scan reports recipients`, `Blocked file notifications`, `Blocked file notifications recipients`, `User request notifications`, `Webhook Scan completed notifications`, `Webhook Scan completed notifications details`, `Webhook File scanned notifications details`, `RabbitMq file scanned notifications details`, `Email notifications settings`, `Webhook notifications settings`, `RabbitMQ notifications settings`.

`Action` is `enabled`, `disabled` or `updated`. **Failure variant** — error severity, PRI `<107>`, `were` becomes `could not be`.

> **LogType 950 appears in two categories**
>
> With `Category="4"` it is a settings change, as above. With `Category="8"` it is a notification delivery result — see section 9. Filter on both fields together.

LogType 975 — SMTP configuration changed

Message fields: `Action` (`enabled`, `disabled`, `updated`), `User`.

```
<110>1 2026-08-13T08:33:20.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta Action="updated"
User="jdavis" <envelope Category="4" LogType="975" UserName="jdavis">]
SMTP configuration was "updated" by "jdavis".
```

Failure variant — error severity, PRI `<107>`, `was` becomes `could not be`.

LogType 1000 — External logger added

The server details are embedded in the message text. Message fields: `Action`, `User`.

```
<110>1 2026-08-13T10:01:00.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta Action="added" User="jdavis"
<envelope Category="4" LogType="1000" UserName="jdavis">] External
logger (serverAddress: siem.example.com; port: 6514) was "added" by
"jdavis".
```

LogType 1001 — External logger updated

Also used when a destination is enabled or disabled, with `Action="enabled"` or `Action="disabled"`.

```
<110>1 2026-08-13T10:03:15.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta Action="disabled"
User="jdavis" <envelope Category="4" LogType="1001" UserName="jdavis">]
External logger (serverAddress: siem.example.com; port: 6514) was
"disabled" by "jdavis".
```

LogType 1002 — External logger deleted

`Action="removed"`.

```
<110>1 2026-08-13T10:05:40.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta Action="removed"
User="jdavis" <envelope Category="4" LogType="1002" UserName="jdavis">]
External logger (serverAddress: siem.example.com; port: 6514) was
"removed" by "jdavis".
```

Failure variants — error severity, PRI `<107>`. Six distinct messages, all with fields `User` and `Action` in present tense (`adding`, `updating`, `removing`, `enabling`, `disabling`):

Cause	Message
Duplicate	`"jdavis" "adding" external logger failed because one with the same configuration already exists.`
Connection test failed	`"jdavis" "adding" external logger failed because the configuration is not valid.`
Not found	`"jdavis" "removing" external logger failed because the configuration does not exist.`
Already in that state	`"jdavis" "enabling" external logger failed because it was already "enabled".`
Limit reached	`"jdavis" "adding" external logger failed because because the maximum number of the same integration type was exceeded.`
Unexpected error	`"jdavis" "adding" external logger failed because an unexpected error occurred.`

LogType 1100 — Data retention changed

Message field: `User`. The detail sentence is part of the message text.

```
<110>1 2026-08-13T08:50:00.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta User="John Davis (jdavis)"
<envelope Category="4" LogType="1100" UserName="jdavis">] Data
retention configuration was successfully updated by "John Davis
(jdavis)". Audit logs older than 90 days will be deleted.
```

Detail sentences, by action:

Action	Success sentence	Failure sentence
Enable report retention	`Reports retention is enabled.`	`Reports retention could not be enabled.`
Disable report retention	`Reports retention is disabled.`	`Reports retention could not be disabled.`
Change report retention days	`Reports older than 90 days will be deleted.`	`Retention days could not be updated for reports.`
Change audit retention days	`Audit logs older than 90 days will be deleted.`	`Retention days could not be updated for audit logs.`
Change RTP history retention days	`Files processed during Real-Time Processing older than 30 days will be deleted.`	`Retention days could not be updated for Real-Time Processing history.`

On failure, severity is error, PRI `<107>`, and `was successfully` becomes `could not be`.

LogType 1200 to 1202 — API key changed

The key value is truncated to its first six characters. Message fields: `TruncatedAPIKey`, `Action`, `User`.

LogType	Action
1200	added
1201	updated
1202	deleted

```
<110>1 2026-08-13T09:00:00.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta TruncatedAPIKey="a3f9c1"
Action="added" User="John Davis (jdavis)" <envelope Category="4"
LogType="1200" UserName="jdavis">] API Key "a3f9c1..." was "added" by
"John Davis (jdavis)".
```

Failure variant — error severity, PRI `<107>`, with `FailureReason`:

```
<107>1 ... [meta User="John Davis (jdavis)" Action="add"
TruncatedAPIKey="a3f9c1" FailureReason="an API Key with the same value
already exists" <envelope Category="4" LogType="1200"
UserName="jdavis">] User "John Davis (jdavis)" was unable to "add" API
Key "a3f9c1" because "an API Key with the same value already exists".
```

Other failure reasons: `an unexpected error occurred`, `the requested user was not found`, `the requested API Key was not found`, `a key rotation is currently in progress`.

> **API key usage is not audited**
>
> These events cover the key's lifecycle only. Requests authenticated with an API key do not produce audit events.

LogType 1300 — SSO configuration changed

Enabled or reconfigured — fields `User`, `SsoType`, `SsoProvider`, `Authority`:

```
<110>1 2026-08-13T09:05:00.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta User="John Davis (jdavis)"
SsoType="Oidc" SsoProvider="AzureAd"
Authority="https://login.microsoftonline.com/contoso" <envelope
Category="4" LogType="1300" UserName="jdavis">] "John Davis (jdavis)"
changed Single Sign-On configuration to type "Oidc", provider
"AzureAd", authority "https://login.microsoftonline.com/contoso".
```

Disabled — field `User` only:

```
<110>1 ... [meta User="John Davis (jdavis)" <envelope Category="4"
LogType="1300" UserName="jdavis">] "John Davis (jdavis)" disabled
Single Sign-On configuration.
```

Failure variant — error severity, PRI `<107>`:

```
<107>1 ... [meta User="John Davis (jdavis)" <envelope Category="4"
LogType="1300" UserName="jdavis">] "John Davis (jdavis)" tried to
change the Single Sign-On configuration, but failed.
```

LogType 1410 — Workflow scanning modules changed

Message fields: `WorkflowId`, `Technologies`.

```
<110>1 2026-08-13T09:30:00.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta WorkflowId="9d4e1f60-3a72-
4b85-8c19-f2073be5a1c8" Technologies="Antimalware, DeepCdr,
VulnerabilityAssessment" <envelope Category="4" LogType="1410"
UserName="jdavis">] Scanning modules for Workflow "9d4e1f60-3a72-4b85-
8c19-f2073be5a1c8" have been updated. New values: "Antimalware,
DeepCdr, VulnerabilityAssessment".
```

LogType 1600 — On-demand scan requested

Single file — file identity fields plus `UserName`:

```
<110>1 2026-08-13T11:20:00.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta fileName="invoice.docx"
filePath="/finance/2026/invoice.docx"
fileHash="5d41402abc4b2a76b9719d911017c592" fileSize="48213"
fileId="0199c0de-7a1e-7000-8000-0000000000ab" lastModified="08/12/2026
16:40:11" UserName="jdavis" <envelope Category="4" LogType="1600"
UserName="jdavis">] Successfully sent request to scan file on demand
(fileName: "invoice.docx"; filePath: "/finance/2026/invoice.docx";
fileHash: "5d41402abc4b2a76b9719d911017c592"; fileSize: 48213; fileId:
"0199c0de-7a1e-7000-8000-0000000000ab"; lastModified: 08/12/2026
16:40:11) . Action performed by "jdavis"
```

Filtered rescan of many files — scan fields instead of file fields:

```
<110>1 2026-08-13T11:22:30.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta scanId="e1b6d842-0f37-4c9b-
8a15-63d0947fe2ba" scanName="Nightly Finance" scanType="Scheduled
Process" UserName="jdavis" <envelope Category="4" LogType="1600"
UserName="jdavis">] Successfully sent request to rescan multiple files
on demand for (ID: "e1b6d842-0f37-4c9b-8a15-63d0947fe2ba", name:
"Nightly Finance", type: "Scheduled Process") . Action performed by
"jdavis"
```

LogType 2000 — Encryption key event

Key generation — fields `Action` and `ActionAndUser`:

```
<110>1 2026-08-13T02:00:00.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta Action="Started"
ActionAndUser="was started by John Davis (jdavis)" <envelope
Category="4" LogType="2000" UserName="jdavis">] Key generation "was
started by John Davis (jdavis)".
```

Completion reads `Key generation "was completed".` Failure reads `Key generation "failed".` at error severity, PRI `<107>`.

Request cancelled during key rotation — field `Request`:

```
<108>1 2026-08-13T02:00:30.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta Request=" POST /api/storage"
<envelope Category="4" LogType="2000" UserName="jdavis">] Request "
POST /api/storage" was cancelled because a key rotation is currently in
progress.
```

LogType 2200 — HTTPS certificate changed

Message fields: `ActionMessage`, `User`.

```
<110>1 2026-08-13T07:45:00.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta ActionMessage="enabled, and
certificate was updated" User="John Davis (jdavis)" <envelope
Category="4" LogType="2200" UserName="jdavis">] HTTPS was "enabled, and
certificate was updated" by "John Davis (jdavis)".
```

Disabling reads `HTTPS was "disabled" by "John Davis (jdavis)".`

LogType 2300 — Telemetry configuration changed

Message field: `Status`. Emitted by the system on startup reconciliation, or by an administrator.

```
<110>1 2026-08-13T07:30:00.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta Status="enabled" <envelope
Category="4" LogType="2300" UserName="jdavis">] Telemetry configuration
was updated. Status: "enabled"
```

---

8. Category 6 — Users

`Category="6".`

LogType 602 to 606 — User account changed

Message fields: `Username` (the account acted on), `Action`.

LogType	Event	Action	Message
602	User created	created	User "mrossi" was "created".
603	User registered	registered	User "mrossi" was "registered".
604	User role updated	updated	User "mrossi"'s role was "updated".
605	User updated	updated	User "mrossi" was "updated".
605	Password reset	reset	User "mrossi"'s password was "reset".

```
<110>1 2026-08-13T09:40:00.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta Username="mrossi"
Action="created" <envelope Category="6" LogType="602"
UserName="mrossi">] User "mrossi" was "created".
```

Role update:

```
<110>1 2026-08-13T09:41:15.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta Username="mrossi"
Action="updated" <envelope Category="6" LogType="604"
UserName="mrossi">] User "mrossi"'s role was "updated".
```

Removal uses `LogType="606"` with `Action="removed"`.

> **Password reset shares LogType 605 with user update**
>
> Both are `LogType="605"`. Distinguish them by the message text or the `Action` field — `reset` versus `updated`.

Failure variant — error severity, PRI `<107>`:

```
<107>1 ... [meta Username="mrossi" Action="created" <envelope
Category="6" LogType="602" UserName="mrossi">] User "mrossi" could not
be "created".
```

> **The actor is the account acted on, not the administrator**
>
> On these events `UserName` and `UserId` identify the user being created, updated or removed. The administrator who performed the action appears in the message text only when MDSS has it, so do not rely on the envelope to identify the operator here.

LogType 1800 — Product tour finalised

Message fields: `UserName`, `TourType`.

```
<110>1 2026-08-13T09:50:00.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta UserName="jdavis"
TourType="Onboarding" <envelope Category="6" LogType="1800"
UserName="jdavis">] User "jdavis" finalized user tour "Onboarding".
```

9. Category 8 — Notifications

`Category="8"`. Delivery results for outbound notifications. All emitted by the system, so `UserName="system"`.

LogType 950 — Email notification sent

Recipients and the notification description are embedded in the message text; there are no message fields.

```
<110>1 2026-08-13T12:16:20.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta <envelope Category="8"
LogType="950" UserName="system">] Email notification for blocked file
invoice.docx was sent to: soc@example.com, ciso@example.com
```

Notification descriptions, by type:

Type	Description text
Report generated	`Email notification that contains the scan Nightly Finance report`
New user registered	`Email notification for the new registered user`
User request processed	`Email notification after user request was processed`
Password reset	`Email notification that contains the password reset details`
Password reset completed	`Email confirmation after password reset`
Blocked file	`Email notification for blocked file invoice.docx`
User updated	`Email confirmation after user update`
Generic	`Email notification`

Partial delivery failure — the message names both sets of recipients:

```
<110>1 ... [meta <envelope Category="8" LogType="950"
UserName="system">] Email notification for blocked file invoice.docx
was sent to: soc@example.com Email could not be sent to:
ciso@example.com
```

Total delivery failure — error severity, PRI `<107>`:

```
<107>1 ... [meta <envelope Category="8" LogType="950"
UserName="system">] Email notification for blocked file invoice.docx
could not be sent to: soc@example.com, ciso@example.com
```

No recipient configured — error severity, PRI `<107>`:

```
<107>1 ... [meta <envelope Category="8" LogType="950"
UserName="system">] Email notification for blocked file invoice.docx
could not be sent. The recipient could not be found.
```

LogType 950 — Webhook notification sent

Message field: `ScanName` or `FileName`.

```
<110>1 2026-08-13T12:16:25.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta ScanName="Nightly Finance"
<envelope Category="8" LogType="950" UserName="system">] Webhook
notification for completion of scan "Nightly Finance" was successfully
sent
```

```
<110>1 2026-08-13T12:16:26.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta FileName="invoice.docx"
<envelope Category="8" LogType="950" UserName="system">] Webhook
notification for scanned file "invoice.docx" was successfully sent
```

Failure variants — error severity, PRI `<107>`: `Failed to send webhook notification for scan "Nightly Finance"` and `Failed to send webhook notification for scanned file "invoice.docx"`.

LogType 950 — Message-queue notification sent

Message field: `FileName`.

```
<110>1 2026-08-13T12:16:27.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta FileName="invoice.docx"
<envelope Category="8" LogType="950" UserName="system">] RabbitMQ
notification for scanned file "invoice.docx" was successfully sent
```

Failure variant — error severity, PRI `<107>`: `Failed to send RabbitMQ notification for scanned file "invoice.docx"`.

LogType 1700 — Report generated

Message fields: scan fields.

```
<110>1 2026-08-13T12:20:00.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta scanId="e1b6d842-0f37-4c9b-
8a15-63d0947fe2ba" scanName="Nightly Finance" scanType="Scheduled
Process" <envelope Category="8" LogType="1700" UserName="system">] PDF
Report of scan (ID: "e1b6d842-0f37-4c9b-8a15-63d0947fe2ba", name:
"Nightly Finance", type: "Scheduled Process") has been created
```

---

10. Category 9 — Group units

`Category="9"`.

LogType 320 to 322 — Group added, updated, removed

Message fields: `groupName`, `groupId`, `Action`, `User`.

LogType	Action
320	added
321	updated
322	removed

```
<110>1 2026-08-13T09:15:00.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta groupName="Finance shares"
groupId="4e7c9105-8d26-4a3f-b012-75ea3c6f81db" Action="added"
User="jdavis" <envelope Category="9" LogType="320" UserName="jdavis">]
Group (name: "Finance shares";  ID: "4e7c9105-8d26-4a3f-b012-
75ea3c6f81db") was "added" by "jdavis".
```

Failure variant — error severity, PRI `<107>`, `was` becomes `could not be`.

---

11. Category 10 — Account units

`Category="10"`.

LogType 330 to 332 — Account added, updated, removed

Message fields: `accountName`, `accountId`, `Action`, `User`.

LogType	Action
330	added
331	updated
332	removed

```
<110>1 2026-08-13T09:17:30.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta accountName="contoso-svc"
accountId="6f18b3d4-9e07-42ca-8b53-1d904af7e26c" Action="added"
User="jdavis" <envelope Category="10" LogType="330" UserName="jdavis">]
Account (name: "contoso-svc";  ID: "6f18b3d4-9e07-42ca-8b53-
1d904af7e26c") was "added" by "jdavis".
```

Failure variant — error severity, PRI `<107>`, `was` becomes `could not be`.

---

12. Category 11 — Remediations

`Category="11"`. Changes to remediation rules. Rule *execution* appears in category 1.

LogType 2101 to 2103 — Remediation rule added, updated, deleted

Message fields: `Type`, `HandlingType`, `WorkflowId`, `WorkflowName`, `Action`, `UserName`.

LogType	Action
2101	added
2102	updated
2103	deleted

```
<110>1 2026-08-13T09:35:00.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta Type="BlockedFileRemediation"
HandlingType="Move" WorkflowId="9d4e1f60-3a72-4b85-8c19-f2073be5a1c8"
WorkflowName="Default workflow" Action="added" UserName="jdavis"
<envelope Category="11" LogType="2101" UserName="jdavis">] Remediation
of type "BlockedFileRemediation" with "Move" action for Workflow (Id:
"9d4e1f60-3a72-4b85-8c19-f2073be5a1c8"; Name: "Default workflow") was
"added" by "jdavis".
```

`Type` is one of `FileTagging`, `BlockedFileRemediation`, `AllowedFileRemediation`, `AllowedSanitizedFileRemediation`, `BlockedSanitizedFileRemediation`, `DiscoveredFileRemediation`, `DeepCdr`, `DeleteEmptyFoldersRemediation`, `ScanFileVersions`. `HandlingType` is `Move`, `Copy`, `Delete`, `Keep` or `NotApplicable`.

Rule disabled — no `HandlingType`:

```
<110>1 ... [meta Type="BlockedFileRemediation" WorkflowId="9d4e1f60-3a72-4b85-8c19-f2073be5a1c8" WorkflowName="Default workflow" UserName="jdavis" <envelope Category="11" LogType="2102" UserName="jdavis">] Remediation of type "BlockedFileRemediation" was disabled for Workflow (Id: "9d4e1f60-3a72-4b85-8c19-f2073be5a1c8"; Name: "Default workflow") by "jdavis".
```

Empty-folder remediation — adds a `Depth` field:

```
<110>1 ... [meta Type="DeleteEmptyFoldersRemediation" WorkflowId="9d4e1f60-3a72-4b85-8c19-f2073be5a1c8" WorkflowName="Default workflow" Depth="3" Action="added" UserName="jdavis" <envelope Category="11" LogType="2101" UserName="jdavis">] Remediation of type "DeleteEmptyFoldersRemediation" for Workflow (Id: "9d4e1f60-3a72-4b85-8c19-f2073be5a1c8"; Name: "Default workflow") with folder depth: 3 was "added" by "jdavis".
```

Failure variant — error severity, PRI `<107>`:

```
<107>1 ... [meta Type="BlockedFileRemediation" WorkflowId="9d4e1f60-3a72-4b85-8c19-f2073be5a1c8" WorkflowName="Default workflow" <envelope Category="11" LogType="2101" UserName="jdavis">] Unable to use remediation of "BlockedFileRemediation" for Workflow (Id: "9d4e1f60-3a72-4b85-8c19-f2073be5a1c8"; Name: "Default workflow")
```

---

13. Category 12 — Workflows

`Category="12"`.

LogType 1400 to 1404 — Workflow changed

Message fields: `WorkflowId`, `WorkflowName`, `Action`, `UserName`, and — except on delete — `FileDefinitionMode`.

LogType	Action
1400	added
1401	updated
1402	deleted
1403	set as default
1404	imported

```
<110>1 2026-08-13T09:32:00.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta WorkflowId="9d4e1f60-3a72-
4b85-8c19-f2073be5a1c8" WorkflowName="Default workflow" Action="added"
UserName="jdavis" FileDefinitionMode="Strict" <envelope Category="12"
LogType="1400" UserName="jdavis">] Workflow (Id: "9d4e1f60-3a72-4b85-
8c19-f2073be5a1c8"; Name: "Default workflow")  was "added" by "jdavis".
File Definition: mode - "Strict"
```

With the configurable blocking strategy, `FileDefinitionMode="Configurable"` and the message lists the individual blocking options.

Failure variant — error severity, PRI `<107>`, with `ErrorMessage`:

```
<107>1 ... [meta Action="add" Workflow="Default workflow"
ErrorMessage="A workflow with this name already exists"
UserName="jdavis" FileDefinitionMode="Strict" <envelope Category="12"
LogType="1400" UserName="jdavis">] Unable to "add" Workflow "Default
workflow". Response message: "A workflow with this name already
exists". Action performed by "jdavis". File Definition: mode - "Strict"
```

---

14. Category 13 — Access control

`Category="13"`. Role and permission assignment. Message field: `User`. The description is part of the message text.

LogType 2400 to 2412

LogType	Event	Success message	Failure message
2400	Role assigned	Role was assigned to a user by "John Davis (jdavis)".	Role could not be assigned to a user by "John Davis (jdavis)".
2401	Role removed	Role was removed from a user by "John Davis (jdavis)".	Role could not be removed from a user by "John Davis (jdavis)".
2402	Custom role created	Custom role was created by "John Davis (jdavis)".	Custom role could not be created by "John Davis (jdavis)".
2403	Custom role deleted	Custom role was deleted by "John Davis (jdavis)".	Custom role could not be deleted by "John Davis (jdavis)".
2410	Permission assigned	Permission was assigned to a user by "John Davis (jdavis)".	Permission could not be assigned to a user by "John Davis (jdavis)".
2411	Permission removed	Permission was removed from a user by "John Davis (jdavis)".	Permission could not be removed from a user by "John Davis (jdavis)".
2412	Roles replaced	Roles were replaced for a user by "John Davis (jdavis)".	Roles could not be replaced for a user by "John Davis (jdavis)".

```
<110>1 2026-08-13T09:45:00.000000+02:00 mdss-prod-01
MetaDefenderStorageSecurity 27725 - [meta User="John Davis (jdavis)"
<envelope Category="13" LogType="2400" UserName="jdavis">] Role was
assigned to a user by "John Davis (jdavis)".
```

Failure variants are emitted at error severity, PRI `<107>`.

> **The affected user is not a field**
>
> These events name the administrator who made the change, not the user whose access changed. The target user is not carried on the event.

15. Reserved event types

The schema defines 112 event types. The 14 below are reserved and are **not** emitted by MDSS 4.5. Do not build rules that depend on them.

LogType	Reserved name
201	File sanitized, original kept
203	File sanitized, original deleted
204	File decryption
350	Security checklist item
351	Security checklist verified
410	File tagging
411	Deep CDR remediation
412	Sanitized files remediation
413	Blocked files remediation
414	Treat files with sensitive data as blocked
415	Treat files with vulnerabilities as blocked
416	Allowed files remediation
417	Strict block files strategy
418	Configurable block files strategy

Category `7` (security checklist) is reserved for the same reason, and category `5` is not defined.

Parsers should handle unrecognised `LogType` and `Category` values without failing — new values may be added in later releases.

16. Quick index

LogType	Event	Category
0	File discovered	0
1	File scanned	0
2	File discovery failed or skipped	0
3	File cancelled	0
100	Scan process started	0
101	Scan process completed	0
102	Scan process cancelled	0
103	Scan process failed	0
200	File tagged	1
205	Blocked file moved	1
206	Blocked file deleted	1
207	Sanitized file moved	1
208	Allowed file moved	1
209	Blocked file copied	1
210	Sanitized file copied	1
211	Allowed file copied	1
212	Blocked file kept	1
213	Allowed file kept	1
214	Sanitized file kept	1
215	Allowed file deleted	1
216	File versions scanned	1
217	Discovered file deleted	1
218	Discovered file moved	1
219	Discovered file copied	1
220	Discovered file kept	1

221	Sanitized file deleted	1
300	Storage added	2
301	Storage updated	2
302	Storage removed	2
320	Group added	9
321	Group updated	9
322	Group removed	9
330	Account added	10
331	Account updated	10
332	Account removed	10
400	Real-time processing changed	2
419	Empty folders deleted	1
600	Signed in	3
601	Signed out	3
602	User created	6
603	User registered	6
604	User role updated	6
605	User updated or password reset	6
606	User removed	6
700	Scan instance added	4
701	Scan instance updated	4
702	Scan instance deleted	4
703	Scan instance imported	4
750	Scan pool added	4
751	Scan pool updated	4
752	Scan pool deleted	4
753	Scan pool imported	4

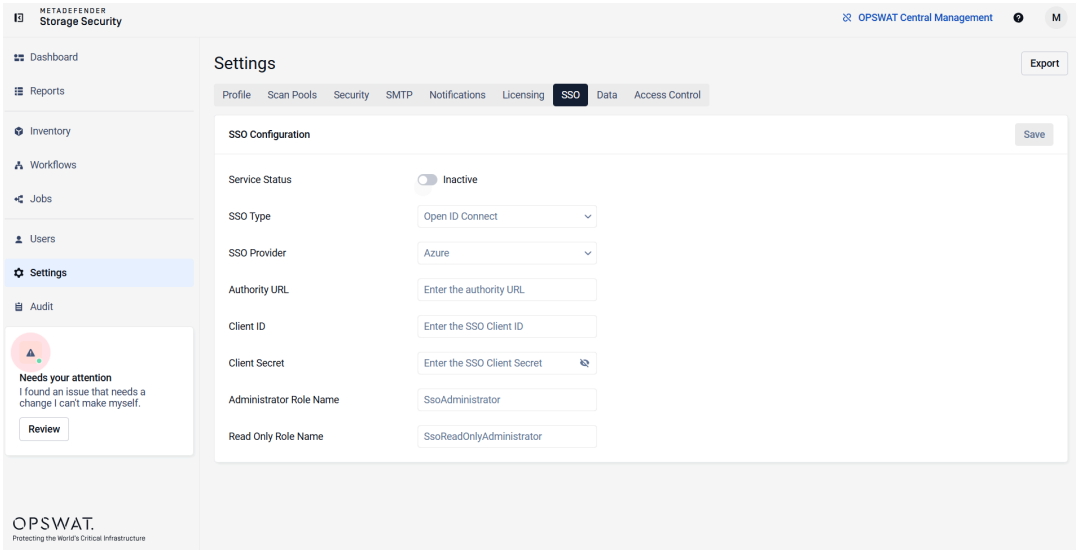
800	Licence activated online	4
801	Licence activated offline	4
802	Licence deactivated	4
900	Configuration imported	4
901	Configuration exported	4
950	Notification settings changed	4
950	Notification delivery result	8
975	SMTP configuration changed	4
1000	External logger added	4
1001	External logger updated, enabled or disabled	4
1002	External logger deleted	4
1100	Data retention changed	4
1200	API key added	4
1201	API key updated	4
1202	API key deleted	4
1300	SSO configuration changed	4
1400	Workflow added	12
1401	Workflow updated	12
1402	Workflow deleted	12
1403	Workflow set as default	12
1404	Workflow imported	12
1410	Workflow scanning modules changed	4
1500	Scan added	0
1501	Scan updated	0
1502	Scan deleted	0
1503	Scan imported	0
1600	On-demand scan requested	4

1700	Report generated	8
1800	Product tour finalised	6
1900	Scan schedule added	0
1901	Scan schedule updated	0
1902	Scan schedule deleted	0
1903	Scan schedule imported	0
1904	Scan schedule skipped	0
2000	Encryption key event	4
2101	Remediation rule added	11
2102	Remediation rule updated	11
2103	Remediation rule deleted	11
2200	HTTPS certificate changed	4
2300	Telemetry configuration changed	4
2400	Role assigned	13
2401	Role removed	13
2402	Custom role created	13
2403	Custom role deleted	13
2410	Permission assigned	13
2411	Permission removed	13
2412	Roles replaced	13

Single Sign On

In order to configure Single Sign On:

1. Navigate to **Settings -> Single Sign On**



2. **Enable** the Single Sign On toggle
3. Select the desired **Single Sign On Provider**
4. Select the desired **Single Sign On Type**
5. Enter the **Client ID**
6. Enter the **Client Secret**
7. Enter the **Authority URL**

> **Info**
>
> For the purpose of secure authentication, when configuring any SSO provider, either HTTPS need to be enabled for MDSS, or the web interface needs to be accessed through **localhost** instead of the deployment machine's IP.

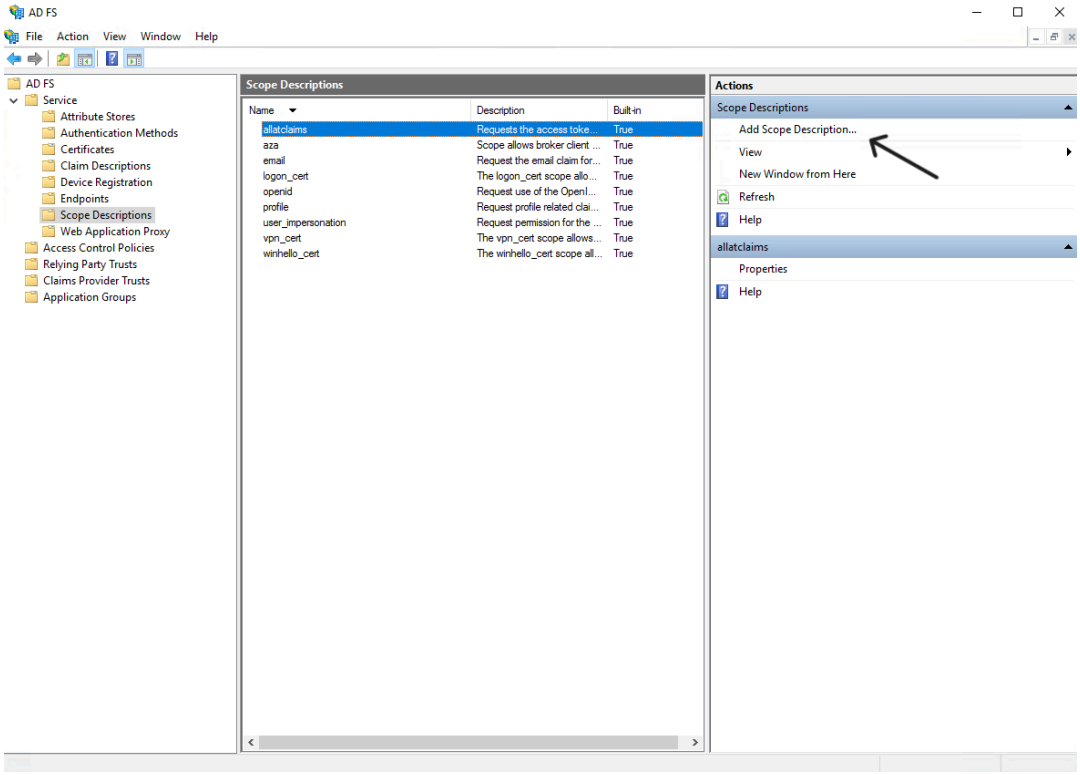
AD FS Specific Configuration

> **Info**
>
> To properly access MDSS, the following AD **Security Groups** are required:
>
> - **SsoAdministrator** - the equivalent of local MetaDefender Storage Security administrator role

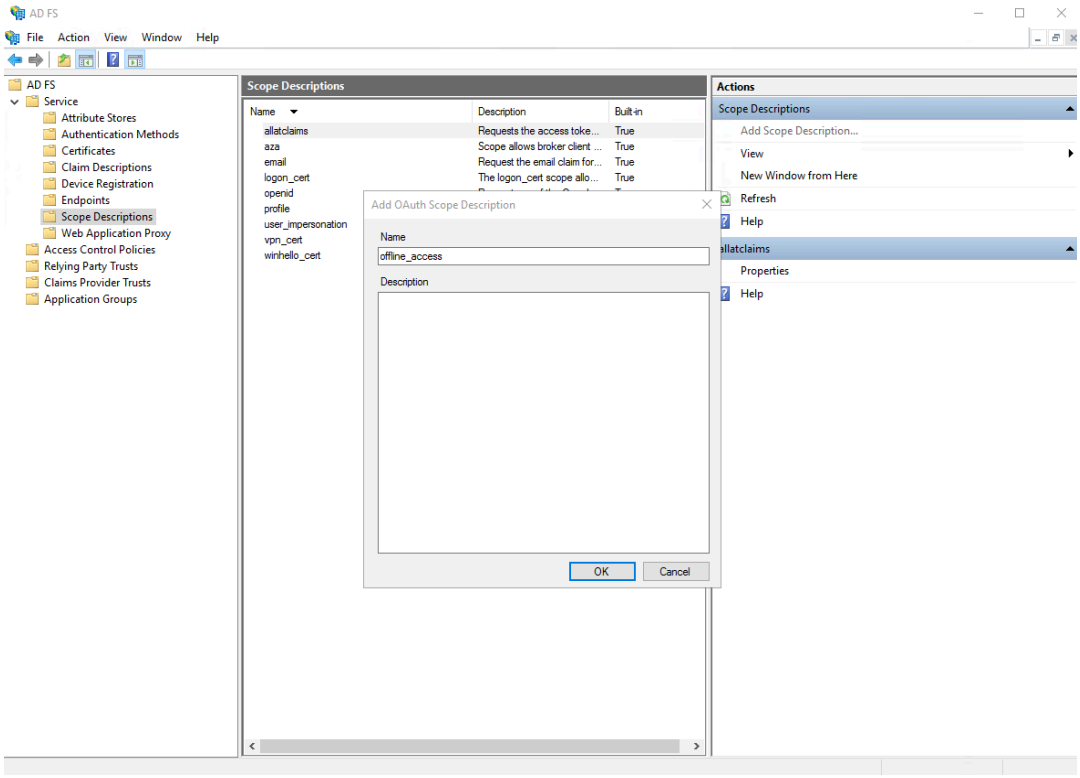
> It is also necessary for the AD user to have an **email address** set up, so that it is set as the MetaDefender Storage Security's user email

To set up AD FS SSO for MDSS, follow these steps:

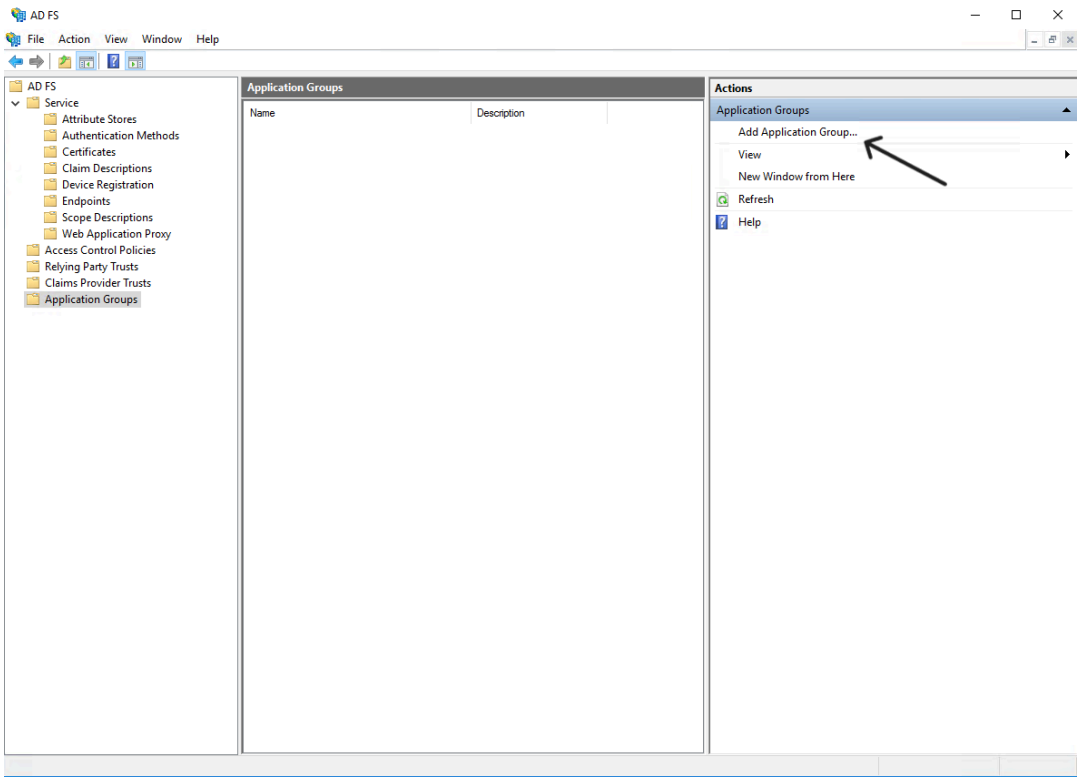
1. Within the AD FS settings, navigate to the "**Scope Descriptions**" directory and click "**Add Scope Description**"



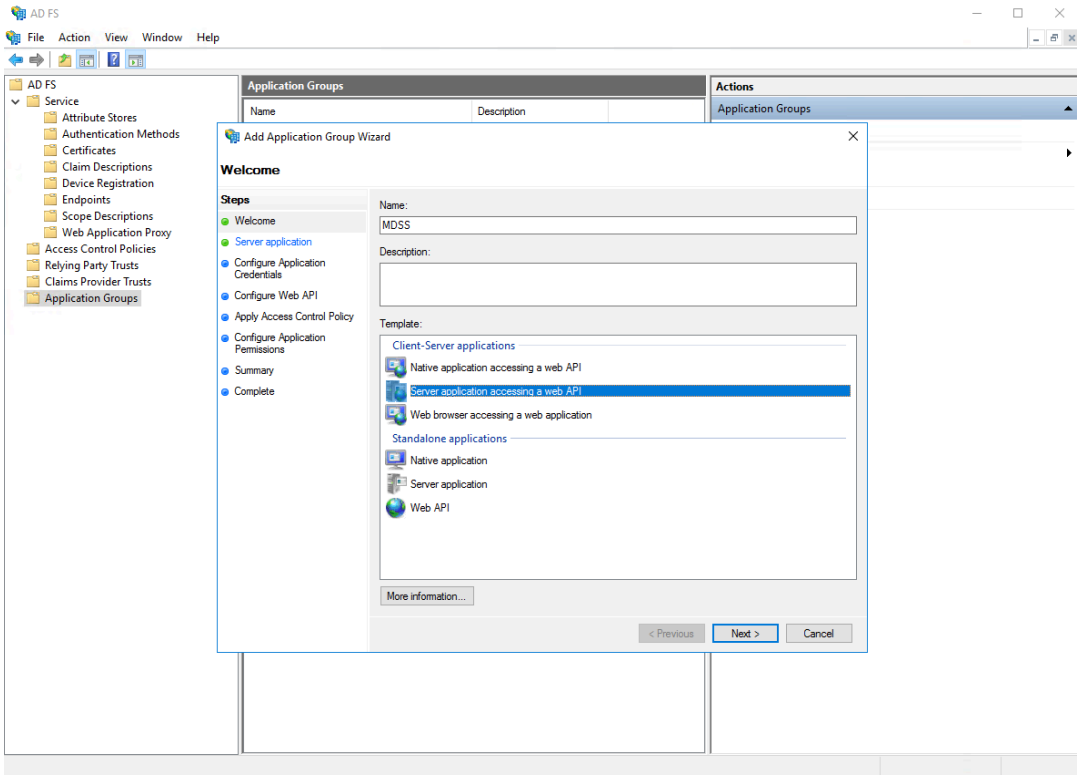
2. Create a scope with the name "**offline_access**"



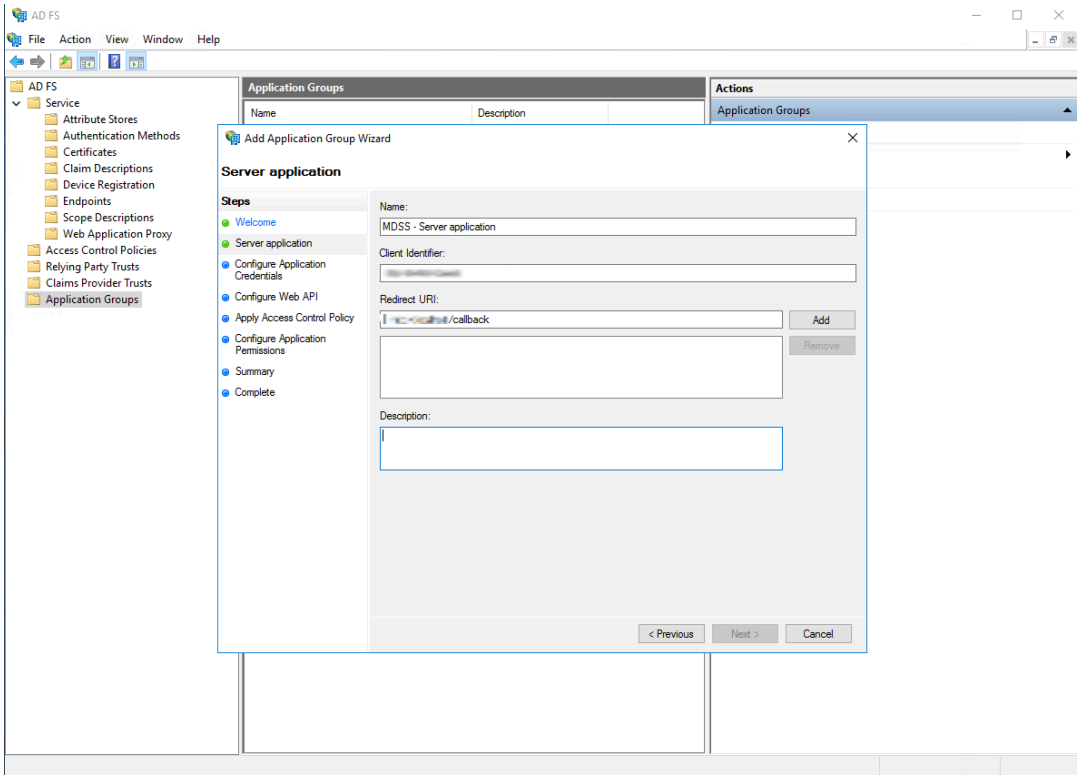
3. Navigate to the "**Application groups**" directory and click "**Add Application Group**"



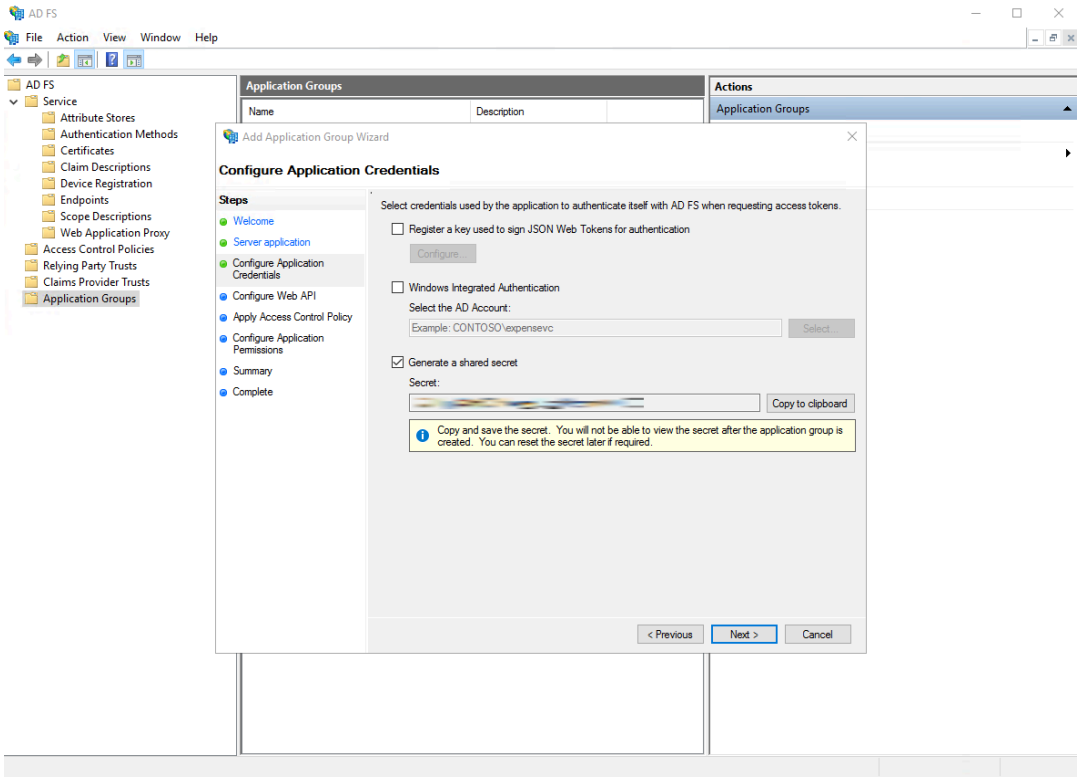
4. Give your application any name you like and for the template, select "**Server application accessing a web API**"



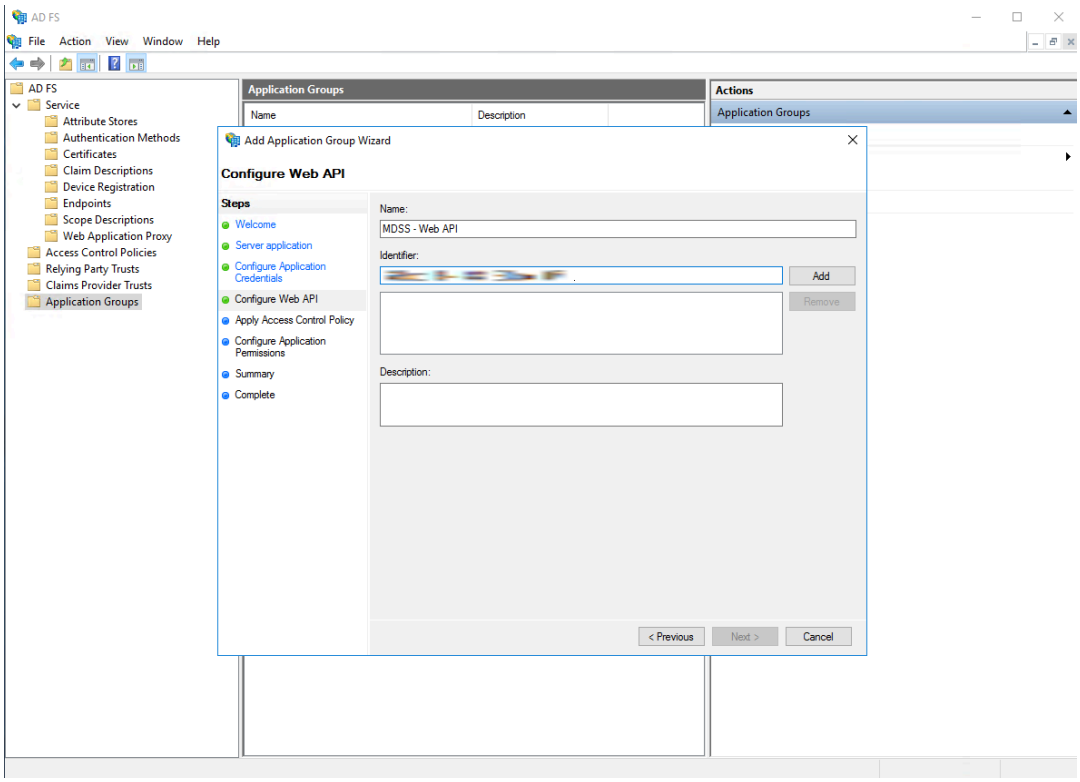
5. Give the server app a name, save the generated **Client Identifier** somewhere, and as the "**Redirect URI**", write the the base URL of the MDSS deployment, followed by the "**/callback**" suffix.



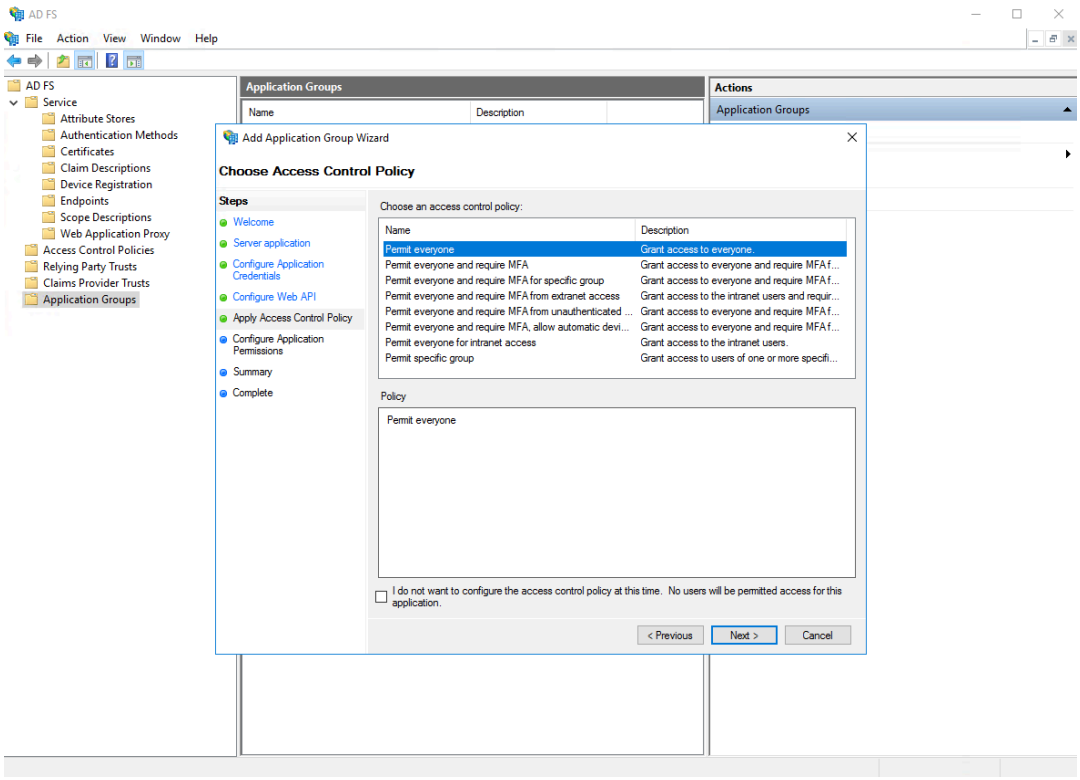
6. Select "**Generate a shared secret**" and store the secret somewhere



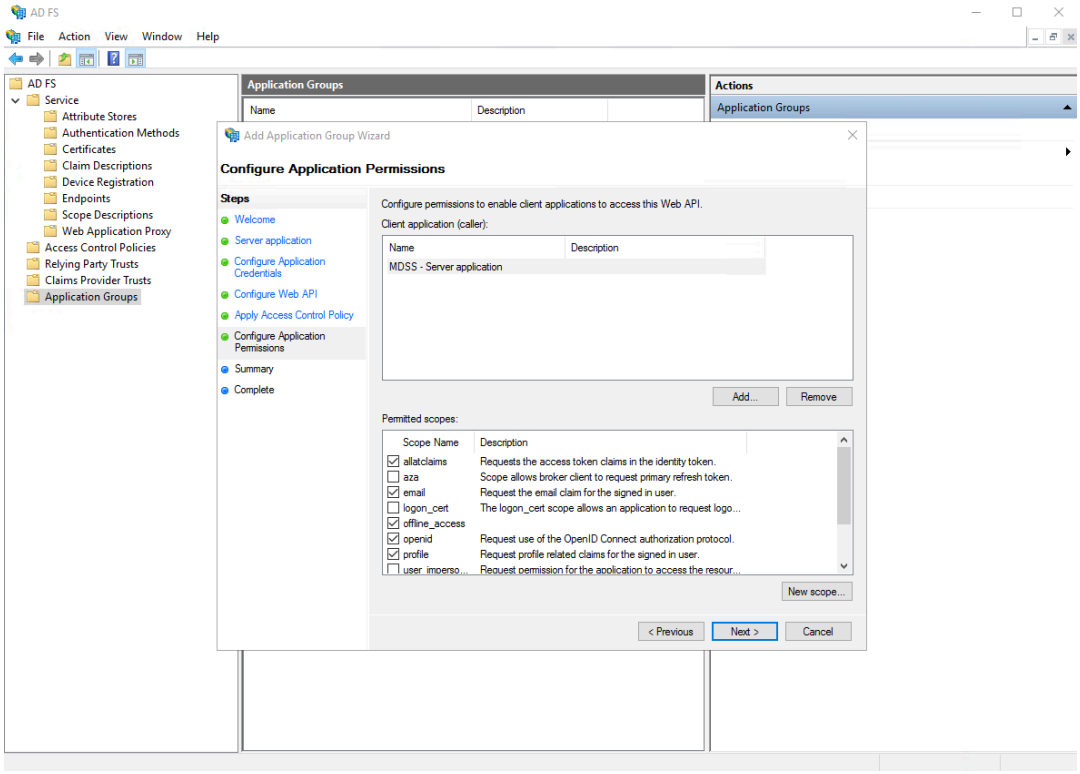
7. For the "**Identifier**" field, put the previously generated **Client Identifier** that you saved



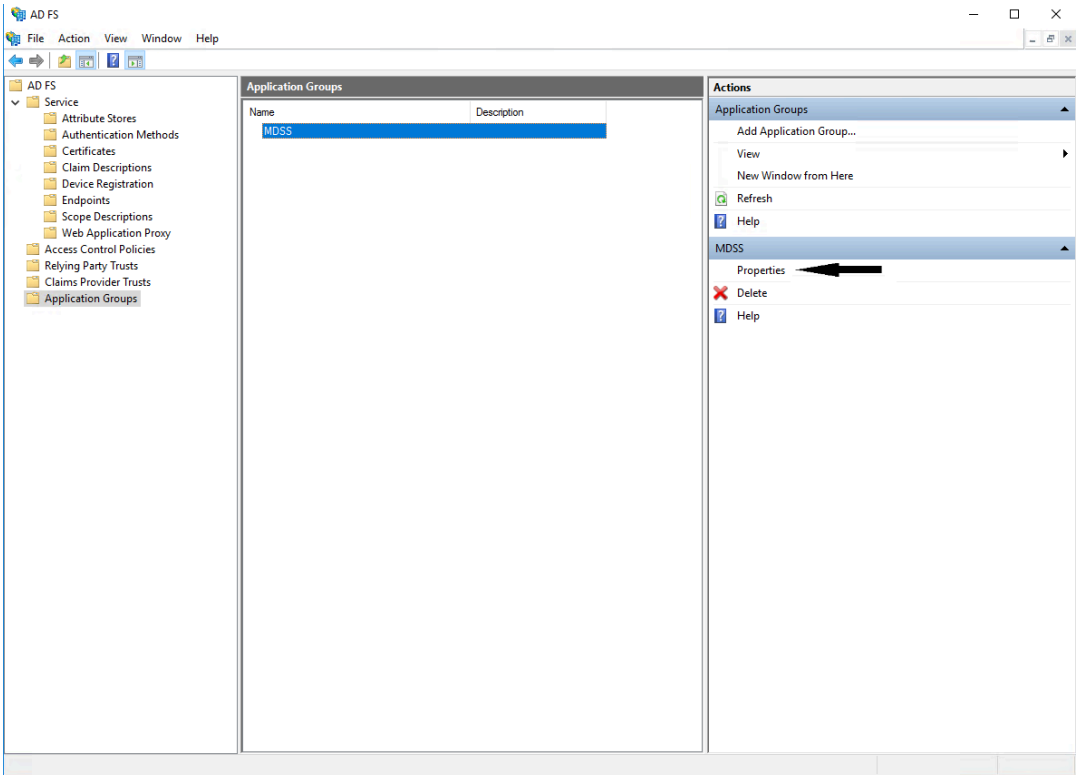
8. For the access **control policy**, select "**Permit everyone**"



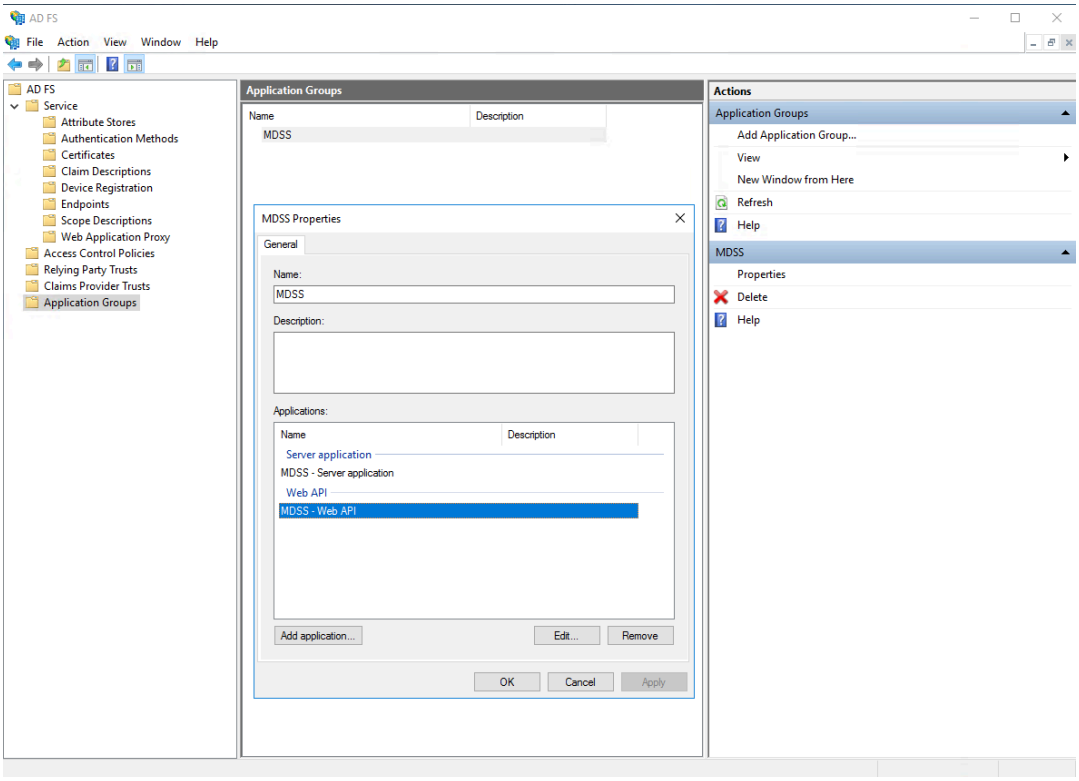
9. For the **permitted scopes**, select the following from the list: **allatclaims**, **email**, **offline_access**, **openid**, **profile**



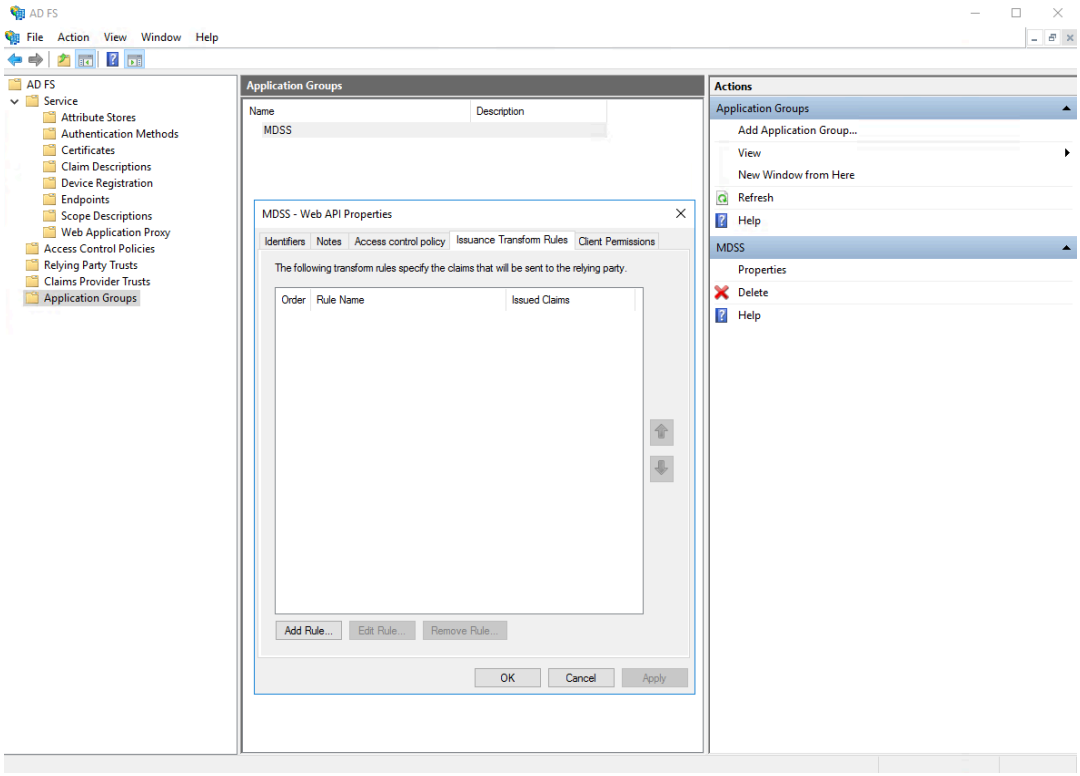
10. After saving the created application group, select it and click on **Properties**



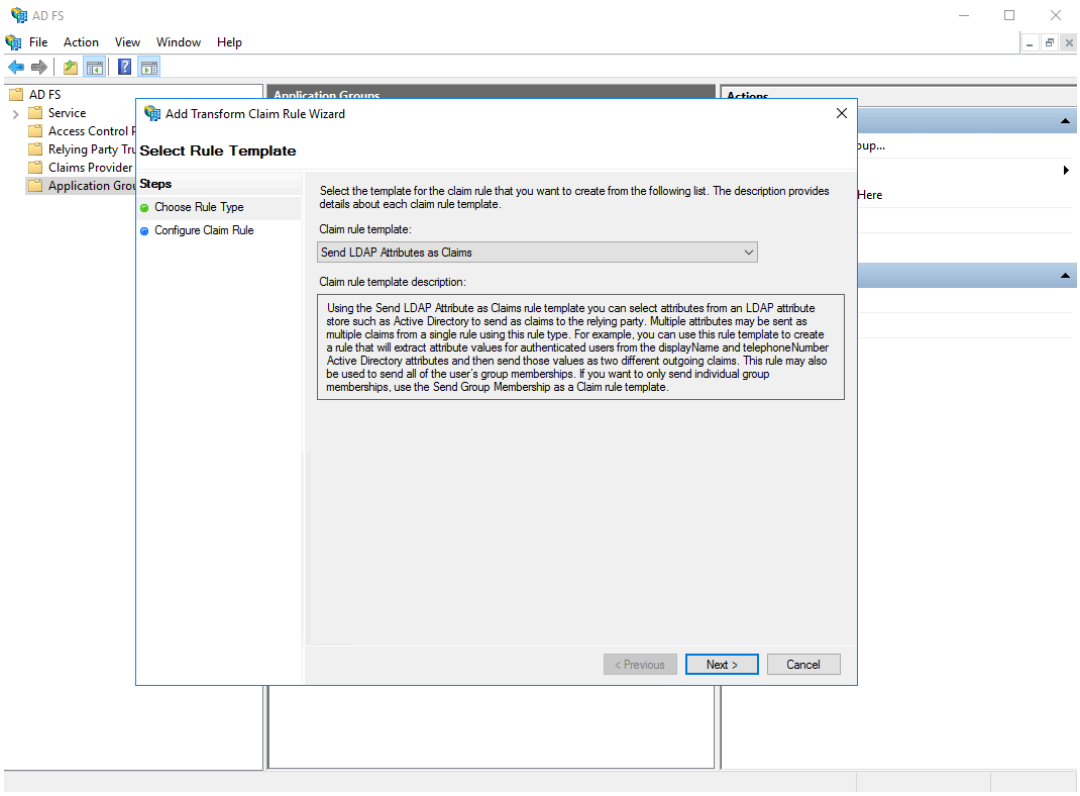
11. Select the configured **Web API** and click on **Edit**



12. Go to "**Issuance Transform Rules**" and click "**Add Rule**"

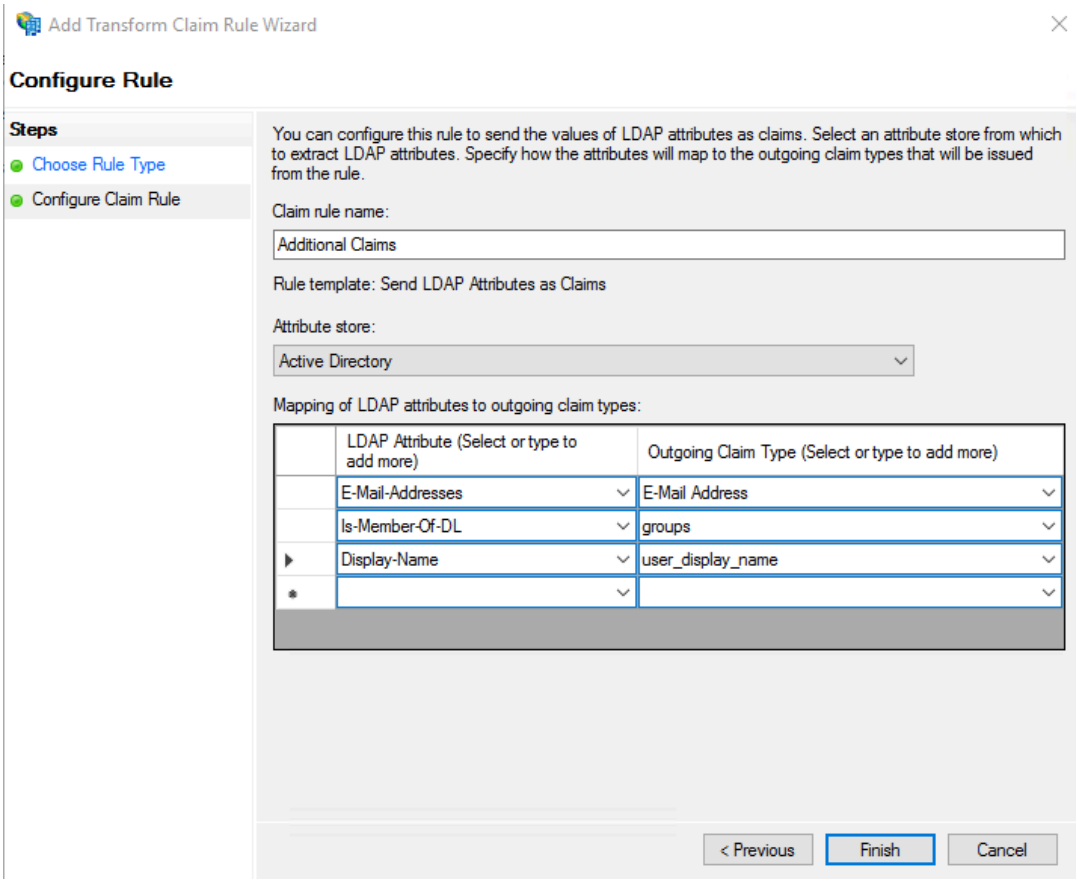


13. Select "**Send LDAP Attributes as Claims**" as the **Claim Rule Template**



14. Give the rule a name, select Active Directory as the attribute store and configure the following:

- **E-Mail Address** as **E-mail Address**
- **Is-Member-Of-DL** as **" groups*****"***
- **Display-Name** as ***"user_display_name"***

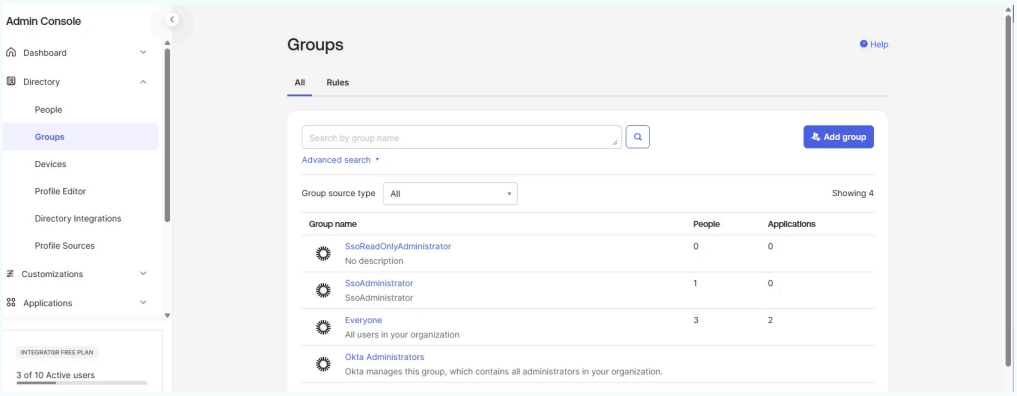


Okta Specific Configuration

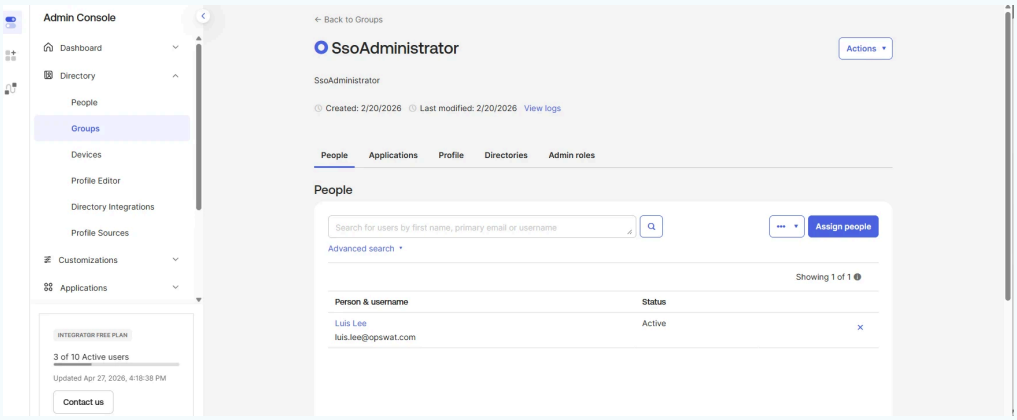
> **Info**
>
> To properly access MDSS, the following Okta **Groups** are required
>
> **Solution:**
>
> Create a Perquisite section on providing specific instructions on how to add the Specific Group and and assign users to them.
>
> For Example:
>
> **Prerequisite:**
>
> The following specific groups needs to be added into OKTA:
>
> **SsoAdministrator** - the equivalent of local MetaDefender Storage Security administrator role.

SsoReadOnlyAdministrator - the equivalent of local MetaDefender Storage Security read-only role.

To add the two required groups in Okta, navigate to **Directory > Groups**, then select **Add Group**.



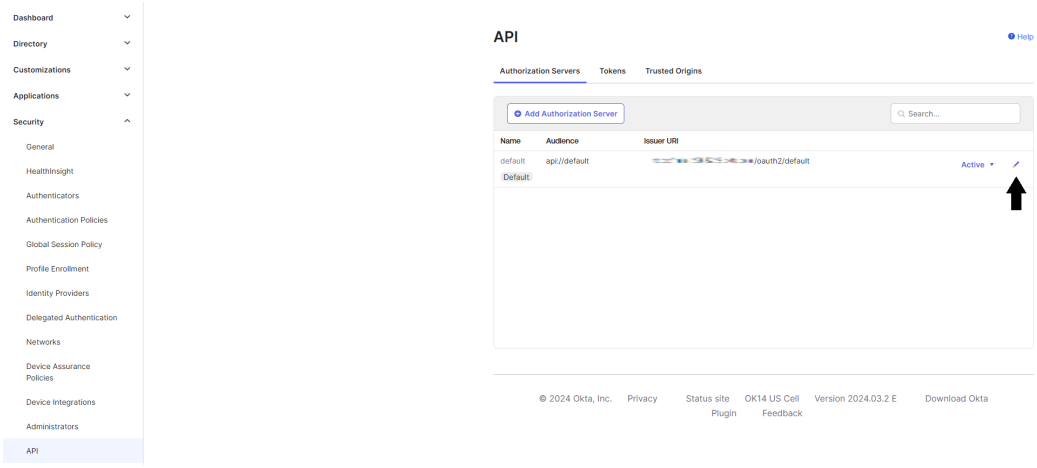
Within the specific group, ensure that users are assigned by selecting the **Assign People** option.



This will help ensure that Okta administrators remember to create the necessary groups and properly assign users to them.

To set up Okta SSO for MDSS, follow these steps:

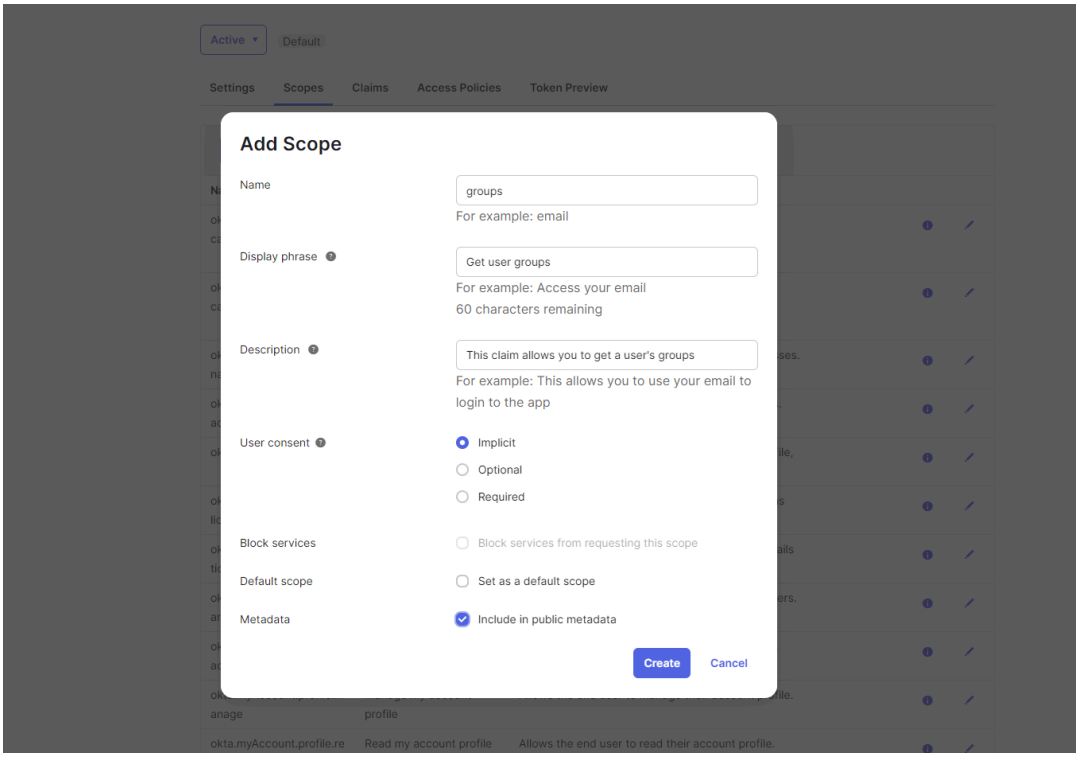
1. Under the **Security** tab, go to the **API** section, locate your **Authorization Server** and click on the pencil icon to edit



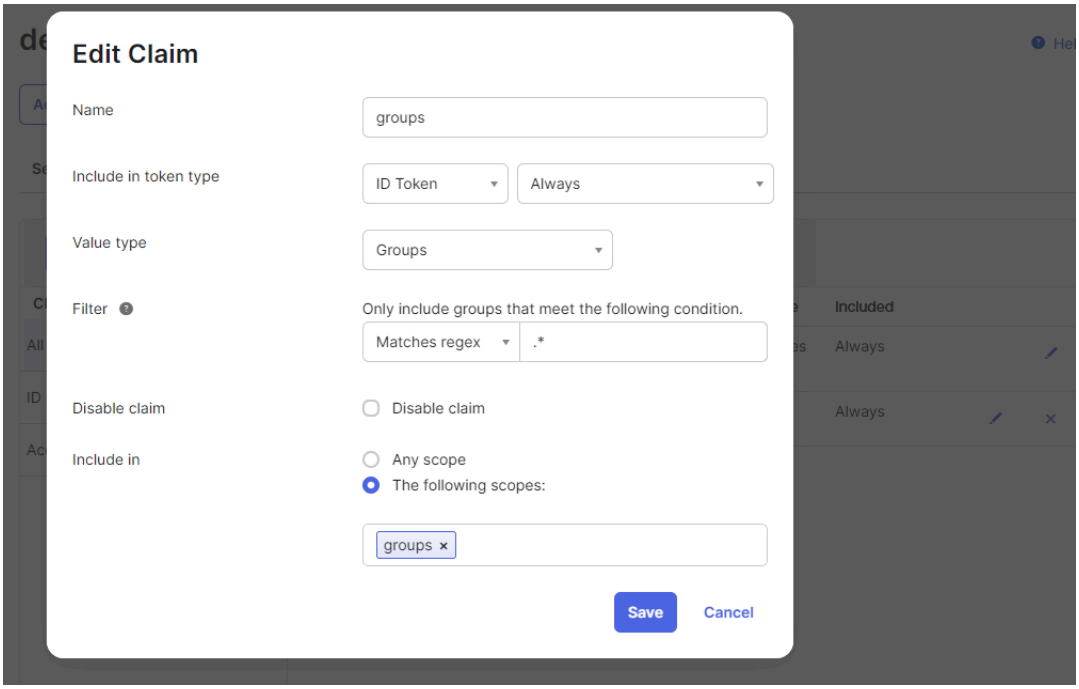
Info

The **Issuer URI** from the **Authorization Server** should be inputted as the **Authority URL** of the MDSS SSO Configuration.

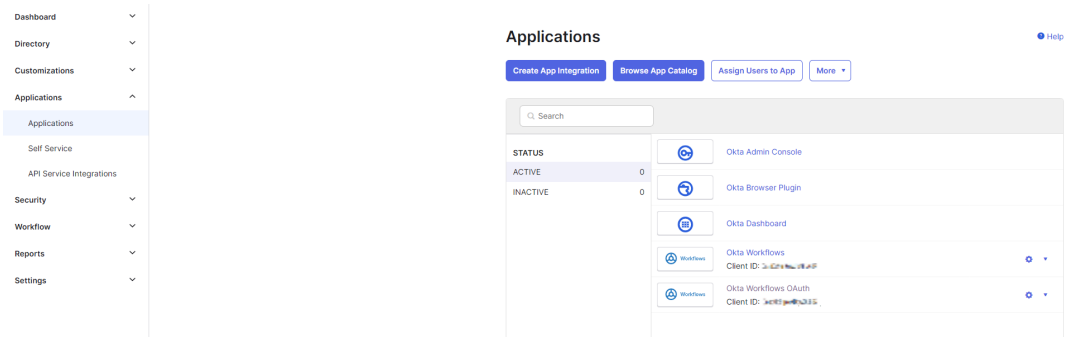
2. Within the **Scopes** tab, add a new scope. Name it "***groups***", select **Implicit** for the **User Consent**, and check the **Include** in public metadata checkbox



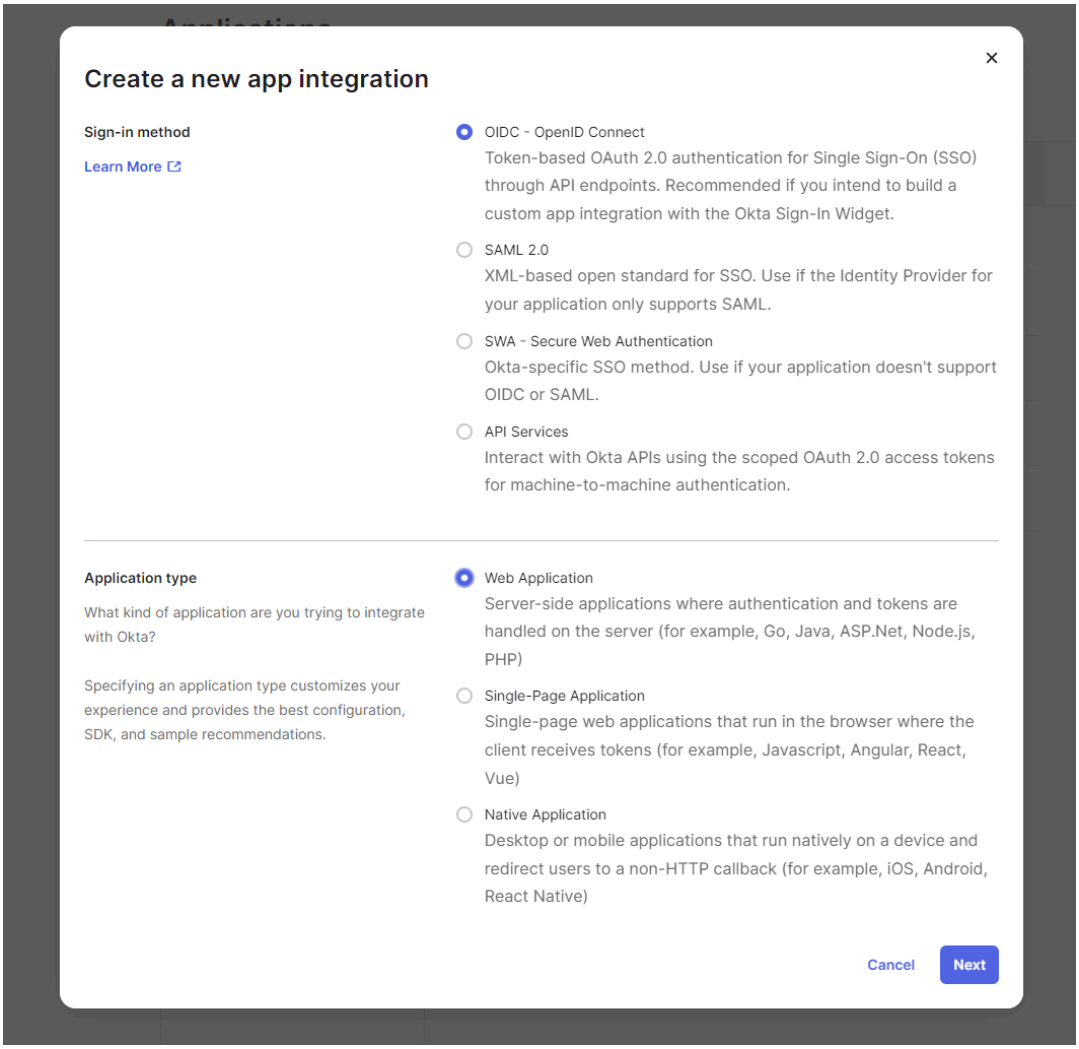
3. Within the **Claims** tab, add a new claim. Name it "***groups***", select **Id Token** and **Always** from the **Include in token type** dropdowns, select **Groups** as the **Value Type**, input "**.***" next to **Matches regex** to get all groups, and include it in the previously created "***groups***" scope



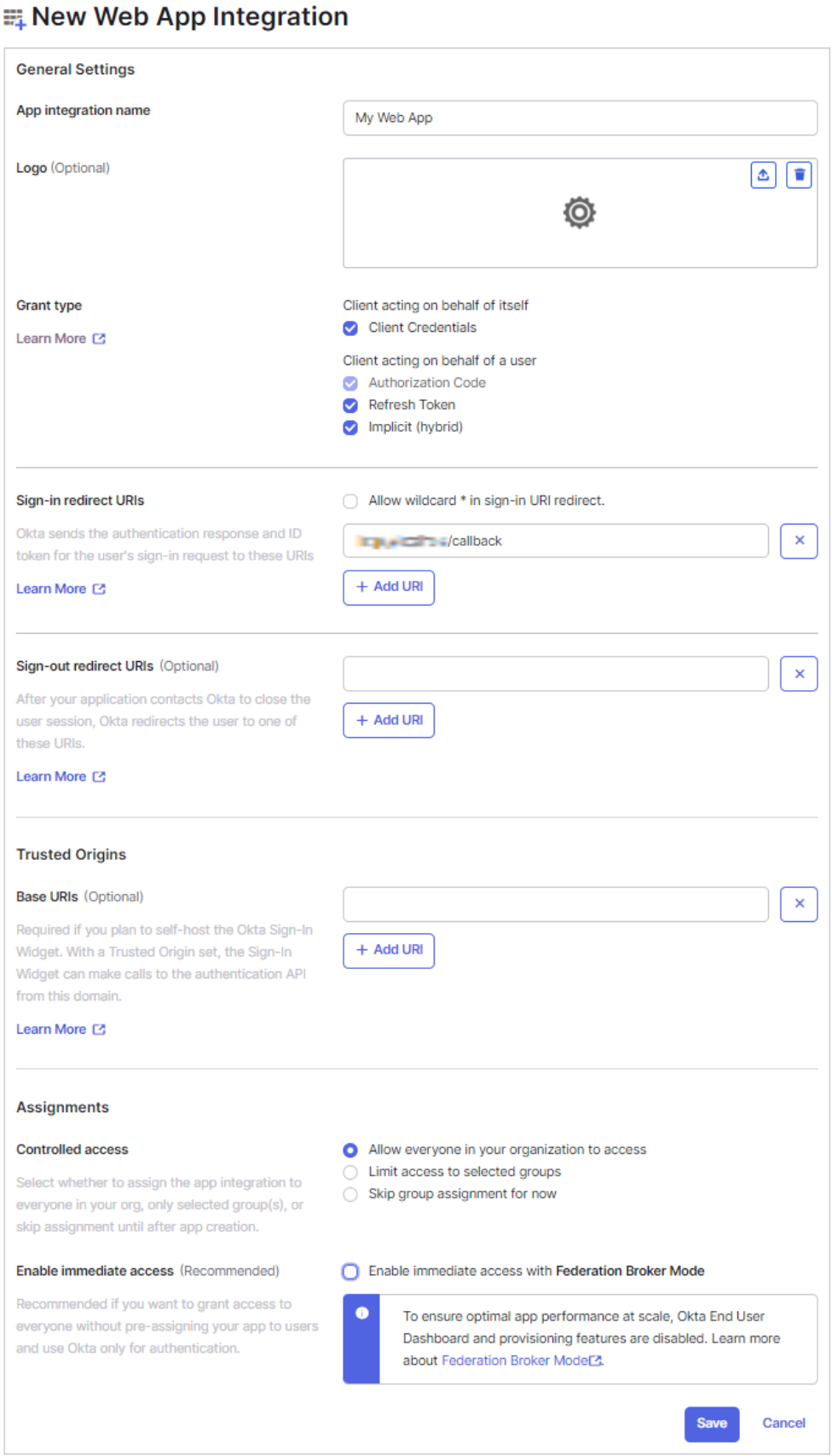
4. Navigate to the **Applications** tab and select the **Applications** section. Afterwards, click "**Create App Integration**"



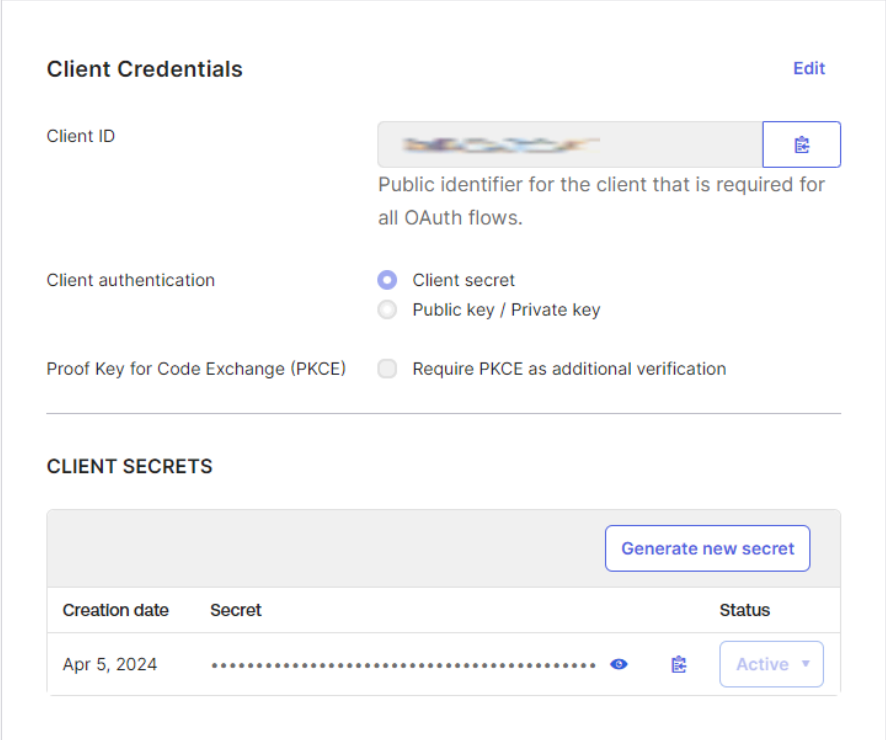
5. For the **Sign-in method**, select **OIDC - OpenID Connect**, and for the **Application Type**, select **Web Application**



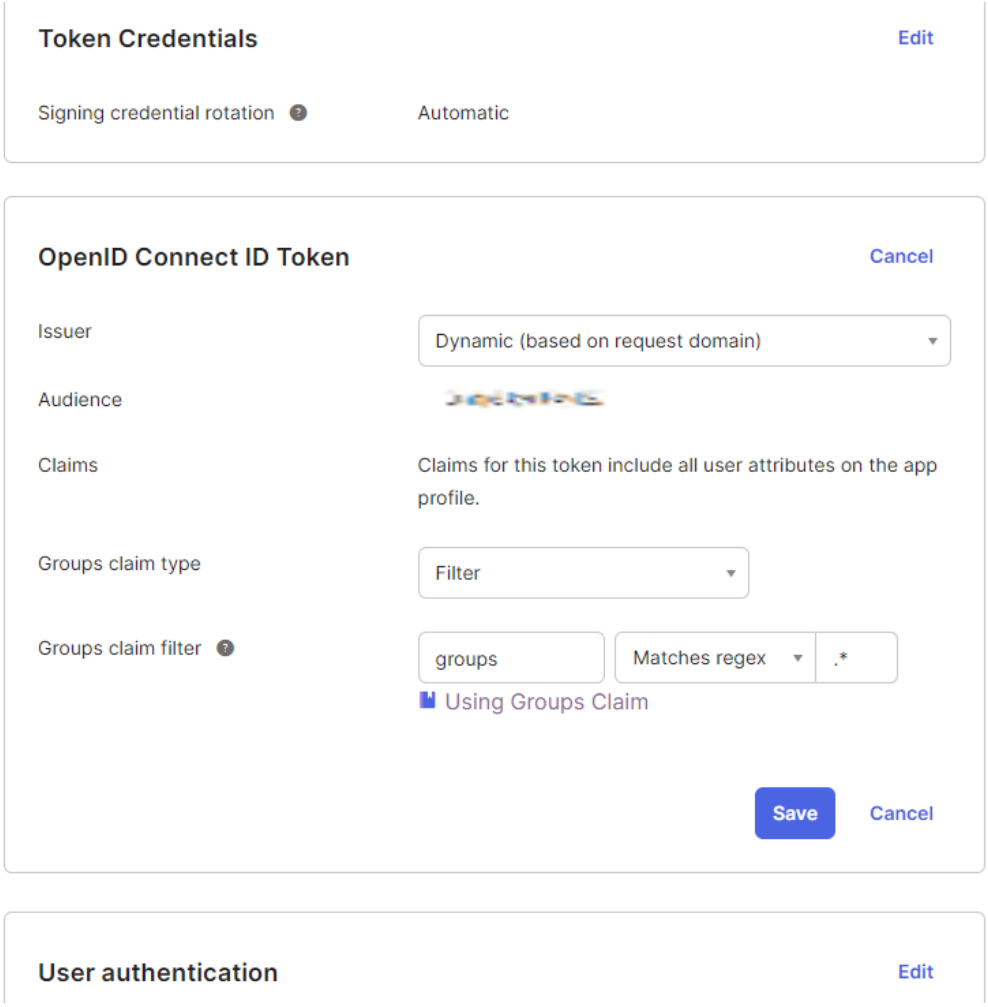
6. Give your app integration a name, for the **Grant Type,** tick the checkboxes. Under the **Sign-in redirect URIs**, write the the base URL of the MDSS deployment, followed by the "**/callback**" suffix. For the **Controlled access**, select **Allow everyone in your organization to access.**


New Web App Integration
General Settings
App integration name
My Web App
Logo (Optional)
Grant type
Learn More
Client acting on behalf of itself
Client Credentials
Client acting on behalf of a user
Authorization Code
Refresh Token
Implicit (hybrid)
Sign-in redirect URIs
Allow wildcard * in sign-in URI redirect.
Okta sends the authentication response and ID token for the user's sign-in request to these URIs
/callback
Learn More
+ Add URI
Sign-out redirect URIs (Optional)
After your application contacts Okta to close the user session, Okta redirects the user to one of these URIs.
+ Add URI
Learn More
Trusted Origins
Base URIs (Optional)
Required if you plan to self-host the Okta Sign-In Widget. With a Trusted Origin set, the Sign-In Widget can make calls to the authentication API from this domain.
+ Add URI
Learn More
Assignments
Controlled access
Select whether to assign the app integration to everyone in your org, only selected group(s), or skip assignment until after app creation.
Allow everyone in your organization to access
Limit access to selected groups
Skip group assignment for now
Enable immediate access (Recommended)
Recommended if you want to grant access to everyone without pre-assigning your app to users and use Okta only for authentication.
Enable immediate access with Federation Broker Mode
To ensure optimal app performance at scale, Okta End User Dashboard and provisioning features are disabled. Learn more about Federation Broker Mode.
Save
Cancel

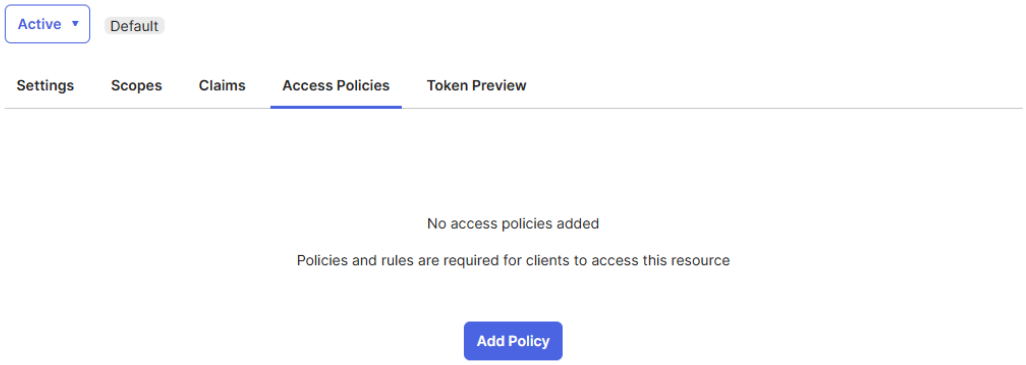
7. Save the **Client ID**, select **Client Secret** for the Client authentication, generate a new secret and save it.



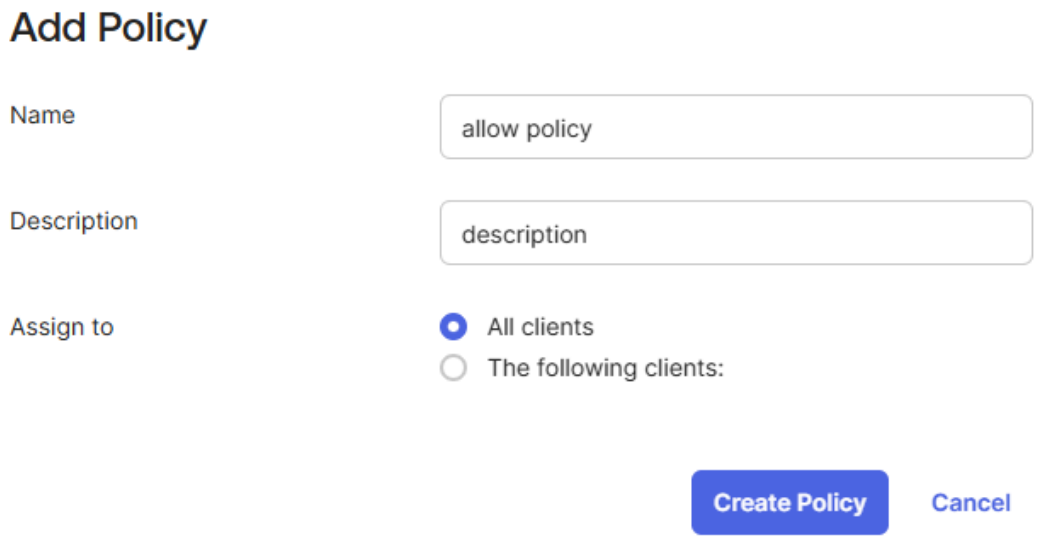
8. Within your **Application**, navigate to the **Sign On** tab, and scroll down to **OpenID Connect ID Token**. There, click the edit button and, for the **Groups Claim Type**, select **Filter**, and for the **Groups Claim Filter**, select **groups**. Select **Matches regex** from the dropdown and input "**.***"



9. Under the **Security** tab, go to the **API** section, locate **Access Policies** and add a new one.



10. Add policy and assign to **All clients** or **your desired clients.**



11. Create a rule, and make sure that on **Advanced** label you have checked **Implicit[hybrid].**

Add Rule

Rule Name

allow rule

IF Grant type is

Client acting on behalf of itself

- [x] Client Credentials

Core grants

- [x] Authorization Code
- [x] Device Authorization

Advanced

Non-interactive grants

- [ ] SAML 2.0 Assertion
- [ ] Token Exchange

Okta direct auth API grants

- [ ] OTP
- [ ] OOB
- [ ] MFA OTP
- [ ] MFA OOB

Other grants

- [x] Implicit (hybrid)
- [ ] Resource Owner Password

AND User is

- (•) Any user assigned the app
- ( ) Assigned the app and a member of one of the following:

AND Scopes requested

- (•) Any scopes
- ( ) The following scopes:

THEN Use this inline hook

None (disabled)

AND Access token lifetime is

1 Hours

AND Refresh token lifetime is

90 Days

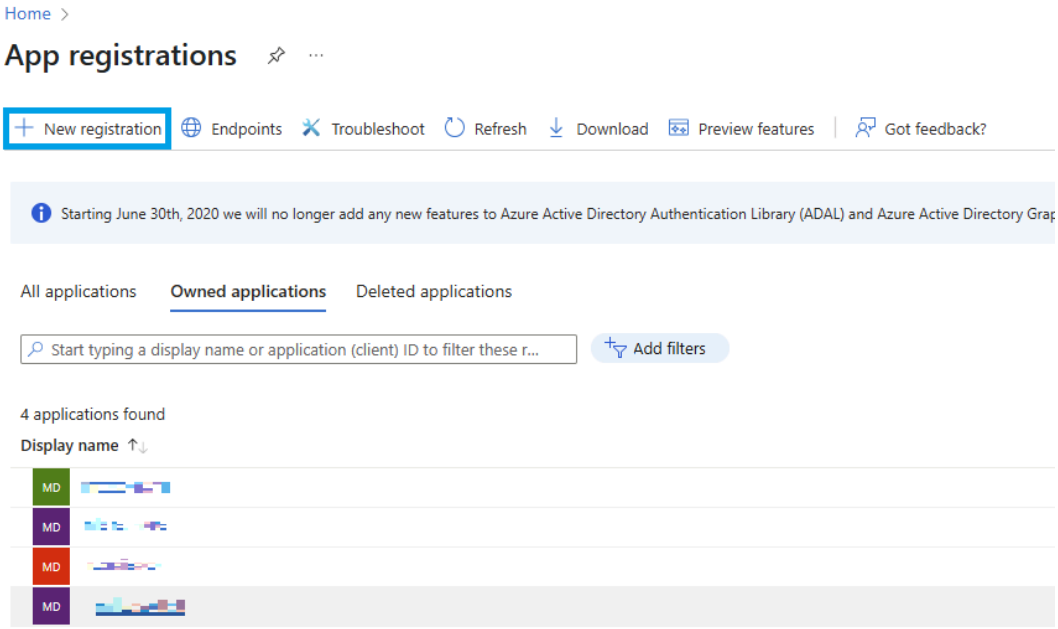
but will expire if not used every 7 Days

Create rule Cancel

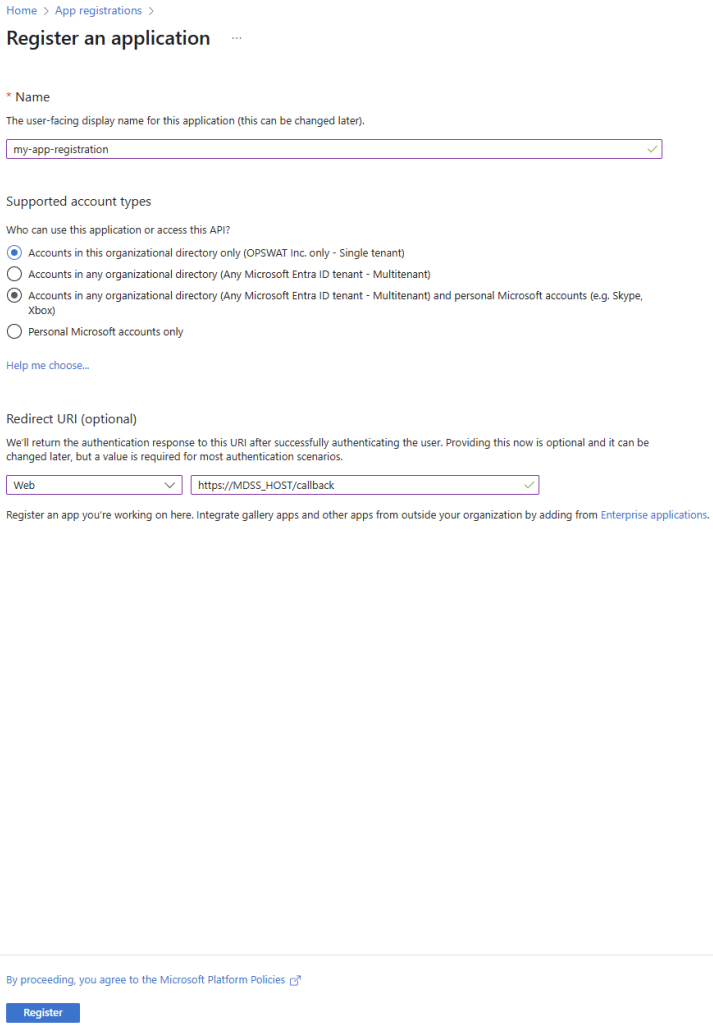
Azure AD Specific Configuration

To set up Azure AD SSO for MDSS, follow these steps:

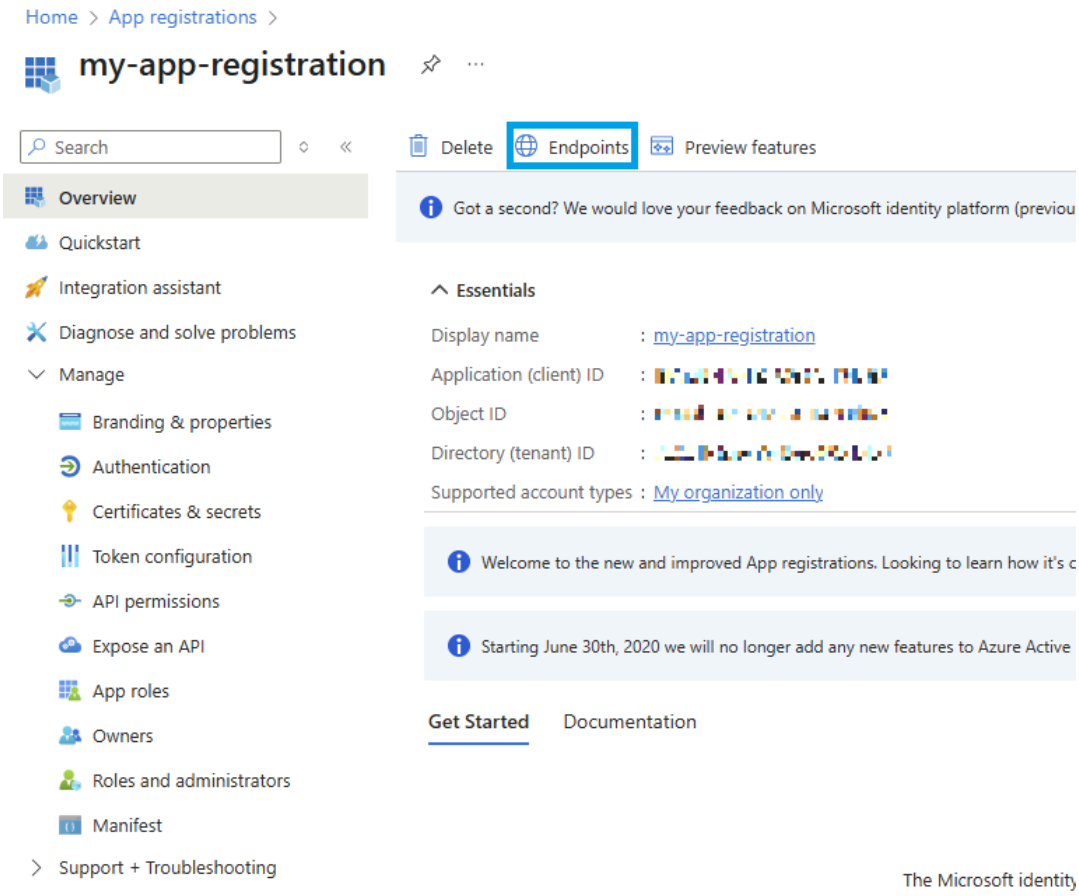
1. In the Microsoft Azure portal, navigate to **App registrations** and click on **New registration**



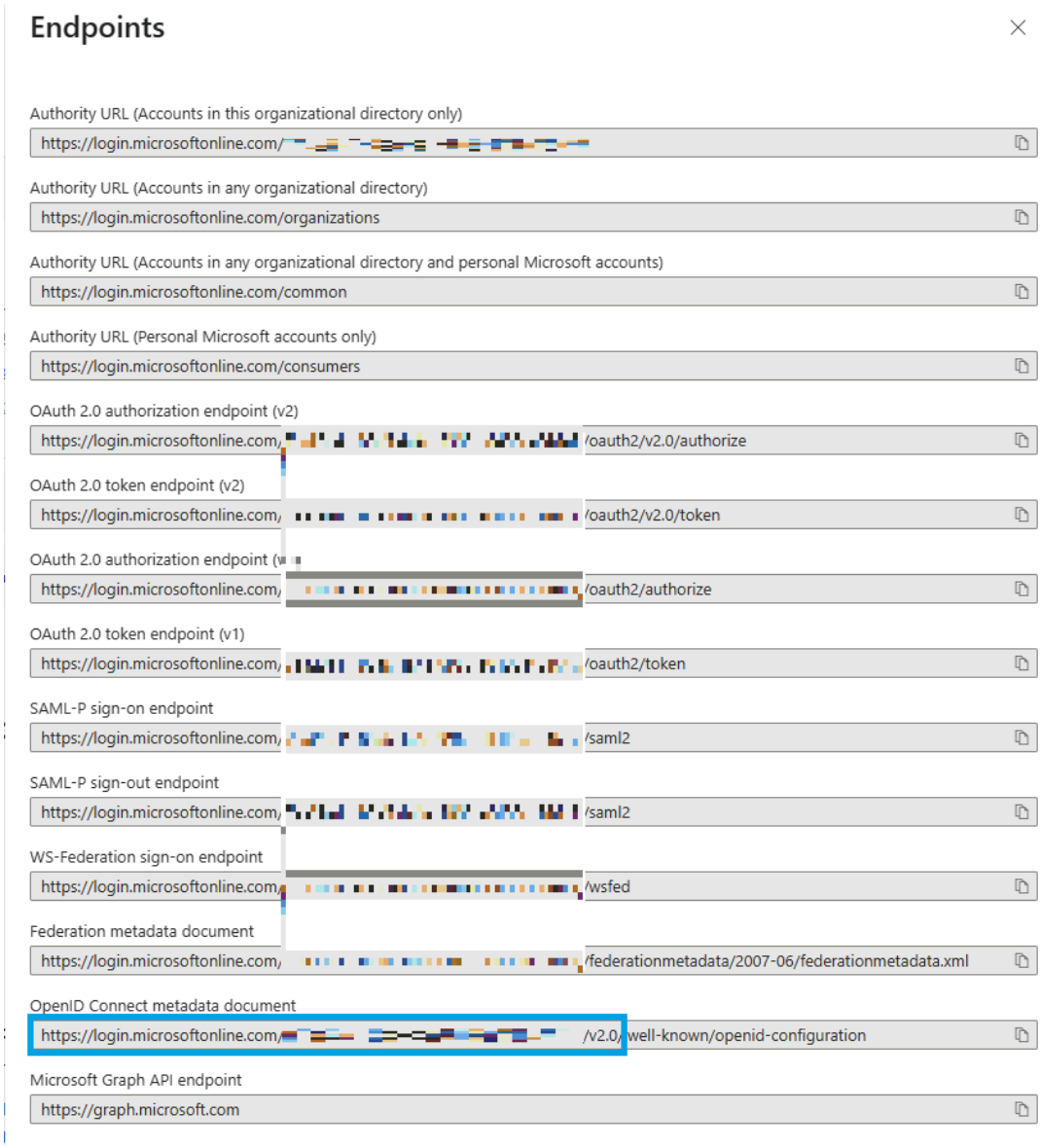
2. In the **Register an application** window, enter a name for your application, select your preferred configuration for **Supported account types** (recommended is Single tenant), and configure the **Redirect URI**. The redirect URI should be composed of the address where MDSS is deployed, along with the **/callback** suffix added to the path.



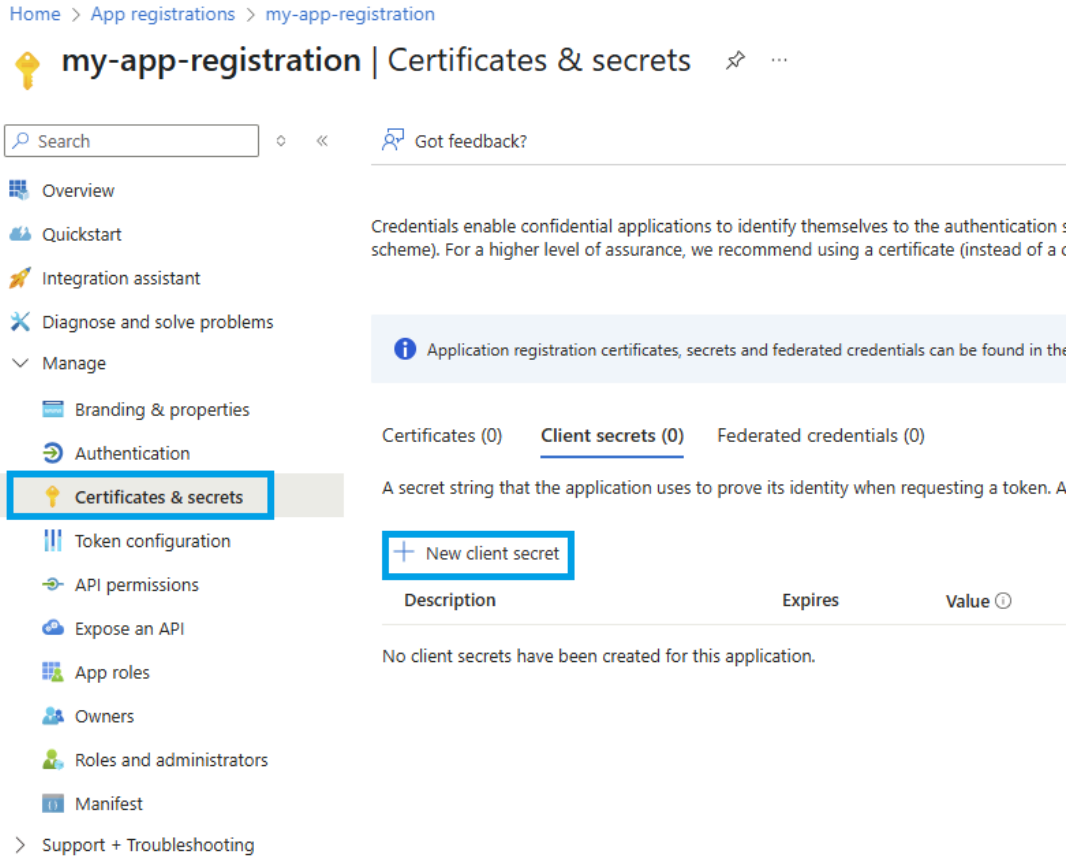
3. Afterwards, navigate to the **Overview** tab. There, to successfully configure the SSO Configuration in MDSS afterwards, store the **Application [Client] ID** and the **Direcory [Tenant] ID** somewhere safe on your computer. Then, click on the **Endpoints** button.



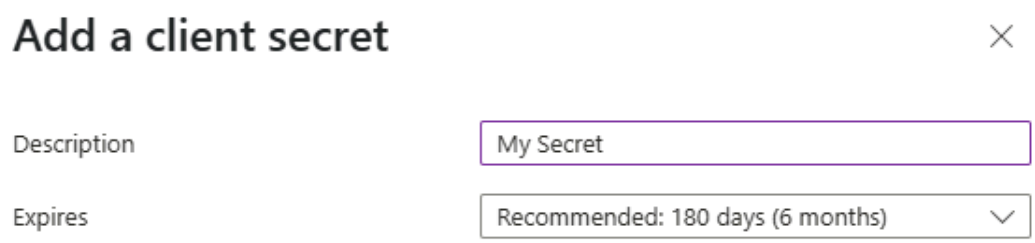
4. There, the authority URL is located in the right-hand side menu and is the following: **"https: //login.microsoftonline.com//v2.0"**



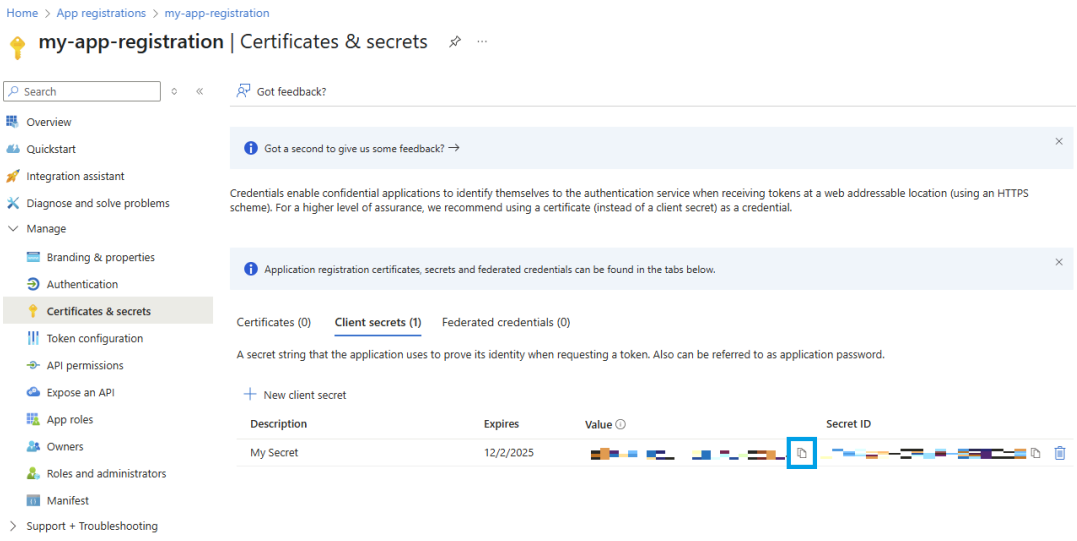
5. Navigate to the **Certificates & secrets** tab and click on **New client secret**



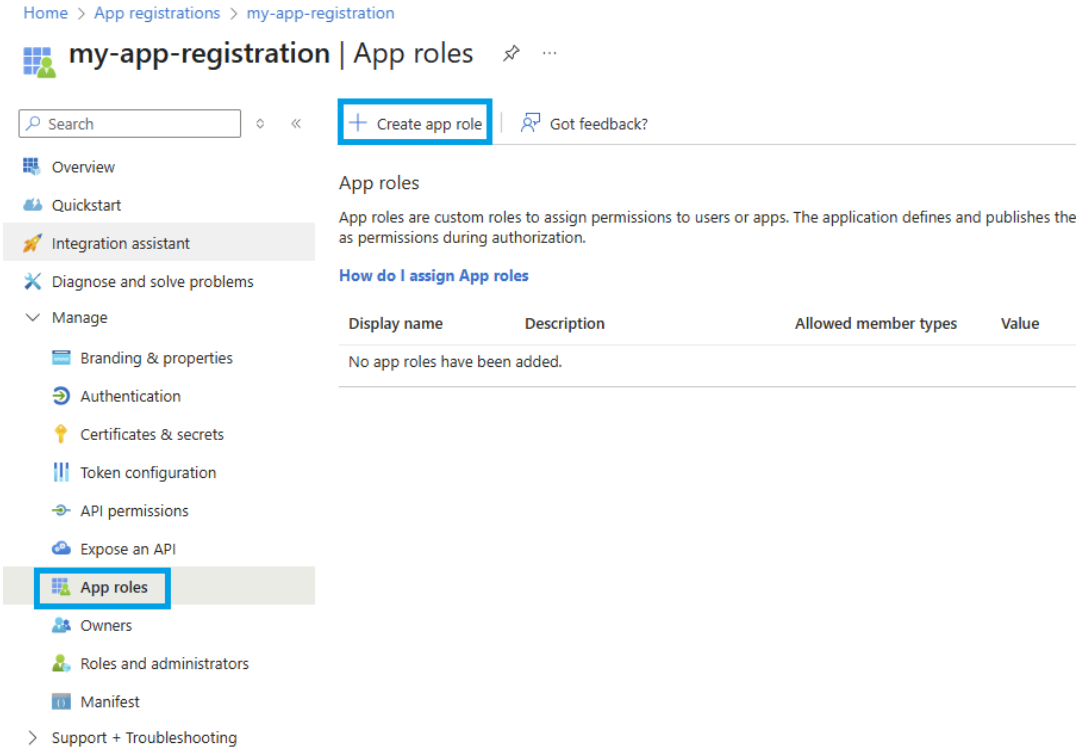
6. Give a description to your client secret, configure the expiration to your liking, and add it



7. Copy your secret value and store it somewhere safe on your computer (you will only be able to copy it at this stage)

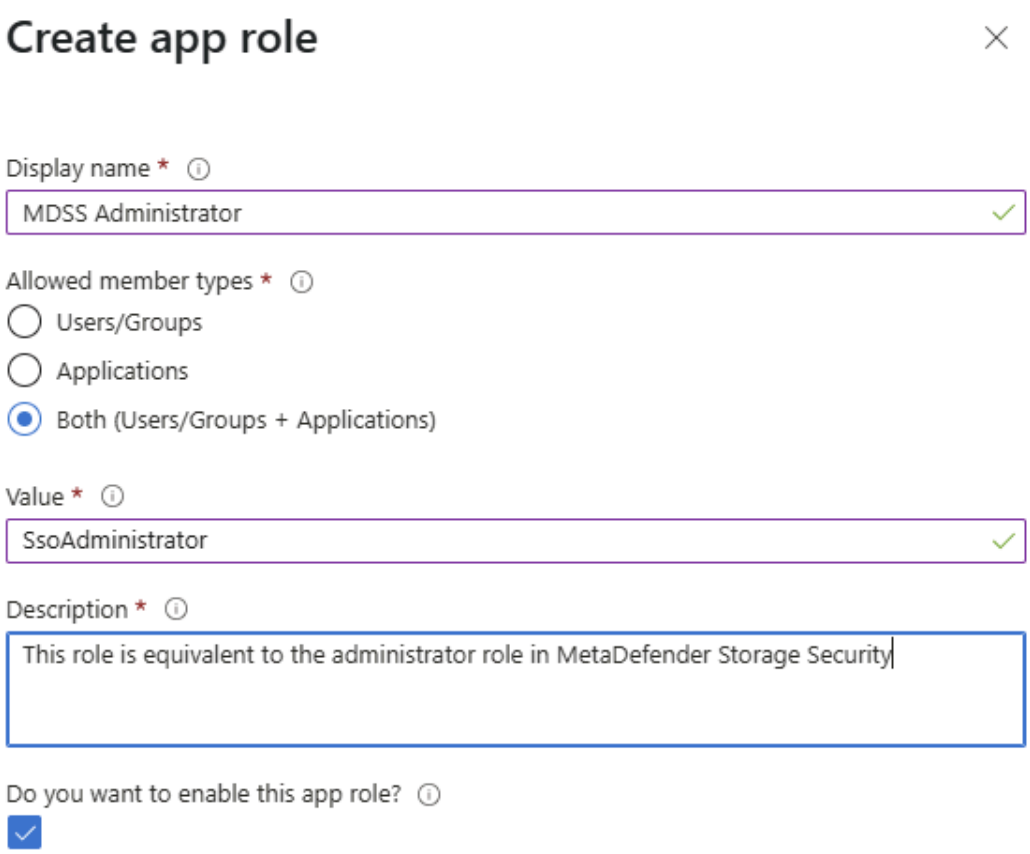


8. Navigate to **App Roles** and click on **Create app role**

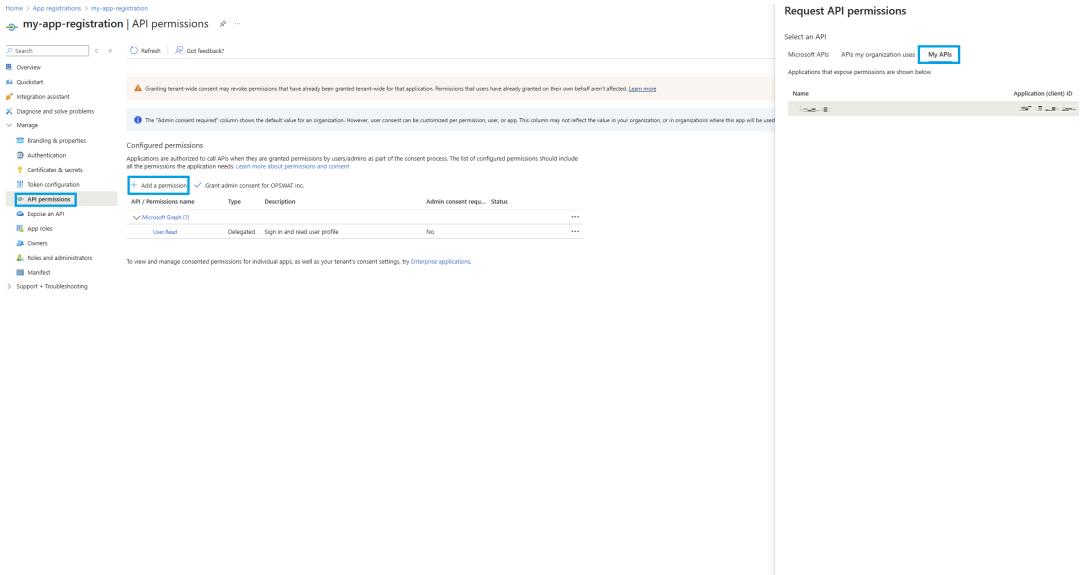


9. Give your role a Display name, configure the **Allowed member types** to be set to **Both (Users/Groups + Applications)**. Then, for the value, give one of the two values to determine the role that this user will have within MDSS:

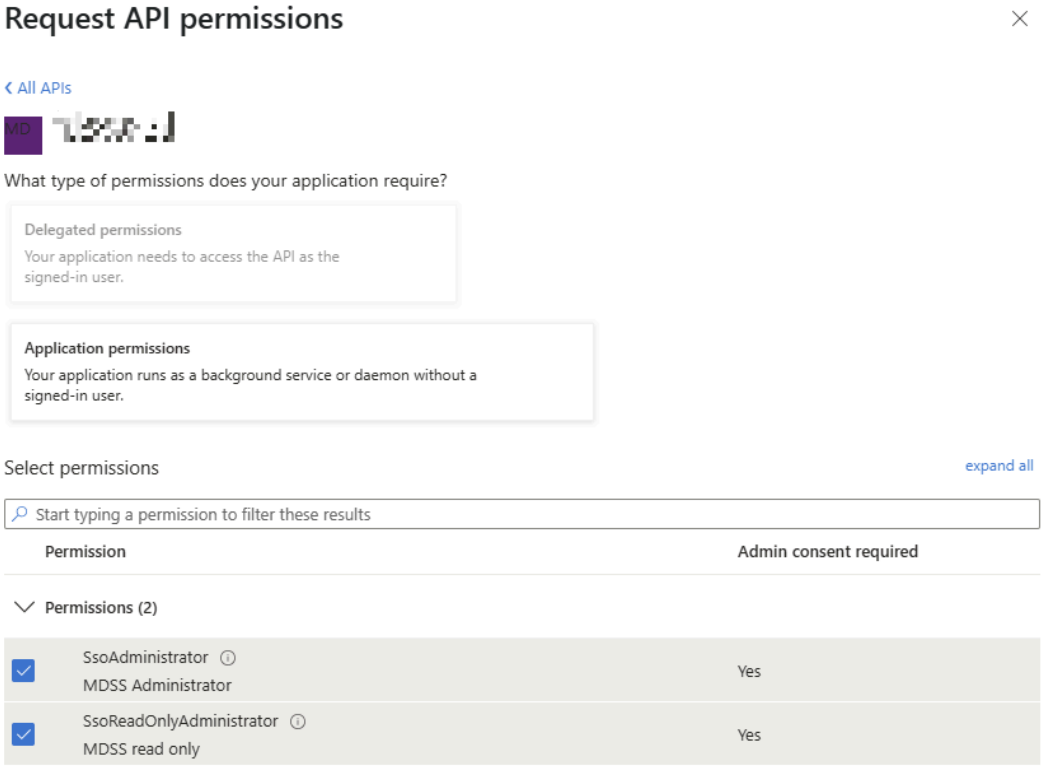
- **SsoAdministrator** - equivalent to the administrator role in MDSS
- **SsoReadOnlyAdministrator** - equivalent to the read-only admin role in MDSS



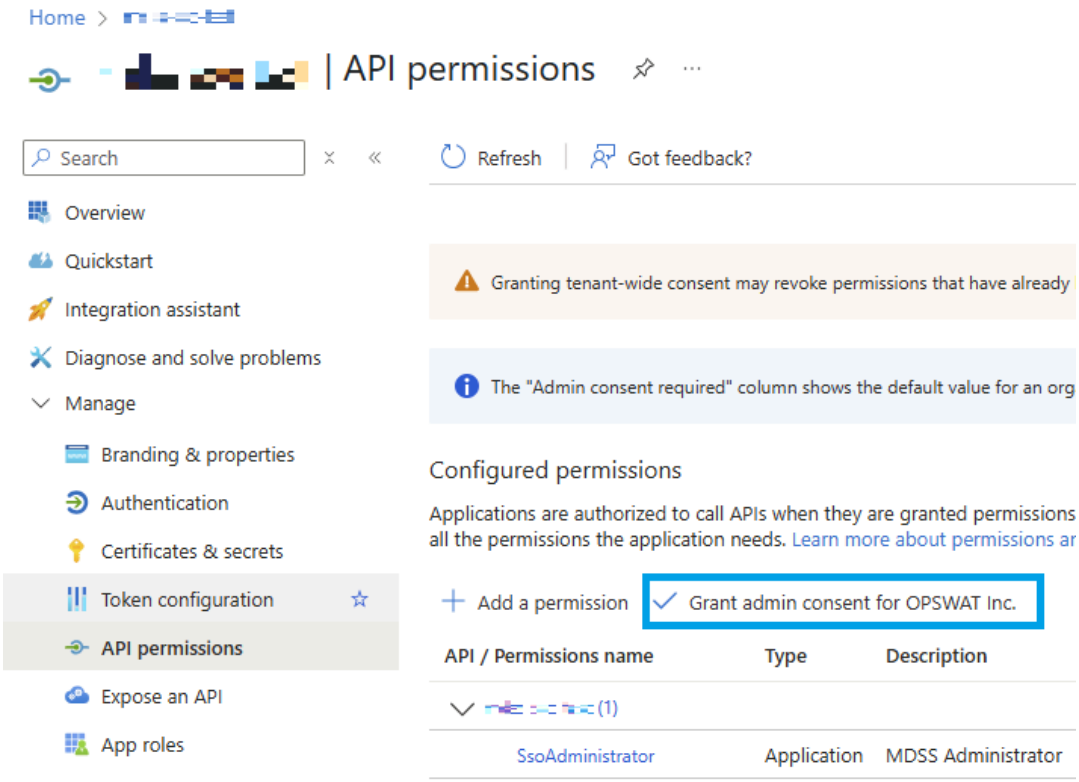
10. Navigate to the **API permissions** and click on **Add a permission**. Then, select the **My APIs** tab and find your app



11. Click on your app and select the app role you have configured.

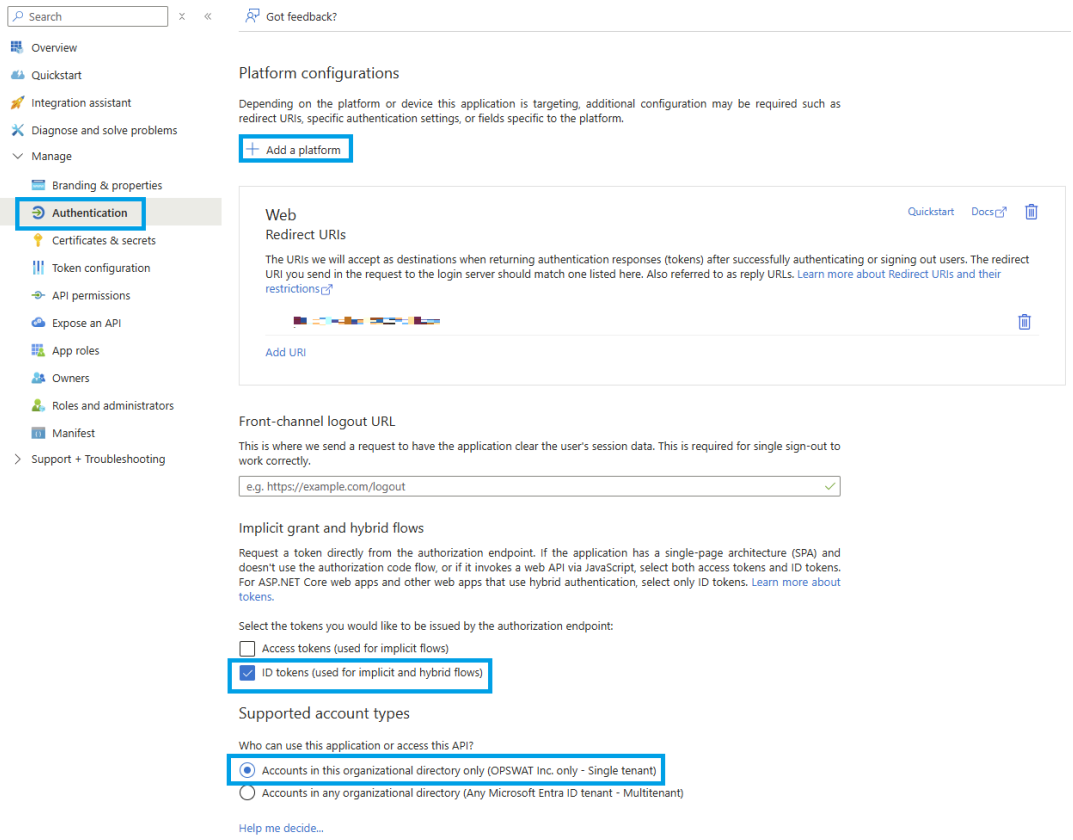


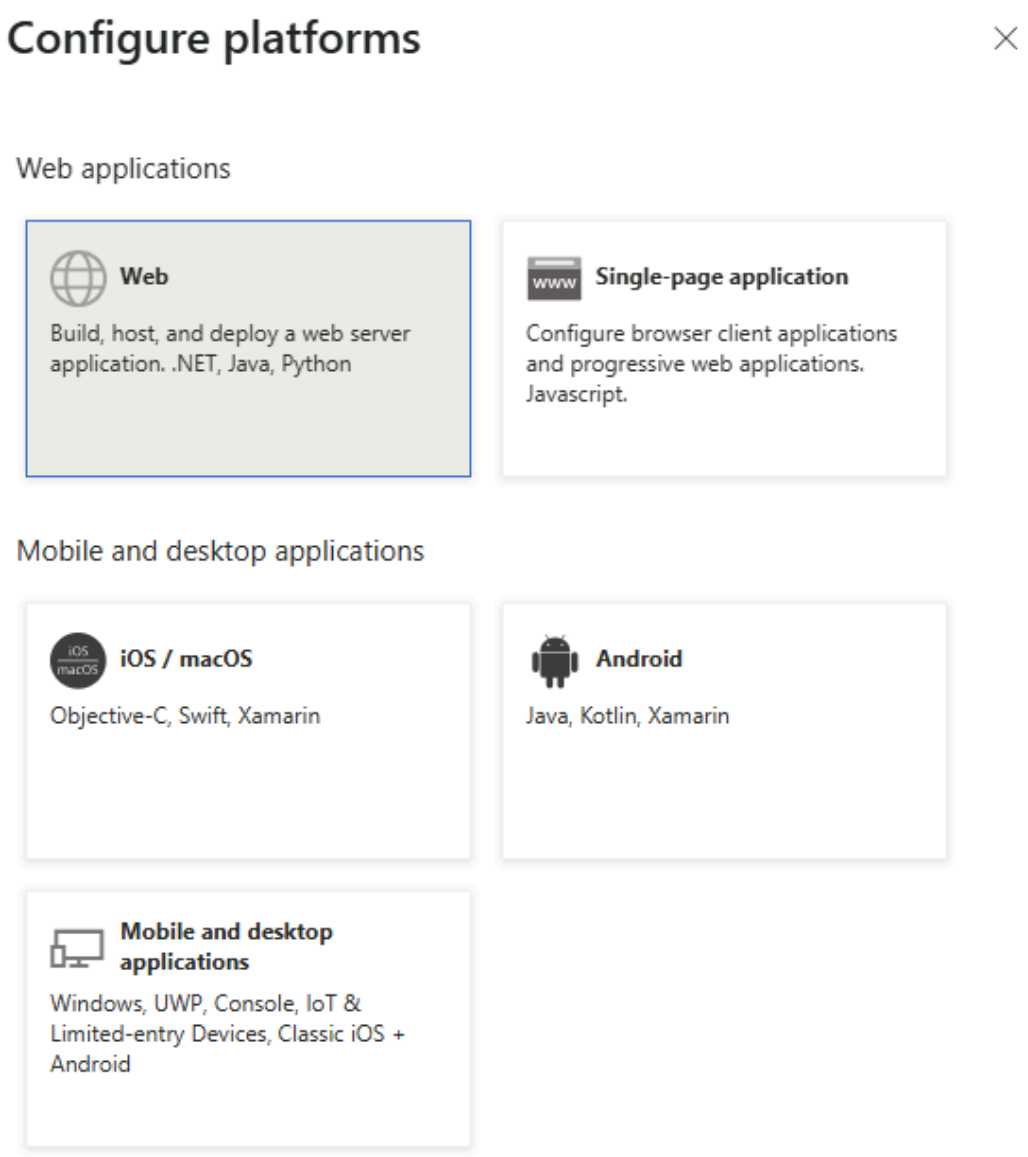
12. Next, click on **Grant admin consent**



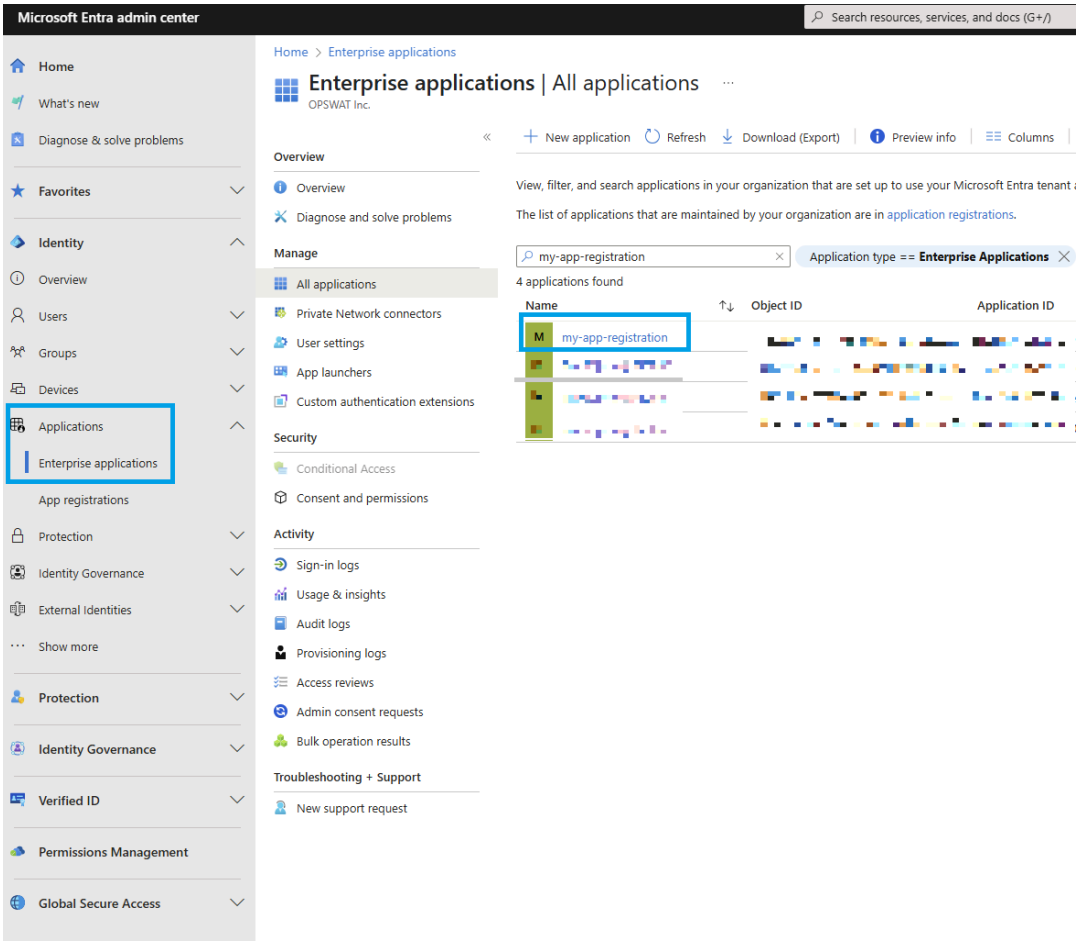
13. Go to the **Authentication** tab. Here, click **Add a platform** and select the **Web** option. Then, click on the checkbox for **ID tokens** and also for **Supported account types**,

select whatever you prefer (recommended is Single tenant).

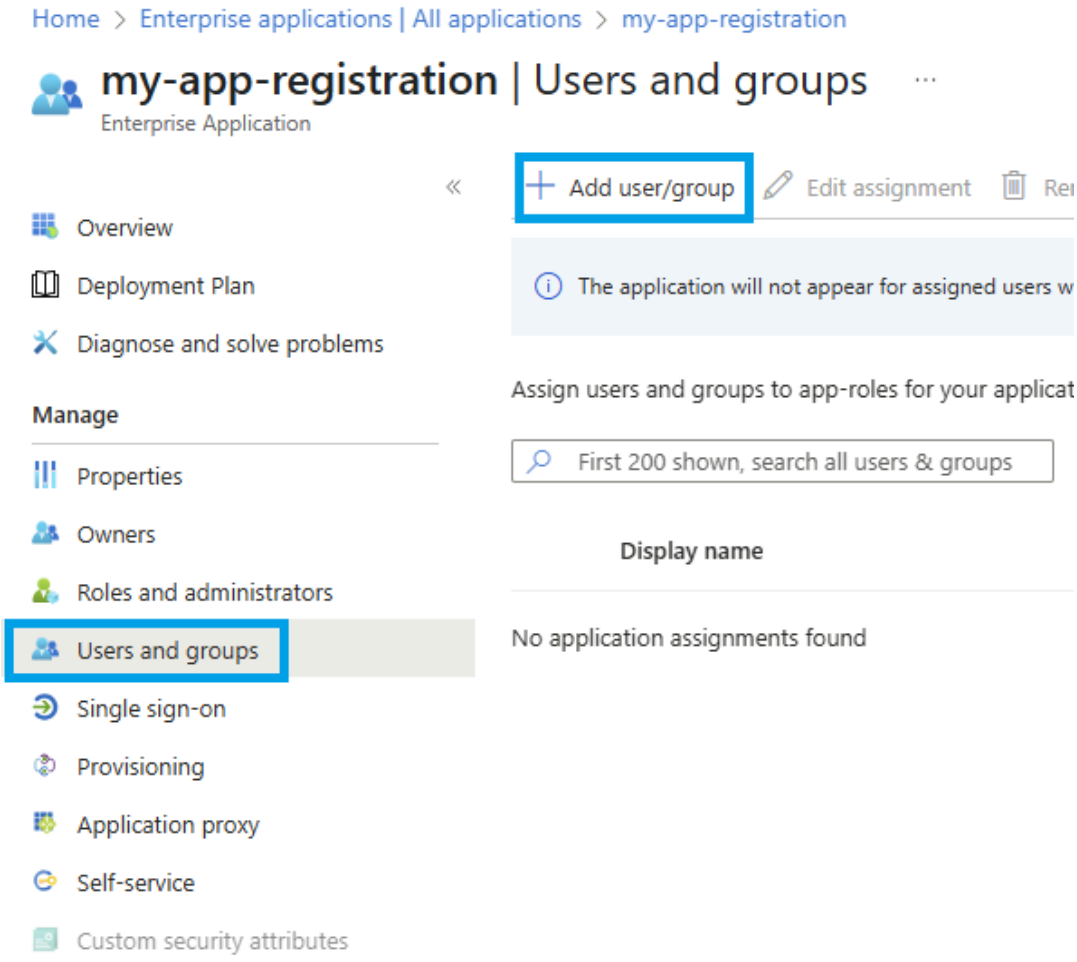




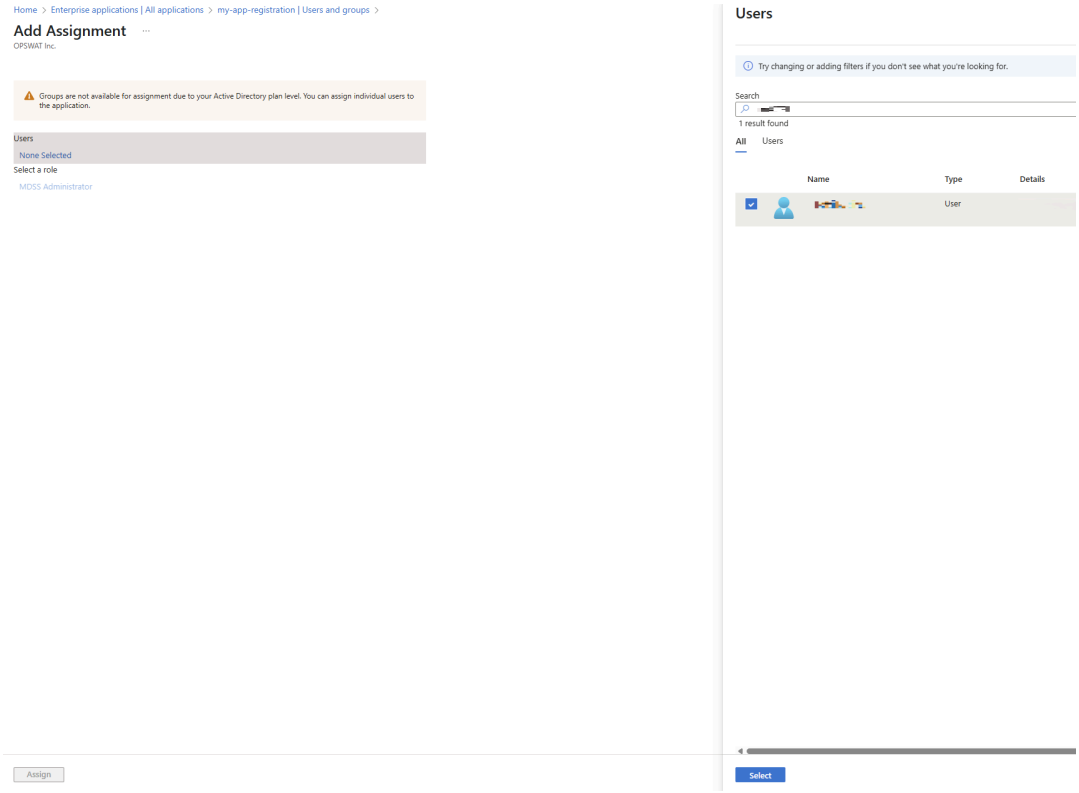
14. Now, leave the **Azure Portal** and navigate to the **Microsoft Entra admin center**. Here, find the **Enterprise applications** window under the **Applications** tab on the left. Search for your configured app.



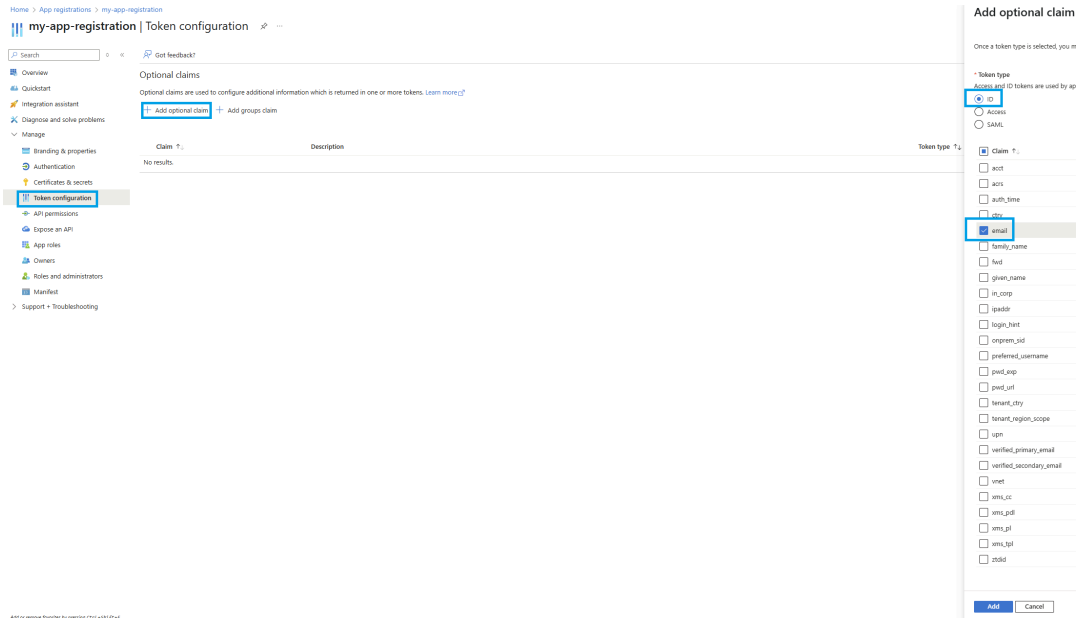
15. Navigate to the **Users and groups** tab and select **Add user/group**



16. Find your user and assign the configured App Role to it.



17. Lastly, navigate to **App registrations**, find your app and click on the **Token configuration**. There, click on **Add optional claim**, select **ID**, and add the **email** claim.



PingFederate Specific Configuration

> **Info**
>
> To properly access MDSS, the following AD **Security Groups** are required:

- **SsoAdministrator** - the equivalent of local MetaDefender Storage Security administrator role
- **SsoReadOnlyAdministrator** - the equivalent of local MetaDefender Storage Security read-only role

It is also necessary for the AD user to have an **email address** set up, so that it is set as the MetaDefender Storage Security's user email

This documentation was tested on PingFederate 12.1 with an Active Directory datastore.

Create the scopes

1. Go to System > OAuth Settings > Scope Management.
2. On the **Common Scopes** tab, add the following **Scope Values** along with a description. Click Add after entering each value and description.
   - openid
   - profile
   - email
   - offline_access
3. Skip the Exclusive Scopes tab.
4. On the Default Scope tab, enter a description for Default Scope. A description is required. If Default Scope Description is empty, PingFederate will log the following error: The requested scope is invalid, unknown, malformed, or exceeds that which the client is permitted to request.
5. Click Save.

Create a configuration on PingFederate

Create the Access Token Manager

1. Go to Applications> OAuth > Access Token Management.
2. Click Create New Instance
3. On the Type tab:

- Instance Name: Enter an instance name. For example, MDSS Access Token Manager.
- Instance ID: Enter the instance ID. For example, MDSS.
- Type: Select JSON Web Tokens.
- Parent Instance: Leave the default, None.

4. On the Instance Configuration tab:

- Use Centralized Signing Key: Select the checkbox.Leaving this checkbox unselected causes PingFederate to expect “Active Signing Certificate Key ID” to be configured.
- JWS Algorithm: Select an algorithm. For example, RSA using SHA-256.
- At the bottom of the screen, click Show Advanced Fields.
  - JWT ID Claim Length: Add a number greater than zero (0). For example, 24. If you do not enter a value, the JTI claim is omitted in the access token.

5. Click Next.
6. On the Access Token Attribute Contract tab:

- In the Extend the Contract text box, add the following claims to be generated in the Ping access token. Click Add after entering each claim.
  - userName
- Subject Attribute Name: Select the userName claim to be used for auditing purposes.

7. Click Next twice to skip the Resource URIs and Access Control tabs.
8. Click Save.

Add the objectGUID Attribute

1. Go to System > Data Stores > Your Data Store > LDAP Configuration.
2. On the LDAP Configuration tab, click Advanced at the bottom.
3. On the LDAP Binary Attributes tab, in the Binary Attribute name field, use objectGUID and click Add.
4. Click Save

Create the OpenID Connect Policy.

1. Go to Applications> OAuth > OpenID Connect Policy Management.
2. Click Add Policy.
3. On the Manage Policy tab:

- Policy ID: Enter a policy ID. For example, OIDC.
- Name: Enter a policy name. For example, OIDC Policy.
- Access Token Manager: Select the access token manager that you previously created. MDSS Access Token Manager.
- Tick **Include User Info in ID Token**

4. Click Next.
5. On the Attribute Contract tab:
   - Click **Delete** to remove all the attributes except **sub**.
   - Add the following attributes:

- Displayname
- Email
- Groups
- upn
- userName

6. Click Next, then click Next again to skip the Attributes Scope tab.
7. On the Attribute Sources & User Lookup tab, click Add Attribute Source.
8. After entering the information on each tab that follows, click Next to advance.

Data Store:

- Attribute Source ID: Enter an attribute source ID. For example, MDSSLDAP.
- Attribute Source Description: Enter a description. For example: MDSSLDAP
- Active Data Store: Select your Active Directory domain name from the drop-down.

LDAP Directory Search:

- Base DN: Enter your base DN to find your users and groups.
- Search Scope: Leave the default, Subtree.
- Attributes to return from search: Select and select the following.Click Add Attribute.
  - displayName
  - memberOf
  - objectGUID
  - userPrincipalName
  - mail
- LDAP Binary Attribute Encoding Types:
  - ObjectGUID: Select Hex for the Attribute Encoding Type.
- LDAP Filter:
  - Filter: Enter a filter. For example, `userPrincipalName=${userName}`.

9. On the Summary page, click Done.
10. Click Next to advance, and on the Contract Fulfillment tab, map the Attribute Contract for the ID token:

Attribute Contract	Source	Value
displayname	MDSSLDAP	displayName
email	MDSSLDAP	mail
groups	MDSSLDAP	memberof
sub	MDSSLDAP	objectGUID
upn	MDSSLDAP	userPrincipalName
userName	No Mapping	

11. Click Next, then click Next again to skip the Insurance Criteria tab.
12. Click Save

Create the OAuth Client Application

1. Go to Applications > OAuth > Clients.
2. Click Add Client.
3. On the Clients | Client page:
    1. Client ID: Enter the client ID. For example, MDSS
    2. Name: Enter a name. For example, MDSS.
    3. Client Authentication: Select Client Secret.
    - Client Secret: You can input your own client secret or generate a secret. After you leave this page, you cannot view the secret again. You only have the option to change the secret
    - Redirection URIs: write the the base URL of the MDSS deployment, followed by the "**/callback**" suffix.
    - Allowed Grant Types: Check Authorization Code, Implicit, Refresh Token, Client Credentials.
    - Default Access Token Manager: Select the access token manager you previously created. MDSS Access Token Manager.
    - OpenID Connect: For Policy, select the one you previously created. For example, the one used in this documentation is OIDC
4. Click Save.

Create the Password Grant Flow Configuration

1. Create the Password Credential Validator.
    1. Go to System > Data & Credential Stores > Password Credential Validators.

2. Click Create New Instance.
3. In the Password Credential Validators | Create New Instance page, enter the information as follows for each tab, then click Next to advance.
   - On the Type tab:
     - Instance Name: Enter the instance name. For example, MDSS Validator.
     - Instance ID: Enter the instance ID. For example, MDSS.
     - Type: Select LDAP Username Password Credential Validator.
   - On the Instance Configuration tab:
     - LDAP Datastore: Select the data store you are using.
     - Search Base: Enter your base DN to find your users and groups.
     - Search Filter: Enter a filter. For example, userPrincipalName=${userName}.
     - Scope of Search: Select Subtree.
   - On the Extended Contract tab:
     - By default, the following are added:
       - DN
       - email
       - givenName
       - username
4. Click Next then click Save.

2. Map the Validator in the Authorization Server Settings.
   1. Go to System > OAuth Settings > Authorization Server Settings.
   2. In Password Credentials Validator, select the one you previously created. For example, this documentation uses MDSS Validator.
   3. Click Save.

3. Create the Resource Owner Credentials Grant Mapping.
   1. Go to Authentication > OAuth > Resource Owner Credentials Mapping.
   2. In the Resource Owner Credentials Grant Mapping window:
      - Source Password Validator Instance: Select the one you previously created and click Add Mapping.
   3. In the Resource Owner Credentials Grant Mapping | Resource Owner Credentials Mapping page, click Next to skip the Attribute Sources & User Lookup tab.
   4. On the Contract Fulfillment tab:
      - For USER_KEY, select Password Credentials Validator, and for Value, select username.
   5. Click Next to skip the Insurance Criteria tab then click Save.

4. Create the Access Token Mapping - Map the Password Credentials Validator to the Access Token Manager.This mapping is needed for the Password Grant workflow. If the mapping does not exist, PingFederate logs the following error: There are no access token managers available for the selected client and authentication context.
    1. Go to Applications > Access Token Mappings.
        - Context: Select the one you previously created. For example, this documentation uses MDSS Validator.
        - Access Token Manager: Select the one previously created. For example, this documentation uses MDSS Access Token Manager.
    2. Click Add Mapping.
    3. Click Next to skip the Attribute Sources & User Lookup tab.
    4. On the Contract Fulfilment tab select userName
    5. Click Next to skip the Insurance Criteria tab then click Save.

Create the Authorization Code Flow Configuration

1. Create the IdP Adapter.
    1. Go to Authentication > Integration > IdP Adapters.
    2. Create Create New Instance.
    3. On the Type tab:
        - Instance Name: Enter a name, for example, HTML Form Auth Adapter.
        - Instance ID: Enter an ID, for example, HTMLFormAuthAdapter.
        - Type: Select HTML Form IdP Adapter.
        - Parent Instance: Select None.
    4. Click Next.
    5. On the IdP Adapter tab:Under Password Credential Validator Instance, click Add a new row to 'Credential Validators.' then select a validator (in this documentation, MDSS Validator is used), and click Update.
    6. Click Next.
    7. Click Next to skip the Extended Contract tab.
    8. On the Adapter Attributes tab:
        - Unique User Key Attribute: Select username and check Pseudonym.
    9. Click Next to skip the Adapter Contract Mapping tab then click Save.
2. Create IdP Adapter Grant Mapping.
    1. Go to Authentication > OAuth > IdP Adapter Grant Mapping.
    2. Source Adapter Instance: Select the Adapter instance you just created and click Add Mapping.

3. On the Attribute Sources & User Lookup page, click Add Attribute Source.
4. Enter the information as follows for each tab, then click Next to advance.
   - On the Data Store tab:
     - Attribute Source ID: Enter an ID with alphanumeric values.
     - Attribute Source Description. Enter a description.
     - Active Data Store: Select the active directory in use.
   - On the LDAP Directory Search tab:
     - Base DN: Enter your base DN to find your users and groups.
     - Search Scope: Use the default, Subtree.
     - Attributes to return from search: Select , then, once loaded, from the attribute list, select userPrincipalName.
5. Click Add Attribute then click Next.
6. On the LDAP Filter tab:
   - Filter: Enter the filter. For example, `userPrincipalName=${userName}`.
7. Click Next then click Save.
8. In the IdP Adapter Grant Mapping | IdP Adapter Mapping page, finish creating the IdP Grant Mapping.On the Contract Fulfillment Lookup tab, use the following table.

Contract	Source	Value
USER_KEY	Select the source previously created.	Subject DN
USER_NAME	Select the source previously created.	userPrincipalName

I. Click Next then click Save

3. Map the IdP Adapter to Access Token Manager.
4. Go to Applications > OAuth > Access Token Mappings.
   - Context: Select IdP Adapter:Adapter Name.
   - Access Token Manager: Select the access token manager instance previously created. For example, in this documentation, it is MDSS Access Token Manager.
5. Click Add Mapping.If you do not perform this mapping, PingFederate generates the following log file message: There are no mapped authentication sources to choose from. Please map an IdP Adapter or IdP connection first.
6. Skip the Attribute Sources & User Lookup tab, and on the Contract Fulfillment tab, add the following:

Contract	Source	Value
userName	Adapter	username

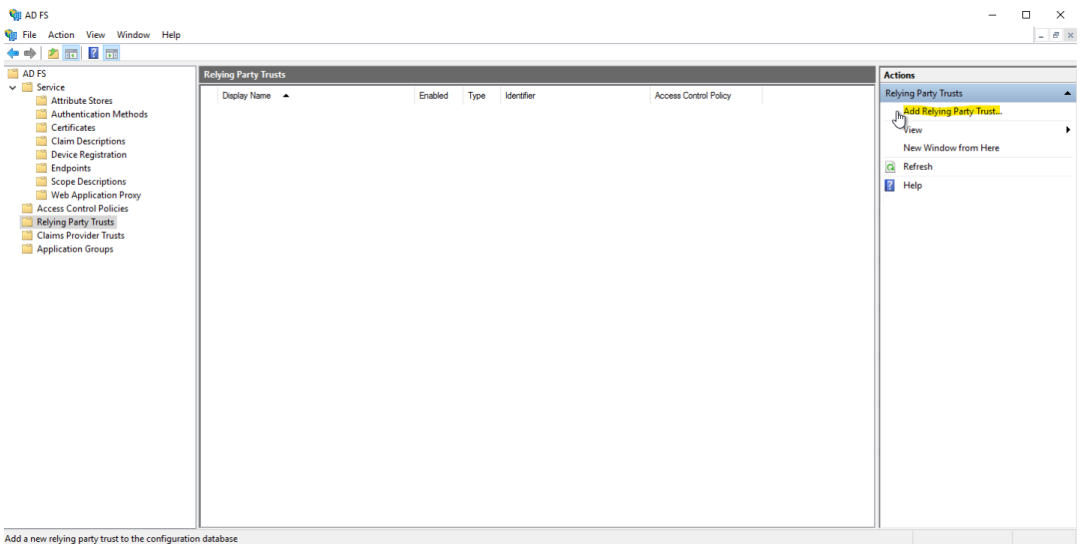
- Click Next to skip the Insurance Criteria tab then click Save.

AD FS SAML2 Specific Configuration

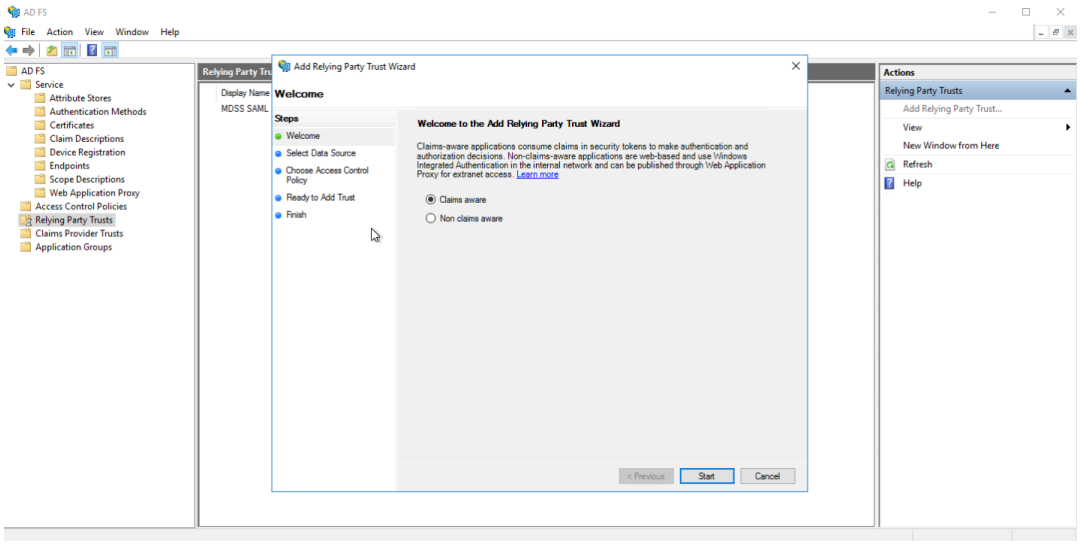
> **Info**
>
> To properly access MDSS, the following AD **Security Groups** are required:
>
> - **SsoAdministrator** - the equivalent of local MetaDefender Storage Security administrator role
> - **SsoReadOnlyAdministrator** - the equivalent of local MetaDefender Storage Security read-only role
>
> It is also necessary for the AD user to have an **email address** set up, so that it is set as the MetaDefender Storage Security's user email.
>
> The only supported secure hash algorithm for signing SAML requests is **SHA-256**.

To set up AD FS SSO with SAML2 for **MDSS**, follow these steps:

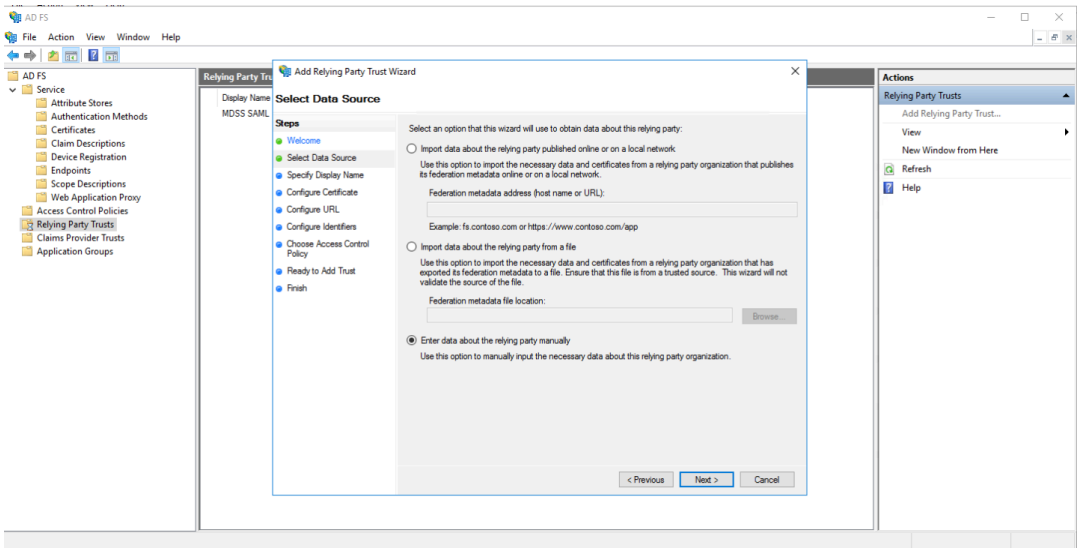
1. Within the AD FS settings, navigate to the "**Relaying Party Trusts**" directory and click "**Add Relaying Party Trust**"



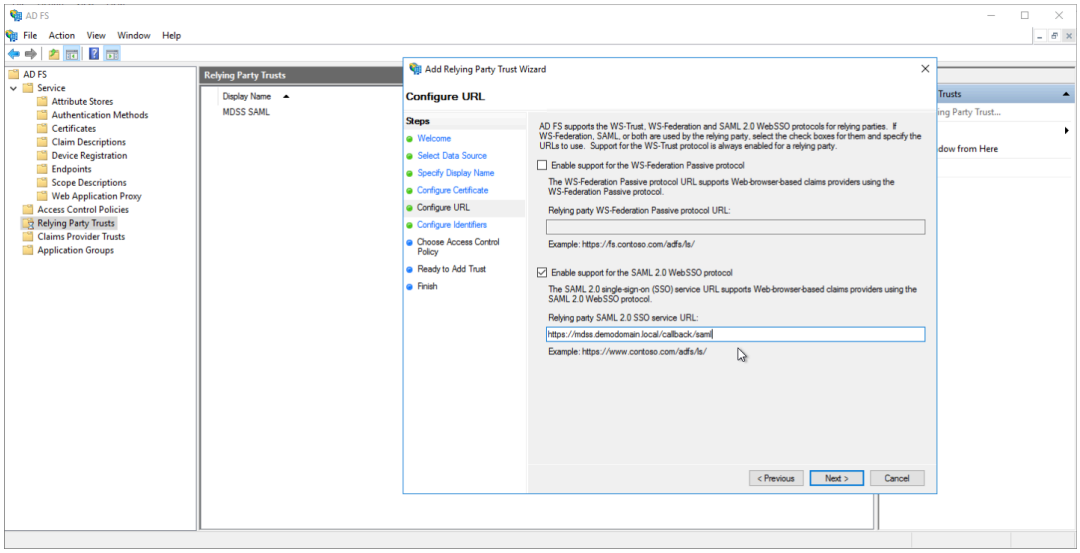
2. Check **Claims Aware** for the first step



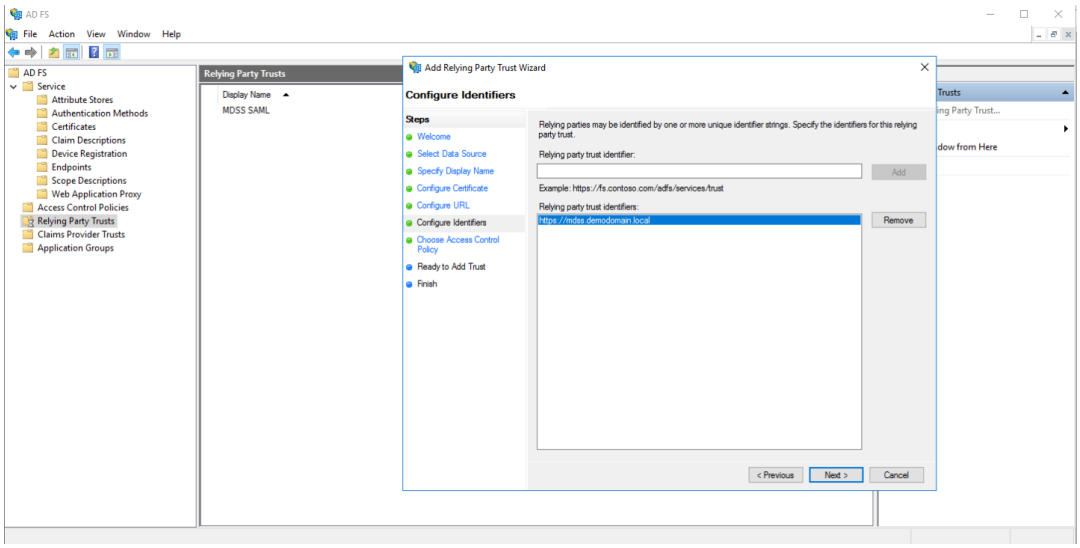
3. Select Enter data about the relaying party manually



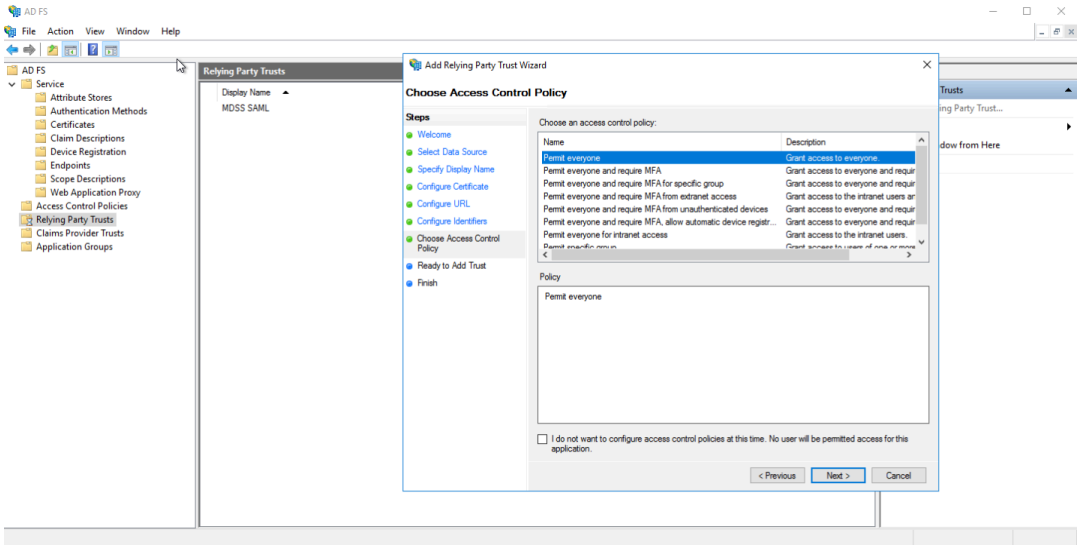
4. Give your Relaying party any name you like, and at the configure certificate step, do not enter any encryption certificate and go to the next step (MDSS does not currently support claim encryption)
5. Check Enable support for the **SAML 2.0 WebSSO** protocol, and enter the service URL of **MDSS** (this URI is of form *https:///callback/saml*)



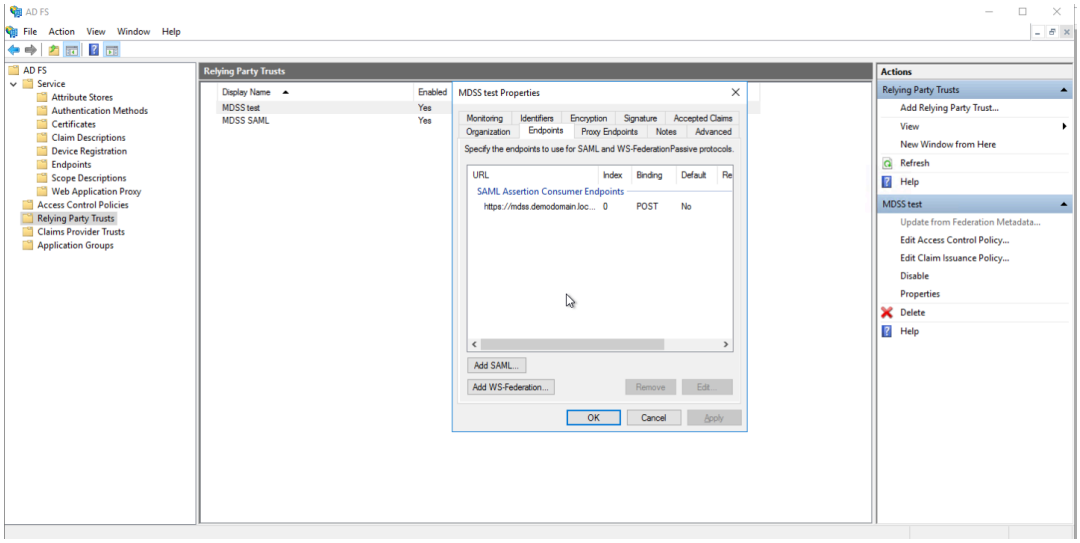
6. Enter the URI of the **MDSS** instance as the relaying party identifier [this URI is of form *https://*]



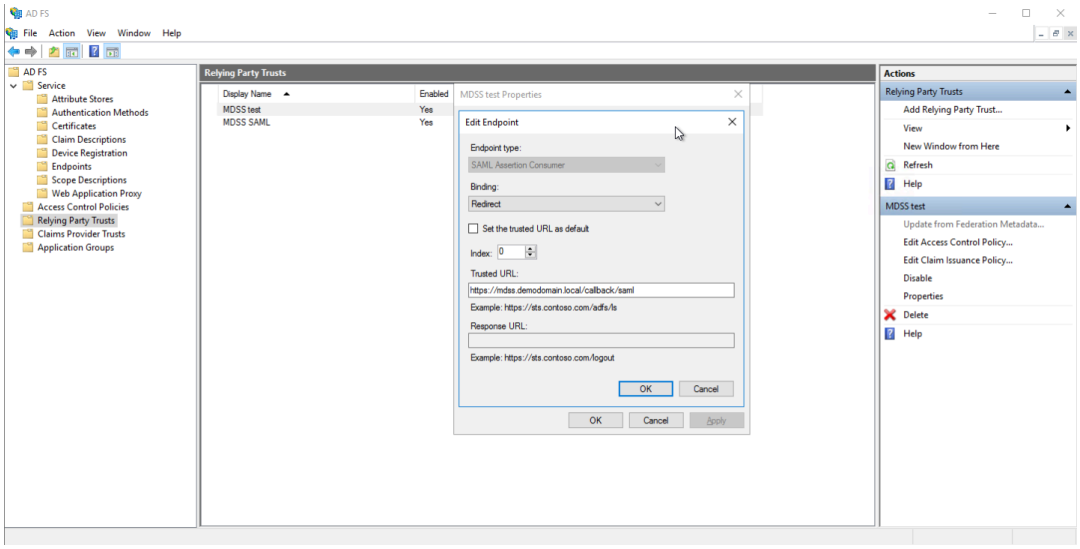
7. For the access **control policy**, select "**Permit everyone**"



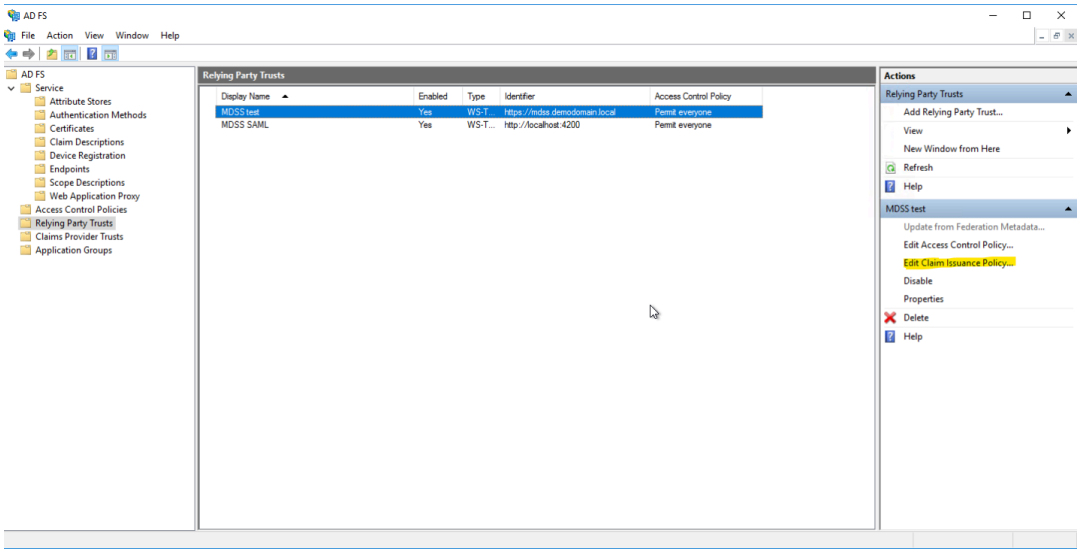
8. Confirm the settings added so far and finish.
9. Select the created Relaying Party Trust, click on **Edit Access Control Policy**, and go to the Endpoints tab.



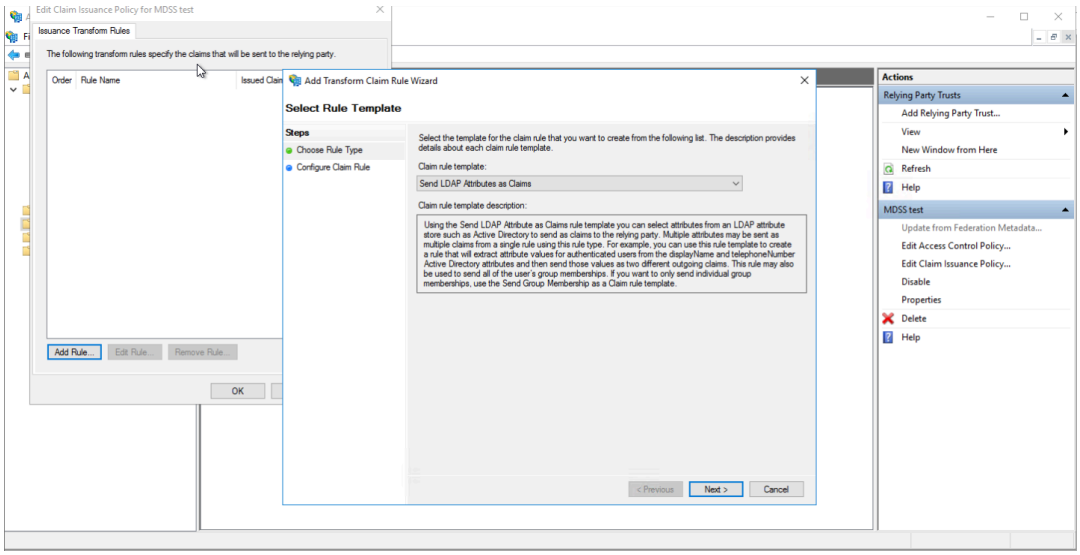
10. Select the configured endpoint, change the binding type to **Redirect**, and save it.



11. Select the created Relaying Party Trust and click on **Edit Claim Issuance Policy**

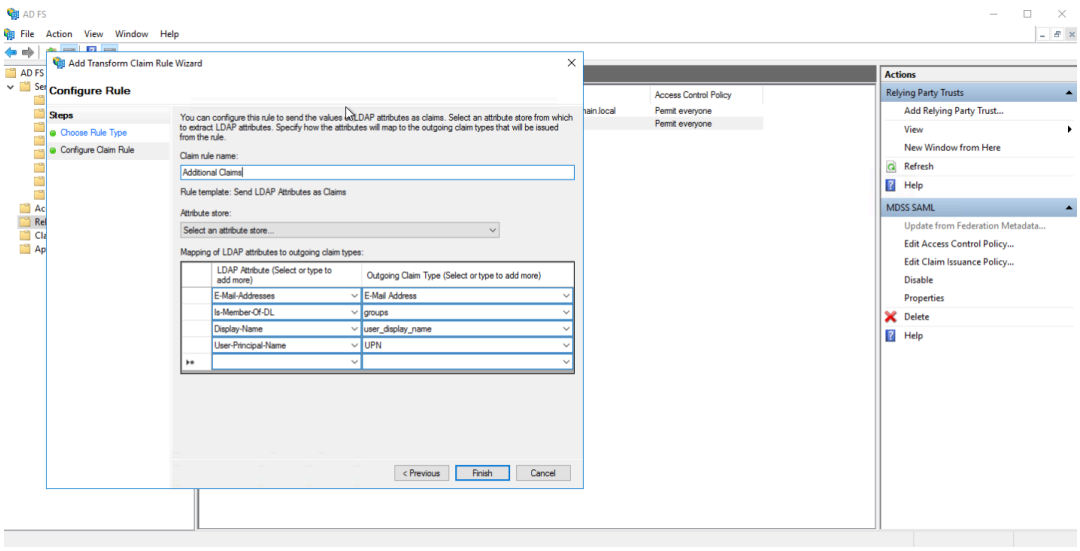


12. Add a rule and select "**Send LDAP Attributes as Claims**" as the **Claim Rule Template**

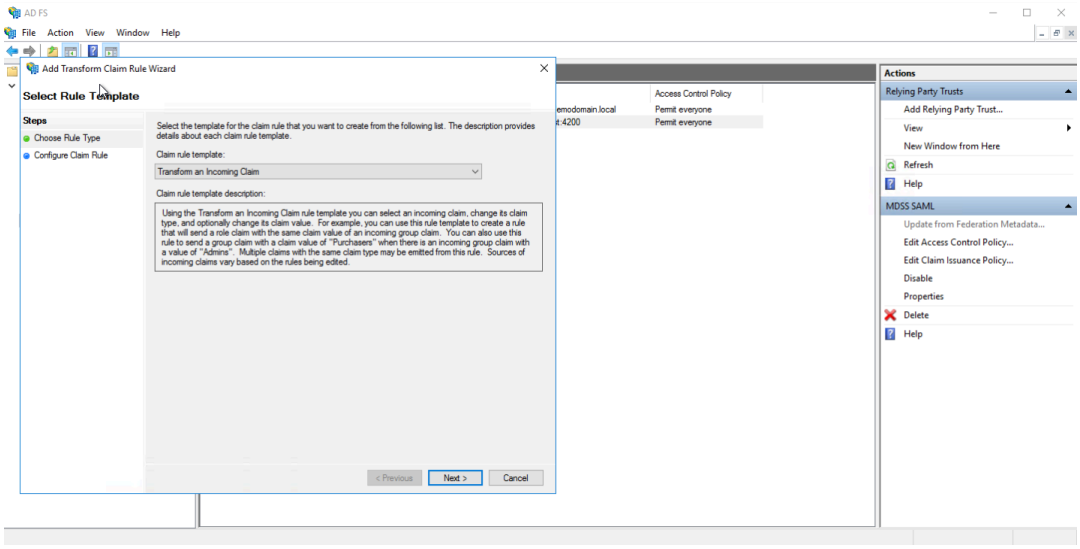


13. Give the rule a name, select **Active Directory** as the attribute store and configure the following:

- **E-Mail Address** as **E-mail Address**
- **Is-Member-Of-DL** as **" groups*****
- **Display-Name** as ***"user_display_name"***
- **User-Principal-Name** as ***"UPN"***

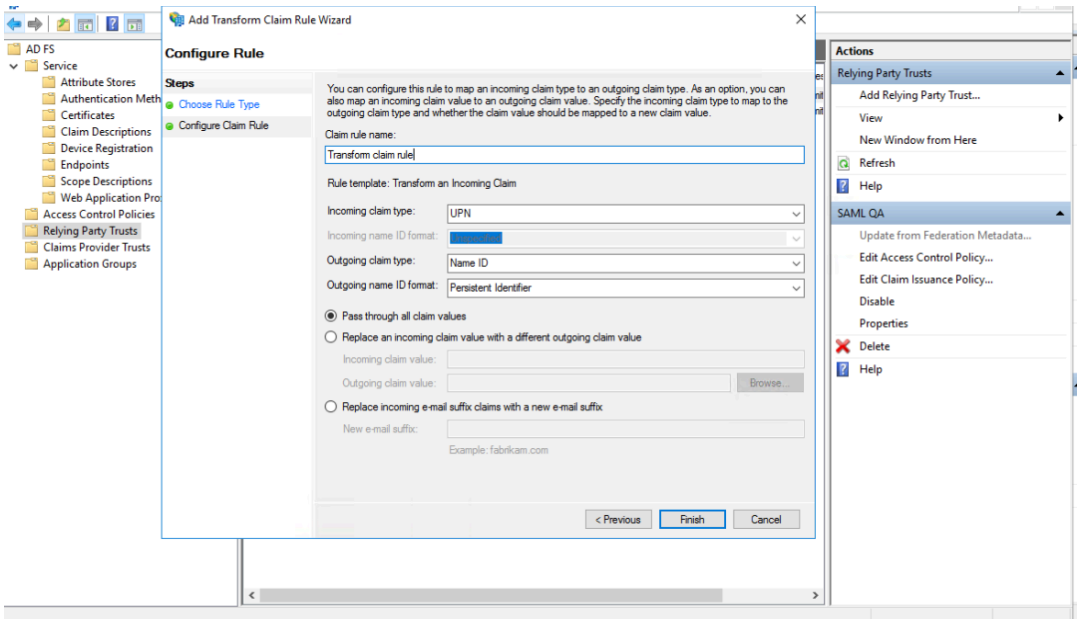


14. Add a rule and select "**Transform an Incoming Claim**" as the Claim Rule Template

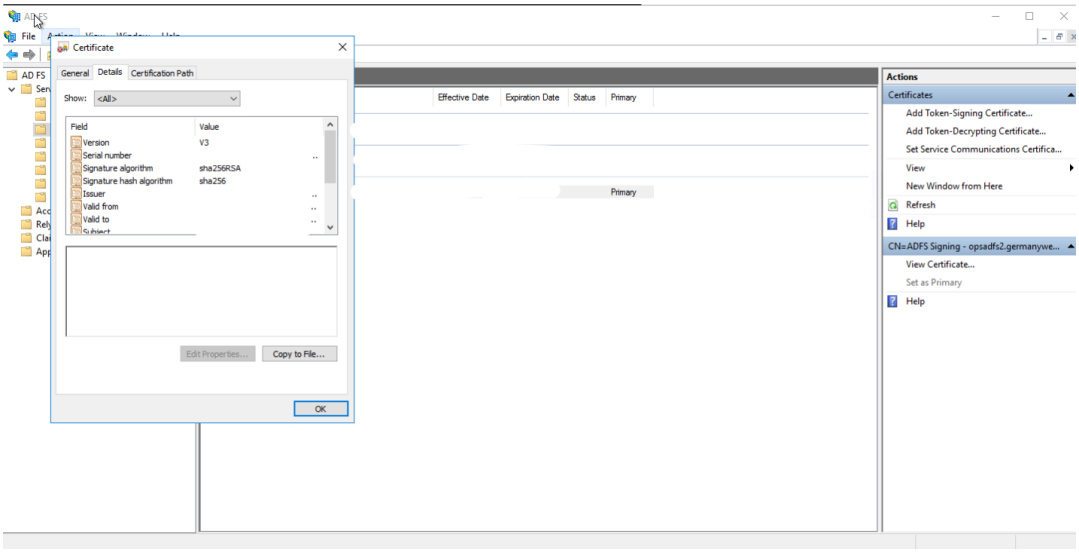


15. Give the rule a name, select **Active Directory** as the attribute store and configure the following:

- **“UPN”** at **Incoming claim type**
- **"Name ID"** at **Outgoing claim type**
- **“Persistent Identifier”** at ***Outgoing name ID format*** __ Next, within the



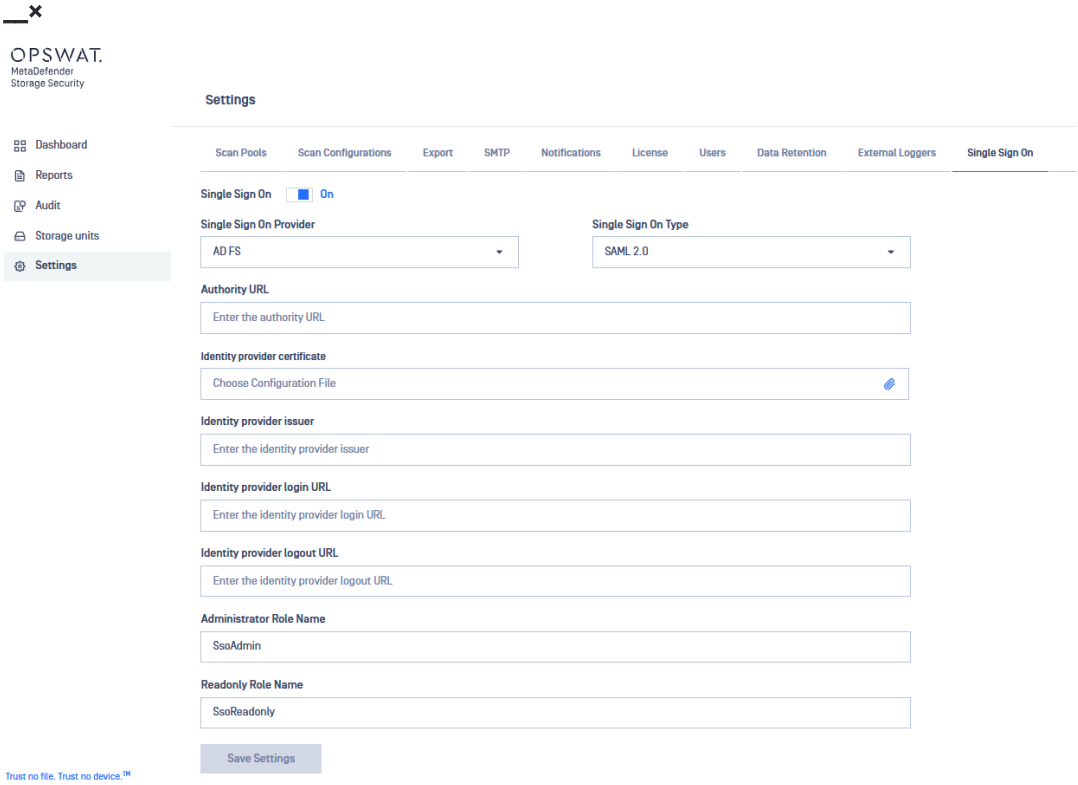
16. Next, within the **AD FS settings**, navigate to the “**Service/Certificates**” directory and double click on your token signing certificate. On the Details tab click Copy to File to save the certificate and use it when configuring SSO on MDSS.



17. On **MDSS**, under the **Single Sign On page** from Settings, configure your provider with the following settings:

- **Authority URL**: the base URL of your AD FS server used for retrieving Federation Metadata (eg. https:/adfs..com/)
- **Identity provider certificate**: the certificate obtained earlier from AD FS
- (Optional) **Identity provider issuer**: the claim issuer identifier used to sign the incoming claims (eg. https://adfs..com/adfs/services/trust)
- (Optional) **Identity provider login URL**: the login URL of the AD FS instance (eg. https://adfs..com/adfs/ls/)
- (Optional) **Identity provider logout URL**: the logout URL of the AD FS instance (eg. https://adfs..com/adfs/ls/)
- **Administrator account role name**: if you use custom group names assigned to your SSO users, pick a different role from the default
- **ReadOnly account role name**: if you use custom group names assigned to your SSO users, pick a different role from the default

> **Info**
>
> If your AD FS instance supports **Federation metadata** and has it enabled and configured on the */FederationMetadata/2007-06/FederationMetadata.xml* URL, the Issuer, login and logout URL fields are not required, and will be retrieved from the received federation metadata. Otherwise, they must be provided.
>
> If the fields are populated, they will override any value retrieved from the federation metadata, and cause the **Authority URL** to not be validated.


OPSWAT.
MetaDefender
Storage Security
Dashboard
Reports
Audit
Storage units
Settings
Trust no file. Trust no device.™
Settings
Scan Pools
Scan Configurations
Export
SMTP
Notifications
License
Users
Data Retention
External Loggers
Single Sign On
Single Sign On
On
Single Sign On Provider
AD FS
Single Sign On Type
SAML 2.0
Authority URL
Enter the authority URL
Identity provider certificate
Choose Configuration File
Identity provider issuer
Enter the identity provider issuer
Identity provider login URL
Enter the identity provider login URL
Identity provider logout URL
Enter the identity provider logout URL
Administrator Role Name
SsoAdmin
Readonly Role Name
SsoReadonly
Save Settings

Database procedures

> **Warning**
>
> Whether you use the internal PostgreSQL or an external one, the installed version should be 17.

MetaDefender Storage Security includes an internal PostgreSQL instance by default, currently running on version 17.

For environments with high loads or where high availability is required, the internal PostgreSQL instance can be replaced with a cloud-managed alternative. Instructions for making this switch are provided here: AWS RDS with PostgreSQL

AWS RDS with PostgreSQL

Support AWS Services with PostgreSQL Engines

MetaDefender Storage Security natively supports AWS RDS and Aurora with PostgreSQL engine (Supported PostgreSQL versions)**.** MetaDefender Storage Security does not require any specific pre-installation steps to work with Amazon RDS - all required extensions are performed internally during installation of the product.

Regarding Aurora support, as it generates 2 endpoints, **Cluster endpoint** for administrate, insert and read. And the **reader endpoint** that is only for reading using the LB that get the information from any instance of the cluster. MetaDefender Storage Security only supports connections to 1 endpoint, the cluster endpoint, that allow the application do all the actions needed. Info from AWS

You can create and configure AWS RDS and PostgreSQL by following the guide here.

Database Configuration

High Availability with AWS RDS

AWS RDS supports various multi-az deployment that can be configured following this documentation. You can compare the different configuration options available in this AWS documentation. For having MetaDefender Storage Security installed using any of this approaches we recommend to follow the instructions indicated by AWS in case of having MDSS installed in a EC2 instance. For EKS Cluster deployment OPSWAT provide a terraform code to deploy it together with the K8S cluster, see Deployment on EKS

Database Sizing

It depends on how many requests or traffic is sent to MetaDefender Storage Security, and how complex the files are. As average the minimum database size desired **for each 1,000,000 analysis reports** added is **6 GB.**

The recommended AWS RDS Instance Type is **db.r6g.xlarge** and the storage type recommended is General Purpose SSD. For gp2 storage type **the minimum size is 20 GiB** so this is marking as the minimum storage needed for working with MetaDefender Storage Security.

Security Group Configuration

MetaDefender Storage Security does not require that the RDS database is publicly accessible. For enhanced security, OPSWAT recommends the following:

- Do NOT deploy the database in a public subnet.
- Do NOT include ingress security group rules with 0.0.0.0/0 sources
- Do NOT set the Amazon RDS Publicly Accessible parameter to true in terraform project for Kubernetes deployment

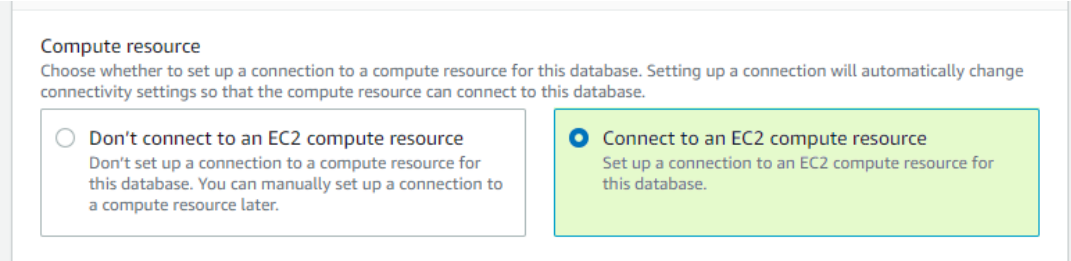
Database Connection

For general information of how to connect to the RDS depending on the scenarios it is recommended to read this docs from AWS.

Connect to RDS in Private Subnet

To connect MetaDefender Storage Security with RDS hosted in a private subnet, the configuration will depend on the type of deployment.

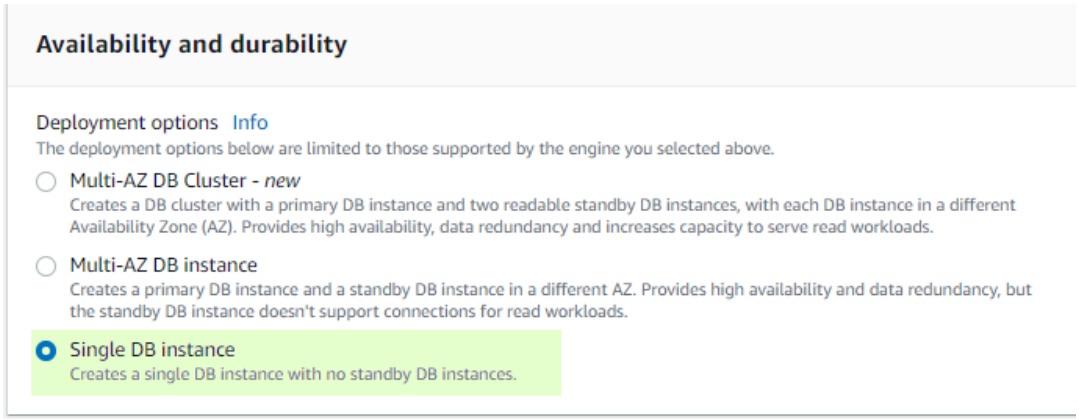
For Single EC2 deployment, it is needed to indicate that the RDS will be only available from the EC2 instance where MetaDefender Storage Security is running, configuring it from the Connectivity section when creating the RDS instance as following.



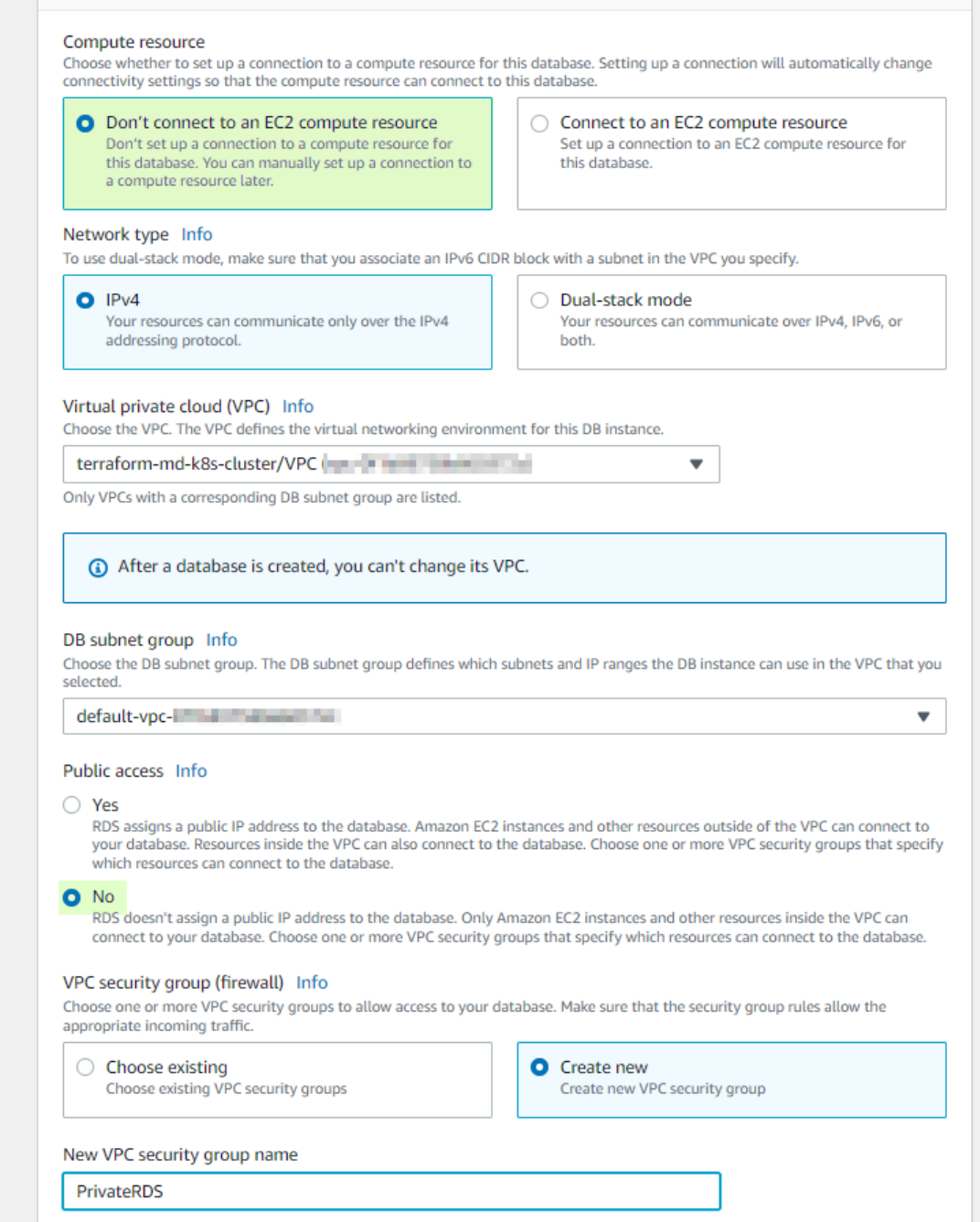
For EKS deployment, using the terraform project provided by OPSWAT it is deployed in a private subnet only allowing access from VPC CIDR where the EKS cluster is deployed. In

case of creating the RDS instance from the console follow these steps

1. Indicate if you want to deploy it in Multi-AZ or Single DB



2. Indicate not to connect to an EC2 and the VPC public access “No”. For multiple VPC, deploy it in a different VPC than EKS. This example is using the same VPC



Multiple VPC for MetaDefender Storage Security and AWS RDS

When working with multiple VPCs where we have deployed MetaDefender Storage Security either in a Single EC2 or with EKS in one VPC and the RDS instance in a different VPC, it will be needed to configure a VPC peering between both VPC for MetaDefender Storage Security to use the database.

Steps to configure it

1. Create a Peering Connection between both VPCs

2. Modify the route table to route the traffic to the peering for the requests from both VPCs
3. Modify the security group to allow connections from both VPCs

Database Endpoint Management

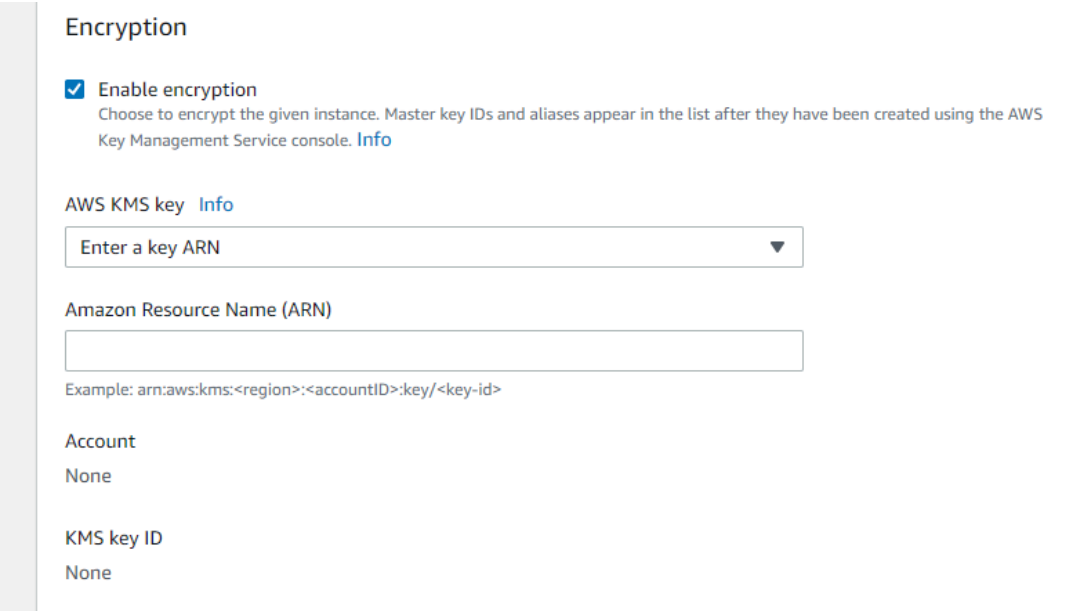
The database connection endpoint is generated by AWS once the RDS instance is created you can access to this information on the **Connectivity & security** tab. Once you have this information it should be set up in the `ConfigMap` , configuring the hostname of the database and the port to match the new RDS instance.

More detailed information from AWS here.

Database Encryption

MetaDefender Storage Security supports both native OS encryption or EBS encrypted volumes. The database is secured via credentials and can be configured to encrypt everything at rest. In general, OPSWAT recommends the use of a 3rd party database layer, e.g. Amazon Aurora or RDS, which should be encrypted. It is best practice to not share the database layer on the same hosts/VM/EC2 instance.

For encrypting RDS this is the recommended configuration



Exporting database

We offer the option to export your database if you need to use it for migration or debugging purposes.

```
PS> .\mdss.ps1 -u export_db
```

```
sudo mdss -u export_db
```

Upgrade Guide to PostgreSQL [MDSS v4.0.0]

MDSS v4.0.0 Upgrade Guide: MongoDB to PostgreSQL Migration

Overview

Starting with MDSS version 4.0.0, PostgreSQL replaces MongoDB as the primary database backend. This guide covers the upgrade process, migration scenarios, and best practices for a seamless transition.

Key Changes in v4.0.0

- **Database Backend**: PostgreSQL replaces MongoDB
- **Automatic Migration**: Data is migrated by default during upgrade
- **External Database Support**: Improved support for external PostgreSQL instances

Pre-Upgrade Considerations

When Data Migration Occurs

Data migration happens automatically when upgrading from any MDSS version < 4.0.0 and any of the following conditions are met:

- Previous version uses internal/bundled MongoDB
- New version is configured to use external PostgreSQL
- Both previous and new versions are configured with external databases

> **Warning**
>
> Data migration from MongoDB to PostgreSQL takes about **2-3 hours / 1M files** in the original database. In this time MDSS is not available for operation. Other upgrade options are available below.

When Data Migration is Skipped

Data migration is **automatically skipped** when all the following conditions are met:

- Previous version uses external MongoDB
- New version is configured with bundled PostgreSQL deployment

> **Info**
>
> ⚠️ Important: This prevents unintentional migration of cloud/external data to local deployments.

Data migration is also skipped after a successful installation or upgrade of MDSS v4.0.0 on the same machine so that **data is migrated only once**. This is done in order to ensure data in MDSS v4.0.0 is not overwritten by an unintentional migration from an older version.

Upgrade Options

Option 1: Standard Upgrade with Migration

Recommended for: Small to medium deployments where historical data is required.

1. **Backup your current deployment**
2. **Upgrade to v4.0.0** using your standard deployment process
3. **Monitor the migration** - duration depends on data volume

Configuration: No additional configuration needed for default migration.

Option 2: Skip Data Migration

Recommended for: Large deployments or when historical data is not critical.

Add the following to your `customer.env` file before upgrading:

```
SKIP_MONGO_TO_PG=yes
```

> **Info**
>
> 💡 Time Savings: For large datasets, migration can take several hours. Skipping migration provides immediate availability of the new version.

Option 3: Blue-Green Deployment

Recommended for: Production environments requiring zero downtime and maximum safety.

Process:

1. **Deploy v4.0.0 in parallel** to your existing environment **without starting any scans**
2. **Configure the new deployment** with the same settings as the old one
3. **Test thoroughly** without activating storage processing
4. **Stop storage processing** on the old version (while keeping it running for rollback capability)
5. **Activate storage processing** on the new v4.0.0 deployment
6. **Monitor the new deployment** for proper functionality
7. **Decommission old environment** after validation period

Benefits:

- Controlled transition of storage processing
- Easy rollback by reversing the process
- No data migration time
- Fresh start with optimized database
- Prevents duplicate storage scanning

External PostgreSQL Configuration

Recommended Providers

For production deployments, consider these managed PostgreSQL services for better performance, reliability and high availability options:

- **AWS RDS PostgreSQL**
- **Google Cloud SQL for PostgreSQL**
- **Azure Database for PostgreSQL**

Connection Configuration

To use an external PostgreSQL database, add the following to your `customer.env` file:

```
POSTGRESQL_URL=Host={your_pg_host};Port=5432;Username=
{your_pg_user};Password={your_pg_password};Database=MDSS
```

Example configurations:

```
# AWS RDS
POSTGRESQL_URL=Host=mdss-prod.cluster-xyz.us-east-
1.rds.amazonaws.com;Port=5432;Username=mdss;Password=SecurePassword123;
Database=MDSS

# Google Cloud SQL
POSTGRESQL_URL=Host=10.1.2.3;Port=5432;Username=mdss;Password=SecurePas
sword123;Database=MDSS

# Self-hosted with HA
POSTGRESQL_URL=Host=postgres-
cluster.internal;Port=5432;Username=mdss;Password=SecurePassword123;Dat
abase=MDSS
```

Database Configuration Recommendations

Connection Limits

Ensure your PostgreSQL instance has adequate connection limits:

```
-- Recommended minimum for production
ALTER SYSTEM SET max_connections = 1000;
SELECT pg_reload_conf();
```

Performance Tuning

Consider these PostgreSQL settings for optimal MDSS performance:

```
-- Memory settings (adjust based on your server capacity)
ALTER SYSTEM SET shared_buffers = '8GB'; -- for best performance set to
about 1/4 of total available memory
ALTER SYSTEM SET effective_cache_size = '16GB'; -- for best performance
set to about 1/2 of total available memory
ALTER SYSTEM SET work_mem = '256MB';
ALTER SYSTEM SET temp_buffers = '64MB';
ALTER SYSTEM SET maintenance_work_mem = '2GB';

-- WAL (Write-Ahead Logging) configuration
ALTER SYSTEM SET wal_level = 'minimal';
ALTER SYSTEM SET max_wal_senders = 0;
ALTER SYSTEM SET max_replication_slots = 0;
ALTER SYSTEM SET max_wal_size = '2GB';
ALTER SYSTEM SET min_wal_size = '160MB';

-- Connection and logging
ALTER SYSTEM SET log_statement = 'none';
ALTER SYSTEM SET log_min_duration_statement = 1000;
```

More details on configuring allocated resources on a PostgreSQL database can be found in their official documentation here.

What Gets Migrated

- User accounts and permissions
- Configuration settings
- Historical data and logs
- Custom configurations
- Dashboards and reports
- Storages

> **Warning**
>
> **Special attention** on Real Time Processing, Storage Remediations and Scan Configurations migration.
>
> The idea of Workflow is the result of merging Scan Configuration and Storage remediations. To not lose any remediations from storage, a Workflow shall be created starting from Default Scan Configuration and appending the Storage Remediations.
>
> Remediation of DeepCdr with encrypt original will be migrated to Keep Allowed and Keep Blocked for the original file
>
> The existent Scan Configuration will be migrated with only Keep Allowed and Keep Blocked remediations which are the defaults.
>
> Real Time Processing shall be migrated using the new Workflow created from that specific storage

Troubleshooting

Connection Issues

```
# Verify PostgreSQL connectivity
psql -h your-host -p 5432 -U mdss -d MDSS -c "SELECT version();"
```

Rollback Procedure on Linux

If you need to rollback after upgrade:

1. **Set** in `customer.env`: `ENV_IMAGE_TAG=stable3.6.1`
2. **Run the update command: **sudo mdss -u update**

3. **Verify connectivity** to your original MongoDB database
4. **Confirm functionality** and data integrity

In order to perform the rollback on an offline deployment you need to (re)deploy the docker offline toolkit for version 3.6.1.

Rollback Procedure on Windows

If you need to rollback on a Windows deployment:

1. Stop MDSS
2. Backup the MongoDB data folder: `C:\Program Files\OPSWAT\MetaDefender Storage Security\data\mongo` - preferably before upgrading to v4.0.0 but this folder should be kept even after an upgrade
3. Uninstall MDSS 4.0.0
4. Install MDSS 3.6.1
5. Stop MDSS (after the installation is complete it start automatically)
6. Replace the MongoDB data folder with the previously created backup.
7. Start MDSS

Running the data migration manually

In order to migrate the data from an older MongoDB database and overwrite any existing data in the new PostgreSQL database:

1. Clear the **SKIP_MONGO_TO_PG** variable from the `.env` and `customer.env` files and from the system environment variables (Windows only)
2. Delete the PostgreSQL data docker volume `mdss_postgres_data` (Linux only): `docker volume rm`mdss_postgres_data``
3. Restart MDSS v4.0.0

> **Info**
>
> 💡 Notes:
>
> - The migration process doesn't modify your original MongoDB database, so rollback is straightforward by reverting to the previous MDSS version.
> - Modifications performed after the upgrade will not be kept after the rollback.
> - Rollback is only supported to version 3.6.1.

> **Warning**

> The only backup of the original MongoDB database is in the original docker volume called **mdss_****mongo_db. Uninstalling MDSS or performing any cleanup operations will delete this volume permanetly.__

Database Vacuum

Over time, the MDSS database accumulates index bloat and heap fragmentation as a result of deleted rows — for example, after a retention policy run or a large scan cleanup job. The `mdss -u vacuum` command provides two maintenance modes to address these issues.

Normal mode -

```
sudo mdss -u vacuum
```

Rebuilds bloated indexes with no service interruption. All MDSS services remain running throughout.

What it does:

- Runs `VACUUM ANALYZE` on all tables — clears dead rows and updates query planner statistics
- Runs `REINDEX TABLE CONCURRENTLY` on `files`, `object_identity`, and `scan_results` — rebuilds indexes from scratch without locking reads or writes

What you get: Query performance is restored. Index sizes typically shrink by 55–70% after a large deletion.

What you don't get: Heap disk space is not reclaimed. Table file sizes on disk remain unchanged — this is expected PostgreSQL behavior. Only `VACUUM FULL` can physically rewrite and shrink the heap file.

Full mode -

```
sudo mdss -u vacuum -f
```

> **Warning**
>
> The full vacuum requires a service outage

What it does:

1. Stops all MDSS services (`mdss stop`)

2. Runs `VACUUM FULL ANALYZE` — rewrites every table into a compact heap file; all dead-row pages are fully eliminated
3. Runs `REINDEX DATABASE` — rebuilds every index from the freshly compacted heap
4. Restarts all MDSS services (`mdss start`)

> **External PostgreSQL:** For deployments using an external PostgreSQL server, no temporary container is used. Services are still stopped before and restarted after the operation.

What you get: Both index bloat and heap fragmentation are resolved. Disk space is returned to the OS. Table sizes drop in proportion to the number of live rows remaining.

What you don't get: There is no way to run this without a service interruption. If downtime is not acceptable, run normal mode instead — query performance will be restored, but disk space will not be reclaimed until a maintenance window is available.

Planning downtime for full vacuum

The duration depends primarily on the size of the PostgreSQL database on disk. Because services are stopped before the operation runs, there is no lock contention and the work proceeds at full I/O speed.

DB size	Vacuum full	Service stop/start	Total downtime estimate
<1 GB	~1 - 2 min	~2 - 5 min	~3 - 7 min
~5 GB	~2 - 5 min	~2 - 5 min	~4 - 10 min
~20 GB	~5 - 10 min	~2 - 5 min	~7 - 15 min
~100 GB	~30 - 40 min	~2 - 5 min	~35 - 45 min
500 GB+	> 3 h	~2 - 5 min	> 3 h

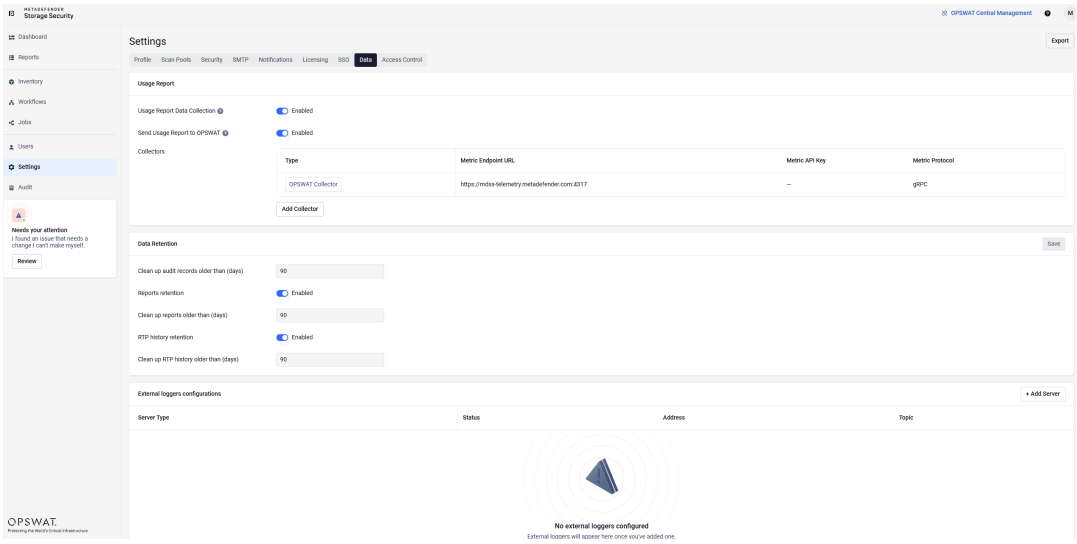
> **Info**
>
> On HDD storage, network-attached storage, or a heavily loaded host, the VACUUM FULL + REINDEX duration will be significantly longer.

Database Retention

To effectively manage data volume, MDSS provides the ability to clean up specific types of information after a defined period.

MDSS focuses on certain types of information that tend to grow significantly over time.

- Audit records can be automatically cleaned after a configurable number of days.
- Report records can be automatically cleaned after a configurable number of days.
- Real-time processing history can also be cleaned after a configurable number of days.



File Discovery Debounce

The MDSS file discovery system uses a debounce mechanism to determine when files are stable and ready for processing. Several key environment variables control this behavior, working together to create a consistent file discovery experience while accommodating the unique characteristics of different storage types.

Environment Variables

Global Debounce Interval

`FILE_DISCOVERY_DEBOUNCE_INTERVAL=0`

This variable defines the minimum time that must elapse before a previously processed file is considered "new" again after being edited.

- **Default value**: 0 seconds (files are considered new after any edit)
- **Purpose**: Prevents duplicate processing of the same file when multiple rapid edits occur
- **Global setting**: Applies to all storage types as a baseline

Storage-Specific Debounce Times

`SFTP_DISCOVERY_DEBOUNCE_TIME_SECONDS=5`

`NFS_DISCOVERY_DEBOUNCE_TIME_SECONDS=5`

`SMB_DISCOVERY_DEBOUNCE_TIME_SECONDS=120`

These variables define how long the system waits to confirm a file is fully uploaded and stable before processing it. The system checks if the file has been modified within this time period. If no modifications are detected during this interval, the file is considered ready for processing.

- **Default value**: 5 seconds
- **Purpose**: Prevents processing of partially uploaded files

Interaction Between Settings

The interaction between these settings follows this rule:

Storage-specific debounce values must be lower than or equal to the global `FILE_DISCOVERY_DEBOUNCE_INTERVAL`. If a storage-specific value is set to be bigger than the global interval, the system will automatically use the global `FILE_DISCOVERY_DEBOUNCE_INTERVAL` value instead. This ensures consistent minimum

debounce times across all storage types. However, if the global `FILE_DISCOVERY_DEBOUNCE_INTERVAL` is set to 0, the system will honor the storage-specific values, allowing for customized debounce intervals per storage type.

The SMB service operates in two modes, controlled by the environment variable `SMBSERVICE_FILE_READY_CHECK_MODE`:

- `FILE_OPEN_CHECK` (value: `1`) – the default mode set by MDSS.
- `DEBOUNCE_CHECK` (value: `0`).

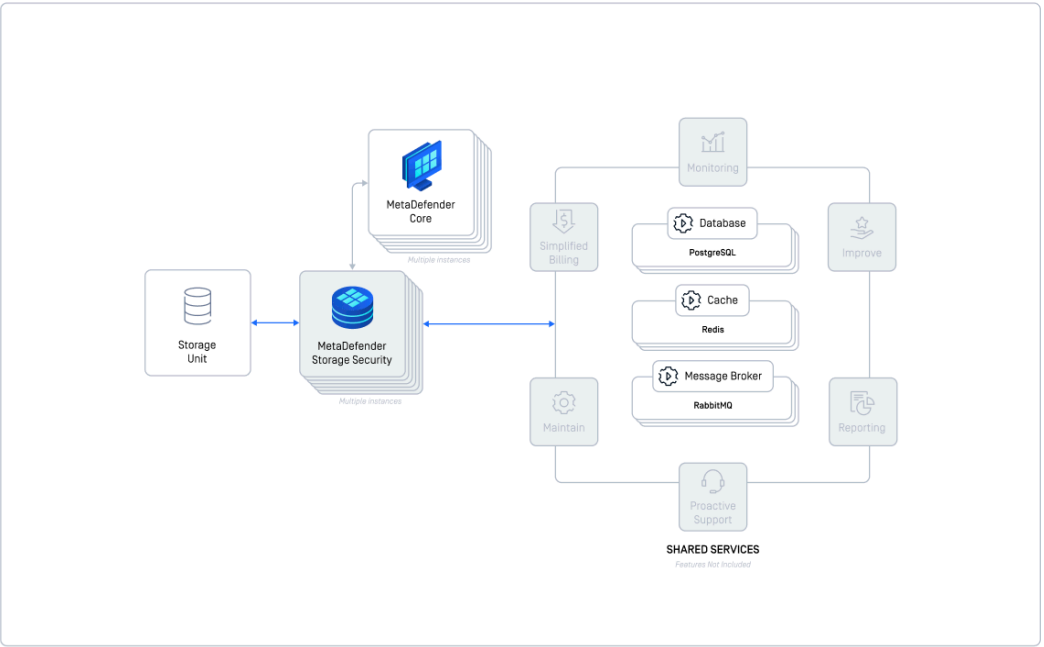
To enable file debounce for SMB, set `SMBSERVICE_FILE_READY_CHECK_MODE` to `0`.

Active-Active configuration

This guide explains how to configure an active-active deployment of MDSS where multiple instances can use the same shared external services for improved performance and scalability.

Overview

In an active-active deployment, multiple MDSS instances work together using shared external components (RabbitMQ, PostgreSql, and Redis) to distribute workload, add redundancy and improve throughput. This configuration is particularly useful when handling large volumes of files.



Active-Active Configuration Behavior

In an active-active configuration, file processing operations are distributed dynamically across available instances:

- **File Discovery** - any available MDSS instance can detect and identify files requiring processing
- **File Scanning** - any available MDSS instance can perform the security scanning operation
- **Remediation** - any available MDSS instance can execute the remediation actions

Key Points

- Operations may be handled by different instances (distributed processing) or by the same instance (consolidated processing)
- The actual distribution depends on which instance processes the message first
- This design ensures optimal load balancing and high availability across your deployment

This approach maximizes system efficiency while maintaining consistent security coverage regardless of which specific instances handle each operation.

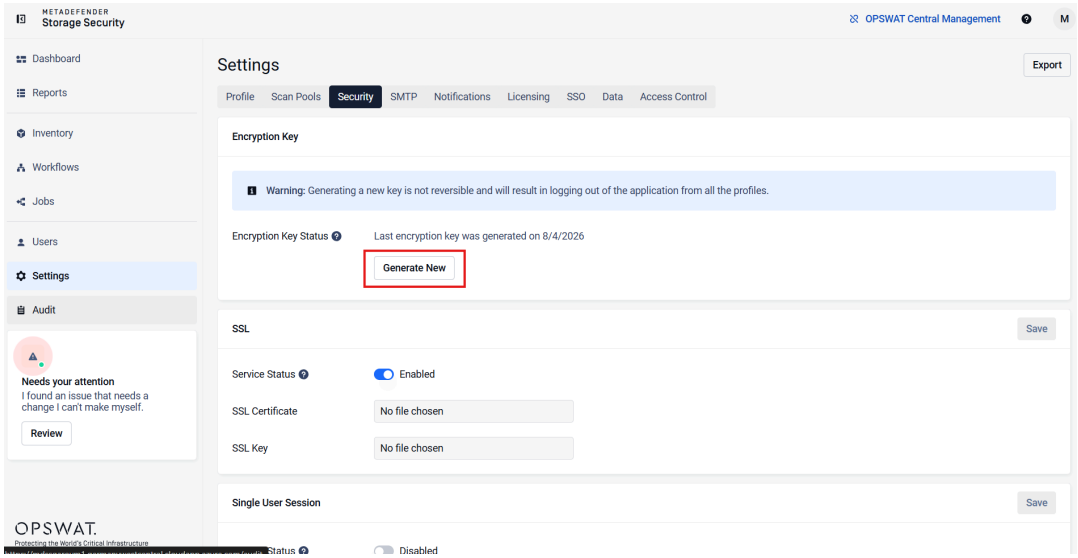
External Services Deployment Options

External services are required for this type of deployment, a deployment and configuration guide is available here: External Services Configuration

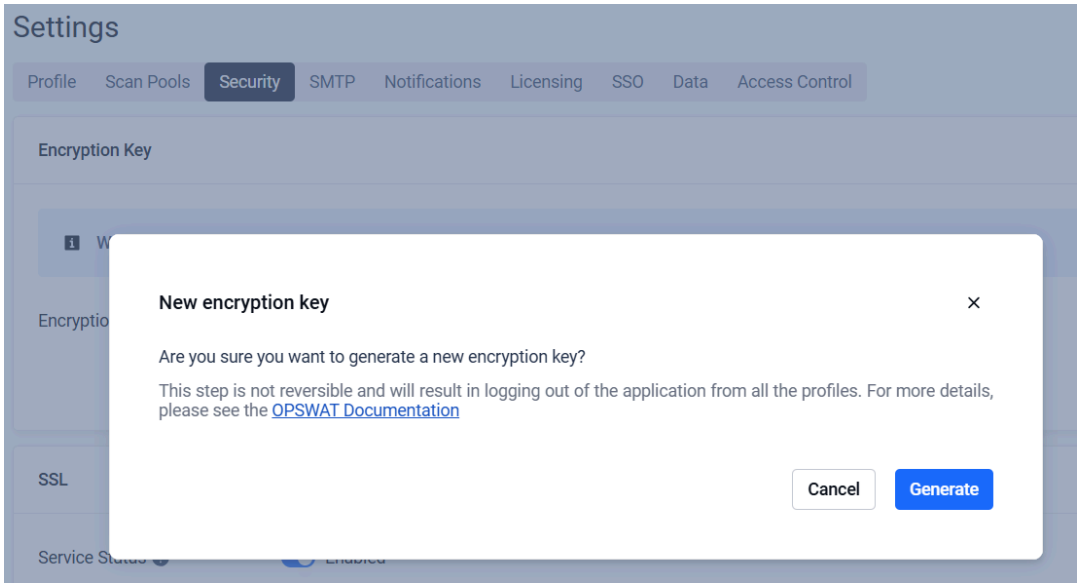
Security & Encryption Keys

To enhance your system's security, you can generate a new master encryption key. This action will re-encrypt all sensitive data—such as storage credentials, API keys, and others—and securely retire the previous key.

You can start this process by navigating to **Settings** and selecting the **Security** tab. Here, click the **Generate New **button from the **Encryption Key** section.



A confirmation dialog will appear to ensure you understand the consequences. Please note that this action is irreversible and will immediately log out all active users from the application. To proceed, click **Generate**.



While the key rotation is in progress, the system prioritizes data integrity. To prevent data corruption, any operations that access or modify encrypted information will be temporarily

unavailable. For example, you will not be able to add or edit storage configurations or user accounts during this time. The process is designed to be as fast as possible, but the total duration will depend on the amount of data stored in your system. We recommend performing this critical security operation during a planned maintenance window or a period of low system activity to minimize disruption for your users.

My OPSWAT Central Management

Central Management is a centralized console that lets you manage multiple MetaDefender products & instances of the same product from a single platform. Customers get improved data flows visibility and provide better reports for each product and entire account. It also provides critical information like product instance health, license, and connection status, report history, license, and audit trails.

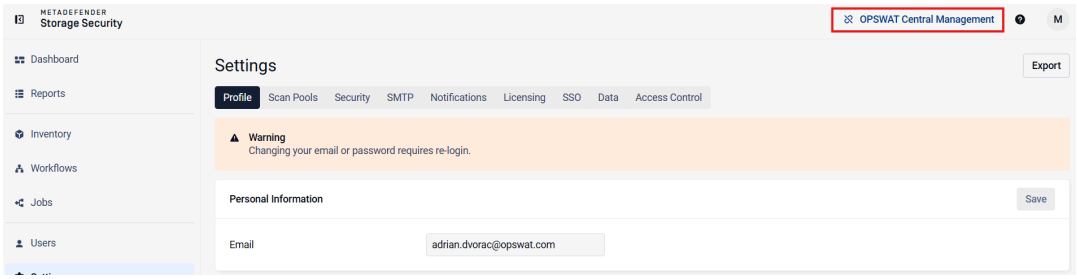
This scope of this topic is to describe how to enroll into MetaDefender Storage Security into My OPSWAT Central Management.

> **Info**
>
> MetaDefender Storage Security currently supports integration with Central Management v8

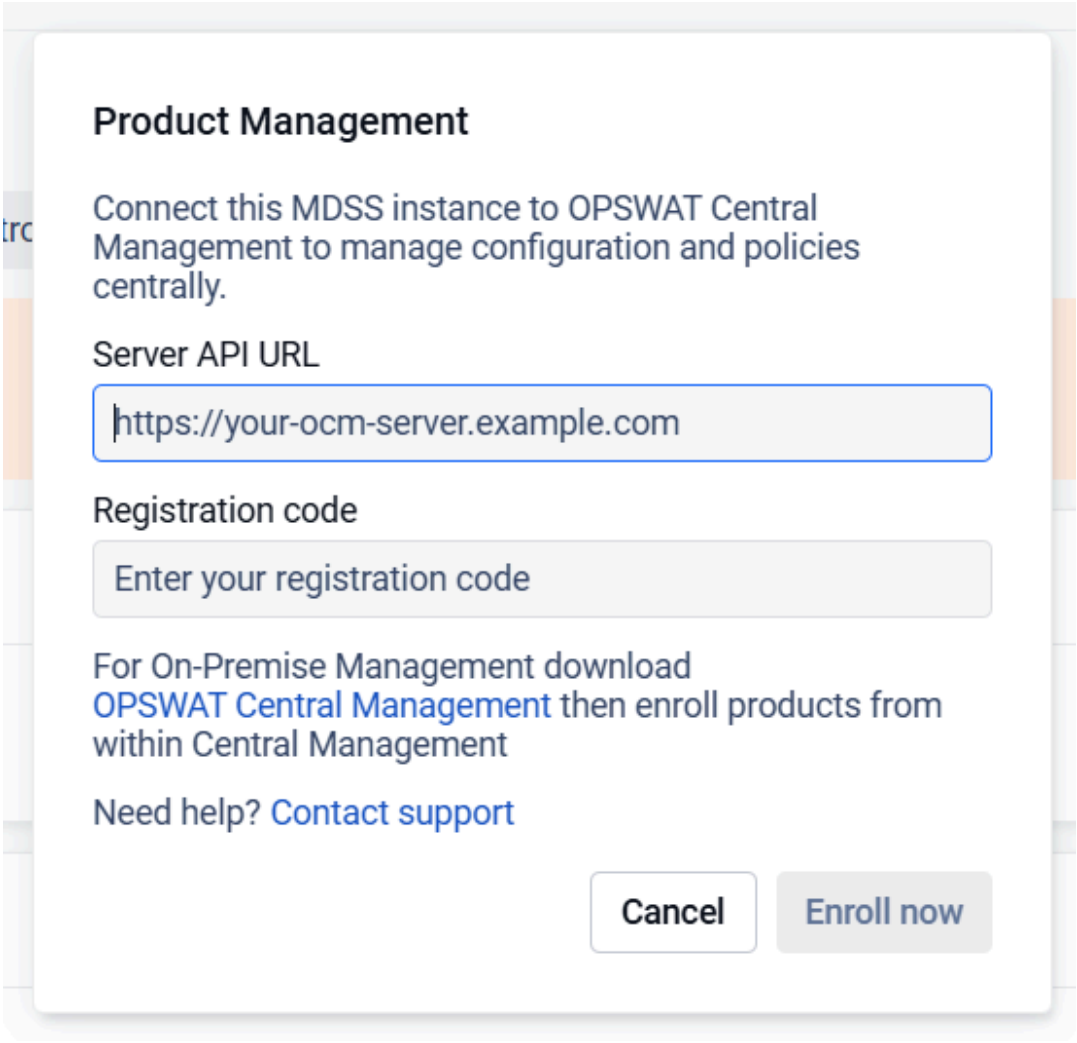
Enrolling the product to Central Management

To enroll MetaDefender Storage Security into My OPSWAT Central Management, these steps should be followed:

1. In the top-right corner, next to the username, there will be a button with the text **OPSWAT Central Management **[if the product is not yet enrolled to Central Management; if the product is already enrolled, the text will say **Managed**]

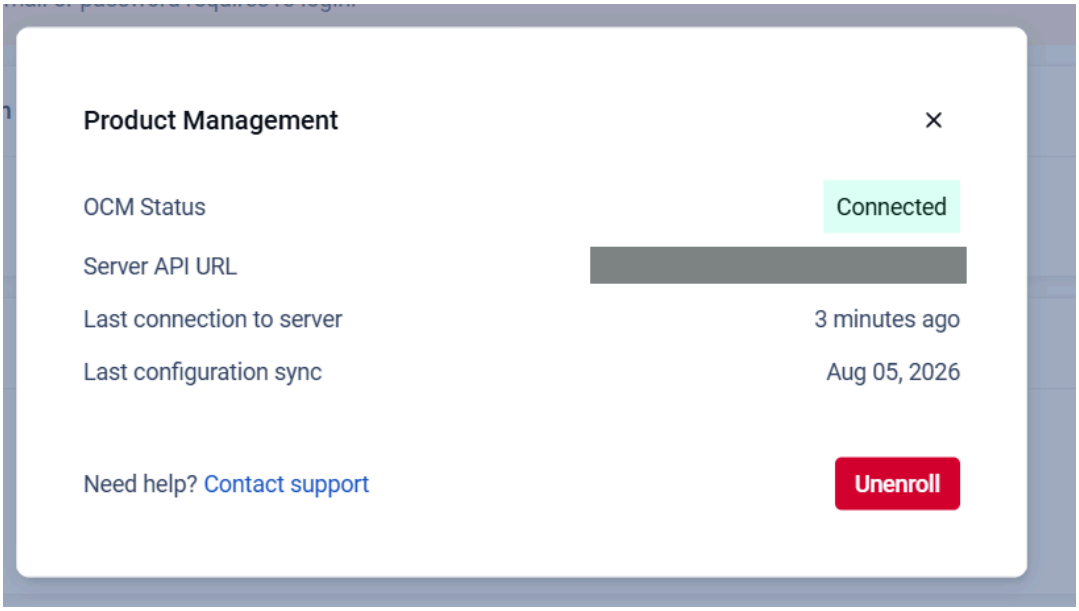


2. Clicking the button will open a form containing the necessary fields to enroll. These are **Server URL**, which is the address of the Central Management server to which you want to enroll the product, and **Registration Code**, which can be found in the Central Management UI by navigating to **Settings -> Global**. The registration code will be present on that page.

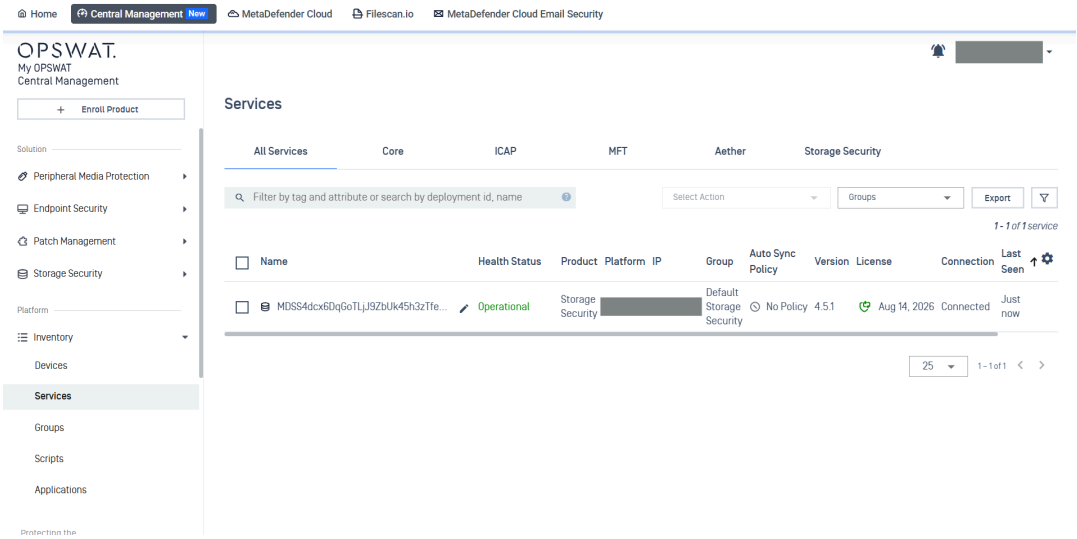


3. After completing the form, click on **Enroll Now.** If the information is correct, MDSS should display a message saying that enrollment was successful.

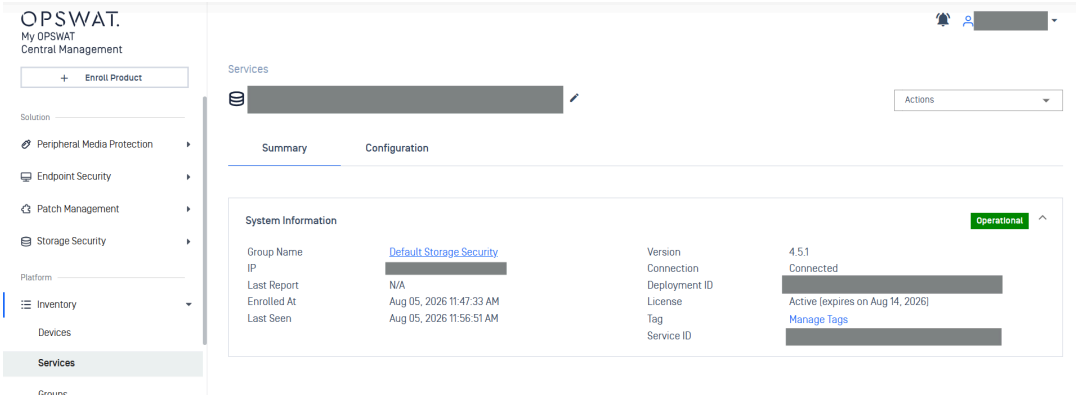
Once you have successfully enrolled your MetaDefender Storage Security instance, the button **OPSWAT Central Management** will reveal **Product Management **information about the connection to the **OCM **platform.

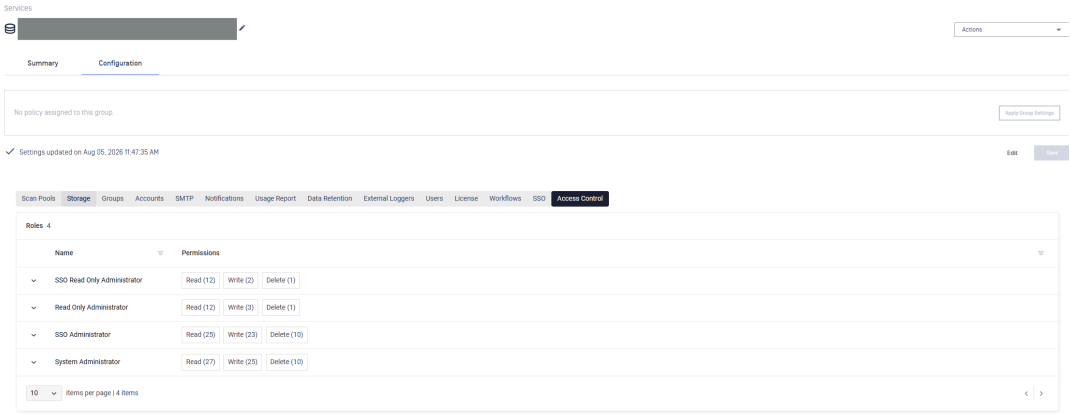


Additionally, navigating to the Central Management server, you should be able to see your enrolled instances under the **Inventory > Services **tab



Furthermore, clicking on the card above will take you to a page where more information about each instance can be seen:

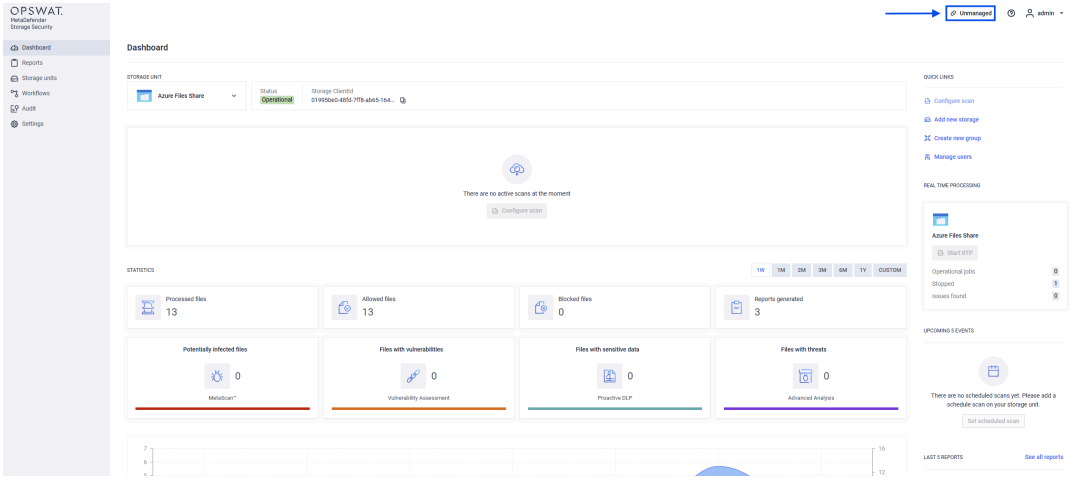




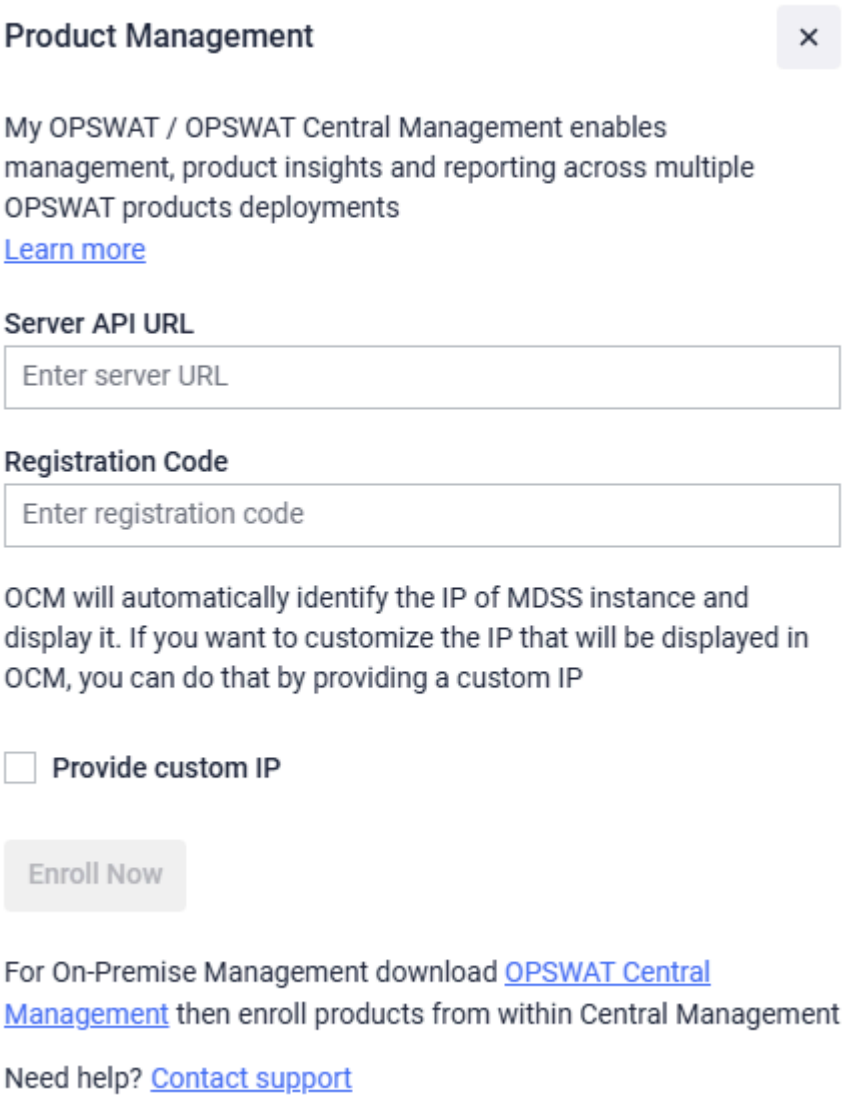
—published

To enroll MetaDefender Storage Security into My OPSWAT Central Management, these steps should be followed:

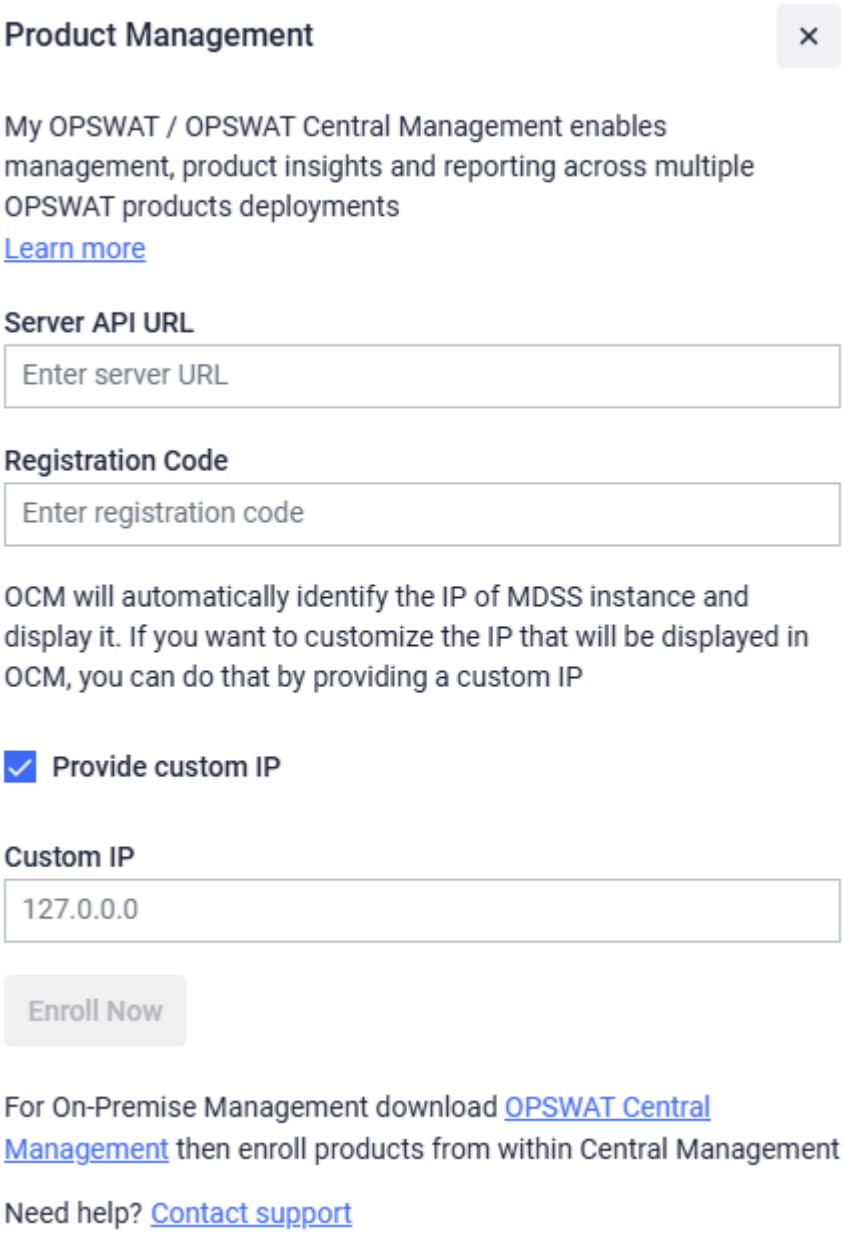
1. In the top-right corner, next to the username, there will be a button with the text **Unmanaged** (if the product is not yet enrolled to Central Mangement; if the product is already enrolled, the text will say **Managed**)



2. Clicking the button will open a form containing the necessary fields to enroll. These are **Server URL**, which is the address of the Central Management server to which you want to enroll the product, and **Registration Code**, which can be found in the Central Management UI by navigating to **Settings -> Global**. The registration code will be present on that page.

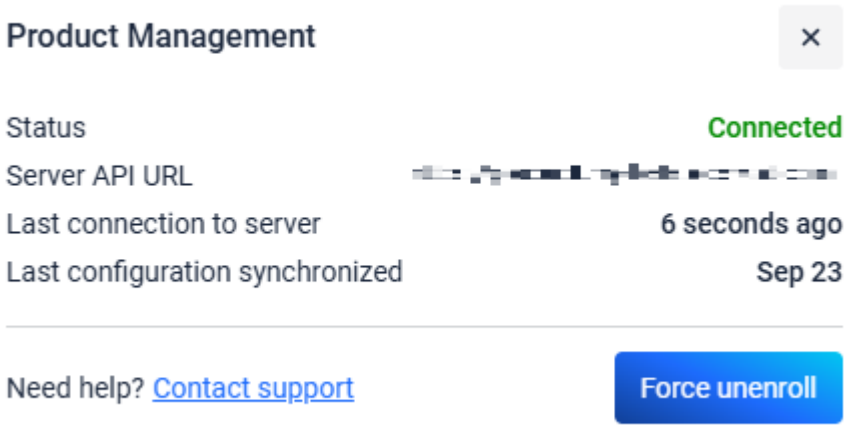


3. Additionalliy, you can provide a **Custom IP**. This constitutes the **IP** of the MDSS instance, not the Central Management one.

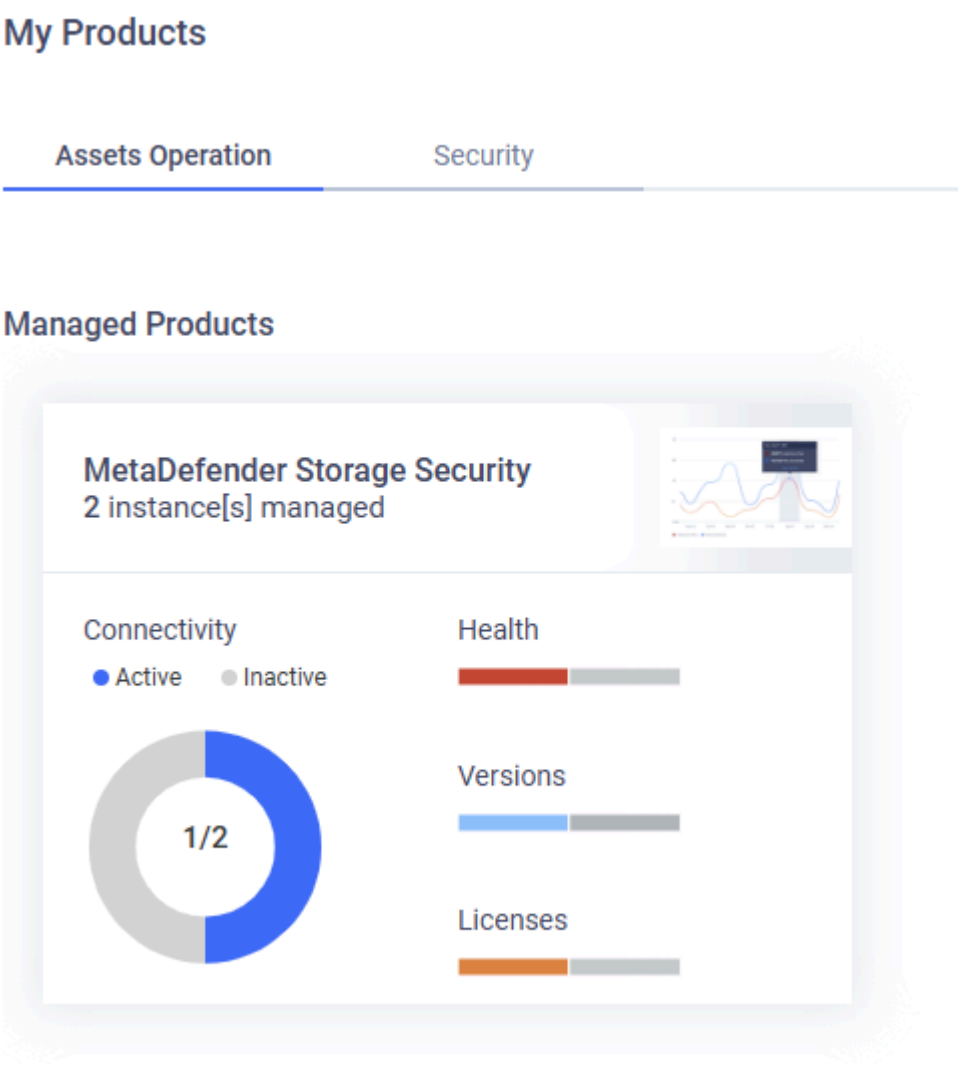


4. After completing the form, click on **Enroll Now.** If the information is correct, MDSS should display a message saying that enrollment was successful.

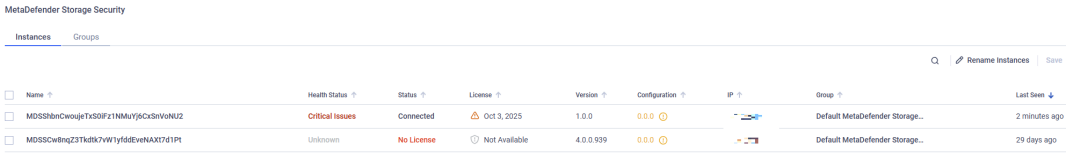
Once you have successfully enrolled your MetaDefender Storage Security instance, the button will now have the text **Managed** and clicking on it will reveal additional information about the connection to the Central Management platform.



Additionally, navigating to the Central Management server, you should be able to see your enrolled instances under the **Products** tab



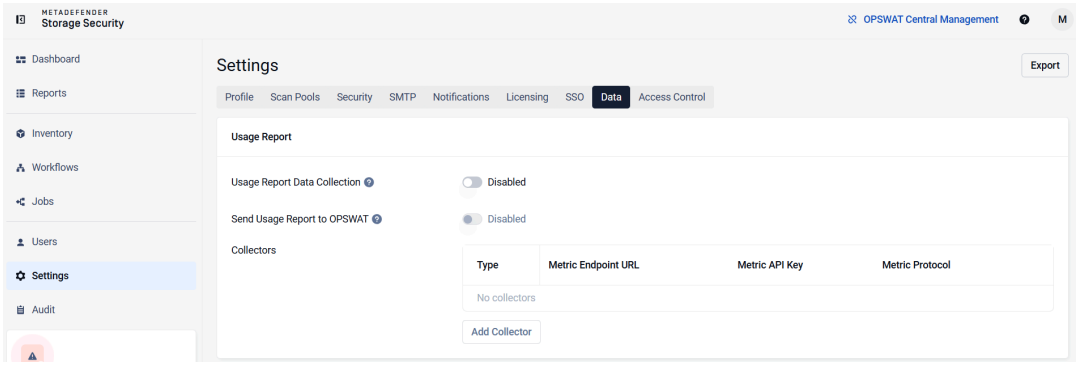
Furthermore, clicking on the card above will take you to a page where more information about each instance can be seen



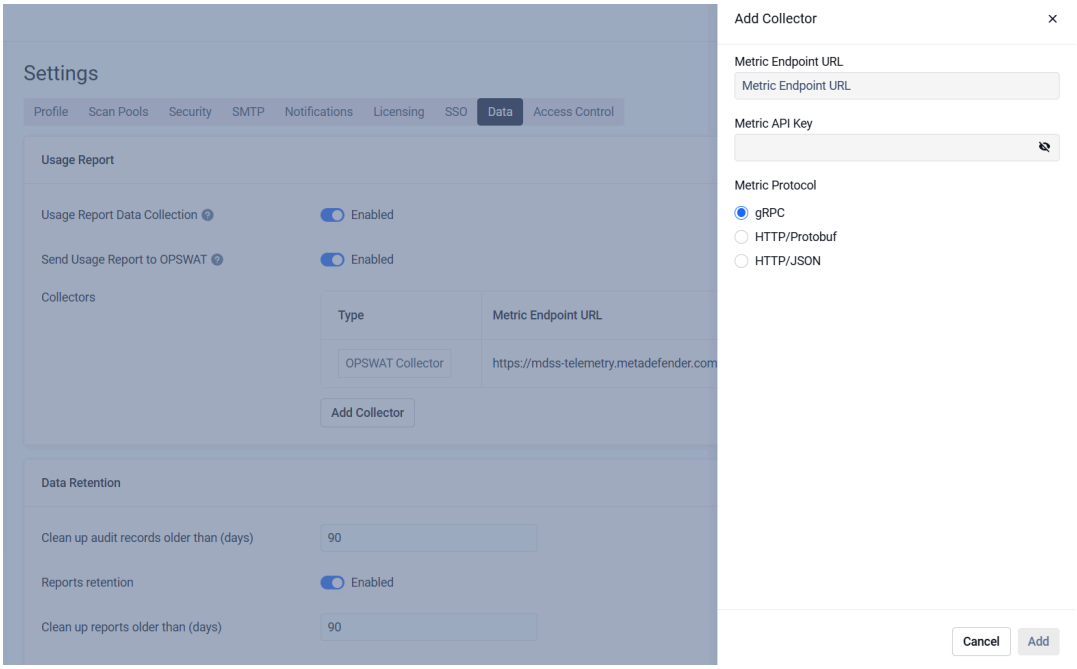
Telemetry

To configure the telemetry output and its collectors in MetaDefender Storage Security, navigate to the **Settings > Data **tab and switch the toggle **Usage Report Data Collection**.

Once enabled, the system will begin collecting operational data. At this time, only metrics are collected. Logs and traces are not yet included.



MetaDefender Storage Security supports adding custom collectors when the telemetry is active by providing the metrics URL and the protocol [HTTP(s) / gRPC]



Automatic Scaling (Autoscaler)

MetaDefender Storage Security (MDSS) continuously monitors its own workload and automatically adjusts how much data it processes at once, so scans keep moving during busy periods and resources are freed up when activity is low. This happens on its own, with no manual setup.

This page explains what automatic scaling does, what you can see on the built-in **System** dashboard, the recommendations it may show you, and how to turn it off if you need to.

Overview

The amount of work flowing through MDSS rises and falls throughout the day as files are discovered, scanned, and remediated. Automatic scaling (the "autoscaler") keeps performance steady across those changes.

Its goal is to complete your files as fast as possible while keeping the system stable, by using the resources available to it as fully and efficiently as it can. Instead of running at a fixed pace, MDSS watches how busy the system is and adjusts how much work it processes in parallel. When there is work to do and capacity to spare, it raises throughput to get the most out of your hardware. When a resource approaches its limit, it settles at the highest rate that resource can sustain. When the backlog is cleared, it releases the resources it no longer needs.

Automatic scaling makes the resources you already have work as efficiently as possible. It does not add or remove servers on its own. When it detects that more capacity is needed, it tells you what to add through on-screen recommendations.

Automatic scaling is enabled by default and works out of the box. No setup is required.

How it works

Automatic scaling checks the system every few seconds and adjusts how much work MDSS takes on, so the available resources are used as fully as they can be without putting the system at risk.

MDSS pays attention to indicators such as:

- how busy the processors (CPU) and memory are,
- how large the backlog of waiting work is,
- how quickly scans are being completed,
- the health and responsiveness of connected MetaDefender Core scan engines, and
- available disk space.

Based on these, its behavior is deliberately smooth and cautious:

- **It raises throughput** when there is a backlog and spare capacity, using more of the available resources to clear work faster.
- **It settles at a sustainable level** when a resource comes under sustained pressure, running it at the highest rate it can sustain instead of overcommitting it and risking instability.
- **It throttles to protect the system** when a resource reaches a critical limit. This can happen when CPU or memory runs out of headroom, when the output pipeline cannot drain as fast as new work arrives, or when the connected MetaDefender Core scan engines cannot take on more scan load. In these situations MDSS reduces how much it takes on so that processing stays reliable and errors are avoided, then returns to full throughput as soon as the pressure clears.
- **It rests when idle**, returning to a light baseline once the backlog is cleared so resources are free for other work.

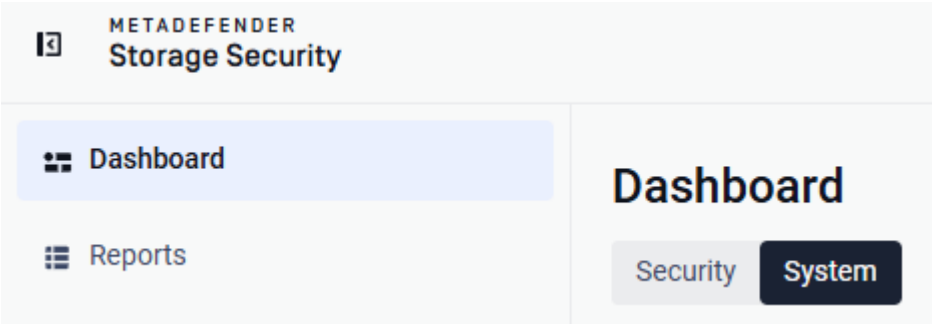
Built-in safety guardrails

Separately from performance tuning, MDSS includes a safety guardrail that protects your data and the system. If free disk space becomes critically low, MDSS automatically **pauses** processing so the system does not run out of room, and **resumes** automatically once space is recovered. When this happens, it shows a message explaining what to do.

The System dashboard

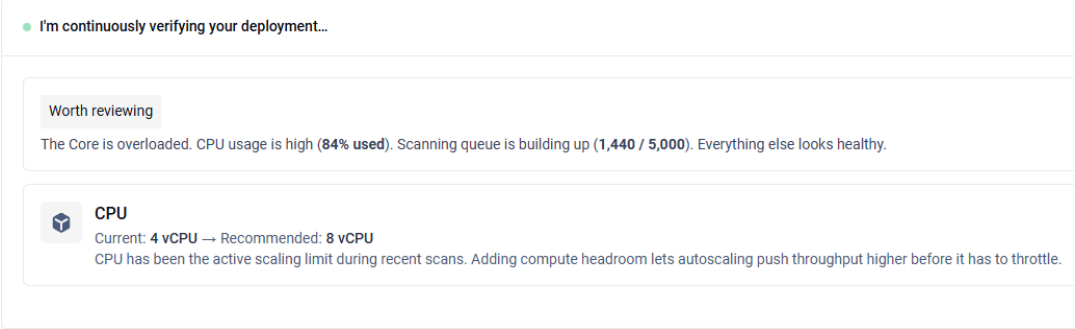
MDSS includes a **System** dashboard that shows, in real time, what automatic scaling is doing and why. It refreshes automatically every few seconds. The dashboard is for monitoring only; the system tunes itself, so there is nothing to configure here.

The dashboard appears as a **System** tab alongside the main **Dashboard** view, for users with the appropriate access.



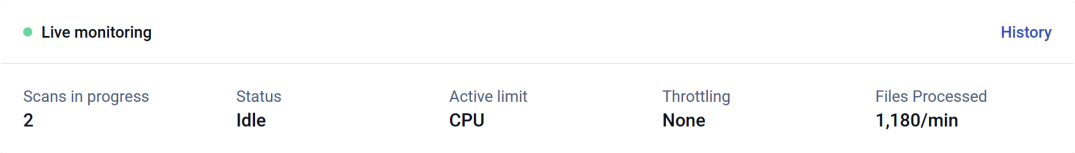
Autoscaling insight

The top card summarizes, in a single sentence, what MDSS is doing right now. Examples include *"I'm scaling up to keep scanning moving while you review this,"* and *"I'm continuously verifying your deployment."* When there is something to address, it explains the cause in plain language and marks how urgent it is **(Action required**, **Recommended**, or **Worth reviewing**]. When everything is healthy, it confirms that no action is needed.



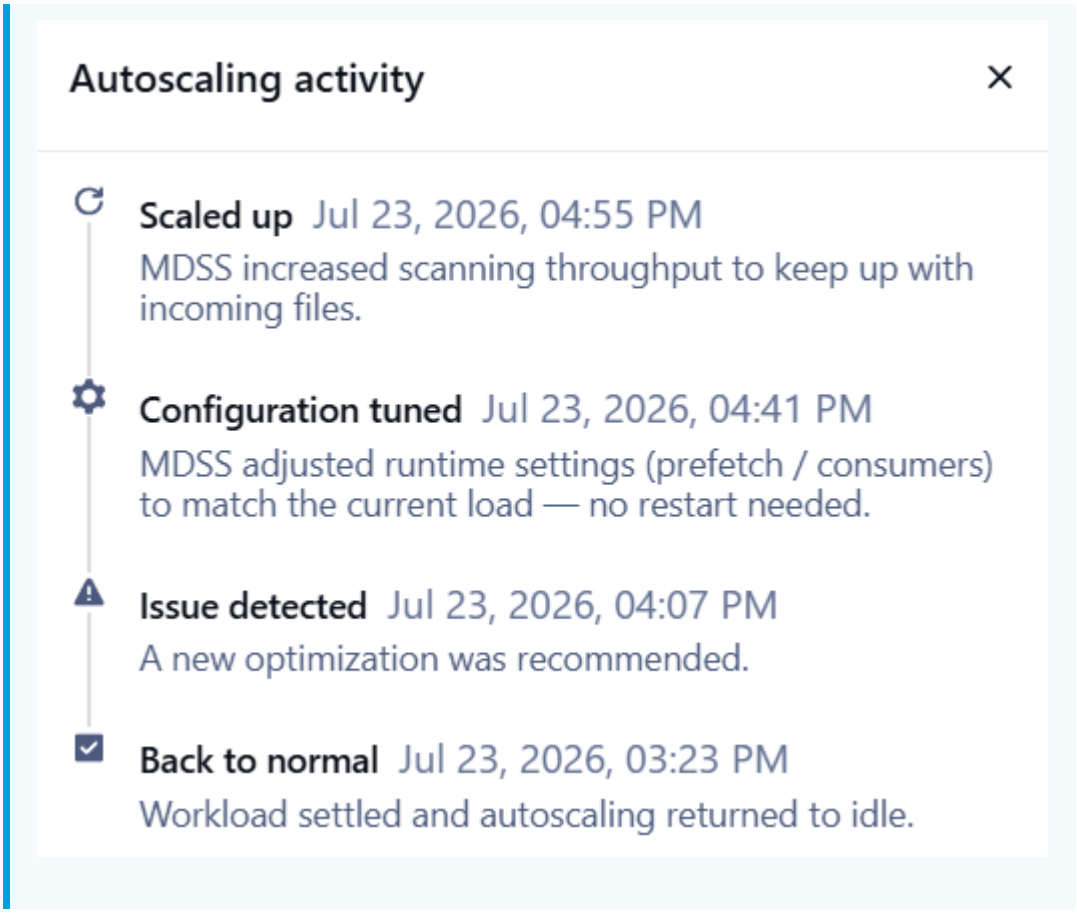
Live status

A strip of key figures gives a quick summary: how many scans are in progress, the current status (such as **Scaling up **or **Idle**], what is currently limiting performance (if anything], and how many files are being processed per minute. A **History** button opens a timeline of recent activity.



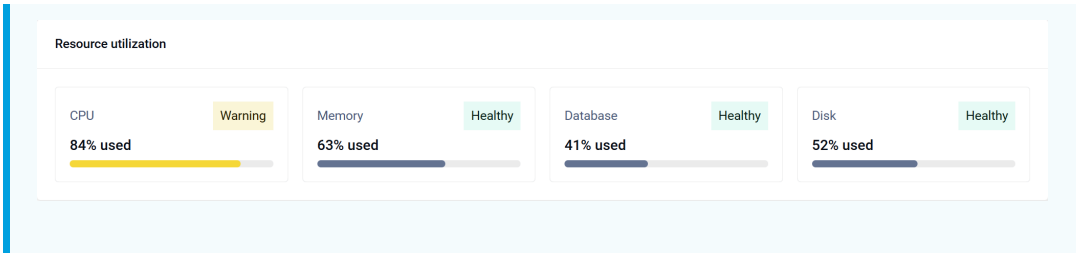
Autoscaling activity

A running timeline of notable events, such as speeding up, slowing down, or pausing. Each event is described in plain language, for example *"MDSS increased scanning throughput to keep up with incoming files."*



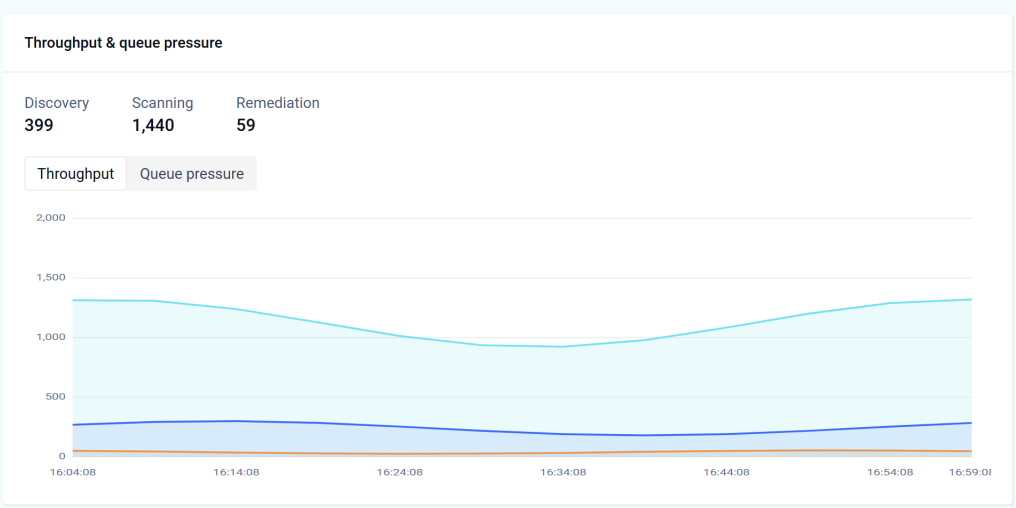
Resource utilization

Cards show current usage of CPU, memory, disk, database, and cache, each with a healthy, warning, or critical indicator.



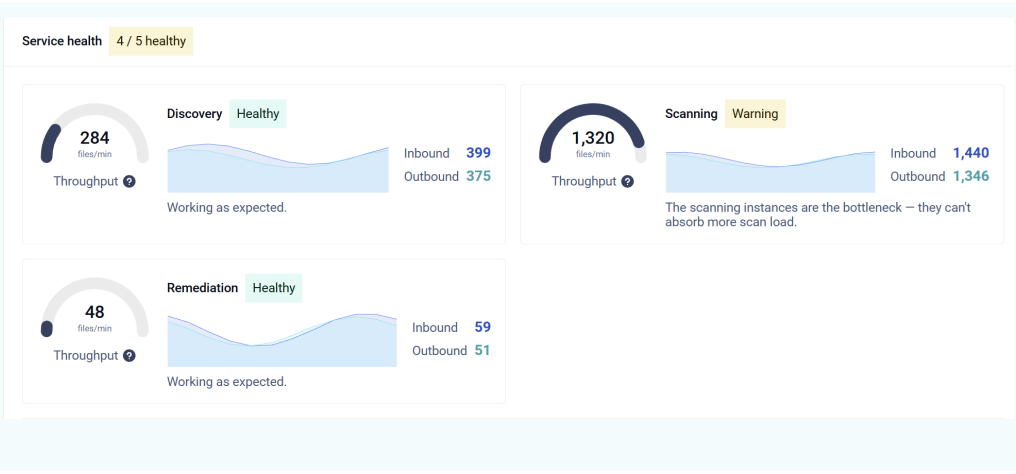
Throughput & queue pressure

Shows how much work is waiting at each stage and lets you switch between two live charts: **Throughput** (files processed per minute over time) and **Queue pressure** (backlog size over time). This makes it easy to see whether MDSS is keeping up with incoming work.



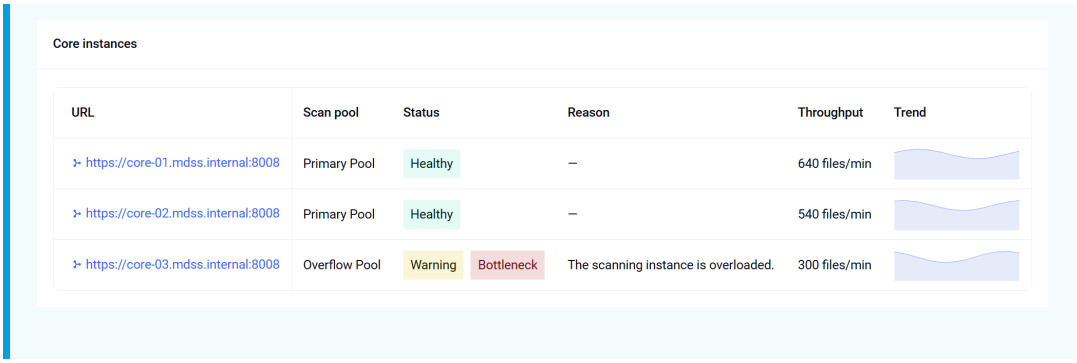
Service health

Shows the health of each MDSS service, with a summary of how many are healthy, each service's current processing rate, and a short explanation of any bottleneck.



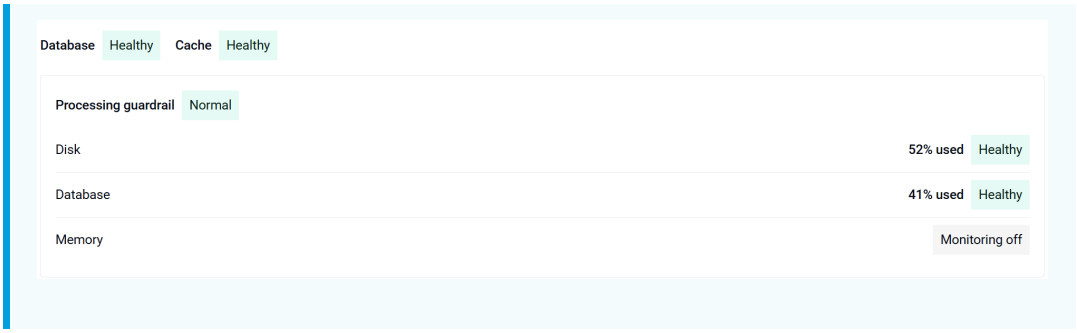
MetaDefender Core instances

A table of the MetaDefender Core scan engines currently used by the active jobs, showing each engine's address, health status, and current processing rate. An engine that is holding back overall performance is flagged as a bottleneck.



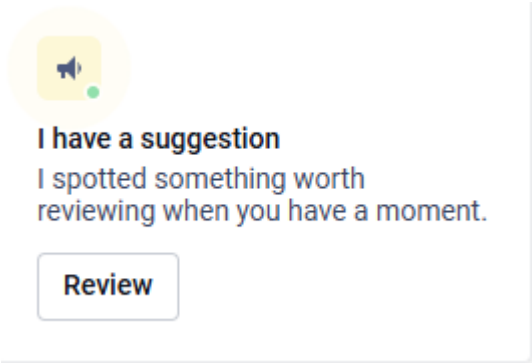
Processing status

When the safety guardrail is active, a card shows whether processing is **Normal** or **Paused**, along with the reason and the current disk space status. If processing is paused, MDSS also shows a banner and a recommended action to resolve it.



Status indicators elsewhere

Beyond the System dashboard, a compact status card appears in the sidebar. If performance becomes degraded, a banner appears across the application with a link to the recommended actions, so you are kept informed even when you are not viewing the dashboard.



Autoscaling states

The **Status** on the dashboard reflects what automatic scaling is doing at that moment:

State	Meaning
Idle	Little or no work to do, MDSS is running at a light baseline to conserve resources.
Scaling up	Demand is high and resources are available, so MDSS is increasing how much it processes at once.
Holding	Conditions are near a limit, so MDSS is holding steady rather than changing course.
Scaling down	A resource is under sustained pressure, so MDSS is easing back to relieve it.
Throttling	A resource has reached a critical limit, so MDSS is temporarily processing less at once to keep things reliable and avoid errors. It returns to full throughput automatically once the pressure clears. See the **How it works** section for the situations that trigger this.
Paused	The safety guardrail has paused processing to avoid running out of disk space. Processing resumes automatically once space is recovered.

Recommendations you may see

When MDSS determines that your hardware or a supporting component has become the limiting factor, it shows a single, prioritized recommendation. Recommendations are advisory. MDSS keeps running as efficiently as it can, and acting on a recommendation will improve performance or resolve a constraint.

Recommendation	Why you are seeing it	What to do
Increase specs	The MDSS host is below the minimum recommended hardware.	Bring the host up to the minimum recommended CPU and memory.
Increase CPU	Performance is being held back by available CPU.	Add CPU to the host, or add an additional MDSS instance to share the load.
Increase memory	Performance is being held back by available memory.	Add memory to the host, or add an additional MDSS instance.
Use an external database	The database is limiting throughput or growing large on the local host.	Move the database to a dedicated external host.
Use an external cache	The local cache is limiting throughput.	Move the cache to a dedicated external host.
Use an external MetaDefender Core	The local MetaDefender Core is limiting scan throughput.	Switch to an external MetaDefender Core so scanning can scale independently.
Increase MetaDefender Core performance	Your external MetaDefender Core is at capacity.	Increase its resources or add more Core nodes.
Increase storage	Processing was paused because disk space or database capacity is critically low.	Free up or add disk space to resume processing.

> MDSS shows the single most important recommendation at any time rather than a long list, so you can focus on the change that will have the greatest impact.

Turning automatic scaling off

Automatic scaling is enabled by default, and we recommend leaving it on. If you need to turn it off, you can do so with an environment variable:

```
SCANNING_AUTOSCALER_ENABLED=false
```

With this set, MDSS stops adjusting how much it processes and runs at a steady baseline instead. It continues to monitor performance and show the dashboard. Restart MDSS for the change to take effect.

> **Note:** The safety guardrail that pauses processing when disk space is critically low stays active regardless of this setting, so the system stays protected even when automatic scaling is turned off.

Frequently asked questions

Does automatic scaling add or remove servers? No. It makes your existing deployment work as efficiently as possible. When more capacity is needed, it recommends what to add rather than provisioning it for you.

Does automatic scaling slow down my scans? No. It works to complete your scans as fast as possible by using the available system resources as fully and efficiently as it safely can. If a resource reaches a critical limit, MDSS temporarily processes less at once (throttling). This keeps scanning reliable and prevents the system from being overloaded, which would otherwise cause errors or instability. As soon as the pressure clears, MDSS returns to full throughput.

Do I need to configure anything to use it? No. It is enabled by default and self-tuning.

Why does processing sometimes pause? The safety guardrail pauses processing when disk space becomes critically low, and resumes automatically once space is recovered. Follow the on-screen **Increase storage** recommendation to resolve it.

Why am I seeing a recommendation to add hardware or move a component externally? Because MDSS has determined that resource is currently limiting performance.

Automatic scaling settings

MetaDefender Storage Security (MDSS) adjusts how much it processes automatically, based on how busy the system is. This page lists the settings that control that behavior, with their default values and a short explanation of each one. For an overview of how automatic scaling works, see the Automatic Scaling page.

Altering these settings is optional. They are provided for cases where you want to adapt the behavior to a specific environment. Each setting is applied as an environment variable. MDSS reads them when the service starts, so restart MDSS after making a change. The settings that control scaling apply to the scanning part of MDSS, which is why their names begin with `SCANNING_AUTOSCALER_`.

1. General behavior

Setting	Default	Unit	What it does
SCANNING_AUTOSCALER_ENABLED	true	on/off	Turns automatic scaling on or off. When off, MDSS still monitors performance and shows the dashboard, but it no longer adjusts how much it processes by itself.
SCANNING_AUTOSCALER_PROBE_INTERVAL	10	seconds	How often MDSS checks the system and decides whether to adjust.
SCANNING_AUTOSCALER_INITIAL_PREFETCH	20	items	How many items each scanning worker starts with, and the level it returns to when there is no work.
SCANNING_AUTOSCALER_MIN_PREFETCH	5	items	The fewest items a worker will handle at once when scaling down.
SCANNING_AUTOSCALER_MAX_PREFETCH	200	items	The most items a worker will handle at once when scaling up. MDSS will not go above 200 by default, and never above an internal maximum of 400 even if you set a higher number.
SCANNING_AUTOSCALER_IDLE_RESET_TICKS	30	checks	How many quiet checks in a row before MDSS returns to its starting level. At the default check interval this is

			about five minutes.
SCANNING_AUTOSCALER_THROTTLE_DURATION	30	seconds	After MDSS reaches a critical limit and pulls back, how long it waits before testing whether it can speed up again.
SCANNING_AUTOSCALER_PROBES_COUNT_SCALEUP	5	checks	How many healthy checks in a row are needed before MDSS speeds up. A higher number makes it ramp up more cautiously.
SCANNING_AUTOSCALER_PROBES_COUNT_SCALEDOWN	2	checks	How many warning checks in a row before MDSS eases back. A lower number makes it back off sooner.
SCANNING_AUTOSCALER_LOCAL_HARDWARE_HYSTERESIS	5.0	percentage points	A small buffer around the CPU and memory limits that keeps MDSS from

			switching back and forth when usage sits right at a limit.
SCANNING_AUTOSCALER_OUTBOUND_HYSTERESIS	5.0	percentage points	The same kind of buffer for the queue of scanned results waiting for the next step.
SCANNING_AUTOSCALER_DOWNSTREAM_HYSTERESIS	10.0	percentage points	The same kind of buffer for how loaded the scan instances are.

2. Resource limits

These set the points at which a resource is considered under pressure. When a resource passes its warning level, MDSS starts to ease back gradually. When it passes its critical level, MDSS reduces its load right away.

Setting	Default	Unit	What it does
SCANNING_AUTOSCALER_CPU_WARNING_THRESHOLD	90	percent	CPU usage that MDSS treats as a warning.
SCANNING_AUTOSCALER_CPU_CRITICAL_THRESHOLD	95	percent	CPU usage that makes MDSS reduce its load immediately.
SCANNING_AUTOSCALER_MEMORY_WARNING_THRESHOLD	80	percent	Memory usage that MDSS treats as a warning.
SCANNING_AUTOSCALER_MEMORY_CRITICAL_THRESHOLD	90	percent	Memory usage that makes MDSS reduce its load immediately.
SCANNING_AUTOSCALER_OUTBOUND_WARNING_THRESHOLD	70	percent of the limit below	How full the results queue can get, as a percentage of the limit below, before MDSS treats it as a warning.
SCANNING_AUTOSCALER_OUTBOUND_CRITICAL_THRESHOLD	9000	items waiting	The number of scanned results waiting in the queue that makes MDSS reduce its load immediately. This is also the

			maximum size of that queue.

The queue of incoming work has no limit to set. Any waiting work simply tells MDSS there is something to process.

3. Scan instance settings

These control how MDSS reads the load and health of the connected MetaDefender Core scan instances and how much work it sends to each one.

Setting	Default	Unit	What it does
SCANNING_AUTOSCALER_DOWNSTREAM_DESIRED_LOAD	40	percent	The load MDSS aim to keep each scan instance at, as a percentag of what that instance can hold.
SCANNING_AUTOSCALER_DOWNSTREAM_WINDOW_SIZE	100	recent results	How many recent results MDSS look at when judging how loade a scan instance i
SCANNING_AUTOSCALER_DOWNSTREAM_CRITICAL_ERROR_RATE_THRESHOLD	0.10	share [0 to 1]	The share of recent requests that fail before MDSS treats a scan insatnce as unhealthy and pulls work away from it. Th default of 0.10 means 10 percent.
SCANNING_AUTOSCALER_DOWNSTREAM_CRITICAL_ERROR_RATE_WINDOW_SIZE	100	recent results	How many recent results are used for the failure

			rate check above.
SCANNING_AUTOSCALER_DOWNSTREAM_WARNING_429_RATE_THRESHOLD	0.10	share (0 to 1)	The share of recent requests a scan instance turns away for being too busy before MDSS treats it as a warning. The default of 0.10 means 10 percent.
SCANNING_AUTOSCALER_DOWNSTREAM_WARNING_429_RATE_WINDOW_SIZE	100	recent results	How many recent results are used for the too-busy check above.

4. Disk space protection

MDSS includes a safety guardrail that pauses processing when disk space runs low and resumes it once space is recovered. This protects your data and keeps working even when automatic scaling is turned off.

Setting	Default	Unit	What it does
GUARDRAILS_CHECK_INTERVAL_SECONDS	30	seconds	How often MDSS checks available disk space. The lowest allowed value is 10.
GUARDRAILS_USED_CRITICAL_PERCENT	90	percent	How full the disk can get before MDSS pauses processing to avoid running out of space.
GUARDRAILS_USED_RESUME_PERCENT	80	percent	How far disk usage must drop before MDSS resumes processing. The gap below the pause level prevents rapid pausing and resuming.
GUARDRAILS_DISK_MONITOR_PATH	/var/log/mdss (Linux), install drive (Windows)	path	The disk location MDSS watches for free space.
SCAN_INSTANCE_DISK_CRITICAL_THRESHOLD_PERCENT	5	percent free	How little free disk space a

			scan instance can have before MDSS stops sending it work.
SCAN_INSTANCE_HEALTH_JOB_INTERVAL_SECONDS	30	seconds	How often MDSS checks the health of each scan instance.
PERFORMANCE_MODE	false	on/off	When set to true, turns off the disk space protection described here. Leave it off in normal use.

Knowledge Base

The MDSS API Gateway - What It Is and Which Port It Uses

Applies to: MetaDefender Storage Security (MDSS) · All supported deployments (Docker on Linux, native services on Windows, Kubernetes)

MetaDefender Storage Security is built from a set of independent services — one that discovers files in storage, one that scans them, one that handles users and permissions, one that manages licensing, and so on. Customers never talk to those services individually. Every request from a browser, a script, or another product arrives at a single service called the **API Gateway**, which checks who is asking, whether they are allowed, and then routes the request to whichever service does the work.

This page explains what that means in practice, which ports a customer needs to open, and how to answer the questions that come up most often in a deployment conversation.

---

1. The short version

Question	Answer
What is the API Gateway?	The single front door into MDSS — for the web console and for all API traffic.
Which port does it use?	`8005` (HTTP) and `8006` (HTTPS) internally.
Which port does the customer connect to?	`80` (HTTP) or `443` (HTTPS) — the address of the MDSS console.
What does the customer open on the firewall?	Just `443` in a standard deployment.
Is the API included in the product?	Yes. Every action in the UI is available through the API, at no extra cost or module.

> **The one thing to remember**
>
> `8005` is the API Gateway's internal port. Customers do not connect to it. They connect to the MDSS console address on **443**, and everything — the UI and the API — is served from there.

---

2. What the API Gateway does

Think of the API Gateway as the reception desk of the MDSS deployment. Everyone entering the building goes through it, gets identified, and gets directed to the right department. Nobody walks into a department directly.

It has four jobs:

It is the only way in. All other MDSS services run on a private internal network with no exposure to the customer's network. This is the security argument that resonates most: MDSS may be a dozen services, but it presents **one** door to the outside world.

It authenticates every single request. Whether the caller is an administrator in a browser, an automated script using an API key, or a user arriving through the customer's SSO provider, the gateway verifies the identity before anything else happens. Nothing reaches a backend service unauthenticated.

It enforces what each user is allowed to do. MDSS distinguishes full administrators, tenant administrators, and read-only administrators. The gateway enforces those boundaries centrally, so the rules are applied consistently and cannot be bypassed by calling a service directly. In multi-tenant deployments, it also resolves which tenant a request belongs to and keeps tenants isolated from one another.

It powers everything customers see and automate. The web console is driven entirely by the gateway's API, including live scan progress that updates in the browser as files are processed. The same API is what customers use to integrate MDSS into their own tooling.

---

3. Ports

What the customer actually connects to

In every supported deployment, a web front end sits in front of the API Gateway and serves both the console and the API on the same address:

Port	Purpose	Notes
443	HTTPS — MDSS console and API	The standard, recommended option. Requires a certificate to be configured during setup.
80	HTTP — MDSS console and API	Enabled by default. Suitable for lab and evaluation environments only.

A customer browsing to `https://mdss.customer.com` gets the console. A script calling `https://mdss.customer.com/api/...` reaches the API. Same host, same port, same certificate.

The gateway's own ports

Port	Purpose
8005	API Gateway, HTTP
8006	API Gateway, HTTPS

These sit *behind* the web front end. In a Docker deployment they are not published to the host at all — the gateway is reachable only from inside the MDSS internal network. On a Windows native-services installation they are local ports on the MDSS server itself.

Both are configurable at install time if they conflict with something already running on the customer's server. The default of `8005` is what appears in configuration files, support packages, and log output, which is the main reason to know the number.

What to tell a customer about their firewall

For a standard deployment, one inbound rule:

- **Inbound TCP 80 and 443** to the MDSS server, from wherever administrators and API clients connect.

That is the complete list for reaching MDSS. Ports `8005` and `8006` do **not** need to be opened, and neither do the ports used by the internal services. MDSS still needs *outbound* access to the storage it scans, to the MetaDefender Core scanning engine, and to OPSWAT for licensing — but those are separate conversations, covered in the deployment documentation.

---

4. FAQ

"Do we need to open port 8005?" No. Customers connect on 443. `8005` is internal to the MDSS server.

"Can we change the port MDSS runs on?" Yes. Both the front-end port and the gateway port are set at installation and can be changed afterwards. Customers who already run something on 443 commonly move MDSS to another port.

"Is the API a separate license?" No. It is included, and it is the same API the MDSS console uses.

"Can we put MDSS behind our own load balancer or reverse proxy?" Yes — this is a normal deployment pattern. Terminate TLS at the customer's proxy and forward to MDSS. Bring in Sales Engineering to confirm the specifics for the customer's environment.

“Does the API support our SSO?” The gateway handles SSO sign-in for console users. Automated and scripted access uses API keys rather than SSO. Confirm the customer’s specific identity provider with Sales Engineering.

“How is the API secured?” Every request is authenticated before it reaches any backend service, using either a token, an API key, or an SSO session. Permissions are then checked against the caller’s role. Over HTTPS, all of it is encrypted in transit.

External Loggers — Streaming the MDSS Audit Trail to a SIEM

MetaDefender Storage Security can forward its complete audit trail to a SIEM or log platform in real time — every file scanned with its verdict, every action taken on a blocked file, and every configuration, user and permission change. The feature is called **external loggers**, it is included in the product, and it supports four destination types: Syslog over UDP, Syslog over TCP, Syslog over TCP with TLS, and Apache Kafka.

This page documents the transports, the message formats, every field on the wire, the complete event-type reference, and what the stream does not include.

---

1. The short version

Question	Answer
Can MDSS integrate with a SIEM?	Yes, over Syslog (UDP, TCP, or TCP with TLS) or Apache Kafka.
Is it a separate module or licence?	No. It is included in the product.
What is sent?	The complete MDSS audit trail — the same events shown in the console's audit log.
How current is it?	Events are sent individually as they happen, typically within a second.
Can I send only some events?	Not from MDSS. Every enabled destination receives the whole stream; filter at your collector.
How many destinations can I configure?	Five of each type, per tenant.
Which permission is needed to configure it?	Write permission on settings.
What format are the messages in?	RFC 5424 for Syslog; JSON for Kafka. CEF and LEEF are not produced.

The two things to plan for

Volume. MDSS does not filter server-side, and file-level events dominate the stream. Size the feed and agree a collector-side filter before you enable it — see section 11.

Scope. External loggers carry the audit trail only. Service and diagnostic logs, API request activity, and failed sign-in attempts are not included — see section 12.

2. What the stream contains

Every destination receives the same content: the complete MDSS audit trail. That is the same set of events shown under **Audit log** in the console. Nothing is added for external destinations, and nothing is held back.

Scan activity. Every file discovered and every file scanned, with the verdict, the reason it was blocked, both hashes, size, path, the storage it came from, the scan that processed it, and the workflow applied. Also scan-level lifecycle events: started, completed, cancelled, failed.

Post actions. What MDSS did about each file — moved, copied, deleted, kept, tagged or sanitised — including the destination storage and path for moves and copies.

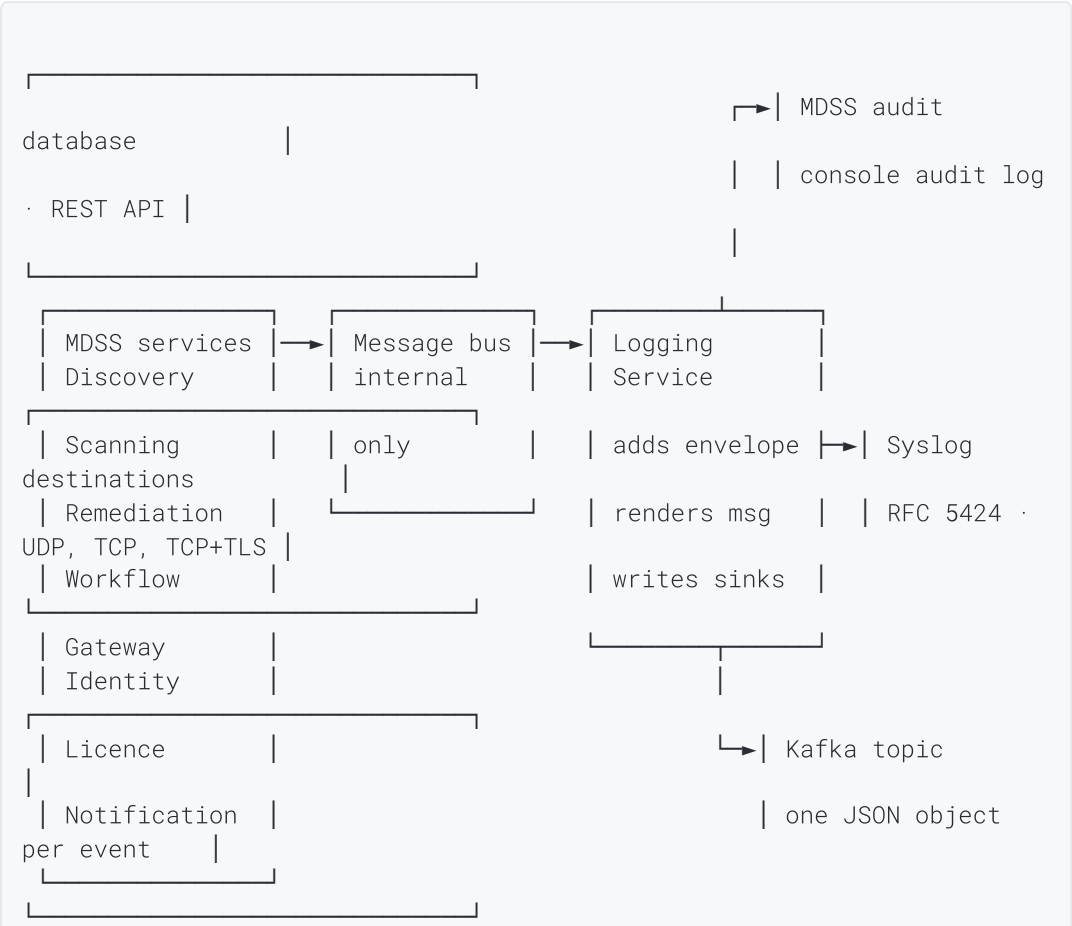
Administrative activity. Storage, group and account changes. Workflow, scan, schedule and remediation changes. User and role changes. Settings changes, including API keys, SSO, TLS certificates, data retention, licence activation, and the external loggers themselves.

Authentication. Successful sign-ins and sign-outs.

Failed operations are carried as the same event type at `Error` level rather than as separate event types — a scan that could not complete, a post action that failed, a settings change that was rejected.

3. How the stream works

MDSS is built from independent services. Each publishes its audit events onto an internal message bus, and a single Logging Service consumes them. For every event, the Logging Service writes to the MDSS audit database and to each enabled external destination in the same operation.



Because the fan-out happens after the audit event is created, the SIEM and the console audit log always describe the same events with the same field values.

Delivery semantics

Aspect	Behaviour
Ordering	Events are emitted in the order the Logging Service processes them, and each carries an event timestamp and a sortable event id.
Latency	Sub-second under normal load. Events are batched — see section 13.
Independence	A failure writing to one destination does not affect the others, and never affects the audit database. A slow or unreachable collector never delays a scan.
Retry	Best-effort. Events produced while a destination is unreachable are **not** queued for later delivery. They remain in the MDSS audit database.
Configuration changes	Applied to the next event. No service restart, no interruption to running scans.

4. Supported destinations

Destination	`loggerType`	Default port	Payload	Transport security
Syslog over UDP	`0`	514	RFC 5424	None
Apache Kafka	1	9092 (typical)	JSON	PLAINTEXT · SSL · SASL_PLAINTEXT · SASL_SSL
Syslog over TCP	2	1468	RFC 5424	None
Syslog over TCP with TLS	3	6514	RFC 5424	TLS, server certificate validated

Up to **five destinations of each type** may be configured per tenant — five Syslog UDP destinations, five Kafka destinations, and so on. Each is enabled or disabled independently.

Syslog options

Option	Detail
Output format	RFC5424.The only format offered. CEF and LEEF are not produced.
Facility	Any of the 24 standard Syslog facilities, values 0–23, in the usual order from `KernelMessages` to `LocalUse7`. Defaults to `UserLevelMessages` (1).
Application name	The MDSS product name, sent in the RFC 5424 APP-NAME field.
Framing	TCP destinations frame each message with CRLF.

Kafka options

Option	Detail
Brokers	Comma-separated `host:port` list.
Topic	A single topic name. All events go to it, on any partition.
Message key	The event timestamp. Events are not keyed per file or per storage.
Security protocol	`PLAINTEXT`, `SSL`, `SASL_PLAINTEXT` or `SASL_SSL`.
SASL mechanism	`PLAIN`, `SCRAM-SHA-256` or `SCRAM-SHA-512`, with username and password.

Choosing a transport. Use Kafka if you already operate a broker — events arrive as JSON with named fields, so no log parser is required. Otherwise use Syslog over TCP with TLS. Plain UDP is the least reliable option; see the delivery semantics above.

---

5. Configure in the console

Go to **Settings → External loggers**. You need an account with write permission on settings.

1. Select **Add integration** and choose the integration type.
2. For a Syslog destination, enter the server address and port, then choose a facility. The output format is RFC 5424.
3. For Kafka, enter the broker list and topic, then choose the security protocol and — for a SASL protocol — the mechanism, username and password.
4. Save. MDSS tests the connection before storing the configuration. If the test fails, nothing is saved.
5. Use the enable toggle in the list to start or stop delivery at any time without deleting the configuration.

> **Two rules before you save**
>
> A configuration identical to an existing one is rejected as a duplicate. And a connection test must succeed, so the destination has to be reachable from the MDSS deployment at the moment you save — open the firewall first.

---

6. Configure over the API

Everything in the console is available on the REST API. The base address is your MDSS console address, for example `https://mdss.example.com/api/`. Authenticate with a bearer token from `/api/user/authenticate` in the `Authorization` header, or with an API key in an `ApiKey` header. All external logger endpoints require write permission on settings.

Method	Path	Purpose
GET	/api/externallogger	List all configured destinations
POST	/api/externallogger/udpSyslog	Add a Syslog destination (any of the three variants)
PUT	/api/externallogger/udpSyslog	Update a Syslog destination
POST	/api/externallogger/kafka	Add a Kafka destination
PUT	/api/externallogger/kafka	Update a Kafka destination
PUT	/api/externallogger/status	Enable or disable a destination
DELETE	/api/externallogger/{id}	Remove a destination

List destinations

`GET /api/externallogger` returns every destination for the calling tenant.

```
{
  "entries": [
    {
      "id": "c9f1e0a4-...",
      "isEnabled": true,
      "loggerType": 3,
      "connectionSettings": {
        "serverAddress": "siem.example.com",
        "port": 6514,
        "facility": 13,
        "format": 0
      }
    }
  ],
  "result": 0
}
```

Add a Syslog destination

Despite the path, `POST /api/externallogger/udpSyslog` creates **all three** Syslog variants — the `loggerType` field selects which.

```
{
  "isEnabled": true,
  "serverAddress": "siem.example.com",
  "port": 6514,
  "loggerType": 3,
  "facility": 13,
  "format": 0
}
```

Field	Notes
`serverAddress`	Hostname or IP address.
`port`	Destination port.
`loggerType`	`0` UDP, 2 TCP, 3 TCP with TLS.
`facility`	`0`–23. Defaults to 1.
`format`	`0` for RFC 5424.

`PUT /api/externallogger/udpSyslog` takes the same body plus the `id` of the destination to update. All fields are replaced.

Add a Kafka destination

`configuration` is a JSON **string** — serialise the security settings and pass them as an escaped string value, not as a nested object.

```
{
  "isEnabled": true,
  "serverAddressWithPortList": "broker1:9092,broker2:9092",
  "loggerType": 1,
  "topic": "mdss-audit",
  "configuration": "
{\"securityProtocol\":\"SASL_SSL\",\"saslMechanism\":\"SCRAM-SHA-
512\",\"saslUsername\":\"mdss\",\"saslPassword\":\"...\"}"
}
```

The `configuration` string, unescaped:

```
{
  "securityProtocol": "SASL_SSL",
  "saslMechanism": "SCRAM-SHA-512",
  "saslUsername": "mdss",
  "saslPassword": "..."
}
```

`securityProtocol` accepts `PLAINTEXT`, `SSL`, `SASL_PLAINTEXT` or `SASL_SSL`. `saslMechanism` accepts `PLAIN`, `SCRAM-SHA-256` or `SCRAM-SHA-512`, and is only required for a SASL protocol.

`PUT /api/externallogger/kafka` takes the same body plus the `id`.

Enable, disable, and delete

`PUT /api/externallogger/status` starts or stops delivery without changing the stored connection settings.

```
{
  "id": "c9f1e0a4-...",
  "isEnabled": false
}
```

`DELETE /api/externallogger/{id}` removes the configuration permanently. Delivery stops with the next event.

Responses carry a numeric `result` field and, on failure, a message. See section 14 for the failure cases.

---

7. Message formats

Both examples below are the same event — a file blocked as infected on an SMB share — as each transport delivers it.

Syslog, RFC 5424

A standard RFC 5424 message. Every field appears twice: once inside the structured-data element `[meta ...]` as quoted key–value pairs, and once inside the human-readable message text. Parse the structured data; treat the message text as a description for analysts.

```
<14>1 2026-08-13T10:15:42.000000+00:00 mdss-host
MetaDefenderStorageSecurity 7208 - [meta
  fileName="invoice.docx"
  filePath="/finance/2026/invoice.docx"
  fileHash="5d41402abc4b2a76b9719d911017c592"
  sha256="e3b0c44298fc1c149afbf4c8996fb924..."
  fileSize="48213"
  fileId="0199c0de-7a1e-7000-8000-0000000000ab"
  dataId="bzIxMDgwOU5xTFZ2b2E"
  result="Blocked"
  blockedReason="Infected"
  numberOfInfectedEngines="3"
  AVCount="32"
  threatFound="Ahnlab: Trojan/Win32.Agent"
  storageName="Finance-SMB"
  storageType="Category: FileShare, Protocol: Smb, Vendor: Generic"
  storageId="stor-77"
  scanId="scan-12"
  scanName="Nightly Finance"
  scanType="Scheduled Process"
  Workflow="Default workflow"
  LogType="1"
  Category="0"
  EventTimestamp="2026-08-13 10:15:42"
  UserId="system"
  UserName="system"
  TenantId="default"
  Namespace="ExternalLogger"
  Id="0199c0de-7a1e-7000-8000-000000000001"]
File (fileName: "invoice.docx"; filePath: "/finance/2026/invoice.docx";
... result:
"Blocked"; blockedReason: "Infected"; ...) from storage (name:
"Finance-SMB"; ...)
was successfully scanned by scan (ID: "scan-12", ...) with the
following
configuration "Default workflow".
```

Wrapped here for readability; on the wire each event is a single message.

> **Numeric values in Syslog**
>
> In RFC 5424 structured data all values are quoted strings, including numeric ones. Cast `fileSize`, `AVCount` and `numberOfInfectedEngines` in your parser if you need them as numbers.

Kafka, JSON

One JSON object per event, UTF-8 encoded. `Properties` holds the fields; the two message forms are provided alongside them so an event can be displayed without re-rendering it.

```
{
  "Timestamp": "2026-08-13T10:15:42.0000000+00:00",
  "Level": "Information",
  "MessageTemplate": "File (fileName: {fileName}; filePath: {filePath};
...",
  "RenderedMessage": "File (fileName: \"invoice.docx\"; ...",
  "Properties": {
    "fileName": "invoice.docx",
    "filePath": "/finance/2026/invoice.docx",
    "fileHash": "5d41402abc4b2a76b9719d911017c592",
    "sha256": "e3b0c44298fc1c149afbf4c8996fb924...",
    "fileSize": 48213,
    "fileId": "0199c0de-7a1e-7000-8000-0000000000ab",
    "dataId": "bzIxMDgwOU5xTFZ2b2E",
    "result": "Blocked",
    "blockedReason": "Infected",
    "numberOfInfectedEngines": 3,
    "AVCount": 32,
    "threatFound": "Ahnlab: Trojan/Win32.Agent",
    "storageName": "Finance-SMB",
    "storageType": "Category: FileShare, Protocol: Smb, Vendor:
Generic",
    "storageId": "stor-77",
    "scanId": "scan-12",
    "scanName": "Nightly Finance",
    "scanType": "Scheduled Process",
    "Workflow": "Default workflow",
    "LogType": 1,
    "Category": 0,
    "EventTimestamp": "2026-08-13 10:15:42",
    "UserId": "system",
    "UserName": "system",
    "TenantId": "default",
    "Namespace": "ExternalLogger",
    "Id": "0199c0de-7a1e-7000-8000-000000000001"
  }
}
```


8. Event envelope reference

These fields are present on **every** event, whatever its type. Build correlation rules and index-time extractions on these; everything else varies by event type.

Field	Type	Description
`Id`	string	Unique event identifier, a time-ordered UUID. Sorting by it sorts by creation order. Use it to deduplicate.
`Level`	string	`Information`, `Warning` or `Error`. `Error` marks a failed operation.
`LogType`	integer	The event type. See section 10 for all values.
`Category`	integer	The functional group the event belongs to. Convenient for coarse filtering.
`Timestamp`	datetime	When the event was written, with offset. In Syslog this is the message header timestamp.
`EventTimestamp`	string	When the event occurred at its source. UTC, formatted `yyyy-MM-dd HH:mm:ss`. Prefer this for event time.
`UserId`	string	Identifier of the user who performed the action, or `system` for actions MDSS took on its own.
`UserName`	string	Display name of that user, or `system`.
`TenantId`	string	The tenant the event belongs to. Several tenants can share one collector and remain separable.
`Namespace`	string	Always `ExternalLogger`. A quick discriminator if the same collector receives other MDSS output.
`MessageTemplate`	string	Kafka only. The message text with field placeholders — a stable signature for an event type, unaffected by values.
`RenderedMessage`	string	Kafka only. The message with values substituted. In Syslog this is the message body.

9. Scan event field reference

File-level events — discovery, scan and post actions — carry these fields in addition to the envelope. Which of them appear depends on how far the file has progressed, so **treat all non-envelope fields as optional** in your parser.

File identity — always present on file events

Field	Type	Description
`fileName`	string	File name without path.
`filePath`	string	Full path within the storage unit.
`fileHash`	string	MDSS content hash for the file.
`fileSize`	integer	Size in bytes.
`fileId`	string	MDSS identifier for the file. Absent for files MDSS has not yet registered.
`lastModified`	datetime	Last-modified time reported by the storage. Present on discovery events.

Scan result — present once the file has been scanned

Field	Type	Description
`result`	string	The verdict, for example `Allowed` or `Blocked`.
`sha256`	string	SHA-256 of the file content, as computed by the scanning engine.
`dataId`	string	Scan identifier from MetaDefender. Use it to look up the full scan report, including per-engine detail.
`AVCount`	integer	How many anti-malware engines processed the file.

Detection detail — present only when the verdict is blocked

Field	Type	Description
`blockedReason`	string	Why the file was blocked — an infection, a vulnerability, or sensitive data, according to the workflow's blocking rules.
`numberOfInfectedEngines`	integer	How many engines flagged the file.
`threatFound`	string	An engine name and the threat it reported, as a single string.

Context — storage, scan, workflow and destination

Field	Type	Description
`storageName`	string	Name of the storage unit the file was found in.
`storageType`	string	Category, protocol and vendor of that storage, as one descriptive string.
`storageId`	string	Identifier of the storage unit.
`scanId`	string	Identifier of the scan that processed the file.
`scanName`	string	Name of that scan.
`scanType`	string	`Real Time Process`, `Scheduled Process` or `Instant Process`.
`Workflow`	string	Name of the workflow applied. Present on successful scan events.
`PostAction`	string	Post-action events only. Which action was applied.
`destinationStorageName`	string	Move and copy actions only. Name of the destination storage. `destinationStorageType` and `destinationStorageId` accompany it.
`RelativeObjectName`	string	Move and copy actions only. Path the file was written to at the destination.

File versions

For storages that keep file versions, version-level events use parallel field names — `fileVersionName`, `fileVersionPath`, `fileVersionHash`, `fileVersionSize`, `fileVersionId` and `createdAt` — alongside `fileId` identifying the parent file.

---

10. Event type reference

The full catalogue, grouped by category. `LogType` identifies the event. These numeric values are stable across releases — build filters and detection rules on them rather than on message text.

Category 0 — Scan activities

LogType	Event	Notes
0	File discovered	A file was found in storage and registered.
1	File scanned	Carries the verdict. `Level` is `Error` when the file could not be scanned.
2	File discovery failed	Includes the failure reason.
3	File cancelled	Processing cancelled by a user.
100–103	Process started, completed, cancelled, failed	Scan-level lifecycle, one per scan run and storage.
1500–1503	Scan added, updated, deleted, imported	Scan configuration changes.
1900–1904	Schedule added, updated, deleted, imported, skipped	Scan schedule changes and skipped runs.

Category 1 — Post actions

LogType	Event	Notes
200	File tagged	Tag written to the file or its metadata.
205–206	Blocked file moved, deleted	Includes the destination for moves.
207	Sanitized file moved	Deep CDR output written to the destination.
208	Allowed file moved	
209–211	Blocked, sanitized, allowed file copied	
212–214	Blocked, allowed, sanitized file kept	The file was left in place by policy.
215	Allowed file deleted	
216	File versions scanned	
217–220	Discovered file deleted, moved, copied, kept	Actions applied without scanning, from a discovery-only workflow.
221	Sanitized file deleted	
419	Empty folders deleted	Lists the folder paths removed.

Category 2 — Storage units

LogType	Event	Notes
300–302	Storage added, updated, removed	
400	Real-time processing changed	Real-time protection enabled, disabled or reconfigured on a storage.

Category 3 — Authentication

LogType	Event	Notes
600	Signed in	Successful sign-ins only. See section 12.
601	Signed out	

Category 4 — Settings

LogType	Event	Notes
700–703	Scan engine instance added, updated, deleted, imported	
750–753	Scan pool added, updated, deleted, imported	
800–802	Licence activated online, activated offline, deactivated	
900–901	Configuration imported, exported	
950	Notification settings changed	Also used for delivery results, under category 8.
975	SMTP configuration changed	
1000–1002	External logger added, updated, deleted	Changes to this integration are themselves audited.
1100	Data retention changed	Retention enabled, disabled, or the window changed.
1200–1202	API key created, updated, deleted	Key lifecycle. Individual API calls are not audited.
1300	SSO configuration changed	
1410	Workflow technologies changed	Which scanning technologies a workflow uses.
1600	On-demand scan requested	A user asked for a file or a filtered set to be scanned.
2000	Encryption key event	Key generation started, completed or failed.
2200	TLS certificate changed	
2300	Telemetry configuration changed	

Category 6 — Users

LogType	Event	Notes
602–606	User created, registered, role updated, updated, removed	Includes password resets and the property that changed.
1800	Product tour finalised	

Category 8 — Notifications

LogType	Event	Notes
950	Notification sent	Delivery result for an email, webhook or message-queue notification.
1700	Report generated	

Categories 9 to 13

Category	LogType	Event
9 Group units	320–322	Group added, updated, removed
10 Account units	330–332	Account added, updated, removed
11 Remediations	2101–2103	Remediation rule added, updated, deleted. Rule execution appears under category 1.
12 Workflows	1400–1404	Workflow added, updated, deleted, set as default, imported
13 Access control	2400–2403	Role assigned, removed, created, deleted
13 Access control	2410–2412	Permission assigned, removed, roles replaced

> **Reserved values**
>
> The schema defines 112 event types, of which 98 are in use. Event types 201, 203, 204, 350, 351 and 410–418, and category 7, are reserved and are not currently emitted. Category 5 is not defined. Do not build rules that depend on them, and

> handle unrecognised values without failing — new types may be added in later releases.

---

11. Filtering at the collector

MDSS sends the whole audit stream to each enabled destination. There is no server-side filter by event type or severity.

On a large deployment, file-level events dominate the volume: a scan of one million files produces roughly one million discovery events plus one million scan events. If your SIEM licence is volume-based, filter before indexing.

`LogType` and `Category` are on every event and are designed for exactly this.

Security events only

Keep blocked files and the actions taken on them, plus all administrative activity. Drop routine discovery and per-file allow verdicts.

```
keep  Category = 1                          # all post actions
keep  Category in (2,3,4,6,9,10,11,12,13)  # all administrative
activity
keep  LogType = 1 and result = "Blocked"    # blocked verdicts
keep  Level = "Error"                       # every failure
drop  everything else                       # discovery and allowed
verdicts
```

Compliance and change-audit only

Drop file-level events entirely and keep the administrative trail — a small, steady volume.

```
drop  Category in (0,1)
keep  everything else
```

Where to apply it

Transport	Approach
Kafka	Filter in your consumer or stream processor on `Properties.LogType` and `Properties.Category`. Cleanest option — unwanted events are never indexed and never counted.
Syslog	Filter on the relay, matching the structured-data pairs as substrings, for example `LogType="1"`. Both rsyslog and syslog-ng can do this with a message-content filter before forwarding.
SIEM ingest pipeline	Most platforms can drop events at ingest time. Confirm with your vendor whether dropped events still count toward your licence — often they do not.

> **Size this before you enable it**
>
> Estimate volume from your file count and scan frequency, and agree the filter with whoever owns the SIEM licence. Turning on an unfiltered feed against a multi-million-file environment is the most common cause of an unpleasant surprise in the first week.

---

12. Not included in the stream

External loggers carry the audit trail, and only the audit trail. The following are outside its scope in MDSS 4.5, listed so you can plan around them rather than discover them during integration.

Not in the stream	What this means	Alternative
Failed sign-in attempts	Successful sign-ins and sign-outs are emitted; failed attempts are not. The feed cannot be used for brute-force or password-spray detection against the MDSS console.	When MDSS is integrated with an identity provider through SSO, authentication failures appear in that provider's own logs.
Source address and session identifiers	Events identify the acting user by id and display name. There is no client IP address, host name, user agent or session identifier on any audit event, so events cannot be correlated by network location.	Access logs from the reverse proxy or load balancer in front of MDSS, shipped separately and joined on user and time.
Per-engine scan detail	A blocked file reports the number of engines that flagged it, the number that ran, and one engine-and-threat string. The full per-engine verdict list, CVE identifiers from vulnerability assessment, sensitive-data match detail, and the Deep CDR breakdown of what was removed are not on the wire.	`dataId` is present on every scanned-file event. Use it to retrieve the complete report from MDSS or MetaDefender Core.
API request activity	Audit events record outcomes, not requests. Individual REST calls, per-request API-key usage, and rejected calls such as permission denials are not audit events. Creating and deleting an API key is audited; using one is not.	Reverse proxy or gateway access logs.
Service and diagnostic logs	Application logs, stack traces, storage-adapter connection diagnostics, and everything in a support package stay local to the deployment. A failed scan appears as an audit event at `Error` level, without the underlying exception.	Collect the MDSS service log files with your existing log agent if you also want platform health in the SIEM.
Server-side event filtering	A destination is either enabled or disabled. There is no option to send only one category, only blocked files, or only a minimum severity to a given destination.	Filter at the collector — see section 11.
Guaranteed delivery and replay	Delivery is best-effort. Events produced while a destination is unreachable are not re-sent when it recovers, so a collector outage becomes a gap in the SIEM's copy. The events themselves are never lost from MDSS.	Prefer TCP or TCP with TLS over UDP. Reconcile a known outage window with the audit API (section 15). A highly available Kafka cluster is the most durable option.
CEF, LEEF and HTTP collectors	Syslog output is RFC 5424 with fields in the structured-data element. There is no CEF or	

	LEEF formatter, and no HTTP event-collector transport for the audit stream.	Map the RFC 5424 structured data or the Kafka JSON to your platform's schema once during onboarding. Both provide named fields, so no pattern matching is required.

13. Limits and tuning

Item	Value	Notes
Destinations per type, per tenant	5	Counted separately for each of the four types. Exceeding it returns a specific error.
Syslog batch size	100	Events per batch. Set SERILOG_BATCH_POSTING_LIMIT to change it.
Kafka batch size	50	Events per batch. Set KAFKA_BATCH_POSTING_LIMIT.
Kafka batch interval	5 s	A partial batch is flushed after this interval. Set KAFKA_BATCH_POSTING_PERIOD.
Kafka delivery flush timeout	10 s	Per batch.
TLS certificate validation	enabled	For Syslog TCP with TLS. EXTERNAL_LOGGER_TCP_TLS_IGNORE_CERTIFICATES can relax it to ignore chain errors, or all errors, for a collector with a self-signed certificate.
Retention of delivered events	not applicable	The MDSS data-retention policy trims the MDSS audit database only. Events already delivered are unaffected, so retention in the SIEM is governed entirely by the SIEM.

> **On relaxing TLS validation**
>
> Only do this for a collector whose certificate you control and cannot get signed. It is a deployment-wide setting and applies to every Syslog TLS destination.

14. Troubleshooting

The configuration will not save

MDSS validates a destination before storing it. The failure cases are:

Result	Cause	Resolution
Failed to test configuration	The connection test did not succeed — wrong address or port, the collector is not listening, a firewall is blocking the path, or TLS validation failed.	Verify reachability from the MDSS host, then retry. For TLS, confirm the collector's certificate chain is trusted.
Same configuration	An identical destination already exists.	Edit the existing entry instead of adding a second one.
Number of integrations exceeded	Five destinations of this type already exist.	Delete one, or use a relay to fan out beyond five.
Already enabled / already disabled	The status change requested is the current state.	No action needed.
Not found	The `id` does not exist for this tenant.	List the destinations and use a current id.

The destination saved, but no events arrive

- Check the destination is **enabled**. A saved configuration with delivery switched off is silent.
- Confirm MDSS is producing audit events at all — open the console audit log. If it is empty, no destination will receive anything. Run a small scan to generate events.
- For UDP, remember there is no delivery confirmation. A firewall can drop the traffic silently and both ends will look healthy. Retest with TCP to prove the path.
- For Kafka, verify the topic exists and that the credentials have produce rights on it.
- If a collector-side filter is in place, confirm it is not dropping everything. Match on `Namespace="ExternalLogger"` first to prove events are arriving, then narrow.

Events arrive but fields are missing

Field composition varies by event type and by how far a file has progressed — a discovered file carries no verdict, and an allowed file carries no `blockedReason`. This is expected. See section 9 for which fields appear when, and treat all non-envelope fields as optional.

Timestamps look wrong

`EventTimestamp` is always UTC. `Timestamp` carries an explicit offset. If events appear shifted, check the time zone your SIEM applies at ingest rather than the MDSS configuration.

15. Pulling audit events instead

Where a push feed is not wanted, or to reconcile a period when a destination was unreachable, the same audit events are available on the REST API.

```
GET /api/audit/{startIndex}/{count}
```

Returns audit entries with filtering, and a total count. The total is capped at 10,001 as a performance guard, so narrow the filter rather than paging through an unbounded result set.

The MDSS data-retention policy applies to this API — events older than the configured retention window are no longer available. For long-term retention, the SIEM copy is the record.

---

16. Questions that come up

"Is SIEM integration an extra licence?" No. External loggers are part of the product.

"Which SIEMs are supported?" Any platform that can receive RFC 5424 Syslog or consume from a Kafka topic. There is no per-vendor integration to install; the fields are named in both formats, so mapping to a platform's schema is a one-time configuration task.

"Can we send different events to different destinations?" Not from MDSS. Every enabled destination receives the whole stream. Route and filter at the collector.

"Can we send to more than five collectors?" Five per type is the limit — twenty in total across the four types. Beyond that, send to a relay and fan out from there.

"Will this slow down our scans?" No. The audit database write is independent of the external destinations, and a slow or unreachable collector does not delay scanning.

"What happens if our SIEM goes down?" Delivery is best-effort and not replayed, so those events will be missing from the SIEM's copy. They remain in the MDSS audit database and can be recovered with the audit API within the retention window.

"Is the traffic encrypted?" Use Syslog over TCP with TLS, or Kafka with `SSL` or `SASL_SSL`. Plain UDP and TCP Syslog are unencrypted.

"Do we get the full scan report for every file?" You get the verdict, the reason, engine counts, a named threat, and both hashes. For the full per-engine report, pivot into MDSS or MetaDefender Core on the `dataId` carried in the event.

"Can we get failed login alerts from MDSS?" Not from this feed in 4.5 — only successful sign-ins and sign-outs are emitted. Where MDSS uses SSO, the identity provider's logs carry authentication failures.

---

17. Where to go deeper

Topic	Where to look
Full API endpoint reference	MetaDefender Storage Security API
Audit log in the console	**Audit log** in the MDSS navigation
Configuring destinations	**Settings → External loggers**
Data retention settings	**Settings → Data retention**
Notification webhooks and message-queue notifications	File scanned RabbitMQ notifications
Environment variables and deployment tuning	Deployment documentation
Sizing the feed for a large environment	Sales Engineering

CONFIGURATION _ SETUP

Is there a limitation on importing configuration to MetaDefender Storage Security?

> **Check Your Version:**
>
> This article applies to all MetaDefender Storage Security releases deployed on Windows or Linux systems.

Yes. We encountered multiple compatibility issues when attempting to import configurations into an already configured MetaDefender Storage Security . These issues can lead to system instability and conflicts.

To address this, we have decided to offer the import functionality exclusively for fresh installations. This ensures a smooth migration of your configuration to a new deployment without the risk of compatibility problems.

> **Support:**
>
> If **Further Assistance** is required, please proceed to create a support case or chat with our support engineer.

[Linux] What are MDSS-related resources and how to perform disk cleanup?

This guide provides an overview of MDSS resources, including paths, containers, and volumes, along with actionable recommendations for managing disk space.

By following these guidelines, you can safely clean unnecessary files while maintaining the integrity of critical data.

Primary Cleanup Mechanism

The main method for managing disk space in MDSS is configuring the **Database Retention Policy**. This policy automatically removes outdated data based on retention settings, reducing manual cleanup requirements. For more information on setting up and using the retention policy, see the Database Retention Configuration Guide.

Filesystem Paths

MD Storage Security uses several paths on the host system for its operations. Below is a breakdown of their purposes and cleanup recommendations:

1. `/etc/mdss` the main installation directory containing Docker Compose files and the `mdss.sh` script.
2. `/etc/mdss/services_logs` stores MDSS container logs mounted from each running container.
   - **Cleanup Guidance**: Log cleanup is generally unnecessary if proper logging configurations are in place. To adjust logging levels or enable extra logging features, refer to How to Enable Extra Logging in the Configuration.
3. `/var/log/mdss` contains logs generated by MDSS scripts.
   - **Cleanup Guidance**: Can be safely cleaned if the logs are no longer needed.
4. `/var/lib/docker` houses all Docker container filesystems and volumes.
   - **Important Note**: Avoid making direct changes to this path. Use `docker` commands for all operations to prevent accidental data loss.

Docker Containers

MDSS services run inside Docker containers. Below are the key containers and their roles:

1. **Containers with Names Starting with** `mdss_*` **and** `mdcs_*` run MDSS services.
2. `mdcs_rabbitmq` provides RabbitMQ services for communication between MDSS components.
3. `mdss_rediscache` temporary data storage using Redis.
4. `mdss_potgresql` database container for persistent data, including settings, storage units, and processing history.

Docker Volumes

Volumes store persistent and temporary data required by MDSS. Here's an overview:

1. `mdss_mongo_db` stores the old MDSS database (persistent data).
   - **Important Note**: Do not delete this volume unless performing a clean reinstallation.
2. `mdss_mongo_backup` temporary old database files for backups.
   - **Cleanup Guidance**: Can be safely removed when MDSS is not running.
3. `mdss_rediscache` temporary data storage.

- **Cleanup Guidance**: Can be safely removed when MDSS is not running.

4. `mdss_postgres_data` stores the MDSS database (persistent data).
   - **Important Note**: Do not delete this volume unless performing a clean reinstallation.

Useful Commands for Disk Usage Management

When investigating disk usage issues, use the following commands:

1. `df -h` displays overall disk usage in a human-readable format.
2. `du -h <PATH>` checks the size of a specific path on the system.
3. `docker system df -v` provides a detailed report of disk usage for Docker containers, images, and volumes.
4. `docker system prune -a --volumes` removes all unused containers, networks, images, and volumes.
   - **Important Note**: Make sure all MDSS services are running before executing this command to avoid removing critical data.

Additional Resources

- For more detailed information, refer to the Sizing Guide.
- We also recommend configuring an external database to enhance storage capacity for MDSS operations. For detailed instructions, please refer to the following article: Using an External Database.

> **Support**
>
> If you have any difficulty performing disk cleanup, please follow these instructions on How To Create a Support Package, before creating a support case or chatting with our support engineer.

How to Enable Specific Modules in the Configuration?

Enabling Modules

During the installation it is advisable to activate only those modules you intend to use, as a measure to conserve resources.

For instance, if your purpose is to scan Amazon S3 buckets, then you should only have the `amazonsdk` module enabled in `ENABLED_MODULES` environment variable inside the `customer.env` file.

```
ENABLED_MODULES=amazonsdk
```

Please follow Custom configuration to learn how to modify the `customer.env` file.

It's important to remember that turning modules on or off is a non-destructive action, allowing you the flexibility to activate additional modules later if you need to work with different types of storage.

By default, all modules are enabled, which means that `ENABLED_MODULES` will look like this right after the installation:

```
ENABLED_MODULES=azureblob,amazonsdk,googlecloud,alibabacloud,azurefiles
,smb,box,onedrive,sftp,nfs
```

Please change it accordingly but remember that in order for these changes to be applied you need to restart MetaDefender Storage Security.

Disabling Services

The following services can be disabled when they are managed externally, to prevent deploying their local container versions:

- MongoDB
- PostgreSQL
- RabbitMQ
- Redis

They can be disabled by adding them individually to the `DISABLED_SERVICES` variable in `customer.env` :

```
DISABLED_SERVICES=mongo,postgres,rabbitmq,redis
```

Which API endpoints from MD Core does MDSS utilize?

Endpoints	Permissions	Usage
`/file`	Processing result fetching - Self-Only/Anyone Download processed file - Self-Only/Anyone	Process files and retrieve results Download processed files
/readyz	-	System health
/stat	System Information - Full	System health
/status	-	System health
/admin/license	License - Read-Only/Full	License information
/version	-	Version information

Advanced File API Filtering and Sorting

Filtering and sorting on the File and PDF report APIs include support for a variety of filter and sort combinations.

Some filtering and all sorting parameters support sending a list of values separated by comma, which take part of a logical OR filter [the property can be any of the given values].

Filtering

Filtering supports the following query parameter fields:

Query parameter	Possible values	Description	Allows list of values
startDate	A valid DateTime		no
endDate	A valid DateTime		no
search	A string value		no
scanType	- 0 = Instant - 1 = Scheduled - 2 = RealTime		yes
storageId	A valid storage id		yes
scanId	A valid scan id		yes
scanWorkflowSnapshotId	A valid snapshot id		yes
processingState	- InProgress = 0 - Failed = 1 - Canceled = 2 - Available = 3	State of processing in MDSS	yes
result	- 0 = Allowed - 1 = Blocked - 2 = Processing	Result of MDSS	yes
scanAllResultI	- See core result codes	General result of the Scan Instance	yes
scanResultICount	An integer >= 0	The number of engine results that are not “No threat detected”	yes
vulnerabilityCount	An integer >= 0	The number of vulnerabilities detected	yes
dlpDetection	Boolean true or false	DLP detection	no
remediations	- 0 = Tagging - 1 = DeepCdrSanitization - 2 = DeepCdrDelete - 3 = DeepCdrEncrypt - 4 = DeepCdrKeep - 5 = AllowedMoved - 6 = BlockedMoved - 7 = BlockedDelete - 8 = SanitizedMoved - 9 = AllowedCopied - 10 = BlockedCopied - 11 = SanitizedCopied - 100 = SoftDelete	Remediations performed	yes

Sorting

Sorting supports multiple parameters, which are used if there is an equality between the values of the preceding sort. If multiple sorts are used, the property and order are matched in order between the two lists of values. The following query parameter fields are available:

Query parameter	Possible values
sortBy	- 0 = DiscoveryStarted - 1 = ScanId - 2 = ProcessingState - 3 = Result - 4 = ScanAllResultI - 5 = ScanResultICount
sortOrder	- 0 = Ascending - 1 = Descending

Is SNMP monitoring supported for MetaDefender Storage Security?

At the current time SNMP monitoring is not supported for our MetaDefender Storage Security product.

This limitation is affecting all versions of the product.

> **Support:**
>
> If **Further Assistance** is required, please proceed to create a support case or chat with our support engineer.

[Linux] How to download docker images from alternate location?

If Docker Hub is inaccessible during installation, you can proceed with either an Linux Offline Installation or by specifying an alternative container registry. To configure an alternate registry, add the necessary details to the `customer.env` file.

```
MDSS_REPO=public.ecr.aws/v2f5u9p9/opswat-mdss
POSTGRES_IMAGE=public.ecr.aws/v2f5u9p9/opswat-mdss/postgres
RABBITMQ_IMAGE=public.ecr.aws/v2f5u9p9/opswat-mdss/rabbitmq
REDIS_IMAGE=public.ecr.aws/v2f5u9p9/opswat-mdss/garnet-alpine
```

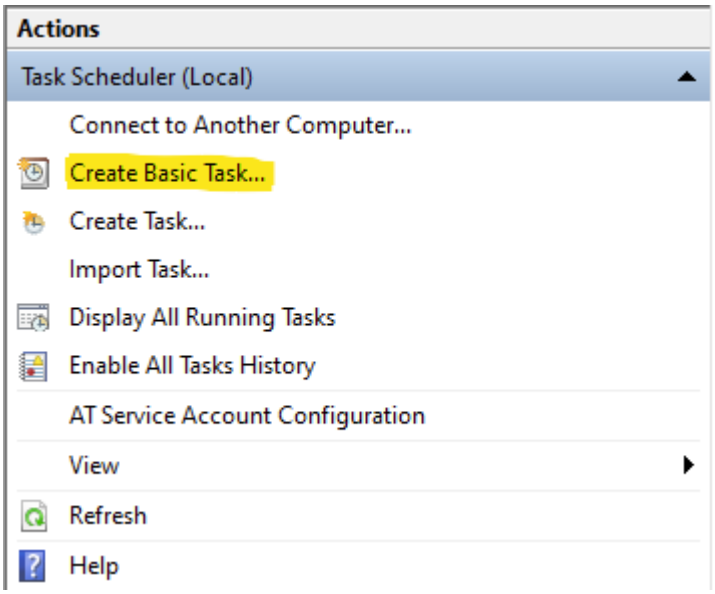
[Windows] How to create a persistent mount for SMB and NFS?

> **Info**

> All the below steps must be performed on the same Windows Server machine where MetaDefender Storage Security is installed.

Step 1

Navigate to **Task Scheduler** and click on **Create Basic Task** (on the right side)



Step 2

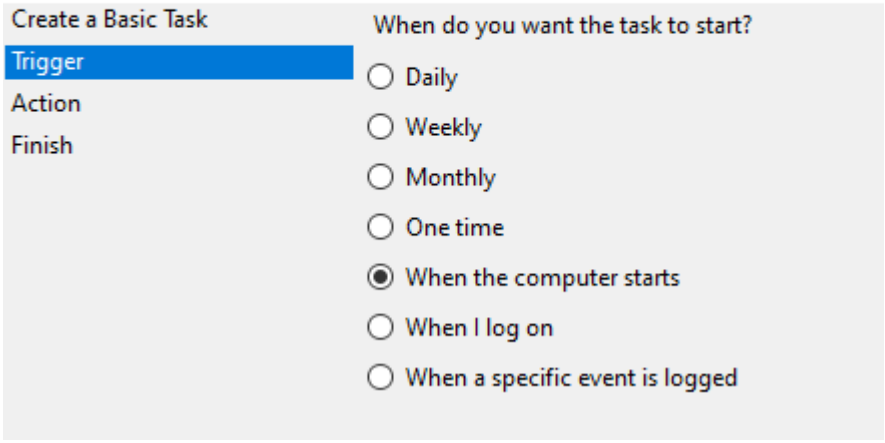
Give your task a specific name and click **Next**

Step 3

Select **When the computer starts**



Task Trigger

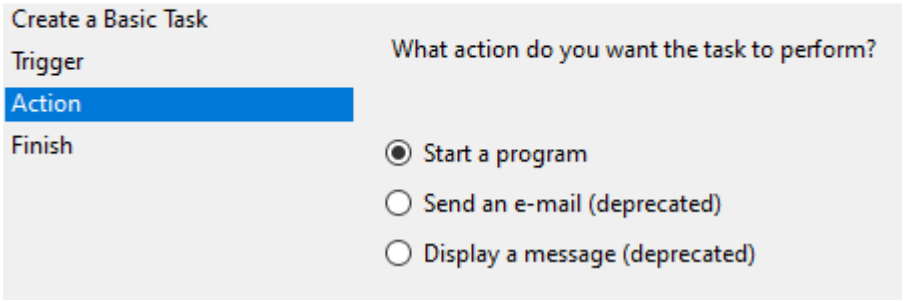


Step 4

Select **Start a program**



Action



Step 5

Enter your mount command in the **Program/script** field.

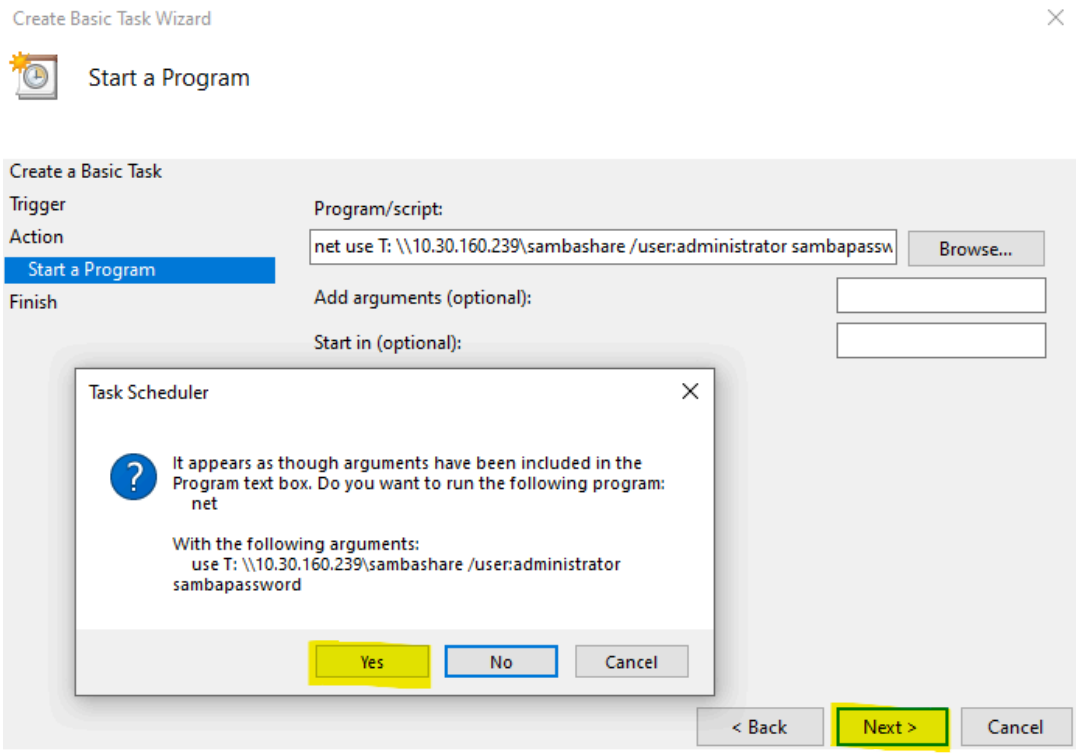
For SMB mount, below is an example: (the password must be provided here because at startup, Windows will not prompt you for it)

```
net use T: \\10.30.160.239\sambashare /user:sambauser sambapassword
```

For NFS mount, below is an example: (no password is required for NFS):

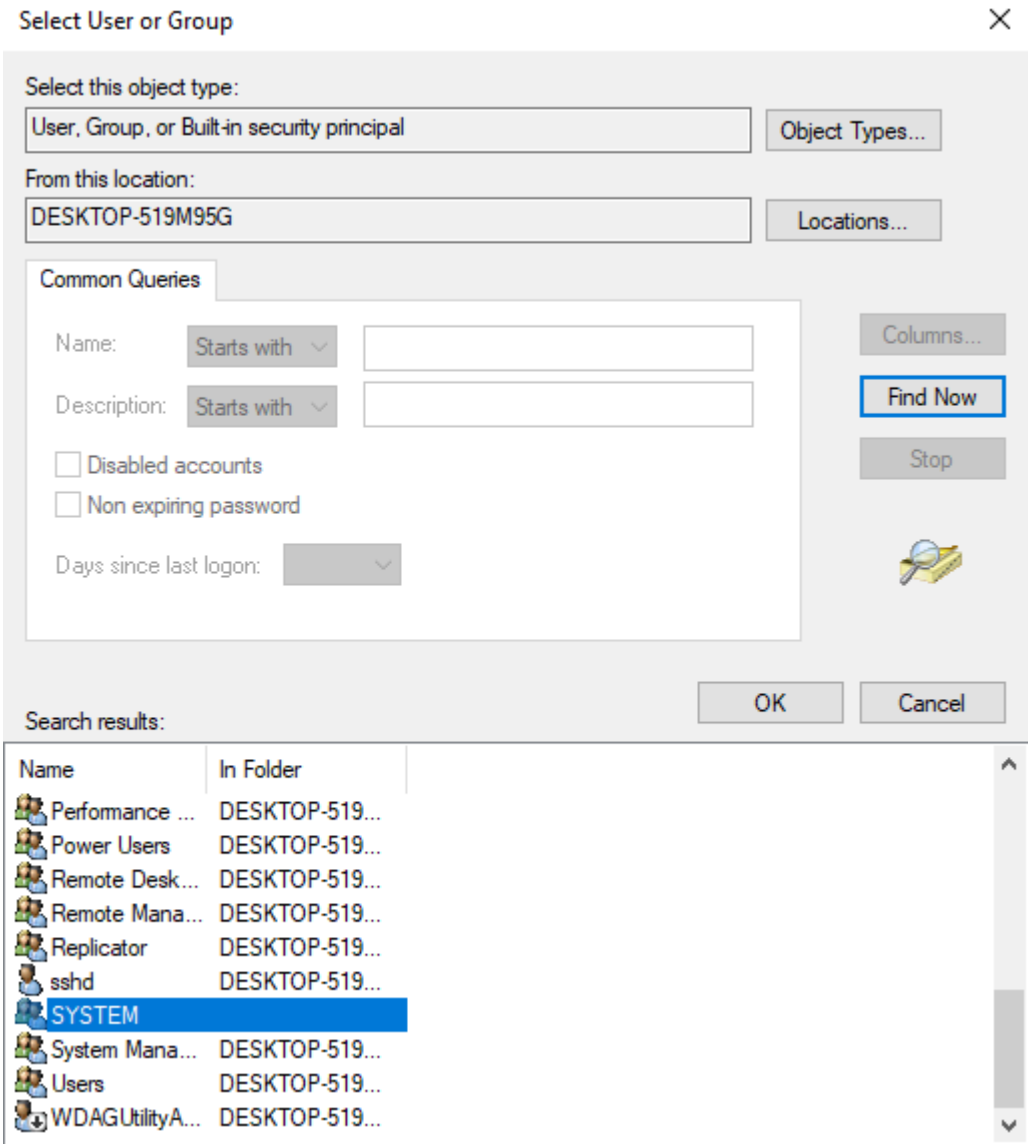
```
mount -o "nolock,sec=sys" 192.168.207.139:/srv/company-public-files/ Y:
```

Click **Next -> Yes -> Finish**



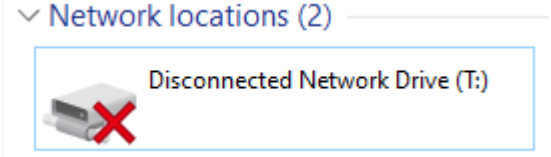
Step 6

From **Task Scheduler**, navigate to **Task Scheduler Library** -> Select your newly created task -> Right click -> Properties -> General -> Change User or Group -> Advanced -> Find Now -> Choose **SYSTEM** -> Click OK and that's it.



Warning

When logged in as a normal user or administrator, the mapped network drive will appear as disconnected. It is not disconnected, the user that is logged in does not have privileges to access it. If you open a terminal as a NT SYSTEM, you will be able to access the newly mapped network drive.



[K8s] How to enable Horizontal Pod Autoscaling based on RabbitMQ queue metrics

This guide outlines the process of setting up Horizontal Pod Autoscaling (HPA) for the Scanning service based on RabbitMQ queue size metrics. This configuration automatically scales the number of scanning pods up or down in response to the number of messages in the scan queue.

> **Info**
>
> This documentation provides a general implementation approach that will need to be adapted to your specific environment. The exact commands, configurations, and values presented here should be reviewed and modified according to your organization's specific Kubernetes infrastructure, network architecture, and operational requirements.

Prerequisites

- Kubernetes cluster with HPA support
- If using an external RabbitMQ instance:
  - RabbitMQ version 3.8.0 or higher
  - RabbitMQ Prometheus plugin must be enabled
  - Port 15692 must be accessible for metrics scraping
  - The RabbitMQ management interface must be available
- Basic understanding of Kubernetes and Prometheus

1. Install Prometheus (if not already deployed)

If Prometheus is not already deployed in your cluster, install it using Helm:`

```
helm repo add prometheus-community https://prometheus-
community.github.io/helm-charts
helm install prometheus prometheus-community/prometheus --namespace
default
```

2. Configure Prometheus to Scrape RabbitMQ Metrics

Add the following scrape configuration to your Prometheus ConfigMap to collect metrics from RabbitMQ:

```
- job_name: rabbitmq
  kubernetes_sd_configs:
  - role: service
    namespaces:
      names:
        - default
  relabel_configs:
  - action: keep
    source_labels: [__meta_kubernetes_service_name]
    regex: rabbitmq
  - action: keep
    source_labels: [__meta_kubernetes_service_port_name]
    regex: 15692
  - action: labelmap
    regex: __meta_kubernetes_service_label_(.+)
  - source_labels: [__meta_kubernetes_namespace]
    target_label: kubernetes_namespace
  - source_labels: [__meta_kubernetes_service_name]
    target_label: kubernetes_service_name
  metrics_path: /metrics
```

Apply the updated ConfigMap and restart Prometheus to apply the changes.

> **Info**
>
> **Note for External RabbitMQ**: If using an external RabbitMQ instance, you'll need to modify the scrape configuration to target your external instance instead of using Kubernetes service discovery.

3. Install Prometheus Adapter (if not already deployed)

The Prometheus Adapter is required to expose Prometheus metrics to the Kubernetes metrics API:

> **Info**
>
> Please update `prometheus.url` and `prometheus.port` according to your environment

```
helm install adapter prometheus-community/prometheus-adapter \
  --set prometheus.url=http://prometheus-server.default.svc \
  --set prometheus.port=80
```

4. Configure Prometheus Adapter

Update the Prometheus Adapter ConfigMap to expose the RabbitMQ queue metric:

```
data:
  config.yaml: |
    rules:
    - seriesQuery:
'{__name__="rabbitmq_queue_messages_ready",kubernetes_namespace!=""}'
      seriesFilters: []
      resources:
        overrides:
          kubernetes_namespace: {resource: "namespace"}
      name:
        matches: "rabbitmq_queue_messages_ready"
        as: "rabbitmq_scan_queue_messages"
      metricsQuery:
sum(rabbitmq_queue_messages_ready{queue=~"object_ready_for_scan_queue_(
Low|Medium|High)"}) by (<<.GroupBy>>)
```

This configuration:

- Queries metrics with name “rabbitmq_queue_messages_ready”
- Associates metrics with Kubernetes namespaces
- Renames the metric to “rabbitmq_scan_queue_messages”
- Filters for scan queues with Low, Medium, and High priorities
- Sums the total number of messages across these queues

After modifying the ConfigMap, restart the adapter:

```
kubectl rollout restart deployment adapter-prometheus-adapter
```

5. Verify the Custom Metric

Check that the metric is properly exposed to the Kubernetes API:

```
kubectl get --raw /apis/custom.metrics.k8s.io/v1beta1/ | jq
```

You should see “rabbitmq_scan_ queue_messages” listed in the output.

```
$ kubectl get --raw /apis/custom.metrics.k8s.io/v1beta1/ | jq
{
  "kind": "APIResourceList",
  "apiVersion": "v1",
  "groupVersion": "custom.metrics.k8s.io/v1beta1",
  "resources": [
    {
      "name": "namespaces/rabbitmq_scan_queue_messages",
      "singularName": "",
      "namespaced": false,
      "kind": "MetricValueList",
      "verbs": [
        "get"
      ]
    }
  ]
}
```

To get the metric value:

```
$ kubectl get --raw
/apis/custom.metrics.k8s.io/v1beta1/namespaces/default/metrics/rabbitmq
_scan_queue_messages | jq
```

You should see the actual value of the queue size:

```
$ kubectl get --raw
/apis/custom.metrics.k8s.io/v1beta1/namespaces/default/metrics/rabbitmq
_scan_queue_messages | jq
{
  "kind": "MetricValueList",
  "apiVersion": "custom.metrics.k8s.io/v1beta1",
  "metadata": {},
  "items": [
    {
      "describedObject": {
        "kind": "Namespace",
        "name": "default",
        "apiVersion": "/v1"
      },
      "metricName": "rabbitmq_scan_queue_messages",
      "timestamp": "2025-03-28T11:37:19Z",
      "value": "4994",
      "selector": null
    }
  ]
}
```

6. Create a Horizontal Pod Autoscaler

Create an HPA resource that uses the custom metric to scale the Scanning service:

```
apiVersion: autoscaling/v2
kind: HorizontalPodAutoscaler
metadata:
  name: scanningservice-hpa
  namespace: default  # Change if your deployment is in a different
namespace
spec:
  scaleTargetRef:
    apiVersion: apps/v1
    kind: Deployment
    name: scanningservice
  minReplicas: 1  # Minimum number of pods
  maxReplicas: 10  # Maximum number of pods
  metrics:
  - type: Object
    object:
      metric:
        name: rabbitmq_scan_queue_messages
      describedObject:
        apiVersion: v1
        kind: Namespace
        name: default  # Or the namespace where your RabbitMQ is
running
      target:
        type: Value
        value: 5000  # 5000 is the maximum number of messages in the
queue set by default in MDSS
```

Apply the HPA:

```
$ kubectl apply -f scanningservice-hpa.yaml
```

7. Monitor the HPA

Check the status of your HPA:

```
kubectl get hpa scanningservice-hpa
kubectl describe hpa scanningservice-hpa
```

Scaling Behavior

- When the total number of messages in the scan queues exceeds 5000, the HPA will scale up the number of scanning pods (up to the maximum of 10).
- When the number of messages decreases, the HPA will gradually scale down the number of pods.

Troubleshooting

If the HPA isn't working as expected:

1. Verify Prometheus is collecting RabbitMQ metrics:

```
kubectl port-forward svc/prometheus-server 9090:80
```

Then visit http://localhost:9090 and query:

```
rabbitmq_queue_messages_ready{queue=~"object_ready_for_scan_queue_(Low|Medium|High)"}
```

2. Check that the Prometheus Adapter can access the metrics:

```
kubectl logs -l app.kubernetes.io/name=prometheus-adapter
```

3. Verify the custom metric is available:

```
kubectl get --raw
/apis/custom.metrics.k8s.io/v1beta1/namespaces/default/metrics/rabbitmq
_scan_queue_messages
```

4. Ensure the HPA is targeting the correct deployment and namespace.

How to Configure and Use Syslog and Serilog Sinks?

Syslog Configuration

Recommended Tools:

- Visual Syslog Server (recommended)
- Syslog Watcher Manager (Note: Has a limit of 5000 messages/hour)

Configuration Steps:

Currently, we support Syslog (UDP) using the RFC5424 Output format for external logger configuration.

To visualize MetaDefender Storage Security audit logs centrally, integrate a Syslog (UDP) server using these details:

- Server address: IPv4, IPv6, and Host Name formats supported.
- Port: Specified Syslog server port.
- Syslog Facility: As per configuration needs.
- Output format: RFC5424.

You can add up to 5 external logger configurations of each type.

Syslog Message Format

RFC5424 message format is supported:

VERSION TIMESTAMP HOSTNAME APP-NAME PROCID MSGID STRUCTURED-DATA MSG

- PRI: Priority value
- VERSION: Syslog protocol specification version
- TIMESTAMP: Formalized timestamp
- HOSTNAME: Sending machine
- APP-NAME: Application or device originating message
- PROCID: Process name or ID
- MSGID: Message type
- STRUCTURED-DATA: Parsable data format
- MSG: Informative free-form message

Example Syslog Message

```
<110>1 2024-03-26T12:27:58.276724+02:00 LP10-D8569
MetaDefenderStorageSecurity 36800 - [meta UserName="jdavis"
UserId="e69e8c2d-4dcc-4489-8f40-0df84199de52"
EventTimestamp="03/26/2024 10:27:58" Category="3" LogType="600"] John
Davis (jdavis) logged in.
```

Serilog Sinks

What is Serilog?

Serilog is a structured logging library for .NET applications, which allows logging to various destinations called sinks, including Syslog, files, HTTP endpoints, and console.

Commonly Used Serilog Sinks and Configurations:

1. Serilog.Sinks.Syslog

Logs events to remote syslog servers via UDP or TCP, supporting RFC3164 and RFC5424 formats.

```
"WriteTo": [
  {
    "Name": "TcpSyslog",
    "Args": {
      "host": "<ip_host>",
      "port": 514,
      "appName": "<your_app_name>",
      "format": "RFC5424",
      "facility": "<facility_name>",
      "outputTemplate": "[{Timestamp:u}] [{Level}] {SourceContext}:
{Message:lj}{NewLine}{Exception}"
    }
  }
]
```

2. Serilog.Sinks.Http

Sends log events via HTTP/S to remote endpoints.

```
"WriteTo": [
  {
    "Name": "Http",
    "Args": {
      "requestUri": "<your_request_uri>",
      "queueLimitBytes": null
    }
  }
]
```

3. Serilog.Sinks.Console

Writes log events to the console.

```
"WriteTo": [
  {
    "Name": "Console",
    "Args": {
      "outputTemplate": "[{Timestamp:u}] [{Level}] {Namespace}:
{Message:lj}{NewLine}{Exception}"
    }
  }
]
```

4. Serilog.Sinks.File

Writes logs to a file.

```
"WriteTo": [
  {
    "Name": "File",
    "Args": {
      "buffered": false,
      "fileSizeLimitBytes": 500000000,
      "outputTemplate": "[{Timestamp:u}] [{Level}] {Namespace}:
{Message:lj}{NewLine}{Exception}",
      "path": "logs/log.txt",
      "retainedFileCountLimit": "10",
      "rollingInterval": "Day",
      "rollOnFileSizeLimit": true
    }
  }
]
```

Testing & Validation:

Use tools like Visual Syslog Server or test HTTP endpoints to validate your logging configurations and ensure logs are captured correctly.

> **Support:**
>
> If **Further Assistance** is required, please proceed to log a **support case or chatting with our support engineer**.

Does MetaDefender Storage Security support symlinks scanning?

Yes, MDSS fully supports symbolic links (symlinks) **when using the NFS storage type**. This means that MDSS can seamlessly follow these links and process the files they point to.

All major types of symlinks are supported across both **Windows** and **Linux** deployments, including:

- **Soft links (symbolic links)**
- **Hard links**
- **Junction points** (Windows-specific)

Feature	Soft Link	Hard Link	Junction Point
What it is	File containing a path string	Directory entry for file data	Filesystem pointer
Points to	File or Directory	File only	Directory only
Cross Volume?	Yes	No	Yes (Local Volumes Only)
Target Deleted?	Link becomes broken	Other links remain valid	Link becomes broken
Platform	Linux/Unix, Windows	Linux/Unix, Windows	Windows only

---

> **Symlink scanning exclusivity**
>
> Symlink scanning is **exclusively applicable to NFS** and is not supported for other storage types. To learn more about integrating an NFS share, please refer to this page.

> **Broken link handling in MDSS**
>
> When MDSS encounters a broken link or a link pointing to a non-existent or inaccessible target, it will generate an error indicating that it was unable to locate the file at the specified path (the path to which the broken symlink was pointing).

Does a CVE affect MetaDefender Storage Security?

In today's rapidly evolving digital landscape, understanding the impact of security vulnerabilities is more crucial than ever. The Common Vulnerabilities and Exposures (CVE) list is an invaluable resource for identifying potential security risks associated with software products. This article provides a comprehensive overview of various CVEs, helping you determine whether MetaDefender Storage Security is affected. By staying informed about these vulnerabilities, you can take proactive measures to protect your systems and data from potential threats.

CVE	Summary
CVE-2024-27322	MetaDefender Storage Security doesn't use R programming language within the product, we are not affected by CVE-2024-27322.
CVE-2024-4603	This vulnerability affects the functions `EVP_PKEY_param_check()` and `EVP_PKEY_public_check()`. Since these are not used, MetaDefender Storage Security is not affected.
CVE-2024-0727	Upon thorough review and analysis, it has been determined that all versions of the License SDK integrated with the MDSS product do not utilize any of the mentioned vulnerable functions. Hence, MetaDefender Storage Security is not affected by CVE-2024-0727.
CVE-2023-46589	MetaDefender Storage Security does not use Apache so it's not being affect by CVE-2023-46589
CVE-2023-44487	MetaDefender Storage Security is not impacted by CVE-2023-44487.
CVE-2024-41110	We tested with versions of Docker up to `Docker version 27.1.1`, build 6312585 and can confirm that MetaDefender Storage Security is not impacted by CVE-2024-41110
CVE-2024-7592	MetaDefender Storage Security is container based, and the python version used by MetaDefender Storage Security internally is 3.12, hence MetaDefender Storage Security is not impacted by CVE-2024-7592. Python libraries present on the host machine where MDSS is installed can be removed.
CVE-2018-15133	MetaDefender Storage Security does not use PHP and/or Laravel Framework so it's not affected

Support

If **Further Assistance** is required, please proceed to log a support case or chat with our support engineer.

How do I Check Port 80 and 443 Usage Before Installing MDSS on Windows and Linux?

Introduction

Before installing MDSS, it is crucial to check the availability of ports 80 and 443. If these ports are in use by another application, the MDSS service will not start. This document provides step-by-step instructions to check port 80 and 443 usage on both Windows and Linux systems.

Windows

1. Checking Port 80 and 443 Using PowerShell

Steps:

1. Open PowerShell as an Administrator.
2. Copy and paste the following command:

```
Get-NetTCPConnection -LocalPort 80,443 | ForEach-Object {
    Get-CimInstance Win32_Process -Filter "ProcessId = '$($_.OwningProcess)'"
} | Select-Object ProcessId, Name, ExecutablePath
```

3. Interpret the Output:

- If no application is using the ports, you will see an error message like this:

```
Get-NetTCPConnection : No MSFT_NetTCPConnection objects found with property
'LocalPort' equal to '80'.
Get-NetTCPConnection : No MSFT_NetTCPConnection objects found with property
'LocalPort' equal to '443'.
```

This indicates that port 80 and 443 are available, and you can proceed with the MDSS installation.

- If another application is using the ports, the output will look like this:

```
ProcessId Name      ExecutablePath
--------- ----      --------------
    47752 httpd.exe c:\xampp\apache\bin\httpd.exe
```

This means that httpd.exe is currently using port 80 and 443.

---

2. Checking Port 80 and 443 Using Netstat

Steps:

1. Open Command Prompt (CMD) as an Administrator.
2. Run the following commands:

```
netstat -ano | findstr :80
netstat -ano | findstr :443
```

3. Interpret the Output:

- If the ports are in use, you will see an output like this:

```
TCP    0.0.0.0:80      0.0.0.0:0      LISTENING    47752
TCP    0.0.0.0:443     0.0.0.0:0      LISTENING    47752
```

- The last column (47752) is the Process ID (PID) of the application using the ports.

4. To identify the application using the PID, run:

```
tasklist | findstr 47752
```

Example Output:

```
httpd.exe                    47752 Console                    1     22,456 K
```

This confirms that httpd.exe is using port 80 and 443.

Linux

Checking Port 80 and 443 Using Netstat

Steps:

1. Open a Terminal.
2. Run the following command:

```
netstat -tulpn | grep -E ':80|:443'
```

3. Interpret the Output:

- If ports 80 and 443 are in use, you will see an output like this:

```
tcp    0    0 0.0.0.0:80     0.0.0.0:*     LISTEN     1234/nginx
tcp    0    0 0.0.0.0:443    0.0.0.0:*     LISTEN     5678/apache2
```

** Netstat Command Options Explained: **

- `-t` ➔ Show TCP connections
- `-u` ➔ Show UDP connections
- `-l` ➔ Show Listening ports
- `-p` ➔ Show the process name
- `-n` ➔ Show numeric addresses instead of resolving hostnames

---

Conclusion

- If ports 80 and 443 are available, you can proceed with the MDSS installation.
- If ports 80 and 443 are in use, you need to stop or reconfigure the conflicting application before installing MDSS.
- Use the provided commands on Windows and Linux to check and troubleshoot port usage effectively.

> **Support:**
>
> If **Further Assistance** is required, please proceed to log a **support case or chatting with our support engineer**.

What's the Best Practice for Managing Logs and Data Retention in MDSS?

> **Check Your Version:**
>
> This article applies to MetaDefender Storage Security versions up to 3.5.1

If you're experiencing storage issues on your MetaDefender Storage Security (MDSS) deployment, there are several strategies you can use to manage and free up disk space. This article outlines recommended practices for monitoring storage, adjusting configurations, and leveraging built-in features to maintain system performance and availability.

Recommended Actions

1.Configure Database Retention

To help manage storage usage, you can configure the system to automatically delete older records from the MDSS database. This helps prevent data buildup and keeps your storage usage under control. Refer to this support article: Database Retention

- **Enable automatic cleanup for the following record types:**
  - Audit records
  - Report records
  - Real-time processing history
- **Set retention periods** to define how many days these records are kept before being automatically deleted.
- **Lower retention thresholds** as needed to reduce overall database size and free up space.

2. Increase Disk Size for Key Directories

Especially on Linux-based installations, directories like `/var` often store temporary files related to file scans and remediation. If storage is running low:

- Extend the disk size allocated to MDSS.
- **Recommended formula:**
- *Temporary space ≥ 2 × [Size of the largest file in GB]**

3. Regularly Monitor Disk Space

- Regularly monitor disk space and identify large directories or files that may be consuming excessive storage.

4. Extend `/var` if Remediation Files Are Large

If remediation actions produce temporary files that fill up your `/var` directory:

- Consider resizing or extending the `/var` partition.
- Monitor this location closely, especially if you process large files.

5. Cloud Deployments: Use Native Monitoring Tools

If you've deployed MDSS in a cloud environment (e.g., AWS, Azure, GCP):

- Use built-in monitoring tools to track disk space.
- Set up automated alerts when usage reaches critical thresholds.

6. Upgrade to the Latest Version:

If you are using an older version of MDSS, upgrade to the latest version as it may include improvements for storage management. You can check and download the latest version by logging in to **My OPSWAT** and navigating to "Product Downloads".

Performance Limitations on Windows:

- Be aware that on Windows, each Docker container can only be assigned 2GB of RAM, which may impact performance. Consider moving to MDSS Linux for better resource management if possible

> **Support:**
>
> If **Further Assistance** is required, please proceed to log a **support case or chatting with our support engineer**.

How to disable the Local PostgreSQL when using an external Database?

> **Check Your Version:**
>
> This article applies to MetaDefender Storage Security v4.x

Overview

If you prefer to connect the MetaDefender Storage Security (MDSS) application to your own remote PostgreSql database server, you can disable the built-in PostgreSql container and its related references by editing the Docker Compose files. While the bundled PostgreSql service consumes minimal resources when idle, you can still reclaim those resources by following the steps below.

Instructions

1. Stop the MDSS Application

Before making any configuration changes, stop the MDSS services:

```
sudo mdss -c stop
```

---

2. Disable the Built-in PostgreSql Container

Open the following file in a text editor: `/etc/mdss/docker-compose.main.yml`

Locate the `postgresql` service section and **add the following**:

```
profiles:
     - disabled
```

3. Start the MDSS Application

Once all modifications are complete, start the MDSS services again:

```
sudo mdss -c start
```

Verification

After restarting, verify that:

- MDSS is running without the internal PostgreSql container.
- The application is successfully connected to your external PostgreSql server.

You can check logs or test basic application functionality to ensure a proper connection.

> **Support:**
>
> If you have followed all of the steps above but are still experiencing issues, please follow these instructions on how to generate a Support Package before creating a support case or chatting with one of our support engineers.

Why remediation actions are not working?

> **Check Your Version:**
>
> This article applies to all MetaDefender Storage Security versions.

Remediation actions are executed after a successful file scan.

Please follow the steps below to analyze why remediation actions may not be working in your environment:

Step 1: Review correct setup

1. Make sure that the workflow has been setup correctly.
2. Ensure that MetaDefender Storage Security is connected to correct storage unit and there are not permission issues.
3. Check if MetaDefender Storage Security is connected to the expected MetaDefender Core Instance.

Step 2: Ensure that there are no issue scanning files

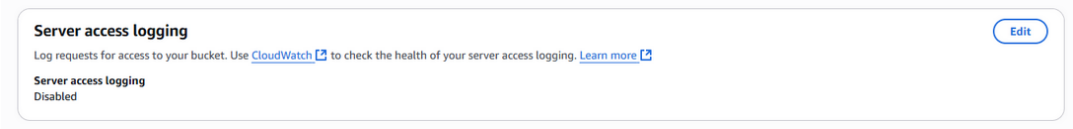
Remediation actions are executed after a successful file scan. If a file was not scanned, please check on MetaDefender Core the reasons why. You can review the different scan results codes in here.

Step 3: Transfer Speeds

Issues related to transfer speeds can cause file upload to take longer than expected which can cause issues performing remediation actions. For example in AWS S3 integration:

AWS

1. Low transfer speeds With big files, usually, there may be an extended period of time that it is used for file uploads. This can be caused due to a network infrastructure limitation. For checking the transfer speed in AWS for example, we recommend using “Server Access logging”.



2. Temporary credentials expire during file upload Depending on the transfer speeds, the temporary credentials provided by the IAM may expire mid-upload. This issue would be improved if transfer speeds improve. Alternatively, you can increase the temporary credential timeout period through AWS AIM Console settings as needed.



Step 4: Credentials and permission to access Storage units

Credentials and permissions are what allow access to MetaDefender Storage Security access storage units to apply remediation actions. In cases where these are not set correctly or lack enough priviledge, this function would run into issues. For example in SMB integrations:

SMB

1. **Permission** ** **restrictions preventing access to the SMB share.** To troubleshoot, please:
    1. Verify that the user account has appropriate permissions on the SMB share.
    2. Check both share-level and NTFS permissions for read/write access.
    3. Ensure the user account is not locked or disabled.

2. **Authentication** ****protocol error.** This issue could result from an authentication protocol mismatch between MDSS client and your SMB server. To troubleshoot:
    1. **If** ****your SMB server runs on Windows**: Configure the username from MDSS UI to be in UPN format (user@domain.com) to enable Kerberos authentication
    2. **If** ****your SMB server runs on Linux**: Use the format DOMAIN\username for NTLM authentication

> **Info:**
>
> Based on our analysis and extensive experience with similar connectivity challenges, we strongly recommend implementing **SMB Share via NFS Storage Unit Configuration**. This approach has consistently delivered superior results for customers experiencing SMB connectivity issues.

> **Support:**
>
> If **Further Assistance** is required, please proceed to log a **support case or chatting with our support engineer**.

What is the expected MetaDefender Storage Security Remediation Behavior Behind F5 Load Balance?

> **Check Your Version:**
>
> This article applies to all MetaDefender Storage Security versions.

Issue:

When F5 is configured with cookie-based persistence, MetaDefender Storage Security remediation could fail. This could occur if the XML provided was not well-formed or was not valid during initial communication. **cookie-based persistence on F5** causes inconsistent routing of related S3 API requests during remediation workflows.

Description

When persistence is enabled, the F5 load balancer modifies the headers cookies of API requests from MetaDefender Storage Security to the S3 compatible storage, causing API responses to get corrupted and not being processed by our MetaDefender Storage Security. While switching F5 to source address persistence seems the least invasive there is no guarantee that it will not modify the headers for tracking.

Mitigation:

1. Disable persistence for the virtual server handling S3 traffic, OR
2. Create a separate virtual server with FastL4 profile for S3 connections

> **Info:**
>
> S3 API calls are stateless and don't require session affinity - persistence only adds processing overhead that corrupts the XML payloads.

> **Support:**
>
> If **Further Assistance** is required, please proceed to log a **support case or chatting with our support engineer**.

Why connection to SMB share cannot be established?

> **Check Your Version:**
>
> This article applies to all MetaDefender Storage Security versions.

Issue:

MetaDefender Storage Security connection with SMB fails with error:

```
smbprotocol.exceptions.SMBOSError: [Error 0] [NtStatus 0xc00000c9] Unknown NtStatus error returned 'STATUS_NETWORK_NAME_DELETED': '\\{IP_HOSTNAME}ftp\CN
```

Description

- `NtStatus 0xc00000c9` corresponds to `STATUS_NETWORK_NAME_DELETED`.
- This error typically occurs when the network share or resource you are trying to access has been removed, deleted, or is temporarily unavailable.
- It can also happen if the SMB session has become stale (e.g., the server closed the connection due to timeout, network issues, or a manual server-side operation).

Possible Causes:

- The network share `\\[IP_HOSTNAME]\ftp\CN` was deleted or unshared on the server. The SMB server might be up but the whole path might be unshared.
- The server at `[IP_HOSTNAME]` rebooted, crashed, or restarted its SMB service.
- There is a network connectivity issue between our SMB service and customer's SMB server.
- Permissions on the share changed, making it inaccessible.

> **Support:**
>
> If **Further Assistance** is required, please proceed to log a **support case or chatting with our support engineer**.

What permissions are needed for the user of the storage of Google Cloud?

Introduction:

This knowledge base article provides information on what roles the user that maps the Google Cloud Storage should be.

Permissions Overview

For MDSS to operate correctly when integrating with Google Cloud Storage, the user account must have sufficient privileges. The documentation initially recommends that the user be granted the Owner role. This role provides comprehensive permissions across the Google Cloud project, including the ability to:

- Create, modify, and delete buckets and objects
- Configure access controls and security settings
- Manage project resources and billing

Important Note: While granting the Owner role ensures all necessary permissions are available, it is generally best practice to adhere to the principle of least privilege. In cases where only storage operations are required, consider using more specific roles such as:

- Storage Admin (roles/storage.admin): Grants full control over Cloud Storage resources without broader project permissions.
- Storage Object Admin (roles/storage.objectAdmin): Provides full control over objects in the storage buckets while limiting administrative capabilities on bucket settings.

Select the role based on the required functionality and security guidelines of your organization.

Detailed Configuration Steps

1. Evaluating Requirements

- Assess MDSS Needs: Determine if MDSS requires full project management capabilities or just access to storage resources. For most scenarios where the sole purpose is mapping storage, the Storage Admin role may suffice.
- Review Security Policies: Consult your organization's IT and security policies to ensure compliance with role assignments and the principle of least privilege.

2. Assigning Permissions via the Google Cloud Console

- Log into the Google Cloud Console: Access your Google Cloud project.
- Navigate to IAM & Admin: Select "IAM & Admin" from the navigation menu.
- Locate the User Account: Find the user account that MDSS will use for mapping the storage.
- Assign the Appropriate Role:
  - For comprehensive permissions, assign the Owner role.
  - Alternatively, assign Storage Admin or Storage Object Admin if full project permissions are not required.
- Save Changes: Confirm and save the changes to update the permissions.

3. Verifying Permissions

- Test Storage Access: Use MDSS to perform operations such as creating, reading, updating, and deleting objects to verify that the assigned role meets the required functionality.
- Audit Logs: Regularly review the Cloud Audit Logs to ensure no unintended or unauthorized actions are performed.

Additional Considerations

- Security Best Practices: Always follow the principle of least privilege. Grant only the permissions that are necessary for the MDSS operations to minimize security risks.
- Periodic Review: Regularly review IAM roles and permissions in your Google Cloud project. Reassess whether the granted permissions still match the operational requirements of MDSS.
- Role Customization: If none of the predefined roles align with your needs, consider creating a custom role that aggregates only the required permissions for storage mapping. This approach can offer a more tailored security posture while meeting functional requirements.

Conclusion

Mapping Google Cloud Storage for MDSS requires careful consideration of the permissions assigned to the user account. While the initial recommendation is to use the Owner role,

assessing the operational needs and following best security practices might suggest using more limited roles such as Storage Admin. By following the configuration steps and periodic reviews outlined in this article, you can ensure both functionality and security in your MDSS deployment.

> **Support:**
>
> If **Further Assistance** is required, please proceed to log a **support case or chatting with our support engineer**.

How to Integrate Cerberus SFTP with MDSS?

> **Check Your Version:**
>
> This article applies to all supported MetaDefender Storage Security releases deployed on Windows and Linux systems

> **Info:**
>
> This guide provides instructions to setup Cerberus SFTP shared folder configuration to integrate with MDSS using the basic credentials (user/pass)

What is Cerberus SFTP?

Cerberus SFTP Server enables organizations to become more efficient with fast, secure, compliant and easy file transfers. Homepage Cerberus FTP Server - The Secure and Compliant FTP Server | Cerberus FTP Server

Step-by-Step Setup for Cerberus SFTP Server

> **Info:**
>
> Only supported on a Windows Server, recommended to install Cerberus on a Windows Server 2022

1. Download and Install Cerberus FTP Server

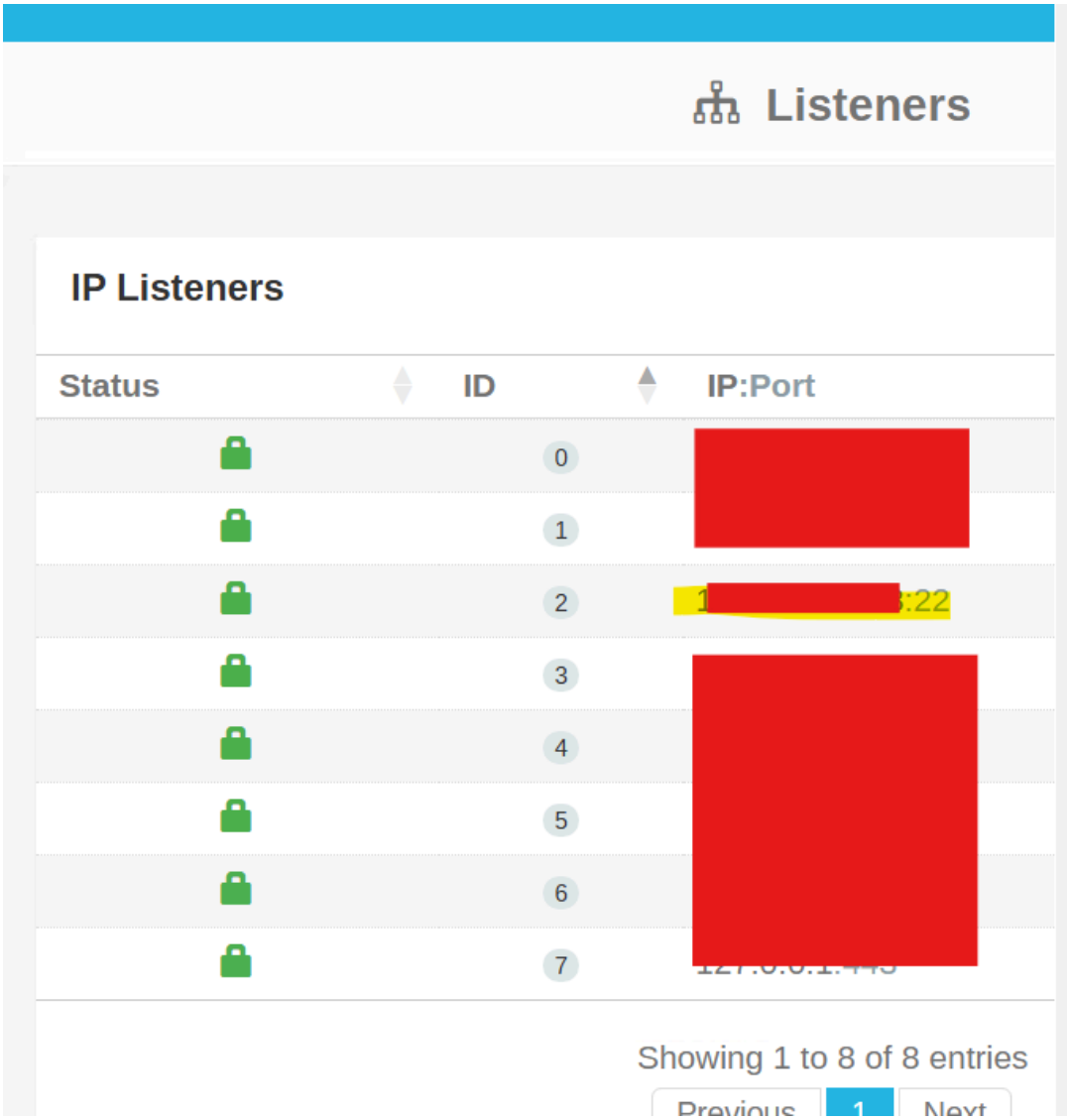
- Go to the Cerberus FTP Server website and download the installer. FTP Server Download | Cerberus FTP Server
- Run the installer as an Administrator.

- Enter first account

2. Enable SSH for SFTP

- SFTP requires SSH. Cerberus uses the built-in OpenSSH on Windows.
- Ensure OpenSSH is enabled on your system:
  - Go to **Settings > Apps > Optional Features**.
  - Install **OpenSSH Server** if it's not already installed.

3. Set Up an SFTP Listener



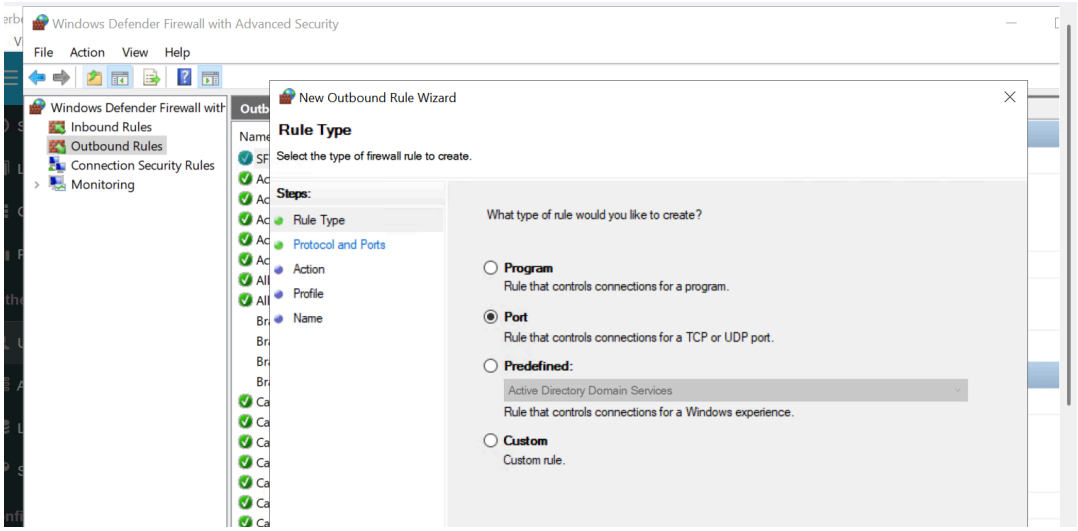
How to setup an SFTP Listener (in case it doesn't create by default):

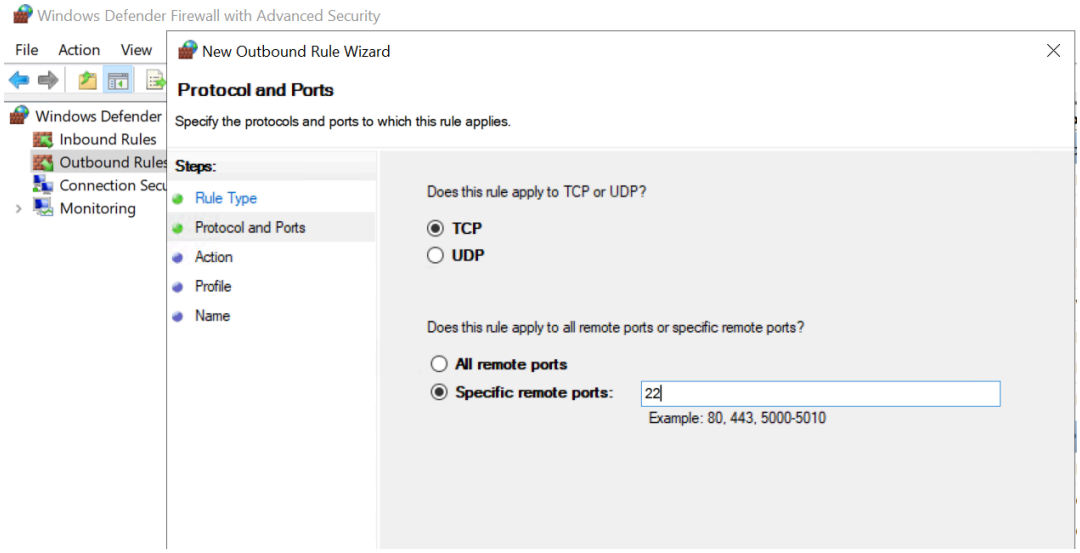
- Open Cerberus FTP Server.
- Go to **Server Manager > Listeners**.

- Add a new listener:
  - **Protocol**: SFTP
  - **Port**: 22 (or another if needed)
  - **IP Address**: Choose the appropriate one (current server's IP) or use `0.0.0.0` for all.

4. Configure Firewall and Router

- Open port **22** (or your chosen port) on your firewall.

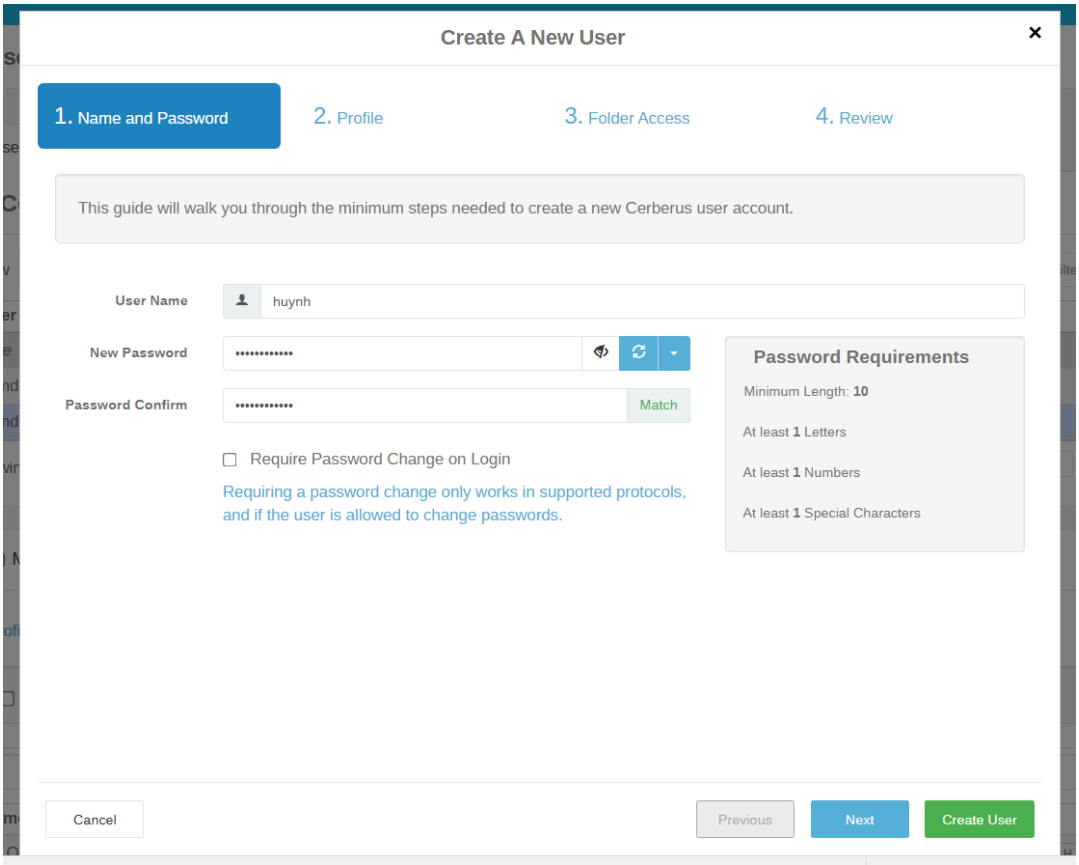




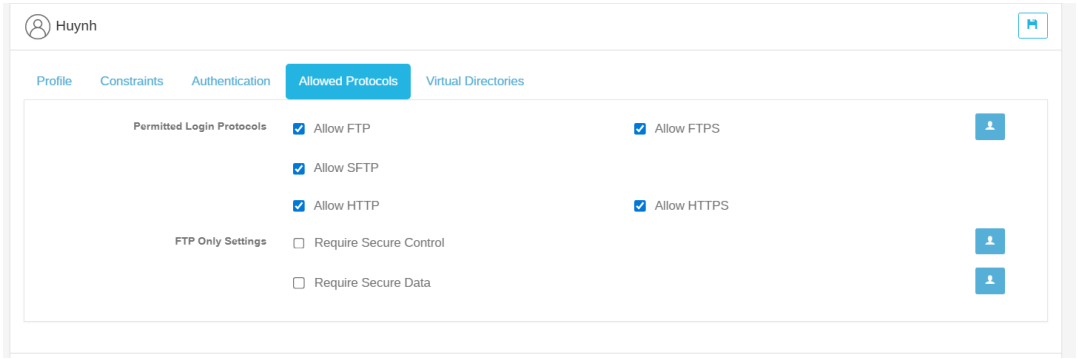
- Set up **port forwarding** on your router to direct traffic to your server's internal IP (if needed)

5. Mapping a folder with Cerberus local users

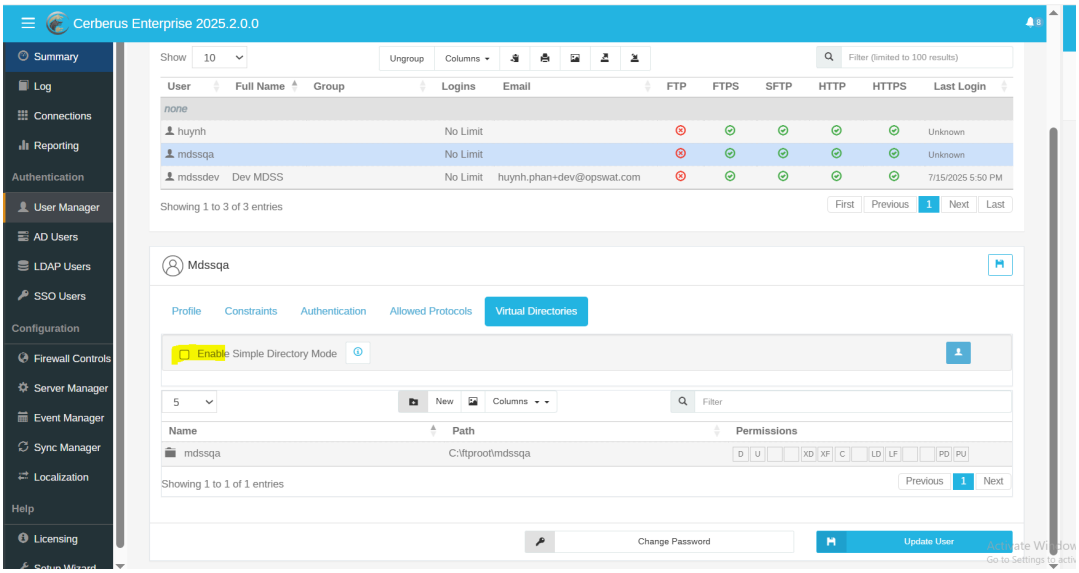
- Create a local user who has full permissions to the folder



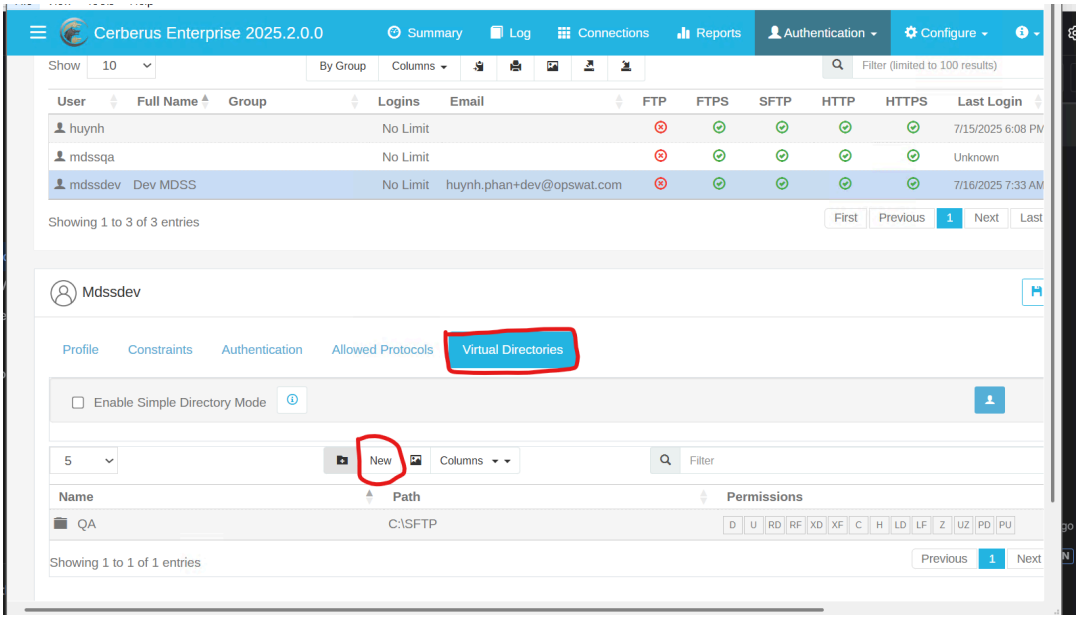
- Choose the user in the list
- Make sure the user is having the permission to login into SFTP protocol



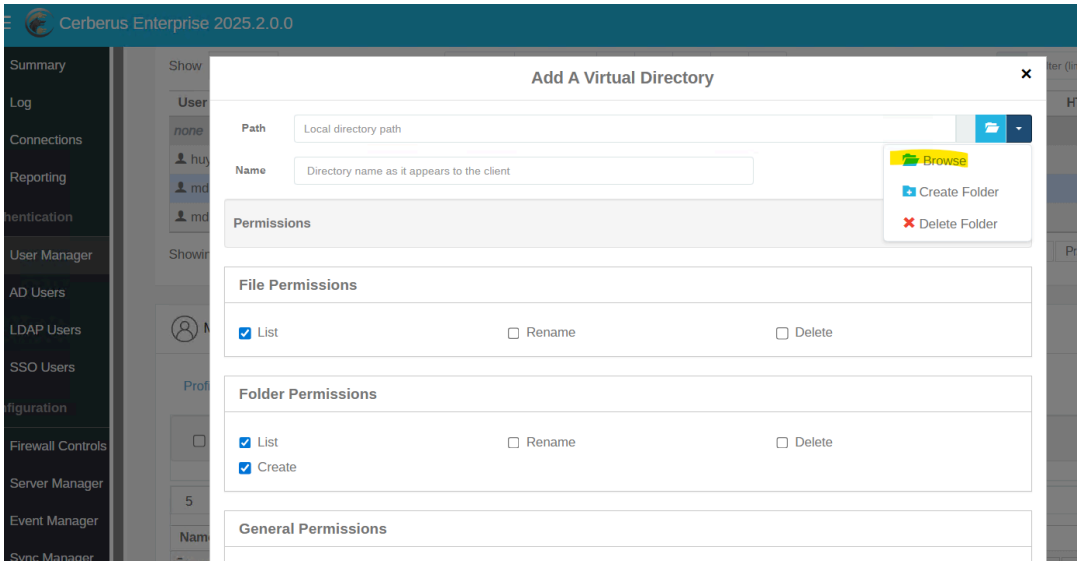
- Make sure Simple directory mode option is disable

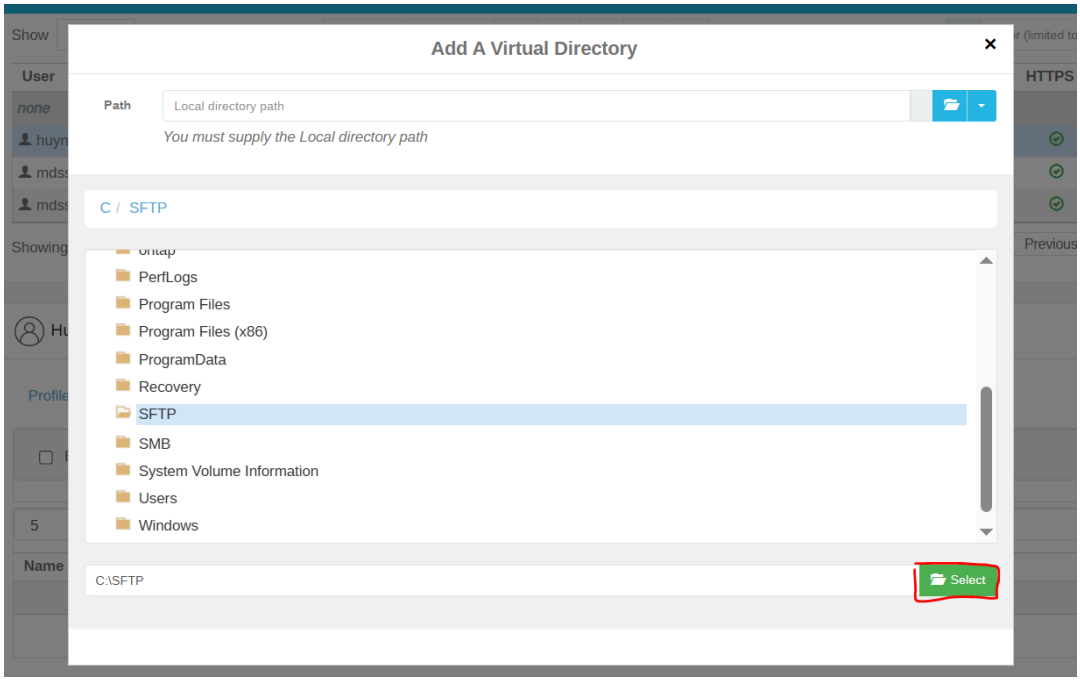


- Click New Virtual Directory

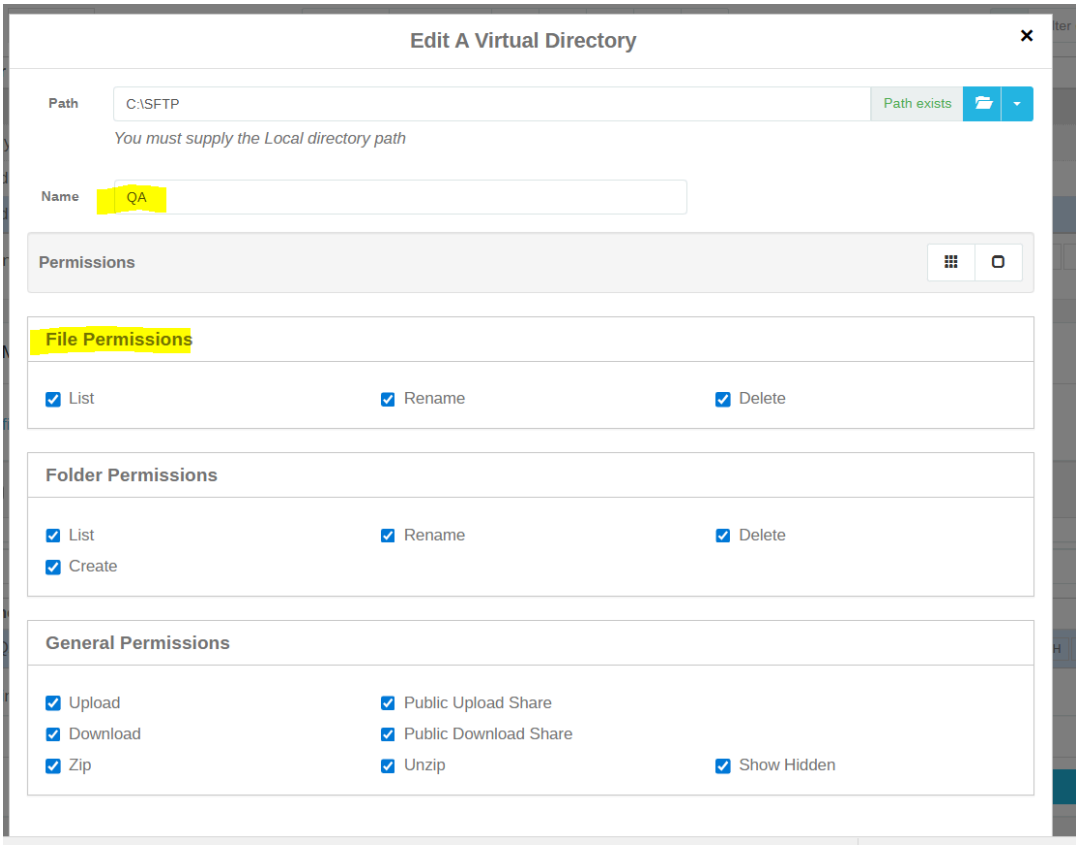


- Open “Browse” to choose the mapping directory from your Windows server or shared folder

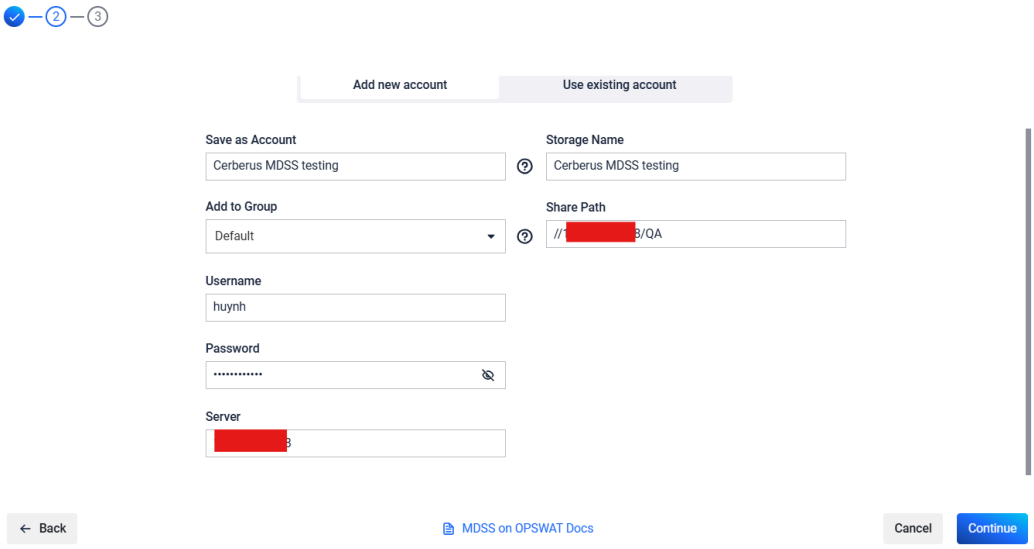




- Enter the shared name and give all permissions to the folder (save the shared name to configure later on from MDSS)



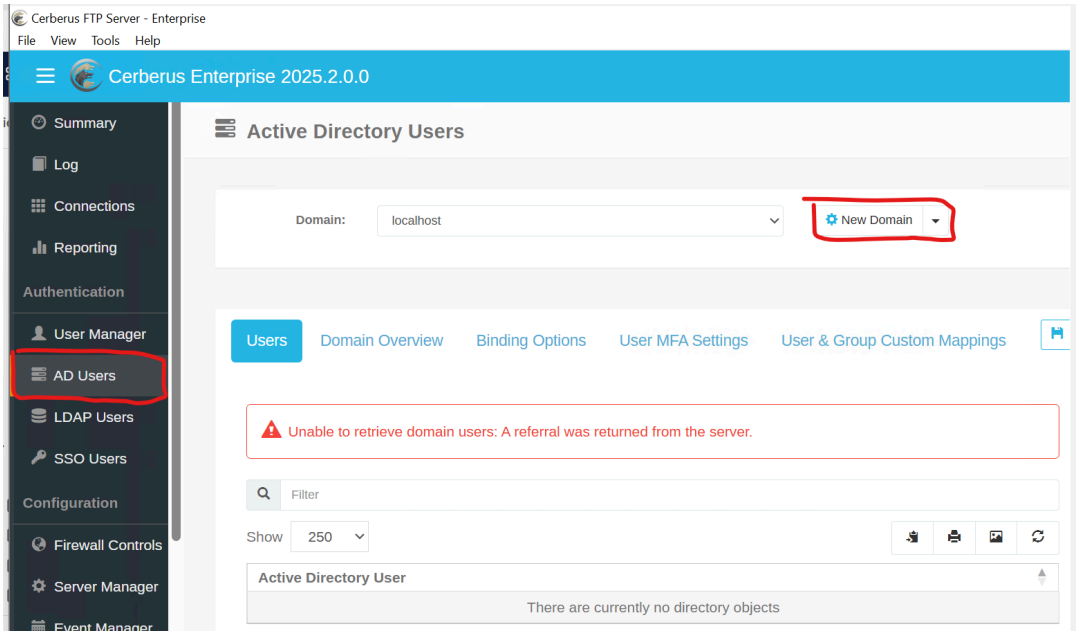
- Now the shared path is good to go integrating with MDSS, we could try with WinSCP first to see if it works, share path should come with the format as //CerberusIP/Name as configured, username and password are the credentials configured to the folder.



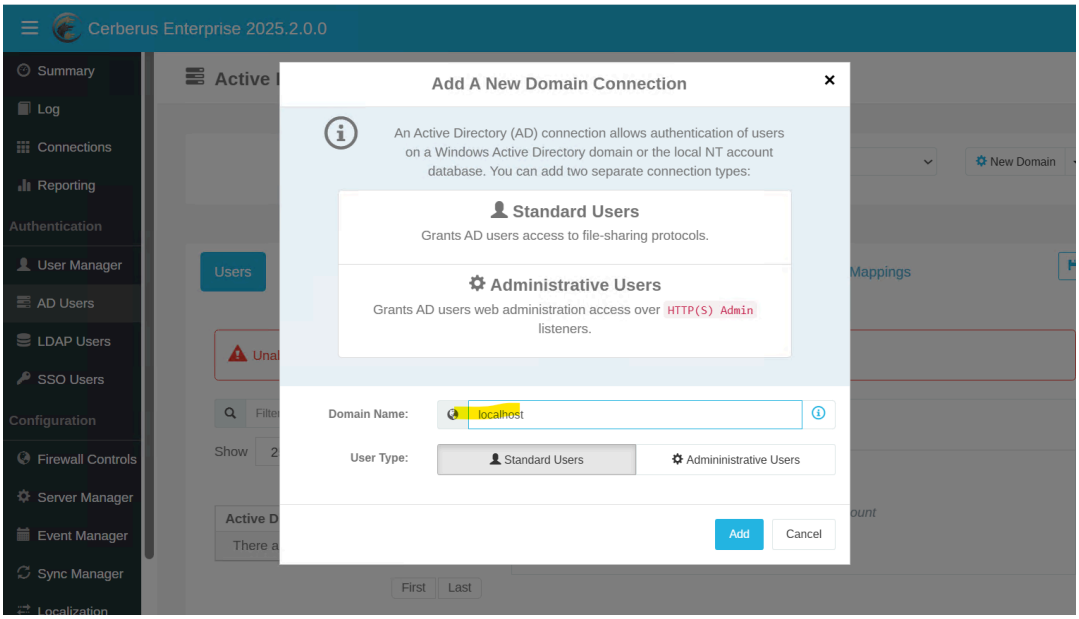
Mapping a shared folder with AD users via Cerberus group

As Cerberus is allowing AD integration, we could also integrate an AD or LDAP for users management

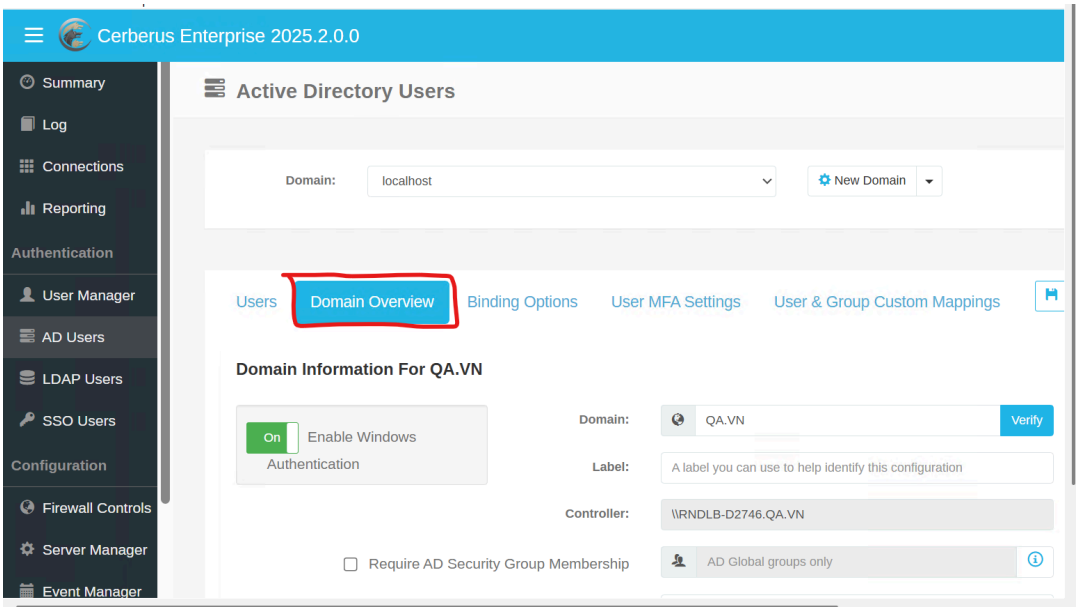
1. To add an AD, simply go to Authentication> AD users > Add New Domain



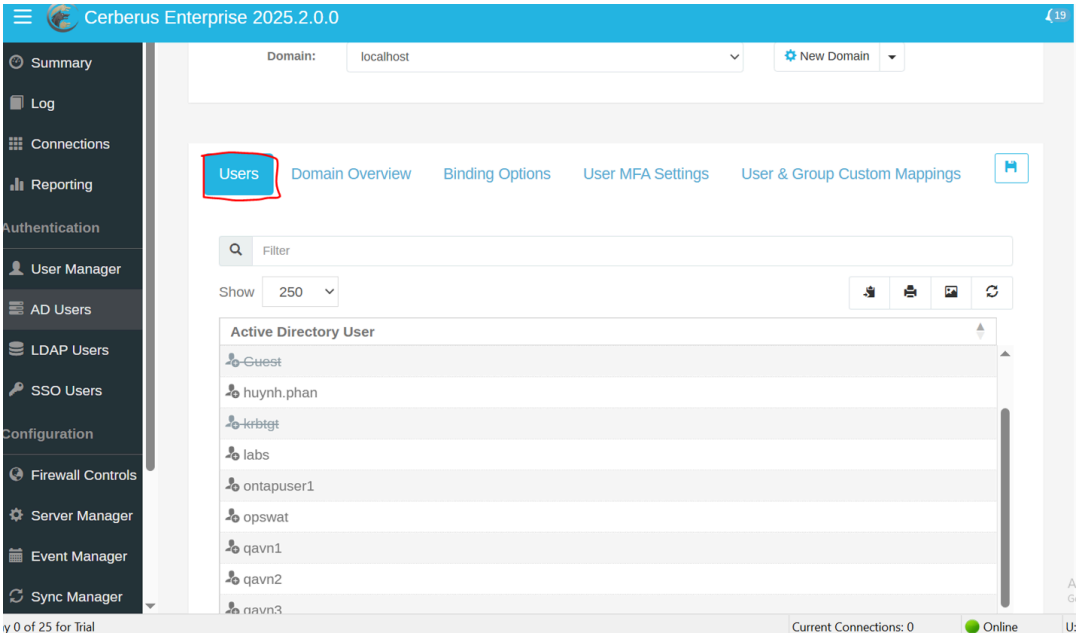
Fill in domain name



We could modify the domain later on after added

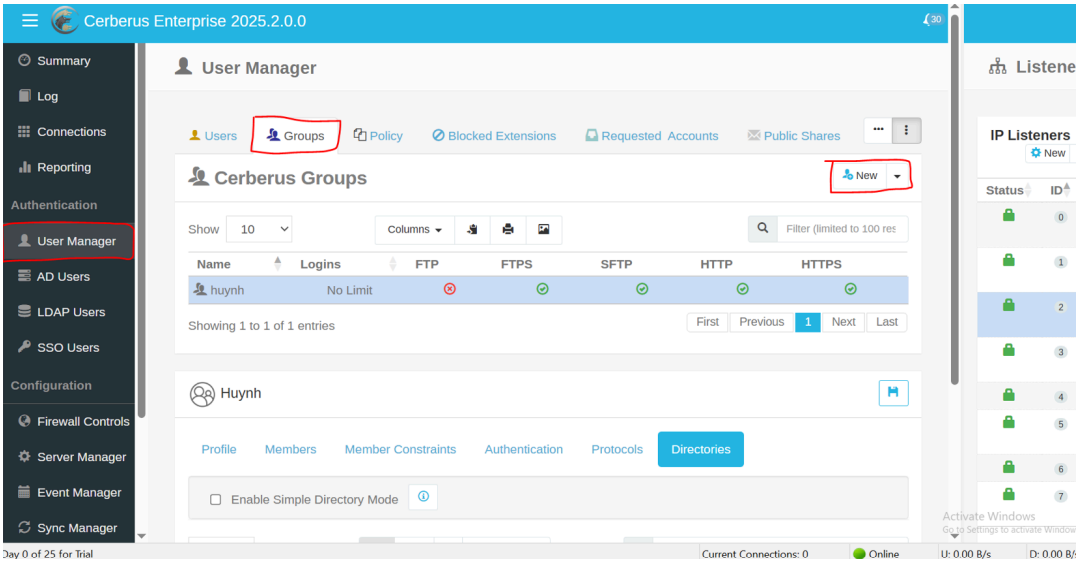


After connected successfully to the AD, the users list could be displayed at Users tab

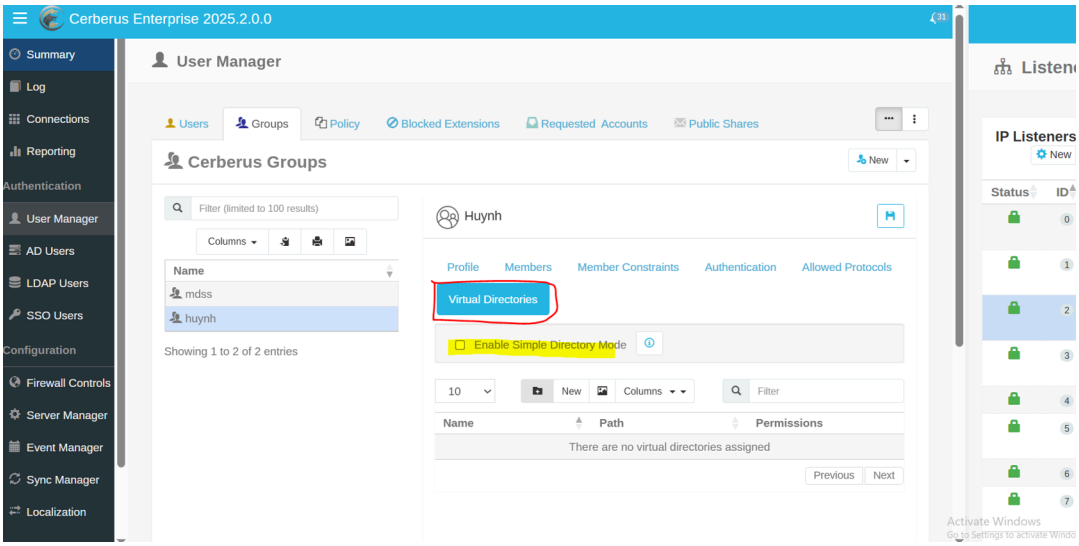


Synchronized AD users could be unable to map a Virtual Directory, to map a folder to multiple (AD) users, we could use a Cerberus group

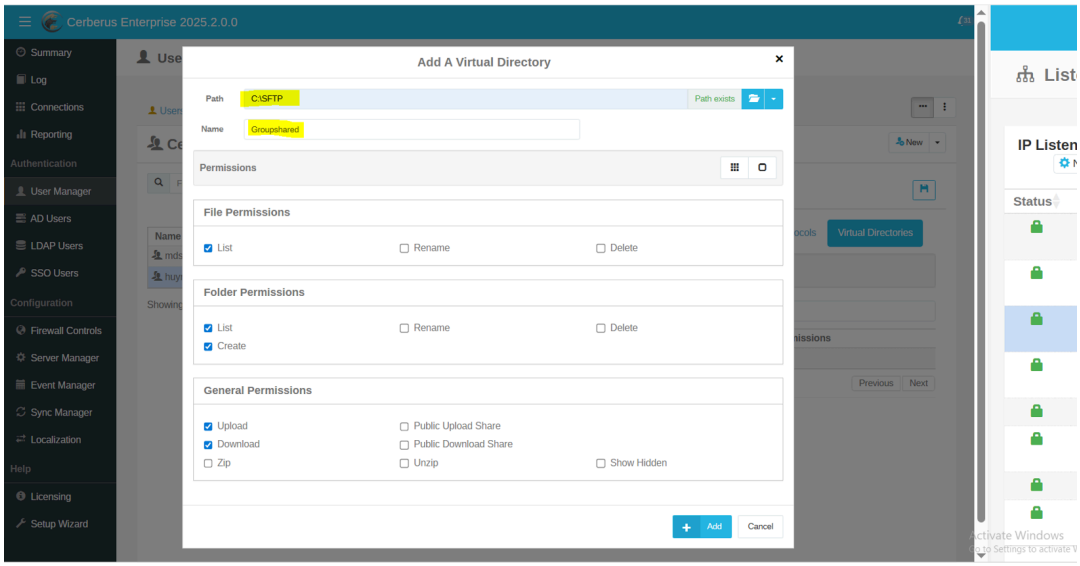
2. Add a group from User manager



3. Make sure Single mode is disabled at Virtual Directories tab for the group

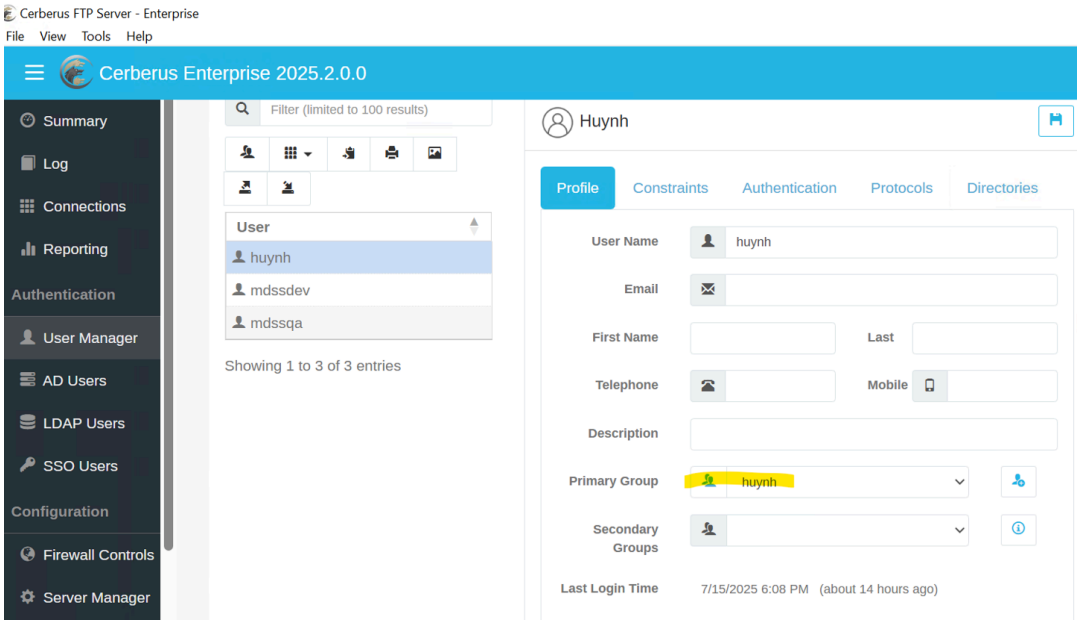


4. Create a New mapping, map a directory into the group

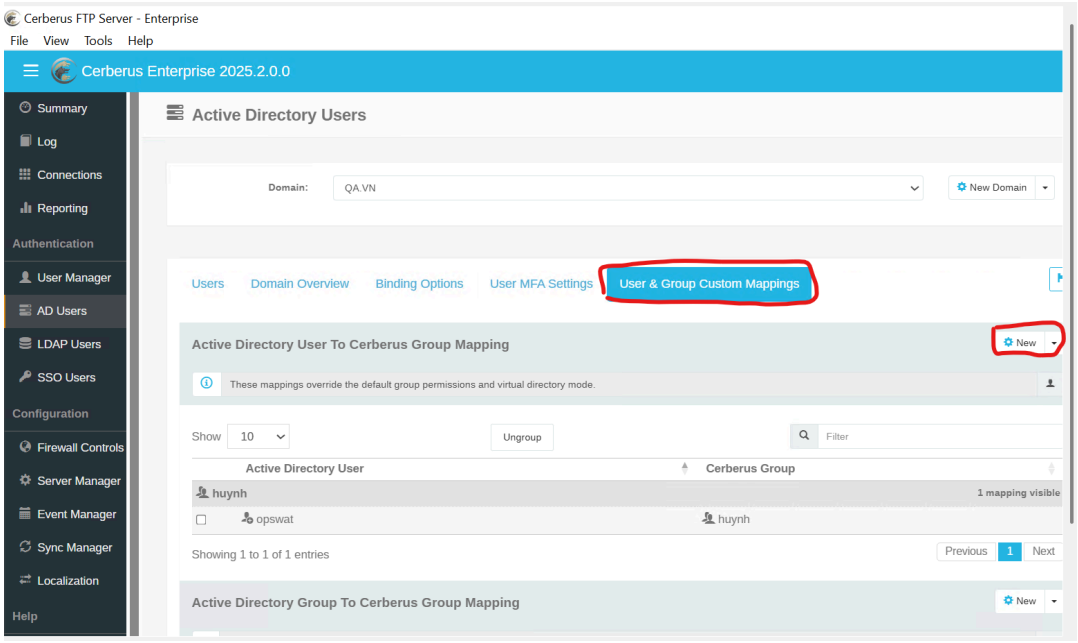


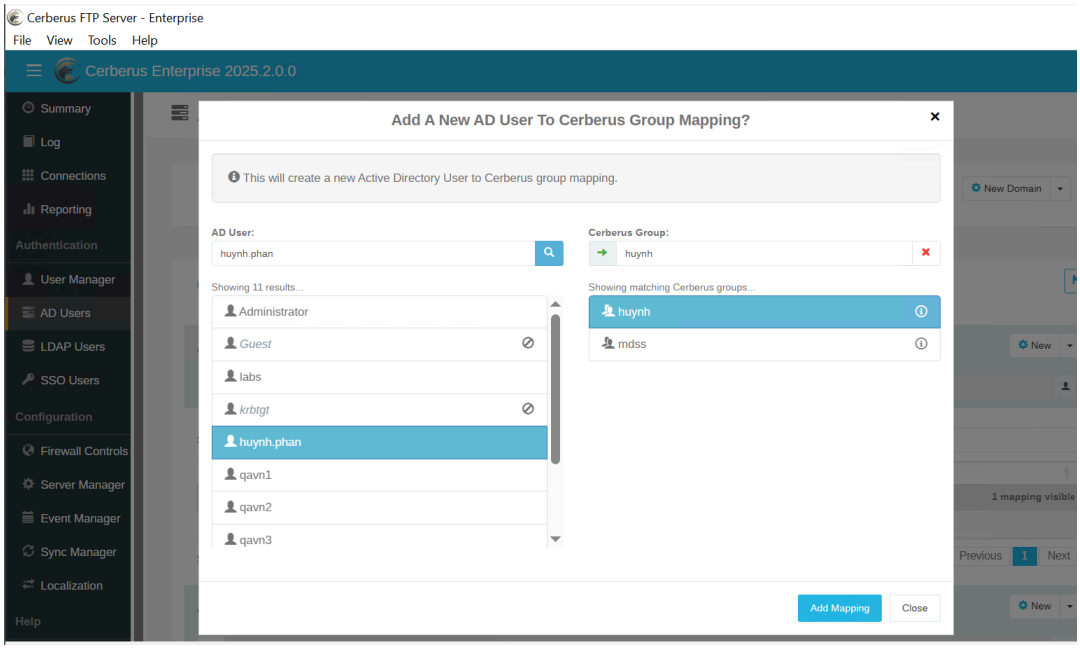
5. Assign the users into the created Cerberus group

a. Local users: go to User profile, and assign a primary group

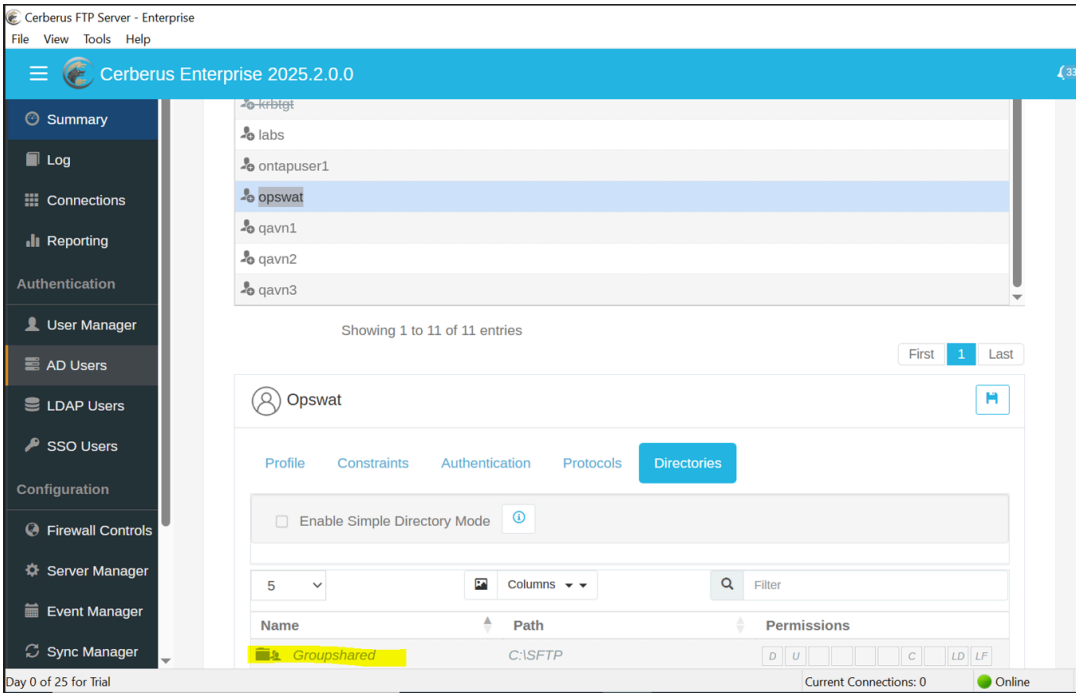


b. AD users





Head to the user's Directory, the group mapped folder should be displayed

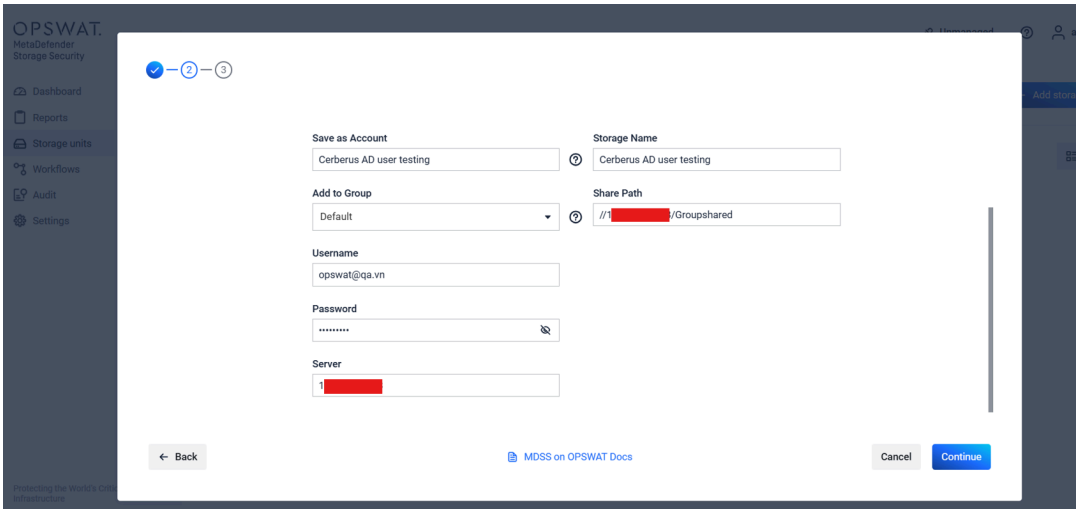


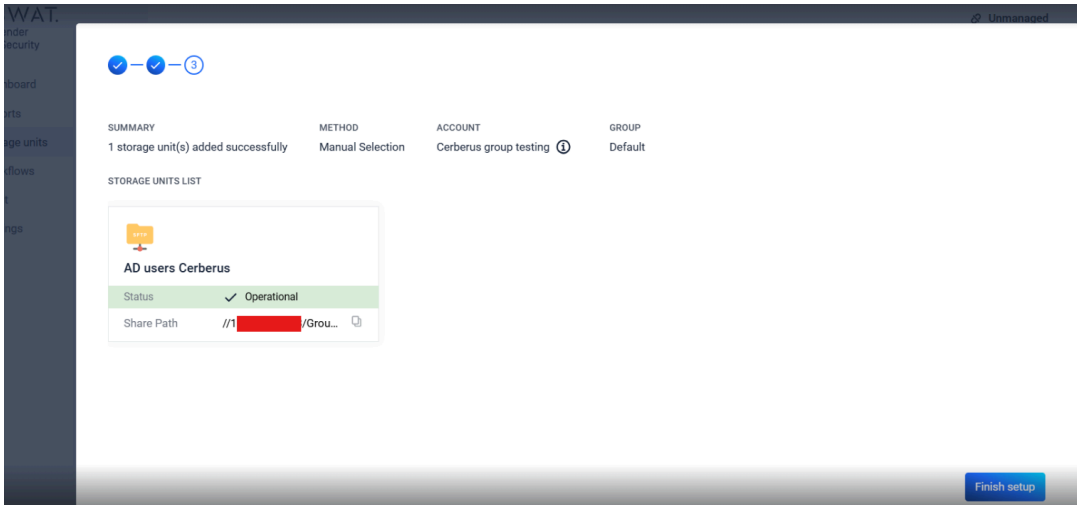
From then on, we could configure in MDSS the SFTP mapping Directory for the assigned users to the group with the share path format as //CerberusIP/Name

> **Info:**
>
> Format should be **username@domainame** for username

server:

Share Path ///Groupshared





Webhooks

We've prepared MDSS to be able to accept an API request sent by Cerberus

With the request, we need some information as well:

1. A header with an API key for auth
2. A payload containing a storageclient id and a metadata

Example:

```
{
"metadata": "{'Name': 'folder1/folder2/test-file.exe' }",
"storageClientId": '0c5454e3-d576-44c5-8ce4-cdc078011d0b'
}
```

> **Warning:**
>
> Scans with Deep CDR enabled have limited functionality, this is will be resolved in future releases.

> **Support:**
>
> If **Further Assistance** is required, please proceed to log a **support case or chatting with our support engineer**.

How to Handle SSL/TLS Issues with OPSWAT MetaDefender Core Webhook Callback?

Overview

This article describes how to resolve SSL/TLS certificate errors that can cause the webhook callback functionality to fail in OPSWAT MetaDefender Core version 5 on both Windows and Linux platforms.

Environment

OPSWAT MetaDefender Core version: 5

Supported Platforms: Windows, Linux

Problem Description

When the webhook callback functionality is invoked, it may fail due to SSL/TLS errors. The core.log file will contain an error similar to the following:

[core.webhook] SSL/TLS failed, issue='The issuer certificate of a locally looked up certificate could not be found, No certificates could be verified'

Root Cause

The webhook server's SSL certificate chain is not trusted by the operating system. This can occur if the intermediate or root certificate authorities are not installed in the local certificate store.

Resolution

Windows

1. Obtain the webhook server's SSL certificate chain (root CA, intermediate CA, and server certificate).
2. Open the Microsoft Management Console (mmc.exe).
3. Add the Certificates snap-in for the local computer.
4. Navigate to Trusted Root Certification Authorities > Certificates.
5. Import the root, intermediate and server certificates into the Trusted Root Certification Authorities store.
6. Restart the OPSWAT MetaDefender Core services:

- OSPWAT MetaDefender Core

After the service restart, the Trusted root certificates will be exported to a certificate located in the MetaDefender Core installation folder Data folder (by default C:\Program Files\OPSWAT\MetaDefender Core\data)

Linux

By default, MetaDefender Core loads root CAs from the following locations:

- /etc/ssl/certs/
- /usr/share/ssl/
- /etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem

Steps to import the certificates: __

Debian/Ubuntu

1. sudo cp -f <cert_file> /usr/local/share/ca-certificates/
2. sudo update-ca-certificates
3. sudo systemctl restart ometascan

CentOS/RHEL

1. sudo cp -f <cert_file> /etc/pki/ca-trust/source/anchors/
2. sudo update-ca-trust enable
3. sudo update-ca-trust extract
4. sudo systemctl restart ometascan

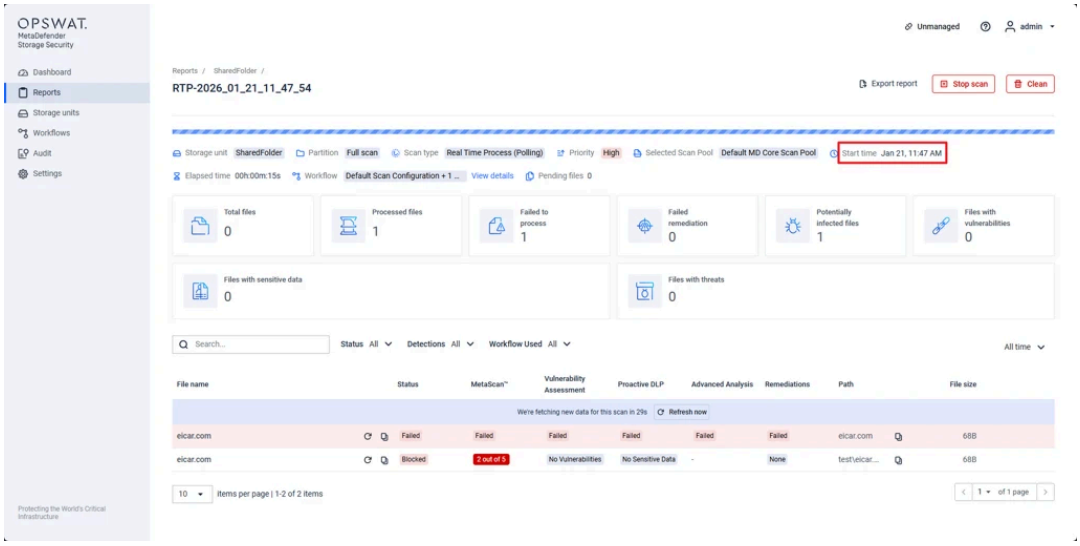
Validation

After completing the steps, trigger a webhook callback to confirm that the SSL/TLS error no longer occurs. Check the core.log for any remaining warnings or errors.

Why does MetaDefender Storage Security reset the RTP StartTime every day?

> **Check Your Version:**
>
> This article applies to all MetaDefender Storage Security v4.2.0 deployed on Windows and Linux systems.

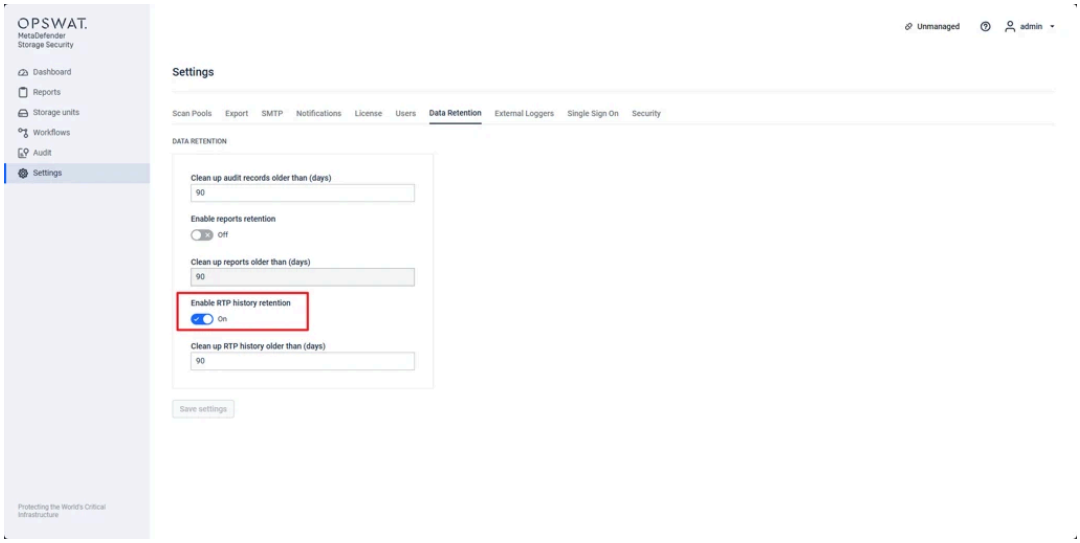
Issue: MetaDefender Storage Security resets the Real-Time Processing (RTP) Start Time every day.



Resolution: The reason for this behavior is enabling “Enable RTP history retention” under **Settings > Data Retention**.

This issue will be fixed in version 4.4.0.

Workaround: Currently, the workaround is to disable “Enable RTP history retention.”



> **Support:**
>
> If **Further Assistance** is required, please proceed to log a support case or chatting with our support engineer.

How to Exclude the OPSWAT Folder from Windows Defender?

> **Please Note**

> This article applies to MetaDefender Storage Security deployed on Windows systems.

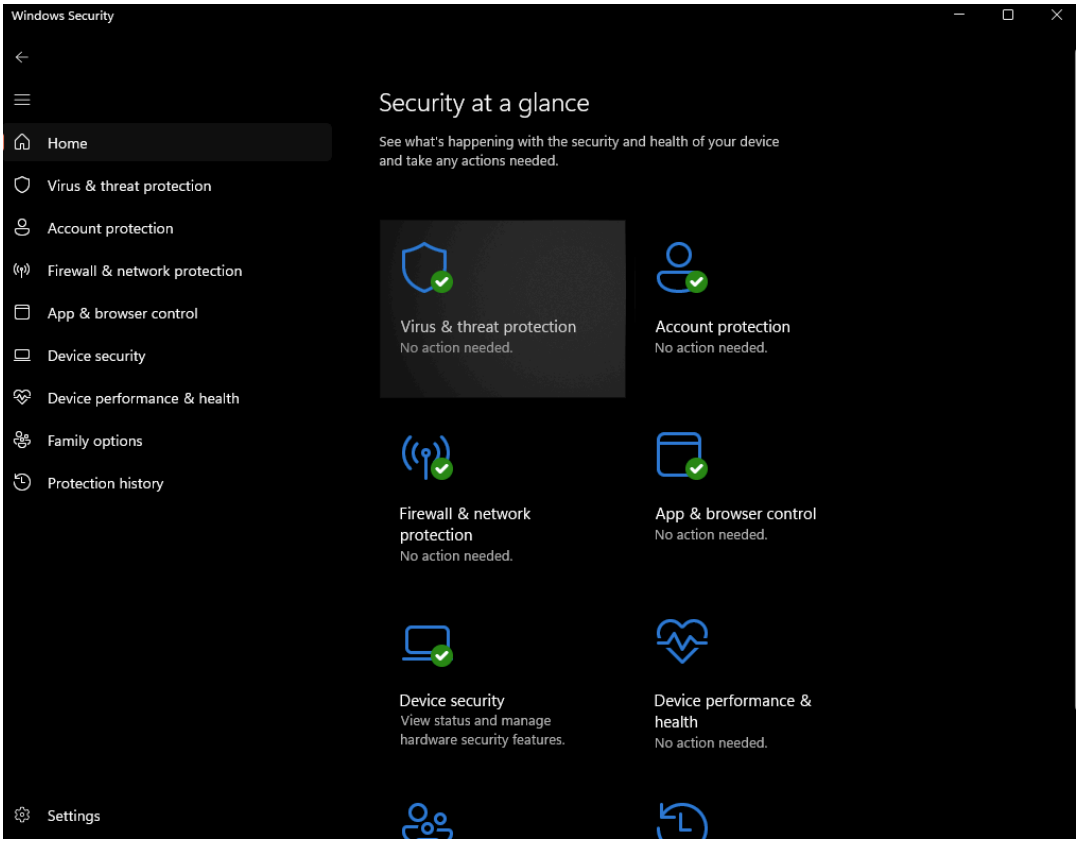
When using MetaDefender Storage Security deployed on Windows systems, it is important exclude the OPSWAT directory from **all** existing Anti-Malware software programs on the machine. Failure to exclude the OPSWAT directory can lead to performance degradation under high load, as the Anti-Malware software will also scan files that are streamed from the storage integration to MetaDefender Core, and may also slow down communication between certain components of the product.

Some common Anti-Malware software to perform these exclusions on are, including but not limited to: Windows Defender, McAfee, Norton, Bitdefender, Malwarebytes, SentinelOne.

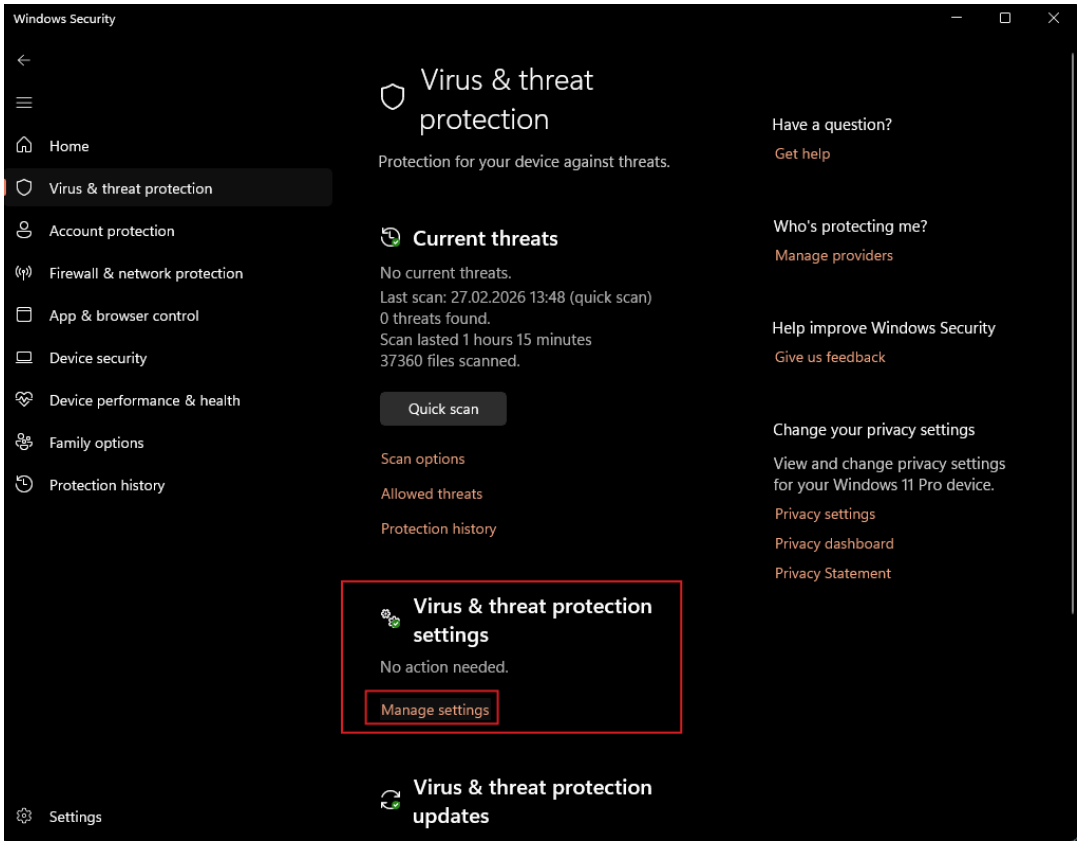
How to exclude on Windows Defender

Ensure you have **administrator privileges** before adding exclusions.

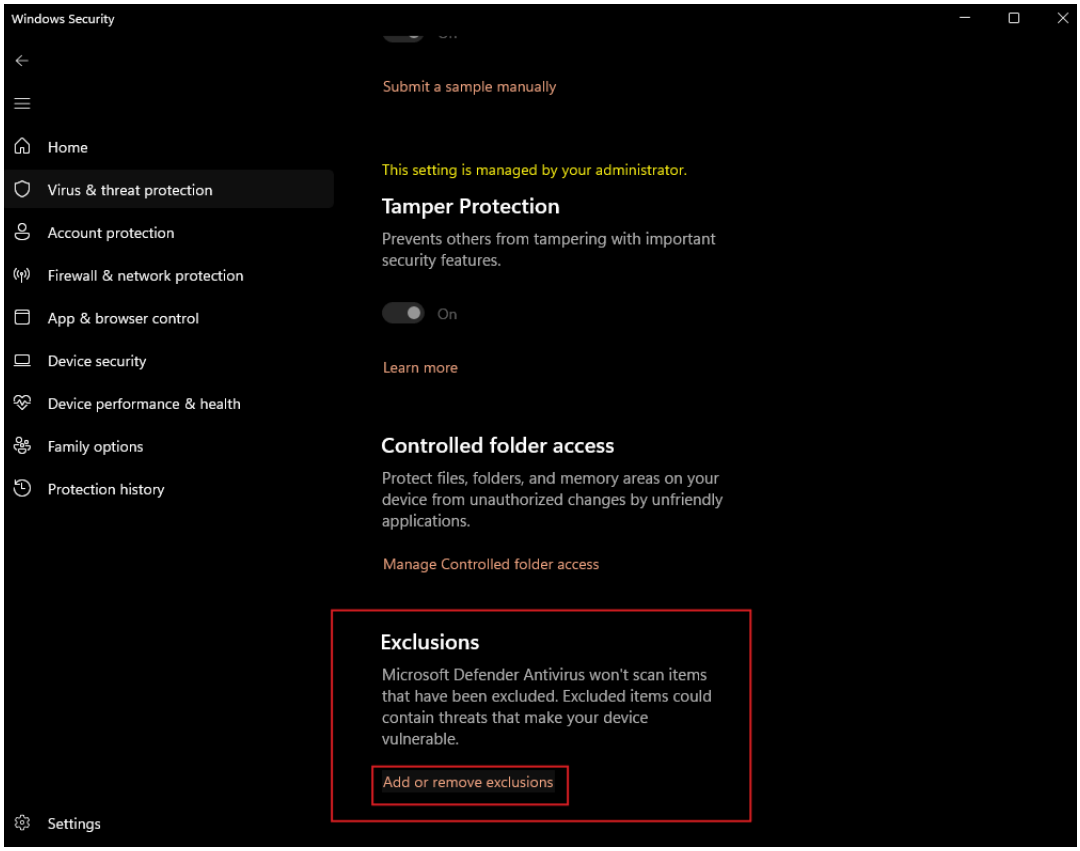
1. Navigate to “Windows Security” > “Virus & threat protection”



2. Under “Virus & threat protection settings” click “Manage settings”



3. Scroll down to “Exclusions” and click “Add or remove exclusions”



3. Add the “OPSWAT” folder. By default it is located in the installation directory: `C:\Program Files\OPSWAT`.
4. Add the “Temp” folder located at `C:\Users\<user>\AppData\Local\Temp`.

What are the Syslog Facilities and Levels in MetaDefender Storage Security?

> **Check Your Version:**
>
> This article applies to all supported versions of MetaDefender Storage Security.

A Syslog facility is a field within a Syslog message that identifies the source or category of the message, such as the kernel, mail system, or a specific application. This functions as a filter that actually instructs MetaDefender Storage Security to forward all the logs using the configured `Facility`.

These facilities, originally based on Unix processes and daemons, work with Syslog Levels (like Emergency, Critical, or Informational) to provide a more comprehensive way to manage and analyze logs in a system or network.

Numerical Code	Facility	Facility Description
0	kernel Messages	Messages generated by the operating system kernel
1	User Level Messages	Messages from user-level processes and applications
2	Mail System	Log entries related to mail servers and email processing
3	System Daemons	Messages from system daemons or background services
4	Security or Authorization Messages 1	Events related to user authentication and authorization, such as login or logout attempts
5	Internal Messages	Messages generated by the syslog daemon itself
6	Line Printer Subsystem	Messages concerning the printing system
7	Network News Subsystem	Log entries related to Usenet news services
8	UUCP Subsystem	Messages about Unix-to-Unix Copy (UUCP) communication
9	Clock Daemon 1	Messages from scheduled tasks or the cron daemon
10	Security or Authorization Messages 2	Private authentication-related events, often used for security-sensitive logs
11	FTP Daemon	Log entries for the FTP (File Transfer Protocol) service
12	NTP Subsystem	Messages from the Network Time Protocol daemon
13	Log Audit	General security-related events and authorization failures
14	Log Alert	Originating process or system component that sent a log message
15	Clock Daemon 2	-
16-23	Local User 0-7	User-defined facilities reserved for administrators or specific applications to

		use1414

> **Support:**
>
> If **Further Assistance** is required, please proceed to log a **support case or chat with our support engineer**.

How to protect the customer.env file in MetaDefender Storage Security?

> **Check Your Version:**
>
> This article applies to all MetaDefender Storage Security releases deployed on Windows and Linux systems.

The customer.env file stores the Postgres username and Postgres password in plaintext, these credentials are randomly generated at startup and are required for MetaDefender Storage Security to connect to the internal database that is not exposed outside of the machine.

Options for security:

- If you are connecting MDSS to an external database, it is recommended to setup **access control** for the external database at Client Authentication to ensure that only the server running MetaDefender Storage Security can access the database.
- The password must remain in plaintext, it cannot be hashed as it is sent in plaintext over the network, therefore ensure you have a **secure network**.
- Remove the `customer.env` file after MetaDefender Storage Security service starts, and place it back only when starting/stopping MetaDefender Storage Security service, or you may configure permissions for the file so that only authorized users have access to it, by default only **root user** has access to it.

> **Support:**
>
> If **Further Assistance** is required, please proceed to log a **support case or chatting with our support engineer**.

How Can I Improve Folder Discovery and Scanning Performance in MetaDefender Storage Security?

> **Check Your Product:**

> This article applies to all MetaDefender Storage Security releases deployed on Windows or Linux systems.

When using MetaDefender Storage Security (MDSS) to scan large or deeply nested folder structures, you may notice that the initial discovery process takes longer than expected. This article explains how MDSS performs folder discovery, why deep or complex directory structures can impact scanning speed, and how to optimize performance using event-based scanning.

The information provided applies to **all supported storage services** (e.g., Box, Amazon S3, Google Drive, local storage).

Discovery Service Workflow

MDSS uses a **Discovery Service** to locate and prepare files for malware scanning. The workflow proceeds as follows:

1. **Initial Discovery**
   - MDSS begins by enumerating all objects (files and folders) at the root level of the designated storage path.
2. **Analysis Phase**
   - Each discovered object is analyzed:
     - **Files** are immediately sent to MetaDefender Core for malware scanning.
     - **Folders** initiate a **recursive discovery** process, scanning their contents level by level.
3. **Sequential Traversal**
   - Discovery proceeds **hierarchically**, meaning that deeper folder structures take longer to complete because each subfolder is processed sequentially.

How to Improve Scanning Performance

If your environment contains a large number of folders or deep directory trees, the following methods can significantly reduce discovery and scanning time:

1. Implement Event-Based Scanning

Instead of relying solely on recursive discovery scans, use **Event-Based scanning** (also known as Real-Time Protection) to process files as they are created or modified.

Benefits:

- Files are scanned immediately, without full-folder traversal.
- Reduces overall discovery and processing time.

- Optimizes resource utilization and system performance.

2. Limit the Scope of Initial Discovery

If full discovery is required:

- Target only critical folders.
- Adjust scan depth (if applicable).
- Schedule discovery tasks during off-peak hours to minimize performance impact.

Additional Resources

- **Event-Based Handling Overview**
- **Event-Based Request Format**

> **Support:**
>
> If **Further Assistance** is required, please proceed to log a **support case or chatting with our support engineer**.

How to create a PostgreSQL Database in AWS?

> **Check Your Version:**
>
> Affected product: MDSS 4.0.0 and newer

Overview:

MetaDefender Storage Security (MDSS) requires a PostgreSQL database to store configuration data, scan results, and operational metadata. This guide walks administrators through the complete process of provisioning a PostgreSQL instance on AWS (using Aurora or RDS), configuring the required database and permissions, and establishing the connection with MDSS.

Prerequisites

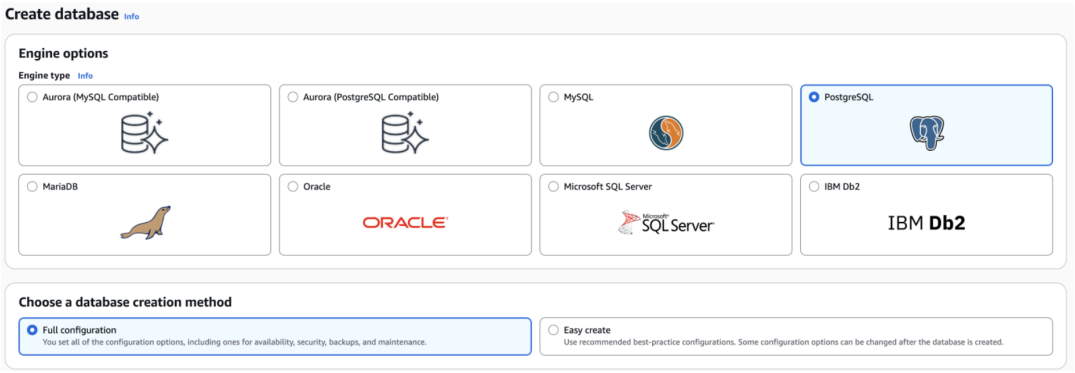
- An active AWS account with permissions to create RDS or Aurora PostgreSQL instances.
- Access to the target PostgreSQL server via pgAdmin or psql.
- MDSS 4.0.0 or newer installed, with access to its configuration files (customer.env).
- Network connectivity between the MDSS host and the AWS RDS/Aurora endpoint (security groups and firewall rules must allow traffic on port 5432).

Steps to configure:

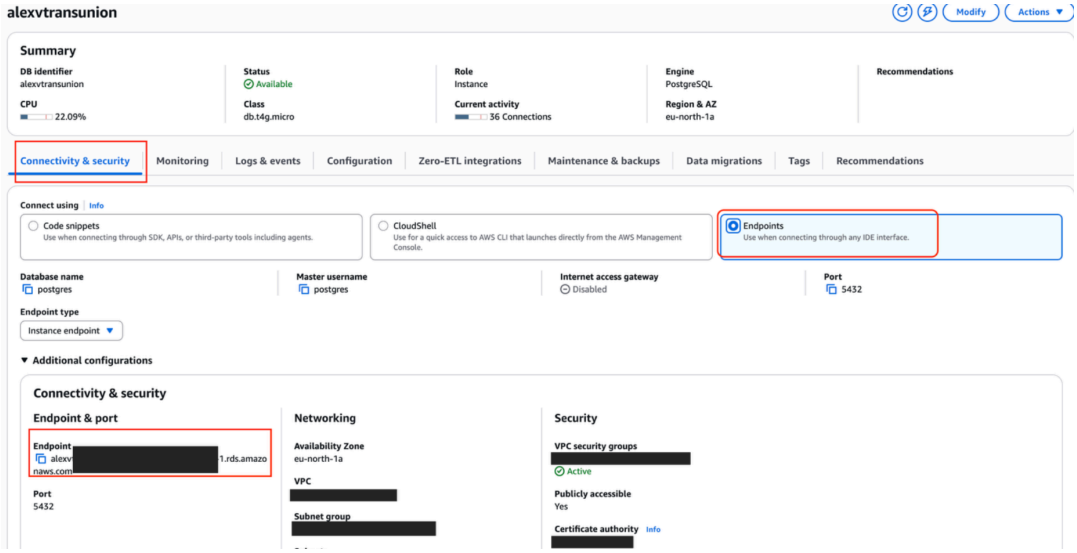
1. Create the PostgreSQL instance in AWS

In AWS, search for Aurora and RDS.

Select Create and choose full configuration.



After the instance is created, open the database details and copy the endpoint. This will be the PostgreSQL host. The default port is 5432. If the port has been changed, copy that value as well.

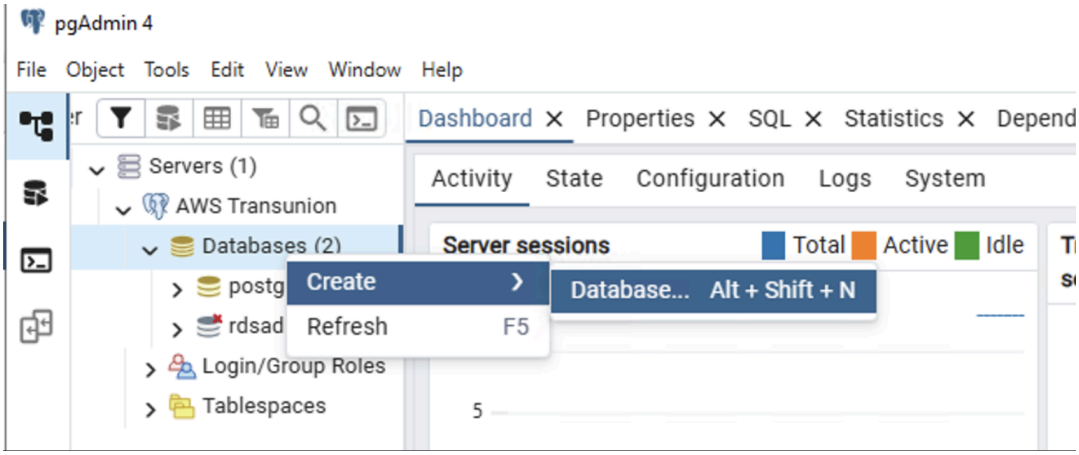


2. Create the MDSS database and assign permissions

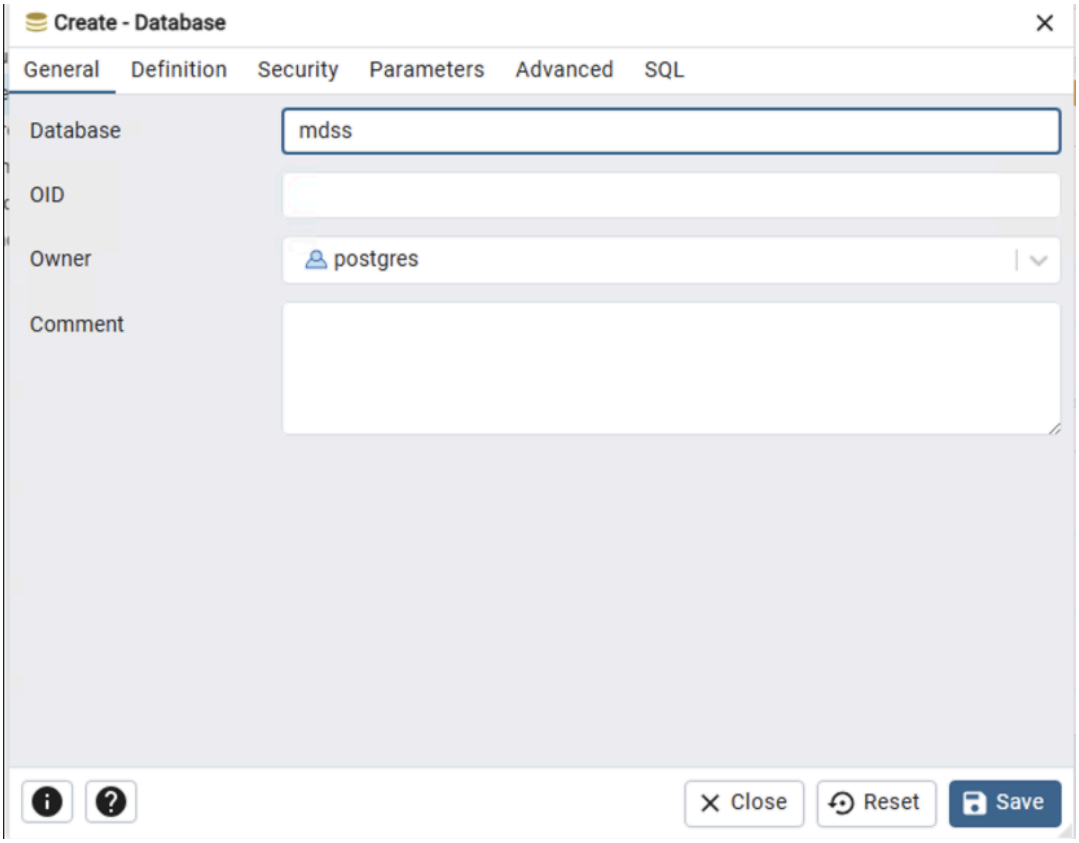
Option A: Using pgAdmin

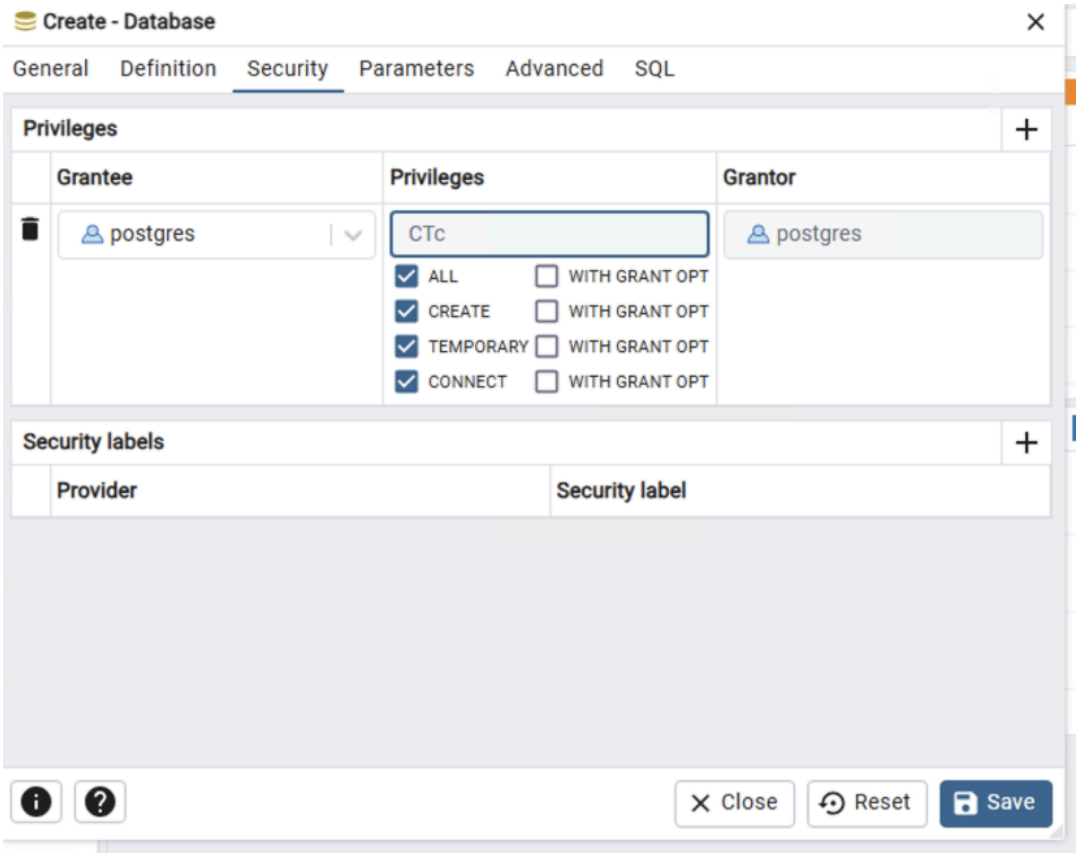
In pgAdmin, connect to the target PostgreSQL server.

Right-click Databases, then select Create > Database...



On the General tab, enter “mdss” as the database name. On the Security tab, assign the required privileges to the target user, then click Save.





Option B: Using psql

Use the following commands to connect, create the database, and grant the required permissions.

```
psql -h db.example.com -p 5432 -U myuser

 -- 1. Create database
CREATE DATABASE mdss;

 -- 2. Database connection
GRANT CONNECT ON DATABASE mdss TO myuser;

 -- 3. Schema permissions
GRANT CREATE, USAGE ON SCHEMA public TO myuser;

 -- 4. Full privileges on existing objects

GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA public TO myuser;
GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA public TO myuser;
GRANT ALL PRIVILEGES ON ALL FUNCTIONS IN SCHEMA public TO myuser;
GRANT ALL PRIVILEGES ON ALL PROCEDURES IN SCHEMA public TO myuser;

 -- 5. Default privileges for new objects
ALTER DEFAULT PRIVILEGES IN SCHEMA public
GRANT ALL PRIVILEGES ON TABLES TO myuser;

ALTER DEFAULT PRIVILEGES IN SCHEMA public
GRANT ALL PRIVILEGES ON SEQUENCES TO myuser;

ALTER DEFAULT PRIVILEGES IN SCHEMA public
GRANT ALL PRIVILEGES ON FUNCTIONS TO myuser;

 -- 6. For encryption extensions (if needed)
GRANT USAGE ON SCHEMA pg_catalog TO myuser;
```

3. Configure the new PostgreSQL server in MDSS

Add the connection details to customer.env.

```
POSTGRES_USER=user
POSTGRES_PASSWORD=password
POSTGRES_DB=mdss
POSTGRESQL_URL=Host=postgres;Port=5432;Username=user;Password=password;
Database=mdss
```

Save the file and start the MDSS service.

Verify functionality:

Once the MDSS service has started, use the following checks to confirm that the database connection is working correctly.

1. Check the database connection directly from the MDSS server

From the MDSS host or any machine with network access to the RDS/Aurora endpoint, run the following command to verify that the database is reachable and the credentials are valid:

```
psql -h <POSTGRES_HOST> -p 5432 -U <POSTGRES_USER> -d mdss -c
"\conninfo"
```

A successful response will display the connection details, confirming that the user, host, port, and database are all correct. If the connection fails, verify that the endpoint, credentials, and AWS security group rules are configured correctly.

2. Verify the MDSS web interface

Open a browser and navigate to the MDSS management interface. If the database connection is healthy, you will see the user configuration wizard. Any database connectivity issues will typically surface as a page showing errors connecting to the database.

> **Support:**
>
> If Further Assistance is required, please proceed to create a support case or chat with our support engineer.

How to set up Active Active configuration?

> **Check Your Version:**
>
> This article applies to all MetaDefender Storage Security version deployed in both Linux or Windows.

Summary: Guide for Configuring MDSS Active-Active Setup

Description: Below is a detailed guide to configure an Active-Active setup for MDSS, along with a recommended startup approach to ensure stability.

Step 1 — Deploy External Services

Set up the following services on dedicated servers (separate from MDSS nodes):

- **PostgreSQL** — Install and create the MDSS database and user
- **RabbitMQ** — Install and create a user with appropriate permissions
- **Redis** — Install and configure a password for remote access

Reference documentation: External Services Configuration - MetaDefender Storage Security

Step 2 — Configure MDSS to Use External Services

On each MDSS node, update the `/etc/mdss/customer.env` file:

```
# External RabbitMQ
RABBITMQ_URI=amqp://<user>:<password>@<rabbitmq_host>:5672
RABBITMQ_HOST=<rabbitmq_host>
RABBITMQ_PORT=5672
RABBITMQ_DEFAULT_USER=<user>
RABBITMQ_DEFAULT_PASS=<password>

# External Redis
CACHE_SERVICE_URI=<redis_host>:6379,user=default,password=
<password>,syncTimeout=10000
CACHE_SERVICE_URL=<redis_host>
CACHE_SERVICE_PORT=6379

# External PostgreSQL
POSTGRES_HOST=<postgres_host>
POSTGRES_PORT=5432
POSTGRES_DB=mdss
POSTGRES_USER=<user>
POSTGRES_PASSWORD=<password>
```

Step 3 — Disable Bundled Services

Since external services are used, disable the built-in services:

`DISABLED_SERVICES=postgres,rabbitmq,redis`

This ensures each MDSS node does not start local instances.

Step 4 — Start MDSS Nodes (Recommended Approach)

To ensure stable initialization:

1. Start only **one MDSS node** first
2. Verify all services are running properly
3. Perform a test scan (e.g., upload a sample file)
4. Once validated, start additional nodes using the same configuration

Step 5 — (Optional) Load Balancer

A load balancer is optional but recommended:

- Provides high availability for Web UI/API via a single endpoint
- Should include health checks (e.g., port 443)

Note: Not required for scanning, as workload distribution is handled via RabbitMQ.

How It Works

- File events (e.g., RTP) are published to the shared RabbitMQ queue
- The first available MDSS node processes the request
- All nodes share the same PostgreSQL database, ensuring consistent state and no duplicate scanning

> **Support:**
>
> If Further Assistance is required, please proceed to **create a support case or chat with our support engineer.**

AWS Lambda with S3 Trigger for MDSS Real-Time Processing

> **Prerequisites**
>
> Before proceeding with the Lambda function creation, ensure the following requirements are met:

1. IAM User Permissions

- The IAM user you are using for Lambda creation must have the following permissions, if you are using an admin user then ignore this:
  - Create Lambda functions
  - Assign IAM roles
  - Configure S3 triggers
  - Access the target S3 buckets

2. Account-Level Verification

- Confirm there are no account-level naming restrictions that would prevent your chosen Lambda function name

- Verify your AWS account has sufficient permissions and service quotas to create new Lambda functions in the desired region
- Ensure you have access to the target AWS region where the Lambda function will be deployed

3. S3 Bucket Configuration

- Verify that S3 bucket policies are configured to allow access from the Lambda function's execution role
- Required S3 permissions may include:
  - s3:GetObject - to read objects from the bucket
  - s3:PutObject - to write objects to the bucket (if applicable)
  - s3:DeleteObject - to delete objects from the bucket (if applicable)

4. IAM Execution Role

- Ensure you have a pre-configured IAM role with:
- Lambda execution permissions
- S3 access permissions for your target bucket(s)
- CloudWatch Logs permissions for function monitoring

Create IAM execution role for Lambda

First create a policy that will be used by the LAMBDA execution role.

Go to IAM → Policies → Create Policy. Give it a name, for example: MDSSLambdaS3AccessPolicy and use the following JSON

```
{
  "Version": "2012-10-17",
  "Statement": [

    {
      "Sid": "S3BucketListAccess",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::bucketname"
      ]
    },
    {
      "Sid": "S3ObjectAccess",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::bucketname/*"
      ]
    },

    {
      "Sid": "CloudWatchLogsAccess",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource": "*"
    }
  ]
}
```

Now we need to create an IAM role that will be used by the Lambda function

Got to

- IAM → Roles → Create Role
- Trusted entity: AWS Service → Lambda
- Attach policy: Attach the policy you created above MDSSLambdaS3AccessPolicy
- Role name: Give it a name, for example MDSSLambdaExecutionRole

Create Lambda Function

Now navigate lambda in AWS management console

Click “Create function”

- Select “Author from scratch”
- Function name: Example: MetaDefenderStorageSecurityProcessor
- Runtime: Select Python (choose the latest compatible version)
- Under change default execution role : Execution role → Use another role → select the role you created for lambda

Configure Advanced Settings (Optional but Recommended)

1. Expand “Advanced configuration”
2. Enable “Tags”
3. Add relevant tags for resource organization:

- Key: Purpose | Value: MetaDefenderScan
- Key: Environment | Value: Production/Development
- Key: Owner | Value: [Your Team/Department]

Click create function

Configure S3 trigger

In the newly created lambda Lambda go to → Configuration → Triggers → Add Trigger

Under trigger configuration -> select a source, choose S3 from the drop down

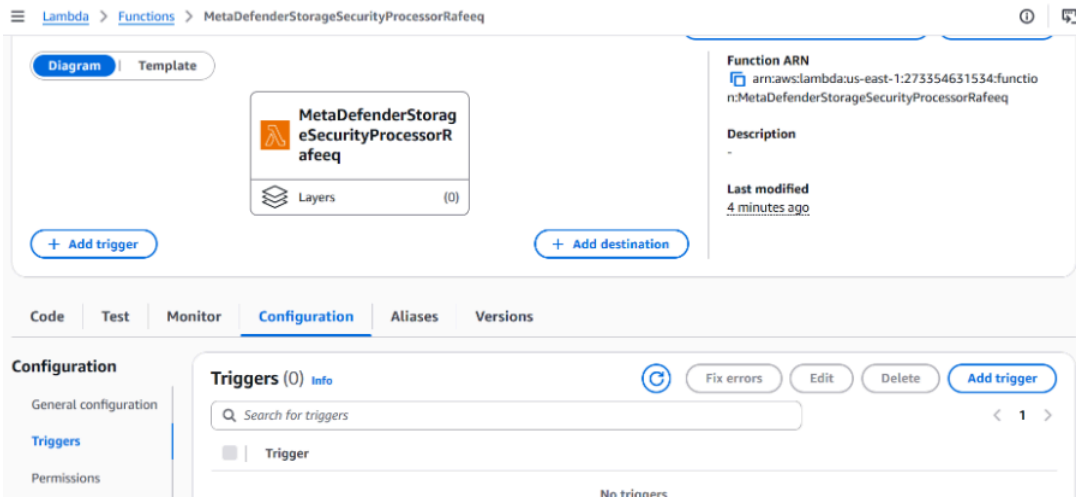
Select your bucket from the drop down

Under Event types: Choose the appropriate event type (Default is "All object create events” which will work for the Lambda). Alternative options: Object create, delete, or restore events based on your requirements.

Prefix (Optional): Specify a prefix to filter objects by path. Example: uploads/ to only trigger on objects in the uploads folder

Suffix (Optional): Specify a suffix to filter objects by file extension. Example: .pdf to only trigger on PDF files

Recursive invocation: Check this option to acknowledge potential recursive invocations

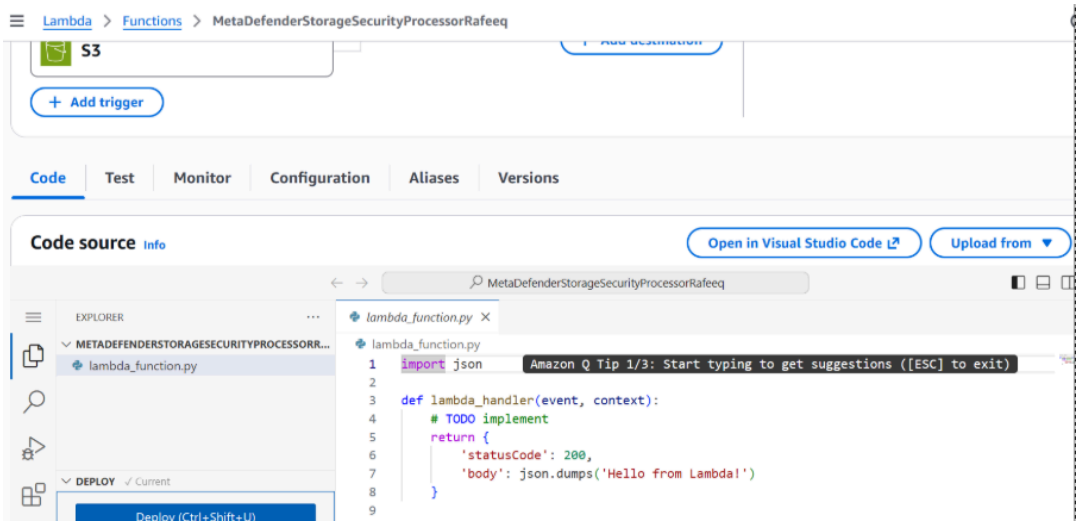


Click Add

Deploy Lambda Code

Now we need to update Lambda with the code that it should execute when it gets triggered

For that, go to code section of your lambda function



Delete the default code in there and copy paste the following code

```
import os
import json
import urllib.request
from urllib.parse import unquote
def lambda_handler(event, context):
    for eventRecord in event['Records']:
        eventRecord['s3']['object']['key']=
unquote(eventRecord['s3']['object']['key'].replace("+", " "))
        payload = {
            'metadata': json.dumps(eventRecord),
            'storageClientId': os.getenv('STORAGECLIENTID', "")
        }
        req = urllib.request.Request(
            url=os.getenv('APIENDPOINT', ""),
            data=json.dumps(payload).encode('utf-8'),
            headers={
                'ApiKey': os.getenv('APIKEY', ""),
                'Content-Type': 'application/json'
            },
            method='POST'
        )
        urllib.request.urlopen(req)
```

Click deploy to save your code

Configure environment variables for Lambda

Now we need to set environment variables for the lambda function so that we can configure MDSS endpoint with lambda

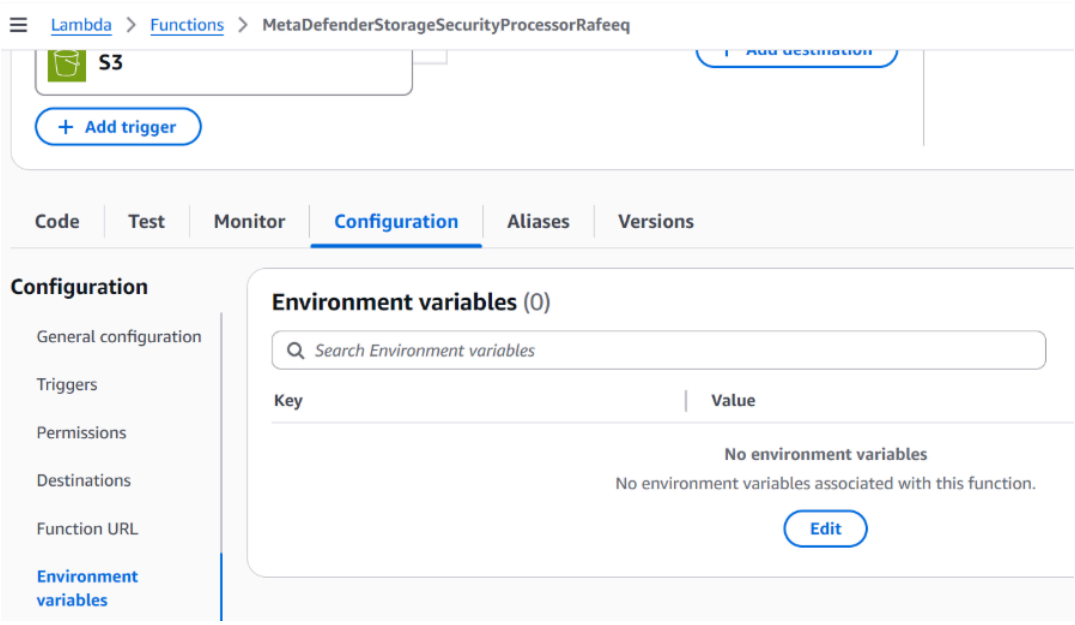
Go to environment variables under your lambda function

Add the following environment variables

APIENDPOINT – Your MDSS URL + /api/webhook/realtime Example: https://mdss-example.com/api/webhook/realtime

APIKEY – An api key generated from MDSS (Go to MDSS -> click on the dropdown next your profile -> click on profile information -> select configure api key -> click on generate api key -> click on copy and save)

STORAGECLIENTID -> Your storage client ID from MDSS. To obtain: Navigate to your desired storage configuration and copy the storageClientId (Click on storage units option in MDSS -> under listed storage units you will be able to see storage client ID and a copy button next to it)



Setup RTP scan on MDSS

Once lambda setup is done, we need to configure a new RTP scan on MDSS

Open MDSS web console → configure scan → select Real time processing → Type: Event based → select the storage unit → set priority → set optional scan name and partition → choose the workflow → Start RTP

Test

Upload a file to the s3 bucket and you should be able to see the file getting processed MDSS

How to configure SMTP server on MetaDefender Storage Security to send notification to Gmail mailbox?

> **Check Your Product:**
>
> This article applies to MetaDefender Storage Security releases version 3.3.0 or newer deployed on Windows or Linux systems.

To be able to send notification to your Gmail mailbox from MetaDefender Storage Security the following fields should be configured properly under MetaDefender Storage Security:

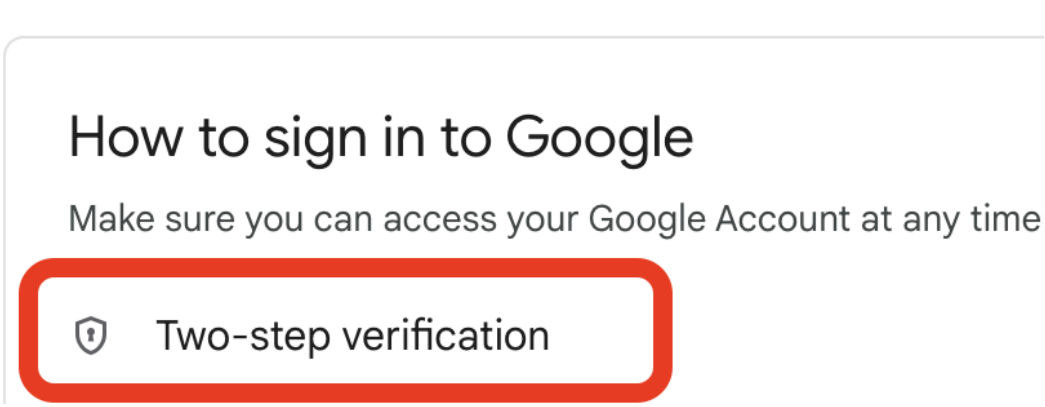
- HOST: smtp.gmail.com
- Port: 587
- Base URL: the address to use in the email for links; this address should point to the MetaDefender Storage Security web interface
- Sender email address (Optional): Ex.: MDSS_no-reply@test.com

- Sender name (Optional): Ex.: MDSS_No-Reply
- Username: username of the Gmail mailbox used for SMTP integration.
- Password: App password created for Gmail mailbox provided under “Email” field.
- Please choose a security option: Auto

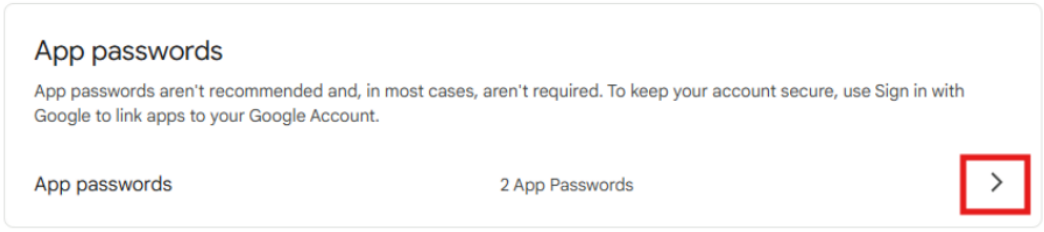
In order to achieve that, the following configuration should be done on Gmail mailbox account:

1. Create App password for Gmail account

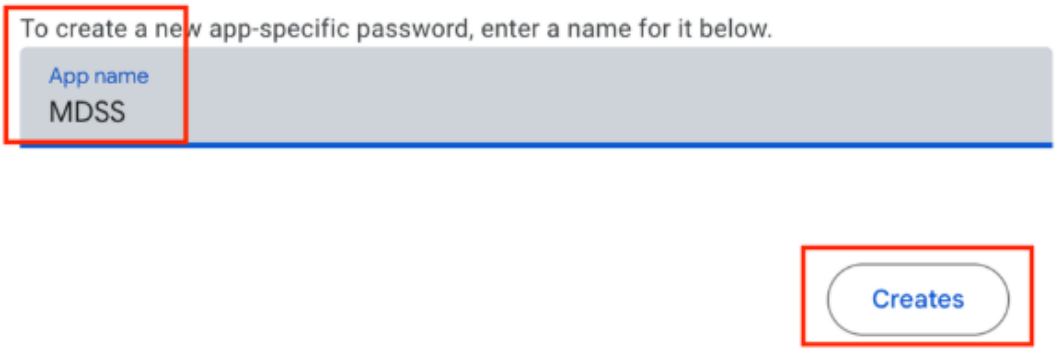
- Login to https://myaccount.google.com/security
- Under “Signing in to Google”:



- Click on Two-Step Verification
- Scroll down to section “App passwords” and click arrow in front of “App passwords”

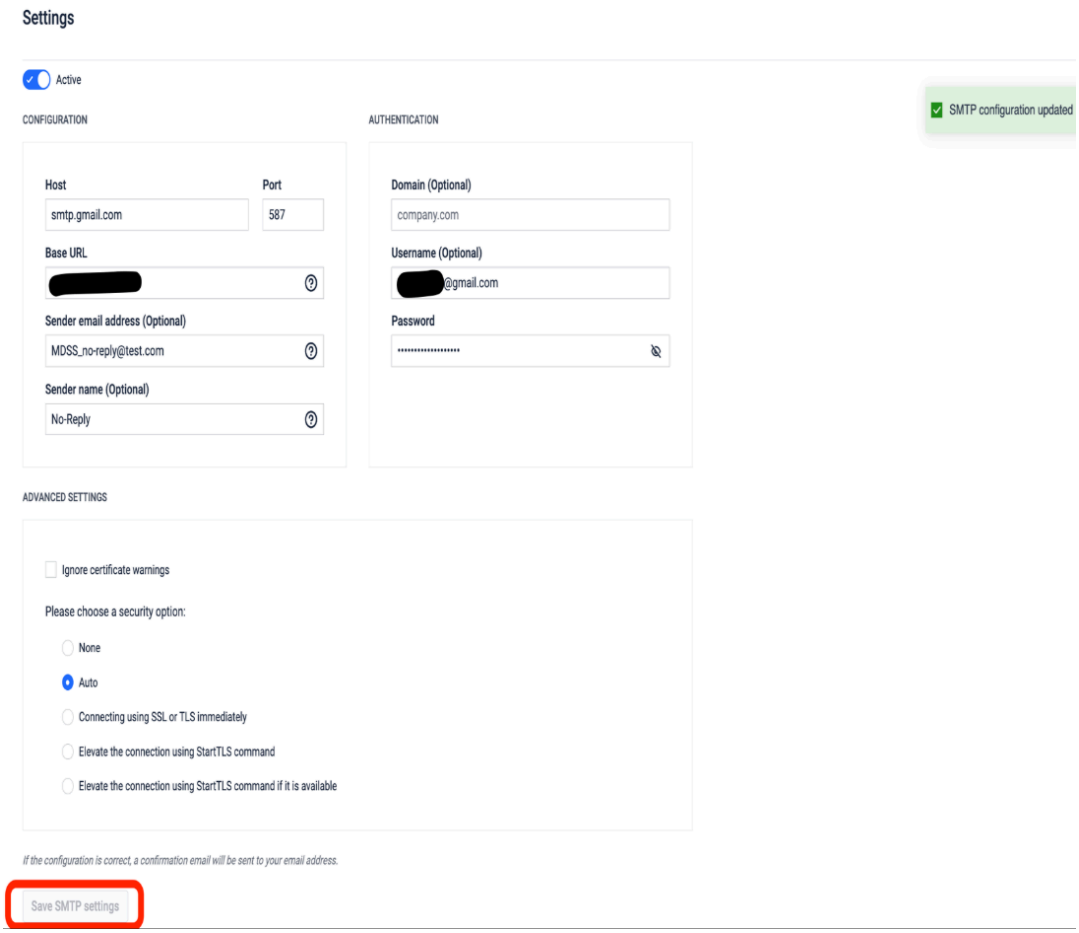


- In new page opened, write a name for your App password and click “Creates”



- Save the App password generated and click “Finished”. Further we will use the App password generated as password for mailbox used for MetaDefender Storage Security configuration as mentioned above and as in below example.

Example:



IMPORTANT: For field “Password” use App password created under Gmail account and not use the password which you use to login on Gmail mailbox.

> **Support:**
>
> If **Further Assistance** is required, please proceed to log a **support case or chatting with our support engineer**.

What are the Maximum and Minimum Data Retention Periods for MetaDefender Storage Security?

> **Check Your Version:**

> This article applies to all MetaDefender Storage Security releases deployed on Windows and Linux systems.

MetaDefender Storage Security allows you to define how many days scan reports are retained.

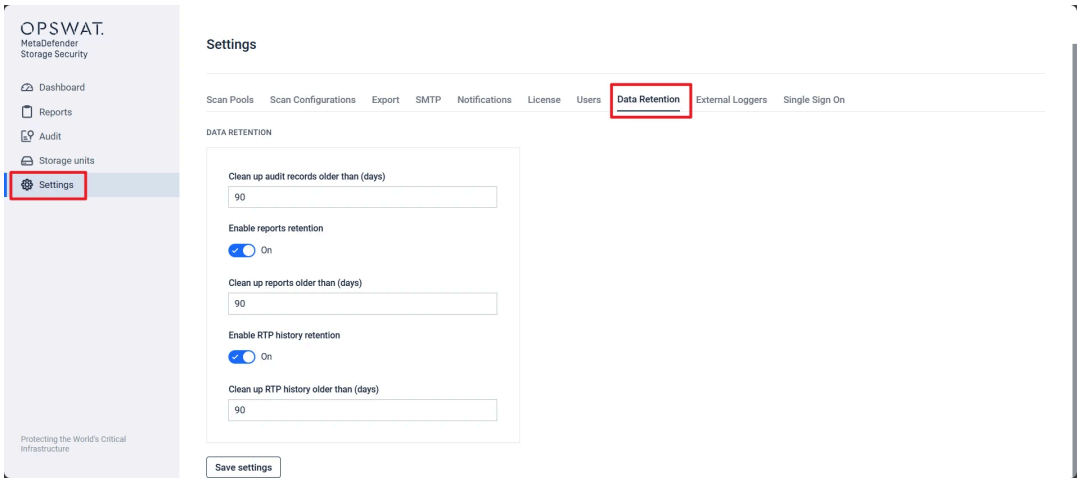
Data Retention Days Range

- **Maximum value:** 50,000 days
- **Minimum value:** 1 day

These values define the range you can enter when configuring the Data Retention Days setting in the MetaDefender Storage Security UI.

Steps to Configure

You can set the retention period by navigating to: Settings > Data Retention



For further details on data retention settings, refer to: Database Retention - MetaDefender Storage Security

> **Support:**
>
> If **Further Assistance** is required, please proceed to log a support case or chatting with our support engineer.

How to change PostgreSQL DB port used by MDSS

Steps

1. Stop MDSS Services

Open Services (services.msc) and stop the following:

- MDSS service
- PostgreSQL service
- Mdss_rabbitmq

2. Edit Configuration
3. Navigate to:

C:\Program Files\OPSWAT\MetaDefender Storage Security\config

2. Open customer.env in a text editor.
3. Update the following parameters:

POSTGRESQL_PORT=<new_port> # e.g., 5435
POSTGRESQL_URL=jdbc:postgresql://localhost:<new_port>/mdss

4. Save and close the file.
5. Refresh Environment
6. Open PowerShell as Administrator.
7. Run:

cd “C:\Program Files\OPSWAT\MetaDefender Storage Security\scripts” .\mdss.ps1 -c refresh

This refreshes environment variables and restarts MDSS services.

4. Start Services

If not already started, manually start the services stopped in Step 1.

5. Verify

Confirm MDSS is listening on the new port:

netstat -ano | findstr :<new_port>

6. Troubleshooting

- Check MDSS logs:

C:\Program Files\OPSWAT\MetaDefender Storage Security\logs

- Ensure no other application is using the new port.

> **Support:**
>
> If Further Assistance is required, please proceed to log a support case or chatting with our support engineer.

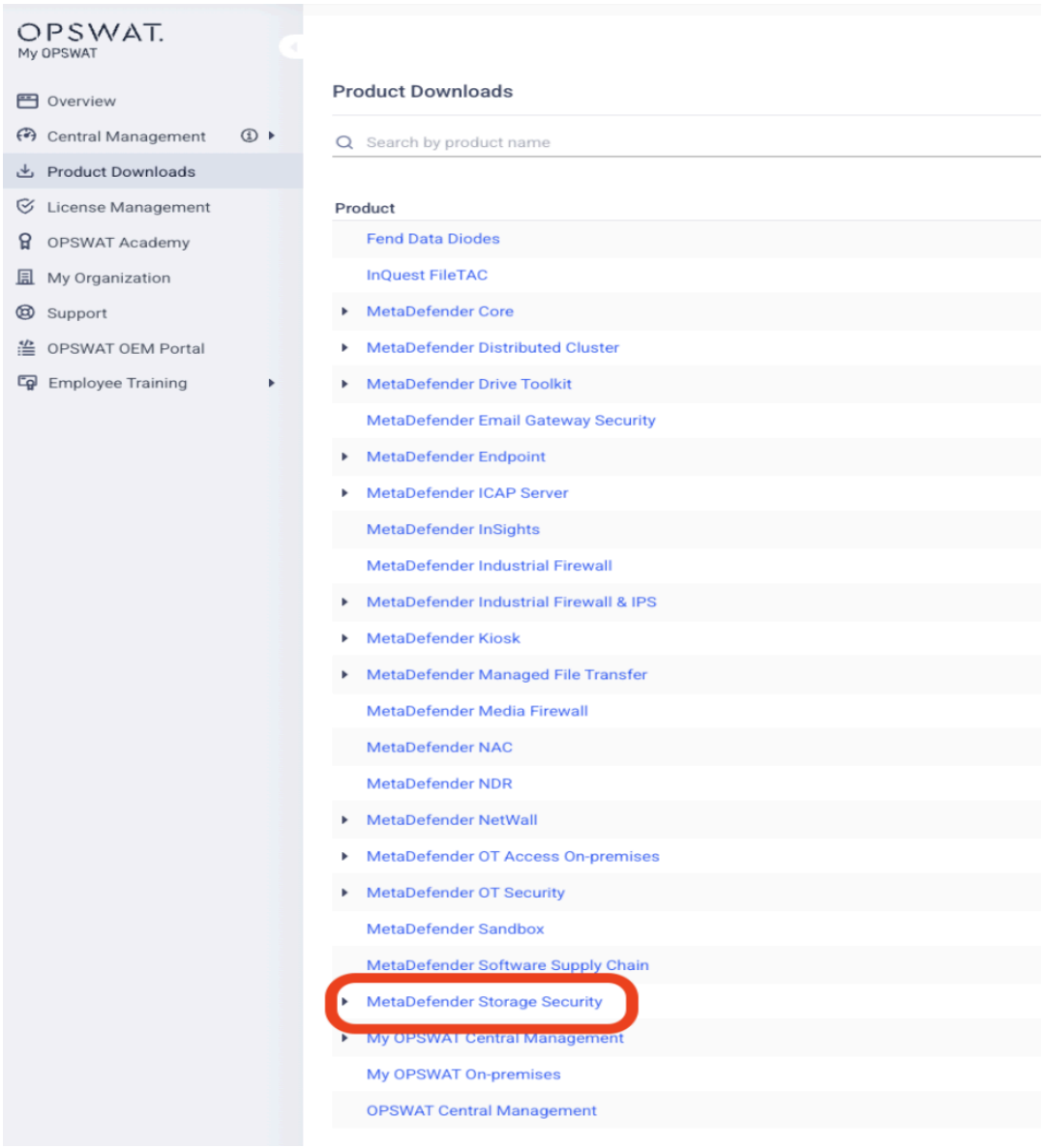
What is the latest MetaDefender Storage Security version?

> **Check Your Version:**
>
> This article applies to all MetaDefender Storage Security releases deployed on Windows and Linux systems.

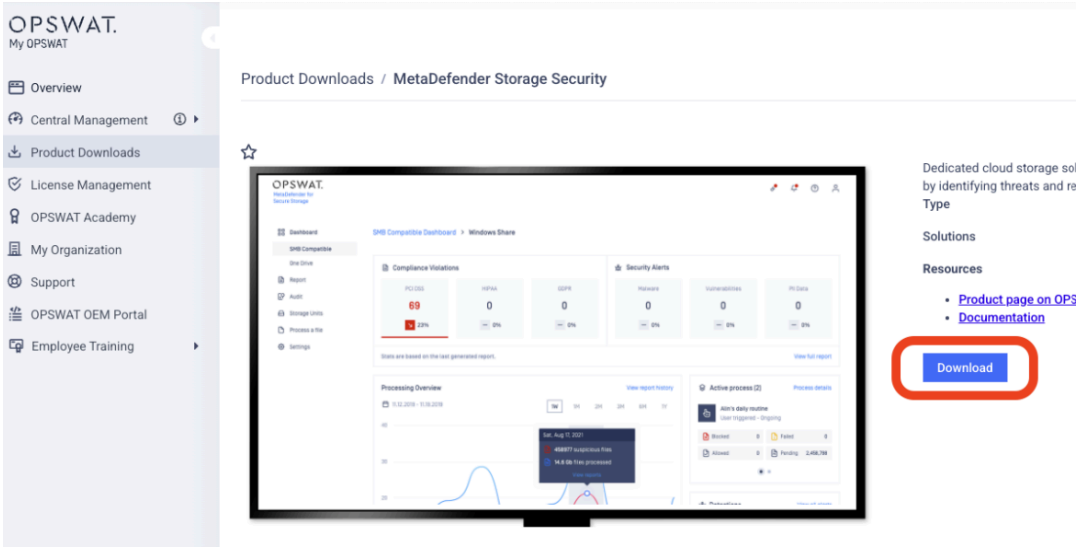
Browse MetaDefender Storage Security Release Notes for details on the latest version, version history, version comparisons and release notes.

Alternatively, go directly through the My OPSWAT for a list of available downloads.:

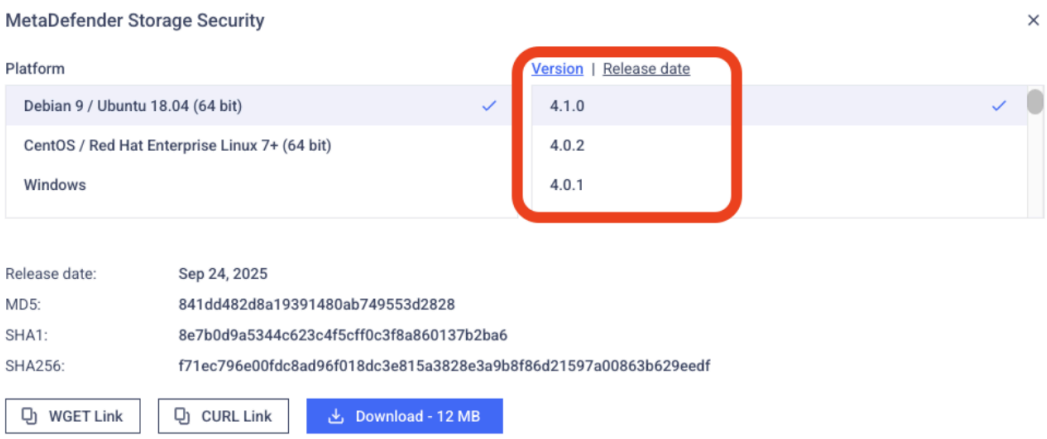
1. Login to My OPSWAT portal
2. Click on “MetaDefender Storage Security”



3. Click on “Download” button



4. In the new window opened, always the version from the top is the latest version



**Pro Tip: **

OPSWAT highly recommends that users upgrade to the latest version of MetaDefender Storage Security. Current versions incorporate state-of-the-art features and necessary bug fixes, and are freely available for all license holders to download.

Support:

Feel free to contact OPSWAT support for further guidance through your Upgrade process. Please follow these instructions on How To Create a Support Package, before logging a Support Ticket with the OPSWAT team.

Why is the Discovery Service becoming unresponsive due to RabbitMQ connection issues?

> **Check Your Version:**
>
> This article applies to MetaDefender Secure Storage version older than 4.1.0 deployed on Windows and Linux systems.

Issue:

The Discovery Service becomes unresponsive or stops working. Log entries show timeout and retry messages in the PublishHandler, along with RabbitMQ connection errors such as:

```
Already closed: The AMQP operation was interrupted
Close reason: code=406
```

Possible Causes:

- Missing or misconfigured target exchange in RabbitMQ.
- Transient network interruptions or broker restarts leading to dropped connections.
- RabbitMQ reaching connection or channel limits, causing timeouts.

Resolution:

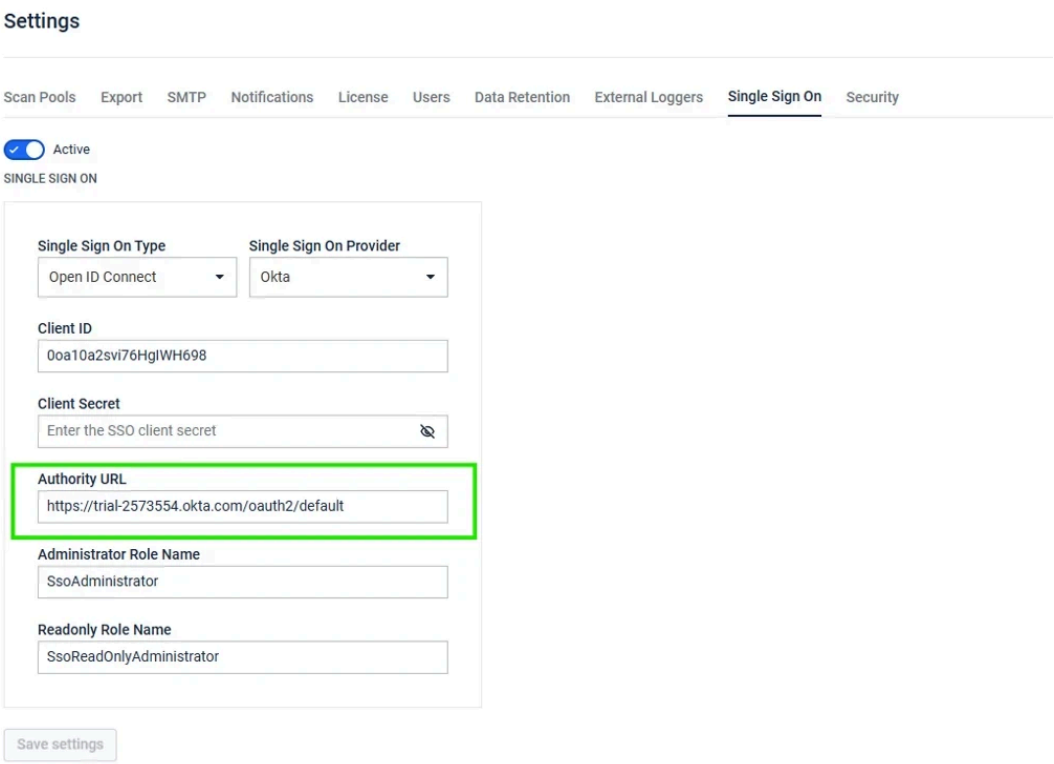
Upgrade the Helm chart to use MDSS version 4.1.0. This version includes fixes for Discovery Service stability and RabbitMQ connection handling.

> **Support:**
>
> If **Further Assistance** is required, please proceed to log a support case or chatting with our support engineer.

Changing the Authority URL in SSO will redirect to initial one

> **Check Your Version:**
>
> This article applies to Metadefender Storage Security V4.2.0

Issue: Once you update the **Authority URL** in the MetaDefender Storage Security SSO configuration page, save your changes, sign out, and then try logging in again via SSO. The system continues to redirect to the previous Authority URL.



Solution:

1. After changing the SSO configuration page with the new Authority URL and related data, save the settings.
2. **Restart MDSS:**

Windows : Restart the OPSWAT MetaDefender Security Storage service under Windows Services.

Linux: Restart the Metadefender Storage Security using the following command:

```
MDSS -c restart
```

Restarting the MDSS service clears the previously cached URL and forces MDSS to load the newly saved configuration.

Please note that this is fixed in MDSS V4.3.0.

> **Support:**
>
> If **Further Assistance** is required, please proceed to log a **support case or chatting with our support engineer**.

Scan Priorities & Throughput Tuning

> **Info**
>
> Available in **MetaDefender Storage Security 3.6.0** and later.

This guide explains how MetaDefender Storage Security (MDSS) controls **how fast** your storages are scanned, and how you can tune that speed. It covers three settings:

- **Scan Priority** (Low / Medium / High)
- **Prefetch Count** (`RABBITMQ_DISCOVERY_PREFETCH_COUNT`, `RABBITMQ_SCANNING_PREFETCH_COUNT`, `RABBITMQ_REMEDIATIONS_PREFETCH_COUNT`)
- **Consumer Multiplier** (`RABBITMQ_CONSUMER_MULTIPLIER`)

No prior knowledge of the internals is required — everything is explained with a simple analogy and worked examples.

How scanning works (in one minute)

When MDSS scans a storage, the work moves through an internal pipeline made up of three stages:

1. **Discovery** — MDSS walks through your storage and finds every file that needs to be scanned.
2. **Scanning** — each file found is then scanned for threats.
3. **Remediation** — when a file needs action (for example, a threat is found), MDSS applies the configured action to it, such as moving, deleting, or quarantining the file.

All three stages process files using parallel **workers**. The settings in this guide simply control **how many workers run** and **how much work each worker holds at a time**.

> **Info**
>
> Moving-team analogy — used throughout this guide. Think of scanning your files like a team clearing a pile of boxes:
>
> - Workers (Consumer Multiplier) = how many movers are working.
> - Prefetch Count = how many boxes each mover carries per trip.
> - Scan Priority = how many movers you put on a job.
>
> More movers, each carrying more per trip = the pile clears faster — as long as you have enough people (your server's CPU and memory) to keep up.

---

1. Scan Priority (Low / Medium / High)

Every scan you start is given a **priority**. The priority decides how much processing power that scan receives relative to other scans. Higher-priority scans are automatically assigned **more parallel workers**, so they finish faster.

Priority	Relative processing power	Best for
Low *(default)*	Baseline	Routine, scheduled, or background scans where finishing time isn't critical
Medium	3× the workers of Low	Standard on-demand scans a user is actively waiting on
High	6× the workers of Low	Urgent, time-sensitive scans that must complete as quickly as possible

Key things to know:

- **Low is the default.** If you don't choose a priority, the scan runs as Low.
- **Priority is set per scan.** Two scans on the same storage can run at different priorities at the same time.
- **Higher priority does not pause lower-priority scans.** All priorities run in parallel — High simply gets many more workers, so it drains its queue much faster and effectively finishes ahead.

---

2. Prefetch Count

What it is: the number of files a **single worker** pulls and holds at one time before reporting them as done.

In the moving-team analogy, this is how many boxes each mover carries per trip. Carrying more per trip means fewer empty-handed walks back — the mover keeps working instead of waiting for the next box.

Setting	Controls	Default	Maximum
`RABBITMQ_DISCOVERY_PREFETCH_COUNT`	Discovery stage (finding files)	10	400
`RABBITMQ_SCANNING_PREFETCH_COUNT`	Scanning stage (scanning files)	10	400
`RABBITMQ_REMEDIATIONS_PREFETCH_COUNT`	Remediation stage (acting on files)	10	400

Effect of the value:

- **Too low (e.g. 1):** each worker finishes one file, then waits to be handed the next. Small idle gaps add up and reduce throughput.
- **Balanced (e.g. 10–50):** the worker always has the next files ready, so it never sits idle. Recommended for most deployments.
- **Too high (e.g. 400):** a single worker can hoard a large batch of files while other workers sit idle, and memory usage rises. Rarely beneficial.

> **Info**
>
> Example: `RABBITMQSCANNINGPREFETCH_COUNT=20` Each scanning worker keeps up to 20 files lined up. As soon as it finishes one, the next is already waiting — no time wasted asking for more work.

> **Info**
>
> Any value above the maximum (400) is automatically capped.

---

3. Consumer Multiplier

What it is: how many **workers** the service runs in parallel. This is how many movers you put to work at once.

Setting	Default	Maximum
`RABBITMQ_CONSUMER_MULTIPLIER`	1	10

The important detail: the multiplier is a **base number** that is automatically scaled up for higher priorities. You set one value, and MDSS applies it proportionally:

Priority	Workers created
Low	multiplier × 1
Medium	multiplier × 3
High	multiplier × 6

> **Info**
>
> Example: `RABBITMQCONSUMERMULTIPLIER=2`
>
> - Low-priority scans → 2 workers
> - Medium-priority scans → 6 workers (2 × 3)

- High-priority scans → 12 workers (2 × 6)

> **Info**
>
> This is exactly why High-priority scans are faster — they automatically receive 6× the workers of Low.

When to increase it: when scans are running slower than you'd like, files are clearly piling up, **and** your server still has spare CPU and memory. Each extra worker scans another file in parallel.

When to leave it at the default (1): most deployments. Raising it above 3–5 is rarely necessary and increases load on the system. Any value above the maximum (10) is automatically capped.

---

4. Putting it all together

The total number of files a stage can process **at once** is:

```
workers × prefetch count
```

Remember that the number of **workers** depends on both the multiplier *and* the priority (Low ×1, Medium ×3, High ×6).

A step-by-step tuning walkthrough

The best way to understand these settings is to follow a real tuning session. Imagine a customer scanning a large file share. We start with the out-of-the-box defaults and adjust one thing at a time, checking the effect after each change.

Iteration 0 — Start with the defaults

```
RABBITMQ_CONSUMER_MULTIPLIER     = 1   (default)
RABBITMQ_SCANNING_PREFETCH_COUNT = 10  (default)
```

Files the Scanning stage can process at once, per priority:

Priority	Workers (multiplier × tier)	Prefetch each	Files in progress at once
Low	1 [1×1]	10	**10**
Medium	3 [1×3]	10	**30**
High	6 [1×6]	10	**60**

> **Info**
>
> Observation: A High-priority scan completes reasonably fast, but a large Low-priority scan feels slow. Checking the server, CPU and memory still have plenty of headroom — so there's room to push harder.

Iteration 1 — Increase the prefetch count

Each worker is finishing its files and then waiting for the next batch. We give every worker a bigger armful by raising the prefetch count from 10 to 20:

```
RABBITMQ_CONSUMER_MULTIPLIER     = 1
RABBITMQ_SCANNING_PREFETCH_COUNT = 20   ← changed
```

Priority	Workers	Prefetch each	Files in progress at once
Low	1	20	**20** *(was 10)*
Medium	3	20	**60** *(was 30)*
High	6	20	**120** *(was 60)*

> **Info**
>
> Observation: Throughput roughly doubles and workers no longer sit idle between files. But the Low-priority scan still isn't keeping up with demand, and the CPU is still not fully used. The bottleneck now is the number of workers, not how much each one holds.

Iteration 2 — Increase the consumer multiplier

We add more workers by raising the multiplier from 1 to 2. This doubles the workers at **every** priority:

```
RABBITMQ_CONSUMER_MULTIPLIER     = 2    ← changed
RABBITMQ_SCANNING_PREFETCH_COUNT = 20
```

Priority	Workers (multiplier × tier)	Prefetch each	Files in progress at once
Low	2 (2×1)	20	**40** *(was 20)*
Medium	6 (2×3)	20	**120** *(was 60)*
High	12 (2×6)	20	**240** *(was 120)*

> **Info**
>
> Observation: Scanning is now fast at every priority — a High scan can move up to 240 files through scanning at once, 6× a Low scan. The CPU is now well used but not maxed out, which is the healthy target.

Iteration 3 — Tune the other stages if needed

Scanning is no longer the bottleneck, but the customer notices that after scanning, **acting on flagged files (remediation) is lagging behind**. Each stage has its own prefetch count, so we raise the remediation stage too:

```
RABBITMQ_CONSUMER_MULTIPLIER          = 2
RABBITMQ_SCANNING_PREFETCH_COUNT      = 20
RABBITMQ_REMEDIATIONS_PREFETCH_COUNT  = 20   ← changed
RABBITMQ_DISCOVERY_PREFETCH_COUNT     = 20   ← optional, if finding
files is also slow
```

> **Info**
>
> Observation: The whole pipeline — finding, scanning, and acting on files — now flows smoothly. Note that `RABBITMQCONSUMERMULTIPLIER` is a single setting that applies to all stages, while each stage has its own prefetch count, so you can fine-tune any stage independently.

When to stop

Keep increasing only while the queues are backing up **and** the server still has spare CPU and memory. The moment CPU approaches 80%, stop — adding more workers to a maxed-out server makes things slower, not faster. At that point the answer is more hardware, not bigger numbers.

---

5. Quick reference

You want to...	Do this
Finish a specific scan faster	Start it as **High** priority (6× the workers)
Run a non-urgent background scan	Leave it as **Low** (the default)
Speed up scanning overall (CPU has headroom)	Increase `RABBITMQ_CONSUMER_MULTIPLIER`
Smooth out workers that idle between files	Increase the relevant `*_PREFETCH_COUNT`
Speed up the **finding** of files	Tune `RABBITMQ_DISCOVERY_PREFETCH_COUNT`
Speed up the **scanning** of files	Tune `RABBITMQ_SCANNING_PREFETCH_COUNT`
Speed up **acting on** flagged files	Tune `RABBITMQ_REMEDIATIONS_PREFETCH_COUNT`

Default and maximum values

Setting	Default	Maximum
`RABBITMQ_DISCOVERY_PREFETCH_COUNT`	10	400
`RABBITMQ_SCANNING_PREFETCH_COUNT`	10	400
`RABBITMQ_REMEDIATIONS_PREFETCH_COUNT`	10	400
`RABBITMQ_CONSUMER_MULTIPLIER`	1	10

Important notes

- **These settings increase parallelism, not raw machine speed.** They help only when workers are waiting for work while your CPU and memory still have room to spare. On a server that is already at full CPU, raising these values will **not** help — add more resources instead.
- **Changing the environment variables requires a service restart** to take effect. Set them in the service's environment configuration (`.env` / `customer.env`).
- **Values above the maximum are automatically capped** to the limits shown above.

Service Instance Scaling on Linux

> **Info**

> This article is applicable only to MetaDefender Storage Security deployments that are running on **Linux**.
>
> Available in **MetaDefender Storage Security 4.4.0** and later.

This guide explains how to run **extra instances** of MetaDefender Storage Security (MDSS) services so your deployment can handle more work in parallel. It's an optional setting for larger or busier environments.

If you've read the Scan Priorities & Throughput Tuning guide, here's the key difference:

- That guide tunes how hard a **single** service container works (more workers, bigger batches).
- This guide adds **more containers** of the same service, so the work is shared across them.

> **Info**
>
> Analogy: if a single service container is a moving team clearing boxes, then instance scaling adds more teams — each with their own truck — all working the same job at the same time.

How it works

By default, each scalable service runs as **one** container. You can add up to **two extra** containers per service using the `*_ADDITIONAL_INSTANCES` settings.

The value is simply **how many extra containers to add on top of the default one**:

Value	Total containers that run
`0`	1 (default — just the original)
1	2
2	3 (the maximum)

The maximum is **2 additional** (3 total). Any higher value is automatically reduced to 2.

When MDSS starts, it reads these values and launches the extra containers automatically. They join the same workload and start sharing it immediately — no other configuration is needed.

What you can scale

There are two groups of services you can scale.

1. Central services

These are the core engines of the scanning pipeline:

Setting	Service	What it does
DISCOVERY_SERVICE_ADDITIONAL_INSTANCES	Discovery	Walks through your storage and finds files to scan
SCANNING_SERVICE_ADDITIONAL_INSTANCES	Scanning	Scans each file for threats
REMEDIATIONS_SERVICE_ADDITIONAL_INSTANCES	Remediation	Acts on flagged files (move, delete, quarantine, etc.)

2. Storage connectors (per integration)

Each storage type you connect to has its own connector container. You can scale each one independently, so you can add capacity only where you need it:

Setting	Storage type
AMAZONSDK_ADDITIONAL_INSTANCES	Amazon S3
AZUREBLOB_ADDITIONAL_INSTANCES	Azure Blob Storage
AZUREFILES_ADDITIONAL_INSTANCES	Azure Files
NFS_ADDITIONAL_INSTANCES	NFS
SMB_ADDITIONAL_INSTANCES	SMB / CIFS
SFTP_ADDITIONAL_INSTANCES	SFTP
FTP_ADDITIONAL_INSTANCES	FTP
MFT_ADDITIONAL_INSTANCES	Managed File Transfer (MFT)
BOX_ADDITIONAL_INSTANCES	Box
GRAPH_ADDITIONAL_INSTANCES	Microsoft 365 (OneDrive / SharePoint Online)
GOOGLECLOUD_ADDITIONAL_INSTANCES	Google Cloud Storage
ALIBABACLOUD_ADDITIONAL_INSTANCES	Alibaba Cloud OSS
ORACLESDK_ADDITIONAL_INSTANCES	Oracle Cloud Storage

> **Info**
>
> A connector is only scaled if that storage type is enabled in your deployment. Setting a value for a connector you don't use has no effect.

Examples

Example 1 — Default (no scaling)

```
SCANNING_SERVICE_ADDITIONAL_INSTANCES=0
```

One scanning container runs. This is the default and is right for most deployments.

Example 2 — Add one extra scanning container

```
SCANNING_SERVICE_ADDITIONAL_INSTANCES=1
```

Two scanning containers run and share the scanning workload — roughly doubling scanning capacity.

Example 3 — Scale the whole central pipeline

```
DISCOVERY_SERVICE_ADDITIONAL_INSTANCES=1
SCANNING_SERVICE_ADDITIONAL_INSTANCES=2
REMEDIATIONS_SERVICE_ADDITIONAL_INSTANCES=1
```

Discovery runs 2 containers, Scanning runs 3, and Remediation runs 2 — useful for a large, busy environment where every stage needs more throughput.

When should you scale instances?

Add instances when **a single container is already working at full capacity** and your server still has spare CPU and memory to run more containers.

A good order to follow:

1. **First, tune the single container** using the prefetch and consumer-multiplier settings (see *Scan Priorities & Throughput Tuning*). This is the simplest change and often enough.
2. **Then, add instances** if one container — even fully tuned — still can't keep up, and you have the hardware to run more.

If your server's CPU is already near 100%, adding more containers will **not** help — they'll compete for the same resources. In that case, the answer is more hardware (a bigger server, or additional servers), not more instances.

How to apply changes

1. Set the desired *ADDITIONAL INSTANCES values in your environment configuration (__customer.env*)*
2. Restart MDSS so the extra containers are created

> **Info**
>
> Changes only take effect after a restart, because the extra containers are created at startup.

Things to keep in mind

- **The default (0) is right for most deployments.** Only scale when you have a clear throughput need and spare hardware.

- **The maximum is 2 additional instances (3 total) per service.** Higher values are automatically capped.
- **Only the services listed in this guide can be scaled.** Other MDSS services are designed to run as a single instance and should not be duplicated.
- **More instances need more resources.** Each extra container uses additional CPU and memory. Make sure your server has the capacity before scaling.
- **Instance scaling and worker tuning work together.** You can both add instances *and* tune each container's workers/prefetch for maximum throughput.

How to move the location of the MetaDefender Storage Security services_logs folder?

> **Check Your Version:**
>
> This article applies to all versions of MetaDefender Storage Security Linux deployments.

Background

When dealing with disk space issues related to the logging created by MDSS in environments where MDSS default log partition might be highly restricted, MDSS supports the ability to use symlinks to point the logs folder to a different partition/location.

Steps

The following provides steps on how to add a symlink for the `/etc/mdss/services_logs` directory/folder:

1. **Change name of the current services_logs folder and it backup**

```
sudo mv services_logs/ services_logs_v1/
```

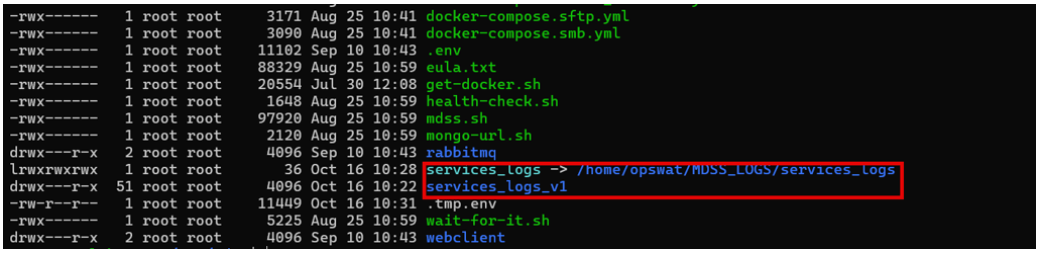
2. **Create a symlink:**

```
sudo ln -s [absolute_path_to_destination_folder]/services_logs
[MDSS_dicretory]
example: sudo ln -s /home/opswat/MDSS_LOGS/services_logs /etc/mdss/
```

3. Restart MDSS:

```
sudo mdss -c restart
```

4. Once the product restarts, you will be able to see the symlink created by executing the command: `ls -al`. Sample symnlink created shown below:



Notes:

After restart, a new file structure and logs will be created on the destination of the symlink.

Further restarts of MDSS will not affect symlink functionality.

Support:

If **Further Assistance** is required, please proceed to log a support case or chat with our support engineer.

Errors and Troubleshooting

Why does MetaDefender Storage Security get stuck in a remediation loop, causing inaccessibility?

> **Check Your Version:**
>
> This article applies to all MetaDefender Storage Security releases deployed on Windows and Linux systems.

Scenario:

In certain environments, MetaDefender Storage Security (MDSS) repeatedly retries remediation actions on specific files, even when the remediation fails or when files are already processed as *allowed* (depending on customer configuration).

As a result, multiple files may become stuck in the remediation process, eventually causing the MDSS web interface to become unresponsive until the MDSS service is restarted.

Root Cause

The remediation loop occurs when MDSS retries remediation actions multiple times without an effective retry limit per real-time process or global configuration.

By default, MDSS performs up to **3 remediation retries** with **30-second intervals**. When too many real-time processes (RTPs) are running on a single MDSS instance, **resource contention** can further increase the likelihood of remediation loops or degraded responsiveness.

Resolution

- **Distribute workload** Deploy MDSS in an **active-active** model by distributing RTP workloads across multiple MDSS instances. For example: one instance handling 3 RTPs and another handling 4 RTPs instead of running all RTPs on a single instance.
- **Review remediation retry configuration** Adjust the remediation process retry parameters according to the official documentation: https://www.opswat.com/docs/mdss/configuration/remediation-process-retries
- **Investigate failed remediations** Check the scan report details of failed files to identify the underlying causes, such as:
  - Permission or ownership issues
  - File locking by other applications

- Interference from antivirus or endpoint protection

> **Support:**
>
> If **Further Assistance** is required, please proceed to log a **support case or chatting with our support engineer**.

How to fix 'Name does not resolve' error in RHEL / Rocky Linux 8 with Podman

Overview

By default, **Rocky Linux / RHEL 8.x** uses the **CNI DNS plugin** as its container networking DNS backend (most common with Podman + CNI). This can cause services to fail to communicate with the database or external network.

Rocky Linux / RHEL 9.x ships with **aardvark-dns** and **netavark**, Podman's modern network stack, which resolves these issues.

> **Info**
>
> **Long-term recommendation: Upgrade to Rocky Linux / RHEL 9.** The steps below are a workaround for systems that cannot yet be upgraded.

Temporary solution: Change DNS library

> **Info**
>
> ⚠️ Note: This procedure requires an active internet connection and must be performed with `sudo` (root) privileges.

Step 1: Stop MDSS

```
sudo mdss -c stop
```

Step 2 — Install `netavark` and `aardvark-dns`

```
sudo dnf install -y netavark aardvark-dns
```

Step 3 — Configure Podman to Use the new network backend

Edit `/etc/containers/containers.conf` and add the following section:

```
[network]
network_backend = "netavark"
dns_enabled = true
```

> **Info**
>
> If the file does not exist, create it at `/etc/containers/containers.conf`.

Step 4 — Clean Up Old Podman Configuration

Remove the old CNI network configuration and restart Podman:

```
sudo podman container prune -f
sudo podman network prune -f
sudo rm -rf /etc/cni/net.d/*
sudo rm -rf /var/lib/cni/networks/*
sudo systemctl restart podman
```

Step 5 - Validate the new DNS library is used

Run these commands:

```
echo "Network Backend: $(sudo podman info --format
'{{.Host.NetworkBackend}}')"
echo "DNS Packages: $(rpm -qa | grep -E 'dnsname|netavark|aardvark')"
```

You should see something like this:

```
Network Backend: netavark
DNS Packages: aardvark-dns-1.16.0-1.el9.x86_64
```

Step 6 — Start MDSS

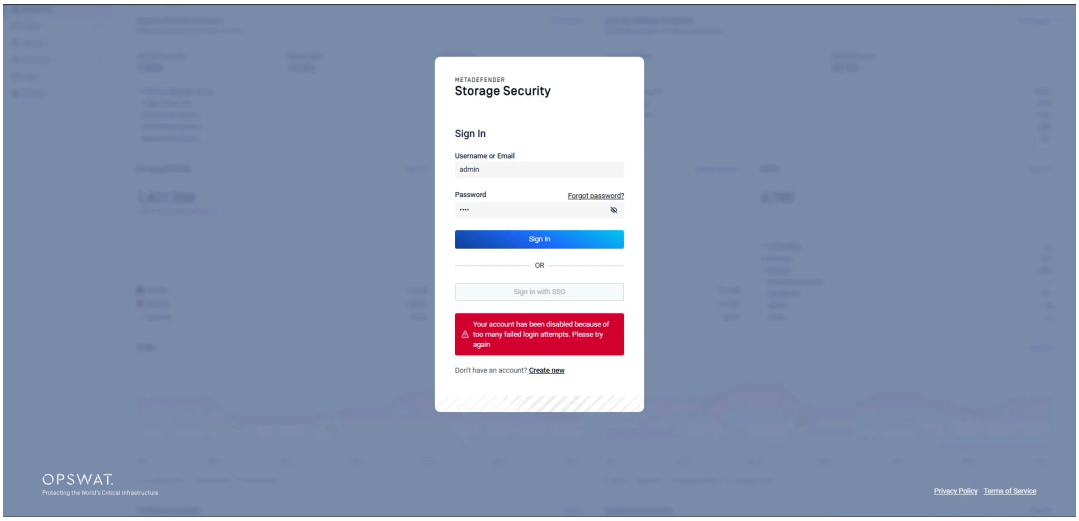
```
sudo mdss -c start
```

It should now work as expected.

Why is my MetaDefender Storage Security account disabled due to too many failed login attempts?

> **Check Your Version:**
>
> This article applies to MetaDefender Storage Security v4.0.x releases deployed on Windows and Linux systems.

Users may encounter the error message “Your account has been disabled because of too many failed login attempts. Please try again” when attempting to log into the MetaDefender Storage Security dashboard.



Starting with version v4.0.x, MetaDefender Storage Security implemented an enhanced security mechanism to **block users who repeatedly enter incorrect passwords**, even with the **correct username or email**.

This mechanism temporarily blocks the user from logging in. To regain access, the user must **wait for a specific interval** and then **enter the correct password**.

To prevent security breaches, the system applies a progressive delay mechanism after each failed login attempt. The delay increases exponentially, doubling after every failed attempt and starting from the very first failure. This approach helps slow down repeated login attempts while still allowing legitimate users to retry

The delay progression works as follows:

After **waiting for the specified interval**, you **can attempt to log in again** using the **correct password**.

Failed attempt	Delay
1st	0s → **1s**
2nd	1s → **2s**
3rd	2s → **4s**
4th	4s → **8s**
...	doubles each time
after ~12 failures	capped at **60 minutes**1st1st

> **Support:**
>
> If Further Assistance is required, please proceed to create a support case or chat with our support engineer.

Troubleshooting errors when configuring HTTPS communication for webserver

> **Check Your Version:**
>
> This article applies to all MetaDefender Storage Security releases deployed on Windows and Linux.

Issue:

The MetaDefender Storage Security (MDSS) web GUI is inaccessible via HTTPS despite enabling HTTPS and uploading SSL certificates. Symptoms include:

- The HTTPS enablement script reports SSL certificate validation failure.
- The web browser shows an endless loading loop when trying to connect via HTTPS.

Root Cause:

- Depending on the error message when running `mdss.ps1 -u enable_https`:
  - "**WARNING: Invalid certificate structure!**" indicates the SSL certificate is not in the correct PEM format required by MDSS, causing SSL certificate validation to fail (e.g. if the certificate is in DER format, it will cause this error).
  - "**WARNING: Invalid key structure!**" indicates the private key might have been extracted from a .pfx file with a passphrase, which MDSS does not currently support.

- The internal CA certificate also needs to be installed in the Windows "Trusted Root Certification Authorities" store to be trusted by MDSS (or `/etc/mdss/ca_certificates/` on Linux).

Resolution:

1. Verify that the SSL certificate and private key are in **PEM format**, indicated by headers such as "-----BEGIN CERTIFICATE-----" and "-----BEGIN PRIVATE KEY-----".
2. If extracting the certificate and private key from the .pfx file, use OpenSSL commands to extract without a passphrase:
   - Extract certificate: `openssl pkcs12 -in certificate.pfx -clcerts -nokeys -out ssl.crt`
   - Extract private key **without passphrase**: `openssl pkcs12 -in certificate.pfx -nocerts -out ssl.key -nodes`
3. Validate the certificate and key formats using OpenSSL:
   - Verify certificate: `openssl x509 -in ssl.crt -text -noout`
   - Verify private key: `openssl rsa -in ssl.key -check` (should output "RSA key ok")
4. Confirm that the MD5 hashes of the certificate and private key match:
   - `openssl x509 -noout -modulus -in ssl.crt | openssl md5`
   - `openssl rsa -noout -modulus -in ssl.key | openssl md5`
5. Ensure the internal CA root certificate is installed in the Windows "Trusted Root Certification Authorities" store so MDSS can trust the certificate chain (or `/etc/mdss/ca_certificates/` on Linux).
   - Refer to: https://www.opswat.com/docs/mdss/configuration/custom-ca-certificates
6. Disable HTTPS on MDSS before re-enabling it manually:
   - Run: `mdss.ps1 -u disable_https` (Windows)
   - Copy the validated `ssl.crt` and `ssl.key` files to `C:\Program Files\OPSWAT\MetaDefender Storage Security\config\nginx\certificates` on Windows (or `/etc/mdss/webclient/ on Linux`)
   - Run: `mdss.ps1 -u enable_https` (Windows)
7. Access the MDSS web console via HTTPS URL: `https://`
8. If issues persist, generate and upload a support package for further investigation.

> **Support:**
>
> If **Further Assistance** is required, please proceed to log a support case or chat with our support engineer.

Why does a report fail to load with error "API took too long to respond"?

> **Check Your Version:**
>
> This article applies to all MDSS versions

> When opening a report in MDSS, the UI displays the following error:

`API took too long to respond. Please try again later`

The database queries are taking more than 60 seconds to return, triggering the default web server (nginx) timeout.

Increase the **nginx proxy timeout** and **PostgreSQL query timeout** values.

Both changes are required.

For Windows

1. Stop MDSS services
2. Increase Nginx Timeout Create a backup of the nginx configuration file at `C:\Program Files\OPSWAT\MetaDefender Storage Security\webclient\default.conf`, then edit the **default.conf** file Add or modify the following values in the appropriate `location` or `http` block:

```
proxy_connect_timeout 300s;
proxy_send_timeout 300s;
proxy_read_timeout 300s;
```

3. Increase PostgreSQL Timeout Edit the MDSS environment configuration file at `C:\Program Files\OPSWAT\MetaDefender Storage Security\config\customer.env` Modify the `POSTGRESQL_URL` parameter to include increased timeout values. Example:

```
POSTGRESQL_URL=Host=postgres;Port=5432;Username=mdss;Password=
<password>;Database=MDSS;Timeout=300;CommandTimeout=300
```

4. Start MDSS services

For Linux

1. Stop MDSS service

```
sudo mdss -c stop
```

2. Increase Nginx Timeout Run the bellow command

```
sudo awk '/proxy_intercept_errors off;/{print; print "
proxy_connect_timeout 300s;"; print "        proxy_send_timeout
300s;"; print "        proxy_read_timeout    300s;"; next}1'
/etc/mdss/webclient/default.conf | sudo tee
/etc/mdss/webclient/default.conf.tmp && sudo mv
/etc/mdss/webclient/default.conf.tmp /etc/mdss/webclient/default.conf
```

This will create a backup of the config file `/etc/mdss/webclient/default.conf`and increase the nginx timeout to 300ms

3. Increase the timeout for the PostgreSQL database by modifying the `POSTGRESQL_URL` in the `/etc/mdss/customer.env` file:
   - Set `Timeout` to 300.
   - Set `CommandTimeout` to 300.

Here's an example of how the `POSTGRESQL_URL` should look:

```
POSTGRESQL_URL=Host=postgres;Port=5432;Username=mdss;Password=a3ZPzF1VI
N3RzCu5YWrl;Database=MDSS;Timeout=300;CommandTimeout=300
```

4. Start MDSS service

```
sudo mdss -c start
```

> **Note**
>
> - Increasing the timeout allows **long-running report queries** to complete successfully.
> - If the issue occurs frequently, it may indicate:
>   - very large report datasets
>   - insufficient database resources
>   - missing database indexes
>
> In those cases, further **database performance tuning** may be required.

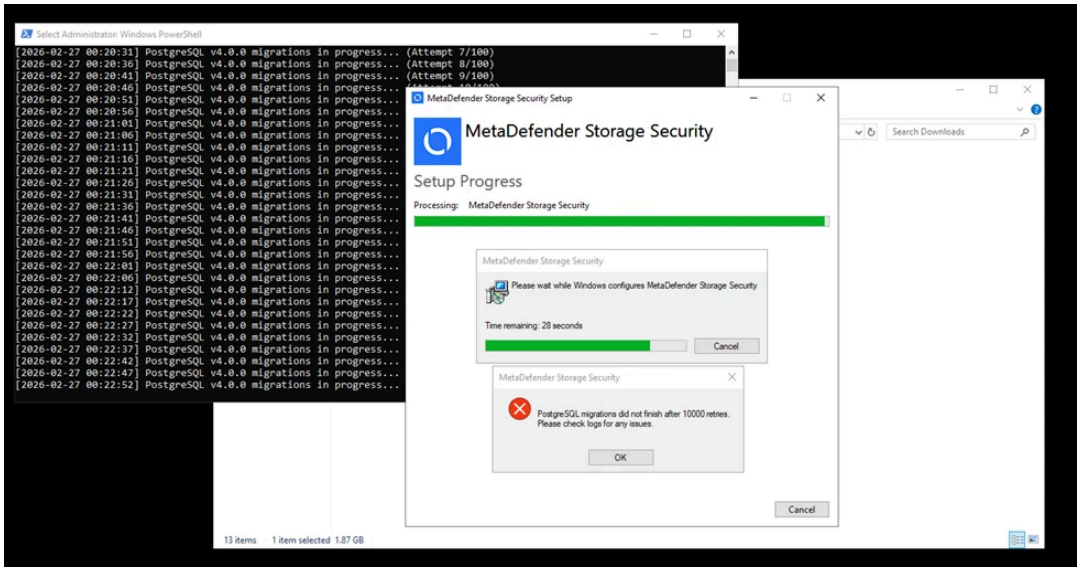
> **Support:**
>
> If **Further Assistance** is required, please proceed to log a **support case or chatting with our support engineer**.

Why am I receiving the error "PostgreSQL migrations did not finish" when installing MetaDefender Storage Security?

> **Check Your Version:**
>
> This article applies to MetaDefender Storage Security v4.0.x releases deployed on Windows systems.

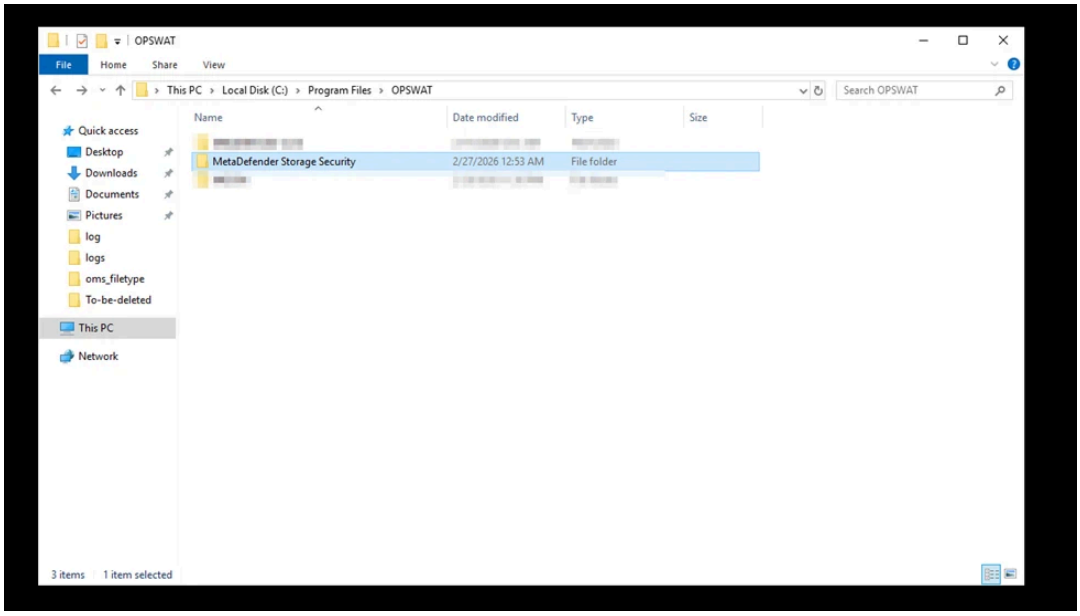
Issue:

- When installing MetaDefender Storage Security on Windows server, the error "PostgreSQL migrations did not finish after 10000 retries. Please check logs for any issues.“ is received, even on a fresh installation.



Main Cause:

- This occurs because MetaDefender Storage Security was previously installed on the machine but not completely removed after an uninstall or problem. This leftover data causes the installer to recognize an existing installation and attempt an upgrade instead of a fresh install.



Resolution:

Please follow the steps below to safely remove and reinstall MetaDefender Storage Security (MDSS):

1. Stop MDSS Services

Stop all related MDSS services from **Services (services.msc)** or by using the following commands:

```
net stop mdss
net stop mdss_postgresql
net stop mdss_rabbitmq
```

---

2. Remove MDSS Windows Services

Run the following commands as Administrator to remove existing services:

```
sc.exe delete "mdss_postgresql"
sc.exe delete "mdss_rabbitmq"
sc.exe delete "mdss"
```

---

3. Remove Installation Directory

Delete the default installation folder:

```
C:\Program Files\OPSWAT\MetaDefender Storage Security
```

Ensure all files are removed.

---

4. Handle Locked Files (if any)

If some files cannot be deleted:

- Ensure all MDSS services are stopped
- Close any open log files
- Restart the system if needed

Advanced:

- Use **Process Explorer** to identify which process is locking the files

---

5. Remove Registry Entry

Clean up the registry by running:

```
reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\OPSWAT\MetaDefender Storage Security" /f
```

---

6. Reboot the System

Restart the machine to ensure all remaining components are fully cleared.

7. Reinstall MDSS

Run the installer again after completing all steps above.

> **Support:**
>
> If Further Assistance is required, please proceed to create a support case or chat with our support engineer.

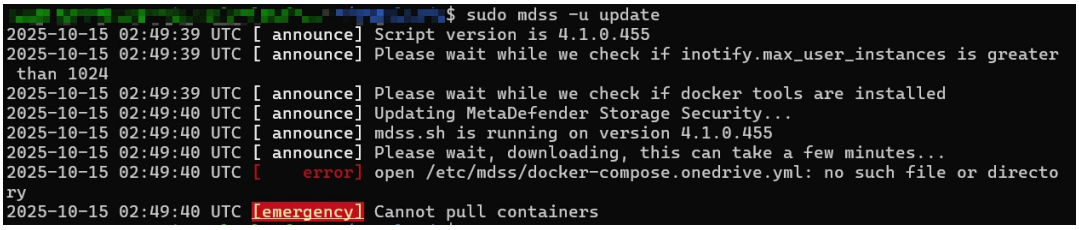
Why am I getting a "stat /etc/mdss/docker-compose.onedrive.yml: no such file or directory" error when upgrading MetaDefender Storage Security from 3.6.1 to 4.1.0?

> **Check Your Version:**

> This article applies to MetaDefender Storage Security versions v4.1.0 deployed on Linux systems.

Issue

During an upgrade from **MetaDefender Storage Security** version **3.6.1** to **4.1.0**, you may encounter the following error:



`[error] stat /etc/mdss/docker-compose.onedrive.yml: no such file or directory [emergency] Cannot pull containers`

This error occurs when the `ENABLED_MODULES` variable in the configuration file `/etc/mdss/customer.env` includes the value `onedrive`, which is no longer valid in version 4.1.0.

Cause

In version 4.1.0, the `/etc/mdss/docker-compose.onedrive.yml` has been replaced by the `/etc/mdss/docker-compose.graph.yml`.

The upgrade process expects the updated module name, and referencing `onedrive` in customer.env causes it to look for a non-existent configuration file [`docker-compose.onedrive.yml`], resulting in the error.

Resolution

To fix the issue:

1. Open the file `/etc/mdss/customer.env`.
2. Locate the line that starts with `ENABLED_MODULES=`.

```
ENABLED_MODULES=smb,box,onedrive,sftp,nfs,mft,ftp
```

3. If `onedrive` is listed, replace it with `graph`.

```
ENABLED_MODULES=smb,box,graph,sftp,nfs,mft,ftp
```

Example:

- **Before:** ENABLED_MODULES=smb,box,**onedrive**,sftp,nfs,mft,ftp
- **After:** ENABLED_MODULES=smb,box,**graph**,sftp,nfs,mft,ftp

4. Save the file and re-run the upgrade command: `sudo mdss -u update`

> **Support:**
>
> If **Further Assistance** is required, please proceed to log a support case or chatting with our support engineer.

Why is RabbitMQ consuming excessive memory in MetaDefender Secure Storage (MDSS) Kubernetes deployment?

> **Check Your Version:**
>
> This article applies to **MetaDefender Storage Security (MDSS)** deployment on **Kubernetes** environment.

Overview

This article addresses a specific memory exhaustion issue affecting RabbitMQ components within MetaDefender Secure Storage (MDSS) Kubernetes deployments. It details the symptoms of the memory leak and provides a configuration change to the Helm Chart to permanently resolve the instability.

Issue

RabbitMQ v4.1.0 instances might experience continuous memory growth (memory leaks). This is specifically caused by the improper cleanup of "deleted consumer metrics" within the `rabbitmq:4.1.0-management-alpine` container image.

Symptoms include:

- Steadily climbing RAM usage without release.
- High resource consumption attributed to the Management Plugin.
- Potential Out of Memory (OOM) crashes or pod restarts.

Solution

To resolve this, you will need to switch the container image to the standard Alpine version, which excludes the Management Plugin.

1. Modify the Configuration

Open the `values.yaml` file used for your MDSS deployment.

2. Update the Image Tag

Locate the RabbitMQ image section and remove the `-management` suffix.

3. Change From:

```
image: rabbitmq:4.1.0-management-alpine
```

Change To:

```
image: rabbitmq:4.1.0-alpine
```

4. Apply the Changes

Execute the Helm upgrade command to apply the new configuration:

```
helm upgrade <release-name> ./<chart-path> -f values.yaml -n <namespace>
```

5. Monitor

Verify the pod is running the new image and monitor memory usage over the next 24 hours to confirm stability.

> **Support:**
>
> If **Further Assistance** is required, please proceed to log a **support case or chatting with our support engineer**.

Is the Scheduled Scan in MetaDefender Storage Security Based on OS Time or an Internal Timer?

> **Check Your Version:**
>
> This article is applied to MetaDefender Storage Security deployments.

Overview

This article explains how the **scheduled scan timing** works in **MetaDefender Storage Security**, specifically whether it relies on the operating system's time or an internal timer mechanism within the product.

Question

There may be uncertainty about how **scheduled scans** are triggered in MetaDefender Storage Security — specifically whether the scheduling is determined by the **operating**

system's local time or by an **internal timer** within the product.

Clarification

- The **scheduled scan** in MetaDefender Storage Security runs according to the **operating system's local time**.
- For example, if a scheduled scan is configured to run **every 1 hour**, and the system time is currently **4:03**, the next scan will initiate at **5:03 (OS time)**.

Additional Notes

- Ensure that the **system clock** and **timezone settings** on the host operating system are accurate, as these directly affect the timing of scheduled scans.
- Any drift or misconfiguration in system time may result in delayed or early scan execution.

> **Support:**
>
> If **Further Assistance** is required, please proceed to log a **support case or chatting with our support engineer**.

Why does MDSS installation might fail with "net/http: TLS handshake timeout" when pulling Docker containers?

> **Check Your Version:**
>
> This article applies to all MDSS releases deployed as a Docker Image.

Overview

During first start or installation, **MetaDefender Storage Security (MDSS)** pulls multiple Docker images from Docker Hub's CDN (`production.cloudflare.docker.com`). In some environments, this process fails with errors like:

```
failed to copy: httpReadSeeker: failed open: failed to do request:
Get "https://production.cloudflare.docker.com/registry-
v2/docker/registry/v2/blobs/sha256/...":
net/http: TLS handshake timeout

[emergency] Cannot pull containers
```

Key observations from the affected systems:

- DNS, ping and `curl` tests to Docker Hub and Cloudflare all worked (TLS handshakes succeeded).
- Pulling **one MDSS image at a time** with `docker pull opswat/<image>:<tag>` worked.
- The error occurred **only when MDSS tried to pull many images in parallel**.

Conclusion: the network itself was healthy, but **too many concurrent image downloads** caused some TLS handshakes to time out (combination of Docker's defaults, CDN behavior, and/or network limits). This is consistent with Docker's documented behavior where reducing `max-concurrent-downloads` stabilizes image pulls under load.

Resolution

1. Reduce Docker's concurrent downloads

Goal: Force Docker to pull layers sequentially (or with lower parallelism), reducing pressure on the network and avoiding TLS handshake timeouts.

1. Create or edit /etc/docker/daemon.json on the MDSS host:

```
{
"max-concurrent-downloads": 1
}
```

You can later tune this to `2` or `3`, but using `1` is the safest starting point to verify the fix. Docker's `max-concurrent-downloads` is an officially documented setting controlling concurrent layer downloads.

2. Restart Docker:

```
sudo systemctl restart docker
```

3. Re-run the MDSS start/activation:

```
./mdss.sh -c start
```

2. Optional: Re-try with a modest concurrency value

If installation works with `1` but you want faster future upgrades:

1. Adjust `daemon.json`, for example:

```
{
  "max-concurrent-downloads": 2
}
```

2. Restart Docker and test an image pull or a service update.

If timeouts reappear, reduce back to 1.

3. Verify network devices (optional but recommended)

Even with reduced concurrency, it is good practice to verify with the network team that:

- No firewall, IDS/IPS, or TLS-inspection device is limiting or throttling HTTPS connections to:
  - `registry-1.docker.io`
  - `production.cloudflare.docker.com`
- There are no strict connection or rate limits for outbound HTTPS from that host.

Many Docker handshake timeout reports involve some interaction between Docker's parallel pulls and upstream devices, so confirming this can help avoid future issues.

> **Support:**
>
> If **Further Assistance** is required, please proceed to log a **support case or chat with one of our support engineers**.

How to resolve "Remediation Reached the Configured Timeout" for SMB Storage

> **Check Your Version:** This article applies to all MetaDefender Storage Security

Issue

When running a Discovery workflow with Remediation against SMB storage, some files may fail with the following error:

```
opswat.mdcs.job.dispatcher.ObjectProcessingStuckException: Remediation
reached the configured timeout ---> System.TimeoutException: 1 or more
hours passed since MetaDefender Storage Security started remediations
for the file --- End of inner exception stack trace ---
```

Possible issues

By default, MetaDefender Storage Security waits up to **1 hour** for a remediation task to complete. If the remediation process takes longer than the configured timeout, the file is

marked as failed.

This can happen when:

- The server does not meet the recommended system requirements.
- The SMB storage configuration is not optimized for MetaDefender Storage Security.
- The storage contains a large number of files or large file sizes.
- SMB remediation takes longer than NFS remediation due to protocol or environment differences.

**\

Resolutions**

1. Verify the Server Meets System Requirements

Confirm that the server hosting MetaDefender Storage Security meets the required system specifications.

Refer to the official system requirements:

General System Requirements - MetaDefender Storage Security

2. Use the Recommended SMB Storage Approach

For SMB-compatible storage, OPSWAT highly recommends using the recommended integration approach documented below:

Recommended approach when adding SMB units on Linux deployments - MetaDefender Storage Security

This approach can help improve reliability and reduce remediation-related timeout issues when working with SMB shares.

3. Increase the Remediation Timeout

If remediation tasks require more than the default timeout of **1 hour**, increase the configured remediation timeout (to 3 hours for example).

On the MetaDefender Storage Security server, edit the `customer.env` file and add the following value:

```
REMEDIATION_STUCK_TIMEOUT_HOURS=3
```

If this value already exists, update it to:

```
REMEDIATION_STUCK_TIMEOUT_HOURS=3
```

For instructions on modifying `customer.env`, refer to:

Custom configuration - MetaDefender Storage Security

> **Support:** If **Further Assistance** is required, please collect a new MetaDefender Storage Security support package and proceed to log a support case or chatting with our support engineer.

How to troubleshoot slow historical data retrieval from the AVEVA PI Server?

> **Check Your Version:** This article applies to MetaDefender NetWall used with the OPSWAT PI Connector.

Issue

Historical data transfer from the Blue side to the Red side is slower than expected. Symptoms include delayed backfill of historical values, slow snapshot updates, and general performance degradation that becomes more noticeable under higher load or during large backfill operations.

Possible Causes

This issue may occur in either of the following situations:

- The AVEVA PI Data Archive on the Red side is taking longer than expected to process historical-data requests. The Red Flanker measures this time but does not control it.
- The PI Buffer Subsystem is not enabled on the Red Flanker, so writes to the destination PI Server are not buffered.

Retrieval time is measured from the moment the Red Flanker issues the AVEVA PI AF SDK call `PIPoint.RecordedValues()` until the call returns. This call retrieves historical data from the PI Data Archive. If the call itself is slow, the delay is occurring inside the PI Data Archive, not in the OPSWAT components.

Troubleshooting Steps

1. Enable the PI Buffer Subsystem on the Red Flanker

Confirm that the PI Buffer Subsystem is enabled on the Red Flanker node. Buffering allows writes to the destination PI Server to be queued rather than blocking on each write, and is required for the reference performance figures below to apply.

2. Collect the PiHistoryStore statistics

The `PiHistoryStore` statistics are generated once per minute and recorded in both syslog and the Windows Event Log on the Red Flanker. Collect several consecutive samples covering a period when the slowness is observed.

The following sample is from an OPSWAT reference environment and is shown here as a **healthy baseline**, not as an example of the problem:

> 09:26:28.67 PI_STATS 3460-pi HistoryStoresTotal 18082
>
> 09:26:28.67 PI_STATS 3460-pi HistoryStoresPerSecond 0.0
>
> 09:26:28.67 PI_STATS 3460-pi Last History Store Time 7/28/2026 9:22:30 AM
>
> 09:26:28.67 PI_STATS 3460-pi Collective Main Connection Status: Primary
>
> 09:26:28.67 PI_STATS 3460-pi PiHistoryStore(09:25:53) 3460-pi Blocks:12116 Fetches:12115 elapsed 13.01secs, Red Fetch longest:11ms, avg:1.07ms, total:12.96secs, BlueSort 1ms
>
> 09:26:28.67 PI_STATS 3460-pi PiHistoryStore(09:25:53) longest red fetch length:84 avg:28.37 # of values fetched:343672 Total Blue Values:343672

In this sample:

- 12,116 history blocks containing 343,672 values were transferred from the Blue side to the Red side.
- The Red Flanker performed 12,115 historical-data reads and retrieved 343,672 values.
- The longest individual read took 11 milliseconds; the average read took 1.07 milliseconds.
- The reads consumed 12.96 seconds of read time within a 13.01 second sampling interval.
- Each read returned an average of 28.37 values, and the largest returned 84 values.

3. Compare your figures against the reference baseline

Metric	Reference environment	Indicates slow PI Data Archive response
Average read time (`avg`)	~1 ms	Tens of milliseconds — for example, ~42 ms
Longest read time (`longest`)	~11 ms	Consistently above ~50 ms
Average values per read (`avg length`)	~28 values	Higher averages increase per-read cost

An average read time in the tens of milliseconds against a reference of roughly 1 millisecond means the PI Data Archive is taking substantially longer to satisfy each request. Larger average read lengths also raise the cost of each individual read, so consider both figures together.

4. Tuning Historical Backfill for best results

If the comparison in step #3 looks good, please refer to the following documentation for guidance on tuning the configuration to optimize performance:Optimizing AVEVA Pi Historical Backfill - MetaDefender Optical Diode

5. Escalate to AVEVA with supporting evidence (If Needed)

If the `PIPoint.RecordedValues()` call consistently takes significantly longer than the reference results, open a support case with AVEVA and provide:

- PI Server logs covering the same period
- Red Flanker event logs covering the same period

AVEVA Support can determine why historical-data retrieval is taking longer than expected.

Reference Environment

The reference figures above were produced in an OPSWAT environment with the following characteristics:

- The PI System contains approximately 264,000 tags.
- Two physical computers connected through a 1 Gbps network.
- One computer runs the OPSWAT Red Flanker and acts as the PI API node.
- The other computer runs the PI Server.
- The PI Buffer Subsystem is enabled.

Recommendation

Capture `PiHistoryStore` statistics routinely rather than only during an incident, so a healthy baseline for your own environment is available for comparison.

> **Support:** If **Further Assistance** is required, please proceed to log a support case or chatting with our support engineer.

Troubleshooting Guide

Diagnostic

Logs location

Unix

Type of logs	Location
Internal services logs	/etc/mdss/services_logs/{service-name}/
Installation logs	/var/log/mdss/
Script logs	/etc/mdss/logs

Windows

Type of logs	Location
Script logs	C:\Program Files\OPSWAT\MetaDefender Storage Security\logs\
Internal services logs	C:\Program Files\OPSWAT\MetaDefender Storage Security\services{service-name}\logs\
Windows Service logs	C:\Windows\System32\opswat.mdss.windows.service\
Installation logs	C:\Users\AppData\Local\Temp\ C:\Program Files\OPSWAT\MetaDefender for Secure Storage\logs\

How to read the logs

The log files are plain text files that can be opened with any text editor.

For MetaDefender Storage Security, the default logging level is set to **Information**. To access additional log levels, you need to enable Extra Logging in the Configuration. Extra logging is recommended only for troubleshooting purposes and should be enabled only when necessary.

For more details, refer to this article: How to Enable Extra Logging in the Configuration?

File Locations

- **Linux**: Log files are located at `/etc/mdss/services_logs`
- **Windows**: The default path is `C:\Program Files\OPSWAT\MetaDefender Storage Security\services\`

Log Format

The messages stored in the service logs follow this format:

```
[TIMESTAMP] [LEVEL] service.name: Message
```

Example:

```
[2024-06-12 10:17:55Z] [Information] nfs.service: HTTP POST
/ObjectOperations/Download responded 200 in 37.0824 ms
```

Log Levels

- **Debug : Provides detailed information useful for troubleshooting.**
- **Information**: The default logging level, capturing general operational messages.
- **Warning**: Highlights potentially harmful situations.
- **Error**: Logs issues that affect functionality or cause interruptions.
- **Fatal**: Reserved for very critical issues that require immediate attention.

> **Support:**
>
> If you have any difficulty reading MetaDefender Storage Security logs, please create a support case or chat with our support engineer.

Analysis Guide

This guide helps customer support representatives efficiently locate error messages in product logs when troubleshooting customer issues.

Behavior	Container
Failed to add a storage unit	mdss_nfsservice / mdss_smbservice / mdss_sftpservice (if applicable) *mdss{storageType}storagesservice* *mdss_storagesservice*
Failed to add MD Core or Cloud instance	mdss_workflowmanagerservice
Failed to start a scan No files are discovered	mdss_nfsservice / mdss_smbservice / mdss_sftpservice (if applicable) *mdss{storageType}discoveryservice* *mdss_discoveryservice*
Failed to scan a file No files are scanned	mdcs_scanningservice
Failed to remediate a file Remediations not applied Sanitization failed Sanitization not applied	mdss_remediationsservice mdss__{storageType}*_remediationsservice*

How to generate a support package

Linux deployment

Run the following command:

```
sudo mdss -u support_package
```

In case of a successful generation, you should see the following message:

```
Support package was exported to
/etc/mdss/mdss_3.6.1.10601_support_package_2025-06-03_16-16-44.tar
```

Windows deployment

> **PowerShell Compatibility Notice**
>
> Our product has been thoroughly tested and optimized for compatibility with **PowerShell 5.x**, which is the default Windows PowerShell version included with Windows Server 2019, 2022 and 2025.
>
> When generating a support package for troubleshooting purposes, please ensure that you use **Windows PowerShell 5.x** and not PowerShell 7 (PowerShell Core). This

> will make sure that all diagnostic information is correctly captured and formatted for our analysis tools.

Before you begin, please run the following command in an elevated **PowerShell** to allow the utility script [**mdss.ps1**] to be executed

```
PS> Set-ExecutionPolicy RemoteSigned
```

In order to generate a support package please run the following commands in the scripts folder within the installation folder [by default *C:\Program Files\OPSWAT\MetaDefender Storage Security\scripts*]

```
PS> .\mdss.ps1 -u support_package
```

In case of a successful generation, you should see the following message:

```
MetaDefender Storage Security support package was exported to
C:\Program Files\OPSWAT\MetaDefender Storage
Security\support_package_{date}.zip
```

For Kubernetes Deployment

In case of issues that require further investigation by OPSWAT support, a package can be generated using the `sp.sh` script what contains pod logs, configurations and details regarding the Kubernetes deployment. In order to generate the support package, make the `sp.sh` script executable and run the following command:

./sp.sh

Notes:

- The namespace name where the application is deployed needs to be specified as an argument, otherwise the default namespace is used.
- The script uses `kubectl` to extract the required information, make sure `kubectl` is installed and configured with the correct context.
- The script generates the support package as a zip file in the same directory where it is executed.

Maximum limit

The package can grow very large on systems with extensive logs. In order to prevent this, you can use the -m / --max-size argument as such:

Linux

```
sudo mdss -u support_package -m 500M
sudo mdss -u support_package -m 1G
sudo mdss -u support_package -m 1.5G
```

Windows

```
.\mdss.ps1 -u support_package
.\mdss.ps1 -u support_package -MaxSize 500M
.\mdss.ps1 -u support_package -MaxSize 1G
.\mdss.ps1 -u support_package -m 1.5G
```

Limiting the number of log files per service

Linux only. Cap how many of the most-recent log files are collected per service.

Overrides the `LOGS_PER_SERVICE` setting; omit it to collect all files per service.

```
sudo mdss -u support_package -l 14          # 14 most-recent log files
per service
sudo mdss -u support_package -m 1G -l 14    # combine with a total size
cap
```

How the size budget is allocated internally

When -m is provided, the total budget is split into two parts:

1. Settings/host info reservation — 50MB reserved for non-log data (settings, host info, env files). Configurable via env var **RESERVED_FOR_SETTINGS**.
2. Logs budget = max_size - 50MB — everything remaining goes to logs.

The logs budget itself is then divided into:

- Container logs — each container is capped at the last 25,000 lines (configurable via **CONTAINER_LOG_LINES**)
- Script logs — always included in full (usually small)
- Service logs — whatever budget remains after container + script logs

How service logs are collected (the two-phase approach)

Phase 1 — Fair representation: Takes the N most recent log files from each service (default: 1 file, configurable via **MIN_FILES_PER_SERVICE**). This guarantees every service has at least some representation in the package, even if the budget is tight. **Phase 2** —

Fill remaining budget: Any budget left after Phase 1 is filled with the most recently modified log files across all services, globally sorted by timestamp — most recent first.Files are never arbitrarily truncated — they are only truncated if they exceed the remaining budget, and when truncated, the last N bytes are kept (most recent content) via tail -c.

Environment variable overrides

Variable	Default	Description
RESERVED_FOR_SETTINGS	50MB	Space reserved for settings/host info
MIN_FILES_ PER_SERVICE	1	Minimum files per service in Phase 1
CONTAINER_LOG_LINES	25000	Max container log lines when -m is active
SERVICES_LOG_PATH	./services_logs	Path to service log files

> **Default limit**
>
> There is a maximum size set by default, which, if not modified it limits the support package to **2GB** on Windows.
>
> On Linux by default there is not limit.

—published

Linux deployment

Run the following command:

```
sudo mdss -u support_package
```

In case of a successful generation, you should see the following message:

```
Support package was exported to
/etc/mdss/mdss_3.6.1.10601_support_package_2025-06-03_16-16-44.tar
```

Windows deployment

> **PowerShell Compatibility Notice**
>
> Our product has been thoroughly tested and optimized for compatibility with **PowerShell 5.x**, which is the default Windows PowerShell version included with

> Windows Server 2019, 2022 and 2025.
>
> When generating a support package for troubleshooting purposes, please ensure that you use **Windows PowerShell 5.x** and not PowerShell 7 (PowerShell Core). This will make sure that all diagnostic information is correctly captured and formatted for our analysis tools.

Before you begin, please run the following command in an elevated **PowerShell** to allow the utility script (**mdss.ps1**) to be executed

```
PS> Set-ExecutionPolicy RemoteSigned
```

In order to generate a support package please run the following commands in the scripts folder within the installation folder (by default *C:\Program Files\OPSWAT\MetaDefender Storage Security\scripts*)

```
PS> .\mdss.ps1 -u support_package
```

In case of a successful generation, you should see the following message:

```
MetaDefender Storage Security support package was exported to
C:\Program Files\OPSWAT\MetaDefender Storage
Security\support_package_{date}.zip
```

For Kubernetes Deployment

In case of issues that require further investigation by OPSWAT support, a package can be generated using the `sp.sh` script what contains pod logs, configurations and details regarding the Kubernetes deployment. In order to generate the support package, make the `sp.sh` script executable and run the following command:

./sp.sh

Notes:

- The namespace name where the application is deployed needs to be specified as an argument, otherwise the default namespace is used.
- The script uses `kubectl` to extract the required information, make sure `kubectl` is installed and configured with the correct context.
- The script generates the support package as a zip file in the same directory where it is executed.

Maximum limit

The package can grow very large on systems with extensive logs. In order to prevent this, you can use the -m / --max-size argument as such:

Linux

```
sudo mdss -u support_package -m 500M
sudo mdss -u support_package -m 1G
sudo mdss -u support_package -m 1.5G
```

Windows

```
.\mdss.ps1 -u support_package
.\mdss.ps1 -u support_package -MaxSize 500M
.\mdss.ps1 -u support_package -MaxSize 1G
.\mdss.ps1 -u support_package -m 1.5G
```

How the size budget is allocated internally

When -m is provided, the total budget is split into two parts:

1. Settings/host info reservation — 50MB reserved for non-log data (settings, host info, env files). Configurable via env var **RESERVED_FOR_SETTINGS**.
2. Logs budget = max_size - 50MB — everything remaining goes to logs.

The logs budget itself is then divided into:

- Container logs — each container is capped at the last 25,000 lines (configurable via **CONTAINER_LOG_LINES**)
- Script logs — always included in full (usually small)
- Service logs — whatever budget remains after container + script logs

How service logs are collected (the two-phase approach)

Phase 1 — Fair representation: Takes the N most recent log files from each service (default: 1 file, configurable via **MIN_FILES_PER_SERVICE**). This guarantees every service has at least some representation in the package, even if the budget is tight. **Phase 2** — Fill remaining budget: Any budget left after Phase 1 is filled with the most recently modified log files across all services, globally sorted by timestamp — most recent first.Files are never arbitrarily truncated — they are only truncated if they exceed the remaining budget, and when truncated, the last N bytes are kept (most recent content) via tail -c.

Environment variable overrides

Variable	Default	Description
RESERVED_FOR_SETTINGS	50MB	Space reserved for settings/host info
MIN_FILES_ PER_SERVICE	1	Minimum files per service in Phase 1
CONTAINER_LOG_LINES	25000	Max container log lines when -m is active
SERVICES_LOG_PATH	./services_logs	Path to service log files

> **Default limit**
>
> There is a maximum size set by default, which, if not modified it limits the support package to **2GB** on Windows and **5GB** on Linux.

How to Enable Extra Logging in the Configuration?

Logging supports different log levels to have the desired granularity. Default logging is set to **Information**.

To change log level adjust **MinimumLevel.Default** as follows:

- Debug: provides detailed information useful for troubleshooting.
- Information: the default logging level, capturing general operational messages.
- Warning: only highlights potentially harmful situations.
- Error: logs only issues that affect functionality or cause interruptions.
- Fatal: reserved for very critical issues that require immediate attention.

A typical `appsettings.json` configuration file appears as follows depends on the desired Serilog Sink:

- for **File Serilog Sink**

> **Info**
>
> Default maximum size of a log file is 500Mb which can be adjust by changing `fileSizeLimitBytes`
>
> Rolling interval is configured to be daily by the `rollingIntervalor` on file size limit `rollOnFileSizeLimit: true`
>
> Default limit of retained files is set to 10 using the `retainedFileCountLimit` property

```
{
  "Serilog": {
    "Using": [],
    "MinimumLevel": {
      "Default": "Information",
      "Override": {
        "Microsoft": "Warning",
        "System": "Warning",
        "Microsoft.Hosting.Lifetime": "Warning"
      }
    },
    "Enrich": [ "FromLogContext", "WithMachineName", "WithProcessId",
"WithProcessName", "WithThreadId" ],
    "WriteTo": [
      {
        "Name": "File",
        "Args": {
          "buffered": false,
          "fileSizeLimitBytes": 500000000,
          "outputTemplate": "[{Timestamp:u}] [{Level}] {Namespace}:
{Message:lj}{NewLine}{Exception}",
          "path": "logs/log.txt",
          "retainedFileCountLimit": "10",
          "rollingInterval": "Day",
          "rollOnFileSizeLimit": true
        }
      }
    ]
  }
}
```

- for **HTTP Serilog Sink**

```
{
  "Serilog": {
    "MinimumLevel": {
      "Default": "Information",
      "Override": {
        "Microsoft": "Warning",
        "System": "Warning",
        "Microsoft.Hosting.Lifetime": "Information"
      }
    },
    "Enrich": [
      "FromLogContext",
      "WithMachineName",
      "WithProcessId",
      "WithProcessName",
      "WithThreadId"
    ],
    "WriteTo": [
      {
        "Name": "Http",
        "Args": {
          "requestUri": "<REQUEST_URI>",
          "queueLimitBytes": null
        }
      }
    ]
  }
}
```

- for **Syslog Serilog Sink**

```
{
  "Serilog": {
    "Using": [
      "Serilog.Sinks.Syslog"
    ],
    "MinimumLevel": {
      "Default": "Information",
      "Override": {
        "Microsoft": "Warning",
        "System": "Warning",
        "Microsoft.Hosting.Lifetime": "Information"
      }
    },
    "Enrich": [
      "FromLogContext",
      "WithMachineName",
      "WithProcessId",
      "WithProcessName",
      "WithThreadId"
    ],
    "WriteTo": [
      {
        "Name": "TcpSyslog",
        "Args": {
          "host": "<HOST>",
          "port": 514,
          "appName": "MetaDefenderStorageSecurity",
          "format": "RFC5424",
          "facility": "<SYSLOG_FACILITY_NAME>",
          "outputTemplate": "[{Timestamp:u}] [{Level}] {SourceContext}:
{Message:lj}{NewLine}{Exception}"
        }
      }
    ]
  }
}
```

Linux-based systems

Use the **appsettings.json** file from the `configurations` directory

Note: The default path on Linux is `/etc/mdss/configurations`.

> On Linux, logging settings are applied immediately after any changes, so a system restart is not required.

Windows-based systems

On Windows systems, each service has its own logging configuration file. You can locate the `appsettings.json` file by navigating to the service's directory and then accessing the specific `<service>` folder.

Note: The default path on Windows is `C:\Program Files\OPSWAT\MetaDefender Storage Security\services\`.

> On Windows, logging settings take effect only after the service has been restarted.

Enable debug logs for script commands

In order to troubleshoot please run :

```
sudo LOG_LEVEL=7 [mdss-command]
```

```
PS> .\mdss.ps1 [mdss-command] -log_level=7
```

where **mdss-command** is the command that has an issue. For example, if MetaDefender Storage Security cannot be started please run the following command:

```
sudo LOG_LEVEL=7 mdss -c start
```

```
PS> .\mdss.ps1 -c start -log_level 7
```

Resolving error code 1722 when OPSWAT ONTAP Connector tries to connect to ONTAP AV Connector

Overview

This document describes a troubleshooting and resolution procedure for a scenario where the **OPSWAT ONTAP Connector** receives **RPC_S_SERVER_UNAVAILABLE**** (error 1722, 0x6BA)** when connecting to a named pipe on a hardened Windows Server, even though the pipe is confirmed to exist on the server.

The issue was observed against a server running NetApp ONTAP AV Connector, where the OPSWAT ONTAP Connector connects to the pipe `\\127.0.0.1\pipe\ntapvscp`. The same pattern applies to any same-host RPC-over-named-pipes integration that uses an SMB-

style pipe path (`\\127.0.0.1\pipe\...`, `\\localhost\pipe\...`, or `\\<hostname>\pipe\...`).

Symptoms

The OPSWAT ONTAP Connector logs an entry similar to the following when the registration call fails:

```
[2026-05-06 11:23:49] [Error] [1722] VS_Registration2 failed
```

Additional indicators:

- The Win32 error code `1722` (`RPC_S_SERVER_UNAVAILABLE`) appears in the OPSWAT ONTAP Connector log.
- The named pipe is confirmed to exist on the server (visible under `\\.\pipe\`).
- The connection target is the loopback interface (`127.0.0.1`), so no network device or external firewall is involved.
- The host has been hardened according to a security baseline (CIS, STIG, or vendor-specific hardening).

Root Cause

Named-pipe access through an SMB-style path (for example `\\127.0.0.1\pipe\ntapvscp`) routes through the SMB redirector and requires:

1. A listener on TCP 445.
2. A valid inbound firewall rule allowing the connection.
3. SMB Server bound to a network interface (which is what creates the listener).

On a hardened host, all three of these layers are commonly disabled to reduce the attack surface. The combination produces the observed failure chain:

```
App opens \\127.0.0.1\pipe\ntapvscp
    -> Routed through the SMB redirector
        -> SMB attempts to connect to 127.0.0.1:445
            -> No listener on 445
                -> SMB returns ERROR_NETNAME_DELETED (64) or
ERROR_UNEXP_NET_ERR (59)
                    -> RPC layer surfaces RPC_S_SERVER_UNAVAILABLE
(1722)
```

Note that the AV Connector itself, the named pipe, and the local RPC subsystem are healthy. Only the SMB transport layer used to reach the pipe is broken.

Diagnostic Procedure

Run the following commands in an elevated PowerShell session on the affected host.

1. Confirm the named pipe exists

```
Get-ChildItem \\.\pipe\ | Where-Object Name -like "*ntapvscp*"
```

2. Confirm RPC over the local NPFS path works (bypasses SMB)

```
rpcping -s . -t ncacn_np -e \pipe\ntapvscp -v 3
```

A successful result (`Completed 1 calls in N ms`) proves the pipe and the local RPC stack are healthy.

3. Reproduce the failure over the SMB path

```
rpcping -s 127.0.0.1 -t ncacn_np -e \pipe\ntapvscp -v 3
```

A failure with `Exception 1722` and an inner status of `0x40` (`ERROR_NETNAME_DELETED`) or `0x3B` (`ERROR_UNEXP_NET_ERR`) confirms the SMB path is broken.

4. Test TCP 445 reachability on loopback

```
Test-NetConnection 127.0.0.1 -Port 445
```

`TcpTestSucceeded : False` indicates nothing is listening on TCP 445.

5. Identify which layer is broken

```
# Is the Server service running?
Get-Service LanmanServer, LanmanWorkstation

# Is anything listening on 445?
Get-NetTCPConnection -LocalPort 445 -State Listen
netstat -ano | findstr :445

# Is SMB Server bound to any network interface?
Get-SmbServerNetworkInterface

# What does the firewall rule for SMB-In look like?
Get-NetFirewallRule -DisplayName "File and Printer Sharing (SMB-In)" |
  Format-Table DisplayName, Enabled, Profile

# Is "File and Printer Sharing for Microsoft Networks" bound to the
active adapter?
Get-NetAdapterBinding -ComponentID ms_server

# What is the active network profile?
Get-NetConnectionProfile
```

A typical hardened-host signature is:

- `LanmanServer` is running.
- `Get-NetTCPConnection -LocalPort 445 -State Listen` returns nothing.
- `Get-SmbServerNetworkInterface` returns nothing.
- The `File and Printer Sharing (SMB-In)` firewall rule is `Enabled: False`.
- `Get-NetAdapterBinding -ComponentID ms_server` shows `Enabled: False` on the active adapter.

Resolution

The fix restores SMB inbound on the host while keeping the customer's hardening intact for everything except loopback.

Run the following in an elevated PowerShell session:

```
# 1. Enable the inbound firewall rule for SMB
Enable-NetFirewallRule -DisplayName "File and Printer Sharing (SMB-In)"

# 2. Scope the rule to loopback only (do not expose 445 on the network)
Set-NetFirewallRule -DisplayName "File and Printer Sharing (SMB-In)" -
RemoteAddress 127.0.0.1

# 3. Re-bind "File and Printer Sharing for Microsoft Networks" to the
active adapter
Enable-NetAdapterBinding -Name "Ethernet" -ComponentID ms_server

# 4. Restart the Server service so it picks up the new binding
Restart-Service LanmanServer -Force
```

If the active adapter is named something other than `Ethernet`, substitute the correct name from `Get-NetAdapterBinding -ComponentID ms_server`.

Verification

After applying the fix, run the following to confirm each layer is healthy:

```
# Adapter binding restored
Get-NetAdapterBinding -ComponentID ms_server
# Expected: active adapter shows Enabled : True

# SMB Server bound to interface
Get-SmbServerNetworkInterface
# Expected: at least one row returned

# TCP listener up on 445
Get-NetTCPConnection -LocalPort 445 -State Listen
# Expected: LocalAddress :: , LocalPort 445, State Listen,
OwningProcess 4

# Loopback reachability
Test-NetConnection 127.0.0.1 -Port 445
# Expected: TcpTestSucceeded : True

# SMB session establishment works
net use \\127.0.0.1\IPC$
# Expected: "The command completed successfully"

# RPC over the SMB path now works
rpcping -s 127.0.0.1 -t ncacn_np -e \pipe\ntapvscp -v 3
# Expected: Completed 1 calls in N ms
```

Once `rpcping` succeeds against the SMB path, reproduce the original failure with the OPSWAT ONTAP Connector. The connector should now open the pipe and complete the RPC

call without `RPC server is unavailable`, and `VS_Registration2` should complete successfully.

Why This Happens on Hardened Hosts

Common hardening baselines disable inbound SMB to reduce lateral-movement risk. Typical changes include:

- Disabling the `File and Printer Sharing (SMB-In)` firewall rule for all profiles.
- Unchecking “File and Printer Sharing for Microsoft Networks” on every network adapter, which removes the binding the SMB Server uses to create its TCP 445 listener.
- Stopping or disabling the `LanmanServer` service.

Any one of these disables inbound SMB. The hardened host in this case had two of the three applied (the firewall rule and the adapter binding). The Server service was still running, but with no adapter binding it had nothing to listen on, so port 445 was effectively closed even on loopback.

Recommendations

For the customer

1. Document the exception in the host’s hardening baseline. A subsequent hardening sweep applied through GPO, Intune, or a hardening tool will revert these settings unless the exception is encoded in the baseline.
2. Keep the firewall rule scoped to `127.0.0.1` only. This restores SMB exactly enough for same-host named-pipe IPC and does not expose port 445 to the network.
3. If an EDR product is present, verify it does not re-block SMB at the session layer. Some EDRs flag SMB sessions as lateral movement and reset them even when the OS allows the traffic.

Reference: Error Codes Encountered

Code	Hex	Name	Meaning
1722	0x6BA	RPC_S_SERVER_UNAVAILABLE	Top-level RPC error surfaced to the client
64	0x40	ERROR_NETNAME_DELETED	The specified network name is no longer available (no SMB listener)
59	0x3B	ERROR_UNEXP_NET_ERR	An unexpected network error occurred (SMB session/negotiation failure)
1706	0x6AA	RPC_S_NO_ENDPOINT_FOUND	rpcping endpoint string formatted incorrectly (no real failure)

Reference: rpcping Endpoint Syntax

When `-s` already specifies the server, the `-e` argument must be the bare endpoint name without server prefix:

Form	Result
`-s 127.0.0.1 -e \pipe tapvscp`	Correct (SMB path)
`-s . -e \pipe tapvscp`	Correct (local NPFS path)
`-s 127.0.0.1 -e \\.\pipe tapvscp`	Returns 1706
`-s 127.0.0.1 -e \\127.0.0.1\pipe tapvscp`	Returns 1706

INSTALLATION

Unable to remove docker network

If you encounter some message regarding your network:

network mdss_stack id xxx has active endpoints

while you tried to remove or update MDSS, please try to restart docker:

```
systemctl restart docker
```

Running behind a proxy

Application-level proxy (customer.env)

MDSS services read proxy settings from `/etc/mdss/customer.env` (see Custom configuration).

```
HTTP_PROXY="http://proxy_ip:proxy_port"
HTTPS_PROXY="https://proxy_ip:proxy_port"

NO_PROXY=apigateway,commonservices,core,discoveryalibabacloudservice,discoveryamazonsdkservice,discoveryazureblobservice,discoveryazurefileservice,discoveryboxservice,discoverygooglecloudservice,discoverymftservice,discoverynfsservice,discoveryonedriveservice,discoveryservice,discoverysftpservice,discoverysmbservice,jobdispatcher,licensingservice,loadbalancerservice,loggingservice,mongodb,mongomigrations,nfsservice,node,notificationservice,pgmigrations,postgres,rabbitmq,redis,remediationsservice,remediationsservice-alibabacloud,remediationsservice-amazonsdk,remediationsservice-azureblob,remediationsservice-azurefiles,remediationsservice-box,remediationsservice-googlecloud,remediationsservice-mft,remediationsservice-nfs,remediationsservice-onedrive,remediationsservice-sftp,remediationsservice-smb,scanningservice,sftpservice,smbservice,storagesservice,storagesservice-alibabacloud,storagesservice-amazonsdk,storagesservice-azureblob,storagesservice-azurefiles,storagesservice-box,storagesservice-googlecloud,storagesservice-mft,storagesservice-nfs,storagesservice-onedrive,storagesservice-sftp,storagesservice-smb,identityservice,webclient,workflowmanagerservice
```

```
HTTP_PROXY="http://username:password@proxy_ip:proxy_port"
HTTPS_PROXY="http://username:password@proxy_ip:proxy_port"

NO_PROXY=apigateway,commonservices,core,discoveryalibabacloudservice,di
scoveryamazonsdkservice,discoveryazureblobservice,discoveryazurefilesse
rvice,discoveryboxservice,discoverygooglecloudservice,discoverymftservi
ce,discoverynfsservice,discoveryonedriveservice,discoveryservice,discov
erysftpservice,discoverysmbservice,jobdispatcher,licensingservice,loadb
alancerservice,loggingservice,mongodb,mongomigrations,nfsservice,node,n
otificationservice,pgmigrations,postgres,rabbitmq,redis,remediationsser
vice,remediationsservice-alibabacloud,remediationsservice-
amazonsdk,remediationsservice-azureblob,remediationsservice-
azurefiles,remediationsservice-box,remediationsservice-
googlecloud,remediationsservice-mft,remediationsservice-
nfs,remediationsservice-onedrive,remediationsservice-
sftp,remediationsservice-
smb,scanningservice,sftpservice,smbservice,storagesservice,storagesserv
ice-alibabacloud,storagesservice-amazonsdk,storagesservice-
azureblob,storagesservice-azurefiles,storagesservice-
box,storagesservice-googlecloud,storagesservice-mft,storagesservice-
nfs,storagesservice-onedrive,storagesservice-sftp,storagesservice-
smb,identityservice,webclient,workflowmanagerservice
```

> **Warning**
>
> The configured scan instance address should also be added to the `no_poxy` list if connecting to it does not require a proxy.

Docker daemon proxy (pulling MDSS images)

If a proxy is required to access to docker hub in order to pull MDSS images, then this guide should be followed: https://docs.docker.com/network/proxy/

Create the drop-in config file or edit it if it already exists:

```
sudo mkdir -p /etc/systemd/system/docker.service.d
sudo nano /etc/systemd/system/docker.service.d/http-proxy.conf
```

Set the proxy settings:

```
[Service]
Environment="HTTP_PROXY=http://proxy_ip:proxy_port"
Environment="HTTPS_PROXY=http://proxy_ip:proxy_port"
Environment="NO_PROXY=localhost,127.0.0.1"
```

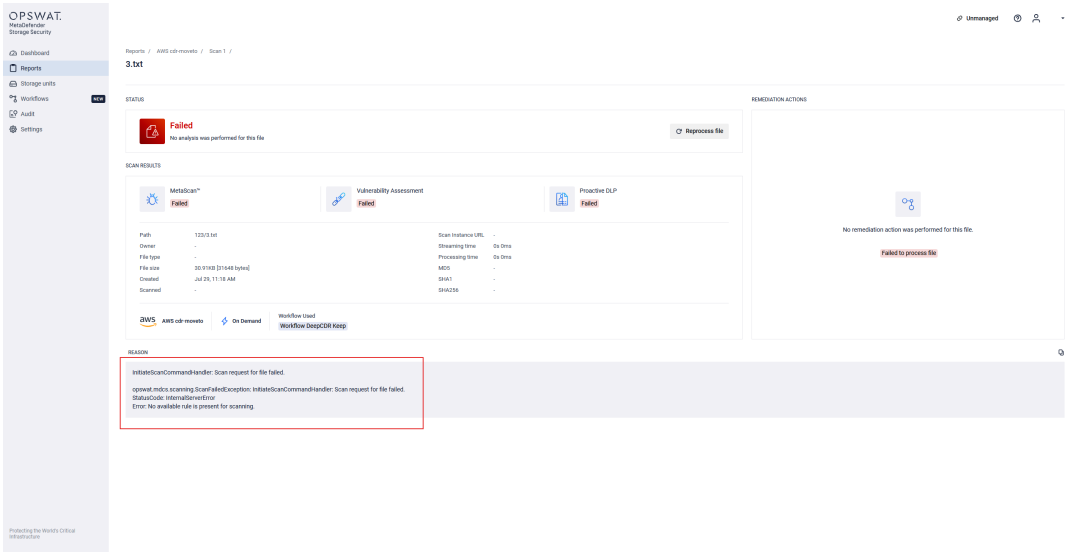
Apply the changes:

```
sudo systemctl daemon-reload
sudo systemctl restart docker
```

Why I am getting error "No available rule is present for scanning"

When triggering a scan, you may encounter a scan failure with the following error message:

> **Error**
>
> opswat.mdcs.scanning.ScanFailedException: InitiateScanCommandHandler: Scan request for object failed. StatusCode: InternalServerError Error: No available rule is present for scanning.



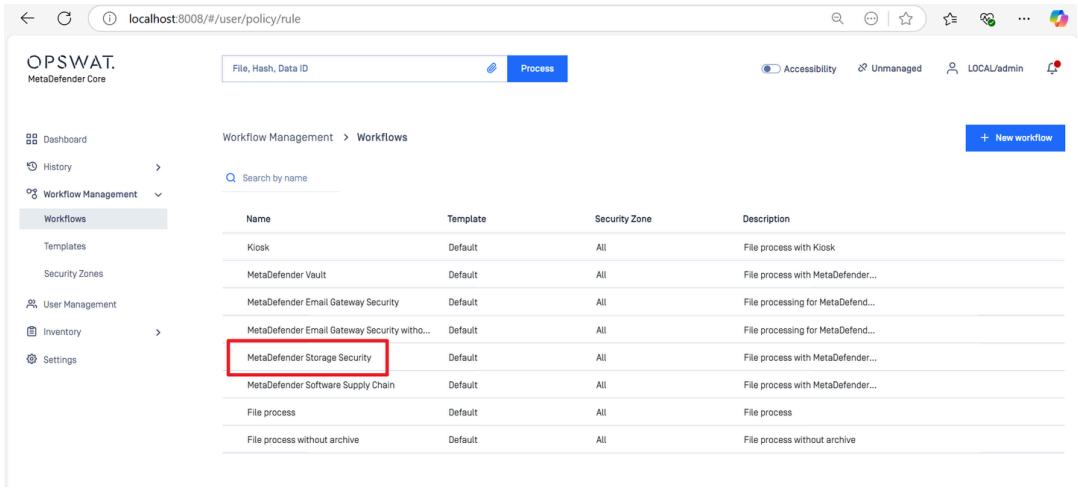
Cause

This error typically occurs when the workflow name configured in MetaDefender for Secure Storage (MDSS) does not match the workflow name set in MetaDefender Core.

MetaDefender Storage Security

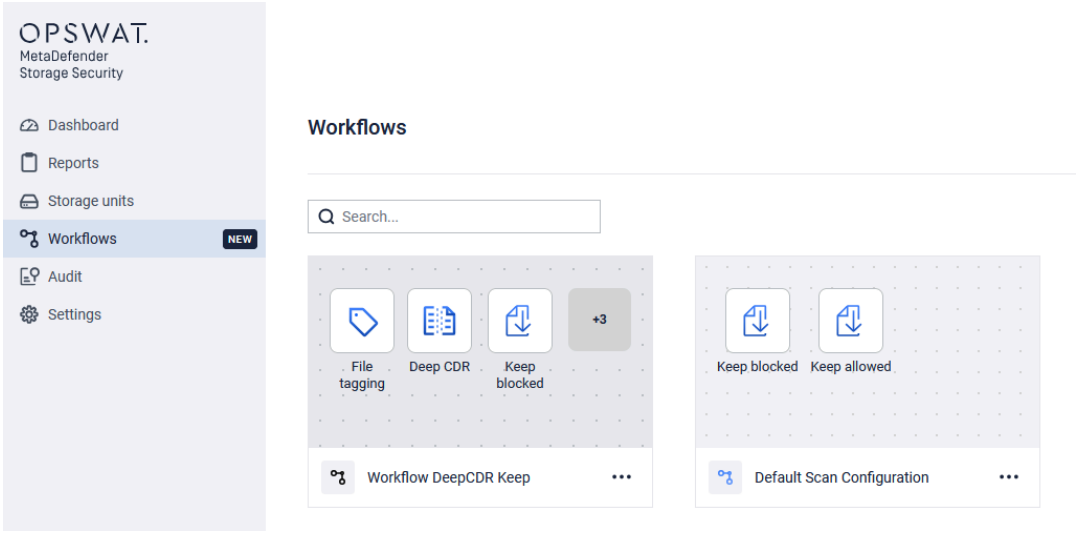


MetaDefender Core



Steps to Resolve:

1. **Log into MetaDefender Core**
   - Navigate to Workflows.
   - Identify the workflow associated with MDSS.
   - The workflow name should be either: “MetaDefender Storage Security” or “MetaDefender for Secure Storage”
2. **Verify and Update the Workflow in MDSS**
   - If the workflow name in Core is “MetaDefender Storage Security”, log into MDSS Configuration.
   - Go to **Workflows** and click on your workflow



- Edit the scan configuration and update the rule name to “MetaDefender Storage Security”.



- Ensure the workflow name exactly matches the one in Core.

3. **Apply Changes and Restart the Service**

- Click “Save” to save the configuration.
- Restart the scanning service if necessary and retry the scan to verify if the issue is resolved.

> **Support:**
>
> If **Further Assistance** is required, please proceed to log a **support case or chatting with our support engineer**.

Why am I getting the 'Configured user limit on inotify instances has been reached' error in MDSS on Linux/Kubernetes?

Linux uses **inotify** to monitor file system events, but it enforces limits on how many files and directories a single user can watch. The default limits (often **128 instances** and **8,192 watches**) are too low for Kubernetes workloads. You will need to raise this value higher to run MDSS.

> **Please Note:**
>
> If using a **cloud-managed cluster** (e.g., GKE, EKS, AKS), nodes are preconfigured, and changes may not be necessary or possible. Ensure this setting is adjusted on **all Kubernetes nodes** if needed.

Sample Error Log:

```
[2025-03-27 08:02:01Z] [Fatal] : Unable to start Discovery service
|
 System.IO.IOException: The configured user limit (128) on the number
of inotify instances has been reached, or the per-process limit on the
number of open file descriptors has been reached.        |
   at System.IO.FileSystemWatcher.StartRaisingEvents()
|
    at
Microsoft.Extensions.FileProviders.Physical.PhysicalFilesWatcher.TryEna
bleFileSystemWatcher()     |
    at
Microsoft.Extensions.FileProviders.Physical.PhysicalFilesWatcher.Create
FileChangeToken(String filter)
|
    at
Microsoft.Extensions.Primitives.ChangeToken.ChangeTokenRegistration`1..
ctor(Func`1 changeTokenProducer, Action`1 changeTokenConsumer, TState
state)                                    |
    at Microsoft.Extensions.Primitives.ChangeToken.OnChange(Func`1
changeTokenProducer, Action changeTokenConsumer)
|
    at
Microsoft.Extensions.Configuration.FileConfigurationProvider..ctor(File
ConfigurationSource source)
|
    at
Microsoft.Extensions.Configuration.Json.JsonConfigurationSource.Build(I
ConfigurationBuilder builder)
|
    at Microsoft.Extensions.Configuration.ConfigurationBuilder.Build()
|
    at
Microsoft.Extensions.Hosting.HostBuilder.InitializeAppConfiguration()
|
    at Microsoft.Extensions.Hosting.HostBuilder.Build()
|
    at opswat.mdss.discovery.service.Program.Main(String[] args) in
/app/Backend/src/Discovery/opswat.mdss.discovery.service/Program.cs:lin
e 27
```

You can check your current inotify instances of your nodes by running these commands:

```
sysctl fs.inotify.max_user_instances
sysctl fs.inotify.max_user_watches
```

```
root@cxk8s-server-01:~# sysctl fs.inotify.max_user_instances
fs.inotify.max_user_instances = 128
root@cxk8s-server-01:~# sysctl fs.inotify.max_user_watches
fs.inotify.max_user_watches = 8192
```

Solution:

1. To immediately raise the limits without restarting, run:

```
sudo sysctl -w fs.inotify.max_user_instances=8192
sudo sysctl -w fs.inotify.max_user_watches=1048576
```

This takes effect immediately but will reset after a reboot. You can modify the values to be higher based on your needs.

2. To ensure these limits remain after a restart, add them to the system configuration file:

```
echo "fs.inotify.max_user_instances=8192" | sudo tee -a
/etc/sysctl.conf
echo "fs.inotify.max_user_watches=1048576" | sudo tee -a
/etc/sysctl.conf
```

3. Once updated, apply the new settings by running:

```
sudo sysctl -p
```

> **Support:**
>
> If **Further Assistance** is required, please proceed to log a support case or chat with our support engineer.

How to handle empty objects in Discovery?

To skip the discovery of empty objects, please add the following property in your `customer.env` file:

```
DISCOVERY_SERVICE_IGNORE_EMPTY_OBJECTS=1
```

By default, this value is set to 0, which means we will **not** ignore empty objects.

After the property is added in your `customer.env` file, please restart MetaDefender Storage Security for changes to take effect.

Permission denied while uninstalling on Linux

On some Linux distributions that have **SELinux (Security-Enhanced Linux)** enabled by default you may encounter a “Permission denied” message when uninstalling MDSS. The uninstall still completes successfully and only some docker containers might still be left running if `mdss -u clean` was not executed before the uninstall. This is due to SELinux

policies and can be avoided by disabling SELinux temporarily before uninstalling by running:

```
sudo setenforce 0
```

Portable package and offline docker toolkit are not starting due to RabbitMQ deprecated feature not being permitted?

After deploying MetaDefender Storage Security from the **portable package** or the **offline Docker toolkit**, the product does not become available. The `mdcs_rabbitmq` container is running, but the backend containers (licensing service, API gateway and the other services) restart continuously.

Service logs contain repeated entries similar to:

```
[Fatal] : (EventBusLibrary) RabbitMq subscribeChannel has been closed
unexpectedly
(ReplyCode: 541, ReplyText: INTERNAL_ERROR - Feature
`transient_nonexcl_queues` is deprecated.
By default, this feature is not permitted anymore.)
```

Messages such as `nc: bad address 'licensingservice'` or `Error loading shared library libgssapi_krb5.so.2` may also appear. These are side effects of the restart loop, not the cause.

Affected deployments:

| **Versions** | 4.5.0 and 4.5.1 |

| **Affected** | Portable package, offline Docker toolkit |

| **Not affected** | Deployments made with the Linux (RPM/DEB) or Windows installers |

Confirming the issue

Run the following in your MDSS deployment directory:

```
ls -la ./rabbitmq/
```

If `rabbitmq.conf` is listed as a directory (a `d` at the start of the permissions column) instead of a regular file, this issue applies to your deployment.

You can confirm it a second way:

```
docker exec mdcs_rabbitmq rabbitmqctl eval
'rabbit_deprecated_features:is_permitted(transient_nonexcl_queues).'
```

A healthy deployment returns `true`. An affected deployment returns `false`.

Solution:

Run these commands in your MDSS deployment directory:

```
sudo rm -r ./rabbitmq/rabbitmq.conf
echo 'deprecated_features.permit.transient_nonexcl_queues = true' |
sudo tee ./rabbitmq/rabbitmq.conf
sudo chmod 704 ./rabbitmq/rabbitmq.conf
sudo ./mdss.sh -c restart
```

The services reconnect automatically once RabbitMQ restarts. Verify the result with:

```
docker exec mdcs_rabbitmq rabbitmqctl eval
'rabbit_deprecated_features:is_permitted(transient_nonexcl_queues).'
```

The command must now return `true`, and the service containers must stop restarting.

> The missing file is included in the packages starting with version **4.5.2**. New deployments made from 4.5.2 or later are not affected.

> **When upgrading an affected deployment,** apply the `rm -r` step above at least once. As long as `rabbitmq.conf` exists as a directory, neither unpacking a newer package nor running an update can replace it with the correct file, and the deployment remains affected after the upgrade.

INTEGRATIONS

NFS storage unit is not detecting any files

Root Cause

The `nolock` flag was not included in the NFS mount command previously. While it is generally not required, certain environments, especially those using older NFS servers or specific NFS configurations, depend on this flag to ensure proper file access during MDSS scans. In such cases, omitting the `nolock` flag can lead to scanning failures.

Some older NFS servers lock files when opened by another application, which prevents MDSS from scanning them. To prevent this issue, the `nolock` flag is required in the mount command.

Solution

[Linux]

1. Execute the following command to mount the NFS storage: `sudo mount -o nolock {nfs_server_ip}:/srv/company-shared-files /mnt/mdss/nfs/company-files`

This command mounts the shared files from the NFS Server to the company-files directory on the NFS Client.

2. Ensure Persistent Mounting To maintain the mount across reboots, add the following entry to the `/etc/fstab` file: `{nfs_server_ip}:/srv/company-shared-files /mnt/mdss/nfs/company-files nfs rw,hard,intr,nolock 0 0`

Without this step, the mount will be lost when the NFS Client machine is restarted.

For more details, refer to this article: [Linux] How to add an NFS storage unit

[Windows]

For instructions on setting up NFS storage in Windows, refer to the following article: [Windows] How to add an NFS storage unit

Following the instruction mentioned in the article and in the terminal, run the following command:

```
mount -o "nolock,sec=sys" {nfs-server-ip}:{nfs-share-location} {mounted-drive}
```

For example, the NFS share will be mounted in the Y drive:

```
mount -o "nolock,sec=sys" 192.168.207.139:/srv/company-public-files/ Y:
```

> **Support:**
>
> If **Further Assistance** is required, please proceed to create a support case or chat with our support engineer.

Why my files are not moving on SharePoint On-Prem with MDSS, despite UI confirmation?

Issue

When moving files within SharePoint On-Prem, the UI indicates that the file has been successfully moved. However, upon verification, the file is not transferred to the target destination.

Root Cause

The issue occurs due to missing handling for maintaining folder structures during the file movement process.

Solution

Upgrade MetaDefender Storage Security to version **3.5.3 or later**, where proper handling for folder structure preservation in SharePoint On-Prem has been implemented.

> **Support:**
>
> If you encounter any issues during the upgrade process or require further assistance, please contact OPSWAT support via My OPSWAT at: Home - My OPSWAT
>
> Our support team will be able to provide you with the necessary guidance and resolution for any upgrade or compatibility concerns.

Scan stuck in the "processing" state on the SMB Service

Symptom

The log appears to be stuck with the following entries:

```
Starting processing server. Listening on 127.0.0.1:6002
```

```
Starting health server. Listening on 127.0.0.1:7002
```

`Using configured transport receive timeout of: 600 Starting worker`

Under normal conditions, the system should continuously log events in all `600x` files instead of remaining stuck at this stage.

Possible Cause

SMB Service process stuck due to insufficient CPU resources The `psutil.open_files()` function hangs or freezes for several minutes, issue occurs specifically on Windows.

Solution

The issue was fixed starting with Version 3.5.2

> **Support:**
>
> If Further Assistance is required, please proceed to create a support case or chat with our support engineer.

Release Notes

Release notes

MetaDefender™ Storage Security 4.5.2

Release date: August 19, 2026

End of support: February 19, 2028

Maintenance Release

- Deep CDR carries dedicated workflow branches for file types it does not sanitize, so you can keep, move, copy or delete them and clear the source folder in one pass.
- Workflows validate before a scan runs, and Deep CDR requires an API key on every scan instance in the primary and failover pools.
- Reports name the exact outcome per file, including unsupported file types, the sanitization detail returned by MD Core, and the remediation you configured.
- Scanning applies a retry budget while MD Core is busy and holds its scaling steady while an instance is unavailable, so throughput stays predictable under load.
- Stopping a real-time scan completes in seconds, the report refreshes on its own, and rescan sits in the report actions.
- Schedules coordinate so a location runs one scan at a time, consecutive FTP scans run back to back, and real-time scans follow newly created child folders.
- The portable package and the offline Docker toolkit deploy on a clean host, and upgrades carry databases holding non-Latin file names.
- MDSS runs on the cache you already have, including AWS ElastiCache, and reads CPU and memory from pod limits on Kubernetes.
- The NetApp ONTAP Connector ships at 1.0.44 with the full share path, so several SVMs connect to one MDSS.
- OPSWAT SAML sign-on, email notifications and telemetry collectors follow your configuration, and inventory tables let you pick the columns you need.

MetaDefender™ Storage Security 4.5.1

Release date: July 30, 2026

End of support: January 30, 2028

Maintenance Release

- Real-time protection jobs each apply their own workflow, so multiple policies can run against a single storage unit.

- Disk usage in the warning band keeps scanning running, scan health reflects real load, and autoscaling ships enabled on all deployment types with per-instance sizing recommendations.
- The NetApp ONTAP Connector delivers files over HTTPS, and you can configure the response it returns to NetApp when a file scan times out.
- Real-time protection keeps its status and discovery cycle detail, and partition-based FTP scans resume without reconfiguration.
- Stopped jobs report accurately, their files can be rescanned in place, FTP scans run to completion, and event-based scans handle partitioned storage units.
- Remediation actions deliver to a second destination, tags follow files moved into folder-based units, and Central Management copy workflows run as configured.
- PDF exports honor the filters you applied accurately per storage unit.
- The dashboard loads faster against a 10 million file scan with a searchable unit selector, and job schedules support valid month days and 52-week cycles.
- Single sign-on from the virtual appliance keeps its identity provider, notification targets are validated, and S3 accounts show the correct region and endpoint fields

---

MetaDefender™ Storage Security 4.5.0

Release date: July 22, 2026

End of support: January 22, 2028

Highlights

MetaDefender Storage Security 4.5.0 introduces a redesigned user interface, centralized management through OPSWAT Central Management (OCM) v10, a new autoscaling engine, significant security enhancements, and multiple platform and storage integration improvements.

New Features

Redesigned User Interface

The application has been rebuilt using the Blue Line design system, delivering a modern user experience with:

- Updated Dashboard, Reports, Inventory, Jobs, Workflows, Settings, and Users pages
- Improved reporting with dedicated Threats, Sanitization, and Data Loss Prevention views
- Guided onboarding for first-time deployments

- Dark theme support
- Backward-compatible legacy URL redirects

OPSWAT Central Management (OCM) v10 Integration

MetaDefender Storage Security now supports centralized management through OCM v10, including:

- Instance enrollment and license management
- Remote configuration
- Deployment ID synchronization across managed environments

Autoscaling Engine

A new autoscaling engine dynamically adjusts system resources based on workload.

Key capabilities include:

- CPU, memory, and file throughput monitoring
- Scaling recommendations
- `/healthz` endpoint for health monitoring
- Dashboard visibility into scaling status

Supported deployment models include MetaDefender Core, Cloud and Distributed Cluster.

New SMB Service for Windows deployments

The Windows SMB Service is a new, fully in-house SMB client implementation for Windows deployments. Built with no third-party dependencies, it delivers improved reliability and resolves the connection issues found in earlier versions.

Security Improvements

This release includes multiple security enhancements, including:

- Fixes for OData injection vulnerabilities
- License forgery protection
- Penetration testing remediations, including JWT secret removal, improved SSO security, and sensitive data protection
- Non-root container enforcement for Kubernetes deployments
- Improved Windows file permission security

Platform Improvements

Platform updates include:

- Updated infrastructure components (RabbitMQ, Garnet, Alpine Linux)
- Improved job dispatcher with automatic recovery for orphaned scan jobs
- Configurable scan result retention policies
- Database growth monitoring and protection
- Decoupled scanning service architecture for cross-product reuse
- Prevention of overlapping scans within storage groups
- Optimized scanning and results storage for archives

Storage and Integration Improvements

Storage connectors have been enhanced with improved reliability and functionality, including:

- Better error reporting for NFS and SFTP
- Improved SharePoint Cloud real-time protection
- Microsoft Graph connection throttling for OneDrive and SharePoint
- NetApp ONTAP enhancements
- Autodiscovery support for all S3-compatible storage providers
- Updated Diode integration documentation

Telemetry

Telemetry has been renamed **Usage Report** and now includes:

- Kubernetes containerized collector
- Improved usage reporting accuracy

Resolved Issues

This release resolves several issues, including:

- Scheduled scans starting at incorrect times due to timezone offsets
- Recovery of cancelled or stuck scan jobs after service restart
- Dashboard threat counts matching report data
- Improved stability when scanning large file volumes
- RabbitMQ startup synchronization issues

- Improved error handling across storage integrations

Known limitation: Remediation counters on reports for scans performed before version 4.0.0

After upgrading from a version earlier than 4.0.0, reports for scans that completed on the older version may display inconsistent remediation counters:

- The **Keep** counter may show 0 even when files were kept.
- The **Remediated** counter excludes kept files, so it may show 0 when keeping files was the only configured remediation action.

All other values on these reports remain accurate, including the allowed and blocked file totals and the **Move**, **Copy**, **Delete**, and **Tagging** counters.

This limitation applies only to scans completed before the upgrade. Scans performed after the upgrade display all counters correctly.

Changelog

MetaDefender Storage Security v4.4.2

Release Date: May 14, 2026

Version supported until November 14, 2027

Maintenance Release
- **SFTP scan reliability.** Fixed an issue where SFTP scans could fail with repeated connection errors against servers that limit concurrent sessions. - **Windows upgrade from v3.6.1 and v4.4.0.** Fixed a crash during the MongoDB migration step that blocked Windows upgrades to the latest version. - **Offline toolkit package.** Fixed the offline installer so air-gapped deployments include all required components and the platform service starts as expected. **Maintenance Release (v4.4.1)** - **NGINX security update.** Updated NGINX to 1.31.0, which patches CVE-2026-42945. Previous MDSS versions are not affected by this CVE; the update ships as a precaution. - **RTP validation for circular remediations.** Real-time scans now reject workflows whose move or copy remediation targets the same storage unit being scanned, preventing the retry loop seen previously. - **Additional S3 region.** Added the New Zealand (ap-southeast-6) region to the AWS S3 and S3-compatible storage selectors. - **Reduced error log noise.** Cleaned up spurious error log entries from background job cleanups and certain file-download failure paths.
Highlights - **New Storage Integration: Scality RING -** Added native integration for Scality RING S3-compatible object storage, with full coverage for multiscanning, CDR, DLP, file tagging, and remediation actions. - **Azure Blob storage autodiscovery.** Azure Blob accounts can now automatically discover and onboard new containers as they are created. Container selection can be fully automatic or scoped to a manual subset, and the feature can be toggled per account. - **Access Control (ABAC Phase I).** New Settings → Access Control tab showing default roles and their permissions. - **Real-Time Processing start date.** Added an optional "Pick files modified since" date picker to the RTP scan modal, so older files (e.g., OneDrive uploads that retain their original `LastModified`) can be included in the scan. - **Scan size visibility.** Individual scan reports and active scans now show `Total Files Size` and `Processed Files Size`, and `Total Files Count` is back in the report view. - **Users included in config export/import.** Configuration export can now optionally include MDSS users (local and SSO), with matching users reconciled on import.
Improvements - **Scan reliability and gRPC performance.** Reused gRPC channels across NFS/SFTP discovery, object operations, and telemetry to prevent port exhaustion; added watchdog timeouts and retries to prevent stuck scans and stuck remediations; fixed timing edge cases that could mark instant scans complete prematurely; and added parallel consumers on non-priority RPC queues for better authentication throughput. - **Logging and diagnostics.** Added a separate error/warning log file with its own rotation, persisted PostgreSQL/Redis/RabbitMQ logs across container restarts, identified the specific MD Core instance in API key failure logs, and clarified the support package export error around `LOGS_PER_SERVICE`. - **Cancel on-demand scans from Reports.** On-demand scans can now be cancelled directly from the Reports tab, matching the existing RTP cancel behavior. - **Persistent service scaling.** Extra service instances can now be configured in `customer.env` and survive upgrades. - **Discovery throttling for Discovery-Only scans.** Added configurable queue-depth-aware throttling so Discovery-Only workflows back off when downstream queues are saturated and resume once they drain. - **Scan reliability guardrails.** Scans no longer get stuck on slow storage or remediation, and instant scans now wait for discovery to actually finish before reporting completion. - **Workflow display in scan details and reports.** Active scan details now show only the currently running workflow, while reports keep the full workflow history with a clearer "current vs. previously used" layout. - **Adaptive Analysis status accuracy.** Adaptive Analysis and Sandbox now show "Skipped" (not "Failed") when MD Core skipped the file, and clean verdicts display a green badge. - **Adding storage no longer auto-starts a full RTP scan.** New storage units are created without an automatic RTP scan, so the Reports view stays clean until you explicitly start one. - **Delete**

RTP scans from Reports. RTP scans (including partition scans) can now be deleted from the Reports page, not just cleaned, with support for bulk and mixed-type deletion. - **Timestamps and cleaner messages on RTP errors.** Expanded error details now show when each error occurred and present a friendlier message without raw stack traces. - **Upgrade reliability.** Fixed Windows upgrades silently overwriting `customer.env`, and restored RTP partition scans that stopped working after upgrading to 4.3.0. - **Stability at scale.** Reduced Garnet memory usage on Windows and fixed a service crash triggered by a large number of scans in the database. - **Integration fixes.** Resolved a SharePoint Online issue where slow Graph subscription creation prevented RTP from starting, and blocked the same GCP bucket from being added twice through different credential types (ADC vs. keys). - **Dependency upgrades.** Upgraded RabbitMQ to 4.2.4, Redis to 8.6.0, and Garnet to 1.0.99.

Info - Upgrades from v4.3.0 or earlier

RTP behavior during upgrade.*This applies when upgrading from any version older than v4.3.1. Customers already on v4.3.1 or later are not affected.*

Active RTP scans are paused during the upgrade and resume automatically once it completes. Files added or modified during the upgrade window can be picked up by running an RTP report cleanup afterward with RTP Handling with Comprehensive Detection enabled. On NAS storage units this cleanup reprocesses all files and may take some time depending on volume.

MetaDefender Storage Security v4.3.2

Release Date: April 03, 2026

Version supported until: October 03, 2027

Highlights

Workflow Cards: Storage Unit Destination

- Workflow cards now show which storage units are set as destinations for remediation actions, so you can quickly see where your data ends up.
- **How to enable:** Navigate to Workflows and select Extended View from the top right.

Improvements

- Certificates are now picked up automatically after a machine restart, without requiring a product restart separately.
- Fixed a race condition during Podman restarts that previously caused orphaned containers running in the background.

MetaDefender Storage Security v4.3.1

Release Date: March 06, 2026

Version supported until: September 06, 2027

Improvements

- Resolved issue that malformed scanning paths for active RTP scans and Scheduled Scans, that target partitions, on FTP, NFS, SFTP, SMB, and SharePoint On-Premise storage units
- Resolved issue that forced RTP scans on NAS storage units to reprocess files processed before upgrade

MetaDefender Storage Security v4.3.0

Release Date: March 05, 2026

Version supported until: September 05, 2027

This release introduces Microsoft Teams support for enhanced collaboration security, auto-discovery for SharePoint Online to streamline setup, a new reprocess failed files feature for easier remediation, stability improvements, and concurrent scanning scenarios.

Highlights

- **Multitenancy (MDSS Cloud)**
  - Support for multiple tenants within a single MDSS Cloud deployment
- **OpenTelemetry (Initial Release)**
  - Collect and export telemetry data for monitoring and observability
- **Microsoft Teams Scanning**
  - Scan and sanitize file attachments shared in Microsoft 365 Teams channels and chats
- **SharePoint Online Auto-Discovery**
  - Automatically discover and connect SharePoint Online sites—no manual configuration required
- **Reprocess Failed Files**
  - Create new scans targeting only previously failed files, with the flexibility to apply any workflow
- **Flexible Scan Scheduling**
  - Schedule scans down to the minute for precise timing control
- **Real-Time Protection Limits (Cloud)**
  - Configure scan limits for MDSS Cloud deployments to manage resource usage

Improvements

- **Scan Priority UX**
  - Added tooltips and reordered priority options for clearer configuration
- **Storage Unit Display**
  - Storage unit name now visible in scan configuration for easier identification
- **Sanitization Workflow Control**
  - Original files deleted only after successful sanitization. New option to configure delete behavior separately for allowed and blocked files—enabling workflows like Deep CDR for blocked files only while leaving clean files untouched
- **Connection Reliability**
  - Automatic retry on temporary connection failures
- **Performance**
  - Loading indicator on download button when generating large scan reports
- **Report Export UX**
  - Faster remediation processing for large-scale deployments
- **SMTP Configuration**
  - Input validation for host field with helpful error messages for invalid entries
- **SharePoint Storage Units**
  - Cloud and On-Prem storage units now use Site URL and Document Library URL fields. Existing configurations remain compatible, with a post-upgrade prompt to update
- **Bug Fixes & Documentation**
  - Fixed authentication failures when running multiple SMB scans simultaneously
  - Resolved partition scan errors across all users
  - Reports now correctly deleted only after retention period expires and only for completed scans
  - Notification imports now save valid settings even when some notification types fail validation
  - Updated documentation to reflect recent changes that include UI, windows installs, API keys, and scan reprocess actions.

MetaDefender Storage Security v4.2.0

Release Date: December 15, 2025

Version supported until: May 25, 2026

MetaDefender Storage Security 4.2.0 delivers significant enhancements to cloud integration, identity scanning capabilities, and workflow automation, alongside critical stability improvements and bug fixes.

Highlights

- **GCP Autodiscovery**
  - Automated bucket discovery for Google Cloud Platform
- **Oracle Cloud Enhancements**
  - Improved support for Oracle Native while keeping its S3-compatible storage configurations
- **Cross Domain**
  - Compliant data transfer across classification domains for high-security environments of workloads with isolated toxic handling, RabbitMQ-orchestrated processing, and webhook-based discovery
- **Identity Detection**
  - Identity detection across backup filesystems with PDF reporting and remediation integration. Supports on-demand and scheduled scans with intelligent incremental scanning. Real-time processing (RTP) not supported.
- **PDF Report Enhancements**
  - Improved file distribution visualization, enhanced tooltips, and identity scan results inclusion
- **PostgreSQL Optimization**
  - Resolved stability and performance issues for large-scale deployments

Improvements

- Discovery workflow execution and event-based scanning capabilities
- Advanced file versioning support and remediation workflow performance
- Optimized FTP connection pooling and file discovery mechanisms
- Enhanced MDSS Cloud rate limiting and tenant administrator access controls
- Improved SharePoint OnPrem workflow persistence
- Robust storage account validation and credential management
- Advanced password security in account management interfaces
- Refined form validation for account creation and RabbitMQ configuration
- Improved UI responsiveness and rendering performance across viewing contexts
- Streamlined onboarding experience and intelligent default behaviors
- Enhanced file distribution visualization and reporting accuracy
- Comprehensive RabbitMQ validation, audit logging, and notification delivery

- Refined SMTP lifecycle management
- Improved webhook configuration interface and user guidance
- Optimized database operation efficiency during export operations

MetaDefender Storage Security v4.1.0

Release Date: September 23, 2025

Version supported until March 23, 2027

Highlights

- **Sandbox Analysis Integration**
  - Full sandbox analysis capabilities with MITRE technique mapping and threat intelligence dashboard integrated with MD Cloud and MD Core deployments for advanced threat detection.
- **Storage Management Redesign**
  - New dual view modes (Groups and Accounts) for organizing storage units with comprehensive account-level operations including editing, deletion, and bulk scanning capabilities.
- **HTTPS Configuration**
  - Enable HTTPS directly through the Security settings interface with real-time certificate validation and clear error messages, eliminating lengthy timeout periods.
- **Enhanced Real-Time Protection**
  - Configure multiple RTP scans for different partitions within the same storage unit for all scanning configurations per partition.
- **SharePoint Historical Versions**
  - Scan all historical versions of SharePoint files, not just the latest version, ensuring comprehensive security coverage across file version history.
- **Multiple Workflow Destinations**
  - Configure up to 5 copy/move destinations in workflow remediations

Improvements

- **User Interface**
  - Form consistency across SMB/SFTP and FTP configurations with interactive guided tour for new users
  - Enhanced inline notifications with auto-scroll functionality and completely rebuilt audit system with improved filtering

- **Integration & Connectivity**
  - FTP storage protocol support
  - Enhanced SFTP ports beyond port 22
  - Individual file webhooks for real-time integration and secure syslog transmission with TLS support
- **Security & Platform**
  - Streamlined licensing without legacy SKUs
  - Workflow processing without multiscanning requirements
- **Reporting & Analytics**
  - Enhanced PDF reports with new file statistics and detailed remediation information
  - Proper handling of files with successful scans but failed remediations
- **Bug Fixes & Documentation**
  - Resolved audit expand functionality, filtering issues, and file path handling improvements
  - Comprehensive API documentation updates and myOPSWAT setup instructions

This release focuses on advanced threat detection capabilities and storage management flexibility while enhancing security and user experience across the platform.

MetaDefender Storage Security v4.0.1 (Hotfix)

Release Date: August 25, 2025

Version supported until February 25, 2027

- SMTP Re-activation Issue
  - Fixed a critical functionality bug where SMTP service could not be re-activated after being deactivated, rendering email notifications permanently unusable until system intervention.
- Database Migration Report Recovery
  - Resolved issues where scan reports became inaccessible after upgrading from previous versions (3.5.1/3.6.1), particularly affecting canceled scans and PDF export functionality during database migration processes.
- **Multi-tenancy Filter Disabled for MDSS Cloud**
  - Temporarily disabled PostgreSQL tenant ID filtering for cloud deployments as the multitenancy feature is not yet complete, preventing authentication and permission issues for Tenant Admin users until proper tenant configuration is implemented.

MetaDefender Storage Security v4.0.0

Release Date: August 12, 2025

Version supported until February 12, 2027

Highlights

- Migrated from MongoDB to **PostgreSQL 17** to align with MetaDefender Core and ICAP Server. This simplifies deployments and improves performance for complex queries and large datasets.
- The new **Workflows** feature creates an automated security processing pipeline:
  - 5-stage security processing: Scan Configuration → Advanced Threats → Vulnerabilities → Sanitization → File Tagging
  - Automatically sorts files into Original, Allowed, Blocked, and Sanitized categories
  - Executes automated actions (Copy, Move, Delete) based on scan results
  - Process thousands of files without manual intervention
- **Security Updates**
  - New account creation and login flows
  - Enhanced encryption key handling and secure key rotation
  - Security patches for known vulnerabilities

Improvements

- **Performance**
  - Upgraded RabbitMQ to version 4.1
  - Enhanced SharePoint Cloud real-time processing
  - Custom date range functionality in Dashboard
- **Integration**
  - Upgraded Microsoft Graph SDK to version 5.79.0
  - Added automatic file tagging for Google Cloud Platform
  - Extended AWS regional support
- **Platform**
  - Updated PostgreSQL documentation
  - Improved Azure AD configuration guide
  - Better error handling

This release focuses on database modernization and workflow automation while maintaining platform stability.

MetaDefender Storage Security v3.6.1

Release Date: May 20, 2025

Version supported until November 20, 2026

Highlights

- Streamlined Autodiscovery of S3 Buckets so users can now easily add S3 storage by providing AWS credentials. MetaDefender Storage Security can now automatically discover available buckets, allowing you to enable continuous discovery or manually select buckets for integration via a simplified interface.
- Advanced Remediation Options
  - Configure 'Empty Folder Cleanup' to preserve specific subfolders during parent folder deletion, preventing critical data loss.
- Expanded SharePoint Support
  - Integrate with SharePoint Online Government Cloud (GCC) using a simple configuration checkbox for correct authentication.
  - Discover, scan, and manage content within SharePoint On-Premises subsites, providing comprehensive coverage for hierarchical structures.
- Granular File Rescan so users can rescan individual files directly from scan reports without needing to rescan the entire storage unit or move files, significantly improving efficiency for addressing specific issues.

Improvements

- My OPSWAT Central Management Integration: Access My OPSWAT Central Management settings (SMTP, Notifications, License, Data Retention, Syslog) more easily within MetaDefender Storage Security and utilize integrated read-only user roles, including permissions for managing user invitations.
- Improved Error Handling & Feedback: Enhanced API error handling provides more specific, actionable messages (distinguishing connection, permission, config issues) in a standardized format, improving troubleshooting and UI feedback. Added a clearer error message when attempting to add storage without existing scan configurations.
- UI & UX Refinements
  - The MetaDefender Storage Security Cloud UI now hides unavailable integration options for better clarity.
  - Dashboard charts have an improved "no data" state visualization.
  - User Management features backend-powered search with input validation and minor bug fixes.
  - File remediation details are displayed more comprehensively in the UI.

  - The “Manage Storage Unit” interface now allows separate editing of storage settings and underlying account credentials.

- API & Backend Improvements
  - Real-Time Processing (RTP) scan reports now have a default, non-null name for consistent API identification.
  - API key security is enhanced: copying is restricted to the moment of generation, and GET requests for keys are disallowed.
  - The ‘Scan Folder’ API now prevents conflicts with ‘Delete Empty Folders’ remediation by returning a `400 Bad Request`.
- Deployment & Scalability
  - The MongoDB database name used by MetaDefender Storage Security is now configurable, supporting external MongoDB instances with predefined names.
  - Improved reliability for scanning large SharePoint On-Premises deployments by managing request rates and using retry mechanisms.
  - Enhanced internal component version identification for cross-platform consistency.
- More Reliable Windows Deployments by reducing failures and simplified setup through preemptive port validation and improved installation configuration.
- Stronger Security & Data Accuracy by ensuring secured MetaDefender Core connectivity (HTTPS) and corrected S3 file tagging for dependable security verdicts.
- Faster Windows Performance & Simpler Stack by improving speed and streamlined dependencies by migrating Windows caching to Garnet.

MetaDefender Storage Security v3.6.0

Release Date: March 31, 2025

Version supported until September 30, 2026

Highlights

- MDSS has undergone a major overhaul, featuring a redesigned UI and achieving feature parity with previous versions.
- Users now control scanning priority (performance or thoroughness) for storage unit scans, allowing for tailored resource allocation.
- A real-time processing overview provides immediate monitoring of storage scan activity and a detailed On-Demand Scan Report.
- Users can now cancel the scanning of individual files, optimizing resource management and preventing unnecessary processing.

- Introduced dedicated permissions for Tenant Admins in MetaDefender Storage Security Cloud, enabling granular tenant management without full admin access.
- Users can now specify a OneDrive group, user, and folder location for scanning. This allows for granular security policies and targeted scanning within OneDrive groups. Remediation actions are updated to accommodate group and user specifications.
- The configuration options that are irrelevant (My OPSWAT Central Management integration) are hidden in MetaDefender Storage Security Cloud deployments, simplifying the UI.
- A "Destination Storage for Remediations" section is added to the dashboard, centralizing remediation action visibility.
- Implemented a configurable debouncing mechanism for RTP scans of productivity files (.docx, .xlsx, .pptx) to prevent exceeding MetaDefender Cloud API limits during high-volume live document editing. This applies to the SharePoint Online Integration and provides configurable debounce settings (interval) and information on MDCloud API request limits.
- Storage Units are now editable in My OPSWAT Central Management. My OPSWAT Central Management configuration is simplified with a dedicated modal and active/inactive/loading states, and user management now features sorting and ordering capabilities.
- Remediation data is included in scan details, providing a comprehensive remediation overview.
- The /file API endpoint is updated to retrieve file lists with filtering options. File remediation history is improved by including remediation information in API responses.
- An optional "Delete empty folders after remediation" setting is added for SMB/NFS/SFTP shares, with audit logging of deleted folders.
- Password security is enhanced to Level 1 compliance, the old password requirement is enforced, existing users migrate on change, and strong authentication is maintained.
- Expanded syslog messages now include Data ID, threat details, and comprehensive scan results for improved SIEM integration.

Improvements

- The shutdown process for all services is improved for a clean and controlled shutdown.
- Authorization issues with Box Webhooks are resolved with a dedicated endpoint.
- A non-dismissible warning/error message is displayed if the database version is less than MongoDB 6.
- The `privateprocessing` header is added to MetaDefender Cloud scan requests by default, ensuring immediate file deletion from MetaDefender Cloud servers after scanning.

MetaDefender Storage Security v3.5.3

Release Date: 23 January 2025

Version supported until 23 July 2026

This release of MetaDefender Storage Security focuses on enhanced functionality, improved performance, and bug fixes to provide a more robust and efficient security solution for your storage environments.

Highlights

- Manage storage units (read-only) remotely via OPSWAT Cloud Management (OCM) with vPack integration.
- Preserve AWS checksum metadata during file transfers between storage locations, including S3-compatible integrations.
- Added support for Hitachi S3, including object deletion without version ID.

Improvements

- Significantly reduced scan times for small files on S3.
- Resolved issues impacting S3 scanning, audit log accuracy, and OCM integration.
- Refined the storage unit management interface in OCM for better usability.

MetaDefender Storage Security v3.5.2

Release Date: 18 December 2024

Version supported until 18 June 2026

Highlights

- MDSS can now connect with ADFS servers that utilize larger OpenID tokens (over 4KB).
- Windows deployments can now leverage SharePoint OnPrem for storage and remediation actions.
- Move existing storage units between groups with the updated Storage Units API.
- Integrate MDSS with Kafka to streamline external logging, including audit events.

Improvements

- The offline package now includes Docker binaries and a dedicated package for seamless offline MongoDB upgrades.
- JSON formatting for console logs allows easier integration with popular log management tools like Corallogix.

- MDSS Cloud now efficiently retrieves sanitized files from MetaDefender Cloud scan pools.
- Database Retention settings documentation has been updated to provide comprehensive information on data segregation, isolation, retention policies, and file handling in S3 and EC2 environments.
- Windows Upgrade Enhancements:
  - MDSS automatically clears RabbitMQ queues upon restart after upgrading from version 3.4.2.
  - The upgrade process now seamlessly handles MongoDB database upgrades from version 6 to 7.

MetaDefender Storage Security v3.5.1

Release Date: 19 November 2024

Version supported until 19 May 2026

Highlights

- We've boosted security for cloud deployments with support for AWS PrivateLink, allowing users to connect to MetaDefender Storage Security securely within their Amazon Virtual Private Cloud (VPC)
- Significantly improved performance for remediation tasks, enabling quicker responses to security threats.
- Single Sign-On (SSO) via SAML 2.0 - Business network administrators can now easily integrate with their existing identity providers using SAML 2.0 protocol. This allows for streamlined user authentication and authorization, enhancing security and simplifying access management.

Improvements

- We've addressed stability issues affecting SMB on Windows environments
- Users can now use custom URLs for S3 integration, enabling secure access to S3 buckets via AWS PrivateLink.
- We've improved the OPSWAT Cloud Management (OCM) synchronization job to reduce unnecessary configuration downloads and ensure the latest version of the vPack package is always available.
- To improve performance and scalability, we've added data retention settings for real-time processing for large datasets.
- We've added PIN functionality to OPSWAT Cloud Management, ensuring only authorized users can access and modify your configurations.

MetaDefender Storage Security v3.5.0

Release Date: 23 October 2024

Version supported until 23 April 2026

Highlights

New Integration: Native NetApp Storage

- New Integration: Native NetApp Storage using the ONTAP connector.
- New Integration: OPSWAT MetaDefender Managed File Transfer (MFT)
- New Integration: Cubbit Storage
- Support for PingFederate as an SSO (single sign-on) provider via OpenID Connect
- Scan management now includes balanced priority queues for real-time processing and instant scans

Improvements

- Improved API documentation for some API endpoints.
- Updated the Serilog package to version 4.0.1 to enhance integration capabilities and security.
- Documentation is now available describing the usage of MetaDefender Core and MetaDefender Cloud APIs, including required roles and permissions for correct access.
- Upgraded multiple node packages to enhance security and reliability.

MetaDefender Storage Security v3.4.4

Release Date: 12 September 2024

Version supported until 12 March 2026

This release brings significant enhancements and bug fixes to improve the overall user experience and security of the system. We've focused on enhancing SSO integration and resolved several critical issues, including security vulnerabilities and database errors. We're committed to continuously improving our product and addressing user needs.

Highlights

- SSO Integration Enhancements
- Enhanced discovery error handling for improved system stability

Improvements

- Resolved stuck files issue where files wouldn't be marked as Failed.
- Addressed NFS issue with non-ascii folder/filenames causing slow scans.

- Restricted services ports accessibility to localhost only, enhancing security.
- Fixed assigned role issue where role changes weren't reflected correctly.
- Resolved issue preventing adding SMB units across network domains.
- Investigated and addressed "Database Operation Failed" errors appearing in logs.
- Upgraded Webpack to version 5.91.0
- Made updates to our licensing system to further strengthen its security and reliability.

MetaDefender Storage Security v3.4.3

Release Date: 21 August 2024

Version supported until 21 August 2026

This release brings major improvements and fixes, enhancing security, integrations, automation, data management, and user experience. Key updates include strengthened security for encrypted files and user-controlled decryption, enhanced integration process with Box, automated folder scanning and webhook notifications for streamlined workflows, improved data management with import/export enhancements, and a more user-friendly experience with onboarding validation and NFS discovery refinements.

Highlights

- Added backend APIs for password-protected files, enabling secure scanning and access control.
- Users can now directly enter passwords for encrypted files within the MDSS interface.
- Configurable real-time push notifications for new Box files through Event-Based Real-Time Processing.
- Introducing REST APIs for automating folder scanning and storage management (S3, EFS), enabling users to initiate on-demand scans of any desired folder within their storage.
- Webhook notifications for scan completion, eliminating polling.
- Improved inter-service communication efficiency with enhanced caching.
- Data retention settings are now included in the export configuration.
- Extended filter options for scan reports (by start date).
- Workflow rule validation during onboarding for compatibility.
- Hidden files and folders can now be skipped during NFS discovery.

MetaDefender Storage Security v3.4.2

Release Date: 17 July 2024

Version supported until 17 January 2026

This release brings major improvements and fixes, enhancing performance and usability across the system. Key updates include better configuration handling, storage licensing enforcement, and SMB service stability. We've improved installation messaging, disk space management, and security with Grpc.Core migration. User management and event logging are more robust, and new features like event-based SMB/NFS setup and Mongo 6.0 deployment are included.

Highlights

- Database: We deploy Mongo 6.0 database on new installations.
- SMB Service: We fixed out-of-range file descriptors, and addressed files remaining in "Pending" status when moving sanitized files while also ensuring file logging works as expected.
- Windows Native: Fixed the inability to import configuration during onboarding and parametrized the API Gateway port for better support.
- Licensing: Users can no longer add storage if the license is expired or missing.
- Installation and DevOps: Improved clarity of installation failure messages, prevented rapid disk space usage by ensuring that resources are not being consumed while the service is idle.
- Security and User Management: Migrated from the Grpc.Core library and ensured container configuration in production compose files.
- RTP and Scanning: Fixed errors post-upgrade during file processing for RTP (Event-based) and Corrected error messages returned from the scanning API.
- Audit: Corrected double scan delete event records and properly displayed applied post-action information.
- Logging and Notifications: Added logging for error responses in the Storage Service platform and updated email notifications.
- SSO admins can now successfully enable the SMTP server
- Event Based RTP: Introduced event-based SMB/NFS and implemented the Download Connector post-storage setup

MetaDefender Storage Security v3.4.1

Release Date: 14 June 2024

Version supported until 14 December 2025

Highlights

- API Key Functionality Expanded Across All REST APIs: We have extended the API Key functionality, initially exclusive to event-based RTP, to cover our entire application. This enhancement allows users to generate and utilize an API Key for all available REST API

endpoints, facilitating long-term integrations. We recommend periodically rotating the API Key to maintain security.

- As part of our ongoing rebranding to MetaDefender Storage Security, we have updated the default rule to MetaDefender Storage Security inside MetaDefender Core in all new installations. This change ensures that new users start with the latest configuration tailored to MetaDefender Storage Security.
- We have introduced a new field in the report to clearly mark discovery errors. This field will capture and display all errors when discovery fails due to a general issue, improving transparency and troubleshooting capabilities.
- We have boosted our integration with myOPSWAT by introducing an advanced health status report for our product MetaDefender Storage Security. This new feature enables myOPSWAT to effectively diagnose and report problems within our product, enhancing overall functionality and user experience.
- SSO administrators now have the ability to accept or decline new user invitations, aligning their permissions with those of local administrators. This update ensures greater control and parity in user management across our platform.

Performance, Security, and Usability Enhancements

- Discovery Service: We've implemented a fix for the multithreaded access issue in our Redis cache, ensuring enhanced stability and performance for the discovery service.
- We have upgraded RabbitMQ to version 3.13, enhancing performance and stability.
- Box Integration: Improved validation when the specified location does not exist on the remote storage.
- Windows Native: We have made quality of life improvements and enhanced error messaging for Windows Native, aiming to streamline user experience and provide clearer feedback during install operations. Also, we now include the Visual C++ Redistributable (`vc_redist`) with our product, enabling full installation on offline Windows systems without the need for additional downloads. This enhancement simplifies setup and improves accessibility.
- Database Migrations: We've improved the logging mechanisms in `mongo-migrations` to ensure more detailed and effective troubleshooting.
- Added robust error handling for pre and post-process events in remediations, ensuring smoother operation and improved reliability during critical workflows.

MetaDefender Storage Security v3.4.0

Release date: 13 May 2024

Version supported until 13 November 2025

Introducing Windows Native Compatibility for Our Application

Highlights

- Windows Native Support
- We are announcing a new integration capability with Oracle Cloud Object Storage (OCI) via AWS SDK: This integration employs path-based access to connect to OCI, accommodating the platform's limitation on not supporting virtual hosted access.
- We've introduced Single Sign-On support for MDSS using Active Directory Federation Services and OpenID Connect, streamlining login processes and enhancing security and user experience for seamless authentication and easier access management.
- Strengthened API Security Enhancements against various security vulnerabilities, ensuring a more secure and reliable environment for our users: Enhanced HTTPS Enforcement, Strict-Transport-Security (HSTS) Implementation, X-Content-Type-Options Header Upgrade, Mandatory Operation Security Field

Bug fixes/Enhancements

- Stress Testing Enhancements: Conducted stress tests under heavy load on a machine with 8 cores and 16GB of RAM, where RabbitMQ and MongoDB utilized 25% of RAM, in both AWS and SMB environments.
- Improved Real-Time Processing for NFS: Enhanced Real-Time Protection with Deep Content Disarm and Reconstruction for NFS on Windows shares, improving security performance.
- Streamlined Command-Line Upgrading for MDSS: Updated the command-line upgrade process to consistently display the EULA page, particularly when using clean commands or exporting support packages, enhancing user compliance and experience during upgrades.
- Event Limitation and Scaling Guidance: Implemented an event limitation in the discovery process; the system will pause when it reaches 5,000 events. Users are encouraged to scale up their systems to maintain continuous operation.
- DocumentDB Integration: Successfully integrated our system with DocumentDB, enhancing our database management capabilities.
- Storage Limitation and UI Enhancements for Simpler Deployments: Introduced a storage limitation per instance to prevent overload and added UI warnings for excessive CPU usage, along with a sizing guide to help customers effectively scale their systems.

MetaDefender Storage Security v3.3.4

Release date: 28 March 2024

Version supported until 28 September 2025

Introducing the Wasabi storage integration, Copy Functionality for duplicating files in place, seamless preservation of tags during storage transfers, and enhanced High Availability and Disaster Recovery options for uninterrupted data access across regions.

Highlights

- We're pleased to announce that Wasabi is now a supported storage type! Whether you're in search of cost-effective cloud storage solutions or high-performance storage options, integrating Wasabi provides you with a robust and dependable choice for storing your data.
- Introducing Copy Functionality: Now, you can duplicate files while keeping them in their original location, providing enhanced flexibility and control over your data management compared to the previous method of removing files from the source.
- With our latest update, tags remain intact when files are moved between storage locations, safeguarding valuable metadata and ensuring a seamless experience across storage movements.
- We improved the support for High Availability and Disaster Recovery (HA/DR) that enables the selection of a failover scan pool. In the event of downtime in one region's assigned pool, a backup pool from another region seamlessly assumes control, guaranteeing uninterrupted access to your data.

Bug fixes/Enhancements

- The Scan Report now includes comprehensive details regarding Document Library and Folder Location within SharePoint, ensuring complete information coverage.
- You can now effortlessly delete duplicated scan configurations after importing them.
- Now, it's no longer possible to remove a scan configuration that is in use, as this issue has been resolved.
- Efficient handling of key name collisions during storage discovery ensures the continuity of the ongoing scan, facilitating completion without hindrance.
- The scan would be efficiently completed within an appropriate timeframe.
- The display of stop time for RTP reports is accurate when the RTP scan has been initiated, ensuring precision in data presentation.

For further details on the steps involved in integrating Wasabi you can access this link Add A Wasabi Storage.

MetaDefender Storage Security v3.3.3

Release date: 14 February 2024

Version supported until 14 August 2025

With this release, we're introducing NFS storage integration, offering functionality similar to SMB storage.

Highlights

- Add, edit, and delete NFS from the Storage unit, with the addition only possible from the onboarding page.
- Validate and add unique units, preventing duplicates, and properly import and export NFS units.
- Start, stop, and restart RTP and retrieve files once while creating/moving/modifying files after starting RTP.
- Initiate, cancel, or modify multiple instant scans, with updated reports for empty files, small files (1K - 1MB), medium files (100MB), and large files (1GB).
- Ensure file scan results display correctly, reflecting MDCore's response and post-actions applied.
- Perform post-actions such as DeepCDR (Keep/Encrypt/Delete original files), moving sanitized/allowed/blocked files to another storage (S3/Box/Azure Blobs), receiving files from another storage (sanitized files from Box/Azure Blobs), and deleting blocked files.
- Implement logging mechanisms to audit NFS-related actions and include NFS services in the logs.
- Improved logging support by allowing extensive configuration and rotation.
- Polling time intervals support configuration.

Bug fixes/Enhancements

- Preventing duplicated folder structure for Box.
- Improving the orchestration of the scanning process to address instances of scans becoming stuck.
- Additional checks on the Windows docker service before starting MDSS

You can find more information on the Add an NFS Storage steps by accessing the hyperlink.

MetaDefender Storage Security v3.3.2

Release date: 21 December 2023

Version supported until 21 June 2025

Highlights

- AWS GovCloud (US)
- Client-Side Encryption for S3 buckets
- Performance improvements

- Native Podman support for RHEL 8
- Removed import functionality post-onboarding
  - This change addresses conflicts that occurred when an import was applied to partially configured instances, leading to unexpected behavior and bugs. Import functionality is now restricted to after onboarding, which remains available for use.

Bug fixes/Enhancements

- File location on retry
- SMB Connection Caching
- Outdated UI Reports

MetaDefender Storage Security v3.3.1

Release date: 9 October 2023

Version supported until: 9 April 2025

Highlights

- Integration with My OPSWAT portal
- Microsoft SharePoint Integration
- Scan Configuration History
- Azure Gov Storage Integration
- MongoDB v6 Migration Guide
- Amazon S3 URL Validity Control
- UI Session Expiration Customization

Bug fixes

- Onboarding: Users can now successfully add an MD Cloud instance
- SMB Storage Integration: Resolved an issue by adding an alternative method to check for file uploads in the SMB storage integration
- Addressed an issue related to queries when utilizing Cosmos DB
- Resolved an issue where scans appeared as stuck when processing spanned multiple days

MetaDefender Storage Security v3.3.0

Release date: 13 July 2023

Version supported until: 13 January 2025

Highlights

- SFTP Storage integration now available under Network Attached Storage section
- Transitioned Core Pool settings from the storage level to the scan level to enhance flexibility
- Simplified the licensing. With a valid license, access to all storage integrations is now granted.
- Mark unavailable storage units, based on ENABLED_MODULES from environments variable file

Bug fixes

- Better Failure Handling**:** We've made improvements to how the system manages failures.
- Introducing an option to set the interval for flagging a file as failed if it gets stuck during processing. Adjust this with the `MARK_STUCK_FILE_AS_FAILED_HOURS` environment variable in the configuration file.
- Significant performance improvements in file discovery.

MetaDefender Storage Security v3.2.0

Release date: 18 May 2023

Version supported until: 18 November 2024

Highlights

- Flexible deployments - User has now the ability to deploy only storage services that will be used. This can be done through an environment variable.
- Generic API for storage units - Exposed a generic API (api/storage/) to handle the Add/Edit/Delete operations on storage units.
- Processing indicator improvements - Showing a single progress bar which indicates the overall processing (discovery, scanning and remediations) progress
- Angular 15 update - Migrated the UI to Angular 15. We suggest to clear the browser cache before upgrading
- API for Offline Activation - Removed content encoding when calling /api/settings/admin/license/activate/offline
- System Checks - Added RabbitMQ and Redis details

Bug fixes

- Reports Performance improvements - Improved the scan report performance. Added the option to filter by date, improved the search and pagination. Added Refresh button to the Real-Time Processing report.
- Fixed the issue with Keep folder Structure for SMB remediations
- Import settings Fix for empty destination on Remediations

- Remediation actions Remediation Actions resilience improvement
- Fixed Document DB integration
- S3 compatible file download Fixed the download error for some S3 Compatible providers

MetaDefender Storage Security v3.1.4

Release date: 21 February 2023

Version supported until: 21 August 2024

Highlights

- SMB integration SMB integration refactoring for high availability and scalability. Removed discovery debounce time
- OneDrive integration refactoring for high availability and scalability
- Real-time data display on the Dashboard
- Event-based Real-Time processing Moved from Blob-trigger to eventgrid and documented the setup
- RAM authentication option for Alibaba Cloud storage unit
- Terraform example for configuring MDSS

Bug fixes

- Fixed the issue with Box storage unit set as a remediation destination
- Improved UI for showing blocked files
- More reliable mechanism to download files from the storage

MetaDefender Storage Security v3.1.3

Release date: 22 December 2022

Version supported until: 22 June 2024

Highlights

- SSO integration - Added SSO capability using OIDC (Open ID Connect) for Azure AD identity provider
- Azure Files refactoring - Refactored Azure Files storage unit integration to use Azure Files SDK
- Windows Server 2022 - Added Windows Server 2022 to the list of supported operating systems
- Google Cloud Provider Authentication - IAM role authentication option for a GCP storage unit

- Alibaba Cloud Authentication - RAM authentication option for Alibaba Cloud storage unit
- Terraform resources configuration - Terraform example for configuring MDSS

Bug fixes

- Amazon S3/Alibaba Cloud/Google Cloud Provider event based real-time - Improved event-based real-time validation and events tracking mechanism
- Decrypt logging - Added logs when a file is decrypted
- Box - Revert encryption mechanism bug fixes
- Report bug fixes - Date filter and user name bug fixes

Known limitations

- Windows 11 installation with Docker 4.15.0 - As a workaround, please downgrade Docker

MetaDefender Storage Security v3.1.2

Release date: 27 October 2022

Version supported until: 27 April 2024

Highlights

- Event-Based Real-time processing - Enhanced the MetaDefender Storage Security Real-Time processing by adding the option to process notifications when a new object is added to an Amazon S3, Azure Blob, Alibaba Cloud and Google Cloud Provider storage.
- UI improvements - Consistency changes for input controls
- Amazon S3/ S3 Compatible Added the option to keep the folder structure when moving files to an Amazon S3/ S3 Compatible storage unit
- Vulnerabilities display - Enhanced the vulnerabilities details table with a new CVSS 3 section

Bug Fixes

- Remediations action rollback Improved rollback mechanism when applying remediations
- Decrypt logging Added logs when a file is decrypted

MetaDefender Storage Security v3.1.1

Release date: 06 October 2022

Version supported until: 06 April 2024

Highlights

- Box storage migration - Discover, scan and apply remediation actions on objects from Box.
- Logs improvements - Added the same logging system to all micro-services
- Documented environment variables - Provided information about the usage of each environment variable

Bug Fixes

- Reduced number of requests for license validation
- Reset Password page UI fixes

MetaDefender Storage Security v3.1.0

Release date: 31 August 2022

Version supported until: March 2, 2024

Highlights

- Alibaba Cloud storage integration - Discover, scan and apply remediation actions on objects from Alibaba Cloud
- Google Cloud storage integration - Discover, scan and apply remediation actions on objects from Google Cloud
- Job dispatcher service improvements - High-availability improvements for the job dispatcher service
- Log aggregation and persistence - Logs created inside the containers will now persist when restarting MetaDefender Storage Security

Bug fixes

- Real-Time Processing handling type display- The handling type can now be seen on the dashboard as well
- Improve validation of move remediation actions - Fixed validation for same type of move remediation action, when having a possible circular dependency between storages
- Audit filter - The filter is now resetting when moving to another page
- Date picker validation improvement - Improved filtering reports based on date

MetaDefender Storage Security API

MetaDefender Storage Security API v1

> Scroll down for example requests and responses.

This section of the user guide describes how you can programmatically interact with the MetaDefender Storage Security REST API. Below are some common tasks that can be done using the available REST APIs:

- Authenticate to obtain a JSON Web Token(JWT)
- Start or stop a process(scan)
- Add / remove storage units

About this REST API

The exposed endpoint is located by default at `http(s)://md-storage-server/api/` (for example, the authentication endpoint is available at `http(s)://md-storage-server/api/user/authenticate`). All requests are handled by the NGINX web server before being proxied to the backend API Gateway service.

All endpoints perform authentication and authorization checks. For these checks to succeed, a valid token should be presented in the Authorization header in the form of Bearer.

Please note that all issued tokens have a timestamp and signature associated in order to prevent long-term usage without re - authentication. The lifespan of the token is currently set to 60 minutes, meaning you will have to request a new token before it expires in order to avoid error responses.

Useful links

- https://swagger.io/tools/swagger-ui/

Base URLs:

- <MDSS_HOST>

Authentication

- HTTP Authentication, scheme: bearer As mentioned earlier, all endpoints perform authentication and authorization checks. In order for these checks to succeed, a valid token should be presented in the Authorization header in the form of `Bearer <JWT>`.

Suggested application logic

If you plan to integrate **MetaDefender Storage Security** in your custom application or workflow, please consider the following scenarios for successfully making REST API requests:

Scenario	Possible use cases
Short-lived integration	You are building or enhancing an application that requires sporadic or on-demand access to **MetaDefender Storage Security** REST APIs.
	The application is not expected to make more than a few REST API calls per hour.
	The application does not need to preserve a session.
Long-lived integration	You are building or enhancing an application that requires continuous, uninterrupted, or hard to predict access to **MetaDefender Storage Security** REST APIs.
	Requests are being triggered based on external factors and your application should maintain connectivity with **MetaDefender Storage Security** REST API.
	Session preserving is necessary and authentication should happen without user-interaction.
	Your application will make a significant number of REST API requests and you need increased performance
API Key integration	You are building or enhancing an application that requires continuous, uninterrupted, or hard to predict access to **MetaDefender Storage Security** REST APIs.
	Requests are being triggered based on external factors and your application should maintain connectivity with **MetaDefender Storage Security** REST API.
	Authentication should happen without user-interaction.
	Your application will make a significant number of REST API requests and you need increased performance.

Short-lived integration

- Obtain a signed accessToken by calling `/api/user/authenticate` API
- Use this token to call your desired REST API by providing it in the Authorization header
- Expire the token by calling `/api/user/logout`
- Repeat steps 1-3 the next time your application needs to call a REST API

Long-lived integration

- Obtain a signed token by calling `/api/user/authenticate` API
- Securely save the received accessToken and the refreshToken
- Use the accessToken to call your desired REST API by providing it in the Authorization header
- Add an exception handler in case you receive a 401 Unauthorized response because the JWT has expired call `/api/user/refreshToken` to obtain a new accessToken by providing the saved refreshToken.

  > a) the accessToken expires after an hour of creation; the expiry time is represented in UTC format by the accessTokenExpiryTime value.

> b) the refreshToken expires after an hour of creation; the expiry time is represented in UTC format by the refreshTokenExpiryTime value. c) if the refreshToken has expired as well, obtain a signed token by calling `/api/user/authenticate` API

- Use the newly issued accessToken to call your desired REST API by providing it in the Authorization header

API Key integration

- In the **MetaDefender Storage Security** interface, navigate to Settings → Profile → Configure API Key
- Generate the key, copy it, and store it somewhere safe
- Use the API Key to call your desired REST API by providing it as a header with the Key: `ApiKey` and Value: `<the value of your API Key>`

General considerations

- The access token expiration date cannot be extended. By default, the access token is valid for an hour after calling `/api/user/authenticate` API to obtain it. The refresh token is also valid for an hour but can be extended by calling `/api/user/refreshToken` and it is also automatically extended with an hour with each non-GET request.
- A refresh token is used to request a new access token when the current one expires without requiring re-authentication using a username and password.
- The refresh token is used to forcibly expire any previously issued JWT when the refresh token expires or is removed by calling `/api/user/logout`.
- A 3rd party application that needs persistent connectivity with **MetaDefender Storage Security** should implement a timeout mechanism to ensure that the refresh token is renewed before it expires by calling `/api/user/refreshToken` whenever the JWT (access token) is expired but before the refresh token expires as well.
- API Keys cannot be used to authenticate requests to the `/api/user` and `/api/apikey` endpoints.

Abac

Attribute-Based Access Control management endpoints

Get Roles

`GET /api/abac/roles`

Retrieve all ABAC roles. Set includePermissions to true to include the full permission list for each role.

Parameters

Name	In	Type	Required	Description
includePermissions	query	boolean	false	none

> Example responses

> 200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "roles": [
    {
      "id": "string",
      "name": "string",
      "permissions": [
        {
          "id": "string",
          "action": "string",
          "resource": "string"
        }
      ]
    }
  ]
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	GetRolesQueryResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Create Role

`POST /api/abac/roles`

Create a new ABAC role. Provide an optional templateRoleId to inherit all permissions from an existing role; any IDs in permissionIds are merged on top of the template.

> Body parameter

```
{
  "name": "string",
  "permissionIds": [
    "string"
  ],
  "templateRoleId": "string"
}
```


Parameters

Name	In	Type	Required	Description
body	body	CreateRoleParameters	true	none

Example responses

200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "role": {
    "id": "string",
    "name": "string",
    "permissions": [
      {
        "id": "string",
        "action": "string",
        "resource": "string"
      }
    ]
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	CreateRoleCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Get Role by ID

`GET /api/abac/roles/{roleId}`

Retrieve a single role and its associated permissions by role ID.

Parameters

Name	In	Type	Required	Description
roleId	path	string(guid)	true	none

Example responses

200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "role": {
    "id": "string",
    "name": "string",
    "permissions": [
      {
        "id": "string",
        "action": "string",
        "resource": "string"
      }
    ]
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	GetRoleByIdQueryResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Update Role

`PUT /api/abac/roles/{roleId}`

Replace an existing role's name and full permission set in a single operation. The supplied permissionIds become the role's complete permission list (previously assigned permissions not in the list are removed). Predefined system roles cannot be updated.

> Body parameter

```
{
  "name": "string",
  "permissionIds": [
    "string"
  ]
}
```

Parameters

Name	In	Type	Required	Description
roleId	path	string(guid)	true	none
body	body	UpdateRoleParameters	true	none

> Example responses

> 200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```

Responses

Status	Meaning	Description	Schema
200	OK	none	UpdateRoleCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Delete Role

`DELETE /api/abac/roles/{roleId}`

Permanently delete a role. Predefined system roles cannot be deleted.

Parameters

Name	In	Type	Required	Description
roleId	path	string(guid)	true	none

> Example responses

> 200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	DeleteRoleCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Get Permissions

`GET /api/abac/permissions`

Retrieve all available ABAC permissions (action + resource pairs).

> Example responses

> 200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "permissions": [
    {
      "id": "string",
      "action": "string",
      "resource": "string"
    }
  ]
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	GetPermissionsQueryResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Create Permission

`POST /api/abac/permissions`

Create a new ABAC permission defined by an action and a resource.

> Body parameter

```
{
  "action": "string",
  "resource": "string"
}
```


Parameters

Name	In	Type	Required	Description
body	body	CreatePermissionParameters	true	none

Example responses

200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "permission": {
    "id": "string",
    "action": "string",
    "resource": "string"
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	CreatePermissionCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Delete Permission

`DELETE /api/abac/permissions/{permissionId}`

Permanently delete a permission by ID. Predefined base permissions cannot be deleted.

Parameters

Name	In	Type	Required	Description
permissionId	path	string(guid)	true	none

> Example responses

> 200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	DeletePermissionCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Assign Permission to Role

`POST /api/abac/roles/{roleId}/permissions`

Assign a permission to the specified role.

> Body parameter


```
{
  "permissionId": "string"
}
```

Parameters

Name	In	Type	Required	Description
roleId	path	string(guid)	true	none
body	body	RolePermissionParameters	true	none

> Example responses

> 200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	AssignPermissionToRoleCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Remove Permission from Role

`DELETE /api/abac/roles/{roleId}/permissions/{permissionId}`

Remove a permission from the specified role. Permissions that were assigned to a predefined role during initialization cannot be removed.

Parameters

Name	In	Type	Required	Description
roleId	path	string(guid)	true	none
permissionId	path	string(guid)	true	none

> Example responses

> 200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	RemovePermissionFromRoleCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Assign Role to User

`POST /api/abac/users/{userId}/roles`

Assign a role to a user, optionally with an expiry date after which the assignment is no longer valid.

> Body parameter

```
{
  "roleId": "string",
  "expiresAt": "2019-08-24T14:15:22Z"
}
```


Parameters

Name	In	Type	Required	Description
userId	path	string	true	none
body	body	AssignRoleToUserParameters	true	none

Example responses

200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "roleBindingId": "string"
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	AssignRoleToUserCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Replace User Roles

`PUT /api/abac/users/{userId}/roles`

Atomically replace all role assignments for a user with the provided set of role IDs. All existing role bindings are removed and new ones are created in a single transaction.

Body parameter

```
{
  "roleIds": [
    "string"
  ]
}
```

Parameters

Name	In	Type	Required	Description
userId	path	string	true	none
body	body	ReplaceUserRolesParameters	true	none

Example responses

200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```

Responses

Status	Meaning	Description	Schema
200	OK	none	ReplaceUserRolesCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Remove Role from User

```
DELETE /api/abac/users/{userId}/roles/{roleBindingId}
```

Remove a role binding from a user using the role binding ID.

Parameters

Name	In	Type	Required	Description
userId	path	string	true	none
roleBindingId	path	string(guid)	true	none

> Example responses

> 200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	RemoveRoleFromUserCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Assign Permission to User

`POST /api/abac/users/{userId}/permissions`

Assign a permission directly to a user, optionally with an expiry date.

> Body parameter

```
{
  "permissionId": "string",
  "expiresAt": "2019-08-24T14:15:22Z"
}
```

Parameters

Name	In	Type	Required	Description
userId	path	string	true	none
body	body	AssignPermissionToUserParameters	true	none

Example responses

200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "userPermissionId": "string"
}
```

Responses

Status	Meaning	Description	Schema
200	OK	none	AssignPermissionToUserCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Remove Permission from User

`DELETE /api/abac/users/{userId}/permissions/{userPermissionId}`

Remove a directly assigned permission from a user using the user permission ID.

Parameters

Name	In	Type	Required	Description
userId	path	string	true	none
userPermissionId	path	string(guid)	true	none

Example responses

200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	RemovePermissionFromUserCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Account

Manage your accounts

Add an account

`POST /api/account`

Add a new storage account to the system

Body parameter

```
CredentialsFile: string
```

Parameters

Name	In	Type	Required	Description
Name	query	string	false	display name for the account
Description	query	string	false	description of the account purpose or scope
Credentials	query	string	false	access credentials for the storage service
ProtocolType	query	any	false	type of protocol (0 = SMB, 1 = S3, etc.)
VendorType	query	any	false	vendor type of storage (0 = AmazonS3, 1 = OneDrive, etc.)
AutoDiscovery	query	boolean	false	if true, enables automatic storage detection
GroupId	query	string	false	id of the group account storages should be added to by default
StorageIds	query	array[string]	false	id's of specific storage units under this account
body	body	object	false	none
» CredentialsFile	body	string(binary)¦null	false	none

Example responses

200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "account": {
    "id": "string",
    "name": "string",
    "description": "string",
    "credentials": "string",
    "protocolType": 0,
    "vendorType": 0,
    "autoDiscovery": true,
    "autodiscoveryDestinationGroupId": "string",
    "destinationGroup": {
      "id": "string",
      "name": "string"
    }
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	AddAccountCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Bulk delete accounts

`DELETE /api/account`

Deletes up to 100 accounts in a single request. Per-account ABAC (Accounts.Delete) plus per-cascaded-storage ABAC (Storages.Delete) are enforced. When forceDelete=true, child storages are cascade-deleted along with their scans. If any cascaded storage has a running scan, the request is rejected with HTTP 409. When forceDelete=false, accounts with children are returned in the failed list with localized reason; only empty accounts are deleted.

> Body parameter

```
{
  "accountIds": [
    "string"
  ],
  "forceDelete": true
}
```

Parameters

Name	In	Type	Required	Description
body	body	BulkDeleteAccountsParameters	true	none

Example responses

200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "succeeded": [
    "string"
  ],
  "failed": [
    {
      "id": "string",
      "reasonKey": "string",
      "reason": "string",
      "childFailures": [
        {}
      ]
    }
  ],
  "confirmationRequired": true,
  "preview": [
    {
      "accountId": "string",
      "memberStorageIds": [
        "string"
      ]
    }
  ],
  "scansRunning": true,
  "runningScans": [
    {
      "scanId": "string",
      "storageId": "string",
      "accountId": "string",
      "groupId": "string"
    }
  ]
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	BulkDeleteAccountsCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

List accounts (paginated, filtered, sorted)

`GET /api/account`

Returns a paginated, filtered, and sorted list of accounts. Supports multi-value filters: vendorType (StorageVendorType) and protocolType (StorageProtocolType). The autodiscoveryEnabled boolean filter restricts results to accounts with auto-discovery enabled or disabled. The includeStorages flag (default true) controls whether associated storage units are loaded per account; set to false to skip the per-account N+1 storage scan RPC calls. Default Count is 100 (maximum 100). Returns an IPagedResponse containing Items, TotalCount, StartIndex, and Count.

Parameters

Name	In	Type	Required	Description
Name	query	string	false	none
VendorType	query	array[integer]	false	none
ProtocolType	query	array[integer]	false	none
AutodiscoveryEnabled	query	boolean	false	none
IncludeStorages	query	boolean	false	none
StartIndex	query	integer(int32)	false	none
Count	query	integer(int32)	false	none
SortBy	query	array[integer]	false	none
SortOrder	query	array[integer]	false	none

Enumerated Values

Parameter	Value
SortBy	0
SortBy	1
SortOrder	0
SortOrder	1

> Example responses

200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "items": [
    {
      "id": "string",
      "name": "string",
      "description": "string",
      "storages": [
        {
          "id": "string",
          "groupId": "string",
          "accountId": "string",
          "name": "string",
          "storageClientId": "string",
          "storageType": {
            "name": "string",
            "categoryType": 0,
            "protocolType": 0,
            "vendorType": 0
          },
          "storageStatus": {
            "message": "string",
            "statusType": 0
          },
          "scansInProgress": true,
          "isRtpInProgress": true,
          "isScheduledScanInProgress": true,
          "storageFunctionality": "string",
          "isAutodiscovered": true,
          "groupRef": {
            "id": "string",
            "name": "string"
          },
          "$type": "string"
        }
      ],
      "credentials": "string",
      "autoDiscovery": true,
      "groupId": "string",
      "destinationGroup": {
        "id": "string",
        "name": "string"
      },
      "protocolType": 0,
      "vendorType": 0
    }
```

```
"accounts": [
    {
      "id": "string",
      "name": "string",
      "description": "string",
      "storages": [
        {
          "id": "string",
          "groupId": "string",
          "accountId": "string",
          "name": "string",
          "storageClientId": "string",
          "storageType": {
            "name": "string",
            "categoryType": 0,
            "protocolType": 0,
            "vendorType": 0
          },
          "storageStatus": {
            "message": "string",
            "statusType": 0
          },
          "scansInProgress": true,
          "isRtpInProgress": true,
          "isScheduledScanInProgress": true,
          "storageFunctionality": "string",
          "isAutodiscovered": true,
          "groupRef": {
            "id": "string",
            "name": "string"
          },
          "$type": "string"
        }
      ],
      "credentials": "string",
      "autoDiscovery": true,
      "groupId": "string",
      "destinationGroup": {
        "id": "string",
        "name": "string"
      },
      "protocolType": 0,
      "vendorType": 0
    }
  ],
  "totalCount": 0,
  "startIndex": 0,
  "count": 0
}
```

Responses

Status	Meaning	Description	Schema
200	OK	none	ListAccounts

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Update an account

`PATCH /api/account`

Update an existing account's configuration

> Body parameter

```
CredentialsFile: string
```

Parameters

Name	In	Type	Required	Description
AccountId	query	string	false	id of the account to update
Name	query	string	false	display name for the account
Description	query	string	false	description of the account purpose or scope
Credentials	query	string	false	access credentials for the storage service
ProtocolType	query	any	false	type of protocol (0 = SMB, 1 = S3, etc.)
VendorType	query	any	false	vendor type of storage (0 = AmazonS3, 1 = OneDrive, etc.)
AutoDiscovery	query	boolean	false	if true, enables automatic storage detection
GroupId	query	string	false	id of the group account storages should be added to by default
body	body	object	false	none
» CredentialsFile	body	string(binary)¦null	false	none

Example responses

200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "accountId": "string"
}
```

Responses

Status	Meaning	Description	Schema
200	OK	none	UpdateAccountCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Delete an account

`DELETE /api/account/{accountId}`

Permanently delete an account and its storage references

Parameters

Name	In	Type	Required	Description
accountId	path	string	true	id of the account to delete
forceDelete	query	boolean	false	none

> Example responses

> 200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "succeeded": [
    "string"
  ],
  "failed": [
    {
      "id": "string",
      "reasonKey": "string",
      "reason": "string",
      "childFailures": [
        {}
      ]
    }
  ],
  "confirmationRequired": true,
  "preview": [
    {
      "accountId": "string",
      "memberStorageIds": [
        "string"
      ]
    }
  ],
  "scansRunning": true,
  "runningScans": [
    {
      "scanId": "string",
      "storageId": "string",
      "accountId": "string",
      "groupId": "string"
    }
  ]
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	BulkDeleteAccountsCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Fetch account by ID

`GET /api/account/{accountId}`

Retrieve a single account's details by ID

Parameters

Name	In	Type	Required	Description
accountId	path	string	true	id of the account to get

> Example responses

> 200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "account": {
    "id": "string",
    "name": "string",
    "description": "string",
    "storages": [
      {
        "id": "string",
        "groupId": "string",
        "accountId": "string",
        "name": "string",
        "storageClientId": "string",
        "storageType": {
          "name": "string",
          "categoryType": 0,
          "protocolType": 0,
          "vendorType": 0
        },
        "storageStatus": {
          "message": "string",
          "statusType": 0
        },
        "scansInProgress": true,
        "isRtpInProgress": true,
        "isScheduledScanInProgress": true,
        "storageFunctionality": "string",
        "isAutodiscovered": true,
        "groupRef": {
          "id": "string",
          "name": "string"
        },
        "$type": "string"
      }
    ],
    "credentials": "string",
    "autoDiscovery": true,
    "groupId": "string",
    "destinationGroup": {
      "id": "string",
      "name": "string"
    },
    "protocolType": 0,
    "vendorType": 0
  }
}
```

Responses

Status	Meaning	Description	Schema
200	OK	none	GetAccountById

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Fetch available storage units for an account

`GET /api/account/{accountId}/storages`

List all storage units linked to a particular account

Parameters

Name	In	Type	Required	Description
accountId	path	string	true	ID of the account

> Example responses

> 200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "entries": [
    {
      "autodiscoverySource": "string",
      "autodiscoverySourceUrl": "string"
    }
  ],
  "protocolType": 0,
  "vendorType": 0
}
```

Responses

Status	Meaning	Description	Schema
200	OK	none	EnumerateAccountStoragesQueryResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Fetch account sources

`GET /api/account/{accountId}/sources`

Fetch account sources

Parameters

Name	In	Type	Required	Description
filter	query	string	false	none
accountId	path	string	true	none

> Example responses

> 200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "entries": [
    "string"
  ]
}
```

Responses

Status	Meaning	Description	Schema
200	OK	none	EnumerateAccountSourcesQueryResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Audit

List audit information

Fetch audit logs

`GET /api/audit/{startIndex}/{count}`

Parameters

Name	In	Type	Required	Description
startIndex	path	string	true	none
count	path	string	true	none
logType	query	string	false	none
categoryType	query	string	false	none
logLevel	query	string	false	none
searchText	query	string	false	none

> Example responses

> 200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "entries": [
    {
      "id": "string",
      "logLevel": 0,
      "details": "string",
      "logType": 0,
      "userId": "string",
      "category": 0,
      "timeStamp": "2019-08-24T14:15:22Z",
      "userName": "string"
    }
  ],
  "filterCount": 0,
  "totalCount": 0
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	EnumerateLogsQueryResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Configuration

Import or export configuration file

Export configuration file

`GET /api/configuration/export`

Export the current configuration settings to an archive. The file will be encrypted using the provided password.

Parameters

Name	In	Type	Required	Description
exportLicense	query	boolean	false	none
exportSmtp	query	boolean	false	none
exportNotifications	query	boolean	false	none
exportRetention	query	boolean	false	none
exportUsers	query	boolean	false	none
password	query	string	false	none

> Example responses

> 200 Response

Responses

Status	Meaning	Description	Schema
200	OK	none	string

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Import configuration file

`POST /api/configuration/import`

> Body parameter

```
ConfigurationFile: string
password: string
```

Parameters

Name	In	Type	Required	Description
body	body	object	false	none
» ConfigurationFile	body	string(binary)¦null	false	none
» password	body	string¦null	false	none

Example responses

200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "areSmtpSettingsImported": true,
  "isLicenseImported": true,
  "isRetentionImported": true,
  "areNotificationsImported": true,
  "hasNotificationsPartialFailure": true,
  "activationDto": {
    "result": 0,
    "responseKey": "string",
    "responseMessage": "string",
    "responseMessageParams": {
      "property1": "string",
      "property2": "string"
    }
  },
  "newLocalUserId": "string",
  "areUsersImported": true
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	ImportSettingsCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Get enabled modules

`GET /api/configuration/enabledModules`

> Example responses

> 200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "enabledModules": [
    0
  ]
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	GetEnabledModules

This operation does not require authentication

ExternalLogger

Manage external loggers

Retrieve external loggers

`GET /api/externallogger`

> Example responses

200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "entries": [
    {
      "id": "string",
      "isEnabled": true,
      "loggerType": 0,
      "connectionSettings": {
        "$type": "string"
      }
    }
  ]
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	EnumerateExternalLoggersQueryResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Update external logger state

`PUT /api/externallogger/status`

Body parameter


```
{
  "id": "string",
  "isEnabled": true
}
```

Parameters

Name	In	Type	Required	Description
body	body	UpdateExternalLoggerStatusParameters	true	none

> Example responses

> 200 Response

Responses

Status	Meaning	Description	Schema
200	OK	none	string

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Add a new Syslog server configuration

`POST /api/externallogger/udpSyslog`

> Body parameter

```
{
  "isEnabled": true,
  "serverAddress": "string",
  "port": 0,
  "loggerType": 0,
  "facility": 0,
  "format": 0,
  "$type": "string"
}
```

Parameters

Name	In	Type	Required	Description
body	body	AddUdpSyslogExternalLoggerParameters	true	none

> Example responses

> 200 Response

Responses

Status	Meaning	Description	Schema
200	OK	none	string

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Update a Syslog server configuration

`PUT /api/externallogger/udpSyslog`

> Body parameter

```
{
  "isEnabled": true,
  "serverAddress": "string",
  "port": 0,
  "loggerType": 0,
  "facility": 0,
  "format": 0,
  "$type": "string",
  "id": "string"
}
```

Parameters

Name	In	Type	Required	Description
body	body	UpdateUdpSyslogExternalLoggerParameters	true	none

> Example responses

> 200 Response

Responses

Status	Meaning	Description	Schema
200	OK	none	string

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Add a new Kafka server configuration

`POST /api/externallogger/kafka`

> Body parameter

```
{
  "isEnabled": true,
  "serverAddressWithPortList": "string",
  "loggerType": 0,
  "topic": "string",
  "configuration": "string",
  "$type": "string"
}
```

Parameters

Name	In	Type	Required	Description
body	body	AddKafkaExternalLoggerParameters	true	none

> Example responses

> 200 Response

Responses

Status	Meaning	Description	Schema
200	OK	none	string

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Update a Kafka server configuration

`PUT /api/externallogger/kafka`

> Body parameter

```
{
  "isEnabled": true,
  "serverAddressWithPortList": "string",
  "loggerType": 0,
  "topic": "string",
  "configuration": "string",
  "$type": "string",
  "id": "string"
}
```

Parameters

Name	In	Type	Required	Description
body	body	UpdateKafkaExternalLoggerParameters	true	none

> Example responses

> 200 Response

Responses

Status	Meaning	Description	Schema
200	OK	none	string

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Delete external logger

`DELETE /api/externallogger/{id}`

Parameters

Name	In	Type	Required	Description
id	path	string	true	none

> Example responses

> 200 Response

Responses

Status	Meaning	Description	Schema
200	OK	none	string

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

File

Retrieve processed files information

Rescan a file on demand

`PUT /api/file`

This request is used to update a scanned file with passwords, in case it is an encrypted archive andit could not be scanned because the passwords to decrypt it were not provided. It can also be used withoutproviding any passwords to simply rescan a specific file from a finished scan.

> Body parameter

```
{
  "fileId": "string",
  "fileIds": [
    "string"
  ],
  "scanId": "string",
  "storageProtocolType": 0,
  "passwords": [
    "string"
  ],
  "workflowId": "string",
  "mdssBaseUrl": "string"
}
```


Parameters

Name	In	Type	Required	Description
body	body	OnDemandScanParameters	true	none

Example responses

200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	OnDemandScanCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Enumerate processed files

```
GET /api/file
```

Parameters

Name	In	Type	Required	Description
StartIndex	query	integer(int32)	false	starting position for pagination (0-based index)
Count	query	integer(int32)	false	none
StartDate	query	string(date-time)	false	filter files by scan date
EndDate	query	string(date-time)	false	filter files by scan date
Search	query	string	false	text filter
ScanType	query	array[integer]	false	scan type such as (on-demand, scheduled, real time)
StorageId	query	array[string]	false	filter based on a list of possible storage id
ScanId	query	array[string]	false	filter based on a list of possible scan id
ScanWorkflowSnapshotId	query	array[string]	false	filter based on a list of possible scan workflow snapshot id
ProcessingState	query	array[integer]	false	none
Result	query	array[integer]	false	filter by scan result (0 = Clean, 1 = Blocked, 2 = Processing)
ScanAllResultI	query	array[integer]	false	filter by MD Core scan result (0 = NoThreatDetected, 1 = Infected, 2 = Suspicious, etc.)
ScanResultICount	query	array[integer]	false	the number of engine results that are not “No threat detected”
SandboxVerdict	query	array[integer]	false	filter by Sandbox verdict (0 = NoThreat, 1 = Malicious, 2 = Suspicious)
VulnerabilityCount	query	array[integer]	false	the number of vulnerabilities detected
HasVulnerabilities	query	boolean	false	filter by presence of vulnerabilities
DlpDetection	query	boolean	false	DLP detection
HasBlockedFileVersions	query	boolean	false	filter by presence of blocked file versions

Remediations	query	array[integer]	false	filter by remediation performed on the file
SkippedScan	query	boolean	false	filter by whether the scan was skipped
SortBy	query	array[integer]	false	none
SortOrder	query	array[integer]	false	none
Expand	query	array[string]	false	Possible values for expand: workflow_snapshot

Enumerated Values

Parameter	Value
ScanType	0
ScanType	1
ScanType	2
ProcessingState	0
ProcessingState	1
ProcessingState	2
ProcessingState	3
ProcessingState	4
Result	0
Result	1
Result	2
ScanAllResultI	0
ScanAllResultI	1
ScanAllResultI	2
ScanAllResultI	3
ScanAllResultI	7
ScanAllResultI	8
ScanAllResultI	9
ScanAllResultI	10
ScanAllResultI	12
ScanAllResultI	13
ScanAllResultI	14
ScanAllResultI	15
ScanAllResultI	16
ScanAllResultI	17
ScanAllResultI	18
ScanAllResultI	19

ScanAllResultI	20
ScanAllResultI	21
ScanAllResultI	22
ScanAllResultI	23
ScanAllResultI	24
ScanAllResultI	25
ScanAllResultI	26
ScanAllResultI	27
ScanAllResultI	28
ScanAllResultI	29
ScanAllResultI	30
ScanAllResultI	31
ScanAllResultI	32
ScanAllResultI	33
ScanAllResultI	34
ScanAllResultI	36
ScanAllResultI	38
ScanAllResultI	39
ScanAllResultI	40
ScanAllResultI	41
ScanAllResultI	42
ScanAllResultI	43
ScanAllResultI	255
ScanAllResultI	1014
ScanAllResultI	9999
SandboxVerdict	0
SandboxVerdict	1
SandboxVerdict	2
SandboxVerdict	3

SandboxVerdict	4
SandboxVerdict	5
SandboxVerdict	999
Remediations	0
Remediations	5
Remediations	6
Remediations	7
Remediations	8
Remediations	9
Remediations	10
Remediations	11
Remediations	12
Remediations	13
Remediations	14
Remediations	15
Remediations	16
Remediations	17
Remediations	18
Remediations	19
Remediations	20
Remediations	21
Remediations	22
Remediations	23
Remediations	24
Remediations	25
Remediations	26
Remediations	27
Remediations	28
Remediations	29

Remediations	30
Remediations	31
Remediations	32
Remediations	33
Remediations	100
Remediations	101
Remediations	102
SortBy	0
SortBy	1
SortBy	2
SortBy	3
SortBy	4
SortBy	5
SortBy	6
SortBy	7
SortBy	8
SortOrder	0
SortOrder	1

Example responses

200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "entries": [
    {
      "result": 0,
      "responseKey": "string",
      "responseMessage": "string",
      "responseMessageParams": {
        "property1": "string",
        "property2": "string"
      },
      "id": "string",
      "scanId": "string",
      "name": "string",
      "path": "string",
      "hash": "string",
      "fileOwner": {
        "userId": "string",
        "fullName": "string",
        "userName": "string",
        "emailAddress": "string"
      },
      "size": 0,
      "fileTypeCategory": 0,
      "extension": "string",
      "storageType": {
        "name": "string",
        "categoryType": 0,
        "protocolType": 0,
        "vendorType": 0
      },
      "storageName": "string",
      "storageLocation": "string",
      "scanName": "string",
      "progress": {
        "upload": 0,
        "scan": 0,
        "archiveExtraction": 0
      },
      "scanResult": {
        "extractedFiles": {
          "dataId": "string",
          "scanResultI": 0,
          "detectedBy": 0,
          "filesExtractedCount": 0
        },
```

```
"scanDetails": [
            {
              "engineName": "string",
              "threatFound": "string",
              "scanResultI": 0,
              "defTime": "string",
              "scanTime": 0.1,
              "engId": "string",
              "waitTime": 0.1
            }
          ],
          "dataId": "string",
          "scanAllResultI": 0,
          "scanAllResultA": "string",
          "startTime": "string",
          "totalTime": 0.1,
          "totalAvs": 0,
          "totalDetections": 0,
          "progressPercentage": 0
        },
        "fileInfo": {
          "fileSize": 0,
          "uploadTimestamp": "string",
          "md5": "string",
          "sha1": "string",
          "sha256": "string",
          "fileTypeCategory": "string",
          "fileTypeDescription": "string",
          "fileTypeExtension": "string",
          "displayName": "string",
          "fileTypeId": "string"
        },
        "fileScanInfo": {
          "finalVerdict": {
            "blocked": true,
            "verdict": "string",
            "confidence": 0.1,
            "threatLevel": 0.1
          },
          "overviewReport": {
            "analysisState": "string",
            "signalGroups": [
              {
                "description": "string",
                "verdict": "string",
                "signals": [
                  {
                    "originType": "string",
                    "signalReadable": "string",
                    "strength": 0.1
                  }
                ],
                "mitreTechniques": [
```

```
"name": "string",
                    "tacticName": "string"
                  }
                ]
              }
            ],
            "iocs": [
              {
                "data": "string",
                "type": "string",
                "origin": "string",
                "verdict": "string"
              }
            ],
            "yaraMatches": [
              {
                "ruleName": "string",
                "ruleDescription": "string",
                "verdict": "string",
                "matchedStrings": [
                  "string"
                ],
                "author": "string",
                "version": "string",
                "threatLevel": 0.1,
                "confidence": 0.1,
                "strength": 0.1
              }
            ],
            "tags": [
              {
                "name": "string",
                "verdict": "string"
              }
            ],
            "metaData": {
              "entropy": 0.1,
              "forensicAnalysisRecommended": true,
              "fuzzyFsioHash": "string"
            }
          },
          "errorCategory": "string",
          "errorCode": 0,
          "errorDetails": "string"
        },
        "processInfo": {
          "postProcessing": {
            "actionsRan": "string",
            "actionsFailed": "string",
            "convertedTo": "string",
            "copyMoveDestination": "string",
            "convertedDestination": "string",
            "sanitizationDetails": {
```

```
"description": "string",
              "details": "string"
            }
          },
          "progressPercentage": 0,
          "userAgent": "string",
          "profile": "string",
          "result": "string",
          "blockedReason": "string",
          "fileTypeSkippedScan": true,
          "processingTime": 0.1,
          "queueTime": 0.1,
          "resultI": 0
        },
        "dataId": "string",
        "dlpInfo": {
          "hits": null,
          "verdict": 0
        },
        "sbomInfo": {
          "finalVerdict": {
            "blocked": true,
            "licensingPackageCounts": {
              "allowed": 0,
              "blocked": 0,
              "unknown": 0,
              "unsupported": 0
            },
            "severity": 0,
            "totalPackageCount": 0,
            "verdict": "string",
            "vulnerabilityCounts": {
              "critical": 0,
              "high": 0,
              "medium": 0,
              "low": 0,
              "unknown": 0
            }
          },
          "overviewReport": {
            "isPartialReport": true,
            "osInfo": {
              "osName": "string",
              "osVersion": "string"
            },
            "scanMode": "string",
            "steps": [
              {
                "command": "string",
                "packages": [
                  {
                    "authors": "string",
                    "releaseDate": "2019-08-24T14:15:22Z",
```

```
"group": "string",
                    "archive": true,
                    "executable": true,
                    "uid": "string",
                    "licenses": {
                      "allowed": [
                        {
                          "id": "string",
                          "url": "string",
                          "category": "string",
                          "usageRestriction": {
                            "permissions": [
                              null
                            ],
                            "conditions": [
                              null
                            ],
                            "limitations": [
                              null
                            ]
                          }
                        }
                      ],
                      "blocked": [
                        {
                          "id": "string",
                          "url": "string",
                          "category": "string",
                          "usageRestriction": {
                            "permissions": [
                              null
                            ],
                            "conditions": [
                              null
                            ],
                            "limitations": [
                              null
                            ]
                          }
                        }
                      ]
                    },
                    "packageName": "string",
                    "packageVersion": "string",
                    "hashes": [
                      {
                        "sha256": "string",
                        "fileName": "string"
                      }
                    ],
                    "vulnerabilityCounts": {
                      "critical": 0,
                      "high": 0,
```

```
"low": 0,
                    "unknown": 0
                  },
                  "vulnerabilities": [
                    {
                      "id": "string",
                      "severity": 0,
                      "source": "string",
                      "fixedVersions": "string",
                      "cwes": [
                        "string"
                      ]
                    }
                  ],
                  "arch": "string",
                  "osName": "string",
                  "osVersion": "string",
                  "dependencies": [
                    {
                      "ecosystem": "string",
                      "group": "string",
                      "packageName": "string",
                      "packageVersion": "string",
                      "vulnerabilities": [
                        {
                          "id": "string",
                          "severity": 0,
                          "source": "string",
                          "fixedVersions": "string",
                          "cwes": [
                            null
                          ]
                        }
                      ],
                      "vulnerabilityCounts": {
                        "critical": 0,
                        "high": 0,
                        "medium": 0,
                        "low": 0,
                        "unknown": 0
                      }
                    }
                  ]
                }
              ],
              "licenseStatus": "string",
              "licensingPackageCounts": {
                "allowed": 0,
                "blocked": 0,
                "unknown": 0,
                "unsupported": 0
              },
              "step": 0,
```

```
"sha256": "string",
                "severity": 0,
                "vulnerabilityCounts": {
                  "critical": 0,
                  "high": 0,
                  "medium": 0,
                  "low": 0,
                  "unknown": 0
                }
              }
            ],
            "packages": [
              {
                "authors": "string",
                "releaseDate": "2019-08-24T14:15:22Z",
                "ecosystem": "string",
                "group": "string",
                "archive": true,
                "executable": true,
                "uid": "string",
                "licenses": {
                  "allowed": [
                    {
                      "id": "string",
                      "url": "string",
                      "category": "string",
                      "usageRestriction": {
                        "permissions": [
                          "string"
                        ],
                        "conditions": [
                          "string"
                        ],
                        "limitations": [
                          "string"
                        ]
                      }
                    }
                  ],
                  "blocked": [
                    {
                      "id": "string",
                      "url": "string",
                      "category": "string",
                      "usageRestriction": {
                        "permissions": [
                          "string"
                        ],
                        "conditions": [
                          "string"
                        ],
                        "limitations": [
                          "string"
```

```
}
                    }
                  ]
                },
                "packageName": "string",
                "packageVersion": "string",
                "target": "string",
                "hashes": [
                  {
                    "sha256": "string",
                    "fileName": "string"
                  }
                ],
                "vulnerabilities": [
                  {
                    "id": "string",
                    "severity": 0,
                    "source": "string",
                    "fixedVersions": "string",
                    "cwes": [
                      "string"
                    ]
                  }
                ],
                "vulnerabilityCounts": {
                  "critical": 0,
                  "high": 0,
                  "medium": 0,
                  "low": 0,
                  "unknown": 0
                },
                "dependencies": [
                  {
                    "ecosystem": "string",
                    "group": "string",
                    "packageName": "string",
                    "packageVersion": "string",
                    "vulnerabilities": [
                      {
                        "id": "string",
                        "severity": 0,
                        "source": "string",
                        "fixedVersions": "string",
                        "cwes": [
                          "string"
                        ]
                      }
                    ],
                    "vulnerabilityCounts": {
                      "critical": 0,
                      "high": 0,
                      "medium": 0,
                      "low": 0,
```

```
}
                    }
                  ]
                }
              ],
              "dependenciesPackageCount": 0,
              "dependenciesVulnerabilityTotal": 0,
              "dependenciesVulnerabilityCounts": {
                "critical": 0,
                "high": 0,
                "medium": 0,
                "low": 0,
                "unknown": 0
              }
            },
            "resultTemplateHash": "string"
          },
          "vulnerabilityInfo": {
            "vulnerabilityInfoResult": {
              "code": 0,
              "hash": "string",
              "method": 0,
              "timeStamp": "string",
              "timing": 0,
              "detectedProduct": {
                "hasVulnerability": true,
                "isCurrent": true,
                "product": {
                  "id": 0,
                  "name": "string"
                },
                "remediationLink": "string",
                "severity": "string",
                "sigName": "string",
                "signature": 0,
                "vendor": {
                  "id": 0,
                  "name": "string"
                },
                "version": "string",
                "versionData": {
                  "countBehind": 0,
                  "feedId": 0,
                  "version": "string"
                },
                "vulnerabilities": [
                  {
                    "description": "string",
                    "details": {
                      "cpe": "string",
                      "cve": "string",
                      "cvss": {
                        "accessComplexity": "string",
```

```
"authentication": "string",
                      "availabilityImpact": "string",
                      "confidentialityImpact": "string",
                      "generatedOnEpoch": "string",
                      "integrityImpact": "string",
                      "score": "string",
                      "source": "string"
                    },
                    "cvss3": {
                      "attackComplexity": "string",
                      "attackVector": "string",
                      "availabilityImpact": "string",
                      "baseScore": "string",
                      "baseSeverity": "string",
                      "confidentialityImpact": "string",
                      "exploitabilityScore": "string",
                      "impactScore": "string",
                      "integrityImpact": "string",
                      "privilegesRequired": "string",
                      "scope": "string",
                      "userInteraction": "string",
                      "vectorString": "string"
                    },
                    "cwe": "string",
                    "lastModifiedEpoch": "string",
                    "publishedEpoch": "string",
                    "references": [
                      "string"
                    ]
                  },
                  "severity": "string",
                  "severityIndex": 0,
                  "staticId": 0
                }
              ]
            }
          }
        },
        "sessionCookie": "string",
        "fileTypeInfo": {
          "fileInfoExtended": {
            "extensions": "string",
            "groupId": "string",
            "typeId": "string"
          }
        },
        "scanInstanceUrl": "string",
        "scanWorkflowSnapshotId": "string",
        "coreEngines": [
          {
            "engineId": "string",
            "engineName": "string",
            "engineVersion": "string",
```

```
"definitionTime": "string"
          }
        ]
      },
      "processingState": 0,
      "exception": {
        "exceptionDetails": "string",
        "exceptionMessage": "string"
      },
      "created": "2019-08-24T14:15:22Z",
      "lastModified": "2019-08-24T14:15:22Z",
      "discoveryStarted": "2019-08-24T14:15:22Z",
      "fileProcessingDetails": {
        "streamingStartedTime": "2019-08-24T14:15:22Z",
        "streamingCompletedTime": "2019-08-24T14:15:22Z",
        "streamingTimeSpanMs": 0,
        "scanCompletedTime": "2019-08-24T14:15:22Z",
        "processingTimeSpanMs": 0
      },
      "coreEngines": [
        {
          "engineId": "string",
          "engineName": "string",
          "engineVersion": "string",
          "dbVersion": "string",
          "definitionTime": "string"
        }
      ],
      "remediation": {
        "deepCdr": {
          "sanitizationDetails": {
            "failureCategory": "string",
            "description": "string",
            "details": "string"
          },
          "cdrObjectState": 0,
          "fileWasReplaced": true
        },
        "postActionFailedInformation": [
          {
            "objectActionType": 0,
            "exception": {
              "exceptionDetails": "string",
              "exceptionMessage": "string"
            }
          }
        ],
        "objectRemediationActions": [
          {
            "objectActionType": 0,
            "objectActionState": 0,
            "cdrObjectState": 0,
            "exceptions": [
```

```
],
            "id": "string",
            "fileId": "string",
            "fileScanCompletedTime": "2019-08-24T14:15:22Z",
            "remediationId": "string",
            "tenantId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z"
          }
        ]
      },
      "metaDefenderCoreUrl": "string",
      "discoveryStartedDaySec": 0,
      "objectStorageMetadata": "string",
      "scanWorkflowSnapshotId": "string",
      "scanWorkflowSnapshot": {
        "id": "string",
        "scanId": "string",
        "workflow": {
          "id": "string",
          "scanPoolId": "string",
          "scanProcessFlow": 0,
          "isIdentityScanningEnabled": true,
          "scanIntervalDays": 0,
          "rules": [
            "string"
          ],
          "type": 0,
          "workflowSupportedTechnologies": {
            "dlp": {
              "status": 0
            },
            "deepCdr": {
              "status": 0
            },
            "sandBox": {
              "status": 0
            },
            "metascan": {
              "status": 0
            }
          },
          "name": "string",
          "userAgent": "string",
          "scanPool": {
            "id": "string",
            "name": "string",
            "scanPoolType": 0,
            "isDefault": true,
            "scanInstances": [
              {
                "id": "string",
                "scanPoolId": "string",
                "url": "string",
```

```
"timeout": "string",
                "scanInstanceType": 0
              }
            ]
          },
          "failOverScanPoolId": "string",
          "failOverScanPool": {
            "id": "string",
            "name": "string",
            "scanPoolType": 0,
            "isDefault": true,
            "scanInstances": [
              {
                "id": "string",
                "scanPoolId": "string",
                "url": "string",
                "apiKey": "string",
                "timeout": "string",
                "scanInstanceType": 0
              }
            ]
          },
          "filters": {
            "id": "string",
            "minimumSize": 0,
            "maximumSize": 0,
            "minimumDateTime": "2019-08-24T14:15:22Z",
            "maximumDateTime": "2019-08-24T14:15:22Z"
          },
          "fileDefinition": {
            "blockingStrategy": 0,
            "configurableBlockingStrategy": {
              "shouldTreatFilesWithSensitiveDataAsBlocked": true,
              "shouldTreatFilesWithVulnerabilitiesAsBlocked": true
            }
          },
          "remediations": [
            {
              "id": "string",
              "workflowId": "string",
              "isEnabled": true,
              "configuration": "string",
              "type": 0,
              "handlingType": 0
            }
          ],
          "tenantId": "string"
        },
        "startTimestamp": 0,
        "stopTimestamp": 0,
        "scanPool": {
          "id": "string",
          "name": "string",
```

```
"isDefault": true,
          "scanInstances": [
            {
              "id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ]
        },
        "scanInstances": [
          {
            "id": "string",
            "scanPoolId": "string",
            "url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ],
        "failOverScanPool": {
          "id": "string",
          "name": "string",
          "scanPoolType": 0,
          "isDefault": true,
          "scanInstances": [
            {
              "id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ]
        },
        "failOverScanInstances": [
          {
            "id": "string",
            "scanPoolId": "string",
            "url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ],
        "storage": {
          "id": "string",
          "name": "string",
          "groupId": "string",
          "clientId": "string",
```

```
"source": "string",
          "storageFunctionality": "string",
          "storageType": {
            "name": "string",
            "categoryType": 0,
            "protocolType": 0,
            "vendorType": 0
          },
          "storageStatus": {
            "message": "string",
            "statusType": 0
          },
          "workflowId": "string",
          "lastUpdated": "2019-08-24T14:15:22Z",
          "tenantId": "string",
          "groupRef": {
            "id": "string",
            "name": "string"
          },
          "isAutodiscovered": true
        },
        "workflowStatistics": {
          "taggingStatistics": {
            "total": 0
          },
          "keepAllowedStatistics": {
            "total": 0
          },
          "keepBlockedStatistics": {
            "total": 0
          },
          "keepSanitizedStatistics": {
            "total": 0
          },
          "movedAllowedStatistics": {
            "total": 0,
            "destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
              "accountId": "string",
              "source": "string",
              "storageFunctionality": "string",
              "storageType": {
                "name": "string",
                "categoryType": 0,
                "protocolType": 0,
                "vendorType": 0
              },
              "storageStatus": {
                "message": "string",
                "statusType": 0
```

```
"workflowId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z",
              "tenantId": "string",
              "groupRef": {
                "id": "string",
                "name": "string"
              },
              "isAutodiscovered": true
            }
          },
          "movedSanitizedStatistics": {
            "total": 0,
            "destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
              "accountId": "string",
              "source": "string",
              "storageFunctionality": "string",
              "storageType": {
                "name": "string",
                "categoryType": 0,
                "protocolType": 0,
                "vendorType": 0
              },
              "storageStatus": {
                "message": "string",
                "statusType": 0
              },
              "workflowId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z",
              "tenantId": "string",
              "groupRef": {
                "id": "string",
                "name": "string"
              },
              "isAutodiscovered": true
            }
          },
          "movedBlockedStatistics": {
            "total": 0,
            "destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
              "accountId": "string",
              "source": "string",
              "storageFunctionality": "string",
              "storageType": {
                "name": "string",
                "categoryType": 0,
```

```
"vendorType": 0
              },
              "storageStatus": {
                "message": "string",
                "statusType": 0
              },
              "workflowId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z",
              "tenantId": "string",
              "groupRef": {
                "id": "string",
                "name": "string"
              },
              "isAutodiscovered": true
            }
          },
          "copyAllowedStatistics": {
            "total": 0,
            "destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
              "accountId": "string",
              "source": "string",
              "storageFunctionality": "string",
              "storageType": {
                "name": "string",
                "categoryType": 0,
                "protocolType": 0,
                "vendorType": 0
              },
              "storageStatus": {
                "message": "string",
                "statusType": 0
              },
              "workflowId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z",
              "tenantId": "string",
              "groupRef": {
                "id": "string",
                "name": "string"
              },
              "isAutodiscovered": true
            }
          },
          "copyBlockedStatistics": {
            "total": 0,
            "destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
```

```
"source": "string",
              "storageFunctionality": "string",
              "storageType": {
                "name": "string",
                "categoryType": 0,
                "protocolType": 0,
                "vendorType": 0
              },
              "storageStatus": {
                "message": "string",
                "statusType": 0
              },
              "workflowId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z",
              "tenantId": "string",
              "groupRef": {
                "id": "string",
                "name": "string"
              },
              "isAutodiscovered": true
            }
          },
          "deleteAllowedStatistics": {
            "total": 0
          },
          "deleteBlockedStatistics": {
            "total": 0
          },
          "lastCalculatedStatisticsTime": "2019-08-24T14:15:22Z"
        },
        "account": {
          "id": "string",
          "name": "string",
          "description": "string",
          "credentials": "string",
          "protocolType": 0,
          "vendorType": 0,
          "autoDiscovery": true,
          "autodiscoveryDestinationGroupId": "string",
          "destinationGroup": {
            "id": "string",
            "name": "string"
          }
        },
        "realTimeStartDate": "2019-08-24T14:15:22Z"
      },
      "versions": [
        {
          "result": 0,
          "responseKey": "string",
          "responseMessage": "string",
          "responseMessageParams": {
            "property1": "string",
```

```
},
          "id": "string",
          "scanId": "string",
          "name": "string",
          "path": "string",
          "hash": "string",
          "fileOwner": {
            "userId": "string",
            "fullName": "string",
            "userName": "string",
            "emailAddress": "string"
          },
          "size": 0,
          "fileTypeCategory": 0,
          "extension": "string",
          "storageType": {
            "name": "string",
            "categoryType": 0,
            "protocolType": 0,
            "vendorType": 0
          },
          "storageName": "string",
          "storageLocation": "string",
          "scanName": "string",
          "progress": {
            "upload": 0,
            "scan": 0,
            "archiveExtraction": 0
          },
          "scanResult": {
            "extractedFiles": {
              "dataId": "string",
              "scanResultI": 0,
              "detectedBy": 0,
              "filesExtractedCount": 0
            },
            "scanResults": {
              "scanDetails": [
                {
                  "engineName": "string",
                  "threatFound": "string",
                  "scanResultI": 0,
                  "defTime": "string",
                  "scanTime": 0.1,
                  "engId": "string",
                  "waitTime": 0.1
                }
              ],
              "dataId": "string",
              "scanAllResultI": 0,
              "scanAllResultA": "string",
              "startTime": "string",
              "totalTime": 0.1,
```

```
"totalDetections": 0,
              "progressPercentage": 0
            },
            "fileInfo": {
              "fileSize": 0,
              "uploadTimestamp": "string",
              "md5": "string",
              "sha1": "string",
              "sha256": "string",
              "fileTypeCategory": "string",
              "fileTypeDescription": "string",
              "fileTypeExtension": "string",
              "displayName": "string",
              "fileTypeId": "string"
            },
            "fileScanInfo": {
              "finalVerdict": {
                "blocked": true,
                "verdict": "string",
                "confidence": 0.1,
                "threatLevel": 0.1
              },
              "overviewReport": {
                "analysisState": "string",
                "signalGroups": [
                  {
                    "description": "string",
                    "verdict": "string",
                    "signals": [
                      {
                        "originType": "string",
                        "signalReadable": "string",
                        "strength": 0.1
                      }
                    ],
                    "mitreTechniques": [
                      {
                        "name": "string",
                        "tacticName": "string"
                      }
                    ]
                  }
                ],
                "iocs": [
                  {
                    "data": "string",
                    "type": "string",
                    "origin": "string",
                    "verdict": "string"
                  }
                ],
                "yaraMatches": [
                  {
```

```
"ruleDescription": "string",
                    "verdict": "string",
                    "matchedStrings": [
                      "string"
                    ],
                    "author": "string",
                    "version": "string",
                    "threatLevel": 0.1,
                    "confidence": 0.1,
                    "strength": 0.1
                  }
                ],
                "tags": [
                  {
                    "name": "string",
                    "verdict": "string"
                  }
                ],
                "metaData": {
                  "entropy": 0.1,
                  "forensicAnalysisRecommended": true,
                  "fuzzyFsioHash": "string"
                }
              },
              "errorCategory": "string",
              "errorCode": 0,
              "errorDetails": "string"
            },
            "processInfo": {
              "postProcessing": {
                "actionsRan": "string",
                "actionsFailed": "string",
                "convertedTo": "string",
                "copyMoveDestination": "string",
                "convertedDestination": "string",
                "sanitizationDetails": {
                  "failureCategory": "string",
                  "description": "string",
                  "details": "string"
                }
              },
              "progressPercentage": 0,
              "userAgent": "string",
              "profile": "string",
              "result": "string",
              "blockedReason": "string",
              "fileTypeSkippedScan": true,
              "processingTime": 0.1,
              "queueTime": 0.1,
              "resultI": 0
            },
            "dataId": "string",
            "dlpInfo": {
```

```
"verdict": 0
            },
            "sbomInfo": {
              "finalVerdict": {
                "blocked": true,
                "licensingPackageCounts": {
                  "allowed": 0,
                  "blocked": 0,
                  "unknown": 0,
                  "unsupported": 0
                },
                "severity": 0,
                "totalPackageCount": 0,
                "verdict": "string",
                "vulnerabilityCounts": {
                  "critical": 0,
                  "high": 0,
                  "medium": 0,
                  "low": 0,
                  "unknown": 0
                }
              },
              "overviewReport": {
                "isPartialReport": true,
                "osInfo": {
                  "osName": "string",
                  "osVersion": "string"
                },
                "scanMode": "string",
                "steps": [
                  {
                    "command": "string",
                    "packages": [
                      {
                        "authors": "string",
                        "releaseDate": "2019-08-24T14:15:22Z",
                        "ecosystem": "string",
                        "group": "string",
                        "archive": true,
                        "executable": true,
                        "uid": "string",
                        "licenses": {
                          "allowed": [
                            {}
                          ],
                          "blocked": [
                            {}
                          ]
                        },
                        "packageName": "string",
                        "packageVersion": "string",
                        "hashes": [
                          {
```

```
"fileName": "string"
                        }
                      ],
                      "vulnerabilityCounts": {
                        "critical": 0,
                        "high": 0,
                        "medium": 0,
                        "low": 0,
                        "unknown": 0
                      },
                      "vulnerabilities": [
                        {
                          "id": "string",
                          "severity": 0,
                          "source": "string",
                          "fixedVersions": "string",
                          "cwes": [
                            null
                          ]
                        }
                      ],
                      "arch": "string",
                      "osName": "string",
                      "osVersion": "string",
                      "dependencies": [
                        {
                          "ecosystem": "string",
                          "group": "string",
                          "packageName": "string",
                          "packageVersion": "string",
                          "vulnerabilities": [
                            null
                          ],
                          "vulnerabilityCounts": {}
                        }
                      ]
                    }
                  ],
                  "licenseStatus": "string",
                  "licensingPackageCounts": {
                    "allowed": 0,
                    "blocked": 0,
                    "unknown": 0,
                    "unsupported": 0
                  },
                  "step": 0,
                  "vulnerabilityCount": 0,
                  "sha256": "string",
                  "severity": 0,
                  "vulnerabilityCounts": {
                    "critical": 0,
                    "high": 0,
                    "medium": 0,
```

```
"unknown": 0
                    }
                  }
                ],
                "packages": [
                  {
                    "authors": "string",
                    "releaseDate": "2019-08-24T14:15:22Z",
                    "ecosystem": "string",
                    "group": "string",
                    "archive": true,
                    "executable": true,
                    "uid": "string",
                    "licenses": {
                      "allowed": [
                        {
                          "id": "string",
                          "url": "string",
                          "category": "string",
                          "usageRestriction": {
                            "permissions": [
                              null
                            ],
                            "conditions": [
                              null
                            ],
                            "limitations": [
                              null
                            ]
                          }
                        }
                      ],
                      "blocked": [
                        {
                          "id": "string",
                          "url": "string",
                          "category": "string",
                          "usageRestriction": {
                            "permissions": [
                              null
                            ],
                            "conditions": [
                              null
                            ],
                            "limitations": [
                              null
                            ]
                          }
                        }
                      ]
                    },
                    "packageName": "string",
                    "packageVersion": "string",
```

```
"hashes": [
                        {
                          "sha256": "string",
                          "fileName": "string"
                        }
                      ],
                      "vulnerabilities": [
                        {
                          "id": "string",
                          "severity": 0,
                          "source": "string",
                          "fixedVersions": "string",
                          "cwes": [
                            "string"
                          ]
                        }
                      ],
                      "vulnerabilityCounts": {
                        "critical": 0,
                        "high": 0,
                        "medium": 0,
                        "low": 0,
                        "unknown": 0
                      },
                      "dependencies": [
                        {
                          "ecosystem": "string",
                          "group": "string",
                          "packageName": "string",
                          "packageVersion": "string",
                          "vulnerabilities": [
                            {
                              "id": "string",
                              "severity": 0,
                              "source": "string",
                              "fixedVersions": "string",
                              "cwes": [
                                null
                              ]
                            }
                          ],
                          "vulnerabilityCounts": {
                            "critical": 0,
                            "high": 0,
                            "medium": 0,
                            "low": 0,
                            "unknown": 0
                          }
                        }
                      ]
                    }
                  ],
                  "dependenciesPackageCount": 0,
```

```
"dependenciesVulnerabilityCounts": {
                  "critical": 0,
                  "high": 0,
                  "medium": 0,
                  "low": 0,
                  "unknown": 0
                }
              },
              "resultTemplateHash": "string"
            },
            "vulnerabilityInfo": {
              "vulnerabilityInfoResult": {
                "code": 0,
                "hash": "string",
                "method": 0,
                "timeStamp": "string",
                "timing": 0,
                "detectedProduct": {
                  "hasVulnerability": true,
                  "isCurrent": true,
                  "product": {
                    "id": 0,
                    "name": "string"
                  },
                  "remediationLink": "string",
                  "severity": "string",
                  "sigName": "string",
                  "signature": 0,
                  "vendor": {
                    "id": 0,
                    "name": "string"
                  },
                  "version": "string",
                  "versionData": {
                    "countBehind": 0,
                    "feedId": 0,
                    "version": "string"
                  },
                  "vulnerabilities": [
                    {
                      "description": "string",
                      "details": {
                        "cpe": "string",
                        "cve": "string",
                        "cvss": {
                          "accessComplexity": "string",
                          "accessVector": "string",
                          "authentication": "string",
                          "availabilityImpact": "string",
                          "confidentialityImpact": "string",
                          "generatedOnEpoch": "string",
                          "integrityImpact": "string",
                          "score": "string",
```

```
},
                        "cvss3": {
                          "attackComplexity": "string",
                          "attackVector": "string",
                          "availabilityImpact": "string",
                          "baseScore": "string",
                          "baseSeverity": "string",
                          "confidentialityImpact": "string",
                          "exploitabilityScore": "string",
                          "impactScore": "string",
                          "integrityImpact": "string",
                          "privilegesRequired": "string",
                          "scope": "string",
                          "userInteraction": "string",
                          "vectorString": "string"
                        },
                        "cwe": "string",
                        "lastModifiedEpoch": "string",
                        "publishedEpoch": "string",
                        "references": [
                          "string"
                        ]
                      },
                      "severity": "string",
                      "severityIndex": 0,
                      "staticId": 0
                    }
                  ]
                }
              }
            },
            "sessionCookie": "string",
            "fileTypeInfo": {
              "fileInfoExtended": {
                "extensions": "string",
                "groupId": "string",
                "typeId": "string"
              }
            },
            "scanInstanceUrl": "string",
            "scanWorkflowSnapshotId": "string",
            "coreEngines": [
              {
                "engineId": "string",
                "engineName": "string",
                "engineVersion": "string",
                "dbVersion": "string",
                "definitionTime": "string"
              }
            ]
          },
          "processingState": 0,
          "exception": {
```

```
"exceptionMessage": "string"
          },
          "created": "2019-08-24T14:15:22Z",
          "lastModified": "2019-08-24T14:15:22Z",
          "discoveryStarted": "2019-08-24T14:15:22Z",
          "fileProcessingDetails": {
            "streamingStartedTime": "2019-08-24T14:15:22Z",
            "streamingCompletedTime": "2019-08-24T14:15:22Z",
            "streamingTimeSpanMs": 0,
            "scanCompletedTime": "2019-08-24T14:15:22Z",
            "processingTimeSpanMs": 0
          },
          "coreEngines": [
            {
              "engineId": "string",
              "engineName": "string",
              "engineVersion": "string",
              "dbVersion": "string",
              "definitionTime": "string"
            }
          ],
          "remediation": {
            "deepCdr": {
              "sanitizationDetails": {
                "failureCategory": "string",
                "description": "string",
                "details": "string"
              },
              "cdrObjectState": 0,
              "fileWasReplaced": true
            },
            "postActionFailedInformation": [
              {
                "objectActionType": 0,
                "exception": {
                  "exceptionDetails": "string",
                  "exceptionMessage": "string"
                }
              }
            ],
            "objectRemediationActions": [
              {
                "objectActionType": 0,
                "objectActionState": 0,
                "cdrObjectState": 0,
                "exceptions": [
                  "string"
                ],
                "id": "string",
                "fileId": "string",
                "fileScanCompletedTime": "2019-08-24T14:15:22Z",
                "remediationId": "string",
                "tenantId": "string",
```

```
}
            ]
          },
          "metaDefenderCoreUrl": "string",
          "discoveryStartedDaySec": 0,
          "objectStorageMetadata": "string",
          "scanWorkflowSnapshotId": "string",
          "scanWorkflowSnapshot": {
            "id": "string",
            "scanId": "string",
            "workflow": {
              "id": "string",
              "scanPoolId": "string",
              "scanProcessFlow": 0,
              "isIdentityScanningEnabled": true,
              "scanIntervalDays": 0,
              "rules": [
                "string"
              ],
              "type": 0,
              "workflowSupportedTechnologies": {
                "dlp": {
                  "status": 0
                },
                "deepCdr": {
                  "status": 0
                },
                "sandBox": {
                  "status": 0
                },
                "metascan": {
                  "status": 0
                }
              },
              "name": "string",
              "userAgent": "string",
              "scanPool": {
                "id": "string",
                "name": "string",
                "scanPoolType": 0,
                "isDefault": true,
                "scanInstances": [
                  {
                    "id": "string",
                    "scanPoolId": "string",
                    "url": "string",
                    "apiKey": "string",
                    "timeout": "string",
                    "scanInstanceType": 0
                  }
                ]
              },
              "failOverScanPoolId": "string",
```

```
"id": "string",
                "name": "string",
                "scanPoolType": 0,
                "isDefault": true,
                "scanInstances": [
                  {
                    "id": "string",
                    "scanPoolId": "string",
                    "url": "string",
                    "apiKey": "string",
                    "timeout": "string",
                    "scanInstanceType": 0
                  }
                ]
              },
              "filters": {
                "id": "string",
                "minimumSize": 0,
                "maximumSize": 0,
                "minimumDateTime": "2019-08-24T14:15:22Z",
                "maximumDateTime": "2019-08-24T14:15:22Z"
              },
              "fileDefinition": {
                "blockingStrategy": 0,
                "configurableBlockingStrategy": {
                  "shouldTreatFilesWithSensitiveDataAsBlocked": true,
                  "shouldTreatFilesWithVulnerabilitiesAsBlocked": true
                }
              },
              "remediations": [
                {
                  "id": "string",
                  "workflowId": "string",
                  "isEnabled": true,
                  "configuration": "string",
                  "type": 0,
                  "handlingType": 0
                }
              ],
              "tenantId": "string"
            },
            "startTimestamp": 0,
            "stopTimestamp": 0,
            "scanPool": {
              "id": "string",
              "name": "string",
              "scanPoolType": 0,
              "isDefault": true,
              "scanInstances": [
                {
                  "id": "string",
                  "scanPoolId": "string",
                  "url": "string",
```

```
"timeout": "string",
                  "scanInstanceType": 0
                }
              ]
            },
            "scanInstances": [
              {
                "id": "string",
                "scanPoolId": "string",
                "url": "string",
                "apiKey": "string",
                "timeout": "string",
                "scanInstanceType": 0
              }
            ],
            "failOverScanPool": {
              "id": "string",
              "name": "string",
              "scanPoolType": 0,
              "isDefault": true,
              "scanInstances": [
                {
                  "id": "string",
                  "scanPoolId": "string",
                  "url": "string",
                  "apiKey": "string",
                  "timeout": "string",
                  "scanInstanceType": 0
                }
              ]
            },
            "failOverScanInstances": [
              {
                "id": "string",
                "scanPoolId": "string",
                "url": "string",
                "apiKey": "string",
                "timeout": "string",
                "scanInstanceType": 0
              }
            ],
            "storage": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
              "accountId": "string",
              "source": "string",
              "storageFunctionality": "string",
              "storageType": {
                "name": "string",
                "categoryType": 0,
                "protocolType": 0,
```

```
},
              "storageStatus": {
                "message": "string",
                "statusType": 0
              },
              "workflowId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z",
              "tenantId": "string",
              "groupRef": {
                "id": "string",
                "name": "string"
              },
              "isAutodiscovered": true
            },
            "workflowStatistics": {
              "taggingStatistics": {
                "total": 0
              },
              "keepAllowedStatistics": {
                "total": 0
              },
              "keepBlockedStatistics": {
                "total": 0
              },
              "keepSanitizedStatistics": {
                "total": 0
              },
              "movedAllowedStatistics": {
                "total": 0,
                "destinationStorageInformation": {
                  "id": "string",
                  "name": "string",
                  "groupId": "string",
                  "clientId": "string",
                  "accountId": "string",
                  "source": "string",
                  "storageFunctionality": "string",
                  "storageType": {
                    "name": "string",
                    "categoryType": 0,
                    "protocolType": 0,
                    "vendorType": 0
                  },
                  "storageStatus": {
                    "message": "string",
                    "statusType": 0
                  },
                  "workflowId": "string",
                  "lastUpdated": "2019-08-24T14:15:22Z",
                  "tenantId": "string",
                  "groupRef": {
                    "id": "string",
                    "name": "string"
```

```
"isAutodiscovered": true
                }
              },
              "movedSanitizedStatistics": {
                "total": 0,
                "destinationStorageInformation": {
                  "id": "string",
                  "name": "string",
                  "groupId": "string",
                  "clientId": "string",
                  "accountId": "string",
                  "source": "string",
                  "storageFunctionality": "string",
                  "storageType": {
                    "name": "string",
                    "categoryType": 0,
                    "protocolType": 0,
                    "vendorType": 0
                  },
                  "storageStatus": {
                    "message": "string",
                    "statusType": 0
                  },
                  "workflowId": "string",
                  "lastUpdated": "2019-08-24T14:15:22Z",
                  "tenantId": "string",
                  "groupRef": {
                    "id": "string",
                    "name": "string"
                  },
                  "isAutodiscovered": true
                }
              },
              "movedBlockedStatistics": {
                "total": 0,
                "destinationStorageInformation": {
                  "id": "string",
                  "name": "string",
                  "groupId": "string",
                  "clientId": "string",
                  "accountId": "string",
                  "source": "string",
                  "storageFunctionality": "string",
                  "storageType": {
                    "name": "string",
                    "categoryType": 0,
                    "protocolType": 0,
                    "vendorType": 0
                  },
                  "storageStatus": {
                    "message": "string",
                    "statusType": 0
                  },
```

```
"lastUpdated": "2019-08-24T14:15:22Z",
                  "tenantId": "string",
                  "groupRef": {
                    "id": "string",
                    "name": "string"
                  },
                  "isAutodiscovered": true
                }
              },
              "copyAllowedStatistics": {
                "total": 0,
                "destinationStorageInformation": {
                  "id": "string",
                  "name": "string",
                  "groupId": "string",
                  "clientId": "string",
                  "accountId": "string",
                  "source": "string",
                  "storageFunctionality": "string",
                  "storageType": {
                    "name": "string",
                    "categoryType": 0,
                    "protocolType": 0,
                    "vendorType": 0
                  },
                  "storageStatus": {
                    "message": "string",
                    "statusType": 0
                  },
                  "workflowId": "string",
                  "lastUpdated": "2019-08-24T14:15:22Z",
                  "tenantId": "string",
                  "groupRef": {
                    "id": "string",
                    "name": "string"
                  },
                  "isAutodiscovered": true
                }
              },
              "copyBlockedStatistics": {
                "total": 0,
                "destinationStorageInformation": {
                  "id": "string",
                  "name": "string",
                  "groupId": "string",
                  "clientId": "string",
                  "accountId": "string",
                  "source": "string",
                  "storageFunctionality": "string",
                  "storageType": {
                    "name": "string",
                    "categoryType": 0,
                    "protocolType": 0,
```

```
},
                  "storageStatus": {
                    "message": "string",
                    "statusType": 0
                  },
                  "workflowId": "string",
                  "lastUpdated": "2019-08-24T14:15:22Z",
                  "tenantId": "string",
                  "groupRef": {
                    "id": "string",
                    "name": "string"
                  },
                  "isAutodiscovered": true
                }
              },
              "deleteAllowedStatistics": {
                "total": 0
              },
              "deleteBlockedStatistics": {
                "total": 0
              },
              "lastCalculatedStatisticsTime": "2019-08-24T14:15:22Z"
            },
            "account": {
              "id": "string",
              "name": "string",
              "description": "string",
              "credentials": "string",
              "protocolType": 0,
              "vendorType": 0,
              "autoDiscovery": true,
              "autodiscoveryDestinationGroupId": "string",
              "destinationGroup": {
                "id": "string",
                "name": "string"
              }
            },
            "realTimeStartDate": "2019-08-24T14:15:22Z"
          },
          "versions": [],
          "hasBlockedVersions": true,
          "versionsCount": 0,
          "objectType": 0,
          "skippedScan": true,
          "$type": "string",
          "url": "string",
          "fileId": "string"
        }
      ],
      "hasBlockedVersions": true,
      "versionsCount": 0,
      "objectType": 0,
      "skippedScan": true,
```

```
}
  ],
  "filterCount": 0,
  "totalCount": 0
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	EnumerateFiles

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Rescan multiple files on demand

`PUT /api/file/rescan`

This request is used to rescan and update existing files from a scan based on a filter.

> Body parameter

```
{
  "scanId": "string",
  "workflowId": "string",
  "passwords": [
    "string"
  ],
  "filterParameters": {
    "expand": [
      "string"
    ],
    "startDate": "2019-08-24T14:15:22Z",
    "endDate": "2019-08-24T14:15:22Z",
    "search": "string",
    "scanType": [
      0
    ],
    "storageId": [
      "string"
    ],
    "scanId": [
      "string"
    ],
    "scanWorkflowSnapshotId": [
      "string"
    ],
    "processingState": [
      0
    ],
    "result": [
      0
    ],
    "scanAllResultI": [
      0
    ],
    "scanResultICount": [
      0
    ],
    "sandboxVerdict": [
      0
    ],
    "vulnerabilityCount": [
      0
    ],
    "hasVulnerabilities": true,
    "dlpDetection": true,
    "hasBlockedFileVersions": true,
    "remediations": [
      0
    ],
    "skippedScan": true,
    "sortBy": [
      0
```

```
"sortOrder": [
      0
    ]
  },
  "storageProtocolType": 0,
  "mdssBaseUrl": "string"
}
```


Parameters

Name	In	Type	Required	Description
body	body	OnDemandFilteredScanParameters	true	none

Example responses

200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	OnDemandScanCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Fetch processing results for a file

`GET /api/file/{fileId}`

File processing is done asynchronously and each analysis request is tracked by a file ID. Because processing a file is a potentially time-consuming operation, scheduling a file for processing and retrieving the results needs to be done using two separate API calls.

This request needs to be made multiple times until the analysis is complete. Analysis completion can be tracked using the processingState and the progress values from the response...

Parameters

Name	In	Type	Required	Description
fileId	path	string	true	none
expand	query	array[string]	false	Possible values for expand: workflow_snapshot

> Example responses

> 200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "id": "string",
  "scanId": "string",
  "name": "string",
  "path": "string",
  "hash": "string",
  "fileOwner": {
    "userId": "string",
    "fullName": "string",
    "userName": "string",
    "emailAddress": "string"
  },
  "size": 0,
  "storageType": {
    "name": "string",
    "categoryType": 0,
    "protocolType": 0,
    "vendorType": 0
  },
  "storageName": "string",
  "storageLocation": "string",
  "scanName": "string",
  "progress": {
    "upload": 0,
    "scan": 0,
    "archiveExtraction": 0
  },
  "scanResult": {
    "extractedFiles": {
      "dataId": "string",
      "scanResultI": 0,
      "detectedBy": 0,
      "filesExtractedCount": 0
    },
    "scanResults": {
      "scanDetails": [
        {
          "engineName": "string",
          "threatFound": "string",
          "scanResultI": 0,
          "defTime": "string",
          "scanTime": 0.1,
          "engId": "string",
          "waitTime": 0.1
        }
```

```
"dataId": "string",
      "scanAllResultI": 0,
      "scanAllResultA": "string",
      "startTime": "string",
      "totalTime": 0.1,
      "totalAvs": 0,
      "totalDetections": 0,
      "progressPercentage": 0
    },
    "fileInfo": {
      "fileSize": 0,
      "uploadTimestamp": "string",
      "md5": "string",
      "sha1": "string",
      "sha256": "string",
      "fileTypeCategory": "string",
      "fileTypeDescription": "string",
      "fileTypeExtension": "string",
      "displayName": "string",
      "fileTypeId": "string"
    },
    "fileScanInfo": {
      "finalVerdict": {
        "blocked": true,
        "verdict": "string",
        "confidence": 0.1,
        "threatLevel": 0.1
      },
      "overviewReport": {
        "analysisState": "string",
        "signalGroups": [
          {
            "description": "string",
            "verdict": "string",
            "signals": [
              {
                "originType": "string",
                "signalReadable": "string",
                "strength": 0.1
              }
            ],
            "mitreTechniques": [
              {
                "name": "string",
                "tacticName": "string"
              }
            ]
          }
        ],
        "iocs": [
          {
            "data": "string",
            "type": "string",
```

```
"verdict": "string"
          }
        ],
        "yaraMatches": [
          {
            "ruleName": "string",
            "ruleDescription": "string",
            "verdict": "string",
            "matchedStrings": [
              "string"
            ],
            "author": "string",
            "version": "string",
            "threatLevel": 0.1,
            "confidence": 0.1,
            "strength": 0.1
          }
        ],
        "tags": [
          {
            "name": "string",
            "verdict": "string"
          }
        ],
        "metaData": {
          "entropy": 0.1,
          "forensicAnalysisRecommended": true,
          "fuzzyFsioHash": "string"
        }
      },
      "errorCategory": "string",
      "errorCode": 0,
      "errorDetails": "string"
    },
    "processInfo": {
      "postProcessing": {
        "actionsRan": "string",
        "actionsFailed": "string",
        "convertedTo": "string",
        "copyMoveDestination": "string",
        "convertedDestination": "string",
        "sanitizationDetails": {
          "failureCategory": "string",
          "description": "string",
          "details": "string"
        }
      },
      "progressPercentage": 0,
      "userAgent": "string",
      "profile": "string",
      "result": "string",
      "blockedReason": "string",
      "fileTypeSkippedScan": true,
```

```
"queueTime": 0.1,
      "resultI": 0
    },
    "dataId": "string",
    "dlpInfo": {
      "hits": null,
      "verdict": 0
    },
    "sbomInfo": {
      "finalVerdict": {
        "blocked": true,
        "licensingPackageCounts": {
          "allowed": 0,
          "blocked": 0,
          "unknown": 0,
          "unsupported": 0
        },
        "severity": 0,
        "totalPackageCount": 0,
        "verdict": "string",
        "vulnerabilityCounts": {
          "critical": 0,
          "high": 0,
          "medium": 0,
          "low": 0,
          "unknown": 0
        }
      },
      "overviewReport": {
        "isPartialReport": true,
        "osInfo": {
          "osName": "string",
          "osVersion": "string"
        },
        "scanMode": "string",
        "steps": [
          {
            "command": "string",
            "packages": [
              {
                "authors": "string",
                "releaseDate": "2019-08-24T14:15:22Z",
                "ecosystem": "string",
                "group": "string",
                "archive": true,
                "executable": true,
                "uid": "string",
                "licenses": {
                  "allowed": [
                    {
                      "id": "string",
                      "url": "string",
                      "category": "string",
```

```
"permissions": [
                        "string"
                      ],
                      "conditions": [
                        "string"
                      ],
                      "limitations": [
                        "string"
                      ]
                    }
                  }
                ],
                "blocked": [
                  {
                    "id": "string",
                    "url": "string",
                    "category": "string",
                    "usageRestriction": {
                      "permissions": [
                        "string"
                      ],
                      "conditions": [
                        "string"
                      ],
                      "limitations": [
                        "string"
                      ]
                    }
                  }
                ]
              },
              "packageName": "string",
              "packageVersion": "string",
              "hashes": [
                {
                  "sha256": "string",
                  "fileName": "string"
                }
              ],
              "vulnerabilityCounts": {
                "critical": 0,
                "high": 0,
                "medium": 0,
                "low": 0,
                "unknown": 0
              },
              "vulnerabilities": [
                {
                  "id": "string",
                  "severity": 0,
                  "source": "string",
                  "fixedVersions": "string",
                  "cwes": [
```

```
]
                  }
                ],
                "arch": "string",
                "osName": "string",
                "osVersion": "string",
                "dependencies": [
                  {
                    "ecosystem": "string",
                    "group": "string",
                    "packageName": "string",
                    "packageVersion": "string",
                    "vulnerabilities": [
                      {
                        "id": "string",
                        "severity": 0,
                        "source": "string",
                        "fixedVersions": "string",
                        "cwes": [
                          "string"
                        ]
                      }
                    ],
                    "vulnerabilityCounts": {
                      "critical": 0,
                      "high": 0,
                      "medium": 0,
                      "low": 0,
                      "unknown": 0
                    }
                  }
                ]
              }
            ],
            "licenseStatus": "string",
            "licensingPackageCounts": {
              "allowed": 0,
              "blocked": 0,
              "unknown": 0,
              "unsupported": 0
            },
            "step": 0,
            "vulnerabilityCount": 0,
            "sha256": "string",
            "severity": 0,
            "vulnerabilityCounts": {
              "critical": 0,
              "high": 0,
              "medium": 0,
              "low": 0,
              "unknown": 0
            }
          }
```

```
"packages": [
          {
            "authors": "string",
            "releaseDate": "2019-08-24T14:15:22Z",
            "ecosystem": "string",
            "group": "string",
            "archive": true,
            "executable": true,
            "uid": "string",
            "licenses": {
              "allowed": [
                {
                  "id": "string",
                  "url": "string",
                  "category": "string",
                  "usageRestriction": {
                    "permissions": [
                      "string"
                    ],
                    "conditions": [
                      "string"
                    ],
                    "limitations": [
                      "string"
                    ]
                  }
                }
              ],
              "blocked": [
                {
                  "id": "string",
                  "url": "string",
                  "category": "string",
                  "usageRestriction": {
                    "permissions": [
                      "string"
                    ],
                    "conditions": [
                      "string"
                    ],
                    "limitations": [
                      "string"
                    ]
                  }
                }
              ]
            },
            "packageName": "string",
            "packageVersion": "string",
            "target": "string",
            "hashes": [
              {
                "sha256": "string",
```

```
}
            ],
            "vulnerabilities": [
              {
                "id": "string",
                "severity": 0,
                "source": "string",
                "fixedVersions": "string",
                "cwes": [
                  "string"
                ]
              }
            ],
            "vulnerabilityCounts": {
              "critical": 0,
              "high": 0,
              "medium": 0,
              "low": 0,
              "unknown": 0
            },
            "dependencies": [
              {
                "ecosystem": "string",
                "group": "string",
                "packageName": "string",
                "packageVersion": "string",
                "vulnerabilities": [
                  {
                    "id": "string",
                    "severity": 0,
                    "source": "string",
                    "fixedVersions": "string",
                    "cwes": [
                      "string"
                    ]
                  }
                ],
                "vulnerabilityCounts": {
                  "critical": 0,
                  "high": 0,
                  "medium": 0,
                  "low": 0,
                  "unknown": 0
                }
              }
            ]
          }
        ],
        "dependenciesPackageCount": 0,
        "dependenciesVulnerabilityTotal": 0,
        "dependenciesVulnerabilityCounts": {
          "critical": 0,
          "high": 0,
```

```
"low": 0,
          "unknown": 0
        }
      },
      "resultTemplateHash": "string"
    },
    "vulnerabilityInfo": {
      "vulnerabilityInfoResult": {
        "code": 0,
        "hash": "string",
        "method": 0,
        "timeStamp": "string",
        "timing": 0,
        "detectedProduct": {
          "hasVulnerability": true,
          "isCurrent": true,
          "product": {
            "id": 0,
            "name": "string"
          },
          "remediationLink": "string",
          "severity": "string",
          "sigName": "string",
          "signature": 0,
          "vendor": {
            "id": 0,
            "name": "string"
          },
          "version": "string",
          "versionData": {
            "countBehind": 0,
            "feedId": 0,
            "version": "string"
          },
          "vulnerabilities": [
            {
              "description": "string",
              "details": {
                "cpe": "string",
                "cve": "string",
                "cvss": {
                  "accessComplexity": "string",
                  "accessVector": "string",
                  "authentication": "string",
                  "availabilityImpact": "string",
                  "confidentialityImpact": "string",
                  "generatedOnEpoch": "string",
                  "integrityImpact": "string",
                  "score": "string",
                  "source": "string"
                },
                "cvss3": {
                  "attackComplexity": "string",
```

```
"availabilityImpact": "string",
                  "baseScore": "string",
                  "baseSeverity": "string",
                  "confidentialityImpact": "string",
                  "exploitabilityScore": "string",
                  "impactScore": "string",
                  "integrityImpact": "string",
                  "privilegesRequired": "string",
                  "scope": "string",
                  "userInteraction": "string",
                  "vectorString": "string"
                },
                "cwe": "string",
                "lastModifiedEpoch": "string",
                "publishedEpoch": "string",
                "references": [
                  "string"
                ]
              },
              "severity": "string",
              "severityIndex": 0,
              "staticId": 0
            }
          ]
        }
      }
    },
    "sessionCookie": "string",
    "fileTypeInfo": {
      "fileInfoExtended": {
        "extensions": "string",
        "groupId": "string",
        "typeId": "string"
      }
    },
    "scanInstanceUrl": "string",
    "scanWorkflowSnapshotId": "string",
    "coreEngines": [
      {
        "engineId": "string",
        "engineName": "string",
        "engineVersion": "string",
        "dbVersion": "string",
        "definitionTime": "string"
      }
    ]
  },
  "processingState": 0,
  "exception": {
    "exceptionDetails": "string",
    "exceptionMessage": "string"
  },
  "created": "2019-08-24T14:15:22Z",
```

```
"discoveryStarted": "2019-08-24T14:15:22Z",
  "fileProcessingDetails": {
    "streamingStartedTime": "2019-08-24T14:15:22Z",
    "streamingCompletedTime": "2019-08-24T14:15:22Z",
    "streamingTimeSpanMs": 0,
    "scanCompletedTime": "2019-08-24T14:15:22Z",
    "processingTimeSpanMs": 0
  },
  "coreEngines": [
    {
      "engineId": "string",
      "engineName": "string",
      "engineVersion": "string",
      "dbVersion": "string",
      "definitionTime": "string"
    }
  ],
  "remediation": {
    "deepCdr": {
      "sanitizationDetails": {
        "failureCategory": "string",
        "description": "string",
        "details": "string"
      },
      "cdrObjectState": 0,
      "fileWasReplaced": true
    },
    "postActionFailedInformation": [
      {
        "objectActionType": 0,
        "exception": {
          "exceptionDetails": "string",
          "exceptionMessage": "string"
        }
      }
    ],
    "objectRemediationActions": [
      {
        "objectActionType": 0,
        "objectActionState": 0,
        "cdrObjectState": 0,
        "exceptions": [
          "string"
        ],
        "id": "string",
        "fileId": "string",
        "fileScanCompletedTime": "2019-08-24T14:15:22Z",
        "remediationId": "string",
        "tenantId": "string",
        "lastUpdated": "2019-08-24T14:15:22Z"
      }
    ]
  },
```

```
"discoveryStartedDaySec": 0,
  "fileDto": {
    "result": 0,
    "responseKey": "string",
    "responseMessage": "string",
    "responseMessageParams": {
      "property1": "string",
      "property2": "string"
    },
    "id": "string",
    "scanId": "string",
    "name": "string",
    "path": "string",
    "hash": "string",
    "fileOwner": {
      "userId": "string",
      "fullName": "string",
      "userName": "string",
      "emailAddress": "string"
    },
    "size": 0,
    "fileTypeCategory": 0,
    "extension": "string",
    "storageType": {
      "name": "string",
      "categoryType": 0,
      "protocolType": 0,
      "vendorType": 0
    },
    "storageName": "string",
    "storageLocation": "string",
    "scanName": "string",
    "progress": {
      "upload": 0,
      "scan": 0,
      "archiveExtraction": 0
    },
    "scanResult": {
      "extractedFiles": {
        "dataId": "string",
        "scanResultI": 0,
        "detectedBy": 0,
        "filesExtractedCount": 0
      },
      "scanResults": {
        "scanDetails": [
          {
            "engineName": "string",
            "threatFound": "string",
            "scanResultI": 0,
            "defTime": "string",
            "scanTime": 0.1,
            "engId": "string",
```

```
}
        ],
        "dataId": "string",
        "scanAllResultI": 0,
        "scanAllResultA": "string",
        "startTime": "string",
        "totalTime": 0.1,
        "totalAvs": 0,
        "totalDetections": 0,
        "progressPercentage": 0
      },
      "fileInfo": {
        "fileSize": 0,
        "uploadTimestamp": "string",
        "md5": "string",
        "sha1": "string",
        "sha256": "string",
        "fileTypeCategory": "string",
        "fileTypeDescription": "string",
        "fileTypeExtension": "string",
        "displayName": "string",
        "fileTypeId": "string"
      },
      "fileScanInfo": {
        "finalVerdict": {
          "blocked": true,
          "verdict": "string",
          "confidence": 0.1,
          "threatLevel": 0.1
        },
        "overviewReport": {
          "analysisState": "string",
          "signalGroups": [
            {
              "description": "string",
              "verdict": "string",
              "signals": [
                {
                  "originType": "string",
                  "signalReadable": "string",
                  "strength": 0.1
                }
              ],
              "mitreTechniques": [
                {
                  "name": "string",
                  "tacticName": "string"
                }
              ]
            }
          ],
          "iocs": [
            {
```

```
"type": "string",
              "origin": "string",
              "verdict": "string"
            }
          ],
          "yaraMatches": [
            {
              "ruleName": "string",
              "ruleDescription": "string",
              "verdict": "string",
              "matchedStrings": [
                "string"
              ],
              "author": "string",
              "version": "string",
              "threatLevel": 0.1,
              "confidence": 0.1,
              "strength": 0.1
            }
          ],
          "tags": [
            {
              "name": "string",
              "verdict": "string"
            }
          ],
          "metaData": {
            "entropy": 0.1,
            "forensicAnalysisRecommended": true,
            "fuzzyFsioHash": "string"
          }
        },
        "errorCategory": "string",
        "errorCode": 0,
        "errorDetails": "string"
      },
      "processInfo": {
        "postProcessing": {
          "actionsRan": "string",
          "actionsFailed": "string",
          "convertedTo": "string",
          "copyMoveDestination": "string",
          "convertedDestination": "string",
          "sanitizationDetails": {
            "failureCategory": "string",
            "description": "string",
            "details": "string"
          }
        },
        "progressPercentage": 0,
        "userAgent": "string",
        "profile": "string",
        "result": "string",
```

```
"fileTypeSkippedScan": true,
        "processingTime": 0.1,
        "queueTime": 0.1,
        "resultI": 0
      },
      "dataId": "string",
      "dlpInfo": {
        "hits": null,
        "verdict": 0
      },
      "sbomInfo": {
        "finalVerdict": {
          "blocked": true,
          "licensingPackageCounts": {
            "allowed": 0,
            "blocked": 0,
            "unknown": 0,
            "unsupported": 0
          },
          "severity": 0,
          "totalPackageCount": 0,
          "verdict": "string",
          "vulnerabilityCounts": {
            "critical": 0,
            "high": 0,
            "medium": 0,
            "low": 0,
            "unknown": 0
          }
        },
        "overviewReport": {
          "isPartialReport": true,
          "osInfo": {
            "osName": "string",
            "osVersion": "string"
          },
          "scanMode": "string",
          "steps": [
            {
              "command": "string",
              "packages": [
                {
                  "authors": "string",
                  "releaseDate": "2019-08-24T14:15:22Z",
                  "ecosystem": "string",
                  "group": "string",
                  "archive": true,
                  "executable": true,
                  "uid": "string",
                  "licenses": {
                    "allowed": [
                      {
                        "id": "string",
```

```
"category": "string",
                        "usageRestriction": {
                          "permissions": [
                            "string"
                          ],
                          "conditions": [
                            "string"
                          ],
                          "limitations": [
                            "string"
                          ]
                        }
                      }
                    ],
                    "blocked": [
                      {
                        "id": "string",
                        "url": "string",
                        "category": "string",
                        "usageRestriction": {
                          "permissions": [
                            "string"
                          ],
                          "conditions": [
                            "string"
                          ],
                          "limitations": [
                            "string"
                          ]
                        }
                      }
                    ]
                  },
                  "packageName": "string",
                  "packageVersion": "string",
                  "hashes": [
                    {
                      "sha256": "string",
                      "fileName": "string"
                    }
                  ],
                  "vulnerabilityCounts": {
                    "critical": 0,
                    "high": 0,
                    "medium": 0,
                    "low": 0,
                    "unknown": 0
                  },
                  "vulnerabilities": [
                    {
                      "id": "string",
                      "severity": 0,
                      "source": "string",
```

```
"cwes": [
                        "string"
                      ]
                    }
                  ],
                  "arch": "string",
                  "osName": "string",
                  "osVersion": "string",
                  "dependencies": [
                    {
                      "ecosystem": "string",
                      "group": "string",
                      "packageName": "string",
                      "packageVersion": "string",
                      "vulnerabilities": [
                        {
                          "id": "string",
                          "severity": 0,
                          "source": "string",
                          "fixedVersions": "string",
                          "cwes": [
                            "string"
                          ]
                        }
                      ],
                      "vulnerabilityCounts": {
                        "critical": 0,
                        "high": 0,
                        "medium": 0,
                        "low": 0,
                        "unknown": 0
                      }
                    }
                  ]
                }
              ],
              "licenseStatus": "string",
              "licensingPackageCounts": {
                "allowed": 0,
                "blocked": 0,
                "unknown": 0,
                "unsupported": 0
              },
              "step": 0,
              "vulnerabilityCount": 0,
              "sha256": "string",
              "severity": 0,
              "vulnerabilityCounts": {
                "critical": 0,
                "high": 0,
                "medium": 0,
                "low": 0,
                "unknown": 0
```

```
}
          ],
          "packages": [
            {
              "authors": "string",
              "releaseDate": "2019-08-24T14:15:22Z",
              "ecosystem": "string",
              "group": "string",
              "archive": true,
              "executable": true,
              "uid": "string",
              "licenses": {
                "allowed": [
                  {
                    "id": "string",
                    "url": "string",
                    "category": "string",
                    "usageRestriction": {
                      "permissions": [
                        "string"
                      ],
                      "conditions": [
                        "string"
                      ],
                      "limitations": [
                        "string"
                      ]
                    }
                  }
                ],
                "blocked": [
                  {
                    "id": "string",
                    "url": "string",
                    "category": "string",
                    "usageRestriction": {
                      "permissions": [
                        "string"
                      ],
                      "conditions": [
                        "string"
                      ],
                      "limitations": [
                        "string"
                      ]
                    }
                  }
                ]
              },
              "packageName": "string",
              "packageVersion": "string",
              "target": "string",
              "hashes": [
```

```
"sha256": "string",
                  "fileName": "string"
                }
              ],
              "vulnerabilities": [
                {
                  "id": "string",
                  "severity": 0,
                  "source": "string",
                  "fixedVersions": "string",
                  "cwes": [
                    "string"
                  ]
                }
              ],
              "vulnerabilityCounts": {
                "critical": 0,
                "high": 0,
                "medium": 0,
                "low": 0,
                "unknown": 0
              },
              "dependencies": [
                {
                  "ecosystem": "string",
                  "group": "string",
                  "packageName": "string",
                  "packageVersion": "string",
                  "vulnerabilities": [
                    {
                      "id": "string",
                      "severity": 0,
                      "source": "string",
                      "fixedVersions": "string",
                      "cwes": [
                        "string"
                      ]
                    }
                  ],
                  "vulnerabilityCounts": {
                    "critical": 0,
                    "high": 0,
                    "medium": 0,
                    "low": 0,
                    "unknown": 0
                  }
                }
              ]
            }
          ],
          "dependenciesPackageCount": 0,
          "dependenciesVulnerabilityTotal": 0,
          "dependenciesVulnerabilityCounts": {
```

```
"high": 0,
            "medium": 0,
            "low": 0,
            "unknown": 0
          }
        },
        "resultTemplateHash": "string"
      },
      "vulnerabilityInfo": {
        "vulnerabilityInfoResult": {
          "code": 0,
          "hash": "string",
          "method": 0,
          "timeStamp": "string",
          "timing": 0,
          "detectedProduct": {
            "hasVulnerability": true,
            "isCurrent": true,
            "product": {
              "id": 0,
              "name": "string"
            },
            "remediationLink": "string",
            "severity": "string",
            "sigName": "string",
            "signature": 0,
            "vendor": {
              "id": 0,
              "name": "string"
            },
            "version": "string",
            "versionData": {
              "countBehind": 0,
              "feedId": 0,
              "version": "string"
            },
            "vulnerabilities": [
              {
                "description": "string",
                "details": {
                  "cpe": "string",
                  "cve": "string",
                  "cvss": {
                    "accessComplexity": "string",
                    "accessVector": "string",
                    "authentication": "string",
                    "availabilityImpact": "string",
                    "confidentialityImpact": "string",
                    "generatedOnEpoch": "string",
                    "integrityImpact": "string",
                    "score": "string",
                    "source": "string"
                  },
```

```
"attackComplexity": "string",
                    "attackVector": "string",
                    "availabilityImpact": "string",
                    "baseScore": "string",
                    "baseSeverity": "string",
                    "confidentialityImpact": "string",
                    "exploitabilityScore": "string",
                    "impactScore": "string",
                    "integrityImpact": "string",
                    "privilegesRequired": "string",
                    "scope": "string",
                    "userInteraction": "string",
                    "vectorString": "string"
                  },
                  "cwe": "string",
                  "lastModifiedEpoch": "string",
                  "publishedEpoch": "string",
                  "references": [
                    "string"
                  ]
                },
                "severity": "string",
                "severityIndex": 0,
                "staticId": 0
              }
            ]
          }
        }
      },
      "sessionCookie": "string",
      "fileTypeInfo": {
        "fileInfoExtended": {
          "extensions": "string",
          "groupId": "string",
          "typeId": "string"
        }
      },
      "scanInstanceUrl": "string",
      "scanWorkflowSnapshotId": "string",
      "coreEngines": [
        {
          "engineId": "string",
          "engineName": "string",
          "engineVersion": "string",
          "dbVersion": "string",
          "definitionTime": "string"
        }
      ]
    },
    "processingState": 0,
    "exception": {
      "exceptionDetails": "string",
      "exceptionMessage": "string"
```

```
"created": "2019-08-24T14:15:22Z",
    "lastModified": "2019-08-24T14:15:22Z",
    "discoveryStarted": "2019-08-24T14:15:22Z",
    "fileProcessingDetails": {
      "streamingStartedTime": "2019-08-24T14:15:22Z",
      "streamingCompletedTime": "2019-08-24T14:15:22Z",
      "streamingTimeSpanMs": 0,
      "scanCompletedTime": "2019-08-24T14:15:22Z",
      "processingTimeSpanMs": 0
    },
    "coreEngines": [
      {
        "engineId": "string",
        "engineName": "string",
        "engineVersion": "string",
        "dbVersion": "string",
        "definitionTime": "string"
      }
    ],
    "remediation": {
      "deepCdr": {
        "sanitizationDetails": {
          "failureCategory": "string",
          "description": "string",
          "details": "string"
        },
        "cdrObjectState": 0,
        "fileWasReplaced": true
      },
      "postActionFailedInformation": [
        {
          "objectActionType": 0,
          "exception": {
            "exceptionDetails": "string",
            "exceptionMessage": "string"
          }
        }
      ],
      "objectRemediationActions": [
        {
          "objectActionType": 0,
          "objectActionState": 0,
          "cdrObjectState": 0,
          "exceptions": [
            "string"
          ],
          "id": "string",
          "fileId": "string",
          "fileScanCompletedTime": "2019-08-24T14:15:22Z",
          "remediationId": "string",
          "tenantId": "string",
          "lastUpdated": "2019-08-24T14:15:22Z"
        }
```

```
},
    "metaDefenderCoreUrl": "string",
    "discoveryStartedDaySec": 0,
    "objectStorageMetadata": "string",
    "scanWorkflowSnapshotId": "string",
    "scanWorkflowSnapshot": {
      "id": "string",
      "scanId": "string",
      "workflow": {
        "id": "string",
        "scanPoolId": "string",
        "scanProcessFlow": 0,
        "isIdentityScanningEnabled": true,
        "scanIntervalDays": 0,
        "rules": [
          "string"
        ],
        "type": 0,
        "workflowSupportedTechnologies": {
          "dlp": {
            "status": 0
          },
          "deepCdr": {
            "status": 0
          },
          "sandBox": {
            "status": 0
          },
          "metascan": {
            "status": 0
          }
        },
        "name": "string",
        "userAgent": "string",
        "scanPool": {
          "id": "string",
          "name": "string",
          "scanPoolType": 0,
          "isDefault": true,
          "scanInstances": [
            {
              "id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ]
        },
        "failOverScanPoolId": "string",
        "failOverScanPool": {
          "id": "string",
```

```
"scanPoolType": 0,
          "isDefault": true,
          "scanInstances": [
            {
              "id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ]
        },
        "filters": {
          "id": "string",
          "minimumSize": 0,
          "maximumSize": 0,
          "minimumDateTime": "2019-08-24T14:15:22Z",
          "maximumDateTime": "2019-08-24T14:15:22Z"
        },
        "fileDefinition": {
          "blockingStrategy": 0,
          "configurableBlockingStrategy": {
            "shouldTreatFilesWithSensitiveDataAsBlocked": true,
            "shouldTreatFilesWithVulnerabilitiesAsBlocked": true
          }
        },
        "remediations": [
          {
            "id": "string",
            "workflowId": "string",
            "isEnabled": true,
            "configuration": "string",
            "type": 0,
            "handlingType": 0
          }
        ],
        "tenantId": "string"
      },
      "startTimestamp": 0,
      "stopTimestamp": 0,
      "scanPool": {
        "id": "string",
        "name": "string",
        "scanPoolType": 0,
        "isDefault": true,
        "scanInstances": [
          {
            "id": "string",
            "scanPoolId": "string",
            "url": "string",
            "apiKey": "string",
            "timeout": "string",
```

```
}
        ]
      },
      "scanInstances": [
        {
          "id": "string",
          "scanPoolId": "string",
          "url": "string",
          "apiKey": "string",
          "timeout": "string",
          "scanInstanceType": 0
        }
      ],
      "failOverScanPool": {
        "id": "string",
        "name": "string",
        "scanPoolType": 0,
        "isDefault": true,
        "scanInstances": [
          {
            "id": "string",
            "scanPoolId": "string",
            "url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ]
      },
      "failOverScanInstances": [
        {
          "id": "string",
          "scanPoolId": "string",
          "url": "string",
          "apiKey": "string",
          "timeout": "string",
          "scanInstanceType": 0
        }
      ],
      "storage": {
        "id": "string",
        "name": "string",
        "groupId": "string",
        "clientId": "string",
        "accountId": "string",
        "source": "string",
        "storageFunctionality": "string",
        "storageType": {
          "name": "string",
          "categoryType": 0,
          "protocolType": 0,
          "vendorType": 0
        },
```

```
"message": "string",
          "statusType": 0
        },
        "workflowId": "string",
        "lastUpdated": "2019-08-24T14:15:22Z",
        "tenantId": "string",
        "groupRef": {
          "id": "string",
          "name": "string"
        },
        "isAutodiscovered": true
      },
      "workflowStatistics": {
        "taggingStatistics": {
          "total": 0
        },
        "keepAllowedStatistics": {
          "total": 0
        },
        "keepBlockedStatistics": {
          "total": 0
        },
        "keepSanitizedStatistics": {
          "total": 0
        },
        "movedAllowedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
```

```
},
        "movedSanitizedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "movedBlockedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
```

```
"groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "copyAllowedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "copyBlockedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
```

```
"message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "deleteAllowedStatistics": {
          "total": 0
        },
        "deleteBlockedStatistics": {
          "total": 0
        },
        "lastCalculatedStatisticsTime": "2019-08-24T14:15:22Z"
      },
      "account": {
        "id": "string",
        "name": "string",
        "description": "string",
        "credentials": "string",
        "protocolType": 0,
        "vendorType": 0,
        "autoDiscovery": true,
        "autodiscoveryDestinationGroupId": "string",
        "destinationGroup": {
          "id": "string",
          "name": "string"
        }
      },
      "realTimeStartDate": "2019-08-24T14:15:22Z"
    },
    "versions": [
      {
        "result": 0,
        "responseKey": "string",
        "responseMessage": "string",
        "responseMessageParams": {
          "property1": "string",
          "property2": "string"
        },
        "id": "string",
        "scanId": "string",
        "name": "string",
        "path": "string",
        "hash": "string",
        "fileOwner": {
          "userId": "string",
```

```
"userName": "string",
          "emailAddress": "string"
        },
        "size": 0,
        "fileTypeCategory": 0,
        "extension": "string",
        "storageType": {
          "name": "string",
          "categoryType": 0,
          "protocolType": 0,
          "vendorType": 0
        },
        "storageName": "string",
        "storageLocation": "string",
        "scanName": "string",
        "progress": {
          "upload": 0,
          "scan": 0,
          "archiveExtraction": 0
        },
        "scanResult": {
          "extractedFiles": {
            "dataId": "string",
            "scanResultI": 0,
            "detectedBy": 0,
            "filesExtractedCount": 0
          },
          "scanResults": {
            "scanDetails": [
              {
                "engineName": "string",
                "threatFound": "string",
                "scanResultI": 0,
                "defTime": "string",
                "scanTime": 0.1,
                "engId": "string",
                "waitTime": 0.1
              }
            ],
            "dataId": "string",
            "scanAllResultI": 0,
            "scanAllResultA": "string",
            "startTime": "string",
            "totalTime": 0.1,
            "totalAvs": 0,
            "totalDetections": 0,
            "progressPercentage": 0
          },
          "fileInfo": {
            "fileSize": 0,
            "uploadTimestamp": "string",
            "md5": "string",
            "sha1": "string",
```

```
"fileTypeCategory": "string",
            "fileTypeDescription": "string",
            "fileTypeExtension": "string",
            "displayName": "string",
            "fileTypeId": "string"
          },
          "fileScanInfo": {
            "finalVerdict": {
              "blocked": true,
              "verdict": "string",
              "confidence": 0.1,
              "threatLevel": 0.1
            },
            "overviewReport": {
              "analysisState": "string",
              "signalGroups": [
                {
                  "description": "string",
                  "verdict": "string",
                  "signals": [
                    {
                      "originType": "string",
                      "signalReadable": "string",
                      "strength": 0.1
                    }
                  ],
                  "mitreTechniques": [
                    {
                      "name": "string",
                      "tacticName": "string"
                    }
                  ]
                }
              ],
              "iocs": [
                {
                  "data": "string",
                  "type": "string",
                  "origin": "string",
                  "verdict": "string"
                }
              ],
              "yaraMatches": [
                {
                  "ruleName": "string",
                  "ruleDescription": "string",
                  "verdict": "string",
                  "matchedStrings": [
                    "string"
                  ],
                  "author": "string",
                  "version": "string",
                  "threatLevel": 0.1,
```

```
"strength": 0.1
                }
              ],
              "tags": [
                {
                  "name": "string",
                  "verdict": "string"
                }
              ],
              "metaData": {
                "entropy": 0.1,
                "forensicAnalysisRecommended": true,
                "fuzzyFsioHash": "string"
              }
            },
            "errorCategory": "string",
            "errorCode": 0,
            "errorDetails": "string"
          },
          "processInfo": {
            "postProcessing": {
              "actionsRan": "string",
              "actionsFailed": "string",
              "convertedTo": "string",
              "copyMoveDestination": "string",
              "convertedDestination": "string",
              "sanitizationDetails": {
                "failureCategory": "string",
                "description": "string",
                "details": "string"
              }
            },
            "progressPercentage": 0,
            "userAgent": "string",
            "profile": "string",
            "result": "string",
            "blockedReason": "string",
            "fileTypeSkippedScan": true,
            "processingTime": 0.1,
            "queueTime": 0.1,
            "resultI": 0
          },
          "dataId": "string",
          "dlpInfo": {
            "hits": null,
            "verdict": 0
          },
          "sbomInfo": {
            "finalVerdict": {
              "blocked": true,
              "licensingPackageCounts": {
                "allowed": 0,
                "blocked": 0,
```

```
"unsupported": 0
              },
              "severity": 0,
              "totalPackageCount": 0,
              "verdict": "string",
              "vulnerabilityCounts": {
                "critical": 0,
                "high": 0,
                "medium": 0,
                "low": 0,
                "unknown": 0
              }
            },
            "overviewReport": {
              "isPartialReport": true,
              "osInfo": {
                "osName": "string",
                "osVersion": "string"
              },
              "scanMode": "string",
              "steps": [
                {
                  "command": "string",
                  "packages": [
                    {
                      "authors": "string",
                      "releaseDate": "2019-08-24T14:15:22Z",
                      "ecosystem": "string",
                      "group": "string",
                      "archive": true,
                      "executable": true,
                      "uid": "string",
                      "licenses": {
                        "allowed": [
                          {
                            "id": "string",
                            "url": "string",
                            "category": "string",
                            "usageRestriction": {
                              "permissions": [],
                              "conditions": [],
                              "limitations": []
                            }
                          }
                        ],
                        "blocked": [
                          {
                            "id": "string",
                            "url": "string",
                            "category": "string",
                            "usageRestriction": {
                              "permissions": [],
                              "conditions": [],
```

```
}
                        }
                    ]
                },
                "packageName": "string",
                "packageVersion": "string",
                "hashes": [
                    {
                        "sha256": "string",
                        "fileName": "string"
                    }
                ],
                "vulnerabilityCounts": {
                    "critical": 0,
                    "high": 0,
                    "medium": 0,
                    "low": 0,
                    "unknown": 0
                },
                "vulnerabilities": [
                    {
                        "id": "string",
                        "severity": 0,
                        "source": "string",
                        "fixedVersions": "string",
                        "cwes": [
                            "string"
                        ]
                    }
                ],
                "arch": "string",
                "osName": "string",
                "osVersion": "string",
                "dependencies": [
                    {
                        "ecosystem": "string",
                        "group": "string",
                        "packageName": "string",
                        "packageVersion": "string",
                        "vulnerabilities": [
                            {
                                "cwes": []
                            }
                        ],
                        "vulnerabilityCounts": {
                            "critical": 0,
                            "high": 0,
                            "medium": 0,
                            "low": 0,
                            "unknown": 0
                        }
                    }
                ]
```

```
],
                    "licenseStatus": "string",
                    "licensingPackageCounts": {
                      "allowed": 0,
                      "blocked": 0,
                      "unknown": 0,
                      "unsupported": 0
                    },
                    "step": 0,
                    "vulnerabilityCount": 0,
                    "sha256": "string",
                    "severity": 0,
                    "vulnerabilityCounts": {
                      "critical": 0,
                      "high": 0,
                      "medium": 0,
                      "low": 0,
                      "unknown": 0
                    }
                  }
                ],
                "packages": [
                  {
                    "authors": "string",
                    "releaseDate": "2019-08-24T14:15:22Z",
                    "ecosystem": "string",
                    "group": "string",
                    "archive": true,
                    "executable": true,
                    "uid": "string",
                    "licenses": {
                      "allowed": [
                        {
                          "id": "string",
                          "url": "string",
                          "category": "string",
                          "usageRestriction": {
                            "permissions": [
                              "string"
                            ],
                            "conditions": [
                              "string"
                            ],
                            "limitations": [
                              "string"
                            ]
                          }
                        }
                      ],
                      "blocked": [
                        {
                          "id": "string",
                          "url": "string",
```

```
"usageRestriction": {
                          "permissions": [
                            "string"
                          ],
                          "conditions": [
                            "string"
                          ],
                          "limitations": [
                            "string"
                          ]
                        }
                      }
                    ]
                  },
                  "packageName": "string",
                  "packageVersion": "string",
                  "target": "string",
                  "hashes": [
                    {
                      "sha256": "string",
                      "fileName": "string"
                    }
                  ],
                  "vulnerabilities": [
                    {
                      "id": "string",
                      "severity": 0,
                      "source": "string",
                      "fixedVersions": "string",
                      "cwes": [
                        "string"
                      ]
                    }
                  ],
                  "vulnerabilityCounts": {
                    "critical": 0,
                    "high": 0,
                    "medium": 0,
                    "low": 0,
                    "unknown": 0
                  },
                  "dependencies": [
                    {
                      "ecosystem": "string",
                      "group": "string",
                      "packageName": "string",
                      "packageVersion": "string",
                      "vulnerabilities": [
                        {
                          "id": "string",
                          "severity": 0,
                          "source": "string",
                          "fixedVersions": "string",
```

```
"string"
                          ]
                        }
                      ],
                      "vulnerabilityCounts": {
                        "critical": 0,
                        "high": 0,
                        "medium": 0,
                        "low": 0,
                        "unknown": 0
                      }
                    }
                  ]
                }
              ],
              "dependenciesPackageCount": 0,
              "dependenciesVulnerabilityTotal": 0,
              "dependenciesVulnerabilityCounts": {
                "critical": 0,
                "high": 0,
                "medium": 0,
                "low": 0,
                "unknown": 0
              }
            },
            "resultTemplateHash": "string"
          },
          "vulnerabilityInfo": {
            "vulnerabilityInfoResult": {
              "code": 0,
              "hash": "string",
              "method": 0,
              "timeStamp": "string",
              "timing": 0,
              "detectedProduct": {
                "hasVulnerability": true,
                "isCurrent": true,
                "product": {
                  "id": 0,
                  "name": "string"
                },
                "remediationLink": "string",
                "severity": "string",
                "sigName": "string",
                "signature": 0,
                "vendor": {
                  "id": 0,
                  "name": "string"
                },
                "version": "string",
                "versionData": {
                  "countBehind": 0,
                  "feedId": 0,
```

```
},
                "vulnerabilities": [
                  {
                    "description": "string",
                    "details": {
                      "cpe": "string",
                      "cve": "string",
                      "cvss": {
                        "accessComplexity": "string",
                        "accessVector": "string",
                        "authentication": "string",
                        "availabilityImpact": "string",
                        "confidentialityImpact": "string",
                        "generatedOnEpoch": "string",
                        "integrityImpact": "string",
                        "score": "string",
                        "source": "string"
                      },
                      "cvss3": {
                        "attackComplexity": "string",
                        "attackVector": "string",
                        "availabilityImpact": "string",
                        "baseScore": "string",
                        "baseSeverity": "string",
                        "confidentialityImpact": "string",
                        "exploitabilityScore": "string",
                        "impactScore": "string",
                        "integrityImpact": "string",
                        "privilegesRequired": "string",
                        "scope": "string",
                        "userInteraction": "string",
                        "vectorString": "string"
                      },
                      "cwe": "string",
                      "lastModifiedEpoch": "string",
                      "publishedEpoch": "string",
                      "references": [
                        "string"
                      ]
                    },
                    "severity": "string",
                    "severityIndex": 0,
                    "staticId": 0
                  }
                ]
              }
            }
          },
          "sessionCookie": "string",
          "fileTypeInfo": {
            "fileInfoExtended": {
              "extensions": "string",
              "groupId": "string",
```

```
}
          },
          "scanInstanceUrl": "string",
          "scanWorkflowSnapshotId": "string",
          "coreEngines": [
            {
              "engineId": "string",
              "engineName": "string",
              "engineVersion": "string",
              "dbVersion": "string",
              "definitionTime": "string"
            }
          ]
        },
        "processingState": 0,
        "exception": {
          "exceptionDetails": "string",
          "exceptionMessage": "string"
        },
        "created": "2019-08-24T14:15:22Z",
        "lastModified": "2019-08-24T14:15:22Z",
        "discoveryStarted": "2019-08-24T14:15:22Z",
        "fileProcessingDetails": {
          "streamingStartedTime": "2019-08-24T14:15:22Z",
          "streamingCompletedTime": "2019-08-24T14:15:22Z",
          "streamingTimeSpanMs": 0,
          "scanCompletedTime": "2019-08-24T14:15:22Z",
          "processingTimeSpanMs": 0
        },
        "coreEngines": [
          {
            "engineId": "string",
            "engineName": "string",
            "engineVersion": "string",
            "dbVersion": "string",
            "definitionTime": "string"
          }
        ],
        "remediation": {
          "deepCdr": {
            "sanitizationDetails": {
              "failureCategory": "string",
              "description": "string",
              "details": "string"
            },
            "cdrObjectState": 0,
            "fileWasReplaced": true
          },
          "postActionFailedInformation": [
            {
              "objectActionType": 0,
              "exception": {
                "exceptionDetails": "string",
```

```
}
            }
          ],
          "objectRemediationActions": [
            {
              "objectActionType": 0,
              "objectActionState": 0,
              "cdrObjectState": 0,
              "exceptions": [
                "string"
              ],
              "id": "string",
              "fileId": "string",
              "fileScanCompletedTime": "2019-08-24T14:15:22Z",
              "remediationId": "string",
              "tenantId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z"
            }
          ]
        },
        "metaDefenderCoreUrl": "string",
        "discoveryStartedDaySec": 0,
        "objectStorageMetadata": "string",
        "scanWorkflowSnapshotId": "string",
        "scanWorkflowSnapshot": {
          "id": "string",
          "scanId": "string",
          "workflow": {
            "id": "string",
            "scanPoolId": "string",
            "scanProcessFlow": 0,
            "isIdentityScanningEnabled": true,
            "scanIntervalDays": 0,
            "rules": [
              "string"
            ],
            "type": 0,
            "workflowSupportedTechnologies": {
              "dlp": {
                "status": 0
              },
              "deepCdr": {
                "status": 0
              },
              "sandBox": {
                "status": 0
              },
              "metascan": {
                "status": 0
              }
            },
            "name": "string",
            "userAgent": "string",
```

```
"id": "string",
              "name": "string",
              "scanPoolType": 0,
              "isDefault": true,
              "scanInstances": [
                {
                  "id": "string",
                  "scanPoolId": "string",
                  "url": "string",
                  "apiKey": "string",
                  "timeout": "string",
                  "scanInstanceType": 0
                }
              ]
            },
            "failOverScanPoolId": "string",
            "failOverScanPool": {
              "id": "string",
              "name": "string",
              "scanPoolType": 0,
              "isDefault": true,
              "scanInstances": [
                {
                  "id": "string",
                  "scanPoolId": "string",
                  "url": "string",
                  "apiKey": "string",
                  "timeout": "string",
                  "scanInstanceType": 0
                }
              ]
            },
            "filters": {
              "id": "string",
              "minimumSize": 0,
              "maximumSize": 0,
              "minimumDateTime": "2019-08-24T14:15:22Z",
              "maximumDateTime": "2019-08-24T14:15:22Z"
            },
            "fileDefinition": {
              "blockingStrategy": 0,
              "configurableBlockingStrategy": {
                "shouldTreatFilesWithSensitiveDataAsBlocked": true,
                "shouldTreatFilesWithVulnerabilitiesAsBlocked": true
              }
            },
            "remediations": [
              {
                "id": "string",
                "workflowId": "string",
                "isEnabled": true,
                "configuration": "string",
                "type": 0,
```

```
}
            ],
            "tenantId": "string"
          },
          "startTimestamp": 0,
          "stopTimestamp": 0,
          "scanPool": {
            "id": "string",
            "name": "string",
            "scanPoolType": 0,
            "isDefault": true,
            "scanInstances": [
              {
                "id": "string",
                "scanPoolId": "string",
                "url": "string",
                "apiKey": "string",
                "timeout": "string",
                "scanInstanceType": 0
              }
            ]
          },
          "scanInstances": [
            {
              "id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ],
          "failOverScanPool": {
            "id": "string",
            "name": "string",
            "scanPoolType": 0,
            "isDefault": true,
            "scanInstances": [
              {
                "id": "string",
                "scanPoolId": "string",
                "url": "string",
                "apiKey": "string",
                "timeout": "string",
                "scanInstanceType": 0
              }
            ]
          },
          "failOverScanInstances": [
            {
              "id": "string",
              "scanPoolId": "string",
              "url": "string",
```

```
"timeout": "string",
              "scanInstanceType": 0
            }
          ],
          "storage": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          },
          "workflowStatistics": {
            "taggingStatistics": {
              "total": 0
            },
            "keepAllowedStatistics": {
              "total": 0
            },
            "keepBlockedStatistics": {
              "total": 0
            },
            "keepSanitizedStatistics": {
              "total": 0
            },
            "movedAllowedStatistics": {
              "total": 0,
              "destinationStorageInformation": {
                "id": "string",
                "name": "string",
                "groupId": "string",
                "clientId": "string",
                "accountId": "string",
                "source": "string",
```

```
"storageType": {
                    "name": "string",
                    "categoryType": 0,
                    "protocolType": 0,
                    "vendorType": 0
                  },
                  "storageStatus": {
                    "message": "string",
                    "statusType": 0
                  },
                  "workflowId": "string",
                  "lastUpdated": "2019-08-24T14:15:22Z",
                  "tenantId": "string",
                  "groupRef": {
                    "id": "string",
                    "name": "string"
                  },
                  "isAutodiscovered": true
                }
              },
              "movedSanitizedStatistics": {
                "total": 0,
                "destinationStorageInformation": {
                  "id": "string",
                  "name": "string",
                  "groupId": "string",
                  "clientId": "string",
                  "accountId": "string",
                  "source": "string",
                  "storageFunctionality": "string",
                  "storageType": {
                    "name": "string",
                    "categoryType": 0,
                    "protocolType": 0,
                    "vendorType": 0
                  },
                  "storageStatus": {
                    "message": "string",
                    "statusType": 0
                  },
                  "workflowId": "string",
                  "lastUpdated": "2019-08-24T14:15:22Z",
                  "tenantId": "string",
                  "groupRef": {
                    "id": "string",
                    "name": "string"
                  },
                  "isAutodiscovered": true
                }
              },
              "movedBlockedStatistics": {
                "total": 0,
                "destinationStorageInformation": {
```

```
"name": "string",
                "groupId": "string",
                "clientId": "string",
                "accountId": "string",
                "source": "string",
                "storageFunctionality": "string",
                "storageType": {
                  "name": "string",
                  "categoryType": 0,
                  "protocolType": 0,
                  "vendorType": 0
                },
                "storageStatus": {
                  "message": "string",
                  "statusType": 0
                },
                "workflowId": "string",
                "lastUpdated": "2019-08-24T14:15:22Z",
                "tenantId": "string",
                "groupRef": {
                  "id": "string",
                  "name": "string"
                },
                "isAutodiscovered": true
              }
            },
            "copyAllowedStatistics": {
              "total": 0,
              "destinationStorageInformation": {
                "id": "string",
                "name": "string",
                "groupId": "string",
                "clientId": "string",
                "accountId": "string",
                "source": "string",
                "storageFunctionality": "string",
                "storageType": {
                  "name": "string",
                  "categoryType": 0,
                  "protocolType": 0,
                  "vendorType": 0
                },
                "storageStatus": {
                  "message": "string",
                  "statusType": 0
                },
                "workflowId": "string",
                "lastUpdated": "2019-08-24T14:15:22Z",
                "tenantId": "string",
                "groupRef": {
                  "id": "string",
                  "name": "string"
                },
```

```
}
            },
            "copyBlockedStatistics": {
              "total": 0,
              "destinationStorageInformation": {
                "id": "string",
                "name": "string",
                "groupId": "string",
                "clientId": "string",
                "accountId": "string",
                "source": "string",
                "storageFunctionality": "string",
                "storageType": {
                  "name": "string",
                  "categoryType": 0,
                  "protocolType": 0,
                  "vendorType": 0
                },
                "storageStatus": {
                  "message": "string",
                  "statusType": 0
                },
                "workflowId": "string",
                "lastUpdated": "2019-08-24T14:15:22Z",
                "tenantId": "string",
                "groupRef": {
                  "id": "string",
                  "name": "string"
                },
                "isAutodiscovered": true
              }
            },
            "deleteAllowedStatistics": {
              "total": 0
            },
            "deleteBlockedStatistics": {
              "total": 0
            },
            "lastCalculatedStatisticsTime": "2019-08-24T14:15:22Z"
          },
          "account": {
            "id": "string",
            "name": "string",
            "description": "string",
            "credentials": "string",
            "protocolType": 0,
            "vendorType": 0,
            "autoDiscovery": true,
            "autodiscoveryDestinationGroupId": "string",
            "destinationGroup": {
              "id": "string",
              "name": "string"
            }
```

```
"realTimeStartDate": "2019-08-24T14:15:22Z"
        },
        "versions": [],
        "hasBlockedVersions": true,
        "versionsCount": 0,
        "objectType": 0,
        "skippedScan": true,
        "$type": "string",
        "url": "string",
        "fileId": "string"
      }
    ],
    "hasBlockedVersions": true,
    "versionsCount": 0,
    "objectType": 0,
    "skippedScan": true,
    "$type": "string"
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	GetFileResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Retrieve archive scan results

`GET /api/file/archive`

Retrieve the archive scan results using either the scanResultId or the parentId

Parameters

Name	In	Type	Required	Description
scanResultId	query	string	false	none
parentId	query	string	false	none
start	query	integer(int32)	false	none
count	query	integer(int32)	false	none

> Example responses

200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "archiveScanResults": [
    {
      "extractedFiles": {
        "dataId": "string",
        "scanResultI": 0,
        "detectedBy": 0,
        "filesExtractedCount": 0
      },
      "scanResults": {
        "scanDetails": [
          {
            "engineName": "string",
            "threatFound": "string",
            "scanResultI": 0,
            "defTime": "string",
            "scanTime": 0.1,
            "engId": "string",
            "waitTime": 0.1
          }
        ],
        "dataId": "string",
        "scanAllResultI": 0,
        "scanAllResultA": "string",
        "startTime": "string",
        "totalTime": 0.1,
        "totalAvs": 0,
        "totalDetections": 0,
        "progressPercentage": 0
      },
      "fileInfo": {
        "fileSize": 0,
        "uploadTimestamp": "string",
        "md5": "string",
        "sha1": "string",
        "sha256": "string",
        "fileTypeCategory": "string",
        "fileTypeDescription": "string",
        "fileTypeExtension": "string",
        "displayName": "string",
        "fileTypeId": "string"
      },
      "fileScanInfo": {
        "finalVerdict": {
          "blocked": true,
```

```
"confidence": 0.1,
          "threatLevel": 0.1
        },
        "overviewReport": {
          "analysisState": "string",
          "signalGroups": [
            {
              "description": "string",
              "verdict": "string",
              "signals": [
                {
                  "originType": "string",
                  "signalReadable": "string",
                  "strength": 0.1
                }
              ],
              "mitreTechniques": [
                {
                  "name": "string",
                  "tacticName": "string"
                }
              ]
            }
          ],
          "iocs": [
            {
              "data": "string",
              "type": "string",
              "origin": "string",
              "verdict": "string"
            }
          ],
          "yaraMatches": [
            {
              "ruleName": "string",
              "ruleDescription": "string",
              "verdict": "string",
              "matchedStrings": [
                "string"
              ],
              "author": "string",
              "version": "string",
              "threatLevel": 0.1,
              "confidence": 0.1,
              "strength": 0.1
            }
          ],
          "tags": [
            {
              "name": "string",
              "verdict": "string"
            }
          ],
```

```
"entropy": 0.1,
            "forensicAnalysisRecommended": true,
            "fuzzyFsioHash": "string"
          }
        },
        "errorCategory": "string",
        "errorCode": 0,
        "errorDetails": "string"
      },
      "processInfo": {
        "postProcessing": {
          "actionsRan": "string",
          "actionsFailed": "string",
          "convertedTo": "string",
          "copyMoveDestination": "string",
          "convertedDestination": "string",
          "sanitizationDetails": {
            "failureCategory": "string",
            "description": "string",
            "details": "string"
          }
        },
        "progressPercentage": 0,
        "userAgent": "string",
        "profile": "string",
        "result": "string",
        "blockedReason": "string",
        "fileTypeSkippedScan": true,
        "processingTime": 0.1,
        "queueTime": 0.1,
        "resultI": 0
      },
      "dataId": "string",
      "dlpInfo": {
        "hits": null,
        "verdict": 0
      },
      "sbomInfo": {
        "finalVerdict": {
          "blocked": true,
          "licensingPackageCounts": {
            "allowed": 0,
            "blocked": 0,
            "unknown": 0,
            "unsupported": 0
          },
          "severity": 0,
          "totalPackageCount": 0,
          "verdict": "string",
          "vulnerabilityCounts": {
            "critical": 0,
            "high": 0,
            "medium": 0,
```

```
"unknown": 0
          }
        },
        "overviewReport": {
          "isPartialReport": true,
          "osInfo": {
            "osName": "string",
            "osVersion": "string"
          },
          "scanMode": "string",
          "steps": [
            {
              "command": "string",
              "packages": [
                {
                  "authors": "string",
                  "releaseDate": "2019-08-24T14:15:22Z",
                  "ecosystem": "string",
                  "group": "string",
                  "archive": true,
                  "executable": true,
                  "uid": "string",
                  "licenses": {
                    "allowed": [
                      {
                        "id": "string",
                        "url": "string",
                        "category": "string",
                        "usageRestriction": {
                          "permissions": [
                            "string"
                          ],
                          "conditions": [
                            "string"
                          ],
                          "limitations": [
                            "string"
                          ]
                        }
                      }
                    ],
                    "blocked": [
                      {
                        "id": "string",
                        "url": "string",
                        "category": "string",
                        "usageRestriction": {
                          "permissions": [
                            "string"
                          ],
                          "conditions": [
                            "string"
                          ],
```

```
"string"
                            ]
                          }
                        }
                      ]
                    },
                    "packageName": "string",
                    "packageVersion": "string",
                    "hashes": [
                      {
                        "sha256": "string",
                        "fileName": "string"
                      }
                    ],
                    "vulnerabilityCounts": {
                      "critical": 0,
                      "high": 0,
                      "medium": 0,
                      "low": 0,
                      "unknown": 0
                    },
                    "vulnerabilities": [
                      {
                        "id": "string",
                        "severity": 0,
                        "source": "string",
                        "fixedVersions": "string",
                        "cwes": [
                          "string"
                        ]
                      }
                    ],
                    "arch": "string",
                    "osName": "string",
                    "osVersion": "string",
                    "dependencies": [
                      {
                        "ecosystem": "string",
                        "group": "string",
                        "packageName": "string",
                        "packageVersion": "string",
                        "vulnerabilities": [
                          {
                            "id": "string",
                            "severity": 0,
                            "source": "string",
                            "fixedVersions": "string",
                            "cwes": [
                              "string"
                            ]
                          }
                        ],
                        "vulnerabilityCounts": {
```

```
"high": 0,
                        "medium": 0,
                        "low": 0,
                        "unknown": 0
                      }
                    }
                  ]
                }
              ],
              "licenseStatus": "string",
              "licensingPackageCounts": {
                "allowed": 0,
                "blocked": 0,
                "unknown": 0,
                "unsupported": 0
              },
              "step": 0,
              "vulnerabilityCount": 0,
              "sha256": "string",
              "severity": 0,
              "vulnerabilityCounts": {
                "critical": 0,
                "high": 0,
                "medium": 0,
                "low": 0,
                "unknown": 0
              }
            }
          ],
          "packages": [
            {
              "authors": "string",
              "releaseDate": "2019-08-24T14:15:22Z",
              "ecosystem": "string",
              "group": "string",
              "archive": true,
              "executable": true,
              "uid": "string",
              "licenses": {
                "allowed": [
                  {
                    "id": "string",
                    "url": "string",
                    "category": "string",
                    "usageRestriction": {
                      "permissions": [
                        "string"
                      ],
                      "conditions": [
                        "string"
                      ],
                      "limitations": [
                        "string"
```

```
}
                    }
                  ],
                  "blocked": [
                    {
                      "id": "string",
                      "url": "string",
                      "category": "string",
                      "usageRestriction": {
                        "permissions": [
                          "string"
                        ],
                        "conditions": [
                          "string"
                        ],
                        "limitations": [
                          "string"
                        ]
                      }
                    }
                  ]
                },
                "packageName": "string",
                "packageVersion": "string",
                "target": "string",
                "hashes": [
                  {
                    "sha256": "string",
                    "fileName": "string"
                  }
                ],
                "vulnerabilities": [
                  {
                    "id": "string",
                    "severity": 0,
                    "source": "string",
                    "fixedVersions": "string",
                    "cwes": [
                      "string"
                    ]
                  }
                ],
                "vulnerabilityCounts": {
                  "critical": 0,
                  "high": 0,
                  "medium": 0,
                  "low": 0,
                  "unknown": 0
                },
                "dependencies": [
                  {
                    "ecosystem": "string",
                    "group": "string",
```

```
"packageVersion": "string",
                  "vulnerabilities": [
                    {
                      "id": "string",
                      "severity": 0,
                      "source": "string",
                      "fixedVersions": "string",
                      "cwes": [
                        "string"
                      ]
                    }
                  ],
                  "vulnerabilityCounts": {
                    "critical": 0,
                    "high": 0,
                    "medium": 0,
                    "low": 0,
                    "unknown": 0
                  }
                }
              ]
            }
          ],
          "dependenciesPackageCount": 0,
          "dependenciesVulnerabilityTotal": 0,
          "dependenciesVulnerabilityCounts": {
            "critical": 0,
            "high": 0,
            "medium": 0,
            "low": 0,
            "unknown": 0
          }
        },
        "resultTemplateHash": "string"
      },
      "vulnerabilityInfo": {
        "vulnerabilityInfoResult": {
          "code": 0,
          "hash": "string",
          "method": 0,
          "timeStamp": "string",
          "timing": 0,
          "detectedProduct": {
            "hasVulnerability": true,
            "isCurrent": true,
            "product": {
              "id": 0,
              "name": "string"
            },
            "remediationLink": "string",
            "severity": "string",
            "sigName": "string",
            "signature": 0,
```

```
"id": 0,
              "name": "string"
            },
            "version": "string",
            "versionData": {
              "countBehind": 0,
              "feedId": 0,
              "version": "string"
            },
            "vulnerabilities": [
              {
                "description": "string",
                "details": {
                  "cpe": "string",
                  "cve": "string",
                  "cvss": {
                    "accessComplexity": "string",
                    "accessVector": "string",
                    "authentication": "string",
                    "availabilityImpact": "string",
                    "confidentialityImpact": "string",
                    "generatedOnEpoch": "string",
                    "integrityImpact": "string",
                    "score": "string",
                    "source": "string"
                  },
                  "cvss3": {
                    "attackComplexity": "string",
                    "attackVector": "string",
                    "availabilityImpact": "string",
                    "baseScore": "string",
                    "baseSeverity": "string",
                    "confidentialityImpact": "string",
                    "exploitabilityScore": "string",
                    "impactScore": "string",
                    "integrityImpact": "string",
                    "privilegesRequired": "string",
                    "scope": "string",
                    "userInteraction": "string",
                    "vectorString": "string"
                  },
                  "cwe": "string",
                  "lastModifiedEpoch": "string",
                  "publishedEpoch": "string",
                  "references": [
                    "string"
                  ]
                },
                "severity": "string",
                "severityIndex": 0,
                "staticId": 0
              }
            ]
```

```
}
      },
      "sessionCookie": "string",
      "fileTypeInfo": {
        "fileInfoExtended": {
          "extensions": "string",
          "groupId": "string",
          "typeId": "string"
        }
      },
      "scanInstanceUrl": "string",
      "scanWorkflowSnapshotId": "string",
      "coreEngines": [
        {
          "engineId": "string",
          "engineName": "string",
          "engineVersion": "string",
          "dbVersion": "string",
          "definitionTime": "string"
        }
      ]
    }
  ]
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	GetArchiveScanResultResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Cancel a file in an ongoing scan

`POST /api/file/cancel`

> Body parameter


```
{
  "fileIds": [
    "string"
  ]
}
```

Parameters

Name	In	Type	Required	Description
body	body	CancelFileParameters	true	none

Example responses

200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "id": "string",
  "scanId": "string",
  "name": "string",
  "path": "string",
  "hash": "string",
  "fileOwner": {
    "userId": "string",
    "fullName": "string",
    "userName": "string",
    "emailAddress": "string"
  },
  "size": 0,
  "storageType": {
    "name": "string",
    "categoryType": 0,
    "protocolType": 0,
    "vendorType": 0
  },
  "storageName": "string",
  "storageLocation": "string",
  "scanName": "string",
  "progress": {
    "upload": 0,
    "scan": 0,
    "archiveExtraction": 0
  },
  "scanResult": {
    "extractedFiles": {
      "dataId": "string",
      "scanResultI": 0,
      "detectedBy": 0,
      "filesExtractedCount": 0
    },
    "scanResults": {
      "scanDetails": [
        {
          "engineName": "string",
          "threatFound": "string",
          "scanResultI": 0,
          "defTime": "string",
          "scanTime": 0.1,
          "engId": "string",
          "waitTime": 0.1
        }
```

```
"dataId": "string",
      "scanAllResultI": 0,
      "scanAllResultA": "string",
      "startTime": "string",
      "totalTime": 0.1,
      "totalAvs": 0,
      "totalDetections": 0,
      "progressPercentage": 0
    },
    "fileInfo": {
      "fileSize": 0,
      "uploadTimestamp": "string",
      "md5": "string",
      "sha1": "string",
      "sha256": "string",
      "fileTypeCategory": "string",
      "fileTypeDescription": "string",
      "fileTypeExtension": "string",
      "displayName": "string",
      "fileTypeId": "string"
    },
    "fileScanInfo": {
      "finalVerdict": {
        "blocked": true,
        "verdict": "string",
        "confidence": 0.1,
        "threatLevel": 0.1
      },
      "overviewReport": {
        "analysisState": "string",
        "signalGroups": [
          {
            "description": "string",
            "verdict": "string",
            "signals": [
              {
                "originType": "string",
                "signalReadable": "string",
                "strength": 0.1
              }
            ],
            "mitreTechniques": [
              {
                "name": "string",
                "tacticName": "string"
              }
            ]
          }
        ],
        "iocs": [
          {
            "data": "string",
            "type": "string",
```

```
"verdict": "string"
          }
        ],
        "yaraMatches": [
          {
            "ruleName": "string",
            "ruleDescription": "string",
            "verdict": "string",
            "matchedStrings": [
              "string"
            ],
            "author": "string",
            "version": "string",
            "threatLevel": 0.1,
            "confidence": 0.1,
            "strength": 0.1
          }
        ],
        "tags": [
          {
            "name": "string",
            "verdict": "string"
          }
        ],
        "metaData": {
          "entropy": 0.1,
          "forensicAnalysisRecommended": true,
          "fuzzyFsioHash": "string"
        }
      },
      "errorCategory": "string",
      "errorCode": 0,
      "errorDetails": "string"
    },
    "processInfo": {
      "postProcessing": {
        "actionsRan": "string",
        "actionsFailed": "string",
        "convertedTo": "string",
        "copyMoveDestination": "string",
        "convertedDestination": "string",
        "sanitizationDetails": {
          "failureCategory": "string",
          "description": "string",
          "details": "string"
        }
      },
      "progressPercentage": 0,
      "userAgent": "string",
      "profile": "string",
      "result": "string",
      "blockedReason": "string",
      "fileTypeSkippedScan": true,
```

```
"queueTime": 0.1,
      "resultI": 0
    },
    "dataId": "string",
    "dlpInfo": {
      "hits": null,
      "verdict": 0
    },
    "sbomInfo": {
      "finalVerdict": {
        "blocked": true,
        "licensingPackageCounts": {
          "allowed": 0,
          "blocked": 0,
          "unknown": 0,
          "unsupported": 0
        },
        "severity": 0,
        "totalPackageCount": 0,
        "verdict": "string",
        "vulnerabilityCounts": {
          "critical": 0,
          "high": 0,
          "medium": 0,
          "low": 0,
          "unknown": 0
        }
      },
      "overviewReport": {
        "isPartialReport": true,
        "osInfo": {
          "osName": "string",
          "osVersion": "string"
        },
        "scanMode": "string",
        "steps": [
          {
            "command": "string",
            "packages": [
              {
                "authors": "string",
                "releaseDate": "2019-08-24T14:15:22Z",
                "ecosystem": "string",
                "group": "string",
                "archive": true,
                "executable": true,
                "uid": "string",
                "licenses": {
                  "allowed": [
                    {
                      "id": "string",
                      "url": "string",
                      "category": "string",
```

```
"permissions": [
                        "string"
                      ],
                      "conditions": [
                        "string"
                      ],
                      "limitations": [
                        "string"
                      ]
                    }
                  }
                ],
                "blocked": [
                  {
                    "id": "string",
                    "url": "string",
                    "category": "string",
                    "usageRestriction": {
                      "permissions": [
                        "string"
                      ],
                      "conditions": [
                        "string"
                      ],
                      "limitations": [
                        "string"
                      ]
                    }
                  }
                ]
              },
              "packageName": "string",
              "packageVersion": "string",
              "hashes": [
                {
                  "sha256": "string",
                  "fileName": "string"
                }
              ],
              "vulnerabilityCounts": {
                "critical": 0,
                "high": 0,
                "medium": 0,
                "low": 0,
                "unknown": 0
              },
              "vulnerabilities": [
                {
                  "id": "string",
                  "severity": 0,
                  "source": "string",
                  "fixedVersions": "string",
                  "cwes": [
```

```
]
                  }
                ],
                "arch": "string",
                "osName": "string",
                "osVersion": "string",
                "dependencies": [
                  {
                    "ecosystem": "string",
                    "group": "string",
                    "packageName": "string",
                    "packageVersion": "string",
                    "vulnerabilities": [
                      {
                        "id": "string",
                        "severity": 0,
                        "source": "string",
                        "fixedVersions": "string",
                        "cwes": [
                          "string"
                        ]
                      }
                    ],
                    "vulnerabilityCounts": {
                      "critical": 0,
                      "high": 0,
                      "medium": 0,
                      "low": 0,
                      "unknown": 0
                    }
                  }
                ]
              }
            ],
            "licenseStatus": "string",
            "licensingPackageCounts": {
              "allowed": 0,
              "blocked": 0,
              "unknown": 0,
              "unsupported": 0
            },
            "step": 0,
            "vulnerabilityCount": 0,
            "sha256": "string",
            "severity": 0,
            "vulnerabilityCounts": {
              "critical": 0,
              "high": 0,
              "medium": 0,
              "low": 0,
              "unknown": 0
            }
          }
```

```
"packages": [
          {
            "authors": "string",
            "releaseDate": "2019-08-24T14:15:22Z",
            "ecosystem": "string",
            "group": "string",
            "archive": true,
            "executable": true,
            "uid": "string",
            "licenses": {
              "allowed": [
                {
                  "id": "string",
                  "url": "string",
                  "category": "string",
                  "usageRestriction": {
                    "permissions": [
                      "string"
                    ],
                    "conditions": [
                      "string"
                    ],
                    "limitations": [
                      "string"
                    ]
                  }
                }
              ],
              "blocked": [
                {
                  "id": "string",
                  "url": "string",
                  "category": "string",
                  "usageRestriction": {
                    "permissions": [
                      "string"
                    ],
                    "conditions": [
                      "string"
                    ],
                    "limitations": [
                      "string"
                    ]
                  }
                }
              ]
            },
            "packageName": "string",
            "packageVersion": "string",
            "target": "string",
            "hashes": [
              {
                "sha256": "string",
```

```
}
            ],
            "vulnerabilities": [
              {
                "id": "string",
                "severity": 0,
                "source": "string",
                "fixedVersions": "string",
                "cwes": [
                  "string"
                ]
              }
            ],
            "vulnerabilityCounts": {
              "critical": 0,
              "high": 0,
              "medium": 0,
              "low": 0,
              "unknown": 0
            },
            "dependencies": [
              {
                "ecosystem": "string",
                "group": "string",
                "packageName": "string",
                "packageVersion": "string",
                "vulnerabilities": [
                  {
                    "id": "string",
                    "severity": 0,
                    "source": "string",
                    "fixedVersions": "string",
                    "cwes": [
                      "string"
                    ]
                  }
                ],
                "vulnerabilityCounts": {
                  "critical": 0,
                  "high": 0,
                  "medium": 0,
                  "low": 0,
                  "unknown": 0
                }
              }
            ]
          }
        ],
        "dependenciesPackageCount": 0,
        "dependenciesVulnerabilityTotal": 0,
        "dependenciesVulnerabilityCounts": {
          "critical": 0,
          "high": 0,
```

```
"low": 0,
          "unknown": 0
        }
      },
      "resultTemplateHash": "string"
    },
    "vulnerabilityInfo": {
      "vulnerabilityInfoResult": {
        "code": 0,
        "hash": "string",
        "method": 0,
        "timeStamp": "string",
        "timing": 0,
        "detectedProduct": {
          "hasVulnerability": true,
          "isCurrent": true,
          "product": {
            "id": 0,
            "name": "string"
          },
          "remediationLink": "string",
          "severity": "string",
          "sigName": "string",
          "signature": 0,
          "vendor": {
            "id": 0,
            "name": "string"
          },
          "version": "string",
          "versionData": {
            "countBehind": 0,
            "feedId": 0,
            "version": "string"
          },
          "vulnerabilities": [
            {
              "description": "string",
              "details": {
                "cpe": "string",
                "cve": "string",
                "cvss": {
                  "accessComplexity": "string",
                  "accessVector": "string",
                  "authentication": "string",
                  "availabilityImpact": "string",
                  "confidentialityImpact": "string",
                  "generatedOnEpoch": "string",
                  "integrityImpact": "string",
                  "score": "string",
                  "source": "string"
                },
                "cvss3": {
                  "attackComplexity": "string",
```

```
"availabilityImpact": "string",
                  "baseScore": "string",
                  "baseSeverity": "string",
                  "confidentialityImpact": "string",
                  "exploitabilityScore": "string",
                  "impactScore": "string",
                  "integrityImpact": "string",
                  "privilegesRequired": "string",
                  "scope": "string",
                  "userInteraction": "string",
                  "vectorString": "string"
                },
                "cwe": "string",
                "lastModifiedEpoch": "string",
                "publishedEpoch": "string",
                "references": [
                  "string"
                ]
              },
              "severity": "string",
              "severityIndex": 0,
              "staticId": 0
            }
          ]
        }
      }
    },
    "sessionCookie": "string",
    "fileTypeInfo": {
      "fileInfoExtended": {
        "extensions": "string",
        "groupId": "string",
        "typeId": "string"
      }
    },
    "scanInstanceUrl": "string",
    "scanWorkflowSnapshotId": "string",
    "coreEngines": [
      {
        "engineId": "string",
        "engineName": "string",
        "engineVersion": "string",
        "dbVersion": "string",
        "definitionTime": "string"
      }
    ]
  },
  "processingState": 0,
  "exception": {
    "exceptionDetails": "string",
    "exceptionMessage": "string"
  },
  "created": "2019-08-24T14:15:22Z",
```

```
"discoveryStarted": "2019-08-24T14:15:22Z",
  "fileProcessingDetails": {
    "streamingStartedTime": "2019-08-24T14:15:22Z",
    "streamingCompletedTime": "2019-08-24T14:15:22Z",
    "streamingTimeSpanMs": 0,
    "scanCompletedTime": "2019-08-24T14:15:22Z",
    "processingTimeSpanMs": 0
  },
  "coreEngines": [
    {
      "engineId": "string",
      "engineName": "string",
      "engineVersion": "string",
      "dbVersion": "string",
      "definitionTime": "string"
    }
  ],
  "remediation": {
    "deepCdr": {
      "sanitizationDetails": {
        "failureCategory": "string",
        "description": "string",
        "details": "string"
      },
      "cdrObjectState": 0,
      "fileWasReplaced": true
    },
    "postActionFailedInformation": [
      {
        "objectActionType": 0,
        "exception": {
          "exceptionDetails": "string",
          "exceptionMessage": "string"
        }
      }
    ],
    "objectRemediationActions": [
      {
        "objectActionType": 0,
        "objectActionState": 0,
        "cdrObjectState": 0,
        "exceptions": [
          "string"
        ],
        "id": "string",
        "fileId": "string",
        "fileScanCompletedTime": "2019-08-24T14:15:22Z",
        "remediationId": "string",
        "tenantId": "string",
        "lastUpdated": "2019-08-24T14:15:22Z"
      }
    ]
  },
```

```
"discoveryStartedDaySec": 0,
  "fileDto": {
    "result": 0,
    "responseKey": "string",
    "responseMessage": "string",
    "responseMessageParams": {
      "property1": "string",
      "property2": "string"
    },
    "id": "string",
    "scanId": "string",
    "name": "string",
    "path": "string",
    "hash": "string",
    "fileOwner": {
      "userId": "string",
      "fullName": "string",
      "userName": "string",
      "emailAddress": "string"
    },
    "size": 0,
    "fileTypeCategory": 0,
    "extension": "string",
    "storageType": {
      "name": "string",
      "categoryType": 0,
      "protocolType": 0,
      "vendorType": 0
    },
    "storageName": "string",
    "storageLocation": "string",
    "scanName": "string",
    "progress": {
      "upload": 0,
      "scan": 0,
      "archiveExtraction": 0
    },
    "scanResult": {
      "extractedFiles": {
        "dataId": "string",
        "scanResultI": 0,
        "detectedBy": 0,
        "filesExtractedCount": 0
      },
      "scanResults": {
        "scanDetails": [
          {
            "engineName": "string",
            "threatFound": "string",
            "scanResultI": 0,
            "defTime": "string",
            "scanTime": 0.1,
            "engId": "string",
```

```
}
        ],
        "dataId": "string",
        "scanAllResultI": 0,
        "scanAllResultA": "string",
        "startTime": "string",
        "totalTime": 0.1,
        "totalAvs": 0,
        "totalDetections": 0,
        "progressPercentage": 0
      },
      "fileInfo": {
        "fileSize": 0,
        "uploadTimestamp": "string",
        "md5": "string",
        "sha1": "string",
        "sha256": "string",
        "fileTypeCategory": "string",
        "fileTypeDescription": "string",
        "fileTypeExtension": "string",
        "displayName": "string",
        "fileTypeId": "string"
      },
      "fileScanInfo": {
        "finalVerdict": {
          "blocked": true,
          "verdict": "string",
          "confidence": 0.1,
          "threatLevel": 0.1
        },
        "overviewReport": {
          "analysisState": "string",
          "signalGroups": [
            {
              "description": "string",
              "verdict": "string",
              "signals": [
                {
                  "originType": "string",
                  "signalReadable": "string",
                  "strength": 0.1
                }
              ],
              "mitreTechniques": [
                {
                  "name": "string",
                  "tacticName": "string"
                }
              ]
            }
          ],
          "iocs": [
            {
```

```
"type": "string",
              "origin": "string",
              "verdict": "string"
            }
          ],
          "yaraMatches": [
            {
              "ruleName": "string",
              "ruleDescription": "string",
              "verdict": "string",
              "matchedStrings": [
                "string"
              ],
              "author": "string",
              "version": "string",
              "threatLevel": 0.1,
              "confidence": 0.1,
              "strength": 0.1
            }
          ],
          "tags": [
            {
              "name": "string",
              "verdict": "string"
            }
          ],
          "metaData": {
            "entropy": 0.1,
            "forensicAnalysisRecommended": true,
            "fuzzyFsioHash": "string"
          }
        },
        "errorCategory": "string",
        "errorCode": 0,
        "errorDetails": "string"
      },
      "processInfo": {
        "postProcessing": {
          "actionsRan": "string",
          "actionsFailed": "string",
          "convertedTo": "string",
          "copyMoveDestination": "string",
          "convertedDestination": "string",
          "sanitizationDetails": {
            "failureCategory": "string",
            "description": "string",
            "details": "string"
          }
        },
        "progressPercentage": 0,
        "userAgent": "string",
        "profile": "string",
        "result": "string",
```

```
"fileTypeSkippedScan": true,
        "processingTime": 0.1,
        "queueTime": 0.1,
        "resultI": 0
      },
      "dataId": "string",
      "dlpInfo": {
        "hits": null,
        "verdict": 0
      },
      "sbomInfo": {
        "finalVerdict": {
          "blocked": true,
          "licensingPackageCounts": {
            "allowed": 0,
            "blocked": 0,
            "unknown": 0,
            "unsupported": 0
          },
          "severity": 0,
          "totalPackageCount": 0,
          "verdict": "string",
          "vulnerabilityCounts": {
            "critical": 0,
            "high": 0,
            "medium": 0,
            "low": 0,
            "unknown": 0
          }
        },
        "overviewReport": {
          "isPartialReport": true,
          "osInfo": {
            "osName": "string",
            "osVersion": "string"
          },
          "scanMode": "string",
          "steps": [
            {
              "command": "string",
              "packages": [
                {
                  "authors": "string",
                  "releaseDate": "2019-08-24T14:15:22Z",
                  "ecosystem": "string",
                  "group": "string",
                  "archive": true,
                  "executable": true,
                  "uid": "string",
                  "licenses": {
                    "allowed": [
                      {
                        "id": "string",
```

```
"category": "string",
                        "usageRestriction": {
                          "permissions": [
                            "string"
                          ],
                          "conditions": [
                            "string"
                          ],
                          "limitations": [
                            "string"
                          ]
                        }
                      }
                    ],
                    "blocked": [
                      {
                        "id": "string",
                        "url": "string",
                        "category": "string",
                        "usageRestriction": {
                          "permissions": [
                            "string"
                          ],
                          "conditions": [
                            "string"
                          ],
                          "limitations": [
                            "string"
                          ]
                        }
                      }
                    ]
                  },
                  "packageName": "string",
                  "packageVersion": "string",
                  "hashes": [
                    {
                      "sha256": "string",
                      "fileName": "string"
                    }
                  ],
                  "vulnerabilityCounts": {
                    "critical": 0,
                    "high": 0,
                    "medium": 0,
                    "low": 0,
                    "unknown": 0
                  },
                  "vulnerabilities": [
                    {
                      "id": "string",
                      "severity": 0,
                      "source": "string",
```

```
"cwes": [
                        "string"
                      ]
                    }
                  ],
                  "arch": "string",
                  "osName": "string",
                  "osVersion": "string",
                  "dependencies": [
                    {
                      "ecosystem": "string",
                      "group": "string",
                      "packageName": "string",
                      "packageVersion": "string",
                      "vulnerabilities": [
                        {
                          "id": "string",
                          "severity": 0,
                          "source": "string",
                          "fixedVersions": "string",
                          "cwes": [
                            "string"
                          ]
                        }
                      ],
                      "vulnerabilityCounts": {
                        "critical": 0,
                        "high": 0,
                        "medium": 0,
                        "low": 0,
                        "unknown": 0
                      }
                    }
                  ]
                }
              ],
              "licenseStatus": "string",
              "licensingPackageCounts": {
                "allowed": 0,
                "blocked": 0,
                "unknown": 0,
                "unsupported": 0
              },
              "step": 0,
              "vulnerabilityCount": 0,
              "sha256": "string",
              "severity": 0,
              "vulnerabilityCounts": {
                "critical": 0,
                "high": 0,
                "medium": 0,
                "low": 0,
                "unknown": 0
```

```
}
          ],
          "packages": [
            {
              "authors": "string",
              "releaseDate": "2019-08-24T14:15:22Z",
              "ecosystem": "string",
              "group": "string",
              "archive": true,
              "executable": true,
              "uid": "string",
              "licenses": {
                "allowed": [
                  {
                    "id": "string",
                    "url": "string",
                    "category": "string",
                    "usageRestriction": {
                      "permissions": [
                        "string"
                      ],
                      "conditions": [
                        "string"
                      ],
                      "limitations": [
                        "string"
                      ]
                    }
                  }
                ],
                "blocked": [
                  {
                    "id": "string",
                    "url": "string",
                    "category": "string",
                    "usageRestriction": {
                      "permissions": [
                        "string"
                      ],
                      "conditions": [
                        "string"
                      ],
                      "limitations": [
                        "string"
                      ]
                    }
                  }
                ]
              },
              "packageName": "string",
              "packageVersion": "string",
              "target": "string",
              "hashes": [
```

```
"sha256": "string",
                  "fileName": "string"
                }
              ],
              "vulnerabilities": [
                {
                  "id": "string",
                  "severity": 0,
                  "source": "string",
                  "fixedVersions": "string",
                  "cwes": [
                    "string"
                  ]
                }
              ],
              "vulnerabilityCounts": {
                "critical": 0,
                "high": 0,
                "medium": 0,
                "low": 0,
                "unknown": 0
              },
              "dependencies": [
                {
                  "ecosystem": "string",
                  "group": "string",
                  "packageName": "string",
                  "packageVersion": "string",
                  "vulnerabilities": [
                    {
                      "id": "string",
                      "severity": 0,
                      "source": "string",
                      "fixedVersions": "string",
                      "cwes": [
                        "string"
                      ]
                    }
                  ],
                  "vulnerabilityCounts": {
                    "critical": 0,
                    "high": 0,
                    "medium": 0,
                    "low": 0,
                    "unknown": 0
                  }
                }
              ]
            }
          ],
          "dependenciesPackageCount": 0,
          "dependenciesVulnerabilityTotal": 0,
          "dependenciesVulnerabilityCounts": {
```

```
"high": 0,
            "medium": 0,
            "low": 0,
            "unknown": 0
          }
        },
        "resultTemplateHash": "string"
      },
      "vulnerabilityInfo": {
        "vulnerabilityInfoResult": {
          "code": 0,
          "hash": "string",
          "method": 0,
          "timeStamp": "string",
          "timing": 0,
          "detectedProduct": {
            "hasVulnerability": true,
            "isCurrent": true,
            "product": {
              "id": 0,
              "name": "string"
            },
            "remediationLink": "string",
            "severity": "string",
            "sigName": "string",
            "signature": 0,
            "vendor": {
              "id": 0,
              "name": "string"
            },
            "version": "string",
            "versionData": {
              "countBehind": 0,
              "feedId": 0,
              "version": "string"
            },
            "vulnerabilities": [
              {
                "description": "string",
                "details": {
                  "cpe": "string",
                  "cve": "string",
                  "cvss": {
                    "accessComplexity": "string",
                    "accessVector": "string",
                    "authentication": "string",
                    "availabilityImpact": "string",
                    "confidentialityImpact": "string",
                    "generatedOnEpoch": "string",
                    "integrityImpact": "string",
                    "score": "string",
                    "source": "string"
                  },
```

```
"attackComplexity": "string",
                    "attackVector": "string",
                    "availabilityImpact": "string",
                    "baseScore": "string",
                    "baseSeverity": "string",
                    "confidentialityImpact": "string",
                    "exploitabilityScore": "string",
                    "impactScore": "string",
                    "integrityImpact": "string",
                    "privilegesRequired": "string",
                    "scope": "string",
                    "userInteraction": "string",
                    "vectorString": "string"
                  },
                  "cwe": "string",
                  "lastModifiedEpoch": "string",
                  "publishedEpoch": "string",
                  "references": [
                    "string"
                  ]
                },
                "severity": "string",
                "severityIndex": 0,
                "staticId": 0
              }
            ]
          }
        }
      },
      "sessionCookie": "string",
      "fileTypeInfo": {
        "fileInfoExtended": {
          "extensions": "string",
          "groupId": "string",
          "typeId": "string"
        }
      },
      "scanInstanceUrl": "string",
      "scanWorkflowSnapshotId": "string",
      "coreEngines": [
        {
          "engineId": "string",
          "engineName": "string",
          "engineVersion": "string",
          "dbVersion": "string",
          "definitionTime": "string"
        }
      ]
    },
    "processingState": 0,
    "exception": {
      "exceptionDetails": "string",
      "exceptionMessage": "string"
```

```
"created": "2019-08-24T14:15:22Z",
    "lastModified": "2019-08-24T14:15:22Z",
    "discoveryStarted": "2019-08-24T14:15:22Z",
    "fileProcessingDetails": {
      "streamingStartedTime": "2019-08-24T14:15:22Z",
      "streamingCompletedTime": "2019-08-24T14:15:22Z",
      "streamingTimeSpanMs": 0,
      "scanCompletedTime": "2019-08-24T14:15:22Z",
      "processingTimeSpanMs": 0
    },
    "coreEngines": [
      {
        "engineId": "string",
        "engineName": "string",
        "engineVersion": "string",
        "dbVersion": "string",
        "definitionTime": "string"
      }
    ],
    "remediation": {
      "deepCdr": {
        "sanitizationDetails": {
          "failureCategory": "string",
          "description": "string",
          "details": "string"
        },
        "cdrObjectState": 0,
        "fileWasReplaced": true
      },
      "postActionFailedInformation": [
        {
          "objectActionType": 0,
          "exception": {
            "exceptionDetails": "string",
            "exceptionMessage": "string"
          }
        }
      ],
      "objectRemediationActions": [
        {
          "objectActionType": 0,
          "objectActionState": 0,
          "cdrObjectState": 0,
          "exceptions": [
            "string"
          ],
          "id": "string",
          "fileId": "string",
          "fileScanCompletedTime": "2019-08-24T14:15:22Z",
          "remediationId": "string",
          "tenantId": "string",
          "lastUpdated": "2019-08-24T14:15:22Z"
        }
```

```
},
    "metaDefenderCoreUrl": "string",
    "discoveryStartedDaySec": 0,
    "objectStorageMetadata": "string",
    "scanWorkflowSnapshotId": "string",
    "scanWorkflowSnapshot": {
      "id": "string",
      "scanId": "string",
      "workflow": {
        "id": "string",
        "scanPoolId": "string",
        "scanProcessFlow": 0,
        "isIdentityScanningEnabled": true,
        "scanIntervalDays": 0,
        "rules": [
          "string"
        ],
        "type": 0,
        "workflowSupportedTechnologies": {
          "dlp": {
            "status": 0
          },
          "deepCdr": {
            "status": 0
          },
          "sandBox": {
            "status": 0
          },
          "metascan": {
            "status": 0
          }
        },
        "name": "string",
        "userAgent": "string",
        "scanPool": {
          "id": "string",
          "name": "string",
          "scanPoolType": 0,
          "isDefault": true,
          "scanInstances": [
            {
              "id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ]
        },
        "failOverScanPoolId": "string",
        "failOverScanPool": {
          "id": "string",
```

```
"scanPoolType": 0,
          "isDefault": true,
          "scanInstances": [
            {
              "id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ]
        },
        "filters": {
          "id": "string",
          "minimumSize": 0,
          "maximumSize": 0,
          "minimumDateTime": "2019-08-24T14:15:22Z",
          "maximumDateTime": "2019-08-24T14:15:22Z"
        },
        "fileDefinition": {
          "blockingStrategy": 0,
          "configurableBlockingStrategy": {
            "shouldTreatFilesWithSensitiveDataAsBlocked": true,
            "shouldTreatFilesWithVulnerabilitiesAsBlocked": true
          }
        },
        "remediations": [
          {
            "id": "string",
            "workflowId": "string",
            "isEnabled": true,
            "configuration": "string",
            "type": 0,
            "handlingType": 0
          }
        ],
        "tenantId": "string"
      },
      "startTimestamp": 0,
      "stopTimestamp": 0,
      "scanPool": {
        "id": "string",
        "name": "string",
        "scanPoolType": 0,
        "isDefault": true,
        "scanInstances": [
          {
            "id": "string",
            "scanPoolId": "string",
            "url": "string",
            "apiKey": "string",
            "timeout": "string",
```

```
}
        ]
      },
      "scanInstances": [
        {
          "id": "string",
          "scanPoolId": "string",
          "url": "string",
          "apiKey": "string",
          "timeout": "string",
          "scanInstanceType": 0
        }
      ],
      "failOverScanPool": {
        "id": "string",
        "name": "string",
        "scanPoolType": 0,
        "isDefault": true,
        "scanInstances": [
          {
            "id": "string",
            "scanPoolId": "string",
            "url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ]
      },
      "failOverScanInstances": [
        {
          "id": "string",
          "scanPoolId": "string",
          "url": "string",
          "apiKey": "string",
          "timeout": "string",
          "scanInstanceType": 0
        }
      ],
      "storage": {
        "id": "string",
        "name": "string",
        "groupId": "string",
        "clientId": "string",
        "accountId": "string",
        "source": "string",
        "storageFunctionality": "string",
        "storageType": {
          "name": "string",
          "categoryType": 0,
          "protocolType": 0,
          "vendorType": 0
        },
```

```
"message": "string",
          "statusType": 0
        },
        "workflowId": "string",
        "lastUpdated": "2019-08-24T14:15:22Z",
        "tenantId": "string",
        "groupRef": {
          "id": "string",
          "name": "string"
        },
        "isAutodiscovered": true
      },
      "workflowStatistics": {
        "taggingStatistics": {
          "total": 0
        },
        "keepAllowedStatistics": {
          "total": 0
        },
        "keepBlockedStatistics": {
          "total": 0
        },
        "keepSanitizedStatistics": {
          "total": 0
        },
        "movedAllowedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
```

```
},
        "movedSanitizedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "movedBlockedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
```

```
"groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "copyAllowedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "copyBlockedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
```

```
"message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "deleteAllowedStatistics": {
          "total": 0
        },
        "deleteBlockedStatistics": {
          "total": 0
        },
        "lastCalculatedStatisticsTime": "2019-08-24T14:15:22Z"
      },
      "account": {
        "id": "string",
        "name": "string",
        "description": "string",
        "credentials": "string",
        "protocolType": 0,
        "vendorType": 0,
        "autoDiscovery": true,
        "autodiscoveryDestinationGroupId": "string",
        "destinationGroup": {
          "id": "string",
          "name": "string"
        }
      },
      "realTimeStartDate": "2019-08-24T14:15:22Z"
    },
    "versions": [
      {
        "result": 0,
        "responseKey": "string",
        "responseMessage": "string",
        "responseMessageParams": {
          "property1": "string",
          "property2": "string"
        },
        "id": "string",
        "scanId": "string",
        "name": "string",
        "path": "string",
        "hash": "string",
        "fileOwner": {
          "userId": "string",
```

```
"userName": "string",
          "emailAddress": "string"
        },
        "size": 0,
        "fileTypeCategory": 0,
        "extension": "string",
        "storageType": {
          "name": "string",
          "categoryType": 0,
          "protocolType": 0,
          "vendorType": 0
        },
        "storageName": "string",
        "storageLocation": "string",
        "scanName": "string",
        "progress": {
          "upload": 0,
          "scan": 0,
          "archiveExtraction": 0
        },
        "scanResult": {
          "extractedFiles": {
            "dataId": "string",
            "scanResultI": 0,
            "detectedBy": 0,
            "filesExtractedCount": 0
          },
          "scanResults": {
            "scanDetails": [
              {
                "engineName": "string",
                "threatFound": "string",
                "scanResultI": 0,
                "defTime": "string",
                "scanTime": 0.1,
                "engId": "string",
                "waitTime": 0.1
              }
            ],
            "dataId": "string",
            "scanAllResultI": 0,
            "scanAllResultA": "string",
            "startTime": "string",
            "totalTime": 0.1,
            "totalAvs": 0,
            "totalDetections": 0,
            "progressPercentage": 0
          },
          "fileInfo": {
            "fileSize": 0,
            "uploadTimestamp": "string",
            "md5": "string",
            "sha1": "string",
```

```
"fileTypeCategory": "string",
            "fileTypeDescription": "string",
            "fileTypeExtension": "string",
            "displayName": "string",
            "fileTypeId": "string"
          },
          "fileScanInfo": {
            "finalVerdict": {
              "blocked": true,
              "verdict": "string",
              "confidence": 0.1,
              "threatLevel": 0.1
            },
            "overviewReport": {
              "analysisState": "string",
              "signalGroups": [
                {
                  "description": "string",
                  "verdict": "string",
                  "signals": [
                    {
                      "originType": "string",
                      "signalReadable": "string",
                      "strength": 0.1
                    }
                  ],
                  "mitreTechniques": [
                    {
                      "name": "string",
                      "tacticName": "string"
                    }
                  ]
                }
              ],
              "iocs": [
                {
                  "data": "string",
                  "type": "string",
                  "origin": "string",
                  "verdict": "string"
                }
              ],
              "yaraMatches": [
                {
                  "ruleName": "string",
                  "ruleDescription": "string",
                  "verdict": "string",
                  "matchedStrings": [
                    "string"
                  ],
                  "author": "string",
                  "version": "string",
                  "threatLevel": 0.1,
```

```
"strength": 0.1
                }
              ],
              "tags": [
                {
                  "name": "string",
                  "verdict": "string"
                }
              ],
              "metaData": {
                "entropy": 0.1,
                "forensicAnalysisRecommended": true,
                "fuzzyFsioHash": "string"
              }
            },
            "errorCategory": "string",
            "errorCode": 0,
            "errorDetails": "string"
          },
          "processInfo": {
            "postProcessing": {
              "actionsRan": "string",
              "actionsFailed": "string",
              "convertedTo": "string",
              "copyMoveDestination": "string",
              "convertedDestination": "string",
              "sanitizationDetails": {
                "failureCategory": "string",
                "description": "string",
                "details": "string"
              }
            },
            "progressPercentage": 0,
            "userAgent": "string",
            "profile": "string",
            "result": "string",
            "blockedReason": "string",
            "fileTypeSkippedScan": true,
            "processingTime": 0.1,
            "queueTime": 0.1,
            "resultI": 0
          },
          "dataId": "string",
          "dlpInfo": {
            "hits": null,
            "verdict": 0
          },
          "sbomInfo": {
            "finalVerdict": {
              "blocked": true,
              "licensingPackageCounts": {
                "allowed": 0,
                "blocked": 0,
```

```
"unsupported": 0
              },
              "severity": 0,
              "totalPackageCount": 0,
              "verdict": "string",
              "vulnerabilityCounts": {
                "critical": 0,
                "high": 0,
                "medium": 0,
                "low": 0,
                "unknown": 0
              }
            },
            "overviewReport": {
              "isPartialReport": true,
              "osInfo": {
                "osName": "string",
                "osVersion": "string"
              },
              "scanMode": "string",
              "steps": [
                {
                  "command": "string",
                  "packages": [
                    {
                      "authors": "string",
                      "releaseDate": "2019-08-24T14:15:22Z",
                      "ecosystem": "string",
                      "group": "string",
                      "archive": true,
                      "executable": true,
                      "uid": "string",
                      "licenses": {
                        "allowed": [
                          {
                            "id": "string",
                            "url": "string",
                            "category": "string",
                            "usageRestriction": {
                              "permissions": [],
                              "conditions": [],
                              "limitations": []
                            }
                          }
                        ],
                        "blocked": [
                          {
                            "id": "string",
                            "url": "string",
                            "category": "string",
                            "usageRestriction": {
                              "permissions": [],
                              "conditions": [],
```

```
}
                        }
                    ]
                },
                "packageName": "string",
                "packageVersion": "string",
                "hashes": [
                    {
                        "sha256": "string",
                        "fileName": "string"
                    }
                ],
                "vulnerabilityCounts": {
                    "critical": 0,
                    "high": 0,
                    "medium": 0,
                    "low": 0,
                    "unknown": 0
                },
                "vulnerabilities": [
                    {
                        "id": "string",
                        "severity": 0,
                        "source": "string",
                        "fixedVersions": "string",
                        "cwes": [
                            "string"
                        ]
                    }
                ],
                "arch": "string",
                "osName": "string",
                "osVersion": "string",
                "dependencies": [
                    {
                        "ecosystem": "string",
                        "group": "string",
                        "packageName": "string",
                        "packageVersion": "string",
                        "vulnerabilities": [
                            {
                                "cwes": []
                            }
                        ],
                        "vulnerabilityCounts": {
                            "critical": 0,
                            "high": 0,
                            "medium": 0,
                            "low": 0,
                            "unknown": 0
                        }
                    }
                ]
```

```
],
                    "licenseStatus": "string",
                    "licensingPackageCounts": {
                      "allowed": 0,
                      "blocked": 0,
                      "unknown": 0,
                      "unsupported": 0
                    },
                    "step": 0,
                    "vulnerabilityCount": 0,
                    "sha256": "string",
                    "severity": 0,
                    "vulnerabilityCounts": {
                      "critical": 0,
                      "high": 0,
                      "medium": 0,
                      "low": 0,
                      "unknown": 0
                    }
                  }
                ],
                "packages": [
                  {
                    "authors": "string",
                    "releaseDate": "2019-08-24T14:15:22Z",
                    "ecosystem": "string",
                    "group": "string",
                    "archive": true,
                    "executable": true,
                    "uid": "string",
                    "licenses": {
                      "allowed": [
                        {
                          "id": "string",
                          "url": "string",
                          "category": "string",
                          "usageRestriction": {
                            "permissions": [
                              "string"
                            ],
                            "conditions": [
                              "string"
                            ],
                            "limitations": [
                              "string"
                            ]
                          }
                        }
                      ],
                      "blocked": [
                        {
                          "id": "string",
                          "url": "string",
```

```
"usageRestriction": {
                          "permissions": [
                            "string"
                          ],
                          "conditions": [
                            "string"
                          ],
                          "limitations": [
                            "string"
                          ]
                        }
                      }
                    ]
                  },
                  "packageName": "string",
                  "packageVersion": "string",
                  "target": "string",
                  "hashes": [
                    {
                      "sha256": "string",
                      "fileName": "string"
                    }
                  ],
                  "vulnerabilities": [
                    {
                      "id": "string",
                      "severity": 0,
                      "source": "string",
                      "fixedVersions": "string",
                      "cwes": [
                        "string"
                      ]
                    }
                  ],
                  "vulnerabilityCounts": {
                    "critical": 0,
                    "high": 0,
                    "medium": 0,
                    "low": 0,
                    "unknown": 0
                  },
                  "dependencies": [
                    {
                      "ecosystem": "string",
                      "group": "string",
                      "packageName": "string",
                      "packageVersion": "string",
                      "vulnerabilities": [
                        {
                          "id": "string",
                          "severity": 0,
                          "source": "string",
                          "fixedVersions": "string",
```

```
"string"
                          ]
                        }
                      ],
                      "vulnerabilityCounts": {
                        "critical": 0,
                        "high": 0,
                        "medium": 0,
                        "low": 0,
                        "unknown": 0
                      }
                    }
                  ]
                }
              ],
              "dependenciesPackageCount": 0,
              "dependenciesVulnerabilityTotal": 0,
              "dependenciesVulnerabilityCounts": {
                "critical": 0,
                "high": 0,
                "medium": 0,
                "low": 0,
                "unknown": 0
              }
            },
            "resultTemplateHash": "string"
          },
          "vulnerabilityInfo": {
            "vulnerabilityInfoResult": {
              "code": 0,
              "hash": "string",
              "method": 0,
              "timeStamp": "string",
              "timing": 0,
              "detectedProduct": {
                "hasVulnerability": true,
                "isCurrent": true,
                "product": {
                  "id": 0,
                  "name": "string"
                },
                "remediationLink": "string",
                "severity": "string",
                "sigName": "string",
                "signature": 0,
                "vendor": {
                  "id": 0,
                  "name": "string"
                },
                "version": "string",
                "versionData": {
                  "countBehind": 0,
                  "feedId": 0,
```

```
},
                "vulnerabilities": [
                  {
                    "description": "string",
                    "details": {
                      "cpe": "string",
                      "cve": "string",
                      "cvss": {
                        "accessComplexity": "string",
                        "accessVector": "string",
                        "authentication": "string",
                        "availabilityImpact": "string",
                        "confidentialityImpact": "string",
                        "generatedOnEpoch": "string",
                        "integrityImpact": "string",
                        "score": "string",
                        "source": "string"
                      },
                      "cvss3": {
                        "attackComplexity": "string",
                        "attackVector": "string",
                        "availabilityImpact": "string",
                        "baseScore": "string",
                        "baseSeverity": "string",
                        "confidentialityImpact": "string",
                        "exploitabilityScore": "string",
                        "impactScore": "string",
                        "integrityImpact": "string",
                        "privilegesRequired": "string",
                        "scope": "string",
                        "userInteraction": "string",
                        "vectorString": "string"
                      },
                      "cwe": "string",
                      "lastModifiedEpoch": "string",
                      "publishedEpoch": "string",
                      "references": [
                        "string"
                      ]
                    },
                    "severity": "string",
                    "severityIndex": 0,
                    "staticId": 0
                  }
                ]
              }
            }
          },
          "sessionCookie": "string",
          "fileTypeInfo": {
            "fileInfoExtended": {
              "extensions": "string",
              "groupId": "string",
```

```
}
          },
          "scanInstanceUrl": "string",
          "scanWorkflowSnapshotId": "string",
          "coreEngines": [
            {
              "engineId": "string",
              "engineName": "string",
              "engineVersion": "string",
              "dbVersion": "string",
              "definitionTime": "string"
            }
          ]
        },
        "processingState": 0,
        "exception": {
          "exceptionDetails": "string",
          "exceptionMessage": "string"
        },
        "created": "2019-08-24T14:15:22Z",
        "lastModified": "2019-08-24T14:15:22Z",
        "discoveryStarted": "2019-08-24T14:15:22Z",
        "fileProcessingDetails": {
          "streamingStartedTime": "2019-08-24T14:15:22Z",
          "streamingCompletedTime": "2019-08-24T14:15:22Z",
          "streamingTimeSpanMs": 0,
          "scanCompletedTime": "2019-08-24T14:15:22Z",
          "processingTimeSpanMs": 0
        },
        "coreEngines": [
          {
            "engineId": "string",
            "engineName": "string",
            "engineVersion": "string",
            "dbVersion": "string",
            "definitionTime": "string"
          }
        ],
        "remediation": {
          "deepCdr": {
            "sanitizationDetails": {
              "failureCategory": "string",
              "description": "string",
              "details": "string"
            },
            "cdrObjectState": 0,
            "fileWasReplaced": true
          },
          "postActionFailedInformation": [
            {
              "objectActionType": 0,
              "exception": {
                "exceptionDetails": "string",
```

```
}
            }
          ],
          "objectRemediationActions": [
            {
              "objectActionType": 0,
              "objectActionState": 0,
              "cdrObjectState": 0,
              "exceptions": [
                "string"
              ],
              "id": "string",
              "fileId": "string",
              "fileScanCompletedTime": "2019-08-24T14:15:22Z",
              "remediationId": "string",
              "tenantId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z"
            }
          ]
        },
        "metaDefenderCoreUrl": "string",
        "discoveryStartedDaySec": 0,
        "objectStorageMetadata": "string",
        "scanWorkflowSnapshotId": "string",
        "scanWorkflowSnapshot": {
          "id": "string",
          "scanId": "string",
          "workflow": {
            "id": "string",
            "scanPoolId": "string",
            "scanProcessFlow": 0,
            "isIdentityScanningEnabled": true,
            "scanIntervalDays": 0,
            "rules": [
              "string"
            ],
            "type": 0,
            "workflowSupportedTechnologies": {
              "dlp": {
                "status": 0
              },
              "deepCdr": {
                "status": 0
              },
              "sandBox": {
                "status": 0
              },
              "metascan": {
                "status": 0
              }
            },
            "name": "string",
            "userAgent": "string",
```

```
"id": "string",
              "name": "string",
              "scanPoolType": 0,
              "isDefault": true,
              "scanInstances": [
                {
                  "id": "string",
                  "scanPoolId": "string",
                  "url": "string",
                  "apiKey": "string",
                  "timeout": "string",
                  "scanInstanceType": 0
                }
              ]
            },
            "failOverScanPoolId": "string",
            "failOverScanPool": {
              "id": "string",
              "name": "string",
              "scanPoolType": 0,
              "isDefault": true,
              "scanInstances": [
                {
                  "id": "string",
                  "scanPoolId": "string",
                  "url": "string",
                  "apiKey": "string",
                  "timeout": "string",
                  "scanInstanceType": 0
                }
              ]
            },
            "filters": {
              "id": "string",
              "minimumSize": 0,
              "maximumSize": 0,
              "minimumDateTime": "2019-08-24T14:15:22Z",
              "maximumDateTime": "2019-08-24T14:15:22Z"
            },
            "fileDefinition": {
              "blockingStrategy": 0,
              "configurableBlockingStrategy": {
                "shouldTreatFilesWithSensitiveDataAsBlocked": true,
                "shouldTreatFilesWithVulnerabilitiesAsBlocked": true
              }
            },
            "remediations": [
              {
                "id": "string",
                "workflowId": "string",
                "isEnabled": true,
                "configuration": "string",
                "type": 0,
```

```
}
            ],
            "tenantId": "string"
          },
          "startTimestamp": 0,
          "stopTimestamp": 0,
          "scanPool": {
            "id": "string",
            "name": "string",
            "scanPoolType": 0,
            "isDefault": true,
            "scanInstances": [
              {
                "id": "string",
                "scanPoolId": "string",
                "url": "string",
                "apiKey": "string",
                "timeout": "string",
                "scanInstanceType": 0
              }
            ]
          },
          "scanInstances": [
            {
              "id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ],
          "failOverScanPool": {
            "id": "string",
            "name": "string",
            "scanPoolType": 0,
            "isDefault": true,
            "scanInstances": [
              {
                "id": "string",
                "scanPoolId": "string",
                "url": "string",
                "apiKey": "string",
                "timeout": "string",
                "scanInstanceType": 0
              }
            ]
          },
          "failOverScanInstances": [
            {
              "id": "string",
              "scanPoolId": "string",
              "url": "string",
```

```
"timeout": "string",
              "scanInstanceType": 0
            }
          ],
          "storage": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          },
          "workflowStatistics": {
            "taggingStatistics": {
              "total": 0
            },
            "keepAllowedStatistics": {
              "total": 0
            },
            "keepBlockedStatistics": {
              "total": 0
            },
            "keepSanitizedStatistics": {
              "total": 0
            },
            "movedAllowedStatistics": {
              "total": 0,
              "destinationStorageInformation": {
                "id": "string",
                "name": "string",
                "groupId": "string",
                "clientId": "string",
                "accountId": "string",
                "source": "string",
```

```
"storageType": {
                    "name": "string",
                    "categoryType": 0,
                    "protocolType": 0,
                    "vendorType": 0
                  },
                  "storageStatus": {
                    "message": "string",
                    "statusType": 0
                  },
                  "workflowId": "string",
                  "lastUpdated": "2019-08-24T14:15:22Z",
                  "tenantId": "string",
                  "groupRef": {
                    "id": "string",
                    "name": "string"
                  },
                  "isAutodiscovered": true
                }
              },
              "movedSanitizedStatistics": {
                "total": 0,
                "destinationStorageInformation": {
                  "id": "string",
                  "name": "string",
                  "groupId": "string",
                  "clientId": "string",
                  "accountId": "string",
                  "source": "string",
                  "storageFunctionality": "string",
                  "storageType": {
                    "name": "string",
                    "categoryType": 0,
                    "protocolType": 0,
                    "vendorType": 0
                  },
                  "storageStatus": {
                    "message": "string",
                    "statusType": 0
                  },
                  "workflowId": "string",
                  "lastUpdated": "2019-08-24T14:15:22Z",
                  "tenantId": "string",
                  "groupRef": {
                    "id": "string",
                    "name": "string"
                  },
                  "isAutodiscovered": true
                }
              },
              "movedBlockedStatistics": {
                "total": 0,
                "destinationStorageInformation": {
```

```
"name": "string",
                "groupId": "string",
                "clientId": "string",
                "accountId": "string",
                "source": "string",
                "storageFunctionality": "string",
                "storageType": {
                  "name": "string",
                  "categoryType": 0,
                  "protocolType": 0,
                  "vendorType": 0
                },
                "storageStatus": {
                  "message": "string",
                  "statusType": 0
                },
                "workflowId": "string",
                "lastUpdated": "2019-08-24T14:15:22Z",
                "tenantId": "string",
                "groupRef": {
                  "id": "string",
                  "name": "string"
                },
                "isAutodiscovered": true
              }
            },
            "copyAllowedStatistics": {
              "total": 0,
              "destinationStorageInformation": {
                "id": "string",
                "name": "string",
                "groupId": "string",
                "clientId": "string",
                "accountId": "string",
                "source": "string",
                "storageFunctionality": "string",
                "storageType": {
                  "name": "string",
                  "categoryType": 0,
                  "protocolType": 0,
                  "vendorType": 0
                },
                "storageStatus": {
                  "message": "string",
                  "statusType": 0
                },
                "workflowId": "string",
                "lastUpdated": "2019-08-24T14:15:22Z",
                "tenantId": "string",
                "groupRef": {
                  "id": "string",
                  "name": "string"
                },
```

```
}
            },
            "copyBlockedStatistics": {
              "total": 0,
              "destinationStorageInformation": {
                "id": "string",
                "name": "string",
                "groupId": "string",
                "clientId": "string",
                "accountId": "string",
                "source": "string",
                "storageFunctionality": "string",
                "storageType": {
                  "name": "string",
                  "categoryType": 0,
                  "protocolType": 0,
                  "vendorType": 0
                },
                "storageStatus": {
                  "message": "string",
                  "statusType": 0
                },
                "workflowId": "string",
                "lastUpdated": "2019-08-24T14:15:22Z",
                "tenantId": "string",
                "groupRef": {
                  "id": "string",
                  "name": "string"
                },
                "isAutodiscovered": true
              }
            },
            "deleteAllowedStatistics": {
              "total": 0
            },
            "deleteBlockedStatistics": {
              "total": 0
            },
            "lastCalculatedStatisticsTime": "2019-08-24T14:15:22Z"
          },
          "account": {
            "id": "string",
            "name": "string",
            "description": "string",
            "credentials": "string",
            "protocolType": 0,
            "vendorType": 0,
            "autoDiscovery": true,
            "autodiscoveryDestinationGroupId": "string",
            "destinationGroup": {
              "id": "string",
              "name": "string"
            }
```

```
"realTimeStartDate": "2019-08-24T14:15:22Z"
        },
        "versions": [],
        "hasBlockedVersions": true,
        "versionsCount": 0,
        "objectType": 0,
        "skippedScan": true,
        "$type": "string",
        "url": "string",
        "fileId": "string"
      }
    ],
    "hasBlockedVersions": true,
    "versionsCount": 0,
    "objectType": 0,
    "skippedScan": true,
    "$type": "string"
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	GetFileResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Group

Manage your groups

Add a group

`POST /api/group`

> Body parameter


```
{
  "name": "string",
  "description": "string",
  "storageIds": [
    "string"
  ]
}
```

Parameters

Name	In	Type	Required	Description
body	body	AddGroupParameters	true	none

Example responses

200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "group": {
    "id": "string",
    "name": "string",
    "description": "string",
    "storages": [
      {
        "id": "string",
        "name": "string",
        "groupId": "string",
        "clientId": "string",
        "accountId": "string",
        "source": "string",
        "storageFunctionality": "string",
        "storageType": {
          "name": "string",
          "categoryType": 0,
          "protocolType": 0,
          "vendorType": 0
        },
        "storageStatus": {
          "message": "string",
          "statusType": 0
        },
        "workflowId": "string",
        "lastUpdated": "2019-08-24T14:15:22Z",
        "tenantId": "string",
        "groupRef": {
          "id": "string",
          "name": "string"
        },
        "isAutodiscovered": true
      }
    ]
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	AddGroupCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Bulk delete groups

`DELETE /api/group`

Deletes up to 100 groups in a single request. Per-group ABAC (Groups.Delete) plus per-cascaded-storage ABAC (Storages.Delete) are enforced. When forceDelete=true, child accounts and storages are cascade-deleted along with their scans. If any cascaded storage has a running scan, the request is rejected with HTTP 409. When forceDelete=false, groups with children are returned in the failed list with localized reason; only empty groups are deleted.

> Body parameter

```
{
  "groupIds": [
    "string"
  ],
  "forceDelete": true
}
```

Parameters

Name	In	Type	Required	Description
body	body	BulkDeleteGroupsParameters	true	none

> Example responses

> 200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "succeeded": [
    "string"
  ],
  "failed": [
    {
      "id": "string",
      "reasonKey": "string",
      "reason": "string",
      "childFailures": [
        {}
      ]
    }
  ],
  "confirmationRequired": true,
  "preview": [
    {
      "groupId": "string",
      "memberStorageIds": [
        "string"
      ]
    }
  ],
  "scansRunning": true,
  "runningScans": [
    {
      "scanId": "string",
      "storageId": "string",
      "accountId": "string",
      "groupId": "string"
    }
  ]
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	BulkDeleteGroupsCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

List groups (paginated, filtered, sorted)

`GET /api/group`

Returns a paginated, filtered, and sorted list of groups. The name filter performs a case-insensitive substring (ILIKE) match. The includeStorages flag (default true) controls whether associated storage units are loaded per group; set to false to skip the per-group N+1 storage scan RPC calls. Default Count is 100 (maximum 100). Returns an IPagedResponse containing Items, TotalCount, StartIndex, and Count.

Parameters

Name	In	Type	Required	Description
Name	query	string	false	none
IncludeStorages	query	boolean	false	none
StartIndex	query	integer(int32)	false	none
Count	query	integer(int32)	false	none
SortBy	query	array[integer]	false	none
SortOrder	query	array[integer]	false	none

Enumerated Values

Parameter	Value
SortBy	0
SortBy	1
SortOrder	0
SortOrder	1

Example responses

200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "items": [
    {
      "id": "string",
      "name": "string",
      "description": "string",
      "storages": [
        {
          "id": "string",
          "groupId": "string",
          "accountId": "string",
          "name": "string",
          "storageClientId": "string",
          "storageType": {
            "name": "string",
            "categoryType": 0,
            "protocolType": 0,
            "vendorType": 0
          },
          "storageStatus": {
            "message": "string",
            "statusType": 0
          },
          "scansInProgress": true,
          "isRtpInProgress": true,
          "isScheduledScanInProgress": true,
          "storageFunctionality": "string",
          "isAutodiscovered": true,
          "groupRef": {
            "id": "string",
            "name": "string"
          },
          "$type": "string"
        }
      ]
    }
  ],
  "groups": [
    {
      "id": "string",
      "name": "string",
      "description": "string",
      "storages": [
        {
          "id": "string",
```

```
"accountId": "string",
          "name": "string",
          "storageClientId": "string",
          "storageType": {
            "name": "string",
            "categoryType": 0,
            "protocolType": 0,
            "vendorType": 0
          },
          "storageStatus": {
            "message": "string",
            "statusType": 0
          },
          "scansInProgress": true,
          "isRtpInProgress": true,
          "isScheduledScanInProgress": true,
          "storageFunctionality": "string",
          "isAutodiscovered": true,
          "groupRef": {
            "id": "string",
            "name": "string"
          },
          "$type": "string"
        }
      ]
    }
  ],
  "totalCount": 0,
  "startIndex": 0,
  "count": 0
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	ListGroups

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Update a group

`PATCH /api/group`

> Body parameter

```
{
  "name": "string",
  "description": "string",
  "groupId": "string"
}
```

Parameters

Name	In	Type	Required	Description
body	body	UpdateGroupParameters	true	none

Example responses

200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "updatedGroup": {
    "id": "string",
    "name": "string",
    "description": "string",
    "storages": [
      {
        "id": "string",
        "name": "string",
        "groupId": "string",
        "clientId": "string",
        "accountId": "string",
        "source": "string",
        "storageFunctionality": "string",
        "storageType": {
          "name": "string",
          "categoryType": 0,
          "protocolType": 0,
          "vendorType": 0
        },
        "storageStatus": {
          "message": "string",
          "statusType": 0
        },
        "workflowId": "string",
        "lastUpdated": "2019-08-24T14:15:22Z",
        "tenantId": "string",
        "groupRef": {
          "id": "string",
          "name": "string"
        },
        "isAutodiscovered": true
      }
    ]
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	UpdateGroupCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Delete a group

`DELETE /api/group/{groupId}`

Parameters

Name	In	Type	Required	Description
groupId	path	string	true	none
forceDelete	query	boolean	false	none

> Example responses

> 200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "succeeded": [
    "string"
  ],
  "failed": [
    {
      "id": "string",
      "reasonKey": "string",
      "reason": "string",
      "childFailures": [
        {}
      ]
    }
  ],
  "confirmationRequired": true,
  "preview": [
    {
      "groupId": "string",
      "memberStorageIds": [
        "string"
      ]
    }
  ],
  "scansRunning": true,
  "runningScans": [
    {
      "scanId": "string",
      "storageId": "string",
      "accountId": "string",
      "groupId": "string"
    }
  ]
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	BulkDeleteGroupsCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Fetch group by ID

`GET /api/group/{groupId}`

Parameters

Name	In	Type	Required	Description
groupId	path	string	true	none

> Example responses

> 200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "group": {
    "id": "string",
    "name": "string",
    "description": "string",
    "storages": [
      {
        "id": "string",
        "groupId": "string",
        "accountId": "string",
        "name": "string",
        "storageClientId": "string",
        "storageType": {
          "name": "string",
          "categoryType": 0,
          "protocolType": 0,
          "vendorType": 0
        },
        "storageStatus": {
          "message": "string",
          "statusType": 0
        },
        "scansInProgress": true,
        "isRtpInProgress": true,
        "isScheduledScanInProgress": true,
        "storageFunctionality": "string",
        "isAutodiscovered": true,
        "groupRef": {
          "id": "string",
          "name": "string"
        },
        "$type": "string"
      }
    ]
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	GetGroupById

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Fetch the number of groups

`GET /api/group/count`

> Example responses

> 200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "groupCount": {
    "count": 0
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	GetGroupsCount

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Health Status

API that responds with 200 OK if application is running.

Get health status

`GET /api/health`

Parameters

Name	In	Type	Required	Description
verbose	query	boolean	false	whether to include extra details

> Example responses

> 200 Response


```
{
  "apiStatus": "string"
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	ApiHealthModel

This operation does not require authentication

Onboarding

Manage onboarding

Fetch onboarding configuration

`GET /api/onboarding`

Parameters

Name	In	Type	Required	Description
newConfigSetup	query	boolean	false	none
newDefaultWorkflow	query	boolean	false	none

> Example responses

200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "hasUserConfigured": true,
  "hasAccountConfigured": true,
  "hasStorageConfigured": true,
  "hasScanInstanceConfigured": true,
  "isOnboardingDone": true,
  "isEulaAgreed": true,
  "isCloudType": true
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	GetOnboarding

This operation does not require authentication

Finish onboarding

`POST /api/onboarding`

Example responses

200 Response

Responses

Status	Meaning	Description	Schema
200	OK	none	string

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Accept Eula

`POST /api/onboarding/eula`

> Example responses

> 200 Response

Responses

Status	Meaning	Description	Schema
200	OK	none	string

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Remediations

Remediations information

Get Remediations by workflow id

`GET /api/remediations/workflow/{id}`

Parameters

Name	In	Type	Required	Description
id	path	string	true	none

> Example responses

> 200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "entries": [
    {
      "id": "string",
      "workflowId": "string",
      "isEnabled": true,
      "configuration": "string",
      "type": 0,
      "handlingType": 0
    }
  ]
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	GetRemediationByWorkflowIdCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Get Remediation by id

`GET /api/remediations/{id}`

Parameters

Name	In	Type	Required	Description
id	path	string	true	none

> Example responses

> 200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "entry": {
    "id": "string",
    "workflowId": "string",
    "isEnabled": true,
    "configuration": "string",
    "type": 0,
    "handlingType": 0
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	GetRemediationByIdCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Delete Remediation

`DELETE /api/remediations/{id}`

Parameters

Name	In	Type	Required	Description
id	path	string	true	none

> Example responses

> 200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "succeeded": [
    "string"
  ],
  "failed": [
    {
      "id": "string",
      "reasonKey": "string",
      "reason": "string",
      "childFailures": [
        {}
      ]
    }
  ]
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	DeleteRemediationCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Add Remediation

`POST /api/remediations`

> Body parameter


```
{
  "workflowId": "string",
  "isEnabled": true,
  "configuration": "string",
  "type": 0,
  "handlingType": 0
}
```

Parameters

Name	In	Type	Required	Description
body	body	AddRemediationParameters	true	none

> Example responses

> 200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	AddRemediationCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Update Remediation

`PATCH /api/remediations`

> Body parameter


```
{
  "id": "string",
  "workflowId": "string",
  "isEnabled": true,
  "configuration": "string",
  "type": 0,
  "handlingType": 0
}
```

Parameters

Name	In	Type	Required	Description
body	body	UpdateRemediationParameters	true	none

> Example responses

> 200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	UpdateRemediationCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Bulk delete remediations

`DELETE /api/remediations`

Deletes multiple remediations in a single request. Returns per-id succeeded/failed results; a non-existent id is reported as failed (not found).

> Body parameter


```
{
  "remediationIds": [
    "string"
  ]
}
```

Parameters

Name	In	Type	Required	Description
body	body	BulkDeleteRemediationsParameters	true	none

Example responses

200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "succeeded": [
    "string"
  ],
  "failed": [
    {
      "id": "string",
      "reasonKey": "string",
      "reason": "string",
      "childFailures": [
        {}
      ]
    }
  ]
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	DeleteRemediationCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Report

Generate reports

Get scans report

`GET /api/report`

Parameters

Name	In	Type	Required	Description
storageId	query	string	false	none
name	query	string	false	none
scanTypesFilter	query	array[integer]	false	none
scanStatesFilter	query	array[integer]	false	none
realTimeHandlingType	query	any	false	none
startDate	query	string	false	none
endDate	query	string	false	none
sortBy	query	array[integer]	false	none
sortOrder	query	array[integer]	false	none
startIndex	query	integer(int32)	false	none
count	query	integer(int32)	false	none
workflowId	query	string	false	none
dateField	query	any	false	none

Enumerated Values

Parameter	Value
scanTypesFilter	0
scanTypesFilter	1
scanTypesFilter	2
scanStatesFilter	0
scanStatesFilter	1
scanStatesFilter	2
scanStatesFilter	3
scanStatesFilter	4
sortBy	0
sortBy	1
sortBy	2
sortOrder	0
sortOrder	1

Example responses

200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "entries": [
    {
      "result": 0,
      "responseKey": "string",
      "responseMessage": "string",
      "responseMessageParams": {
        "property1": "string",
        "property2": "string"
      },
      "id": "string",
      "name": "string",
      "startTime": "2019-08-24T14:15:22Z",
      "stopTime": "2019-08-24T14:15:22Z",
      "scanType": "string",
      "scanningState": 0,
      "scanStatusDto": {
        "pendingFilesCount": 0,
        "pendingFilesSize": 0,
        "allowedFilesCount": 0,
        "allowedFilesSize": 0,
        "blockedFilesCount": 0,
        "blockedFilesSize": 0,
        "sanitizedFilesCount": 0,
        "failedSanitizedFilesCount": 0,
        "remediatedFilesCount": 0,
        "totalFilesCount": 0,
        "totalFilesSize": 0,
        "processingFailedCount": 0,
        "processingFailedSize": 0,
        "processingFailedRemediationCount": 0,
        "processedFilesCount": 0,
        "processedFilesSize": 0,
        "canceledFilesCount": 0,
        "canceledFilesSize": 0
      },
      "scanStatsDto": {
        "infectedFilesCount": 0,
        "threatTotalFilesCount": 0,
        "filesWithVulnerabilitiesCount": 0,
        "filesWithSensitiveDataCount": 0,
        "filesBlockedBySandboxCount": 0,
        "scannedFilesCount": 0,
        "skippedFilesScanCount": 0,
        "scanFilesDistribution": {
```

```
"executablesFilesCount": 0,
          "audioVideoFilesCount": 0,
          "openSSlEncryptedFilesCount": 0,
          "pdfFilesCount": 0,
          "graphicalFilesCount": 0,
          "diskImageFilesCount": 0,
          "textFilesCount": 0,
          "mailFilesCount": 0,
          "applicationFilesCount": 0,
          "documentsFilesCount": 0,
          "otherFilesCount": 0,
          "archivesFilesCount": 0
        }
      },
      "realTimeStartDate": "2019-08-24T14:15:22Z",
      "scanSequenceDto": {
        "previousScanId": "string",
        "nextScanId": "string"
      },
      "scanPartition": "string",
      "workflowId": "string",
      "scanConfigurationId": "string",
      "errors": [
        "string"
      ],
      "priority": 0,
      "scanWorkflowSnapshotDtos": [
        {
          "id": "string",
          "scanId": "string",
          "workflow": {
            "id": "string",
            "scanPoolId": "string",
            "scanProcessFlow": 0,
            "isIdentityScanningEnabled": true,
            "scanIntervalDays": 0,
            "rules": [
              "string"
            ],
            "type": 0,
            "workflowSupportedTechnologies": {
              "dlp": {
                "status": 0
              },
              "deepCdr": {
                "status": 0
              },
              "sandBox": {
                "status": 0
              },
              "metascan": {
                "status": 0
              }
```

```
"name": "string",
            "userAgent": "string",
            "scanPool": {
              "id": "string",
              "name": "string",
              "scanPoolType": 0,
              "isDefault": true,
              "scanInstances": [
                {
                  "id": "string",
                  "scanPoolId": "string",
                  "url": "string",
                  "apiKey": "string",
                  "timeout": "string",
                  "scanInstanceType": 0
                }
              ]
            },
            "failOverScanPoolId": "string",
            "failOverScanPool": {
              "id": "string",
              "name": "string",
              "scanPoolType": 0,
              "isDefault": true,
              "scanInstances": [
                {
                  "id": "string",
                  "scanPoolId": "string",
                  "url": "string",
                  "apiKey": "string",
                  "timeout": "string",
                  "scanInstanceType": 0
                }
              ]
            },
            "filters": {
              "id": "string",
              "minimumSize": 0,
              "maximumSize": 0,
              "minimumDateTime": "2019-08-24T14:15:22Z",
              "maximumDateTime": "2019-08-24T14:15:22Z"
            },
            "fileDefinition": {
              "blockingStrategy": 0,
              "configurableBlockingStrategy": {
                "shouldTreatFilesWithSensitiveDataAsBlocked": true,
                "shouldTreatFilesWithVulnerabilitiesAsBlocked": true
              }
            },
            "remediations": [
              {
                "id": "string",
                "workflowId": "string",
```

```
"configuration": "string",
                "type": 0,
                "handlingType": 0
              }
            ],
            "tenantId": "string"
          },
          "startTimestamp": 0,
          "stopTimestamp": 0,
          "scanPool": {
            "id": "string",
            "name": "string",
            "scanPoolType": 0,
            "isDefault": true,
            "scanInstances": [
              {
                "id": "string",
                "scanPoolId": "string",
                "url": "string",
                "apiKey": "string",
                "timeout": "string",
                "scanInstanceType": 0
              }
            ]
          },
          "scanInstances": [
            {
              "id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ],
          "failOverScanPool": {
            "id": "string",
            "name": "string",
            "scanPoolType": 0,
            "isDefault": true,
            "scanInstances": [
              {
                "id": "string",
                "scanPoolId": "string",
                "url": "string",
                "apiKey": "string",
                "timeout": "string",
                "scanInstanceType": 0
              }
            ]
          },
          "failOverScanInstances": [
            {
```

```
"scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ],
          "storage": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          },
          "workflowStatistics": {
            "taggingStatistics": {
              "total": 0
            },
            "keepAllowedStatistics": {
              "total": 0
            },
            "keepBlockedStatistics": {
              "total": 0
            },
            "keepSanitizedStatistics": {
              "total": 0
            },
            "movedAllowedStatistics": {
              "total": 0,
              "destinationStorageInformation": {
                "id": "string",
                "name": "string",
                "groupId": "string",
```

```
"accountId": "string",
                "source": "string",
                "storageFunctionality": "string",
                "storageType": {
                  "name": "string",
                  "categoryType": 0,
                  "protocolType": 0,
                  "vendorType": 0
                },
                "storageStatus": {
                  "message": "string",
                  "statusType": 0
                },
                "workflowId": "string",
                "lastUpdated": "2019-08-24T14:15:22Z",
                "tenantId": "string",
                "groupRef": {
                  "id": "string",
                  "name": "string"
                },
                "isAutodiscovered": true
              }
            },
            "movedSanitizedStatistics": {
              "total": 0,
              "destinationStorageInformation": {
                "id": "string",
                "name": "string",
                "groupId": "string",
                "clientId": "string",
                "accountId": "string",
                "source": "string",
                "storageFunctionality": "string",
                "storageType": {
                  "name": "string",
                  "categoryType": 0,
                  "protocolType": 0,
                  "vendorType": 0
                },
                "storageStatus": {
                  "message": "string",
                  "statusType": 0
                },
                "workflowId": "string",
                "lastUpdated": "2019-08-24T14:15:22Z",
                "tenantId": "string",
                "groupRef": {
                  "id": "string",
                  "name": "string"
                },
                "isAutodiscovered": true
              }
            },
```

```
"total": 0,
              "destinationStorageInformation": {
                "id": "string",
                "name": "string",
                "groupId": "string",
                "clientId": "string",
                "accountId": "string",
                "source": "string",
                "storageFunctionality": "string",
                "storageType": {
                  "name": "string",
                  "categoryType": 0,
                  "protocolType": 0,
                  "vendorType": 0
                },
                "storageStatus": {
                  "message": "string",
                  "statusType": 0
                },
                "workflowId": "string",
                "lastUpdated": "2019-08-24T14:15:22Z",
                "tenantId": "string",
                "groupRef": {
                  "id": "string",
                  "name": "string"
                },
                "isAutodiscovered": true
              }
            },
            "copyAllowedStatistics": {
              "total": 0,
              "destinationStorageInformation": {
                "id": "string",
                "name": "string",
                "groupId": "string",
                "clientId": "string",
                "accountId": "string",
                "source": "string",
                "storageFunctionality": "string",
                "storageType": {
                  "name": "string",
                  "categoryType": 0,
                  "protocolType": 0,
                  "vendorType": 0
                },
                "storageStatus": {
                  "message": "string",
                  "statusType": 0
                },
                "workflowId": "string",
                "lastUpdated": "2019-08-24T14:15:22Z",
                "tenantId": "string",
                "groupRef": {
```

```
"name": "string"
                },
                "isAutodiscovered": true
              }
            },
            "copyBlockedStatistics": {
              "total": 0,
              "destinationStorageInformation": {
                "id": "string",
                "name": "string",
                "groupId": "string",
                "clientId": "string",
                "accountId": "string",
                "source": "string",
                "storageFunctionality": "string",
                "storageType": {
                  "name": "string",
                  "categoryType": 0,
                  "protocolType": 0,
                  "vendorType": 0
                },
                "storageStatus": {
                  "message": "string",
                  "statusType": 0
                },
                "workflowId": "string",
                "lastUpdated": "2019-08-24T14:15:22Z",
                "tenantId": "string",
                "groupRef": {
                  "id": "string",
                  "name": "string"
                },
                "isAutodiscovered": true
              }
            },
            "deleteAllowedStatistics": {
              "total": 0
            },
            "deleteBlockedStatistics": {
              "total": 0
            },
            "lastCalculatedStatisticsTime": "2019-08-24T14:15:22Z"
          },
          "account": {
            "id": "string",
            "name": "string",
            "description": "string",
            "credentials": "string",
            "protocolType": 0,
            "vendorType": 0,
            "autoDiscovery": true,
            "autodiscoveryDestinationGroupId": "string",
            "destinationGroup": {
```

```
"name": "string"
            }
          },
          "realTimeStartDate": "2019-08-24T14:15:22Z"
        }
      ],
      "storageId": "string",
      "discoveryCycleTiming": {
        "currentCycleStartedAt": "2019-08-24T14:15:22Z",
        "lastCycleStartedAt": "2019-08-24T14:15:22Z",
        "lastCycleFinishedAt": "2019-08-24T14:15:22Z",
        "lastCycleDurationSeconds": 0.1
      },
      "$type": "string"
    }
  ],
  "totalCount": 0
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	GetScansReportQueryResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Download PDF Report

```
GET /api/report/download/{scanId}
```

Parameters

Name	In	Type	Required	Description
TypeOfReport	query	TypeOfReport	false	none
StartIndex	query	integer(int32)	false	starting position for pagination (0-based index)
Count	query	integer(int32)	false	none
StartDate	query	string(date-time)	false	filter files by scan date
EndDate	query	string(date-time)	false	filter files by scan date
Search	query	string	false	text filter
ScanType	query	array[integer]	false	scan type such as (on-demand, scheduled, real time)
StorageId	query	array[string]	false	filter based on a list of possible storage id
ScanId	query	array[string]	false	filter based on a list of possible scan id
ScanWorkflowSnapshotId	query	array[string]	false	filter based on a list of possible scan workflow snapshot id
ProcessingState	query	array[integer]	false	none
Result	query	array[integer]	false	filter by scan result (0 = Clean, 1 = Blocked, 2 = Processing)
ScanAllResultI	query	array[integer]	false	filter by MD Core scan result (0 = NoThreatDetected, 1 = Infected, 2 = Suspicious, etc.)
ScanResultICount	query	array[integer]	false	the number of engine results that are not “No threat detected”
SandboxVerdict	query	array[integer]	false	filter by Sandbox verdict (0 = NoThreat, 1 = Malicious, 2 = Suspicious)
VulnerabilityCount	query	array[integer]	false	the number of vulnerabilities detected
HasVulnerabilities	query	boolean	false	filter by presence of vulnerabilities
DlpDetection	query	boolean	false	DLP detection

HasBlockedFileVersions	query	boolean	false	filter by presence of blocked file versions
Remediations	query	array[integer]	false	filter by remediation performed on the file
SkippedScan	query	boolean	false	filter by whether the scan was skipped
SortBy	query	array[integer]	false	none
SortOrder	query	array[integer]	false	none
Expand	query	array[string]	false	Possible values for expand: workflow_snapshot
scanId	path	string	true	none

Enumerated Values

Parameter	Value
TypeOfReport	0
TypeOfReport	1
ScanType	0
ScanType	1
ScanType	2
ProcessingState	0
ProcessingState	1
ProcessingState	2
ProcessingState	3
ProcessingState	4
Result	0
Result	1
Result	2
ScanAllResultI	0
ScanAllResultI	1
ScanAllResultI	2
ScanAllResultI	3
ScanAllResultI	7
ScanAllResultI	8
ScanAllResultI	9
ScanAllResultI	10
ScanAllResultI	12
ScanAllResultI	13
ScanAllResultI	14
ScanAllResultI	15
ScanAllResultI	16
ScanAllResultI	17

ScanAllResultI	18
ScanAllResultI	19
ScanAllResultI	20
ScanAllResultI	21
ScanAllResultI	22
ScanAllResultI	23
ScanAllResultI	24
ScanAllResultI	25
ScanAllResultI	26
ScanAllResultI	27
ScanAllResultI	28
ScanAllResultI	29
ScanAllResultI	30
ScanAllResultI	31
ScanAllResultI	32
ScanAllResultI	33
ScanAllResultI	34
ScanAllResultI	36
ScanAllResultI	38
ScanAllResultI	39
ScanAllResultI	40
ScanAllResultI	41
ScanAllResultI	42
ScanAllResultI	43
ScanAllResultI	255
ScanAllResultI	1014
ScanAllResultI	9999
SandboxVerdict	0
SandboxVerdict	1

SandboxVerdict	2
SandboxVerdict	3
SandboxVerdict	4
SandboxVerdict	5
SandboxVerdict	999
Remediations	0
Remediations	5
Remediations	6
Remediations	7
Remediations	8
Remediations	9
Remediations	10
Remediations	11
Remediations	12
Remediations	13
Remediations	14
Remediations	15
Remediations	16
Remediations	17
Remediations	18
Remediations	19
Remediations	20
Remediations	21
Remediations	22
Remediations	23
Remediations	24
Remediations	25
Remediations	26
Remediations	27

Remediations	28
Remediations	29
Remediations	30
Remediations	31
Remediations	32
Remediations	33
Remediations	100
Remediations	101
Remediations	102
SortBy	0
SortBy	1
SortBy	2
SortBy	3
SortBy	4
SortBy	5
SortBy	6
SortBy	7
SortBy	8
SortOrder	0
SortOrder	1

Example responses

200 Response

Responses

Status	Meaning	Description	Schema
200	OK	none	string

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Scan

Manage your scans

Get scan by ID

`GET /api/scan/{scanId}`

Parameters

Name	In	Type	Required	Description
scanId	path	string	true	none

> Example responses

> 200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "scan": {
    "result": 0,
    "responseKey": "string",
    "responseMessage": "string",
    "responseMessageParams": {
      "property1": "string",
      "property2": "string"
    },
    "id": "string",
    "name": "string",
    "startTime": "2019-08-24T14:15:22Z",
    "stopTime": "2019-08-24T14:15:22Z",
    "scanType": "string",
    "scanningState": 0,
    "scanStatusDto": {
      "pendingFilesCount": 0,
      "pendingFilesSize": 0,
      "allowedFilesCount": 0,
      "allowedFilesSize": 0,
      "blockedFilesCount": 0,
      "blockedFilesSize": 0,
      "sanitizedFilesCount": 0,
      "failedSanitizedFilesCount": 0,
      "remediatedFilesCount": 0,
      "totalFilesCount": 0,
      "totalFilesSize": 0,
      "processingFailedCount": 0,
      "processingFailedSize": 0,
      "processingFailedRemediationCount": 0,
      "processedFilesCount": 0,
      "processedFilesSize": 0,
      "canceledFilesCount": 0,
      "canceledFilesSize": 0
    },
    "scanStatsDto": {
      "infectedFilesCount": 0,
      "threatTotalFilesCount": 0,
      "filesWithVulnerabilitiesCount": 0,
      "filesWithSensitiveDataCount": 0,
      "filesBlockedBySandboxCount": 0,
      "scannedFilesCount": 0,
      "skippedFilesScanCount": 0,
      "scanFilesDistribution": {
        "documentsEncryptedFilesCount": 0,
```

```
"audioVideoFilesCount": 0,
        "openSSlEncryptedFilesCount": 0,
        "pdfFilesCount": 0,
        "graphicalFilesCount": 0,
        "diskImageFilesCount": 0,
        "textFilesCount": 0,
        "mailFilesCount": 0,
        "applicationFilesCount": 0,
        "documentsFilesCount": 0,
        "otherFilesCount": 0,
        "archivesFilesCount": 0
      }
    },
    "realTimeStartDate": "2019-08-24T14:15:22Z",
    "scanSequenceDto": {
      "previousScanId": "string",
      "nextScanId": "string"
    },
    "scanPartition": "string",
    "workflowId": "string",
    "scanConfigurationId": "string",
    "errors": [
      "string"
    ],
    "priority": 0,
    "scanWorkflowSnapshotDtos": [
      {
        "id": "string",
        "scanId": "string",
        "workflow": {
          "id": "string",
          "scanPoolId": "string",
          "scanProcessFlow": 0,
          "isIdentityScanningEnabled": true,
          "scanIntervalDays": 0,
          "rules": [
            "string"
          ],
          "type": 0,
          "workflowSupportedTechnologies": {
            "dlp": {
              "status": 0
            },
            "deepCdr": {
              "status": 0
            },
            "sandBox": {
              "status": 0
            },
            "metascan": {
              "status": 0
            }
          },
```

```
"userAgent": "string",
          "scanPool": {
            "id": "string",
            "name": "string",
            "scanPoolType": 0,
            "isDefault": true,
            "scanInstances": [
              {
                "id": "string",
                "scanPoolId": "string",
                "url": "string",
                "apiKey": "string",
                "timeout": "string",
                "scanInstanceType": 0
              }
            ]
          },
          "failOverScanPoolId": "string",
          "failOverScanPool": {
            "id": "string",
            "name": "string",
            "scanPoolType": 0,
            "isDefault": true,
            "scanInstances": [
              {
                "id": "string",
                "scanPoolId": "string",
                "url": "string",
                "apiKey": "string",
                "timeout": "string",
                "scanInstanceType": 0
              }
            ]
          },
          "filters": {
            "id": "string",
            "minimumSize": 0,
            "maximumSize": 0,
            "minimumDateTime": "2019-08-24T14:15:22Z",
            "maximumDateTime": "2019-08-24T14:15:22Z"
          },
          "fileDefinition": {
            "blockingStrategy": 0,
            "configurableBlockingStrategy": {
              "shouldTreatFilesWithSensitiveDataAsBlocked": true,
              "shouldTreatFilesWithVulnerabilitiesAsBlocked": true
            }
          },
          "remediations": [
            {
              "id": "string",
              "workflowId": "string",
              "isEnabled": true,
```

```
"type": 0,
              "handlingType": 0
            }
          ],
          "tenantId": "string"
        },
        "startTimestamp": 0,
        "stopTimestamp": 0,
        "scanPool": {
          "id": "string",
          "name": "string",
          "scanPoolType": 0,
          "isDefault": true,
          "scanInstances": [
            {
              "id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ]
        },
        "scanInstances": [
          {
            "id": "string",
            "scanPoolId": "string",
            "url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ],
        "failOverScanPool": {
          "id": "string",
          "name": "string",
          "scanPoolType": 0,
          "isDefault": true,
          "scanInstances": [
            {
              "id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ]
        },
        "failOverScanInstances": [
          {
            "id": "string",
```

```
"url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ],
        "storage": {
          "id": "string",
          "name": "string",
          "groupId": "string",
          "clientId": "string",
          "accountId": "string",
          "source": "string",
          "storageFunctionality": "string",
          "storageType": {
            "name": "string",
            "categoryType": 0,
            "protocolType": 0,
            "vendorType": 0
          },
          "storageStatus": {
            "message": "string",
            "statusType": 0
          },
          "workflowId": "string",
          "lastUpdated": "2019-08-24T14:15:22Z",
          "tenantId": "string",
          "groupRef": {
            "id": "string",
            "name": "string"
          },
          "isAutodiscovered": true
        },
        "workflowStatistics": {
          "taggingStatistics": {
            "total": 0
          },
          "keepAllowedStatistics": {
            "total": 0
          },
          "keepBlockedStatistics": {
            "total": 0
          },
          "keepSanitizedStatistics": {
            "total": 0
          },
          "movedAllowedStatistics": {
            "total": 0,
            "destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
```

```
"source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "movedSanitizedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "movedBlockedStatistics": {
```

```
"destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
              "accountId": "string",
              "source": "string",
              "storageFunctionality": "string",
              "storageType": {
                "name": "string",
                "categoryType": 0,
                "protocolType": 0,
                "vendorType": 0
              },
              "storageStatus": {
                "message": "string",
                "statusType": 0
              },
              "workflowId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z",
              "tenantId": "string",
              "groupRef": {
                "id": "string",
                "name": "string"
              },
              "isAutodiscovered": true
            }
          },
          "copyAllowedStatistics": {
            "total": 0,
            "destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
              "accountId": "string",
              "source": "string",
              "storageFunctionality": "string",
              "storageType": {
                "name": "string",
                "categoryType": 0,
                "protocolType": 0,
                "vendorType": 0
              },
              "storageStatus": {
                "message": "string",
                "statusType": 0
              },
              "workflowId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z",
              "tenantId": "string",
              "groupRef": {
                "id": "string",
```

```
},
              "isAutodiscovered": true
            }
          },
          "copyBlockedStatistics": {
            "total": 0,
            "destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
              "accountId": "string",
              "source": "string",
              "storageFunctionality": "string",
              "storageType": {
                "name": "string",
                "categoryType": 0,
                "protocolType": 0,
                "vendorType": 0
              },
              "storageStatus": {
                "message": "string",
                "statusType": 0
              },
              "workflowId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z",
              "tenantId": "string",
              "groupRef": {
                "id": "string",
                "name": "string"
              },
              "isAutodiscovered": true
            }
          },
          "deleteAllowedStatistics": {
            "total": 0
          },
          "deleteBlockedStatistics": {
            "total": 0
          },
          "lastCalculatedStatisticsTime": "2019-08-24T14:15:22Z"
        },
        "account": {
          "id": "string",
          "name": "string",
          "description": "string",
          "credentials": "string",
          "protocolType": 0,
          "vendorType": 0,
          "autoDiscovery": true,
          "autodiscoveryDestinationGroupId": "string",
          "destinationGroup": {
            "id": "string",
```

```
}
        },
        "realTimeStartDate": "2019-08-24T14:15:22Z"
      }
    ],
    "storageId": "string",
    "discoveryCycleTiming": {
      "currentCycleStartedAt": "2019-08-24T14:15:22Z",
      "lastCycleStartedAt": "2019-08-24T14:15:22Z",
      "lastCycleFinishedAt": "2019-08-24T14:15:22Z",
      "lastCycleDurationSeconds": 0.1
    },
    "$type": "string"
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	GetScanByIdQueryResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Start a scan

`POST /api/scan/start`

To scan a specific folder using the optional Folder parameter, provide the absolute folder path: For Amazon S3 / S3 Compatible Types, Azure Blob, Azure Files, Google Cloud, Alibaba Cloud and Oracle Native: Including the Folder Location integrated in MDSS and excluding the Bucket Name, Container, etc. For Box: With or without the “All Files” folder For Sharepoint and Onedrive: Excluding the Document Library, Site, or Group For OPSWAT MFT Storage: The desired Folder Path when integrating with user For NFS / SMB / SFTP / FTP / SharePoint OnPrem: Only the folder path beyond your configured storage root (do not include the base path set during integration) Provide the absolute folder path in the following format "{"Folder":"PATH_TO_SCAN"}

> Body parameter

```
{
  "storageId": "string",
  "name": "string",
  "folder": "string",
  "scanPartition": "string",
  "priority": 0,
  "storageIds": [
    "string"
  ],
  "workflowId": "string",
  "mdssBaseUrl": "string",
  "scanConfigDto": {
    "realTimeScanConfig": {
      "isEnabled": true,
      "startDate": "2019-08-24T14:15:22Z",
      "handlingType": 0
    }
  }
}
```


Parameters

Name	In	Type	Required	Description
body	body	AddScanParameters	true	none

Example responses

200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "scanId": "string",
  "scanIds": [
    "string"
  ],
  "failedStorages": [
    {
      "id": "string",
      "reasonKey": "string",
      "reason": "string",
      "childFailures": [
        {}
      ]
    }
  ]
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	StartScanCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Stop a scan

`POST /api/scan/stop/{scanId}`

Parameters

Name	In	Type	Required	Description
scanId	path	string	true	none

Example responses

> 200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "dispatched": [
    "string"
  ],
  "failed": [
    {
      "id": "string",
      "reasonKey": "string",
      "reason": "string",
      "childFailures": [
        {}
      ]
    }
  ]
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	BulkStopScansCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Bulk delete scans

`DELETE /api/scan`

Deletes up to 100 scan records across any storages the caller can access. Per-scan ABAC is enforced and inaccessible scan IDs are returned in the failed list with a localized reason. Partial-delete model — running scans are NOT a hard block: they are returned in the failed list with reasonKey BULK_OPERATION_SCAN_RUNNING while the rest of the batch is deleted normally.

> Body parameter

```
{
  "scanIds": [
    "string"
  ],
  "forceDeleteRtp": true
}
```

Parameters

Name	In	Type	Required	Description
body	body	BulkDeleteScansParameters	true	none

Example responses

200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "succeeded": [
    "string"
  ],
  "failed": [
    {
      "id": "string",
      "reasonKey": "string",
      "reason": "string",
      "childFailures": [
        {}
      ]
    }
  ]
}
```

Responses

Status	Meaning	Description	Schema
200	OK	none	BulkDeleteScansCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Bulk stop scans

`POST /api/scan/stop`

Dispatches stop signals for up to 100 scans in a single request. Per-scan ABAC is enforced and inaccessible scan IDs are returned in the failed list with a localized reason. Stop is fire-and-forget — the response field 'dispatched' contains the scan IDs for which a stop signal was queued; the actual transition to Cancelled happens asynchronously.

> Body parameter

```
{
  "scanIds": [
    "string"
  ]
}
```

Parameters

Name	In	Type	Required	Description
body	body	BulkStopScansParameters	true	none

> Example responses

> 200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "dispatched": [
    "string"
  ],
  "failed": [
    {
      "id": "string",
      "reasonKey": "string",
      "reason": "string",
      "childFailures": [
        {}
      ]
    }
  ]
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	BulkStopScansCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Delete scans

`DELETE /api/scan/{storageId}`

> Body parameter


```
[
  "string"
]
```

Parameters

Name	In	Type	Required	Description
storageId	path	string	true	none
forceDeleteRtp	query	boolean	false	none
body	body	array[string]	true	none

Example responses

200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "succeeded": [
    "string"
  ],
  "failed": [
    {
      "id": "string",
      "reasonKey": "string",
      "reason": "string",
      "childFailures": [
        {}
      ]
    }
  ]
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	BulkDeleteScansCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Fetch last completed scan

`GET /api/scan/last_completed/{storageId}`

Parameters

Name	In	Type	Required	Description
storageId	path	string	true	none

Example responses

200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "scan": {
    "result": 0,
    "responseKey": "string",
    "responseMessage": "string",
    "responseMessageParams": {
      "property1": "string",
      "property2": "string"
    },
    "id": "string",
    "name": "string",
    "startTime": "2019-08-24T14:15:22Z",
    "stopTime": "2019-08-24T14:15:22Z",
    "scanType": "string",
    "scanningState": 0,
    "scanStatusDto": {
      "pendingFilesCount": 0,
      "pendingFilesSize": 0,
      "allowedFilesCount": 0,
      "allowedFilesSize": 0,
      "blockedFilesCount": 0,
      "blockedFilesSize": 0,
      "sanitizedFilesCount": 0,
      "failedSanitizedFilesCount": 0,
      "remediatedFilesCount": 0,
      "totalFilesCount": 0,
      "totalFilesSize": 0,
      "processingFailedCount": 0,
      "processingFailedSize": 0,
      "processingFailedRemediationCount": 0,
      "processedFilesCount": 0,
      "processedFilesSize": 0,
      "canceledFilesCount": 0,
      "canceledFilesSize": 0
    },
    "scanStatsDto": {
      "infectedFilesCount": 0,
      "threatTotalFilesCount": 0,
      "filesWithVulnerabilitiesCount": 0,
      "filesWithSensitiveDataCount": 0,
      "filesBlockedBySandboxCount": 0,
      "scannedFilesCount": 0,
      "skippedFilesScanCount": 0,
      "scanFilesDistribution": {
        "documentsEncryptedFilesCount": 0,
```

```
"audioVideoFilesCount": 0,
        "openSSlEncryptedFilesCount": 0,
        "pdfFilesCount": 0,
        "graphicalFilesCount": 0,
        "diskImageFilesCount": 0,
        "textFilesCount": 0,
        "mailFilesCount": 0,
        "applicationFilesCount": 0,
        "documentsFilesCount": 0,
        "otherFilesCount": 0,
        "archivesFilesCount": 0
      }
    },
    "realTimeStartDate": "2019-08-24T14:15:22Z",
    "scanSequenceDto": {
      "previousScanId": "string",
      "nextScanId": "string"
    },
    "scanPartition": "string",
    "workflowId": "string",
    "scanConfigurationId": "string",
    "errors": [
      "string"
    ],
    "priority": 0,
    "scanWorkflowSnapshotDtos": [
      {
        "id": "string",
        "scanId": "string",
        "workflow": {
          "id": "string",
          "scanPoolId": "string",
          "scanProcessFlow": 0,
          "isIdentityScanningEnabled": true,
          "scanIntervalDays": 0,
          "rules": [
            "string"
          ],
          "type": 0,
          "workflowSupportedTechnologies": {
            "dlp": {
              "status": 0
            },
            "deepCdr": {
              "status": 0
            },
            "sandBox": {
              "status": 0
            },
            "metascan": {
              "status": 0
            }
          },
```

```
"userAgent": "string",
          "scanPool": {
            "id": "string",
            "name": "string",
            "scanPoolType": 0,
            "isDefault": true,
            "scanInstances": [
              {
                "id": "string",
                "scanPoolId": "string",
                "url": "string",
                "apiKey": "string",
                "timeout": "string",
                "scanInstanceType": 0
              }
            ]
          },
          "failOverScanPoolId": "string",
          "failOverScanPool": {
            "id": "string",
            "name": "string",
            "scanPoolType": 0,
            "isDefault": true,
            "scanInstances": [
              {
                "id": "string",
                "scanPoolId": "string",
                "url": "string",
                "apiKey": "string",
                "timeout": "string",
                "scanInstanceType": 0
              }
            ]
          },
          "filters": {
            "id": "string",
            "minimumSize": 0,
            "maximumSize": 0,
            "minimumDateTime": "2019-08-24T14:15:22Z",
            "maximumDateTime": "2019-08-24T14:15:22Z"
          },
          "fileDefinition": {
            "blockingStrategy": 0,
            "configurableBlockingStrategy": {
              "shouldTreatFilesWithSensitiveDataAsBlocked": true,
              "shouldTreatFilesWithVulnerabilitiesAsBlocked": true
            }
          },
          "remediations": [
            {
              "id": "string",
              "workflowId": "string",
              "isEnabled": true,
```

```
"type": 0,
              "handlingType": 0
            }
          ],
          "tenantId": "string"
        },
        "startTimestamp": 0,
        "stopTimestamp": 0,
        "scanPool": {
          "id": "string",
          "name": "string",
          "scanPoolType": 0,
          "isDefault": true,
          "scanInstances": [
            {
              "id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ]
        },
        "scanInstances": [
          {
            "id": "string",
            "scanPoolId": "string",
            "url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ],
        "failOverScanPool": {
          "id": "string",
          "name": "string",
          "scanPoolType": 0,
          "isDefault": true,
          "scanInstances": [
            {
              "id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ]
        },
        "failOverScanInstances": [
          {
            "id": "string",
```

```
"url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ],
        "storage": {
          "id": "string",
          "name": "string",
          "groupId": "string",
          "clientId": "string",
          "accountId": "string",
          "source": "string",
          "storageFunctionality": "string",
          "storageType": {
            "name": "string",
            "categoryType": 0,
            "protocolType": 0,
            "vendorType": 0
          },
          "storageStatus": {
            "message": "string",
            "statusType": 0
          },
          "workflowId": "string",
          "lastUpdated": "2019-08-24T14:15:22Z",
          "tenantId": "string",
          "groupRef": {
            "id": "string",
            "name": "string"
          },
          "isAutodiscovered": true
        },
        "workflowStatistics": {
          "taggingStatistics": {
            "total": 0
          },
          "keepAllowedStatistics": {
            "total": 0
          },
          "keepBlockedStatistics": {
            "total": 0
          },
          "keepSanitizedStatistics": {
            "total": 0
          },
          "movedAllowedStatistics": {
            "total": 0,
            "destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
```

```
"source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "movedSanitizedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "movedBlockedStatistics": {
```

```
"destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
              "accountId": "string",
              "source": "string",
              "storageFunctionality": "string",
              "storageType": {
                "name": "string",
                "categoryType": 0,
                "protocolType": 0,
                "vendorType": 0
              },
              "storageStatus": {
                "message": "string",
                "statusType": 0
              },
              "workflowId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z",
              "tenantId": "string",
              "groupRef": {
                "id": "string",
                "name": "string"
              },
              "isAutodiscovered": true
            }
          },
          "copyAllowedStatistics": {
            "total": 0,
            "destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
              "accountId": "string",
              "source": "string",
              "storageFunctionality": "string",
              "storageType": {
                "name": "string",
                "categoryType": 0,
                "protocolType": 0,
                "vendorType": 0
              },
              "storageStatus": {
                "message": "string",
                "statusType": 0
              },
              "workflowId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z",
              "tenantId": "string",
              "groupRef": {
                "id": "string",
```

```
},
              "isAutodiscovered": true
            }
          },
          "copyBlockedStatistics": {
            "total": 0,
            "destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
              "accountId": "string",
              "source": "string",
              "storageFunctionality": "string",
              "storageType": {
                "name": "string",
                "categoryType": 0,
                "protocolType": 0,
                "vendorType": 0
              },
              "storageStatus": {
                "message": "string",
                "statusType": 0
              },
              "workflowId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z",
              "tenantId": "string",
              "groupRef": {
                "id": "string",
                "name": "string"
              },
              "isAutodiscovered": true
            }
          },
          "deleteAllowedStatistics": {
            "total": 0
          },
          "deleteBlockedStatistics": {
            "total": 0
          },
          "lastCalculatedStatisticsTime": "2019-08-24T14:15:22Z"
        },
        "account": {
          "id": "string",
          "name": "string",
          "description": "string",
          "credentials": "string",
          "protocolType": 0,
          "vendorType": 0,
          "autoDiscovery": true,
          "autodiscoveryDestinationGroupId": "string",
          "destinationGroup": {
            "id": "string",
```

```
}
        },
        "realTimeStartDate": "2019-08-24T14:15:22Z"
      }
    ],
    "storageId": "string",
    "discoveryCycleTiming": {
      "currentCycleStartedAt": "2019-08-24T14:15:22Z",
      "lastCycleStartedAt": "2019-08-24T14:15:22Z",
      "lastCycleFinishedAt": "2019-08-24T14:15:22Z",
      "lastCycleDurationSeconds": 0.1
    },
    "$type": "string"
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	GetLastCompletedScanQueryResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Get an active scan by scan ID

`GET /api/scan/active/{scanId}`

Parameters

Name	In	Type	Required	Description
scanId	path	string	true	none

> Example responses

> 200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "scan": {
    "result": 0,
    "responseKey": "string",
    "responseMessage": "string",
    "responseMessageParams": {
      "property1": "string",
      "property2": "string"
    },
    "id": "string",
    "name": "string",
    "startTime": "2019-08-24T14:15:22Z",
    "stopTime": "2019-08-24T14:15:22Z",
    "scanType": "string",
    "scanningState": 0,
    "scanStatusDto": {
      "pendingFilesCount": 0,
      "pendingFilesSize": 0,
      "allowedFilesCount": 0,
      "allowedFilesSize": 0,
      "blockedFilesCount": 0,
      "blockedFilesSize": 0,
      "sanitizedFilesCount": 0,
      "failedSanitizedFilesCount": 0,
      "remediatedFilesCount": 0,
      "totalFilesCount": 0,
      "totalFilesSize": 0,
      "processingFailedCount": 0,
      "processingFailedSize": 0,
      "processingFailedRemediationCount": 0,
      "processedFilesCount": 0,
      "processedFilesSize": 0,
      "canceledFilesCount": 0,
      "canceledFilesSize": 0
    },
    "scanStatsDto": {
      "infectedFilesCount": 0,
      "threatTotalFilesCount": 0,
      "filesWithVulnerabilitiesCount": 0,
      "filesWithSensitiveDataCount": 0,
      "filesBlockedBySandboxCount": 0,
      "scannedFilesCount": 0,
      "skippedFilesScanCount": 0,
      "scanFilesDistribution": {
        "documentsEncryptedFilesCount": 0,
```

```
"audioVideoFilesCount": 0,
        "openSSlEncryptedFilesCount": 0,
        "pdfFilesCount": 0,
        "graphicalFilesCount": 0,
        "diskImageFilesCount": 0,
        "textFilesCount": 0,
        "mailFilesCount": 0,
        "applicationFilesCount": 0,
        "documentsFilesCount": 0,
        "otherFilesCount": 0,
        "archivesFilesCount": 0
      }
    },
    "realTimeStartDate": "2019-08-24T14:15:22Z",
    "scanSequenceDto": {
      "previousScanId": "string",
      "nextScanId": "string"
    },
    "scanPartition": "string",
    "workflowId": "string",
    "scanConfigurationId": "string",
    "errors": [
      "string"
    ],
    "priority": 0,
    "scanWorkflowSnapshotDtos": [
      {
        "id": "string",
        "scanId": "string",
        "workflow": {
          "id": "string",
          "scanPoolId": "string",
          "scanProcessFlow": 0,
          "isIdentityScanningEnabled": true,
          "scanIntervalDays": 0,
          "rules": [
            "string"
          ],
          "type": 0,
          "workflowSupportedTechnologies": {
            "dlp": {
              "status": 0
            },
            "deepCdr": {
              "status": 0
            },
            "sandBox": {
              "status": 0
            },
            "metascan": {
              "status": 0
            }
          },
```

```
"userAgent": "string",
          "scanPool": {
            "id": "string",
            "name": "string",
            "scanPoolType": 0,
            "isDefault": true,
            "scanInstances": [
              {
                "id": "string",
                "scanPoolId": "string",
                "url": "string",
                "apiKey": "string",
                "timeout": "string",
                "scanInstanceType": 0
              }
            ]
          },
          "failOverScanPoolId": "string",
          "failOverScanPool": {
            "id": "string",
            "name": "string",
            "scanPoolType": 0,
            "isDefault": true,
            "scanInstances": [
              {
                "id": "string",
                "scanPoolId": "string",
                "url": "string",
                "apiKey": "string",
                "timeout": "string",
                "scanInstanceType": 0
              }
            ]
          },
          "filters": {
            "id": "string",
            "minimumSize": 0,
            "maximumSize": 0,
            "minimumDateTime": "2019-08-24T14:15:22Z",
            "maximumDateTime": "2019-08-24T14:15:22Z"
          },
          "fileDefinition": {
            "blockingStrategy": 0,
            "configurableBlockingStrategy": {
              "shouldTreatFilesWithSensitiveDataAsBlocked": true,
              "shouldTreatFilesWithVulnerabilitiesAsBlocked": true
            }
          },
          "remediations": [
            {
              "id": "string",
              "workflowId": "string",
              "isEnabled": true,
```

```
"type": 0,
              "handlingType": 0
            }
          ],
          "tenantId": "string"
        },
        "startTimestamp": 0,
        "stopTimestamp": 0,
        "scanPool": {
          "id": "string",
          "name": "string",
          "scanPoolType": 0,
          "isDefault": true,
          "scanInstances": [
            {
              "id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ]
        },
        "scanInstances": [
          {
            "id": "string",
            "scanPoolId": "string",
            "url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ],
        "failOverScanPool": {
          "id": "string",
          "name": "string",
          "scanPoolType": 0,
          "isDefault": true,
          "scanInstances": [
            {
              "id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ]
        },
        "failOverScanInstances": [
          {
            "id": "string",
```

```
"url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ],
        "storage": {
          "id": "string",
          "name": "string",
          "groupId": "string",
          "clientId": "string",
          "accountId": "string",
          "source": "string",
          "storageFunctionality": "string",
          "storageType": {
            "name": "string",
            "categoryType": 0,
            "protocolType": 0,
            "vendorType": 0
          },
          "storageStatus": {
            "message": "string",
            "statusType": 0
          },
          "workflowId": "string",
          "lastUpdated": "2019-08-24T14:15:22Z",
          "tenantId": "string",
          "groupRef": {
            "id": "string",
            "name": "string"
          },
          "isAutodiscovered": true
        },
        "workflowStatistics": {
          "taggingStatistics": {
            "total": 0
          },
          "keepAllowedStatistics": {
            "total": 0
          },
          "keepBlockedStatistics": {
            "total": 0
          },
          "keepSanitizedStatistics": {
            "total": 0
          },
          "movedAllowedStatistics": {
            "total": 0,
            "destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
```

```
"source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "movedSanitizedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "movedBlockedStatistics": {
```

```
"destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
              "accountId": "string",
              "source": "string",
              "storageFunctionality": "string",
              "storageType": {
                "name": "string",
                "categoryType": 0,
                "protocolType": 0,
                "vendorType": 0
              },
              "storageStatus": {
                "message": "string",
                "statusType": 0
              },
              "workflowId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z",
              "tenantId": "string",
              "groupRef": {
                "id": "string",
                "name": "string"
              },
              "isAutodiscovered": true
            }
          },
          "copyAllowedStatistics": {
            "total": 0,
            "destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
              "accountId": "string",
              "source": "string",
              "storageFunctionality": "string",
              "storageType": {
                "name": "string",
                "categoryType": 0,
                "protocolType": 0,
                "vendorType": 0
              },
              "storageStatus": {
                "message": "string",
                "statusType": 0
              },
              "workflowId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z",
              "tenantId": "string",
              "groupRef": {
                "id": "string",
```

```
},
              "isAutodiscovered": true
            }
          },
          "copyBlockedStatistics": {
            "total": 0,
            "destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
              "accountId": "string",
              "source": "string",
              "storageFunctionality": "string",
              "storageType": {
                "name": "string",
                "categoryType": 0,
                "protocolType": 0,
                "vendorType": 0
              },
              "storageStatus": {
                "message": "string",
                "statusType": 0
              },
              "workflowId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z",
              "tenantId": "string",
              "groupRef": {
                "id": "string",
                "name": "string"
              },
              "isAutodiscovered": true
            }
          },
          "deleteAllowedStatistics": {
            "total": 0
          },
          "deleteBlockedStatistics": {
            "total": 0
          },
          "lastCalculatedStatisticsTime": "2019-08-24T14:15:22Z"
        },
        "account": {
          "id": "string",
          "name": "string",
          "description": "string",
          "credentials": "string",
          "protocolType": 0,
          "vendorType": 0,
          "autoDiscovery": true,
          "autodiscoveryDestinationGroupId": "string",
          "destinationGroup": {
            "id": "string",
```

```
}
        },
        "realTimeStartDate": "2019-08-24T14:15:22Z"
      }
    ],
    "storageId": "string",
    "discoveryCycleTiming": {
      "currentCycleStartedAt": "2019-08-24T14:15:22Z",
      "lastCycleStartedAt": "2019-08-24T14:15:22Z",
      "lastCycleFinishedAt": "2019-08-24T14:15:22Z",
      "lastCycleDurationSeconds": 0.1
    },
    "$type": "string",
    "serviceName": "string",
    "storageName": "string",
    "currentProcessingFilePath": "string",
    "currentProcessingFileProgress": "string",
    "discoveryState": 0,
    "statusMessages": [
      {
        "message": "string",
        "severity": 0,
        "params": {
          "property1": "string",
          "property2": "string"
        }
      }
    ]
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	GetActiveScanQueryResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Get Real-Time scan by storage Id

```
GET /api/scan/realtime/{storageId}
```

Parameters

Name	In	Type	Required	Description
storageId	path	string	true	none
scanPartition	query	string	false	none

Example responses

200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "scan": {
    "result": 0,
    "responseKey": "string",
    "responseMessage": "string",
    "responseMessageParams": {
      "property1": "string",
      "property2": "string"
    },
    "id": "string",
    "name": "string",
    "startTime": "2019-08-24T14:15:22Z",
    "stopTime": "2019-08-24T14:15:22Z",
    "scanType": "string",
    "scanningState": 0,
    "scanStatusDto": {
      "pendingFilesCount": 0,
      "pendingFilesSize": 0,
      "allowedFilesCount": 0,
      "allowedFilesSize": 0,
      "blockedFilesCount": 0,
      "blockedFilesSize": 0,
      "sanitizedFilesCount": 0,
      "failedSanitizedFilesCount": 0,
      "remediatedFilesCount": 0,
      "totalFilesCount": 0,
      "totalFilesSize": 0,
      "processingFailedCount": 0,
      "processingFailedSize": 0,
      "processingFailedRemediationCount": 0,
      "processedFilesCount": 0,
      "processedFilesSize": 0,
      "canceledFilesCount": 0,
      "canceledFilesSize": 0
    },
    "scanStatsDto": {
      "infectedFilesCount": 0,
      "threatTotalFilesCount": 0,
      "filesWithVulnerabilitiesCount": 0,
      "filesWithSensitiveDataCount": 0,
      "filesBlockedBySandboxCount": 0,
      "scannedFilesCount": 0,
      "skippedFilesScanCount": 0,
      "scanFilesDistribution": {
        "documentsEncryptedFilesCount": 0,
```

```
"audioVideoFilesCount": 0,
        "openSSlEncryptedFilesCount": 0,
        "pdfFilesCount": 0,
        "graphicalFilesCount": 0,
        "diskImageFilesCount": 0,
        "textFilesCount": 0,
        "mailFilesCount": 0,
        "applicationFilesCount": 0,
        "documentsFilesCount": 0,
        "otherFilesCount": 0,
        "archivesFilesCount": 0
      }
    },
    "realTimeStartDate": "2019-08-24T14:15:22Z",
    "scanSequenceDto": {
      "previousScanId": "string",
      "nextScanId": "string"
    },
    "scanPartition": "string",
    "workflowId": "string",
    "scanConfigurationId": "string",
    "errors": [
      "string"
    ],
    "priority": 0,
    "scanWorkflowSnapshotDtos": [
      {
        "id": "string",
        "scanId": "string",
        "workflow": {
          "id": "string",
          "scanPoolId": "string",
          "scanProcessFlow": 0,
          "isIdentityScanningEnabled": true,
          "scanIntervalDays": 0,
          "rules": [
            "string"
          ],
          "type": 0,
          "workflowSupportedTechnologies": {
            "dlp": {
              "status": 0
            },
            "deepCdr": {
              "status": 0
            },
            "sandBox": {
              "status": 0
            },
            "metascan": {
              "status": 0
            }
          },
```

```
"userAgent": "string",
          "scanPool": {
            "id": "string",
            "name": "string",
            "scanPoolType": 0,
            "isDefault": true,
            "scanInstances": [
              {
                "id": "string",
                "scanPoolId": "string",
                "url": "string",
                "apiKey": "string",
                "timeout": "string",
                "scanInstanceType": 0
              }
            ]
          },
          "failOverScanPoolId": "string",
          "failOverScanPool": {
            "id": "string",
            "name": "string",
            "scanPoolType": 0,
            "isDefault": true,
            "scanInstances": [
              {
                "id": "string",
                "scanPoolId": "string",
                "url": "string",
                "apiKey": "string",
                "timeout": "string",
                "scanInstanceType": 0
              }
            ]
          },
          "filters": {
            "id": "string",
            "minimumSize": 0,
            "maximumSize": 0,
            "minimumDateTime": "2019-08-24T14:15:22Z",
            "maximumDateTime": "2019-08-24T14:15:22Z"
          },
          "fileDefinition": {
            "blockingStrategy": 0,
            "configurableBlockingStrategy": {
              "shouldTreatFilesWithSensitiveDataAsBlocked": true,
              "shouldTreatFilesWithVulnerabilitiesAsBlocked": true
            }
          },
          "remediations": [
            {
              "id": "string",
              "workflowId": "string",
              "isEnabled": true,
```

```
"type": 0,
              "handlingType": 0
            }
          ],
          "tenantId": "string"
        },
        "startTimestamp": 0,
        "stopTimestamp": 0,
        "scanPool": {
          "id": "string",
          "name": "string",
          "scanPoolType": 0,
          "isDefault": true,
          "scanInstances": [
            {
              "id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ]
        },
        "scanInstances": [
          {
            "id": "string",
            "scanPoolId": "string",
            "url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ],
        "failOverScanPool": {
          "id": "string",
          "name": "string",
          "scanPoolType": 0,
          "isDefault": true,
          "scanInstances": [
            {
              "id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ]
        },
        "failOverScanInstances": [
          {
            "id": "string",
```

```
"url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ],
        "storage": {
          "id": "string",
          "name": "string",
          "groupId": "string",
          "clientId": "string",
          "accountId": "string",
          "source": "string",
          "storageFunctionality": "string",
          "storageType": {
            "name": "string",
            "categoryType": 0,
            "protocolType": 0,
            "vendorType": 0
          },
          "storageStatus": {
            "message": "string",
            "statusType": 0
          },
          "workflowId": "string",
          "lastUpdated": "2019-08-24T14:15:22Z",
          "tenantId": "string",
          "groupRef": {
            "id": "string",
            "name": "string"
          },
          "isAutodiscovered": true
        },
        "workflowStatistics": {
          "taggingStatistics": {
            "total": 0
          },
          "keepAllowedStatistics": {
            "total": 0
          },
          "keepBlockedStatistics": {
            "total": 0
          },
          "keepSanitizedStatistics": {
            "total": 0
          },
          "movedAllowedStatistics": {
            "total": 0,
            "destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
```

```
"source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "movedSanitizedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "movedBlockedStatistics": {
```

```
"destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
              "accountId": "string",
              "source": "string",
              "storageFunctionality": "string",
              "storageType": {
                "name": "string",
                "categoryType": 0,
                "protocolType": 0,
                "vendorType": 0
              },
              "storageStatus": {
                "message": "string",
                "statusType": 0
              },
              "workflowId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z",
              "tenantId": "string",
              "groupRef": {
                "id": "string",
                "name": "string"
              },
              "isAutodiscovered": true
            }
          },
          "copyAllowedStatistics": {
            "total": 0,
            "destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
              "accountId": "string",
              "source": "string",
              "storageFunctionality": "string",
              "storageType": {
                "name": "string",
                "categoryType": 0,
                "protocolType": 0,
                "vendorType": 0
              },
              "storageStatus": {
                "message": "string",
                "statusType": 0
              },
              "workflowId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z",
              "tenantId": "string",
              "groupRef": {
                "id": "string",
```

```
},
              "isAutodiscovered": true
            }
          },
          "copyBlockedStatistics": {
            "total": 0,
            "destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
              "accountId": "string",
              "source": "string",
              "storageFunctionality": "string",
              "storageType": {
                "name": "string",
                "categoryType": 0,
                "protocolType": 0,
                "vendorType": 0
              },
              "storageStatus": {
                "message": "string",
                "statusType": 0
              },
              "workflowId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z",
              "tenantId": "string",
              "groupRef": {
                "id": "string",
                "name": "string"
              },
              "isAutodiscovered": true
            }
          },
          "deleteAllowedStatistics": {
            "total": 0
          },
          "deleteBlockedStatistics": {
            "total": 0
          },
          "lastCalculatedStatisticsTime": "2019-08-24T14:15:22Z"
        },
        "account": {
          "id": "string",
          "name": "string",
          "description": "string",
          "credentials": "string",
          "protocolType": 0,
          "vendorType": 0,
          "autoDiscovery": true,
          "autodiscoveryDestinationGroupId": "string",
          "destinationGroup": {
            "id": "string",
```

```
}
        },
        "realTimeStartDate": "2019-08-24T14:15:22Z"
      }
    ],
    "storageId": "string",
    "discoveryCycleTiming": {
      "currentCycleStartedAt": "2019-08-24T14:15:22Z",
      "lastCycleStartedAt": "2019-08-24T14:15:22Z",
      "lastCycleFinishedAt": "2019-08-24T14:15:22Z",
      "lastCycleDurationSeconds": 0.1
    },
    "$type": "string",
    "isRealTimeEnabled": true,
    "handlingType": 0
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	GetRealTimeProcessingScanQueryResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

ScanInstance

List, add, update and delete Scan Instances

Get Scan Instances

`GET /api/scaninstance`

Parameters

Name	In	Type	Required	Description
scanPoolId	query	string	false	none

> Example responses

> 200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "entries": [
    {
      "id": "string",
      "scanPoolId": "string",
      "url": "string",
      "apiKey": "string",
      "timeout": "string",
      "scanInstanceType": 0
    }
  ]
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	GetAllScanInstancesCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Add a new Scan Instance

`POST /api/scaninstance`

> Body parameter


```
{
  "scanPoolId": "string",
  "url": "http://example.com",
  "apiKey": "string",
  "timeout": "string",
  "scanInstanceType": 0
}
```

Parameters

Name	In	Type	Required	Description
body	body	AddScanInstanceParameters	true	none

> Example responses

> 200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "scanInstanceId": "string"
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	AddScanInstanceCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Update an existing Scan Instance

`PUT /api/scaninstance`

> Body parameter


```
{
  "id": "string",
  "url": "http://example.com",
  "apiKey": "string",
  "timeout": "string"
}
```

Parameters

Name	In	Type	Required	Description
body	body	UpdateScanInstanceParameters	true	none

> Example responses

> 200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	UpdateScanInstanceCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Get Scan Instance by ID

`GET /api/scaninstance/{id}`

Parameters

Name	In	Type	Required	Description
id	path	string	true	none

> Example responses

200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "entry": {
    "id": "string",
    "scanPoolId": "string",
    "url": "string",
    "apiKey": "string",
    "timeout": "string",
    "scanInstanceType": 0
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	GetScanInstanceByIdCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Delete a Scan Instance

`DELETE /api/scaninstance/{id}`

Parameters

Name	In	Type	Required	Description
id	path	string	true	none

Example responses

200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	DeleteScanInstanceCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

ScanInstance_TestScanInstance

`POST /api/scaninstance/Test`

> Body parameter


```
{
  "url": "string",
  "rules": [
    "string"
  ],
  "apiKey": "string",
  "userAgent": "string",
  "isCloudInstance": true
}
```


Parameters

Name	In	Type	Required	Description
body	body	TestScanInstanceParameters	true	none

> Example responses

> 200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	TestScanInstanceCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

ScanPool

List, add, update and delete Scan Pools

Get Scan Pools

`GET /api/scanpool`

> Example responses

> 200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "entries": [
    {
      "id": "string",
      "name": "string",
      "scanPoolType": 0,
      "isDefault": true,
      "scanInstances": [
        {
          "id": "string",
          "scanPoolId": "string",
          "url": "string",
          "apiKey": "string",
          "timeout": "string",
          "scanInstanceType": 0
        }
      ]
    }
  ]
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	GetAllScanPoolsCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Add a new Scan Pool

`POST /api/scanpool`

> Body parameter


```
{
  "name": "string",
  "scanPoolType": 0
}
```

Parameters

Name	In	Type	Required	Description
body	body	AddScanPoolParameters	true	none

> Example responses

> 200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "scanPoolId": "string"
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	AddScanPoolCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Update an existing Scan Pool

`PUT /api/scanpool`

> Body parameter


```
{
  "id": "string",
  "name": "string"
}
```

Parameters

Name	In	Type	Required	Description
body	body	UpdateScanPoolParameters	true	none

> Example responses

> 200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	UpdateScanPoolCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Get Scan Pool by ID

`GET /api/scanpool/{id}`

Parameters

Name	In	Type	Required	Description
id	path	string	true	none

> Example responses

200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "entry": {
    "id": "string",
    "name": "string",
    "scanPoolType": 0,
    "isDefault": true,
    "scanInstances": [
      {
        "id": "string",
        "scanPoolId": "string",
        "url": "string",
        "apiKey": "string",
        "timeout": "string",
        "scanInstanceType": 0
      }
    ]
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	GetScanPoolByIdCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Delete a Scan Pool

```
DELETE /api/scanpool/{id}
```

Parameters

Name	In	Type	Required	Description
id	path	string	true	none

> Example responses

> 200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	DeleteScanPoolCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

ScanWorkflowSnapshot

List scan workflow snapshots

Get all scan workflow snapshots by scan ID

`GET /api/scanworkflowsnapshot/getAllFromScan/{scanId}`

Parameters

Name	In	Type	Required	Description
scanId	path	string	true	none

> Example responses

> 200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "scanWorkflowSnapshots": [
    {
      "id": "string",
      "scanId": "string",
      "workflow": {
        "id": "string",
        "scanPoolId": "string",
        "scanProcessFlow": 0,
        "isIdentityScanningEnabled": true,
        "scanIntervalDays": 0,
        "rules": [
          "string"
        ],
        "type": 0,
        "workflowSupportedTechnologies": {
          "dlp": {
            "status": 0
          },
          "deepCdr": {
            "status": 0
          },
          "sandBox": {
            "status": 0
          },
          "metascan": {
            "status": 0
          }
        },
        "name": "string",
        "userAgent": "string",
        "scanPool": {
          "id": "string",
          "name": "string",
          "scanPoolType": 0,
          "isDefault": true,
          "scanInstances": [
            {
              "id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
```

```
},
        "failOverScanPoolId": "string",
        "failOverScanPool": {
          "id": "string",
          "name": "string",
          "scanPoolType": 0,
          "isDefault": true,
          "scanInstances": [
            {
              "id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ]
        },
        "filters": {
          "id": "string",
          "minimumSize": 0,
          "maximumSize": 0,
          "minimumDateTime": "2019-08-24T14:15:22Z",
          "maximumDateTime": "2019-08-24T14:15:22Z"
        },
        "fileDefinition": {
          "blockingStrategy": 0,
          "configurableBlockingStrategy": {
            "shouldTreatFilesWithSensitiveDataAsBlocked": true,
            "shouldTreatFilesWithVulnerabilitiesAsBlocked": true
          }
        },
        "remediations": [
          {
            "id": "string",
            "workflowId": "string",
            "isEnabled": true,
            "configuration": "string",
            "type": 0,
            "handlingType": 0
          }
        ],
        "tenantId": "string"
      },
      "startTimestamp": 0,
      "stopTimestamp": 0,
      "scanPool": {
        "id": "string",
        "name": "string",
        "scanPoolType": 0,
        "isDefault": true,
        "scanInstances": [
          {
```

```
"scanPoolId": "string",
            "url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ]
      },
      "scanInstances": [
        {
          "id": "string",
          "scanPoolId": "string",
          "url": "string",
          "apiKey": "string",
          "timeout": "string",
          "scanInstanceType": 0
        }
      ],
      "failOverScanPool": {
        "id": "string",
        "name": "string",
        "scanPoolType": 0,
        "isDefault": true,
        "scanInstances": [
          {
            "id": "string",
            "scanPoolId": "string",
            "url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ]
      },
      "failOverScanInstances": [
        {
          "id": "string",
          "scanPoolId": "string",
          "url": "string",
          "apiKey": "string",
          "timeout": "string",
          "scanInstanceType": 0
        }
      ],
      "storage": {
        "id": "string",
        "name": "string",
        "groupId": "string",
        "clientId": "string",
        "accountId": "string",
        "source": "string",
        "storageFunctionality": "string",
        "storageType": {
```

```
"categoryType": 0,
          "protocolType": 0,
          "vendorType": 0
        },
        "storageStatus": {
          "message": "string",
          "statusType": 0
        },
        "workflowId": "string",
        "lastUpdated": "2019-08-24T14:15:22Z",
        "tenantId": "string",
        "groupRef": {
          "id": "string",
          "name": "string"
        },
        "isAutodiscovered": true
      },
      "workflowStatistics": {
        "taggingStatistics": {
          "total": 0
        },
        "keepAllowedStatistics": {
          "total": 0
        },
        "keepBlockedStatistics": {
          "total": 0
        },
        "keepSanitizedStatistics": {
          "total": 0
        },
        "movedAllowedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
```

```
"id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "movedSanitizedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "movedBlockedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
```

```
"statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "copyAllowedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "copyBlockedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
```

```
"categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "deleteAllowedStatistics": {
          "total": 0
        },
        "deleteBlockedStatistics": {
          "total": 0
        },
        "lastCalculatedStatisticsTime": "2019-08-24T14:15:22Z"
      },
      "account": {
        "id": "string",
        "name": "string",
        "description": "string",
        "credentials": "string",
        "protocolType": 0,
        "vendorType": 0,
        "autoDiscovery": true,
        "autodiscoveryDestinationGroupId": "string",
        "destinationGroup": {
          "id": "string",
          "name": "string"
        }
      },
      "realTimeStartDate": "2019-08-24T14:15:22Z"
    }
  ]
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	GetScanWorkflowSnapshotsFromScanQueryResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Settings

List or update your settings

Update notifications configuration

`PUT /api/settings/notifications`

> Body parameter

```
{
  "emailNotificationsConfig": {
    "generatedReportNotificationsConfig": {
      "isEnabled": true,
      "recipientsType": 0
    },
    "userRequestNotificationsConfig": {
      "isEnabled": true
    },
    "blockedFileNotificationsConfig": {
      "isEnabled": true,
      "recipientsType": 0
    }
  },
  "webhookNotificationsConfig": {
    "scanCompletedNotificationsConfig": {
      "isEnabled": true
    },
    "fileScannedNotificationConfig": {
      "isEnabled": true,
      "notificationScope": 0
    },
    "destinationAddress": "string",
    "headers": {
      "property1": "string",
      "property2": "string"
    },
    "requestType": 0
  },
  "rabbitMqNotificationsConfig": {
    "fileScannedNotificationConfig": {
      "isEnabled": true,
      "notificationScope": 0
    },
    "rabbitMqUrl": "string",
    "headers": {
      "property1": "string",
      "property2": "string"
    }
  }
}
```


Parameters

Name	In	Type	Required	Description
body	body	NotificationsConfigParameters	true	none

> Example responses

200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "newNotificationsConfig": {
    "id": "string",
    "emailNotificationsConfig": {
      "userRequestNotificationsConfig": {
        "isEnabled": true
      },
      "generatedReportNotificationsConfig": {
        "isEnabled": true,
        "recipientsType": 0
      },
      "blockedFileNotificationsConfig": {
        "isEnabled": true,
        "recipientsType": 0
      }
    },
    "webhookNotificationsConfig": {
      "scanCompletedNotificationsConfig": {
        "isEnabled": true
      },
      "fileScannedNotificationConfig": {
        "isEnabled": true,
        "notificationScope": 0
      },
      "destinationAddress": "string",
      "headers": {
        "property1": "string",
        "property2": "string"
      },
      "requestType": 0
    },
    "rabbitMqNotificationsConfig": {
      "fileScannedNotificationConfig": {
        "isEnabled": true,
        "notificationScope": 0
      },
      "rabbitMqUrl": "string",
      "headers": {
        "property1": "string",
        "property2": "string"
      }
    }
  },
  "initialNotificationsConfig": {
    "id": "string",
```

```
"userRequestNotificationsConfig": {
        "isEnabled": true
      },
      "generatedReportNotificationsConfig": {
        "isEnabled": true,
        "recipientsType": 0
      },
      "blockedFileNotificationsConfig": {
        "isEnabled": true,
        "recipientsType": 0
      }
    },
    "webhookNotificationsConfig": {
      "scanCompletedNotificationsConfig": {
        "isEnabled": true
      },
      "fileScannedNotificationConfig": {
        "isEnabled": true,
        "notificationScope": 0
      },
      "destinationAddress": "string",
      "headers": {
        "property1": "string",
        "property2": "string"
      },
      "requestType": 0
    },
    "rabbitMqNotificationsConfig": {
      "fileScannedNotificationConfig": {
        "isEnabled": true,
        "notificationScope": 0
      },
      "rabbitMqUrl": "string",
      "headers": {
        "property1": "string",
        "property2": "string"
      }
    }
  },
  "typeResults": [
    {
      "type": 0,
      "status": 0,
      "errorKey": "string",
      "errorMessage": "string"
    }
  ]
}
```

Responses

Status	Meaning	Description	Schema
200	OK	none	UpdateNotificationsConfigResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Get notifications configuration

`GET /api/settings/notifications`

> Example responses

> 200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "emailNotificationsConfig": {
    "generatedReportNotificationsConfig": {
      "isEnabled": true,
      "recipientsType": 0
    },
    "userRequestNotificationsConfig": {
      "isEnabled": true
    },
    "blockedFileNotificationsConfig": {
      "isEnabled": true,
      "recipientsType": 0
    }
  },
  "webhookNotificationsConfig": {
    "scanCompletedNotificationsConfig": {
      "isEnabled": true
    },
    "fileScannedNotificationConfig": {
      "isEnabled": true,
      "notificationScope": 0
    },
    "destinationAddress": "string",
    "headers": {
      "property1": "string",
      "property2": "string"
    },
    "requestType": 0
  },
  "rabbitMqNotificationsConfig": {
    "fileScannedNotificationConfig": {
      "isEnabled": true,
      "notificationScope": 0
    },
    "rabbitMqUrl": "string",
    "headers": {
      "property1": "string",
      "property2": "string"
    }
  }
}
```

Responses

Status	Meaning	Description	Schema
200	OK	none	GetNotificationsConfigResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Update SMTP configuration

`PATCH /api/settings/smtp`

> Body parameter

```
{
  "host": "string",
  "port": 0,
  "baseUrl": "http://example.com",
  "senderAddress": "string",
  "senderName": "string",
  "domain": "string",
  "username": "string",
  "password": "string",
  "secureSocketOption": 0,
  "ignoreCertWarnings": true,
  "isSmtpEnabled": true
}
```

Parameters

Name	In	Type	Required	Description
body	body	UpdateSmtpConfigParameters	true	none

> Example responses

> 200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "newSmtpConfig": {
    "host": "string",
    "baseUrl": "string",
    "port": 0,
    "senderAddress": "string",
    "senderName": "string",
    "domain": "string",
    "username": "string",
    "secureSocketOption": 0,
    "ignoreCertWarnings": true,
    "isSmtpEnabled": true,
    "replyTo": "string"
  },
  "oldSmtpConfig": {
    "host": "string",
    "baseUrl": "string",
    "port": 0,
    "senderAddress": "string",
    "senderName": "string",
    "domain": "string",
    "username": "string",
    "secureSocketOption": 0,
    "ignoreCertWarnings": true,
    "isSmtpEnabled": true,
    "replyTo": "string"
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	UpdateSmtpConfigCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Fetch SMTP configuration

```
GET /api/settings/smtp
```

Example responses

200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "host": "string",
  "port": 0,
  "baseUrl": "string",
  "senderAddress": "string",
  "senderName": "string",
  "domain": "string",
  "username": "string",
  "secureSocketOption": 0,
  "ignoreCertWarnings": true,
  "isSmtpEnabled": true
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	GetSmtpConfigResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Online license activation

`POST /api/settings/admin/license/activate/online`

Body parameter


```
{
  "key": "string"
}
```

Parameters

Name	In	Type	Required	Description
body	body	OnlineActivationParameters	true	none

> Example responses

> 200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	Activation

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Offline license activation

`POST /api/settings/admin/license/activate/offline`

> Body parameter

```
LicenseContent: string
```

Parameters

Name	In	Type	Required	Description
body	body	object	false	none
» LicenseContent	body	string(binary)¦null	false	none

> Example responses

> 200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```

Responses

Status	Meaning	Description	Schema
200	OK	none	Activation

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Get license details

`GET /api/settings/admin/license`

> Example responses

> 200 Response

```
{
  "apiStatus": "string"
}
```

Responses

Status	Meaning	Description	Schema
200	OK	none	ApiHealthModel

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Deactivate license

`POST /api/settings/admin/license/deactivate`

> Example responses

> 200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```

Responses

Status	Meaning	Description	Schema
200	OK	none	Deactivation

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Update retention configuration

`PUT /api/settings/retention`

> Body parameter

```
{
  "retentionAuditDays": 1,
  "reportRetention": {
    "isEnabled": true,
    "retentionDays": 1
  },
  "rtpHistoryRetention": {
    "isEnabled": true,
    "retentionDays": 1
  }
}
```


Parameters

Name	In	Type	Required	Description
body	body	RetentionConfigParameters	true	none

Example responses

200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	RestResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Fetch retention configuration

`GET /api/settings/retention`

Example responses

200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "retentionAuditDays": 0,
  "reportRetentionConfiguration": {
    "isEnabled": true,
    "retentionDays": 0
  },
  "rtpHistoryRetentionConfiguration": {
    "isEnabled": true,
    "retentionDays": 0
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	GetRetentionConfig

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Generate encryption key

`POST /api/settings/encryption/generate`

Generate a new encryption key, replacing the old one if it exists.

Example responses

200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	GenerateEncryptionKeyCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Get encryption key creation date

`GET /api/settings/encryption/creation-date`

Get the creation date of the encryption key.

> Example responses

> 200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "creationDate": "2019-08-24T14:15:22Z"
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	GetEncryptionKeyCreationDateQueryResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Update SSL configuration

`POST /api/settings/ssl`

Update SSL configuration of MDSS by uploading a certificate and a key to enable SSL.

> Body parameter

```
SslCertificate: string
SslKey: string
IsEnabled: true
```

Parameters

Name	In	Type	Required	Description
body	body	object	false	none
» SslCertificate	body	string(binary)¦null	false	none
» SslKey	body	string(binary)¦null	false	none
» IsEnabled	body	boolean¦null	false	none

> Example responses

> 200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```

Responses

Status	Meaning	Description	Schema
200	OK	none	GenerateEncryptionKeyCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Get SSL configuration

`GET /api/settings/ssl`

Get current SSL configuration status.

> Example responses

> 200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "creationDate": "2019-08-24T14:15:22Z"
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	GetEncryptionKeyCreationDateQueryResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Update Single User Session

`POST /api/settings/single-user-session`

Update Simultaneous Sessions allowed for a Single User.

> Body parameter

```
{
  "isSingleUserSession": true
}
```

Parameters

Name	In	Type	Required	Description
body	body	PostSingleUserSessionParameters	true	none

> Example responses

> 200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```

Responses

Status	Meaning	Description	Schema
200	OK	none	UpdateSingleUserSessionCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Get Single User Session

`GET /api/settings/single-user-session`

Get Simultaneous Sessions allowed for a Single User.

> Example responses

200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "creationDate": "2019-08-24T14:15:22Z"
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	GetEncryptionKeyCreationDateQueryResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Get Telemetry configuration

`GET /api/settings/telemetry`

Get MDSS Open Telemetry configuration.

Example responses

200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "telemetryConfig": {
    "isEnabled": true,
    "sendTelemetryToOpswat": true,
    "autoInstrumentation": true,
    "optelCollectors": [
      {
        "metricEndpoint": {
          "endpointUrl": "string",
          "endpointApiKey": "string",
          "protocol": 0
        },
        "traceEndpoint": {
          "endpointUrl": "string",
          "endpointApiKey": "string",
          "protocol": 0
        },
        "isOpswatCollector": true
      }
    ]
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	GetTelemetryConfigQueryResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Update Telemetry configuration

`POST /api/settings/telemetry`

Update MDSS Open Telemetry configuration.

> Body parameter

```
{
  "telemetryConfig": {
    "isEnabled": true,
    "sendTelemetryToOpswat": true,
    "autoInstrumentation": true,
    "optelCollectors": [
      {
        "metricEndpoint": {
          "endpointUrl": "string",
          "endpointApiKey": "string",
          "protocol": 0
        },
        "traceEndpoint": {
          "endpointUrl": "string",
          "endpointApiKey": "string",
          "protocol": 0
        },
        "isOpswatCollector": true
      }
    ]
  },
  "userInfo": {
    "userId": "string",
    "userName": "string"
  }
}
```


Parameters

Name	In	Type	Required	Description
body	body	UpdateTelemetryConfigCommandRequest	true	none

Example responses

200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```

Responses

Status	Meaning	Description	Schema
200	OK	none	UpdateTelemetryConfigCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Sso

Sso Authentication and Sso configuration update

Get Sso Configuration

`GET /api/sso/config`

Allows retrieval of the current SSO configuration.

> Example responses

> 200 Response


```
{
  "isEnabled": true,
  "ssoProvider": 0,
  "ssoType": 0,
  "baseUrl": "string",
  "clientId": "string",
  "clientSecret": "string",
  "authority": "string",
  "identityProviderCertificate": "string",
  "identityProviderIssuer": "string",
  "loginUrl": "string",
  "logoutUrl": "string",
  "administratorRoleName": "string",
  "readonlyRoleName": "string"
}
```

Responses

Status	Meaning	Description	Schema
200	OK	none	SsoConfig

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Update Sso Configuration

`PATCH /api/sso`

Allows updating the current Sso Configuration.

> Body parameter

```
{
  "clientId": "string",
  "clientSecret": "string",
  "authority": "string",
  "baseUrl": "string",
  "identityProviderIssuer": "string",
  "identityProviderLoginUrl": "string",
  "identityProviderLogoutUrl": "string",
  "identityProviderCertificate": {
    "content": "string"
  },
  "isEnabled": true,
  "ssoType": 0,
  "ssoProvider": 0,
  "administratorRoleName": "string",
  "readonlyRoleName": "string"
}
```

Parameters

Name	In	Type	Required	Description
body	body	UpdateSsoConfigParameters	true	none

> Example responses

> 200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "clientId": "string",
  "authority": "string",
  "baseUrl": "string",
  "isEnabled": true,
  "ssoType": 0,
  "ssoProvider": 0,
  "identityProviderIssuer": "string",
  "identityProviderLoginUrl": "string",
  "identityProviderLogoutUrl": "string",
  "administratorRoleName": "string",
  "readonlyRoleName": "string",
  "ssoConfig": {
    "isEnabled": true,
    "ssoProvider": 0,
    "ssoType": 0,
    "baseUrl": "string",
    "clientId": "string",
    "clientSecret": "string",
    "authority": "string",
    "identityProviderCertificate": "string",
    "identityProviderIssuer": "string",
    "loginUrl": "string",
    "logoutUrl": "string",
    "administratorRoleName": "string",
    "readonlyRoleName": "string"
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	SsoConfigResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Storage

Manage your storage units

Fetch storage by ID

`GET /api/storage/{storageId}`

Parameters

Name	In	Type	Required	Description
storageId	path	string	true	none

> Example responses

> 200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "storage": {
    "id": "string",
    "groupId": "string",
    "accountId": "string",
    "name": "string",
    "storageClientId": "string",
    "storageType": {
      "name": "string",
      "categoryType": 0,
      "protocolType": 0,
      "vendorType": 0
    },
    "storageStatus": {
      "message": "string",
      "statusType": 0
    },
    "scansInProgress": true,
    "isRtpInProgress": true,
    "isScheduledScanInProgress": true,
    "storageFunctionality": "string",
    "isAutodiscovered": true,
    "groupRef": {
      "id": "string",
      "name": "string"
    },
    "$type": "string"
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	GetStorage

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Update a storage

```
PATCH /api/storage/{storageId}
```

Note! The following are templates for what is expected in the Credentials, CredentialsFile and Source fields. Please provide the correct values for your storage integration instead of null/false

Alibaba Cloud storage units:
Credentials:
“{"Endpoint":null,"AccessKeyId":null,"AccessKeySecret":null,"UseRamRole":false}”
Source: “{"BucketName":null,"FolderLocation":null}”

Amazon S3 / S3 Compatible storage units:
Credentials:
“{"ServiceUrl":null,"AccessKeyId":null,"SecretAccessKey":null,"RegionEndpoint":null,"AssumeRoleArn":null,"
Source: “{"BucketName":null,"FolderLocation":null}”

Azure Blob storage units:
Credentials: “{"TenantId":null,"ClientId":null,"ClientSecret":null,"StorageAccount":null}”
Source: “{"Container":null}”

Azure Files storage units:
Credentials: “{"AccountName":null,"AccountKey":null,"ShareName":null}”
Source: “{"FolderLocation":null}”

Box storage units:
CredentialsFile: upload the credentials file
Source: “{"FolderLocation":null}”

Dell Isilon / SMB Compatible storage units:
Credentials: “{"User":null,"Password":null,"Server":null}”
Source: “{"SharePath":null}”

Google Cloud storage units:
CredentialsFile: upload the credentials file
Credentials: “{"UseAdc":false}”
Source: “{"BucketName":null,"FolderLocation":null}”

Graph storage units:
Credentials: “{"TenantId":null,"ClientId":null,"ClientSecret":null}”
Source: “{"Group":null}”

> Body parameter

```
Name: string
StorageVendorType: 0
StorageProtocolType: 0
CredentialsFile: string
Credentials: string
Source: string
GroupId: string
AccountId: string
WorkflowId: string
TransferMetadataAndChecksum: true
```

Parameters

Name	In	Type	Required	Description
storageId	path	string	true	none
body	body	object	false	none
» Name	body	string¦null	false	none
» StorageVendorType	body	StorageVendorType2	false	- 0: AmazonS3
» StorageProtocolType	body	StorageProtocolType2	false	- 0: Smb
» CredentialsFile	body	string(binary)¦null	false	none
» Credentials	body	string¦null	false	none
» Source	body	string¦null	false	none
» GroupId	body	string¦null	false	none
» AccountId	body	string¦null	false	none
» WorkflowId	body	string¦null	false	none
» TransferMetadataAndChecksum	body	boolean¦null	false	none

Detailed descriptions

» StorageVendorType: - 0: AmazonS3

- 1: OneDrive
- 2: Box
- 3: DellIsilon
- 4: AzureFiles
- 5: SmbCompatible

- 6: S3Compatible
- 7: AzureBlob
- 8: AlibabaCloud
- 9: GoogleCloud
- 10: Sftp
- 11: SharePoint
- 12: Nfs
- 13: Wasabi
- 14: OracleCloud
- 15: NetAppOntap
- 16: Cubbit
- 17: Mft
- 18: SharepointOnPrem
- 19: Ftp
- 20: Oracle
- 21: NfsSisl
- 22: ScalityRing

» **StorageProtocolType**: - 0: Smb

- 1: GraphSdk
- 2: BoxSdk
- 3: AwsSdk
- 4: AzureBlobSdk
- 5: AlibabaCloudSdk
- 6: GoogleCloudSdk
- 7: AzureFilesSdk
- 8: Sftp
- 9: Nfs
- 10: Mft
- 11: SharepointOnPrem
- 12: Ftp
- 13: OracleSdk

Enumerated Values

Parameter	Value
» StorageVendorType	0
» StorageVendorType	1
» StorageVendorType	2
» StorageVendorType	3
» StorageVendorType	4
» StorageVendorType	5
» StorageVendorType	6
» StorageVendorType	7
» StorageVendorType	8
» StorageVendorType	9
» StorageVendorType	10
» StorageVendorType	11
» StorageVendorType	12
» StorageVendorType	13
» StorageVendorType	14
» StorageVendorType	15
» StorageVendorType	16
» StorageVendorType	17
» StorageVendorType	18
» StorageVendorType	19
» StorageVendorType	20
» StorageVendorType	21
» StorageVendorType	22
» StorageProtocolType	0
» StorageProtocolType	1
» StorageProtocolType	2
» StorageProtocolType	3

» StorageProtocolType	4
» StorageProtocolType	5
» StorageProtocolType	6
» StorageProtocolType	7
» StorageProtocolType	8
» StorageProtocolType	9
» StorageProtocolType	10
» StorageProtocolType	11
» StorageProtocolType	12
» StorageProtocolType	13

Example responses

200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "updatedStorage": {
    "id": "string",
    "name": "string",
    "groupId": "string",
    "clientId": "string",
    "accountId": "string",
    "source": "string",
    "storageFunctionality": "string",
    "storageType": {
      "name": "string",
      "categoryType": 0,
      "protocolType": 0,
      "vendorType": 0
    },
    "storageStatus": {
      "message": "string",
      "statusType": 0
    },
    "workflowId": "string",
    "lastUpdated": "2019-08-24T14:15:22Z",
    "tenantId": "string",
    "groupRef": {
      "id": "string",
      "name": "string"
    },
    "isAutodiscovered": true
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	UpdateNewStorageCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Delete a storage

```
DELETE /api/storage/{storageId}
```

Parameters

Name	In	Type	Required	Description
storageId	path	string	true	none

Example responses

200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "succeeded": [
    "string"
  ],
  "failed": [
    {
      "id": "string",
      "reasonKey": "string",
      "reason": "string",
      "childFailures": [
        {}
      ]
    }
  ],
  "scansRunning": true,
  "runningScans": [
    {
      "scanId": "string",
      "storageId": "string",
      "accountId": "string",
      "groupId": "string"
    }
  ]
}
```

Responses

Status	Meaning	Description	Schema
200	OK	none	BulkDeleteStoragesCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

List storage units (paginated, filtered, sorted)

`GET /api/storage`

Returns a paginated, filtered, and sorted list of storage units. Supports multi-value comma-separated filters: status (StorageStatusType), vendorType (StorageVendorType), protocolType (StorageProtocolType), accountId, and groupId. The name filter performs a case-insensitive substring (ILIKE) match. Sorting is configurable by id or name. Default Count is 100 (maximum 100). Returns an IPagedResponse containing Items, TotalCount, StartIndex, and Count.

Parameters

Name	In	Type	Required	Description
Name	query	string	false	none
Status	query	array[integer]	false	none
VendorType	query	array[integer]	false	none
ProtocolType	query	array[integer]	false	none
AccountId	query	array[string]	false	none
GroupId	query	array[string]	false	none
StartIndex	query	integer(int32)	false	none
Count	query	integer(int32)	false	none
SortBy	query	array[integer]	false	none
SortOrder	query	array[integer]	false	none

Enumerated Values

Parameter	Value
SortBy	0
SortBy	1
SortOrder	0
SortOrder	1

Example responses

200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "items": [
    {
      "id": "string",
      "groupId": "string",
      "accountId": "string",
      "name": "string",
      "storageClientId": "string",
      "storageType": {
        "name": "string",
        "categoryType": 0,
        "protocolType": 0,
        "vendorType": 0
      },
      "storageStatus": {
        "message": "string",
        "statusType": 0
      },
      "scansInProgress": true,
      "isRtpInProgress": true,
      "isScheduledScanInProgress": true,
      "storageFunctionality": "string",
      "isAutodiscovered": true,
      "groupRef": {
        "id": "string",
        "name": "string"
      },
      "$type": "string"
    }
  ],
  "entries": [
    {
      "id": "string",
      "groupId": "string",
      "accountId": "string",
      "name": "string",
      "storageClientId": "string",
      "storageType": {
        "name": "string",
        "categoryType": 0,
        "protocolType": 0,
        "vendorType": 0
      },
      "storageStatus": {
        "message": "string",
```

```
},
      "scansInProgress": true,
      "isRtpInProgress": true,
      "isScheduledScanInProgress": true,
      "storageFunctionality": "string",
      "isAutodiscovered": true,
      "groupRef": {
        "id": "string",
        "name": "string"
      },
      "$type": "string"
    }
  ],
  "totalCount": 0,
  "startIndex": 0,
  "count": 0
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	ListStorages

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Add a storage

`POST /api/storage`

Note! The following are templates for what is expected in the Credentials, CredentialsFile and Source fields. Please provide the correct values for your storage integration instead of null/false

Alibaba Cloud storage units:
Credentials:
“{"Endpoint":null,"AccessKeyId":null,"AccessKeySecret":null,"UseRamRole":false}”
Source: “{"BucketName":null,"FolderLocation":null}”

Amazon S3 / S3 Compatible storage units:
Credentials:
“{"ServiceUrl":null,"AccessKeyId":null,"SecretAccessKey":null,"RegionEndpoint":null,"AssumeRoleArn":null,"
Source: “{"BucketName":null,"FolderLocation":null}”

Azure Blob storage units:
Credentials: “{"TenantId":null,"ClientId":null,"ClientSecret":null,"StorageAccount":null}”

Source: “{"Container":null}”

Azure Files storage units:
Credentials: “{"AccountName":null,"AccountKey":null,"ShareName":null}”
Source: “{"FolderLocation":null}”

Box storage units:
CredentialsFile: upload the credentials file
Source: “{"FolderLocation":null}”

Dell Isilon / SMB Compatible storage units:
Credentials: “{"User":null,"Password":null,"Server":null}”
Source: “{"SharePath":null}”

Google Cloud storage units:
CredentialsFile: upload the credentials file
Credentials: “{"UseAdc":false}”
Source: “{"BucketName":null,"FolderLocation":null}”

Graph storage units:
Credentials: “{"TenantId":null,"ClientId":null,"ClientSecret":null}”
Source: “{"Group":null}”

> Body parameter

```
Id: string
StorageClientId: string
Name: string
StorageVendorType: 0
StorageProtocolType: 0
CredentialsFile: string
Credentials: string
Source: string
GroupId: string
AccountId: string
WorkflowId: string
TransferMetadataAndChecksum: true
```

Parameters

Name	In	Type	Required	Description
body	body	object	false	none
» Id	body	string¦null	false	none
» StorageClientId	body	string¦null	false	none
» Name	body	string	false	none
» StorageVendorType	body	StorageVendorType2	false	- 0: AmazonS3
» StorageProtocolType	body	StorageProtocolType2	false	- 0: Smb
» CredentialsFile	body	string(binary)¦null	false	none
» Credentials	body	string¦null	false	none
» Source	body	string	false	none
» GroupId	body	string	false	none
» AccountId	body	string¦null	false	none
» WorkflowId	body	string¦null	false	none
» TransferMetadataAndChecksum	body	boolean¦null	false	none

Detailed descriptions

» StorageVendorType: - 0: AmazonS3

- 1: OneDrive
- 2: Box
- 3: DellIsilon
- 4: AzureFiles
- 5: SmbCompatible
- 6: S3Compatible
- 7: AzureBlob
- 8: AlibabaCloud
- 9: GoogleCloud
- 10: Sftp
- 11: SharePoint
- 12: Nfs
- 13: Wasabi

- 14: OracleCloud
- 15: NetAppOntap
- 16: Cubbit
- 17: Mft
- 18: SharepointOnPrem
- 19: Ftp
- 20: Oracle
- 21: NfsSisl
- 22: ScalityRing

» **StorageProtocolType**: - 0: Smb

- 1: GraphSdk
- 2: BoxSdk
- 3: AwsSdk
- 4: AzureBlobSdk
- 5: AlibabaCloudSdk
- 6: GoogleCloudSdk
- 7: AzureFilesSdk
- 8: Sftp
- 9: Nfs
- 10: Mft
- 11: SharepointOnPrem
- 12: Ftp
- 13: OracleSdk

Enumerated Values

Parameter	Value
» StorageVendorType	0
» StorageVendorType	1
» StorageVendorType	2
» StorageVendorType	3
» StorageVendorType	4
» StorageVendorType	5
» StorageVendorType	6
» StorageVendorType	7
» StorageVendorType	8
» StorageVendorType	9
» StorageVendorType	10
» StorageVendorType	11
» StorageVendorType	12
» StorageVendorType	13
» StorageVendorType	14
» StorageVendorType	15
» StorageVendorType	16
» StorageVendorType	17
» StorageVendorType	18
» StorageVendorType	19
» StorageVendorType	20
» StorageVendorType	21
» StorageVendorType	22
» StorageProtocolType	0
» StorageProtocolType	1
» StorageProtocolType	2
» StorageProtocolType	3

» StorageProtocolType	4
» StorageProtocolType	5
» StorageProtocolType	6
» StorageProtocolType	7
» StorageProtocolType	8
» StorageProtocolType	9
» StorageProtocolType	10
» StorageProtocolType	11
» StorageProtocolType	12
» StorageProtocolType	13

Example responses

200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "storageId": "string"
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	AddNewStorageCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Bulk move storages to a target group

`PATCH /api/storage`

Moves up to 100 storages to a target group in a single request. Per-storage ABAC (Write) is enforced — inaccessible storage IDs are returned in the failed list with a localized reason. The target group must exist and be accessible; otherwise the entire request fails with a localized 'target group not found' response.

Body parameter

```
{
  "storageIds": [
    "string"
  ],
  "targetGroupId": "string"
}
```

Parameters

Name	In	Type	Required	Description
body	body	MoveStoragesParameters	true	none

Example responses

200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "succeeded": [
    "string"
  ],
  "failed": [
    {
      "id": "string",
      "reasonKey": "string",
      "reason": "string",
      "childFailures": [
        {}
      ]
    }
  ],
  "targetGroupId": "string"
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	MoveStoragesCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Bulk delete storages

`DELETE /api/storage`

Deletes up to 100 storages in a single request. Per-storage ABAC is enforced — inaccessible storage IDs are returned in the failed list with a localized reason. If any of the target storages has a running scan, the request is rejected with HTTP 409 and the runningScans list. Otherwise, all scans associated with the target storages are deleted as part of the cascade before the storage rows are removed.

> Body parameter

```
{
  "storageIds": [
    "string"
  ]
}
```


Parameters

Name	In	Type	Required	Description
body	body	BulkDeleteStoragesParameters	true	none

Example responses

200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "succeeded": [
    "string"
  ],
  "failed": [
    {
      "id": "string",
      "reasonKey": "string",
      "reason": "string",
      "childFailures": [
        {}
      ]
    }
  ],
  "scansRunning": true,
  "runningScans": [
    {
      "scanId": "string",
      "storageId": "string",
      "accountId": "string",
      "groupId": "string"
    }
  ]
}
```

Responses

Status	Meaning	Description	Schema
200	OK	none	BulkDeleteStoragesCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Fetch storage users

`GET /api/storage/{storageId}/users`

Parameters

Name	In	Type	Required	Description
storageId	path	string	true	none
filter	query	string	false	none

Example responses

200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "entries": [
    {
      "id": "string",
      "fullName": "string"
    }
  ]
}
```

Responses

Status	Meaning	Description	Schema
200	OK	none	EnumerateStorageUsersQueryResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Add batch of storages

`POST /api/storage/batch`

Note! The following are templates for what is expected in the Credentials, CredentialsFile and Source fields. Please provide the correct values for your storage integration instead of null/false

Alibaba Cloud storage units:
Credentials:
“{"Endpoint":null,"AccessKeyId":null,"AccessKeySecret":null,"UseRamRole":false}”
Source: “{"BucketName":null,"FolderLocation":null}”

Amazon S3 / S3 Compatible storage units:
Credentials:
“{"ServiceUrl":null,"AccessKeyId":null,"SecretAccessKey":null,"RegionEndpoint":null,"AssumeRoleArn":null,"
Source: “{"BucketName":null,"FolderLocation":null}”

Azure Blob storage units:
Credentials: “{"TenantId":null,"ClientId":null,"ClientSecret":null,"StorageAccount":null}”
Source: “{"Container":null}”

Azure Files storage units:
Credentials: “{"AccountName":null,"AccountKey":null,"ShareName":null}”
Source: “{"FolderLocation":null}”

Box storage units:
CredentialsFile: upload the credentials file
Source: “{"FolderLocation":null}”

Dell Isilon / SMB Compatible storage units:
Credentials: “{"User":null,"Password":null,"Server":null}”

Google Cloud storage units:

CredentialsFile: upload the credentials file

Credentials: “{"UseAdc":false}”

Source: “{"BucketName":null,"FolderLocation":null}”

Graph storage units:

Credentials: “{"TenantId":null,"ClientId":null,"ClientSecret":null}”

Source: “{"Group":null}”

Body parameter

```
{
  "addStorageParametersList": [
    {
      "id": "string",
      "storageClientId": "string",
      "name": "string",
      "storageVendorType": 0,
      "storageProtocolType": 0,
      "credentialsFile": "string",
      "credentials": "string",
      "source": "string",
      "groupId": "string",
      "accountId": "string",
      "workflowId": "string",
      "transferMetadataAndChecksum": true
    }
  ]
}
```

Parameters

Name	In	Type	Required	Description
body	body	AddBatchStorageParameters	true	none

Example responses

200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "storageId": "string"
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	AddNewStorageCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Get batch of add storages results

`GET /api/storage/results`

Parameters

Name	In	Type	Required	Description
token	query	string	false	none

Example responses

200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "addStorageResultInfos": [
    {
      "result": 0,
      "responseKey": "string",
      "responseMessage": "string",
      "responseMessageParams": {
        "property1": "string",
        "property2": "string"
      },
      "storageStatus": {
        "message": "string",
        "statusType": 0
      },
      "source": "string",
      "name": "string",
      "vendorType": 0,
      "protocolType": 0
    }
  ],
  "isCompleted": true
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	GetBatchResultsResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Add a scan schedule

`PUT /api/storage/{storageId}/scan_schedule`

> Body parameter

```
{
  "name": "string",
  "workflowId": "string",
  "recurrencePattern": {
    "type": "string",
    "minutelyRecurrence": {
      "everyNumberOfMinutes": 5
    },
    "hourlyRecurrence": {
      "everyNumberOfHours": 1
    },
    "dailyRecurrence": {
      "everyNumberOfDays": 1
    },
    "weeklyRecurrence": {
      "daysOfWeek": [
        0
      ],
      "everyNumberOfWeeks": 0
    },
    "monthlyRecurrence": {
      "everyNumberOfMonths": 1,
      "dayOfMonth": 1
    },
    "startDate": "2019-08-24T14:15:22Z",
    "timeToStart": "2019-08-24T14:15:22Z",
    "avoidConcurrentScheduleRuns": true
  },
  "scanPartition": "string",
  "priority": 0,
  "$type": "string"
}
```


Parameters

Name	In	Type	Required	Description
storageId	path	string	true	none
body	body	AddScanScheduleParameters	true	none

Example responses

200 Response

Responses

Status	Meaning	Description	Schema
200	OK	none	string

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Update a scan schedule

`PUT /api/storage/scan_schedule/update/{storageId}`

> Body parameter

```
{
  "name": "string",
  "workflowId": "string",
  "recurrencePattern": {
    "type": "string",
    "minutelyRecurrence": {
      "everyNumberOfMinutes": 5
    },
    "hourlyRecurrence": {
      "everyNumberOfHours": 1
    },
    "dailyRecurrence": {
      "everyNumberOfDays": 1
    },
    "weeklyRecurrence": {
      "daysOfWeek": [
        0
      ],
      "everyNumberOfWeeks": 0
    },
    "monthlyRecurrence": {
      "everyNumberOfMonths": 1,
      "dayOfMonth": 1
    },
    "startDate": "2019-08-24T14:15:22Z",
    "timeToStart": "2019-08-24T14:15:22Z",
    "avoidConcurrentScheduleRuns": true
  },
  "scanPartition": "string",
  "priority": 0,
  "$type": "string",
  "id": "string"
}
```

Parameters

Name	In	Type	Required	Description
storageId	path	string	true	none
body	body	UpdateScanScheduleParameters	true	none

> Example responses

> 200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	UpdateScanScheduleCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Fetch scan schedules

`GET /api/storage/scan_schedules/{sortDirection}/{startIndex}/{count}`

Parameters

Name	In	Type	Required	Description
sortDirection	path	SortDirectionFilter	true	none
startIndex	path	integer(int32)	true	none
count	path	integer(int32)	true	none
name	query	string	false	none
user	query	string	false	none
type	query	string	false	none
storageId	query	string	false	none

Enumerated Values

Parameter	Value
sortDirection	0
sortDirection	1

Example responses

200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "entries": [
    {
      "id": "string",
      "name": "string",
      "workflowId": "string",
      "scanConfigurationId": "string",
      "type": "string",
      "scanPartition": "string",
      "createdAt": "2019-08-24T14:15:22Z",
      "lastScanTime": "2019-08-24T14:15:22Z",
      "nextScanTime": "2019-08-24T14:15:22Z",
      "recurrencePatternDto": {
        "type": 0,
        "minutelyRecurrence": {
          "everyNumberOfMinutes": 0
        },
        "hourlyRecurrence": {
          "everyNumberOfHours": 0
        },
        "dailyRecurrence": {
          "everyNumberOfDays": 0
        },
        "weeklyRecurrence": {
          "daysOfWeek": [
            0
          ],
          "everyNumberOfWeeks": 0
        },
        "monthlyRecurrence": {
          "everyNumberOfMonths": 0,
          "dayOfMonth": 0
        },
        "startDate": "2019-08-24T14:15:22Z",
        "timeToStart": "2019-08-24T14:15:22Z",
        "avoidConcurrentScheduleRuns": true
      },
      "createdBy": "string",
      "priority": 0,
      "storageId": "string"
    }
  ],
  "totalCount": 0
}
```

Responses

Status	Meaning	Description	Schema
200	OK	none	EnumerateScanSchedules

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Delete scan schedules

`DELETE /api/storage/scan_schedule`

Deletes up to 100 scan schedule records in a single request. Per-schedule ABAC (Storages.Delete on the schedule's storage) is enforced — inaccessible IDs are returned in the failed list with a localized reason. Schedules that don't exist are also returned in the failed list with reasonKey BULK_OPERATION_ITEM_NOT_FOUND.

> Body parameter

```
[
  "string"
]
```

Parameters

Name	In	Type	Required	Description
body	body	array[string]	true	none

> Example responses

> 200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "succeeded": [
    "string"
  ],
  "failed": [
    {
      "id": "string",
      "reasonKey": "string",
      "reason": "string",
      "childFailures": [
        {}
      ]
    }
  ]
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	DeleteScanSchedulesCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Retrieve storage user name

`GET /api/storage/{storageId}/{userId}`

Parameters

Name	In	Type	Required	Description
storageId	path	string	true	none
userId	path	string	true	none

> Example responses

200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "userName": "string"
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	RetrieveUserNameFromStorageQueryResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

User

Create, list and update user accounts

Fetch active users

`GET /api/user/active/{startIndex}/{count}`

Parameters

Name	In	Type	Required	Description
startIndex	path	string	true	none
count	path	string	true	none
searchTerm	query	string	false	none
orderType	query	any	false	none
orderBy	query	any	false	none
searchText	query	string	false	none

Example responses

200 Response


```
{
  "entries": [
    {
      "id": "string",
      "userName": "string",
      "fullName": "string",
      "email": "string",
      "roles": [
        {
          "bindingId": "string",
          "roleId": "string",
          "roleName": "string",
          "expiresAt": "2019-08-24T14:15:22Z"
        }
      ],
      "directPermissions": [
        {
          "id": "string",
          "permissionName": "string",
          "expiresAt": "2019-08-24T14:15:22Z"
        }
      ]
    }
  ],
  "totalCount": 0
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	EnumerateActiveUsers

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Register a user

`POST /api/user/register`

Body parameter

```
{
  "fullName": "string",
  "userName": "string",
  "password": "string",
  "email": "string",
  "ssoUserId": "string"
}
```


Parameters

Name	In	Type	Required	Description
body	body	RegisterUserParameters	true	none

> Example responses

> 200 Response

Responses

Status	Meaning	Description	Schema
200	OK	none	string

This operation does not require authentication

Create a user

`POST /api/user/create`

> Body parameter


```
{
  "fullName": "string",
  "userName": "string",
  "password": "string",
  "email": "string",
  "ssoUserId": "string",
  "role": 0
}
```

Parameters

Name	In	Type	Required	Description
body	body	CreateUserParameters	true	none

> Example responses

> 200 Response

Responses

Status	Meaning	Description	Schema
200	OK	none	string

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Authenticate with a username and password

`POST /api/user/authenticate`

Authenticate with a username and password to obtain a JWT token,Most of the APIs require authentication in the form of providing a JWT token. Call this API in order to receive a token but please note that it's only valid for an hour so it should be periodically refreshed.

> Body parameter

```
{
  "userName": "string",
  "password": "string"
}
```

Parameters

Name	In	Type	Required	Description
body	body	AuthenticateUserCommandRequest	true	none

Example responses

200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "fullName": "string",
  "email": "string",
  "userName": "string",
  "role": 0,
  "user": {
    "id": "string",
    "userName": "string",
    "fullName": "string",
    "email": "string",
    "role": 0,
    "roles": [
      "string"
    ],
    "tenantId": "string",
    "ssoUserId": "string",
    "passwordHash": "string",
    "passwordSalt": "string",
    "passwordHashAlgorithm": 0,
    "preferences": {
      "theme": 0,
      "language": 0
    }
  },
  "userId": "string"
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	AuthenticateUserCommandResponseWithoutTokens

This operation does not require authentication

Fetch current user information

`GET /api/user/me`

Retrieve information about the currently authenticated user.

> Example responses

> 200 Response


```
{
  "username": "string",
  "email": "string",
  "authProvider": "string",
  "role": "string",
  "id": "string",
  "roles": [
    {
      "bindingId": "string",
      "roleId": "string",
      "roleName": "string",
      "expiresAt": "2019-08-24T14:15:22Z"
    }
  ],
  "directPermissions": [
    {
      "id": "string",
      "permissionName": "string",
      "expiresAt": "2019-08-24T14:15:22Z"
    }
  ],
  "preferences": {
    "theme": 0,
    "language": 0
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	CurrentUserInfo

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Refresh user token

`POST /api/user/refreshToken`

Refresh an expired accessToken using a valid refreshToken

> Example responses

> 200 Response

Responses

Status	Meaning	Description	Schema
200	OK	none	string

This operation does not require authentication

Logout

`POST /api/user/logout`

> Example responses

> 200 Response

Responses

Status	Meaning	Description	Schema
200	OK	none	string

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Update user role

`PUT /api/user/role`

> Body parameter

```
{
  "userId": "string",
  "role": 0
}
```


Parameters

Name	In	Type	Required	Description
body	body	UpdateUserRoleParameters	true	none

Example responses

200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "user": {
    "id": "string",
    "userName": "string",
    "fullName": "string",
    "email": "string",
    "role": 0,
    "roles": [
      "string"
    ],
    "tenantId": "string",
    "ssoUserId": "string",
    "passwordHash": "string",
    "passwordSalt": "string",
    "passwordHashAlgorithm": 0,
    "preferences": {
      "theme": 0,
      "language": 0
    }
  }
}
```

Responses

Status	Meaning	Description	Schema
200	OK	none	UpdateUserCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Fetch users

`GET /api/user/requests`

Parameters

Name	In	Type	Required	Description
startIndex	query	integer(int32)	false	none
count	query	integer(int32)	false	none
orderType	query	any	false	none
orderBy	query	any	false	none
searchText	query	string	false	none

> Example responses

> 200 Response

```
{
  "entries": [
    {
      "id": "string",
      "userName": "string",
      "fullName": "string",
      "email": "string",
      "role": 0,
      "roles": [
        "string"
      ],
      "tenantId": "string",
      "ssoUserId": "string",
      "passwordHash": "string",
      "passwordSalt": "string",
      "passwordHashAlgorithm": 0,
      "preferences": {
        "theme": 0,
        "language": 0
      }
    }
  ],
  "totalCount": 0
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	EnumerateUsers

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Delete a user

`DELETE /api/user/{userId}`

Parameters

Name	In	Type	Required	Description
userId	path	string	true	none

> Example responses

200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "user": {
    "id": "string",
    "userName": "string",
    "fullName": "string",
    "email": "string",
    "role": 0,
    "roles": [
      "string"
    ],
    "tenantId": "string",
    "ssoUserId": "string",
    "passwordHash": "string",
    "passwordSalt": "string",
    "passwordHashAlgorithm": 0,
    "preferences": {
      "theme": 0,
      "language": 0
    }
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	UserCleanupCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Update current user

`PUT /api/user`

Body parameter

```
{
  "userId": "string",
  "role": 0,
  "userName": "string",
  "fullName": "string",
  "currentPassword": "string",
  "newPassword": "string",
  "email": "string",
  "preferences": {
    "theme": 0,
    "language": 0
  }
}
```


Parameters

Name	In	Type	Required	Description
body	body	UpdateUserParameters	true	none

Example responses

200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "user": {
    "id": "string",
    "userName": "string",
    "fullName": "string",
    "email": "string",
    "role": 0,
    "roles": [
      "string"
    ],
    "tenantId": "string",
    "ssoUserId": "string",
    "passwordHash": "string",
    "passwordSalt": "string",
    "passwordHashAlgorithm": 0,
    "preferences": {
      "theme": 0,
      "language": 0
    }
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	UpdateUserCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Request password reset

`POST /api/user/password/reset`

> Body parameter


```
{
  "userInput": "string"
}
```

Parameters

Name	In	Type	Required	Description
body	body	RequestResetPasswordCommandRequest	true	none

> Example responses

> 200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	RequestResetPasswordCommandResponse

This operation does not require authentication

Reset user password

`POST /api/user/password`

> Body parameter


```
{
  "newPassword": "stringstring",
  "newPasswordConfirmation": "stringstring",
  "secureToken": "string"
}
```

Parameters

Name	In	Type	Required	Description
body	body	UpdatePasswordCommandRequest	true	none

Example responses

200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "user": {
    "id": "string",
    "userName": "string",
    "fullName": "string",
    "email": "string",
    "role": 0,
    "roles": [
      "string"
    ],
    "tenantId": "string",
    "ssoUserId": "string",
    "passwordHash": "string",
    "passwordSalt": "string",
    "passwordHashAlgorithm": 0,
    "preferences": {
      "theme": 0,
      "language": 0
    }
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	UpdatePasswordCommandResponse

This operation does not require authentication

Get User Permissions

`GET /api/user/{userId}/permissions`

Parameters

Name	In	Type	Required	Description
userId	path	string	true	none

Example responses

200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "roles": [
    {
      "bindingId": "string",
      "roleId": "string",
      "roleName": "string",
      "expiresAt": "2019-08-24T14:15:22Z"
    }
  ],
  "directPermissions": [
    {
      "id": "string",
      "permissionName": "string",
      "expiresAt": "2019-08-24T14:15:22Z"
    }
  ]
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	GetUserPermissionsQueryResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

User Tour

Finalize and list user tours

Fetch tours completed by a user

`GET /api/usertour/{userId}`

Parameters

Name	In	Type	Required	Description
userId	path	string	true	none

> Example responses

> 200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "userId": "string",
  "userTours": [
    {
      "tourType": 0,
      "finalizedDate": "2019-08-24T14:15:22Z"
    }
  ]
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	GetUserTourQueryResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Mark a specific Tour as completed by a user

`POST /api/usertour/finalizeUserTour`

> Body parameter

```
{
  "userId": "string",
  "userTourType": 0
}
```

Parameters

Name	In	Type	Required	Description
body	body	FinalizeUserTour	true	none

> Example responses

> 200 Response

Responses

Status	Meaning	Description	Schema
200	OK	none	string

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Webhook

File event trigger of real time processing

`POST /api/webhook/realtime`

This endpoint takes the parameters and tries to find the file in the specified storage and applies the workflow for the specified file

Body parameter


```
{
  "metadata": "string",
  "storageClientId": "string",
  "scanId": "string"
}
```


Parameters

Name	In	Type	Required	Description
body	body	WebhookEventBasedRtpParameters	true	none

Example responses

200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "correlationId": "string"
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	WebhookEventBasedRtpCommandResponse
400	Bad Request	none	WebhookEventBasedRtpCommandResponse
404	Not Found	none	WebhookEventBasedRtpCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

File event trigger of real time processing by storage client ID

`POST /api/webhook/realtime/{storageClientId}/{scanId}`

This endpoint takes the parameter and tries to find the file in the specified storage and applies the workflow for the specified file

> Body parameter

```
null
```

Parameters

Name	In	Type	Required	Description
storageClientId	path	string	true	none
scanId	path	string	true	none
body	body	any	true	none

> Example responses

> 200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "correlationId": "string"
}
```

Responses

Status	Meaning	Description	Schema
200	OK	none	WebhookEventBasedRtpCommandResponse
400	Bad Request	none	WebhookEventBasedRtpCommandResponse
404	Not Found	none	WebhookEventBasedRtpCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

File event trigger of real time processing for Box

`POST /api/webhook/realtime/public/{tenantId}/{storageClientId}/{scanId}`

This endpoint takes the parameter and tries to find the file in the specified Box storage and applies the workflow for the specified file

> Body parameter

```
null
```

Parameters

Name	In	Type	Required	Description
storageClientId	path	string	true	none
scanId	path	string	true	none
tenantId	path	string	true	none
body	body	any	true	none

> Example responses

> 200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "correlationId": "string"
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	WebhookEventBasedRtpCommandResponse
400	Bad Request	none	WebhookEventBasedRtpCommandResponse
404	Not Found	none	WebhookEventBasedRtpCommandResponse

This operation does not require authentication

Webhook_EventHandlerGraphNotification

`POST /api/webhook/realtime/graph/{storageClientId}/{scanId}`

> Body parameter


```
null
```


Parameters

Name	In	Type	Required	Description
storageClientId	path	string	true	none
scanId	path	string	true	none
validationToken	query	string	false	none
body	body	any	false	none

> Example responses

200 Response

Responses

Status	Meaning	Description	Schema
200	OK	none	string

This operation does not require authentication

Webhook_EventHandlerGraphNotification2

`POST /api/webhook/realtime/graph/{tenantId}/{storageClientId}/{scanId}`

Body parameter

```
null
```

Parameters

Name	In	Type	Required	Description
storageClientId	path	string	true	none
scanId	path	string	true	none
validationToken	query	string	false	none
tenantId	path	string	true	none
body	body	any	false	none

Example responses

200 Response

Responses

Status	Meaning	Description	Schema
200	OK	none	string

This operation does not require authentication

Workflow

List, add, update and delete Workflows

Get Workflows

`GET /api/workflow`

> Example responses

> 200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "entries": [
    {
      "id": "string",
      "scanPoolId": "string",
      "scanProcessFlow": 0,
      "isIdentityScanningEnabled": true,
      "scanIntervalDays": 0,
      "rules": [
        "string"
      ],
      "type": 0,
      "workflowSupportedTechnologies": {
        "dlp": {
          "status": 0
        },
        "deepCdr": {
          "status": 0
        },
        "sandBox": {
          "status": 0
        },
        "metascan": {
          "status": 0
        }
      },
      "name": "string",
      "userAgent": "string",
      "scanPool": {
        "id": "string",
        "name": "string",
        "scanPoolType": 0,
        "isDefault": true,
        "scanInstances": [
          {
            "id": "string",
            "scanPoolId": "string",
            "url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ]
      },
      "failOverScanPoolId": "string",
```

```
"id": "string",
        "name": "string",
        "scanPoolType": 0,
        "isDefault": true,
        "scanInstances": [
          {
            "id": "string",
            "scanPoolId": "string",
            "url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ]
      },
      "filters": {
        "id": "string",
        "minimumSize": 0,
        "maximumSize": 0,
        "minimumDateTime": "2019-08-24T14:15:22Z",
        "maximumDateTime": "2019-08-24T14:15:22Z"
      },
      "fileDefinition": {
        "blockingStrategy": 0,
        "configurableBlockingStrategy": {
          "shouldTreatFilesWithSensitiveDataAsBlocked": true,
          "shouldTreatFilesWithVulnerabilitiesAsBlocked": true
        }
      },
      "remediations": [
        {
          "id": "string",
          "workflowId": "string",
          "isEnabled": true,
          "configuration": "string",
          "type": 0,
          "handlingType": 0
        }
      ],
      "tenantId": "string"
    }
  ],
  "scanPoolHasApiKey": {
    "property1": true,
    "property2": true
  }
}
```

Responses

Status	Meaning	Description	Schema
200	OK	none	GetAllWorkflowsCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Add a new Workflow

`POST /api/workflow`

> Body parameter


```
{
  "scanPoolId": "string",
  "rules": [
    "string"
  ],
  "name": "string",
  "userAgent": "string",
  "failOverScanPoolId": "string",
  "filters": {
    "minimumSize": 0,
    "maximumSize": 0,
    "minimumDateTime": "2019-08-24T14:15:22Z",
    "maximumDateTime": "2019-08-24T14:15:22Z"
  },
  "scanProcessFlow": 0,
  "isIdentityScanningEnabled": true,
  "scanIntervalDays": 1
}
```


Parameters

Name	In	Type	Required	Description
body	body	AddWorkflowParameters	true	none

> Example responses

> 200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "workflowId": "string"
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	AddWorkflowCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Update an existing Workflow

`PATCH /api/workflow`

> Body parameter

```
{
  "id": "string",
  "scanPoolId": "string",
  "scanProcessFlow": 0,
  "rules": [
    "string"
  ],
  "name": "string",
  "userAgent": "string",
  "failOverScanPoolId": "string",
  "failOverDisabled": true,
  "filters": {
    "minimumSize": 0,
    "maximumSize": 0,
    "minimumDateTime": "2019-08-24T14:15:22Z",
    "maximumDateTime": "2019-08-24T14:15:22Z"
  },
  "fileDefinition": {
    "blockingStrategy": 0,
    "configurableBlockingStrategy": {
      "shouldTreatFilesWithSensitiveDataAsBlocked": true,
      "shouldTreatFilesWithVulnerabilitiesAsBlocked": true
    }
  },
  "isIdentityScanningEnabled": true,
  "scanIntervalDays": 1
}
```


Parameters

Name	In	Type	Required	Description
body	body	UpdateWorkflowParameters	true	none

Example responses

200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```

Responses

Status	Meaning	Description	Schema
200	OK	none	UpdateWorkflowCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Get Workflow by ID

`GET /api/workflow/{id}`

Parameters

Name	In	Type	Required	Description
id	path	string	true	none

> Example responses

> 200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "entry": {
    "id": "string",
    "scanPoolId": "string",
    "scanProcessFlow": 0,
    "isIdentityScanningEnabled": true,
    "scanIntervalDays": 0,
    "rules": [
      "string"
    ],
    "type": 0,
    "workflowSupportedTechnologies": {
      "dlp": {
        "status": 0
      },
      "deepCdr": {
        "status": 0
      },
      "sandBox": {
        "status": 0
      },
      "metascan": {
        "status": 0
      }
    },
    "name": "string",
    "userAgent": "string",
    "scanPool": {
      "id": "string",
      "name": "string",
      "scanPoolType": 0,
      "isDefault": true,
      "scanInstances": [
        {
          "id": "string",
          "scanPoolId": "string",
          "url": "string",
          "apiKey": "string",
          "timeout": "string",
          "scanInstanceType": 0
        }
      ]
    },
    "failOverScanPoolId": "string",
    "failOverScanPool": {
```

```
"name": "string",
      "scanPoolType": 0,
      "isDefault": true,
      "scanInstances": [
        {
          "id": "string",
          "scanPoolId": "string",
          "url": "string",
          "apiKey": "string",
          "timeout": "string",
          "scanInstanceType": 0
        }
      ]
    },
    "filters": {
      "id": "string",
      "minimumSize": 0,
      "maximumSize": 0,
      "minimumDateTime": "2019-08-24T14:15:22Z",
      "maximumDateTime": "2019-08-24T14:15:22Z"
    },
    "fileDefinition": {
      "blockingStrategy": 0,
      "configurableBlockingStrategy": {
        "shouldTreatFilesWithSensitiveDataAsBlocked": true,
        "shouldTreatFilesWithVulnerabilitiesAsBlocked": true
      }
    },
    "remediations": [
      {
        "id": "string",
        "workflowId": "string",
        "isEnabled": true,
        "configuration": "string",
        "type": 0,
        "handlingType": 0
      }
    ],
    "tenantId": "string"
  },
  "scanPoolHasApiKey": {
    "property1": true,
    "property2": true
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	GetWorkflowByIdCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Delete a Workflow

`DELETE /api/workflow/{id}`

Parameters

Name	In	Type	Required	Description
id	path	string	true	none

> Example responses

> 200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	DeleteWorkflowCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Set a Workflow as default

`POST /api/workflow/setDefault/{id}`

Parameters

Name	In	Type	Required	Description
id	path	string	true	none

Example responses

200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```

Responses

Status	Meaning	Description	Schema
200	OK	none	SetDefaultWorkflowCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Refresh supported technologies for a Workflow and return updated Workflow

`POST /api/workflow/enabledTechnologies`

Body parameter

```
{
  "workflowId": "string"
}
```

Parameters

Name	In	Type	Required	Description
body	body	RefreshSupportedTechnologiesCommandRequest	true	none

> Example responses

> 200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "workflowDto": {
    "id": "string",
    "scanPoolId": "string",
    "scanProcessFlow": 0,
    "isIdentityScanningEnabled": true,
    "scanIntervalDays": 0,
    "rules": [
      "string"
    ],
    "type": 0,
    "workflowSupportedTechnologies": {
      "dlp": {
        "status": 0
      },
      "deepCdr": {
        "status": 0
      },
      "sandBox": {
        "status": 0
      },
      "metascan": {
        "status": 0
      }
    },
    "name": "string",
    "userAgent": "string",
    "scanPool": {
      "id": "string",
      "name": "string",
      "scanPoolType": 0,
      "isDefault": true,
      "scanInstances": [
        {
          "id": "string",
          "scanPoolId": "string",
          "url": "string",
          "apiKey": "string",
          "timeout": "string",
          "scanInstanceType": 0
        }
      ]
    },
    "failOverScanPoolId": "string",
    "failOverScanPool": {
```

```
"name": "string",
      "scanPoolType": 0,
      "isDefault": true,
      "scanInstances": [
        {
          "id": "string",
          "scanPoolId": "string",
          "url": "string",
          "apiKey": "string",
          "timeout": "string",
          "scanInstanceType": 0
        }
      ]
    },
    "filters": {
      "id": "string",
      "minimumSize": 0,
      "maximumSize": 0,
      "minimumDateTime": "2019-08-24T14:15:22Z",
      "maximumDateTime": "2019-08-24T14:15:22Z"
    },
    "fileDefinition": {
      "blockingStrategy": 0,
      "configurableBlockingStrategy": {
        "shouldTreatFilesWithSensitiveDataAsBlocked": true,
        "shouldTreatFilesWithVulnerabilitiesAsBlocked": true
      }
    },
    "remediations": [
      {
        "id": "string",
        "workflowId": "string",
        "isEnabled": true,
        "configuration": "string",
        "type": 0,
        "handlingType": 0
      }
    ],
    "tenantId": "string"
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	RefreshSupportedTechnologiesCommandResponse

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Deprecated, soon to be removed

Fetch the number of accounts

`GET /api/account/count`

Get the total number of accounts in the system

> Example responses

> 200 Response


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "accountCount": {
    "count": 0
  }
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	GetAccountsCount

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Fetch all storage units

`GET /api/storage/all`

> Example responses

> 200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "entries": [
    {
      "id": "string",
      "groupId": "string",
      "accountId": "string",
      "name": "string",
      "storageClientId": "string",
      "storageType": {
        "name": "string",
        "categoryType": 0,
        "protocolType": 0,
        "vendorType": 0
      },
      "storageStatus": {
        "message": "string",
        "statusType": 0
      },
      "scansInProgress": true,
      "isRtpInProgress": true,
      "isScheduledScanInProgress": true,
      "storageFunctionality": "string",
      "isAutodiscovered": true,
      "groupRef": {
        "id": "string",
        "name": "string"
      },
      "$type": "string"
    }
  ]
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	EnumerateStorages

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Fetch all storage units by filters (storage type or status)

`GET /api/storage/enumerate/{startIndex}/{count}`

Parameters

Name	In	Type	Required	Description
startIndex	path	string	true	none
count	path	string	true	none
sortingOrder	query	string	false	none
search	query	string	false	none
storageType	query	integer(int32)	false	none
storageStatus	query	integer(int32)	false	none

Example responses

200 Response

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "entries": [
    {
      "id": "string",
      "groupId": "string",
      "accountId": "string",
      "name": "string",
      "storageClientId": "string",
      "storageType": {
        "name": "string",
        "categoryType": 0,
        "protocolType": 0,
        "vendorType": 0
      },
      "storageStatus": {
        "message": "string",
        "statusType": 0
      },
      "scansInProgress": true,
      "isRtpInProgress": true,
      "isScheduledScanInProgress": true,
      "storageFunctionality": "string",
      "isAutodiscovered": true,
      "groupRef": {
        "id": "string",
        "name": "string"
      },
      "$type": "string"
    }
  ]
}
```


Responses

Status	Meaning	Description	Schema
200	OK	none	EnumerateStorages2

To perform this operation, you must be authenticated by means of one of the following methods: Bearer

Schemas

GetRolesQueryResponse


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "roles": [
    {
      "id": "string",
      "name": "string",
      "permissions": [
        {
          "id": "string",
          "action": "string",
          "resource": "string"
        }
      ]
    }
  ]
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» roles	[Role]¦null	false	none	none

Role

```
{
  "id": "string",
  "name": "string",
  "permissions": [
    {
      "id": "string",
      "action": "string",
      "resource": "string"
    }
  ]
}
```


Properties

Name	Type	Required	Restrictions	Description
id	string(guid)	true	none	none
name	string	true	none	none
permissions	[Permission]¦null	false	none	none

Permission


```
{
  "id": "string",
  "action": "string",
  "resource": "string"
}
```


Properties

Name	Type	Required	Restrictions	Description
id	string(guid)	true	none	none
action	string	true	none	none
resource	string	true	none	none

RestResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```


Properties

Name	Type	Required	Restrictions	Description
result	ResultType	false	none	- 0: Success - 1: Error - 2: InternalError - 3: NotFound - 4: Forbidden - 5: Conflict
responseKey	string¦null	false	none	none
responseMessage	string¦null	false	none	none
responseMessageParams	object¦null	false	none	none
» **additionalProperties**	string	false	none	none

ResultType


```
0
```


- 0: Success
- 1: Error
- 2: InternalError
- 3: NotFound
- 4: Forbidden
- 5: Conflict

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: Success - 1: Error - 2: InternalError - 3: NotFound - 4: Forbidden - 5: Conflict

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2
anonymous	3
anonymous	4
anonymous	5

GetRoleByIdQueryResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "role": {
    "id": "string",
    "name": "string",
    "permissions": [
      {
        "id": "string",
        "action": "string",
        "resource": "string"
      }
    ]
  }
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» role	Role¦null	false	none	none

CreateRoleCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "role": {
    "id": "string",
    "name": "string",
    "permissions": [
      {
        "id": "string",
        "action": "string",
        "resource": "string"
      }
    ]
  }
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» role	Role¦null	false	none	none

CreateRoleParameters


```
{
  "name": "string",
  "permissionIds": [
    "string"
  ],
  "templateRoleId": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
name	string	true	none	none
permissionIds	[string]¦null	false	none	none
templateRoleId	string(guid)¦null	false	none	none

UpdateRoleCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```

Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none

UpdateRoleParameters

```
{
  "name": "string",
  "permissionIds": [
    "string"
  ]
}
```

Properties

Name	Type	Required	Restrictions	Description
name	string	true	none	none
permissionIds	[string]¦null	false	none	none

DeleteRoleCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```

Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none

GetPermissionsQueryResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "permissions": [
    {
      "id": "string",
      "action": "string",
      "resource": "string"
    }
  ]
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» permissions	[Permission]¦null	false	none	none

CreatePermissionCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "permission": {
    "id": "string",
    "action": "string",
    "resource": "string"
  }
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» permission	Permission¦null	false	none	none

CreatePermissionParameters


```
{
  "action": "string",
  "resource": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
action	string	true	none	none
resource	string	true	none	none

DeletePermissionCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```

Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none

AssignPermissionToRoleCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none

RolePermissionParameters


```
{
  "permissionId": "string"
}
```


Properties

Name	Type	Required	Restrictions	Description
permissionId	string(guid)	true	none	none

RemovePermissionFromRoleCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none

AssignRoleToUserCommandResponse


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "roleBindingId": "string"
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» roleBindingId	string(guid)¦null	false	none	none

AssignRoleToUserParameters

```
{
  "roleId": "string",
  "expiresAt": "2019-08-24T14:15:22Z"
}
```

Properties

Name	Type	Required	Restrictions	Description
roleId	string(guid)	true	none	none
expiresAt	string(date-time)¦null	false	none	none

ReplaceUserRolesCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```

Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none

ReplaceUserRolesParameters

```
{
  "roleIds": [
    "string"
  ]
}
```

Properties

Name	Type	Required	Restrictions	Description
roleIds	[string]	true	none	none

RemoveRoleFromUserCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```

Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none

AssignPermissionToUserCommandResponse


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "userPermissionId": "string"
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» userPermissionId	string(guid)¦null	false	none	none

AssignPermissionToUserParameters


```
{
  "permissionId": "string",
  "expiresAt": "2019-08-24T14:15:22Z"
}
```

Properties

Name	Type	Required	Restrictions	Description
permissionId	string(guid)	true	none	none
expiresAt	string(date-time)¦null	false	none	none

RemovePermissionFromUserCommandResponse


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none

AddAccountCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "account": {
    "id": "string",
    "name": "string",
    "description": "string",
    "credentials": "string",
    "protocolType": 0,
    "vendorType": 0,
    "autoDiscovery": true,
    "autodiscoveryDestinationGroupId": "string",
    "destinationGroup": {
      "id": "string",
      "name": "string"
    }
  }
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» account	Account¦null	false	none	none

Account

```
{
  "id": "string",
  "name": "string",
  "description": "string",
  "credentials": "string",
  "protocolType": 0,
  "vendorType": 0,
  "autoDiscovery": true,
  "autodiscoveryDestinationGroupId": "string",
  "destinationGroup": {
    "id": "string",
    "name": "string"
  }
}
```

Properties

Name	Type	Required	Restrictions	Description
id	string	true	none	none
name	string	true	none	none
description	string	true	none	none
credentials	string	true	none	none
protocolType	StorageProtocolType	true	none	- 0: Smb - 1: GraphSdk - 2: BoxSdk - 3: AwsSdk - 4: AzureBlobSdk - 5: AlibabaCloudSdk - 6: GoogleCloudSdk - 7: AzureFilesSdk - 8: Sftp - 9: Nfs - 10: Mft - 11: SharepointOnPrem - 12: Ftp - 13: OracleSdk - 100: GitHubSdk - 101: DockerHubSdk - 102: BitbucketSdk - 103: AmazonEcrSdk - 104: QuaySdk - 105: JFrogContainerSdk - 106: JFrogBinarySdk - 107: AzureAcrSdk - 108: GitLabSourceSdk - 109: GitLabContainerSdk - 110: SvnSdk - 111: AzureDevOpsSourceSdk - 112: AzureDevOpsBinarySdk - 113: DirectFile - 114: NexusBinarySdk - 115: GiteaSdk - 116: HarborSdk
vendorType	StorageVendorType¦null	false	none	- 0: AmazonS3 - 1: OneDrive - 2: Box - 3: Dellsilon - 4: AzureFiles - 5: SmbCompatible - 6: S3Compatible - 7: AzureBlob

				- 8: AlibabaCloud - 9: GoogleCloud - 10: Sftp - 11: SharePoint - 12: Nfs - 13: Wasabi - 14: OracleCloud - 15: NetAppOntap - 16: Cubbit - 17: Mft - 18: SharepointOnPrem - 19: Ftp - 20: Oracle - 21: NfsSisl - 22: ScalityRing - 100: GitHub - 101: DockerHub - 102: Bitbucket - 103: AmazonEcr - 104: Quay - 105: JFrogContainer - 106: JFrogBinary - 107: AzureAcr - 108: GitLabSource - 109: GitLabContainer - 110: Svn - 111: AzureDevOpsSource - 112: AzureDevOpsBinary - 113: DirectFile - 114: NexusBinary - 115: Gitea - 116: Harbor
autoDiscovery	boolean	true	none	none
autodiscoveryDestinationGroupId	string¦null	false	none	none
destinationGroup	GroupReference¦null	false	none	none

StorageProtocolType

```
0
```

- 0: Smb
- 1: GraphSdk
- 2: BoxSdk

- 3: AwsSdk
- 4: AzureBlobSdk
- 5: AlibabaCloudSdk
- 6: GoogleCloudSdk
- 7: AzureFilesSdk
- 8: Sftp
- 9: Nfs
- 10: Mft
- 11: SharepointOnPrem
- 12: Ftp
- 13: OracleSdk
- 100: GitHubSdk
- 101: DockerHubSdk
- 102: BitbucketSdk
- 103: AmazonEcrSdk
- 104: QuaySdk
- 105: JFrogContainerSdk
- 106: JFrogBinarySdk
- 107: AzureAcrSdk
- 108: GitLabSourceSdk
- 109: GitLabContainerSdk
- 110: SvnSdk
- 111: AzureDevOpsSourceSdk
- 112: AzureDevOpsBinarySdk
- 113: DirectFile
- 114: NexusBinarySdk
- 115: GiteaSdk
- 116: HarborSdk

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: Smb - 1: GraphSdk - 2: BoxSdk - 3: AwsSdk - 4: AzureBlobSdk - 5: AlibabaCloudSdk - 6: GoogleCloudSdk - 7: AzureFilesSdk - 8: Sftp - 9: Nfs - 10: Mft - 11: SharepointOnPrem - 12: Ftp - 13: OracleSdk - 100: GitHubSdk - 101: DockerHubSdk - 102: BitbucketSdk - 103: AmazonEcrSdk - 104: QuaySdk - 105: JFrogContainerSdk - 106: JFrogBinarySdk - 107: AzureAcrSdk - 108: GitLabSourceSdk - 109: GitLabContainerSdk - 110: SvnSdk - 111: AzureDevOpsSourceSdk - 112: AzureDevOpsBinarySdk - 113: DirectFile - 114: NexusBinarySdk - 115: GiteaSdk - 116: HarborSdk

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2
anonymous	3
anonymous	4
anonymous	5
anonymous	6
anonymous	7
anonymous	8
anonymous	9
anonymous	10
anonymous	11
anonymous	12
anonymous	13
anonymous	100
anonymous	101
anonymous	102
anonymous	103
anonymous	104
anonymous	105
anonymous	106
anonymous	107
anonymous	108
anonymous	109
anonymous	110
anonymous	111
anonymous	112

anonymous	113
anonymous	114
anonymous	115
anonymous	116

StorageVendorType

```
0
```

- 0: AmazonS3
- 1: OneDrive
- 2: Box
- 3: DellIsilon
- 4: AzureFiles
- 5: SmbCompatible
- 6: S3Compatible
- 7: AzureBlob
- 8: AlibabaCloud
- 9: GoogleCloud
- 10: Sftp
- 11: SharePoint
- 12: Nfs
- 13: Wasabi
- 14: OracleCloud
- 15: NetAppOntap
- 16: Cubbit
- 17: Mft
- 18: SharepointOnPrem
- 19: Ftp
- 20: Oracle
- 21: NfsSisl
- 22: ScalityRing
- 100: GitHub
- 101: DockerHub
- 102: Bitbucket

- 103: AmazonEcr
- 104: Quay
- 105: JFrogContainer
- 106: JFrogBinary
- 107: AzureAcr
- 108: GitLabSource
- 109: GitLabContainer
- 110: Svn
- 111: AzureDevOpsSource
- 112: AzureDevOpsBinary
- 113: DirectFile
- 114: NexusBinary
- 115: Gitea
- 116: Harbor

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: AmazonS3 - 1: OneDrive - 2: Box - 3: DellIsilon - 4: AzureFiles - 5: SmbCompatible - 6: S3Compatible - 7: AzureBlob - 8: AlibabaCloud - 9: GoogleCloud - 10: Sftp - 11: SharePoint - 12: Nfs - 13: Wasabi - 14: OracleCloud - 15: NetAppOntap - 16: Cubbit - 17: Mft - 18: SharepointOnPrem - 19: Ftp - 20: Oracle - 21: NfsSisl - 22: ScalityRing - 100: GitHub - 101: DockerHub - 102: Bitbucket - 103: AmazonEcr - 104: Quay - 105: JFrogContainer - 106: JFrogBinary - 107: AzureAcr - 108: GitLabSource - 109: GitLabContainer - 110: Svn - 111: AzureDevOpsSource - 112: AzureDevOpsBinary - 113: DirectFile - 114: NexusBinary - 115: Gitea - 116: Harbor

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2
anonymous	3
anonymous	4
anonymous	5
anonymous	6
anonymous	7
anonymous	8
anonymous	9
anonymous	10
anonymous	11
anonymous	12
anonymous	13
anonymous	14
anonymous	15
anonymous	16
anonymous	17
anonymous	18
anonymous	19
anonymous	20
anonymous	21
anonymous	22
anonymous	100
anonymous	101
anonymous	102
anonymous	103

anonymous	104
anonymous	105
anonymous	106
anonymous	107
anonymous	108
anonymous	109
anonymous	110
anonymous	111
anonymous	112
anonymous	113
anonymous	114
anonymous	115
anonymous	116

GroupReference

```
{
  "id": "string",
  "name": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
id	string	true	none	none
name	string	true	none	none

StorageProtocolType2

```
0
```

- 0: Smb

- 1: GraphSdk
- 2: BoxSdk
- 3: AwsSdk
- 4: AzureBlobSdk
- 5: AlibabaCloudSdk
- 6: GoogleCloudSdk
- 7: AzureFilesSdk
- 8: Sftp
- 9: Nfs
- 10: Mft
- 11: SharepointOnPrem
- 12: Ftp
- 13: OracleSdk

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: Smb - 1: GraphSdk - 2: BoxSdk - 3: AwsSdk - 4: AzureBlobSdk - 5: AlibabaCloudSdk - 6: GoogleCloudSdk - 7: AzureFilesSdk - 8: Sftp - 9: Nfs - 10: Mft - 11: SharepointOnPrem - 12: Ftp - 13: OracleSdk

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2
anonymous	3
anonymous	4
anonymous	5
anonymous	6
anonymous	7
anonymous	8
anonymous	9
anonymous	10
anonymous	11
anonymous	12
anonymous	13

StorageVendorType2

```
0
```

- 0: AmazonS3
- 1: OneDrive
- 2: Box
- 3: DellIsilon
- 4: AzureFiles
- 5: SmbCompatible
- 6: S3Compatible
- 7: AzureBlob
- 8: AlibabaCloud
- 9: GoogleCloud

- 10: Sftp
- 11: SharePoint
- 12: Nfs
- 13: Wasabi
- 14: OracleCloud
- 15: NetAppOntap
- 16: Cubbit
- 17: Mft
- 18: SharepointOnPrem
- 19: Ftp
- 20: Oracle
- 21: NfsSisl
- 22: ScalityRing

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: AmazonS3 - 1: OneDrive - 2: Box - 3: DellIsilon - 4: AzureFiles - 5: SmbCompatible - 6: S3Compatible - 7: AzureBlob - 8: AlibabaCloud - 9: GoogleCloud - 10: Sftp - 11: SharePoint - 12: Nfs - 13: Wasabi - 14: OracleCloud - 15: NetAppOntap - 16: Cubbit - 17: Mft - 18: SharepointOnPrem - 19: Ftp - 20: Oracle - 21: NfsSisl - 22: ScalityRing

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2
anonymous	3
anonymous	4
anonymous	5
anonymous	6
anonymous	7
anonymous	8
anonymous	9
anonymous	10
anonymous	11
anonymous	12
anonymous	13
anonymous	14
anonymous	15
anonymous	16
anonymous	17
anonymous	18
anonymous	19
anonymous	20
anonymous	21
anonymous	22

BulkDeleteAccountsCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "succeeded": [
    "string"
  ],
  "failed": [
    {
      "id": "string",
      "reasonKey": "string",
      "reason": "string",
      "childFailures": [
        {}
      ]
    }
  ],
  "confirmationRequired": true,
  "preview": [
    {
      "accountId": "string",
      "memberStorageIds": [
        "string"
      ]
    }
  ],
  "scansRunning": true,
  "runningScans": [
    {
      "scanId": "string",
      "storageId": "string",
      "accountId": "string",
      "groupId": "string"
    }
  ]
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» succeeded	[string]	false	none	none
» failed	[BulkFailedItem]	false	none	none
» confirmationRequired	boolean	false	none	none
» preview	[BulkAccountPreviewItem]	false	none	none
» scansRunning	boolean	false	none	none
» runningScans	[BulkRunningScan]	false	none	none

BulkFailedItem

```
{
  "id": "string",
  "reasonKey": "string",
  "reason": "string",
  "childFailures": [
    {
      "id": "string",
      "reasonKey": "string",
      "reason": "string",
      "childFailures": []
    }
  ]
}
```

Properties

Name	Type	Required	Restrictions	Description
id	string	false	none	none
reasonKey	string	false	none	none
reason	string	false	none	none
childFailures	[BulkFailedItem]	false	none	none

BulkAccountPreviewItem

```
{
  "accountId": "string",
  "memberStorageIds": [
    "string"
  ]
}
```

Properties

Name	Type	Required	Restrictions	Description
accountId	string	false	none	none
memberStorageIds	[string]	false	none	none

BulkRunningScan

```
{
  "scanId": "string",
  "storageId": "string",
  "accountId": "string",
  "groupId": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
scanId	string	false	none	none
storageId	string	false	none	none
accountId	string¦null	false	none	none
groupId	string¦null	false	none	none

BulkDeleteAccountsParameters

```
{
  "accountIds": [
    "string"
  ],
  "forceDelete": true
}
```

Properties

Name	Type	Required	Restrictions	Description
accountIds	[string]	false	none	none
forceDelete	boolean	true	none	none

GetAccountById

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "account": {
    "id": "string",
    "name": "string",
    "description": "string",
    "storages": [
      {
        "id": "string",
        "groupId": "string",
        "accountId": "string",
        "name": "string",
        "storageClientId": "string",
        "storageType": {
          "name": "string",
          "categoryType": 0,
          "protocolType": 0,
          "vendorType": 0
        },
        "storageStatus": {
          "message": "string",
          "statusType": 0
        },
        "scansInProgress": true,
        "isRtpInProgress": true,
        "isScheduledScanInProgress": true,
        "storageFunctionality": "string",
        "isAutodiscovered": true,
        "groupRef": {
          "id": "string",
          "name": "string"
        },
        "$type": "string"
      }
    ],
    "credentials": "string",
    "autoDiscovery": true,
    "groupId": "string",
    "destinationGroup": {
      "id": "string",
      "name": "string"
    },
    "protocolType": 0,
    "vendorType": 0
  }
```

```
}
```

Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» account	AccountWithStorage	true	none	none

AccountWithStorage

```
{
  "id": "string",
  "name": "string",
  "description": "string",
  "storages": [
    {
      "id": "string",
      "groupId": "string",
      "accountId": "string",
      "name": "string",
      "storageClientId": "string",
      "storageType": {
        "name": "string",
        "categoryType": 0,
        "protocolType": 0,
        "vendorType": 0
      },
      "storageStatus": {
        "message": "string",
        "statusType": 0
      },
      "scansInProgress": true,
      "isRtpInProgress": true,
      "isScheduledScanInProgress": true,
      "storageFunctionality": "string",
      "isAutodiscovered": true,
      "groupRef": {
        "id": "string",
        "name": "string"
      },
      "$type": "string"
    }
  ],
  "credentials": "string",
  "autoDiscovery": true,
  "groupId": "string",
  "destinationGroup": {
    "id": "string",
    "name": "string"
  },
  "protocolType": 0,
  "vendorType": 0
}
```

Properties

Name	Type	Required	Restrictions	Description
id	string	true	none	none
name	string	true	none	none
description	string	true	none	none
storages	[Storage]¦null	false	none	none
credentials	string	true	none	none
autoDiscovery	boolean	true	none	none
groupId	string¦null	false	none	none
destinationGroup	GroupReference¦null	false	none	none
protocolType	integer(int32)	true	none	none
vendorType	integer(int32)¦null	false	none	none

Storage

```
{
  "id": "string",
  "groupId": "string",
  "accountId": "string",
  "name": "string",
  "storageClientId": "string",
  "storageType": {
    "name": "string",
    "categoryType": 0,
    "protocolType": 0,
    "vendorType": 0
  },
  "storageStatus": {
    "message": "string",
    "statusType": 0
  },
  "scansInProgress": true,
  "isRtpInProgress": true,
  "isScheduledScanInProgress": true,
  "storageFunctionality": "string",
  "isAutodiscovered": true,
  "groupRef": {
    "id": "string",
    "name": "string"
  },
  "$type": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
id	string	false	none	none
groupId	string	false	none	none
accountId	string	false	none	none
name	string	false	none	none
storageClientId	string	false	none	none
storageType	StorageType	false	none	none
storageStatus	StorageStatus	false	none	none
scansInProgress	boolean	false	none	none
isRtpInProgress	boolean	false	none	none
isScheduledScanInProgress	boolean	false	none	none
storageFunctionality	string	false	none	none
isAutodiscovered	boolean	false	none	none
groupRef	GroupReference¦null	false	none	none
$type	string	true	none	none

StorageType

```
{
  "name": "string",
  "categoryType": 0,
  "protocolType": 0,
  "vendorType": 0
}
```

Properties

Name	Type	Required	Restrictions	Description
name	string	false	none	none
categoryType	StorageCategoryType	false	none	- 0: Local - 1: Cloud - 2: Object
protocolType	StorageProtocolType2	false	none	- 0: Smb - 1: GraphSdk - 2: BoxSdk - 3: AwsSdk - 4: AzureBlobSdk - 5: AlibabaCloudSdk - 6: GoogleCloudSdk - 7: AzureFilesSdk - 8: Sftp - 9: Nfs - 10: Mft - 11: SharepointOnPrem - 12: Ftp - 13: OracleSdk
vendorType	StorageVendorType2	false	none	- 0: AmazonS3 - 1: OneDrive - 2: Box - 3: DellIsilon - 4: AzureFiles - 5: SmbCompatible - 6: S3Compatible - 7: AzureBlob - 8: AlibabaCloud - 9: GoogleCloud - 10: Sftp - 11: SharePoint - 12: Nfs - 13: Wasabi - 14: OracleCloud - 15: NetAppOntap - 16: Cubbit - 17: Mft - 18: SharepointOnPrem - 19: Ftp - 20: Oracle - 21: NfsSisl - 22: ScalityRing

StorageCategoryType

```
0
```

- 0: Local
- 1: Cloud
- 2: Object

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: Local - 1: Cloud - 2: Object

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2

StorageStatus

```
{
  "message": "string",
  "statusType": 0
}
```

Properties

Name	Type	Required	Restrictions	Description
message	string|null	false	none	none
statusType	integer(int32)	true	none	none

AmazonSdkStorage


```
{
  "id": "string",
  "groupId": "string",
  "accountId": "string",
  "name": "string",
  "storageClientId": "string",
  "storageType": {
    "name": "string",
    "categoryType": 0,
    "protocolType": 0,
    "vendorType": 0
  },
  "storageStatus": {
    "message": "string",
    "statusType": 0
  },
  "scansInProgress": true,
  "isRtpInProgress": true,
  "isScheduledScanInProgress": true,
  "storageFunctionality": "string",
  "isAutodiscovered": true,
  "groupRef": {
    "id": "string",
    "name": "string"
  },
  "$type": "string",
  "serviceUrl": {
    "property1": "string",
    "property2": "string"
  },
  "bucketName": "string",
  "folderLocation": "string"
}
```


Properties

allOf - discriminator: Storage.$type

Name	Type	Required	Restrictions	Description
anonymous	Storage	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» serviceUrl	object	false	none	none
»» **additionalProperties**	string	false	none	none
» bucketName	string	false	none	none
» folderLocation	string	false	none	none

AlibabaCloudStorage


```
{
  "id": "string",
  "groupId": "string",
  "accountId": "string",
  "name": "string",
  "storageClientId": "string",
  "storageType": {
    "name": "string",
    "categoryType": 0,
    "protocolType": 0,
    "vendorType": 0
  },
  "storageStatus": {
    "message": "string",
    "statusType": 0
  },
  "scansInProgress": true,
  "isRtpInProgress": true,
  "isScheduledScanInProgress": true,
  "storageFunctionality": "string",
  "isAutodiscovered": true,
  "groupRef": {
    "id": "string",
    "name": "string"
  },
  "$type": "string",
  "bucketName": "string",
  "folderLocation": "string"
}
```


Properties

allOf - discriminator: Storage.$type

Name	Type	Required	Restrictions	Description
anonymous	Storage	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» bucketName	string	false	none	none
» folderLocation	string	false	none	none

AzureBlobStorage


```
{
  "id": "string",
  "groupId": "string",
  "accountId": "string",
  "name": "string",
  "storageClientId": "string",
  "storageType": {
    "name": "string",
    "categoryType": 0,
    "protocolType": 0,
    "vendorType": 0
  },
  "storageStatus": {
    "message": "string",
    "statusType": 0
  },
  "scansInProgress": true,
  "isRtpInProgress": true,
  "isScheduledScanInProgress": true,
  "storageFunctionality": "string",
  "isAutodiscovered": true,
  "groupRef": {
    "id": "string",
    "name": "string"
  },
  "$type": "string",
  "container": "string"
}
```


Properties

allOf - discriminator: Storage.$type

Name	Type	Required	Restrictions	Description
anonymous	Storage	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» container	string	false	none	none

AzureFilesStorage


```
{
  "id": "string",
  "groupId": "string",
  "accountId": "string",
  "name": "string",
  "storageClientId": "string",
  "storageType": {
    "name": "string",
    "categoryType": 0,
    "protocolType": 0,
    "vendorType": 0
  },
  "storageStatus": {
    "message": "string",
    "statusType": 0
  },
  "scansInProgress": true,
  "isRtpInProgress": true,
  "isScheduledScanInProgress": true,
  "storageFunctionality": "string",
  "isAutodiscovered": true,
  "groupRef": {
    "id": "string",
    "name": "string"
  },
  "$type": "string",
  "folderLocation": "string",
  "shareName": "string"
}
```


Properties

allOf - discriminator: Storage.$type

Name	Type	Required	Restrictions	Description
anonymous	Storage	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» folderLocation	string	false	none	none
» shareName	string	false	none	none

BoxStorage


```
{
  "id": "string",
  "groupId": "string",
  "accountId": "string",
  "name": "string",
  "storageClientId": "string",
  "storageType": {
    "name": "string",
    "categoryType": 0,
    "protocolType": 0,
    "vendorType": 0
  },
  "storageStatus": {
    "message": "string",
    "statusType": 0
  },
  "scansInProgress": true,
  "isRtpInProgress": true,
  "isScheduledScanInProgress": true,
  "storageFunctionality": "string",
  "isAutodiscovered": true,
  "groupRef": {
    "id": "string",
    "name": "string"
  },
  "$type": "string",
  "userName": "string",
  "groupName": "string",
  "userId": "string",
  "folderPath": "string"
}
```

Properties

allOf - discriminator: Storage.$type

Name	Type	Required	Restrictions	Description
anonymous	Storage	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» userName	string	false	none	none
» groupName	string	false	none	none
» userId	string	false	none	none
» folderPath	string	false	none	none

GoogleCloudStorage

```
{
  "id": "string",
  "groupId": "string",
  "accountId": "string",
  "name": "string",
  "storageClientId": "string",
  "storageType": {
    "name": "string",
    "categoryType": 0,
    "protocolType": 0,
    "vendorType": 0
  },
  "storageStatus": {
    "message": "string",
    "statusType": 0
  },
  "scansInProgress": true,
  "isRtpInProgress": true,
  "isScheduledScanInProgress": true,
  "storageFunctionality": "string",
  "isAutodiscovered": true,
  "groupRef": {
    "id": "string",
    "name": "string"
  },
  "$type": "string",
  "bucketName": "string",
  "folderLocation": "string"
}
```


Properties

allOf - discriminator: Storage.$type

Name	Type	Required	Restrictions	Description
anonymous	Storage	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» bucketName	string	false	none	none
» folderLocation	string	false	none	none

GraphStorage


```
{
  "id": "string",
  "groupId": "string",
  "accountId": "string",
  "name": "string",
  "storageClientId": "string",
  "storageType": {
    "name": "string",
    "categoryType": 0,
    "protocolType": 0,
    "vendorType": 0
  },
  "storageStatus": {
    "message": "string",
    "statusType": 0
  },
  "scansInProgress": true,
  "isRtpInProgress": true,
  "isScheduledScanInProgress": true,
  "storageFunctionality": "string",
  "isAutodiscovered": true,
  "groupRef": {
    "id": "string",
    "name": "string"
  },
  "$type": "string",
  "group": "string",
  "groupUrl": "string",
  "member": {
    "id": "string",
    "name": "string",
    "nameUrl": "string"
  },
  "folderLocation": "string",
  "userInfo": {
    "upn": "string",
    "userId": "string"
  }
}
```


Properties

allOf - discriminator: Storage.$type

Name	Type	Required	Restrictions	Description
anonymous	Storage	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» group	string¦null	false	none	none
» groupUrl	string¦null	false	none	none
» member	StorageMember¦null	false	none	none
» folderLocation	string¦null	false	none	none
» userInfo	GraphUserInfo¦null	false	none	none

StorageMember

```
{
  "id": "string",
  "name": "string",
  "nameUrl": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
id	string¦null	false	none	none
name	string¦null	false	none	none
nameUrl	string¦null	false	none	none

GraphUserInfo

```
{
  "upn": "string",
  "userId": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
upn	string¦null	false	none	none
userId	string¦null	false	none	none

SftpStorage


```
{
  "id": "string",
  "groupId": "string",
  "accountId": "string",
  "name": "string",
  "storageClientId": "string",
  "storageType": {
    "name": "string",
    "categoryType": 0,
    "protocolType": 0,
    "vendorType": 0
  },
  "storageStatus": {
    "message": "string",
    "statusType": 0
  },
  "scansInProgress": true,
  "isRtpInProgress": true,
  "isScheduledScanInProgress": true,
  "storageFunctionality": "string",
  "isAutodiscovered": true,
  "groupRef": {
    "id": "string",
    "name": "string"
  },
  "$type": "string",
  "sharePath": "string"
}
```


Properties

allOf - discriminator: Storage.$type

Name	Type	Required	Restrictions	Description
anonymous	Storage	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» sharePath	string¦null	false	none	none

SmbStorage


```
{
  "id": "string",
  "groupId": "string",
  "accountId": "string",
  "name": "string",
  "storageClientId": "string",
  "storageType": {
    "name": "string",
    "categoryType": 0,
    "protocolType": 0,
    "vendorType": 0
  },
  "storageStatus": {
    "message": "string",
    "statusType": 0
  },
  "scansInProgress": true,
  "isRtpInProgress": true,
  "isScheduledScanInProgress": true,
  "storageFunctionality": "string",
  "isAutodiscovered": true,
  "groupRef": {
    "id": "string",
    "name": "string"
  },
  "$type": "string",
  "sharePath": "string"
}
```


Properties

allOf - discriminator: Storage.$type

Name	Type	Required	Restrictions	Description
anonymous	Storage	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» sharePath	string	false	none	none

NfsStorage


```
{
  "id": "string",
  "groupId": "string",
  "accountId": "string",
  "name": "string",
  "storageClientId": "string",
  "storageType": {
    "name": "string",
    "categoryType": 0,
    "protocolType": 0,
    "vendorType": 0
  },
  "storageStatus": {
    "message": "string",
    "statusType": 0
  },
  "scansInProgress": true,
  "isRtpInProgress": true,
  "isScheduledScanInProgress": true,
  "storageFunctionality": "string",
  "isAutodiscovered": true,
  "groupRef": {
    "id": "string",
    "name": "string"
  },
  "$type": "string",
  "user": "string",
  "sharePath": "string"
}
```


Properties

allOf - discriminator: Storage.$type

Name	Type	Required	Restrictions	Description
anonymous	Storage	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» user	string	false	none	none
» sharePath	string	false	none	none

MftStorage


```
{
  "id": "string",
  "groupId": "string",
  "accountId": "string",
  "name": "string",
  "storageClientId": "string",
  "storageType": {
    "name": "string",
    "categoryType": 0,
    "protocolType": 0,
    "vendorType": 0
  },
  "storageStatus": {
    "message": "string",
    "statusType": 0
  },
  "scansInProgress": true,
  "isRtpInProgress": true,
  "isScheduledScanInProgress": true,
  "storageFunctionality": "string",
  "isAutodiscovered": true,
  "groupRef": {
    "id": "string",
    "name": "string"
  },
  "$type": "string",
  "folderLocation": "string",
  "scanUsers": "string"
}
```


Properties

allOf - discriminator: Storage.$type

Name	Type	Required	Restrictions	Description
anonymous	Storage	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» folderLocation	string	false	none	none
» scanUsers	string	false	none	none

SharepointOnPremStorage


```
{
  "id": "string",
  "groupId": "string",
  "accountId": "string",
  "name": "string",
  "storageClientId": "string",
  "storageType": {
    "name": "string",
    "categoryType": 0,
    "protocolType": 0,
    "vendorType": 0
  },
  "storageStatus": {
    "message": "string",
    "statusType": 0
  },
  "scansInProgress": true,
  "isRtpInProgress": true,
  "isScheduledScanInProgress": true,
  "storageFunctionality": "string",
  "isAutodiscovered": true,
  "groupRef": {
    "id": "string",
    "name": "string"
  },
  "$type": "string",
  "documentLibrary": "string",
  "documentLibraryUrl": "string",
  "folderLocation": "string"
}
```


Properties

allOf - discriminator: Storage.$type

Name	Type	Required	Restrictions	Description
anonymous	Storage	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» documentLibrary	string	false	none	none
» documentLibraryUrl	string	false	none	none
» folderLocation	string	false	none	none

FtpStorage


```
{
  "id": "string",
  "groupId": "string",
  "accountId": "string",
  "name": "string",
  "storageClientId": "string",
  "storageType": {
    "name": "string",
    "categoryType": 0,
    "protocolType": 0,
    "vendorType": 0
  },
  "storageStatus": {
    "message": "string",
    "statusType": 0
  },
  "scansInProgress": true,
  "isRtpInProgress": true,
  "isScheduledScanInProgress": true,
  "storageFunctionality": "string",
  "isAutodiscovered": true,
  "groupRef": {
    "id": "string",
    "name": "string"
  },
  "$type": "string",
  "folderPath": "string"
}
```

Properties

allOf - discriminator: Storage.$type

Name	Type	Required	Restrictions	Description
anonymous	Storage	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» folderPath	string¦null	false	none	none

OracleSdkStorage


```
{
  "id": "string",
  "groupId": "string",
  "accountId": "string",
  "name": "string",
  "storageClientId": "string",
  "storageType": {
    "name": "string",
    "categoryType": 0,
    "protocolType": 0,
    "vendorType": 0
  },
  "storageStatus": {
    "message": "string",
    "statusType": 0
  },
  "scansInProgress": true,
  "isRtpInProgress": true,
  "isScheduledScanInProgress": true,
  "storageFunctionality": "string",
  "isAutodiscovered": true,
  "groupRef": {
    "id": "string",
    "name": "string"
  },
  "$type": "string",
  "bucketName": "string",
  "folderLocation": "string"
}
```

Properties

allOf - discriminator: Storage.$type

Name	Type	Required	Restrictions	Description
anonymous	Storage	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» bucketName	string¦null	false	none	none
» folderLocation	string¦null	false	none	none

EnumerateAccountStoragesQueryResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "entries": [
    {
      "autodiscoverySource": "string",
      "autodiscoverySourceUrl": "string"
    }
  ],
  "protocolType": 0,
  "vendorType": 0
}
```

Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» entries	[AccountStorage]	false	none	none
» protocolType	integer(int32)¦null	false	none	none
» vendorType	integer(int32)¦null	false	none	none

AccountStorage

```
{
  "autodiscoverySource": "string",
  "autodiscoverySourceUrl": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
autodiscoverySource	string¦null	true	none	none
autodiscoverySourceUrl	string¦null	false	none	none

ListAccounts

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "items": [
    {
      "id": "string",
      "name": "string",
      "description": "string",
      "storages": [
        {
          "id": "string",
          "groupId": "string",
          "accountId": "string",
          "name": "string",
          "storageClientId": "string",
          "storageType": {
            "name": "string",
            "categoryType": 0,
            "protocolType": 0,
            "vendorType": 0
          },
          "storageStatus": {
            "message": "string",
            "statusType": 0
          },
          "scansInProgress": true,
          "isRtpInProgress": true,
          "isScheduledScanInProgress": true,
          "storageFunctionality": "string",
          "isAutodiscovered": true,
          "groupRef": {
            "id": "string",
            "name": "string"
          },
          "$type": "string"
        }
      ],
      "credentials": "string",
      "autoDiscovery": true,
      "groupId": "string",
      "destinationGroup": {
        "id": "string",
        "name": "string"
      },
      "protocolType": 0,
      "vendorType": 0
    }
```

```
"accounts": [
    {
      "id": "string",
      "name": "string",
      "description": "string",
      "storages": [
        {
          "id": "string",
          "groupId": "string",
          "accountId": "string",
          "name": "string",
          "storageClientId": "string",
          "storageType": {
            "name": "string",
            "categoryType": 0,
            "protocolType": 0,
            "vendorType": 0
          },
          "storageStatus": {
            "message": "string",
            "statusType": 0
          },
          "scansInProgress": true,
          "isRtpInProgress": true,
          "isScheduledScanInProgress": true,
          "storageFunctionality": "string",
          "isAutodiscovered": true,
          "groupRef": {
            "id": "string",
            "name": "string"
          },
          "$type": "string"
        }
      ],
      "credentials": "string",
      "autoDiscovery": true,
      "groupId": "string",
      "destinationGroup": {
        "id": "string",
        "name": "string"
      },
      "protocolType": 0,
      "vendorType": 0
    }
  ],
  "totalCount": 0,
  "startIndex": 0,
  "count": 0
}
```

Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» items	[AccountWithStorage]¦null	false	none	none
» accounts	[AccountWithStorage]¦null	false	none	none
» totalCount	integer(int32)	false	none	none
» startIndex	integer(int32)	false	none	none
» count	integer(int32)	false	none	none

ListSortOption

```
0
```

- 0: Id
- 1: Name

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: Id - 1: Name

Enumerated Values

Property	Value
anonymous	0
anonymous	1

SortingOrder

```
0
```

- 0: Ascending
- 1: Descending

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: Ascending - 1: Descending

Enumerated Values

Property	Value
anonymous	0
anonymous	1

GetAccountsCount

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "accountCount": {
    "count": 0
  }
}
```

Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» accountCount	CountResult	true	none	none

CountResult

```
{
  "count": 0
}
```

Properties

Name	Type	Required	Restrictions	Description
count	integer(int64)	false	none	none

UpdateAccountCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "accountId": "string"
}
```

Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» accountId	string¦null	false	none	none

EnumerateAccountSourcesQueryResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "entries": [
    "string"
  ]
}
```

Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» entries	[string]¦null	false	none	none

EnumerateLogsQueryResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "entries": [
    {
      "id": "string",
      "logLevel": 0,
      "details": "string",
      "logType": 0,
      "userId": "string",
      "category": 0,
      "timeStamp": "2019-08-24T14:15:22Z",
      "userName": "string"
    }
  ],
  "filterCount": 0,
  "totalCount": 0
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» result	ResultType2	false	none	- 0: Success - 1: Error - 2: InternalError
» entries	[AuditLog]¦null	false	none	none
» filterCount	integer(int64)	false	none	none
» totalCount	integer(int64)	false	none	none

ResultType2

```
0
```

- 0: Success
- 1: Error
- 2: InternalError

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: Success - 1: Error - 2: InternalError

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2

AuditLog

```
{
  "id": "string",
  "logLevel": 0,
  "details": "string",
  "logType": 0,
  "userId": "string",
  "category": 0,
  "timeStamp": "2019-08-24T14:15:22Z",
  "userName": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
id	string¦null	false	none	none
logLevel	AuditLogLevel	false	none	- 0: Debug - 1: Info - 2: Warn - 3: Error
details	string¦null	false	none	none
logType	LogType¦null	false	none	- 0: FileDiscovered - 1: FileScanned - 2: FileDiscoveryFailed - 3: FileCancelled - 100: ProcessStarted - 101: ProcessCompleted - 102: ProcessCancelled - 103: ProcessFailed - 200: FileTagged - 201: FileSanitizedKeptOriginal - 203: FileSanitizedDeletedOriginal - 204: FileDecryption - 205: BlockedFileMoved - 206: BlockedFileDeleted - 207: SanitizedFileMoved - 208: AllowedFileMoved - 209: BlockedFileCopied - 210: SanitizedFileCopied - 211: AllowedFileCopied - 212: BlockedFileKept - 213: AllowedFileKept - 214: SanitizedFileKept - 215: AllowedFileDeleted - 216: FileVersionsScanned - 217: DiscoveredFileDeleted - 218: DiscoveredFileMoved - 219: DiscoveredFileCopied - 220: DiscoveredFileKept - 221: SanitizedFileDeleted - 222: CdrUnsupportedFileMoved - 223: CdrUnsupportedFileCopied - 224: CdrUnsupportedFileDeleted - 225: CdrUnsupportedFileKept - 300: StorageAdded - 301: StorageUpdated - 302: StorageRemoved - 320: GroupAdded - 321: GroupUpdated

				- 322: GroupRemoved - 330: AccountAdded - 331: AccountUpdated - 332: AccountRemoved - 350: SecurityChecklistItem - 351: SecurityChecklistVerified - 400: Rtp - 410: FileTagging - 411: DeepCdrRemediation - 412: SanitizedFilesRemediation - 413: BlockedFilesRemediation - 414: TreatFilesWithSensitiveDataAsBlocked - 415: TreatFilesWithVulnerabilitiesAsBlocked - 416: AllowedFilesRemediation - 417: StrictBlockFilesStrategy - 418: ConfigurableBlockFilesStrategy - 419: DeletedEmptyFolders - 600: LoggedIn - 601: LoggedOut - 602: UserCreated - 603: UserRegistered - 604: UserRoleUpdated - 605: UserUpdated - 606: UserRemoved - 700: ScanInstanceAdd - 701: ScanInstanceUpdate - 702: ScanInstanceDelete - 703: ScanInstanceImport - 750: ScanPoolAdd - 751: ScanPoolUpdate - 752: ScanPoolDelete - 753: ScanPoolImport - 800: OnlineLicenseActivated - 801: OfflineLicenseActivated - 802: LicenseDeactivated - 900: ConfigurationImported - 901: ConfigurationExported - 950: Notifications - 975: Smtp - 1000: ExternalLoggerAdd - 1001: ExternalLoggerUpdate - 1002: ExternalLoggerDelete - 1100: DataRetention - 1200: ApiKeyAdd - 1201: ApiKeyUpdate - 1202: ApiKeyDelete - 1300: SsoConfiguration - 1400: WorkflowAdd

				- 1401: WorkflowUpdate - 1402: WorkflowDelete - 1403: WorkflowSetDefault - 1404: WorkflowImport - 1410: WorkflowTechnologies - 1500: ScanAdd - 1501: ScanUpdate - 1502: ScanDelete - 1503: ScanImport - 1600: OnDemandScanRequest - 1700: ReportGenerated - 1800: TourFinalized - 1900: ScanScheduleAdd - 1901: ScanScheduleUpdate - 1902: ScanScheduleDelete - 1903: ScanScheduleImport - 1904: ScanScheduleSkip - 2000: Encryption - 2101: RemediationAdd - 2102: RemediationUpdate - 2103: RemediationDelete - 2200: Certificates - 2300: Telemetry - 2400: AbacRoleAssigned - 2401: AbacRoleRemoved - 2402: AbacRoleCreated - 2403: AbacRoleDeleted - 2410: AbacPermissionAssigned - 2411: AbacPermissionRemoved - 2412: AbacRolesReplaced - 10105: ScanScheduleStart
userId	string¦null	false	none	none
category	AuditLogCategoryType	false	none	- 0: Processes - 1: PostActions - 2: StorageUnits - 3: Authentication - 4: Settings - 6: Users - 8: Notifications - 9: GroupUnits - 10: AccountUnits
timeStamp	string(date-time)¦null	false	none	none
userName	string¦null	false	none	none

AuditLogLevel

```
0
```

- 0: Debug
- 1: Info
- 2: Warn
- 3: Error

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: Debug - 1: Info - 2: Warn - 3: Error

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2
anonymous	3

LogType

```
0
```

- 0: FileDiscovered
- 1: FileScanned
- 2: FileDiscoveryFailed
- 3: FileCancelled
- 100: ProcessStarted
- 101: ProcessCompleted

- 102: ProcessCancelled
- 103: ProcessFailed
- 200: FileTagged
- 201: FileSanitizedKeptOriginal
- 203: FileSanitizedDeletedOriginal
- 204: FileDecryption
- 205: BlockedFileMoved
- 206: BlockedFileDeleted
- 207: SanitizedFileMoved
- 208: AllowedFileMoved
- 209: BlockedFileCopied
- 210: SanitizedFileCopied
- 211: AllowedFileCopied
- 212: BlockedFileKept
- 213: AllowedFileKept
- 214: SanitizedFileKept
- 215: AllowedFileDeleted
- 216: FileVersionsScanned
- 217: DiscoveredFileDeleted
- 218: DiscoveredFileMoved
- 219: DiscoveredFileCopied
- 220: DiscoveredFileKept
- 221: SanitizedFileDeleted
- 222: CdrUnsupportedFileMoved
- 223: CdrUnsupportedFileCopied
- 224: CdrUnsupportedFileDeleted
- 225: CdrUnsupportedFileKept
- 300: StorageAdded
- 301: StorageUpdated
- 302: StorageRemoved
- 320: GroupAdded
- 321: GroupUpdated
- 322: GroupRemoved
- 330: AccountAdded
- 331: AccountUpdated
- 332: AccountRemoved
- 350: SecurityChecklistItem

- 351: SecurityChecklistVerified
- 400: Rtp
- 410: FileTagging
- 411: DeepCdrRemediation
- 412: SanitizedFilesRemediation
- 413: BlockedFilesRemediation
- 414: TreatFilesWithSensitiveDataAsBlocked
- 415: TreatFilesWithVulnerabilitiesAsBlocked
- 416: AllowedFilesRemediation
- 417: StrictBlockFilesStrategy
- 418: ConfigurableBlockFilesStrategy
- 419: DeletedEmptyFolders
- 600: LoggedIn
- 601: LoggedOut
- 602: UserCreated
- 603: UserRegistered
- 604: UserRoleUpdated
- 605: UserUpdated
- 606: UserRemoved
- 700: ScanInstanceAdd
- 701: ScanInstanceUpdate
- 702: ScanInstanceDelete
- 703: ScanInstanceImport
- 750: ScanPoolAdd
- 751: ScanPoolUpdate
- 752: ScanPoolDelete
- 753: ScanPoolImport
- 800: OnlineLicenseActivated
- 801: OfflineLicenseActivated
- 802: LicenseDeactivated
- 900: ConfigurationImported
- 901: ConfigurationExported
- 950: Notifications
- 975: Smtp
- 1000: ExternalLoggerAdd
- 1001: ExternalLoggerUpdate
- 1002: ExternalLoggerDelete

- 1100: DataRetention
- 1200: ApiKeyAdd
- 1201: ApiKeyUpdate
- 1202: ApiKeyDelete
- 1300: SsoConfiguration
- 1400: WorkflowAdd
- 1401: WorkflowUpdate
- 1402: WorkflowDelete
- 1403: WorkflowSetDefault
- 1404: WorkflowImport
- 1410: WorkflowTechnologies
- 1500: ScanAdd
- 1501: ScanUpdate
- 1502: ScanDelete
- 1503: ScanImport
- 1600: OnDemandScanRequest
- 1700: ReportGenerated
- 1800: TourFinalized
- 1900: ScanScheduleAdd
- 1901: ScanScheduleUpdate
- 1902: ScanScheduleDelete
- 1903: ScanScheduleImport
- 1904: ScanScheduleSkip
- 2000: Encryption
- 2101: RemediationAdd
- 2102: RemediationUpdate
- 2103: RemediationDelete
- 2200: Certificates
- 2300: Telemetry
- 2400: AbacRoleAssigned
- 2401: AbacRoleRemoved
- 2402: AbacRoleCreated
- 2403: AbacRoleDeleted
- 2410: AbacPermissionAssigned
- 2411: AbacPermissionRemoved
- 2412: AbacRolesReplaced
- 10105: ScanScheduleStart

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: FileDiscovered - 1: FileScanned - 2: FileDiscoveryFailed - 3: FileCancelled - 100: ProcessStarted - 101: ProcessCompleted - 102: ProcessCancelled - 103: ProcessFailed - 200: FileTagged - 201: FileSanitizedKeptOriginal - 203: FileSanitizedDeletedOriginal - 204: FileDecryption - 205: BlockedFileMoved - 206: BlockedFileDeleted - 207: SanitizedFileMoved - 208: AllowedFileMoved - 209: BlockedFileCopied - 210: SanitizedFileCopied - 211: AllowedFileCopied - 212: BlockedFileKept - 213: AllowedFileKept - 214: SanitizedFileKept - 215: AllowedFileDeleted - 216: FileVersionsScanned - 217: DiscoveredFileDeleted - 218: DiscoveredFileMoved - 219: DiscoveredFileCopied - 220: DiscoveredFileKept - 221: SanitizedFileDeleted - 222: CdrUnsupportedFileMoved - 223: CdrUnsupportedFileCopied - 224: CdrUnsupportedFileDeleted - 225: CdrUnsupportedFileKept - 300: StorageAdded - 301: StorageUpdated - 302: StorageRemoved - 320: GroupAdded - 321: GroupUpdated - 322: GroupRemoved - 330: AccountAdded - 331: AccountUpdated - 332: AccountRemoved - 350: SecurityChecklistItem - 351: SecurityChecklistVerified - 400: Rtp - 410: FileTagging

				- 411: DeepCdrRemediation - 412: SanitizedFilesRemediation - 413: BlockedFilesRemediation - 414: TreatFilesWithSensitiveDataAsBlocked - 415: TreatFilesWithVulnerabilitiesAsBlocked - 416: AllowedFilesRemediation - 417: StrictBlockFilesStrategy - 418: ConfigurableBlockFilesStrategy - 419: DeletedEmptyFolders - 600: LoggedIn - 601: LoggedOut - 602: UserCreated - 603: UserRegistered - 604: UserRoleUpdated - 605: UserUpdated - 606: UserRemoved - 700: ScanInstanceAdd - 701: ScanInstanceUpdate - 702: ScanInstanceDelete - 703: ScanInstanceImport - 750: ScanPoolAdd - 751: ScanPoolUpdate - 752: ScanPoolDelete - 753: ScanPoolImport - 800: OnlineLicenseActivated - 801: OfflineLicenseActivated - 802: LicenseDeactivated - 900: ConfigurationImported - 901: ConfigurationExported - 950: Notifications - 975: Smtp - 1000: ExternalLoggerAdd - 1001: ExternalLoggerUpdate - 1002: ExternalLoggerDelete - 1100: DataRetention - 1200: ApiKeyAdd - 1201: ApiKeyUpdate - 1202: ApiKeyDelete - 1300: SsoConfiguration - 1400: WorkflowAdd - 1401: WorkflowUpdate - 1402: WorkflowDelete - 1403: WorkflowSetDefault - 1404: WorkflowImport - 1410: WorkflowTechnologies - 1500: ScanAdd - 1501: ScanUpdate - 1502: ScanDelete

				- 1503: ScanImport - 1600: OnDemandScanRequest - 1700: ReportGenerated - 1800: TourFinalized - 1900: ScanScheduleAdd - 1901: ScanScheduleUpdate - 1902: ScanScheduleDelete - 1903: ScanScheduleImport - 1904: ScanScheduleSkip - 2000: Encryption - 2101: RemediationAdd - 2102: RemediationUpdate - 2103: RemediationDelete - 2200: Certificates - 2300: Telemetry - 2400: AbacRoleAssigned - 2401: AbacRoleRemoved - 2402: AbacRoleCreated - 2403: AbacRoleDeleted - 2410: AbacPermissionAssigned - 2411: AbacPermissionRemoved - 2412: AbacRolesReplaced - 10105: ScanScheduleStart

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2
anonymous	3
anonymous	100
anonymous	101
anonymous	102
anonymous	103
anonymous	200
anonymous	201
anonymous	203
anonymous	204
anonymous	205
anonymous	206
anonymous	207
anonymous	208
anonymous	209
anonymous	210
anonymous	211
anonymous	212
anonymous	213
anonymous	214
anonymous	215
anonymous	216
anonymous	217
anonymous	218
anonymous	219

anonymous	220
anonymous	221
anonymous	222
anonymous	223
anonymous	224
anonymous	225
anonymous	300
anonymous	301
anonymous	302
anonymous	320
anonymous	321
anonymous	322
anonymous	330
anonymous	331
anonymous	332
anonymous	350
anonymous	351
anonymous	400
anonymous	410
anonymous	411
anonymous	412
anonymous	413
anonymous	414
anonymous	415
anonymous	416
anonymous	417
anonymous	418
anonymous	419
anonymous	600

anonymous	601
anonymous	602
anonymous	603
anonymous	604
anonymous	605
anonymous	606
anonymous	700
anonymous	701
anonymous	702
anonymous	703
anonymous	750
anonymous	751
anonymous	752
anonymous	753
anonymous	800
anonymous	801
anonymous	802
anonymous	900
anonymous	901
anonymous	950
anonymous	975
anonymous	1000
anonymous	1001
anonymous	1002
anonymous	1100
anonymous	1200
anonymous	1201
anonymous	1202
anonymous	1300

anonymous	1400
anonymous	1401
anonymous	1402
anonymous	1403
anonymous	1404
anonymous	1410
anonymous	1500
anonymous	1501
anonymous	1502
anonymous	1503
anonymous	1600
anonymous	1700
anonymous	1800
anonymous	1900
anonymous	1901
anonymous	1902
anonymous	1903
anonymous	1904
anonymous	2000
anonymous	2101
anonymous	2102
anonymous	2103
anonymous	2200
anonymous	2300
anonymous	2400
anonymous	2401
anonymous	2402
anonymous	2403
anonymous	2410

anonymous	2411
anonymous	2412
anonymous	10105

AuditLogCategoryType

```
0
```

- 0: Processes
- 1: PostActions
- 2: StorageUnits
- 3: Authentication
- 4: Settings
- 6: Users
- 8: Notifications
- 9: GroupUnits
- 10: AccountUnits

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: Processes - 1: PostActions - 2: StorageUnits - 3: Authentication - 4: Settings - 6: Users - 8: Notifications - 9: GroupUnits - 10: AccountUnits

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2
anonymous	3
anonymous	4
anonymous	6
anonymous	8
anonymous	9
anonymous	10

ImportSettingsCommandResponse


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "areSmtpSettingsImported": true,
  "isLicenseImported": true,
  "isRetentionImported": true,
  "areNotificationsImported": true,
  "hasNotificationsPartialFailure": true,
  "activationDto": {
    "result": 0,
    "responseKey": "string",
    "responseMessage": "string",
    "responseMessageParams": {
      "property1": "string",
      "property2": "string"
    }
  },
  "newLocalUserId": "string",
  "areUsersImported": true
}
```

Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» result	ResultType3	false	none	- 0: Success - 1: FailedToUpgradeConfigFile - 2: FailedRequestBodyIsEmpty - 3: FailedToActivateLicense - 4: FailedToDeserializeConfigFile - 5: FailedOutdatedVersion - 6: FailedInvalidConfigFile - 7: FailedMissingPassword - 8: FailedWrongPassword
» areSmtpSettingsImported	boolean	false	none	none
» isLicenseImported	boolean	false	none	none
» isRetentionImported	boolean	false	none	none
» areNotificationsImported	boolean	false	none	none
» hasNotificationsPartialFailure	boolean	false	none	none
» activationDto	Activation¦null	false	none	none
» newLocalUserId	string¦null	false	none	none
» areUsersImported	boolean	false	none	none

ResultType3

```
0
```

- 0: Success
- 1: FailedToUpgradeConfigFile
- 2: FailedRequestBodyIsEmpty
- 3: FailedToActivateLicense
- 4: FailedToDeserializeConfigFile
- 5: FailedOutdatedVersion
- 6: FailedInvalidConfigFile
- 7: FailedMissingPassword
- 8: FailedWrongPassword

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: Success - 1: FailedToUpgradeConfigFile - 2: FailedRequestBodyIsEmpty - 3: FailedToActivateLicense - 4: FailedToDeserializeConfigFile - 5: FailedOutdatedVersion - 6: FailedInvalidConfigFile - 7: FailedMissingPassword - 8: FailedWrongPassword

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2
anonymous	3
anonymous	4
anonymous	5
anonymous	6
anonymous	7
anonymous	8

Activation

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```

Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none

GetEnabledModules

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "enabledModules": [
    0
  ]
}
```

Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» enabledModules	[integer]¦null	false	none	none

EnumerateExternalLoggersQueryResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "entries": [
    {
      "id": "string",
      "isEnabled": true,
      "loggerType": 0,
      "connectionSettings": {
        "$type": "string"
      }
    }
  ]
}
```

Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» result	ResultType4	false	none	- 0: Success - 1: Error - 2: InternalError
» entries	[ExternalLoggerConfig]¦null	false	none	none

ResultType4

```
0
```

- 0: Success
- 1: Error
- 2: InternalError

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: Success - 1: Error - 2: InternalError

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2

ExternalLoggerConfig

```
{
  "id": "string",
  "isEnabled": true,
  "loggerType": 0,
  "connectionSettings": {
    "$type": "string"
  }
}
```


Properties

Name	Type	Required	Restrictions	Description
id	string¦null	false	none	none
isEnabled	boolean	true	none	none
loggerType	ExternalLoggerType	false	none	- 0: SyslogUdp - 1: Kafka - 2: TcpSyslog - 3: TcpSyslogWithTls
connectionSettings	ExternalLoggerConnectionSettings¦null	false	none	none

ExternalLoggerType


```
0
```


- 0: SyslogUdp
- 1: Kafka
- 2: TcpSyslog
- 3: TcpSyslogWithTls

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: SyslogUdp - 1: Kafka - 2: TcpSyslog - 3: TcpSyslogWithTls

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2
anonymous	3

ExternalLoggerConnectionSettings

```
{
  "$type": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
$type	string	true	none	none

SyslogUdpConnectionSettings

```
{
  "$type": "string",
  "serverAddress": "string",
  "port": 0,
  "facility": 0,
  "format": 0
}
```

Properties

allOf - discriminator: ExternalLoggerConnectionSettings.$type

Name	Type	Required	Restrictions	Description
anonymous	ExternalLoggerConnectionSettings	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» serverAddress	string¦null	false	none	none
» port	integer(int32)	false	none	none
» facility	SyslogFacility	false	none	- 0: KernelMessages - 1: UserLevelMessages - 2: MailSystem - 3: SystemDaemons - 4: SecurityOrAuthorizationMessages1 - 5: InternalMessages - 6: LinePrinterSubsystem - 7: NetworkNewsSubsystem - 8: UUCPSubsystem - 9: ClockDaemon1 - 10: SecurityOrAuthorizationMessages2 - 11: FTPDaemon - 12: NTPSubsystem - 13: LogAudit - 14: LogAlert - 15: ClockDaemon2 - 16: LocalUse0 - 17: LocalUse1 - 18: LocalUse2 - 19: LocalUse3 - 20: LocalUse4 - 21: LocalUse5 - 22: LocalUse6 - 23: LocalUse7
» format	SyslogOutputFormat	false	none	- 0: RFC5424

SyslogFacility

```
0
```

- 0: KernelMessages
- 1: UserLevelMessages
- 2: MailSystem
- 3: SystemDaemons

- 4: SecurityOrAuthorizationMessages1
- 5: InternalMessages
- 6: LinePrinterSubsystem
- 7: NetworkNewsSubsystem
- 8: UUCPSubsystem
- 9: ClockDaemon1
- 10: SecurityOrAuthorizationMessages2
- 11: FTPDaemon
- 12: NTPSubsystem
- 13: LogAudit
- 14: LogAlert
- 15: ClockDaemon2
- 16: LocalUse0
- 17: LocalUse1
- 18: LocalUse2
- 19: LocalUse3
- 20: LocalUse4
- 21: LocalUse5
- 22: LocalUse6
- 23: LocalUse7

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: KernelMessages - 1: UserLevelMessages - 2: MailSystem - 3: SystemDaemons - 4: SecurityOrAuthorizationMessages1 - 5: InternalMessages - 6: LinePrinterSubsystem - 7: NetworkNewsSubsystem - 8: UUCPSubsystem - 9: ClockDaemon1 - 10: SecurityOrAuthorizationMessages2 - 11: FTPDaemon - 12: NTPSubsystem - 13: LogAudit - 14: LogAlert - 15: ClockDaemon2 - 16: LocalUse0 - 17: LocalUse1 - 18: LocalUse2 - 19: LocalUse3 - 20: LocalUse4 - 21: LocalUse5 - 22: LocalUse6 - 23: LocalUse7

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2
anonymous	3
anonymous	4
anonymous	5
anonymous	6
anonymous	7
anonymous	8
anonymous	9
anonymous	10
anonymous	11
anonymous	12
anonymous	13
anonymous	14
anonymous	15
anonymous	16
anonymous	17
anonymous	18
anonymous	19
anonymous	20
anonymous	21
anonymous	22
anonymous	23

SyslogOutputFormat

```
0
```

- 0: RFC5424

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: RFC5424

Enumerated Values

Property	Value
anonymous	0

SyslogTcpConnectionSettings

```
{
  "$type": "string",
  "serverAddress": "string",
  "port": 0,
  "facility": 0,
  "format": 0
}
```

Properties

allOf - discriminator: ExternalLoggerConnectionSettings.$type

Name	Type	Required	Restrictions	Description
anonymous	ExternalLoggerConnectionSettings	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» serverAddress	string¦null	false	none	none
» port	integer(int32)	false	none	none
» facility	SyslogFacility	false	none	- 0: KernelMessages - 1: UserLevelMessages - 2: MailSystem - 3: SystemDaemons - 4: SecurityOrAuthorizationMessages1 - 5: InternalMessages - 6: LinePrinterSubsystem - 7: NetworkNewsSubsystem - 8: UUCPSubsystem - 9: ClockDaemon1 - 10: SecurityOrAuthorizationMessages2 - 11: FTPDaemon - 12: NTPSubsystem - 13: LogAudit - 14: LogAlert - 15: ClockDaemon2 - 16: LocalUse0 - 17: LocalUse1 - 18: LocalUse2 - 19: LocalUse3 - 20: LocalUse4 - 21: LocalUse5 - 22: LocalUse6 - 23: LocalUse7
» format	SyslogOutputFormat	false	none	- 0: RFC5424

KafkaConnectionSettings

```
{
  "$type": "string",
  "serverAddressWithPortList": "string",
  "topic": "string",
  "configuration": "string"
}
```

Properties

allOf - discriminator: ExternalLoggerConnectionSettings.$type

Name	Type	Required	Restrictions	Description
anonymous	ExternalLoggerConnectionSettings	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» serverAddressWithPortList	string¦null	false	none	none
» topic	string¦null	false	none	none
» configuration	string¦null	false	none	none

UpdateExternalLoggerStatusParameters

```
{
  "id": "string",
  "isEnabled": true
}
```

Properties

Name	Type	Required	Restrictions	Description
id	string	true	none	none
isEnabled	boolean	true	none	none

AddUdpSyslogExternalLoggerParameters

```
{
  "isEnabled": true,
  "serverAddress": "string",
  "port": 0,
  "loggerType": 0,
  "facility": 0,
  "format": 0,
  "$type": "string"
}
```


Properties

allOf - discriminator: AddUpdateSyslogExternalLoggersParameters.$type

Name	Type	Required	Restrictions	Description
anonymous	AddUpdateSyslogExternalLoggersParameters	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none

AddUpdateSyslogExternalLoggersParameters


```
{
  "isEnabled": true,
  "serverAddress": "string",
  "port": 0,
  "loggerType": 0,
  "facility": 0,
  "format": 0,
  "$type": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
isEnabled	boolean	true	none	none
serverAddress	string	true	none	none
port	integer(int32)	true	none	none
loggerType	ExternalLoggerType	false	none	- 0: SyslogUdp - 1: Kafka - 2: TcpSyslog - 3: TcpSyslogWithTls
facility	SyslogFacility	false	none	- 0: KernelMessages - 1: UserLevelMessages - 2: MailSystem - 3: SystemDaemons - 4: SecurityOrAuthorizationMessages1 - 5: InternalMessages - 6: LinePrinterSubsystem - 7: NetworkNewsSubsystem - 8: UUCPSubsystem - 9: ClockDaemon1 - 10: SecurityOrAuthorizationMessages2 - 11: FTPDaemon - 12: NTPSubsystem - 13: LogAudit - 14: LogAlert - 15: ClockDaemon2 - 16: LocalUse0 - 17: LocalUse1 - 18: LocalUse2 - 19: LocalUse3 - 20: LocalUse4 - 21: LocalUse5 - 22: LocalUse6 - 23: LocalUse7
format	SyslogOutputFormat	false	none	- 0: RFC5424
$type	string	true	none	none

UpdateUdpSyslogExternalLoggerParameters

```
{
  "isEnabled": true,
  "serverAddress": "string",
  "port": 0,
  "loggerType": 0,
  "facility": 0,
  "format": 0,
  "$type": "string",
  "id": "string"
}
```


Properties

allOf - discriminator: AddUpdateSyslogExternalLoggersParameters.$type

Name	Type	Required	Restrictions	Description
anonymous	AddUpdateSyslogExternalLoggersParameters	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» id	string	true	none	none

AddKafkaExternalLoggerParameters


```
{
  "isEnabled": true,
  "serverAddressWithPortList": "string",
  "loggerType": 0,
  "topic": "string",
  "configuration": "string",
  "$type": "string"
}
```


Properties

allOf - discriminator: AddUpdateKafkaExternalLoggersParameters.$type

Name	Type	Required	Restrictions	Description
anonymous	AddUpdateKafkaExternalLoggersParameters	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none

AddUpdateKafkaExternalLoggersParameters

```
{
  "isEnabled": true,
  "serverAddressWithPortList": "string",
  "loggerType": 0,
  "topic": "string",
  "configuration": "string",
  "$type": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
isEnabled	boolean	true	none	none
serverAddressWithPortList	string	true	none	none
loggerType	ExternalLoggerType	false	none	- 0: SyslogUdp - 1: Kafka - 2: TcpSyslog - 3: TcpSyslogWithTls
topic	string	true	none	none
configuration	string	true	none	none
$type	string	true	none	none

UpdateKafkaExternalLoggerParameters

```
{
  "isEnabled": true,
  "serverAddressWithPortList": "string",
  "loggerType": 0,
  "topic": "string",
  "configuration": "string",
  "$type": "string",
  "id": "string"
}
```


Properties

allOf - discriminator: AddUpdateKafkaExternalLoggersParameters.$type

Name	Type	Required	Restrictions	Description
anonymous	AddUpdateKafkaExternalLoggersParameters	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» id	string	true	none	none

OnDemandScanCommandResponse


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none

OnDemandScanParameters

```
{
  "fileId": "string",
  "fileIds": [
    "string"
  ],
  "scanId": "string",
  "storageProtocolType": 0,
  "passwords": [
    "string"
  ],
  "workflowId": "string",
  "mdssBaseUrl": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
fileId	string¦null	false	none	ID of the file to rescan
fileIds	[string]¦null	false	none	IDs of the files to rescan
scanId	string	true	none	scan ID associated with the file
storageProtocolType	integer(int32)	true	none	protocol used by the storage (e.g., SMB, S3)
passwords	[string]	true	none	optional passwords for encrypted file scanning
workflowId	string	true	none	workflow ID to be used for the on-demand scan
mdssBaseUrl	string¦null	false	none	base URL for MDSS, if not provided will use Request.Host

OnDemandFilteredScanParameters

```
{
  "scanId": "string",
  "workflowId": "string",
  "passwords": [
    "string"
  ],
  "filterParameters": {
    "expand": [
      "string"
    ],
    "startDate": "2019-08-24T14:15:22Z",
    "endDate": "2019-08-24T14:15:22Z",
    "search": "string",
    "scanType": [
      0
    ],
    "storageId": [
      "string"
    ],
    "scanId": [
      "string"
    ],
    "scanWorkflowSnapshotId": [
      "string"
    ],
    "processingState": [
      0
    ],
    "result": [
      0
    ],
    "scanAllResultI": [
      0
    ],
    "scanResultICount": [
      0
    ],
    "sandboxVerdict": [
      0
    ],
    "vulnerabilityCount": [
      0
    ],
    "hasVulnerabilities": true,
    "dlpDetection": true,
    "hasBlockedFileVersions": true,
    "remediations": [
      0
    ],
    "skippedScan": true,
    "sortBy": [
      0
```

```
"sortOrder": [
      0
    ]
  },
  "storageProtocolType": 0,
  "mdssBaseUrl": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
scanId	string	true	none	scan ID associated with the file
workflowId	string	true	none	workflow ID to use when re-scanning
passwords	[string]¦null	false	none	optional passwords for encrypted file scanning
filterParameters	FileFilterSortParameters	true	none	Filters to select files to be re-scanned
storageProtocolType	integer(int32)	true	none	storage protocol type to use when re-scanning
mdssBaseUrl	string¦null	false	none	base URL for MDSS, if not provided will use Request.Host

FileFilterSortParameters

```
{
  "expand": [
    "string"
  ],
  "startDate": "2019-08-24T14:15:22Z",
  "endDate": "2019-08-24T14:15:22Z",
  "search": "string",
  "scanType": [
    0
  ],
  "storageId": [
    "string"
  ],
  "scanId": [
    "string"
  ],
  "scanWorkflowSnapshotId": [
    "string"
  ],
  "processingState": [
    0
  ],
  "result": [
    0
  ],
  "scanAllResultI": [
    0
  ],
  "scanResultICount": [
    0
  ],
  "sandboxVerdict": [
    0
  ],
  "vulnerabilityCount": [
    0
  ],
  "hasVulnerabilities": true,
  "dlpDetection": true,
  "hasBlockedFileVersions": true,
  "remediations": [
    0
  ],
  "skippedScan": true,
  "sortBy": [
    0
  ],
  "sortOrder": [
    0
  ]
}
```

Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	ExpandableParameters	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» startDate	string(date-time)	true	none	filter files by scan date
» endDate	string(date-time)	true	none	filter files by scan date
» search	string¦null	false	none	text filter
» scanType	[ScanType]¦null	false	none	scan type such as (on-demand, scheduled, real time)
» storageId	[string]¦null	false	none	filter based on a list of possible storage id
» scanId	[string]¦null	false	none	filter based on a list of possible scan id
» scanWorkflowSnapshotId	[string]¦null	false	none	filter based on a list of possible scan workflow snapshot id
» processingState	[ProcessingState]¦null	false	none	[- 0: InProgress - 1: Failed - 2: Canceled - 3: Available - 4: FailedRemediation]
» result	[ResultI]¦null	false	none	filter by scan result (0 = Clean, 1 = Blocked, 2 = Processing)
» scanAllResultI	[ScanInstanceResultI]¦null	false	none	filter by MD Core scan result (0 = NoThreatDetected, 1 = Infected, 2 = Suspicious, etc.)
» scanResultICount	[integer]¦null	false	none	the number of engine results that

				are not “No threat detected”
» sandboxVerdict	[SandboxVerdict]¦null	false	none	filter by Sandbox verdict [0 = NoThreat, 1 = Malicious, 2 = Suspicious]
» vulnerabilityCount	[integer]¦null	false	none	the number of vulnerabilities detected
» hasVulnerabilities	boolean¦null	false	none	filter by presence of vulnerabilities
» dlpDetection	boolean¦null	false	none	DLP detection
» hasBlockedFileVersions	boolean¦null	false	none	filter by presence of blocked file versions
» remediations	[ObjectActionType]¦null	false	none	filter by remediation performed on the file
» skippedScan	boolean¦null	false	none	filter by whether the scan was skipped
» sortBy	[FileSortOption]¦null	false	none	[- 0: DiscoveryStarted - 1: ScanId - 2: ProcessingState - 3: Result - 4: ScanAllResultI - 5: ScanResultICount - 6: VulnerabilityCount - 7: SandboxVerdict - 8: SkippedScan]
» sortOrder	[SortingOrder2]¦null	false	none	[- 0: Ascending - 1: Descending]

ScanType

```
0
```

- 0: Instant
- 1: Scheduled
- 2: RealTime

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: Instant - 1: Scheduled - 2: RealTime

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2

ProcessingState

```
0
```

- 0: InProgress
- 1: Failed
- 2: Canceled
- 3: Available
- 4: FailedRemediation

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: InProgress - 1: Failed - 2: Canceled - 3: Available - 4: FailedRemediation

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2
anonymous	3
anonymous	4

ResultI

```
0
```

- 0: Allowed
- 1: Blocked
- 2: Processing

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: Allowed - 1: Blocked - 2: Processing

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2

ScanInstanceResultI

```
0
```

- 0: NoThreatDetected
- 1: Infected
- 2: Suspicious
- 3: Failed
- 7: Allowlisted
- 8: Blocklisted
- 9: ExceededArchiveDepth
- 10: NotScanned
- 12: EncryptedArchive
- 13: ExceededArchiveSize
- 14: ExceededArchiveFileNumber
- 15: PasswordProtectedDocument
- 16: ExceededArchiveTimeout
- 17: Mismatch
- 18: PotentiallyVulnerableFile
- 19: Cancelled
- 20: SensitiveDataFound
- 21: YaraRuleMatched
- 22: PotentiallyUnwanted
- 23: UnsupportedFileType
- 24: ExtractionFailed
- 25: ScanFailed
- 26: SuspiciousVerdictbySandbox
- 27: LikelyMaliciousVerdictbySandbox
- 28: MaliciousVerdictbySandbox
- 29: BlockedVerdictbySandbox
- 30: BlockedVerdictbyDeepCdr
- 31: GlobalTimeoutExceeded
- 32: VulnerableVerdictbySbom
- 33: NonVulnerableVerdictbySbom
- 34: BlockedVerdictbySbom
- 36: BlockedbyPostAction
- 38: KnownBad
- 39: KnownGood

- 40: Unknown
- 41: AllowedVerdictbyCoo
- 42: BlockedVerdictbyCoo
- 43: UnknownVerdictbyCoo
- 255: InProgress
- 1014: SkipProcessingFastSymlink
- 9999: NullResult

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: NoThreatDetected - 1: Infected - 2: Suspicious - 3: Failed - 7: Allowlisted - 8: Blocklisted - 9: ExceededArchiveDepth - 10: NotScanned - 12: EncryptedArchive - 13: ExceededArchiveSize - 14: ExceededArchiveFileNumber - 15: PasswordProtectedDocument - 16: ExceededArchiveTimeout - 17: Mismatch - 18: PotentiallyVulnerableFile - 19: Cancelled - 20: SensitiveDataFound - 21: YaraRuleMatched - 22: PotentiallyUnwanted - 23: UnsupportedFileType - 24: ExtractionFailed - 25: ScanFailed - 26: SuspiciousVerdictbySandbox - 27: LikelyMaliciousVerdictbySandbox - 28: MaliciousVerdictbySandbox - 29: BlockedVerdictbySandbox - 30: BlockedVerdictbyDeepCdr - 31: GlobalTimeoutExceeded - 32: VulnerableVerdictbySbom - 33: NonVulnerableVerdictbySbom - 34: BlockedVerdictbySbom - 36: BlockedbyPostAction - 38: KnownBad - 39: KnownGood - 40: Unknown - 41: AllowedVerdictbyCoo - 42: BlockedVerdictbyCoo - 43: UnknownVerdictbyCoo - 255: InProgress - 1014: SkipProcessingFastSymlink - 9999: NullResult

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2
anonymous	3
anonymous	7
anonymous	8
anonymous	9
anonymous	10
anonymous	12
anonymous	13
anonymous	14
anonymous	15
anonymous	16
anonymous	17
anonymous	18
anonymous	19
anonymous	20
anonymous	21
anonymous	22
anonymous	23
anonymous	24
anonymous	25
anonymous	26
anonymous	27
anonymous	28
anonymous	29
anonymous	30

anonymous	31
anonymous	32
anonymous	33
anonymous	34
anonymous	36
anonymous	38
anonymous	39
anonymous	40
anonymous	41
anonymous	42
anonymous	43
anonymous	255
anonymous	1014
anonymous	9999

SandboxVerdict

```
0
```

- 0: NOTHREAT
- 1: MALICIOUS
- 2: LIKELYMALICIOUS
- 3: SUSPICIOUS
- 4: BENIGN
- 5: UNKNOWN
- 999: FAILED

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: NOTHREAT - 1: MALICIOUS - 2: LIKELYMALICIOUS - 3: SUSPICIOUS - 4: BENIGN - 5: UNKNOWN - 999: FAILED

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2
anonymous	3
anonymous	4
anonymous	5
anonymous	999

ObjectActionType

```
0
```

- 0: Tagging
- 5: AllowedMoved
- 6: BlockedMoved
- 7: BlockedDelete
- 8: AllowedSanitizedMoved
- 9: AllowedCopied
- 10: BlockedCopied
- 11: AllowedSanitizedCopied
- 12: AllowedSanitizedDeleted

- 13: AllowedDeleted
- 14: AllowedKept
- 15: BlockedKept
- 16: AllowedSanitizedKept
- 17: BlockedSanitizedCopied
- 18: BlockedSanitizedMoved
- 19: BlockedSanitizedDeleted
- 20: BlockedSanitizedKept
- 21: ScanFileVersions
- 22: DiscoveredMoved
- 23: DiscoveredCopied
- 24: DiscoveredKept
- 25: DiscoveredDelete
- 26: AllowedCdrUnsupportedKept
- 27: AllowedCdrUnsupportedMoved
- 28: AllowedCdrUnsupportedCopied
- 29: AllowedCdrUnsupportedDeleted
- 30: BlockedCdrUnsupportedKept
- 31: BlockedCdrUnsupportedMoved
- 32: BlockedCdrUnsupportedCopied
- 33: BlockedCdrUnsupportedDeleted
- 100: SoftDelete
- 101: PackageDelete
- 102: Copy

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: Tagging - 5: AllowedMoved - 6: BlockedMoved - 7: BlockedDelete - 8: AllowedSanitizedMoved - 9: AllowedCopied - 10: BlockedCopied - 11: AllowedSanitizedCopied - 12: AllowedSanitizedDeleted - 13: AllowedDeleted - 14: AllowedKept - 15: BlockedKept - 16: AllowedSanitizedKept - 17: BlockedSanitizedCopied - 18: BlockedSanitizedMoved - 19: BlockedSanitizedDeleted - 20: BlockedSanitizedKept - 21: ScanFileVersions - 22: DiscoveredMoved - 23: DiscoveredCopied - 24: DiscoveredKept - 25: DiscoveredDelete - 26: AllowedCdrUnsupportedKept - 27: AllowedCdrUnsupportedMoved - 28: AllowedCdrUnsupportedCopied - 29: AllowedCdrUnsupportedDeleted - 30: BlockedCdrUnsupportedKept - 31: BlockedCdrUnsupportedMoved - 32: BlockedCdrUnsupportedCopied - 33: BlockedCdrUnsupportedDeleted - 100: SoftDelete - 101: PackageDelete - 102: Copy

Enumerated Values

Property	Value
anonymous	0
anonymous	5
anonymous	6
anonymous	7
anonymous	8
anonymous	9
anonymous	10
anonymous	11
anonymous	12
anonymous	13
anonymous	14
anonymous	15
anonymous	16
anonymous	17
anonymous	18
anonymous	19
anonymous	20
anonymous	21
anonymous	22
anonymous	23
anonymous	24
anonymous	25
anonymous	26
anonymous	27
anonymous	28
anonymous	29
anonymous	30

anonymous	31
anonymous	32
anonymous	33
anonymous	100
anonymous	101
anonymous	102

FileSortOption

```
0
```

- 0: DiscoveryStarted
- 1: ScanId
- 2: ProcessingState
- 3: Result
- 4: ScanAllResultI
- 5: ScanResultICount
- 6: VulnerabilityCount
- 7: SandboxVerdict
- 8: SkippedScan

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: DiscoveryStarted - 1: ScanId - 2: ProcessingState - 3: Result - 4: ScanAllResultI - 5: ScanResultICount - 6: VulnerabilityCount - 7: SandboxVerdict - 8: SkippedScan

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2
anonymous	3
anonymous	4
anonymous	5
anonymous	6
anonymous	7
anonymous	8

SortingOrder2

```
0
```

- 0: Ascending
- 1: Descending

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: Ascending - 1: Descending

Enumerated Values

Property	Value
anonymous	0
anonymous	1

ExpandableParameters

```
{
  "expand": [
    "string"
  ]
}
```

Properties

Name	Type	Required	Restrictions	Description
expand	[string]¦null	false	none	Possible values for expand: workflow_snapshot

GetFileResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "id": "string",
  "scanId": "string",
  "name": "string",
  "path": "string",
  "hash": "string",
  "fileOwner": {
    "userId": "string",
    "fullName": "string",
    "userName": "string",
    "emailAddress": "string"
  },
  "size": 0,
  "storageType": {
    "name": "string",
    "categoryType": 0,
    "protocolType": 0,
    "vendorType": 0
  },
  "storageName": "string",
  "storageLocation": "string",
  "scanName": "string",
  "progress": {
    "upload": 0,
    "scan": 0,
    "archiveExtraction": 0
  },
  "scanResult": {
    "extractedFiles": {
      "dataId": "string",
      "scanResultI": 0,
      "detectedBy": 0,
      "filesExtractedCount": 0
    },
    "scanResults": {
      "scanDetails": [
        {
          "engineName": "string",
          "threatFound": "string",
          "scanResultI": 0,
          "defTime": "string",
          "scanTime": 0.1,
          "engId": "string",
          "waitTime": 0.1
        }
```

```
"dataId": "string",
      "scanAllResultI": 0,
      "scanAllResultA": "string",
      "startTime": "string",
      "totalTime": 0.1,
      "totalAvs": 0,
      "totalDetections": 0,
      "progressPercentage": 0
    },
    "fileInfo": {
      "fileSize": 0,
      "uploadTimestamp": "string",
      "md5": "string",
      "sha1": "string",
      "sha256": "string",
      "fileTypeCategory": "string",
      "fileTypeDescription": "string",
      "fileTypeExtension": "string",
      "displayName": "string",
      "fileTypeId": "string"
    },
    "fileScanInfo": {
      "finalVerdict": {
        "blocked": true,
        "verdict": "string",
        "confidence": 0.1,
        "threatLevel": 0.1
      },
      "overviewReport": {
        "analysisState": "string",
        "signalGroups": [
          {
            "description": "string",
            "verdict": "string",
            "signals": [
              {
                "originType": "string",
                "signalReadable": "string",
                "strength": 0.1
              }
            ],
            "mitreTechniques": [
              {
                "name": "string",
                "tacticName": "string"
              }
            ]
          }
        ],
        "iocs": [
          {
            "data": "string",
            "type": "string",
```

```
"verdict": "string"
          }
        ],
        "yaraMatches": [
          {
            "ruleName": "string",
            "ruleDescription": "string",
            "verdict": "string",
            "matchedStrings": [
              "string"
            ],
            "author": "string",
            "version": "string",
            "threatLevel": 0.1,
            "confidence": 0.1,
            "strength": 0.1
          }
        ],
        "tags": [
          {
            "name": "string",
            "verdict": "string"
          }
        ],
        "metaData": {
          "entropy": 0.1,
          "forensicAnalysisRecommended": true,
          "fuzzyFsioHash": "string"
        }
      },
      "errorCategory": "string",
      "errorCode": 0,
      "errorDetails": "string"
    },
    "processInfo": {
      "postProcessing": {
        "actionsRan": "string",
        "actionsFailed": "string",
        "convertedTo": "string",
        "copyMoveDestination": "string",
        "convertedDestination": "string",
        "sanitizationDetails": {
          "failureCategory": "string",
          "description": "string",
          "details": "string"
        }
      },
      "progressPercentage": 0,
      "userAgent": "string",
      "profile": "string",
      "result": "string",
      "blockedReason": "string",
      "fileTypeSkippedScan": true,
```

```
"queueTime": 0.1,
      "resultI": 0
    },
    "dataId": "string",
    "dlpInfo": {
      "hits": null,
      "verdict": 0
    },
    "sbomInfo": {
      "finalVerdict": {
        "blocked": true,
        "licensingPackageCounts": {
          "allowed": 0,
          "blocked": 0,
          "unknown": 0,
          "unsupported": 0
        },
        "severity": 0,
        "totalPackageCount": 0,
        "verdict": "string",
        "vulnerabilityCounts": {
          "critical": 0,
          "high": 0,
          "medium": 0,
          "low": 0,
          "unknown": 0
        }
      },
      "overviewReport": {
        "isPartialReport": true,
        "osInfo": {
          "osName": "string",
          "osVersion": "string"
        },
        "scanMode": "string",
        "steps": [
          {
            "command": "string",
            "packages": [
              {
                "authors": "string",
                "releaseDate": "2019-08-24T14:15:22Z",
                "ecosystem": "string",
                "group": "string",
                "archive": true,
                "executable": true,
                "uid": "string",
                "licenses": {
                  "allowed": [
                    {
                      "id": "string",
                      "url": "string",
                      "category": "string",
```

```
"permissions": [
                        "string"
                      ],
                      "conditions": [
                        "string"
                      ],
                      "limitations": [
                        "string"
                      ]
                    }
                  }
                ],
                "blocked": [
                  {
                    "id": "string",
                    "url": "string",
                    "category": "string",
                    "usageRestriction": {
                      "permissions": [
                        "string"
                      ],
                      "conditions": [
                        "string"
                      ],
                      "limitations": [
                        "string"
                      ]
                    }
                  }
                ]
              },
              "packageName": "string",
              "packageVersion": "string",
              "hashes": [
                {
                  "sha256": "string",
                  "fileName": "string"
                }
              ],
              "vulnerabilityCounts": {
                "critical": 0,
                "high": 0,
                "medium": 0,
                "low": 0,
                "unknown": 0
              },
              "vulnerabilities": [
                {
                  "id": "string",
                  "severity": 0,
                  "source": "string",
                  "fixedVersions": "string",
                  "cwes": [
```

```
]
                  }
                ],
                "arch": "string",
                "osName": "string",
                "osVersion": "string",
                "dependencies": [
                  {
                    "ecosystem": "string",
                    "group": "string",
                    "packageName": "string",
                    "packageVersion": "string",
                    "vulnerabilities": [
                      {
                        "id": "string",
                        "severity": 0,
                        "source": "string",
                        "fixedVersions": "string",
                        "cwes": [
                          "string"
                        ]
                      }
                    ],
                    "vulnerabilityCounts": {
                      "critical": 0,
                      "high": 0,
                      "medium": 0,
                      "low": 0,
                      "unknown": 0
                    }
                  }
                ]
              }
            ],
            "licenseStatus": "string",
            "licensingPackageCounts": {
              "allowed": 0,
              "blocked": 0,
              "unknown": 0,
              "unsupported": 0
            },
            "step": 0,
            "vulnerabilityCount": 0,
            "sha256": "string",
            "severity": 0,
            "vulnerabilityCounts": {
              "critical": 0,
              "high": 0,
              "medium": 0,
              "low": 0,
              "unknown": 0
            }
          }
```

```
"packages": [
          {
            "authors": "string",
            "releaseDate": "2019-08-24T14:15:22Z",
            "ecosystem": "string",
            "group": "string",
            "archive": true,
            "executable": true,
            "uid": "string",
            "licenses": {
              "allowed": [
                {
                  "id": "string",
                  "url": "string",
                  "category": "string",
                  "usageRestriction": {
                    "permissions": [
                      "string"
                    ],
                    "conditions": [
                      "string"
                    ],
                    "limitations": [
                      "string"
                    ]
                  }
                }
              ],
              "blocked": [
                {
                  "id": "string",
                  "url": "string",
                  "category": "string",
                  "usageRestriction": {
                    "permissions": [
                      "string"
                    ],
                    "conditions": [
                      "string"
                    ],
                    "limitations": [
                      "string"
                    ]
                  }
                }
              ]
            },
            "packageName": "string",
            "packageVersion": "string",
            "target": "string",
            "hashes": [
              {
                "sha256": "string",
```

```
}
            ],
            "vulnerabilities": [
              {
                "id": "string",
                "severity": 0,
                "source": "string",
                "fixedVersions": "string",
                "cwes": [
                  "string"
                ]
              }
            ],
            "vulnerabilityCounts": {
              "critical": 0,
              "high": 0,
              "medium": 0,
              "low": 0,
              "unknown": 0
            },
            "dependencies": [
              {
                "ecosystem": "string",
                "group": "string",
                "packageName": "string",
                "packageVersion": "string",
                "vulnerabilities": [
                  {
                    "id": "string",
                    "severity": 0,
                    "source": "string",
                    "fixedVersions": "string",
                    "cwes": [
                      "string"
                    ]
                  }
                ],
                "vulnerabilityCounts": {
                  "critical": 0,
                  "high": 0,
                  "medium": 0,
                  "low": 0,
                  "unknown": 0
                }
              }
            ]
          }
        ],
        "dependenciesPackageCount": 0,
        "dependenciesVulnerabilityTotal": 0,
        "dependenciesVulnerabilityCounts": {
          "critical": 0,
          "high": 0,
```

```
"low": 0,
          "unknown": 0
        }
      },
      "resultTemplateHash": "string"
    },
    "vulnerabilityInfo": {
      "vulnerabilityInfoResult": {
        "code": 0,
        "hash": "string",
        "method": 0,
        "timeStamp": "string",
        "timing": 0,
        "detectedProduct": {
          "hasVulnerability": true,
          "isCurrent": true,
          "product": {
            "id": 0,
            "name": "string"
          },
          "remediationLink": "string",
          "severity": "string",
          "sigName": "string",
          "signature": 0,
          "vendor": {
            "id": 0,
            "name": "string"
          },
          "version": "string",
          "versionData": {
            "countBehind": 0,
            "feedId": 0,
            "version": "string"
          },
          "vulnerabilities": [
            {
              "description": "string",
              "details": {
                "cpe": "string",
                "cve": "string",
                "cvss": {
                  "accessComplexity": "string",
                  "accessVector": "string",
                  "authentication": "string",
                  "availabilityImpact": "string",
                  "confidentialityImpact": "string",
                  "generatedOnEpoch": "string",
                  "integrityImpact": "string",
                  "score": "string",
                  "source": "string"
                },
                "cvss3": {
                  "attackComplexity": "string",
```

```
"availabilityImpact": "string",
                  "baseScore": "string",
                  "baseSeverity": "string",
                  "confidentialityImpact": "string",
                  "exploitabilityScore": "string",
                  "impactScore": "string",
                  "integrityImpact": "string",
                  "privilegesRequired": "string",
                  "scope": "string",
                  "userInteraction": "string",
                  "vectorString": "string"
                },
                "cwe": "string",
                "lastModifiedEpoch": "string",
                "publishedEpoch": "string",
                "references": [
                  "string"
                ]
              },
              "severity": "string",
              "severityIndex": 0,
              "staticId": 0
            }
          ]
        }
      }
    },
    "sessionCookie": "string",
    "fileTypeInfo": {
      "fileInfoExtended": {
        "extensions": "string",
        "groupId": "string",
        "typeId": "string"
      }
    },
    "scanInstanceUrl": "string",
    "scanWorkflowSnapshotId": "string",
    "coreEngines": [
      {
        "engineId": "string",
        "engineName": "string",
        "engineVersion": "string",
        "dbVersion": "string",
        "definitionTime": "string"
      }
    ]
  },
  "processingState": 0,
  "exception": {
    "exceptionDetails": "string",
    "exceptionMessage": "string"
  },
  "created": "2019-08-24T14:15:22Z",
```

```
"discoveryStarted": "2019-08-24T14:15:22Z",
  "fileProcessingDetails": {
    "streamingStartedTime": "2019-08-24T14:15:22Z",
    "streamingCompletedTime": "2019-08-24T14:15:22Z",
    "streamingTimeSpanMs": 0,
    "scanCompletedTime": "2019-08-24T14:15:22Z",
    "processingTimeSpanMs": 0
  },
  "coreEngines": [
    {
      "engineId": "string",
      "engineName": "string",
      "engineVersion": "string",
      "dbVersion": "string",
      "definitionTime": "string"
    }
  ],
  "remediation": {
    "deepCdr": {
      "sanitizationDetails": {
        "failureCategory": "string",
        "description": "string",
        "details": "string"
      },
      "cdrObjectState": 0,
      "fileWasReplaced": true
    },
    "postActionFailedInformation": [
      {
        "objectActionType": 0,
        "exception": {
          "exceptionDetails": "string",
          "exceptionMessage": "string"
        }
      }
    ],
    "objectRemediationActions": [
      {
        "objectActionType": 0,
        "objectActionState": 0,
        "cdrObjectState": 0,
        "exceptions": [
          "string"
        ],
        "id": "string",
        "fileId": "string",
        "fileScanCompletedTime": "2019-08-24T14:15:22Z",
        "remediationId": "string",
        "tenantId": "string",
        "lastUpdated": "2019-08-24T14:15:22Z"
      }
    ]
  },
```

```
"discoveryStartedDaySec": 0,
  "fileDto": {
    "result": 0,
    "responseKey": "string",
    "responseMessage": "string",
    "responseMessageParams": {
      "property1": "string",
      "property2": "string"
    },
    "id": "string",
    "scanId": "string",
    "name": "string",
    "path": "string",
    "hash": "string",
    "fileOwner": {
      "userId": "string",
      "fullName": "string",
      "userName": "string",
      "emailAddress": "string"
    },
    "size": 0,
    "fileTypeCategory": 0,
    "extension": "string",
    "storageType": {
      "name": "string",
      "categoryType": 0,
      "protocolType": 0,
      "vendorType": 0
    },
    "storageName": "string",
    "storageLocation": "string",
    "scanName": "string",
    "progress": {
      "upload": 0,
      "scan": 0,
      "archiveExtraction": 0
    },
    "scanResult": {
      "extractedFiles": {
        "dataId": "string",
        "scanResultI": 0,
        "detectedBy": 0,
        "filesExtractedCount": 0
      },
      "scanResults": {
        "scanDetails": [
          {
            "engineName": "string",
            "threatFound": "string",
            "scanResultI": 0,
            "defTime": "string",
            "scanTime": 0.1,
            "engId": "string",
```

```
}
        ],
        "dataId": "string",
        "scanAllResultI": 0,
        "scanAllResultA": "string",
        "startTime": "string",
        "totalTime": 0.1,
        "totalAvs": 0,
        "totalDetections": 0,
        "progressPercentage": 0
      },
      "fileInfo": {
        "fileSize": 0,
        "uploadTimestamp": "string",
        "md5": "string",
        "sha1": "string",
        "sha256": "string",
        "fileTypeCategory": "string",
        "fileTypeDescription": "string",
        "fileTypeExtension": "string",
        "displayName": "string",
        "fileTypeId": "string"
      },
      "fileScanInfo": {
        "finalVerdict": {
          "blocked": true,
          "verdict": "string",
          "confidence": 0.1,
          "threatLevel": 0.1
        },
        "overviewReport": {
          "analysisState": "string",
          "signalGroups": [
            {
              "description": "string",
              "verdict": "string",
              "signals": [
                {
                  "originType": "string",
                  "signalReadable": "string",
                  "strength": 0.1
                }
              ],
              "mitreTechniques": [
                {
                  "name": "string",
                  "tacticName": "string"
                }
              ]
            }
          ],
          "iocs": [
            {
```

```
"type": "string",
              "origin": "string",
              "verdict": "string"
            }
          ],
          "yaraMatches": [
            {
              "ruleName": "string",
              "ruleDescription": "string",
              "verdict": "string",
              "matchedStrings": [
                "string"
              ],
              "author": "string",
              "version": "string",
              "threatLevel": 0.1,
              "confidence": 0.1,
              "strength": 0.1
            }
          ],
          "tags": [
            {
              "name": "string",
              "verdict": "string"
            }
          ],
          "metaData": {
            "entropy": 0.1,
            "forensicAnalysisRecommended": true,
            "fuzzyFsioHash": "string"
          }
        },
        "errorCategory": "string",
        "errorCode": 0,
        "errorDetails": "string"
      },
      "processInfo": {
        "postProcessing": {
          "actionsRan": "string",
          "actionsFailed": "string",
          "convertedTo": "string",
          "copyMoveDestination": "string",
          "convertedDestination": "string",
          "sanitizationDetails": {
            "failureCategory": "string",
            "description": "string",
            "details": "string"
          }
        },
        "progressPercentage": 0,
        "userAgent": "string",
        "profile": "string",
        "result": "string",
```

```
"fileTypeSkippedScan": true,
        "processingTime": 0.1,
        "queueTime": 0.1,
        "resultI": 0
      },
      "dataId": "string",
      "dlpInfo": {
        "hits": null,
        "verdict": 0
      },
      "sbomInfo": {
        "finalVerdict": {
          "blocked": true,
          "licensingPackageCounts": {
            "allowed": 0,
            "blocked": 0,
            "unknown": 0,
            "unsupported": 0
          },
          "severity": 0,
          "totalPackageCount": 0,
          "verdict": "string",
          "vulnerabilityCounts": {
            "critical": 0,
            "high": 0,
            "medium": 0,
            "low": 0,
            "unknown": 0
          }
        },
        "overviewReport": {
          "isPartialReport": true,
          "osInfo": {
            "osName": "string",
            "osVersion": "string"
          },
          "scanMode": "string",
          "steps": [
            {
              "command": "string",
              "packages": [
                {
                  "authors": "string",
                  "releaseDate": "2019-08-24T14:15:22Z",
                  "ecosystem": "string",
                  "group": "string",
                  "archive": true,
                  "executable": true,
                  "uid": "string",
                  "licenses": {
                    "allowed": [
                      {
                        "id": "string",
```

```
"category": "string",
                        "usageRestriction": {
                          "permissions": [
                            "string"
                          ],
                          "conditions": [
                            "string"
                          ],
                          "limitations": [
                            "string"
                          ]
                        }
                      }
                    ],
                    "blocked": [
                      {
                        "id": "string",
                        "url": "string",
                        "category": "string",
                        "usageRestriction": {
                          "permissions": [
                            "string"
                          ],
                          "conditions": [
                            "string"
                          ],
                          "limitations": [
                            "string"
                          ]
                        }
                      }
                    ]
                  },
                  "packageName": "string",
                  "packageVersion": "string",
                  "hashes": [
                    {
                      "sha256": "string",
                      "fileName": "string"
                    }
                  ],
                  "vulnerabilityCounts": {
                    "critical": 0,
                    "high": 0,
                    "medium": 0,
                    "low": 0,
                    "unknown": 0
                  },
                  "vulnerabilities": [
                    {
                      "id": "string",
                      "severity": 0,
                      "source": "string",
```

```
"cwes": [
                        "string"
                      ]
                    }
                  ],
                  "arch": "string",
                  "osName": "string",
                  "osVersion": "string",
                  "dependencies": [
                    {
                      "ecosystem": "string",
                      "group": "string",
                      "packageName": "string",
                      "packageVersion": "string",
                      "vulnerabilities": [
                        {
                          "id": "string",
                          "severity": 0,
                          "source": "string",
                          "fixedVersions": "string",
                          "cwes": [
                            "string"
                          ]
                        }
                      ],
                      "vulnerabilityCounts": {
                        "critical": 0,
                        "high": 0,
                        "medium": 0,
                        "low": 0,
                        "unknown": 0
                      }
                    }
                  ]
                }
              ],
              "licenseStatus": "string",
              "licensingPackageCounts": {
                "allowed": 0,
                "blocked": 0,
                "unknown": 0,
                "unsupported": 0
              },
              "step": 0,
              "vulnerabilityCount": 0,
              "sha256": "string",
              "severity": 0,
              "vulnerabilityCounts": {
                "critical": 0,
                "high": 0,
                "medium": 0,
                "low": 0,
                "unknown": 0
```

```
}
          ],
          "packages": [
            {
              "authors": "string",
              "releaseDate": "2019-08-24T14:15:22Z",
              "ecosystem": "string",
              "group": "string",
              "archive": true,
              "executable": true,
              "uid": "string",
              "licenses": {
                "allowed": [
                  {
                    "id": "string",
                    "url": "string",
                    "category": "string",
                    "usageRestriction": {
                      "permissions": [
                        "string"
                      ],
                      "conditions": [
                        "string"
                      ],
                      "limitations": [
                        "string"
                      ]
                    }
                  }
                ],
                "blocked": [
                  {
                    "id": "string",
                    "url": "string",
                    "category": "string",
                    "usageRestriction": {
                      "permissions": [
                        "string"
                      ],
                      "conditions": [
                        "string"
                      ],
                      "limitations": [
                        "string"
                      ]
                    }
                  }
                ]
              },
              "packageName": "string",
              "packageVersion": "string",
              "target": "string",
              "hashes": [
```

```
"sha256": "string",
                  "fileName": "string"
                }
              ],
              "vulnerabilities": [
                {
                  "id": "string",
                  "severity": 0,
                  "source": "string",
                  "fixedVersions": "string",
                  "cwes": [
                    "string"
                  ]
                }
              ],
              "vulnerabilityCounts": {
                "critical": 0,
                "high": 0,
                "medium": 0,
                "low": 0,
                "unknown": 0
              },
              "dependencies": [
                {
                  "ecosystem": "string",
                  "group": "string",
                  "packageName": "string",
                  "packageVersion": "string",
                  "vulnerabilities": [
                    {
                      "id": "string",
                      "severity": 0,
                      "source": "string",
                      "fixedVersions": "string",
                      "cwes": [
                        "string"
                      ]
                    }
                  ],
                  "vulnerabilityCounts": {
                    "critical": 0,
                    "high": 0,
                    "medium": 0,
                    "low": 0,
                    "unknown": 0
                  }
                }
              ]
            }
          ],
          "dependenciesPackageCount": 0,
          "dependenciesVulnerabilityTotal": 0,
          "dependenciesVulnerabilityCounts": {
```

```
"high": 0,
            "medium": 0,
            "low": 0,
            "unknown": 0
          }
        },
        "resultTemplateHash": "string"
      },
      "vulnerabilityInfo": {
        "vulnerabilityInfoResult": {
          "code": 0,
          "hash": "string",
          "method": 0,
          "timeStamp": "string",
          "timing": 0,
          "detectedProduct": {
            "hasVulnerability": true,
            "isCurrent": true,
            "product": {
              "id": 0,
              "name": "string"
            },
            "remediationLink": "string",
            "severity": "string",
            "sigName": "string",
            "signature": 0,
            "vendor": {
              "id": 0,
              "name": "string"
            },
            "version": "string",
            "versionData": {
              "countBehind": 0,
              "feedId": 0,
              "version": "string"
            },
            "vulnerabilities": [
              {
                "description": "string",
                "details": {
                  "cpe": "string",
                  "cve": "string",
                  "cvss": {
                    "accessComplexity": "string",
                    "accessVector": "string",
                    "authentication": "string",
                    "availabilityImpact": "string",
                    "confidentialityImpact": "string",
                    "generatedOnEpoch": "string",
                    "integrityImpact": "string",
                    "score": "string",
                    "source": "string"
                  },
```

```
"attackComplexity": "string",
                    "attackVector": "string",
                    "availabilityImpact": "string",
                    "baseScore": "string",
                    "baseSeverity": "string",
                    "confidentialityImpact": "string",
                    "exploitabilityScore": "string",
                    "impactScore": "string",
                    "integrityImpact": "string",
                    "privilegesRequired": "string",
                    "scope": "string",
                    "userInteraction": "string",
                    "vectorString": "string"
                  },
                  "cwe": "string",
                  "lastModifiedEpoch": "string",
                  "publishedEpoch": "string",
                  "references": [
                    "string"
                  ]
                },
                "severity": "string",
                "severityIndex": 0,
                "staticId": 0
              }
            ]
          }
        }
      },
      "sessionCookie": "string",
      "fileTypeInfo": {
        "fileInfoExtended": {
          "extensions": "string",
          "groupId": "string",
          "typeId": "string"
        }
      },
      "scanInstanceUrl": "string",
      "scanWorkflowSnapshotId": "string",
      "coreEngines": [
        {
          "engineId": "string",
          "engineName": "string",
          "engineVersion": "string",
          "dbVersion": "string",
          "definitionTime": "string"
        }
      ]
    },
    "processingState": 0,
    "exception": {
      "exceptionDetails": "string",
      "exceptionMessage": "string"
```

```
"created": "2019-08-24T14:15:22Z",
    "lastModified": "2019-08-24T14:15:22Z",
    "discoveryStarted": "2019-08-24T14:15:22Z",
    "fileProcessingDetails": {
      "streamingStartedTime": "2019-08-24T14:15:22Z",
      "streamingCompletedTime": "2019-08-24T14:15:22Z",
      "streamingTimeSpanMs": 0,
      "scanCompletedTime": "2019-08-24T14:15:22Z",
      "processingTimeSpanMs": 0
    },
    "coreEngines": [
      {
        "engineId": "string",
        "engineName": "string",
        "engineVersion": "string",
        "dbVersion": "string",
        "definitionTime": "string"
      }
    ],
    "remediation": {
      "deepCdr": {
        "sanitizationDetails": {
          "failureCategory": "string",
          "description": "string",
          "details": "string"
        },
        "cdrObjectState": 0,
        "fileWasReplaced": true
      },
      "postActionFailedInformation": [
        {
          "objectActionType": 0,
          "exception": {
            "exceptionDetails": "string",
            "exceptionMessage": "string"
          }
        }
      ],
      "objectRemediationActions": [
        {
          "objectActionType": 0,
          "objectActionState": 0,
          "cdrObjectState": 0,
          "exceptions": [
            "string"
          ],
          "id": "string",
          "fileId": "string",
          "fileScanCompletedTime": "2019-08-24T14:15:22Z",
          "remediationId": "string",
          "tenantId": "string",
          "lastUpdated": "2019-08-24T14:15:22Z"
        }
```

```
},
    "metaDefenderCoreUrl": "string",
    "discoveryStartedDaySec": 0,
    "objectStorageMetadata": "string",
    "scanWorkflowSnapshotId": "string",
    "scanWorkflowSnapshot": {
      "id": "string",
      "scanId": "string",
      "workflow": {
        "id": "string",
        "scanPoolId": "string",
        "scanProcessFlow": 0,
        "isIdentityScanningEnabled": true,
        "scanIntervalDays": 0,
        "rules": [
          "string"
        ],
        "type": 0,
        "workflowSupportedTechnologies": {
          "dlp": {
            "status": 0
          },
          "deepCdr": {
            "status": 0
          },
          "sandBox": {
            "status": 0
          },
          "metascan": {
            "status": 0
          }
        },
        "name": "string",
        "userAgent": "string",
        "scanPool": {
          "id": "string",
          "name": "string",
          "scanPoolType": 0,
          "isDefault": true,
          "scanInstances": [
            {
              "id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ]
        },
        "failOverScanPoolId": "string",
        "failOverScanPool": {
          "id": "string",
```

```
"scanPoolType": 0,
          "isDefault": true,
          "scanInstances": [
            {
              "id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ]
        },
        "filters": {
          "id": "string",
          "minimumSize": 0,
          "maximumSize": 0,
          "minimumDateTime": "2019-08-24T14:15:22Z",
          "maximumDateTime": "2019-08-24T14:15:22Z"
        },
        "fileDefinition": {
          "blockingStrategy": 0,
          "configurableBlockingStrategy": {
            "shouldTreatFilesWithSensitiveDataAsBlocked": true,
            "shouldTreatFilesWithVulnerabilitiesAsBlocked": true
          }
        },
        "remediations": [
          {
            "id": "string",
            "workflowId": "string",
            "isEnabled": true,
            "configuration": "string",
            "type": 0,
            "handlingType": 0
          }
        ],
        "tenantId": "string"
      },
      "startTimestamp": 0,
      "stopTimestamp": 0,
      "scanPool": {
        "id": "string",
        "name": "string",
        "scanPoolType": 0,
        "isDefault": true,
        "scanInstances": [
          {
            "id": "string",
            "scanPoolId": "string",
            "url": "string",
            "apiKey": "string",
            "timeout": "string",
```

```
}
        ]
      },
      "scanInstances": [
        {
          "id": "string",
          "scanPoolId": "string",
          "url": "string",
          "apiKey": "string",
          "timeout": "string",
          "scanInstanceType": 0
        }
      ],
      "failOverScanPool": {
        "id": "string",
        "name": "string",
        "scanPoolType": 0,
        "isDefault": true,
        "scanInstances": [
          {
            "id": "string",
            "scanPoolId": "string",
            "url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ]
      },
      "failOverScanInstances": [
        {
          "id": "string",
          "scanPoolId": "string",
          "url": "string",
          "apiKey": "string",
          "timeout": "string",
          "scanInstanceType": 0
        }
      ],
      "storage": {
        "id": "string",
        "name": "string",
        "groupId": "string",
        "clientId": "string",
        "accountId": "string",
        "source": "string",
        "storageFunctionality": "string",
        "storageType": {
          "name": "string",
          "categoryType": 0,
          "protocolType": 0,
          "vendorType": 0
        },
```

```
"message": "string",
          "statusType": 0
        },
        "workflowId": "string",
        "lastUpdated": "2019-08-24T14:15:22Z",
        "tenantId": "string",
        "groupRef": {
          "id": "string",
          "name": "string"
        },
        "isAutodiscovered": true
      },
      "workflowStatistics": {
        "taggingStatistics": {
          "total": 0
        },
        "keepAllowedStatistics": {
          "total": 0
        },
        "keepBlockedStatistics": {
          "total": 0
        },
        "keepSanitizedStatistics": {
          "total": 0
        },
        "movedAllowedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
```

```
},
        "movedSanitizedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "movedBlockedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
```

```
"groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "copyAllowedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "copyBlockedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
```

```
"message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "deleteAllowedStatistics": {
          "total": 0
        },
        "deleteBlockedStatistics": {
          "total": 0
        },
        "lastCalculatedStatisticsTime": "2019-08-24T14:15:22Z"
      },
      "account": {
        "id": "string",
        "name": "string",
        "description": "string",
        "credentials": "string",
        "protocolType": 0,
        "vendorType": 0,
        "autoDiscovery": true,
        "autodiscoveryDestinationGroupId": "string",
        "destinationGroup": {
          "id": "string",
          "name": "string"
        }
      },
      "realTimeStartDate": "2019-08-24T14:15:22Z"
    },
    "versions": [
      {
        "result": 0,
        "responseKey": "string",
        "responseMessage": "string",
        "responseMessageParams": {
          "property1": "string",
          "property2": "string"
        },
        "id": "string",
        "scanId": "string",
        "name": "string",
        "path": "string",
        "hash": "string",
        "fileOwner": {
          "userId": "string",
```

```
"userName": "string",
          "emailAddress": "string"
        },
        "size": 0,
        "fileTypeCategory": 0,
        "extension": "string",
        "storageType": {
          "name": "string",
          "categoryType": 0,
          "protocolType": 0,
          "vendorType": 0
        },
        "storageName": "string",
        "storageLocation": "string",
        "scanName": "string",
        "progress": {
          "upload": 0,
          "scan": 0,
          "archiveExtraction": 0
        },
        "scanResult": {
          "extractedFiles": {
            "dataId": "string",
            "scanResultI": 0,
            "detectedBy": 0,
            "filesExtractedCount": 0
          },
          "scanResults": {
            "scanDetails": [
              {
                "engineName": "string",
                "threatFound": "string",
                "scanResultI": 0,
                "defTime": "string",
                "scanTime": 0.1,
                "engId": "string",
                "waitTime": 0.1
              }
            ],
            "dataId": "string",
            "scanAllResultI": 0,
            "scanAllResultA": "string",
            "startTime": "string",
            "totalTime": 0.1,
            "totalAvs": 0,
            "totalDetections": 0,
            "progressPercentage": 0
          },
          "fileInfo": {
            "fileSize": 0,
            "uploadTimestamp": "string",
            "md5": "string",
            "sha1": "string",
```

```
"fileTypeCategory": "string",
            "fileTypeDescription": "string",
            "fileTypeExtension": "string",
            "displayName": "string",
            "fileTypeId": "string"
          },
          "fileScanInfo": {
            "finalVerdict": {
              "blocked": true,
              "verdict": "string",
              "confidence": 0.1,
              "threatLevel": 0.1
            },
            "overviewReport": {
              "analysisState": "string",
              "signalGroups": [
                {
                  "description": "string",
                  "verdict": "string",
                  "signals": [
                    {
                      "originType": "string",
                      "signalReadable": "string",
                      "strength": 0.1
                    }
                  ],
                  "mitreTechniques": [
                    {
                      "name": "string",
                      "tacticName": "string"
                    }
                  ]
                }
              ],
              "iocs": [
                {
                  "data": "string",
                  "type": "string",
                  "origin": "string",
                  "verdict": "string"
                }
              ],
              "yaraMatches": [
                {
                  "ruleName": "string",
                  "ruleDescription": "string",
                  "verdict": "string",
                  "matchedStrings": [
                    "string"
                  ],
                  "author": "string",
                  "version": "string",
                  "threatLevel": 0.1,
```

```
"strength": 0.1
                }
              ],
              "tags": [
                {
                  "name": "string",
                  "verdict": "string"
                }
              ],
              "metaData": {
                "entropy": 0.1,
                "forensicAnalysisRecommended": true,
                "fuzzyFsioHash": "string"
              }
            },
            "errorCategory": "string",
            "errorCode": 0,
            "errorDetails": "string"
          },
          "processInfo": {
            "postProcessing": {
              "actionsRan": "string",
              "actionsFailed": "string",
              "convertedTo": "string",
              "copyMoveDestination": "string",
              "convertedDestination": "string",
              "sanitizationDetails": {
                "failureCategory": "string",
                "description": "string",
                "details": "string"
              }
            },
            "progressPercentage": 0,
            "userAgent": "string",
            "profile": "string",
            "result": "string",
            "blockedReason": "string",
            "fileTypeSkippedScan": true,
            "processingTime": 0.1,
            "queueTime": 0.1,
            "resultI": 0
          },
          "dataId": "string",
          "dlpInfo": {
            "hits": null,
            "verdict": 0
          },
          "sbomInfo": {
            "finalVerdict": {
              "blocked": true,
              "licensingPackageCounts": {
                "allowed": 0,
                "blocked": 0,
```

```
"unsupported": 0
              },
              "severity": 0,
              "totalPackageCount": 0,
              "verdict": "string",
              "vulnerabilityCounts": {
                "critical": 0,
                "high": 0,
                "medium": 0,
                "low": 0,
                "unknown": 0
              }
            },
            "overviewReport": {
              "isPartialReport": true,
              "osInfo": {
                "osName": "string",
                "osVersion": "string"
              },
              "scanMode": "string",
              "steps": [
                {
                  "command": "string",
                  "packages": [
                    {
                      "authors": "string",
                      "releaseDate": "2019-08-24T14:15:22Z",
                      "ecosystem": "string",
                      "group": "string",
                      "archive": true,
                      "executable": true,
                      "uid": "string",
                      "licenses": {
                        "allowed": [
                          {
                            "id": "string",
                            "url": "string",
                            "category": "string",
                            "usageRestriction": {
                              "permissions": [],
                              "conditions": [],
                              "limitations": []
                            }
                          }
                        ],
                        "blocked": [
                          {
                            "id": "string",
                            "url": "string",
                            "category": "string",
                            "usageRestriction": {
                              "permissions": [],
                              "conditions": [],
```

```
}
                        }
                    ]
                },
                "packageName": "string",
                "packageVersion": "string",
                "hashes": [
                    {
                        "sha256": "string",
                        "fileName": "string"
                    }
                ],
                "vulnerabilityCounts": {
                    "critical": 0,
                    "high": 0,
                    "medium": 0,
                    "low": 0,
                    "unknown": 0
                },
                "vulnerabilities": [
                    {
                        "id": "string",
                        "severity": 0,
                        "source": "string",
                        "fixedVersions": "string",
                        "cwes": [
                            "string"
                        ]
                    }
                ],
                "arch": "string",
                "osName": "string",
                "osVersion": "string",
                "dependencies": [
                    {
                        "ecosystem": "string",
                        "group": "string",
                        "packageName": "string",
                        "packageVersion": "string",
                        "vulnerabilities": [
                            {
                                "cwes": []
                            }
                        ],
                        "vulnerabilityCounts": {
                            "critical": 0,
                            "high": 0,
                            "medium": 0,
                            "low": 0,
                            "unknown": 0
                        }
                    }
                ]
```

```
],
                    "licenseStatus": "string",
                    "licensingPackageCounts": {
                      "allowed": 0,
                      "blocked": 0,
                      "unknown": 0,
                      "unsupported": 0
                    },
                    "step": 0,
                    "vulnerabilityCount": 0,
                    "sha256": "string",
                    "severity": 0,
                    "vulnerabilityCounts": {
                      "critical": 0,
                      "high": 0,
                      "medium": 0,
                      "low": 0,
                      "unknown": 0
                    }
                  }
                ],
                "packages": [
                  {
                    "authors": "string",
                    "releaseDate": "2019-08-24T14:15:22Z",
                    "ecosystem": "string",
                    "group": "string",
                    "archive": true,
                    "executable": true,
                    "uid": "string",
                    "licenses": {
                      "allowed": [
                        {
                          "id": "string",
                          "url": "string",
                          "category": "string",
                          "usageRestriction": {
                            "permissions": [
                              "string"
                            ],
                            "conditions": [
                              "string"
                            ],
                            "limitations": [
                              "string"
                            ]
                          }
                        }
                      ],
                      "blocked": [
                        {
                          "id": "string",
                          "url": "string",
```

```
"usageRestriction": {
                          "permissions": [
                            "string"
                          ],
                          "conditions": [
                            "string"
                          ],
                          "limitations": [
                            "string"
                          ]
                        }
                      }
                    ]
                  },
                  "packageName": "string",
                  "packageVersion": "string",
                  "target": "string",
                  "hashes": [
                    {
                      "sha256": "string",
                      "fileName": "string"
                    }
                  ],
                  "vulnerabilities": [
                    {
                      "id": "string",
                      "severity": 0,
                      "source": "string",
                      "fixedVersions": "string",
                      "cwes": [
                        "string"
                      ]
                    }
                  ],
                  "vulnerabilityCounts": {
                    "critical": 0,
                    "high": 0,
                    "medium": 0,
                    "low": 0,
                    "unknown": 0
                  },
                  "dependencies": [
                    {
                      "ecosystem": "string",
                      "group": "string",
                      "packageName": "string",
                      "packageVersion": "string",
                      "vulnerabilities": [
                        {
                          "id": "string",
                          "severity": 0,
                          "source": "string",
                          "fixedVersions": "string",
```

```
"string"
                          ]
                        }
                      ],
                      "vulnerabilityCounts": {
                        "critical": 0,
                        "high": 0,
                        "medium": 0,
                        "low": 0,
                        "unknown": 0
                      }
                    }
                  ]
                }
              ],
              "dependenciesPackageCount": 0,
              "dependenciesVulnerabilityTotal": 0,
              "dependenciesVulnerabilityCounts": {
                "critical": 0,
                "high": 0,
                "medium": 0,
                "low": 0,
                "unknown": 0
              }
            },
            "resultTemplateHash": "string"
          },
          "vulnerabilityInfo": {
            "vulnerabilityInfoResult": {
              "code": 0,
              "hash": "string",
              "method": 0,
              "timeStamp": "string",
              "timing": 0,
              "detectedProduct": {
                "hasVulnerability": true,
                "isCurrent": true,
                "product": {
                  "id": 0,
                  "name": "string"
                },
                "remediationLink": "string",
                "severity": "string",
                "sigName": "string",
                "signature": 0,
                "vendor": {
                  "id": 0,
                  "name": "string"
                },
                "version": "string",
                "versionData": {
                  "countBehind": 0,
                  "feedId": 0,
```

```
},
                "vulnerabilities": [
                  {
                    "description": "string",
                    "details": {
                      "cpe": "string",
                      "cve": "string",
                      "cvss": {
                        "accessComplexity": "string",
                        "accessVector": "string",
                        "authentication": "string",
                        "availabilityImpact": "string",
                        "confidentialityImpact": "string",
                        "generatedOnEpoch": "string",
                        "integrityImpact": "string",
                        "score": "string",
                        "source": "string"
                      },
                      "cvss3": {
                        "attackComplexity": "string",
                        "attackVector": "string",
                        "availabilityImpact": "string",
                        "baseScore": "string",
                        "baseSeverity": "string",
                        "confidentialityImpact": "string",
                        "exploitabilityScore": "string",
                        "impactScore": "string",
                        "integrityImpact": "string",
                        "privilegesRequired": "string",
                        "scope": "string",
                        "userInteraction": "string",
                        "vectorString": "string"
                      },
                      "cwe": "string",
                      "lastModifiedEpoch": "string",
                      "publishedEpoch": "string",
                      "references": [
                        "string"
                      ]
                    },
                    "severity": "string",
                    "severityIndex": 0,
                    "staticId": 0
                  }
                ]
              }
            }
          },
          "sessionCookie": "string",
          "fileTypeInfo": {
            "fileInfoExtended": {
              "extensions": "string",
              "groupId": "string",
```

```
}
          },
          "scanInstanceUrl": "string",
          "scanWorkflowSnapshotId": "string",
          "coreEngines": [
            {
              "engineId": "string",
              "engineName": "string",
              "engineVersion": "string",
              "dbVersion": "string",
              "definitionTime": "string"
            }
          ]
        },
        "processingState": 0,
        "exception": {
          "exceptionDetails": "string",
          "exceptionMessage": "string"
        },
        "created": "2019-08-24T14:15:22Z",
        "lastModified": "2019-08-24T14:15:22Z",
        "discoveryStarted": "2019-08-24T14:15:22Z",
        "fileProcessingDetails": {
          "streamingStartedTime": "2019-08-24T14:15:22Z",
          "streamingCompletedTime": "2019-08-24T14:15:22Z",
          "streamingTimeSpanMs": 0,
          "scanCompletedTime": "2019-08-24T14:15:22Z",
          "processingTimeSpanMs": 0
        },
        "coreEngines": [
          {
            "engineId": "string",
            "engineName": "string",
            "engineVersion": "string",
            "dbVersion": "string",
            "definitionTime": "string"
          }
        ],
        "remediation": {
          "deepCdr": {
            "sanitizationDetails": {
              "failureCategory": "string",
              "description": "string",
              "details": "string"
            },
            "cdrObjectState": 0,
            "fileWasReplaced": true
          },
          "postActionFailedInformation": [
            {
              "objectActionType": 0,
              "exception": {
                "exceptionDetails": "string",
```

```
}
            }
          ],
          "objectRemediationActions": [
            {
              "objectActionType": 0,
              "objectActionState": 0,
              "cdrObjectState": 0,
              "exceptions": [
                "string"
              ],
              "id": "string",
              "fileId": "string",
              "fileScanCompletedTime": "2019-08-24T14:15:22Z",
              "remediationId": "string",
              "tenantId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z"
            }
          ]
        },
        "metaDefenderCoreUrl": "string",
        "discoveryStartedDaySec": 0,
        "objectStorageMetadata": "string",
        "scanWorkflowSnapshotId": "string",
        "scanWorkflowSnapshot": {
          "id": "string",
          "scanId": "string",
          "workflow": {
            "id": "string",
            "scanPoolId": "string",
            "scanProcessFlow": 0,
            "isIdentityScanningEnabled": true,
            "scanIntervalDays": 0,
            "rules": [
              "string"
            ],
            "type": 0,
            "workflowSupportedTechnologies": {
              "dlp": {
                "status": 0
              },
              "deepCdr": {
                "status": 0
              },
              "sandBox": {
                "status": 0
              },
              "metascan": {
                "status": 0
              }
            },
            "name": "string",
            "userAgent": "string",
```

```
"id": "string",
              "name": "string",
              "scanPoolType": 0,
              "isDefault": true,
              "scanInstances": [
                {
                  "id": "string",
                  "scanPoolId": "string",
                  "url": "string",
                  "apiKey": "string",
                  "timeout": "string",
                  "scanInstanceType": 0
                }
              ]
            },
            "failOverScanPoolId": "string",
            "failOverScanPool": {
              "id": "string",
              "name": "string",
              "scanPoolType": 0,
              "isDefault": true,
              "scanInstances": [
                {
                  "id": "string",
                  "scanPoolId": "string",
                  "url": "string",
                  "apiKey": "string",
                  "timeout": "string",
                  "scanInstanceType": 0
                }
              ]
            },
            "filters": {
              "id": "string",
              "minimumSize": 0,
              "maximumSize": 0,
              "minimumDateTime": "2019-08-24T14:15:22Z",
              "maximumDateTime": "2019-08-24T14:15:22Z"
            },
            "fileDefinition": {
              "blockingStrategy": 0,
              "configurableBlockingStrategy": {
                "shouldTreatFilesWithSensitiveDataAsBlocked": true,
                "shouldTreatFilesWithVulnerabilitiesAsBlocked": true
              }
            },
            "remediations": [
              {
                "id": "string",
                "workflowId": "string",
                "isEnabled": true,
                "configuration": "string",
                "type": 0,
```

```
}
            ],
            "tenantId": "string"
          },
          "startTimestamp": 0,
          "stopTimestamp": 0,
          "scanPool": {
            "id": "string",
            "name": "string",
            "scanPoolType": 0,
            "isDefault": true,
            "scanInstances": [
              {
                "id": "string",
                "scanPoolId": "string",
                "url": "string",
                "apiKey": "string",
                "timeout": "string",
                "scanInstanceType": 0
              }
            ]
          },
          "scanInstances": [
            {
              "id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ],
          "failOverScanPool": {
            "id": "string",
            "name": "string",
            "scanPoolType": 0,
            "isDefault": true,
            "scanInstances": [
              {
                "id": "string",
                "scanPoolId": "string",
                "url": "string",
                "apiKey": "string",
                "timeout": "string",
                "scanInstanceType": 0
              }
            ]
          },
          "failOverScanInstances": [
            {
              "id": "string",
              "scanPoolId": "string",
              "url": "string",
```

```
"timeout": "string",
              "scanInstanceType": 0
            }
          ],
          "storage": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          },
          "workflowStatistics": {
            "taggingStatistics": {
              "total": 0
            },
            "keepAllowedStatistics": {
              "total": 0
            },
            "keepBlockedStatistics": {
              "total": 0
            },
            "keepSanitizedStatistics": {
              "total": 0
            },
            "movedAllowedStatistics": {
              "total": 0,
              "destinationStorageInformation": {
                "id": "string",
                "name": "string",
                "groupId": "string",
                "clientId": "string",
                "accountId": "string",
                "source": "string",
```

```
"storageType": {
                    "name": "string",
                    "categoryType": 0,
                    "protocolType": 0,
                    "vendorType": 0
                  },
                  "storageStatus": {
                    "message": "string",
                    "statusType": 0
                  },
                  "workflowId": "string",
                  "lastUpdated": "2019-08-24T14:15:22Z",
                  "tenantId": "string",
                  "groupRef": {
                    "id": "string",
                    "name": "string"
                  },
                  "isAutodiscovered": true
                }
              },
              "movedSanitizedStatistics": {
                "total": 0,
                "destinationStorageInformation": {
                  "id": "string",
                  "name": "string",
                  "groupId": "string",
                  "clientId": "string",
                  "accountId": "string",
                  "source": "string",
                  "storageFunctionality": "string",
                  "storageType": {
                    "name": "string",
                    "categoryType": 0,
                    "protocolType": 0,
                    "vendorType": 0
                  },
                  "storageStatus": {
                    "message": "string",
                    "statusType": 0
                  },
                  "workflowId": "string",
                  "lastUpdated": "2019-08-24T14:15:22Z",
                  "tenantId": "string",
                  "groupRef": {
                    "id": "string",
                    "name": "string"
                  },
                  "isAutodiscovered": true
                }
              },
              "movedBlockedStatistics": {
                "total": 0,
                "destinationStorageInformation": {
```

```
"name": "string",
                "groupId": "string",
                "clientId": "string",
                "accountId": "string",
                "source": "string",
                "storageFunctionality": "string",
                "storageType": {
                  "name": "string",
                  "categoryType": 0,
                  "protocolType": 0,
                  "vendorType": 0
                },
                "storageStatus": {
                  "message": "string",
                  "statusType": 0
                },
                "workflowId": "string",
                "lastUpdated": "2019-08-24T14:15:22Z",
                "tenantId": "string",
                "groupRef": {
                  "id": "string",
                  "name": "string"
                },
                "isAutodiscovered": true
              }
            },
            "copyAllowedStatistics": {
              "total": 0,
              "destinationStorageInformation": {
                "id": "string",
                "name": "string",
                "groupId": "string",
                "clientId": "string",
                "accountId": "string",
                "source": "string",
                "storageFunctionality": "string",
                "storageType": {
                  "name": "string",
                  "categoryType": 0,
                  "protocolType": 0,
                  "vendorType": 0
                },
                "storageStatus": {
                  "message": "string",
                  "statusType": 0
                },
                "workflowId": "string",
                "lastUpdated": "2019-08-24T14:15:22Z",
                "tenantId": "string",
                "groupRef": {
                  "id": "string",
                  "name": "string"
                },
```

```
}
            },
            "copyBlockedStatistics": {
              "total": 0,
              "destinationStorageInformation": {
                "id": "string",
                "name": "string",
                "groupId": "string",
                "clientId": "string",
                "accountId": "string",
                "source": "string",
                "storageFunctionality": "string",
                "storageType": {
                  "name": "string",
                  "categoryType": 0,
                  "protocolType": 0,
                  "vendorType": 0
                },
                "storageStatus": {
                  "message": "string",
                  "statusType": 0
                },
                "workflowId": "string",
                "lastUpdated": "2019-08-24T14:15:22Z",
                "tenantId": "string",
                "groupRef": {
                  "id": "string",
                  "name": "string"
                },
                "isAutodiscovered": true
              }
            },
            "deleteAllowedStatistics": {
              "total": 0
            },
            "deleteBlockedStatistics": {
              "total": 0
            },
            "lastCalculatedStatisticsTime": "2019-08-24T14:15:22Z"
          },
          "account": {
            "id": "string",
            "name": "string",
            "description": "string",
            "credentials": "string",
            "protocolType": 0,
            "vendorType": 0,
            "autoDiscovery": true,
            "autodiscoveryDestinationGroupId": "string",
            "destinationGroup": {
              "id": "string",
              "name": "string"
            }
```

```
"realTimeStartDate": "2019-08-24T14:15:22Z"
        },
        "versions": [],
        "hasBlockedVersions": true,
        "versionsCount": 0,
        "objectType": 0,
        "skippedScan": true,
        "$type": "string",
        "url": "string",
        "fileId": "string"
      }
    ],
    "hasBlockedVersions": true,
    "versionsCount": 0,
    "objectType": 0,
    "skippedScan": true,
    "$type": "string"
  }
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» id	string¦null	false	none	none
» scanId	string¦null	false	none	none
» name	string¦null	false	none	none
» path	string¦null	false	none	none
» hash	string¦null	false	none	none
» fileOwner	FileOwner¦null	false	none	none
» size	integer(int64)	false	none	none
» storageType	StorageType¦null	false	none	none
» storageName	string¦null	false	none	none
» storageLocation	string¦null	false	none	none
» scanName	string¦null	false	none	none
» progress	Progress¦null	false	none	none
» scanResult	CoreScanResult¦null	false	none	none
» processingState	ProcessingState2	false	none	- 0: InProgress - 1: Failed - 2: Canceled - 3: Available - 4: FailedRemediation
» exception	Exception¦null	false	none	none
» created	string(date-time)	false	none	none
» lastModified	string(date-time)	false	none	none
» discoveryStarted	string(date-time)	false	none	none
» fileProcessingDetails	FileProcessingDetails¦null	false	none	none
» coreEngines	[CoreEngine]¦null	false	none	none
» remediation	FileRemediation¦null	false	none	none
» metaDefenderCoreUrl	string¦null	false	none	none
» discoveryStartedDaySec	integer(int64)	false	none	none

» fileDto	File¦null	false	none	none

FileOwner

```
{
  "userId": "string",
  "fullName": "string",
  "userName": "string",
  "emailAddress": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
userId	string¦null	false	none	none
fullName	string¦null	false	none	none
userName	string¦null	false	none	none
emailAddress	string¦null	false	none	none

Progress

```
{
  "upload": 0,
  "scan": 0,
  "archiveExtraction": 0
}
```

Properties

Name	Type	Required	Restrictions	Description
upload	integer	false	none	none
scan	integer	false	none	none
archiveExtraction	integer	false	none	none

CoreScanResult

```
{
  "extractedFiles": {
    "dataId": "string",
    "scanResultI": 0,
    "detectedBy": 0,
    "filesExtractedCount": 0
  },
  "scanResults": {
    "scanDetails": [
      {
        "engineName": "string",
        "threatFound": "string",
        "scanResultI": 0,
        "defTime": "string",
        "scanTime": 0.1,
        "engId": "string",
        "waitTime": 0.1
      }
    ],
    "dataId": "string",
    "scanAllResultI": 0,
    "scanAllResultA": "string",
    "startTime": "string",
    "totalTime": 0.1,
    "totalAvs": 0,
    "totalDetections": 0,
    "progressPercentage": 0
  },
  "fileInfo": {
    "fileSize": 0,
    "uploadTimestamp": "string",
    "md5": "string",
    "sha1": "string",
    "sha256": "string",
    "fileTypeCategory": "string",
    "fileTypeDescription": "string",
    "fileTypeExtension": "string",
    "displayName": "string",
    "fileTypeId": "string"
  },
  "fileScanInfo": {
    "finalVerdict": {
      "blocked": true,
      "verdict": "string",
      "confidence": 0.1,
      "threatLevel": 0.1
    },
    "overviewReport": {
      "analysisState": "string",
      "signalGroups": [
        {
          "description": "string",
```

```
"signals": [
            {
              "originType": "string",
              "signalReadable": "string",
              "strength": 0.1
            }
          ],
          "mitreTechniques": [
            {
              "name": "string",
              "tacticName": "string"
            }
          ]
        }
      ],
      "iocs": [
        {
          "data": "string",
          "type": "string",
          "origin": "string",
          "verdict": "string"
        }
      ],
      "yaraMatches": [
        {
          "ruleName": "string",
          "ruleDescription": "string",
          "verdict": "string",
          "matchedStrings": [
            "string"
          ],
          "author": "string",
          "version": "string",
          "threatLevel": 0.1,
          "confidence": 0.1,
          "strength": 0.1
        }
      ],
      "tags": [
        {
          "name": "string",
          "verdict": "string"
        }
      ],
      "metaData": {
        "entropy": 0.1,
        "forensicAnalysisRecommended": true,
        "fuzzyFsioHash": "string"
      }
    },
    "errorCategory": "string",
    "errorCode": 0,
    "errorDetails": "string"
```

```
"processInfo": {
    "postProcessing": {
      "actionsRan": "string",
      "actionsFailed": "string",
      "convertedTo": "string",
      "copyMoveDestination": "string",
      "convertedDestination": "string",
      "sanitizationDetails": {
        "failureCategory": "string",
        "description": "string",
        "details": "string"
      }
    },
    "progressPercentage": 0,
    "userAgent": "string",
    "profile": "string",
    "result": "string",
    "blockedReason": "string",
    "fileTypeSkippedScan": true,
    "processingTime": 0.1,
    "queueTime": 0.1,
    "resultI": 0
  },
  "dataId": "string",
  "dlpInfo": {
    "hits": null,
    "verdict": 0
  },
  "sbomInfo": {
    "finalVerdict": {
      "blocked": true,
      "licensingPackageCounts": {
        "allowed": 0,
        "blocked": 0,
        "unknown": 0,
        "unsupported": 0
      },
      "severity": 0,
      "totalPackageCount": 0,
      "verdict": "string",
      "vulnerabilityCounts": {
        "critical": 0,
        "high": 0,
        "medium": 0,
        "low": 0,
        "unknown": 0
      }
    },
    "overviewReport": {
      "isPartialReport": true,
      "osInfo": {
        "osName": "string",
        "osVersion": "string"
```

```
"scanMode": "string",
      "steps": [
        {
          "command": "string",
          "packages": [
            {
              "authors": "string",
              "releaseDate": "2019-08-24T14:15:22Z",
              "ecosystem": "string",
              "group": "string",
              "archive": true,
              "executable": true,
              "uid": "string",
              "licenses": {
                "allowed": [
                  {
                    "id": "string",
                    "url": "string",
                    "category": "string",
                    "usageRestriction": {
                      "permissions": [
                        "string"
                      ],
                      "conditions": [
                        "string"
                      ],
                      "limitations": [
                        "string"
                      ]
                    }
                  }
                ],
                "blocked": [
                  {
                    "id": "string",
                    "url": "string",
                    "category": "string",
                    "usageRestriction": {
                      "permissions": [
                        "string"
                      ],
                      "conditions": [
                        "string"
                      ],
                      "limitations": [
                        "string"
                      ]
                    }
                  }
                ]
              },
              "packageName": "string",
              "packageVersion": "string",
```

```
{
                    "sha256": "string",
                    "fileName": "string"
                  }
                ],
                "vulnerabilityCounts": {
                  "critical": 0,
                  "high": 0,
                  "medium": 0,
                  "low": 0,
                  "unknown": 0
                },
                "vulnerabilities": [
                  {
                    "id": "string",
                    "severity": 0,
                    "source": "string",
                    "fixedVersions": "string",
                    "cwes": [
                      "string"
                    ]
                  }
                ],
                "arch": "string",
                "osName": "string",
                "osVersion": "string",
                "dependencies": [
                  {
                    "ecosystem": "string",
                    "group": "string",
                    "packageName": "string",
                    "packageVersion": "string",
                    "vulnerabilities": [
                      {
                        "id": "string",
                        "severity": 0,
                        "source": "string",
                        "fixedVersions": "string",
                        "cwes": [
                          "string"
                        ]
                      }
                    ],
                    "vulnerabilityCounts": {
                      "critical": 0,
                      "high": 0,
                      "medium": 0,
                      "low": 0,
                      "unknown": 0
                    }
                  }
                ]
              }
```

```
"licenseStatus": "string",
          "licensingPackageCounts": {
            "allowed": 0,
            "blocked": 0,
            "unknown": 0,
            "unsupported": 0
          },
          "step": 0,
          "vulnerabilityCount": 0,
          "sha256": "string",
          "severity": 0,
          "vulnerabilityCounts": {
            "critical": 0,
            "high": 0,
            "medium": 0,
            "low": 0,
            "unknown": 0
          }
        }
      ],
      "packages": [
        {
          "authors": "string",
          "releaseDate": "2019-08-24T14:15:22Z",
          "ecosystem": "string",
          "group": "string",
          "archive": true,
          "executable": true,
          "uid": "string",
          "licenses": {
            "allowed": [
              {
                "id": "string",
                "url": "string",
                "category": "string",
                "usageRestriction": {
                  "permissions": [
                    "string"
                  ],
                  "conditions": [
                    "string"
                  ],
                  "limitations": [
                    "string"
                  ]
                }
              }
            ],
            "blocked": [
              {
                "id": "string",
                "url": "string",
                "category": "string",
```

```
"permissions": [
                    "string"
                  ],
                  "conditions": [
                    "string"
                  ],
                  "limitations": [
                    "string"
                  ]
                }
              }
            ]
          },
          "packageName": "string",
          "packageVersion": "string",
          "target": "string",
          "hashes": [
            {
              "sha256": "string",
              "fileName": "string"
            }
          ],
          "vulnerabilities": [
            {
              "id": "string",
              "severity": 0,
              "source": "string",
              "fixedVersions": "string",
              "cwes": [
                "string"
              ]
            }
          ],
          "vulnerabilityCounts": {
            "critical": 0,
            "high": 0,
            "medium": 0,
            "low": 0,
            "unknown": 0
          },
          "dependencies": [
            {
              "ecosystem": "string",
              "group": "string",
              "packageName": "string",
              "packageVersion": "string",
              "vulnerabilities": [
                {
                  "id": "string",
                  "severity": 0,
                  "source": "string",
                  "fixedVersions": "string",
                  "cwes": [
```

```
]
                }
              ],
              "vulnerabilityCounts": {
                "critical": 0,
                "high": 0,
                "medium": 0,
                "low": 0,
                "unknown": 0
              }
            }
          ]
        }
      ],
      "dependenciesPackageCount": 0,
      "dependenciesVulnerabilityTotal": 0,
      "dependenciesVulnerabilityCounts": {
        "critical": 0,
        "high": 0,
        "medium": 0,
        "low": 0,
        "unknown": 0
      }
    },
    "resultTemplateHash": "string"
  },
  "vulnerabilityInfo": {
    "vulnerabilityInfoResult": {
      "code": 0,
      "hash": "string",
      "method": 0,
      "timeStamp": "string",
      "timing": 0,
      "detectedProduct": {
        "hasVulnerability": true,
        "isCurrent": true,
        "product": {
          "id": 0,
          "name": "string"
        },
        "remediationLink": "string",
        "severity": "string",
        "sigName": "string",
        "signature": 0,
        "vendor": {
          "id": 0,
          "name": "string"
        },
        "version": "string",
        "versionData": {
          "countBehind": 0,
          "feedId": 0,
          "version": "string"
```

```
"vulnerabilities": [
          {
            "description": "string",
            "details": {
              "cpe": "string",
              "cve": "string",
              "cvss": {
                "accessComplexity": "string",
                "accessVector": "string",
                "authentication": "string",
                "availabilityImpact": "string",
                "confidentialityImpact": "string",
                "generatedOnEpoch": "string",
                "integrityImpact": "string",
                "score": "string",
                "source": "string"
              },
              "cvss3": {
                "attackComplexity": "string",
                "attackVector": "string",
                "availabilityImpact": "string",
                "baseScore": "string",
                "baseSeverity": "string",
                "confidentialityImpact": "string",
                "exploitabilityScore": "string",
                "impactScore": "string",
                "integrityImpact": "string",
                "privilegesRequired": "string",
                "scope": "string",
                "userInteraction": "string",
                "vectorString": "string"
              },
              "cwe": "string",
              "lastModifiedEpoch": "string",
              "publishedEpoch": "string",
              "references": [
                "string"
              ]
            },
            "severity": "string",
            "severityIndex": 0,
            "staticId": 0
          }
        ]
      }
    }
  },
  "sessionCookie": "string",
  "fileTypeInfo": {
    "fileInfoExtended": {
      "extensions": "string",
      "groupId": "string",
      "typeId": "string"
```

```
},
  "scanInstanceUrl": "string",
  "scanWorkflowSnapshotId": "string",
  "coreEngines": [
    {
      "engineId": "string",
      "engineName": "string",
      "engineVersion": "string",
      "dbVersion": "string",
      "definitionTime": "string"
    }
  ]
}
```


Properties

Name	Type	Required	Restrictions	Description
extractedFiles	ExtractedFiles¦null	false	none	none
scanResults	ScanResults¦null	false	none	none
fileInfo	FileInfo¦null	false	none	none
fileScanInfo	FileScanInfo¦null	false	none	none
processInfo	ProcessInfo¦null	false	none	none
dataId	string	true	none	none
dlpInfo	DlpInfo¦null	false	none	none
sbomInfo	SbomInfo¦null	false	none	none
vulnerabilityInfo	VulnerabilityInfo¦null	false	none	none
sessionCookie	string¦null	false	none	none
fileTypeInfo	FileTypeInfo¦null	false	none	none
scanInstanceUrl	string¦null	false	none	none
scanWorkflowSnapshotId	string¦null	false	none	none
coreEngines	[CoreEngine]¦null	false	none	none

ExtractedFiles

```
{
  "dataId": "string",
  "scanResultI": 0,
  "detectedBy": 0,
  "filesExtractedCount": 0
}
```


Properties

Name	Type	Required	Restrictions	Description
dataId	string	true	none	none
scanResultI	integer(int32)|null	false	none	none
detectedBy	integer(int32)|null	false	none	none
filesExtractedCount	integer(int32)|null	false	none	none

ScanResults


```
{
  "scanDetails": [
    {
      "engineName": "string",
      "threatFound": "string",
      "scanResultI": 0,
      "defTime": "string",
      "scanTime": 0.1,
      "engId": "string",
      "waitTime": 0.1
    }
  ],
  "dataId": "string",
  "scanAllResultI": 0,
  "scanAllResultA": "string",
  "startTime": "string",
  "totalTime": 0.1,
  "totalAvs": 0,
  "totalDetections": 0,
  "progressPercentage": 0
}
```

Properties

Name	Type	Required	Restrictions	Description
scanDetails	[EngineResult]¦null	true	none	none
dataId	string	true	none	none
scanAllResultI	integer(int32)	false	none	none
scanAllResultA	string	true	none	none
startTime	string	true	none	none
totalTime	number(double)	false	none	none
totalAvs	integer(int32)	false	none	none
totalDetections	integer(int32)¦null	false	none	none
progressPercentage	integer(int32)	false	none	none

EngineResult

```
{
  "engineName": "string",
  "threatFound": "string",
  "scanResultI": 0,
  "defTime": "string",
  "scanTime": 0.1,
  "engId": "string",
  "waitTime": 0.1
}
```

Properties

Name	Type	Required	Restrictions	Description
engineName	string	true	none	none
threatFound	string	true	none	none
scanResultI	integer(int32)	false	none	none
defTime	string	true	none	none
scanTime	number(double)	false	none	none
engId	string	true	none	none
waitTime	number(double)	false	none	none

FileInfo

```
{
  "fileSize": 0,
  "uploadTimestamp": "string",
  "md5": "string",
  "sha1": "string",
  "sha256": "string",
  "fileTypeCategory": "string",
  "fileTypeDescription": "string",
  "fileTypeExtension": "string",
  "displayName": "string",
  "fileTypeId": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
fileSize	integer(int64)	false	none	none
uploadTimestamp	string	true	none	none
md5	string	true	none	none
sha1	string	true	none	none
sha256	string	true	none	none
fileTypeCategory	string	true	none	none
fileTypeDescription	string	true	none	none
fileTypeExtension	string	true	none	none
displayName	string	true	none	none
fileTypeId	string¦null	false	none	none

FileScanInfo

```
{
  "finalVerdict": {
    "blocked": true,
    "verdict": "string",
    "confidence": 0.1,
    "threatLevel": 0.1
  },
  "overviewReport": {
    "analysisState": "string",
    "signalGroups": [
      {
        "description": "string",
        "verdict": "string",
        "signals": [
          {
            "originType": "string",
            "signalReadable": "string",
            "strength": 0.1
          }
        ],
        "mitreTechniques": [
          {
            "name": "string",
            "tacticName": "string"
          }
        ]
      }
    ],
    "iocs": [
      {
        "data": "string",
        "type": "string",
        "origin": "string",
        "verdict": "string"
      }
    ],
    "yaraMatches": [
      {
        "ruleName": "string",
        "ruleDescription": "string",
        "verdict": "string",
        "matchedStrings": [
          "string"
        ],
        "author": "string",
        "version": "string",
        "threatLevel": 0.1,
        "confidence": 0.1,
        "strength": 0.1
      }
    ],
    "tags": [
```

```
"name": "string",
        "verdict": "string"
      }
    ],
    "metaData": {
      "entropy": 0.1,
      "forensicAnalysisRecommended": true,
      "fuzzyFsioHash": "string"
    }
  },
  "errorCategory": "string",
  "errorCode": 0,
  "errorDetails": "string"
}
```


Properties

Name	Type	Required	Restrictions	Description
finalVerdict	FileScanInfoFinalVerdict¦null	false	none	none
overviewReport	FileScanInfoOverviewReport¦null	false	none	none
errorCategory	string¦null	false	none	none
errorCode	integer(int32)¦null	false	none	none
errorDetails	string¦null	false	none	none

FileScanInfoFinalVerdict


```
{
  "blocked": true,
  "verdict": "string",
  "confidence": 0.1,
  "threatLevel": 0.1
}
```

Properties

Name	Type	Required	Restrictions	Description
blocked	boolean¦null	false	none	none
verdict	string	true	none	none
confidence	number(float)	true	none	none
threatLevel	number(float)	true	none	none

FileScanInfoOverviewReport

```
{
  "analysisState": "string",
  "signalGroups": [
    {
      "description": "string",
      "verdict": "string",
      "signals": [
        {
          "originType": "string",
          "signalReadable": "string",
          "strength": 0.1
        }
      ],
      "mitreTechniques": [
        {
          "name": "string",
          "tacticName": "string"
        }
      ]
    }
  ],
  "iocs": [
    {
      "data": "string",
      "type": "string",
      "origin": "string",
      "verdict": "string"
    }
  ],
  "yaraMatches": [
    {
      "ruleName": "string",
      "ruleDescription": "string",
      "verdict": "string",
      "matchedStrings": [
        "string"
      ],
      "author": "string",
      "version": "string",
      "threatLevel": 0.1,
      "confidence": 0.1,
      "strength": 0.1
    }
  ],
  "tags": [
    {
      "name": "string",
      "verdict": "string"
    }
  ],
  "metaData": {
    "entropy": 0.1,
```

```
"fuzzyFsioHash": "string"
  }
}
```

Properties

Name	Type	Required	Restrictions	Description
analysisState	string	true	none	none
signalGroups	[FileScanInfoSignalGroup]	true	none	none
iocs	[FileScanInfoIoc]¦null	false	none	none
yaraMatches	[FileScanInfoYaraMatch]¦null	false	none	none
tags	[FileScanInfoTag]¦null	false	none	none
metaData	FileScanInfoMetaData¦null	false	none	none

FileScanInfoSignalGroup

```
{
  "description": "string",
  "verdict": "string",
  "signals": [
    {
      "originType": "string",
      "signalReadable": "string",
      "strength": 0.1
    }
  ],
  "mitreTechniques": [
    {
      "name": "string",
      "tacticName": "string"
    }
  ]
}
```

Properties

Name	Type	Required	Restrictions	Description
description	string	true	none	none
verdict	string	true	none	none
signals	[FileScanInfoSignal]	true	none	none
mitreTechniques	[FileScanInfoMitreTechnique]¦null	false	none	none

FileScanInfoSignal

```
{
  "originType": "string",
  "signalReadable": "string",
  "strength": 0.1
}
```

Properties

Name	Type	Required	Restrictions	Description
originType	string	true	none	none
signalReadable	string	true	none	none
strength	number(float)	true	none	none

FileScanInfoMitreTechnique

```
{
  "name": "string",
  "tacticName": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
name	string¦null	false	none	none
tacticName	string¦null	false	none	none

FileScanInfoIoc

```
{
  "data": "string",
  "type": "string",
  "origin": "string",
  "verdict": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
data	string¦null	false	none	none
type	string¦null	false	none	none
origin	string¦null	false	none	none
verdict	string¦null	false	none	none

FileScanInfoYaraMatch

```
{
  "ruleName": "string",
  "ruleDescription": "string",
  "verdict": "string",
  "matchedStrings": [
    "string"
  ],
  "author": "string",
  "version": "string",
  "threatLevel": 0.1,
  "confidence": 0.1,
  "strength": 0.1
}
```

Properties

Name	Type	Required	Restrictions	Description
ruleName	string¦null	false	none	none
ruleDescription	string¦null	false	none	none
verdict	string¦null	false	none	none
matchedStrings	[string]¦null	false	none	none
author	string¦null	false	none	none
version	string¦null	false	none	none
threatLevel	number{float}¦null	false	none	none
confidence	number{float}¦null	false	none	none
strength	number{float}¦null	false	none	none

FileScanInfoTag

```
{
  "name": "string",
  "verdict": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
name	string¦null	false	none	none
verdict	string¦null	false	none	none

FileScanInfoMetaData

```
{
  "entropy": 0.1,
  "forensicAnalysisRecommended": true,
  "fuzzyFsioHash": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
entropy	number(float)¦null	false	none	none
forensicAnalysisRecommended	boolean¦null	false	none	none
fuzzyFsioHash	string¦null	false	none	none

ProcessInfo


```
{
  "postProcessing": {
    "actionsRan": "string",
    "actionsFailed": "string",
    "convertedTo": "string",
    "copyMoveDestination": "string",
    "convertedDestination": "string",
    "sanitizationDetails": {
      "failureCategory": "string",
      "description": "string",
      "details": "string"
    }
  },
  "progressPercentage": 0,
  "userAgent": "string",
  "profile": "string",
  "result": "string",
  "blockedReason": "string",
  "fileTypeSkippedScan": true,
  "processingTime": 0.1,
  "queueTime": 0.1,
  "resultI": 0
}
```

Properties

Name	Type	Required	Restrictions	Description
postProcessing	PostProcessing¦null	false	none	none
progressPercentage	integer(int32)	false	none	none
userAgent	string	true	none	none
profile	string	true	none	none
result	string¦null	false	none	none
blockedReason	string	true	none	none
fileTypeSkippedScan	boolean	false	none	none
processingTime	number(double)	false	none	none
queueTime	number(double)	false	none	none
resultI	ResultI2	false	none	- 0: Allowed - 1: Blocked - 2: Processing

PostProcessing

```
{
  "actionsRan": "string",
  "actionsFailed": "string",
  "convertedTo": "string",
  "copyMoveDestination": "string",
  "convertedDestination": "string",
  "sanitizationDetails": {
    "failureCategory": "string",
    "description": "string",
    "details": "string"
  }
}
```

Properties

Name	Type	Required	Restrictions	Description
actionsRan	string	true	none	none
actionsFailed	string	true	none	none
convertedTo	string¦null	false	none	none
copyMoveDestination	string¦null	false	none	none
convertedDestination	string¦null	false	none	none
sanitizationDetails	SanitizationDetails¦null	false	none	none

SanitizationDetails

```
{
  "failureCategory": "string",
  "description": "string",
  "details": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
failureCategory	string¦null	false	none	none
description	string¦null	false	none	none
details	string¦null	false	none	none

ResultI2

```
0
```

- 0: Allowed
- 1: Blocked
- 2: Processing

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: Allowed - 1: Blocked - 2: Processing

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2

DlpInfo

```
{
  "hits": null,
  "verdict": 0
}
```

Properties

Name	Type	Required	Restrictions	Description
hits	any	false	none	none
verdict	integer(int64)¦null	false	none	none

SbomInfo

```
{
  "finalVerdict": {
    "blocked": true,
    "licensingPackageCounts": {
      "allowed": 0,
      "blocked": 0,
      "unknown": 0,
      "unsupported": 0
    },
    "severity": 0,
    "totalPackageCount": 0,
    "verdict": "string",
    "vulnerabilityCounts": {
      "critical": 0,
      "high": 0,
      "medium": 0,
      "low": 0,
      "unknown": 0
    }
  },
  "overviewReport": {
    "isPartialReport": true,
    "osInfo": {
      "osName": "string",
      "osVersion": "string"
    },
    "scanMode": "string",
    "steps": [
      {
        "command": "string",
        "packages": [
          {
            "authors": "string",
            "releaseDate": "2019-08-24T14:15:22Z",
            "ecosystem": "string",
            "group": "string",
            "archive": true,
            "executable": true,
            "uid": "string",
            "licenses": {
              "allowed": [
                {
                  "id": "string",
                  "url": "string",
                  "category": "string",
                  "usageRestriction": {
                    "permissions": [
                      "string"
                    ],
                    "conditions": [
                      "string"
                    ],
```

```
"string"
                    ]
                  }
                }
              ],
              "blocked": [
                {
                  "id": "string",
                  "url": "string",
                  "category": "string",
                  "usageRestriction": {
                    "permissions": [
                      "string"
                    ],
                    "conditions": [
                      "string"
                    ],
                    "limitations": [
                      "string"
                    ]
                  }
                }
              ]
            },
            "packageName": "string",
            "packageVersion": "string",
            "hashes": [
              {
                "sha256": "string",
                "fileName": "string"
              }
            ],
            "vulnerabilityCounts": {
              "critical": 0,
              "high": 0,
              "medium": 0,
              "low": 0,
              "unknown": 0
            },
            "vulnerabilities": [
              {
                "id": "string",
                "severity": 0,
                "source": "string",
                "fixedVersions": "string",
                "cwes": [
                  "string"
                ]
              }
            ],
            "arch": "string",
            "osName": "string",
            "osVersion": "string",
```

```
{
                "ecosystem": "string",
                "group": "string",
                "packageName": "string",
                "packageVersion": "string",
                "vulnerabilities": [
                  {
                    "id": "string",
                    "severity": 0,
                    "source": "string",
                    "fixedVersions": "string",
                    "cwes": [
                      "string"
                    ]
                  }
                ],
                "vulnerabilityCounts": {
                  "critical": 0,
                  "high": 0,
                  "medium": 0,
                  "low": 0,
                  "unknown": 0
                }
              }
            ]
          }
        ],
        "licenseStatus": "string",
        "licensingPackageCounts": {
          "allowed": 0,
          "blocked": 0,
          "unknown": 0,
          "unsupported": 0
        },
        "step": 0,
        "vulnerabilityCount": 0,
        "sha256": "string",
        "severity": 0,
        "vulnerabilityCounts": {
          "critical": 0,
          "high": 0,
          "medium": 0,
          "low": 0,
          "unknown": 0
        }
      }
    ],
    "packages": [
      {
        "authors": "string",
        "releaseDate": "2019-08-24T14:15:22Z",
        "ecosystem": "string",
        "group": "string",
```

```
"executable": true,
        "uid": "string",
        "licenses": {
          "allowed": [
            {
              "id": "string",
              "url": "string",
              "category": "string",
              "usageRestriction": {
                "permissions": [
                  "string"
                ],
                "conditions": [
                  "string"
                ],
                "limitations": [
                  "string"
                ]
              }
            }
          ],
          "blocked": [
            {
              "id": "string",
              "url": "string",
              "category": "string",
              "usageRestriction": {
                "permissions": [
                  "string"
                ],
                "conditions": [
                  "string"
                ],
                "limitations": [
                  "string"
                ]
              }
            }
          ]
        },
        "packageName": "string",
        "packageVersion": "string",
        "target": "string",
        "hashes": [
          {
            "sha256": "string",
            "fileName": "string"
          }
        ],
        "vulnerabilities": [
          {
            "id": "string",
            "severity": 0,
```

```
"fixedVersions": "string",
            "cwes": [
              "string"
            ]
          }
        ],
        "vulnerabilityCounts": {
          "critical": 0,
          "high": 0,
          "medium": 0,
          "low": 0,
          "unknown": 0
        },
        "dependencies": [
          {
            "ecosystem": "string",
            "group": "string",
            "packageName": "string",
            "packageVersion": "string",
            "vulnerabilities": [
              {
                "id": "string",
                "severity": 0,
                "source": "string",
                "fixedVersions": "string",
                "cwes": [
                  "string"
                ]
              }
            ],
            "vulnerabilityCounts": {
              "critical": 0,
              "high": 0,
              "medium": 0,
              "low": 0,
              "unknown": 0
            }
          }
        ]
      }
    ],
    "dependenciesPackageCount": 0,
    "dependenciesVulnerabilityTotal": 0,
    "dependenciesVulnerabilityCounts": {
      "critical": 0,
      "high": 0,
      "medium": 0,
      "low": 0,
      "unknown": 0
    }
  },
  "resultTemplateHash": "string"
```

```
}
```

Properties

Name	Type	Required	Restrictions	Description
finalVerdict	FinalVerdict¦null	false	none	none
overviewReport	OverviewReport¦null	false	none	none
resultTemplateHash	string	false	none	none

FinalVerdict

```
{
  "blocked": true,
  "licensingPackageCounts": {
    "allowed": 0,
    "blocked": 0,
    "unknown": 0,
    "unsupported": 0
  },
  "severity": 0,
  "totalPackageCount": 0,
  "verdict": "string",
  "vulnerabilityCounts": {
    "critical": 0,
    "high": 0,
    "medium": 0,
    "low": 0,
    "unknown": 0
  }
}
```

Properties

Name	Type	Required	Restrictions	Description
blocked	boolean	false	none	none
licensingPackageCounts	LicensingIssues¦null	false	none	none
severity	Severity	false	none	- 0: None - 1: Critical - 2: High - 3: Medium - 4: Low - 5: Unknown
totalPackageCount	integer(int32)	false	none	none
verdict	string	false	none	none
vulnerabilityCounts	VulnerabilityIssues¦null	false	none	none

LicensingIssues

```
{
  "allowed": 0,
  "blocked": 0,
  "unknown": 0,
  "unsupported": 0
}
```

Properties

Name	Type	Required	Restrictions	Description
allowed	integer(int32)	false	none	none
blocked	integer(int32)	false	none	none
unknown	integer(int32)	false	none	none
unsupported	integer(int32)	false	none	none

Severity

```
0
```

- 0: None
- 1: Critical
- 2: High
- 3: Medium
- 4: Low
- 5: Unknown

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: None - 1: Critical - 2: High - 3: Medium - 4: Low - 5: Unknown

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2
anonymous	3
anonymous	4
anonymous	5

VulnerabilityIssues

```
{
  "critical": 0,
  "high": 0,
  "medium": 0,
  "low": 0,
  "unknown": 0
}
```


Properties

Name	Type	Required	Restrictions	Description
critical	integer(int32)	false	none	none
high	integer(int32)	false	none	none
medium	integer(int32)	false	none	none
low	integer(int32)	false	none	none
unknown	integer(int32)¦null	false	none	none

OverviewReport

```
{
  "isPartialReport": true,
  "osInfo": {
    "osName": "string",
    "osVersion": "string"
  },
  "scanMode": "string",
  "steps": [
    {
      "command": "string",
      "packages": [
        {
          "authors": "string",
          "releaseDate": "2019-08-24T14:15:22Z",
          "ecosystem": "string",
          "group": "string",
          "archive": true,
          "executable": true,
          "uid": "string",
          "licenses": {
            "allowed": [
              {
                "id": "string",
                "url": "string",
                "category": "string",
                "usageRestriction": {
                  "permissions": [
                    "string"
                  ],
                  "conditions": [
                    "string"
                  ],
                  "limitations": [
                    "string"
                  ]
                }
              }
            ],
            "blocked": [
              {
                "id": "string",
                "url": "string",
                "category": "string",
                "usageRestriction": {
                  "permissions": [
                    "string"
                  ],
                  "conditions": [
                    "string"
                  ],
                  "limitations": [
                    "string"
```

```
}
            }
          ]
        },
        "packageName": "string",
        "packageVersion": "string",
        "hashes": [
          {
            "sha256": "string",
            "fileName": "string"
          }
        ],
        "vulnerabilityCounts": {
          "critical": 0,
          "high": 0,
          "medium": 0,
          "low": 0,
          "unknown": 0
        },
        "vulnerabilities": [
          {
            "id": "string",
            "severity": 0,
            "source": "string",
            "fixedVersions": "string",
            "cwes": [
              "string"
            ]
          }
        ],
        "arch": "string",
        "osName": "string",
        "osVersion": "string",
        "dependencies": [
          {
            "ecosystem": "string",
            "group": "string",
            "packageName": "string",
            "packageVersion": "string",
            "vulnerabilities": [
              {
                "id": "string",
                "severity": 0,
                "source": "string",
                "fixedVersions": "string",
                "cwes": [
                  "string"
                ]
              }
            ],
            "vulnerabilityCounts": {
              "critical": 0,
              "high": 0,
```

```
"low": 0,
                "unknown": 0
              }
            }
          ]
        }
      ],
      "licenseStatus": "string",
      "licensingPackageCounts": {
        "allowed": 0,
        "blocked": 0,
        "unknown": 0,
        "unsupported": 0
      },
      "step": 0,
      "vulnerabilityCount": 0,
      "sha256": "string",
      "severity": 0,
      "vulnerabilityCounts": {
        "critical": 0,
        "high": 0,
        "medium": 0,
        "low": 0,
        "unknown": 0
      }
    }
  ],
  "packages": [
    {
      "authors": "string",
      "releaseDate": "2019-08-24T14:15:22Z",
      "ecosystem": "string",
      "group": "string",
      "archive": true,
      "executable": true,
      "uid": "string",
      "licenses": {
        "allowed": [
          {
            "id": "string",
            "url": "string",
            "category": "string",
            "usageRestriction": {
              "permissions": [
                "string"
              ],
              "conditions": [
                "string"
              ],
              "limitations": [
                "string"
              ]
            }
```

```
],
        "blocked": [
          {
            "id": "string",
            "url": "string",
            "category": "string",
            "usageRestriction": {
              "permissions": [
                "string"
              ],
              "conditions": [
                "string"
              ],
              "limitations": [
                "string"
              ]
            }
          }
        ]
      },
      "packageName": "string",
      "packageVersion": "string",
      "target": "string",
      "hashes": [
        {
          "sha256": "string",
          "fileName": "string"
        }
      ],
      "vulnerabilities": [
        {
          "id": "string",
          "severity": 0,
          "source": "string",
          "fixedVersions": "string",
          "cwes": [
            "string"
          ]
        }
      ],
      "vulnerabilityCounts": {
        "critical": 0,
        "high": 0,
        "medium": 0,
        "low": 0,
        "unknown": 0
      },
      "dependencies": [
        {
          "ecosystem": "string",
          "group": "string",
          "packageName": "string",
          "packageVersion": "string",
```

```
{
              "id": "string",
              "severity": 0,
              "source": "string",
              "fixedVersions": "string",
              "cwes": [
                "string"
              ]
            }
          ],
          "vulnerabilityCounts": {
            "critical": 0,
            "high": 0,
            "medium": 0,
            "low": 0,
            "unknown": 0
          }
        }
      ]
    }
  ],
  "dependenciesPackageCount": 0,
  "dependenciesVulnerabilityTotal": 0,
  "dependenciesVulnerabilityCounts": {
    "critical": 0,
    "high": 0,
    "medium": 0,
    "low": 0,
    "unknown": 0
  }
}
```


Properties

Name	Type	Required	Restrictions	Description
isPartialReport	boolean	false	none	none
osInfo	OsInfo¦null	false	none	none
scanMode	string	false	none	none
steps	[oneOf]¦null	false	none	none
packages	[oneOf]¦null	false	none	none
dependenciesPackageCount	integer(int32)¦null	false	none	none
dependenciesVulnerabilityTotal	integer(int32)¦null	false	none	none
dependenciesVulnerabilityCounts	VulnerabilityCounts¦null	false	none	none

OsInfo


```
{
  "osName": "string",
  "osVersion": "string"
}
```


Properties

Name	Type	Required	Restrictions	Description
osName	string	false	none	none
osVersion	string	false	none	none

SbomStep

```
{
  "command": "string",
  "packages": [
    {
      "authors": "string",
      "releaseDate": "2019-08-24T14:15:22Z",
      "ecosystem": "string",
      "group": "string",
      "archive": true,
      "executable": true,
      "uid": "string",
      "licenses": {
        "allowed": [
          {
            "id": "string",
            "url": "string",
            "category": "string",
            "usageRestriction": {
              "permissions": [
                "string"
              ],
              "conditions": [
                "string"
              ],
              "limitations": [
                "string"
              ]
            }
          }
        ],
        "blocked": [
          {
            "id": "string",
            "url": "string",
            "category": "string",
            "usageRestriction": {
              "permissions": [
                "string"
              ],
              "conditions": [
                "string"
              ],
              "limitations": [
                "string"
              ]
            }
          }
        ]
      },
      "packageName": "string",
      "packageVersion": "string",
      "hashes": [
```

```
"sha256": "string",
          "fileName": "string"
        }
      ],
      "vulnerabilityCounts": {
        "critical": 0,
        "high": 0,
        "medium": 0,
        "low": 0,
        "unknown": 0
      },
      "vulnerabilities": [
        {
          "id": "string",
          "severity": 0,
          "source": "string",
          "fixedVersions": "string",
          "cwes": [
            "string"
          ]
        }
      ],
      "arch": "string",
      "osName": "string",
      "osVersion": "string",
      "dependencies": [
        {
          "ecosystem": "string",
          "group": "string",
          "packageName": "string",
          "packageVersion": "string",
          "vulnerabilities": [
            {
              "id": "string",
              "severity": 0,
              "source": "string",
              "fixedVersions": "string",
              "cwes": [
                "string"
              ]
            }
          ],
          "vulnerabilityCounts": {
            "critical": 0,
            "high": 0,
            "medium": 0,
            "low": 0,
            "unknown": 0
          }
        }
      ]
    }
  ],
```

```
"licensingPackageCounts": {
    "allowed": 0,
    "blocked": 0,
    "unknown": 0,
    "unsupported": 0
  },
  "step": 0,
  "vulnerabilityCount": 0,
  "sha256": "string",
  "severity": 0,
  "vulnerabilityCounts": {
    "critical": 0,
    "high": 0,
    "medium": 0,
    "low": 0,
    "unknown": 0
  }
}
```


Properties

Name	Type	Required	Restrictions	Description
command	string	false	none	none
packages	[oneOf]¦null	false	none	none
licenseStatus	string	false	none	none
licensingPackageCounts	LicensingIssues¦null	false	none	none
step	integer(int32)	false	none	none
vulnerabilityCount	integer(int32)	false	none	none
sha256	string	false	none	none
severity	Severity	false	none	- 0: None - 1: Critical - 2: High - 3: Medium - 4: Low - 5: Unknown
vulnerabilityCounts	VulnerabilityCounts¦null	false	none	none

ContainerPackage

```
{
  "authors": "string",
  "releaseDate": "2019-08-24T14:15:22Z",
  "ecosystem": "string",
  "group": "string",
  "archive": true,
  "executable": true,
  "uid": "string",
  "licenses": {
    "allowed": [
      {
        "id": "string",
        "url": "string",
        "category": "string",
        "usageRestriction": {
          "permissions": [
            "string"
          ],
          "conditions": [
            "string"
          ],
          "limitations": [
            "string"
          ]
        }
      }
    ],
    "blocked": [
      {
        "id": "string",
        "url": "string",
        "category": "string",
        "usageRestriction": {
          "permissions": [
            "string"
          ],
          "conditions": [
            "string"
          ],
          "limitations": [
            "string"
          ]
        }
      }
    ]
  },
  "packageName": "string",
  "packageVersion": "string",
  "hashes": [
    {
      "sha256": "string",
      "fileName": "string"
```

```
],
  "vulnerabilityCounts": {
    "critical": 0,
    "high": 0,
    "medium": 0,
    "low": 0,
    "unknown": 0
  },
  "vulnerabilities": [
    {
      "id": "string",
      "severity": 0,
      "source": "string",
      "fixedVersions": "string",
      "cwes": [
        "string"
      ]
    }
  ],
  "arch": "string",
  "osName": "string",
  "osVersion": "string",
  "dependencies": [
    {
      "ecosystem": "string",
      "group": "string",
      "packageName": "string",
      "packageVersion": "string",
      "vulnerabilities": [
        {
          "id": "string",
          "severity": 0,
          "source": "string",
          "fixedVersions": "string",
          "cwes": [
            "string"
          ]
        }
      ],
      "vulnerabilityCounts": {
        "critical": 0,
        "high": 0,
        "medium": 0,
        "low": 0,
        "unknown": 0
      }
    }
  ]
}
```

Properties

Name	Type	Required	Restrictions	Description
authors	string¦null	false	none	none
releaseDate	string(date-time)¦null	false	none	none
ecosystem	string	false	none	none
group	string	false	none	none
archive	boolean¦null	false	none	none
executable	boolean¦null	false	none	none
uid	string	false	none	none
licenses	Licenses¦null	false	none	none
packageName	string	false	none	none
packageVersion	string	false	none	none
hashes	[Hash]¦null	false	none	none
vulnerabilityCounts	VulnerabilityCounts¦null	false	none	none
vulnerabilities	[oneOf]¦null	false	none	none
arch	string	false	none	none
osName	string	false	none	none
osVersion	string	false	none	none
dependencies	[oneOf]¦null	false	none	none

Licenses

```
{
  "allowed": [
    {
      "id": "string",
      "url": "string",
      "category": "string",
      "usageRestriction": {
        "permissions": [
          "string"
        ],
        "conditions": [
          "string"
        ],
        "limitations": [
          "string"
        ]
      }
    }
  ],
  "blocked": [
    {
      "id": "string",
      "url": "string",
      "category": "string",
      "usageRestriction": {
        "permissions": [
          "string"
        ],
        "conditions": [
          "string"
        ],
        "limitations": [
          "string"
        ]
      }
    }
  ]
}
```


Properties

Name	Type	Required	Restrictions	Description
allowed	[LicenseInfo]¦null	false	none	none
blocked	[LicenseInfo]¦null	false	none	none

LicenseInfo

```
{
  "id": "string",
  "url": "string",
  "category": "string",
  "usageRestriction": {
    "permissions": [
      "string"
    ],
    "conditions": [
      "string"
    ],
    "limitations": [
      "string"
    ]
  }
}
```

Properties

Name	Type	Required	Restrictions	Description
id	string¦null	false	none	none
url	string¦null	false	none	none
category	string¦null	false	none	none
usageRestriction	UsageRestriction¦null	false	none	none

UsageRestriction

```
{
  "permissions": [
    "string"
  ],
  "conditions": [
    "string"
  ],
  "limitations": [
    "string"
  ]
}
```

Properties

Name	Type	Required	Restrictions	Description
permissions	[string]¦null	false	none	none
conditions	[string]¦null	false	none	none
limitations	[string]¦null	false	none	none

Hash

```
{
  "sha256": "string",
  "fileName": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
sha256	string	false	none	none
fileName	string¦null	false	none	none

VulnerabilityCounts

```
{
  "critical": 0,
  "high": 0,
  "medium": 0,
  "low": 0,
  "unknown": 0
}
```

Properties

Name	Type	Required	Restrictions	Description
critical	integer(int32)	false	none	none
high	integer(int32)	false	none	none
medium	integer(int32)	false	none	none
low	integer(int32)	false	none	none
unknown	integer(int32)	false	none	none

SbomVulnerability

```
{
  "id": "string",
  "severity": 0,
  "source": "string",
  "fixedVersions": "string",
  "cwes": [
    "string"
  ]
}
```

Properties

Name	Type	Required	Restrictions	Description
id	string¦null	false	none	none
severity	Severity	false	none	- 0: None - 1: Critical - 2: High - 3: Medium - 4: Low - 5: Unknown
source	string¦null	false	none	none
fixedVersions	string¦null	false	none	none
cwes	[string]¦null	false	none	none

Dependency


```
{
  "ecosystem": "string",
  "group": "string",
  "packageName": "string",
  "packageVersion": "string",
  "vulnerabilities": [
    {
      "id": "string",
      "severity": 0,
      "source": "string",
      "fixedVersions": "string",
      "cwes": [
        "string"
      ]
    }
  ],
  "vulnerabilityCounts": {
    "critical": 0,
    "high": 0,
    "medium": 0,
    "low": 0,
    "unknown": 0
  }
}
```


Properties

Name	Type	Required	Restrictions	Description
ecosystem	string	false	none	none
group	string	false	none	none
packageName	string	false	none	none
packageVersion	string	false	none	none
vulnerabilities	[oneOf]¦null	false	none	none
vulnerabilityCounts	VulnerabilityCounts¦null	false	none	none

SourceCodePackage

```
{
  "authors": "string",
  "releaseDate": "2019-08-24T14:15:22Z",
  "ecosystem": "string",
  "group": "string",
  "archive": true,
  "executable": true,
  "uid": "string",
  "licenses": {
    "allowed": [
      {
        "id": "string",
        "url": "string",
        "category": "string",
        "usageRestriction": {
          "permissions": [
            "string"
          ],
          "conditions": [
            "string"
          ],
          "limitations": [
            "string"
          ]
        }
      }
    ],
    "blocked": [
      {
        "id": "string",
        "url": "string",
        "category": "string",
        "usageRestriction": {
          "permissions": [
            "string"
          ],
          "conditions": [
            "string"
          ],
          "limitations": [
            "string"
          ]
        }
      }
    ]
  },
  "packageName": "string",
  "packageVersion": "string",
  "target": "string",
  "hashes": [
    {
      "sha256": "string",
```

```
}
  ],
  "vulnerabilities": [
    {
      "id": "string",
      "severity": 0,
      "source": "string",
      "fixedVersions": "string",
      "cwes": [
        "string"
      ]
    }
  ],
  "vulnerabilityCounts": {
    "critical": 0,
    "high": 0,
    "medium": 0,
    "low": 0,
    "unknown": 0
  },
  "dependencies": [
    {
      "ecosystem": "string",
      "group": "string",
      "packageName": "string",
      "packageVersion": "string",
      "vulnerabilities": [
        {
          "id": "string",
          "severity": 0,
          "source": "string",
          "fixedVersions": "string",
          "cwes": [
            "string"
          ]
        }
      ],
      "vulnerabilityCounts": {
        "critical": 0,
        "high": 0,
        "medium": 0,
        "low": 0,
        "unknown": 0
      }
    }
  ]
}
```

Properties

Name	Type	Required	Restrictions	Description
authors	string¦null	false	none	none
releaseDate	string(date-time)¦null	false	none	none
ecosystem	string	false	none	none
group	string	false	none	none
archive	boolean¦null	false	none	none
executable	boolean¦null	false	none	none
uid	string	false	none	none
licenses	Licenses¦null	false	none	none
packageName	string	false	none	none
packageVersion	string	false	none	none
target	string	false	none	none
hashes	[Hash]¦null	false	none	none
vulnerabilities	[oneOf]¦null	false	none	none
vulnerabilityCounts	VulnerabilityCounts¦null	false	none	none
dependencies	[oneOf]¦null	false	none	none

VulnerabilityInfo

```
{
  "vulnerabilityInfoResult": {
    "code": 0,
    "hash": "string",
    "method": 0,
    "timeStamp": "string",
    "timing": 0,
    "detectedProduct": {
      "hasVulnerability": true,
      "isCurrent": true,
      "product": {
        "id": 0,
        "name": "string"
      },
      "remediationLink": "string",
      "severity": "string",
      "sigName": "string",
      "signature": 0,
      "vendor": {
        "id": 0,
        "name": "string"
      },
      "version": "string",
      "versionData": {
        "countBehind": 0,
        "feedId": 0,
        "version": "string"
      },
      "vulnerabilities": [
        {
          "description": "string",
          "details": {
            "cpe": "string",
            "cve": "string",
            "cvss": {
              "accessComplexity": "string",
              "accessVector": "string",
              "authentication": "string",
              "availabilityImpact": "string",
              "confidentialityImpact": "string",
              "generatedOnEpoch": "string",
              "integrityImpact": "string",
              "score": "string",
              "source": "string"
            },
            "cvss3": {
              "attackComplexity": "string",
              "attackVector": "string",
              "availabilityImpact": "string",
              "baseScore": "string",
              "baseSeverity": "string",
              "confidentialityImpact": "string",
```

```
"impactScore": "string",
              "integrityImpact": "string",
              "privilegesRequired": "string",
              "scope": "string",
              "userInteraction": "string",
              "vectorString": "string"
            },
            "cwe": "string",
            "lastModifiedEpoch": "string",
            "publishedEpoch": "string",
            "references": [
              "string"
            ]
          },
          "severity": "string",
          "severityIndex": 0,
          "staticId": 0
        }
      ]
    }
  }
}
```


Properties

Name	Type	Required	Restrictions	Description
vulnerabilityInfoResult	VulnerabilityInfoResult¦null	false	none	none

VulnerabilityInfoResult

```
{
  "code": 0,
  "hash": "string",
  "method": 0,
  "timeStamp": "string",
  "timing": 0,
  "detectedProduct": {
    "hasVulnerability": true,
    "isCurrent": true,
    "product": {
      "id": 0,
      "name": "string"
    },
    "remediationLink": "string",
    "severity": "string",
    "sigName": "string",
    "signature": 0,
    "vendor": {
      "id": 0,
      "name": "string"
    },
    "version": "string",
    "versionData": {
      "countBehind": 0,
      "feedId": 0,
      "version": "string"
    },
    "vulnerabilities": [
      {
        "description": "string",
        "details": {
          "cpe": "string",
          "cve": "string",
          "cvss": {
            "accessComplexity": "string",
            "accessVector": "string",
            "authentication": "string",
            "availabilityImpact": "string",
            "confidentialityImpact": "string",
            "generatedOnEpoch": "string",
            "integrityImpact": "string",
            "score": "string",
            "source": "string"
          },
          "cvss3": {
            "attackComplexity": "string",
            "attackVector": "string",
            "availabilityImpact": "string",
            "baseScore": "string",
            "baseSeverity": "string",
            "confidentialityImpact": "string",
            "exploitabilityScore": "string",
```

```
"integrityImpact": "string",
            "privilegesRequired": "string",
            "scope": "string",
            "userInteraction": "string",
            "vectorString": "string"
          },
          "cwe": "string",
          "lastModifiedEpoch": "string",
          "publishedEpoch": "string",
          "references": [
            "string"
          ]
        },
        "severity": "string",
        "severityIndex": 0,
        "staticId": 0
      }
    ]
  }
}
```


Properties

Name	Type	Required	Restrictions	Description
code	integer(int64)¦null	false	none	none
hash	string	true	none	none
method	integer(int64)¦null	false	none	none
timeStamp	string	true	none	none
timing	integer(int64)¦null	false	none	none
detectedProduct	DetectedProduct¦null	false	none	none

DetectedProduct

```
{
  "hasVulnerability": true,
  "isCurrent": true,
  "product": {
    "id": 0,
    "name": "string"
  },
  "remediationLink": "string",
  "severity": "string",
  "sigName": "string",
  "signature": 0,
  "vendor": {
    "id": 0,
    "name": "string"
  },
  "version": "string",
  "versionData": {
    "countBehind": 0,
    "feedId": 0,
    "version": "string"
  },
  "vulnerabilities": [
    {
      "description": "string",
      "details": {
        "cpe": "string",
        "cve": "string",
        "cvss": {
          "accessComplexity": "string",
          "accessVector": "string",
          "authentication": "string",
          "availabilityImpact": "string",
          "confidentialityImpact": "string",
          "generatedOnEpoch": "string",
          "integrityImpact": "string",
          "score": "string",
          "source": "string"
        },
        "cvss3": {
          "attackComplexity": "string",
          "attackVector": "string",
          "availabilityImpact": "string",
          "baseScore": "string",
          "baseSeverity": "string",
          "confidentialityImpact": "string",
          "exploitabilityScore": "string",
          "impactScore": "string",
          "integrityImpact": "string",
          "privilegesRequired": "string",
          "scope": "string",
          "userInteraction": "string",
          "vectorString": "string"
```

```
"cwe": "string",
        "lastModifiedEpoch": "string",
        "publishedEpoch": "string",
        "references": [
          "string"
        ]
      },
      "severity": "string",
      "severityIndex": 0,
      "staticId": 0
    }
  ]
}
```


Properties

Name	Type	Required	Restrictions	Description
hasVulnerability	boolean¦null	false	none	none
isCurrent	boolean¦null	false	none	none
product	Product¦null	false	none	none
remediationLink	string	true	none	none
severity	string	true	none	none
sigName	string	true	none	none
signature	integer(int64)¦null	false	none	none
vendor	Vendor¦null	false	none	none
version	string	true	none	none
versionData	VersionData¦null	false	none	none
vulnerabilities	[Vulnerability]¦null	true	none	none

Product


```
{
  "id": 0,
  "name": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
id	integer(int64)¦null	false	none	none
name	string	true	none	none

Vendor


```
{
  "id": 0,
  "name": "string"
}
```


Properties

Name	Type	Required	Restrictions	Description
id	integer(int64)¦null	false	none	none
name	string	true	none	none

VersionData


```
{
  "countBehind": 0,
  "feedId": 0,
  "version": "string"
}
```


Properties

Name	Type	Required	Restrictions	Description
countBehind	integer(int64)¦null	false	none	none
feedId	integer(int64)¦null	false	none	none
version	string	true	none	none

Vulnerability


```
{
  "description": "string",
  "details": {
    "cpe": "string",
    "cve": "string",
    "cvss": {
      "accessComplexity": "string",
      "accessVector": "string",
      "authentication": "string",
      "availabilityImpact": "string",
      "confidentialityImpact": "string",
      "generatedOnEpoch": "string",
      "integrityImpact": "string",
      "score": "string",
      "source": "string"
    },
    "cvss3": {
      "attackComplexity": "string",
      "attackVector": "string",
      "availabilityImpact": "string",
      "baseScore": "string",
      "baseSeverity": "string",
      "confidentialityImpact": "string",
      "exploitabilityScore": "string",
      "impactScore": "string",
      "integrityImpact": "string",
      "privilegesRequired": "string",
      "scope": "string",
      "userInteraction": "string",
      "vectorString": "string"
    },
    "cwe": "string",
    "lastModifiedEpoch": "string",
    "publishedEpoch": "string",
    "references": [
      "string"
    ]
  },
  "severity": "string",
  "severityIndex": 0,
  "staticId": 0
}
```

Properties

Name	Type	Required	Restrictions	Description
description	string	true	none	none
details	VulnerabilityDetails¦null	false	none	none
severity	string	true	none	none
severityIndex	integer(int32)¦null	false	none	none
staticId	integer(int64)¦null	false	none	none

VulnerabilityDetails

```
{
  "cpe": "string",
  "cve": "string",
  "cvss": {
    "accessComplexity": "string",
    "accessVector": "string",
    "authentication": "string",
    "availabilityImpact": "string",
    "confidentialityImpact": "string",
    "generatedOnEpoch": "string",
    "integrityImpact": "string",
    "score": "string",
    "source": "string"
  },
  "cvss3": {
    "attackComplexity": "string",
    "attackVector": "string",
    "availabilityImpact": "string",
    "baseScore": "string",
    "baseSeverity": "string",
    "confidentialityImpact": "string",
    "exploitabilityScore": "string",
    "impactScore": "string",
    "integrityImpact": "string",
    "privilegesRequired": "string",
    "scope": "string",
    "userInteraction": "string",
    "vectorString": "string"
  },
  "cwe": "string",
  "lastModifiedEpoch": "string",
  "publishedEpoch": "string",
  "references": [
    "string"
  ]
}
```

Properties

Name	Type	Required	Restrictions	Description
cpe	string	true	none	none
cve	string	true	none	none
cvss	Cvss¦null	false	none	none
cvss3	Cvss3¦null	false	none	none
cwe	string	true	none	none
lastModifiedEpoch	string	true	none	none
publishedEpoch	string	true	none	none
references	[string]	true	none	none

Cvss

```
{
  "accessComplexity": "string",
  "accessVector": "string",
  "authentication": "string",
  "availabilityImpact": "string",
  "confidentialityImpact": "string",
  "generatedOnEpoch": "string",
  "integrityImpact": "string",
  "score": "string",
  "source": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
accessComplexity	string	true	none	none
accessVector	string	true	none	none
authentication	string	true	none	none
availabilityImpact	string	true	none	none
confidentialityImpact	string	true	none	none
generatedOnEpoch	string	true	none	none
integrityImpact	string	true	none	none
score	string	true	none	none
source	string	true	none	none

Cvss3


```
{
  "attackComplexity": "string",
  "attackVector": "string",
  "availabilityImpact": "string",
  "baseScore": "string",
  "baseSeverity": "string",
  "confidentialityImpact": "string",
  "exploitabilityScore": "string",
  "impactScore": "string",
  "integrityImpact": "string",
  "privilegesRequired": "string",
  "scope": "string",
  "userInteraction": "string",
  "vectorString": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
attackComplexity	string	true	none	none
attackVector	string	true	none	none
availabilityImpact	string	true	none	none
baseScore	string	true	none	none
baseSeverity	string	true	none	none
confidentialityImpact	string	true	none	none
exploitabilityScore	string	true	none	none
impactScore	string	true	none	none
integrityImpact	string	true	none	none
privilegesRequired	string	true	none	none
scope	string	true	none	none
userInteraction	string	true	none	none
vectorString	string	true	none	none

FileTypeInfo

```
{
  "fileInfoExtended": {
    "extensions": "string",
    "groupId": "string",
    "typeId": "string"
  }
}
```

Properties

Name	Type	Required	Restrictions	Description
fileInfoExtended	FileInfoExtended¦null	false	none	none

FileInfoExtended

```
{
  "extensions": "string",
  "groupId": "string",
  "typeId": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
extensions	string¦null	false	none	none
groupId	string¦null	false	none	none
typeId	string¦null	false	none	none

CoreEngine

```
{
  "engineId": "string",
  "engineName": "string",
  "engineVersion": "string",
  "dbVersion": "string",
  "definitionTime": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
engineId	string¦null	false	none	none
engineName	string	false	none	none
engineVersion	string	false	none	none
dbVersion	string	false	none	none
definitionTime	string	false	none	none

ProcessingState2

```
0
```

- 0: InProgress
- 1: Failed
- 2: Canceled
- 3: Available
- 4: FailedRemediation

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: InProgress - 1: Failed - 2: Canceled - 3: Available - 4: FailedRemediation

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2
anonymous	3
anonymous	4

Exception

```
{
  "exceptionDetails": "string",
  "exceptionMessage": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
exceptionDetails	string¦null	false	none	none
exceptionMessage	string¦null	false	none	none

FileProcessingDetails


```
{
  "streamingStartedTime": "2019-08-24T14:15:22Z",
  "streamingCompletedTime": "2019-08-24T14:15:22Z",
  "streamingTimeSpanMs": 0,
  "scanCompletedTime": "2019-08-24T14:15:22Z",
  "processingTimeSpanMs": 0
}
```


Properties

Name	Type	Required	Restrictions	Description
streamingStartedTime	string(date-time)	false	none	none
streamingCompletedTime	string(date-time)	false	none	none
streamingTimeSpanMs	integer(int64)	false	none	none
scanCompletedTime	string(date-time)	false	none	none
processingTimeSpanMs	integer(int64)	false	none	none

FileRemediation

```
{
  "deepCdr": {
    "sanitizationDetails": {
      "failureCategory": "string",
      "description": "string",
      "details": "string"
    },
    "cdrObjectState": 0,
    "fileWasReplaced": true
  },
  "postActionFailedInformation": [
    {
      "objectActionType": 0,
      "exception": {
        "exceptionDetails": "string",
        "exceptionMessage": "string"
      }
    }
  ],
  "objectRemediationActions": [
    {
      "objectActionType": 0,
      "objectActionState": 0,
      "cdrObjectState": 0,
      "exceptions": [
        "string"
      ],
      "id": "string",
      "fileId": "string",
      "fileScanCompletedTime": "2019-08-24T14:15:22Z",
      "remediationId": "string",
      "tenantId": "string",
      "lastUpdated": "2019-08-24T14:15:22Z"
    }
  ]
}
```


Properties

Name	Type	Required	Restrictions	Description
deepCdr	DeepCdr¦null	false	none	none
postActionFailedInformation	[PostActionFailedInformation]¦null	false	none	none
objectRemediationActions	[ObjectRemediationAction]¦null	true	none	none

DeepCdr

```
{
  "sanitizationDetails": {
    "failureCategory": "string",
    "description": "string",
    "details": "string"
  },
  "cdrObjectState": 0,
  "fileWasReplaced": true
}
```

Properties

Name	Type	Required	Restrictions	Description
sanitizationDetails	SanitizationDetails|null	false	none	none
cdrObjectState	CdrObjectState|null	false	none	- 0: Original - 1: CdrOriginal - 2: CdrSanitized
fileWasReplaced	boolean	false	none	none

CdrObjectState

```
0
```

- 0: Original
- 1: CdrOriginal
- 2: CdrSanitized

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: Original - 1: CdrOriginal - 2: CdrSanitized

Enumerated Values

Property	Value
anonymous	0

anonymous	1
anonymous	2

PostActionFailedInformation

```
{
  "objectActionType": 0,
  "exception": {
    "exceptionDetails": "string",
    "exceptionMessage": "string"
  }
}
```

Properties

Name	Type	Required	Restrictions	Description
objectActionType	ObjectActionType2	false	none	- 0: Tagging - 5: AllowedMoved - 6: BlockedMoved - 7: BlockedDelete - 8: AllowedSanitizedMoved - 9: AllowedCopied - 10: BlockedCopied - 11: AllowedSanitizedCopied - 12: AllowedSanitizedDeleted - 13: AllowedDeleted - 14: AllowedKept - 15: BlockedKept - 16: AllowedSanitizedKept - 17: BlockedSanitizedCopied - 18: BlockedSanitizedMoved - 19: BlockedSanitizedDeleted - 20: BlockedSanitizedKept - 21: ScanFileVersions - 22: DiscoveredMoved - 23: DiscoveredCopied - 24: DiscoveredKept - 25: DiscoveredDelete - 26: AllowedCdrUnsupportedKept - 27: AllowedCdrUnsupportedMoved - 28: AllowedCdrUnsupportedCopied - 29: AllowedCdrUnsupportedDeleted - 30: BlockedCdrUnsupportedKept - 31: BlockedCdrUnsupportedMoved - 32: BlockedCdrUnsupportedCopied - 33: BlockedCdrUnsupportedDeleted - 100: SoftDelete - 101: PackageDelete - 102: Copy
exception	Exception¦null	false	none	none

ObjectActionType2

```
0
```

- 0: Tagging
- 5: AllowedMoved
- 6: BlockedMoved
- 7: BlockedDelete
- 8: AllowedSanitizedMoved
- 9: AllowedCopied
- 10: BlockedCopied
- 11: AllowedSanitizedCopied
- 12: AllowedSanitizedDeleted
- 13: AllowedDeleted
- 14: AllowedKept
- 15: BlockedKept
- 16: AllowedSanitizedKept
- 17: BlockedSanitizedCopied
- 18: BlockedSanitizedMoved
- 19: BlockedSanitizedDeleted
- 20: BlockedSanitizedKept
- 21: ScanFileVersions
- 22: DiscoveredMoved
- 23: DiscoveredCopied
- 24: DiscoveredKept
- 25: DiscoveredDelete
- 26: AllowedCdrUnsupportedKept
- 27: AllowedCdrUnsupportedMoved
- 28: AllowedCdrUnsupportedCopied
- 29: AllowedCdrUnsupportedDeleted
- 30: BlockedCdrUnsupportedKept
- 31: BlockedCdrUnsupportedMoved
- 32: BlockedCdrUnsupportedCopied
- 33: BlockedCdrUnsupportedDeleted
- 100: SoftDelete

- 101: PackageDelete
- 102: Copy

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: Tagging - 5: AllowedMoved - 6: BlockedMoved - 7: BlockedDelete - 8: AllowedSanitizedMoved - 9: AllowedCopied - 10: BlockedCopied - 11: AllowedSanitizedCopied - 12: AllowedSanitizedDeleted - 13: AllowedDeleted - 14: AllowedKept - 15: BlockedKept - 16: AllowedSanitizedKept - 17: BlockedSanitizedCopied - 18: BlockedSanitizedMoved - 19: BlockedSanitizedDeleted - 20: BlockedSanitizedKept - 21: ScanFileVersions - 22: DiscoveredMoved - 23: DiscoveredCopied - 24: DiscoveredKept - 25: DiscoveredDelete - 26: AllowedCdrUnsupportedKept - 27: AllowedCdrUnsupportedMoved - 28: AllowedCdrUnsupportedCopied - 29: AllowedCdrUnsupportedDeleted - 30: BlockedCdrUnsupportedKept - 31: BlockedCdrUnsupportedMoved - 32: BlockedCdrUnsupportedCopied - 33: BlockedCdrUnsupportedDeleted - 100: SoftDelete - 101: PackageDelete - 102: Copy

Enumerated Values

Property	Value
anonymous	0
anonymous	5
anonymous	6
anonymous	7
anonymous	8
anonymous	9
anonymous	10
anonymous	11
anonymous	12
anonymous	13
anonymous	14
anonymous	15
anonymous	16
anonymous	17
anonymous	18
anonymous	19
anonymous	20
anonymous	21
anonymous	22
anonymous	23
anonymous	24
anonymous	25
anonymous	26
anonymous	27
anonymous	28
anonymous	29
anonymous	30

anonymous	31
anonymous	32
anonymous	33
anonymous	100
anonymous	101
anonymous	102

ObjectRemediationAction


```
{
  "objectActionType": 0,
  "objectActionState": 0,
  "cdrObjectState": 0,
  "exceptions": [
    "string"
  ],
  "id": "string",
  "fileId": "string",
  "fileScanCompletedTime": "2019-08-24T14:15:22Z",
  "remediationId": "string",
  "tenantId": "string",
  "lastUpdated": "2019-08-24T14:15:22Z"
}
```

Properties

Name	Type	Required	Restrictions	Description
objectActionType	ObjectActionType2	true	none	- 0: Tagging - 5: AllowedMoved - 6: BlockedMoved - 7: BlockedDelete - 8: AllowedSanitizedMoved - 9: AllowedCopied - 10: BlockedCopied - 11: AllowedSanitizedCopied - 12: AllowedSanitizedDeleted - 13: AllowedDeleted - 14: AllowedKept - 15: BlockedKept - 16: AllowedSanitizedKept - 17: BlockedSanitizedCopied - 18: BlockedSanitizedMoved - 19: BlockedSanitizedDeleted - 20: BlockedSanitizedKept - 21: ScanFileVersions - 22: DiscoveredMoved - 23: DiscoveredCopied - 24: DiscoveredKept - 25: DiscoveredDelete - 26: AllowedCdrUnsupportedKept - 27: AllowedCdrUnsupportedMoved - 28: AllowedCdrUnsupportedCopied - 29: AllowedCdrUnsupportedDeleted - 30: BlockedCdrUnsupportedKept - 31: BlockedCdrUnsupportedMoved - 32: BlockedCdrUnsupportedCopied - 33: BlockedCdrUnsupportedDeleted - 100: SoftDelete - 101: PackageDelete - 102: Copy
objectActionState	ObjectActionState	true	none	- 0: NotApplied - 1: Applied - 3: CannotBeApplied

				- 4: Error - 5: SanitizationSkipped
cdrObjectState	CdrObjectState¦null	false	none	- 0: Original - 1: CdrOriginal - 2: CdrSanitized
exceptions	[string]	true	none	none
id	string	true	none	none
fileId	string	true	none	none
fileScanCompletedTime	string(date-time)	true	none	none
remediationId	string¦null	false	none	none
tenantId	string¦null	false	none	none
lastUpdated	string(date-time)¦null	false	none	none

ObjectActionState

```
0
```

- 0: NotApplied
- 1: Applied
- 3: CannotBeApplied
- 4: Error
- 5: SanitizationSkipped

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: NotApplied - 1: Applied - 3: CannotBeApplied - 4: Error - 5: SanitizationSkipped

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	3
anonymous	4
anonymous	5

File

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "id": "string",
  "scanId": "string",
  "name": "string",
  "path": "string",
  "hash": "string",
  "fileOwner": {
    "userId": "string",
    "fullName": "string",
    "userName": "string",
    "emailAddress": "string"
  },
  "size": 0,
  "fileTypeCategory": 0,
  "extension": "string",
  "storageType": {
    "name": "string",
    "categoryType": 0,
    "protocolType": 0,
    "vendorType": 0
  },
  "storageName": "string",
  "storageLocation": "string",
  "scanName": "string",
  "progress": {
    "upload": 0,
    "scan": 0,
    "archiveExtraction": 0
  },
  "scanResult": {
    "extractedFiles": {
      "dataId": "string",
      "scanResultI": 0,
      "detectedBy": 0,
      "filesExtractedCount": 0
    },
    "scanResults": {
      "scanDetails": [
        {
          "engineName": "string",
          "threatFound": "string",
          "scanResultI": 0,
          "defTime": "string",
          "scanTime": 0.1,
          "engId": "string",
```

```
}
      ],
      "dataId": "string",
      "scanAllResultI": 0,
      "scanAllResultA": "string",
      "startTime": "string",
      "totalTime": 0.1,
      "totalAvs": 0,
      "totalDetections": 0,
      "progressPercentage": 0
    },
    "fileInfo": {
      "fileSize": 0,
      "uploadTimestamp": "string",
      "md5": "string",
      "sha1": "string",
      "sha256": "string",
      "fileTypeCategory": "string",
      "fileTypeDescription": "string",
      "fileTypeExtension": "string",
      "displayName": "string",
      "fileTypeId": "string"
    },
    "fileScanInfo": {
      "finalVerdict": {
        "blocked": true,
        "verdict": "string",
        "confidence": 0.1,
        "threatLevel": 0.1
      },
      "overviewReport": {
        "analysisState": "string",
        "signalGroups": [
          {
            "description": "string",
            "verdict": "string",
            "signals": [
              {
                "originType": "string",
                "signalReadable": "string",
                "strength": 0.1
              }
            ],
            "mitreTechniques": [
              {
                "name": "string",
                "tacticName": "string"
              }
            ]
          }
        ],
        "iocs": [
          {
```

```
"type": "string",
            "origin": "string",
            "verdict": "string"
          }
        ],
        "yaraMatches": [
          {
            "ruleName": "string",
            "ruleDescription": "string",
            "verdict": "string",
            "matchedStrings": [
              "string"
            ],
            "author": "string",
            "version": "string",
            "threatLevel": 0.1,
            "confidence": 0.1,
            "strength": 0.1
          }
        ],
        "tags": [
          {
            "name": "string",
            "verdict": "string"
          }
        ],
        "metaData": {
          "entropy": 0.1,
          "forensicAnalysisRecommended": true,
          "fuzzyFsioHash": "string"
        }
      },
      "errorCategory": "string",
      "errorCode": 0,
      "errorDetails": "string"
    },
    "processInfo": {
      "postProcessing": {
        "actionsRan": "string",
        "actionsFailed": "string",
        "convertedTo": "string",
        "copyMoveDestination": "string",
        "convertedDestination": "string",
        "sanitizationDetails": {
          "failureCategory": "string",
          "description": "string",
          "details": "string"
        }
      },
      "progressPercentage": 0,
      "userAgent": "string",
      "profile": "string",
      "result": "string",
```

```
"fileTypeSkippedScan": true,
      "processingTime": 0.1,
      "queueTime": 0.1,
      "resultI": 0
    },
    "dataId": "string",
    "dlpInfo": {
      "hits": null,
      "verdict": 0
    },
    "sbomInfo": {
      "finalVerdict": {
        "blocked": true,
        "licensingPackageCounts": {
          "allowed": 0,
          "blocked": 0,
          "unknown": 0,
          "unsupported": 0
        },
        "severity": 0,
        "totalPackageCount": 0,
        "verdict": "string",
        "vulnerabilityCounts": {
          "critical": 0,
          "high": 0,
          "medium": 0,
          "low": 0,
          "unknown": 0
        }
      },
      "overviewReport": {
        "isPartialReport": true,
        "osInfo": {
          "osName": "string",
          "osVersion": "string"
        },
        "scanMode": "string",
        "steps": [
          {
            "command": "string",
            "packages": [
              {
                "authors": "string",
                "releaseDate": "2019-08-24T14:15:22Z",
                "ecosystem": "string",
                "group": "string",
                "archive": true,
                "executable": true,
                "uid": "string",
                "licenses": {
                  "allowed": [
                    {
                      "id": "string",
```

```
"category": "string",
                      "usageRestriction": {
                        "permissions": [
                          "string"
                        ],
                        "conditions": [
                          "string"
                        ],
                        "limitations": [
                          "string"
                        ]
                      }
                    }
                  ],
                  "blocked": [
                    {
                      "id": "string",
                      "url": "string",
                      "category": "string",
                      "usageRestriction": {
                        "permissions": [
                          "string"
                        ],
                        "conditions": [
                          "string"
                        ],
                        "limitations": [
                          "string"
                        ]
                      }
                    }
                  ]
                },
                "packageName": "string",
                "packageVersion": "string",
                "hashes": [
                  {
                    "sha256": "string",
                    "fileName": "string"
                  }
                ],
                "vulnerabilityCounts": {
                  "critical": 0,
                  "high": 0,
                  "medium": 0,
                  "low": 0,
                  "unknown": 0
                },
                "vulnerabilities": [
                  {
                    "id": "string",
                    "severity": 0,
                    "source": "string",
```

```
"cwes": [
                        "string"
                      ]
                    }
                  ],
                  "arch": "string",
                  "osName": "string",
                  "osVersion": "string",
                  "dependencies": [
                    {
                      "ecosystem": "string",
                      "group": "string",
                      "packageName": "string",
                      "packageVersion": "string",
                      "vulnerabilities": [
                        {
                          "id": "string",
                          "severity": 0,
                          "source": "string",
                          "fixedVersions": "string",
                          "cwes": [
                            "string"
                          ]
                        }
                      ],
                      "vulnerabilityCounts": {
                        "critical": 0,
                        "high": 0,
                        "medium": 0,
                        "low": 0,
                        "unknown": 0
                      }
                    }
                  ]
                }
              ],
              "licenseStatus": "string",
              "licensingPackageCounts": {
                "allowed": 0,
                "blocked": 0,
                "unknown": 0,
                "unsupported": 0
              },
              "step": 0,
              "vulnerabilityCount": 0,
              "sha256": "string",
              "severity": 0,
              "vulnerabilityCounts": {
                "critical": 0,
                "high": 0,
                "medium": 0,
                "low": 0,
                "unknown": 0
```

```
}
        ],
        "packages": [
          {
            "authors": "string",
            "releaseDate": "2019-08-24T14:15:22Z",
            "ecosystem": "string",
            "group": "string",
            "archive": true,
            "executable": true,
            "uid": "string",
            "licenses": {
              "allowed": [
                {
                  "id": "string",
                  "url": "string",
                  "category": "string",
                  "usageRestriction": {
                    "permissions": [
                      "string"
                    ],
                    "conditions": [
                      "string"
                    ],
                    "limitations": [
                      "string"
                    ]
                  }
                }
              ],
              "blocked": [
                {
                  "id": "string",
                  "url": "string",
                  "category": "string",
                  "usageRestriction": {
                    "permissions": [
                      "string"
                    ],
                    "conditions": [
                      "string"
                    ],
                    "limitations": [
                      "string"
                    ]
                  }
                }
              ]
            },
            "packageName": "string",
            "packageVersion": "string",
            "target": "string",
            "hashes": [
```

```
"sha256": "string",
                "fileName": "string"
              }
            ],
            "vulnerabilities": [
              {
                "id": "string",
                "severity": 0,
                "source": "string",
                "fixedVersions": "string",
                "cwes": [
                  "string"
                ]
              }
            ],
            "vulnerabilityCounts": {
              "critical": 0,
              "high": 0,
              "medium": 0,
              "low": 0,
              "unknown": 0
            },
            "dependencies": [
              {
                "ecosystem": "string",
                "group": "string",
                "packageName": "string",
                "packageVersion": "string",
                "vulnerabilities": [
                  {
                    "id": "string",
                    "severity": 0,
                    "source": "string",
                    "fixedVersions": "string",
                    "cwes": [
                      "string"
                    ]
                  }
                ],
                "vulnerabilityCounts": {
                  "critical": 0,
                  "high": 0,
                  "medium": 0,
                  "low": 0,
                  "unknown": 0
                }
              }
            ]
          }
        ],
        "dependenciesPackageCount": 0,
        "dependenciesVulnerabilityTotal": 0,
        "dependenciesVulnerabilityCounts": {
```

```
"high": 0,
          "medium": 0,
          "low": 0,
          "unknown": 0
        }
      },
      "resultTemplateHash": "string"
    },
    "vulnerabilityInfo": {
      "vulnerabilityInfoResult": {
        "code": 0,
        "hash": "string",
        "method": 0,
        "timeStamp": "string",
        "timing": 0,
        "detectedProduct": {
          "hasVulnerability": true,
          "isCurrent": true,
          "product": {
            "id": 0,
            "name": "string"
          },
          "remediationLink": "string",
          "severity": "string",
          "sigName": "string",
          "signature": 0,
          "vendor": {
            "id": 0,
            "name": "string"
          },
          "version": "string",
          "versionData": {
            "countBehind": 0,
            "feedId": 0,
            "version": "string"
          },
          "vulnerabilities": [
            {
              "description": "string",
              "details": {
                "cpe": "string",
                "cve": "string",
                "cvss": {
                  "accessComplexity": "string",
                  "accessVector": "string",
                  "authentication": "string",
                  "availabilityImpact": "string",
                  "confidentialityImpact": "string",
                  "generatedOnEpoch": "string",
                  "integrityImpact": "string",
                  "score": "string",
                  "source": "string"
                },
```

```
"attackComplexity": "string",
                  "attackVector": "string",
                  "availabilityImpact": "string",
                  "baseScore": "string",
                  "baseSeverity": "string",
                  "confidentialityImpact": "string",
                  "exploitabilityScore": "string",
                  "impactScore": "string",
                  "integrityImpact": "string",
                  "privilegesRequired": "string",
                  "scope": "string",
                  "userInteraction": "string",
                  "vectorString": "string"
                },
                "cwe": "string",
                "lastModifiedEpoch": "string",
                "publishedEpoch": "string",
                "references": [
                  "string"
                ]
              },
              "severity": "string",
              "severityIndex": 0,
              "staticId": 0
            }
          ]
        }
      }
    },
    "sessionCookie": "string",
    "fileTypeInfo": {
      "fileInfoExtended": {
        "extensions": "string",
        "groupId": "string",
        "typeId": "string"
      }
    },
    "scanInstanceUrl": "string",
    "scanWorkflowSnapshotId": "string",
    "coreEngines": [
      {
        "engineId": "string",
        "engineName": "string",
        "engineVersion": "string",
        "dbVersion": "string",
        "definitionTime": "string"
      }
    ]
  },
  "processingState": 0,
  "exception": {
    "exceptionDetails": "string",
    "exceptionMessage": "string"
```

```
"created": "2019-08-24T14:15:22Z",
  "lastModified": "2019-08-24T14:15:22Z",
  "discoveryStarted": "2019-08-24T14:15:22Z",
  "fileProcessingDetails": {
    "streamingStartedTime": "2019-08-24T14:15:22Z",
    "streamingCompletedTime": "2019-08-24T14:15:22Z",
    "streamingTimeSpanMs": 0,
    "scanCompletedTime": "2019-08-24T14:15:22Z",
    "processingTimeSpanMs": 0
  },
  "coreEngines": [
    {
      "engineId": "string",
      "engineName": "string",
      "engineVersion": "string",
      "dbVersion": "string",
      "definitionTime": "string"
    }
  ],
  "remediation": {
    "deepCdr": {
      "sanitizationDetails": {
        "failureCategory": "string",
        "description": "string",
        "details": "string"
      },
      "cdrObjectState": 0,
      "fileWasReplaced": true
    },
    "postActionFailedInformation": [
      {
        "objectActionType": 0,
        "exception": {
          "exceptionDetails": "string",
          "exceptionMessage": "string"
        }
      }
    ],
    "objectRemediationActions": [
      {
        "objectActionType": 0,
        "objectActionState": 0,
        "cdrObjectState": 0,
        "exceptions": [
          "string"
        ],
        "id": "string",
        "fileId": "string",
        "fileScanCompletedTime": "2019-08-24T14:15:22Z",
        "remediationId": "string",
        "tenantId": "string",
        "lastUpdated": "2019-08-24T14:15:22Z"
      }
```

```
},
  "metaDefenderCoreUrl": "string",
  "discoveryStartedDaySec": 0,
  "objectStorageMetadata": "string",
  "scanWorkflowSnapshotId": "string",
  "scanWorkflowSnapshot": {
    "id": "string",
    "scanId": "string",
    "workflow": {
      "id": "string",
      "scanPoolId": "string",
      "scanProcessFlow": 0,
      "isIdentityScanningEnabled": true,
      "scanIntervalDays": 0,
      "rules": [
        "string"
      ],
      "type": 0,
      "workflowSupportedTechnologies": {
        "dlp": {
          "status": 0
        },
        "deepCdr": {
          "status": 0
        },
        "sandBox": {
          "status": 0
        },
        "metascan": {
          "status": 0
        }
      },
      "name": "string",
      "userAgent": "string",
      "scanPool": {
        "id": "string",
        "name": "string",
        "scanPoolType": 0,
        "isDefault": true,
        "scanInstances": [
          {
            "id": "string",
            "scanPoolId": "string",
            "url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ]
      },
      "failOverScanPoolId": "string",
      "failOverScanPool": {
        "id": "string",
```

```
"scanPoolType": 0,
        "isDefault": true,
        "scanInstances": [
          {
            "id": "string",
            "scanPoolId": "string",
            "url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ]
      },
      "filters": {
        "id": "string",
        "minimumSize": 0,
        "maximumSize": 0,
        "minimumDateTime": "2019-08-24T14:15:22Z",
        "maximumDateTime": "2019-08-24T14:15:22Z"
      },
      "fileDefinition": {
        "blockingStrategy": 0,
        "configurableBlockingStrategy": {
          "shouldTreatFilesWithSensitiveDataAsBlocked": true,
          "shouldTreatFilesWithVulnerabilitiesAsBlocked": true
        }
      },
      "remediations": [
        {
          "id": "string",
          "workflowId": "string",
          "isEnabled": true,
          "configuration": "string",
          "type": 0,
          "handlingType": 0
        }
      ],
      "tenantId": "string"
    },
    "startTimestamp": 0,
    "stopTimestamp": 0,
    "scanPool": {
      "id": "string",
      "name": "string",
      "scanPoolType": 0,
      "isDefault": true,
      "scanInstances": [
        {
          "id": "string",
          "scanPoolId": "string",
          "url": "string",
          "apiKey": "string",
          "timeout": "string",
```

```
}
      ]
    },
    "scanInstances": [
      {
        "id": "string",
        "scanPoolId": "string",
        "url": "string",
        "apiKey": "string",
        "timeout": "string",
        "scanInstanceType": 0
      }
    ],
    "failOverScanPool": {
      "id": "string",
      "name": "string",
      "scanPoolType": 0,
      "isDefault": true,
      "scanInstances": [
        {
          "id": "string",
          "scanPoolId": "string",
          "url": "string",
          "apiKey": "string",
          "timeout": "string",
          "scanInstanceType": 0
        }
      ]
    },
    "failOverScanInstances": [
      {
        "id": "string",
        "scanPoolId": "string",
        "url": "string",
        "apiKey": "string",
        "timeout": "string",
        "scanInstanceType": 0
      }
    ],
    "storage": {
      "id": "string",
      "name": "string",
      "groupId": "string",
      "clientId": "string",
      "accountId": "string",
      "source": "string",
      "storageFunctionality": "string",
      "storageType": {
        "name": "string",
        "categoryType": 0,
        "protocolType": 0,
        "vendorType": 0
      },
```

```
"message": "string",
        "statusType": 0
      },
      "workflowId": "string",
      "lastUpdated": "2019-08-24T14:15:22Z",
      "tenantId": "string",
      "groupRef": {
        "id": "string",
        "name": "string"
      },
      "isAutodiscovered": true
    },
    "workflowStatistics": {
      "taggingStatistics": {
        "total": 0
      },
      "keepAllowedStatistics": {
        "total": 0
      },
      "keepBlockedStatistics": {
        "total": 0
      },
      "keepSanitizedStatistics": {
        "total": 0
      },
      "movedAllowedStatistics": {
        "total": 0,
        "destinationStorageInformation": {
          "id": "string",
          "name": "string",
          "groupId": "string",
          "clientId": "string",
          "accountId": "string",
          "source": "string",
          "storageFunctionality": "string",
          "storageType": {
            "name": "string",
            "categoryType": 0,
            "protocolType": 0,
            "vendorType": 0
          },
          "storageStatus": {
            "message": "string",
            "statusType": 0
          },
          "workflowId": "string",
          "lastUpdated": "2019-08-24T14:15:22Z",
          "tenantId": "string",
          "groupRef": {
            "id": "string",
            "name": "string"
          },
          "isAutodiscovered": true
```

```
},
      "movedSanitizedStatistics": {
        "total": 0,
        "destinationStorageInformation": {
          "id": "string",
          "name": "string",
          "groupId": "string",
          "clientId": "string",
          "accountId": "string",
          "source": "string",
          "storageFunctionality": "string",
          "storageType": {
            "name": "string",
            "categoryType": 0,
            "protocolType": 0,
            "vendorType": 0
          },
          "storageStatus": {
            "message": "string",
            "statusType": 0
          },
          "workflowId": "string",
          "lastUpdated": "2019-08-24T14:15:22Z",
          "tenantId": "string",
          "groupRef": {
            "id": "string",
            "name": "string"
          },
          "isAutodiscovered": true
        }
      },
      "movedBlockedStatistics": {
        "total": 0,
        "destinationStorageInformation": {
          "id": "string",
          "name": "string",
          "groupId": "string",
          "clientId": "string",
          "accountId": "string",
          "source": "string",
          "storageFunctionality": "string",
          "storageType": {
            "name": "string",
            "categoryType": 0,
            "protocolType": 0,
            "vendorType": 0
          },
          "storageStatus": {
            "message": "string",
            "statusType": 0
          },
          "workflowId": "string",
          "lastUpdated": "2019-08-24T14:15:22Z",
```

```
"groupRef": {
            "id": "string",
            "name": "string"
          },
          "isAutodiscovered": true
        }
      },
      "copyAllowedStatistics": {
        "total": 0,
        "destinationStorageInformation": {
          "id": "string",
          "name": "string",
          "groupId": "string",
          "clientId": "string",
          "accountId": "string",
          "source": "string",
          "storageFunctionality": "string",
          "storageType": {
            "name": "string",
            "categoryType": 0,
            "protocolType": 0,
            "vendorType": 0
          },
          "storageStatus": {
            "message": "string",
            "statusType": 0
          },
          "workflowId": "string",
          "lastUpdated": "2019-08-24T14:15:22Z",
          "tenantId": "string",
          "groupRef": {
            "id": "string",
            "name": "string"
          },
          "isAutodiscovered": true
        }
      },
      "copyBlockedStatistics": {
        "total": 0,
        "destinationStorageInformation": {
          "id": "string",
          "name": "string",
          "groupId": "string",
          "clientId": "string",
          "accountId": "string",
          "source": "string",
          "storageFunctionality": "string",
          "storageType": {
            "name": "string",
            "categoryType": 0,
            "protocolType": 0,
            "vendorType": 0
          },
```

```
"message": "string",
            "statusType": 0
          },
          "workflowId": "string",
          "lastUpdated": "2019-08-24T14:15:22Z",
          "tenantId": "string",
          "groupRef": {
            "id": "string",
            "name": "string"
          },
          "isAutodiscovered": true
        }
      },
      "deleteAllowedStatistics": {
        "total": 0
      },
      "deleteBlockedStatistics": {
        "total": 0
      },
      "lastCalculatedStatisticsTime": "2019-08-24T14:15:22Z"
    },
    "account": {
      "id": "string",
      "name": "string",
      "description": "string",
      "credentials": "string",
      "protocolType": 0,
      "vendorType": 0,
      "autoDiscovery": true,
      "autodiscoveryDestinationGroupId": "string",
      "destinationGroup": {
        "id": "string",
        "name": "string"
      }
    },
    "realTimeStartDate": "2019-08-24T14:15:22Z"
  },
  "versions": [
    {
      "result": 0,
      "responseKey": "string",
      "responseMessage": "string",
      "responseMessageParams": {
        "property1": "string",
        "property2": "string"
      },
      "id": "string",
      "scanId": "string",
      "name": "string",
      "path": "string",
      "hash": "string",
      "fileOwner": {
        "userId": "string",
```

```
"userName": "string",
        "emailAddress": "string"
      },
      "size": 0,
      "fileTypeCategory": 0,
      "extension": "string",
      "storageType": {
        "name": "string",
        "categoryType": 0,
        "protocolType": 0,
        "vendorType": 0
      },
      "storageName": "string",
      "storageLocation": "string",
      "scanName": "string",
      "progress": {
        "upload": 0,
        "scan": 0,
        "archiveExtraction": 0
      },
      "scanResult": {
        "extractedFiles": {
          "dataId": "string",
          "scanResultI": 0,
          "detectedBy": 0,
          "filesExtractedCount": 0
        },
        "scanResults": {
          "scanDetails": [
            {
              "engineName": "string",
              "threatFound": "string",
              "scanResultI": 0,
              "defTime": "string",
              "scanTime": 0.1,
              "engId": "string",
              "waitTime": 0.1
            }
          ],
          "dataId": "string",
          "scanAllResultI": 0,
          "scanAllResultA": "string",
          "startTime": "string",
          "totalTime": 0.1,
          "totalAvs": 0,
          "totalDetections": 0,
          "progressPercentage": 0
        },
        "fileInfo": {
          "fileSize": 0,
          "uploadTimestamp": "string",
          "md5": "string",
          "sha1": "string",
```

```
"fileTypeCategory": "string",
          "fileTypeDescription": "string",
          "fileTypeExtension": "string",
          "displayName": "string",
          "fileTypeId": "string"
        },
        "fileScanInfo": {
          "finalVerdict": {
            "blocked": true,
            "verdict": "string",
            "confidence": 0.1,
            "threatLevel": 0.1
          },
          "overviewReport": {
            "analysisState": "string",
            "signalGroups": [
              {
                "description": "string",
                "verdict": "string",
                "signals": [
                  {
                    "originType": "string",
                    "signalReadable": "string",
                    "strength": 0.1
                  }
                ],
                "mitreTechniques": [
                  {
                    "name": "string",
                    "tacticName": "string"
                  }
                ]
              }
            ],
            "iocs": [
              {
                "data": "string",
                "type": "string",
                "origin": "string",
                "verdict": "string"
              }
            ],
            "yaraMatches": [
              {
                "ruleName": "string",
                "ruleDescription": "string",
                "verdict": "string",
                "matchedStrings": [
                  "string"
                ],
                "author": "string",
                "version": "string",
                "threatLevel": 0.1,
```

```
"strength": 0.1
              }
            ],
            "tags": [
              {
                "name": "string",
                "verdict": "string"
              }
            ],
            "metaData": {
              "entropy": 0.1,
              "forensicAnalysisRecommended": true,
              "fuzzyFsioHash": "string"
            }
          },
          "errorCategory": "string",
          "errorCode": 0,
          "errorDetails": "string"
        },
        "processInfo": {
          "postProcessing": {
            "actionsRan": "string",
            "actionsFailed": "string",
            "convertedTo": "string",
            "copyMoveDestination": "string",
            "convertedDestination": "string",
            "sanitizationDetails": {
              "failureCategory": "string",
              "description": "string",
              "details": "string"
            }
          },
          "progressPercentage": 0,
          "userAgent": "string",
          "profile": "string",
          "result": "string",
          "blockedReason": "string",
          "fileTypeSkippedScan": true,
          "processingTime": 0.1,
          "queueTime": 0.1,
          "resultI": 0
        },
        "dataId": "string",
        "dlpInfo": {
          "hits": null,
          "verdict": 0
        },
        "sbomInfo": {
          "finalVerdict": {
            "blocked": true,
            "licensingPackageCounts": {
              "allowed": 0,
              "blocked": 0,
```

```
"unsupported": 0
            },
            "severity": 0,
            "totalPackageCount": 0,
            "verdict": "string",
            "vulnerabilityCounts": {
              "critical": 0,
              "high": 0,
              "medium": 0,
              "low": 0,
              "unknown": 0
            }
          },
          "overviewReport": {
            "isPartialReport": true,
            "osInfo": {
              "osName": "string",
              "osVersion": "string"
            },
            "scanMode": "string",
            "steps": [
              {
                "command": "string",
                "packages": [
                  {
                    "authors": "string",
                    "releaseDate": "2019-08-24T14:15:22Z",
                    "ecosystem": "string",
                    "group": "string",
                    "archive": true,
                    "executable": true,
                    "uid": "string",
                    "licenses": {
                      "allowed": [
                        {
                          "id": "string",
                          "url": "string",
                          "category": "string",
                          "usageRestriction": {
                            "permissions": [
                              null
                            ],
                            "conditions": [
                              null
                            ],
                            "limitations": [
                              null
                            ]
                          }
                        }
                      ],
                      "blocked": [
                        {
```

```
"url": "string",
                          "category": "string",
                          "usageRestriction": {
                            "permissions": [
                              null
                            ],
                            "conditions": [
                              null
                            ],
                            "limitations": [
                              null
                            ]
                          }
                        }
                      ]
                    },
                    "packageName": "string",
                    "packageVersion": "string",
                    "hashes": [
                      {
                        "sha256": "string",
                        "fileName": "string"
                      }
                    ],
                    "vulnerabilityCounts": {
                      "critical": 0,
                      "high": 0,
                      "medium": 0,
                      "low": 0,
                      "unknown": 0
                    },
                    "vulnerabilities": [
                      {
                        "id": "string",
                        "severity": 0,
                        "source": "string",
                        "fixedVersions": "string",
                        "cwes": [
                          "string"
                        ]
                      }
                    ],
                    "arch": "string",
                    "osName": "string",
                    "osVersion": "string",
                    "dependencies": [
                      {
                        "ecosystem": "string",
                        "group": "string",
                        "packageName": "string",
                        "packageVersion": "string",
                        "vulnerabilities": [
                          {
```

```
"severity": 0,
                              "source": "string",
                              "fixedVersions": "string",
                              "cwes": [
                                null
                              ]
                            }
                          ],
                          "vulnerabilityCounts": {
                            "critical": 0,
                            "high": 0,
                            "medium": 0,
                            "low": 0,
                            "unknown": 0
                          }
                        }
                      ]
                    }
                  ],
                  "licenseStatus": "string",
                  "licensingPackageCounts": {
                    "allowed": 0,
                    "blocked": 0,
                    "unknown": 0,
                    "unsupported": 0
                  },
                  "step": 0,
                  "vulnerabilityCount": 0,
                  "sha256": "string",
                  "severity": 0,
                  "vulnerabilityCounts": {
                    "critical": 0,
                    "high": 0,
                    "medium": 0,
                    "low": 0,
                    "unknown": 0
                  }
                }
              ],
              "packages": [
                {
                  "authors": "string",
                  "releaseDate": "2019-08-24T14:15:22Z",
                  "ecosystem": "string",
                  "group": "string",
                  "archive": true,
                  "executable": true,
                  "uid": "string",
                  "licenses": {
                    "allowed": [
                      {
                        "id": "string",
                        "url": "string",
```

```
"usageRestriction": {
                        "permissions": [
                          "string"
                        ],
                        "conditions": [
                          "string"
                        ],
                        "limitations": [
                          "string"
                        ]
                      }
                    }
                  ],
                  "blocked": [
                    {
                      "id": "string",
                      "url": "string",
                      "category": "string",
                      "usageRestriction": {
                        "permissions": [
                          "string"
                        ],
                        "conditions": [
                          "string"
                        ],
                        "limitations": [
                          "string"
                        ]
                      }
                    }
                  ]
                },
                "packageName": "string",
                "packageVersion": "string",
                "target": "string",
                "hashes": [
                  {
                    "sha256": "string",
                    "fileName": "string"
                  }
                ],
                "vulnerabilities": [
                  {
                    "id": "string",
                    "severity": 0,
                    "source": "string",
                    "fixedVersions": "string",
                    "cwes": [
                      "string"
                    ]
                  }
                ],
                "vulnerabilityCounts": {
```

```
"high": 0,
                  "medium": 0,
                  "low": 0,
                  "unknown": 0
                },
                "dependencies": [
                  {
                    "ecosystem": "string",
                    "group": "string",
                    "packageName": "string",
                    "packageVersion": "string",
                    "vulnerabilities": [
                      {
                        "id": "string",
                        "severity": 0,
                        "source": "string",
                        "fixedVersions": "string",
                        "cwes": [
                          "string"
                        ]
                      }
                    ],
                    "vulnerabilityCounts": {
                      "critical": 0,
                      "high": 0,
                      "medium": 0,
                      "low": 0,
                      "unknown": 0
                    }
                  }
                ]
              }
            ],
            "dependenciesPackageCount": 0,
            "dependenciesVulnerabilityTotal": 0,
            "dependenciesVulnerabilityCounts": {
              "critical": 0,
              "high": 0,
              "medium": 0,
              "low": 0,
              "unknown": 0
            }
          },
          "resultTemplateHash": "string"
        },
        "vulnerabilityInfo": {
          "vulnerabilityInfoResult": {
            "code": 0,
            "hash": "string",
            "method": 0,
            "timeStamp": "string",
            "timing": 0,
            "detectedProduct": {
```

```
"isCurrent": true,
              "product": {
                "id": 0,
                "name": "string"
              },
              "remediationLink": "string",
              "severity": "string",
              "sigName": "string",
              "signature": 0,
              "vendor": {
                "id": 0,
                "name": "string"
              },
              "version": "string",
              "versionData": {
                "countBehind": 0,
                "feedId": 0,
                "version": "string"
              },
              "vulnerabilities": [
                {
                  "description": "string",
                  "details": {
                    "cpe": "string",
                    "cve": "string",
                    "cvss": {
                      "accessComplexity": "string",
                      "accessVector": "string",
                      "authentication": "string",
                      "availabilityImpact": "string",
                      "confidentialityImpact": "string",
                      "generatedOnEpoch": "string",
                      "integrityImpact": "string",
                      "score": "string",
                      "source": "string"
                    },
                    "cvss3": {
                      "attackComplexity": "string",
                      "attackVector": "string",
                      "availabilityImpact": "string",
                      "baseScore": "string",
                      "baseSeverity": "string",
                      "confidentialityImpact": "string",
                      "exploitabilityScore": "string",
                      "impactScore": "string",
                      "integrityImpact": "string",
                      "privilegesRequired": "string",
                      "scope": "string",
                      "userInteraction": "string",
                      "vectorString": "string"
                    },
                    "cwe": "string",
                    "lastModifiedEpoch": "string",
```

```
"references": [
                      "string"
                    ]
                  },
                  "severity": "string",
                  "severityIndex": 0,
                  "staticId": 0
                }
              ]
            }
          }
        },
        "sessionCookie": "string",
        "fileTypeInfo": {
          "fileInfoExtended": {
            "extensions": "string",
            "groupId": "string",
            "typeId": "string"
          }
        },
        "scanInstanceUrl": "string",
        "scanWorkflowSnapshotId": "string",
        "coreEngines": [
          {
            "engineId": "string",
            "engineName": "string",
            "engineVersion": "string",
            "dbVersion": "string",
            "definitionTime": "string"
          }
        ]
      },
      "processingState": 0,
      "exception": {
        "exceptionDetails": "string",
        "exceptionMessage": "string"
      },
      "created": "2019-08-24T14:15:22Z",
      "lastModified": "2019-08-24T14:15:22Z",
      "discoveryStarted": "2019-08-24T14:15:22Z",
      "fileProcessingDetails": {
        "streamingStartedTime": "2019-08-24T14:15:22Z",
        "streamingCompletedTime": "2019-08-24T14:15:22Z",
        "streamingTimeSpanMs": 0,
        "scanCompletedTime": "2019-08-24T14:15:22Z",
        "processingTimeSpanMs": 0
      },
      "coreEngines": [
        {
          "engineId": "string",
          "engineName": "string",
          "engineVersion": "string",
          "dbVersion": "string",
```

```
}
      ],
      "remediation": {
        "deepCdr": {
          "sanitizationDetails": {
            "failureCategory": "string",
            "description": "string",
            "details": "string"
          },
          "cdrObjectState": 0,
          "fileWasReplaced": true
        },
        "postActionFailedInformation": [
          {
            "objectActionType": 0,
            "exception": {
              "exceptionDetails": "string",
              "exceptionMessage": "string"
            }
          }
        ],
        "objectRemediationActions": [
          {
            "objectActionType": 0,
            "objectActionState": 0,
            "cdrObjectState": 0,
            "exceptions": [
              "string"
            ],
            "id": "string",
            "fileId": "string",
            "fileScanCompletedTime": "2019-08-24T14:15:22Z",
            "remediationId": "string",
            "tenantId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z"
          }
        ]
      },
      "metaDefenderCoreUrl": "string",
      "discoveryStartedDaySec": 0,
      "objectStorageMetadata": "string",
      "scanWorkflowSnapshotId": "string",
      "scanWorkflowSnapshot": {
        "id": "string",
        "scanId": "string",
        "workflow": {
          "id": "string",
          "scanPoolId": "string",
          "scanProcessFlow": 0,
          "isIdentityScanningEnabled": true,
          "scanIntervalDays": 0,
          "rules": [
            "string"
```

```
"type": 0,
          "workflowSupportedTechnologies": {
            "dlp": {
              "status": 0
            },
            "deepCdr": {
              "status": 0
            },
            "sandBox": {
              "status": 0
            },
            "metascan": {
              "status": 0
            }
          },
          "name": "string",
          "userAgent": "string",
          "scanPool": {
            "id": "string",
            "name": "string",
            "scanPoolType": 0,
            "isDefault": true,
            "scanInstances": [
              {
                "id": "string",
                "scanPoolId": "string",
                "url": "string",
                "apiKey": "string",
                "timeout": "string",
                "scanInstanceType": 0
              }
            ]
          },
          "failOverScanPoolId": "string",
          "failOverScanPool": {
            "id": "string",
            "name": "string",
            "scanPoolType": 0,
            "isDefault": true,
            "scanInstances": [
              {
                "id": "string",
                "scanPoolId": "string",
                "url": "string",
                "apiKey": "string",
                "timeout": "string",
                "scanInstanceType": 0
              }
            ]
          },
          "filters": {
            "id": "string",
            "minimumSize": 0,
```

```
"minimumDateTime": "2019-08-24T14:15:22Z",
            "maximumDateTime": "2019-08-24T14:15:22Z"
          },
          "fileDefinition": {
            "blockingStrategy": 0,
            "configurableBlockingStrategy": {
              "shouldTreatFilesWithSensitiveDataAsBlocked": true,
              "shouldTreatFilesWithVulnerabilitiesAsBlocked": true
            }
          },
          "remediations": [
            {
              "id": "string",
              "workflowId": "string",
              "isEnabled": true,
              "configuration": "string",
              "type": 0,
              "handlingType": 0
            }
          ],
          "tenantId": "string"
        },
        "startTimestamp": 0,
        "stopTimestamp": 0,
        "scanPool": {
          "id": "string",
          "name": "string",
          "scanPoolType": 0,
          "isDefault": true,
          "scanInstances": [
            {
              "id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ]
        },
        "scanInstances": [
          {
            "id": "string",
            "scanPoolId": "string",
            "url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ],
        "failOverScanPool": {
          "id": "string",
          "name": "string",
```

```
"isDefault": true,
          "scanInstances": [
            {
              "id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ]
        },
        "failOverScanInstances": [
          {
            "id": "string",
            "scanPoolId": "string",
            "url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ],
        "storage": {
          "id": "string",
          "name": "string",
          "groupId": "string",
          "clientId": "string",
          "accountId": "string",
          "source": "string",
          "storageFunctionality": "string",
          "storageType": {
            "name": "string",
            "categoryType": 0,
            "protocolType": 0,
            "vendorType": 0
          },
          "storageStatus": {
            "message": "string",
            "statusType": 0
          },
          "workflowId": "string",
          "lastUpdated": "2019-08-24T14:15:22Z",
          "tenantId": "string",
          "groupRef": {
            "id": "string",
            "name": "string"
          },
          "isAutodiscovered": true
        },
        "workflowStatistics": {
          "taggingStatistics": {
            "total": 0
          },
```

```
"total": 0
          },
          "keepBlockedStatistics": {
            "total": 0
          },
          "keepSanitizedStatistics": {
            "total": 0
          },
          "movedAllowedStatistics": {
            "total": 0,
            "destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
              "accountId": "string",
              "source": "string",
              "storageFunctionality": "string",
              "storageType": {
                "name": "string",
                "categoryType": 0,
                "protocolType": 0,
                "vendorType": 0
              },
              "storageStatus": {
                "message": "string",
                "statusType": 0
              },
              "workflowId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z",
              "tenantId": "string",
              "groupRef": {
                "id": "string",
                "name": "string"
              },
              "isAutodiscovered": true
            }
          },
          "movedSanitizedStatistics": {
            "total": 0,
            "destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
              "accountId": "string",
              "source": "string",
              "storageFunctionality": "string",
              "storageType": {
                "name": "string",
                "categoryType": 0,
                "protocolType": 0,
                "vendorType": 0
```

```
"storageStatus": {
                  "message": "string",
                  "statusType": 0
                },
                "workflowId": "string",
                "lastUpdated": "2019-08-24T14:15:22Z",
                "tenantId": "string",
                "groupRef": {
                  "id": "string",
                  "name": "string"
                },
                "isAutodiscovered": true
              }
            },
            "movedBlockedStatistics": {
              "total": 0,
              "destinationStorageInformation": {
                "id": "string",
                "name": "string",
                "groupId": "string",
                "clientId": "string",
                "accountId": "string",
                "source": "string",
                "storageFunctionality": "string",
                "storageType": {
                  "name": "string",
                  "categoryType": 0,
                  "protocolType": 0,
                  "vendorType": 0
                },
                "storageStatus": {
                  "message": "string",
                  "statusType": 0
                },
                "workflowId": "string",
                "lastUpdated": "2019-08-24T14:15:22Z",
                "tenantId": "string",
                "groupRef": {
                  "id": "string",
                  "name": "string"
                },
                "isAutodiscovered": true
              }
            },
            "copyAllowedStatistics": {
              "total": 0,
              "destinationStorageInformation": {
                "id": "string",
                "name": "string",
                "groupId": "string",
                "clientId": "string",
                "accountId": "string",
                "source": "string",
```

```
"storageType": {
                "name": "string",
                "categoryType": 0,
                "protocolType": 0,
                "vendorType": 0
              },
              "storageStatus": {
                "message": "string",
                "statusType": 0
              },
              "workflowId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z",
              "tenantId": "string",
              "groupRef": {
                "id": "string",
                "name": "string"
              },
              "isAutodiscovered": true
            }
          },
          "copyBlockedStatistics": {
            "total": 0,
            "destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
              "accountId": "string",
              "source": "string",
              "storageFunctionality": "string",
              "storageType": {
                "name": "string",
                "categoryType": 0,
                "protocolType": 0,
                "vendorType": 0
              },
              "storageStatus": {
                "message": "string",
                "statusType": 0
              },
              "workflowId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z",
              "tenantId": "string",
              "groupRef": {
                "id": "string",
                "name": "string"
              },
              "isAutodiscovered": true
            }
          },
          "deleteAllowedStatistics": {
            "total": 0
          },
```

```
"total": 0
          },
          "lastCalculatedStatisticsTime": "2019-08-24T14:15:22Z"
        },
        "account": {
          "id": "string",
          "name": "string",
          "description": "string",
          "credentials": "string",
          "protocolType": 0,
          "vendorType": 0,
          "autoDiscovery": true,
          "autodiscoveryDestinationGroupId": "string",
          "destinationGroup": {
            "id": "string",
            "name": "string"
          }
        },
        "realTimeStartDate": "2019-08-24T14:15:22Z"
      },
      "versions": [],
      "hasBlockedVersions": true,
      "versionsCount": 0,
      "objectType": 0,
      "skippedScan": true,
      "$type": "string",
      "url": "string",
      "fileId": "string"
    }
  ],
  "hasBlockedVersions": true,
  "versionsCount": 0,
  "objectType": 0,
  "skippedScan": true,
  "$type": "string"
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	FileBase	false	none	none

and - discriminator: $type

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» storageType	StorageType¦null	false	none	none
» storageName	string¦null	false	none	none
» storageLocation	string¦null	false	none	none
» scanName	string¦null	false	none	none
» progress	Progress¦null	false	none	none
» scanResult	CoreScanResult¦null	false	none	none
» processingState	ProcessingState2	false	none	- 0: InProgress - 1: Failed - 2: Canceled - 3: Available - 4: FailedRemediation
» exception	Exception¦null	false	none	none
» created	string(date-time)	false	none	none
» lastModified	string(date-time)	false	none	none
» discoveryStarted	string(date-time)	false	none	none
» fileProcessingDetails	FileProcessingDetails¦null	false	none	none
» coreEngines	[CoreEngine]¦null	false	none	none
» remediation	FileRemediation¦null	false	none	none
» metaDefenderCoreUrl	string¦null	false	none	none
» discoveryStartedDaySec	integer(int64)	false	none	none
» objectStorageMetadata	string¦null	false	none	none
» scanWorkflowSnapshotId	string¦null	false	none	none
» scanWorkflowSnapshot	ScanWorkflowSnapshot¦null	false	none	none
» versions	[FileVersion]¦null	false	none	none
» hasBlockedVersions	boolean	false	none	none
» versionsCount	integer(int32)	false	none	none

» objectType	ObjectType	false	none	- 0: File - 1: FileVersion
» skippedScan	boolean	false	none	none
» $type	string	true	none	none

ScanWorkflowSnapshot

```
{
  "id": "string",
  "scanId": "string",
  "workflow": {
    "id": "string",
    "scanPoolId": "string",
    "scanProcessFlow": 0,
    "isIdentityScanningEnabled": true,
    "scanIntervalDays": 0,
    "rules": [
      "string"
    ],
    "type": 0,
    "workflowSupportedTechnologies": {
      "dlp": {
        "status": 0
      },
      "deepCdr": {
        "status": 0
      },
      "sandBox": {
        "status": 0
      },
      "metascan": {
        "status": 0
      }
    },
    "name": "string",
    "userAgent": "string",
    "scanPool": {
      "id": "string",
      "name": "string",
      "scanPoolType": 0,
      "isDefault": true,
      "scanInstances": [
        {
          "id": "string",
          "scanPoolId": "string",
          "url": "string",
          "apiKey": "string",
          "timeout": "string",
          "scanInstanceType": 0
        }
      ]
    },
    "failOverScanPoolId": "string",
    "failOverScanPool": {
      "id": "string",
      "name": "string",
      "scanPoolType": 0,
      "isDefault": true,
      "scanInstances": [
```

```
"id": "string",
          "scanPoolId": "string",
          "url": "string",
          "apiKey": "string",
          "timeout": "string",
          "scanInstanceType": 0
        }
      ]
    },
    "filters": {
      "id": "string",
      "minimumSize": 0,
      "maximumSize": 0,
      "minimumDateTime": "2019-08-24T14:15:22Z",
      "maximumDateTime": "2019-08-24T14:15:22Z"
    },
    "fileDefinition": {
      "blockingStrategy": 0,
      "configurableBlockingStrategy": {
        "shouldTreatFilesWithSensitiveDataAsBlocked": true,
        "shouldTreatFilesWithVulnerabilitiesAsBlocked": true
      }
    },
    "remediations": [
      {
        "id": "string",
        "workflowId": "string",
        "isEnabled": true,
        "configuration": "string",
        "type": 0,
        "handlingType": 0
      }
    ],
    "tenantId": "string"
  },
  "startTimestamp": 0,
  "stopTimestamp": 0,
  "scanPool": {
    "id": "string",
    "name": "string",
    "scanPoolType": 0,
    "isDefault": true,
    "scanInstances": [
      {
        "id": "string",
        "scanPoolId": "string",
        "url": "string",
        "apiKey": "string",
        "timeout": "string",
        "scanInstanceType": 0
      }
    ]
  },
```

```
{
      "id": "string",
      "scanPoolId": "string",
      "url": "string",
      "apiKey": "string",
      "timeout": "string",
      "scanInstanceType": 0
    }
  ],
  "failOverScanPool": {
    "id": "string",
    "name": "string",
    "scanPoolType": 0,
    "isDefault": true,
    "scanInstances": [
      {
        "id": "string",
        "scanPoolId": "string",
        "url": "string",
        "apiKey": "string",
        "timeout": "string",
        "scanInstanceType": 0
      }
    ]
  },
  "failOverScanInstances": [
    {
      "id": "string",
      "scanPoolId": "string",
      "url": "string",
      "apiKey": "string",
      "timeout": "string",
      "scanInstanceType": 0
    }
  ],
  "storage": {
    "id": "string",
    "name": "string",
    "groupId": "string",
    "clientId": "string",
    "accountId": "string",
    "source": "string",
    "storageFunctionality": "string",
    "storageType": {
      "name": "string",
      "categoryType": 0,
      "protocolType": 0,
      "vendorType": 0
    },
    "storageStatus": {
      "message": "string",
      "statusType": 0
    },
```

```
"lastUpdated": "2019-08-24T14:15:22Z",
    "tenantId": "string",
    "groupRef": {
      "id": "string",
      "name": "string"
    },
    "isAutodiscovered": true
  },
  "workflowStatistics": {
    "taggingStatistics": {
      "total": 0
    },
    "keepAllowedStatistics": {
      "total": 0
    },
    "keepBlockedStatistics": {
      "total": 0
    },
    "keepSanitizedStatistics": {
      "total": 0
    },
    "movedAllowedStatistics": {
      "total": 0,
      "destinationStorageInformation": {
        "id": "string",
        "name": "string",
        "groupId": "string",
        "clientId": "string",
        "accountId": "string",
        "source": "string",
        "storageFunctionality": "string",
        "storageType": {
          "name": "string",
          "categoryType": 0,
          "protocolType": 0,
          "vendorType": 0
        },
        "storageStatus": {
          "message": "string",
          "statusType": 0
        },
        "workflowId": "string",
        "lastUpdated": "2019-08-24T14:15:22Z",
        "tenantId": "string",
        "groupRef": {
          "id": "string",
          "name": "string"
        },
        "isAutodiscovered": true
      }
    },
    "movedSanitizedStatistics": {
      "total": 0,
```

```
"id": "string",
        "name": "string",
        "groupId": "string",
        "clientId": "string",
        "accountId": "string",
        "source": "string",
        "storageFunctionality": "string",
        "storageType": {
          "name": "string",
          "categoryType": 0,
          "protocolType": 0,
          "vendorType": 0
        },
        "storageStatus": {
          "message": "string",
          "statusType": 0
        },
        "workflowId": "string",
        "lastUpdated": "2019-08-24T14:15:22Z",
        "tenantId": "string",
        "groupRef": {
          "id": "string",
          "name": "string"
        },
        "isAutodiscovered": true
      }
    },
    "movedBlockedStatistics": {
      "total": 0,
      "destinationStorageInformation": {
        "id": "string",
        "name": "string",
        "groupId": "string",
        "clientId": "string",
        "accountId": "string",
        "source": "string",
        "storageFunctionality": "string",
        "storageType": {
          "name": "string",
          "categoryType": 0,
          "protocolType": 0,
          "vendorType": 0
        },
        "storageStatus": {
          "message": "string",
          "statusType": 0
        },
        "workflowId": "string",
        "lastUpdated": "2019-08-24T14:15:22Z",
        "tenantId": "string",
        "groupRef": {
          "id": "string",
          "name": "string"
```

```
"isAutodiscovered": true
      }
    },
    "copyAllowedStatistics": {
      "total": 0,
      "destinationStorageInformation": {
        "id": "string",
        "name": "string",
        "groupId": "string",
        "clientId": "string",
        "accountId": "string",
        "source": "string",
        "storageFunctionality": "string",
        "storageType": {
          "name": "string",
          "categoryType": 0,
          "protocolType": 0,
          "vendorType": 0
        },
        "storageStatus": {
          "message": "string",
          "statusType": 0
        },
        "workflowId": "string",
        "lastUpdated": "2019-08-24T14:15:22Z",
        "tenantId": "string",
        "groupRef": {
          "id": "string",
          "name": "string"
        },
        "isAutodiscovered": true
      }
    },
    "copyBlockedStatistics": {
      "total": 0,
      "destinationStorageInformation": {
        "id": "string",
        "name": "string",
        "groupId": "string",
        "clientId": "string",
        "accountId": "string",
        "source": "string",
        "storageFunctionality": "string",
        "storageType": {
          "name": "string",
          "categoryType": 0,
          "protocolType": 0,
          "vendorType": 0
        },
        "storageStatus": {
          "message": "string",
          "statusType": 0
        },
```

```
"lastUpdated": "2019-08-24T14:15:22Z",
        "tenantId": "string",
        "groupRef": {
          "id": "string",
          "name": "string"
        },
        "isAutodiscovered": true
      }
    },
    "deleteAllowedStatistics": {
      "total": 0
    },
    "deleteBlockedStatistics": {
      "total": 0
    },
    "lastCalculatedStatisticsTime": "2019-08-24T14:15:22Z"
  },
  "account": {
    "id": "string",
    "name": "string",
    "description": "string",
    "credentials": "string",
    "protocolType": 0,
    "vendorType": 0,
    "autoDiscovery": true,
    "autodiscoveryDestinationGroupId": "string",
    "destinationGroup": {
      "id": "string",
      "name": "string"
    }
  },
  "realTimeStartDate": "2019-08-24T14:15:22Z"
}
```

Properties

Name	Type	Required	Restrictions	Description
id	string	true	none	none
scanId	string	true	none	none
workflow	Workflow	true	none	none
startTimestamp	integer(int64)	true	none	none
stopTimestamp	integer(int64)	true	none	none
scanPool	ScanPool¦null	false	none	none
scanInstances	[ScanInstance]¦null	false	none	none
failOverScanPool	ScanPool¦null	false	none	none
failOverScanInstances	[ScanInstance]¦null	false	none	none
storage	NewStorage¦null	false	none	none
workflowStatistics	WorkflowStatistics	true	none	none
account	Account¦null	false	none	none
realTimeStartDate	string(date-time)¦null	false	none	none

Workflow

```
{
  "id": "string",
  "scanPoolId": "string",
  "scanProcessFlow": 0,
  "isIdentityScanningEnabled": true,
  "scanIntervalDays": 0,
  "rules": [
    "string"
  ],
  "type": 0,
  "workflowSupportedTechnologies": {
    "dlp": {
      "status": 0
    },
    "deepCdr": {
      "status": 0
    },
    "sandBox": {
      "status": 0
    },
    "metascan": {
      "status": 0
    }
  },
  "name": "string",
  "userAgent": "string",
  "scanPool": {
    "id": "string",
    "name": "string",
    "scanPoolType": 0,
    "isDefault": true,
    "scanInstances": [
      {
        "id": "string",
        "scanPoolId": "string",
        "url": "string",
        "apiKey": "string",
        "timeout": "string",
        "scanInstanceType": 0
      }
    ]
  },
  "failOverScanPoolId": "string",
  "failOverScanPool": {
    "id": "string",
    "name": "string",
    "scanPoolType": 0,
    "isDefault": true,
    "scanInstances": [
      {
        "id": "string",
        "scanPoolId": "string",
```

```
"apiKey": "string",
        "timeout": "string",
        "scanInstanceType": 0
      }
    ]
  },
  "filters": {
    "id": "string",
    "minimumSize": 0,
    "maximumSize": 0,
    "minimumDateTime": "2019-08-24T14:15:22Z",
    "maximumDateTime": "2019-08-24T14:15:22Z"
  },
  "fileDefinition": {
    "blockingStrategy": 0,
    "configurableBlockingStrategy": {
      "shouldTreatFilesWithSensitiveDataAsBlocked": true,
      "shouldTreatFilesWithVulnerabilitiesAsBlocked": true
    }
  },
  "remediations": [
    {
      "id": "string",
      "workflowId": "string",
      "isEnabled": true,
      "configuration": "string",
      "type": 0,
      "handlingType": 0
    }
  ],
  "tenantId": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
id	string	true	none	none
scanPoolId	string¦null	false	none	none
scanProcessFlow	ScanProcessFlow¦null	false	none	- 0: WithScanning - 1: WithoutScanning
isIdentityScanningEnabled	boolean	true	none	none
scanIntervalDays	integer(int32)¦null	false	none	none
rules	[string]¦null	false	none	none
type	WorkflowType	false	none	- 0: Default - 1: Basic
workflowSupportedTechnologies	WorkflowSupportedTechnologies¦null	false	none	none
name	string	true	none	none
userAgent	string¦null	false	none	none
scanPool	ScanPool¦null	false	none	none
failOverScanPoolId	string¦null	false	none	none
failOverScanPool	ScanPool¦null	false	none	none
filters	Filters	true	none	none
fileDefinition	FileDefinition¦null	false	none	none
remediations	[Remediation]	true	none	none
tenantId	string¦null	false	none	none

ScanProcessFlow

```
0
```

- 0: WithScanning
- 1: WithoutScanning

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: WithScanning - 1: WithoutScanning

Enumerated Values

Property	Value
anonymous	0
anonymous	1

WorkflowType

```
0
```

- 0: Default
- 1: Basic

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: Default - 1: Basic

Enumerated Values

Property	Value
anonymous	0
anonymous	1

WorkflowSupportedTechnologies

```
{
  "dlp": {
    "status": 0
  },
  "deepCdr": {
    "status": 0
  },
  "sandBox": {
    "status": 0
  },
  "metascan": {
    "status": 0
  }
}
```


Properties

Name	Type	Required	Restrictions	Description
dlp	SupportedTechnology	true	none	none
deepCdr	SupportedTechnology	true	none	none
sandBox	SupportedTechnology	true	none	none
metascan	SupportedTechnology	true	none	none

SupportedTechnology


```
{
  "status": 0
}
```


Properties

Name	Type	Required	Restrictions	Description
status	TechnologyStatus	true	none	- 0: Unknown - 1: Disabled - 2: Enabled

TechnologyStatus

```
0
```

- 0: Unknown
- 1: Disabled
- 2: Enabled

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: Unknown - 1: Disabled - 2: Enabled

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2

ScanPool

```
{
  "id": "string",
  "name": "string",
  "scanPoolType": 0,
  "isDefault": true,
  "scanInstances": [
    {
      "id": "string",
      "scanPoolId": "string",
      "url": "string",
      "apiKey": "string",
      "timeout": "string",
      "scanInstanceType": 0
    }
  ]
}
```

Properties

Name	Type	Required	Restrictions	Description
id	string	true	none	none
name	string	true	none	none
scanPoolType	ScanInstanceType	false	none	- 0: MdCore - 1: MdCloud
isDefault	boolean	false	none	none
scanInstances	[ScanInstance]¦null	false	none	none

ScanInstanceType

```
0
```

- 0: MdCore
- 1: MdCloud

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: MdCore - 1: MdCloud

Enumerated Values

Property	Value
anonymous	0
anonymous	1

ScanInstance

```
{
  "id": "string",
  "scanPoolId": "string",
  "url": "string",
  "apiKey": "string",
  "timeout": "string",
  "scanInstanceType": 0
}
```


Properties

Name	Type	Required	Restrictions	Description
id	string	true	none	none
scanPoolId	string	true	none	none
url	string	true	none	none
apiKey	string¦null	false	none	none
timeout	string(duration)	false	none	none
scanInstanceType	ScanInstanceType	false	none	- 0: MdCore - 1: MdCloud

Filters


```
{
  "id": "string",
  "minimumSize": 0,
  "maximumSize": 0,
  "minimumDateTime": "2019-08-24T14:15:22Z",
  "maximumDateTime": "2019-08-24T14:15:22Z"
}
```

Properties

Name	Type	Required	Restrictions	Description
id	string	true	none	none
minimumSize	integer(int64)	false	none	none
maximumSize	integer(int64)	false	none	none
minimumDateTime	string(date-time)	false	none	none
maximumDateTime	string(date-time)	false	none	none

FileDefinition

```
{
  "blockingStrategy": 0,
  "configurableBlockingStrategy": {
    "shouldTreatFilesWithSensitiveDataAsBlocked": true,
    "shouldTreatFilesWithVulnerabilitiesAsBlocked": true
  }
}
```

Properties

Name	Type	Required	Restrictions	Description
blockingStrategy	FileBlockingStrategy	true	none	- 0: Strict - 1: Configurable
configurableBlockingStrategy	ConfigurableBlockingStrategy	true	none	none

FileBlockingStrategy

```
0
```

- 0: Strict
- 1: Configurable

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: Strict - 1: Configurable

Enumerated Values

Property	Value
anonymous	0
anonymous	1

ConfigurableBlockingStrategy

```
{
  "shouldTreatFilesWithSensitiveDataAsBlocked": true,
  "shouldTreatFilesWithVulnerabilitiesAsBlocked": true
}
```

Properties

Name	Type	Required	Restrictions	Description
shouldTreatFilesWithSensitiveDataAsBlocked	boolean	false	none	none
shouldTreatFilesWithVulnerabilitiesAsBlocked	boolean	false	none	none

Remediation

```
{
  "id": "string",
  "workflowId": "string",
  "isEnabled": true,
  "configuration": "string",
  "type": 0,
  "handlingType": 0
}
```

Properties

Name	Type	Required	Restrictions	Description
id	string	true	none	none
workflowId	string	true	none	none
isEnabled	boolean	true	none	none
configuration	string	true	none	none
type	RemediationType	true	none	- 0: FileTagging - 1: DeepCdr - 2: BlockedFileRemediation - 3: AllowedSanitizedFileRemediation - 4: AllowedFileRemediation - 5: BlockedSanitizedFileRemediation - 6: DeleteEmptyFoldersRemediation - 7: ScanFileVersions - 8: DiscoveredFileRemediation - 9: AllowedCdrUnsupportedFileRemediation - 10: BlockedCdrUnsupportedFileRemediation
handlingType	RemediationHandlingType	true	none	- 0: Delete - 1: Move - 2: Copy - 3: Keep - 999: NotApplicable

RemediationType

```
0
```

- 0: FileTagging
- 1: DeepCdr
- 2: BlockedFileRemediation
- 3: AllowedSanitizedFileRemediation
- 4: AllowedFileRemediation
- 5: BlockedSanitizedFileRemediation
- 6: DeleteEmptyFoldersRemediation
- 7: ScanFileVersions

- 8: DiscoveredFileRemediation
- 9: AllowedCdrUnsupportedFileRemediation
- 10: BlockedCdrUnsupportedFileRemediation

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: FileTagging - 1: DeepCdr - 2: BlockedFileRemediation - 3: AllowedSanitizedFileRemediation - 4: AllowedFileRemediation - 5: BlockedSanitizedFileRemediation - 6: DeleteEmptyFoldersRemediation - 7: ScanFileVersions - 8: DiscoveredFileRemediation - 9: AllowedCdrUnsupportedFileRemediation - 10: BlockedCdrUnsupportedFileRemediation

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2
anonymous	3
anonymous	4
anonymous	5
anonymous	6
anonymous	7
anonymous	8
anonymous	9
anonymous	10

RemediationHandlingType

```
0
```

- 0: Delete
- 1: Move
- 2: Copy
- 3: Keep
- 999: NotApplicable

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: Delete - 1: Move - 2: Copy - 3: Keep - 999: NotApplicable

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2
anonymous	3
anonymous	999

NewStorage

```
{
  "id": "string",
  "name": "string",
  "groupId": "string",
  "clientId": "string",
  "accountId": "string",
  "source": "string",
  "storageFunctionality": "string",
  "storageType": {
    "name": "string",
    "categoryType": 0,
    "protocolType": 0,
    "vendorType": 0
  },
  "storageStatus": {
    "message": "string",
    "statusType": 0
  },
  "workflowId": "string",
  "lastUpdated": "2019-08-24T14:15:22Z",
  "tenantId": "string",
  "groupRef": {
    "id": "string",
    "name": "string"
  },
  "isAutodiscovered": true
}
```

Properties

Name	Type	Required	Restrictions	Description
id	string	true	none	none
name	string	true	none	none
groupId	string	true	none	none
clientId	string	true	none	none
accountId	string	true	none	none
source	string	true	none	none
storageFunctionality	string	true	none	none
storageType	NewStorageType	true	none	none
storageStatus	NewStorageStatus	true	none	none
workflowId	string¦null	false	none	none
lastUpdated	string(date-time)¦null	false	none	none
tenantId	string¦null	false	none	none
groupRef	GroupReference¦null	false	none	none
isAutodiscovered	boolean	false	none	none

NewStorageType

```
{
  "name": "string",
  "categoryType": 0,
  "protocolType": 0,
  "vendorType": 0
}
```

Properties

Name	Type	Required	Restrictions	Description
name	string	true	none	none
categoryType	StorageCategoryType2	false	none	- 0: Local - 1: Cloud - 2: Object
protocolType	StorageProtocolType	false	none	- 0: Smb - 1: GraphSdk - 2: BoxSdk - 3: AwsSdk - 4: AzureBlobSdk - 5: AlibabaCloudSdk - 6: GoogleCloudSdk - 7: AzureFilesSdk - 8: Sftp - 9: Nfs - 10: Mft - 11: SharepointOnPrem - 12: Ftp - 13: OracleSdk - 100: GitHubSdk - 101: DockerHubSdk - 102: BitbucketSdk - 103: AmazonEcrSdk - 104: QuaySdk - 105: JFrogContainerSdk - 106: JFrogBinarySdk - 107: AzureAcrSdk - 108: GitLabSourceSdk - 109: GitLabContainerSdk - 110: SvnSdk - 111: AzureDevOpsSourceSdk - 112: AzureDevOpsBinarySdk - 113: DirectFile - 114: NexusBinarySdk - 115: GiteaSdk - 116: HarborSdk
vendorType	StorageVendorType	false	none	- 0: AmazonS3 - 1: OneDrive - 2: Box - 3: Dellsilon - 4: AzureFiles - 5: SmbCompatible - 6: S3Compatible - 7: AzureBlob - 8: AlibabaCloud

				- 9: GoogleCloud - 10: Sftp - 11: SharePoint - 12: Nfs - 13: Wasabi - 14: OracleCloud - 15: NetAppOntap - 16: Cubbit - 17: Mft - 18: SharepointOnPrem - 19: Ftp - 20: Oracle - 21: NfsSisl - 22: ScalityRing - 100: GitHub - 101: DockerHub - 102: Bitbucket - 103: AmazonEcr - 104: Quay - 105: JFrogContainer - 106: JFrogBinary - 107: AzureAcr - 108: GitLabSource - 109: GitLabContainer - 110: Svn - 111: AzureDevOpsSource - 112: AzureDevOpsBinary - 113: DirectFile - 114: NexusBinary - 115: Gitea - 116: Harbor

StorageCategoryType2

```
0
```

- 0: Local
- 1: Cloud
- 2: Object

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: Local - 1: Cloud - 2: Object

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2

NewStorageStatus

```
{
  "message": "string",
  "statusType": 0
}
```

Properties

Name	Type	Required	Restrictions	Description
message	string¦null	false	none	none
statusType	StorageStatusType	true	none	- 0: NotTested - 1: Testing - 2: Operational - 3: Error

StorageStatusType

```
0
```

- 0: NotTested
- 1: Testing

- 2: Operational
- 3: Error

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: NotTested - 1: Testing - 2: Operational - 3: Error

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2
anonymous	3

WorkflowStatistics

```
{
  "taggingStatistics": {
    "total": 0
  },
  "keepAllowedStatistics": {
    "total": 0
  },
  "keepBlockedStatistics": {
    "total": 0
  },
  "keepSanitizedStatistics": {
    "total": 0
  },
  "movedAllowedStatistics": {
    "total": 0,
    "destinationStorageInformation": {
      "id": "string",
      "name": "string",
      "groupId": "string",
      "clientId": "string",
      "accountId": "string",
      "source": "string",
      "storageFunctionality": "string",
      "storageType": {
        "name": "string",
        "categoryType": 0,
        "protocolType": 0,
        "vendorType": 0
      },
      "storageStatus": {
        "message": "string",
        "statusType": 0
      },
      "workflowId": "string",
      "lastUpdated": "2019-08-24T14:15:22Z",
      "tenantId": "string",
      "groupRef": {
        "id": "string",
        "name": "string"
      },
      "isAutodiscovered": true
    }
  },
  "movedSanitizedStatistics": {
    "total": 0,
    "destinationStorageInformation": {
      "id": "string",
      "name": "string",
      "groupId": "string",
      "clientId": "string",
      "accountId": "string",
      "source": "string",
```

```
"storageType": {
        "name": "string",
        "categoryType": 0,
        "protocolType": 0,
        "vendorType": 0
      },
      "storageStatus": {
        "message": "string",
        "statusType": 0
      },
      "workflowId": "string",
      "lastUpdated": "2019-08-24T14:15:22Z",
      "tenantId": "string",
      "groupRef": {
        "id": "string",
        "name": "string"
      },
      "isAutodiscovered": true
    }
  },
  "movedBlockedStatistics": {
    "total": 0,
    "destinationStorageInformation": {
      "id": "string",
      "name": "string",
      "groupId": "string",
      "clientId": "string",
      "accountId": "string",
      "source": "string",
      "storageFunctionality": "string",
      "storageType": {
        "name": "string",
        "categoryType": 0,
        "protocolType": 0,
        "vendorType": 0
      },
      "storageStatus": {
        "message": "string",
        "statusType": 0
      },
      "workflowId": "string",
      "lastUpdated": "2019-08-24T14:15:22Z",
      "tenantId": "string",
      "groupRef": {
        "id": "string",
        "name": "string"
      },
      "isAutodiscovered": true
    }
  },
  "copyAllowedStatistics": {
    "total": 0,
    "destinationStorageInformation": {
```

```
"name": "string",
      "groupId": "string",
      "clientId": "string",
      "accountId": "string",
      "source": "string",
      "storageFunctionality": "string",
      "storageType": {
        "name": "string",
        "categoryType": 0,
        "protocolType": 0,
        "vendorType": 0
      },
      "storageStatus": {
        "message": "string",
        "statusType": 0
      },
      "workflowId": "string",
      "lastUpdated": "2019-08-24T14:15:22Z",
      "tenantId": "string",
      "groupRef": {
        "id": "string",
        "name": "string"
      },
      "isAutodiscovered": true
    }
  },
  "copyBlockedStatistics": {
    "total": 0,
    "destinationStorageInformation": {
      "id": "string",
      "name": "string",
      "groupId": "string",
      "clientId": "string",
      "accountId": "string",
      "source": "string",
      "storageFunctionality": "string",
      "storageType": {
        "name": "string",
        "categoryType": 0,
        "protocolType": 0,
        "vendorType": 0
      },
      "storageStatus": {
        "message": "string",
        "statusType": 0
      },
      "workflowId": "string",
      "lastUpdated": "2019-08-24T14:15:22Z",
      "tenantId": "string",
      "groupRef": {
        "id": "string",
        "name": "string"
      },
```

```
}
  },
  "deleteAllowedStatistics": {
    "total": 0
  },
  "deleteBlockedStatistics": {
    "total": 0
  },
  "lastCalculatedStatisticsTime": "2019-08-24T14:15:22Z"
}
```


Properties

Name	Type	Required	Restrictions	Description
taggingStatistics	TaggingStatistics|null	false	none	none
keepAllowedStatistics	KeepStatistics|null	false	none	none
keepBlockedStatistics	KeepStatistics|null	false	none	none
keepSanitizedStatistics	KeepStatistics|null	false	none	none
movedAllowedStatistics	MovedStatistics|null	false	none	none
movedSanitizedStatistics	MovedStatistics|null	false	none	none
movedBlockedStatistics	MovedStatistics|null	false	none	none
copyAllowedStatistics	MovedStatistics|null	false	none	none
copyBlockedStatistics	MovedStatistics|null	false	none	none
deleteAllowedStatistics	DeleteStatistics|null	false	none	none
deleteBlockedStatistics	DeleteStatistics|null	false	none	none
lastCalculatedStatisticsTime	string(date-time)|null	false	none	none

TaggingStatistics


```
{
  "total": 0
}
```

Properties

Name	Type	Required	Restrictions	Description
total	integer(int64)	true	none	none

KeepStatistics

```
{
  "total": 0
}
```

Properties

Name	Type	Required	Restrictions	Description
total	integer(int64)	true	none	none

MovedStatistics

```
{
  "total": 0,
  "destinationStorageInformation": {
    "id": "string",
    "name": "string",
    "groupId": "string",
    "clientId": "string",
    "accountId": "string",
    "source": "string",
    "storageFunctionality": "string",
    "storageType": {
      "name": "string",
      "categoryType": 0,
      "protocolType": 0,
      "vendorType": 0
    },
    "storageStatus": {
      "message": "string",
      "statusType": 0
    },
    "workflowId": "string",
    "lastUpdated": "2019-08-24T14:15:22Z",
    "tenantId": "string",
    "groupRef": {
      "id": "string",
      "name": "string"
    },
    "isAutodiscovered": true
  }
}
```


Properties

Name	Type	Required	Restrictions	Description
total	integer(int64)	true	none	none
destinationStorageInformation	NewStorage	true	none	none

DeleteStatistics


```
{
  "total": 0
}
```

Properties

Name	Type	Required	Restrictions	Description
total	integer(int64)	true	none	none

FileVersion

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "id": "string",
  "scanId": "string",
  "name": "string",
  "path": "string",
  "hash": "string",
  "fileOwner": {
    "userId": "string",
    "fullName": "string",
    "userName": "string",
    "emailAddress": "string"
  },
  "size": 0,
  "fileTypeCategory": 0,
  "extension": "string",
  "storageType": {
    "name": "string",
    "categoryType": 0,
    "protocolType": 0,
    "vendorType": 0
  },
  "storageName": "string",
  "storageLocation": "string",
  "scanName": "string",
  "progress": {
    "upload": 0,
    "scan": 0,
    "archiveExtraction": 0
  },
  "scanResult": {
    "extractedFiles": {
      "dataId": "string",
      "scanResultI": 0,
      "detectedBy": 0,
      "filesExtractedCount": 0
    },
    "scanResults": {
      "scanDetails": [
        {
          "engineName": "string",
          "threatFound": "string",
          "scanResultI": 0,
          "defTime": "string",
          "scanTime": 0.1,
          "engId": "string",
```

```
}
      ],
      "dataId": "string",
      "scanAllResultI": 0,
      "scanAllResultA": "string",
      "startTime": "string",
      "totalTime": 0.1,
      "totalAvs": 0,
      "totalDetections": 0,
      "progressPercentage": 0
    },
    "fileInfo": {
      "fileSize": 0,
      "uploadTimestamp": "string",
      "md5": "string",
      "sha1": "string",
      "sha256": "string",
      "fileTypeCategory": "string",
      "fileTypeDescription": "string",
      "fileTypeExtension": "string",
      "displayName": "string",
      "fileTypeId": "string"
    },
    "fileScanInfo": {
      "finalVerdict": {
        "blocked": true,
        "verdict": "string",
        "confidence": 0.1,
        "threatLevel": 0.1
      },
      "overviewReport": {
        "analysisState": "string",
        "signalGroups": [
          {
            "description": "string",
            "verdict": "string",
            "signals": [
              {
                "originType": "string",
                "signalReadable": "string",
                "strength": 0.1
              }
            ],
            "mitreTechniques": [
              {
                "name": "string",
                "tacticName": "string"
              }
            ]
          }
        ],
        "iocs": [
          {
```

```
"type": "string",
            "origin": "string",
            "verdict": "string"
          }
        ],
        "yaraMatches": [
          {
            "ruleName": "string",
            "ruleDescription": "string",
            "verdict": "string",
            "matchedStrings": [
              "string"
            ],
            "author": "string",
            "version": "string",
            "threatLevel": 0.1,
            "confidence": 0.1,
            "strength": 0.1
          }
        ],
        "tags": [
          {
            "name": "string",
            "verdict": "string"
          }
        ],
        "metaData": {
          "entropy": 0.1,
          "forensicAnalysisRecommended": true,
          "fuzzyFsioHash": "string"
        }
      },
      "errorCategory": "string",
      "errorCode": 0,
      "errorDetails": "string"
    },
    "processInfo": {
      "postProcessing": {
        "actionsRan": "string",
        "actionsFailed": "string",
        "convertedTo": "string",
        "copyMoveDestination": "string",
        "convertedDestination": "string",
        "sanitizationDetails": {
          "failureCategory": "string",
          "description": "string",
          "details": "string"
        }
      },
      "progressPercentage": 0,
      "userAgent": "string",
      "profile": "string",
      "result": "string",
```

```
"fileTypeSkippedScan": true,
      "processingTime": 0.1,
      "queueTime": 0.1,
      "resultI": 0
    },
    "dataId": "string",
    "dlpInfo": {
      "hits": null,
      "verdict": 0
    },
    "sbomInfo": {
      "finalVerdict": {
        "blocked": true,
        "licensingPackageCounts": {
          "allowed": 0,
          "blocked": 0,
          "unknown": 0,
          "unsupported": 0
        },
        "severity": 0,
        "totalPackageCount": 0,
        "verdict": "string",
        "vulnerabilityCounts": {
          "critical": 0,
          "high": 0,
          "medium": 0,
          "low": 0,
          "unknown": 0
        }
      },
      "overviewReport": {
        "isPartialReport": true,
        "osInfo": {
          "osName": "string",
          "osVersion": "string"
        },
        "scanMode": "string",
        "steps": [
          {
            "command": "string",
            "packages": [
              {
                "authors": "string",
                "releaseDate": "2019-08-24T14:15:22Z",
                "ecosystem": "string",
                "group": "string",
                "archive": true,
                "executable": true,
                "uid": "string",
                "licenses": {
                  "allowed": [
                    {
                      "id": "string",
```

```
"category": "string",
                      "usageRestriction": {
                        "permissions": [
                          "string"
                        ],
                        "conditions": [
                          "string"
                        ],
                        "limitations": [
                          "string"
                        ]
                      }
                    }
                  ],
                  "blocked": [
                    {
                      "id": "string",
                      "url": "string",
                      "category": "string",
                      "usageRestriction": {
                        "permissions": [
                          "string"
                        ],
                        "conditions": [
                          "string"
                        ],
                        "limitations": [
                          "string"
                        ]
                      }
                    }
                  ]
                },
                "packageName": "string",
                "packageVersion": "string",
                "hashes": [
                  {
                    "sha256": "string",
                    "fileName": "string"
                  }
                ],
                "vulnerabilityCounts": {
                  "critical": 0,
                  "high": 0,
                  "medium": 0,
                  "low": 0,
                  "unknown": 0
                },
                "vulnerabilities": [
                  {
                    "id": "string",
                    "severity": 0,
                    "source": "string",
```

```
"cwes": [
                        "string"
                      ]
                    }
                  ],
                  "arch": "string",
                  "osName": "string",
                  "osVersion": "string",
                  "dependencies": [
                    {
                      "ecosystem": "string",
                      "group": "string",
                      "packageName": "string",
                      "packageVersion": "string",
                      "vulnerabilities": [
                        {
                          "id": "string",
                          "severity": 0,
                          "source": "string",
                          "fixedVersions": "string",
                          "cwes": [
                            "string"
                          ]
                        }
                      ],
                      "vulnerabilityCounts": {
                        "critical": 0,
                        "high": 0,
                        "medium": 0,
                        "low": 0,
                        "unknown": 0
                      }
                    }
                  ]
                }
              ],
              "licenseStatus": "string",
              "licensingPackageCounts": {
                "allowed": 0,
                "blocked": 0,
                "unknown": 0,
                "unsupported": 0
              },
              "step": 0,
              "vulnerabilityCount": 0,
              "sha256": "string",
              "severity": 0,
              "vulnerabilityCounts": {
                "critical": 0,
                "high": 0,
                "medium": 0,
                "low": 0,
                "unknown": 0
```

```
}
        ],
        "packages": [
          {
            "authors": "string",
            "releaseDate": "2019-08-24T14:15:22Z",
            "ecosystem": "string",
            "group": "string",
            "archive": true,
            "executable": true,
            "uid": "string",
            "licenses": {
              "allowed": [
                {
                  "id": "string",
                  "url": "string",
                  "category": "string",
                  "usageRestriction": {
                    "permissions": [
                      "string"
                    ],
                    "conditions": [
                      "string"
                    ],
                    "limitations": [
                      "string"
                    ]
                  }
                }
              ],
              "blocked": [
                {
                  "id": "string",
                  "url": "string",
                  "category": "string",
                  "usageRestriction": {
                    "permissions": [
                      "string"
                    ],
                    "conditions": [
                      "string"
                    ],
                    "limitations": [
                      "string"
                    ]
                  }
                }
              ]
            },
            "packageName": "string",
            "packageVersion": "string",
            "target": "string",
            "hashes": [
```

```
"sha256": "string",
                "fileName": "string"
              }
            ],
            "vulnerabilities": [
              {
                "id": "string",
                "severity": 0,
                "source": "string",
                "fixedVersions": "string",
                "cwes": [
                  "string"
                ]
              }
            ],
            "vulnerabilityCounts": {
              "critical": 0,
              "high": 0,
              "medium": 0,
              "low": 0,
              "unknown": 0
            },
            "dependencies": [
              {
                "ecosystem": "string",
                "group": "string",
                "packageName": "string",
                "packageVersion": "string",
                "vulnerabilities": [
                  {
                    "id": "string",
                    "severity": 0,
                    "source": "string",
                    "fixedVersions": "string",
                    "cwes": [
                      "string"
                    ]
                  }
                ],
                "vulnerabilityCounts": {
                  "critical": 0,
                  "high": 0,
                  "medium": 0,
                  "low": 0,
                  "unknown": 0
                }
              }
            ]
          }
        ],
        "dependenciesPackageCount": 0,
        "dependenciesVulnerabilityTotal": 0,
        "dependenciesVulnerabilityCounts": {
```

```
"high": 0,
          "medium": 0,
          "low": 0,
          "unknown": 0
        }
      },
      "resultTemplateHash": "string"
    },
    "vulnerabilityInfo": {
      "vulnerabilityInfoResult": {
        "code": 0,
        "hash": "string",
        "method": 0,
        "timeStamp": "string",
        "timing": 0,
        "detectedProduct": {
          "hasVulnerability": true,
          "isCurrent": true,
          "product": {
            "id": 0,
            "name": "string"
          },
          "remediationLink": "string",
          "severity": "string",
          "sigName": "string",
          "signature": 0,
          "vendor": {
            "id": 0,
            "name": "string"
          },
          "version": "string",
          "versionData": {
            "countBehind": 0,
            "feedId": 0,
            "version": "string"
          },
          "vulnerabilities": [
            {
              "description": "string",
              "details": {
                "cpe": "string",
                "cve": "string",
                "cvss": {
                  "accessComplexity": "string",
                  "accessVector": "string",
                  "authentication": "string",
                  "availabilityImpact": "string",
                  "confidentialityImpact": "string",
                  "generatedOnEpoch": "string",
                  "integrityImpact": "string",
                  "score": "string",
                  "source": "string"
                },
```

```
"attackComplexity": "string",
                  "attackVector": "string",
                  "availabilityImpact": "string",
                  "baseScore": "string",
                  "baseSeverity": "string",
                  "confidentialityImpact": "string",
                  "exploitabilityScore": "string",
                  "impactScore": "string",
                  "integrityImpact": "string",
                  "privilegesRequired": "string",
                  "scope": "string",
                  "userInteraction": "string",
                  "vectorString": "string"
                },
                "cwe": "string",
                "lastModifiedEpoch": "string",
                "publishedEpoch": "string",
                "references": [
                  "string"
                ]
              },
              "severity": "string",
              "severityIndex": 0,
              "staticId": 0
            }
          ]
        }
      }
    },
    "sessionCookie": "string",
    "fileTypeInfo": {
      "fileInfoExtended": {
        "extensions": "string",
        "groupId": "string",
        "typeId": "string"
      }
    },
    "scanInstanceUrl": "string",
    "scanWorkflowSnapshotId": "string",
    "coreEngines": [
      {
        "engineId": "string",
        "engineName": "string",
        "engineVersion": "string",
        "dbVersion": "string",
        "definitionTime": "string"
      }
    ]
  },
  "processingState": 0,
  "exception": {
    "exceptionDetails": "string",
    "exceptionMessage": "string"
```

```
"created": "2019-08-24T14:15:22Z",
  "lastModified": "2019-08-24T14:15:22Z",
  "discoveryStarted": "2019-08-24T14:15:22Z",
  "fileProcessingDetails": {
    "streamingStartedTime": "2019-08-24T14:15:22Z",
    "streamingCompletedTime": "2019-08-24T14:15:22Z",
    "streamingTimeSpanMs": 0,
    "scanCompletedTime": "2019-08-24T14:15:22Z",
    "processingTimeSpanMs": 0
  },
  "coreEngines": [
    {
      "engineId": "string",
      "engineName": "string",
      "engineVersion": "string",
      "dbVersion": "string",
      "definitionTime": "string"
    }
  ],
  "remediation": {
    "deepCdr": {
      "sanitizationDetails": {
        "failureCategory": "string",
        "description": "string",
        "details": "string"
      },
      "cdrObjectState": 0,
      "fileWasReplaced": true
    },
    "postActionFailedInformation": [
      {
        "objectActionType": 0,
        "exception": {
          "exceptionDetails": "string",
          "exceptionMessage": "string"
        }
      }
    ],
    "objectRemediationActions": [
      {
        "objectActionType": 0,
        "objectActionState": 0,
        "cdrObjectState": 0,
        "exceptions": [
          "string"
        ],
        "id": "string",
        "fileId": "string",
        "fileScanCompletedTime": "2019-08-24T14:15:22Z",
        "remediationId": "string",
        "tenantId": "string",
        "lastUpdated": "2019-08-24T14:15:22Z"
      }
```

```
},
  "metaDefenderCoreUrl": "string",
  "discoveryStartedDaySec": 0,
  "objectStorageMetadata": "string",
  "scanWorkflowSnapshotId": "string",
  "scanWorkflowSnapshot": {
    "id": "string",
    "scanId": "string",
    "workflow": {
      "id": "string",
      "scanPoolId": "string",
      "scanProcessFlow": 0,
      "isIdentityScanningEnabled": true,
      "scanIntervalDays": 0,
      "rules": [
        "string"
      ],
      "type": 0,
      "workflowSupportedTechnologies": {
        "dlp": {
          "status": 0
        },
        "deepCdr": {
          "status": 0
        },
        "sandBox": {
          "status": 0
        },
        "metascan": {
          "status": 0
        }
      },
      "name": "string",
      "userAgent": "string",
      "scanPool": {
        "id": "string",
        "name": "string",
        "scanPoolType": 0,
        "isDefault": true,
        "scanInstances": [
          {
            "id": "string",
            "scanPoolId": "string",
            "url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ]
      },
      "failOverScanPoolId": "string",
      "failOverScanPool": {
        "id": "string",
```

```
"scanPoolType": 0,
        "isDefault": true,
        "scanInstances": [
          {
            "id": "string",
            "scanPoolId": "string",
            "url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ]
      },
      "filters": {
        "id": "string",
        "minimumSize": 0,
        "maximumSize": 0,
        "minimumDateTime": "2019-08-24T14:15:22Z",
        "maximumDateTime": "2019-08-24T14:15:22Z"
      },
      "fileDefinition": {
        "blockingStrategy": 0,
        "configurableBlockingStrategy": {
          "shouldTreatFilesWithSensitiveDataAsBlocked": true,
          "shouldTreatFilesWithVulnerabilitiesAsBlocked": true
        }
      },
      "remediations": [
        {
          "id": "string",
          "workflowId": "string",
          "isEnabled": true,
          "configuration": "string",
          "type": 0,
          "handlingType": 0
        }
      ],
      "tenantId": "string"
    },
    "startTimestamp": 0,
    "stopTimestamp": 0,
    "scanPool": {
      "id": "string",
      "name": "string",
      "scanPoolType": 0,
      "isDefault": true,
      "scanInstances": [
        {
          "id": "string",
          "scanPoolId": "string",
          "url": "string",
          "apiKey": "string",
          "timeout": "string",
```

```
}
      ]
    },
    "scanInstances": [
      {
        "id": "string",
        "scanPoolId": "string",
        "url": "string",
        "apiKey": "string",
        "timeout": "string",
        "scanInstanceType": 0
      }
    ],
    "failOverScanPool": {
      "id": "string",
      "name": "string",
      "scanPoolType": 0,
      "isDefault": true,
      "scanInstances": [
        {
          "id": "string",
          "scanPoolId": "string",
          "url": "string",
          "apiKey": "string",
          "timeout": "string",
          "scanInstanceType": 0
        }
      ]
    },
    "failOverScanInstances": [
      {
        "id": "string",
        "scanPoolId": "string",
        "url": "string",
        "apiKey": "string",
        "timeout": "string",
        "scanInstanceType": 0
      }
    ],
    "storage": {
      "id": "string",
      "name": "string",
      "groupId": "string",
      "clientId": "string",
      "accountId": "string",
      "source": "string",
      "storageFunctionality": "string",
      "storageType": {
        "name": "string",
        "categoryType": 0,
        "protocolType": 0,
        "vendorType": 0
      },
```

```
"message": "string",
        "statusType": 0
      },
      "workflowId": "string",
      "lastUpdated": "2019-08-24T14:15:22Z",
      "tenantId": "string",
      "groupRef": {
        "id": "string",
        "name": "string"
      },
      "isAutodiscovered": true
    },
    "workflowStatistics": {
      "taggingStatistics": {
        "total": 0
      },
      "keepAllowedStatistics": {
        "total": 0
      },
      "keepBlockedStatistics": {
        "total": 0
      },
      "keepSanitizedStatistics": {
        "total": 0
      },
      "movedAllowedStatistics": {
        "total": 0,
        "destinationStorageInformation": {
          "id": "string",
          "name": "string",
          "groupId": "string",
          "clientId": "string",
          "accountId": "string",
          "source": "string",
          "storageFunctionality": "string",
          "storageType": {
            "name": "string",
            "categoryType": 0,
            "protocolType": 0,
            "vendorType": 0
          },
          "storageStatus": {
            "message": "string",
            "statusType": 0
          },
          "workflowId": "string",
          "lastUpdated": "2019-08-24T14:15:22Z",
          "tenantId": "string",
          "groupRef": {
            "id": "string",
            "name": "string"
          },
          "isAutodiscovered": true
```

```
},
      "movedSanitizedStatistics": {
        "total": 0,
        "destinationStorageInformation": {
          "id": "string",
          "name": "string",
          "groupId": "string",
          "clientId": "string",
          "accountId": "string",
          "source": "string",
          "storageFunctionality": "string",
          "storageType": {
            "name": "string",
            "categoryType": 0,
            "protocolType": 0,
            "vendorType": 0
          },
          "storageStatus": {
            "message": "string",
            "statusType": 0
          },
          "workflowId": "string",
          "lastUpdated": "2019-08-24T14:15:22Z",
          "tenantId": "string",
          "groupRef": {
            "id": "string",
            "name": "string"
          },
          "isAutodiscovered": true
        }
      },
      "movedBlockedStatistics": {
        "total": 0,
        "destinationStorageInformation": {
          "id": "string",
          "name": "string",
          "groupId": "string",
          "clientId": "string",
          "accountId": "string",
          "source": "string",
          "storageFunctionality": "string",
          "storageType": {
            "name": "string",
            "categoryType": 0,
            "protocolType": 0,
            "vendorType": 0
          },
          "storageStatus": {
            "message": "string",
            "statusType": 0
          },
          "workflowId": "string",
          "lastUpdated": "2019-08-24T14:15:22Z",
```

```
"groupRef": {
            "id": "string",
            "name": "string"
          },
          "isAutodiscovered": true
        }
      },
      "copyAllowedStatistics": {
        "total": 0,
        "destinationStorageInformation": {
          "id": "string",
          "name": "string",
          "groupId": "string",
          "clientId": "string",
          "accountId": "string",
          "source": "string",
          "storageFunctionality": "string",
          "storageType": {
            "name": "string",
            "categoryType": 0,
            "protocolType": 0,
            "vendorType": 0
          },
          "storageStatus": {
            "message": "string",
            "statusType": 0
          },
          "workflowId": "string",
          "lastUpdated": "2019-08-24T14:15:22Z",
          "tenantId": "string",
          "groupRef": {
            "id": "string",
            "name": "string"
          },
          "isAutodiscovered": true
        }
      },
      "copyBlockedStatistics": {
        "total": 0,
        "destinationStorageInformation": {
          "id": "string",
          "name": "string",
          "groupId": "string",
          "clientId": "string",
          "accountId": "string",
          "source": "string",
          "storageFunctionality": "string",
          "storageType": {
            "name": "string",
            "categoryType": 0,
            "protocolType": 0,
            "vendorType": 0
          },
```

```
"message": "string",
            "statusType": 0
          },
          "workflowId": "string",
          "lastUpdated": "2019-08-24T14:15:22Z",
          "tenantId": "string",
          "groupRef": {
            "id": "string",
            "name": "string"
          },
          "isAutodiscovered": true
        }
      },
      "deleteAllowedStatistics": {
        "total": 0
      },
      "deleteBlockedStatistics": {
        "total": 0
      },
      "lastCalculatedStatisticsTime": "2019-08-24T14:15:22Z"
    },
    "account": {
      "id": "string",
      "name": "string",
      "description": "string",
      "credentials": "string",
      "protocolType": 0,
      "vendorType": 0,
      "autoDiscovery": true,
      "autodiscoveryDestinationGroupId": "string",
      "destinationGroup": {
        "id": "string",
        "name": "string"
      }
    },
    "realTimeStartDate": "2019-08-24T14:15:22Z"
  },
  "versions": [
    {
      "result": 0,
      "responseKey": "string",
      "responseMessage": "string",
      "responseMessageParams": {
        "property1": "string",
        "property2": "string"
      },
      "id": "string",
      "scanId": "string",
      "name": "string",
      "path": "string",
      "hash": "string",
      "fileOwner": {
        "userId": "string",
```

```
"userName": "string",
        "emailAddress": "string"
      },
      "size": 0,
      "fileTypeCategory": 0,
      "extension": "string",
      "storageType": {
        "name": "string",
        "categoryType": 0,
        "protocolType": 0,
        "vendorType": 0
      },
      "storageName": "string",
      "storageLocation": "string",
      "scanName": "string",
      "progress": {
        "upload": 0,
        "scan": 0,
        "archiveExtraction": 0
      },
      "scanResult": {
        "extractedFiles": {
          "dataId": "string",
          "scanResultI": 0,
          "detectedBy": 0,
          "filesExtractedCount": 0
        },
        "scanResults": {
          "scanDetails": [
            {
              "engineName": "string",
              "threatFound": "string",
              "scanResultI": 0,
              "defTime": "string",
              "scanTime": 0.1,
              "engId": "string",
              "waitTime": 0.1
            }
          ],
          "dataId": "string",
          "scanAllResultI": 0,
          "scanAllResultA": "string",
          "startTime": "string",
          "totalTime": 0.1,
          "totalAvs": 0,
          "totalDetections": 0,
          "progressPercentage": 0
        },
        "fileInfo": {
          "fileSize": 0,
          "uploadTimestamp": "string",
          "md5": "string",
          "sha1": "string",
```

```
"fileTypeCategory": "string",
          "fileTypeDescription": "string",
          "fileTypeExtension": "string",
          "displayName": "string",
          "fileTypeId": "string"
        },
        "fileScanInfo": {
          "finalVerdict": {
            "blocked": true,
            "verdict": "string",
            "confidence": 0.1,
            "threatLevel": 0.1
          },
          "overviewReport": {
            "analysisState": "string",
            "signalGroups": [
              {
                "description": "string",
                "verdict": "string",
                "signals": [
                  {
                    "originType": "string",
                    "signalReadable": "string",
                    "strength": 0.1
                  }
                ],
                "mitreTechniques": [
                  {
                    "name": "string",
                    "tacticName": "string"
                  }
                ]
              }
            ],
            "iocs": [
              {
                "data": "string",
                "type": "string",
                "origin": "string",
                "verdict": "string"
              }
            ],
            "yaraMatches": [
              {
                "ruleName": "string",
                "ruleDescription": "string",
                "verdict": "string",
                "matchedStrings": [
                  "string"
                ],
                "author": "string",
                "version": "string",
                "threatLevel": 0.1,
```

```
"strength": 0.1
              }
            ],
            "tags": [
              {
                "name": "string",
                "verdict": "string"
              }
            ],
            "metaData": {
              "entropy": 0.1,
              "forensicAnalysisRecommended": true,
              "fuzzyFsioHash": "string"
            }
          },
          "errorCategory": "string",
          "errorCode": 0,
          "errorDetails": "string"
        },
        "processInfo": {
          "postProcessing": {
            "actionsRan": "string",
            "actionsFailed": "string",
            "convertedTo": "string",
            "copyMoveDestination": "string",
            "convertedDestination": "string",
            "sanitizationDetails": {
              "failureCategory": "string",
              "description": "string",
              "details": "string"
            }
          },
          "progressPercentage": 0,
          "userAgent": "string",
          "profile": "string",
          "result": "string",
          "blockedReason": "string",
          "fileTypeSkippedScan": true,
          "processingTime": 0.1,
          "queueTime": 0.1,
          "resultI": 0
        },
        "dataId": "string",
        "dlpInfo": {
          "hits": null,
          "verdict": 0
        },
        "sbomInfo": {
          "finalVerdict": {
            "blocked": true,
            "licensingPackageCounts": {
              "allowed": 0,
              "blocked": 0,
```

```
"unsupported": 0
            },
            "severity": 0,
            "totalPackageCount": 0,
            "verdict": "string",
            "vulnerabilityCounts": {
              "critical": 0,
              "high": 0,
              "medium": 0,
              "low": 0,
              "unknown": 0
            }
          },
          "overviewReport": {
            "isPartialReport": true,
            "osInfo": {
              "osName": "string",
              "osVersion": "string"
            },
            "scanMode": "string",
            "steps": [
              {
                "command": "string",
                "packages": [
                  {
                    "authors": "string",
                    "releaseDate": "2019-08-24T14:15:22Z",
                    "ecosystem": "string",
                    "group": "string",
                    "archive": true,
                    "executable": true,
                    "uid": "string",
                    "licenses": {
                      "allowed": [
                        {
                          "id": "string",
                          "url": "string",
                          "category": "string",
                          "usageRestriction": {
                            "permissions": [
                              null
                            ],
                            "conditions": [
                              null
                            ],
                            "limitations": [
                              null
                            ]
                          }
                        }
                      ],
                      "blocked": [
                        {
```

```
"url": "string",
                          "category": "string",
                          "usageRestriction": {
                            "permissions": [
                              null
                            ],
                            "conditions": [
                              null
                            ],
                            "limitations": [
                              null
                            ]
                          }
                        }
                      ]
                    },
                    "packageName": "string",
                    "packageVersion": "string",
                    "hashes": [
                      {
                        "sha256": "string",
                        "fileName": "string"
                      }
                    ],
                    "vulnerabilityCounts": {
                      "critical": 0,
                      "high": 0,
                      "medium": 0,
                      "low": 0,
                      "unknown": 0
                    },
                    "vulnerabilities": [
                      {
                        "id": "string",
                        "severity": 0,
                        "source": "string",
                        "fixedVersions": "string",
                        "cwes": [
                          "string"
                        ]
                      }
                    ],
                    "arch": "string",
                    "osName": "string",
                    "osVersion": "string",
                    "dependencies": [
                      {
                        "ecosystem": "string",
                        "group": "string",
                        "packageName": "string",
                        "packageVersion": "string",
                        "vulnerabilities": [
                          {
```

```
"severity": 0,
                              "source": "string",
                              "fixedVersions": "string",
                              "cwes": [
                                null
                              ]
                            }
                          ],
                          "vulnerabilityCounts": {
                            "critical": 0,
                            "high": 0,
                            "medium": 0,
                            "low": 0,
                            "unknown": 0
                          }
                        }
                      ]
                    }
                  ],
                  "licenseStatus": "string",
                  "licensingPackageCounts": {
                    "allowed": 0,
                    "blocked": 0,
                    "unknown": 0,
                    "unsupported": 0
                  },
                  "step": 0,
                  "vulnerabilityCount": 0,
                  "sha256": "string",
                  "severity": 0,
                  "vulnerabilityCounts": {
                    "critical": 0,
                    "high": 0,
                    "medium": 0,
                    "low": 0,
                    "unknown": 0
                  }
                }
              ],
              "packages": [
                {
                  "authors": "string",
                  "releaseDate": "2019-08-24T14:15:22Z",
                  "ecosystem": "string",
                  "group": "string",
                  "archive": true,
                  "executable": true,
                  "uid": "string",
                  "licenses": {
                    "allowed": [
                      {
                        "id": "string",
                        "url": "string",
```

```
"usageRestriction": {
                        "permissions": [
                          "string"
                        ],
                        "conditions": [
                          "string"
                        ],
                        "limitations": [
                          "string"
                        ]
                      }
                    }
                  ],
                  "blocked": [
                    {
                      "id": "string",
                      "url": "string",
                      "category": "string",
                      "usageRestriction": {
                        "permissions": [
                          "string"
                        ],
                        "conditions": [
                          "string"
                        ],
                        "limitations": [
                          "string"
                        ]
                      }
                    }
                  ]
                },
                "packageName": "string",
                "packageVersion": "string",
                "target": "string",
                "hashes": [
                  {
                    "sha256": "string",
                    "fileName": "string"
                  }
                ],
                "vulnerabilities": [
                  {
                    "id": "string",
                    "severity": 0,
                    "source": "string",
                    "fixedVersions": "string",
                    "cwes": [
                      "string"
                    ]
                  }
                ],
                "vulnerabilityCounts": {
```

```
"high": 0,
                  "medium": 0,
                  "low": 0,
                  "unknown": 0
                },
                "dependencies": [
                  {
                    "ecosystem": "string",
                    "group": "string",
                    "packageName": "string",
                    "packageVersion": "string",
                    "vulnerabilities": [
                      {
                        "id": "string",
                        "severity": 0,
                        "source": "string",
                        "fixedVersions": "string",
                        "cwes": [
                          "string"
                        ]
                      }
                    ],
                    "vulnerabilityCounts": {
                      "critical": 0,
                      "high": 0,
                      "medium": 0,
                      "low": 0,
                      "unknown": 0
                    }
                  }
                ]
              }
            ],
            "dependenciesPackageCount": 0,
            "dependenciesVulnerabilityTotal": 0,
            "dependenciesVulnerabilityCounts": {
              "critical": 0,
              "high": 0,
              "medium": 0,
              "low": 0,
              "unknown": 0
            }
          },
          "resultTemplateHash": "string"
        },
        "vulnerabilityInfo": {
          "vulnerabilityInfoResult": {
            "code": 0,
            "hash": "string",
            "method": 0,
            "timeStamp": "string",
            "timing": 0,
            "detectedProduct": {
```

```
"isCurrent": true,
              "product": {
                "id": 0,
                "name": "string"
              },
              "remediationLink": "string",
              "severity": "string",
              "sigName": "string",
              "signature": 0,
              "vendor": {
                "id": 0,
                "name": "string"
              },
              "version": "string",
              "versionData": {
                "countBehind": 0,
                "feedId": 0,
                "version": "string"
              },
              "vulnerabilities": [
                {
                  "description": "string",
                  "details": {
                    "cpe": "string",
                    "cve": "string",
                    "cvss": {
                      "accessComplexity": "string",
                      "accessVector": "string",
                      "authentication": "string",
                      "availabilityImpact": "string",
                      "confidentialityImpact": "string",
                      "generatedOnEpoch": "string",
                      "integrityImpact": "string",
                      "score": "string",
                      "source": "string"
                    },
                    "cvss3": {
                      "attackComplexity": "string",
                      "attackVector": "string",
                      "availabilityImpact": "string",
                      "baseScore": "string",
                      "baseSeverity": "string",
                      "confidentialityImpact": "string",
                      "exploitabilityScore": "string",
                      "impactScore": "string",
                      "integrityImpact": "string",
                      "privilegesRequired": "string",
                      "scope": "string",
                      "userInteraction": "string",
                      "vectorString": "string"
                    },
                    "cwe": "string",
                    "lastModifiedEpoch": "string",
```

```
"references": [
                      "string"
                    ]
                  },
                  "severity": "string",
                  "severityIndex": 0,
                  "staticId": 0
                }
              ]
            }
          }
        },
        "sessionCookie": "string",
        "fileTypeInfo": {
          "fileInfoExtended": {
            "extensions": "string",
            "groupId": "string",
            "typeId": "string"
          }
        },
        "scanInstanceUrl": "string",
        "scanWorkflowSnapshotId": "string",
        "coreEngines": [
          {
            "engineId": "string",
            "engineName": "string",
            "engineVersion": "string",
            "dbVersion": "string",
            "definitionTime": "string"
          }
        ]
      },
      "processingState": 0,
      "exception": {
        "exceptionDetails": "string",
        "exceptionMessage": "string"
      },
      "created": "2019-08-24T14:15:22Z",
      "lastModified": "2019-08-24T14:15:22Z",
      "discoveryStarted": "2019-08-24T14:15:22Z",
      "fileProcessingDetails": {
        "streamingStartedTime": "2019-08-24T14:15:22Z",
        "streamingCompletedTime": "2019-08-24T14:15:22Z",
        "streamingTimeSpanMs": 0,
        "scanCompletedTime": "2019-08-24T14:15:22Z",
        "processingTimeSpanMs": 0
      },
      "coreEngines": [
        {
          "engineId": "string",
          "engineName": "string",
          "engineVersion": "string",
          "dbVersion": "string",
```

```
}
      ],
      "remediation": {
        "deepCdr": {
          "sanitizationDetails": {
            "failureCategory": "string",
            "description": "string",
            "details": "string"
          },
          "cdrObjectState": 0,
          "fileWasReplaced": true
        },
        "postActionFailedInformation": [
          {
            "objectActionType": 0,
            "exception": {
              "exceptionDetails": "string",
              "exceptionMessage": "string"
            }
          }
        ],
        "objectRemediationActions": [
          {
            "objectActionType": 0,
            "objectActionState": 0,
            "cdrObjectState": 0,
            "exceptions": [
              "string"
            ],
            "id": "string",
            "fileId": "string",
            "fileScanCompletedTime": "2019-08-24T14:15:22Z",
            "remediationId": "string",
            "tenantId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z"
          }
        ]
      },
      "metaDefenderCoreUrl": "string",
      "discoveryStartedDaySec": 0,
      "objectStorageMetadata": "string",
      "scanWorkflowSnapshotId": "string",
      "scanWorkflowSnapshot": {
        "id": "string",
        "scanId": "string",
        "workflow": {
          "id": "string",
          "scanPoolId": "string",
          "scanProcessFlow": 0,
          "isIdentityScanningEnabled": true,
          "scanIntervalDays": 0,
          "rules": [
            "string"
```

```
"type": 0,
          "workflowSupportedTechnologies": {
            "dlp": {
              "status": 0
            },
            "deepCdr": {
              "status": 0
            },
            "sandBox": {
              "status": 0
            },
            "metascan": {
              "status": 0
            }
          },
          "name": "string",
          "userAgent": "string",
          "scanPool": {
            "id": "string",
            "name": "string",
            "scanPoolType": 0,
            "isDefault": true,
            "scanInstances": [
              {
                "id": "string",
                "scanPoolId": "string",
                "url": "string",
                "apiKey": "string",
                "timeout": "string",
                "scanInstanceType": 0
              }
            ]
          },
          "failOverScanPoolId": "string",
          "failOverScanPool": {
            "id": "string",
            "name": "string",
            "scanPoolType": 0,
            "isDefault": true,
            "scanInstances": [
              {
                "id": "string",
                "scanPoolId": "string",
                "url": "string",
                "apiKey": "string",
                "timeout": "string",
                "scanInstanceType": 0
              }
            ]
          },
          "filters": {
            "id": "string",
            "minimumSize": 0,
```

```
"minimumDateTime": "2019-08-24T14:15:22Z",
            "maximumDateTime": "2019-08-24T14:15:22Z"
          },
          "fileDefinition": {
            "blockingStrategy": 0,
            "configurableBlockingStrategy": {
              "shouldTreatFilesWithSensitiveDataAsBlocked": true,
              "shouldTreatFilesWithVulnerabilitiesAsBlocked": true
            }
          },
          "remediations": [
            {
              "id": "string",
              "workflowId": "string",
              "isEnabled": true,
              "configuration": "string",
              "type": 0,
              "handlingType": 0
            }
          ],
          "tenantId": "string"
        },
        "startTimestamp": 0,
        "stopTimestamp": 0,
        "scanPool": {
          "id": "string",
          "name": "string",
          "scanPoolType": 0,
          "isDefault": true,
          "scanInstances": [
            {
              "id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ]
        },
        "scanInstances": [
          {
            "id": "string",
            "scanPoolId": "string",
            "url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ],
        "failOverScanPool": {
          "id": "string",
          "name": "string",
```

```
"isDefault": true,
          "scanInstances": [
            {
              "id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ]
        },
        "failOverScanInstances": [
          {
            "id": "string",
            "scanPoolId": "string",
            "url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ],
        "storage": {
          "id": "string",
          "name": "string",
          "groupId": "string",
          "clientId": "string",
          "accountId": "string",
          "source": "string",
          "storageFunctionality": "string",
          "storageType": {
            "name": "string",
            "categoryType": 0,
            "protocolType": 0,
            "vendorType": 0
          },
          "storageStatus": {
            "message": "string",
            "statusType": 0
          },
          "workflowId": "string",
          "lastUpdated": "2019-08-24T14:15:22Z",
          "tenantId": "string",
          "groupRef": {
            "id": "string",
            "name": "string"
          },
          "isAutodiscovered": true
        },
        "workflowStatistics": {
          "taggingStatistics": {
            "total": 0
          },
```

```
"total": 0
          },
          "keepBlockedStatistics": {
            "total": 0
          },
          "keepSanitizedStatistics": {
            "total": 0
          },
          "movedAllowedStatistics": {
            "total": 0,
            "destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
              "accountId": "string",
              "source": "string",
              "storageFunctionality": "string",
              "storageType": {
                "name": "string",
                "categoryType": 0,
                "protocolType": 0,
                "vendorType": 0
              },
              "storageStatus": {
                "message": "string",
                "statusType": 0
              },
              "workflowId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z",
              "tenantId": "string",
              "groupRef": {
                "id": "string",
                "name": "string"
              },
              "isAutodiscovered": true
            }
          },
          "movedSanitizedStatistics": {
            "total": 0,
            "destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
              "accountId": "string",
              "source": "string",
              "storageFunctionality": "string",
              "storageType": {
                "name": "string",
                "categoryType": 0,
                "protocolType": 0,
                "vendorType": 0
```

```
"storageStatus": {
                  "message": "string",
                  "statusType": 0
                },
                "workflowId": "string",
                "lastUpdated": "2019-08-24T14:15:22Z",
                "tenantId": "string",
                "groupRef": {
                  "id": "string",
                  "name": "string"
                },
                "isAutodiscovered": true
              }
            },
            "movedBlockedStatistics": {
              "total": 0,
              "destinationStorageInformation": {
                "id": "string",
                "name": "string",
                "groupId": "string",
                "clientId": "string",
                "accountId": "string",
                "source": "string",
                "storageFunctionality": "string",
                "storageType": {
                  "name": "string",
                  "categoryType": 0,
                  "protocolType": 0,
                  "vendorType": 0
                },
                "storageStatus": {
                  "message": "string",
                  "statusType": 0
                },
                "workflowId": "string",
                "lastUpdated": "2019-08-24T14:15:22Z",
                "tenantId": "string",
                "groupRef": {
                  "id": "string",
                  "name": "string"
                },
                "isAutodiscovered": true
              }
            },
            "copyAllowedStatistics": {
              "total": 0,
              "destinationStorageInformation": {
                "id": "string",
                "name": "string",
                "groupId": "string",
                "clientId": "string",
                "accountId": "string",
                "source": "string",
```

```
"storageType": {
                "name": "string",
                "categoryType": 0,
                "protocolType": 0,
                "vendorType": 0
              },
              "storageStatus": {
                "message": "string",
                "statusType": 0
              },
              "workflowId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z",
              "tenantId": "string",
              "groupRef": {
                "id": "string",
                "name": "string"
              },
              "isAutodiscovered": true
            }
          },
          "copyBlockedStatistics": {
            "total": 0,
            "destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
              "accountId": "string",
              "source": "string",
              "storageFunctionality": "string",
              "storageType": {
                "name": "string",
                "categoryType": 0,
                "protocolType": 0,
                "vendorType": 0
              },
              "storageStatus": {
                "message": "string",
                "statusType": 0
              },
              "workflowId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z",
              "tenantId": "string",
              "groupRef": {
                "id": "string",
                "name": "string"
              },
              "isAutodiscovered": true
            }
          },
          "deleteAllowedStatistics": {
            "total": 0
          },
```

```
"total": 0
          },
          "lastCalculatedStatisticsTime": "2019-08-24T14:15:22Z"
        },
        "account": {
          "id": "string",
          "name": "string",
          "description": "string",
          "credentials": "string",
          "protocolType": 0,
          "vendorType": 0,
          "autoDiscovery": true,
          "autodiscoveryDestinationGroupId": "string",
          "destinationGroup": {
            "id": "string",
            "name": "string"
          }
        },
        "realTimeStartDate": "2019-08-24T14:15:22Z"
      },
      "versions": [],
      "hasBlockedVersions": true,
      "versionsCount": 0,
      "objectType": 0,
      "skippedScan": true,
      "$type": "string",
      "url": "string",
      "fileId": "string"
    }
  ],
  "hasBlockedVersions": true,
  "versionsCount": 0,
  "objectType": 0,
  "skippedScan": true,
  "$type": "string",
  "url": "string",
  "fileId": "string"
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	File	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» url	string¦null	true	none	none
» fileId	string¦null	true	none	none

ObjectType

```
0
```

- 0: File
- 1: FileVersion

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: File - 1: FileVersion

Enumerated Values

Property	Value
anonymous	0
anonymous	1

FileBase

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "id": "string",
  "scanId": "string",
  "name": "string",
  "path": "string",
  "hash": "string",
  "fileOwner": {
    "userId": "string",
    "fullName": "string",
    "userName": "string",
    "emailAddress": "string"
  },
  "size": 0,
  "fileTypeCategory": 0,
  "extension": "string"
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» id	string	false	none	none
» scanId	string	false	none	none
» name	string	false	none	none
» path	string	false	none	none
» hash	string	false	none	none
» fileOwner	FileOwner	false	none	none
» size	integer(int64)	false	none	none
» fileTypeCategory	FileTypeCategory¦null	false	none	- 0: Other - 1: Archive - 2: Application - 3: Document - 4: EncryptedDocument - 5: Executable - 6: Graphical - 7: DiskImage - 8: AudioVideo - 9: OpenSslEncrypted - 10: Pdf - 11: Text - 12: MailMessage
» extension	string¦null	false	none	none

FileTypeCategory

```
0
```

- 0: Other
- 1: Archive
- 2: Application
- 3: Document
- 4: EncryptedDocument
- 5: Executable
- 6: Graphical
- 7: DiskImage

- 8: AudioVideo
- 9: OpenSslEncrypted
- 10: Pdf
- 11: Text
- 12: MailMessage

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: Other - 1: Archive - 2: Application - 3: Document - 4: EncryptedDocument - 5: Executable - 6: Graphical - 7: DiskImage - 8: AudioVideo - 9: OpenSslEncrypted - 10: Pdf - 11: Text - 12: MailMessage

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2
anonymous	3
anonymous	4
anonymous	5
anonymous	6
anonymous	7
anonymous	8
anonymous	9
anonymous	10
anonymous	11
anonymous	12

GetArchiveScanResultResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "archiveScanResults": [
    {
      "extractedFiles": {
        "dataId": "string",
        "scanResultI": 0,
        "detectedBy": 0,
        "filesExtractedCount": 0
      },
      "scanResults": {
        "scanDetails": [
          {
            "engineName": "string",
            "threatFound": "string",
            "scanResultI": 0,
            "defTime": "string",
            "scanTime": 0.1,
            "engId": "string",
            "waitTime": 0.1
          }
        ],
        "dataId": "string",
        "scanAllResultI": 0,
        "scanAllResultA": "string",
        "startTime": "string",
        "totalTime": 0.1,
        "totalAvs": 0,
        "totalDetections": 0,
        "progressPercentage": 0
      },
      "fileInfo": {
        "fileSize": 0,
        "uploadTimestamp": "string",
        "md5": "string",
        "sha1": "string",
        "sha256": "string",
        "fileTypeCategory": "string",
        "fileTypeDescription": "string",
        "fileTypeExtension": "string",
        "displayName": "string",
        "fileTypeId": "string"
      },
      "fileScanInfo": {
        "finalVerdict": {
          "blocked": true,
```

```
"confidence": 0.1,
          "threatLevel": 0.1
        },
        "overviewReport": {
          "analysisState": "string",
          "signalGroups": [
            {
              "description": "string",
              "verdict": "string",
              "signals": [
                {
                  "originType": "string",
                  "signalReadable": "string",
                  "strength": 0.1
                }
              ],
              "mitreTechniques": [
                {
                  "name": "string",
                  "tacticName": "string"
                }
              ]
            }
          ],
          "iocs": [
            {
              "data": "string",
              "type": "string",
              "origin": "string",
              "verdict": "string"
            }
          ],
          "yaraMatches": [
            {
              "ruleName": "string",
              "ruleDescription": "string",
              "verdict": "string",
              "matchedStrings": [
                "string"
              ],
              "author": "string",
              "version": "string",
              "threatLevel": 0.1,
              "confidence": 0.1,
              "strength": 0.1
            }
          ],
          "tags": [
            {
              "name": "string",
              "verdict": "string"
            }
          ],
```

```
"entropy": 0.1,
            "forensicAnalysisRecommended": true,
            "fuzzyFsioHash": "string"
          }
        },
        "errorCategory": "string",
        "errorCode": 0,
        "errorDetails": "string"
      },
      "processInfo": {
        "postProcessing": {
          "actionsRan": "string",
          "actionsFailed": "string",
          "convertedTo": "string",
          "copyMoveDestination": "string",
          "convertedDestination": "string",
          "sanitizationDetails": {
            "failureCategory": "string",
            "description": "string",
            "details": "string"
          }
        },
        "progressPercentage": 0,
        "userAgent": "string",
        "profile": "string",
        "result": "string",
        "blockedReason": "string",
        "fileTypeSkippedScan": true,
        "processingTime": 0.1,
        "queueTime": 0.1,
        "resultI": 0
      },
      "dataId": "string",
      "dlpInfo": {
        "hits": null,
        "verdict": 0
      },
      "sbomInfo": {
        "finalVerdict": {
          "blocked": true,
          "licensingPackageCounts": {
            "allowed": 0,
            "blocked": 0,
            "unknown": 0,
            "unsupported": 0
          },
          "severity": 0,
          "totalPackageCount": 0,
          "verdict": "string",
          "vulnerabilityCounts": {
            "critical": 0,
            "high": 0,
            "medium": 0,
```

```
"unknown": 0
          }
        },
        "overviewReport": {
          "isPartialReport": true,
          "osInfo": {
            "osName": "string",
            "osVersion": "string"
          },
          "scanMode": "string",
          "steps": [
            {
              "command": "string",
              "packages": [
                {
                  "authors": "string",
                  "releaseDate": "2019-08-24T14:15:22Z",
                  "ecosystem": "string",
                  "group": "string",
                  "archive": true,
                  "executable": true,
                  "uid": "string",
                  "licenses": {
                    "allowed": [
                      {
                        "id": "string",
                        "url": "string",
                        "category": "string",
                        "usageRestriction": {
                          "permissions": [
                            "string"
                          ],
                          "conditions": [
                            "string"
                          ],
                          "limitations": [
                            "string"
                          ]
                        }
                      }
                    ],
                    "blocked": [
                      {
                        "id": "string",
                        "url": "string",
                        "category": "string",
                        "usageRestriction": {
                          "permissions": [
                            "string"
                          ],
                          "conditions": [
                            "string"
                          ],
```

```
"string"
                            ]
                          }
                        }
                      ]
                    },
                    "packageName": "string",
                    "packageVersion": "string",
                    "hashes": [
                      {
                        "sha256": "string",
                        "fileName": "string"
                      }
                    ],
                    "vulnerabilityCounts": {
                      "critical": 0,
                      "high": 0,
                      "medium": 0,
                      "low": 0,
                      "unknown": 0
                    },
                    "vulnerabilities": [
                      {
                        "id": "string",
                        "severity": 0,
                        "source": "string",
                        "fixedVersions": "string",
                        "cwes": [
                          "string"
                        ]
                      }
                    ],
                    "arch": "string",
                    "osName": "string",
                    "osVersion": "string",
                    "dependencies": [
                      {
                        "ecosystem": "string",
                        "group": "string",
                        "packageName": "string",
                        "packageVersion": "string",
                        "vulnerabilities": [
                          {
                            "id": "string",
                            "severity": 0,
                            "source": "string",
                            "fixedVersions": "string",
                            "cwes": [
                              "string"
                            ]
                          }
                        ],
                        "vulnerabilityCounts": {
```

```
"high": 0,
                        "medium": 0,
                        "low": 0,
                        "unknown": 0
                      }
                    }
                  ]
                }
              ],
              "licenseStatus": "string",
              "licensingPackageCounts": {
                "allowed": 0,
                "blocked": 0,
                "unknown": 0,
                "unsupported": 0
              },
              "step": 0,
              "vulnerabilityCount": 0,
              "sha256": "string",
              "severity": 0,
              "vulnerabilityCounts": {
                "critical": 0,
                "high": 0,
                "medium": 0,
                "low": 0,
                "unknown": 0
              }
            }
          ],
          "packages": [
            {
              "authors": "string",
              "releaseDate": "2019-08-24T14:15:22Z",
              "ecosystem": "string",
              "group": "string",
              "archive": true,
              "executable": true,
              "uid": "string",
              "licenses": {
                "allowed": [
                  {
                    "id": "string",
                    "url": "string",
                    "category": "string",
                    "usageRestriction": {
                      "permissions": [
                        "string"
                      ],
                      "conditions": [
                        "string"
                      ],
                      "limitations": [
                        "string"
```

```
}
                    }
                  ],
                  "blocked": [
                    {
                      "id": "string",
                      "url": "string",
                      "category": "string",
                      "usageRestriction": {
                        "permissions": [
                          "string"
                        ],
                        "conditions": [
                          "string"
                        ],
                        "limitations": [
                          "string"
                        ]
                      }
                    }
                  ]
                },
                "packageName": "string",
                "packageVersion": "string",
                "target": "string",
                "hashes": [
                  {
                    "sha256": "string",
                    "fileName": "string"
                  }
                ],
                "vulnerabilities": [
                  {
                    "id": "string",
                    "severity": 0,
                    "source": "string",
                    "fixedVersions": "string",
                    "cwes": [
                      "string"
                    ]
                  }
                ],
                "vulnerabilityCounts": {
                  "critical": 0,
                  "high": 0,
                  "medium": 0,
                  "low": 0,
                  "unknown": 0
                },
                "dependencies": [
                  {
                    "ecosystem": "string",
                    "group": "string",
```

```
"packageVersion": "string",
                  "vulnerabilities": [
                    {
                      "id": "string",
                      "severity": 0,
                      "source": "string",
                      "fixedVersions": "string",
                      "cwes": [
                        "string"
                      ]
                    }
                  ],
                  "vulnerabilityCounts": {
                    "critical": 0,
                    "high": 0,
                    "medium": 0,
                    "low": 0,
                    "unknown": 0
                  }
                }
              ]
            }
          ],
          "dependenciesPackageCount": 0,
          "dependenciesVulnerabilityTotal": 0,
          "dependenciesVulnerabilityCounts": {
            "critical": 0,
            "high": 0,
            "medium": 0,
            "low": 0,
            "unknown": 0
          }
        },
        "resultTemplateHash": "string"
      },
      "vulnerabilityInfo": {
        "vulnerabilityInfoResult": {
          "code": 0,
          "hash": "string",
          "method": 0,
          "timeStamp": "string",
          "timing": 0,
          "detectedProduct": {
            "hasVulnerability": true,
            "isCurrent": true,
            "product": {
              "id": 0,
              "name": "string"
            },
            "remediationLink": "string",
            "severity": "string",
            "sigName": "string",
            "signature": 0,
```

```
"id": 0,
              "name": "string"
            },
            "version": "string",
            "versionData": {
              "countBehind": 0,
              "feedId": 0,
              "version": "string"
            },
            "vulnerabilities": [
              {
                "description": "string",
                "details": {
                  "cpe": "string",
                  "cve": "string",
                  "cvss": {
                    "accessComplexity": "string",
                    "accessVector": "string",
                    "authentication": "string",
                    "availabilityImpact": "string",
                    "confidentialityImpact": "string",
                    "generatedOnEpoch": "string",
                    "integrityImpact": "string",
                    "score": "string",
                    "source": "string"
                  },
                  "cvss3": {
                    "attackComplexity": "string",
                    "attackVector": "string",
                    "availabilityImpact": "string",
                    "baseScore": "string",
                    "baseSeverity": "string",
                    "confidentialityImpact": "string",
                    "exploitabilityScore": "string",
                    "impactScore": "string",
                    "integrityImpact": "string",
                    "privilegesRequired": "string",
                    "scope": "string",
                    "userInteraction": "string",
                    "vectorString": "string"
                  },
                  "cwe": "string",
                  "lastModifiedEpoch": "string",
                  "publishedEpoch": "string",
                  "references": [
                    "string"
                  ]
                },
                "severity": "string",
                "severityIndex": 0,
                "staticId": 0
              }
            ]
```

```
}
      },
      "sessionCookie": "string",
      "fileTypeInfo": {
        "fileInfoExtended": {
          "extensions": "string",
          "groupId": "string",
          "typeId": "string"
        }
      },
      "scanInstanceUrl": "string",
      "scanWorkflowSnapshotId": "string",
      "coreEngines": [
        {
          "engineId": "string",
          "engineName": "string",
          "engineVersion": "string",
          "dbVersion": "string",
          "definitionTime": "string"
        }
      ]
    }
  ]
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» archiveScanResults	[CoreScanResult]	true	none	none

EnumerateFiles

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "entries": [
    {
      "result": 0,
      "responseKey": "string",
      "responseMessage": "string",
      "responseMessageParams": {
        "property1": "string",
        "property2": "string"
      },
      "id": "string",
      "scanId": "string",
      "name": "string",
      "path": "string",
      "hash": "string",
      "fileOwner": {
        "userId": "string",
        "fullName": "string",
        "userName": "string",
        "emailAddress": "string"
      },
      "size": 0,
      "fileTypeCategory": 0,
      "extension": "string",
      "storageType": {
        "name": "string",
        "categoryType": 0,
        "protocolType": 0,
        "vendorType": 0
      },
      "storageName": "string",
      "storageLocation": "string",
      "scanName": "string",
      "progress": {
        "upload": 0,
        "scan": 0,
        "archiveExtraction": 0
      },
      "scanResult": {
        "extractedFiles": {
          "dataId": "string",
          "scanResultI": 0,
          "detectedBy": 0,
          "filesExtractedCount": 0
        },
```

```
"scanDetails": [
            {
              "engineName": "string",
              "threatFound": "string",
              "scanResultI": 0,
              "defTime": "string",
              "scanTime": 0.1,
              "engId": "string",
              "waitTime": 0.1
            }
          ],
          "dataId": "string",
          "scanAllResultI": 0,
          "scanAllResultA": "string",
          "startTime": "string",
          "totalTime": 0.1,
          "totalAvs": 0,
          "totalDetections": 0,
          "progressPercentage": 0
        },
        "fileInfo": {
          "fileSize": 0,
          "uploadTimestamp": "string",
          "md5": "string",
          "sha1": "string",
          "sha256": "string",
          "fileTypeCategory": "string",
          "fileTypeDescription": "string",
          "fileTypeExtension": "string",
          "displayName": "string",
          "fileTypeId": "string"
        },
        "fileScanInfo": {
          "finalVerdict": {
            "blocked": true,
            "verdict": "string",
            "confidence": 0.1,
            "threatLevel": 0.1
          },
          "overviewReport": {
            "analysisState": "string",
            "signalGroups": [
              {
                "description": "string",
                "verdict": "string",
                "signals": [
                  {
                    "originType": "string",
                    "signalReadable": "string",
                    "strength": 0.1
                  }
                ],
                "mitreTechniques": [
```

```
"name": "string",
                    "tacticName": "string"
                  }
                ]
              }
            ],
            "iocs": [
              {
                "data": "string",
                "type": "string",
                "origin": "string",
                "verdict": "string"
              }
            ],
            "yaraMatches": [
              {
                "ruleName": "string",
                "ruleDescription": "string",
                "verdict": "string",
                "matchedStrings": [
                  "string"
                ],
                "author": "string",
                "version": "string",
                "threatLevel": 0.1,
                "confidence": 0.1,
                "strength": 0.1
              }
            ],
            "tags": [
              {
                "name": "string",
                "verdict": "string"
              }
            ],
            "metaData": {
              "entropy": 0.1,
              "forensicAnalysisRecommended": true,
              "fuzzyFsioHash": "string"
            }
          },
          "errorCategory": "string",
          "errorCode": 0,
          "errorDetails": "string"
        },
        "processInfo": {
          "postProcessing": {
            "actionsRan": "string",
            "actionsFailed": "string",
            "convertedTo": "string",
            "copyMoveDestination": "string",
            "convertedDestination": "string",
            "sanitizationDetails": {
```

```
"description": "string",
              "details": "string"
            }
          },
          "progressPercentage": 0,
          "userAgent": "string",
          "profile": "string",
          "result": "string",
          "blockedReason": "string",
          "fileTypeSkippedScan": true,
          "processingTime": 0.1,
          "queueTime": 0.1,
          "resultI": 0
        },
        "dataId": "string",
        "dlpInfo": {
          "hits": null,
          "verdict": 0
        },
        "sbomInfo": {
          "finalVerdict": {
            "blocked": true,
            "licensingPackageCounts": {
              "allowed": 0,
              "blocked": 0,
              "unknown": 0,
              "unsupported": 0
            },
            "severity": 0,
            "totalPackageCount": 0,
            "verdict": "string",
            "vulnerabilityCounts": {
              "critical": 0,
              "high": 0,
              "medium": 0,
              "low": 0,
              "unknown": 0
            }
          },
          "overviewReport": {
            "isPartialReport": true,
            "osInfo": {
              "osName": "string",
              "osVersion": "string"
            },
            "scanMode": "string",
            "steps": [
              {
                "command": "string",
                "packages": [
                  {
                    "authors": "string",
                    "releaseDate": "2019-08-24T14:15:22Z",
```

```
"group": "string",
                    "archive": true,
                    "executable": true,
                    "uid": "string",
                    "licenses": {
                      "allowed": [
                        {
                          "id": "string",
                          "url": "string",
                          "category": "string",
                          "usageRestriction": {
                            "permissions": [
                              null
                            ],
                            "conditions": [
                              null
                            ],
                            "limitations": [
                              null
                            ]
                          }
                        }
                      ],
                      "blocked": [
                        {
                          "id": "string",
                          "url": "string",
                          "category": "string",
                          "usageRestriction": {
                            "permissions": [
                              null
                            ],
                            "conditions": [
                              null
                            ],
                            "limitations": [
                              null
                            ]
                          }
                        }
                      ]
                    },
                    "packageName": "string",
                    "packageVersion": "string",
                    "hashes": [
                      {
                        "sha256": "string",
                        "fileName": "string"
                      }
                    ],
                    "vulnerabilityCounts": {
                      "critical": 0,
                      "high": 0,
```

```
"low": 0,
                    "unknown": 0
                  },
                  "vulnerabilities": [
                    {
                      "id": "string",
                      "severity": 0,
                      "source": "string",
                      "fixedVersions": "string",
                      "cwes": [
                        "string"
                      ]
                    }
                  ],
                  "arch": "string",
                  "osName": "string",
                  "osVersion": "string",
                  "dependencies": [
                    {
                      "ecosystem": "string",
                      "group": "string",
                      "packageName": "string",
                      "packageVersion": "string",
                      "vulnerabilities": [
                        {
                          "id": "string",
                          "severity": 0,
                          "source": "string",
                          "fixedVersions": "string",
                          "cwes": [
                            null
                          ]
                        }
                      ],
                      "vulnerabilityCounts": {
                        "critical": 0,
                        "high": 0,
                        "medium": 0,
                        "low": 0,
                        "unknown": 0
                      }
                    }
                  ]
                }
              ],
              "licenseStatus": "string",
              "licensingPackageCounts": {
                "allowed": 0,
                "blocked": 0,
                "unknown": 0,
                "unsupported": 0
              },
              "step": 0,
```

```
"sha256": "string",
                "severity": 0,
                "vulnerabilityCounts": {
                  "critical": 0,
                  "high": 0,
                  "medium": 0,
                  "low": 0,
                  "unknown": 0
                }
              }
            ],
            "packages": [
              {
                "authors": "string",
                "releaseDate": "2019-08-24T14:15:22Z",
                "ecosystem": "string",
                "group": "string",
                "archive": true,
                "executable": true,
                "uid": "string",
                "licenses": {
                  "allowed": [
                    {
                      "id": "string",
                      "url": "string",
                      "category": "string",
                      "usageRestriction": {
                        "permissions": [
                          "string"
                        ],
                        "conditions": [
                          "string"
                        ],
                        "limitations": [
                          "string"
                        ]
                      }
                    }
                  ],
                  "blocked": [
                    {
                      "id": "string",
                      "url": "string",
                      "category": "string",
                      "usageRestriction": {
                        "permissions": [
                          "string"
                        ],
                        "conditions": [
                          "string"
                        ],
                        "limitations": [
                          "string"
```

```
}
                    }
                  ]
                },
                "packageName": "string",
                "packageVersion": "string",
                "target": "string",
                "hashes": [
                  {
                    "sha256": "string",
                    "fileName": "string"
                  }
                ],
                "vulnerabilities": [
                  {
                    "id": "string",
                    "severity": 0,
                    "source": "string",
                    "fixedVersions": "string",
                    "cwes": [
                      "string"
                    ]
                  }
                ],
                "vulnerabilityCounts": {
                  "critical": 0,
                  "high": 0,
                  "medium": 0,
                  "low": 0,
                  "unknown": 0
                },
                "dependencies": [
                  {
                    "ecosystem": "string",
                    "group": "string",
                    "packageName": "string",
                    "packageVersion": "string",
                    "vulnerabilities": [
                      {
                        "id": "string",
                        "severity": 0,
                        "source": "string",
                        "fixedVersions": "string",
                        "cwes": [
                          "string"
                        ]
                      }
                    ],
                    "vulnerabilityCounts": {
                      "critical": 0,
                      "high": 0,
                      "medium": 0,
                      "low": 0,
```

```
}
                    }
                  ]
                }
              ],
              "dependenciesPackageCount": 0,
              "dependenciesVulnerabilityTotal": 0,
              "dependenciesVulnerabilityCounts": {
                "critical": 0,
                "high": 0,
                "medium": 0,
                "low": 0,
                "unknown": 0
              }
            },
            "resultTemplateHash": "string"
          },
          "vulnerabilityInfo": {
            "vulnerabilityInfoResult": {
              "code": 0,
              "hash": "string",
              "method": 0,
              "timeStamp": "string",
              "timing": 0,
              "detectedProduct": {
                "hasVulnerability": true,
                "isCurrent": true,
                "product": {
                  "id": 0,
                  "name": "string"
                },
                "remediationLink": "string",
                "severity": "string",
                "sigName": "string",
                "signature": 0,
                "vendor": {
                  "id": 0,
                  "name": "string"
                },
                "version": "string",
                "versionData": {
                  "countBehind": 0,
                  "feedId": 0,
                  "version": "string"
                },
                "vulnerabilities": [
                  {
                    "description": "string",
                    "details": {
                      "cpe": "string",
                      "cve": "string",
                      "cvss": {
                        "accessComplexity": "string",
```

```
"authentication": "string",
                    "availabilityImpact": "string",
                    "confidentialityImpact": "string",
                    "generatedOnEpoch": "string",
                    "integrityImpact": "string",
                    "score": "string",
                    "source": "string"
                  },
                  "cvss3": {
                    "attackComplexity": "string",
                    "attackVector": "string",
                    "availabilityImpact": "string",
                    "baseScore": "string",
                    "baseSeverity": "string",
                    "confidentialityImpact": "string",
                    "exploitabilityScore": "string",
                    "impactScore": "string",
                    "integrityImpact": "string",
                    "privilegesRequired": "string",
                    "scope": "string",
                    "userInteraction": "string",
                    "vectorString": "string"
                  },
                  "cwe": "string",
                  "lastModifiedEpoch": "string",
                  "publishedEpoch": "string",
                  "references": [
                    "string"
                  ]
                },
                "severity": "string",
                "severityIndex": 0,
                "staticId": 0
              }
            ]
          }
        }
      },
      "sessionCookie": "string",
      "fileTypeInfo": {
        "fileInfoExtended": {
          "extensions": "string",
          "groupId": "string",
          "typeId": "string"
        }
      },
      "scanInstanceUrl": "string",
      "scanWorkflowSnapshotId": "string",
      "coreEngines": [
        {
          "engineId": "string",
          "engineName": "string",
          "engineVersion": "string",
```

```
"definitionTime": "string"
          }
        ]
      },
      "processingState": 0,
      "exception": {
        "exceptionDetails": "string",
        "exceptionMessage": "string"
      },
      "created": "2019-08-24T14:15:22Z",
      "lastModified": "2019-08-24T14:15:22Z",
      "discoveryStarted": "2019-08-24T14:15:22Z",
      "fileProcessingDetails": {
        "streamingStartedTime": "2019-08-24T14:15:22Z",
        "streamingCompletedTime": "2019-08-24T14:15:22Z",
        "streamingTimeSpanMs": 0,
        "scanCompletedTime": "2019-08-24T14:15:22Z",
        "processingTimeSpanMs": 0
      },
      "coreEngines": [
        {
          "engineId": "string",
          "engineName": "string",
          "engineVersion": "string",
          "dbVersion": "string",
          "definitionTime": "string"
        }
      ],
      "remediation": {
        "deepCdr": {
          "sanitizationDetails": {
            "failureCategory": "string",
            "description": "string",
            "details": "string"
          },
          "cdrObjectState": 0,
          "fileWasReplaced": true
        },
        "postActionFailedInformation": [
          {
            "objectActionType": 0,
            "exception": {
              "exceptionDetails": "string",
              "exceptionMessage": "string"
            }
          }
        ],
        "objectRemediationActions": [
          {
            "objectActionType": 0,
            "objectActionState": 0,
            "cdrObjectState": 0,
            "exceptions": [
```

```
],
            "id": "string",
            "fileId": "string",
            "fileScanCompletedTime": "2019-08-24T14:15:22Z",
            "remediationId": "string",
            "tenantId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z"
          }
        ]
      },
      "metaDefenderCoreUrl": "string",
      "discoveryStartedDaySec": 0,
      "objectStorageMetadata": "string",
      "scanWorkflowSnapshotId": "string",
      "scanWorkflowSnapshot": {
        "id": "string",
        "scanId": "string",
        "workflow": {
          "id": "string",
          "scanPoolId": "string",
          "scanProcessFlow": 0,
          "isIdentityScanningEnabled": true,
          "scanIntervalDays": 0,
          "rules": [
            "string"
          ],
          "type": 0,
          "workflowSupportedTechnologies": {
            "dlp": {
              "status": 0
            },
            "deepCdr": {
              "status": 0
            },
            "sandBox": {
              "status": 0
            },
            "metascan": {
              "status": 0
            }
          },
          "name": "string",
          "userAgent": "string",
          "scanPool": {
            "id": "string",
            "name": "string",
            "scanPoolType": 0,
            "isDefault": true,
            "scanInstances": [
              {
                "id": "string",
                "scanPoolId": "string",
                "url": "string",
```

```
"timeout": "string",
                "scanInstanceType": 0
              }
            ]
          },
          "failOverScanPoolId": "string",
          "failOverScanPool": {
            "id": "string",
            "name": "string",
            "scanPoolType": 0,
            "isDefault": true,
            "scanInstances": [
              {
                "id": "string",
                "scanPoolId": "string",
                "url": "string",
                "apiKey": "string",
                "timeout": "string",
                "scanInstanceType": 0
              }
            ]
          },
          "filters": {
            "id": "string",
            "minimumSize": 0,
            "maximumSize": 0,
            "minimumDateTime": "2019-08-24T14:15:22Z",
            "maximumDateTime": "2019-08-24T14:15:22Z"
          },
          "fileDefinition": {
            "blockingStrategy": 0,
            "configurableBlockingStrategy": {
              "shouldTreatFilesWithSensitiveDataAsBlocked": true,
              "shouldTreatFilesWithVulnerabilitiesAsBlocked": true
            }
          },
          "remediations": [
            {
              "id": "string",
              "workflowId": "string",
              "isEnabled": true,
              "configuration": "string",
              "type": 0,
              "handlingType": 0
            }
          ],
          "tenantId": "string"
        },
        "startTimestamp": 0,
        "stopTimestamp": 0,
        "scanPool": {
          "id": "string",
          "name": "string",
```

```
"isDefault": true,
          "scanInstances": [
            {
              "id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ]
        },
        "scanInstances": [
          {
            "id": "string",
            "scanPoolId": "string",
            "url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ],
        "failOverScanPool": {
          "id": "string",
          "name": "string",
          "scanPoolType": 0,
          "isDefault": true,
          "scanInstances": [
            {
              "id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ]
        },
        "failOverScanInstances": [
          {
            "id": "string",
            "scanPoolId": "string",
            "url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ],
        "storage": {
          "id": "string",
          "name": "string",
          "groupId": "string",
          "clientId": "string",
```

```
"source": "string",
          "storageFunctionality": "string",
          "storageType": {
            "name": "string",
            "categoryType": 0,
            "protocolType": 0,
            "vendorType": 0
          },
          "storageStatus": {
            "message": "string",
            "statusType": 0
          },
          "workflowId": "string",
          "lastUpdated": "2019-08-24T14:15:22Z",
          "tenantId": "string",
          "groupRef": {
            "id": "string",
            "name": "string"
          },
          "isAutodiscovered": true
        },
        "workflowStatistics": {
          "taggingStatistics": {
            "total": 0
          },
          "keepAllowedStatistics": {
            "total": 0
          },
          "keepBlockedStatistics": {
            "total": 0
          },
          "keepSanitizedStatistics": {
            "total": 0
          },
          "movedAllowedStatistics": {
            "total": 0,
            "destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
              "accountId": "string",
              "source": "string",
              "storageFunctionality": "string",
              "storageType": {
                "name": "string",
                "categoryType": 0,
                "protocolType": 0,
                "vendorType": 0
              },
              "storageStatus": {
                "message": "string",
                "statusType": 0
```

```
"workflowId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z",
              "tenantId": "string",
              "groupRef": {
                "id": "string",
                "name": "string"
              },
              "isAutodiscovered": true
            }
          },
          "movedSanitizedStatistics": {
            "total": 0,
            "destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
              "accountId": "string",
              "source": "string",
              "storageFunctionality": "string",
              "storageType": {
                "name": "string",
                "categoryType": 0,
                "protocolType": 0,
                "vendorType": 0
              },
              "storageStatus": {
                "message": "string",
                "statusType": 0
              },
              "workflowId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z",
              "tenantId": "string",
              "groupRef": {
                "id": "string",
                "name": "string"
              },
              "isAutodiscovered": true
            }
          },
          "movedBlockedStatistics": {
            "total": 0,
            "destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
              "accountId": "string",
              "source": "string",
              "storageFunctionality": "string",
              "storageType": {
                "name": "string",
                "categoryType": 0,
```

```
"vendorType": 0
              },
              "storageStatus": {
                "message": "string",
                "statusType": 0
              },
              "workflowId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z",
              "tenantId": "string",
              "groupRef": {
                "id": "string",
                "name": "string"
              },
              "isAutodiscovered": true
            }
          },
          "copyAllowedStatistics": {
            "total": 0,
            "destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
              "accountId": "string",
              "source": "string",
              "storageFunctionality": "string",
              "storageType": {
                "name": "string",
                "categoryType": 0,
                "protocolType": 0,
                "vendorType": 0
              },
              "storageStatus": {
                "message": "string",
                "statusType": 0
              },
              "workflowId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z",
              "tenantId": "string",
              "groupRef": {
                "id": "string",
                "name": "string"
              },
              "isAutodiscovered": true
            }
          },
          "copyBlockedStatistics": {
            "total": 0,
            "destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
```

```
"source": "string",
              "storageFunctionality": "string",
              "storageType": {
                "name": "string",
                "categoryType": 0,
                "protocolType": 0,
                "vendorType": 0
              },
              "storageStatus": {
                "message": "string",
                "statusType": 0
              },
              "workflowId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z",
              "tenantId": "string",
              "groupRef": {
                "id": "string",
                "name": "string"
              },
              "isAutodiscovered": true
            }
          },
          "deleteAllowedStatistics": {
            "total": 0
          },
          "deleteBlockedStatistics": {
            "total": 0
          },
          "lastCalculatedStatisticsTime": "2019-08-24T14:15:22Z"
        },
        "account": {
          "id": "string",
          "name": "string",
          "description": "string",
          "credentials": "string",
          "protocolType": 0,
          "vendorType": 0,
          "autoDiscovery": true,
          "autodiscoveryDestinationGroupId": "string",
          "destinationGroup": {
            "id": "string",
            "name": "string"
          }
        },
        "realTimeStartDate": "2019-08-24T14:15:22Z"
      },
      "versions": [
        {
          "result": 0,
          "responseKey": "string",
          "responseMessage": "string",
          "responseMessageParams": {
            "property1": "string",
```

```
},
          "id": "string",
          "scanId": "string",
          "name": "string",
          "path": "string",
          "hash": "string",
          "fileOwner": {
            "userId": "string",
            "fullName": "string",
            "userName": "string",
            "emailAddress": "string"
          },
          "size": 0,
          "fileTypeCategory": 0,
          "extension": "string",
          "storageType": {
            "name": "string",
            "categoryType": 0,
            "protocolType": 0,
            "vendorType": 0
          },
          "storageName": "string",
          "storageLocation": "string",
          "scanName": "string",
          "progress": {
            "upload": 0,
            "scan": 0,
            "archiveExtraction": 0
          },
          "scanResult": {
            "extractedFiles": {
              "dataId": "string",
              "scanResultI": 0,
              "detectedBy": 0,
              "filesExtractedCount": 0
            },
            "scanResults": {
              "scanDetails": [
                {
                  "engineName": "string",
                  "threatFound": "string",
                  "scanResultI": 0,
                  "defTime": "string",
                  "scanTime": 0.1,
                  "engId": "string",
                  "waitTime": 0.1
                }
              ],
              "dataId": "string",
              "scanAllResultI": 0,
              "scanAllResultA": "string",
              "startTime": "string",
              "totalTime": 0.1,
```

```
"totalDetections": 0,
              "progressPercentage": 0
            },
            "fileInfo": {
              "fileSize": 0,
              "uploadTimestamp": "string",
              "md5": "string",
              "sha1": "string",
              "sha256": "string",
              "fileTypeCategory": "string",
              "fileTypeDescription": "string",
              "fileTypeExtension": "string",
              "displayName": "string",
              "fileTypeId": "string"
            },
            "fileScanInfo": {
              "finalVerdict": {
                "blocked": true,
                "verdict": "string",
                "confidence": 0.1,
                "threatLevel": 0.1
              },
              "overviewReport": {
                "analysisState": "string",
                "signalGroups": [
                  {
                    "description": "string",
                    "verdict": "string",
                    "signals": [
                      {
                        "originType": "string",
                        "signalReadable": "string",
                        "strength": 0.1
                      }
                    ],
                    "mitreTechniques": [
                      {
                        "name": "string",
                        "tacticName": "string"
                      }
                    ]
                  }
                ],
                "iocs": [
                  {
                    "data": "string",
                    "type": "string",
                    "origin": "string",
                    "verdict": "string"
                  }
                ],
                "yaraMatches": [
                  {
```

```
"ruleDescription": "string",
                    "verdict": "string",
                    "matchedStrings": [
                      "string"
                    ],
                    "author": "string",
                    "version": "string",
                    "threatLevel": 0.1,
                    "confidence": 0.1,
                    "strength": 0.1
                  }
                ],
                "tags": [
                  {
                    "name": "string",
                    "verdict": "string"
                  }
                ],
                "metaData": {
                  "entropy": 0.1,
                  "forensicAnalysisRecommended": true,
                  "fuzzyFsioHash": "string"
                }
              },
              "errorCategory": "string",
              "errorCode": 0,
              "errorDetails": "string"
            },
            "processInfo": {
              "postProcessing": {
                "actionsRan": "string",
                "actionsFailed": "string",
                "convertedTo": "string",
                "copyMoveDestination": "string",
                "convertedDestination": "string",
                "sanitizationDetails": {
                  "failureCategory": "string",
                  "description": "string",
                  "details": "string"
                }
              },
              "progressPercentage": 0,
              "userAgent": "string",
              "profile": "string",
              "result": "string",
              "blockedReason": "string",
              "fileTypeSkippedScan": true,
              "processingTime": 0.1,
              "queueTime": 0.1,
              "resultI": 0
            },
            "dataId": "string",
            "dlpInfo": {
```

```
"verdict": 0
            },
            "sbomInfo": {
              "finalVerdict": {
                "blocked": true,
                "licensingPackageCounts": {
                  "allowed": 0,
                  "blocked": 0,
                  "unknown": 0,
                  "unsupported": 0
                },
                "severity": 0,
                "totalPackageCount": 0,
                "verdict": "string",
                "vulnerabilityCounts": {
                  "critical": 0,
                  "high": 0,
                  "medium": 0,
                  "low": 0,
                  "unknown": 0
                }
              },
              "overviewReport": {
                "isPartialReport": true,
                "osInfo": {
                  "osName": "string",
                  "osVersion": "string"
                },
                "scanMode": "string",
                "steps": [
                  {
                    "command": "string",
                    "packages": [
                      {
                        "authors": "string",
                        "releaseDate": "2019-08-24T14:15:22Z",
                        "ecosystem": "string",
                        "group": "string",
                        "archive": true,
                        "executable": true,
                        "uid": "string",
                        "licenses": {
                          "allowed": [
                            {}
                          ],
                          "blocked": [
                            {}
                          ]
                        },
                        "packageName": "string",
                        "packageVersion": "string",
                        "hashes": [
                          {
```

```
"fileName": "string"
                        }
                      ],
                      "vulnerabilityCounts": {
                        "critical": 0,
                        "high": 0,
                        "medium": 0,
                        "low": 0,
                        "unknown": 0
                      },
                      "vulnerabilities": [
                        {
                          "id": "string",
                          "severity": 0,
                          "source": "string",
                          "fixedVersions": "string",
                          "cwes": [
                            null
                          ]
                        }
                      ],
                      "arch": "string",
                      "osName": "string",
                      "osVersion": "string",
                      "dependencies": [
                        {
                          "ecosystem": "string",
                          "group": "string",
                          "packageName": "string",
                          "packageVersion": "string",
                          "vulnerabilities": [
                            null
                          ],
                          "vulnerabilityCounts": {}
                        }
                      ]
                    }
                  ],
                  "licenseStatus": "string",
                  "licensingPackageCounts": {
                    "allowed": 0,
                    "blocked": 0,
                    "unknown": 0,
                    "unsupported": 0
                  },
                  "step": 0,
                  "vulnerabilityCount": 0,
                  "sha256": "string",
                  "severity": 0,
                  "vulnerabilityCounts": {
                    "critical": 0,
                    "high": 0,
                    "medium": 0,
```

```
"unknown": 0
                    }
                  }
                ],
                "packages": [
                  {
                    "authors": "string",
                    "releaseDate": "2019-08-24T14:15:22Z",
                    "ecosystem": "string",
                    "group": "string",
                    "archive": true,
                    "executable": true,
                    "uid": "string",
                    "licenses": {
                      "allowed": [
                        {
                          "id": "string",
                          "url": "string",
                          "category": "string",
                          "usageRestriction": {
                            "permissions": [
                              null
                            ],
                            "conditions": [
                              null
                            ],
                            "limitations": [
                              null
                            ]
                          }
                        }
                      ],
                      "blocked": [
                        {
                          "id": "string",
                          "url": "string",
                          "category": "string",
                          "usageRestriction": {
                            "permissions": [
                              null
                            ],
                            "conditions": [
                              null
                            ],
                            "limitations": [
                              null
                            ]
                          }
                        }
                      ]
                    },
                    "packageName": "string",
                    "packageVersion": "string",
```

```
"hashes": [
                        {
                          "sha256": "string",
                          "fileName": "string"
                        }
                      ],
                      "vulnerabilities": [
                        {
                          "id": "string",
                          "severity": 0,
                          "source": "string",
                          "fixedVersions": "string",
                          "cwes": [
                            "string"
                          ]
                        }
                      ],
                      "vulnerabilityCounts": {
                        "critical": 0,
                        "high": 0,
                        "medium": 0,
                        "low": 0,
                        "unknown": 0
                      },
                      "dependencies": [
                        {
                          "ecosystem": "string",
                          "group": "string",
                          "packageName": "string",
                          "packageVersion": "string",
                          "vulnerabilities": [
                            {
                              "id": "string",
                              "severity": 0,
                              "source": "string",
                              "fixedVersions": "string",
                              "cwes": [
                                null
                              ]
                            }
                          ],
                          "vulnerabilityCounts": {
                            "critical": 0,
                            "high": 0,
                            "medium": 0,
                            "low": 0,
                            "unknown": 0
                          }
                        }
                      ]
                    }
                  ],
                  "dependenciesPackageCount": 0,
```

```
"dependenciesVulnerabilityCounts": {
                  "critical": 0,
                  "high": 0,
                  "medium": 0,
                  "low": 0,
                  "unknown": 0
                }
              },
              "resultTemplateHash": "string"
            },
            "vulnerabilityInfo": {
              "vulnerabilityInfoResult": {
                "code": 0,
                "hash": "string",
                "method": 0,
                "timeStamp": "string",
                "timing": 0,
                "detectedProduct": {
                  "hasVulnerability": true,
                  "isCurrent": true,
                  "product": {
                    "id": 0,
                    "name": "string"
                  },
                  "remediationLink": "string",
                  "severity": "string",
                  "sigName": "string",
                  "signature": 0,
                  "vendor": {
                    "id": 0,
                    "name": "string"
                  },
                  "version": "string",
                  "versionData": {
                    "countBehind": 0,
                    "feedId": 0,
                    "version": "string"
                  },
                  "vulnerabilities": [
                    {
                      "description": "string",
                      "details": {
                        "cpe": "string",
                        "cve": "string",
                        "cvss": {
                          "accessComplexity": "string",
                          "accessVector": "string",
                          "authentication": "string",
                          "availabilityImpact": "string",
                          "confidentialityImpact": "string",
                          "generatedOnEpoch": "string",
                          "integrityImpact": "string",
                          "score": "string",
```

```
},
                        "cvss3": {
                          "attackComplexity": "string",
                          "attackVector": "string",
                          "availabilityImpact": "string",
                          "baseScore": "string",
                          "baseSeverity": "string",
                          "confidentialityImpact": "string",
                          "exploitabilityScore": "string",
                          "impactScore": "string",
                          "integrityImpact": "string",
                          "privilegesRequired": "string",
                          "scope": "string",
                          "userInteraction": "string",
                          "vectorString": "string"
                        },
                        "cwe": "string",
                        "lastModifiedEpoch": "string",
                        "publishedEpoch": "string",
                        "references": [
                          "string"
                        ]
                      },
                      "severity": "string",
                      "severityIndex": 0,
                      "staticId": 0
                    }
                  ]
                }
              }
            },
            "sessionCookie": "string",
            "fileTypeInfo": {
              "fileInfoExtended": {
                "extensions": "string",
                "groupId": "string",
                "typeId": "string"
              }
            },
            "scanInstanceUrl": "string",
            "scanWorkflowSnapshotId": "string",
            "coreEngines": [
              {
                "engineId": "string",
                "engineName": "string",
                "engineVersion": "string",
                "dbVersion": "string",
                "definitionTime": "string"
              }
            ]
          },
          "processingState": 0,
          "exception": {
```

```
"exceptionMessage": "string"
          },
          "created": "2019-08-24T14:15:22Z",
          "lastModified": "2019-08-24T14:15:22Z",
          "discoveryStarted": "2019-08-24T14:15:22Z",
          "fileProcessingDetails": {
            "streamingStartedTime": "2019-08-24T14:15:22Z",
            "streamingCompletedTime": "2019-08-24T14:15:22Z",
            "streamingTimeSpanMs": 0,
            "scanCompletedTime": "2019-08-24T14:15:22Z",
            "processingTimeSpanMs": 0
          },
          "coreEngines": [
            {
              "engineId": "string",
              "engineName": "string",
              "engineVersion": "string",
              "dbVersion": "string",
              "definitionTime": "string"
            }
          ],
          "remediation": {
            "deepCdr": {
              "sanitizationDetails": {
                "failureCategory": "string",
                "description": "string",
                "details": "string"
              },
              "cdrObjectState": 0,
              "fileWasReplaced": true
            },
            "postActionFailedInformation": [
              {
                "objectActionType": 0,
                "exception": {
                  "exceptionDetails": "string",
                  "exceptionMessage": "string"
                }
              }
            ],
            "objectRemediationActions": [
              {
                "objectActionType": 0,
                "objectActionState": 0,
                "cdrObjectState": 0,
                "exceptions": [
                  "string"
                ],
                "id": "string",
                "fileId": "string",
                "fileScanCompletedTime": "2019-08-24T14:15:22Z",
                "remediationId": "string",
                "tenantId": "string",
```

```
}
            ]
          },
          "metaDefenderCoreUrl": "string",
          "discoveryStartedDaySec": 0,
          "objectStorageMetadata": "string",
          "scanWorkflowSnapshotId": "string",
          "scanWorkflowSnapshot": {
            "id": "string",
            "scanId": "string",
            "workflow": {
              "id": "string",
              "scanPoolId": "string",
              "scanProcessFlow": 0,
              "isIdentityScanningEnabled": true,
              "scanIntervalDays": 0,
              "rules": [
                "string"
              ],
              "type": 0,
              "workflowSupportedTechnologies": {
                "dlp": {
                  "status": 0
                },
                "deepCdr": {
                  "status": 0
                },
                "sandBox": {
                  "status": 0
                },
                "metascan": {
                  "status": 0
                }
              },
              "name": "string",
              "userAgent": "string",
              "scanPool": {
                "id": "string",
                "name": "string",
                "scanPoolType": 0,
                "isDefault": true,
                "scanInstances": [
                  {
                    "id": "string",
                    "scanPoolId": "string",
                    "url": "string",
                    "apiKey": "string",
                    "timeout": "string",
                    "scanInstanceType": 0
                  }
                ]
              },
              "failOverScanPoolId": "string",
```

```
"id": "string",
                "name": "string",
                "scanPoolType": 0,
                "isDefault": true,
                "scanInstances": [
                  {
                    "id": "string",
                    "scanPoolId": "string",
                    "url": "string",
                    "apiKey": "string",
                    "timeout": "string",
                    "scanInstanceType": 0
                  }
                ]
              },
              "filters": {
                "id": "string",
                "minimumSize": 0,
                "maximumSize": 0,
                "minimumDateTime": "2019-08-24T14:15:22Z",
                "maximumDateTime": "2019-08-24T14:15:22Z"
              },
              "fileDefinition": {
                "blockingStrategy": 0,
                "configurableBlockingStrategy": {
                  "shouldTreatFilesWithSensitiveDataAsBlocked": true,
                  "shouldTreatFilesWithVulnerabilitiesAsBlocked": true
                }
              },
              "remediations": [
                {
                  "id": "string",
                  "workflowId": "string",
                  "isEnabled": true,
                  "configuration": "string",
                  "type": 0,
                  "handlingType": 0
                }
              ],
              "tenantId": "string"
            },
            "startTimestamp": 0,
            "stopTimestamp": 0,
            "scanPool": {
              "id": "string",
              "name": "string",
              "scanPoolType": 0,
              "isDefault": true,
              "scanInstances": [
                {
                  "id": "string",
                  "scanPoolId": "string",
                  "url": "string",
```

```
"timeout": "string",
                  "scanInstanceType": 0
                }
              ]
            },
            "scanInstances": [
              {
                "id": "string",
                "scanPoolId": "string",
                "url": "string",
                "apiKey": "string",
                "timeout": "string",
                "scanInstanceType": 0
              }
            ],
            "failOverScanPool": {
              "id": "string",
              "name": "string",
              "scanPoolType": 0,
              "isDefault": true,
              "scanInstances": [
                {
                  "id": "string",
                  "scanPoolId": "string",
                  "url": "string",
                  "apiKey": "string",
                  "timeout": "string",
                  "scanInstanceType": 0
                }
              ]
            },
            "failOverScanInstances": [
              {
                "id": "string",
                "scanPoolId": "string",
                "url": "string",
                "apiKey": "string",
                "timeout": "string",
                "scanInstanceType": 0
              }
            ],
            "storage": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
              "accountId": "string",
              "source": "string",
              "storageFunctionality": "string",
              "storageType": {
                "name": "string",
                "categoryType": 0,
                "protocolType": 0,
```

```
},
              "storageStatus": {
                "message": "string",
                "statusType": 0
              },
              "workflowId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z",
              "tenantId": "string",
              "groupRef": {
                "id": "string",
                "name": "string"
              },
              "isAutodiscovered": true
            },
            "workflowStatistics": {
              "taggingStatistics": {
                "total": 0
              },
              "keepAllowedStatistics": {
                "total": 0
              },
              "keepBlockedStatistics": {
                "total": 0
              },
              "keepSanitizedStatistics": {
                "total": 0
              },
              "movedAllowedStatistics": {
                "total": 0,
                "destinationStorageInformation": {
                  "id": "string",
                  "name": "string",
                  "groupId": "string",
                  "clientId": "string",
                  "accountId": "string",
                  "source": "string",
                  "storageFunctionality": "string",
                  "storageType": {
                    "name": "string",
                    "categoryType": 0,
                    "protocolType": 0,
                    "vendorType": 0
                  },
                  "storageStatus": {
                    "message": "string",
                    "statusType": 0
                  },
                  "workflowId": "string",
                  "lastUpdated": "2019-08-24T14:15:22Z",
                  "tenantId": "string",
                  "groupRef": {
                    "id": "string",
                    "name": "string"
```

```
"isAutodiscovered": true
                }
              },
              "movedSanitizedStatistics": {
                "total": 0,
                "destinationStorageInformation": {
                  "id": "string",
                  "name": "string",
                  "groupId": "string",
                  "clientId": "string",
                  "accountId": "string",
                  "source": "string",
                  "storageFunctionality": "string",
                  "storageType": {
                    "name": "string",
                    "categoryType": 0,
                    "protocolType": 0,
                    "vendorType": 0
                  },
                  "storageStatus": {
                    "message": "string",
                    "statusType": 0
                  },
                  "workflowId": "string",
                  "lastUpdated": "2019-08-24T14:15:22Z",
                  "tenantId": "string",
                  "groupRef": {
                    "id": "string",
                    "name": "string"
                  },
                  "isAutodiscovered": true
                }
              },
              "movedBlockedStatistics": {
                "total": 0,
                "destinationStorageInformation": {
                  "id": "string",
                  "name": "string",
                  "groupId": "string",
                  "clientId": "string",
                  "accountId": "string",
                  "source": "string",
                  "storageFunctionality": "string",
                  "storageType": {
                    "name": "string",
                    "categoryType": 0,
                    "protocolType": 0,
                    "vendorType": 0
                  },
                  "storageStatus": {
                    "message": "string",
                    "statusType": 0
                  },
```

```
"lastUpdated": "2019-08-24T14:15:22Z",
                  "tenantId": "string",
                  "groupRef": {
                    "id": "string",
                    "name": "string"
                  },
                  "isAutodiscovered": true
                }
              },
              "copyAllowedStatistics": {
                "total": 0,
                "destinationStorageInformation": {
                  "id": "string",
                  "name": "string",
                  "groupId": "string",
                  "clientId": "string",
                  "accountId": "string",
                  "source": "string",
                  "storageFunctionality": "string",
                  "storageType": {
                    "name": "string",
                    "categoryType": 0,
                    "protocolType": 0,
                    "vendorType": 0
                  },
                  "storageStatus": {
                    "message": "string",
                    "statusType": 0
                  },
                  "workflowId": "string",
                  "lastUpdated": "2019-08-24T14:15:22Z",
                  "tenantId": "string",
                  "groupRef": {
                    "id": "string",
                    "name": "string"
                  },
                  "isAutodiscovered": true
                }
              },
              "copyBlockedStatistics": {
                "total": 0,
                "destinationStorageInformation": {
                  "id": "string",
                  "name": "string",
                  "groupId": "string",
                  "clientId": "string",
                  "accountId": "string",
                  "source": "string",
                  "storageFunctionality": "string",
                  "storageType": {
                    "name": "string",
                    "categoryType": 0,
                    "protocolType": 0,
```

```
},
                  "storageStatus": {
                    "message": "string",
                    "statusType": 0
                  },
                  "workflowId": "string",
                  "lastUpdated": "2019-08-24T14:15:22Z",
                  "tenantId": "string",
                  "groupRef": {
                    "id": "string",
                    "name": "string"
                  },
                  "isAutodiscovered": true
                }
              },
              "deleteAllowedStatistics": {
                "total": 0
              },
              "deleteBlockedStatistics": {
                "total": 0
              },
              "lastCalculatedStatisticsTime": "2019-08-24T14:15:22Z"
            },
            "account": {
              "id": "string",
              "name": "string",
              "description": "string",
              "credentials": "string",
              "protocolType": 0,
              "vendorType": 0,
              "autoDiscovery": true,
              "autodiscoveryDestinationGroupId": "string",
              "destinationGroup": {
                "id": "string",
                "name": "string"
              }
            },
            "realTimeStartDate": "2019-08-24T14:15:22Z"
          },
          "versions": [],
          "hasBlockedVersions": true,
          "versionsCount": 0,
          "objectType": 0,
          "skippedScan": true,
          "$type": "string",
          "url": "string",
          "fileId": "string"
        }
      ],
      "hasBlockedVersions": true,
      "versionsCount": 0,
      "objectType": 0,
      "skippedScan": true,
```

```
}
  ],
  "filterCount": 0,
  "totalCount": 0
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» entries	[File]¦null	false	none	none
» filterCount	integer(int64)	false	none	none
» totalCount	integer(int64)	false	none	none

CancelFileParameters


```
{
  "fileIds": [
    "string"
  ]
}
```


Properties

Name	Type	Required	Restrictions	Description
fileIds	[string]¦null	false	none	none

AddGroupCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "group": {
    "id": "string",
    "name": "string",
    "description": "string",
    "storages": [
      {
        "id": "string",
        "name": "string",
        "groupId": "string",
        "clientId": "string",
        "accountId": "string",
        "source": "string",
        "storageFunctionality": "string",
        "storageType": {
          "name": "string",
          "categoryType": 0,
          "protocolType": 0,
          "vendorType": 0
        },
        "storageStatus": {
          "message": "string",
          "statusType": 0
        },
        "workflowId": "string",
        "lastUpdated": "2019-08-24T14:15:22Z",
        "tenantId": "string",
        "groupRef": {
          "id": "string",
          "name": "string"
        },
        "isAutodiscovered": true
      }
    ]
  }
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» group	Group¦null	false	none	none

Group


```
{
  "id": "string",
  "name": "string",
  "description": "string",
  "storages": [
    {
      "id": "string",
      "name": "string",
      "groupId": "string",
      "clientId": "string",
      "accountId": "string",
      "source": "string",
      "storageFunctionality": "string",
      "storageType": {
        "name": "string",
        "categoryType": 0,
        "protocolType": 0,
        "vendorType": 0
      },
      "storageStatus": {
        "message": "string",
        "statusType": 0
      },
      "workflowId": "string",
      "lastUpdated": "2019-08-24T14:15:22Z",
      "tenantId": "string",
      "groupRef": {
        "id": "string",
        "name": "string"
      },
      "isAutodiscovered": true
    }
  ]
}
```

Properties

Name	Type	Required	Restrictions	Description
id	string	true	none	none
name	string	true	none	none
description	string	true	none	none
storages	[NewStorage]¦null	false	none	none

AddGroupParameters

```
{
  "name": "string",
  "description": "string",
  "storageIds": [
    "string"
  ]
}
```

Properties

Name	Type	Required	Restrictions	Description
name	string	true	none	group name
description	string¦null	false	none	description of the group
storageIds	[string]	true	none	associated storages

BulkDeleteGroupsCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "succeeded": [
    "string"
  ],
  "failed": [
    {
      "id": "string",
      "reasonKey": "string",
      "reason": "string",
      "childFailures": [
        {}
      ]
    }
  ],
  "confirmationRequired": true,
  "preview": [
    {
      "groupId": "string",
      "memberStorageIds": [
        "string"
      ]
    }
  ],
  "scansRunning": true,
  "runningScans": [
    {
      "scanId": "string",
      "storageId": "string",
      "accountId": "string",
      "groupId": "string"
    }
  ]
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» succeeded	[string]	false	none	none
» failed	[BulkFailedItem]	false	none	none
» confirmationRequired	boolean	false	none	none
» preview	[BulkGroupPreviewItem]	false	none	none
» scansRunning	boolean	false	none	none
» runningScans	[BulkRunningScan]	false	none	none

BulkGroupPreviewItem

```
{
  "groupId": "string",
  "memberStorageIds": [
    "string"
  ]
}
```

Properties

Name	Type	Required	Restrictions	Description
groupId	string	false	none	none
memberStorageIds	[string]	false	none	none

BulkDeleteGroupsParameters

```
{
  "groupIds": [
    "string"
  ],
  "forceDelete": true
}
```

Properties

Name	Type	Required	Restrictions	Description
groupIds	[string]	false	none	none
forceDelete	boolean	true	none	none

GetGroupById

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "group": {
    "id": "string",
    "name": "string",
    "description": "string",
    "storages": [
      {
        "id": "string",
        "groupId": "string",
        "accountId": "string",
        "name": "string",
        "storageClientId": "string",
        "storageType": {
          "name": "string",
          "categoryType": 0,
          "protocolType": 0,
          "vendorType": 0
        },
        "storageStatus": {
          "message": "string",
          "statusType": 0
        },
        "scansInProgress": true,
        "isRtpInProgress": true,
        "isScheduledScanInProgress": true,
        "storageFunctionality": "string",
        "isAutodiscovered": true,
        "groupRef": {
          "id": "string",
          "name": "string"
        },
        "$type": "string"
      }
    ]
  }
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» group	GroupWithStorage	true	none	none

GroupWithStorage


```
{
  "id": "string",
  "name": "string",
  "description": "string",
  "storages": [
    {
      "id": "string",
      "groupId": "string",
      "accountId": "string",
      "name": "string",
      "storageClientId": "string",
      "storageType": {
        "name": "string",
        "categoryType": 0,
        "protocolType": 0,
        "vendorType": 0
      },
      "storageStatus": {
        "message": "string",
        "statusType": 0
      },
      "scansInProgress": true,
      "isRtpInProgress": true,
      "isScheduledScanInProgress": true,
      "storageFunctionality": "string",
      "isAutodiscovered": true,
      "groupRef": {
        "id": "string",
        "name": "string"
      },
      "$type": "string"
    }
  ]
}
```

Properties

Name	Type	Required	Restrictions	Description
id	string	true	none	none
name	string	true	none	none
description	string	true	none	none
storages	[Storage]¦null	false	none	none

ListGroups

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "items": [
    {
      "id": "string",
      "name": "string",
      "description": "string",
      "storages": [
        {
          "id": "string",
          "groupId": "string",
          "accountId": "string",
          "name": "string",
          "storageClientId": "string",
          "storageType": {
            "name": "string",
            "categoryType": 0,
            "protocolType": 0,
            "vendorType": 0
          },
          "storageStatus": {
            "message": "string",
            "statusType": 0
          },
          "scansInProgress": true,
          "isRtpInProgress": true,
          "isScheduledScanInProgress": true,
          "storageFunctionality": "string",
          "isAutodiscovered": true,
          "groupRef": {
            "id": "string",
            "name": "string"
          },
          "$type": "string"
        }
      ]
    }
  ],
  "groups": [
    {
      "id": "string",
      "name": "string",
      "description": "string",
      "storages": [
        {
          "id": "string",
```

```
"accountId": "string",
          "name": "string",
          "storageClientId": "string",
          "storageType": {
            "name": "string",
            "categoryType": 0,
            "protocolType": 0,
            "vendorType": 0
          },
          "storageStatus": {
            "message": "string",
            "statusType": 0
          },
          "scansInProgress": true,
          "isRtpInProgress": true,
          "isScheduledScanInProgress": true,
          "storageFunctionality": "string",
          "isAutodiscovered": true,
          "groupRef": {
            "id": "string",
            "name": "string"
          },
          "$type": "string"
        }
      ]
    }
  ],
  "totalCount": 0,
  "startIndex": 0,
  "count": 0
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» items	[GroupWithStorage]¦null	false	none	none
» groups	[GroupWithStorage]¦null	false	none	none
» totalCount	integer(int32)	false	none	none
» startIndex	integer(int32)	false	none	none
» count	integer(int32)	false	none	none

GetGroupsCount


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "groupCount": {
    "count": 0
  }
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» groupCount	CountResult	true	none	none

UpdateGroupCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "updatedGroup": {
    "id": "string",
    "name": "string",
    "description": "string",
    "storages": [
      {
        "id": "string",
        "name": "string",
        "groupId": "string",
        "clientId": "string",
        "accountId": "string",
        "source": "string",
        "storageFunctionality": "string",
        "storageType": {
          "name": "string",
          "categoryType": 0,
          "protocolType": 0,
          "vendorType": 0
        },
        "storageStatus": {
          "message": "string",
          "statusType": 0
        },
        "workflowId": "string",
        "lastUpdated": "2019-08-24T14:15:22Z",
        "tenantId": "string",
        "groupRef": {
          "id": "string",
          "name": "string"
        },
        "isAutodiscovered": true
      }
    ]
  }
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» updatedGroup	Group¦null	false	none	none

UpdateGroupParameters

```
{
  "name": "string",
  "description": "string",
  "groupId": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
name	string¦null	false	none	group name
description	string¦null	false	none	description of the group
groupId	string	true	none	group id to update

ApiHealthModel

```
{
  "apiStatus": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
apiStatus	string¦null	false	none	none

GetOnboarding


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "hasUserConfigured": true,
  "hasAccountConfigured": true,
  "hasStorageConfigured": true,
  "hasScanInstanceConfigured": true,
  "isOnboardingDone": true,
  "isEulaAgreed": true,
  "isCloudType": true
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» hasUserConfigured	boolean	false	none	none
» hasAccountConfigured	boolean	false	none	none
» hasStorageConfigured	boolean	false	none	none
» hasScanInstanceConfigured	boolean	false	none	none
» isOnboardingDone	boolean	false	none	none
» isEulaAgreed	boolean	false	none	none
» isCloudType	boolean	false	none	none

GetRemediationByWorkflowIdCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "entries": [
    {
      "id": "string",
      "workflowId": "string",
      "isEnabled": true,
      "configuration": "string",
      "type": 0,
      "handlingType": 0
    }
  ]
}
```

Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» entries	[Remediation]¦null	false	none	none

GetRemediationByIdCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "entry": {
    "id": "string",
    "workflowId": "string",
    "isEnabled": true,
    "configuration": "string",
    "type": 0,
    "handlingType": 0
  }
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» entry	Remediation|null	false	none	none

AddRemediationCommandResponse


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```

Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none

AddRemediationParameters

```
{
  "workflowId": "string",
  "isEnabled": true,
  "configuration": "string",
  "type": 0,
  "handlingType": 0
}
```

Properties

Name	Type	Required	Restrictions	Description
workflowId	string	true	none	none
isEnabled	boolean	true	none	none
configuration	string	true	none	none
type	RemediationType	true	none	- 0: FileTagging - 1: DeepCdr - 2: BlockedFileRemediation - 3: AllowedSanitizedFileRemediation - 4: AllowedFileRemediation - 5: BlockedSanitizedFileRemediation - 6: DeleteEmptyFoldersRemediation - 7: ScanFileVersions - 8: DiscoveredFileRemediation - 9: AllowedCdrUnsupportedFileRemediation - 10: BlockedCdrUnsupportedFileRemediation
handlingType	RemediationHandlingType	true	none	- 0: Delete - 1: Move - 2: Copy - 3: Keep - 999: NotApplicable

UpdateRemediationCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```

Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none

UpdateRemediationParameters

```
{
  "id": "string",
  "workflowId": "string",
  "isEnabled": true,
  "configuration": "string",
  "type": 0,
  "handlingType": 0
}
```

Properties

Name	Type	Required	Restrictions	Description
id	string	true	none	none
workflowId	string¦null	false	none	none
isEnabled	boolean¦null	false	none	none
configuration	string¦null	false	none	none
type	RemediationType¦null	false	none	- 0: FileTagging - 1: DeepCdr - 2: BlockedFileRemediation - 3: AllowedSanitizedFileRemediation - 4: AllowedFileRemediation - 5: BlockedSanitizedFileRemediation - 6: DeleteEmptyFoldersRemediation - 7: ScanFileVersions - 8: DiscoveredFileRemediation - 9: AllowedCdrUnsupportedFileRemediation - 10: BlockedCdrUnsupportedFileRemediation
handlingType	RemediationHandlingType¦null	false	none	- 0: Delete - 1: Move - 2: Copy - 3: Keep - 999: NotApplicable

DeleteRemediationCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "succeeded": [
    "string"
  ],
  "failed": [
    {
      "id": "string",
      "reasonKey": "string",
      "reason": "string",
      "childFailures": [
        {}
      ]
    }
  ]
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» succeeded	[string]	false	none	none
» failed	[BulkFailedItem]	false	none	none

BulkDeleteRemediationsParameters

```
{
  "remediationIds": [
    "string"
  ]
}
```

Properties

Name	Type	Required	Restrictions	Description
remediationIds	[string]	false	none	none

GetScansReportQueryResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "entries": [
    {
      "result": 0,
      "responseKey": "string",
      "responseMessage": "string",
      "responseMessageParams": {
        "property1": "string",
        "property2": "string"
      },
      "id": "string",
      "name": "string",
      "startTime": "2019-08-24T14:15:22Z",
      "stopTime": "2019-08-24T14:15:22Z",
      "scanType": "string",
      "scanningState": 0,
      "scanStatusDto": {
        "pendingFilesCount": 0,
        "pendingFilesSize": 0,
        "allowedFilesCount": 0,
        "allowedFilesSize": 0,
        "blockedFilesCount": 0,
        "blockedFilesSize": 0,
        "sanitizedFilesCount": 0,
        "failedSanitizedFilesCount": 0,
        "remediatedFilesCount": 0,
        "totalFilesCount": 0,
        "totalFilesSize": 0,
        "processingFailedCount": 0,
        "processingFailedSize": 0,
        "processingFailedRemediationCount": 0,
        "processedFilesCount": 0,
        "processedFilesSize": 0,
        "canceledFilesCount": 0,
        "canceledFilesSize": 0
      },
      "scanStatsDto": {
        "infectedFilesCount": 0,
        "threatTotalFilesCount": 0,
        "filesWithVulnerabilitiesCount": 0,
        "filesWithSensitiveDataCount": 0,
        "filesBlockedBySandboxCount": 0,
        "scannedFilesCount": 0,
        "skippedFilesScanCount": 0,
        "scanFilesDistribution": {
```

```
"executablesFilesCount": 0,
          "audioVideoFilesCount": 0,
          "openSSlEncryptedFilesCount": 0,
          "pdfFilesCount": 0,
          "graphicalFilesCount": 0,
          "diskImageFilesCount": 0,
          "textFilesCount": 0,
          "mailFilesCount": 0,
          "applicationFilesCount": 0,
          "documentsFilesCount": 0,
          "otherFilesCount": 0,
          "archivesFilesCount": 0
        }
      },
      "realTimeStartDate": "2019-08-24T14:15:22Z",
      "scanSequenceDto": {
        "previousScanId": "string",
        "nextScanId": "string"
      },
      "scanPartition": "string",
      "workflowId": "string",
      "scanConfigurationId": "string",
      "errors": [
        "string"
      ],
      "priority": 0,
      "scanWorkflowSnapshotDtos": [
        {
          "id": "string",
          "scanId": "string",
          "workflow": {
            "id": "string",
            "scanPoolId": "string",
            "scanProcessFlow": 0,
            "isIdentityScanningEnabled": true,
            "scanIntervalDays": 0,
            "rules": [
              "string"
            ],
            "type": 0,
            "workflowSupportedTechnologies": {
              "dlp": {
                "status": 0
              },
              "deepCdr": {
                "status": 0
              },
              "sandBox": {
                "status": 0
              },
              "metascan": {
                "status": 0
              }
```

```
"name": "string",
            "userAgent": "string",
            "scanPool": {
              "id": "string",
              "name": "string",
              "scanPoolType": 0,
              "isDefault": true,
              "scanInstances": [
                {
                  "id": "string",
                  "scanPoolId": "string",
                  "url": "string",
                  "apiKey": "string",
                  "timeout": "string",
                  "scanInstanceType": 0
                }
              ]
            },
            "failOverScanPoolId": "string",
            "failOverScanPool": {
              "id": "string",
              "name": "string",
              "scanPoolType": 0,
              "isDefault": true,
              "scanInstances": [
                {
                  "id": "string",
                  "scanPoolId": "string",
                  "url": "string",
                  "apiKey": "string",
                  "timeout": "string",
                  "scanInstanceType": 0
                }
              ]
            },
            "filters": {
              "id": "string",
              "minimumSize": 0,
              "maximumSize": 0,
              "minimumDateTime": "2019-08-24T14:15:22Z",
              "maximumDateTime": "2019-08-24T14:15:22Z"
            },
            "fileDefinition": {
              "blockingStrategy": 0,
              "configurableBlockingStrategy": {
                "shouldTreatFilesWithSensitiveDataAsBlocked": true,
                "shouldTreatFilesWithVulnerabilitiesAsBlocked": true
              }
            },
            "remediations": [
              {
                "id": "string",
                "workflowId": "string",
```

```
"configuration": "string",
                "type": 0,
                "handlingType": 0
              }
            ],
            "tenantId": "string"
          },
          "startTimestamp": 0,
          "stopTimestamp": 0,
          "scanPool": {
            "id": "string",
            "name": "string",
            "scanPoolType": 0,
            "isDefault": true,
            "scanInstances": [
              {
                "id": "string",
                "scanPoolId": "string",
                "url": "string",
                "apiKey": "string",
                "timeout": "string",
                "scanInstanceType": 0
              }
            ]
          },
          "scanInstances": [
            {
              "id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ],
          "failOverScanPool": {
            "id": "string",
            "name": "string",
            "scanPoolType": 0,
            "isDefault": true,
            "scanInstances": [
              {
                "id": "string",
                "scanPoolId": "string",
                "url": "string",
                "apiKey": "string",
                "timeout": "string",
                "scanInstanceType": 0
              }
            ]
          },
          "failOverScanInstances": [
            {
```

```
"scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ],
          "storage": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          },
          "workflowStatistics": {
            "taggingStatistics": {
              "total": 0
            },
            "keepAllowedStatistics": {
              "total": 0
            },
            "keepBlockedStatistics": {
              "total": 0
            },
            "keepSanitizedStatistics": {
              "total": 0
            },
            "movedAllowedStatistics": {
              "total": 0,
              "destinationStorageInformation": {
                "id": "string",
                "name": "string",
                "groupId": "string",
```

```
"accountId": "string",
                "source": "string",
                "storageFunctionality": "string",
                "storageType": {
                  "name": "string",
                  "categoryType": 0,
                  "protocolType": 0,
                  "vendorType": 0
                },
                "storageStatus": {
                  "message": "string",
                  "statusType": 0
                },
                "workflowId": "string",
                "lastUpdated": "2019-08-24T14:15:22Z",
                "tenantId": "string",
                "groupRef": {
                  "id": "string",
                  "name": "string"
                },
                "isAutodiscovered": true
              }
            },
            "movedSanitizedStatistics": {
              "total": 0,
              "destinationStorageInformation": {
                "id": "string",
                "name": "string",
                "groupId": "string",
                "clientId": "string",
                "accountId": "string",
                "source": "string",
                "storageFunctionality": "string",
                "storageType": {
                  "name": "string",
                  "categoryType": 0,
                  "protocolType": 0,
                  "vendorType": 0
                },
                "storageStatus": {
                  "message": "string",
                  "statusType": 0
                },
                "workflowId": "string",
                "lastUpdated": "2019-08-24T14:15:22Z",
                "tenantId": "string",
                "groupRef": {
                  "id": "string",
                  "name": "string"
                },
                "isAutodiscovered": true
              }
            },
```

```
"total": 0,
              "destinationStorageInformation": {
                "id": "string",
                "name": "string",
                "groupId": "string",
                "clientId": "string",
                "accountId": "string",
                "source": "string",
                "storageFunctionality": "string",
                "storageType": {
                  "name": "string",
                  "categoryType": 0,
                  "protocolType": 0,
                  "vendorType": 0
                },
                "storageStatus": {
                  "message": "string",
                  "statusType": 0
                },
                "workflowId": "string",
                "lastUpdated": "2019-08-24T14:15:22Z",
                "tenantId": "string",
                "groupRef": {
                  "id": "string",
                  "name": "string"
                },
                "isAutodiscovered": true
              }
            },
            "copyAllowedStatistics": {
              "total": 0,
              "destinationStorageInformation": {
                "id": "string",
                "name": "string",
                "groupId": "string",
                "clientId": "string",
                "accountId": "string",
                "source": "string",
                "storageFunctionality": "string",
                "storageType": {
                  "name": "string",
                  "categoryType": 0,
                  "protocolType": 0,
                  "vendorType": 0
                },
                "storageStatus": {
                  "message": "string",
                  "statusType": 0
                },
                "workflowId": "string",
                "lastUpdated": "2019-08-24T14:15:22Z",
                "tenantId": "string",
                "groupRef": {
```

```
"name": "string"
                },
                "isAutodiscovered": true
              }
            },
            "copyBlockedStatistics": {
              "total": 0,
              "destinationStorageInformation": {
                "id": "string",
                "name": "string",
                "groupId": "string",
                "clientId": "string",
                "accountId": "string",
                "source": "string",
                "storageFunctionality": "string",
                "storageType": {
                  "name": "string",
                  "categoryType": 0,
                  "protocolType": 0,
                  "vendorType": 0
                },
                "storageStatus": {
                  "message": "string",
                  "statusType": 0
                },
                "workflowId": "string",
                "lastUpdated": "2019-08-24T14:15:22Z",
                "tenantId": "string",
                "groupRef": {
                  "id": "string",
                  "name": "string"
                },
                "isAutodiscovered": true
              }
            },
            "deleteAllowedStatistics": {
              "total": 0
            },
            "deleteBlockedStatistics": {
              "total": 0
            },
            "lastCalculatedStatisticsTime": "2019-08-24T14:15:22Z"
          },
          "account": {
            "id": "string",
            "name": "string",
            "description": "string",
            "credentials": "string",
            "protocolType": 0,
            "vendorType": 0,
            "autoDiscovery": true,
            "autodiscoveryDestinationGroupId": "string",
            "destinationGroup": {
```

```
"name": "string"
            }
          },
          "realTimeStartDate": "2019-08-24T14:15:22Z"
        }
      ],
      "storageId": "string",
      "discoveryCycleTiming": {
        "currentCycleStartedAt": "2019-08-24T14:15:22Z",
        "lastCycleStartedAt": "2019-08-24T14:15:22Z",
        "lastCycleFinishedAt": "2019-08-24T14:15:22Z",
        "lastCycleDurationSeconds": 0.1
      },
      "$type": "string"
    }
  ],
  "totalCount": 0
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» entries	[ScanResponse]¦null	false	none	none
» totalCount	integer(int64)¦null	false	none	none
» result	ResultType5	false	none	- 0: Success - 1: StorageNotFound - 2: Error

ScanResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "id": "string",
  "name": "string",
  "startTime": "2019-08-24T14:15:22Z",
  "stopTime": "2019-08-24T14:15:22Z",
  "scanType": "string",
  "scanningState": 0,
  "scanStatusDto": {
    "pendingFilesCount": 0,
    "pendingFilesSize": 0,
    "allowedFilesCount": 0,
    "allowedFilesSize": 0,
    "blockedFilesCount": 0,
    "blockedFilesSize": 0,
    "sanitizedFilesCount": 0,
    "failedSanitizedFilesCount": 0,
    "remediatedFilesCount": 0,
    "totalFilesCount": 0,
    "totalFilesSize": 0,
    "processingFailedCount": 0,
    "processingFailedSize": 0,
    "processingFailedRemediationCount": 0,
    "processedFilesCount": 0,
    "processedFilesSize": 0,
    "canceledFilesCount": 0,
    "canceledFilesSize": 0
  },
  "scanStatsDto": {
    "infectedFilesCount": 0,
    "threatTotalFilesCount": 0,
    "filesWithVulnerabilitiesCount": 0,
    "filesWithSensitiveDataCount": 0,
    "filesBlockedBySandboxCount": 0,
    "scannedFilesCount": 0,
    "skippedFilesScanCount": 0,
    "scanFilesDistribution": {
      "documentsEncryptedFilesCount": 0,
      "executablesFilesCount": 0,
      "audioVideoFilesCount": 0,
      "openSSlEncryptedFilesCount": 0,
      "pdfFilesCount": 0,
      "graphicalFilesCount": 0,
      "diskImageFilesCount": 0,
      "textFilesCount": 0,
      "mailFilesCount": 0,
```

```
"documentsFilesCount": 0,
      "otherFilesCount": 0,
      "archivesFilesCount": 0
    }
  },
  "realTimeStartDate": "2019-08-24T14:15:22Z",
  "scanSequenceDto": {
    "previousScanId": "string",
    "nextScanId": "string"
  },
  "scanPartition": "string",
  "workflowId": "string",
  "scanConfigurationId": "string",
  "errors": [
    "string"
  ],
  "priority": 0,
  "scanWorkflowSnapshotDtos": [
    {
      "id": "string",
      "scanId": "string",
      "workflow": {
        "id": "string",
        "scanPoolId": "string",
        "scanProcessFlow": 0,
        "isIdentityScanningEnabled": true,
        "scanIntervalDays": 0,
        "rules": [
          "string"
        ],
        "type": 0,
        "workflowSupportedTechnologies": {
          "dlp": {
            "status": 0
          },
          "deepCdr": {
            "status": 0
          },
          "sandBox": {
            "status": 0
          },
          "metascan": {
            "status": 0
          }
        },
        "name": "string",
        "userAgent": "string",
        "scanPool": {
          "id": "string",
          "name": "string",
          "scanPoolType": 0,
          "isDefault": true,
          "scanInstances": [
```

```
"id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ]
        },
        "failOverScanPoolId": "string",
        "failOverScanPool": {
          "id": "string",
          "name": "string",
          "scanPoolType": 0,
          "isDefault": true,
          "scanInstances": [
            {
              "id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ]
        },
        "filters": {
          "id": "string",
          "minimumSize": 0,
          "maximumSize": 0,
          "minimumDateTime": "2019-08-24T14:15:22Z",
          "maximumDateTime": "2019-08-24T14:15:22Z"
        },
        "fileDefinition": {
          "blockingStrategy": 0,
          "configurableBlockingStrategy": {
            "shouldTreatFilesWithSensitiveDataAsBlocked": true,
            "shouldTreatFilesWithVulnerabilitiesAsBlocked": true
          }
        },
        "remediations": [
          {
            "id": "string",
            "workflowId": "string",
            "isEnabled": true,
            "configuration": "string",
            "type": 0,
            "handlingType": 0
          }
        ],
        "tenantId": "string"
      },
      "startTimestamp": 0,
```

```
"scanPool": {
        "id": "string",
        "name": "string",
        "scanPoolType": 0,
        "isDefault": true,
        "scanInstances": [
          {
            "id": "string",
            "scanPoolId": "string",
            "url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ]
      },
      "scanInstances": [
        {
          "id": "string",
          "scanPoolId": "string",
          "url": "string",
          "apiKey": "string",
          "timeout": "string",
          "scanInstanceType": 0
        }
      ],
      "failOverScanPool": {
        "id": "string",
        "name": "string",
        "scanPoolType": 0,
        "isDefault": true,
        "scanInstances": [
          {
            "id": "string",
            "scanPoolId": "string",
            "url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ]
      },
      "failOverScanInstances": [
        {
          "id": "string",
          "scanPoolId": "string",
          "url": "string",
          "apiKey": "string",
          "timeout": "string",
          "scanInstanceType": 0
        }
      ],
      "storage": {
```

```
"name": "string",
        "groupId": "string",
        "clientId": "string",
        "accountId": "string",
        "source": "string",
        "storageFunctionality": "string",
        "storageType": {
          "name": "string",
          "categoryType": 0,
          "protocolType": 0,
          "vendorType": 0
        },
        "storageStatus": {
          "message": "string",
          "statusType": 0
        },
        "workflowId": "string",
        "lastUpdated": "2019-08-24T14:15:22Z",
        "tenantId": "string",
        "groupRef": {
          "id": "string",
          "name": "string"
        },
        "isAutodiscovered": true
      },
      "workflowStatistics": {
        "taggingStatistics": {
          "total": 0
        },
        "keepAllowedStatistics": {
          "total": 0
        },
        "keepBlockedStatistics": {
          "total": 0
        },
        "keepSanitizedStatistics": {
          "total": 0
        },
        "movedAllowedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
```

```
"storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "movedSanitizedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "movedBlockedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
```

```
"storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "copyAllowedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "copyBlockedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
```

```
"name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "deleteAllowedStatistics": {
          "total": 0
        },
        "deleteBlockedStatistics": {
          "total": 0
        },
        "lastCalculatedStatisticsTime": "2019-08-24T14:15:22Z"
      },
      "account": {
        "id": "string",
        "name": "string",
        "description": "string",
        "credentials": "string",
        "protocolType": 0,
        "vendorType": 0,
        "autoDiscovery": true,
        "autodiscoveryDestinationGroupId": "string",
        "destinationGroup": {
          "id": "string",
          "name": "string"
        }
      },
      "realTimeStartDate": "2019-08-24T14:15:22Z"
    }
  ],
  "storageId": "string",
  "discoveryCycleTiming": {
```

```
"lastCycleStartedAt": "2019-08-24T14:15:22Z",
    "lastCycleFinishedAt": "2019-08-24T14:15:22Z",
    "lastCycleDurationSeconds": 0.1
  },
  "$type": "string"
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and - discriminator: $type

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» id	string	true	none	none
» name	string	true	none	none
» startTime	string(date-time)	true	none	none
» stopTime	string(date-time)	true	none	none
» scanType	string	true	none	none
» scanningState	ScanningState	false	none	- 0: NotStarted - 1: Running - 2: Cancelled - 3: Failed - 4: Completed
» scanStatusDto	ScanStatus	true	none	none
» scanStatsDto	ScanStats	true	none	none
» realTimeStartDate	string(date-time)¦null	false	none	none
» scanSequenceDto	ScanSequence¦null	false	none	none
» scanPartition	string¦null	false	none	none
» workflowId	string	true	none	WorkflowId required if ScanConfigurationId is null
» scanConfigurationId	string¦null	false	none	This property is obsolete and will be removed in the future. Use WorkflowId instead.
» errors	[string]	true	none	none
» priority	MessagePriority	false	none	- 0: Low - 1: Medium - 2: High
» scanWorkflowSnapshotDtos	[ScanWorkflowSnapshot]	true	none	none
» storageId	string	true	none	none
» discoveryCycleTiming	DiscoveryCycleTimingResponse¦null	false	none	none

» $type	string	true	none	none

ScanningState

```
0
```

- 0: NotStarted
- 1: Running
- 2: Cancelled
- 3: Failed
- 4: Completed

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: NotStarted - 1: Running - 2: Cancelled - 3: Failed - 4: Completed

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2
anonymous	3
anonymous	4

ScanStatus

```
{
  "pendingFilesCount": 0,
  "pendingFilesSize": 0,
  "allowedFilesCount": 0,
  "allowedFilesSize": 0,
  "blockedFilesCount": 0,
  "blockedFilesSize": 0,
  "sanitizedFilesCount": 0,
  "failedSanitizedFilesCount": 0,
  "remediatedFilesCount": 0,
  "totalFilesCount": 0,
  "totalFilesSize": 0,
  "processingFailedCount": 0,
  "processingFailedSize": 0,
  "processingFailedRemediationCount": 0,
  "processedFilesCount": 0,
  "processedFilesSize": 0,
  "canceledFilesCount": 0,
  "canceledFilesSize": 0
}
```

Properties

Name	Type	Required	Restrictions	Description
pendingFilesCount	integer(int64)	false	none	none
pendingFilesSize	integer(int64)	false	none	none
allowedFilesCount	integer(int64)	false	none	none
allowedFilesSize	integer(int64)	false	none	none
blockedFilesCount	integer(int64)	false	none	none
blockedFilesSize	integer(int64)	false	none	none
sanitizedFilesCount	integer(int64)	false	none	none
failedSanitizedFilesCount	integer(int64)	false	none	none
remediatedFilesCount	integer(int64)	false	none	none
totalFilesCount	integer(int64)	false	none	none
totalFilesSize	integer(int64)	false	none	none
processingFailedCount	integer(int64)	false	none	none
processingFailedSize	integer(int64)	false	none	none
processingFailedRemediationCount	integer(int64)	false	none	none
processedFilesCount	integer(int64)	false	none	none
processedFilesSize	integer(int64)	false	none	none
canceledFilesCount	integer(int64)	false	none	none
canceledFilesSize	integer(int64)	false	none	none

ScanStats

```
{
  "infectedFilesCount": 0,
  "threatTotalFilesCount": 0,
  "filesWithVulnerabilitiesCount": 0,
  "filesWithSensitiveDataCount": 0,
  "filesBlockedBySandboxCount": 0,
  "scannedFilesCount": 0,
  "skippedFilesScanCount": 0,
  "scanFilesDistribution": {
    "documentsEncryptedFilesCount": 0,
    "executablesFilesCount": 0,
    "audioVideoFilesCount": 0,
    "openSSlEncryptedFilesCount": 0,
    "pdfFilesCount": 0,
    "graphicalFilesCount": 0,
    "diskImageFilesCount": 0,
    "textFilesCount": 0,
    "mailFilesCount": 0,
    "applicationFilesCount": 0,
    "documentsFilesCount": 0,
    "otherFilesCount": 0,
    "archivesFilesCount": 0
  }
}
```


Properties

Name	Type	Required	Restrictions	Description
infectedFilesCount	integer(int64)	false	none	none
threatTotalFilesCount	integer(int64)	false	none	none
filesWithVulnerabilitiesCount	integer(int64)	false	none	none
filesWithSensitiveDataCount	integer(int64)	false	none	none
filesBlockedBySandboxCount	integer(int64)	false	none	none
scannedFilesCount	integer(int64)	false	none	none
skippedFilesScanCount	integer(int64)	false	none	none
scanFilesDistribution	ScanFilesDistribution¦null	false	none	none

ScanFilesDistribution

```
{
  "documentsEncryptedFilesCount": 0,
  "executablesFilesCount": 0,
  "audioVideoFilesCount": 0,
  "openSSlEncryptedFilesCount": 0,
  "pdfFilesCount": 0,
  "graphicalFilesCount": 0,
  "diskImageFilesCount": 0,
  "textFilesCount": 0,
  "mailFilesCount": 0,
  "applicationFilesCount": 0,
  "documentsFilesCount": 0,
  "otherFilesCount": 0,
  "archivesFilesCount": 0
}
```


Properties

Name	Type	Required	Restrictions	Description
documentsEncryptedFilesCount	integer(int64)¦null	false	none	none
executablesFilesCount	integer(int64)¦null	false	none	none
audioVideoFilesCount	integer(int64)¦null	false	none	none
openSSlEncryptedFilesCount	integer(int64)¦null	false	none	none
pdfFilesCount	integer(int64)¦null	false	none	none
graphicalFilesCount	integer(int64)¦null	false	none	none
diskImageFilesCount	integer(int64)¦null	false	none	none
textFilesCount	integer(int64)¦null	false	none	none
mailFilesCount	integer(int64)¦null	false	none	none
applicationFilesCount	integer(int64)¦null	false	none	none
documentsFilesCount	integer(int64)¦null	false	none	none
otherFilesCount	integer(int64)¦null	false	none	none
archivesFilesCount	integer(int64)¦null	false	none	none

ScanSequence

```
{
  "previousScanId": "string",
  "nextScanId": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
previousScanId	string¦null	false	none	none
nextScanId	string¦null	false	none	none

MessagePriority

```
0
```

- 0: Low
- 1: Medium
- 2: High

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: Low - 1: Medium - 2: High

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2

DiscoveryCycleTimingResponse

```
{
  "currentCycleStartedAt": "2019-08-24T14:15:22Z",
  "lastCycleStartedAt": "2019-08-24T14:15:22Z",
  "lastCycleFinishedAt": "2019-08-24T14:15:22Z",
  "lastCycleDurationSeconds": 0.1
}
```


Properties

Name	Type	Required	Restrictions	Description
currentCycleStartedAt	string(date-time)¦null	false	none	none
lastCycleStartedAt	string(date-time)¦null	false	none	none
lastCycleFinishedAt	string(date-time)¦null	false	none	none
lastCycleDurationSeconds	number(double)¦null	false	none	none

RealTimeScanResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "id": "string",
  "name": "string",
  "startTime": "2019-08-24T14:15:22Z",
  "stopTime": "2019-08-24T14:15:22Z",
  "scanType": "string",
  "scanningState": 0,
  "scanStatusDto": {
    "pendingFilesCount": 0,
    "pendingFilesSize": 0,
    "allowedFilesCount": 0,
    "allowedFilesSize": 0,
    "blockedFilesCount": 0,
    "blockedFilesSize": 0,
    "sanitizedFilesCount": 0,
    "failedSanitizedFilesCount": 0,
    "remediatedFilesCount": 0,
    "totalFilesCount": 0,
    "totalFilesSize": 0,
    "processingFailedCount": 0,
    "processingFailedSize": 0,
    "processingFailedRemediationCount": 0,
    "processedFilesCount": 0,
    "processedFilesSize": 0,
    "canceledFilesCount": 0,
    "canceledFilesSize": 0
  },
  "scanStatsDto": {
    "infectedFilesCount": 0,
    "threatTotalFilesCount": 0,
    "filesWithVulnerabilitiesCount": 0,
    "filesWithSensitiveDataCount": 0,
    "filesBlockedBySandboxCount": 0,
    "scannedFilesCount": 0,
    "skippedFilesScanCount": 0,
    "scanFilesDistribution": {
      "documentsEncryptedFilesCount": 0,
      "executablesFilesCount": 0,
      "audioVideoFilesCount": 0,
      "openSSlEncryptedFilesCount": 0,
      "pdfFilesCount": 0,
      "graphicalFilesCount": 0,
      "diskImageFilesCount": 0,
      "textFilesCount": 0,
      "mailFilesCount": 0,
```

```
"documentsFilesCount": 0,
      "otherFilesCount": 0,
      "archivesFilesCount": 0
    }
  },
  "realTimeStartDate": "2019-08-24T14:15:22Z",
  "scanSequenceDto": {
    "previousScanId": "string",
    "nextScanId": "string"
  },
  "scanPartition": "string",
  "workflowId": "string",
  "scanConfigurationId": "string",
  "errors": [
    "string"
  ],
  "priority": 0,
  "scanWorkflowSnapshotDtos": [
    {
      "id": "string",
      "scanId": "string",
      "workflow": {
        "id": "string",
        "scanPoolId": "string",
        "scanProcessFlow": 0,
        "isIdentityScanningEnabled": true,
        "scanIntervalDays": 0,
        "rules": [
          "string"
        ],
        "type": 0,
        "workflowSupportedTechnologies": {
          "dlp": {
            "status": 0
          },
          "deepCdr": {
            "status": 0
          },
          "sandBox": {
            "status": 0
          },
          "metascan": {
            "status": 0
          }
        },
        "name": "string",
        "userAgent": "string",
        "scanPool": {
          "id": "string",
          "name": "string",
          "scanPoolType": 0,
          "isDefault": true,
          "scanInstances": [
```

```
"id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ]
        },
        "failOverScanPoolId": "string",
        "failOverScanPool": {
          "id": "string",
          "name": "string",
          "scanPoolType": 0,
          "isDefault": true,
          "scanInstances": [
            {
              "id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ]
        },
        "filters": {
          "id": "string",
          "minimumSize": 0,
          "maximumSize": 0,
          "minimumDateTime": "2019-08-24T14:15:22Z",
          "maximumDateTime": "2019-08-24T14:15:22Z"
        },
        "fileDefinition": {
          "blockingStrategy": 0,
          "configurableBlockingStrategy": {
            "shouldTreatFilesWithSensitiveDataAsBlocked": true,
            "shouldTreatFilesWithVulnerabilitiesAsBlocked": true
          }
        },
        "remediations": [
          {
            "id": "string",
            "workflowId": "string",
            "isEnabled": true,
            "configuration": "string",
            "type": 0,
            "handlingType": 0
          }
        ],
        "tenantId": "string"
      },
      "startTimestamp": 0,
```

```
"scanPool": {
        "id": "string",
        "name": "string",
        "scanPoolType": 0,
        "isDefault": true,
        "scanInstances": [
          {
            "id": "string",
            "scanPoolId": "string",
            "url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ]
      },
      "scanInstances": [
        {
          "id": "string",
          "scanPoolId": "string",
          "url": "string",
          "apiKey": "string",
          "timeout": "string",
          "scanInstanceType": 0
        }
      ],
      "failOverScanPool": {
        "id": "string",
        "name": "string",
        "scanPoolType": 0,
        "isDefault": true,
        "scanInstances": [
          {
            "id": "string",
            "scanPoolId": "string",
            "url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ]
      },
      "failOverScanInstances": [
        {
          "id": "string",
          "scanPoolId": "string",
          "url": "string",
          "apiKey": "string",
          "timeout": "string",
          "scanInstanceType": 0
        }
      ],
      "storage": {
```

```
"name": "string",
        "groupId": "string",
        "clientId": "string",
        "accountId": "string",
        "source": "string",
        "storageFunctionality": "string",
        "storageType": {
          "name": "string",
          "categoryType": 0,
          "protocolType": 0,
          "vendorType": 0
        },
        "storageStatus": {
          "message": "string",
          "statusType": 0
        },
        "workflowId": "string",
        "lastUpdated": "2019-08-24T14:15:22Z",
        "tenantId": "string",
        "groupRef": {
          "id": "string",
          "name": "string"
        },
        "isAutodiscovered": true
      },
      "workflowStatistics": {
        "taggingStatistics": {
          "total": 0
        },
        "keepAllowedStatistics": {
          "total": 0
        },
        "keepBlockedStatistics": {
          "total": 0
        },
        "keepSanitizedStatistics": {
          "total": 0
        },
        "movedAllowedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
```

```
"storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "movedSanitizedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "movedBlockedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
```

```
"storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "copyAllowedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "copyBlockedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
```

```
"name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "deleteAllowedStatistics": {
          "total": 0
        },
        "deleteBlockedStatistics": {
          "total": 0
        },
        "lastCalculatedStatisticsTime": "2019-08-24T14:15:22Z"
      },
      "account": {
        "id": "string",
        "name": "string",
        "description": "string",
        "credentials": "string",
        "protocolType": 0,
        "vendorType": 0,
        "autoDiscovery": true,
        "autodiscoveryDestinationGroupId": "string",
        "destinationGroup": {
          "id": "string",
          "name": "string"
        }
      },
      "realTimeStartDate": "2019-08-24T14:15:22Z"
    }
  ],
  "storageId": "string",
  "discoveryCycleTiming": {
```

```
"lastCycleStartedAt": "2019-08-24T14:15:22Z",
    "lastCycleFinishedAt": "2019-08-24T14:15:22Z",
    "lastCycleDurationSeconds": 0.1
  },
  "$type": "string",
  "isRealTimeEnabled": true,
  "handlingType": 0
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	ScanResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» isRealTimeEnabled	boolean	false	none	none
» handlingType	RealTimeHandlingType	false	none	- 0: Polling - 1: EventBased

RealTimeHandlingType


```
0
```


- 0: Polling
- 1: EventBased

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: Polling - 1: EventBased

Enumerated Values

Property	Value
anonymous	0
anonymous	1

ResultType5

```
0
```

- 0: Success
- 1: StorageNotFound
- 2: Error

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: Success - 1: StorageNotFound - 2: Error

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2

ScanTypeFilter

```
0
```

- 0: Instant
- 1: Scheduled
- 2: RealTime

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: Instant - 1: Scheduled - 2: RealTime

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2

ScanStateFilter

```
0
```

- 0: NotStarted
- 1: Running
- 2: Cancelled
- 3: Failed
- 4: Completed

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: NotStarted - 1: Running - 2: Cancelled - 3: Failed - 4: Completed

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2
anonymous	3
anonymous	4

RealTimeHandlingType2

```
0
```

- 0: Polling
- 1: EventBased

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: Polling - 1: EventBased

Enumerated Values

Property	Value
anonymous	0
anonymous	1

ScanSortOption

```
0
```

- 0: StartTime
- 1: Name

- 2: WorkflowId

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: StartTime - 1: Name - 2: WorkflowId

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2

ReportDateField

```
0
```

- 0: Stop
- 1: Start

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: Stop - 1: Start

Enumerated Values

Property	Value
anonymous	0
anonymous	1

TypeOfReport

```
0
```

- 0: Executive
- 1: Summary

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: Executive - 1: Summary

Enumerated Values

Property	Value
anonymous	0
anonymous	1

GetScanByIdQueryResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "scan": {
    "result": 0,
    "responseKey": "string",
    "responseMessage": "string",
    "responseMessageParams": {
      "property1": "string",
      "property2": "string"
    },
    "id": "string",
    "name": "string",
    "startTime": "2019-08-24T14:15:22Z",
    "stopTime": "2019-08-24T14:15:22Z",
    "scanType": "string",
    "scanningState": 0,
    "scanStatusDto": {
      "pendingFilesCount": 0,
      "pendingFilesSize": 0,
      "allowedFilesCount": 0,
      "allowedFilesSize": 0,
      "blockedFilesCount": 0,
      "blockedFilesSize": 0,
      "sanitizedFilesCount": 0,
      "failedSanitizedFilesCount": 0,
      "remediatedFilesCount": 0,
      "totalFilesCount": 0,
      "totalFilesSize": 0,
      "processingFailedCount": 0,
      "processingFailedSize": 0,
      "processingFailedRemediationCount": 0,
      "processedFilesCount": 0,
      "processedFilesSize": 0,
      "canceledFilesCount": 0,
      "canceledFilesSize": 0
    },
    "scanStatsDto": {
      "infectedFilesCount": 0,
      "threatTotalFilesCount": 0,
      "filesWithVulnerabilitiesCount": 0,
      "filesWithSensitiveDataCount": 0,
      "filesBlockedBySandboxCount": 0,
      "scannedFilesCount": 0,
      "skippedFilesScanCount": 0,
      "scanFilesDistribution": {
        "documentsEncryptedFilesCount": 0,
```

```
"audioVideoFilesCount": 0,
        "openSSlEncryptedFilesCount": 0,
        "pdfFilesCount": 0,
        "graphicalFilesCount": 0,
        "diskImageFilesCount": 0,
        "textFilesCount": 0,
        "mailFilesCount": 0,
        "applicationFilesCount": 0,
        "documentsFilesCount": 0,
        "otherFilesCount": 0,
        "archivesFilesCount": 0
      }
    },
    "realTimeStartDate": "2019-08-24T14:15:22Z",
    "scanSequenceDto": {
      "previousScanId": "string",
      "nextScanId": "string"
    },
    "scanPartition": "string",
    "workflowId": "string",
    "scanConfigurationId": "string",
    "errors": [
      "string"
    ],
    "priority": 0,
    "scanWorkflowSnapshotDtos": [
      {
        "id": "string",
        "scanId": "string",
        "workflow": {
          "id": "string",
          "scanPoolId": "string",
          "scanProcessFlow": 0,
          "isIdentityScanningEnabled": true,
          "scanIntervalDays": 0,
          "rules": [
            "string"
          ],
          "type": 0,
          "workflowSupportedTechnologies": {
            "dlp": {
              "status": 0
            },
            "deepCdr": {
              "status": 0
            },
            "sandBox": {
              "status": 0
            },
            "metascan": {
              "status": 0
            }
          },
```

```
"userAgent": "string",
          "scanPool": {
            "id": "string",
            "name": "string",
            "scanPoolType": 0,
            "isDefault": true,
            "scanInstances": [
              {
                "id": "string",
                "scanPoolId": "string",
                "url": "string",
                "apiKey": "string",
                "timeout": "string",
                "scanInstanceType": 0
              }
            ]
          },
          "failOverScanPoolId": "string",
          "failOverScanPool": {
            "id": "string",
            "name": "string",
            "scanPoolType": 0,
            "isDefault": true,
            "scanInstances": [
              {
                "id": "string",
                "scanPoolId": "string",
                "url": "string",
                "apiKey": "string",
                "timeout": "string",
                "scanInstanceType": 0
              }
            ]
          },
          "filters": {
            "id": "string",
            "minimumSize": 0,
            "maximumSize": 0,
            "minimumDateTime": "2019-08-24T14:15:22Z",
            "maximumDateTime": "2019-08-24T14:15:22Z"
          },
          "fileDefinition": {
            "blockingStrategy": 0,
            "configurableBlockingStrategy": {
              "shouldTreatFilesWithSensitiveDataAsBlocked": true,
              "shouldTreatFilesWithVulnerabilitiesAsBlocked": true
            }
          },
          "remediations": [
            {
              "id": "string",
              "workflowId": "string",
              "isEnabled": true,
```

```
"type": 0,
              "handlingType": 0
            }
          ],
          "tenantId": "string"
        },
        "startTimestamp": 0,
        "stopTimestamp": 0,
        "scanPool": {
          "id": "string",
          "name": "string",
          "scanPoolType": 0,
          "isDefault": true,
          "scanInstances": [
            {
              "id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ]
        },
        "scanInstances": [
          {
            "id": "string",
            "scanPoolId": "string",
            "url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ],
        "failOverScanPool": {
          "id": "string",
          "name": "string",
          "scanPoolType": 0,
          "isDefault": true,
          "scanInstances": [
            {
              "id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ]
        },
        "failOverScanInstances": [
          {
            "id": "string",
```

```
"url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ],
        "storage": {
          "id": "string",
          "name": "string",
          "groupId": "string",
          "clientId": "string",
          "accountId": "string",
          "source": "string",
          "storageFunctionality": "string",
          "storageType": {
            "name": "string",
            "categoryType": 0,
            "protocolType": 0,
            "vendorType": 0
          },
          "storageStatus": {
            "message": "string",
            "statusType": 0
          },
          "workflowId": "string",
          "lastUpdated": "2019-08-24T14:15:22Z",
          "tenantId": "string",
          "groupRef": {
            "id": "string",
            "name": "string"
          },
          "isAutodiscovered": true
        },
        "workflowStatistics": {
          "taggingStatistics": {
            "total": 0
          },
          "keepAllowedStatistics": {
            "total": 0
          },
          "keepBlockedStatistics": {
            "total": 0
          },
          "keepSanitizedStatistics": {
            "total": 0
          },
          "movedAllowedStatistics": {
            "total": 0,
            "destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
```

```
"source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "movedSanitizedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "movedBlockedStatistics": {
```

```
"destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
              "accountId": "string",
              "source": "string",
              "storageFunctionality": "string",
              "storageType": {
                "name": "string",
                "categoryType": 0,
                "protocolType": 0,
                "vendorType": 0
              },
              "storageStatus": {
                "message": "string",
                "statusType": 0
              },
              "workflowId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z",
              "tenantId": "string",
              "groupRef": {
                "id": "string",
                "name": "string"
              },
              "isAutodiscovered": true
            }
          },
          "copyAllowedStatistics": {
            "total": 0,
            "destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
              "accountId": "string",
              "source": "string",
              "storageFunctionality": "string",
              "storageType": {
                "name": "string",
                "categoryType": 0,
                "protocolType": 0,
                "vendorType": 0
              },
              "storageStatus": {
                "message": "string",
                "statusType": 0
              },
              "workflowId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z",
              "tenantId": "string",
              "groupRef": {
                "id": "string",
```

```
},
              "isAutodiscovered": true
            }
          },
          "copyBlockedStatistics": {
            "total": 0,
            "destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
              "accountId": "string",
              "source": "string",
              "storageFunctionality": "string",
              "storageType": {
                "name": "string",
                "categoryType": 0,
                "protocolType": 0,
                "vendorType": 0
              },
              "storageStatus": {
                "message": "string",
                "statusType": 0
              },
              "workflowId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z",
              "tenantId": "string",
              "groupRef": {
                "id": "string",
                "name": "string"
              },
              "isAutodiscovered": true
            }
          },
          "deleteAllowedStatistics": {
            "total": 0
          },
          "deleteBlockedStatistics": {
            "total": 0
          },
          "lastCalculatedStatisticsTime": "2019-08-24T14:15:22Z"
        },
        "account": {
          "id": "string",
          "name": "string",
          "description": "string",
          "credentials": "string",
          "protocolType": 0,
          "vendorType": 0,
          "autoDiscovery": true,
          "autodiscoveryDestinationGroupId": "string",
          "destinationGroup": {
            "id": "string",
```

```
}
        },
        "realTimeStartDate": "2019-08-24T14:15:22Z"
      }
    ],
    "storageId": "string",
    "discoveryCycleTiming": {
      "currentCycleStartedAt": "2019-08-24T14:15:22Z",
      "lastCycleStartedAt": "2019-08-24T14:15:22Z",
      "lastCycleFinishedAt": "2019-08-24T14:15:22Z",
      "lastCycleDurationSeconds": 0.1
    },
    "$type": "string"
  }
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» scan	ScanResponse¦null	false	none	none

StartScanCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "scanId": "string",
  "scanIds": [
    "string"
  ],
  "failedStorages": [
    {
      "id": "string",
      "reasonKey": "string",
      "reason": "string",
      "childFailures": [
        {}
      ]
    }
  ]
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» scanId	string¦null	false	none	none
» scanIds	[string]¦null	false	none	none
» failedStorages	[BulkFailedItem]¦null	false	none	none

AddScanParameters

```
{
  "storageId": "string",
  "name": "string",
  "folder": "string",
  "scanPartition": "string",
  "priority": 0,
  "storageIds": [
    "string"
  ],
  "workflowId": "string",
  "mdssBaseUrl": "string",
  "scanConfigDto": {
    "realTimeScanConfig": {
      "isEnabled": true,
      "startDate": "2019-08-24T14:15:22Z",
      "handlingType": 0
    }
  }
}
```


Properties

Name	Type	Required	Restrictions	Description
storageId	string¦null	false	none	This property is obsolete and will be removed in the future. Use StorageIds instead.
name	string	true	none	user-defined name for the scan
folder	string¦null	false	none	This property is obsolete and will be removed in the future. Use ScanPartition instead.
scanPartition	string¦null	false	none	partiton of storage where the scan will run
priority	integer(int32)	true	none	priority such as (low, medium, high)
storageIds	[string]¦null	false	none	id's of storages to be scanned
workflowId	string	true	none	associated workflow to be executed
mdssBaseUrl	string¦null	false	none	base URL for MDSS, if not provided will use Request.Host
scanConfigDto	ScanConfig¦null	false	none	none

ScanConfig


```
{
  "realTimeScanConfig": {
    "isEnabled": true,
    "startDate": "2019-08-24T14:15:22Z",
    "handlingType": 0
  }
}
```


Properties

Name	Type	Required	Restrictions	Description
realTimeScanConfig	RealTimeScanConfig¦null	false	none	none

RealTimeScanConfig


```
{
  "isEnabled": true,
  "startDate": "2019-08-24T14:15:22Z",
  "handlingType": 0
}
```


Properties

Name	Type	Required	Restrictions	Description
isEnabled	boolean	true	none	none
startDate	string(date-time)¦null	false	none	none
handlingType	RealTimeHandlingType	true	none	- 0: Polling - 1: EventBased

BulkStopScansCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "dispatched": [
    "string"
  ],
  "failed": [
    {
      "id": "string",
      "reasonKey": "string",
      "reason": "string",
      "childFailures": [
        {}
      ]
    }
  ]
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» dispatched	[string]	false	none	none
» failed	[BulkFailedItem]	false	none	none

BulkDeleteScansCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "succeeded": [
    "string"
  ],
  "failed": [
    {
      "id": "string",
      "reasonKey": "string",
      "reason": "string",
      "childFailures": [
        {}
      ]
    }
  ]
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» succeeded	[string]	false	none	none
» failed	[BulkFailedItem]	false	none	none

BulkDeleteScansParameters

```
{
  "scanIds": [
    "string"
  ],
  "forceDeleteRtp": true
}
```

Properties

Name	Type	Required	Restrictions	Description
scanIds	[string]	false	none	none
forceDeleteRtp	boolean	false	none	none

BulkStopScansParameters

```
{
  "scanIds": [
    "string"
  ]
}
```

Properties

Name	Type	Required	Restrictions	Description
scanIds	[string]	false	none	none

GetLastCompletedScanQueryResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "scan": {
    "result": 0,
    "responseKey": "string",
    "responseMessage": "string",
    "responseMessageParams": {
      "property1": "string",
      "property2": "string"
    },
    "id": "string",
    "name": "string",
    "startTime": "2019-08-24T14:15:22Z",
    "stopTime": "2019-08-24T14:15:22Z",
    "scanType": "string",
    "scanningState": 0,
    "scanStatusDto": {
      "pendingFilesCount": 0,
      "pendingFilesSize": 0,
      "allowedFilesCount": 0,
      "allowedFilesSize": 0,
      "blockedFilesCount": 0,
      "blockedFilesSize": 0,
      "sanitizedFilesCount": 0,
      "failedSanitizedFilesCount": 0,
      "remediatedFilesCount": 0,
      "totalFilesCount": 0,
      "totalFilesSize": 0,
      "processingFailedCount": 0,
      "processingFailedSize": 0,
      "processingFailedRemediationCount": 0,
      "processedFilesCount": 0,
      "processedFilesSize": 0,
      "canceledFilesCount": 0,
      "canceledFilesSize": 0
    },
    "scanStatsDto": {
      "infectedFilesCount": 0,
      "threatTotalFilesCount": 0,
      "filesWithVulnerabilitiesCount": 0,
      "filesWithSensitiveDataCount": 0,
      "filesBlockedBySandboxCount": 0,
      "scannedFilesCount": 0,
      "skippedFilesScanCount": 0,
      "scanFilesDistribution": {
        "documentsEncryptedFilesCount": 0,
```

```
"audioVideoFilesCount": 0,
        "openSSlEncryptedFilesCount": 0,
        "pdfFilesCount": 0,
        "graphicalFilesCount": 0,
        "diskImageFilesCount": 0,
        "textFilesCount": 0,
        "mailFilesCount": 0,
        "applicationFilesCount": 0,
        "documentsFilesCount": 0,
        "otherFilesCount": 0,
        "archivesFilesCount": 0
      }
    },
    "realTimeStartDate": "2019-08-24T14:15:22Z",
    "scanSequenceDto": {
      "previousScanId": "string",
      "nextScanId": "string"
    },
    "scanPartition": "string",
    "workflowId": "string",
    "scanConfigurationId": "string",
    "errors": [
      "string"
    ],
    "priority": 0,
    "scanWorkflowSnapshotDtos": [
      {
        "id": "string",
        "scanId": "string",
        "workflow": {
          "id": "string",
          "scanPoolId": "string",
          "scanProcessFlow": 0,
          "isIdentityScanningEnabled": true,
          "scanIntervalDays": 0,
          "rules": [
            "string"
          ],
          "type": 0,
          "workflowSupportedTechnologies": {
            "dlp": {
              "status": 0
            },
            "deepCdr": {
              "status": 0
            },
            "sandBox": {
              "status": 0
            },
            "metascan": {
              "status": 0
            }
          },
```

```
"userAgent": "string",
          "scanPool": {
            "id": "string",
            "name": "string",
            "scanPoolType": 0,
            "isDefault": true,
            "scanInstances": [
              {
                "id": "string",
                "scanPoolId": "string",
                "url": "string",
                "apiKey": "string",
                "timeout": "string",
                "scanInstanceType": 0
              }
            ]
          },
          "failOverScanPoolId": "string",
          "failOverScanPool": {
            "id": "string",
            "name": "string",
            "scanPoolType": 0,
            "isDefault": true,
            "scanInstances": [
              {
                "id": "string",
                "scanPoolId": "string",
                "url": "string",
                "apiKey": "string",
                "timeout": "string",
                "scanInstanceType": 0
              }
            ]
          },
          "filters": {
            "id": "string",
            "minimumSize": 0,
            "maximumSize": 0,
            "minimumDateTime": "2019-08-24T14:15:22Z",
            "maximumDateTime": "2019-08-24T14:15:22Z"
          },
          "fileDefinition": {
            "blockingStrategy": 0,
            "configurableBlockingStrategy": {
              "shouldTreatFilesWithSensitiveDataAsBlocked": true,
              "shouldTreatFilesWithVulnerabilitiesAsBlocked": true
            }
          },
          "remediations": [
            {
              "id": "string",
              "workflowId": "string",
              "isEnabled": true,
```

```
"type": 0,
              "handlingType": 0
            }
          ],
          "tenantId": "string"
        },
        "startTimestamp": 0,
        "stopTimestamp": 0,
        "scanPool": {
          "id": "string",
          "name": "string",
          "scanPoolType": 0,
          "isDefault": true,
          "scanInstances": [
            {
              "id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ]
        },
        "scanInstances": [
          {
            "id": "string",
            "scanPoolId": "string",
            "url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ],
        "failOverScanPool": {
          "id": "string",
          "name": "string",
          "scanPoolType": 0,
          "isDefault": true,
          "scanInstances": [
            {
              "id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ]
        },
        "failOverScanInstances": [
          {
            "id": "string",
```

```
"url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ],
        "storage": {
          "id": "string",
          "name": "string",
          "groupId": "string",
          "clientId": "string",
          "accountId": "string",
          "source": "string",
          "storageFunctionality": "string",
          "storageType": {
            "name": "string",
            "categoryType": 0,
            "protocolType": 0,
            "vendorType": 0
          },
          "storageStatus": {
            "message": "string",
            "statusType": 0
          },
          "workflowId": "string",
          "lastUpdated": "2019-08-24T14:15:22Z",
          "tenantId": "string",
          "groupRef": {
            "id": "string",
            "name": "string"
          },
          "isAutodiscovered": true
        },
        "workflowStatistics": {
          "taggingStatistics": {
            "total": 0
          },
          "keepAllowedStatistics": {
            "total": 0
          },
          "keepBlockedStatistics": {
            "total": 0
          },
          "keepSanitizedStatistics": {
            "total": 0
          },
          "movedAllowedStatistics": {
            "total": 0,
            "destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
```

```
"source": "string",
              "storageFunctionality": "string",
              "storageType": {
                "name": "string",
                "categoryType": 0,
                "protocolType": 0,
                "vendorType": 0
              },
              "storageStatus": {
                "message": "string",
                "statusType": 0
              },
              "workflowId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z",
              "tenantId": "string",
              "groupRef": {
                "id": "string",
                "name": "string"
              },
              "isAutodiscovered": true
            }
          },
          "movedSanitizedStatistics": {
            "total": 0,
            "destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
              "accountId": "string",
              "source": "string",
              "storageFunctionality": "string",
              "storageType": {
                "name": "string",
                "categoryType": 0,
                "protocolType": 0,
                "vendorType": 0
              },
              "storageStatus": {
                "message": "string",
                "statusType": 0
              },
              "workflowId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z",
              "tenantId": "string",
              "groupRef": {
                "id": "string",
                "name": "string"
              },
              "isAutodiscovered": true
            }
          },
          "movedBlockedStatistics": {
```

```
"destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
              "accountId": "string",
              "source": "string",
              "storageFunctionality": "string",
              "storageType": {
                "name": "string",
                "categoryType": 0,
                "protocolType": 0,
                "vendorType": 0
              },
              "storageStatus": {
                "message": "string",
                "statusType": 0
              },
              "workflowId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z",
              "tenantId": "string",
              "groupRef": {
                "id": "string",
                "name": "string"
              },
              "isAutodiscovered": true
            }
          },
          "copyAllowedStatistics": {
            "total": 0,
            "destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
              "accountId": "string",
              "source": "string",
              "storageFunctionality": "string",
              "storageType": {
                "name": "string",
                "categoryType": 0,
                "protocolType": 0,
                "vendorType": 0
              },
              "storageStatus": {
                "message": "string",
                "statusType": 0
              },
              "workflowId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z",
              "tenantId": "string",
              "groupRef": {
                "id": "string",
```

```
},
              "isAutodiscovered": true
            }
          },
          "copyBlockedStatistics": {
            "total": 0,
            "destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
              "accountId": "string",
              "source": "string",
              "storageFunctionality": "string",
              "storageType": {
                "name": "string",
                "categoryType": 0,
                "protocolType": 0,
                "vendorType": 0
              },
              "storageStatus": {
                "message": "string",
                "statusType": 0
              },
              "workflowId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z",
              "tenantId": "string",
              "groupRef": {
                "id": "string",
                "name": "string"
              },
              "isAutodiscovered": true
            }
          },
          "deleteAllowedStatistics": {
            "total": 0
          },
          "deleteBlockedStatistics": {
            "total": 0
          },
          "lastCalculatedStatisticsTime": "2019-08-24T14:15:22Z"
        },
        "account": {
          "id": "string",
          "name": "string",
          "description": "string",
          "credentials": "string",
          "protocolType": 0,
          "vendorType": 0,
          "autoDiscovery": true,
          "autodiscoveryDestinationGroupId": "string",
          "destinationGroup": {
            "id": "string",
```

```
}
        },
        "realTimeStartDate": "2019-08-24T14:15:22Z"
      }
    ],
    "storageId": "string",
    "discoveryCycleTiming": {
      "currentCycleStartedAt": "2019-08-24T14:15:22Z",
      "lastCycleStartedAt": "2019-08-24T14:15:22Z",
      "lastCycleFinishedAt": "2019-08-24T14:15:22Z",
      "lastCycleDurationSeconds": 0.1
    },
    "$type": "string"
  }
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» scan	ScanResponse¦null	false	none	none

GetActiveScanQueryResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "scan": {
    "result": 0,
    "responseKey": "string",
    "responseMessage": "string",
    "responseMessageParams": {
      "property1": "string",
      "property2": "string"
    },
    "id": "string",
    "name": "string",
    "startTime": "2019-08-24T14:15:22Z",
    "stopTime": "2019-08-24T14:15:22Z",
    "scanType": "string",
    "scanningState": 0,
    "scanStatusDto": {
      "pendingFilesCount": 0,
      "pendingFilesSize": 0,
      "allowedFilesCount": 0,
      "allowedFilesSize": 0,
      "blockedFilesCount": 0,
      "blockedFilesSize": 0,
      "sanitizedFilesCount": 0,
      "failedSanitizedFilesCount": 0,
      "remediatedFilesCount": 0,
      "totalFilesCount": 0,
      "totalFilesSize": 0,
      "processingFailedCount": 0,
      "processingFailedSize": 0,
      "processingFailedRemediationCount": 0,
      "processedFilesCount": 0,
      "processedFilesSize": 0,
      "canceledFilesCount": 0,
      "canceledFilesSize": 0
    },
    "scanStatsDto": {
      "infectedFilesCount": 0,
      "threatTotalFilesCount": 0,
      "filesWithVulnerabilitiesCount": 0,
      "filesWithSensitiveDataCount": 0,
      "filesBlockedBySandboxCount": 0,
      "scannedFilesCount": 0,
      "skippedFilesScanCount": 0,
      "scanFilesDistribution": {
        "documentsEncryptedFilesCount": 0,
```

```
"audioVideoFilesCount": 0,
        "openSSlEncryptedFilesCount": 0,
        "pdfFilesCount": 0,
        "graphicalFilesCount": 0,
        "diskImageFilesCount": 0,
        "textFilesCount": 0,
        "mailFilesCount": 0,
        "applicationFilesCount": 0,
        "documentsFilesCount": 0,
        "otherFilesCount": 0,
        "archivesFilesCount": 0
      }
    },
    "realTimeStartDate": "2019-08-24T14:15:22Z",
    "scanSequenceDto": {
      "previousScanId": "string",
      "nextScanId": "string"
    },
    "scanPartition": "string",
    "workflowId": "string",
    "scanConfigurationId": "string",
    "errors": [
      "string"
    ],
    "priority": 0,
    "scanWorkflowSnapshotDtos": [
      {
        "id": "string",
        "scanId": "string",
        "workflow": {
          "id": "string",
          "scanPoolId": "string",
          "scanProcessFlow": 0,
          "isIdentityScanningEnabled": true,
          "scanIntervalDays": 0,
          "rules": [
            "string"
          ],
          "type": 0,
          "workflowSupportedTechnologies": {
            "dlp": {
              "status": 0
            },
            "deepCdr": {
              "status": 0
            },
            "sandBox": {
              "status": 0
            },
            "metascan": {
              "status": 0
            }
          },
```

```
"userAgent": "string",
          "scanPool": {
            "id": "string",
            "name": "string",
            "scanPoolType": 0,
            "isDefault": true,
            "scanInstances": [
              {
                "id": "string",
                "scanPoolId": "string",
                "url": "string",
                "apiKey": "string",
                "timeout": "string",
                "scanInstanceType": 0
              }
            ]
          },
          "failOverScanPoolId": "string",
          "failOverScanPool": {
            "id": "string",
            "name": "string",
            "scanPoolType": 0,
            "isDefault": true,
            "scanInstances": [
              {
                "id": "string",
                "scanPoolId": "string",
                "url": "string",
                "apiKey": "string",
                "timeout": "string",
                "scanInstanceType": 0
              }
            ]
          },
          "filters": {
            "id": "string",
            "minimumSize": 0,
            "maximumSize": 0,
            "minimumDateTime": "2019-08-24T14:15:22Z",
            "maximumDateTime": "2019-08-24T14:15:22Z"
          },
          "fileDefinition": {
            "blockingStrategy": 0,
            "configurableBlockingStrategy": {
              "shouldTreatFilesWithSensitiveDataAsBlocked": true,
              "shouldTreatFilesWithVulnerabilitiesAsBlocked": true
            }
          },
          "remediations": [
            {
              "id": "string",
              "workflowId": "string",
              "isEnabled": true,
```

```
"type": 0,
              "handlingType": 0
            }
          ],
          "tenantId": "string"
        },
        "startTimestamp": 0,
        "stopTimestamp": 0,
        "scanPool": {
          "id": "string",
          "name": "string",
          "scanPoolType": 0,
          "isDefault": true,
          "scanInstances": [
            {
              "id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ]
        },
        "scanInstances": [
          {
            "id": "string",
            "scanPoolId": "string",
            "url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ],
        "failOverScanPool": {
          "id": "string",
          "name": "string",
          "scanPoolType": 0,
          "isDefault": true,
          "scanInstances": [
            {
              "id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ]
        },
        "failOverScanInstances": [
          {
            "id": "string",
```

```
"url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ],
        "storage": {
          "id": "string",
          "name": "string",
          "groupId": "string",
          "clientId": "string",
          "accountId": "string",
          "source": "string",
          "storageFunctionality": "string",
          "storageType": {
            "name": "string",
            "categoryType": 0,
            "protocolType": 0,
            "vendorType": 0
          },
          "storageStatus": {
            "message": "string",
            "statusType": 0
          },
          "workflowId": "string",
          "lastUpdated": "2019-08-24T14:15:22Z",
          "tenantId": "string",
          "groupRef": {
            "id": "string",
            "name": "string"
          },
          "isAutodiscovered": true
        },
        "workflowStatistics": {
          "taggingStatistics": {
            "total": 0
          },
          "keepAllowedStatistics": {
            "total": 0
          },
          "keepBlockedStatistics": {
            "total": 0
          },
          "keepSanitizedStatistics": {
            "total": 0
          },
          "movedAllowedStatistics": {
            "total": 0,
            "destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
```

```
"source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "movedSanitizedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "movedBlockedStatistics": {
```

```
"destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
              "accountId": "string",
              "source": "string",
              "storageFunctionality": "string",
              "storageType": {
                "name": "string",
                "categoryType": 0,
                "protocolType": 0,
                "vendorType": 0
              },
              "storageStatus": {
                "message": "string",
                "statusType": 0
              },
              "workflowId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z",
              "tenantId": "string",
              "groupRef": {
                "id": "string",
                "name": "string"
              },
              "isAutodiscovered": true
            }
          },
          "copyAllowedStatistics": {
            "total": 0,
            "destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
              "accountId": "string",
              "source": "string",
              "storageFunctionality": "string",
              "storageType": {
                "name": "string",
                "categoryType": 0,
                "protocolType": 0,
                "vendorType": 0
              },
              "storageStatus": {
                "message": "string",
                "statusType": 0
              },
              "workflowId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z",
              "tenantId": "string",
              "groupRef": {
                "id": "string",
```

```
},
              "isAutodiscovered": true
            }
          },
          "copyBlockedStatistics": {
            "total": 0,
            "destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
              "accountId": "string",
              "source": "string",
              "storageFunctionality": "string",
              "storageType": {
                "name": "string",
                "categoryType": 0,
                "protocolType": 0,
                "vendorType": 0
              },
              "storageStatus": {
                "message": "string",
                "statusType": 0
              },
              "workflowId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z",
              "tenantId": "string",
              "groupRef": {
                "id": "string",
                "name": "string"
              },
              "isAutodiscovered": true
            }
          },
          "deleteAllowedStatistics": {
            "total": 0
          },
          "deleteBlockedStatistics": {
            "total": 0
          },
          "lastCalculatedStatisticsTime": "2019-08-24T14:15:22Z"
        },
        "account": {
          "id": "string",
          "name": "string",
          "description": "string",
          "credentials": "string",
          "protocolType": 0,
          "vendorType": 0,
          "autoDiscovery": true,
          "autodiscoveryDestinationGroupId": "string",
          "destinationGroup": {
            "id": "string",
```

```
}
        },
        "realTimeStartDate": "2019-08-24T14:15:22Z"
      }
    ],
    "storageId": "string",
    "discoveryCycleTiming": {
      "currentCycleStartedAt": "2019-08-24T14:15:22Z",
      "lastCycleStartedAt": "2019-08-24T14:15:22Z",
      "lastCycleFinishedAt": "2019-08-24T14:15:22Z",
      "lastCycleDurationSeconds": 0.1
    },
    "$type": "string",
    "serviceName": "string",
    "storageName": "string",
    "currentProcessingFilePath": "string",
    "currentProcessingFileProgress": "string",
    "discoveryState": 0,
    "statusMessages": [
      {
        "message": "string",
        "severity": 0,
        "params": {
          "property1": "string",
          "property2": "string"
        }
      }
    ]
  }
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» scan	ActiveScanResponse¦null	false	none	none

ActiveScanResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "id": "string",
  "name": "string",
  "startTime": "2019-08-24T14:15:22Z",
  "stopTime": "2019-08-24T14:15:22Z",
  "scanType": "string",
  "scanningState": 0,
  "scanStatusDto": {
    "pendingFilesCount": 0,
    "pendingFilesSize": 0,
    "allowedFilesCount": 0,
    "allowedFilesSize": 0,
    "blockedFilesCount": 0,
    "blockedFilesSize": 0,
    "sanitizedFilesCount": 0,
    "failedSanitizedFilesCount": 0,
    "remediatedFilesCount": 0,
    "totalFilesCount": 0,
    "totalFilesSize": 0,
    "processingFailedCount": 0,
    "processingFailedSize": 0,
    "processingFailedRemediationCount": 0,
    "processedFilesCount": 0,
    "processedFilesSize": 0,
    "canceledFilesCount": 0,
    "canceledFilesSize": 0
  },
  "scanStatsDto": {
    "infectedFilesCount": 0,
    "threatTotalFilesCount": 0,
    "filesWithVulnerabilitiesCount": 0,
    "filesWithSensitiveDataCount": 0,
    "filesBlockedBySandboxCount": 0,
    "scannedFilesCount": 0,
    "skippedFilesScanCount": 0,
    "scanFilesDistribution": {
      "documentsEncryptedFilesCount": 0,
      "executablesFilesCount": 0,
      "audioVideoFilesCount": 0,
      "openSSlEncryptedFilesCount": 0,
      "pdfFilesCount": 0,
      "graphicalFilesCount": 0,
      "diskImageFilesCount": 0,
      "textFilesCount": 0,
      "mailFilesCount": 0,
```

```
"documentsFilesCount": 0,
      "otherFilesCount": 0,
      "archivesFilesCount": 0
    }
  },
  "realTimeStartDate": "2019-08-24T14:15:22Z",
  "scanSequenceDto": {
    "previousScanId": "string",
    "nextScanId": "string"
  },
  "scanPartition": "string",
  "workflowId": "string",
  "scanConfigurationId": "string",
  "errors": [
    "string"
  ],
  "priority": 0,
  "scanWorkflowSnapshotDtos": [
    {
      "id": "string",
      "scanId": "string",
      "workflow": {
        "id": "string",
        "scanPoolId": "string",
        "scanProcessFlow": 0,
        "isIdentityScanningEnabled": true,
        "scanIntervalDays": 0,
        "rules": [
          "string"
        ],
        "type": 0,
        "workflowSupportedTechnologies": {
          "dlp": {
            "status": 0
          },
          "deepCdr": {
            "status": 0
          },
          "sandBox": {
            "status": 0
          },
          "metascan": {
            "status": 0
          }
        },
        "name": "string",
        "userAgent": "string",
        "scanPool": {
          "id": "string",
          "name": "string",
          "scanPoolType": 0,
          "isDefault": true,
          "scanInstances": [
```

```
"id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ]
        },
        "failOverScanPoolId": "string",
        "failOverScanPool": {
          "id": "string",
          "name": "string",
          "scanPoolType": 0,
          "isDefault": true,
          "scanInstances": [
            {
              "id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ]
        },
        "filters": {
          "id": "string",
          "minimumSize": 0,
          "maximumSize": 0,
          "minimumDateTime": "2019-08-24T14:15:22Z",
          "maximumDateTime": "2019-08-24T14:15:22Z"
        },
        "fileDefinition": {
          "blockingStrategy": 0,
          "configurableBlockingStrategy": {
            "shouldTreatFilesWithSensitiveDataAsBlocked": true,
            "shouldTreatFilesWithVulnerabilitiesAsBlocked": true
          }
        },
        "remediations": [
          {
            "id": "string",
            "workflowId": "string",
            "isEnabled": true,
            "configuration": "string",
            "type": 0,
            "handlingType": 0
          }
        ],
        "tenantId": "string"
      },
      "startTimestamp": 0,
```

```
"scanPool": {
        "id": "string",
        "name": "string",
        "scanPoolType": 0,
        "isDefault": true,
        "scanInstances": [
          {
            "id": "string",
            "scanPoolId": "string",
            "url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ]
      },
      "scanInstances": [
        {
          "id": "string",
          "scanPoolId": "string",
          "url": "string",
          "apiKey": "string",
          "timeout": "string",
          "scanInstanceType": 0
        }
      ],
      "failOverScanPool": {
        "id": "string",
        "name": "string",
        "scanPoolType": 0,
        "isDefault": true,
        "scanInstances": [
          {
            "id": "string",
            "scanPoolId": "string",
            "url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ]
      },
      "failOverScanInstances": [
        {
          "id": "string",
          "scanPoolId": "string",
          "url": "string",
          "apiKey": "string",
          "timeout": "string",
          "scanInstanceType": 0
        }
      ],
      "storage": {
```

```
"name": "string",
        "groupId": "string",
        "clientId": "string",
        "accountId": "string",
        "source": "string",
        "storageFunctionality": "string",
        "storageType": {
          "name": "string",
          "categoryType": 0,
          "protocolType": 0,
          "vendorType": 0
        },
        "storageStatus": {
          "message": "string",
          "statusType": 0
        },
        "workflowId": "string",
        "lastUpdated": "2019-08-24T14:15:22Z",
        "tenantId": "string",
        "groupRef": {
          "id": "string",
          "name": "string"
        },
        "isAutodiscovered": true
      },
      "workflowStatistics": {
        "taggingStatistics": {
          "total": 0
        },
        "keepAllowedStatistics": {
          "total": 0
        },
        "keepBlockedStatistics": {
          "total": 0
        },
        "keepSanitizedStatistics": {
          "total": 0
        },
        "movedAllowedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
```

```
"storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "movedSanitizedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "movedBlockedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
```

```
"storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "copyAllowedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "copyBlockedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
```

```
"name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "deleteAllowedStatistics": {
          "total": 0
        },
        "deleteBlockedStatistics": {
          "total": 0
        },
        "lastCalculatedStatisticsTime": "2019-08-24T14:15:22Z"
      },
      "account": {
        "id": "string",
        "name": "string",
        "description": "string",
        "credentials": "string",
        "protocolType": 0,
        "vendorType": 0,
        "autoDiscovery": true,
        "autodiscoveryDestinationGroupId": "string",
        "destinationGroup": {
          "id": "string",
          "name": "string"
        }
      },
      "realTimeStartDate": "2019-08-24T14:15:22Z"
    }
  ],
  "storageId": "string",
  "discoveryCycleTiming": {
```

```
"lastCycleStartedAt": "2019-08-24T14:15:22Z",
    "lastCycleFinishedAt": "2019-08-24T14:15:22Z",
    "lastCycleDurationSeconds": 0.1
  },
  "$type": "string",
  "serviceName": "string",
  "storageName": "string",
  "currentProcessingFilePath": "string",
  "currentProcessingFileProgress": "string",
  "discoveryState": 0,
  "statusMessages": [
    {
      "message": "string",
      "severity": 0,
      "params": {
        "property1": "string",
        "property2": "string"
      }
    }
  ]
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	ScanResponse	false	none	none

and - discriminator: $type

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» serviceName	string	false	none	none
» storageName	string	false	none	none
» currentProcessingFilePath	string	false	none	none
» currentProcessingFileProgress	string	false	none	none
» discoveryState	DiscoveryState	false	none	- 0: NotStarted - 1: Running - 2: Cancelled - 3: Failed - 4: Completed
» statusMessages	[MessageTemplate]	false	none	none
» $type	string	true	none	none

DiscoveryState

```
0
```

- 0: NotStarted
- 1: Running
- 2: Cancelled
- 3: Failed
- 4: Completed

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: NotStarted - 1: Running - 2: Cancelled - 3: Failed - 4: Completed

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2
anonymous	3
anonymous	4

MessageTemplate

```
{
  "message": "string",
  "severity": 0,
  "params": {
    "property1": "string",
    "property2": "string"
  }
}
```

Properties

Name	Type	Required	Restrictions	Description
message	string	false	none	none
severity	MessageSeverity	false	none	- 0: Information - 1: Warning - 2: Error
params	object¦null	false	none	none
» **additionalProperties**	string	false	none	none

MessageSeverity

```
0
```

- 0: Information

- 1: Warning
- 2: Error

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: Information - 1: Warning - 2: Error

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2

ActiveRealTimeScanResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "id": "string",
  "name": "string",
  "startTime": "2019-08-24T14:15:22Z",
  "stopTime": "2019-08-24T14:15:22Z",
  "scanType": "string",
  "scanningState": 0,
  "scanStatusDto": {
    "pendingFilesCount": 0,
    "pendingFilesSize": 0,
    "allowedFilesCount": 0,
    "allowedFilesSize": 0,
    "blockedFilesCount": 0,
    "blockedFilesSize": 0,
    "sanitizedFilesCount": 0,
    "failedSanitizedFilesCount": 0,
    "remediatedFilesCount": 0,
    "totalFilesCount": 0,
    "totalFilesSize": 0,
    "processingFailedCount": 0,
    "processingFailedSize": 0,
    "processingFailedRemediationCount": 0,
    "processedFilesCount": 0,
    "processedFilesSize": 0,
    "canceledFilesCount": 0,
    "canceledFilesSize": 0
  },
  "scanStatsDto": {
    "infectedFilesCount": 0,
    "threatTotalFilesCount": 0,
    "filesWithVulnerabilitiesCount": 0,
    "filesWithSensitiveDataCount": 0,
    "filesBlockedBySandboxCount": 0,
    "scannedFilesCount": 0,
    "skippedFilesScanCount": 0,
    "scanFilesDistribution": {
      "documentsEncryptedFilesCount": 0,
      "executablesFilesCount": 0,
      "audioVideoFilesCount": 0,
      "openSSlEncryptedFilesCount": 0,
      "pdfFilesCount": 0,
      "graphicalFilesCount": 0,
      "diskImageFilesCount": 0,
      "textFilesCount": 0,
      "mailFilesCount": 0,
```

```
"documentsFilesCount": 0,
      "otherFilesCount": 0,
      "archivesFilesCount": 0
    }
  },
  "realTimeStartDate": "2019-08-24T14:15:22Z",
  "scanSequenceDto": {
    "previousScanId": "string",
    "nextScanId": "string"
  },
  "scanPartition": "string",
  "workflowId": "string",
  "scanConfigurationId": "string",
  "errors": [
    "string"
  ],
  "priority": 0,
  "scanWorkflowSnapshotDtos": [
    {
      "id": "string",
      "scanId": "string",
      "workflow": {
        "id": "string",
        "scanPoolId": "string",
        "scanProcessFlow": 0,
        "isIdentityScanningEnabled": true,
        "scanIntervalDays": 0,
        "rules": [
          "string"
        ],
        "type": 0,
        "workflowSupportedTechnologies": {
          "dlp": {
            "status": 0
          },
          "deepCdr": {
            "status": 0
          },
          "sandBox": {
            "status": 0
          },
          "metascan": {
            "status": 0
          }
        },
        "name": "string",
        "userAgent": "string",
        "scanPool": {
          "id": "string",
          "name": "string",
          "scanPoolType": 0,
          "isDefault": true,
          "scanInstances": [
```

```
"id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ]
        },
        "failOverScanPoolId": "string",
        "failOverScanPool": {
          "id": "string",
          "name": "string",
          "scanPoolType": 0,
          "isDefault": true,
          "scanInstances": [
            {
              "id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ]
        },
        "filters": {
          "id": "string",
          "minimumSize": 0,
          "maximumSize": 0,
          "minimumDateTime": "2019-08-24T14:15:22Z",
          "maximumDateTime": "2019-08-24T14:15:22Z"
        },
        "fileDefinition": {
          "blockingStrategy": 0,
          "configurableBlockingStrategy": {
            "shouldTreatFilesWithSensitiveDataAsBlocked": true,
            "shouldTreatFilesWithVulnerabilitiesAsBlocked": true
          }
        },
        "remediations": [
          {
            "id": "string",
            "workflowId": "string",
            "isEnabled": true,
            "configuration": "string",
            "type": 0,
            "handlingType": 0
          }
        ],
        "tenantId": "string"
      },
      "startTimestamp": 0,
```

```
"scanPool": {
        "id": "string",
        "name": "string",
        "scanPoolType": 0,
        "isDefault": true,
        "scanInstances": [
          {
            "id": "string",
            "scanPoolId": "string",
            "url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ]
      },
      "scanInstances": [
        {
          "id": "string",
          "scanPoolId": "string",
          "url": "string",
          "apiKey": "string",
          "timeout": "string",
          "scanInstanceType": 0
        }
      ],
      "failOverScanPool": {
        "id": "string",
        "name": "string",
        "scanPoolType": 0,
        "isDefault": true,
        "scanInstances": [
          {
            "id": "string",
            "scanPoolId": "string",
            "url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ]
      },
      "failOverScanInstances": [
        {
          "id": "string",
          "scanPoolId": "string",
          "url": "string",
          "apiKey": "string",
          "timeout": "string",
          "scanInstanceType": 0
        }
      ],
      "storage": {
```

```
"name": "string",
        "groupId": "string",
        "clientId": "string",
        "accountId": "string",
        "source": "string",
        "storageFunctionality": "string",
        "storageType": {
          "name": "string",
          "categoryType": 0,
          "protocolType": 0,
          "vendorType": 0
        },
        "storageStatus": {
          "message": "string",
          "statusType": 0
        },
        "workflowId": "string",
        "lastUpdated": "2019-08-24T14:15:22Z",
        "tenantId": "string",
        "groupRef": {
          "id": "string",
          "name": "string"
        },
        "isAutodiscovered": true
      },
      "workflowStatistics": {
        "taggingStatistics": {
          "total": 0
        },
        "keepAllowedStatistics": {
          "total": 0
        },
        "keepBlockedStatistics": {
          "total": 0
        },
        "keepSanitizedStatistics": {
          "total": 0
        },
        "movedAllowedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
```

```
"storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "movedSanitizedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "movedBlockedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
```

```
"storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "copyAllowedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "copyBlockedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
```

```
"name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "deleteAllowedStatistics": {
          "total": 0
        },
        "deleteBlockedStatistics": {
          "total": 0
        },
        "lastCalculatedStatisticsTime": "2019-08-24T14:15:22Z"
      },
      "account": {
        "id": "string",
        "name": "string",
        "description": "string",
        "credentials": "string",
        "protocolType": 0,
        "vendorType": 0,
        "autoDiscovery": true,
        "autodiscoveryDestinationGroupId": "string",
        "destinationGroup": {
          "id": "string",
          "name": "string"
        }
      },
      "realTimeStartDate": "2019-08-24T14:15:22Z"
    }
  ],
  "storageId": "string",
  "discoveryCycleTiming": {
```

```
"lastCycleStartedAt": "2019-08-24T14:15:22Z",
    "lastCycleFinishedAt": "2019-08-24T14:15:22Z",
    "lastCycleDurationSeconds": 0.1
  },
  "$type": "string",
  "serviceName": "string",
  "storageName": "string",
  "currentProcessingFilePath": "string",
  "currentProcessingFileProgress": "string",
  "discoveryState": 0,
  "statusMessages": [
    {
      "message": "string",
      "severity": 0,
      "params": {
        "property1": "string",
        "property2": "string"
      }
    }
  ],
  "isRealTimeEnabled": true,
  "handlingType": 0
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	ActiveScanResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» isRealTimeEnabled	boolean	false	none	none
» handlingType	RealTimeHandlingType	false	none	- 0: Polling - 1: EventBased

GetRealTimeProcessingScanQueryResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "scan": {
    "result": 0,
    "responseKey": "string",
    "responseMessage": "string",
    "responseMessageParams": {
      "property1": "string",
      "property2": "string"
    },
    "id": "string",
    "name": "string",
    "startTime": "2019-08-24T14:15:22Z",
    "stopTime": "2019-08-24T14:15:22Z",
    "scanType": "string",
    "scanningState": 0,
    "scanStatusDto": {
      "pendingFilesCount": 0,
      "pendingFilesSize": 0,
      "allowedFilesCount": 0,
      "allowedFilesSize": 0,
      "blockedFilesCount": 0,
      "blockedFilesSize": 0,
      "sanitizedFilesCount": 0,
      "failedSanitizedFilesCount": 0,
      "remediatedFilesCount": 0,
      "totalFilesCount": 0,
      "totalFilesSize": 0,
      "processingFailedCount": 0,
      "processingFailedSize": 0,
      "processingFailedRemediationCount": 0,
      "processedFilesCount": 0,
      "processedFilesSize": 0,
      "canceledFilesCount": 0,
      "canceledFilesSize": 0
    },
    "scanStatsDto": {
      "infectedFilesCount": 0,
      "threatTotalFilesCount": 0,
      "filesWithVulnerabilitiesCount": 0,
      "filesWithSensitiveDataCount": 0,
      "filesBlockedBySandboxCount": 0,
      "scannedFilesCount": 0,
      "skippedFilesScanCount": 0,
      "scanFilesDistribution": {
        "documentsEncryptedFilesCount": 0,
```

```
"audioVideoFilesCount": 0,
        "openSSlEncryptedFilesCount": 0,
        "pdfFilesCount": 0,
        "graphicalFilesCount": 0,
        "diskImageFilesCount": 0,
        "textFilesCount": 0,
        "mailFilesCount": 0,
        "applicationFilesCount": 0,
        "documentsFilesCount": 0,
        "otherFilesCount": 0,
        "archivesFilesCount": 0
      }
    },
    "realTimeStartDate": "2019-08-24T14:15:22Z",
    "scanSequenceDto": {
      "previousScanId": "string",
      "nextScanId": "string"
    },
    "scanPartition": "string",
    "workflowId": "string",
    "scanConfigurationId": "string",
    "errors": [
      "string"
    ],
    "priority": 0,
    "scanWorkflowSnapshotDtos": [
      {
        "id": "string",
        "scanId": "string",
        "workflow": {
          "id": "string",
          "scanPoolId": "string",
          "scanProcessFlow": 0,
          "isIdentityScanningEnabled": true,
          "scanIntervalDays": 0,
          "rules": [
            "string"
          ],
          "type": 0,
          "workflowSupportedTechnologies": {
            "dlp": {
              "status": 0
            },
            "deepCdr": {
              "status": 0
            },
            "sandBox": {
              "status": 0
            },
            "metascan": {
              "status": 0
            }
          },
```

```
"userAgent": "string",
          "scanPool": {
            "id": "string",
            "name": "string",
            "scanPoolType": 0,
            "isDefault": true,
            "scanInstances": [
              {
                "id": "string",
                "scanPoolId": "string",
                "url": "string",
                "apiKey": "string",
                "timeout": "string",
                "scanInstanceType": 0
              }
            ]
          },
          "failOverScanPoolId": "string",
          "failOverScanPool": {
            "id": "string",
            "name": "string",
            "scanPoolType": 0,
            "isDefault": true,
            "scanInstances": [
              {
                "id": "string",
                "scanPoolId": "string",
                "url": "string",
                "apiKey": "string",
                "timeout": "string",
                "scanInstanceType": 0
              }
            ]
          },
          "filters": {
            "id": "string",
            "minimumSize": 0,
            "maximumSize": 0,
            "minimumDateTime": "2019-08-24T14:15:22Z",
            "maximumDateTime": "2019-08-24T14:15:22Z"
          },
          "fileDefinition": {
            "blockingStrategy": 0,
            "configurableBlockingStrategy": {
              "shouldTreatFilesWithSensitiveDataAsBlocked": true,
              "shouldTreatFilesWithVulnerabilitiesAsBlocked": true
            }
          },
          "remediations": [
            {
              "id": "string",
              "workflowId": "string",
              "isEnabled": true,
```

```
"type": 0,
              "handlingType": 0
            }
          ],
          "tenantId": "string"
        },
        "startTimestamp": 0,
        "stopTimestamp": 0,
        "scanPool": {
          "id": "string",
          "name": "string",
          "scanPoolType": 0,
          "isDefault": true,
          "scanInstances": [
            {
              "id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ]
        },
        "scanInstances": [
          {
            "id": "string",
            "scanPoolId": "string",
            "url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ],
        "failOverScanPool": {
          "id": "string",
          "name": "string",
          "scanPoolType": 0,
          "isDefault": true,
          "scanInstances": [
            {
              "id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ]
        },
        "failOverScanInstances": [
          {
            "id": "string",
```

```
"url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ],
        "storage": {
          "id": "string",
          "name": "string",
          "groupId": "string",
          "clientId": "string",
          "accountId": "string",
          "source": "string",
          "storageFunctionality": "string",
          "storageType": {
            "name": "string",
            "categoryType": 0,
            "protocolType": 0,
            "vendorType": 0
          },
          "storageStatus": {
            "message": "string",
            "statusType": 0
          },
          "workflowId": "string",
          "lastUpdated": "2019-08-24T14:15:22Z",
          "tenantId": "string",
          "groupRef": {
            "id": "string",
            "name": "string"
          },
          "isAutodiscovered": true
        },
        "workflowStatistics": {
          "taggingStatistics": {
            "total": 0
          },
          "keepAllowedStatistics": {
            "total": 0
          },
          "keepBlockedStatistics": {
            "total": 0
          },
          "keepSanitizedStatistics": {
            "total": 0
          },
          "movedAllowedStatistics": {
            "total": 0,
            "destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
```

```
"source": "string",
              "storageFunctionality": "string",
              "storageType": {
                "name": "string",
                "categoryType": 0,
                "protocolType": 0,
                "vendorType": 0
              },
              "storageStatus": {
                "message": "string",
                "statusType": 0
              },
              "workflowId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z",
              "tenantId": "string",
              "groupRef": {
                "id": "string",
                "name": "string"
              },
              "isAutodiscovered": true
            }
          },
          "movedSanitizedStatistics": {
            "total": 0,
            "destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
              "accountId": "string",
              "source": "string",
              "storageFunctionality": "string",
              "storageType": {
                "name": "string",
                "categoryType": 0,
                "protocolType": 0,
                "vendorType": 0
              },
              "storageStatus": {
                "message": "string",
                "statusType": 0
              },
              "workflowId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z",
              "tenantId": "string",
              "groupRef": {
                "id": "string",
                "name": "string"
              },
              "isAutodiscovered": true
            }
          },
          "movedBlockedStatistics": {
```

```
"destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
              "accountId": "string",
              "source": "string",
              "storageFunctionality": "string",
              "storageType": {
                "name": "string",
                "categoryType": 0,
                "protocolType": 0,
                "vendorType": 0
              },
              "storageStatus": {
                "message": "string",
                "statusType": 0
              },
              "workflowId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z",
              "tenantId": "string",
              "groupRef": {
                "id": "string",
                "name": "string"
              },
              "isAutodiscovered": true
            }
          },
          "copyAllowedStatistics": {
            "total": 0,
            "destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
              "accountId": "string",
              "source": "string",
              "storageFunctionality": "string",
              "storageType": {
                "name": "string",
                "categoryType": 0,
                "protocolType": 0,
                "vendorType": 0
              },
              "storageStatus": {
                "message": "string",
                "statusType": 0
              },
              "workflowId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z",
              "tenantId": "string",
              "groupRef": {
                "id": "string",
```

```
},
              "isAutodiscovered": true
            }
          },
          "copyBlockedStatistics": {
            "total": 0,
            "destinationStorageInformation": {
              "id": "string",
              "name": "string",
              "groupId": "string",
              "clientId": "string",
              "accountId": "string",
              "source": "string",
              "storageFunctionality": "string",
              "storageType": {
                "name": "string",
                "categoryType": 0,
                "protocolType": 0,
                "vendorType": 0
              },
              "storageStatus": {
                "message": "string",
                "statusType": 0
              },
              "workflowId": "string",
              "lastUpdated": "2019-08-24T14:15:22Z",
              "tenantId": "string",
              "groupRef": {
                "id": "string",
                "name": "string"
              },
              "isAutodiscovered": true
            }
          },
          "deleteAllowedStatistics": {
            "total": 0
          },
          "deleteBlockedStatistics": {
            "total": 0
          },
          "lastCalculatedStatisticsTime": "2019-08-24T14:15:22Z"
        },
        "account": {
          "id": "string",
          "name": "string",
          "description": "string",
          "credentials": "string",
          "protocolType": 0,
          "vendorType": 0,
          "autoDiscovery": true,
          "autodiscoveryDestinationGroupId": "string",
          "destinationGroup": {
            "id": "string",
```

```
}
        },
        "realTimeStartDate": "2019-08-24T14:15:22Z"
      }
    ],
    "storageId": "string",
    "discoveryCycleTiming": {
      "currentCycleStartedAt": "2019-08-24T14:15:22Z",
      "lastCycleStartedAt": "2019-08-24T14:15:22Z",
      "lastCycleFinishedAt": "2019-08-24T14:15:22Z",
      "lastCycleDurationSeconds": 0.1
    },
    "$type": "string",
    "isRealTimeEnabled": true,
    "handlingType": 0
  }
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» scan	RealTimeScanResponse¦null	false	none	none

GetAllScanInstancesCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "entries": [
    {
      "id": "string",
      "scanPoolId": "string",
      "url": "string",
      "apiKey": "string",
      "timeout": "string",
      "scanInstanceType": 0
    }
  ]
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» entries	[ScanInstance]¦null	false	none	none

GetScanInstanceByIdCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "entry": {
    "id": "string",
    "scanPoolId": "string",
    "url": "string",
    "apiKey": "string",
    "timeout": "string",
    "scanInstanceType": 0
  }
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» entry	ScanInstance|null	false	none	none

AddScanInstanceCommandResponse


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "scanInstanceId": "string"
}
```

Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» scanInstanceId	string¦null	false	none	none

AddScanInstanceParameters

```
{
  "scanPoolId": "string",
  "url": "http://example.com",
  "apiKey": "string",
  "timeout": "string",
  "scanInstanceType": 0
}
```

Properties

Name	Type	Required	Restrictions	Description
scanPoolId	string	true	none	none
url	string(uri)	true	none	none
apiKey	string¦null	false	none	none
timeout	string¦null	false	none	none
scanInstanceType	ScanInstanceType	true	none	- 0: MdCore - 1: MdCloud

UpdateScanInstanceCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none

UpdateScanInstanceParameters


```
{
  "id": "string",
  "url": "http://example.com",
  "apiKey": "string",
  "timeout": "string"
}
```


Properties

Name	Type	Required	Restrictions	Description
id	string	true	none	none
url	string(uri)¦null	false	none	none
apiKey	string¦null	false	none	none
timeout	string¦null	false	none	none

DeleteScanInstanceCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```

Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none

TestScanInstanceCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```

Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none

TestScanInstanceParameters

```
{
  "url": "string",
  "rules": [
    "string"
  ],
  "apiKey": "string",
  "userAgent": "string",
  "isCloudInstance": true
}
```

Properties

Name	Type	Required	Restrictions	Description
url	string	true	none	none
rules	[string]	true	none	none
apiKey	string¦null	false	none	none
userAgent	string¦null	false	none	none
isCloudInstance	boolean¦null	false	none	none

GetAllScanPoolsCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "entries": [
    {
      "id": "string",
      "name": "string",
      "scanPoolType": 0,
      "isDefault": true,
      "scanInstances": [
        {
          "id": "string",
          "scanPoolId": "string",
          "url": "string",
          "apiKey": "string",
          "timeout": "string",
          "scanInstanceType": 0
        }
      ]
    }
  ]
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» entries	[ScanPool]¦null	false	none	none

GetScanPoolByIdCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "entry": {
    "id": "string",
    "name": "string",
    "scanPoolType": 0,
    "isDefault": true,
    "scanInstances": [
      {
        "id": "string",
        "scanPoolId": "string",
        "url": "string",
        "apiKey": "string",
        "timeout": "string",
        "scanInstanceType": 0
      }
    ]
  }
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» entry	ScanPool¦null	false	none	none

AddScanPoolCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "scanPoolId": "string"
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» scanPoolId	string¦null	false	none	none

AddScanPoolParameters


```
{
  "name": "string",
  "scanPoolType": 0
}
```


Properties

Name	Type	Required	Restrictions	Description
name	string	true	none	none
scanPoolType	ScanInstanceType	true	none	- 0: MdCore - 1: MdCloud

UpdateScanPoolCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```

Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none

UpdateScanPoolParameters

```
{
  "id": "string",
  "name": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
id	string	true	none	none
name	string¦null	false	none	none

DeleteScanPoolCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```

Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none

GetScanWorkflowSnapshotsFromScanQueryResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "scanWorkflowSnapshots": [
    {
      "id": "string",
      "scanId": "string",
      "workflow": {
        "id": "string",
        "scanPoolId": "string",
        "scanProcessFlow": 0,
        "isIdentityScanningEnabled": true,
        "scanIntervalDays": 0,
        "rules": [
          "string"
        ],
        "type": 0,
        "workflowSupportedTechnologies": {
          "dlp": {
            "status": 0
          },
          "deepCdr": {
            "status": 0
          },
          "sandBox": {
            "status": 0
          },
          "metascan": {
            "status": 0
          }
        },
        "name": "string",
        "userAgent": "string",
        "scanPool": {
          "id": "string",
          "name": "string",
          "scanPoolType": 0,
          "isDefault": true,
          "scanInstances": [
            {
              "id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
```

```
},
        "failOverScanPoolId": "string",
        "failOverScanPool": {
          "id": "string",
          "name": "string",
          "scanPoolType": 0,
          "isDefault": true,
          "scanInstances": [
            {
              "id": "string",
              "scanPoolId": "string",
              "url": "string",
              "apiKey": "string",
              "timeout": "string",
              "scanInstanceType": 0
            }
          ]
        },
        "filters": {
          "id": "string",
          "minimumSize": 0,
          "maximumSize": 0,
          "minimumDateTime": "2019-08-24T14:15:22Z",
          "maximumDateTime": "2019-08-24T14:15:22Z"
        },
        "fileDefinition": {
          "blockingStrategy": 0,
          "configurableBlockingStrategy": {
            "shouldTreatFilesWithSensitiveDataAsBlocked": true,
            "shouldTreatFilesWithVulnerabilitiesAsBlocked": true
          }
        },
        "remediations": [
          {
            "id": "string",
            "workflowId": "string",
            "isEnabled": true,
            "configuration": "string",
            "type": 0,
            "handlingType": 0
          }
        ],
        "tenantId": "string"
      },
      "startTimestamp": 0,
      "stopTimestamp": 0,
      "scanPool": {
        "id": "string",
        "name": "string",
        "scanPoolType": 0,
        "isDefault": true,
        "scanInstances": [
          {
```

```
"scanPoolId": "string",
            "url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ]
      },
      "scanInstances": [
        {
          "id": "string",
          "scanPoolId": "string",
          "url": "string",
          "apiKey": "string",
          "timeout": "string",
          "scanInstanceType": 0
        }
      ],
      "failOverScanPool": {
        "id": "string",
        "name": "string",
        "scanPoolType": 0,
        "isDefault": true,
        "scanInstances": [
          {
            "id": "string",
            "scanPoolId": "string",
            "url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ]
      },
      "failOverScanInstances": [
        {
          "id": "string",
          "scanPoolId": "string",
          "url": "string",
          "apiKey": "string",
          "timeout": "string",
          "scanInstanceType": 0
        }
      ],
      "storage": {
        "id": "string",
        "name": "string",
        "groupId": "string",
        "clientId": "string",
        "accountId": "string",
        "source": "string",
        "storageFunctionality": "string",
        "storageType": {
```

```
"categoryType": 0,
          "protocolType": 0,
          "vendorType": 0
        },
        "storageStatus": {
          "message": "string",
          "statusType": 0
        },
        "workflowId": "string",
        "lastUpdated": "2019-08-24T14:15:22Z",
        "tenantId": "string",
        "groupRef": {
          "id": "string",
          "name": "string"
        },
        "isAutodiscovered": true
      },
      "workflowStatistics": {
        "taggingStatistics": {
          "total": 0
        },
        "keepAllowedStatistics": {
          "total": 0
        },
        "keepBlockedStatistics": {
          "total": 0
        },
        "keepSanitizedStatistics": {
          "total": 0
        },
        "movedAllowedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
```

```
"id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "movedSanitizedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "movedBlockedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
```

```
"statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "copyAllowedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
              "name": "string",
              "categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "copyBlockedStatistics": {
          "total": 0,
          "destinationStorageInformation": {
            "id": "string",
            "name": "string",
            "groupId": "string",
            "clientId": "string",
            "accountId": "string",
            "source": "string",
            "storageFunctionality": "string",
            "storageType": {
```

```
"categoryType": 0,
              "protocolType": 0,
              "vendorType": 0
            },
            "storageStatus": {
              "message": "string",
              "statusType": 0
            },
            "workflowId": "string",
            "lastUpdated": "2019-08-24T14:15:22Z",
            "tenantId": "string",
            "groupRef": {
              "id": "string",
              "name": "string"
            },
            "isAutodiscovered": true
          }
        },
        "deleteAllowedStatistics": {
          "total": 0
        },
        "deleteBlockedStatistics": {
          "total": 0
        },
        "lastCalculatedStatisticsTime": "2019-08-24T14:15:22Z"
      },
      "account": {
        "id": "string",
        "name": "string",
        "description": "string",
        "credentials": "string",
        "protocolType": 0,
        "vendorType": 0,
        "autoDiscovery": true,
        "autodiscoveryDestinationGroupId": "string",
        "destinationGroup": {
          "id": "string",
          "name": "string"
        }
      },
      "realTimeStartDate": "2019-08-24T14:15:22Z"
    }
  ]
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» scanWorkflowSnapshots	[ScanWorkflowSnapshot]	false	none	none

UpdateNotificationsConfigResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "newNotificationsConfig": {
    "id": "string",
    "emailNotificationsConfig": {
      "userRequestNotificationsConfig": {
        "isEnabled": true
      },
      "generatedReportNotificationsConfig": {
        "isEnabled": true,
        "recipientsType": 0
      },
      "blockedFileNotificationsConfig": {
        "isEnabled": true,
        "recipientsType": 0
      }
    },
    "webhookNotificationsConfig": {
      "scanCompletedNotificationsConfig": {
        "isEnabled": true
      },
      "fileScannedNotificationConfig": {
        "isEnabled": true,
        "notificationScope": 0
      },
      "destinationAddress": "string",
      "headers": {
        "property1": "string",
        "property2": "string"
      },
      "requestType": 0
    },
    "rabbitMqNotificationsConfig": {
      "fileScannedNotificationConfig": {
        "isEnabled": true,
        "notificationScope": 0
      },
      "rabbitMqUrl": "string",
      "headers": {
        "property1": "string",
        "property2": "string"
      }
    }
  },
  "initialNotificationsConfig": {
    "id": "string",
```

```
"userRequestNotificationsConfig": {
        "isEnabled": true
      },
      "generatedReportNotificationsConfig": {
        "isEnabled": true,
        "recipientsType": 0
      },
      "blockedFileNotificationsConfig": {
        "isEnabled": true,
        "recipientsType": 0
      }
    },
    "webhookNotificationsConfig": {
      "scanCompletedNotificationsConfig": {
        "isEnabled": true
      },
      "fileScannedNotificationConfig": {
        "isEnabled": true,
        "notificationScope": 0
      },
      "destinationAddress": "string",
      "headers": {
        "property1": "string",
        "property2": "string"
      },
      "requestType": 0
    },
    "rabbitMqNotificationsConfig": {
      "fileScannedNotificationConfig": {
        "isEnabled": true,
        "notificationScope": 0
      },
      "rabbitMqUrl": "string",
      "headers": {
        "property1": "string",
        "property2": "string"
      }
    }
  },
  "typeResults": [
    {
      "type": 0,
      "status": 0,
      "errorKey": "string",
      "errorMessage": "string"
    }
  ]
}
```

Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» newNotificationsConfig	NotificationsConfig¦null	false	none	none
» initialNotificationsConfig	NotificationsConfig¦null	false	none	none
» typeResults	[NotificationTypeUpdateResult]¦null	false	none	none

NotificationsConfig

```
{
  "id": "string",
  "emailNotificationsConfig": {
    "userRequestNotificationsConfig": {
      "isEnabled": true
    },
    "generatedReportNotificationsConfig": {
      "isEnabled": true,
      "recipientsType": 0
    },
    "blockedFileNotificationsConfig": {
      "isEnabled": true,
      "recipientsType": 0
    }
  },
  "webhookNotificationsConfig": {
    "scanCompletedNotificationsConfig": {
      "isEnabled": true
    },
    "fileScannedNotificationConfig": {
      "isEnabled": true,
      "notificationScope": 0
    },
    "destinationAddress": "string",
    "headers": {
      "property1": "string",
      "property2": "string"
    },
    "requestType": 0
  },
  "rabbitMqNotificationsConfig": {
    "fileScannedNotificationConfig": {
      "isEnabled": true,
      "notificationScope": 0
    },
    "rabbitMqUrl": "string",
    "headers": {
      "property1": "string",
      "property2": "string"
    }
  }
}
```

Properties

Name	Type	Required	Restrictions	Description
id	string	true	none	none
emailNotificationsConfig	EmailNotificationsConfig	true	none	none
webhookNotificationsConfig	WebhookNotificationsConfig	true	none	none
rabbitMqNotificationsConfig	RabbitMqNotificationsConfig	true	none	none

EmailNotificationsConfig

```
{
  "userRequestNotificationsConfig": {
    "isEnabled": true
  },
  "generatedReportNotificationsConfig": {
    "isEnabled": true,
    "recipientsType": 0
  },
  "blockedFileNotificationsConfig": {
    "isEnabled": true,
    "recipientsType": 0
  }
}
```

Properties

Name	Type	Required	Restrictions	Description
userRequestNotificationsConfig	UserRequestNotificationsConfig	true	none	none
generatedReportNotificationsConfig	GeneratedReportNotificationsConfig	true	none	none
blockedFileNotificationsConfig	BlockedFileNotificationsConfig	true	none	none

UserRequestNotificationsConfig

```
{
  "isEnabled": true
}
```

Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	NotificationsConfigBase	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none

NotificationsConfigBase

```
{
  "isEnabled": true
}
```

Properties

Name	Type	Required	Restrictions	Description
isEnabled	boolean	false	none	none

GeneratedReportNotificationsConfig

```
{
  "isEnabled": true,
  "recipientsType": 0
}
```

Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	NotificationsConfigBase	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» recipientsType	GeneratedReportNotificationsRecipientsType	false	none	- 0: OwnerOnly - 1: AllRegisteredUsers

GeneratedReportNotificationsRecipientsType

```
0
```

- 0: OwnerOnly
- 1: AllRegisteredUsers

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: OwnerOnly - 1: AllRegisteredUsers

Enumerated Values

Property	Value
anonymous	0
anonymous	1

BlockedFileNotificationsConfig

```
{
  "isEnabled": true,
  "recipientsType": 0
}
```

Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	NotificationsConfigBase	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» recipientsType	BlockedFileNotificationsRecipientsType	false	none	- 0: AllRegisteredUsers - 1: FileOwner - 2: FileOwnerAndAllRegisteredUsers

BlockedFileNotificationsRecipientsType

```
0
```

- 0: AllRegisteredUsers
- 1: FileOwner
- 2: FileOwnerAndAllRegisteredUsers

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: AllRegisteredUsers - 1: FileOwner - 2: FileOwnerAndAllRegisteredUsers

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2

WebhookNotificationsConfig

```
{
  "scanCompletedNotificationsConfig": {
    "isEnabled": true
  },
  "fileScannedNotificationConfig": {
    "isEnabled": true,
    "notificationScope": 0
  },
  "destinationAddress": "string",
  "headers": {
    "property1": "string",
    "property2": "string"
  },
  "requestType": 0
}
```


Properties

Name	Type	Required	Restrictions	Description
scanCompletedNotificationsConfig	ScanCompletedNotificationsConfig	true	none	none
fileScannedNotificationConfig	FileScannedNotificationConfig	true	none	none
destinationAddress	string¦null	false	none	none
headers	object¦null	false	none	none
» **additionalProperties**	string	false	none	none
requestType	RequestType	false	none	- 0: Post - 1: Put

ScanCompletedNotificationsConfig


```
{
  "isEnabled": true
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	NotificationsConfigBase	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none

FileScannedNotificationConfig

```
{
  "isEnabled": true,
  "notificationScope": 0
}
```

Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	NotificationsConfigBase	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» notificationScope	FileNotificationScope	false	none	- 0: BlockedFilesOnly - 1: AllFiles

FileNotificationScope

```
0
```

- 0: BlockedFilesOnly
- 1: AllFiles

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: BlockedFilesOnly - 1: AllFiles

Enumerated Values

Property	Value
anonymous	0
anonymous	1

RequestType

```
0
```

- 0: Post
- 1: Put

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: Post - 1: Put

Enumerated Values

Property	Value
anonymous	0
anonymous	1

RabbitMqNotificationsConfig

```
{
  "fileScannedNotificationConfig": {
    "isEnabled": true,
    "notificationScope": 0
  },
  "rabbitMqUrl": "string",
  "headers": {
    "property1": "string",
    "property2": "string"
  }
}
```


Properties

Name	Type	Required	Restrictions	Description
fileScannedNotificationConfig	FileScannedNotificationConfig	true	none	none
rabbitMqUrl	string¦null	false	none	none
headers	object¦null	false	none	none
» **additionalProperties**	string	false	none	none

NotificationTypeUpdateResult


```
{
  "type": 0,
  "status": 0,
  "errorKey": "string",
  "errorMessage": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
type	NotificationType	true	none	- 0: Email - 1: Webhook - 2: RabbitMq
status	UpdateStatus	true	none	- 0: Success - 1: Failed - 2: Skipped
errorKey	string¦null	false	none	none
errorMessage	string¦null	false	none	none

NotificationType

```
0
```

- 0: Email
- 1: Webhook
- 2: RabbitMq

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: Email - 1: Webhook - 2: RabbitMq

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2

UpdateStatus

```
0
```

- 0: Success
- 1: Failed
- 2: Skipped

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: Success - 1: Failed - 2: Skipped

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2

NotificationsConfigParameters

```
{
  "emailNotificationsConfig": {
    "generatedReportNotificationsConfig": {
      "isEnabled": true,
      "recipientsType": 0
    },
    "userRequestNotificationsConfig": {
      "isEnabled": true
    },
    "blockedFileNotificationsConfig": {
      "isEnabled": true,
      "recipientsType": 0
    }
  },
  "webhookNotificationsConfig": {
    "scanCompletedNotificationsConfig": {
      "isEnabled": true
    },
    "fileScannedNotificationConfig": {
      "isEnabled": true,
      "notificationScope": 0
    },
    "destinationAddress": "string",
    "headers": {
      "property1": "string",
      "property2": "string"
    },
    "requestType": 0
  },
  "rabbitMqNotificationsConfig": {
    "fileScannedNotificationConfig": {
      "isEnabled": true,
      "notificationScope": 0
    },
    "rabbitMqUrl": "string",
    "headers": {
      "property1": "string",
      "property2": "string"
    }
  }
}
```

Properties

Name	Type	Required	Restrictions	Description
emailNotificationsConfig	EmailNotificationsConfig2¦null	false	none	none
webhookNotificationsConfig	WebhookNotificationsConfig2¦null	false	none	none
rabbitMqNotificationsConfig	RabbitMqNotificationsConfig2¦null	false	none	none

EmailNotificationsConfig2

```
{
  "generatedReportNotificationsConfig": {
    "isEnabled": true,
    "recipientsType": 0
  },
  "userRequestNotificationsConfig": {
    "isEnabled": true
  },
  "blockedFileNotificationsConfig": {
    "isEnabled": true,
    "recipientsType": 0
  }
}
```

Properties

Name	Type	Required	Restrictions	Description
generatedReportNotificationsConfig	GeneratedReportNotificationsConfig2¦null	false	none	none
userRequestNotificationsConfig	UserRequestNotificationsConfig2¦null	false	none	none
blockedFileNotificationsConfig	BlockedFileNotificationsConfig2¦null	false	none	none

GeneratedReportNotificationsConfig2

```
{
  "isEnabled": true,
  "recipientsType": 0
}
```

Properties

Name	Type	Required	Restrictions	Description
isEnabled	boolean	false	none	none
recipientsType	GeneratedReportNotificationsRecipientsType2	false	none	- 0: OwnerOnly - 1: AllRegisteredUsers

GeneratedReportNotificationsRecipientsType2

```
0
```

- 0: OwnerOnly
- 1: AllRegisteredUsers

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: OwnerOnly - 1: AllRegisteredUsers

Enumerated Values

Property	Value
anonymous	0
anonymous	1

UserRequestNotificationsConfig2

```
{
  "isEnabled": true
}
```

Properties

Name	Type	Required	Restrictions	Description
isEnabled	boolean	false	none	none

BlockedFileNotificationsConfig2

```
{
  "isEnabled": true,
  "recipientsType": 0
}
```

Properties

Name	Type	Required	Restrictions	Description
isEnabled	boolean	false	none	none
recipientsType	BlockedFileNotificationsRecipientsType2	false	none	- 0: AllRegisteredUsers - 1: FileOwner - 2: FileOwnerAndAllRegisteredUsers

BlockedFileNotificationsRecipientsType2

```
0
```

- 0: AllRegisteredUsers
- 1: FileOwner
- 2: FileOwnerAndAllRegisteredUsers

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: AllRegisteredUsers - 1: FileOwner - 2: FileOwnerAndAllRegisteredUsers

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2

WebhookNotificationsConfig2

```
{
  "scanCompletedNotificationsConfig": {
    "isEnabled": true
  },
  "fileScannedNotificationConfig": {
    "isEnabled": true,
    "notificationScope": 0
  },
  "destinationAddress": "string",
  "headers": {
    "property1": "string",
    "property2": "string"
  },
  "requestType": 0
}
```

Properties

Name	Type	Required	Restrictions	Description
scanCompletedNotificationsConfig	ScanCompletedNotificationsConfig2¦null	false	none	none
fileScannedNotificationConfig	FileScannedNotificationConfig2¦null	false	none	none
destinationAddress	string¦null	false	none	none
headers	object¦null	false	none	none
» **additionalProperties**	string	false	none	none
requestType	RequestType¦null	false	none	- 0: Post - 1: Put

ScanCompletedNotificationsConfig2

```
{
  "isEnabled": true
}
```

Properties

Name	Type	Required	Restrictions	Description
isEnabled	boolean	true	none	none

FileScannedNotificationConfig2

```
{
  "isEnabled": true,
  "notificationScope": 0
}
```

Properties

Name	Type	Required	Restrictions	Description
isEnabled	boolean	true	none	none
notificationScope	FileNotificationScope	true	none	- 0: BlockedFilesOnly - 1: AllFiles

RabbitMqNotificationsConfig2

```
{
  "fileScannedNotificationConfig": {
    "isEnabled": true,
    "notificationScope": 0
  },
  "rabbitMqUrl": "string",
  "headers": {
    "property1": "string",
    "property2": "string"
  }
}
```

Properties

Name	Type	Required	Restrictions	Description
fileScannedNotificationConfig	FileScannedNotificationConfig2¦null	false	none	none
rabbitMqUrl	string¦null	false	none	none
headers	object¦null	false	none	none
» **additionalProperties**	string	false	none	none

UpdateSmtpConfigCommandResponse


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "newSmtpConfig": {
    "host": "string",
    "baseUrl": "string",
    "port": 0,
    "senderAddress": "string",
    "senderName": "string",
    "domain": "string",
    "username": "string",
    "secureSocketOption": 0,
    "ignoreCertWarnings": true,
    "isSmtpEnabled": true,
    "replyTo": "string"
  },
  "oldSmtpConfig": {
    "host": "string",
    "baseUrl": "string",
    "port": 0,
    "senderAddress": "string",
    "senderName": "string",
    "domain": "string",
    "username": "string",
    "secureSocketOption": 0,
    "ignoreCertWarnings": true,
    "isSmtpEnabled": true,
    "replyTo": "string"
  }
}
```

Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» newSmtpConfig	SmtpConfig¦null	false	none	none
» oldSmtpConfig	SmtpConfig¦null	false	none	none

SmtpConfig


```
{
  "host": "string",
  "baseUrl": "string",
  "port": 0,
  "senderAddress": "string",
  "senderName": "string",
  "domain": "string",
  "username": "string",
  "secureSocketOption": 0,
  "ignoreCertWarnings": true,
  "isSmtpEnabled": true,
  "replyTo": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
host	string	true	none	none
baseUrl	string	true	none	none
port	integer(int32)	true	none	none
senderAddress	string	true	none	none
senderName	string	true	none	none
domain	string	true	none	none
username	string	true	none	none
secureSocketOption	SecureSocketOption	true	none	- 0: None - 1: Auto - 2: SslOnConnect - 3: StartTls - 4: StartTlsWhenAvailable
ignoreCertWarnings	boolean	true	none	none
isSmtpEnabled	boolean	true	none	none
replyTo	string¦null	false	none	none

SecureSocketOption

```
0
```

- 0: None
- 1: Auto
- 2: SslOnConnect
- 3: StartTls
- 4: StartTlsWhenAvailable

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: None - 1: Auto - 2: SslOnConnect - 3: StartTls - 4: StartTlsWhenAvailable

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2
anonymous	3
anonymous	4

UpdateSmtpConfigParameters

```
{
  "host": "string",
  "port": 0,
  "baseUrl": "http://example.com",
  "senderAddress": "string",
  "senderName": "string",
  "domain": "string",
  "username": "string",
  "password": "string",
  "secureSocketOption": 0,
  "ignoreCertWarnings": true,
  "isSmtpEnabled": true
}
```

Properties

Name	Type	Required	Restrictions	Description
host	string¦null	false	none	none
port	integer(int32)¦null	false	none	none
baseUrl	string(uri)¦null	false	none	none
senderAddress	string¦null	false	none	none
senderName	string¦null	false	none	none
domain	string¦null	false	none	none
username	string¦null	false	none	none
password	string¦null	false	none	none
secureSocketOption	SecureSocketOption¦null	false	none	- 0: None - 1: Auto - 2: SslOnConnect - 3: StartTls - 4: StartTlsWhenAvailable
ignoreCertWarnings	boolean¦null	false	none	none
isSmtpEnabled	boolean¦null	false	none	none

GetSmtpConfigResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "host": "string",
  "port": 0,
  "baseUrl": "string",
  "senderAddress": "string",
  "senderName": "string",
  "domain": "string",
  "username": "string",
  "secureSocketOption": 0,
  "ignoreCertWarnings": true,
  "isSmtpEnabled": true
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» host	string¦null	false	none	none
» port	integer(int32)	false	none	none
» baseUrl	string¦null	false	none	none
» senderAddress	string¦null	false	none	none
» senderName	string¦null	false	none	none
» domain	string¦null	false	none	none
» username	string¦null	false	none	none
» secureSocketOption	SecureSocketOption	false	none	- 0: None - 1: Auto - 2: SslOnConnect - 3: StartTls - 4: StartTlsWhenAvailable
» ignoreCertWarnings	boolean	false	none	none
» isSmtpEnabled	boolean	false	none	none

GetNotificationsConfigResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "emailNotificationsConfig": {
    "generatedReportNotificationsConfig": {
      "isEnabled": true,
      "recipientsType": 0
    },
    "userRequestNotificationsConfig": {
      "isEnabled": true
    },
    "blockedFileNotificationsConfig": {
      "isEnabled": true,
      "recipientsType": 0
    }
  },
  "webhookNotificationsConfig": {
    "scanCompletedNotificationsConfig": {
      "isEnabled": true
    },
    "fileScannedNotificationConfig": {
      "isEnabled": true,
      "notificationScope": 0
    },
    "destinationAddress": "string",
    "headers": {
      "property1": "string",
      "property2": "string"
    },
    "requestType": 0
  },
  "rabbitMqNotificationsConfig": {
    "fileScannedNotificationConfig": {
      "isEnabled": true,
      "notificationScope": 0
    },
    "rabbitMqUrl": "string",
    "headers": {
      "property1": "string",
      "property2": "string"
    }
  }
}
```

Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» emailNotificationsConfig	EmailNotificationsConfig2¦null	false	none	none
» webhookNotificationsConfig	WebhookNotificationsConfig2¦null	false	none	none
» rabbitMqNotificationsConfig	RabbitMqNotificationsConfig2¦null	false	none	none

OnlineActivationParameters

```
{
  "key": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
key	string	true	none	none

Deactivation

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none

RetentionConfigParameters


```
{
  "retentionAuditDays": 1,
  "reportRetention": {
    "isEnabled": true,
    "retentionDays": 1
  },
  "rtpHistoryRetention": {
    "isEnabled": true,
    "retentionDays": 1
  }
}
```

Properties

Name	Type	Required	Restrictions	Description
retentionAuditDays	integer(int32)	false	none	none
reportRetention	ReportRetentionParameters	true	none	none
rtpHistoryRetention	ReportRetentionParameters	true	none	none

ReportRetentionParameters

```
{
  "isEnabled": true,
  "retentionDays": 1
}
```

Properties

Name	Type	Required	Restrictions	Description
isEnabled	boolean	false	none	none
retentionDays	integer(int32)	false	none	none

GetRetentionConfig

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "retentionAuditDays": 0,
  "reportRetentionConfiguration": {
    "isEnabled": true,
    "retentionDays": 0
  },
  "rtpHistoryRetentionConfiguration": {
    "isEnabled": true,
    "retentionDays": 0
  }
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» retentionAuditDays	integer(int32)	false	none	none
» reportRetentionConfiguration	ReportRetention¦null	false	none	none
» rtpHistoryRetentionConfiguration	ReportRetention¦null	false	none	none

ReportRetention


```
{
  "isEnabled": true,
  "retentionDays": 0
}
```

Properties

Name	Type	Required	Restrictions	Description
isEnabled	boolean	false	none	none
retentionDays	integer(int32)	false	none	none

GenerateEncryptionKeyCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```

Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none

GetEncryptionKeyCreationDateQueryResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "creationDate": "2019-08-24T14:15:22Z"
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» creationDate	string(date-time)¦null	false	none	none

UpdateSingleUserSessionCommandResponse


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none

PostSingleUserSessionParameters

```
{
  "isSingleUserSession": true
}
```

Properties

Name	Type	Required	Restrictions	Description
isSingleUserSession	boolean	true	none	none

GetTelemetryConfigQueryResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "telemetryConfig": {
    "isEnabled": true,
    "sendTelemetryToOpswat": true,
    "autoInstrumentation": true,
    "optelCollectors": [
      {
        "metricEndpoint": {
          "endpointUrl": "string",
          "endpointApiKey": "string",
          "protocol": 0
        },
        "traceEndpoint": {
          "endpointUrl": "string",
          "endpointApiKey": "string",
          "protocol": 0
        },
        "isOpswatCollector": true
      }
    ]
  }
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» telemetryConfig	TelemetryConfig	true	none	none

TelemetryConfig

```
{
  "isEnabled": true,
  "sendTelemetryToOpswat": true,
  "autoInstrumentation": true,
  "optelCollectors": [
    {
      "metricEndpoint": {
        "endpointUrl": "string",
        "endpointApiKey": "string",
        "protocol": 0
      },
      "traceEndpoint": {
        "endpointUrl": "string",
        "endpointApiKey": "string",
        "protocol": 0
      },
      "isOpswatCollector": true
    }
  ]
}
```


Properties

Name	Type	Required	Restrictions	Description
isEnabled	boolean	true	none	none
sendTelemetryToOpswat	boolean¦null	false	none	none
autoInstrumentation	boolean¦null	false	none	none
optelCollectors	[OptelCollector]¦null	false	none	none

OptelCollector

```
{
  "metricEndpoint": {
    "endpointUrl": "string",
    "endpointApiKey": "string",
    "protocol": 0
  },
  "traceEndpoint": {
    "endpointUrl": "string",
    "endpointApiKey": "string",
    "protocol": 0
  },
  "isOpswatCollector": true
}
```


Properties

Name	Type	Required	Restrictions	Description
metricEndpoint	OptelCollectorEndpoint	true	none	none
traceEndpoint	OptelCollectorEndpoint	true	none	none
isOpswatCollector	boolean¦null	false	none	none

OptelCollectorEndpoint


```
{
  "endpointUrl": "string",
  "endpointApiKey": "string",
  "protocol": 0
}
```


Properties

Name	Type	Required	Restrictions	Description
endpointUrl	string	true	none	none
endpointApiKey	string¦null	false	none	none
protocol	OptelCollectorEndpointProtocol	true	none	- 0: GRPC - 1: HTTP

OptelCollectorEndpointProtocol

```
0
```

- 0: GRPC
- 1: HTTP

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: GRPC - 1: HTTP

Enumerated Values

Property	Value
anonymous	0
anonymous	1

UpdateTelemetryConfigCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```

Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none

UpdateTelemetryConfigCommandRequest

```
{
  "telemetryConfig": {
    "isEnabled": true,
    "sendTelemetryToOpswat": true,
    "autoInstrumentation": true,
    "optelCollectors": [
      {
        "metricEndpoint": {
          "endpointUrl": "string",
          "endpointApiKey": "string",
          "protocol": 0
        },
        "traceEndpoint": {
          "endpointUrl": "string",
          "endpointApiKey": "string",
          "protocol": 0
        },
        "isOpswatCollector": true
      }
    ]
  },
  "userInfo": {
    "userId": "string",
    "userName": "string"
  }
}
```

Properties

Name	Type	Required	Restrictions	Description
telemetryConfig	TelemetryConfig	true	none	none
userInfo	UserInfo¦null	false	none	none

UserInfo

```
{
  "userId": "string",
  "userName": "string"
}
```


Properties

Name	Type	Required	Restrictions	Description
userId	string	true	none	none
userName	string	true	none	none

SsoConfig


```
{
  "isEnabled": true,
  "ssoProvider": 0,
  "ssoType": 0,
  "baseUrl": "string",
  "clientId": "string",
  "clientSecret": "string",
  "authority": "string",
  "identityProviderCertificate": "string",
  "identityProviderIssuer": "string",
  "loginUrl": "string",
  "logoutUrl": "string",
  "administratorRoleName": "string",
  "readonlyRoleName": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
isEnabled	boolean	true	none	none
ssoProvider	SingleSignOnProvider	true	none	- 0: Azure - 1: Okta - 2: Auth0 - 3: Adfs - 4: PingFederate - 5: Opswat
ssoType	SingleSignOnType	true	none	- 0: OpenIdConnect - 1: Saml2
baseUrl	string	true	none	none
clientId	string	true	none	none
clientSecret	string	true	none	none
authority	string	true	none	none
identityProviderCertificate	string	true	none	none
identityProviderIssuer	string	true	none	none
loginUrl	string	true	none	none
logoutUrl	string	true	none	none
administratorRoleName	string	true	none	none
readonlyRoleName	string	true	none	none

SingleSignOnProvider

```
0
```

- 0: Azure
- 1: Okta
- 2: Auth0
- 3: Adfs
- 4: PingFederate
- 5: Opswat

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: Azure - 1: Okta - 2: Auth0 - 3: Adfs - 4: PingFederate - 5: Opswat

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2
anonymous	3
anonymous	4
anonymous	5

SingleSignOnType

```
0
```

- 0: OpenIdConnect
- 1: Saml2

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: OpenIdConnect - 1: Saml2

Enumerated Values

Property	Value
anonymous	0
anonymous	1

SsoConfigResponse


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "clientId": "string",
  "authority": "string",
  "baseUrl": "string",
  "isEnabled": true,
  "ssoType": 0,
  "ssoProvider": 0,
  "identityProviderIssuer": "string",
  "identityProviderLoginUrl": "string",
  "identityProviderLogoutUrl": "string",
  "administratorRoleName": "string",
  "readonlyRoleName": "string",
  "ssoConfig": {
    "isEnabled": true,
    "ssoProvider": 0,
    "ssoType": 0,
    "baseUrl": "string",
    "clientId": "string",
    "clientSecret": "string",
    "authority": "string",
    "identityProviderCertificate": "string",
    "identityProviderIssuer": "string",
    "loginUrl": "string",
    "logoutUrl": "string",
    "administratorRoleName": "string",
    "readonlyRoleName": "string"
  }
}
```

Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» clientId	string¦null	false	none	none
» authority	string¦null	false	none	none
» baseUrl	string¦null	false	none	none
» isEnabled	boolean	false	none	none
» ssoType	SingleSignOnType2	false	none	- 0: OpenIdConnect
» ssoProvider	SingleSignOnProvider2	false	none	- 0: Azure - 1: Okta - 2: Auth0 - 3: Adfs - 4: PingFederate
» identityProviderIssuer	string¦null	false	none	none
» identityProviderLoginUrl	string¦null	false	none	none
» identityProviderLogoutUrl	string¦null	false	none	none
» administratorRoleName	string¦null	false	none	none
» readonlyRoleName	string¦null	false	none	none
» ssoConfig	SsoConfig¦null	false	none	none

SingleSignOnType2

```
0
```

- 0: OpenIdConnect

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: OpenIdConnect

Enumerated Values

Property	Value
anonymous	0

SingleSignOnProvider2

```
0
```

- 0: Azure
- 1: Okta
- 2: Auth0
- 3: Adfs
- 4: PingFederate

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: Azure - 1: Okta - 2: Auth0 - 3: Adfs - 4: PingFederate

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2
anonymous	3
anonymous	4

UpdateSsoConfigParameters


```
{
  "clientId": "string",
  "clientSecret": "string",
  "authority": "string",
  "baseUrl": "string",
  "identityProviderIssuer": "string",
  "identityProviderLoginUrl": "string",
  "identityProviderLogoutUrl": "string",
  "identityProviderCertificate": {
    "content": "string"
  },
  "isEnabled": true,
  "ssoType": 0,
  "ssoProvider": 0,
  "administratorRoleName": "string",
  "readonlyRoleName": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
clientId	string	true	none	none
clientSecret	string	true	none	none
authority	string	false	none	none
baseUrl	string	false	none	none
identityProviderIssuer	string	false	none	none
identityProviderLoginUrl	string	false	none	none
identityProviderLogoutUrl	string	false	none	none
identityProviderCertificate	IdentityProviderCertificate	true	none	none
isEnabled	boolean	true	none	none
ssoType	SingleSignOnType	true	none	- 0: OpenIdConnect - 1: Saml2
ssoProvider	SingleSignOnProvider	true	none	- 0: Azure - 1: Okta - 2: Auth0 - 3: Adfs - 4: PingFederate - 5: Opswat
administratorRoleName	string	true	none	none
readonlyRoleName	string	true	none	none

IdentityProviderCertificate

```
{
  "content": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
content	string¦null	false	none	none

EnumerateStorages


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "entries": [
    {
      "id": "string",
      "groupId": "string",
      "accountId": "string",
      "name": "string",
      "storageClientId": "string",
      "storageType": {
        "name": "string",
        "categoryType": 0,
        "protocolType": 0,
        "vendorType": 0
      },
      "storageStatus": {
        "message": "string",
        "statusType": 0
      },
      "scansInProgress": true,
      "isRtpInProgress": true,
      "isScheduledScanInProgress": true,
      "storageFunctionality": "string",
      "isAutodiscovered": true,
      "groupRef": {
        "id": "string",
        "name": "string"
      },
      "$type": "string"
    }
  ]
}
```

Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» entries	[Storage]¦null	false	none	none

GetStorage

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "storage": {
    "id": "string",
    "groupId": "string",
    "accountId": "string",
    "name": "string",
    "storageClientId": "string",
    "storageType": {
      "name": "string",
      "categoryType": 0,
      "protocolType": 0,
      "vendorType": 0
    },
    "storageStatus": {
      "message": "string",
      "statusType": 0
    },
    "scansInProgress": true,
    "isRtpInProgress": true,
    "isScheduledScanInProgress": true,
    "storageFunctionality": "string",
    "isAutodiscovered": true,
    "groupRef": {
      "id": "string",
      "name": "string"
    },
    "$type": "string"
  }
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» storage	Storage¦null	false	none	none

ListStorages

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "items": [
    {
      "id": "string",
      "groupId": "string",
      "accountId": "string",
      "name": "string",
      "storageClientId": "string",
      "storageType": {
        "name": "string",
        "categoryType": 0,
        "protocolType": 0,
        "vendorType": 0
      },
      "storageStatus": {
        "message": "string",
        "statusType": 0
      },
      "scansInProgress": true,
      "isRtpInProgress": true,
      "isScheduledScanInProgress": true,
      "storageFunctionality": "string",
      "isAutodiscovered": true,
      "groupRef": {
        "id": "string",
        "name": "string"
      },
      "$type": "string"
    }
  ],
  "entries": [
    {
      "id": "string",
      "groupId": "string",
      "accountId": "string",
      "name": "string",
      "storageClientId": "string",
      "storageType": {
        "name": "string",
        "categoryType": 0,
        "protocolType": 0,
        "vendorType": 0
      },
      "storageStatus": {
        "message": "string",
```

```
},
      "scansInProgress": true,
      "isRtpInProgress": true,
      "isScheduledScanInProgress": true,
      "storageFunctionality": "string",
      "isAutodiscovered": true,
      "groupRef": {
        "id": "string",
        "name": "string"
      },
      "$type": "string"
    }
  ],
  "totalCount": 0,
  "startIndex": 0,
  "count": 0
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» items	[Storage]¦null	false	none	none
» entries	[Storage]¦null	false	none	none
» totalCount	integer(int32)	false	none	none
» startIndex	integer(int32)	false	none	none
» count	integer(int32)	false	none	none

EnumerateStorageUsersQueryResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "entries": [
    {
      "id": "string",
      "fullName": "string"
    }
  ]
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» entries	[StorageUser]¦null	false	none	none

StorageUser


```
{
  "id": "string",
  "fullName": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
id	string¦null	false	none	none
fullName	string¦null	false	none	none

AddNewStorageCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "storageId": "string"
}
```

Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» storageId	string¦null	false	none	none

AddBatchStorageParameters

```
{
  "addStorageParametersList": [
    {
      "id": "string",
      "storageClientId": "string",
      "name": "string",
      "storageVendorType": 0,
      "storageProtocolType": 0,
      "credentialsFile": "string",
      "credentials": "string",
      "source": "string",
      "groupId": "string",
      "accountId": "string",
      "workflowId": "string",
      "transferMetadataAndChecksum": true
    }
  ]
}
```


Properties

Name	Type	Required	Restrictions	Description
addStorageParametersList	[AddStorageParameters]	true	none	none

AddStorageParameters


```
{
  "id": "string",
  "storageClientId": "string",
  "name": "string",
  "storageVendorType": 0,
  "storageProtocolType": 0,
  "credentialsFile": "string",
  "credentials": "string",
  "source": "string",
  "groupId": "string",
  "accountId": "string",
  "workflowId": "string",
  "transferMetadataAndChecksum": true
}
```

Properties

Name	Type	Required	Restrictions	Description
id	string¦null	false	none	none
storageClientId	string¦null	false	none	none
name	string	true	none	none
storageVendorType	StorageVendorType2	true	none	- 0: AmazonS3 - 1: OneDrive - 2: Box - 3: DellIsilon - 4: AzureFiles - 5: SmbCompatible - 6: S3Compatible - 7: AzureBlob - 8: AlibabaCloud - 9: GoogleCloud - 10: Sftp - 11: SharePoint - 12: Nfs - 13: Wasabi - 14: OracleCloud - 15: NetAppOntap - 16: Cubbit - 17: Mft - 18: SharepointOnPrem - 19: Ftp - 20: Oracle - 21: NfsSisl - 22: ScalityRing
storageProtocolType	StorageProtocolType2	true	none	- 0: Smb - 1: GraphSdk - 2: BoxSdk - 3: AwsSdk - 4: AzureBlobSdk - 5: AlibabaCloudSdk - 6: GoogleCloudSdk - 7: AzureFilesSdk - 8: Sftp - 9: Nfs - 10: Mft - 11: SharepointOnPrem - 12: Ftp - 13: OracleSdk
credentialsFile	string(binary)¦null	false	none	none
credentials	string¦null	false	none	none

source	string	true	none	none
groupId	string	true	none	none
accountId	string¦null	false	none	none
workflowId	string¦null	false	none	none
transferMetadataAndChecksum	boolean¦null	false	none	none

GetBatchResultsResponse


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "addStorageResultInfos": [
    {
      "result": 0,
      "responseKey": "string",
      "responseMessage": "string",
      "responseMessageParams": {
        "property1": "string",
        "property2": "string"
      },
      "storageStatus": {
        "message": "string",
        "statusType": 0
      },
      "source": "string",
      "name": "string",
      "vendorType": 0,
      "protocolType": 0
    }
  ],
  "isCompleted": true
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» addStorageResultInfos	[AddStorageResultInfo]¦null	false	none	none
» isCompleted	boolean	false	none	none

AddStorageResultInfo

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "storageStatus": {
    "message": "string",
    "statusType": 0
  },
  "source": "string",
  "name": "string",
  "vendorType": 0,
  "protocolType": 0
}
```

Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» storageStatus	StorageStatus	true	none	none
» source	string	true	none	none
» name	string	true	none	none
» vendorType	StorageVendorType2	true	none	- 0: AmazonS3 - 1: OneDrive - 2: Box - 3: DellIsilon - 4: AzureFiles - 5: SmbCompatible - 6: S3Compatible - 7: AzureBlob - 8: AlibabaCloud - 9: GoogleCloud - 10: Sftp - 11: SharePoint - 12: Nfs - 13: Wasabi - 14: OracleCloud - 15: NetAppOntap - 16: Cubbit - 17: Mft - 18: SharepointOnPrem - 19: Ftp - 20: Oracle - 21: NfsSisl - 22: ScalityRing
» protocolType	StorageProtocolType2	true	none	- 0: Smb - 1: GraphSdk - 2: BoxSdk - 3: AwsSdk - 4: AzureBlobSdk - 5: AlibabaCloudSdk - 6: GoogleCloudSdk - 7: AzureFilesSdk - 8: Sftp - 9: Nfs - 10: Mft - 11: SharepointOnPrem - 12: Ftp - 13: OracleSdk

UpdateNewStorageCommandResponse


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "updatedStorage": {
    "id": "string",
    "name": "string",
    "groupId": "string",
    "clientId": "string",
    "accountId": "string",
    "source": "string",
    "storageFunctionality": "string",
    "storageType": {
      "name": "string",
      "categoryType": 0,
      "protocolType": 0,
      "vendorType": 0
    },
    "storageStatus": {
      "message": "string",
      "statusType": 0
    },
    "workflowId": "string",
    "lastUpdated": "2019-08-24T14:15:22Z",
    "tenantId": "string",
    "groupRef": {
      "id": "string",
      "name": "string"
    },
    "isAutodiscovered": true
  }
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» updatedStorage	NewStorage|null	false	none	none

EnumerateStorages2


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "entries": [
    {
      "id": "string",
      "groupId": "string",
      "accountId": "string",
      "name": "string",
      "storageClientId": "string",
      "storageType": {
        "name": "string",
        "categoryType": 0,
        "protocolType": 0,
        "vendorType": 0
      },
      "storageStatus": {
        "message": "string",
        "statusType": 0
      },
      "scansInProgress": true,
      "isRtpInProgress": true,
      "isScheduledScanInProgress": true,
      "storageFunctionality": "string",
      "isAutodiscovered": true,
      "groupRef": {
        "id": "string",
        "name": "string"
      },
      "$type": "string"
    }
  ]
}
```

Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» entries	[Storage]¦null	false	none	none

AddScanScheduleParameters

```
{
  "name": "string",
  "workflowId": "string",
  "recurrencePattern": {
    "type": "string",
    "minutelyRecurrence": {
      "everyNumberOfMinutes": 5
    },
    "hourlyRecurrence": {
      "everyNumberOfHours": 1
    },
    "dailyRecurrence": {
      "everyNumberOfDays": 1
    },
    "weeklyRecurrence": {
      "daysOfWeek": [
        0
      ],
      "everyNumberOfWeeks": 0
    },
    "monthlyRecurrence": {
      "everyNumberOfMonths": 1,
      "dayOfMonth": 1
    },
    "startDate": "2019-08-24T14:15:22Z",
    "timeToStart": "2019-08-24T14:15:22Z",
    "avoidConcurrentScheduleRuns": true
  },
  "scanPartition": "string",
  "priority": 0,
  "$type": "string"
}
```


Properties

allOf - discriminator: ScanScheduleParameters.$type

Name	Type	Required	Restrictions	Description
anonymous	ScanScheduleParameters	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none

ScanScheduleParameters


```
{
  "name": "string",
  "workflowId": "string",
  "recurrencePattern": {
    "type": "string",
    "minutelyRecurrence": {
      "everyNumberOfMinutes": 5
    },
    "hourlyRecurrence": {
      "everyNumberOfHours": 1
    },
    "dailyRecurrence": {
      "everyNumberOfDays": 1
    },
    "weeklyRecurrence": {
      "daysOfWeek": [
        0
      ],
      "everyNumberOfWeeks": 0
    },
    "monthlyRecurrence": {
      "everyNumberOfMonths": 1,
      "dayOfMonth": 1
    },
    "startDate": "2019-08-24T14:15:22Z",
    "timeToStart": "2019-08-24T14:15:22Z",
    "avoidConcurrentScheduleRuns": true
  },
  "scanPartition": "string",
  "priority": 0,
  "$type": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
name	string	true	none	none
workflowId	string	true	none	none
recurrencePattern	RecurrencePatternParameters	true	none	none
scanPartition	string¦null	false	none	none
priority	integer(int32)	true	none	none
$type	string	true	none	none

RecurrencePatternParameters

```
{
  "type": "string",
  "minutelyRecurrence": {
    "everyNumberOfMinutes": 5
  },
  "hourlyRecurrence": {
    "everyNumberOfHours": 1
  },
  "dailyRecurrence": {
    "everyNumberOfDays": 1
  },
  "weeklyRecurrence": {
    "daysOfWeek": [
      0
    ],
    "everyNumberOfWeeks": 0
  },
  "monthlyRecurrence": {
    "everyNumberOfMonths": 1,
    "dayOfMonth": 1
  },
  "startDate": "2019-08-24T14:15:22Z",
  "timeToStart": "2019-08-24T14:15:22Z",
  "avoidConcurrentScheduleRuns": true
}
```

Properties

Name	Type	Required	Restrictions	Description
type	string	true	none	none
minutelyRecurrence	MinutelyRecurrenceParameters¦null	false	none	none
hourlyRecurrence	HourlyRecurrenceParameters¦null	false	none	none
dailyRecurrence	DailyRecurrenceParameters¦null	false	none	none
weeklyRecurrence	WeeklyRecurrenceParameters¦null	false	none	none
monthlyRecurrence	MonthlyRecurrenceParameters¦null	false	none	none
startDate	string(date-time)¦null	false	none	none
timeToStart	string(date-time)¦null	false	none	none
avoidConcurrentScheduleRuns	boolean	false	none	none

MinutelyRecurrenceParameters

```
{
  "everyNumberOfMinutes": 5
}
```

Properties

Name	Type	Required	Restrictions	Description
everyNumberOfMinutes	integer(int32)	false	none	none

HourlyRecurrenceParameters

```
{
  "everyNumberOfHours": 1
}
```

Properties

Name	Type	Required	Restrictions	Description
everyNumberOfHours	integer(int32)	false	none	none

DailyRecurrenceParameters

```
{
  "everyNumberOfDays": 1
}
```

Properties

Name	Type	Required	Restrictions	Description
everyNumberOfDays	integer(int32)	false	none	none

WeeklyRecurrenceParameters

```
{
  "daysOfWeek": [
    0
  ],
  "everyNumberOfWeeks": 0
}
```

Properties

Name	Type	Required	Restrictions	Description
daysOfWeek	[DayOfWeek]	true	none	[- 0: Sunday - 1: Monday - 2: Tuesday - 3: Wednesday - 4: Thursday - 5: Friday - 6: Saturday]
everyNumberOfWeeks	integer(int32)	false	none	none

DayOfWeek

```
0
```

- 0: Sunday
- 1: Monday
- 2: Tuesday
- 3: Wednesday
- 4: Thursday
- 5: Friday
- 6: Saturday

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: Sunday - 1: Monday - 2: Tuesday - 3: Wednesday - 4: Thursday - 5: Friday - 6: Saturday

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2
anonymous	3
anonymous	4
anonymous	5
anonymous	6

MonthlyRecurrenceParameters


```
{
  "everyNumberOfMonths": 1,
  "dayOfMonth": 1
}
```


Properties

Name	Type	Required	Restrictions	Description
everyNumberOfMonths	integer(int32)	false	none	none
dayOfMonth	integer(int32)	false	none	none

UpdateScanScheduleParameters

```
{
  "name": "string",
  "workflowId": "string",
  "recurrencePattern": {
    "type": "string",
    "minutelyRecurrence": {
      "everyNumberOfMinutes": 5
    },
    "hourlyRecurrence": {
      "everyNumberOfHours": 1
    },
    "dailyRecurrence": {
      "everyNumberOfDays": 1
    },
    "weeklyRecurrence": {
      "daysOfWeek": [
        0
      ],
      "everyNumberOfWeeks": 0
    },
    "monthlyRecurrence": {
      "everyNumberOfMonths": 1,
      "dayOfMonth": 1
    },
    "startDate": "2019-08-24T14:15:22Z",
    "timeToStart": "2019-08-24T14:15:22Z",
    "avoidConcurrentScheduleRuns": true
  },
  "scanPartition": "string",
  "priority": 0,
  "$type": "string",
  "id": "string"
}
```


Properties

allOf - discriminator: ScanScheduleParameters.$type

Name	Type	Required	Restrictions	Description
anonymous	ScanScheduleParameters	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» id	string¦null	false	none	none

UpdateScanScheduleCommandResponse


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none

EnumerateScanSchedules

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "entries": [
    {
      "id": "string",
      "name": "string",
      "workflowId": "string",
      "scanConfigurationId": "string",
      "type": "string",
      "scanPartition": "string",
      "createdAt": "2019-08-24T14:15:22Z",
      "lastScanTime": "2019-08-24T14:15:22Z",
      "nextScanTime": "2019-08-24T14:15:22Z",
      "recurrencePatternDto": {
        "type": 0,
        "minutelyRecurrence": {
          "everyNumberOfMinutes": 0
        },
        "hourlyRecurrence": {
          "everyNumberOfHours": 0
        },
        "dailyRecurrence": {
          "everyNumberOfDays": 0
        },
        "weeklyRecurrence": {
          "daysOfWeek": [
            0
          ],
          "everyNumberOfWeeks": 0
        },
        "monthlyRecurrence": {
          "everyNumberOfMonths": 0,
          "dayOfMonth": 0
        },
        "startDate": "2019-08-24T14:15:22Z",
        "timeToStart": "2019-08-24T14:15:22Z",
        "avoidConcurrentScheduleRuns": true
      },
      "createdBy": "string",
      "priority": 0,
      "storageId": "string"
    }
  ],
  "totalCount": 0
}
```

Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» entries	[ScheduledScanResponse]¦null	false	none	none
» totalCount	integer(int64)	false	none	none

ScheduledScanResponse

```
{
  "id": "string",
  "name": "string",
  "workflowId": "string",
  "scanConfigurationId": "string",
  "type": "string",
  "scanPartition": "string",
  "createdAt": "2019-08-24T14:15:22Z",
  "lastScanTime": "2019-08-24T14:15:22Z",
  "nextScanTime": "2019-08-24T14:15:22Z",
  "recurrencePatternDto": {
    "type": 0,
    "minutelyRecurrence": {
      "everyNumberOfMinutes": 0
    },
    "hourlyRecurrence": {
      "everyNumberOfHours": 0
    },
    "dailyRecurrence": {
      "everyNumberOfDays": 0
    },
    "weeklyRecurrence": {
      "daysOfWeek": [
        0
      ],
      "everyNumberOfWeeks": 0
    },
    "monthlyRecurrence": {
      "everyNumberOfMonths": 0,
      "dayOfMonth": 0
    },
    "startDate": "2019-08-24T14:15:22Z",
    "timeToStart": "2019-08-24T14:15:22Z",
    "avoidConcurrentScheduleRuns": true
  },
  "createdBy": "string",
  "priority": 0,
  "storageId": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
id	string¦null	false	none	none
name	string¦null	false	none	none
workflowId	string	true	none	WorkflowId required if ScanConfigurationId is null
scanConfigurationId	string¦null	false	none	This property is obsolete and will be removed in the future. Use WorkflowId instead.
type	string¦null	false	none	none
scanPartition	string¦null	false	none	none
createdAt	string(date-time)	false	none	none
lastScanTime	string(date-time)¦null	false	none	none
nextScanTime	string(date-time)	false	none	none
recurrencePatternDto	RecurrencePattern¦null	false	none	none
createdBy	string¦null	false	none	none
priority	MessagePriority	false	none	- 0: Low - 1: Medium - 2: High
storageId	string	true	none	none

RecurrencePattern

```
{
  "type": 0,
  "minutelyRecurrence": {
    "everyNumberOfMinutes": 0
  },
  "hourlyRecurrence": {
    "everyNumberOfHours": 0
  },
  "dailyRecurrence": {
    "everyNumberOfDays": 0
  },
  "weeklyRecurrence": {
    "daysOfWeek": [
      0
    ],
    "everyNumberOfWeeks": 0
  },
  "monthlyRecurrence": {
    "everyNumberOfMonths": 0,
    "dayOfMonth": 0
  },
  "startDate": "2019-08-24T14:15:22Z",
  "timeToStart": "2019-08-24T14:15:22Z",
  "avoidConcurrentScheduleRuns": true
}
```

Properties

Name	Type	Required	Restrictions	Description
type	RecurrencePatternType	false	none	- 0: Hourly - 1: Daily - 2: Weekly - 3: Monthly - 4: Minutely
minutelyRecurrence	MinutelyRecurrence¦null	false	none	none
hourlyRecurrence	HourlyRecurrence¦null	false	none	none
dailyRecurrence	DailyRecurrence¦null	false	none	none
weeklyRecurrence	WeeklyRecurrence¦null	false	none	none
monthlyRecurrence	MonthlyRecurrence¦null	false	none	none
startDate	string(date-time)¦null	false	none	none
timeToStart	string(date-time)¦null	false	none	none
avoidConcurrentScheduleRuns	boolean	false	none	none

RecurrencePatternType

```
0
```

- 0: Hourly
- 1: Daily
- 2: Weekly
- 3: Monthly
- 4: Minutely

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: Hourly - 1: Daily - 2: Weekly - 3: Monthly - 4: Minutely

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2
anonymous	3
anonymous	4

MinutelyRecurrence

```
{
  "everyNumberOfMinutes": 0
}
```

Properties

Name	Type	Required	Restrictions	Description
everyNumberOfMinutes	integer(int32)	false	none	none

HourlyRecurrence

```
{
  "everyNumberOfHours": 0
}
```

Properties

Name	Type	Required	Restrictions	Description
everyNumberOfHours	integer(int32)	false	none	none

DailyRecurrence

```
{
  "everyNumberOfDays": 0
}
```

Properties

Name	Type	Required	Restrictions	Description
everyNumberOfDays	integer(int32)	false	none	none

WeeklyRecurrence

```
{
  "daysOfWeek": [
    0
  ],
  "everyNumberOfWeeks": 0
}
```

Properties

Name	Type	Required	Restrictions	Description
daysOfWeek	[DayOfWeek]	true	none	[- 0: Sunday - 1: Monday - 2: Tuesday - 3: Wednesday - 4: Thursday - 5: Friday - 6: Saturday]
everyNumberOfWeeks	integer(int32)	true	none	none

MonthlyRecurrence

```
{
  "everyNumberOfMonths": 0,
  "dayOfMonth": 0
}
```

Properties

Name	Type	Required	Restrictions	Description
everyNumberOfMonths	integer(int32)	false	none	none
dayOfMonth	integer(int32)	false	none	none

SortDirectionFilter

```
0
```

- 0: Ascending
- 1: Descending

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: Ascending - 1: Descending

Enumerated Values

Property	Value
anonymous	0
anonymous	1

MoveStoragesCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "succeeded": [
    "string"
  ],
  "failed": [
    {
      "id": "string",
      "reasonKey": "string",
      "reason": "string",
      "childFailures": [
        {}
      ]
    }
  ],
  "targetGroupId": "string"
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» succeeded	[string]	false	none	none
» failed	[BulkFailedItem]	false	none	none
» targetGroupId	string	false	none	none

MoveStoragesParameters

```
{
  "storageIds": [
    "string"
  ],
  "targetGroupId": "string"
}
```


Properties

Name	Type	Required	Restrictions	Description
storageIds	[string]	true	none	none
targetGroupId	string	true	none	none

BulkDeleteStoragesCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "succeeded": [
    "string"
  ],
  "failed": [
    {
      "id": "string",
      "reasonKey": "string",
      "reason": "string",
      "childFailures": [
        {}
      ]
    }
  ],
  "scansRunning": true,
  "runningScans": [
    {
      "scanId": "string",
      "storageId": "string",
      "accountId": "string",
      "groupId": "string"
    }
  ]
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» succeeded	[string]	false	none	none
» failed	[BulkFailedItem]	false	none	none
» scansRunning	boolean	false	none	none
» runningScans	[BulkRunningScan]	false	none	none

BulkDeleteStoragesParameters

```
{
  "storageIds": [
    "string"
  ]
}
```

Properties

Name	Type	Required	Restrictions	Description
storageIds	[string]	false	none	none

DeleteScanSchedulesCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "succeeded": [
    "string"
  ],
  "failed": [
    {
      "id": "string",
      "reasonKey": "string",
      "reason": "string",
      "childFailures": [
        {}
      ]
    }
  ]
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» succeeded	[string]¦null	false	none	none
» failed	[BulkFailedItem]¦null	false	none	none

RetrieveUserNameFromStorageQueryResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "userName": "string"
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» userName	string¦null	false	none	none

EnumerateActiveUsers

```
{
  "entries": [
    {
      "id": "string",
      "userName": "string",
      "fullName": "string",
      "email": "string",
      "roles": [
        {
          "bindingId": "string",
          "roleId": "string",
          "roleName": "string",
          "expiresAt": "2019-08-24T14:15:22Z"
        }
      ],
      "directPermissions": [
        {
          "id": "string",
          "permissionName": "string",
          "expiresAt": "2019-08-24T14:15:22Z"
        }
      ]
    }
  ],
  "totalCount": 0
}
```


Properties

Name	Type	Required	Restrictions	Description
entries	[ActiveUser]¦null	false	none	none
totalCount	integer(int64)	false	none	none

ActiveUser

```
{
  "id": "string",
  "userName": "string",
  "fullName": "string",
  "email": "string",
  "roles": [
    {
      "bindingId": "string",
      "roleId": "string",
      "roleName": "string",
      "expiresAt": "2019-08-24T14:15:22Z"
    }
  ],
  "directPermissions": [
    {
      "id": "string",
      "permissionName": "string",
      "expiresAt": "2019-08-24T14:15:22Z"
    }
  ]
}
```


Properties

Name	Type	Required	Restrictions	Description
id	string	true	none	none
userName	string	true	none	none
fullName	string	true	none	none
email	string	true	none	none
roles	[UserRoleAssignment]¦null	false	none	none
directPermissions	[UserPermission]¦null	false	none	none

UserRoleAssignment


```
{
  "bindingId": "string",
  "roleId": "string",
  "roleName": "string",
  "expiresAt": "2019-08-24T14:15:22Z"
}
```

Properties

Name	Type	Required	Restrictions	Description
bindingId	string(guid)	true	none	none
roleId	string(guid)	true	none	none
roleName	string	true	none	none
expiresAt	string(date-time)¦null	false	none	none

UserPermission

```
{
  "id": "string",
  "permissionName": "string",
  "expiresAt": "2019-08-24T14:15:22Z"
}
```

Properties

Name	Type	Required	Restrictions	Description
id	string(guid)	true	none	none
permissionName	string	true	none	none
expiresAt	string(date-time)¦null	false	none	none

OrderType

```
0
```

- 0: Descending
- 1: Ascending

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: Descending - 1: Ascending

Enumerated Values

Property	Value
anonymous	0
anonymous	1

OrderBy

```
0
```

- 0: Id
- 1: FullName
- 2: Username
- 3: Email
- 4: Role

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: Id - 1: FullName - 2: Username - 3: Email - 4: Role

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2
anonymous	3
anonymous	4

RegisterUserParameters

```
{
  "fullName": "string",
  "userName": "string",
  "password": "string",
  "email": "string",
  "ssoUserId": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
fullName	string	true	none	none
userName	string	true	none	none
password	string¦null	false	none	none
email	string	true	none	none
ssoUserId	string¦null	false	none	none

CreateUserParameters

```
{
  "fullName": "string",
  "userName": "string",
  "password": "string",
  "email": "string",
  "ssoUserId": "string",
  "role": 0
}
```

Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RegisterUserParameters	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» role	UserRole	true	none	- 0: None - 1: ReadOnlyAdministrator - 2: Administrator - 4: SsoAdministrator - 5: SsoReadOnlyAdministrator - 6: TenantAdministrator - 999: Invalid

UserRole

```
0
```

- 0: None
- 1: ReadOnlyAdministrator
- 2: Administrator
- 4: SsoAdministrator
- 5: SsoReadOnlyAdministrator
- 6: TenantAdministrator
- 999: Invalid

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: None - 1: ReadOnlyAdministrator - 2: Administrator - 4: SsoAdministrator - 5: SsoReadOnlyAdministrator - 6: TenantAdministrator - 999: Invalid

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2
anonymous	4
anonymous	5
anonymous	6
anonymous	999

AuthenticateUserCommandResponseWithoutTokens

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "fullName": "string",
  "email": "string",
  "userName": "string",
  "role": 0,
  "user": {
    "id": "string",
    "userName": "string",
    "fullName": "string",
    "email": "string",
    "role": 0,
    "roles": [
      "string"
    ],
    "tenantId": "string",
    "ssoUserId": "string",
    "passwordHash": "string",
    "passwordSalt": "string",
    "passwordHashAlgorithm": 0,
    "preferences": {
      "theme": 0,
      "language": 0
    }
  },
  "userId": "string"
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» fullName	string¦null	false	none	none
» email	string¦null	false	none	none
» userName	string¦null	false	none	none
» role	UserRole¦null	false	none	- 0: None - 1: ReadOnlyAdministrator - 2: Administrator - 4: SsoAdministrator - 5: SsoReadOnlyAdministrator - 6: TenantAdministrator - 999: Invalid
» user	UserDto¦null	false	none	none
» userId	string¦null	false	none	none

UserDto

```
{
  "id": "string",
  "userName": "string",
  "fullName": "string",
  "email": "string",
  "role": 0,
  "roles": [
    "string"
  ],
  "tenantId": "string",
  "ssoUserId": "string",
  "passwordHash": "string",
  "passwordSalt": "string",
  "passwordHashAlgorithm": 0,
  "preferences": {
    "theme": 0,
    "language": 0
  }
}
```

Properties

Name	Type	Required	Restrictions	Description
id	string	true	none	none
userName	string	true	none	none
fullName	string	true	none	none
email	string	true	none	none
role	UserRole	false	none	- 0: None - 1: ReadOnlyAdministrator - 2: Administrator - 4: SsoAdministrator - 5: SsoReadOnlyAdministrator - 6: TenantAdministrator - 999: Invalid
roles	[string]	false	none	none
tenantId	string¦null	false	none	none
ssoUserId	string¦null	false	none	none
passwordHash	string(byte)¦null	false	none	none
passwordSalt	string(byte)¦null	false	none	none
passwordHashAlgorithm	integer(int32)¦null	false	none	none
preferences	UserPreferences¦null	false	none	none

UserPreferences

```
{
  "theme": 0,
  "language": 0
}
```

Properties

Name	Type	Required	Restrictions	Description
theme	UserTheme	false	none	- 0: Light - 1: Dark - 2: System - 3: Company
language	UserLanguage	false	none	- 0: En - 1: Jp

UserTheme

```
0
```

- 0: Light
- 1: Dark
- 2: System
- 3: Company

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: Light - 1: Dark - 2: System - 3: Company

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2
anonymous	3

UserLanguage

```
0
```

- 0: En
- 1: Jp

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: En - 1: Jp

Enumerated Values

Property	Value
anonymous	0
anonymous	1

AuthenticateUserCommandRequest

```
{
  "userName": "string",
  "password": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
userName	string	true	none	login name of the user
password	string	true	none	password

CurrentUserInfo

```
{
  "username": "string",
  "email": "string",
  "authProvider": "string",
  "role": "string",
  "id": "string",
  "roles": [
    {
      "bindingId": "string",
      "roleId": "string",
      "roleName": "string",
      "expiresAt": "2019-08-24T14:15:22Z"
    }
  ],
  "directPermissions": [
    {
      "id": "string",
      "permissionName": "string",
      "expiresAt": "2019-08-24T14:15:22Z"
    }
  ],
  "preferences": {
    "theme": 0,
    "language": 0
  }
}
```


Properties

Name	Type	Required	Restrictions	Description
username	string	true	none	none
email	string	true	none	none
authProvider	string	true	none	none
role	string	true	none	none
id	string	true	none	none
roles	[UserRoleAssignment]¦null	false	none	none
directPermissions	[UserPermission]¦null	false	none	none
preferences	UserPreferences¦null	false	none	none

UpdateUserCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "user": {
    "id": "string",
    "userName": "string",
    "fullName": "string",
    "email": "string",
    "role": 0,
    "roles": [
      "string"
    ],
    "tenantId": "string",
    "ssoUserId": "string",
    "passwordHash": "string",
    "passwordSalt": "string",
    "passwordHashAlgorithm": 0,
    "preferences": {
      "theme": 0,
      "language": 0
    }
  }
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» user	UserDto|null	false	none	none

UpdateUserRoleParameters

```
{
  "userId": "string",
  "role": 0
}
```


Properties

Name	Type	Required	Restrictions	Description
userId	string	true	none	none
role	UserRole	true	none	- 0: None - 1: ReadOnlyAdministrator - 2: Administrator - 4: SsoAdministrator - 5: SsoReadOnlyAdministrator - 6: TenantAdministrator - 999: Invalid

EnumerateUsers


```
{
  "entries": [
    {
      "id": "string",
      "userName": "string",
      "fullName": "string",
      "email": "string",
      "role": 0,
      "roles": [
        "string"
      ],
      "tenantId": "string",
      "ssoUserId": "string",
      "passwordHash": "string",
      "passwordSalt": "string",
      "passwordHashAlgorithm": 0,
      "preferences": {
        "theme": 0,
        "language": 0
      }
    }
  ],
  "totalCount": 0
}
```

Properties

Name	Type	Required	Restrictions	Description
entries	[UserDto]¦null	false	none	none
totalCount	integer(int64)	false	none	none

UserCleanupCommandResponse


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "user": {
    "id": "string",
    "userName": "string",
    "fullName": "string",
    "email": "string",
    "role": 0,
    "roles": [
      "string"
    ],
    "tenantId": "string",
    "ssoUserId": "string",
    "passwordHash": "string",
    "passwordSalt": "string",
    "passwordHashAlgorithm": 0,
    "preferences": {
      "theme": 0,
      "language": 0
    }
  }
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» user	UserDto¦null	false	none	none

UpdateUserParameters

```
{
  "userId": "string",
  "role": 0,
  "userName": "string",
  "fullName": "string",
  "currentPassword": "string",
  "newPassword": "string",
  "email": "string",
  "preferences": {
    "theme": 0,
    "language": 0
  }
}
```

Properties

Name	Type	Required	Restrictions	Description
userId	string¦null	false	none	none
role	UserRole	false	none	- 0: None - 1: ReadOnlyAdministrator - 2: Administrator - 4: SsoAdministrator - 5: SsoReadOnlyAdministrator - 6: TenantAdministrator - 999: Invalid
userName	string¦null	false	none	none
fullName	string¦null	false	none	none
currentPassword	string¦null	false	none	none
newPassword	string¦null	false	none	none
email	string¦null	false	none	none
preferences	UserPreferences¦null	false	none	none

RequestResetPasswordCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```

Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none

RequestResetPasswordCommandRequest

```
{
  "userInput": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
userInput	string	true	none	none

UpdatePasswordCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "user": {
    "id": "string",
    "userName": "string",
    "fullName": "string",
    "email": "string",
    "role": 0,
    "roles": [
      "string"
    ],
    "tenantId": "string",
    "ssoUserId": "string",
    "passwordHash": "string",
    "passwordSalt": "string",
    "passwordHashAlgorithm": 0,
    "preferences": {
      "theme": 0,
      "language": 0
    }
  }
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» user	UserDto¦null	false	none	none

UpdatePasswordCommandRequest

```
{
  "newPassword": "stringstring",
  "newPasswordConfirmation": "stringstring",
  "secureToken": "string"
}
```


Properties

Name	Type	Required	Restrictions	Description
newPassword	string	true	none	none
newPasswordConfirmation	string	true	none	none
secureToken	string	true	none	none

GetUserPermissionsQueryResponse


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "roles": [
    {
      "bindingId": "string",
      "roleId": "string",
      "roleName": "string",
      "expiresAt": "2019-08-24T14:15:22Z"
    }
  ],
  "directPermissions": [
    {
      "id": "string",
      "permissionName": "string",
      "expiresAt": "2019-08-24T14:15:22Z"
    }
  ]
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» roles	[UserRoleAssignment]¦null	false	none	none
» directPermissions	[UserPermission]¦null	false	none	none

GetUserTourQueryResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "userId": "string",
  "userTours": [
    {
      "tourType": 0,
      "finalizedDate": "2019-08-24T14:15:22Z"
    }
  ]
}
```

Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» userId	string¦null	false	none	none
» userTours	[UserTour]¦null	false	none	none

UserTour

```
{
  "tourType": 0,
  "finalizedDate": "2019-08-24T14:15:22Z"
}
```

Properties

Name	Type	Required	Restrictions	Description
tourType	UserTourType	false	none	- 0: OnboardingUi - 1: WorkflowUi - 2: StorageUnits
finalizedDate	string(date-time)	false	none	none

UserTourType

```
0
```

- 0: OnboardingUi
- 1: WorkflowUi
- 2: StorageUnits

Properties

Name	Type	Required	Restrictions	Description
anonymous	integer	false	none	- 0: OnboardingUi - 1: WorkflowUi - 2: StorageUnits

Enumerated Values

Property	Value
anonymous	0
anonymous	1
anonymous	2

FinalizeUserTour

```
{
  "userId": "string",
  "userTourType": 0
}
```

Properties

Name	Type	Required	Restrictions	Description
userId	string	true	none	none
userTourType	UserTourType	true	none	- 0: OnboardingUi - 1: WorkflowUi - 2: StorageUnits

WebhookEventBasedRtpCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "correlationId": "string"
}
```

Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» correlationId	string¦null	false	none	none

WebhookEventBasedRtpParameters

```
{
  "metadata": "string",
  "storageClientId": "string",
  "scanId": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
metadata	string	true	none	none
storageClientId	string	true	none	none
scanId	string¦null	false	none	none

GetAllWorkflowsCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "entries": [
    {
      "id": "string",
      "scanPoolId": "string",
      "scanProcessFlow": 0,
      "isIdentityScanningEnabled": true,
      "scanIntervalDays": 0,
      "rules": [
        "string"
      ],
      "type": 0,
      "workflowSupportedTechnologies": {
        "dlp": {
          "status": 0
        },
        "deepCdr": {
          "status": 0
        },
        "sandBox": {
          "status": 0
        },
        "metascan": {
          "status": 0
        }
      },
      "name": "string",
      "userAgent": "string",
      "scanPool": {
        "id": "string",
        "name": "string",
        "scanPoolType": 0,
        "isDefault": true,
        "scanInstances": [
          {
            "id": "string",
            "scanPoolId": "string",
            "url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ]
      },
      "failOverScanPoolId": "string",
```

```
"id": "string",
        "name": "string",
        "scanPoolType": 0,
        "isDefault": true,
        "scanInstances": [
          {
            "id": "string",
            "scanPoolId": "string",
            "url": "string",
            "apiKey": "string",
            "timeout": "string",
            "scanInstanceType": 0
          }
        ]
      },
      "filters": {
        "id": "string",
        "minimumSize": 0,
        "maximumSize": 0,
        "minimumDateTime": "2019-08-24T14:15:22Z",
        "maximumDateTime": "2019-08-24T14:15:22Z"
      },
      "fileDefinition": {
        "blockingStrategy": 0,
        "configurableBlockingStrategy": {
          "shouldTreatFilesWithSensitiveDataAsBlocked": true,
          "shouldTreatFilesWithVulnerabilitiesAsBlocked": true
        }
      },
      "remediations": [
        {
          "id": "string",
          "workflowId": "string",
          "isEnabled": true,
          "configuration": "string",
          "type": 0,
          "handlingType": 0
        }
      ],
      "tenantId": "string"
    }
  ],
  "scanPoolHasApiKey": {
    "property1": true,
    "property2": true
  }
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» entries	[Workflow]¦null	false	none	none
» scanPoolHasApiKey	object¦null	false	none	none
»» **additionalProperties**	boolean	false	none	none

GetWorkflowByIdCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "entry": {
    "id": "string",
    "scanPoolId": "string",
    "scanProcessFlow": 0,
    "isIdentityScanningEnabled": true,
    "scanIntervalDays": 0,
    "rules": [
      "string"
    ],
    "type": 0,
    "workflowSupportedTechnologies": {
      "dlp": {
        "status": 0
      },
      "deepCdr": {
        "status": 0
      },
      "sandBox": {
        "status": 0
      },
      "metascan": {
        "status": 0
      }
    },
    "name": "string",
    "userAgent": "string",
    "scanPool": {
      "id": "string",
      "name": "string",
      "scanPoolType": 0,
      "isDefault": true,
      "scanInstances": [
        {
          "id": "string",
          "scanPoolId": "string",
          "url": "string",
          "apiKey": "string",
          "timeout": "string",
          "scanInstanceType": 0
        }
      ]
    },
    "failOverScanPoolId": "string",
    "failOverScanPool": {
```

```
"name": "string",
      "scanPoolType": 0,
      "isDefault": true,
      "scanInstances": [
        {
          "id": "string",
          "scanPoolId": "string",
          "url": "string",
          "apiKey": "string",
          "timeout": "string",
          "scanInstanceType": 0
        }
      ]
    },
    "filters": {
      "id": "string",
      "minimumSize": 0,
      "maximumSize": 0,
      "minimumDateTime": "2019-08-24T14:15:22Z",
      "maximumDateTime": "2019-08-24T14:15:22Z"
    },
    "fileDefinition": {
      "blockingStrategy": 0,
      "configurableBlockingStrategy": {
        "shouldTreatFilesWithSensitiveDataAsBlocked": true,
        "shouldTreatFilesWithVulnerabilitiesAsBlocked": true
      }
    },
    "remediations": [
      {
        "id": "string",
        "workflowId": "string",
        "isEnabled": true,
        "configuration": "string",
        "type": 0,
        "handlingType": 0
      }
    ],
    "tenantId": "string"
  },
  "scanPoolHasApiKey": {
    "property1": true,
    "property2": true
  }
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» entry	Workflow¦null	false	none	none
» scanPoolHasApiKey	object¦null	false	none	none
»» **additionalProperties**	boolean	false	none	none

AddWorkflowCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "workflowId": "string"
}
```

Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» workflowId	string¦null	false	none	none

AddWorkflowParameters

```
{
  "scanPoolId": "string",
  "rules": [
    "string"
  ],
  "name": "string",
  "userAgent": "string",
  "failOverScanPoolId": "string",
  "filters": {
    "minimumSize": 0,
    "maximumSize": 0,
    "minimumDateTime": "2019-08-24T14:15:22Z",
    "maximumDateTime": "2019-08-24T14:15:22Z"
  },
  "scanProcessFlow": 0,
  "isIdentityScanningEnabled": true,
  "scanIntervalDays": 1
}
```

Properties

Name	Type	Required	Restrictions	Description
scanPoolId	string¦null	false	none	none
rules	[string]¦null	false	none	none
name	string	true	none	none
userAgent	string¦null	false	none	none
failOverScanPoolId	string¦null	false	none	none
filters	AddFilters¦null	false	none	none
scanProcessFlow	ScanProcessFlow¦null	false	none	- 0: WithScanning - 1: WithoutScanning
isIdentityScanningEnabled	boolean¦null	false	none	none
scanIntervalDays	integer¦null	false	none	none

AddFilters

```
{
  "minimumSize": 0,
  "maximumSize": 0,
  "minimumDateTime": "2019-08-24T14:15:22Z",
  "maximumDateTime": "2019-08-24T14:15:22Z"
}
```


Properties

Name	Type	Required	Restrictions	Description
minimumSize	integer(int64)	false	none	none
maximumSize	integer(int64)	false	none	none
minimumDateTime	string(date-time)	false	none	none
maximumDateTime	string(date-time)	false	none	none

UpdateWorkflowCommandResponse


```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none

UpdateWorkflowParameters


```
{
  "id": "string",
  "scanPoolId": "string",
  "scanProcessFlow": 0,
  "rules": [
    "string"
  ],
  "name": "string",
  "userAgent": "string",
  "failOverScanPoolId": "string",
  "failOverDisabled": true,
  "filters": {
    "minimumSize": 0,
    "maximumSize": 0,
    "minimumDateTime": "2019-08-24T14:15:22Z",
    "maximumDateTime": "2019-08-24T14:15:22Z"
  },
  "fileDefinition": {
    "blockingStrategy": 0,
    "configurableBlockingStrategy": {
      "shouldTreatFilesWithSensitiveDataAsBlocked": true,
      "shouldTreatFilesWithVulnerabilitiesAsBlocked": true
    }
  },
  "isIdentityScanningEnabled": true,
  "scanIntervalDays": 1
}
```

Properties

Name	Type	Required	Restrictions	Description
id	string	true	none	none
scanPoolId	string¦null	false	none	none
scanProcessFlow	ScanProcessFlow¦null	false	none	- 0: WithScanning - 1: WithoutScanning
rules	[string]¦null	false	none	none
name	string¦null	false	none	none
userAgent	string¦null	false	none	none
failOverScanPoolId	string¦null	false	none	none
failOverDisabled	boolean¦null	false	none	none
filters	UpdateFilters¦null	false	none	none
fileDefinition	FileDefinition¦null	false	none	none
isIdentityScanningEnabled	boolean¦null	false	none	none
scanIntervalDays	integer¦null	false	none	none

UpdateFilters

```
{
  "minimumSize": 0,
  "maximumSize": 0,
  "minimumDateTime": "2019-08-24T14:15:22Z",
  "maximumDateTime": "2019-08-24T14:15:22Z"
}
```

Properties

Name	Type	Required	Restrictions	Description
minimumSize	integer(int64)	false	none	none
maximumSize	integer(int64)	false	none	none
minimumDateTime	string(date-time)	false	none	none
maximumDateTime	string(date-time)	false	none	none

DeleteWorkflowCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```

Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none

SetDefaultWorkflowCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  }
}
```

Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none

RefreshSupportedTechnologiesCommandResponse

```
{
  "result": 0,
  "responseKey": "string",
  "responseMessage": "string",
  "responseMessageParams": {
    "property1": "string",
    "property2": "string"
  },
  "workflowDto": {
    "id": "string",
    "scanPoolId": "string",
    "scanProcessFlow": 0,
    "isIdentityScanningEnabled": true,
    "scanIntervalDays": 0,
    "rules": [
      "string"
    ],
    "type": 0,
    "workflowSupportedTechnologies": {
      "dlp": {
        "status": 0
      },
      "deepCdr": {
        "status": 0
      },
      "sandBox": {
        "status": 0
      },
      "metascan": {
        "status": 0
      }
    },
    "name": "string",
    "userAgent": "string",
    "scanPool": {
      "id": "string",
      "name": "string",
      "scanPoolType": 0,
      "isDefault": true,
      "scanInstances": [
        {
          "id": "string",
          "scanPoolId": "string",
          "url": "string",
          "apiKey": "string",
          "timeout": "string",
          "scanInstanceType": 0
        }
      ]
    },
    "failOverScanPoolId": "string",
    "failOverScanPool": {
```

```
"name": "string",
      "scanPoolType": 0,
      "isDefault": true,
      "scanInstances": [
        {
          "id": "string",
          "scanPoolId": "string",
          "url": "string",
          "apiKey": "string",
          "timeout": "string",
          "scanInstanceType": 0
        }
      ]
    },
    "filters": {
      "id": "string",
      "minimumSize": 0,
      "maximumSize": 0,
      "minimumDateTime": "2019-08-24T14:15:22Z",
      "maximumDateTime": "2019-08-24T14:15:22Z"
    },
    "fileDefinition": {
      "blockingStrategy": 0,
      "configurableBlockingStrategy": {
        "shouldTreatFilesWithSensitiveDataAsBlocked": true,
        "shouldTreatFilesWithVulnerabilitiesAsBlocked": true
      }
    },
    "remediations": [
      {
        "id": "string",
        "workflowId": "string",
        "isEnabled": true,
        "configuration": "string",
        "type": 0,
        "handlingType": 0
      }
    ],
    "tenantId": "string"
  }
}
```


Properties

allOf

Name	Type	Required	Restrictions	Description
anonymous	RestResponse	false	none	none

and

Name	Type	Required	Restrictions	Description
anonymous	object	false	none	none
» workflowDto	Workflow¦null	false	none	none

RefreshSupportedTechnologiesCommandRequest

```
{
  "workflowId": "string"
}
```

Properties

Name	Type	Required	Restrictions	Description
workflowId	string	true	none	none

OPSWAT.

