

ONBOARD SENTINELONE TO MANAGED DEFENSE



To onboard or rotate credentials, ensure that you are assigned the Team Admin role within the Managed Defense Portal.

This document describes the configuration steps required for SentinelOne and Mandiant Managed Defense (Managed Defense) integration.

1. Prerequisites for SentinelOne

The following prerequisites must be met before connecting your SentinelOne instance to Mandiant Managed Defense:

The SentinelOne subscription must have the following features:

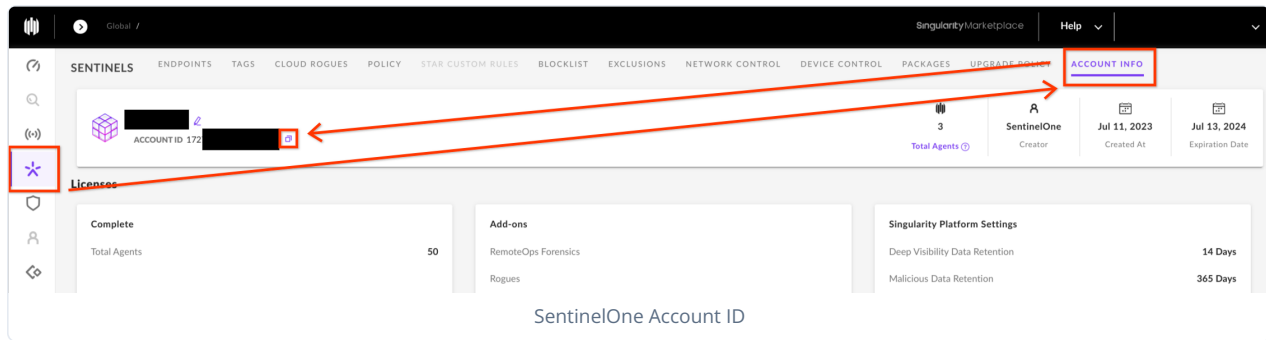
- An active **Singularity Complete** (<https://www.sentinelone.com/platform/singularity-complete/>) subscription for SentinelOne. **Cloud Funnel** (<https://www.sentinelone.com/platform/singularity-cloud-funnel/>) telemetry streaming is a necessary option, and at present it is not available for Singularity Core or Singularity Control packages. Refer to **Platform Packages** (<https://www.sentinelone.com/platform-packages/>) for additional details.
- An active license for the **Cloud Funnel** (<https://www.sentinelone.com/platform/singularity-cloud-funnel/>) Data Lake Streaming Module. This is used to stream telemetry data to Managed Defense for threat hunting and alert investigation
- An active Cloud Storage to receive Hunting Telemetry (Google Cloud Storage, Amazon S3 bucket, or Azure Blob Storage)

Managed Defense needs the following access:

- An API Token with Admin role for the Global or Account level
- API Token with Viewer role for the Global or Account level
- Amazon S3 bucket permissions

2. Collect SentinelOne Account ID

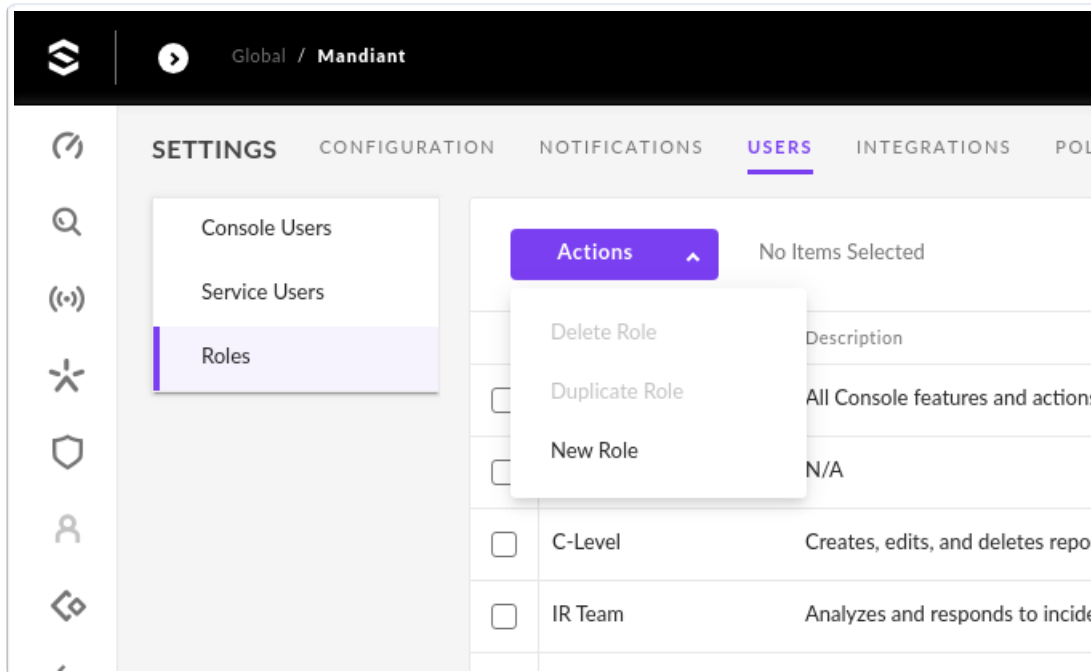
Your Sentinel One Account ID can be found by logging into your Sentinel One Singularity Portal. Once authenticated, click the "Sentinels" navigation button on the left, followed by the **ACCOUNT INFO** tab at the top-right. You receive the basic account information, which includes your **ACCOUNT ID** and a button that lets you copy  content. Click  copy and paste it somewhere for safe keeping. Refer to the following screenshot for a visual on how to copy the **Account ID**.



3. Create new user role

The SentinelOne platform comes with multiple built-in roles. However, only the **Admin** role has all the permissions needed for the Managed Defense service to be successful. This role comes with many permissions that are not needed by Managed Defense. If using the Admin role is not acceptable, follow these steps to create a role to suffice for Managed Defense service. Otherwise, skip to the next step.

1. In SentinelOne, navigate to the User **Roles** page (**Settings > Users > Roles**) and select **New Role** from the **Actions** menu.



Create New Role option in the Actions menu

2. Fill in the **Role Name** and **Description** fields.
3. Select permissions as follows:
 - Endpoints (seven permissions)
 - View
 - View threats
 - Search on Deep Visibility
 - Reconnect to Network
 - File Fetch

- Disconnect from Network
- Fetch Logs
- Endpoint Threats
 - All permissions
- Accounts (one permission)
 - View
- Activity (one permission)
 - View
- Cloud (one permission)
 - View
- Cloud Funnel (one permission)
 - View
- Console Users (one permission)
 - View
- Device Control (one permission)
 - View
- Endpoint Policy (one permission)
 - View
- Exclusions (one permission)
 - View
- Groups (one permission)
 - View
- Identity Threats (one permission)
 - View
- Locations (one permission)
 - View
- Roles (one permission)
 - View
- STAR Custom Rules (one permission)
 - View
- STAR Rule Alerts (three permissions)
 - View
 - Update Incident Status
 - Update Analyst Verdict
- Service Users (one permission)
 - View
- Sites (one permission)

- [View](#)

4. Click **Save**.

New Role

• Role Name:	MD API Role
--------------	-------------

Description:	Role for MD API access requirem...
--------------	------------------------------------

Role Scope: Account

 Search for pages

Endpoints

7/53

Endpoint Threats

16/16

AD Configuration

0/2

AD Exposure Exclusions

0/2

AD Exposures

0/5

Access Settings

0/2

Accounts

 $\frac{1}{4}$

Activity

1/1

☐ Select All

 [View](#)

Account Uninstall Password (2)

 [View Threats](#)

☐ Update Software☐ Unprotect☐ Shut Down☐ Show Passphrase

Cancel

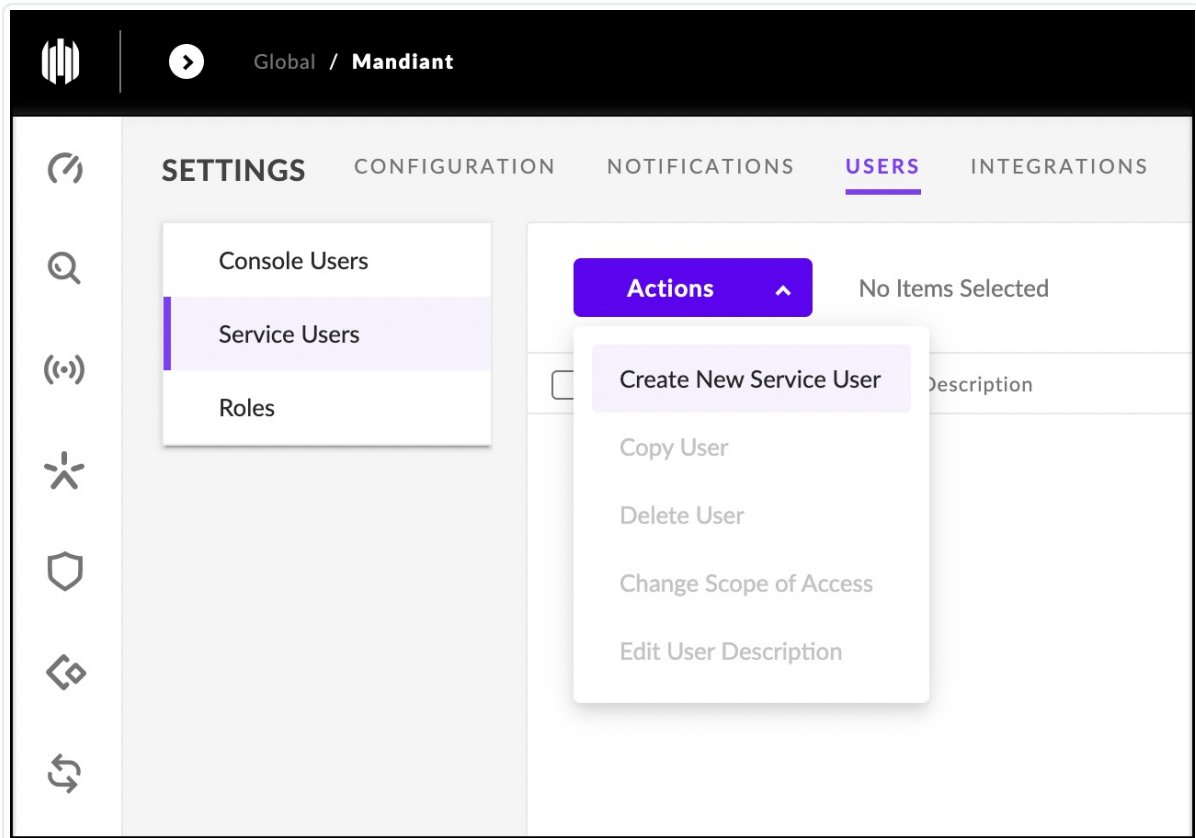
Save

4. Create user accounts and API tokens in SentinelOne

Create MD API Service Account

The MD API service account is used for collecting endpoint details, Endpoint Protection Platform (EPP) threats/Simulated Target Attack Response (STAR) alerts, and executing acquisition/containment actions on a SentinelOne instance.

1. From the SentinelOne instance, navigate to the **Service Users** page (**Settings > Users > Service Users**) and select **Create New Service User** from the **Actions** menu.



Create New Service User option in the Actions menu

2. Fill in the **Name**, **Description**, and **Expiration Date** fields.

Create New Service User



Name *

Name of Service User cannot be edited after creation

Description

Expiration Date *

1 Year

▼

Oct 17, 2025 12:46:50

ⓘ SentinelOne does not recommend exceeding a 1-month expiration duration as it undermines security.

Cancel

Next

Create New Service User screen

3. Select the **Global** access level (or **Account** level if you are on a shared tenant). For the Role, select either **Admin** or the role created in the previous step (for example, **MD API Role**).

×

Select Scope of Access

Set the Scope of Access manually or [Copy The Scope From A Different User](#)

Access Level



Account



Site

Q

1 / 1 Account selected All Accounts ▼ Clear Selection

☒

Mandiant

MD API Role ▼

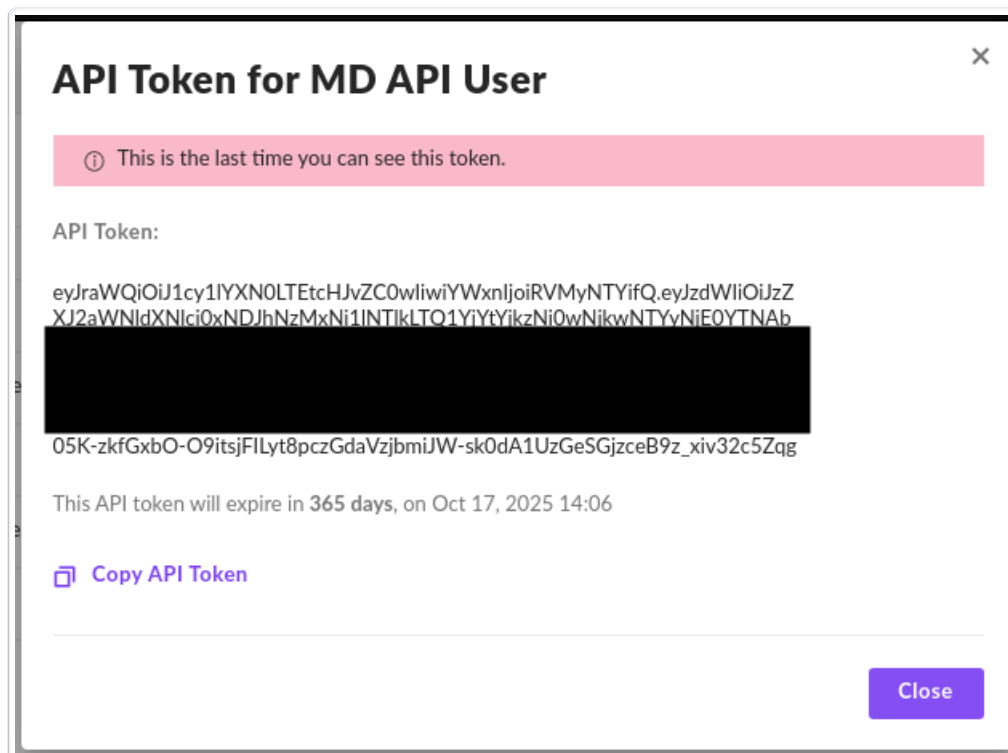
Cancel

Back

Create User

Select Scope of Access for user role

- After clicking **Create User**, record the Service Token details (**API Token** and **expiration date**) and provide them to Managed Defense.



API Token for MD API User

5. Add containment tag to endpoints

Mandiant offers endpoint containment for SentinelOne agents that are tagged within the SentinelOne Console. For any endpoints a customer would like to be containable, the `MD_Containment-Allowlist` tag must be added. Use the following steps to add tags to all applicable endpoints.

Create tags



Follow the tag creation process before tagging individual endpoints.

1. Go to **Sentinels > Tags**.
2. **Actions > Create**.
3. For **Tag Key**, enter `MD_Containment-Allowlist`.
4. For **Tag Value**, select `No Value`.
5. Enter the following description and click **Create**.
`Endpoints with this tag are allowed to be contained by Mandiant Managed Defense`

Apply tags

After the tag is created, you can tag each endpoint.

1. Go to **Sentinels > Endpoints**.
2. Check an endpoint, then choose **Actions** and search for `tags`.
For large groups of endpoints, use the **Endpoint Name** filter. You can upload a CSV file of endpoints to create a filter.
3. Select **Manage Tags**.
4. For **Tag Key**, select `MD_Containment-Allowlist` and `No Value`, then click **Add Tag**.

5. Click **Apply Changes**.
6. Repeat this process for every endpoint that should be tagged for the allow list.

6. Configure Google Cloud Storage

You can export SentinelOne Cloud Funnel data to Google Cloud Storage. Mandiant recommends using Google Cloud Storage since this data is sent to Google Security Operations (SecOps). Using Google Cloud Storage minimizes data transfer fees.

Create the Google Cloud Storage Bucket

1. Follow the Google Cloud documentation for **Creating Buckets** (<https://cloud.google.com/storage/docs/creating-buckets>) to create a new Google Cloud Storage bucket using the **Standard Storage** class to store the SentinelOne Cloud Funnel telemetry data.
2. After creating the bucket, give SentinelOne permission to write to it. From the bucket, click **Permissions** and then **Grant Access**.
3. Click **Add principals**, and add SentinelOne service account email according to your region:

Region	Service Principal
Canada	dvca1-evdb@gcp-s1-prod-scalyr-cs.iam.gserviceaccount.com
USA	dvus1-evdb@gcp-s1-prod-scalyr-cs.iam.gserviceaccount.com
Europe	dveu1-evdb@gcp-s1-prod-scalyr-cs.iam.gserviceaccount.com
Asia Pacific	dvap1-evdb@gcp-s1-prod-scalyr-cs.iam.gserviceaccount.com
India	advaps11-evdb@gcp-s1-prod-scalyr-cs.iam.gserviceaccount.com

4. Under **Assign Roles**, select **Storage Object Creator**.
5. Click **+Add Another Role** and select **Storage Object Viewer**.
6. Click **Save** to write the permission changes.

7. Configure an S3 bucket

Alternatively, if you don't choose Google Cloud Storage, you can store Cloud Funnel data in an Amazon S3 bucket. Follow the instructions in the SentinelOne support article **How to Configure Your S3 Bucket** (<https://support.sentinelone.com/hc/en-us/articles/9289437366295-How-To-Configure-Your-S3-Bucket>). Mandiant accesses the data stored in the bucket using Google Security Operations (SecOps), which results in AWS data transfer costs.

Once the S3 bucket is created, create and configure an IAM User for Mandiant to access the bucket:

1. Create an IAM User that has read access for the data contained in that Amazon S3 bucket.
2. Attach the required policy (replace `BUCKET_ARN` with the ARN of your S3 Bucket):

```
{
  "Statement": [
    {
      "Action": "s3:GetObject",
      "Effect": "Allow",
      "Resource": "BUCKET_ARN/*",
      "Sid": "Read"
    },
    {
      "Action": "s3:ListBucket",
      "Effect": "Allow",
      "Resource": "BUCKET_ARN",
      "Sid": "List"
    }
  ],
  "Version": "2012-10-17"
}
```

3. Create access keys for the IAM User.
4. Record the S3 bucket information in a location for safe keeping.

8. Configure Azure to receive hunting telemetry

The following document covers creating a new Azure Blob Storage account to store telemetry data from your EDR's telemetry streaming service. Managed Defense can also use an existing blob storage account that holds data from the streaming service provided the following requirements are met:

1. Existing consumers of the data in blob storage do not delete data from the storage account.
2. The blob storage has at least three days of retention.
3. The storage contains the necessary telemetry required for the Managed Defense threat hunting service.

To create an Azure Blob Storage account:

1. **Create an Azure Blob Storage Account (Required).**
2. **Configure a Storage Lifecycle Policy (Recommended).**
3. **Configure IP Address Access Restrictions on Storage Account (Optional).**
4. **Configure a Storage Account Share Access Signature (Required).**

Create an Azure Blob Storage account



For the following steps, you require permission to create a storage account in the destination Azure Resource group.

1. Sign in to <https://portal.azure.com>.
2. Navigate to **Storage Accounts** and select **Create**.
3. On the **Create a storage account** page, provide the storage account information starting with the **Project details** section:
 - a. Select the subscription for the new storage account.
 - b. Create a resource group named `mandiantmd`.
4. For the **Instance details**, select the following default options:
 - **Storage account name:** Choose a unique name for your storage account. Storage account names must be

between 3 and 24 characters in length and may contain numbers and lowercase letters only.

- **Region:** Select the appropriate region for your storage account.
- **Performance:**
- **Redundancy:** or

[Home](#) > [Storage accounts](#) >

Create a storage account ...

[Basics](#) [Advanced](#) [Networking](#) [Data protection](#) [Encryption](#) [Tags](#) [Review + create](#)

Azure Storage is a Microsoft-managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. Azure Storage includes Azure Blobs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azure Tables. The cost of your storage account depends on the usage and the options you choose below. [Learn more about Azure storage accounts](#) ↗

Project details

Select the subscription in which to create the new storage account. Choose a new or existing resource group to organize and manage your storage account together with other resources.

Subscription *

mandiantmdatpqa

Resource group *

mandiantmde

[Create new](#)

Instance details

Storage account name * ⓘ

uniquecustomername

Region * ⓘ

(US) West US 2

[Deploy to an Azure Extended Zone](#)

Primary service ⓘ

Select a primary service

Performance * ⓘ

☒ **Standard:** Recommended for most scenarios (general-purpose v2 account)

☐ **Premium:** Recommended for scenarios that require low latency.

Redundancy * ⓘ

Zone-redundant storage (ZRS)

Previous

Next

Review + create

5. On the **Advanced** tab, clear the **Allow enabling anonymous access on individual containers** checkbox.

Home > Storage accounts >

Create a storage account ...

Basics Advanced Networking Data protection Encryption Tags Review + create

Security

Configure security settings that impact your storage account.

Require secure transfer for REST API operations ☒ ⓘ

Allow enabling anonymous access on individual containers ☐ ⓘ

Enable storage account key access ⓘ ☒

6. After configuring the preceding settings, click **Review + create**.

Refer to the Microsoft documentation **Create a Storage Account** (<https://learn.microsoft.com/en-us/azure/storage/common/storage-account-create?tabs=azure-portal>) for additional information about setting up Microsoft Azure Blob Storage.

Configure a storage lifecycle policy

To reduce storage costs, you can configure a storage lifecycle policy to automatically delete data from Azure Blob Storage. Mandiant recommends keeping data available in Azure Blob Storage for three to seven days in case there are operational issues with data ingestion.

1. From the **Data management** section of the storage account, select **Lifecycle management**.
2. Select the **List View** tab.
3. Select **Add a rule** and set the rule name to `delete-policy`.
4. Select **Limit blobs with filters** under the **Rule Scope** section.
5. Select **Block blobs** and **Append blobs** under the **Blob type** section.
6. Select **Base blobs** under the **Blob subtype** section.
7. Create a rule with the following condition:
 - *If Base blobs were created more than three days ago delete the blob.*

The lifecycle policy may take up to 48 hours to take effect. For more information, refer to the **Configure a lifecycle management policy** (<https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-policy-configure?tabs=azure-portal>) Microsoft documentation.

Optional: Configure IP address access restrictions on storage account

Managed Defense uses Google Security Operations (Google SecOps) to acquire storage account data. You can optionally configure ACLs for IP addresses of the Storage Transfer Service (STS) infrastructure used by Google SecOps to access their storage account. The IP address ranges are published in the following JSON file: **IP ranges** (<https://www.gstatic.com/storage-transfer-service/ipranges.json>)

Configure IP address access restrictions by following these steps:

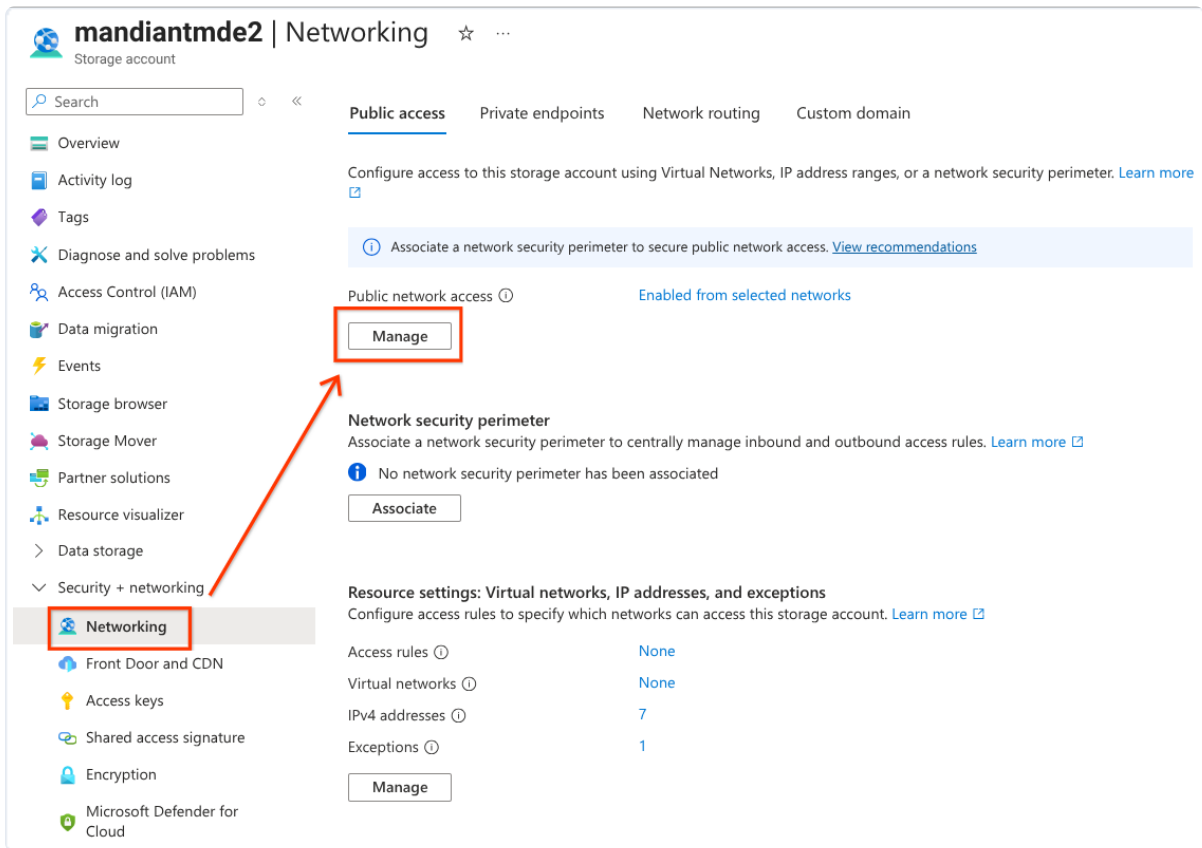
We recommend reading data from this JSON file at least weekly to keep your security configuration up to date. When a new range is added to the file, the system waits at least 7 days before using that range for requests from STS.



For a sample Python script that fetches IP ranges from a JSON file, see [IP addresses for default domains \(https://docs.cloud.google.com/vpc/docs/configure-private-google-access#ip-addr-defaults\)](https://docs.cloud.google.com/vpc/docs/configure-private-google-access#ip-addr-defaults).

Compare the current IP range `creationTime` to the IP range `creationTime` read from the previous JSON file. If these differ, update the IP access restrictions.

1. Go to **Security + networking** and then click **Networking**.
2. From **Public network access**, click **Manage**.



mandiantmde2 | Networking ☆ ...

Storage account

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
Security + networking
Networking
Front Door and CDN
Access keys
Shared access signature
Encryption
Microsoft Defender for Cloud

Public access Private endpoints Network routing Custom domain

Configure access to this storage account using Virtual Networks, IP address ranges, or a network security perimeter. [Learn more](#)

Associate a network security perimeter to secure public network access. [View recommendations](#)

Public network access ⓘ Enabled from selected networks

Manage

Network security perimeter
Associate a network security perimeter to centrally manage inbound and outbound access rules. [Learn more](#)

No network security perimeter has been associated

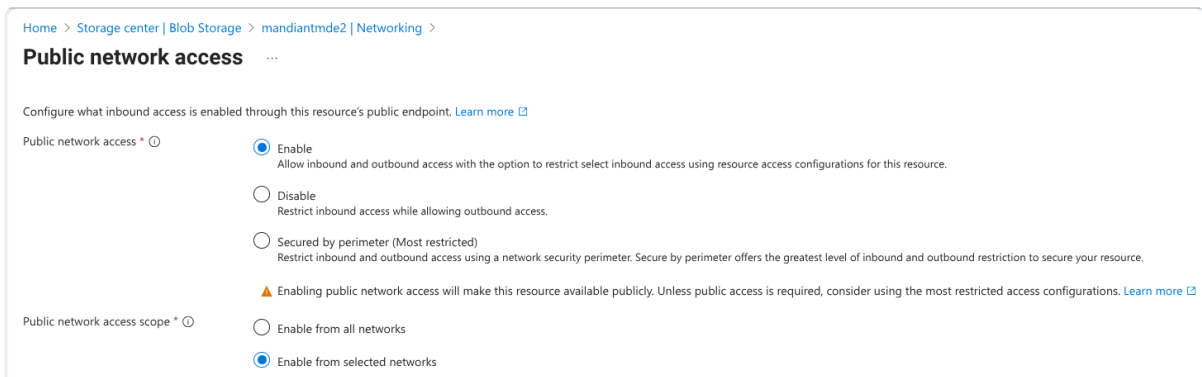
Associate

Resource settings: Virtual networks, IP addresses, and exceptions
Configure access rules to specify which networks can access this storage account. [Learn more](#)

Access rules ⓘ None
Virtual networks ⓘ None
IPv4 addresses ⓘ 7
Exceptions ⓘ 1

Manage

3. For **Public network access**, select **Enable**.
4. For **Public network access scope**, select **Enable from selected networks**.



Home > Storage center | Blob Storage > mandiantmde2 | Networking >

Public network access ...

Configure what inbound access is enabled through this resource's public endpoint. [Learn more](#)

Public network access * ⓘ

☒ **Enable**
Allow inbound and outbound access with the option to restrict select inbound access using resource access configurations for this resource.

☐ **Disable**
Restrict inbound access while allowing outbound access.

☐ **Secured by perimeter (Most restricted)**
Restrict inbound and outbound access using a network security perimeter. Secure by perimeter offers the greatest level of inbound and outbound restriction to secure your resource.

▲ Enabling public network access will make this resource available publicly. Unless public access is required, consider using the most restricted access configurations. [Learn more](#)

Public network access scope * ⓘ

☐ **Enable from all networks**

☒ **Enable from selected networks**

5. In the **IPv4 Addresses** section, enter the **IP ranges** (<https://www.gstatic.com/storage-transfer-service/ipranges.json>), one row for each range.
6. Under **Exceptions**, select **Allow trusted Microsoft services to access this resource**.

Exceptions

☒ Allow trusted Microsoft services to access this resource

☐ Allow read access to storage logging from any network

☐ Allow read access to storage metrics from any network

7. When complete, save your changes.



If you choose not to implement **IP restrictions**, you must set the **Public network access** parameter to **Enabled from all networks**. Selecting the **Disabled** option prevents you from accessing the blob storage account.

Refer to Microsoft documentation: [Configure Azure Storage firewalls and virtual networks](https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-portal#grant-access-from-an-internet-ip-range) (<https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-portal#grant-access-from-an-internet-ip-range>) to configure network access restrictions on storage.

Configure a storage account shared access signature

Once you have an Azure Storage account, Managed Defense requires a Shared Access Signature (SAS) to access the stored data.

1. On the storage account navigation pane, in the **Security + networking** section and select **Shared access signature**.
 1. Select the following parameters:

An account-level SAS can delegate access to multiple storage services (i.e. blob, file, queue, table). Note that stored access policies are currently not supported for an account-level SAS.

[Learn more about creating an account SAS](#)

Allowed services 

☒ Blob ☐ File ☐ Queue ☐ Table

Allowed resource types 

☐ Service ☒ Container ☒ Object

Allowed permissions 

☒ Read ☐ Write ☐ Delete ☒ List ☐ Add ☐ Create ☐ Update ☐ Process ☐ Immutable storage ☐ Permanent delete

Blob versioning permissions 

☐ Enables deletion of versions

Allowed blob index permissions 

☒ Read/Write ☒ Filter

Start and expiry date/time 

Start

End

(UTC-08:00) Pacific Time (US & Canada) 

Allowed IP addresses 

For example, 168.1.5.65 or 168.1.5.65-168.1.5.70

Allowed protocols 

☒ HTTPS only ☐ HTTPS and HTTP

Preferred routing tier 

☒ Basic (default) ☐ Microsoft network routing ☐ Internet routing

 Some routing options are disabled because the endpoints are not published.

Signing key 

[Generate SAS and connection string](#)

Generate SAS and connection string

2. Click **Generate SAS and connection string (SAS Token)** (<https://learn.microsoft.com/en-us/azure/storage/common/storage-sas-overview>). Add this value to the SAS Token field in the credentials file as you need to send these credentials to Mandiant.
3. Click **Endpoints** from the storage account and copy the values from **Storage account resource ID** and **Blob service > Primary Endpoint**. Add these values to the credentials file as you need to send these credentials to Mandiant.

9. Configure Cloud Funnel export

1. Sign in to the SentinelOne management console.
2. In the **Settings** toolbar, select **Integrations > Cloud Funnel**.
3. In the **Cloud Provider** list, select the storage platform you have set up as your Cloud Provider.
4. Fill out the form for that storage platform with the information from set up. For example, if you use Google Cloud Storage, enter the name of the Cloud Storage bucket in the **GCS Storage Name** field.
5. Click **Validate** to validate whether the bucket exists, and that SentinelOne has read and write access to the bucket.
6. Select **Enable Telemetry Streaming** to stream your XDR data to your bucket.
7. Click **Save**.

Mandiant does not delete data read from the bucket. To reduce storage fees, Mandiant recommends [setting an object lifecycle policy](https://cloud.google.com/storage/docs/lifecycle) (<https://cloud.google.com/storage/docs/lifecycle>) on the storage bucket with a minimum of three days of retention for objects.

10. Post-onboarding Cloud Funnel configuration

After setting up the Cloud Funnel streaming, it's required to set up a filter to only allow the EDR telemetry data to stream to the cloud storage. This not only ensures that Managed Defense only gets the data that we need for speedy investigations and hunting, but it also limits the data that is ingressed or egressed and also the data stored in your selected cloud storage platform.

This configuration contains the following components:

1. **Additional configuration for Cloud Funnel exports**
2. **Post-onboarding validation**

Additional configuration for Cloud Funnel exports

The following configuration requires the updated SentinelOne Singularity Data Lake Console XDR web interface.

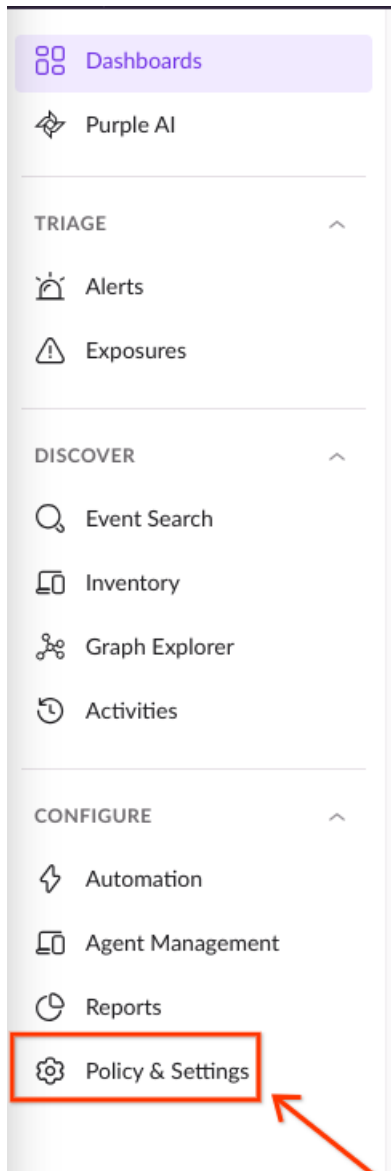
If the legacy Singularity console is still in use, use the following steps to activate the Singularity Data Lake XDR web interface in your console:



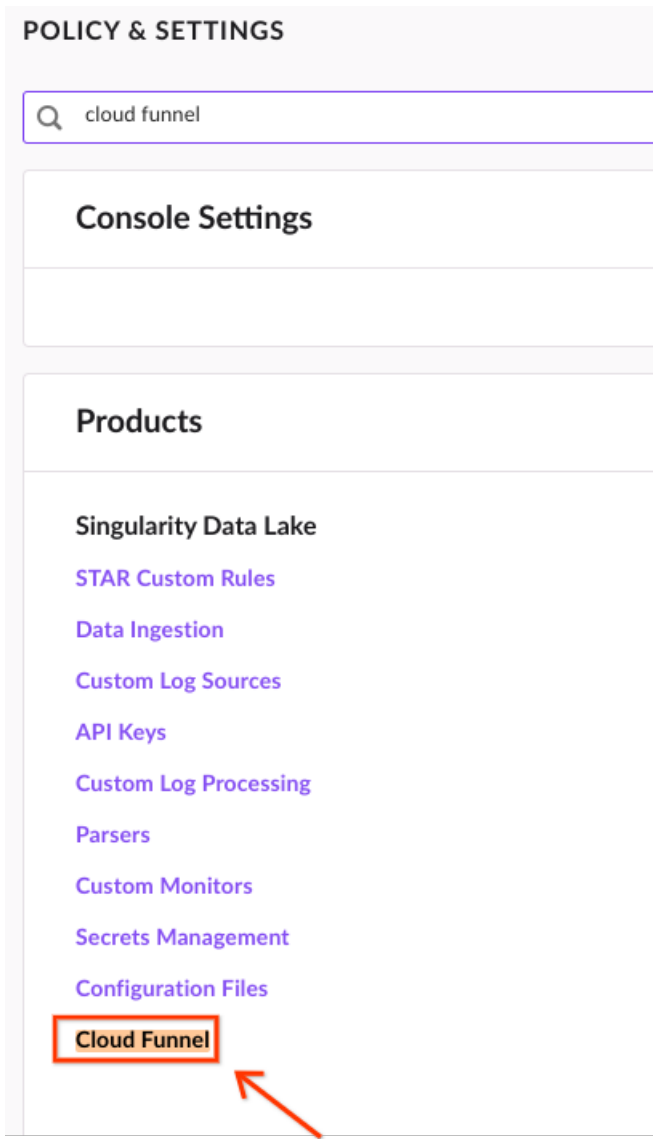
1. In the console, locate and click your username.
2. From the menu, select **My User**.
3. Within the new window that appears, click **Change Deep Visibility Mode** and then choose **Enhanced** from the available options. The Singularity Data Lake feature is then successfully activated. The sidebar within the Console shows the indication **Visibility Enhanced**.

Configure Telemetry Streaming for Cloud Funnel

1. In the Singularity Data Lake XDR console, click **Policy & Settings**.



2. Use the search bar to search for the string `cloud funnel`. Once loaded, click the highlighted menu item.



3. From the SentinelOne Cloud Funnel configuration screen, navigate to **Telemetry Streaming** and paste the following query in the query filter search bar:

```
(i.scheme = 'edr')
```

4. Click **Validate** and wait for a green checkbox indicator. If for any reason the validation fails, take note of the error message and reach out to your Managed Defense Service Transition Manager (STM).

Post-onboarding validation

After you complete configuration from within the SentinelOne Singularity Portal, you need to verify that Managed Defense only gets the data that we need for speedy investigations and hunting, as well as reducing egress costs.

To do this, reach out to your STM to make them aware that the additional configuration has been completed. Once your STM has received this information, they utilize the SentinelOne information on our records and validate the filter state.

11. Connect SentinelOne to the MD Portal

Once you have generated your API and telemetry credentials in SentinelOne, follow these steps to securely onboard the integration directly within the MD Portal:

1. From the MD Portal navigation bar, click **Integrations**.
2. Click **Add new integration**.
3. For the **Type**, choose **SentinelOne**, and then click **Next**.
4. Fill out the required fields with the SentinelOne credentials that you created in the previous steps:
 - **API Credentials (All Customers):** Enter your **SentinelOne Console URL**, **SentinelOne Account ID**, **API Token**, and your credential **Expiration date**.
 - **Event Telemetry:** For **Include Event Telemetry**, select your **Source Type**.
 - If using Amazon S3: Enter your **S3 URI**, **Access Key ID**, and **Secret Access Key**.
 - If using Google Cloud Storage: Enter your **Storage bucket URI**.

Upon selecting this source type, a message appears displaying a specific Mandiant service account.



Before submitting this integration, you must navigate to your cloud storage environment and grant this exact service account the necessary permissions to fetch data from the source.

If you do not grant these permissions prior to clicking Save, automatic feed creations will not work. This will require manual intervention and a Mandiant Service Transition Manager (STM) needs to contact you to resolve the failure.

- If using Azure Blob Storage: Enter your **Azure URI** and **SAS Token**.



Organizations that have connected their own Google SecOps instance to the service will only see the options for providing an API client to Mandiant for orchestrations. You should configure the SentinelOne data feeds within your SecOps instance.

5. Click **Save** to finalize the configuration. A banner appears confirming that the integration was onboarded successfully.

After saving the configuration, the integration will be in a **Provisioning** state and will not display any errors with the integration. Please give the integration until the next business day and check back to see if it is in an **Operational** state. The Service Delivery Engineering team will be in contact with you if there is an issue with recommended remediation steps.

If you encounter issues with connecting your technology to the portal, see [Troubleshoot technology onboarding for Managed Defense](https://docs.mandiant.com/home/md-troubleshoot-technology-onboarding) (<https://docs.mandiant.com/home/md-troubleshoot-technology-onboarding>).