

ONBOARD SENTINELONE SINGULARITY TO MANDIANT THREAT DEFENSE



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

Mandiant Analysts use file acquisition from endpoints to reach a high quality and conclusive hunt investigation outcome. In order to meet that requirement, this document outlines the configuration steps needed for SentinelOne and MD Portal integration.

1. SentinelOne Singularity prerequisites

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

The SentinelOne subscription must have the following features:

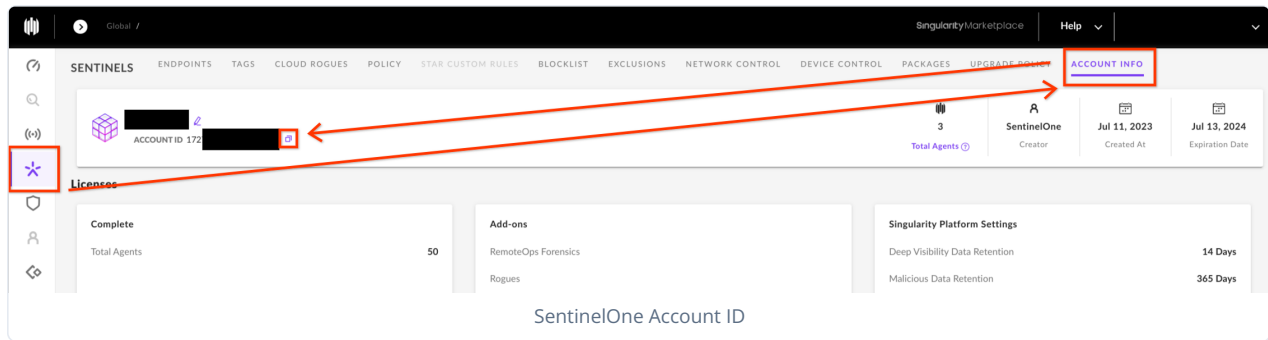
- An active **Singularity Complete** (<https://www.sentinelone.com/platform/singularity-complete/>) subscription for SentinelOne. **Cloud Funnel** (<https://www.sentinelone.com/platform/singularity-cloud-funnel/>) telemetry streaming is a necessary option, and now it is not available for Singularity 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 module is used to stream telemetry data to Mandiant Threat Defense for threat hunting and alert investigation.

Mandiant Threat Defense needs the following access:

- An API Token with Admin role for the Global or Account level
- **Ensure that you are assigned the Team Admin role within the Managed Defense Portal to onboard or rotate credentials.**

2. Collect SentinelOne account ID

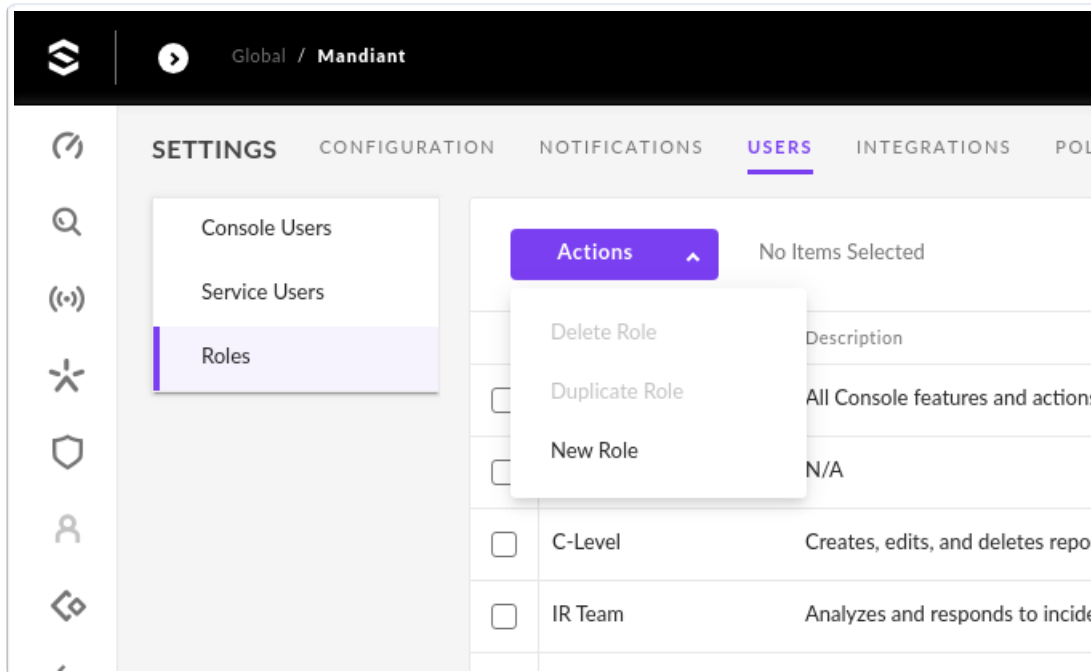
Your Sentinel One Account ID can be found by logging into your Sentinel One Singularity Portal. Once authenticated, click the "Sentinels" navigation button on the left, followed by the **ACCOUNT INFO** tab at the top-right. You receive the basic account information, which includes your **ACCOUNT ID** and a button that lets you copy content. Click copy and paste it somewhere safe. Refer to the following screenshot for a visual guide 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 Mandiant Threat Defense service to be successful. This role comes with many permissions that are not needed by Mandiant Threat Defense. If using the Admin role is not acceptable, follow these steps to create a role to suffice for Mandiant Threat 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

◦ 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	1/4
Activity	1/1

Select All

- ☒ View
- ☐ Account Uninstall Password (2)
- ☒ View Threats ⓘ
- ☐ Update Software
- ☐ Unprotect
- ☐ Uninstall
- ☐ Shut Down
- ☐ Show Passphrase

Cancel

Save

4. Create user accounts and API tokens in SentinelOne

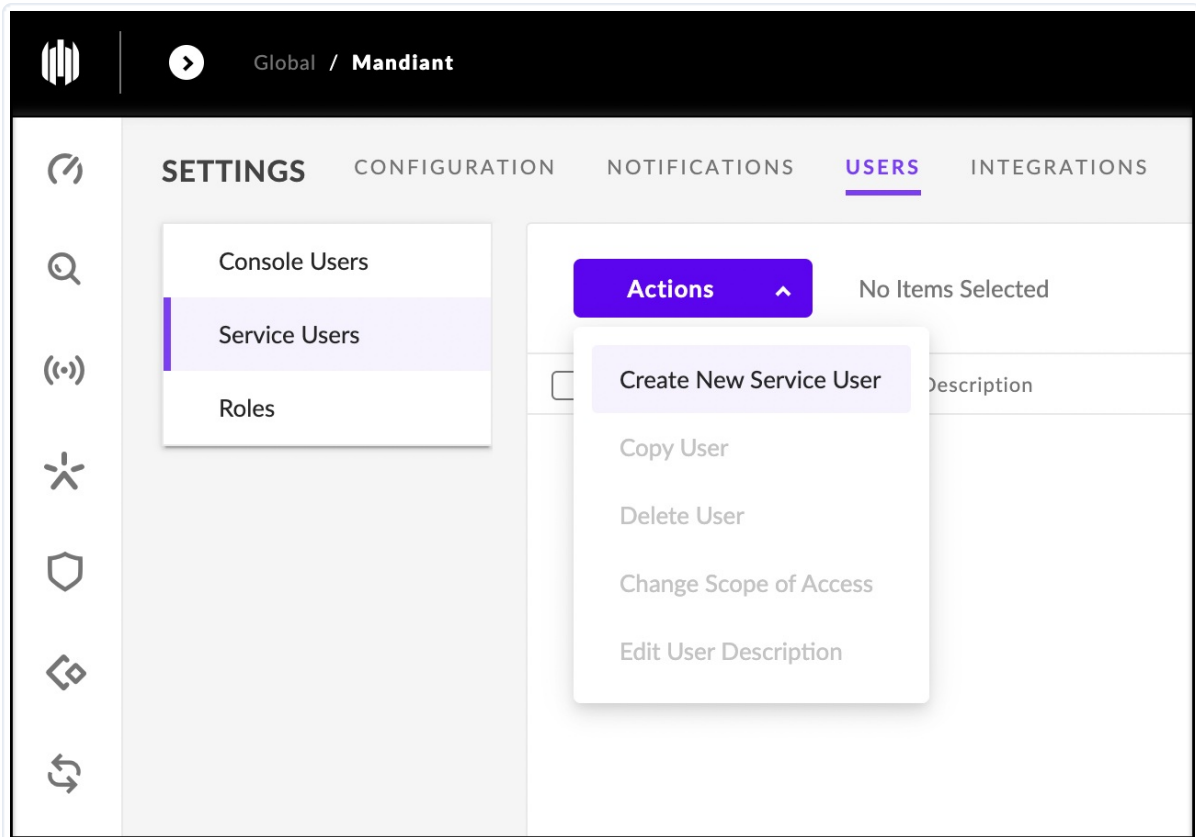
Mandiant Threat Defense SentinelOne integration requires one service account:

- **API Admin Service Account**

Create MD API Admin service account

The MD API Admin service account is used for collecting endpoint details, Endpoint Protection Platform (EPP) threats/Simulated Target Attack Response (STAR) alerts, and executing acquisition 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 *

MD API User

Name of Service User cannot be edited after creation

Description

API user for Managed Defense Service

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) and **Admin** role. If more granular role permissions are required, see the preceding section on user account creation for granular level details.

×

Select Scope of Access

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

Access Level



Global



Account



Site

Global

Admin ▼

Cancel

Back

Create User

Select Scope of Access for MD API Admin

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

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

×

API Token for MD API Admin

ⓘ This is the last time you can see this token.

API Token:

bHBvXG1sL7ceBrViKoillknOGeoSe9qHscH8X9bHj1EjsAUqhjhscjCEJvRXzzL97DYuhIGx1IfEL2UP

This API token will expire on Oct 1, 2025 00:00

📋 Copy API Token

⬇️ Download API Token

Close

API Token for MD API Admin

Add containment tag to endpoints

6. Connect SentinelOne to the MD Portal

This feature is released as a Public Preview.
Pre-GA products and features are available "as is" and might have limited support. For more information, please contact your TSC, your CSM, or go to [Support](https://docs.mandiant.com/home/mandiant-support-cases).
(<https://docs.mandiant.com/home/mandiant-support-cases>)

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**.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

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 Mandiant Threat Detection** (<https://docs.mandiant.com/home/mtd-troubleshoot-technology-onboarding>).