# ONBOARD CROWDSTRIKE FALCON 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 you require for CrowdStrike Falcon and Managed Defense (MD) integration.

---

## 1. Prerequisites

You must meet the following prerequisites before connecting your CrowdStrike Falcon instance to the MD Portal:

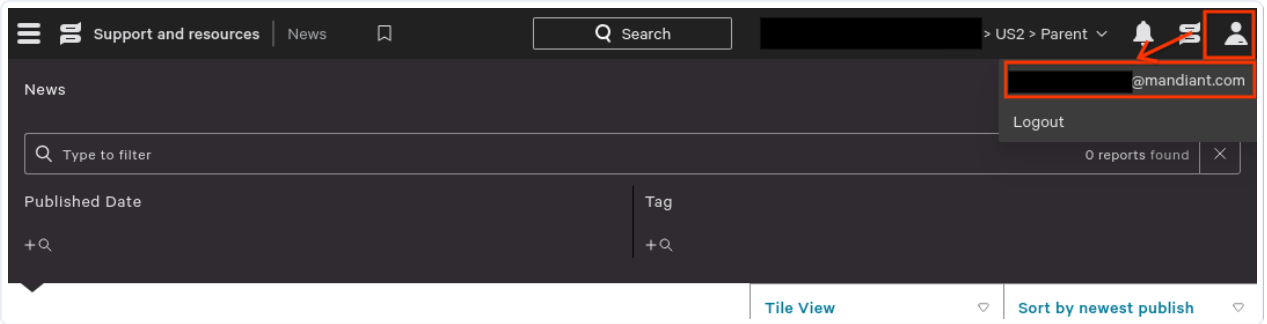
- An active CrowdStrike Falcon subscription of Falcon Enterprise, Falcon Elite, or Falcon Complete. Falcon Essentials is not supported. Refer to **Endpoint, Cloud & Identity Protection Products | CrowdStrike (https://www.crowdstrike.com/products/)**for additional details.
- An active license for Falcon Data Replicator ( **Falcon Data Replicator (FDR) | Data Sheet | CrowdStrike (https://www.crowdstrike.com/resources/data-sheets/falcon-data-replicator/)**). This is used to stream telemetry data to Mandiant for threat hunting.
- CrowdStrike Falcon tenants must be in the *US-1*, *US-2*, *EU-1*, or *US-GOV-1* CrowdStrike region. See **CrowdStrike regions table (https://docs.mandiant.com/home/associate-customer-crowdstrike-falcon-instance-md)** for details.

## 2. Find Tenant Customer ID

To find your tenant's Customer ID (CID), log in to the Falcon Portal for your environment.

The links for the Falcon Portals in the different CrowdStrike regions are listed in the **CrowdStrike regions table (https://docs.mandiant.com/home/md-crowdstrike-associate-customer-crowdstrike-falcon-instance-with-managed-defense)** of this document.

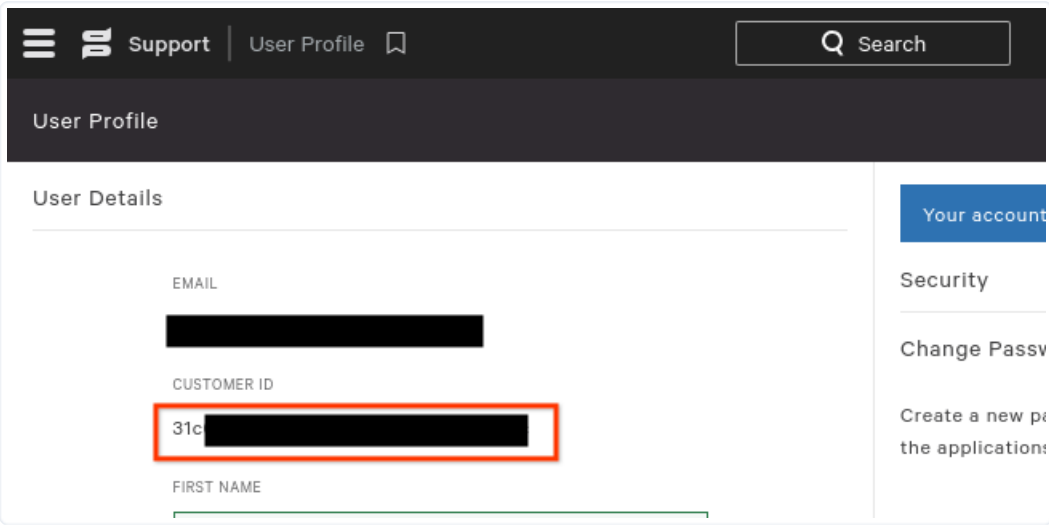
Access the **User Profile** section of the portal.



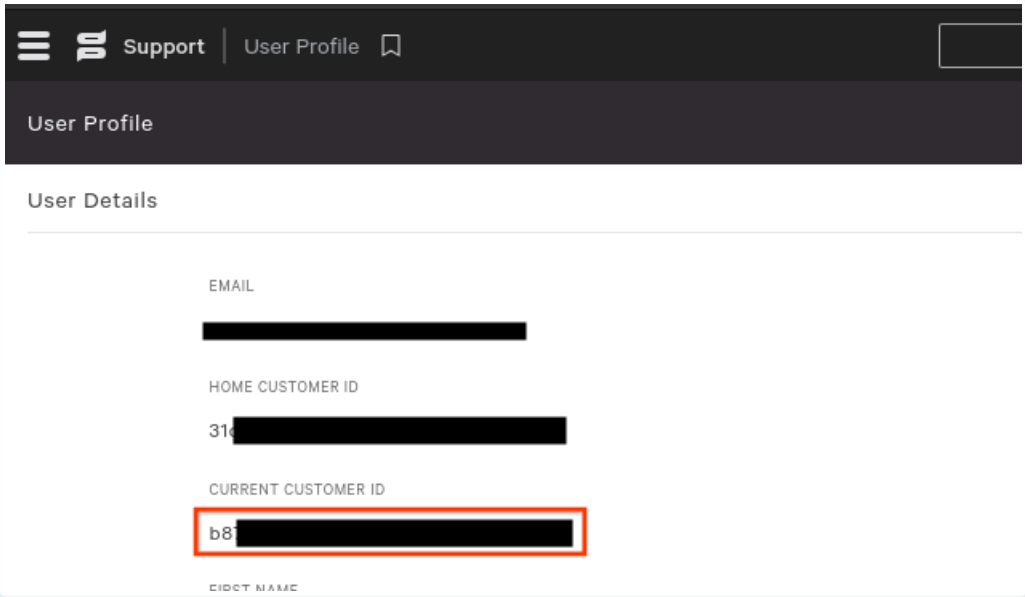

Copy the **Customer ID** and paste it somewhere that you can reference it.

This CID is also used in the next step when submitting the support ticket to CrowdStrike.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.




For child tenants, you are presented with a slightly different display. There are two IDs: **Home Customer ID** and **Current Customer ID**. If providing the CID for a child tenant, use the **Current Customer ID**.




## 3. Associate instance with Managed Defense

There are currently four CrowdStrike regions: *US-1*, *US-2*, *EU-1*, and *US-GOV-1*. The following table shows the Customer IDs (CIDs) for each of the regions for customer tenant association:

| Region | URL | API Base URL | Managed Service Tenant CID |
|---|---|---|---|
| US-1 | **https://falcon.crowdstrike.com** | api.crowdstrike.com | `818e18c4cf294fc4b52b481058bce27b` |

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

| Region | URL | API Base URL | Managed Service Tenant CID |
|---|---|---|---|
| US-2 | **https://falcon.us-2.crowdstrike.com** | api.us-2.crowdstrike.com | `31c035d79c1b477aada26cf91d02b09c` |
| EU-1 | **https://falcon.eu-1.crowdstrike.com** | api.eu-1.crowdstrike.com | `460a3fac505943c4b4ed584c4d85eb07` |
| US-GOV-1 | **https://falcon.laggar.gcw.crowdstrike.com/** | api.laggar.gcw.crowdstrike.com | `cc80ed46932148698bf1989f9a41b729` |

Use the *Tenant CID / Parent CID* for the region where the customer's CrowdStrike instance is deployed. Be sure to include the correct *Tenant CID / Parent CID* in the CrowdStrike customer support ticket.

## Falcon Complete Customers

As a Falcon Complete Customer, you do not use Falcon Flight Control and use an access method referred to as CID Switching in the CrowdStrike backend. In these situations, CrowdStrike Support must associate your CID with the Mandiant parent tenant and every individual user that needs to access the tenant.

### Child Tenant Association Steps

1. Use the **CrowdStrike Managed Service Provider Addendum Authorization Form (https://dyzz9obi78pm5.cloudfront.net/app/image/id/63d8b68183f44206ea1987c2/n/crowdstrike-managed-service-provider-addendum-authorization-form.docx)** to authorize Mandiant to access your CrowdStrike Falcon tenant.
2. Once you have completed the form, open a support ticket within the **CrowdStrike Support Portal (https://supportportal.crowdstrike.com/s/my-cases)** or by emailing **support@crowdstrike.com ()**. Mandiant can also open a support ticket on your behalf, but CrowdStrike Support will ask you to confirm with an approval via email (replying all to the support ticket).
   a. **Subject**: Associate *<Customer Name>* Tenant to Mandiant Parent.
   b. **Description**: Please allow Mandiant (**CID**: *<Mandiant Tenant CID / Parent CID>*) to have read-only access to *<Customer Tenant>*.
   c. **Product**: Provisioning
   d. **Component**: Add Access
   e. **Add Attachment**: Attach the completed consent form **CrowdStrike Managed Service Provider Addendum Authorization Form (https://dyzz9obi78pm5.cloudfront.net/app/image/id/63d8b68183f44206ea1987c2/n/crowdstrike-managed-service-provider-addendum-authorization-form.docx)**.

After you have sent the request to CrowdStrike support, Mandiant must submit a request to CrowdStrike support to allow all users in the tenant to have read-only access to your tenant account.

## Falcon Enterprise or Falcon Elite Customers

Your CrowdStrike Falcon tenant needs to be associated as a child tenant of the Mandiant CrowdStrike account so it is accessible through Falcon Flight Control. This step allows Mandiant to access your tenant account. This step is performed by CrowdStrike support with your authorization.

### Child Tenant Association Steps

1. Use the **CrowdStrike Managed Service Provider Addendum Authorization Form**

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

(https://dyzz9obi78pm5.cloudfront.net/app/image/id/63d8b68183f44206ea1987c2/n/crowdstrike-managed-service-provider-addendum-authorization-form.docx) to authorize Mandiant to access your CrowdStrike Falcon tenant.

2. Once you have completed the form, open a support ticket within the **CrowdStrike Support Portal** (https://supportportal.crowdstrike.com/s/my-cases) or by emailing **support@crowdstrike.com** (). Mandiant can also open a support ticket on your behalf, but CrowdStrike Support will ask you to confirm with an approval via email (replying all to the support ticket).

New Case

   a. **Subject**: Associate *<Customer Name>* Tenant to Mandiant Parent.
   b. **Description**: Please associate the *<Customer Tenant>* to have a *<primary | non-primary>* parent of Mandiant (**CID**: *<Mandiant Tenant CID / Parent CID>*). Please disable the feature flag for MSSP Policy Management for this tenant, as Mandiant will not be managing policy from the parent. The Splunk model for this relationship should be to have all events in both the parent and the child.

> **What is the difference between a primary and non-primary parent?**
>
> - CrowdStrike tenants can be associated with one or more parent tenants. Only the primary parent tenant can be used to push policies to child tenants. If a child tenant only has one parent, then that parent is the primary parent.
> - Mandiant does not offer policy management to CrowdStrike customers, so Mandiant does not need our tenant to be a primary parent tenant unless it is the only parent. If you have another MSSP or third-party that manages their CrowdStrike tenant, Mandiant should be a non-primary parent tenant. This will allow the other parent to continue managing your tenant's policies.

   c. **Product**: Provisioning
   d. **Component**: Add Access
   e. **Add Attachment**: Attach the completed consent form **CrowdStrike Managed Service Provider Addendum Authorization Form.docx** (https://dyzz9obi78pm5.cloudfront.net/app/image/id/63d8b68183f44206ea1987c2/n/crowdstrike-managed-service-provider-addendum-authorization-form.docx).

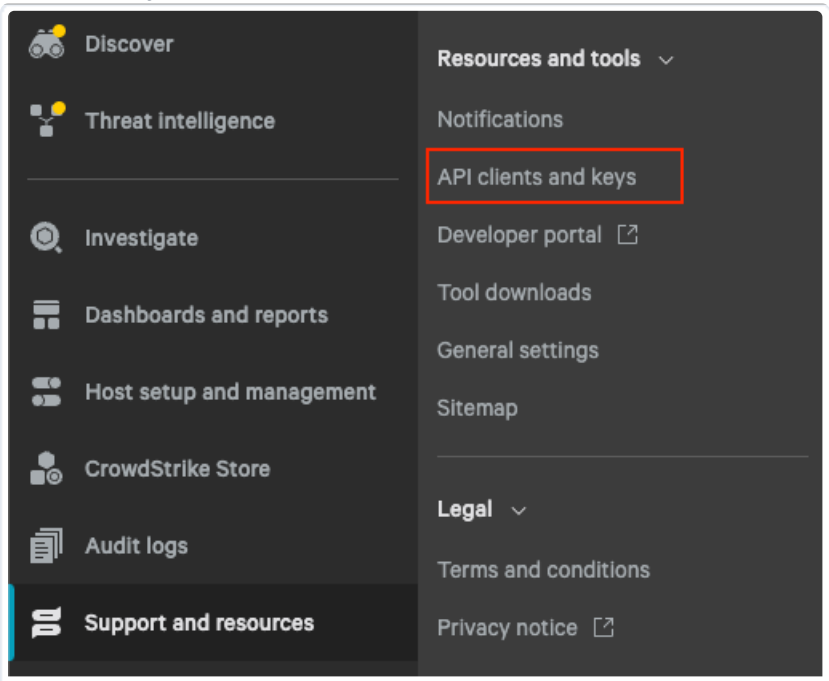
3. CrowdStrike will provision your tenant as a child tenant to Mandiant.
4. Confirm that you can log into your tenant account using your CrowdStrike account credentials once CrowdStrike has confirmed it is accessible to Mandiant.

## 4. Create an OAuth account

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

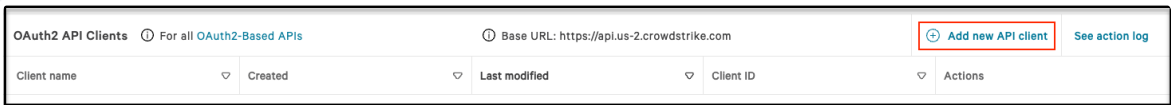
Mandiant requires an OAuth key with permissions that will specific actions to be performed in the customer's environment. The minimum required permission is to read alerts.

1. To access the options to generate OAuth tokens, navigate to the **Support and resources** menu and select **API clients and keys**:




API Clients and Keys

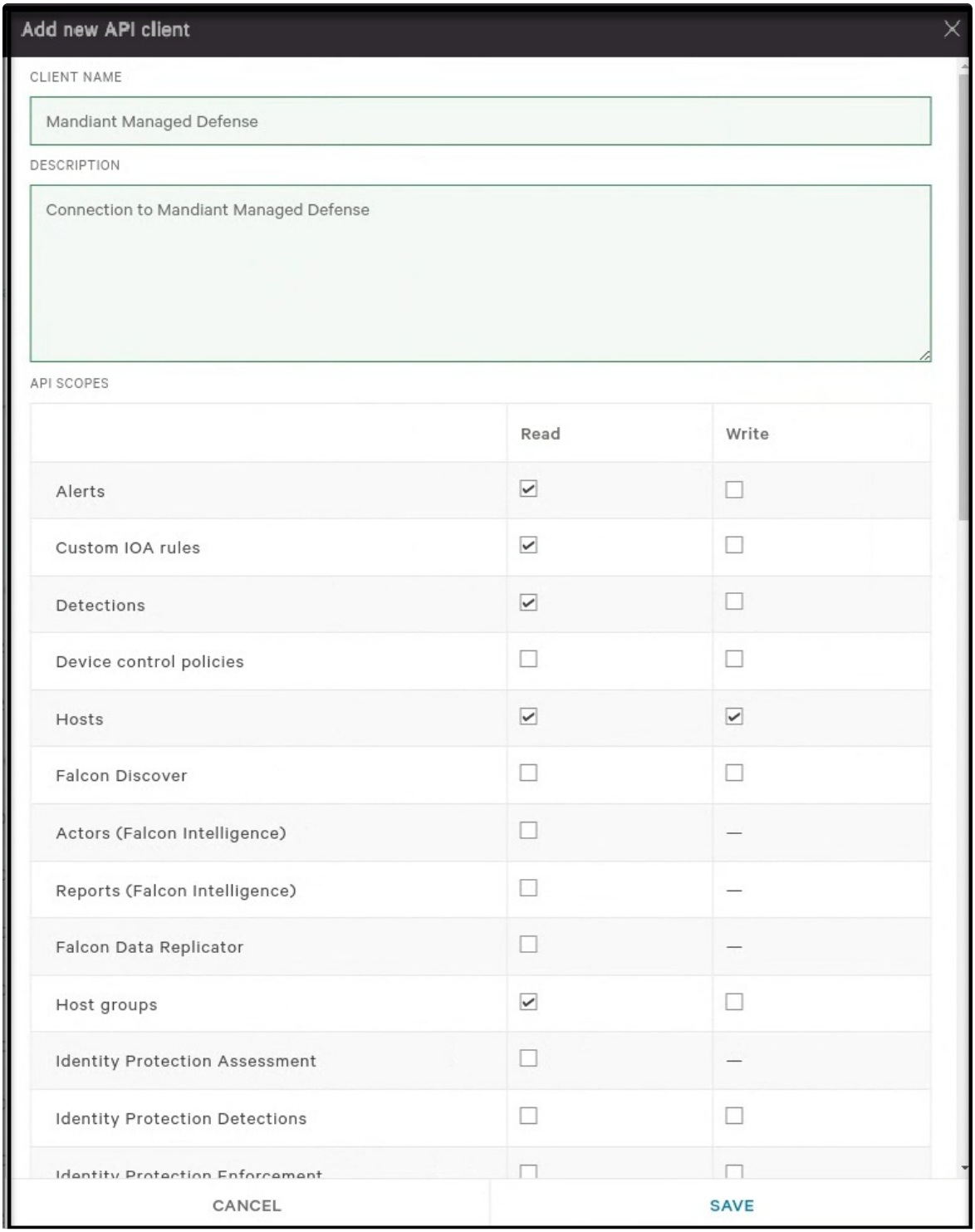
2. In the **OAuth2 API Clients** section, click **Add new API client**.




OAuth2 API Clients

3. In the **Add new API client** dialog that is displayed, assign permissions to the API client. Name the client *Mandiant Managed Defense* with a description of *Connection to Mandiant Managed Defense*:

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.




Add New API Client Screen

The following is a list of available permissions for the API Scope. Select all the options marked as *Required* and if necessary, the rows marked as *Optional* and then click the **SAVE** button at the bottom of the screen.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

| | Read | Write |
|---|---|---|
| **Alerts** | **Required** | Not Required |
| **Custom IOA rules** | **Required** | Not Required |
| **Detections** | **Required** | Not Required |
| Device control policies | Not Required | Not Required |
| **Hosts** | **Required** | **Optional**[2] |
| Falcon Discover | Optional | -- |
| Actors (Falcon X) | Not Required | -- |
| Reports (Falcon X) | Not Required | -- |
| **Host groups** | **Required** | Not Required |
| **Incidents** | **Required** | **Optional**[1] |
| Installation Tokens | Not Required | Not Required |
| IOC Manager APIs | Not Required | Not Required |
| Machine Learning Exclusions | Not Required | Not Required |
| Flight Control | Not Required | Not Required |
| Overwatch Dashboard | Not Required | -- |
| Prevention policies | Not Required | Not Required |
| **Quarantined files** | **Required** | Not Required |
| Real time response (admin) | -- | Not Required |
| **Real time response** | **Required** | **Required** |
| Response policies | Not Required | Not Required |
| Scheduled Reports | Not Required | -- |
| IOA Exclusions | Not Required | Not Required |
| Sensor Download | Not Required | -- |
| Sensor update policies | Not Required | Not Required |
| Sensor Visibility Exclusions | Not Required | Not Required |
| Spotlight vulnerabilities | Not Required | -- |
| **Event streams** | **Required** | -- |
| User management | Not Required | Not Required |

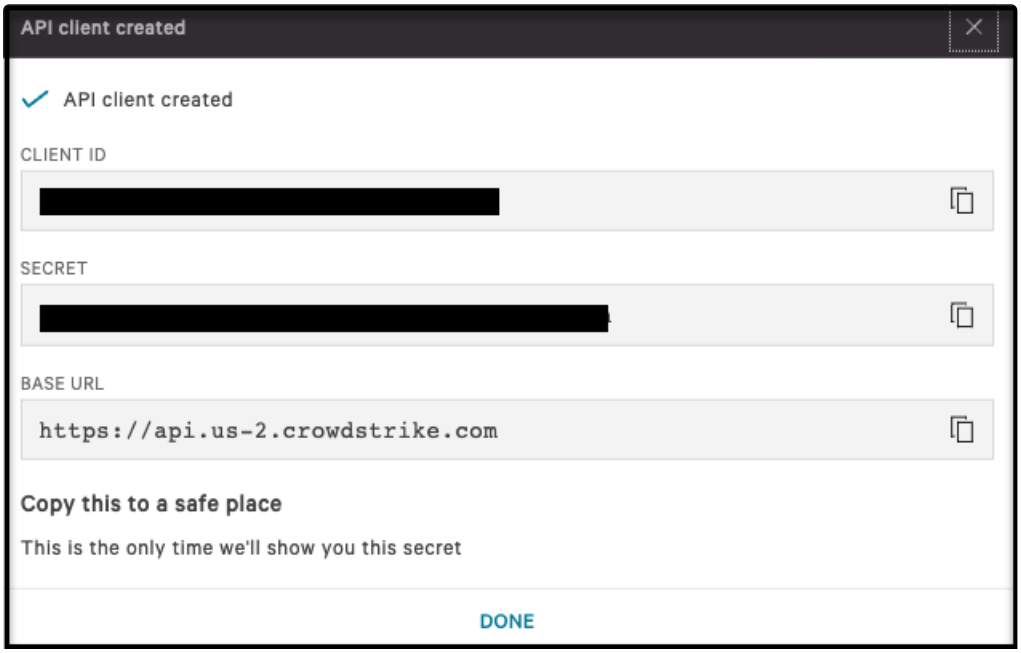
MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

| | Read | Write |
|---|---|---|
| Zero Trust Assessment | Not Required | -- |

**Optional Write:**

1. Required if the option to sync alert disposition and comments in the CrowdStrike Falcon Console is selected. This is a future feature for Managed Services.
2. Required if the customer wants to enable endpoint containment or deeper forensic analysis during rapid response.

After clicking **SAVE**, the **API client created** dialog is displayed. It contains the information required for the integration. Capture the required information (**Client ID**, **Secret**, and **Base URL**) somewhere that you can reference it.




API Client Created

### Disable API Allowlisting

If you have the **IP Allowlist** **(https://falcon.us-2.crowdstrike.com/documentation/46/crowdstrike-oauth2-based-apis#ip-allowlist)** restrictions enabled, the option must be disabled to allow Mandiant to access the tenant. The IP Allowlist functionality controls the IP addresses that are allowed to communicate with the tenant via the API. Mandiant does not have a static set of IP addresses that can be configured in an IP Allowlist.

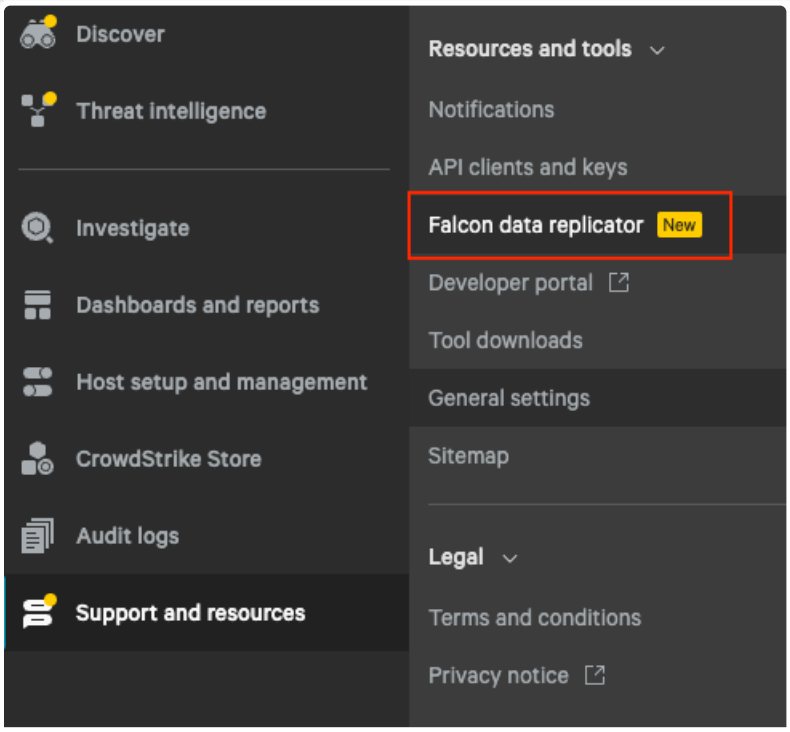
## 5. Configure CrowdStrike Falcon Data Replicator

Mandiant uses Falcon Data Replicator to send CrowdStrike Falcon telemetry data to the Managed Services backend to enable threat hunting and additional detection.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

> The CrowdStrike Falcon tenant requires a license to enable this feature. The Falcon data replicator menu will not be available if the tenant does not have this feature.

To configure Falcon Data Replicator, select **Falcon data replicator** from the **Support and resources** menu.




Falcon Data Replicator Menu

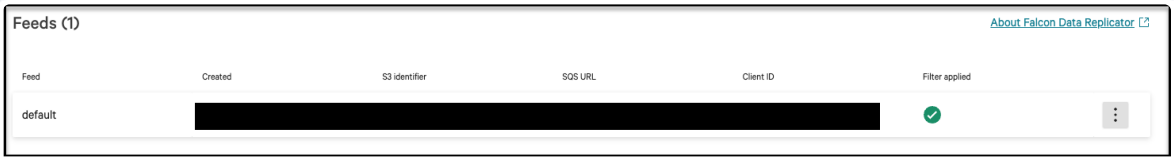
Mandiant can use either a new or existing Falcon Data Replicator feed.

## New Falcon Data Replicator Feed

1. Click the **Add** button to create a new Falcon Data Replicator feed. This will generate an **S3 identifier**, **SQS URL**, **Client ID**, and **Client secret**.

   > Note that the **Client secret** will be provided only once in a pop-up dialog after creating a new Falcon Data Replicator feed. Save it in a secured place.

2. Provide the generated **Feed**, **S3 identifier**, **SQS URL**, **Client ID**, and **Client secret** values to Mandiant.




Falcon Data Replicator Feeds

> CrowdStrike limits the number of Falcon data replicator feeds per tenant. Mandiant can share an existing Falcon data replicator feed with another customer consumer application if the feed does not have a filter that excludes the events required by Mandiant.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

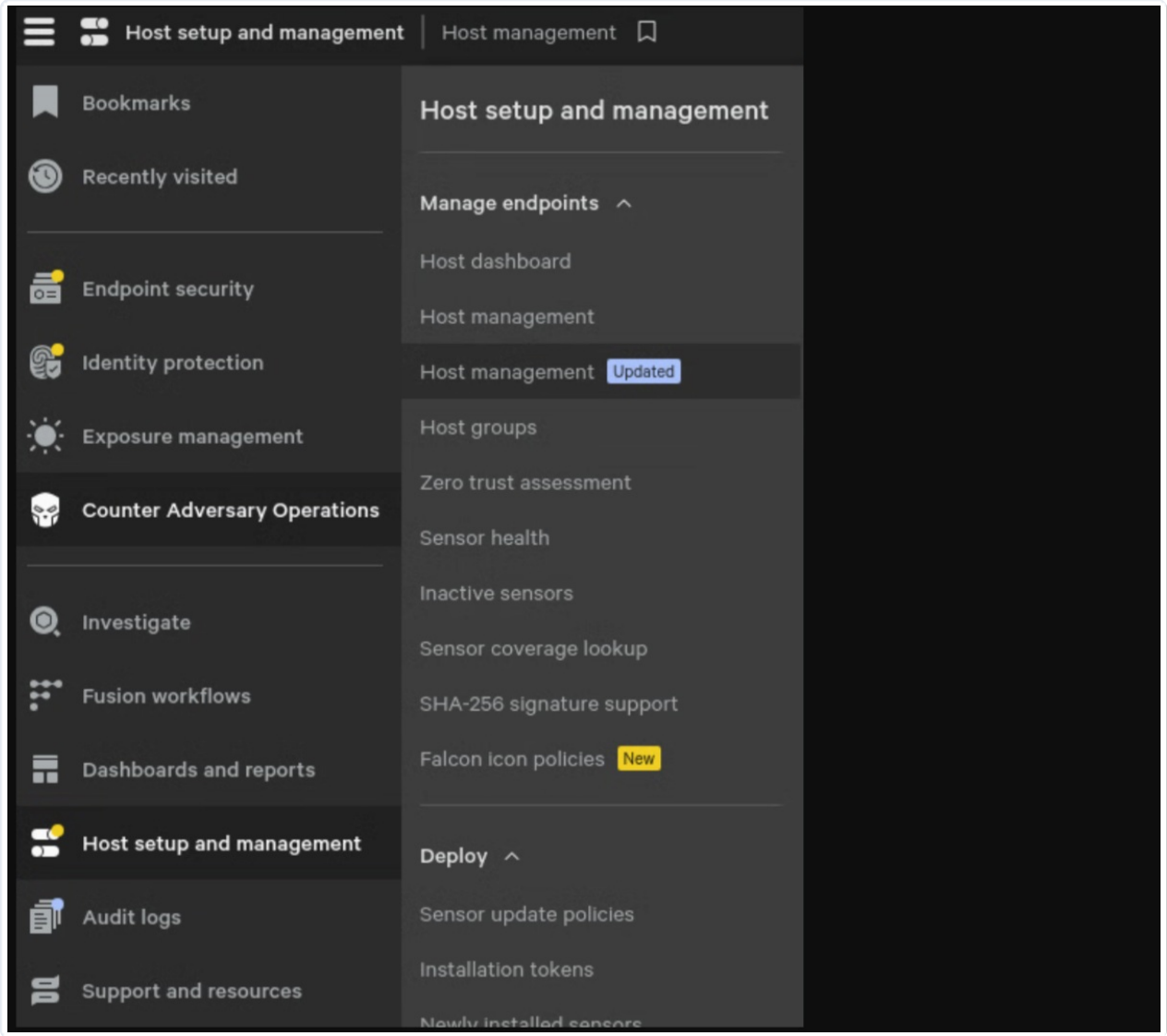
You can find additional details in the **CrowdStrike Falcon Data Replicator (https://falcon.us-2.crowdstrike.com/documentation/9/falcon-data-replicator)** documentation.

### Existing Falcon Data Replicator Feed

To use an existing Falcon Data Replicator feed, provide the **S3 identifier**, **SQS URL**, **Client ID**, and **Client secret** from the Falcon Data Replicator feeds list. Mandiant also requires the **Client secret** for the configured feed, which cannot be retrieved from the Falcon interface after the initial configuration of the feed.

## 6. Configure CrowdStrike Containment

To authorize endpoint containment, a CrowdStrike agent must be part of the `MD_Containment_Allowlist` **Falcon Grouping Tags**. You can add these tags from the **Host Management** interface in the Falcon Console.




Host Setup and Management

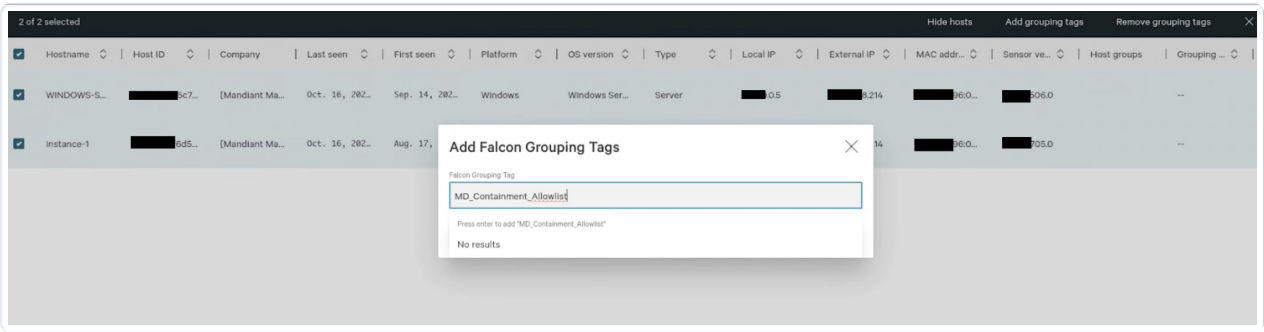
1. Select **Host Management** menu option in the Falcon Console.
2. On the Host Management screen, select all endpoints to include in the **Falcon Grouping Tags**.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

> The Falcon Console limits tagging to 1,000 endpoints at a time.

3. Use `MD_Containment_Allowlist` as the **Falcon Grouping Tag** name.
4. Click **Apply**.

Repeat this process for any endpoints that Mandiant is authorized to contain.




Add Falcon Grouping Tags

## 7. Connect Crowdstrike 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)**

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

1. Sign in to the MD Portal.
2. From **Settings**, click **Integrations**.
3. Click **Add new integration**.
4. From the menu, select **CrowdStrike Falcon** for the **Type**, and then click **Next**.
5. Fill out the input parameters with your CrowdStrike credentials:
   - **API Credentials (All Customers):** Enter your **Crowdstrike Integration ID** (formerly Tenant Customer ID), **OAuth Client ID**, **OAuth Client secret**, and **Base URL**.
   - **Aggregate Tenants:** If this is an aggregate parent tenant, select **Yes** for **Include Child Tenants**, and then input your child tenants as a comma-separated list.
   - **Event Telemetry (Private Customers Only):** Under the **Include Event Telemetry** section, select **Amazon SQS V2** as your **Source Type**. Enter your **Queue name**, **S3 URI**, **SQS queue access key ID** , and **SQS queue secret access key**.

     > 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 CrowdStrike data feeds within your SecOps instance.

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

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

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)**.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.