Cisco Stealthwatch

Cisco Threat Response Integration Guide 7.1.2

Table of Contents

Introduction

Cisco Threat Response (CTR) is the platform in the Cisco cloud that helps you detect, investigate, analyze, and respond to threats using data aggregated from multiple products and sources.

This integration allows you to use Cisco Threat Response Pivot menu, Cisco Threat Response Casebook in your SMC appliance UI, send Stealthwatch Alarms to Cisco Threat Response and allows CTR to retrieve information about security events from your Stealthwatch deployment during the investigation process.

For more information about Cisco Threat Response, see https://www.cisco.com/c/en/us/products/security/threat-response.html. For videos about the use and benefits of the application on YouTube, see http://cs.co/CTRvideos.

Cisco Threat Response Regional Clouds

Region	Link	Supported Stealthwatch Integrations
North America	https://visibility.amp.cisco.com	• Threat Response Pivot Menu • Threat Response Casebook • Sending Stealthwatch Alarms to CTR as Incidents • Enrichment with Stealthwatch Security Events
Europe	https://visibility.eu.amp.cisco.com	• Threat Response Pivot Menu • Threat Response Casebook • Sending Stealthwatch Alarms to CTR as Incidents • Enrichment with Stealthwatch Security Events
Asia (APJC)	https://visibility.apjc.amp.cisco.com	• Threat Response Pivot Menu

Region	Link	Supported Stealthwatch Integrations
		• Threat Response Casebook • Sending Stealthwatch Alarms to CTR as Incidents

Guidelines and Limitations for Choosing a Regional Cloud

- When possible, use the regional cloud nearest to your Stealthwatch deployment.
- Data in different clouds cannot be aggregated or merged.
- If you need to aggregate data from multiple regions, devices in all regions must send data to the same regional cloud.
- You can create an account on each regional cloud. Data on each cloud will be separate.

Contacting Support

If you need technical support, please do one of the following:

- Contact your local Cisco Partner
- Contact Cisco Stealthwatch Support
  - To open a case by web: http://www.cisco.com/c/en/us/support/index.html
  - To open a case by email: tac@cisco.com
  - For phone support: 1-800-553-2447 (U.S.)
  - For worldwide support numbers: www.cisco.com/en/US/partner/support/tsd_cisco_worldwide_contacts.html

Stealthwatch Data and Threat Response

About Sending Stealthwatch Alarms to Cisco Threat Response

When Cisco Threat Response Integration is configured, Stealthwatch will send active security alarms with Critical and Major severity to the Cisco Threat Response private intelligence store as Incidents with corresponding Sightings, Observables and Indicators objects created from the Alarm metadata.

This information will be available in the Incidents tab and during the investigation process as corresponding Sightings and Indicators derived from the Incident.

- Incidents created for Alarms derived from Relationship policy will not include IP addresses as observables as this information is not available in the Alarm.
- If you do not want Stealthwatch to send Alarms to Cisco Threat Response, do not select **Global Intelligence** and **Private Intelligence** scopes when creating the API Client in Cisco Threat Response.
- Please contact Technical Support if you want to change the minimal severity of the alarms to be sent to Cisco Threat Response.

About Stealthwatch Enrichment Data for Threat Response

Once your SMC is registered with the Cisco Security Services Exchange and the Stealthwatch module is configured in Cisco Threat Response, you will be able to see the enrichment data from Stealthwatch in the Threat Response Investigation workflow.

For every valid IP address requested in the investigation, Stealthwatch will return security events associated with this IP in the form of corresponding Sightings and Indicator objects, with the following limitations and rules:

- Security Events from *all* configured domains.
- Security Events for the last 15 days.
- Top 10 Security Events by points.
- Security Events where the IP was a subject for source or destination.

Please contact Technical Support if you want to change these settings, specifically if Enrichment requests from Stealthwatch Enterprise are failing on Cisco Threat Response with “Relay Module Timeout".

About the Cisco Threat Intel Model

Before sending to Cisco Threat Response, Stealthwatch alarms and security events are transformed to Cisco Threat Intel Model (CTIM) objects.

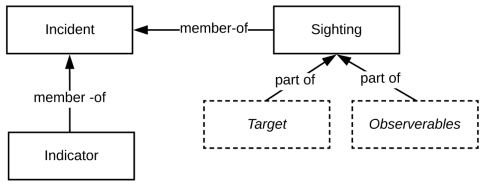
To read more about Cisco Threat Intel Model, refer to the Cisco Threat Intel Model documentation.

The key entities used in this translation are listed below:

- Incident – Discrete instance of indicators affecting an organization, as well as information associated with incident response.
- Sighting – A record of the appearance of a cyber observable at a given date and time.
- Observable – A simple, atomic value which has a consistent identity and is stable enough to be attributed an intent or nature: domain names, IP addresses, file hashes, specific devices or users. Stealthwatch shares information only about observables of IP address type.
- Target – The device, identity, or resource that a threat has targeted. Target is identified by one or more Observables.
- Indicator – Describes a pattern of behavior or a set of conditions which indicate malicious behavior.

About Translating Stealthwatch Alarms to CTIM Objects

Every critical and major alarm is translated to an Incident, a Sighting, an Indicator object, and the relationships between them. The picture below shows the representation of Stealthwatch alarm in CTIM model (simplified):



When building a Sighting object for the Incident, Stealthwatch includes Observables with the following constraints:

- Alarms derived from the Relationship Policy Event will not have Observables in the Sighting object.
- Alarms that have Source as “Multiple Source” or Target as “Multiple Destinations” will not include corresponding Observables in the Sighting object.

When building a Target object for the Sighting, the following constraints apply:

- Target object is included only for Alarms generated from the following types of core events:
    - beaconing-host
    - bot-infected-host
    - bot-infected-host-controlled
    - brute-force-login
    - fake-app-detect
    - half-open-attack
    - host-lock-violation
    - icmp-received
    - max-flows-served
    - new-flows-served
    - packet-flood
    - ping
    - port-scan
    - addr-scan-talking-detect
    - slow-connection-flood
    - ssh-rev-shell
    - suspect-long-flow
    - suspect-quiet-long-flow
    - suspect-udp-activity
    - syns-received
    - target-data-hoarding
    - touched
    - udp-received
    - watch-host-active
    - high-target-index
    - high-ddos-target-index
    - high-recon-index
    - attack-index

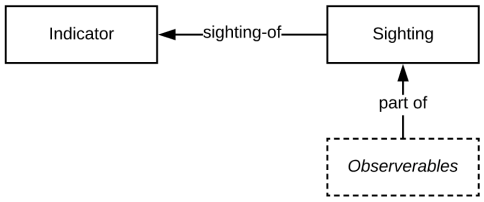
> For more information about Stealthwatch Security Events, refer to Stealthwatch Security Events and Alarm Categories.

- Target object is not included if alarm target is “Multiple Destinations”.
- Target object is not included if alarm target is an external IP address.

About Translating Stealthwatch Security Events to CTIM Objects

Upon an investigation request from Cisco Threat Response, Stealthwatch returns Security Events associated with an IP address.

Every Security Event is translated to the CTIM model Sighting and Indicator objects, with the relationships, as shown on the picture below:



When translating Stealthwatch Security Events to a CTIM object, the following constraints and rules apply:

- Target objects are not included in the Sighting objects for Security Events

Cisco Cloud Accounts

Required Account for Cisco Threat Response Access

In order to use Cisco Threat Response and associated tools, you must have one of the following accounts on the regional cloud you will use:

- Cisco Security Account
- AMP for Endpoints account
- Cisco Threat Grid account

Create an Account to Access Cisco Threat Response

> If you or your organization already has an account on the regional cloud you will use, use the existing account. Do not create a new account.

To create an account on a regional cloud, complete the following steps:

1. Determine which Cisco Threat Response cloud to use: Refer to the supported functionality and guidelines and limitations in Cisco Threat Response Regional Clouds section.
2. If you do not already have an account on the regional cloud you will use, ask your management if your organization already has a Cisco Security Account (CSA) set up in that cloud.
3. If anyone else in your organization already has a Cisco Security Account in that region:
    - Have the administrator of that account add an account for you using the Manage Access To Your Organization's Cisco Security Account instructions.
4. Otherwise, create a new Cisco Security Account for your organization (You will be its administrator):
    a. In your browser, go to your chosen regional cloud.
    b. For links, refer to the Cisco Threat Response Regional Clouds section.
    c. Click the link to create an account.
    d. Look for an email message to complete the registration.
5. On the Cisco Security Dashboard, launch Threat Response. On first log in you'll be asked to review and agree to the cloud subscription agreement. Once you accept the agreement, click **Launch**.

> To add users in your organization, click on **Users** at the top of the page.

6. If it's your first use of Cisco Threat Response, you'll be asked to connect your Stealthwatch device. To do this:
    a. Under **Connect a Device such as SMA Email or NGFW**, click **Connect**.
    b. Select **Register Device**. The Cisco Security Services Exchange portal will open in a new window. To register your SMC, refer to the Register your SMC in Cisco Cloud section. Start on step 2.
    c. Once registration is complete, in the Cisco Security Services Exchange portal, click **Confirm Device is Connected**.
7. Continue to the Configuring your Stealthwatch and Cisco Threat Response Integration section.

Manage Access To Your Organization's Cisco Security Account

If you are a Cisco Security Account owner or administrator, you can grant additional users access to your organization's Cisco Security Account and manage existing users, including resending the account activation email.

To manage users, complete the following steps:

1. In a browser window, go to your regional Cisco Security Account:
    - North America: https://castle.amp.cisco.com/my/users
    - Europe: https://castle.eu.amp.cisco.com/my/users
2. Click **Users**.
3. Add or edit user access. If you select Account Administrator, the user will have permissions to grant and manage user access.

Configuring Stealthwatch and Cisco Threat Response Integration

Configuring Cisco Threat Response Integration

Configuring the CTR Integration in Stealthwatch will enable:

- Cisco Threat Response Pivot menu in Stealthwatch UI.
- Cisco Threat Response Casebook in Stealthwatch UI.
- Sending Stealthwatch Alarms to Cisco Threat Response.

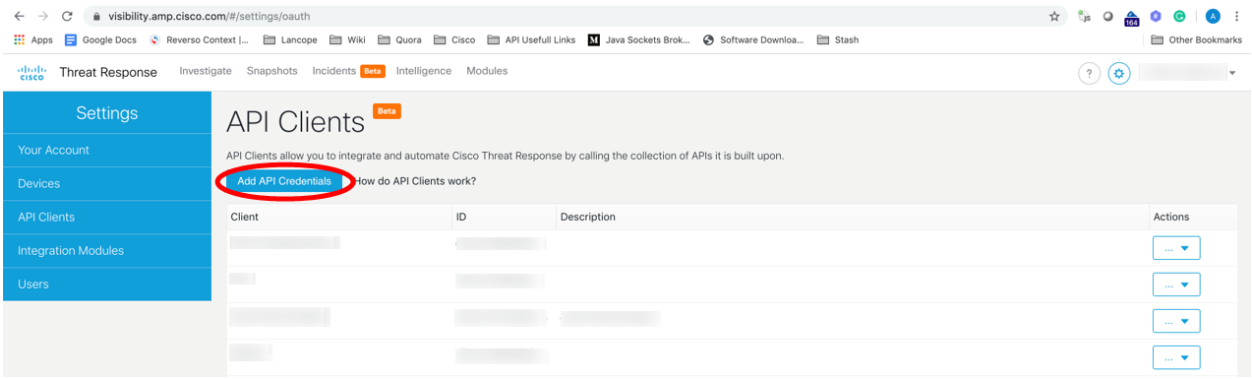
Prerequisites

- SMC v7.1.2 or later
- You have an account to access CTR (see Required Account for Cisco Threat Response Access).
- Your SMC must be able to connect outbound to the Cisco clouds:
  - North America clouds:
    - api-sse.cisco.com, port 443
    - visibility.amp.cisco.com, port 443
  - EU clouds:
    - api.eu.sse.itd.cisco.com, port 443
    - visibility.eu.amp.cisco.com, port 443
- Your Stealthwatch deployment is generating security events and Alarms as expected.

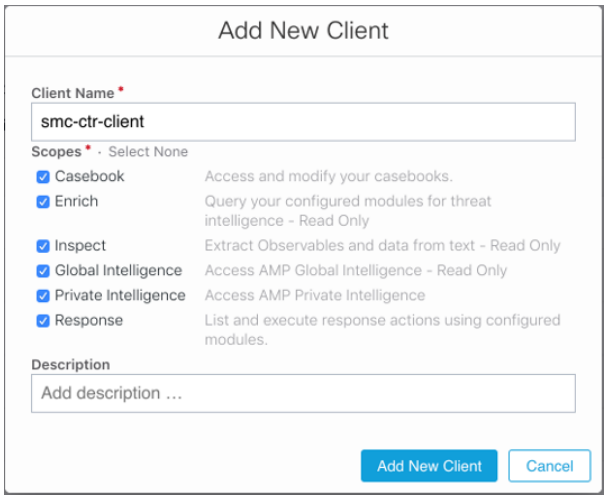
Procedure

To configure the CTR Integration, complete the following steps:

1. Go to your regional Cisco Threat Response cloud:
   - North America cloud: https://visibility.amp.cisco.com
   - Europe cloud: https://visibility.eu.amp.cisco.com
2. Sign in using the credentials for your AMP for Endpoints, Cisco Threat Grid, or Cisco Security account.
3. Go to **Settings > API Clients**.
4. Click **Add API Credentials**.

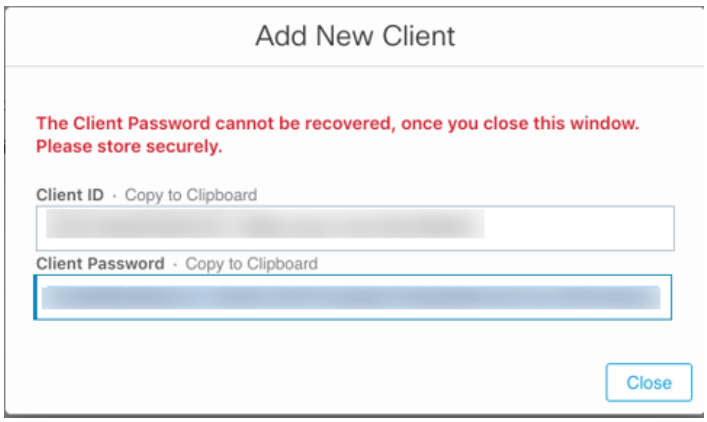


5. In the opened dialog fill in the name and description for the API Client and select all scopes then click **Add New Client**.



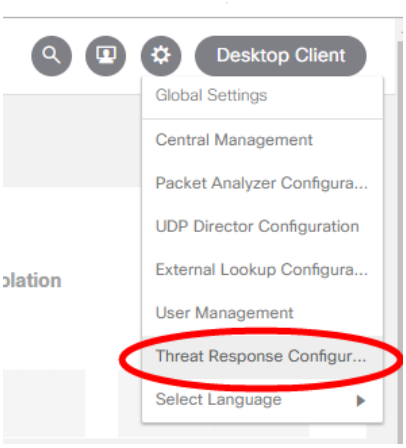
If you do not want Stealthwatch to send Alarms to Cisco Threat Response, do not select **Global Intelligence** and **Private Intelligence** scopes.

6. The system will create a Client ID and Client Password for you.

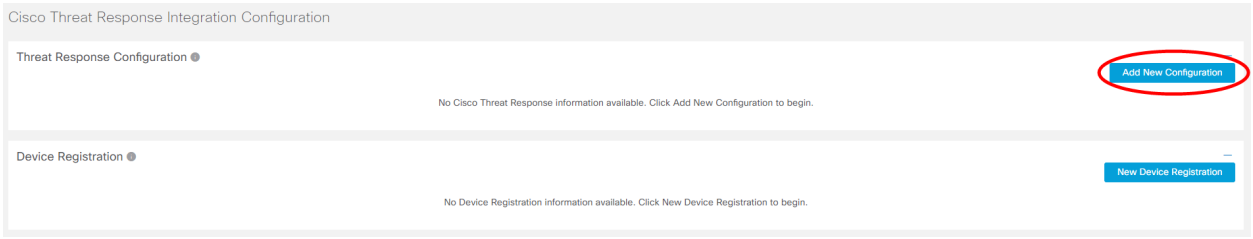


> The Client Password cannot be recovered once you close this window.

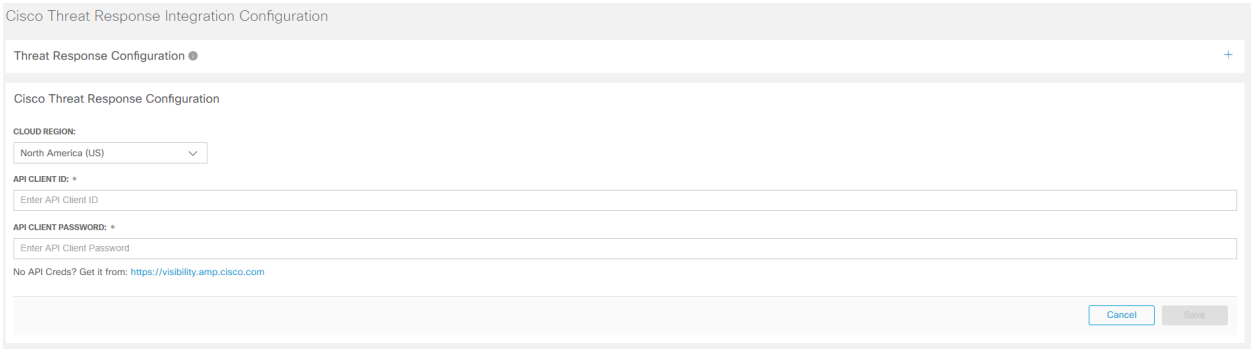
7. Log in to your SMC as Master Admin or Configuration manager.
8. From the navigation menu, click the Global Settings icon and select **Threat Response Configuration**.



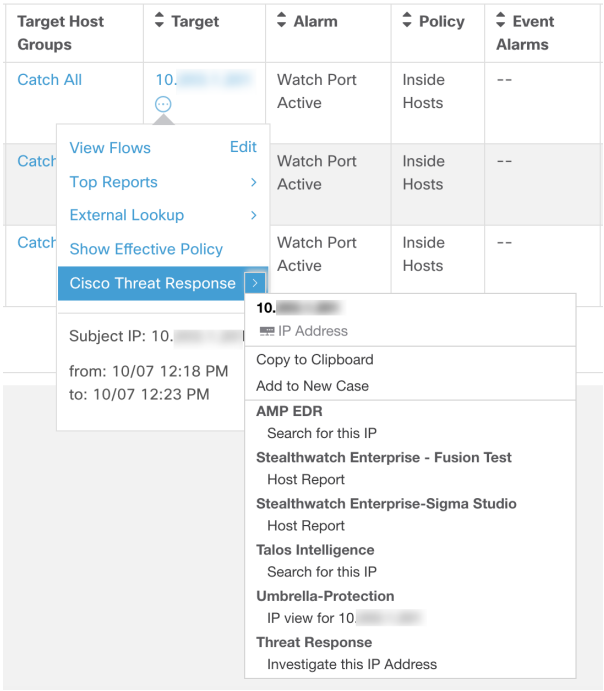
9. In the Threat Response Configuration section, click **Add New Configuration**.



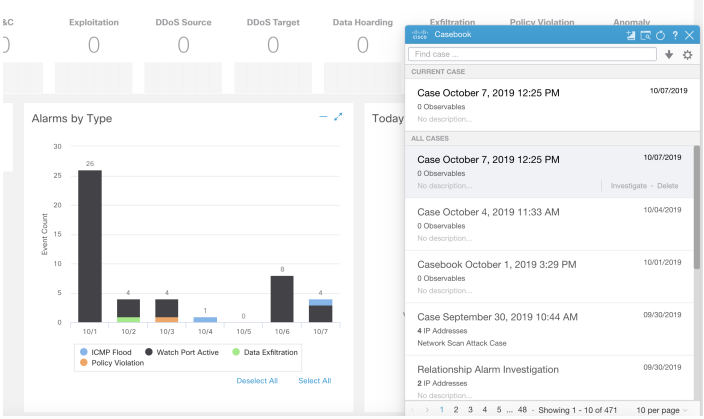
10. In the opened form, select the regional cloud used to create the API Client and paste the Client ID and Client Password from Step 6. Then click **Save**.



11. System will validate and store the API credentials.
12. Verify that your SMC has the Threat Response Pivot Menu and Casebook available.
    - For Threat Response Pivot Menu:
        - Open any page in the SMC that contains a relevant IP address.
        - Click the ellipsis ( ) beside the applicable IP address.
        - In the pop-up menu that appears, click the arrow next to Cisco Threat Response. A secondary pop-up menu appears with menu content.



    - For Threat Response Casebook:
        - Navigate to any page in your SMC. Notice a Threat Response Casebook Icon ( ) in the right bottom corner of the page.
        - Click on the icon to expand the widget.



13. Verify your Stealthwatch alarm in CTR:
    a. Wait until Stealthwatch detects Critical or Major Security Alarm or generate a test security alarm.
    b. Log in to your regional Cisco Threat Response cloud.
    c. Navigate to Incidents tab from Threat Response menu.
    d. Your Alarm should be available in the list.

Additional Information

For additional information about the integration, refer to the following links:

- About Cisco Threat Response Pivot menu
- About Cisco Threat Response Casebook

> You have to log in to Cisco Threat Response to view the Pivot menu and Casebook help.

- About Sending Stealthwatch Alarms to Cisco Threat Response

Register your SMC in the Cisco Cloud

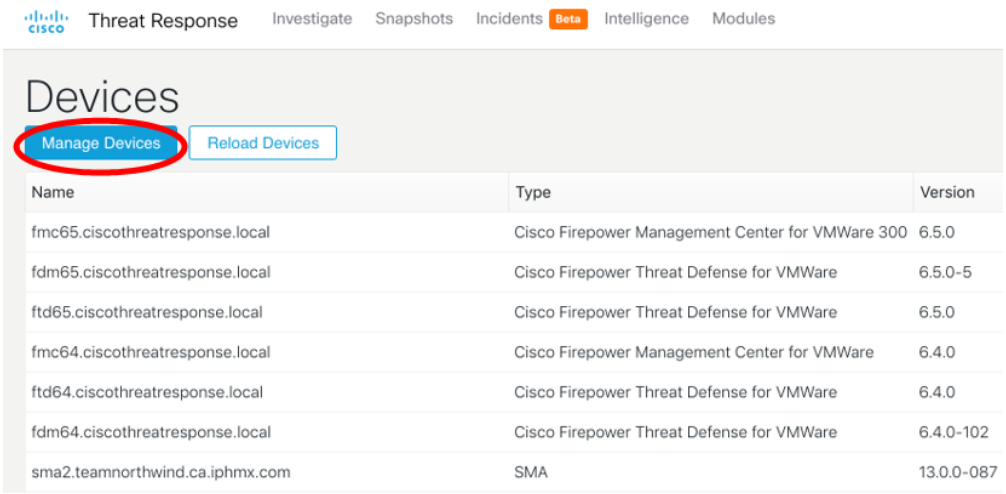
Registering your SMC in Cisco Security Exchange Cloud will allow Threat Response to retrieve enrichment data such as Security Events from your SMC to be included in the investigation workflows.

For more details, refer to the About Stealthwatch Enrichment Data for Threat Response section.

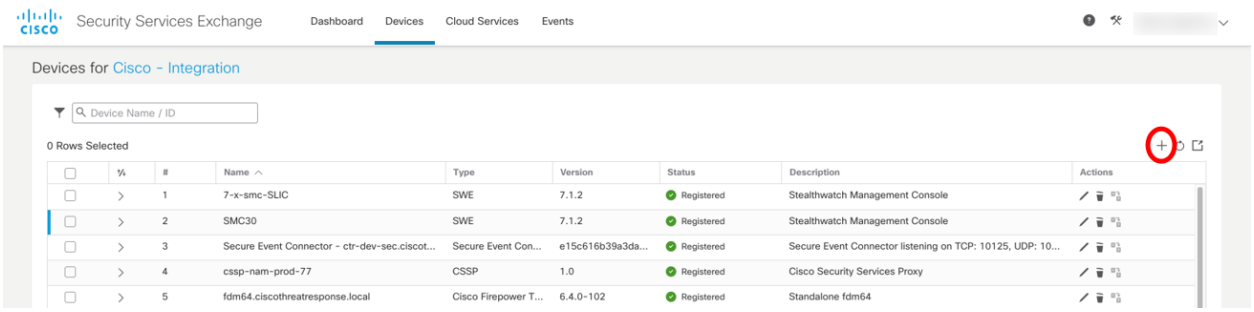
Procedure

To register your SMC in Cisco Secured Exchange Cloud, complete the following steps:

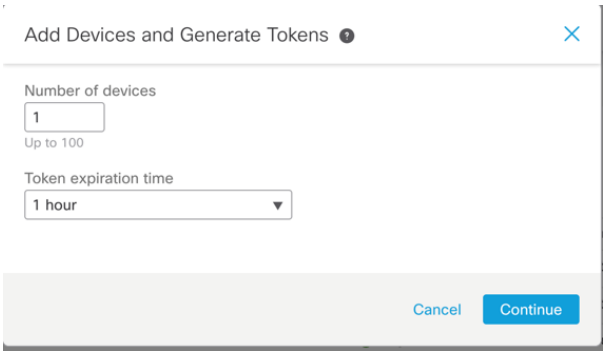
1. Go to your regional Cisco Threat Response cloud and log in using the credentials for your AMP for Endpoints, Cisco Threat Grid, or Cisco Security account.
2. Navigate to **Module > Devices** and click **Manage Devices**. The Cisco Security Services Exchange portal opens.



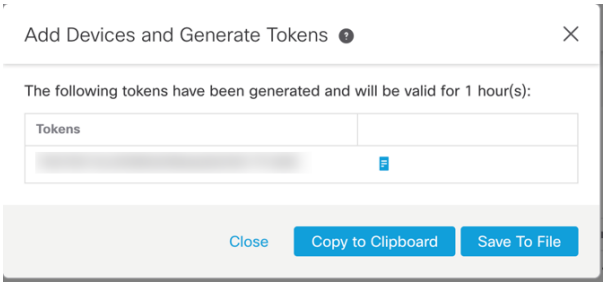
3. In your Cisco Security Services Exchange portal, enable **Cisco Threat Response** in Cloud Services Menu.
4. Click the **Add Devices and Generate Tokens plus icon** located on the right of the page, above the table with your devices.



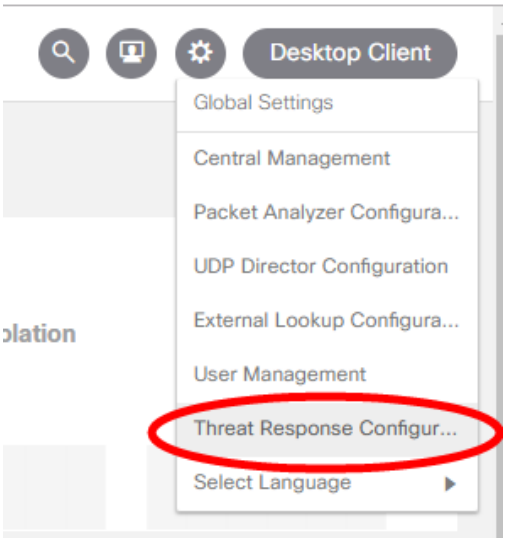
5. In the opened dialog, click **Continue** and let system generate a token for your device.



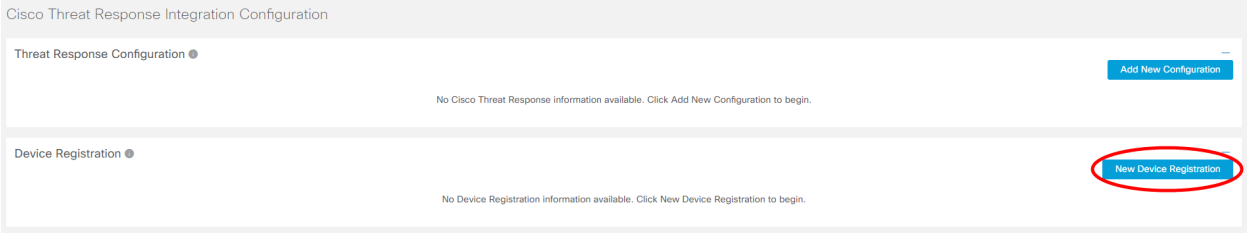
6. Copy the generated token into the memory buffer or save the generated token into the file.



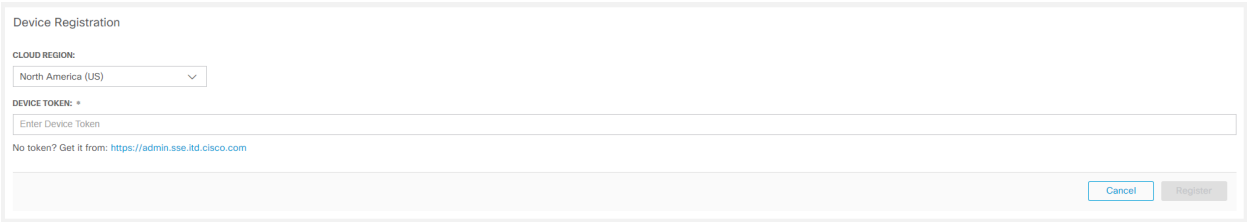
7. Log in to your SMC as Master Admin or Configuration manager.
8. From the navigation menu, click the Global Settings icon and select **Threat Response Configuration**.



9. In the Device Registration section, click **New Device Registration**.



10. In the opened dialog, select the Cloud Region that matches your Cisco Threat Response regional cloud and insert the Security Services Exchange token generated and saved in step 5. Click **Register**.



11. The device will be registered in Cisco Security Services Exchange and the status will show as **Enrolled**.
12. Verify the status of the device in the Cisco Security Services Exchange portal. The status of the device should show as **Registered**.

Configuring Stealthwatch Integration Module in Cisco Threat Response

For Threat Response to retrieve enrichment data from Stealthwatch the integration module must be configured.

Prerequisites

- Your SMC is registered in the Cisco Security Services Exchange cloud.
- Cisco Threat Response is enabled in Cisco Security Services Exchange portal Cloud Services.

  Refer to the Register your SMC in the Cisco Cloud section for more details.

Procedure

To configure the Stealthwatch module in Cisco Threat Response, complete the following steps:

1. Go to your regional Cisco Threat Response cloud and log in using the credentials for your AMP for Endpoints, Cisco Threat Grid, or Cisco Security account.
2. Click **Modules** in the navigation pane and then click **Add New Module** in the *Your Configurations* area on the *Modules* page.

   Alternatively, you can expand **Modules** in the navigation pane and click **Available Modules**.
3. On the *Available Modules* page, click **Add New Module** in the Stealthwatch Enterprise module pane.
4. In the opened dialog:
   a. Name your module.
   b. In the Registered Device drop down, locate your SMC.
   c. Click **Save**.
5. Verify that Cisco Threat Response can retrieve enrichment data from your SMC. To do this:
   a. Review your SMC Security Dashboards and notice an IP that generates security events.
   b. Enter this IP into the Investigation search panel in Cisco Threat Response.
   c. The graph should show you other hosts involved in Security Events with the requested host.
   d. The Sightings will represent the security events associated with the requested host.

Access Security Services Exchange

Before you begin

- In your browser, disable pop-up blocking.

Procedure

1. In a browser window, go to your regional Cisco Threat Response cloud:
   - North America cloud: https://visibility.amp.cisco.com
   - Europe cloud: https://visibility.eu.amp.cisco.com
2. Sign in using the credentials for your AMP for Endpoints, Cisco Threat Grid, or Cisco Security account. Your account credentials are specific to the regional cloud you sign in to.

3. Navigate to Security Services Exchange: Click **Settings > Devices > Manage Devices**. The Security Services Exchange will open in a new browser window.

Known Issues and Limitations

- Failover is not supported for the CTR integration in v7.1.2. The configuration needs to be repeated for the secondary SMC for the integration to work.
- Backup and Restore is not supported for Device Registration in the Cisco Security Services Exchange Cloud portal. The Device Registration panel in the Cisco Threat Response configuration on your SMC shows the actual status of the device registration in the cloud. Therefore, restoring configuration from the backup for the device registration is not available. If deleted after the backup, the registration will have to be re-done again after restore.

Copyright Information