



Cisco Secure Network Analytics

Cisco SecureX Integration Guide 7.5.0



Table of Contents

Introduction	4
What's New	4
Upgrading from 7.4 to 7.5	4
SecureX Regional Clouds	5
Guidelines and Limitations for Choosing a Regional Cloud	6
Secure Network Analytics Data and SecureX	7
About the SecureX Ribbon and Menu	7
SecureX Ribbon	7
SecureX Menu	7
About Secure Network Analytics Tiles for the SecureX dashboard	8
About Sending Secure Network Analytics Alarms to Cisco SecureX Threat Response	10
About Secure Network Analytics Enrichment Data for SecureX	11
About the Cisco Threat Intel Model	11
About Translating Secure Network Analytics Alarms to CTIM Objects	12
About Translating Secure Network Analytics Security Events to CTIM Objects	13
Cisco Cloud Accounts	14
Required Account for SecureX Access	14
Create an Account to Access SecureX	14
Manage Access To Your Organization's Cisco Security Account	14
Configuring Secure Network Analytics and SecureX	15
Configuring the SecureX Integration	15
Prerequisites	15
Procedure	16
Authorize the SecureX Ribbon and Menu	19
Authorize from SecureX Ribbon	19
Authorize from the SecureX Configuration Page	20
Unauthorize the Current SecureX Ribbon	20
Configure the Threat Response Incident Action	20

Verification	21
Register your Manager in the Cisco Cloud	22
Automatic Registration Procedure	23
Link your Accounts	24
Manual Registration Procedure	24
Configuring Secure Network Analytics Integration Module in SecureX	26
Prerequisites	26
Procedure	26
Configuring the SecureX dashboard with Secure Network Analytics Tiles	28
Known Issues and Limitations	31
Contacting Support	32
Change History	33

Introduction

Cisco SecureX 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 enables you to do the following in Secure Network Analytics (formerly Stealthwatch):

- Use Secure Network Analytics (shown as Stealthwatch) tiles on the SecureX dashboard to monitor key operational metrics.
- Utilize the SecureX menu to pivot to your other Cisco Security and third-party integrations.
- Provide access to your SecureX ribbon.
- Send Secure Network Analytics Alarms to the Cisco SecureX threat response (formerly Cisco Threat Response) Private Intelligence Store.
- Allow SecureX to request Security Events from Secure Network Analytics to enrich the investigation context in threat response workflows.

To learn more about SecureX, go to the following links:

- [SecureX website](#)
- [SecureX documentation](#)

What's New

In v7.4.0 we rebranded our Cisco Stealthwatch Enterprise products to Cisco Secure Network Analytics. For a complete list, refer to the [Release Notes](#). In this guide, you will see our former product name, Stealthwatch, used whenever necessary to maintain clarity, as well as terminology such as Stealthwatch Management Console and SMC.

Please note that Secure Network Analytics is currently shown as Stealthwatch Enterprise in SecureX.

Upgrading from 7.4 to 7.5

If your SecureX configuration in 7.4 had the option to send Secure Network Analytics alarms to Cisco SecureX threat response enabled, the Threat Response Incident action will be automatically configured to continue sending alarms.

SecureX Regional Clouds

Region	Link	Supported Secure Network Analytics Integrations
North America	<ul style="list-style-type: none"> • Threat Response Web Console: https://visibility.amp.cisco.com • SecureX Portal: https://securex.us.security.cisco.com 	<ul style="list-style-type: none"> • SecureX Menu • SecureX Ribbon • Sending Secure Network Analytics Alarms to Cisco SecureX threat response • Enrichment with Secure Network Analytics Security Events
Europe	<ul style="list-style-type: none"> • Threat Response Web Console: https://visibility.eu.amp.cisco.com • SecureX Portal: https://securex.eu.security.cisco.com 	<ul style="list-style-type: none"> • SecureX Menu • SecureX Ribbon • Sending Secure Network Analytics Alarms to Cisco SecureX threat response • Enrichment with Secure Network Analytics Security Events
Asia (APJC)	<ul style="list-style-type: none"> • Threat Response Web Console: https://visibility.apjc.amp.cisco.com • SecureX Portal: https://securex.apjc.security.cisco.com 	<ul style="list-style-type: none"> • SecureX Menu • SecureX Ribbon • Sending Secure Network Analytics Alarms to Cisco SecureX threat response

Guidelines and Limitations for Choosing a Regional Cloud

- When possible, use the regional cloud nearest to your Secure Network Analytics 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.

Secure Network Analytics Data and SecureX

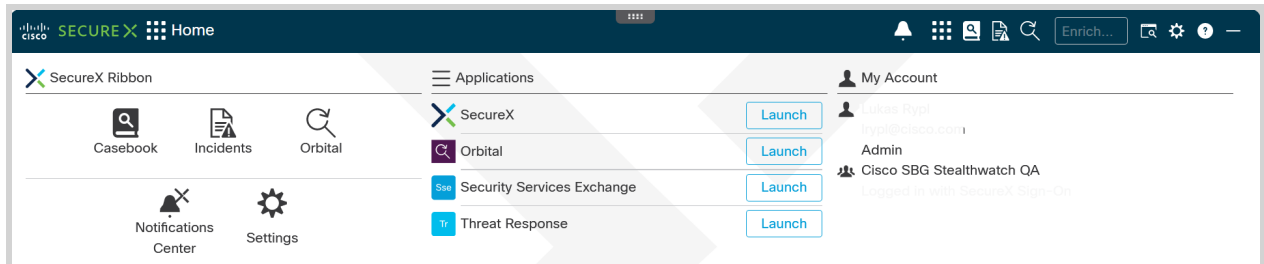
About the SecureX Ribbon and Menu

SecureX Ribbon

The SecureX ribbon is a widget that appears in your Cisco Secure Network Analytics Manager (formerly Stealthwatch Management Console) UI at the bottom of the page. The ribbon provides a distributed set of capabilities that unify visibility, enable automation, accelerate incident response workflows, and improve threat hunting. These capabilities are presented in the form of applications (apps) and tools in the ribbon.

With the ribbon configured, you can manage your incidents, casebooks, search for observables, initiate investigation and threat hunting, access your other products integrated with SecureX, and more from any page in your Manager.

To configure the ribbon, refer to the [Authorize the SecureX ribbon and Menu](#) section.



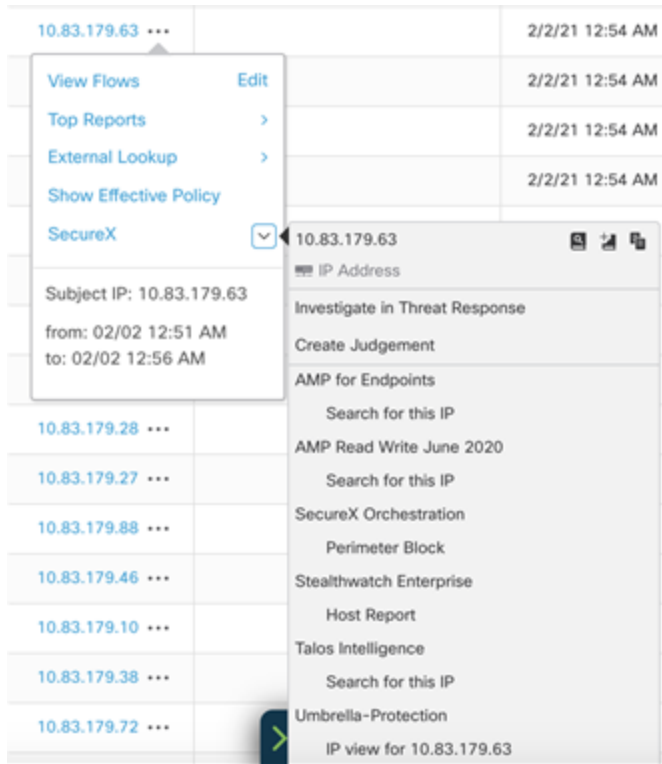
For more information about the ribbon, refer to the [Cisco SecureX Ribbon](#) section of the [Cisco SecureX Getting Started Guide](#).

SecureX Menu

The SecureX provides a central point of access that allows you to leverage Cisco threat intelligence resources with data from other Cisco products.

The menu links to other products and groups that are integrated with SecureX. You can perform some actions directly in the menu, or pivot to the integrated product to perform additional actions.

In Secure Network Analytics, the menu is available by clicking the **⋮ (Ellipsis)** icon beside applicable IP addresses in the Manager after the SecureX integration is configured.



For more information about functions available from the menu, refer to the [SecureX menu](#) help topic.

i You have to log in to SecureX to view the menu help.

About Secure Network Analytics Tiles for the SecureX dashboard

The following Secure Network Analytics (shown as Stealthwatch) tiles are available for the SecureX dashboard:

Tile Name	Description	Available Time Period	Pivots to...
Top Alarming Hosts	Provides Top 7 inside hosts, sorted by alarm severity, that have been active on your network since the last reset hour.	Last 24 hours	Host Report

Tile Name	Description	Available Time Period	Pivots to...
Alarming Hosts by Category	Top 7 inside hosts, sorted by alarm severity, that have been active on your network since the last reset hour.	Last 24 hours	Network Security dashboard
Top Alarms By Count	Represents Top 10 alarms by count.	Last 24 hours Last 7 days	Network Security dashboard
Visibility Assessment	Number of hosts in the Visibility Assessment Categories including Internal Network Scanners, Remote Access Breach, Possible Malware, Vulnerable Protocol Servers, DNS Risk.	Last 24 hours Last 7 days	Visibility Assessment dashboard
Network Visibility	Provides statistics for the number of hosts and the amount of traffic.	Last 24 hours Last 7 days	Visibility Assessment dashboard
Top Inside Host Groups by Traffic	Top 10 Inside host groups by traffic communicated with each other.	Last 12 hours	Host Group Report for Inside Host Group
Top Outside Host Groups by Traffic	Top 10 Outside host groups by traffic communicated with Inside Hosts Group.	Last 12 hours	Host Group Report for Inside Host Group

To learn how to configure your SecureX dashboard with Secure Network Analytics (shown as Stealthwatch) tiles, refer to the [Configuring the SecureX dashboard with Secure Network Analytics Tiles](#) section.

About Sending Secure Network Analytics Alarms to Cisco SecureX Threat Response

When the SecureX integration is configured, you can enable your system to promote Secure Network Analytics alarms to the Cisco SecureX threat response Private Intelligence store as Incidents with corresponding Sightings, Observables and Indicators objects created from the alarms metadata.

This information will be available in the Incident Manager during the investigation process as corresponding Sightings and Indicators derived from the Incident, and in the threat response web console.

The Threat Response Incident action in Response Management, besides general action parameters, allows you to configure the following options:

- **Incident Confidence Level:** Allows you to choose the confidence level that you want to set for the Incidents sent to Cisco SecureX threat response.
- **Create a new Target entity:** Allows you to enable Secure Network Analytics to designate hosts from the Alarm as Targets in Cisco SecureX threat response. For more information, refer to the [About Translating Secure Network Analytics Alarms to CTIM Objects](#) section.
 - If you want only internal IP addresses to be included when determining which host information should be sent to Cisco SecureX threat response, select the **Create Targets in Threat Response for internal hosts only** option.
 - If you want both internal and external IP addresses to be included when determining which host information should be sent to Cisco SecureX threat response, select the **Create Targets in Threat Response for internal and external hosts** option.
- **Use host details from the alarm data:** Allows you to specify whether the Target object should be built for Source and Target host, just the Source host, or just the Target host.

For more information, refer to the *Configuring Response Management* help topic (**Configure > DETECTION Response Management**. Click the  **(Help)** icon).



- If you configured sending Secure Network Analytics Alarms to Cisco

SecureX threat response in previous Secure Network Analytics (formerly Stealthwatch) versions, the Threat Response Incident action will be automatically created.

- Incidents created for Alarms derived from Relationship policy will not include IP addresses as observables as this information is not available in the Alarm.
- Incident will include the Target object in certain conditions specified in the [About Translating Secure Network Analytics Alarms to CTIM Objects](#) section.
- Incidents created from Secure Network Analytics Alarms can be viewed from the CTR console located with regional clouds. For more information, refer to the [SecureX Regional Clouds](#) section.

About Secure Network Analytics Enrichment Data for SecureX

Once your Manager is registered with the Cisco Security Services Exchange and the Secure Network Analytics module is configured in SecureX, you will be able to see the enrichment data from Secure Network Analytics in the threat response workflow.

For every valid IP address requested in the investigation, Secure Network Analytics will return Security Events associated with this IP in the form of corresponding Sightings and Indicator objects.

You can configure the following parameters for the security events returned in the SecureX Configuration form:

- Whether to allow investigation requests from SecureX.
- Which Secure Network Analytics domains to return Security Events.
- Number of top events to be sent.
- What time period to return Security Events.

About the Cisco Threat Intel Model

Before sending to SecureX, Secure Network Analytics alarms and security events are transformed to Cisco Threat Intel Model (CTIM) objects.

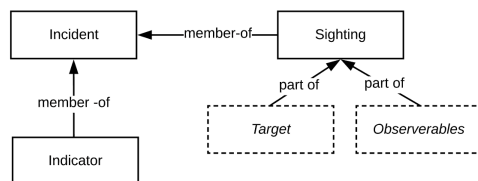
To read more about CTIM, refer to the [Threat Intel Model](#) documentation.

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. Secure Network Analytics 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 Secure Network Analytics Alarms to CTIM Objects

Every alarm sent with the Threat Response Incident action is translated to an Incident, a Sighting, an Indicator object, and the relationships between them. The picture below shows the representation of Secure Network Analytics alarm in CTIM model (simplified):



When building a Sighting object for the Incident, Secure Network Analytics 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.

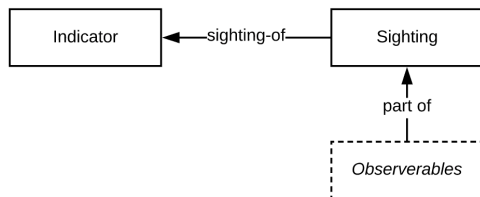
Rules for building a Target object for the Sighting are taken from the Threat Response Incident action that process the alarm with the following additional constraint:

- Target object is not included if alarm source or destination is “Multiple Destinations.”

About Translating Secure Network Analytics Security Events to CTIM Objects

Upon an investigation request from SecureX, Secure Network Analytics 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 Secure Network Analytics 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 SecureX Access

In order to use SecureX 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

For more information, refer to the [SecureX Sign-On Guide](#).



If you or your organization already has any of the above accounts on the regional cloud, you will use the existing account. Do not create a new account.

Create an Account to Access SecureX

Refer to the [SecureX Sign-On Guide](#) for more information on creating your account.

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>
 - Europe: <https://castle.eu.amp.cisco.com>
 - Asia (APJC): <https://castle.apjc.amp.cisco.com>
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 Secure Network Analytics and SecureX

Configuring the SecureX Integration

Configuring the SecureX integration in Secure Network Analytics will enable:

- SecureX Menu in Secure Network Analytics UI.
- SecureX Ribbon in Secure Network Analytics UI.
- Sending Secure Network Analytics Alarms to the Cisco SecureX threat response Private Intelligence Store.

Prerequisites

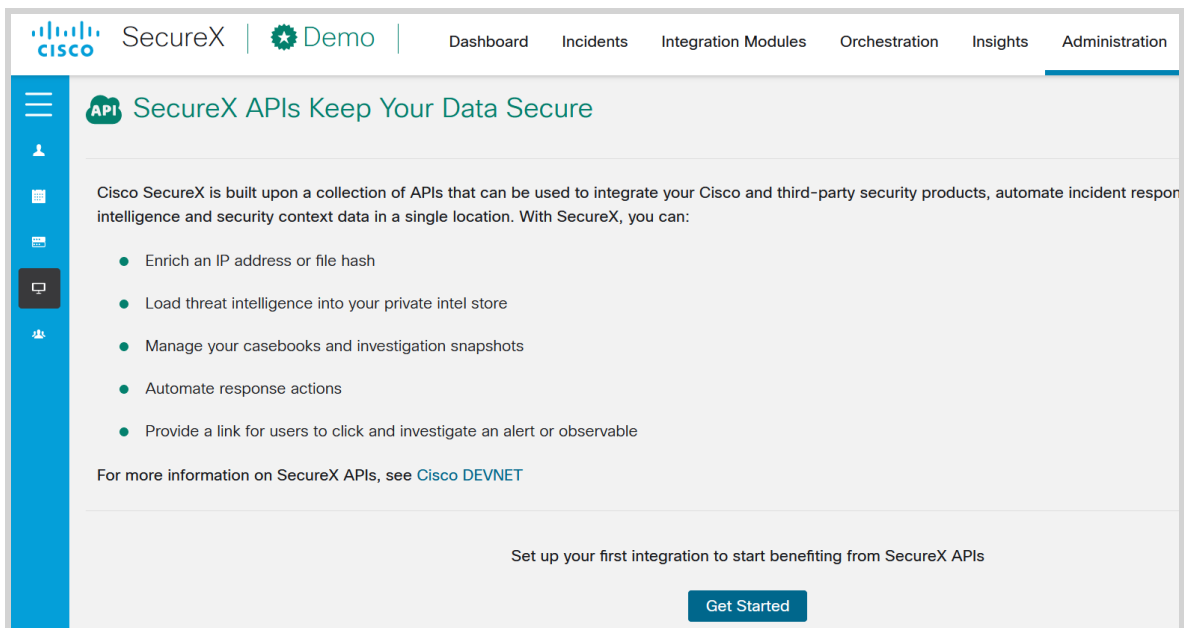
- Manager v7.2.1 or later
- You have an account to access SecureX (see [Required Account for SecureX Access](#)).
- Your Manager must be able to connect outbound to the Cisco clouds, SecureX Private Intelligence API, and regional SecureX portals :
 - North America clouds:
 - `api-sse.cisco.com`, port 443
 - `visibility.amp.cisco.com`, port 443
 - `private.intel.amp.cisco.com`, port 443
 - `securex.us.security.cisco.com`, port 443
 - EU clouds:
 - `api.eu.sse.itd.cisco.com`, port 443
 - `visibility.eu.amp.cisco.com`, port 443
 - `private.intel.eu.amp.cisco.com`, port 443
 - `securex.eu.security.cisco.com`, port 443
 - Asia (APJC) clouds:
 - `api.apjc.sse.itd.cisco.com`, port 443
 - `visibility.apjc.amp.cisco.com`, port 443
 - `private.intel.apjc.amp.cisco.com`, port 443
 - `securex.apjc.security.cisco.com`, port 443

- Orbital users only: Allow the following additional hosts for outbound connections:
 - North America: orbital.amp.cisco.com, port 443
 - Europe: orbital.eu.amp.cisco.com, port 443
 - Asia: orbital.apjc.amp.cisco.com, port 443
- Your Secure Network Analytics deployment is generating security events and Alarms as expected.

Procedure

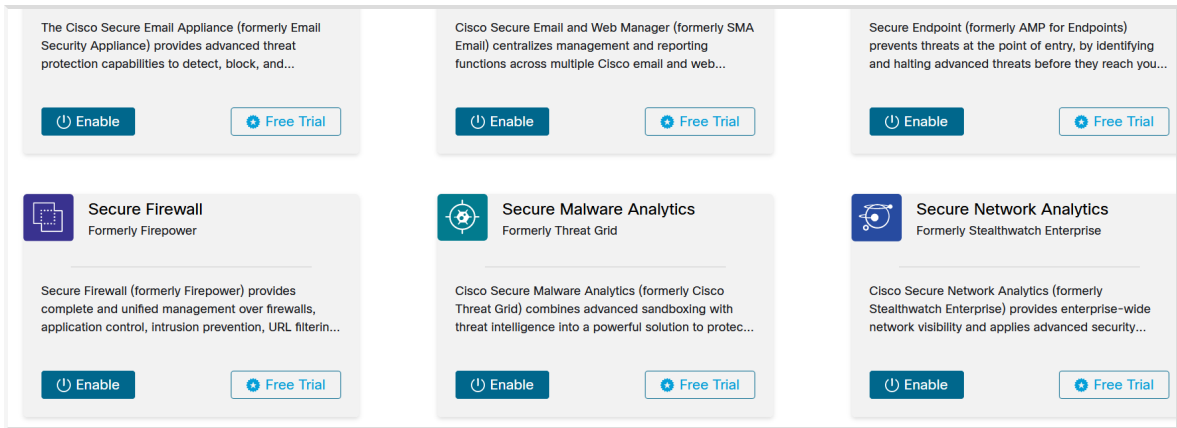
To configure the SecureX integration, complete the following steps:

1. Go to your regional SecureX cloud:
 - North America cloud: <https://securex.us.security.cisco.com>
 - Europe cloud: <https://securex.eu.security.cisco.com>
 - Asia (APJC) cloud: <https://securex.apjc.security.cisco.com>
2. Sign in using the credentials for your SecureX for Endpoints, Cisco Threat Grid, or Cisco Security account.
3. Select **Administration > API Clients**.
4. Click the **Get Started** button, if you are configuring for the first time.

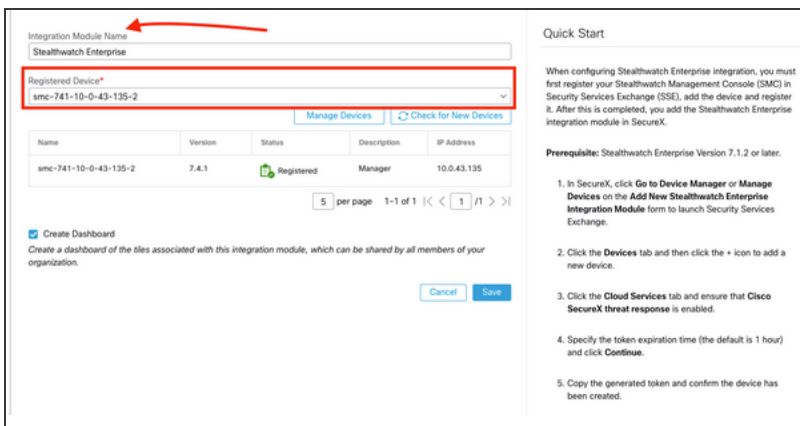


5. Select the SecureX ribbon and select the **Configure a Module** button.

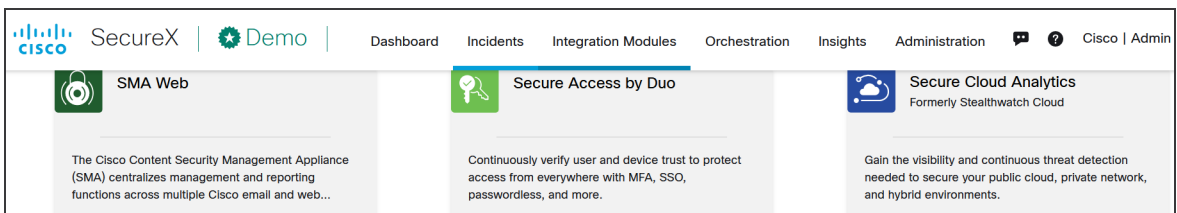
6. Select the **Secure Network Analytics** tile and click the **Enable** button.



7. Add new **Secure Network Analysis** Integration Module and select your device from the drop-down list. Check the **Create Dashboard** checkbox and click **Save**.



8. Select **Integration Modules** tab and select the Integration.



9. In the opened dialog, fill in the name and description for the API Client and select the following scopes:

- Admin
- Feedback
- Integration
- Casebook
- Global Intel:read
- Notification
- Enrich:read
- Inspect:read
- Oauth

- Orbital
- Registry
- Users
- Private Intel
- Response
- Webhook
- Profile
- Telemetry:write

i The scopes cannot be changed after the API Client has been generated.

10. Click **Add New Client**.

i To create a new client ID, select **Administration > API Clients** and click **Generate API Client**.

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

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

12. Log in to your Manager as Primary Admin or Configuration manager.

13. From the navigation menu, click the **Configure > INTEGRATIONS SecureX**.

14. In the SecureX **Configuration** section, click **Add New Configuration**.

15. In the opened form, select the regional cloud used to create the API Client and paste the Client ID and Client Password from Step 11.
16. Select the Integration Options you want to enable, then click **Save**. The system will validate and store the API credentials.

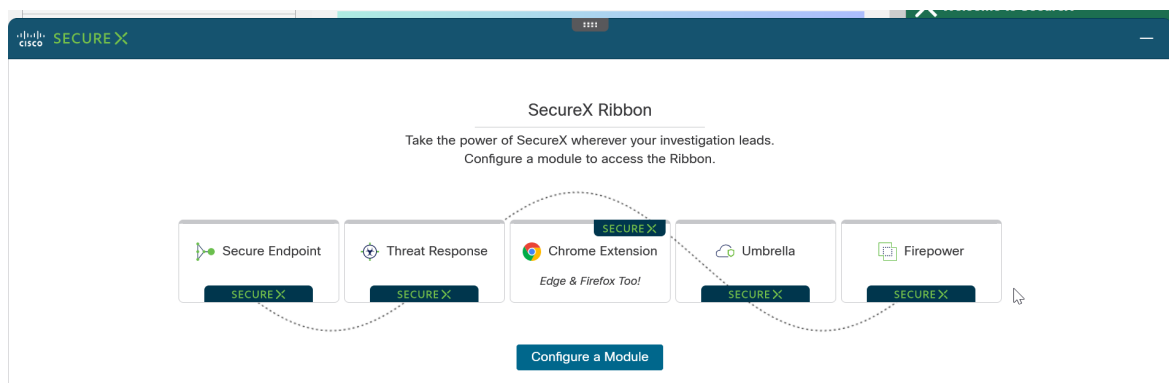
Authorize the SecureX Ribbon and Menu

Once the SecureX configuration is complete, you can authorize the SecureX ribbon and menu from the ribbon on any page on your Manager or from the SecureX configuration page.

The SecureX ribbon authentication widget on the SecureX configuration page shows you the current status of ribbon authorization and allows you to authorize or unauthorize the ribbon.

Authorize from SecureX Ribbon

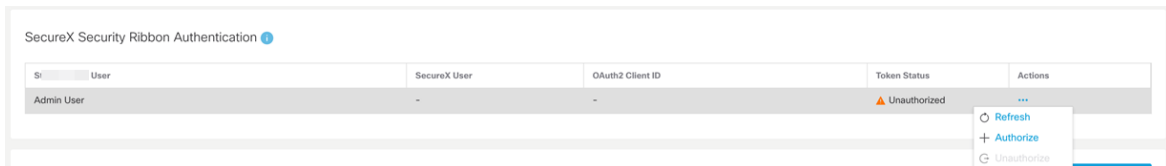
1. Expand the SecureX ribbon located at the bottom of the page on your Manager.



2. Click **Get SecureX**. You will be redirected to the SecureX login page.
3. Log in to SecureX with your credentials.
4. You will be asked to authorize the Manager SecureX ribbon client to access SecureX with scopes specified.
5. Grant Access. You will be redirected to your Manager page with the ribbon open and you can start using the ribbon on your Manager.

Authorize from the SecureX Configuration Page

1. Log in to your Manager.
2. Select **Configure > INTEGRATIONS SecureX**.
3. Open the **Actions** menu in the SecureX **Security Ribbon Authentication** widget and select **... > Authorize**. You will be redirected to the SecureX login page.



4. Log in to SecureX with your credentials.
5. You will be asked to authorize the Manager SecureX ribbon client to access SecureX with scopes specified.
6. Grant Access. You will be redirected to your Manager page with the ribbon open and you can start using the ribbon on your Manager.

In case you need to use the SecureX Ribbon under another SecureX account you need to unauthorize your current user and authorize again with a new one.

Unauthorize the Current SecureX Ribbon

1. On the SecureX Configuration page, open the Actions menu in the SecureX **Security Ribbon Authentication** widget and select **... > click Unauthorize**.
2. Authorize with another user following the steps above.

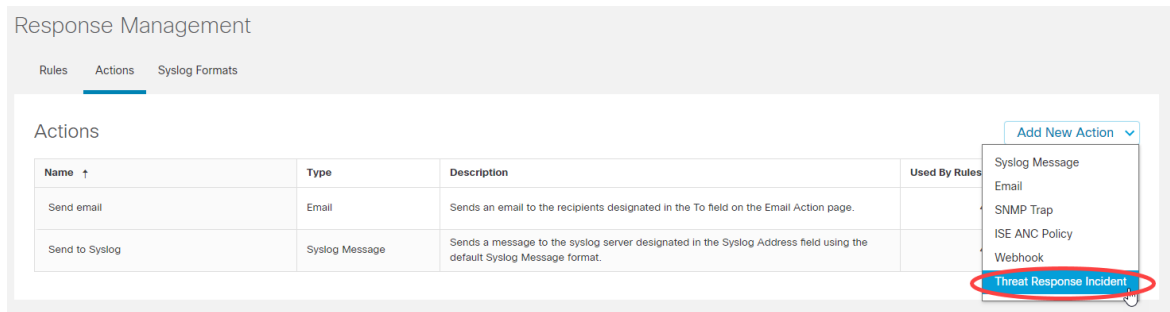
Configure the Threat Response Incident Action



If you have configured sending Secure Network Analytics Alarms to Cisco SecureX threat response in previous Secure Network Analytics (formerly Stealthwatch) versions, the Threat Response Incident action will be automatically created.

To configure the Threat Response Incident action in Response Management, complete the following steps:

1. Log in to your Manager.
2. Select **Configure > DETECTION Response Management**.
3. Click the **Actions** tab, then click **Add New Action > Threat Response Incident**.



4. Fill out the form and click **Save**.

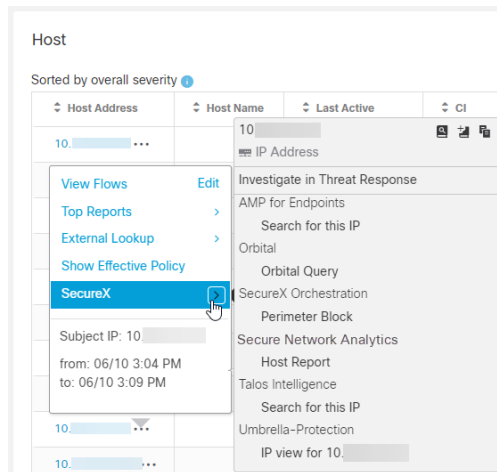
The screenshot shows the 'Threat Response Incident Action' configuration form. The 'Name' field contains 'Test' and the 'Description' field contains 'Testing'. The 'Enabled' toggle is turned on. The 'Incident Confidence Level' is set to 'Low'. The checkbox 'Create a new Target entity in SecureX Threat Response for alarms processed by this action.' is checked. Below it, the radio button 'Create targets in Threat Response for internal hosts only.' is selected. At the bottom, the 'Use host details from the alarm data:' dropdown is set to 'Source and Target Hosts'.

For more information about the action options, refer to the [About Sending Secure Network Analytics Alarms to Cisco SecureX Threat Response](#) section and the *Configuring Response Management* help topic.


Verification

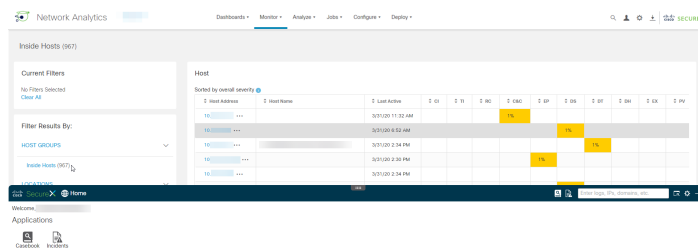
1. Verify that your Manager has the SecureX menu and ribbon available.
 - For SecureX menu:
 - Open any page in the Manager that contains a relevant IP address.
 - Click the **⋯ (Ellipsis)** icon beside the applicable IP address.

- In the pop-up menu that appears, click the arrow next to SecureX. A secondary pop-up menu appears with menu content.



- For SecureX ribbon:

- Navigate to any page in your Manager. Click the  (SecureX ribbon) icon on the bottom of the page to expand the widget.



2. Verify your Secure Network Analytics alarm in SecureX:

- Wait until Secure Network Analytics detects Critical or Major Security Alarm or generate a test security alarm.
- Log in to your regional SecureX cloud.
- Navigate to Incidents app in the SecureX ribbon, or Incident Manager in Cisco SecureX threat response.
- Your alarm should be available in the list.

Register your Manager in the Cisco Cloud

The Cisco Security Services Exchange (SSE) cloud is available for your Manager in Central Management. Registering your Manager in the SSE cloud will allow SecureX to retrieve enrichment data, such as Security Events, from your Manager to be included in the investigation workflows and retrieve Secure Network Analytics (shown as Stealthwatch) tiles for SecureX dashboard.

For more details, refer to the [About Secure Network Analytics Enrichment Data for SecureX](#) and [About Secure Network Analytics Tiles for SecureX dashboard](#) sections.



- SSE is enabled by default.
- If you use Automatic Registration, you will need to link your SSE account and your Smart Licensing Account.



If you are using a custom Manager Identity certificate that is different from the one provided by the default Manager Identity certificate, contact [technical support](#) as your Manager may require additional configuration steps.

Automatic Registration Procedure

Your Manager will automatically register in the SSE cloud if the following conditions are met:

- SSE option is enabled for your Manager under External Services.
- Your Manager is not already registered in SSE.
- Your product is registered with Cisco Smart Software Licensing. For more information, refer to the [Smart Software Licensing](#) guide.

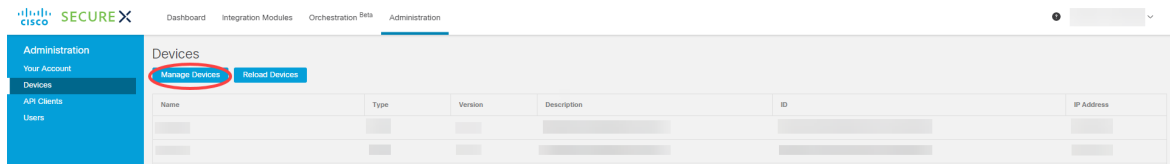
To enable or disable SSE, complete the following steps:

1. Log in to your Manager.
2. Select **Configure > GLOBAL Central Management**.
3. Click the **⋮ (Ellipsis)** icon under the Actions column for your Manager, then click **Edit Appliance Configuration**.
4. Click **General**.
5. Under External Services, check or uncheck the **Cisco Security Services Exchange** check box to enable or disable automatic registration.
6. Click **Apply Settings**. If you have enabled SSE, continue to step 7 to register your device.
7. Return to the Security Insight Dashboard.
8. Select **Configure > INTEGRATIONS SecureX**.
9. In the **Device Registration** section, click **New Device Registration**.
10. Select **Register Automatically**.

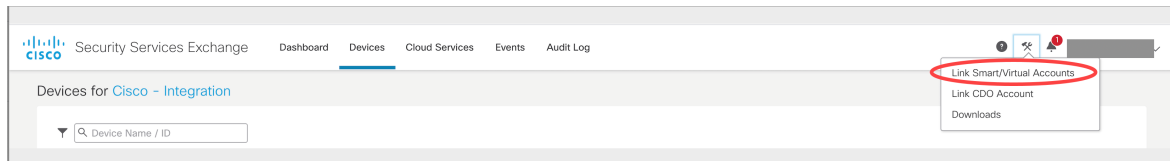
Link your Accounts

To link your Smart Licensing Account with your Cisco Security Services Exchange account, complete the following steps:

1. Go to your regional SecureX cloud and log in using the credentials for your AMP for Endpoints, Cisco Threat Grid, or Cisco Security account.
2. Click the **Administration** tab. Choose **Devices > Manage Devices** to be taken to Security Services Exchange.



3. Click the **(Tools)** icon, then click **Link Smart/Virtual Accounts**.

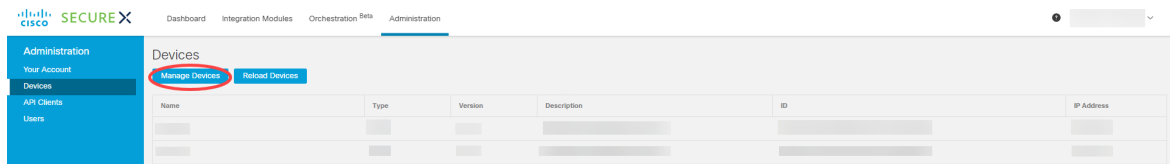


4. Select your Smart account from the pop-up with the list of accounts.

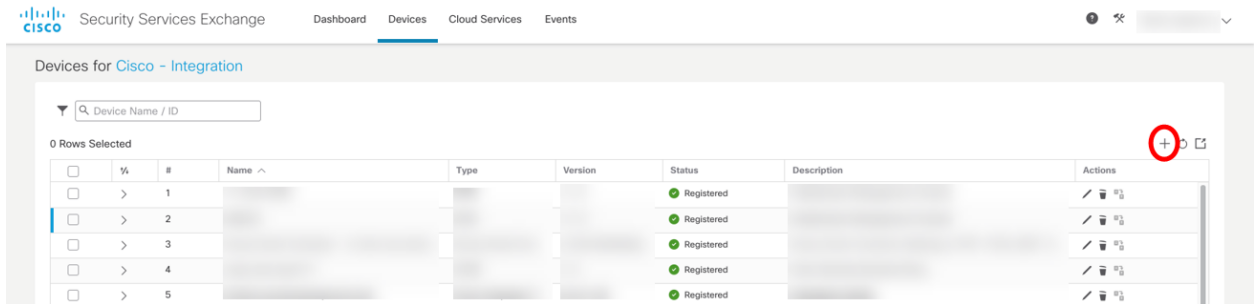
Manual Registration Procedure

To manually register your Manager in Security Services Exchange, complete the following steps:

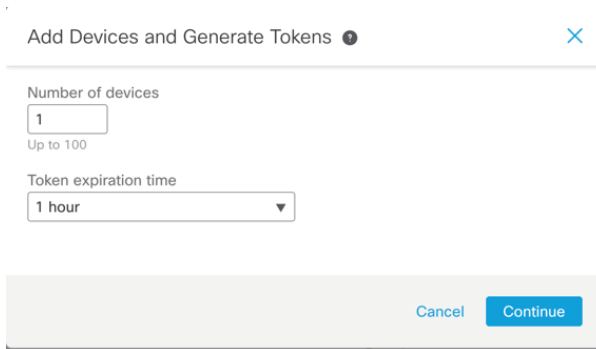
1. Go to your regional SecureX cloud and log in using the credentials for your SecureX for Endpoints, Cisco Threat Grid, or Cisco Security account.
2. Click the **Administration** tab. Choose **Devices > Manage Devices** to be taken to Security Services Exchange.



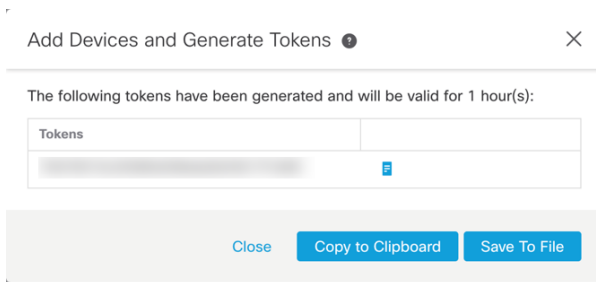
3. Click the **Devices** tab and then click the **+** (**Add Devices and Generate Tokens**) icon located on the right of the page, above the table with your devices.



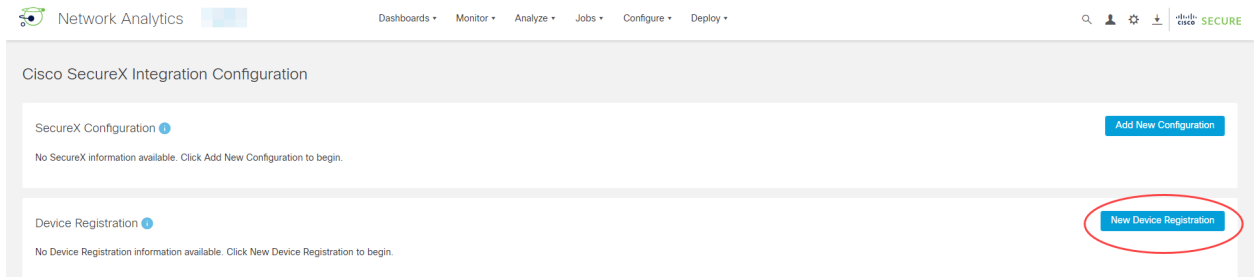
4. In the opened dialog, click **Continue** and let system generate a token for your device.



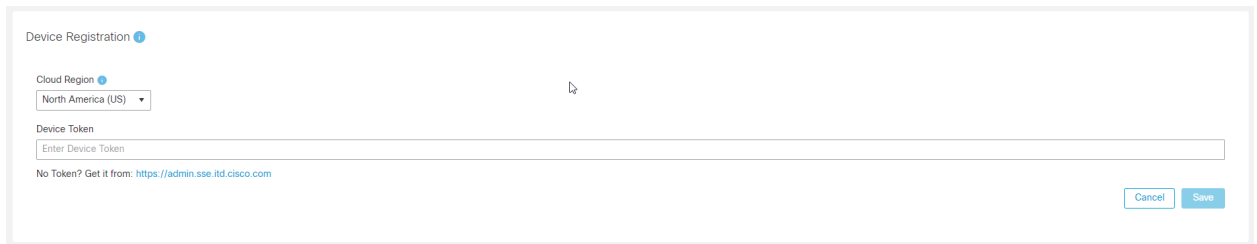
5. Copy the generated token into the clipboard or save the generated token into the file.



6. Log in to your Manager as Primary Admin or Configuration Manager.
7. Select **Configure > INTEGRATIONS SecureX**.
8. In the Device Registration section, click **New Device Registration**.



- In the opened dialog, select the Cloud Region that matches your SecureX regional cloud and insert the Security Services Exchange token generated and saved in step 5 and click **Save**.



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

Configuring Secure Network Analytics Integration Module in SecureX

For SecureX to retrieve enrichment data and dashboard tiles from Secure Network Analytics the integration module must be configured.

Prerequisites

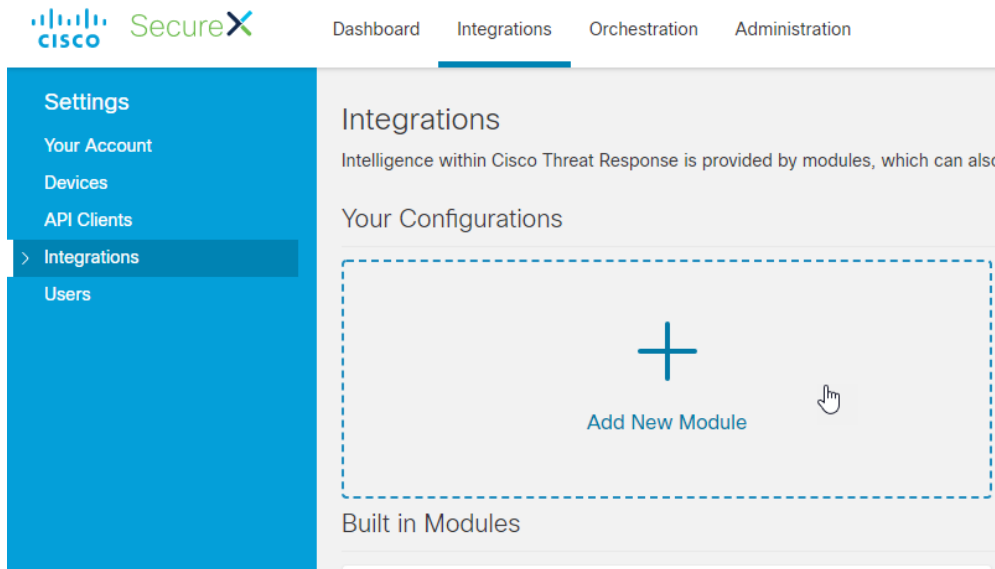
- Your Manager is registered in the Cisco Security Services Exchange cloud.
- Cisco SecureX threat response is enabled in Cisco Security Services Exchange portal Cloud Services.

Refer to the [Register your Manager in the Cisco Cloud](#) section for more details.

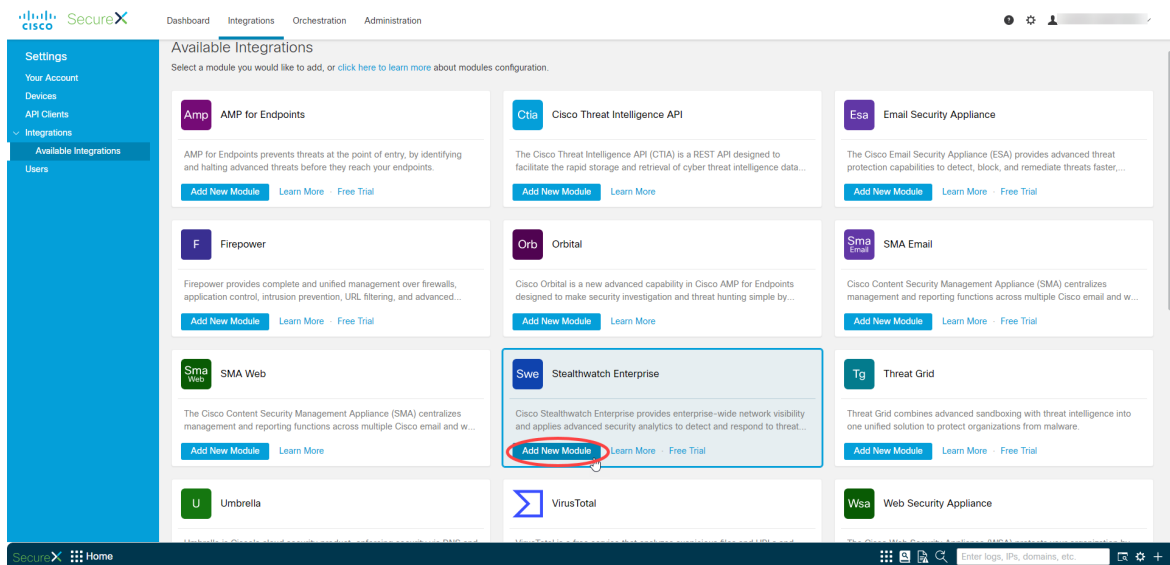
Procedure

To configure the Secure Network Analytics module in SecureX, complete the following steps:

1. Go to your regional SecureX cloud and log in using the credentials for your AMP for Endpoints, Cisco Threat Grid, or Cisco Security account.
2. Select **Integration Modules > Integrations**.
3. Click **Add New Module**. The Available Integrations page opens.



4. Find the Stealthwatch Enterprise module and click **Add New Module**.



5. In the opened dialog:
 - a. Name your module.
 - b. In the Registered Device drop down, locate your Manager.
 - c. Click **Save**.

6. Verify that Cisco SecureX threat response can retrieve enrichment data from your Manager. To do this:
 - a. Review your Manager Security dashboards and notice an IP that generates security events.
 - b. Enter this IP into the Investigation search panel in Cisco SecureX 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.

Configuring the SecureX dashboard with Secure Network Analytics Tiles

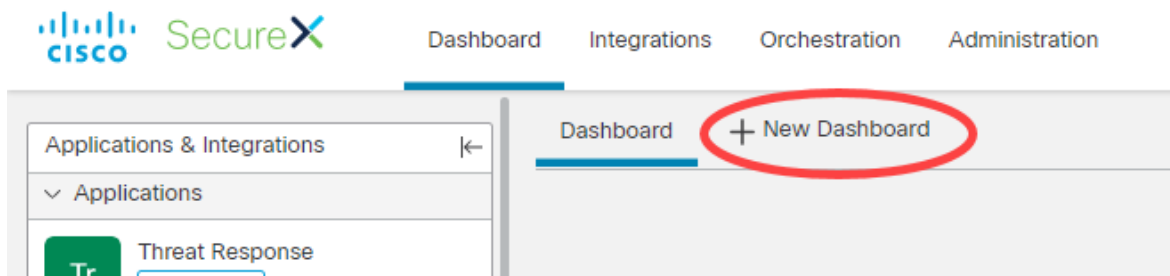


The Secure Network Analytics Integration Module has to be configured before adding Secure Network Analytics (shown as Stealthwatch) tiles to the SecureX dashboard.

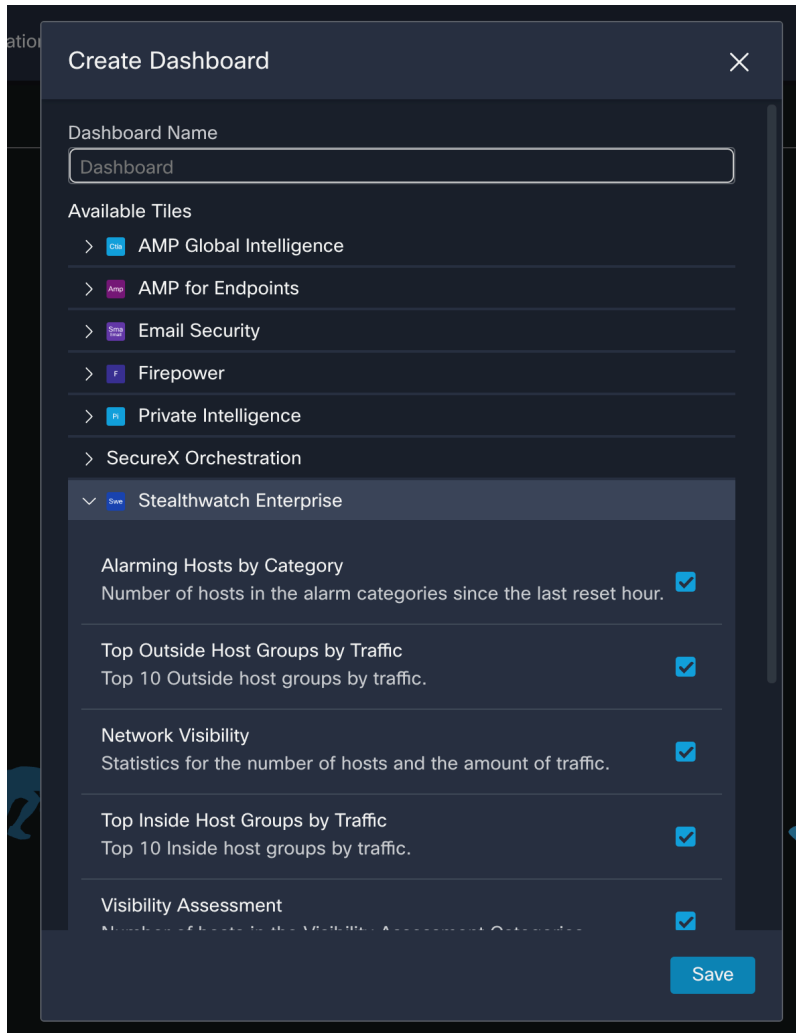
To add Secure Network Analytics (shown as Stealthwatch) tiles to the dashboard, complete the following steps:

1. In a browser window, go to your regional SecureX portal:
 - North America: <https://securex.us.security.cisco.com>
 - Europe: <https://securex.eu.security.cisco.com>
 - Asia (APJC): <https://securex.apjc.security.cisco.com>
2. Log in using your Cisco Security or Cisco Threat Grid account.

3. On the dashboard menu bar, click **New Dashboard** to open the **Create Dashboard** form.



4. In the opened dialog, fill in the **Dashboard Name** and locate the Stealthwatch Enterprise module under Available Tiles.
5. Expand Stealthwatch Enterprise and select the tiles you want to add to the dashboard.



6. Click **Save**.

The tiles you selected will appear on the dashboard layout with relevant data.

Known Issues and Limitations

- Failover is not supported for the SecureX integration in v7.5. The configuration needs to be repeated for the secondary Manager for the integration to work from both Managers in the Secure Network Analytics failover pair.
- Backup and Restore is not supported for Device Registration in the Cisco Security Services Exchange Cloud portal. The Device Registration panel in the SecureX configuration on your Manager 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.

Contacting Support

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

- Contact your local Cisco Partner
- Contact Cisco 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:
<https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>

Change History

Document Version	Published Date	Description
1_0	January 19, 2024	Initial Version.

Copyright Information

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

