Integrating with Cisco SecureX or Cisco Threat Response

This chapter contains the following topic:

Integrating Your Appliance with Cisco SecureX or Cisco Threat Response

Cisco SecureX is a security platform embedded with every Cisco security product. It is cloud-native with no new technology to deploy. Cisco SecureX simplifies the demands of threat protection by providing a platform that unifies visibility, enables automation, and strengthens your security across network, endpoints, cloud, and applications. By connecting technology in an integrated platform, Cisco SecureX delivers measurable insights, desirable outcomes, and unparalleled cross-team collaboration. Cisco SecureX enables you to expand your capabilities by connecting your security infrastructure.

Cisco Threat Response is a threat incident response orchestration hub that supports and automates integrations across multiple Cisco Security products. As a key pillar of the Cisco integrated security architecture, Threat Response accelerates key security operations functions: detection, investigation, and remediation.

Integrating the Appliance with Cisco SecureX or Cisco Threat Response contains the following sections:

- How to Integrate Your Appliance with Cisco SecureX or Cisco Threat Response
- Performing Threat Analysis using Cisco SecureX Ribbon

You can integrate your appliance with Cisco SecureX or Cisco Threat Response, and perform the following actions in Cisco SecureX or Cisco Threat Response:

- View and send the email data from multiple appliances in your organization.
- Identify, investigate and remediate threats observed in the email reports, sender and target relationships, search for multiple email addresses and subject lines and message tracking.
- Block compromised users or users violating outgoing email policies.

- Resolve the identified threats rapidly and provide recommended actions to take against the identified threats.
- Document the threats to save the investigation and enable collaboration of information among other devices.
- Block malicious domains, track suspicious observances, initiate an approval workflow or to create an IT ticket to update email policy.

You can access Cisco SecureX using the following URL:

https://securex.us.security.cisco.com/login

Cisco Security Management Appliance (SMA) centralizes management and reporting functions across multiple Cisco email security appliances. For more information on observables that can be enriched by the SMA Email module, go to https://securex.us.security.cisco.com/settings/modules/available, navigate to the module to integrate with Cisco SecureX, and click **Learn More**.

How to Integrate Your Appliance with Cisco SecureX or Cisco Threat Response

Table 1: How to Integrate Your Appliance with Cisco SecureX or Cisco Threat Response

	Do This	**More Info**
Step 1	Review the prerequisites.	Prerequisites
Step 2	On your Security Management appliance, enable the Cisco SecureX or Cisco Threat Response integration.	Enable the Cisco SecureX Integration on your Security Management Appliance
Step 3	On Cisco SecureX, add your appliance as a device, register it, and generate a registration token.	For more information, go to https://securex.us.security.cisco.com/help/settings-devices
Step 4	On your Security Management appliance, complete the Cisco SecureX or Cisco Threat Response registration.	Register Cisco SecureX or Cisco Threat Response on Your Security Management Appliance
Step 5	Confirm whether the registration was successful.	Confirm Whether the Registration was Successful
Step 6	On Cisco SecureX, add SMA Email Module.	For more information, go to https://securex.us.security.cisco.com/settings/modules/available, navigate to the module to integrate with Cisco SecureX, click **Add New Module**, and see the instructions on the page.

Prerequisites

Note If you already have a Cisco Threat Response user account, you do not need to create a Cisco SecureX user account. You can log in to Cisco SecureX using your Cisco Threat Response user account credentials.

- Make sure that you create a user account in Cisco SecureX with admin access rights. To create a new user account, go to **Cisco SecureX login** page using the URL https://securex.us.security.cisco.com/login and click **Create a SecureX Sign-on Account** in the login page. If you are unable to create a new user account, contact Cisco TAC for assistance.
- [Only if you are not using a proxy server] Make sure that you open HTTPS (In and Out) 443 port on the firewall for the following FQDNs to register your appliance with Cisco SecureX or Cisco Threat Response:
  - api-sse.cisco.com (applicable for NAM users only)
  - api.eu.sse.itd.cisco.com (applicable for European Union (EU) users only)
  - api.apj.sse.itd.cisco.com (applicable for APJC users only)
  - est.sco.cisco.com (applicable for APJC, EU, and NAM users)

  For more information, see Firewall Information.

Enable the Cisco SecureX Integration on your Security Management Appliance

Step 1 Log in to your appliance.

Step 2 Select **Networks** > **Cloud Service Settings**.

Step 3 Click **Edit Settings**.

Step 4 Check the **Enable** check box.

Step 5 Submit and commit your changes.

Step 6 Wait for few minutes, and check whether the **Register** button appears on your appliance.

Note In a clustered configuration, you can only register your logged-in appliance with Cisco SecureX or Cisco Threat Response in the machine mode. If you have already registered your appliance with Cisco SecureX or Cisco Threat Response in the standalone mode, make sure to deregister the appliance manually before you join it to a cluster.

Note To enable this integration using the CLI, use the `threatresponseconfig` command.

What to do next

Register your appliance on Cisco SecureX or Cisco Threat Response. For more information, go to https://securex.us.security.cisco.com/settings/modules/available, navigate to the module to integrate with Cisco SecureX, click **Add New Module**, and see the instructions on the page.

Register Cisco SecureX or Cisco Threat Response on Your Security Management Appliance

Step 1 Go to **Networks** > **Cloud Service Settings**.

Step 2 In **Cloud Services Settings**, enter the registration token, and click **Register**.

Note To register Cisco SecureX or Cisco Threat Response using the CLI, use the `cloudserviceconfig` command.

What to do next

Confirm Whether the Registration was Successful

Confirm Whether the Registration was Successful

- On Security Services Exchange, confirm successful registration by reviewing the status in Security Services Exchange.
- On Cisco SecureX, navigate to the **Devices** page and view the SMA that has been registered with Security Services Exchange.

Note If you want to switch to another Cisco SecureX or Cisco Threat Response server (for example, 'Europe - api.eu.sse.itd.cisco.com'), you must first deregister your appliance from Cisco SecureX or Cisco Threat Response and follow steps mentioned in How to Integrate Your Appliance with Cisco SecureX or Cisco Threat Response.

After you have integrated your appliance with Cisco SecureX or Cisco Threat Response, you do not need to integrate your Email Security appliance with Cisco SecureX or Cisco Threat Response because the email and web reporting features are centralized.

After successful registration of your appliance on Security Services Exchange, add the SMA Email module on Cisco SecureX. For more information, go to https://securex.us.security.cisco.com/settings/modules/available, navigate to the module to integrate with Cisco SecureX, and click **Add New Module**, and see the instructions on the page.

Enabling Cisco SecureX or Threat Response on content Security Gateway

Step 1 Log into your appliance.

Step 2 Select **Networks** > **Cloud Service Settings**.

Step 3 Click **Enable**.

Step 4 Check the **Enable Cloud Service** check box.

Step 5 Choose the Cisco SecureX server.

Step 6 Submit and commit your changes.

Enabling Cisco Cloud Services Portal on Content Security Gateway

Step 1 Log in to your email gateway.

Step 2 Select **Networks > Cloud Service Settings**.

Step 3 Click **Enable**.

Step 4 Check the **Enable Cisco Cloud Services** check box.

Step 5 Choose the required Cisco Secure server to connect your email gateway to the Cisco Cloud Services portal.

Step 6 Submit and commit your changes. Wait for few minutes, and check whether the Register button appears on your content security gateway.

What to do next

Performing Threat Analysis using Cisco SecureX Ribbon

Note When you upgrade from Security Management Appliance 13.6.1 or earlier versions, **Casebook** will be part of the Cisco SecureX Ribbon.

Cisco SecureX supports a distributed set of capabilities that unify visibility, enable automation, accelerate incident response workflows, and improve threat hunting. These distributed capabilities are presented in the form of applications (apps) and tools in the Cisco SecureX Ribbon.

This topic contains the following sections:

- Accessing the Cisco SecureX Ribbon
- Adding Observable to Casebook for Threat Analysis using Cisco SecureX Ribbon and Pivot Menu

You will find the Cisco SecureX Ribbon at the bottom pane of the page, and it persists as you move between the dashboard and other security products in your environment. Cisco SecureX Ribbon consists of the following icons and elements:

- Expand/Collapse Ribbon
- Home
- Casebook App
- Incidents App

- Orbital App
- Enrichment Search Box
- Find Observables
- Settings

For more information on Cisco SecureX Ribbon, see https://securex.us.security.cisco.com/help/ribbon.

Accessing the Cisco SecureX Ribbon

Before you begin

Make sure that you meet all the prerequisites that are mentioned in Prerequisites.

Note Suppose you have already configured **Casebook** for Security Management Appliance 13.6.1 or earlier versions, you need to create a **Client ID** and **Client Secret** in Cisco SecureX API client with additional scopes, as mentioned in the following procedure.

You can drag the Cisco SecureX Ribbon, positioned at the bottom pane of the page, from right using button.

Step 1 Log in to the new web interface of your appliance. For more information, see Accessing the Web Interface.

Step 2 Click the Cisco SecureX Ribbon.

Step 3 Create a **Client ID** and **Client Secret** in **SecureX API Clients**. For more information to generate API Client credentials, see Creating an API Client.

While creating a client ID and client password, make sure that you choose the following scopes:

- casebook
- enrich:read
- global-intel:read
- inspect:read
- integration:read
- profile
- private-intel
- response
- registry/user/ribbon
- telemetry:write
- users:read
- orbital (if you have access)

Step 4 Enter the client ID and client password obtained in Step 3 in the **Login to use SecureX Ribbon** dialog box in your appliance.

Step 5 Select the required Cisco SecureX server in the **Login to use SecureX Ribbon** dialog box.

Step 6 Click **Authenticate**.

Note If you want to edit the client ID, client password, and Cisco SecureX server, right-click on the Cisco SecureX Ribbon, and add the details.

What to do next

Adding Observable to Casebook for Threat Analysis using Cisco SecureX Ribbon and Pivot Menu

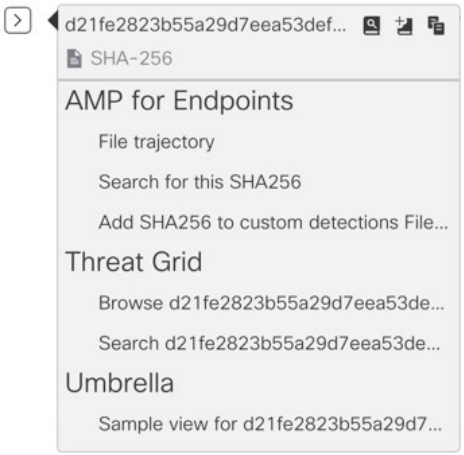
Adding Observable to Casebook for Threat Analysis using Cisco SecureX Ribbon and Pivot Menu

Before you begin

Make sure that you obtain the client ID and client password to access the Cisco SecureX Ribbon and pivot menu widgets on your appliance. For more information, see Accessing the Cisco SecureX Ribbon.

Step 1 Log in to the new web interface of your appliance. For more information, see Accessing the Web Interface.

Step 2 Navigate to the **Email Reporting** or **Web Reporting** page, click the pivot menu button next to the required observable (for example, bit.ly).



Perform the following:

- Click button to add an observable to active case.
- Click button to add the observable to new case.

Note Use the pivot menu button to pivot an observable to other devices registered on the portal (for example, AMP for Endpoints) to investigate for threat analysis.

Step 3 Hover over icon and click button to open the **Casebook**. Check whether the observable is added to a new or an existing case.

Step 4 (Optional) Click button to add a title, description, or notes to the **Casebook**.

Note You can search for observables for threat analysis in two different ways:

- Click the **Enrichment** search box from the Cisco SecureX Ribbon and search for the observables.
- Click the **Casebook** icon inside the Cisco SecureX Ribbon and search for the observables in the search field.

For more information on Cisco SecureX Ribbon, see https://securex.us.security.cisco.com/help/ribbon.

Performing Remedial Actions on Messages in Cisco SecureX Threat Response

Before you begin

In Cisco Threat Response, you can now investigate and apply the following remedial actions on messages processed by your email gateway:

- Delete
- Forward
- Forward and Delete

Make sure you have met the following prerequisites before you perform remedial actions on messages in Cisco Threat Response:

- Enabled and registered your email gateway with the Cisco SecureX server. For more information, see Enable the Cisco SecureX or Cisco Threat Response Integration on your Cisco Content Security Appliance and Registering Cisco SecureX or Cisco Threat Response on Cisco Content Security Appliance.
- Added your email gateway module to Cisco SecureX and specified the Remediation Forwarding Address in Cisco SecureX. For more information, go to https://securex.us.security.cisco.com/settings/modules/available navigate to the required Email Security Appliance module to integrate with Cisco SecureX, click Add New Module, and see the instructions on the page.
- Enabled and configured the remediation profiles in the **System Administration > Account Settings** page in your email gateway. For more information, see the Remediating Messages in Mailboxes chapter.

Step 1 Log in to Cisco SecureX with your user credentials.

Step 2 Perform an investigation for threat analysis by entering required IOCs (for example, URLs, Email Message ID and so on) in the Investigate panel and click Investigate. For more information, see the Investigate topic in the Help section at https://visibility.amp.cisco.com/help/investigate.

Step 3 Click the pivot menu button next to the Cisco Message ID or Email Message ID and select the required remedial action (for example, 'Forward'). For more information, see the Investigate topic in the Help section at https://visibility.amp.cisco.com/help/investigate.