



Integrating with Cisco SecureX Threat Response

This chapter contains the following sections:

- [Integrating your Appliance with Cisco SecureX Threat Response, on page 1](#)
- [How to Integrate Your Appliance with Cisco SecureX Threat Response, on page 2](#)
- [Performing Threat Analysis using Cisco SecureX Ribbon, on page 5](#)
- [Improving User Experience of Email Gateway using Cisco Success Network, on page 8](#)

Integrating your Appliance with Cisco SecureX 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.

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

- [How to Integrate Your Appliance with Cisco SecureX Threat Response, on page 2](#)
- [Performing Threat Analysis using Cisco SecureX Ribbon, on page 5](#)

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

- View and send the email data from multiple 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 Threat Response using the following URL:

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

Cisco Secure Email Gateway provides advanced threat protection capabilities to detect, block, and remediate threats faster, prevent data loss, and secure important information in transit with end-to-end encryption. For more information on observables that can be enriched by the ESA 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 Threat Response

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

	Do This	More Info
Step 1	Review the prerequisites.	Prerequisites, on page 2
Step 2	On your Email Security appliance, enable the Cisco SecureX Threat Response integration.	Enable the Cisco SecureX Threat Response Integration on your Cisco Email Security Appliance, on page 3
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 Email Security appliance, complete the Cisco SecureX Threat Response registration.	Registering Cisco SecureX Threat Response on Cisco Email Security Appliance, on page 4
Step 5	Confirm whether the registration was successful.	Confirm Whether the Registration was Successful, on page 4
Step 6	On Cisco SecureX, add Email Security Appliance Module.	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.

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.
- Ensure that the configured DNS server can resolve the hostname you specified for accessing the email gateway.
- [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 email gateway with Cisco SecureX 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 Threat Response Integration on your Cisco Email Security Appliance

Procedure

- 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** Choose the required Cisco SecureX Threat Response server to connect your appliance to Cisco SecureX Threat Response.
- Step 6** Submit and commit your changes.
- Step 7** 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 Threat Response in the machine mode. If you have already registered your appliance with Cisco SecureX 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 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.

Registering Cisco SecureX Threat Response on Cisco Email Security Appliance

Procedure

-
- 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 Threat Response using the CLI, use the `cloudserviceconfig` command.

What to do next

[Confirm Whether the Registration was Successful, on page 4](#)

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 ESA that has been registered with Security Services Exchange.



Note If you want to switch to another Cisco SecureX Threat Response server (for example, 'Europe - api.eu.sse.itd.cisco.com'), you must first deregister your email gateway from Cisco SecureX Threat Response and follow steps mentioned in [How to Integrate Your Appliance with Cisco SecureX Threat Response, on page 2](#).

After you have integrated your email gateway with Cisco SecureX Threat Response, you do not need to integrate your Cisco Secure Manager Email and Web Gateway with Cisco SecureX Threat Response.

After successful registration of your email gateway on Security Services Exchange, add the ESA 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, click **Add New Module**, and see the instructions on the page.

Performing Threat Analysis using Cisco SecureX Ribbon



Note When you upgrade from Email Security appliance 13.5.1 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, on page 5](#)
- [Adding Observable to Casebook for Threat Analysis using Cisco SecureX Ribbon and Pivot Menu, on page 7](#)

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, on page 2](#).



Note Suppose you have already configured **Casebook** for Email Security appliance 13.5.1 or earlier versions. You need to create a new **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.

Procedure

- Step 1** Log in to the new web interface of your email gateway. For more information, see [Accessing the Web-Based Graphical User Interface \(GUI\)](#).
- 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 email gateway.
- 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, on page 7](#)


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

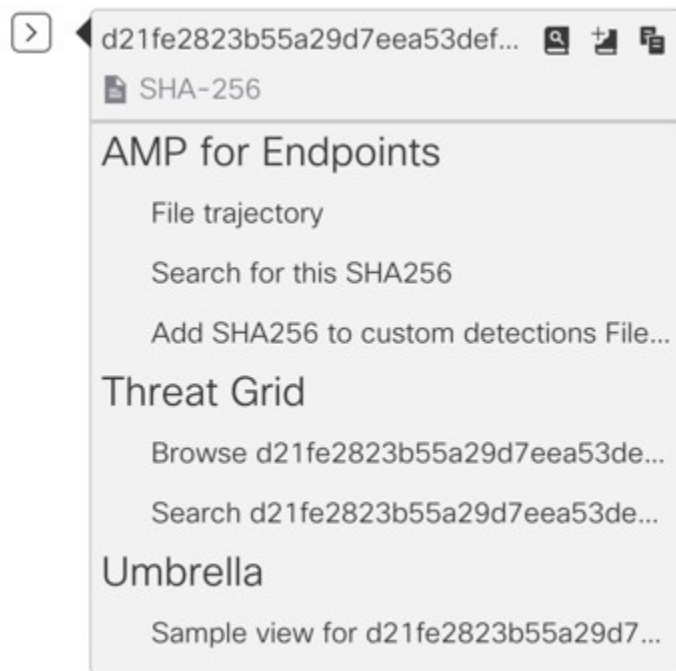
Before you begin

Make sure that you obtain the client ID and client password to access the Cisco SecureX Ribbon and pivot menu widgets on your email gateway. For more information, see [Accessing the Cisco SecureX Ribbon, on page 5](#).



Procedure

Step 1 Log in to the new web interface of your email gateway. For more information, see [Accessing the Web-Based Graphical User Interface \(GUI\)](#).


Step 2 Navigate to the **Email 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



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

Improving User Experience of Email Gateway using Cisco Success Network

Overview

You can use the Cisco Success Network (CSN) feature to send your email gateway and feature usage details to Cisco. These details are used by Cisco to identify the email gateway version and the features activated but not enabled on your email gateway.

The ability to send your email gateway and feature usage details to Cisco helps an organization to:

- Improve the effectiveness of the product in user networks by performing analytics on collected telemetry data and suggesting users with recommendations using a digital campaign.
- Improve user experience with email gateway.

The following table shows a sample data of email gateway and feature usage details sent to Cisco:

Statistics	Sample Data
Email Gateway Details	
UID	4215XXXXXXXXXXXXXXXXXXXX-XXXXXXXXXXXX
Model	C100V
sIVAN	Email Gateway (for a smart license) or null (for a classic license)
Deployment	Cluster/Standalone.

Statistics	Sample Data
userAccountID	Enter SLPIID (in smart license) or VLNID (in classic license).
Version	1X.X.X-XXX
Install Date	1582535814000 (milli-seconds since epoch)
Feature Information	
Name	Email Gateway Feature
Enabled	Yes
Status	In Compliance
Expiry Date	1831591683 (seconds since epoch)
Feature ID	a4deXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX

Related Topics

- [Enabling CSN on Email Gateway, on page 9](#)
- [Disabling CSN on Email Gateway, on page 10](#)

Enabling CSN on Email Gateway

Before you begin

Make sure that you enable and register your email gateway with Cisco SecureX or Cisco Threat Response. For more information, see [How to Integrate Your Appliance with Cisco SecureX Threat Response, on page 2](#).

Procedure

-
- Step 1** Go to **Security Services > Cloud Service Settings**.
 - Step 2** Click **Edit Settings** under Cisco Success Network. **Edit Global Settings**.
 - Step 3** Check the **Enable** checkbox.
 - Step 4** Submit and commit your changes.
-

Disabling CSN on Email Gateway

Procedure

- Step 1** Go to **Security Services > Cloud Service Settings**.
 - Step 2** Click **Edit Settings** under Cisco Success Network. **Edit Global Settings**.
 - Step 3** Uncheck the **Enable** checkbox.
 - Step 4** Submit and commit your changes.
-