Integrating with Cisco SecureX Threat Response

This chapter contains the following sections:

- Integrating your Email Gateway with Cisco SecureX Threat Response, on page 1
- How to Integrate your Email Gateway with Cisco SecureX Threat Response, on page 2
- Deregister Secure Email Gateway from Cisco Cloud Services Portal, on page 6
- Performing Threat Analysis using Cisco SecureX Ribbon, on page 6
- Performing Remedial Actions on Messages in Cisco SecureX Threat Response, on page 10
- Improving User Experience of Email Gateway using Cisco Success Network, on page 11

Integrating your Email Gateway 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 Email Gateway with Cisco SecureX Threat Response contains the following sections:

- How to Integrate your Email Gateway with Cisco SecureX Threat Response, on page 2
- Performing Threat Analysis using Cisco SecureX Ribbon, on page 6

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

- View and send the email data from multiple email gateways 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://xdr.us.security.cisco.com/administration/integrations, navigate to the module to integrate with Cisco SecureX and click **Learn More**.

How to Integrate your Email Gateway with Cisco SecureX Threat Response

Table 1: How to Integrate your Email Gateway with Cisco SecureX Threat Response

	Do This	More Info
Step 1	Review the prerequisites.	Prerequisites, on page 3
Step 2	[Applicable only for users using the Classic Licensing mode]. **Note** If you are using the Smart Licensing mode , you can skip this step because Cisco Cloud Services Portal is automatically enabled on your email gateway. Enable the Cisco Cloud Services portal on your email gateway.	Enabling Cisco Cloud Services Portal on Email Gateway, on page 4
Step 3	On Cisco SecureX , add your email gateway as a device, register it, and generate a registration token.	For more information, go to https://securex.us.security.cisco.com/help/settings-devices

	Do This	More Info
Step 4	[Applicable only for users using the Classic Licensing mode]. **Note** If you are using the Smart Licensing mode, you can skip this step because your email gateway is automatically registered with Cisco Cloud Services Portal. Register your email gateway with the Cisco Cloud Services portal.	Registering Email Gateway with Cisco Cloud Services Portal, on page 5
Step 5	Confirm whether the registration was successful.	Confirm Whether the Registration was Successful, on page 5
Step 6	Enable Cisco SecureX Threat Response on your email gateway	Enabling Cisco SecureX Threat Response on Email Gateway, on page 5
Step 7	On Cisco SecureX , add Cisco Secure Email Gateway Module.	For more information, go to https://securex.us.security.cisco.com/settings/modules/available, navigate to the required Cisco Secure Email Gateway 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.

- [For users with smart licensing registered on the email gateway] Make sure you have already linked your smart account (created in Cisco Smart Software Manager portal) to Cisco Security Services Exchange . For more information, see the following documentation at:
  - [Applicable for NAM users] https://admin.sse.itd.cisco.com/assets/static/online-help/index.html#!t_link_accounts.html
  - [Applicable for European Union (EU) users] https://admin.eu.sse.itd.cisco.com/assets/static/online-help/index.html#!t_link_accounts.html
  - [Applicable for APJC users] https://admin.apj.sse.itd.cisco.com/assets/static/online-help/index.html#!t_link_accounts.html

Enabling Cisco Cloud Services Portal on Email Gateway

Procedure

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.

Step 7 Wait for few minutes, and check whether the **Register** button appears on the Cloud Services Settings page.

In a clustered configuration, you can only register your logged-in email gateway with the Cisco Cloud Services portal in the machine mode. If you have already registered your email gateway with the Cisco Cloud Services portal in the standalone mode, make sure to deregister the email gateway manually before you join it to a cluster.

Note To enable Cisco Cloud Services portal using the CLI, use the `cloudserviceconfig` command.

What to do next

Register your email gateway with the Cisco Cloud Services portal. 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 Email Gateway with Cisco Cloud Services Portal

Procedure

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

Step 2 Enter the registration token under Cloud Services Settings and click **Register**.

Note To register your email gateway with or the Cisco Cloud Services portal using the CLI, use the `cloudserviceconfig` command.

What to do next

Confirm Whether the Registration was Successful, on page 5

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 emal gateway from Cisco Cloud Service Portal and follow steps mentioned in Deregister Secure Email Gateway from Cisco Cloud Services Portal, on page 6.

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 Excange, add the ESA Email module on Cisco SecureX. For more information, go tohttps://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.

Enabling Cisco SecureX Threat Response on Email Gateway

Procedure

Step 1 Log in to your email gateway.

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

Step 3 Click **Edit Global Settings**.

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

Step 5 Submit and commit your changes.

Deregister Secure Email Gateway from Cisco Cloud Services Portal

Perform the following steps to deregister Secure Email Gateway from Cisco Cloud Services portal.

Procedure

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

Step 2 Click **Deregister** on the **Cloud Service Settings** page.

Step 3 Click **Deregister** on the **Deregister Appliance** pop-up window.

After deregistering the Secure Email Gateway from Cisco Cloud Services Portal, you can do any of the following by clicking **Edit Global Settings**:

- Switch to another Cisco XDR server.
- Change the registration token obtained from the Cisco Cloud Services portal.

Note You need to get a new token from the respective Cisco XDR Server region to register again.

Performing Threat Analysis using Cisco SecureX Ribbon

Note When you upgrade from Cisco Secure Email Gateway 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 7
- Adding Observable to Casebook for Threat Analysis using Cisco SecureX Ribbon and Pivot Menu, on page 8

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 3.

Note Suppose you have already configured **Casebook** for Cisco Secure Email Gateway 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 8

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

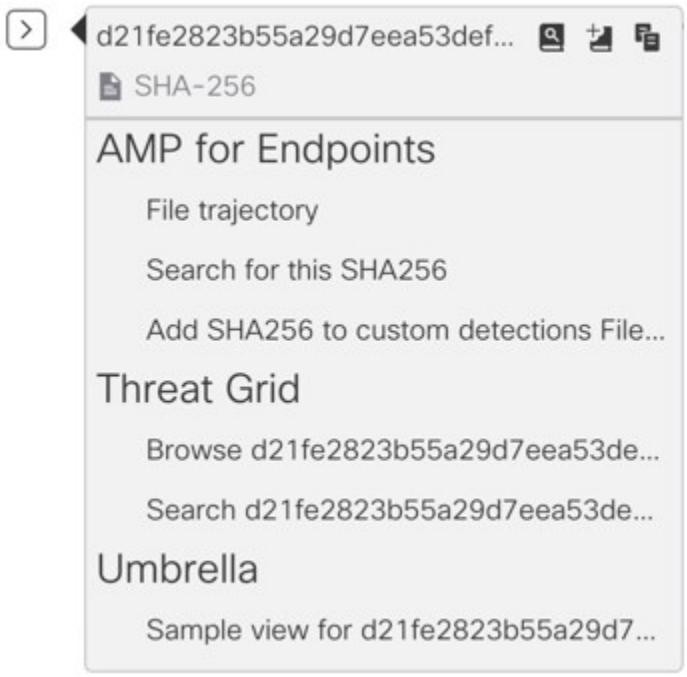
Before you begin

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 7.

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 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

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

- Delete
- Forward
- Forward and Delete

Before you begin

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

- Enabled and registered your email gateway with the Cisco SecureX server. For more information, see How to Integrate your Email Gateway with Cisco SecureX Threat Response, on page 2.
- 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 Cisco Secure Email Gateway 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 Remediating Messages in Mailboxes.

Procedure

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 MessageID, 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 Select the required message based on the investigation results using the corresponding **Cisco Message ID** or **Email MessageID** . For more information, see the Investigate topic in the Help section at https://visibility.amp.cisco.com/help/investigate.

Step 4 Click the pivot menu button next to the Cisco Message ID or Email MessageID 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.

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	4215XXXXXXXXXXXXXXXX-XXXXXXXXXXXX
Model	C100V
sIVAN	Email Gateway (for a smart license) or null (for a classic license)
Deployment	Cluster/Standalone.
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)

Statistics	Sample Data
Feature ID	a4deXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX

Related Topics

- Enabling CSN on Email Gateway, on page 12
- Disabling CSN on Email Gateway, on page 12

Enabling CSN on Email Gateway

Before you begin

Make sure that you enable and register your email gateway with the Cisco Cloud Service Portal. For more information, see How to Integrate your Email Gateway with Cisco SecureX Threat Response, on page 2.

Procedure

Step 1 Go to **Security Services** > **Cloud Service Settings**.

Step 2 Click **Edit Global Settings**.

Step 3 Check the **Enable** checkbox under Cisco Success Network.

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 Global Settings**.

Step 3 Uncheck the the **Enable** checkbox under Cisco Success Network.

Step 4 Submit and commit your changes.