Integrate with Cisco SecureX and Cisco Threat Response

This topic contains the following sections:

Integrating Your Appliance with Cisco SecureX and 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.

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

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

- View and send the web data from multiple appliances in your organization.
- Identify, investigate and remediate threats observed in the web reports and tracking.
- Block compromised URL or web traffic.
- 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 web policy.

You can access Cisco SecureX and Cisco Threat Response using the following URLs:

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

The Cisco Secure Web Appliance 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 Secure Web Appliance module, go to https://securex.us.security.cisco.com/settings/modules/availablehttps://xdr.us.security.cisco.com/administration/integrations, navigate to the module to integrate with Cisco SecureX and click **Learn More**.

When you integrate Secure Web Appliance with SecureX, it validates Secure Web Appliance's web tracking data. The transaction timeout (60 seconds) occurs due to the processing delay on Secure Web Appliance resulting an integration failure. Reduce the integration time limit from the default 30 days to 1 or 2 days for a successful integration. However, this reduction will impact the monitoring effectiveness on Secure Web Appliance.

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

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

	Do This	More Info
Step 1	Review the prerequisites.	Prerequisites, on page 3
Step 2	On your Secure Web Appliance, enable the Cisco SecureX or Cisco Threat Response integration.	Enable the Cisco SecureX or Cisco Threat Response Integration on your Cisco Secure Web 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 Secure Web Appliance, complete the Cisco SecureX or Cisco Threat Response registration.	Registering Cisco SecureX or Cisco Threat Response on Cisco Secure Web 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 Web Secirity Appliance Module.	For more information, go to https://securex.us.security.cisco.com/settings/modules/available, navigate to the required Secure Web 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 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)

Enable the Cisco SecureX or Cisco Threat Response Integration on your Cisco Secure Web Appliance

Procedure

Step 1 Log in to your appliance.

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

Step 3 Click **Edit Settings**.

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

Step 5 Choose the required Cisco SecureX or Cisco Threat Response server to connect your appliance to Cisco SecureX or Cisco 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.

What to do next

Register your appliance on Cisco SecureX or Cisco Threat Response. 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.

Registering Cisco SecureX or Cisco Threat Response on Cisco Secure Web Appliance

Procedure

Step 1 Go to **Network** > **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, on page 4

Registering Cisco Secure Web Appliance on Security Service Exchange (SSE) portal using Smart License

When you upgrade to AsyncOS 14.x, Cisco Cloud Services is automatically enabled if the appliance is already registered to Cisco Smart Software Manager. Follow the below steps to add your appliance to SSE portal.

Procedure

Step 1 Schedule a maintenance window.

Step 2 Go to **System Administration** > **Smart Software Licensing**.

Step 3 From the **Action** drop-down list, select **Deregister** and click **Go**.

Step 4 Delete any SWA entries from the SSE portal.

Step 5 Go to **Network** > **Cloud Service Settings**.

Step 6 Check the **Enable Cisco Cloud Services** checkbox.

Step 7 Click **Enable**.

Step 8 Submit and commit your changes.

Step 9 Paste the registration token.

Step 10 Click **Register**.

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 Secure Web Appliance 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 and Cisco Threat Response, on page 2.

After you have integrated your appliance with Cisco SecureX or Cisco Threat Response, you do not need to integrate your Cisco Security Management appliance with Cisco SecureX or Cisco Threat Response.

After successful registration of your appliance on Security Services Excange, add the Secure Web Appliance Web 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 Cloud Services Portal on Secure Web Appliance

Procedure

Step 1 Log in to your Secure Web Appliance.

Step 2 Select **Network** > **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 Secure Web Appliance 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.

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

What to do next

Register your Secure Web Appliance 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 Secure Web Appliance with Cisco Cloud Services Portal

Procedure

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

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

Note To register your Secure Web Appliance with or the Cisco Cloud Services portal using the CLI, use the `cloudserviceconfig` command.

You cannot disable or deregister Cisco Cloud Services if smart licensing is registered on your appliance.

Performing Threat Analysis using Cisco SecureXRibbon

Note When you downgrade from AsyncOS 14.0 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 AsyncOS 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 appliance. For more information, see Understanding the Web Reporting Pages on the New 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, 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 appliance. For more information, see Accessing the Cisco SecureX Ribbon, on page 7.

Procedure

Step 1 Log in to the new web interface of your appliance. For more information, see Understanding the Web Reporting Pages on the New Web Interface.

Step 2 Navigate to the **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, Secure Endpoint) 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.