



Integrating with Cisco Threat Response

This chapter contains the following sections:

- [Integrating the Appliance with Cisco Threat Response, on page 1](#)
- [Performing Threat Analysis using Casebooks, on page 3](#)

Integrating the Appliance with Cisco Threat Response

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

- View the email reporting, message tracking, and web tracking data from multiple appliances in your organization.
- Identify, investigate and remediate threats observed in the email reports, message tracking, and web tracking.
- 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.



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

To integrate your appliance with Cisco Threat Response, you need to register your appliance with Cisco Threat Response.

You can access Cisco Threat Response using any one of the following URLs:

- <https://visibility.amp.cisco.com>
- <https://visibility.eu.amp.cisco.com/>



Note If you access Cisco Threat Response using a regional URL - <https://visibility.apjc.amp.cisco.com> the Cisco Threat Response integration with your appliance is not currently supported.

Before you begin

- Make sure that you create a user account in Cisco Threat Response with admin access rights. To create a new user account, go to Cisco Threat Response login page using the following URL - <https://visibility.amp.cisco.com> and click **Create a Cisco Security account** in the login page. If you are unable to create a new user account, contact Cisco TAC for assistance.
- Make sure that you enable Cisco Threat Response integration on the Cisco Security Services Exchange (SSE) portal. For more information, go to <https://securex.us.security.cisco.com/settings/modules/available>, navigate to the module to integrate with Cisco Threat Response, click **Add New Module**, and see the instructions on the page.
- Make sure that you open HTTPS (In and Out) 443 port on the firewall for the following FQDNs to register your appliance with Cisco Threat Response:
 - api-sse.cisco.com (applicable for Americas users only)
 - api.eu.sse.itd.cisco.com (applicable for European Union (EU) users only)

For more information, see [Firewall Information](#).

-
- Step 1** Log in to your appliance.
- Step 2** Select **Networks > Cloud Service Settings**.
- Step 3** Click **Edit Settings**.
- Step 4** Check **Enable**.
- Step 5** Choose the required Cisco Threat Response server to connect your appliance to Cisco Threat Response.
- Step 6** Submit and commit your changes.
- Step 7** Navigate back to the Cloud Service Settings page after few minutes to register your appliance with Cisco Threat Response.
- Step 8** Obtain a registration token from Cisco Threat Response to register your appliance with 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 Threat Response, click **Add New Module**, and see the instructions on the page.
- Step 9** Enter the registration token obtained from Cisco Threat Response and click **Register**.
- Step 10** Add your appliance as an integration module to 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 Threat Response, click **Add New Module**, and see the instructions on the page.
-

What to do next

After you add your appliance as an integration module in Cisco Threat Response, you can view the email reporting, message tracking, and web tracking information from your appliance in 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 Threat Response, click **Add New Module**, and see the instructions on the page.



Note To deregister your appliance connection from Cisco Threat Response, click **Deregister** in the Cloud Services Settings page in your appliance.

Performing Threat Analysis using Casebooks

The casebook and pivot menu are widgets available in Cisco Threat Response.

Casebook - It is used to record, organize, and share sets of observables of interest primarily during an investigation and threat analysis. You can use a casebook to get the current verdicts or dispositions on the observables. For more information, see the Cisco Threat Response documentation at <https://visibility.amp.cisco.com/#/help/casebooks>.

Pivot Menu - It is used to pivot an observable to a new case, an existing case, or to other devices registered in Cisco Threat Response (for example, AMP for Endpoints, Cisco Umbrella, Cisco Talos Intelligence, and so on) to investigate for threat analysis. For more information, see the Cisco Threat Response documentation at <https://visibility.amp.cisco.com/#/help/pivot-menus>.

The Email Security appliance now includes the casebook and pivot menu widgets. You can perform the following actions in your appliance using the casebook and pivot menu widgets:

- Add an observable to a casebook to investigate for threat analysis.
- Pivot an observable to a new case, an existing case, or other devices registered in Cisco Threat Response (for example, AMP for Endpoints, Cisco Umbrella, Cisco Talos Intelligence, and so on) to investigate for threat analysis.

The following is a list of observables supported for this release:

- IP addresses
- Domains
- URLs
- File Hashes (SHA-256 only)



Note

- The pivot menu widget is positioned next to the observables in the email reporting pages of your appliance.
- The casebook widget is positioned at the bottom-right corner of the email reporting pages of your appliance.

Related Topics

- [Obtaining Client ID and Client Password Credentials, on page 4](#)
- [Adding Observable to Casebook for Threat Analysis, on page 5](#)

Obtaining Client ID and Client Password Credentials

You need the client ID and client password to access the casebook and pivot menu widgets on your appliance.

Before you begin

Make sure that you meet all the prerequisites mentioned in the ‘Before you begin’ section of [Integrating the Appliance with Cisco Threat Response, on page 1](#)

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

Step 2 Click the **Casebook**  button.

Step 3 Add a new API Client.

a) Click the **Threat Response API Clients** link.

When you click on the Threat Response API Clients link, it redirects you to Cisco Threat Response login page.

b) Log in to Cisco Threat Response.

c) Click **Add API Credentials**.

d) Enter the name of your appliance (for example, ‘Email_Security_Appliance’) as the client name.

e) Select the following scopes to provide full access to the casebook and pivot menu widgets:

- Casebook
- Enrich
- Private Intelligence
- Response
- Inspect

- Note**
- If you want to access the casebook widget only, select the following scopes - casebook, private intelligence, and inspect.
 - If you want to access the pivot menu widget only, select the following scopes - enrich and response.

f) Click **Add New Client**.

g) Copy the client ID and client password to the clipboard.

Note Make sure that you note the client ID and client password before you close the ‘Add New Client’ dialog box.

h) Click **Close**.

Note If you want to add a new API client, you do not need to delete the existing API client.

Step 4 Enter the client ID and client password obtained in Step 3 in the ‘Login to use Casebook/Pivot Menu’ dialog box in your appliance.

Step 5 Select the required Cisco Threat Response server in the ‘Login to use Casebook/Pivot Menu’ dialog box.

Step 6 Click **Authenticate**.

Note If you want to edit the client ID, client password, and Cisco Threat Response server, right-click on the Casebook



button and add the details.

What to do next


Add an observable to a casebook to investigate for threat analysis. See [Adding Observable to Casebook for Threat Analysis, on page 5](#)

Adding Observable to Casebook for Threat Analysis

Before you begin



Make sure that you obtain the client ID and client password to access the casebook and pivot menu widgets on your appliance. For more information, see [Obtaining Client ID and Client Password Credentials, on page 4](#).


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


Step 2 Navigate to the Email Reporting page, click on the pivot menu  button next to the required observable (for example, schemas.microsoft.com) and click **Add to New Case** or **Add to Current Case**.

The screenshot shows the Cisco Email Security Appliance interface. The top navigation bar includes the Cisco logo, 'Email Security Appliance', and tabs for 'Monitoring' and 'Tracking'. Below the navigation, there are sections for 'Reports / URL Filtering: Incoming' and 'URL Filtering' with 'Incoming' and 'Outgoing' tabs. The main content area is titled 'Top URL Spam Messages' and lists several URLs. A dropdown menu is open for 'schemas.microsoft.com', showing a count of '3' and a list of actions: 'Clean URL', 'Copy to Clipboard', 'Add to Current Case', 'Add to New Case', 'AMP for Endpoints' (with a search option), 'Talos Intelligence' (with a search option), 'Umbrella (investigate only)' (with a search option), and 'Threat Response' (with an 'Investigate this URL' option).

Note

- Use the drag and drop  button next to the observable to drag and drop the observable into an existing case.
- 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 Click the **Casebook**  button to 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.

Step 5 Click **Investigate this Case** to investigate the observable for threat analysis. For more information, see the Cisco Threat Response documentation at <https://visibility.amp.cisco.com/#/help/introduction>.
