

Cisco Threat Response (CTR) and ESA Integration

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Step 1. Navigate to Network > Cloud Service Settings](#)

[Step 2. Click on Edit Settings](#)

[Step 3. Select the checkbox Enable and the Threat Response Server](#)

[Step 4. Submit and Commit changes](#)

[Step 5. Log into the CTR portal and generate the Registration Token requested in the ESA](#)

[Step 6. Paste the Registration Token \(generated from CTR portal\) in the ESA](#)

[Step 7. Verify that your ESA device is in the SSE portal](#)

[Step 8. Navigate to the CTR portal and add a new ESA module](#)

[Verify](#)

[Troubleshoot](#)

[ESA device is not shown in the CTR portal](#)

[CTR investigation is not showing data from the ESA](#)

[ESA is not requesting the Registration token](#)

[Registration failed because of an invalid or expired token](#)

[Related Information](#)

Introduction

This document describes the process to Integrate Cisco Threat Response (CTR) with Email Security Appliance (ESA) and how to verify this in order to perform some CTR investigations.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Threat Response
- Email Security Appliance

Components Used

The information in this document is based on these software and hardware versions:

- CTR Account
- Cisco Security Services Exchange
- ESA C100V on software version 13.0.0-392

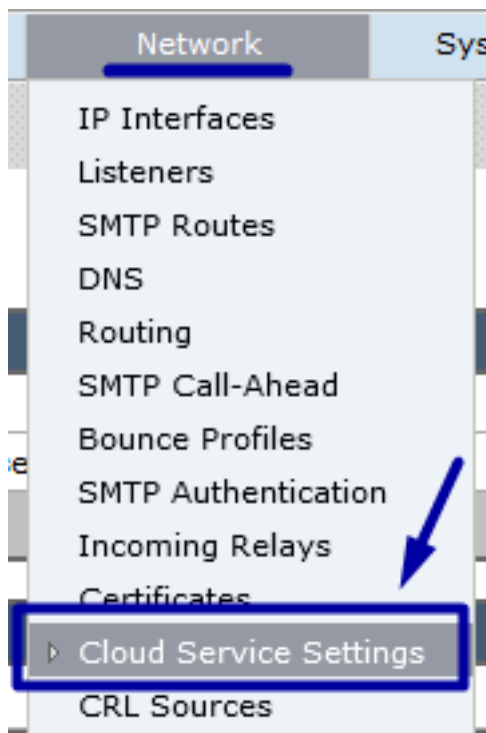
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

In order to configure the Integration CTR and ESA, log in to your Email Security Virtual Appliance and follow these quick steps:

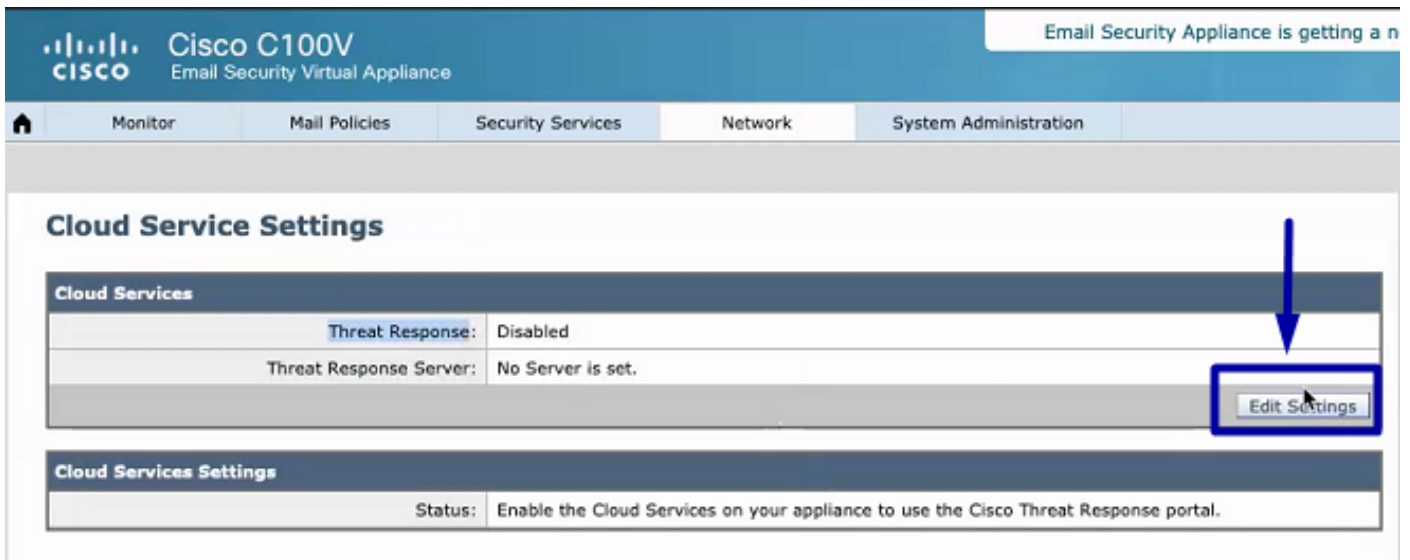
Step 1. Navigate to Network > Cloud Service Settings

Once in the ESA, navigate to the context menu Network > Cloud Service Settings, in order to see the currently Threat Response Status (Disabled / Enabled) as shown in the image.



Step 2. Click on Edit Settings

Until now Threat Response feature in the ESA is disabled, in order to enable the feature, click on Edit Settings as shown in the image:



Step 3. Select the checkbox Enable and the Threat Response Server

Select the checkbox Enable, then choose the Threat Response Server, please see the image below:

Cloud Service Settings



Note: The default selection for Threat Response Server URL is AMERICAS (api-sse.cisco.com). For EUROPE businesses, click the drop-down menu and choose EUROPE (api.eu.sse.itd.cisco.com)

Step 4. Submit and Commit changes

It is required to submit and commit the changes, in order to save and apply any change. Now if the ESA interface is refreshed a Registration token is requested in order to register the Integration, as shown in the image below.

Note: You can see a Success message: Your changes have been committed.



Cloud Service Settings

Success — Your changes have been committed.

Cloud Services	
Threat Response:	Enabled
Threat Response Server:	AMERICAS (api-sse.cisco.com)
Edit Settings	

Cloud Services Settings	
Status:	The Cisco Cloud Service is busy. Navigate back to this page after some time to check the appliance status.

Cloud Service Settings

Cloud Services	
Threat Response:	Enabled
Threat Response Server:	AMERICAS (api-sse.cisco.com)
Edit Settings	

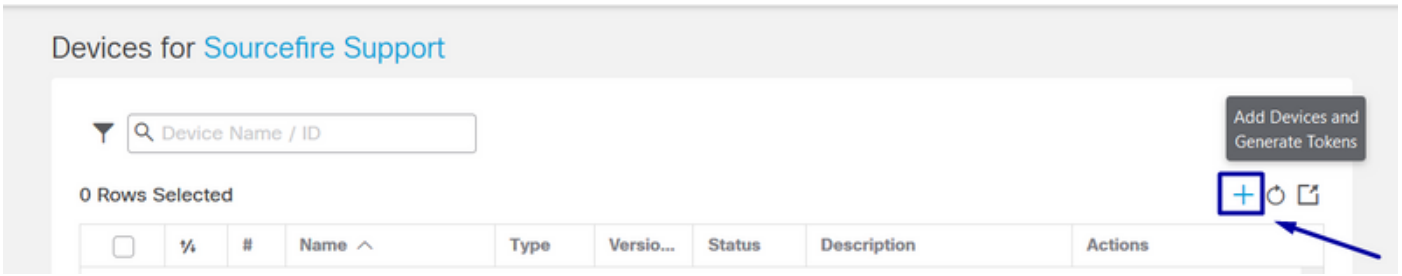
Cloud Services Settings	
Registration Token: ?	<input type="text"/>
Register	

Step 5. Log into the CTR portal and generate the Registration Token requested in the ESA

1.- Once in the CTR portal, navigate to Modules > Devices > Manage Devices, please see the next image.

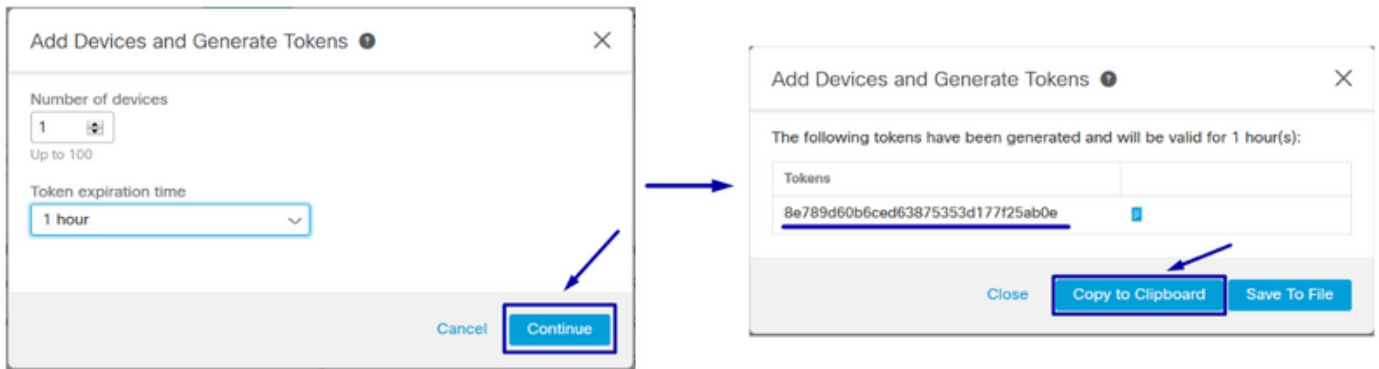
The screenshot shows a web browser at the URL <https://visibility.amp.cisco.com/settings/devices>. The navigation menu includes Threat Response, Investigate, Snapshots, Incidents (Beta), Intelligence, and Modules. The 'Modules' menu item is highlighted with a blue box and an arrow. Below the navigation, the breadcrumb 'Settings > Devices' is shown. The 'Devices' section has a blue sidebar with 'Settings', 'Your Account', 'Devices', 'API Clients', and '> Modules'. The 'Devices' item in the sidebar is highlighted with a blue box and an arrow. In the main content area, the 'Devices' title is followed by 'Manage Devices' and 'Reload Devices' buttons. The 'Manage Devices' button is highlighted with a blue box and an arrow. Below the buttons is a table with columns 'Name' and 'Type'.

2.- Manage Devices link redirects you to the Security Services Exchange (SSE), once there, click on the icon Add Devices and Generate Tokens as shown in the image.



3.- Click on Continue in order to generate the Token, once the Token is generated, click on Copy to Clipboard, as shown in the image.

Tip: You can select the number of devices to add (from 1 and up to 100) and also select the Token expiration time (1hr, 2hrs, 4hrs, 6hrs, 8hrs, 12hrs, 01 days, 02 days, 03 days, 04 days and 05 days).



Step 6. Paste the Registration Token (generated from CTR portal) in the ESA

Once the Registration Token is generated, paste it in the Cloud Services Settings section in the ESA, as the image below.

Note: You can see a Success message: A request to register your appliance with the Cisco Threat Response portal is initiated. Navigate back to this page after some time to check the appliance status.

Cloud Service Settings



Cloud Service Settings

Success — A request to register your appliance with the Cisco Threat Response portal is initiated. Navigate back to this page after some time to check the appliance status.

Cloud Services

Threat Response:	Enabled
Threat Response Server:	AMERICAS (api-sse.cisco.com)

[Edit Settings](#)

Cloud Services Settings

Status:	The appliance registration is in progress. Navigate back to this page after some time to check the appliance status.
---------	--

Step 7. Verify that your ESA device is in the SSE portal

You can navigate to the SSE portal (CTR > Modules > Devices > Manage Devices), and in the Search Tab look at your ESA device, as shown in the image.

Security Services Exchange Audit Log Brenda Marquez

Devices for Sourcefire Support

Search:

0 Rows Selected

	%	#	Name ^	Type	Versio...	Status	Description	Actions
<input type="checkbox"/>	<input type="checkbox"/>	1	esa03.mex-amp.inl...	ESA	13.0.0	Registered	ESA	Edit Delete Refresh

ID: 874141f7-903f-4be9-b14e-45a7f... IP Address: 127.0.0.1 Connector Version: 1.3.34
Created: 2020-05-11 20:41:05 UTC

Step 8. Navigate to the CTR portal and add a new ESA module

1.- Once you are in the CTR portal, navigate to Modules > Add New Module, as shown in the image.

Threat Response Investigate Snapshots Incidents Intelligence **Modules** Brenda Marquez

Settings > Modules

Modules

Intelligence within Cisco Threat Response is provided by modules, which can also enable response capabilities. [Click here to view all the available modules.](#)

Your Configurations

[Add New Module](#)

AMP for Endpoints
AMP for Endpoints prevents threats at the point of entry, by identifying and halting advanced threats before they reach your endpoints. [Edit](#) [Learn More](#)

2.- Choose the module type, in this case, the module is an Email Security Appliance module as the image below.

Settings

Your Account

Devices

API Clients

▼ Modules

Available Modules

Users

Available Modules

Select a module you would like to add, or [click here to learn more](#) about modules configuration.



AMP for Endpoints

AMP for Endpoints prevents threats at the point of entry, by identifying and halting advanced threats before they reach your endpoints.

[Add New Module](#)

[Learn More](#) · [Free Trial](#)



Email Security Appliance

The Cisco Email Security Appliance (ESA) provides advanced threat protection capabilities to detect, block, and remediate threats faster, prevent data loss, and secu...

[Add New Module](#)

[Learn More](#)

3.- Enter the fields: Module Name, Registered Device (select the one previously registered) and Request Timeframe (days), and Save, as shown in the image.

Threat Response Investigate Snapshots Incidents Beta Intelligence Modules ? ⚙️ Brenda Marquez ▼

Settings > Modules > Available Modules > Email Security Appliance > Add New Module

Settings

Your Account

Devices

API Clients

▼ Modules

Available Modules

Users

Add New Email Security Appliance Module

Module Name*

Registered Device*

esa03.mex-amp.inlab
Type ESA
ID 874141f7-903f-4be9-b14e-45a7f34a2032
IP Address 127.0.0.1

Request Timeframe (days)

[Save](#) [Cancel](#)

Quick Start [Help](#)

When configuring Email Security Appliance (ESA) integration, you must first enable the integration in ESA. You then enable Threat Response in Security Services Exchange, add the device and register it. After this is completed, you add the ESA module.

Prerequisite: ESA running minimum AsyncOS 13.0.0-314 (LD) release.

Note: Customers with multiple ESAs reporting to an SMA can use the SMA Module configuration for Email Security. Customers that do not have an SMA, can use the ESA Module for integration.

- In ESA, navigate to **Networks > Cloud Service Settings > Edit Settings**, enable integration and confirm that the ESA is ready to accept a registration token.
- Click the **Settings** icon (gear) and then click **Devices > Manage Devices** to be taken to Security Services Exchange.
- Enable **Cisco Threat Response** integration on the **Cloud Services** tab, and then click the **Devices** tab and click the + icon to add a new device.
- Specify the token expiration time (the default is 1 hour), and click **Continue**.
- Copy the generated token and confirm the device has been created.
- Navigate to your ESA (**Network > Cloud Service Settings**) to insert the token, and then click **Register**. Confirm successful registration by reviewing the status in Security Services Exchange and confirm the ESA is displayed on the **Devices** page.
- Complete the **Add New Email Security Appliance Module** form:
 - Module Name** - Leave the default name or enter a name that is meaningful to you.
 - Registered Device** - From the drop-down list, choose the device you registered in Security Services Exchange.
 - Request Timeframe (days)** - Enter the timeframe (in days) for querying the API endpoint (default is 30 days).
- Click **Save** to complete the ESA module configuration.

Verify

In order to verify the CTR and ESA Integration, you can send a test email, which you can also see it from your ESA, navigate to Monitor > Message Tracking, and find the test email. In this case, I filtered by Email Subject as the image below.

The screenshot displays the Cisco C100V Email Security Virtual Appliance interface. At the top, the navigation menu includes Monitor, Mail Policies, Security Services, Network, and System Administration. The main content area is titled "Message Tracking" and contains a search form. The search criteria are: Envelope Sender (Begins With), Envelope Recipient (Begins With), and Subject (Begins With) set to "test test". The Message Received section is selected, with "Last Day" chosen. The time range is from 05/13/2020 13:00 to 05/14/2020 13:42 (GMT +00:00). A blue arrow points to the "Search" button. Below the search form, the results section shows one item: "1 14 May 2020 13:23:57 (GMT +00:00) MID: 8". The email details are: SENDER: mgmt01@cisco.com, RECIPIENT: testingBren@cisco.com, SUBJECT: test test, and LAST STATE: Message 8 to testingBren@cisco.com received remote SMTP response 'ok: Me:'. The interface also shows "Generated: 14 May 2020 13:42 (GMT +00:00)" and "Export All... | Export..." options.

Now, from the CTR portal, you can perform an Investigation, navigate to Investigate, and use some email observables, as shown in the image.

The screenshot shows the Cisco Threat Response Investigate interface. At the top, there are navigation tabs: Threat Response, Investigate (selected), Snapshots, Incidents, Intelligence, and Modules. The user is Brenda Marquez. The interface displays search filters: 1 Target, 1 Observable, 0 Indicators, 0 Domains, 0 File Hashes, 0 IP Addresses, 0 URLs, and 1 Module. The search query is `email_subject:"test test"`. The Relations Graph shows a central node for 'Email Subject test test' connected to 'Target Email', 'Email Subject test test', 'Cisco Message ID 8', and 'Email Address mgmt01@cisco.c...'. The Sighting chart shows 1 sighting in the environment. The Sighting table lists one sighting from the 'esa03' module, observed 9 hours ago, with a description of an incoming message.

Tip: You can use the same syntax for other email observables as follows in the image.

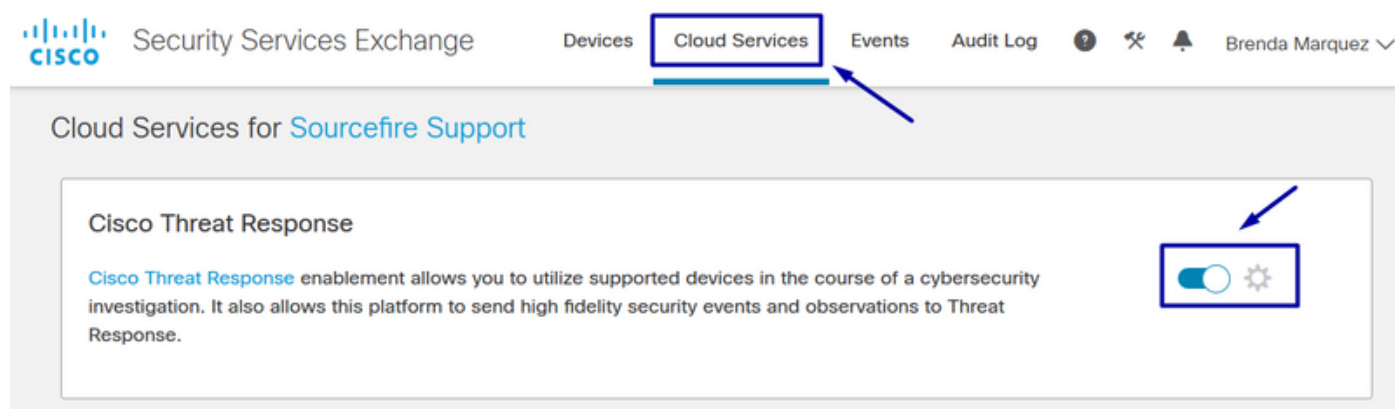
IP address	<code>ip:"4.2.2.2"</code>	Email subject	<code>email_subject:"Invoice Due"</code>
Domain	<code>domain:"cisco.com"</code>	Cisco Message ID (MID)	<code>cisco_mid:"12345"</code>
Sender email address	<code>email:"noreply@cisco.com"</code>	SHA256 filehash	<code>sha256:"sha256filehash"</code>
Email message header	<code>email_messageid:"123-abc-456@cisco.com"</code>	Email attachment file name	<code>file_name:"invoice.pdf"</code>

Troubleshoot

If you are a CES customer or if you manage your ESA devices via an SMA, you can only connect to Threat Response via your SMA. Please ensure your SMA runs AsyncOS 12.5 or higher. If you do not manage your ESA with an SMA and you integrate the ESA directly, ensure it is at AsyncOS version 13.0 or higher.

ESA device is not shown in the CTR portal

If your ESA device is not shown in the drop-down Registered Device while the ESA module is added in the CTR portal, please ensure to have enabled CTR in SSE, in CTR navigate to Modules > Devices > Manage Devices, then in SSE portal navigate to Cloud Services and enable CTR, as the image below:



CTR investigation is not showing data from the ESA

Please ensure that:

- The syntax of the investigation is correct, the email observables are shown above in the Verify Section.
- You have selected the proper Threat Response Server or Cloud (Americas/Europe).

ESA is not requesting the Registration token

Please ensure to commit the changes, when Threat Response has been enabled, otherwise, the changes won't be applied to the Threat Response section in the ESA.

Registration failed because of an invalid or expired token

Please ensure that the token is generated from the correct Cloud:

If you use Europe (EU) Cloud for ESA, generate the token from:

<https://admin.eu.sse.itd.cisco.com/>

If you use Americas (NAM) Cloud for ESA, generate the token from:

<https://admin.sse.itd.cisco.com/>

Also, remember that the Registration token has an expiration time (select the most convenient time to complete the Integration in time).

Related Information

- You can find the information contained in this article in the [Cisco Threat Response and ESA Integration](#) video.
- [Technical Support & Documentation - Cisco Systems](#)