

Quick Start Guide for Email Security

Start your first investigation today with Cisco Threat Response

One of the newest ways to take full advantage of your email security investment is by using Cisco Threat Response, which dramatically cuts the time and manual effort required to investigate and remediate cybersecurity incidents.

Start investigating with Threat Response today in three steps.

Step 1: Access Cisco Threat Response

If you own Email Security, Advanced Malware Protection (AMP) for Endpoints, Cisco Umbrella™, or Threat Grid, you are entitled to a free Threat Response account. To get your account, go to your login screen at [U.S. cloud](#), [EU cloud](#), or [Asia Pacific cloud*](#).

If you don't own any of these products, you can sign up for a free trial of these products, which will allow you to also try Threat Response: [Umbrella](#), [AMP for Endpoints](#), [Email Security](#), or [Threat Grid](#).



- A.** If you have an AMP or Threat Grid account, use your existing credentials to log in. If someone in your company has an account, ask them to send you an invitation from the Users page. If these cases apply to you, You can go directly to Step 2 (page 6). If these cases don't apply to you, continue to step B.
- B.** Click “Create a Cisco Security Account” to create your account and get started (option available on the U.S. cloud only at this time).


Contents

Step 1: Access Cisco Threat Response

Step 2: Configure modules




Step 3: Start investigating

C. Add your information and click “Create Account.” Use your business email address (personal email addresses are not accepted).



Security

The Cisco Security account is a single destination for managing multiple applications within the Cisco Security portfolio.

-  AMP for Endpoints
-  Threat Grid
-  Threat Response and more...

Account Registration

First name

Last name

Organization name

Email

Password

- be between 8 and 50 characters.
- contain at least one upper case, one lower case, and one numeric character.
- contain at least one of these following special characters: `!#$%&'()*+,-./:;<=>@[\]^_`{|}~`
- follow above rules or be a unicode password (8 characters minimum).

Password confirmation

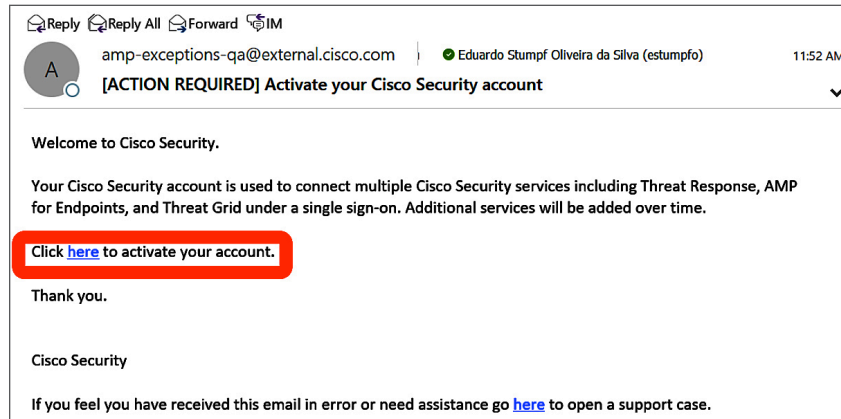
Contents

Step 1: Access Cisco Threat Response

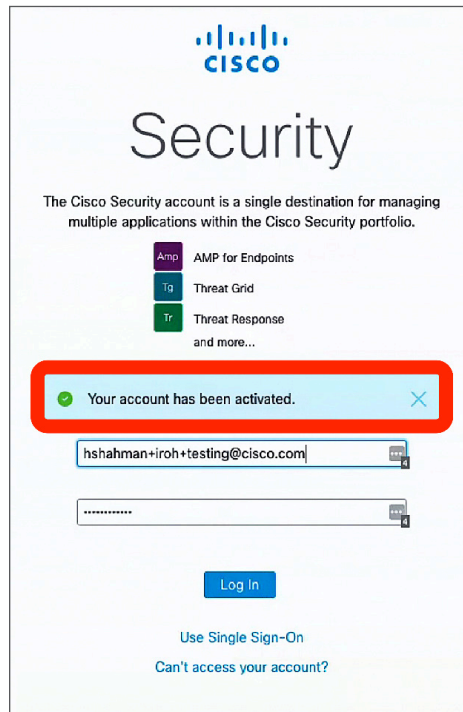
Step 2: Configure modules

Step 3: Start investigating

D. After the “Account Registration Complete” message, check your email as follows. On the email, click on the activation link to verify ownership of the account.



E. Your account is registered. Log in with the password you created in step C.



Contents

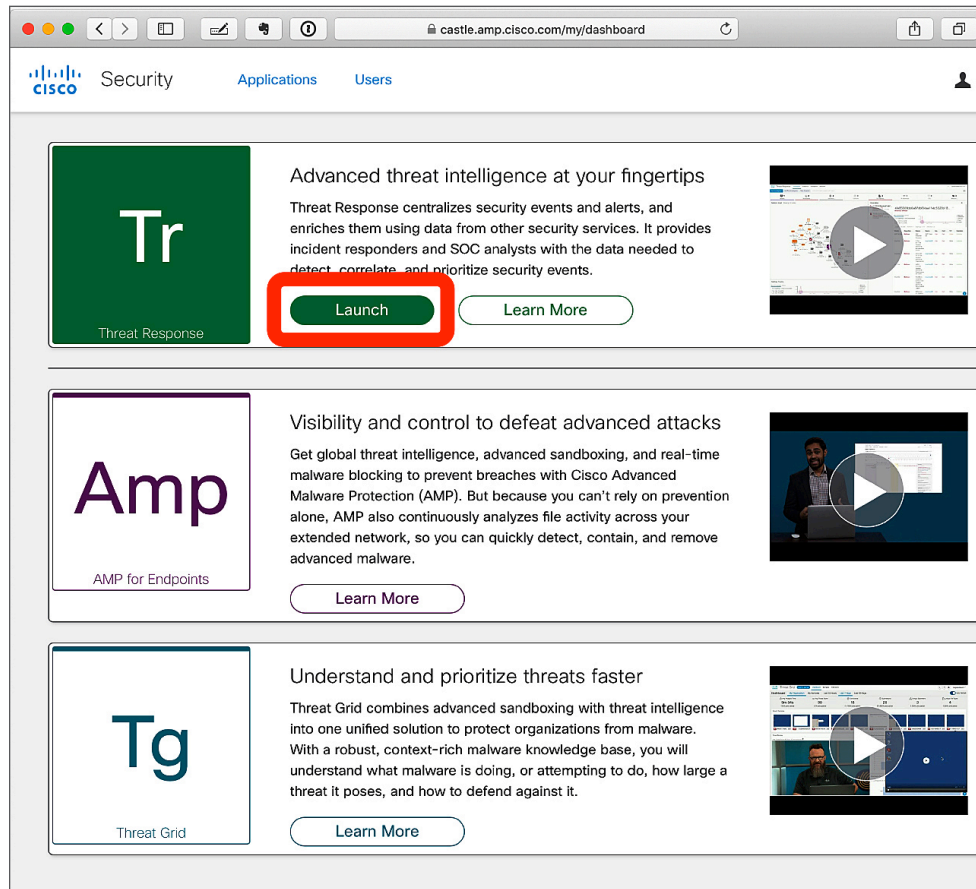
Step 1: Access Cisco Threat Response

Step 2: Configure modules

Step 3: Start investigating

F. At the Cisco Security Dashboard, launch Threat Response. On first login, you'll be asked to review and agree to the cloud subscription agreement. Once you accept the agreement, click on "Launch".

Besides, if at any time you want to add users in your organization, you can do so by clicking on "users" at the top of the page.



Contents

Step 1: Access Cisco Threat Response

Step 2: Configure modules

Step 3: Start investigating

- G.** You are now in Threat Response. Under “Connect a Device,” click on Connect. Step 2 will guide you to configure your Email Security Appliance (ESA), or Security Management Appliance (SMA) device as a new module.

Account Activation

To start using Threat Response, please configure your first product to activate your account.

If you are an AMP for Endpoints or Threat Grid customer, please ask that account administrator to invite you to their organization to get started.

Configure Umbrella or
AMP for Endpoints

Configure

Connect a Device such
as SMA Email

Connect

Contents

[Step 1: Access Cisco Threat Response](#)

[Step 2: Configure modules](#)

[Step 3: Start investigating](#)

Step 2: Configure modules

Configuring at least one module is required to activate your account with Threat Response. Besides, the more modules you configure, the more powerful Threat Response becomes.

Before getting started:

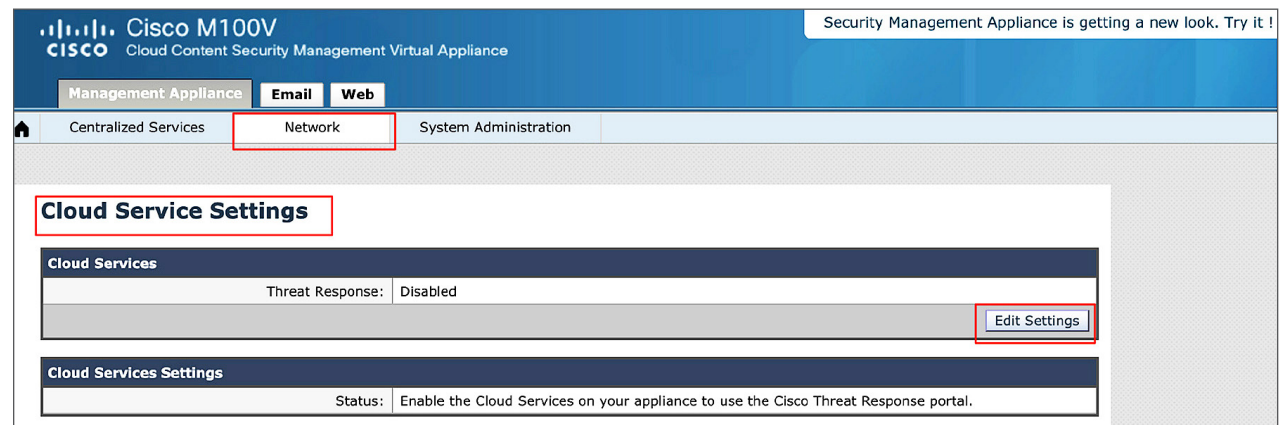
This step will focus on the configuration of the appropriate module for your Email Security product. The steps are slightly different if you have independently managed ESA devices, or if you are using SMA. Those differences are called out in the relevant steps. If you have SMA, in any step that directs to “your ESA or SMA”, perform those steps only on your SMA. If you have CES, follow the SMA directions.

If you are a CES customer or if you manage your ESA devices via an SMA, you will be only be connecting to Threat Response using your SMA. Make sure your SMA is running AsyncOS 12.5 or higher.

If you do not manage your ESA with an SMA and are integrating the ESA directly, make sure it is at AsyncOS version 13.0 or higher.

A. Let’s start by linking your ESA or SMA to Cisco Services Exchange. Don’t close the tab from Step 1, which we’ll come back to later in this guide.

Log-in to your ESA or SMA to prepare linking it to Cisco Services Exchange. Go to Network > Cloud Service Settings > Edit Settings to enable Threat Response integration.



The screenshot displays the Cisco M100V Cloud Content Security Management Virtual Appliance interface. At the top, there is a navigation bar with tabs for 'Management Appliance', 'Email', and 'Web'. Below this, a secondary navigation bar includes 'Centralized Services', 'Network', and 'System Administration'. The 'Network' tab is active, and within it, 'Cloud Service Settings' is selected. The main content area shows a table for 'Cloud Services' with a row for 'Threat Response' set to 'Disabled' and an 'Edit Settings' button. Below this is a section for 'Cloud Services Settings' with a 'Status' field set to 'Enable the Cloud Services on your appliance to use the Cisco Threat Response portal.'

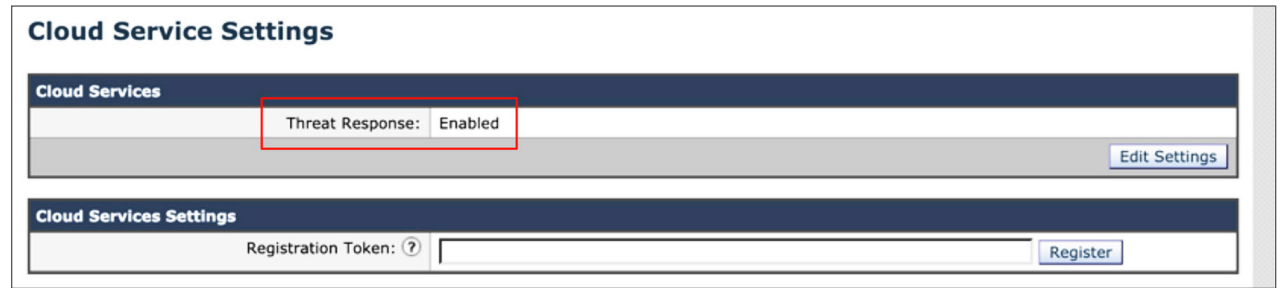
Contents

Step 1: Access Cisco Threat Response

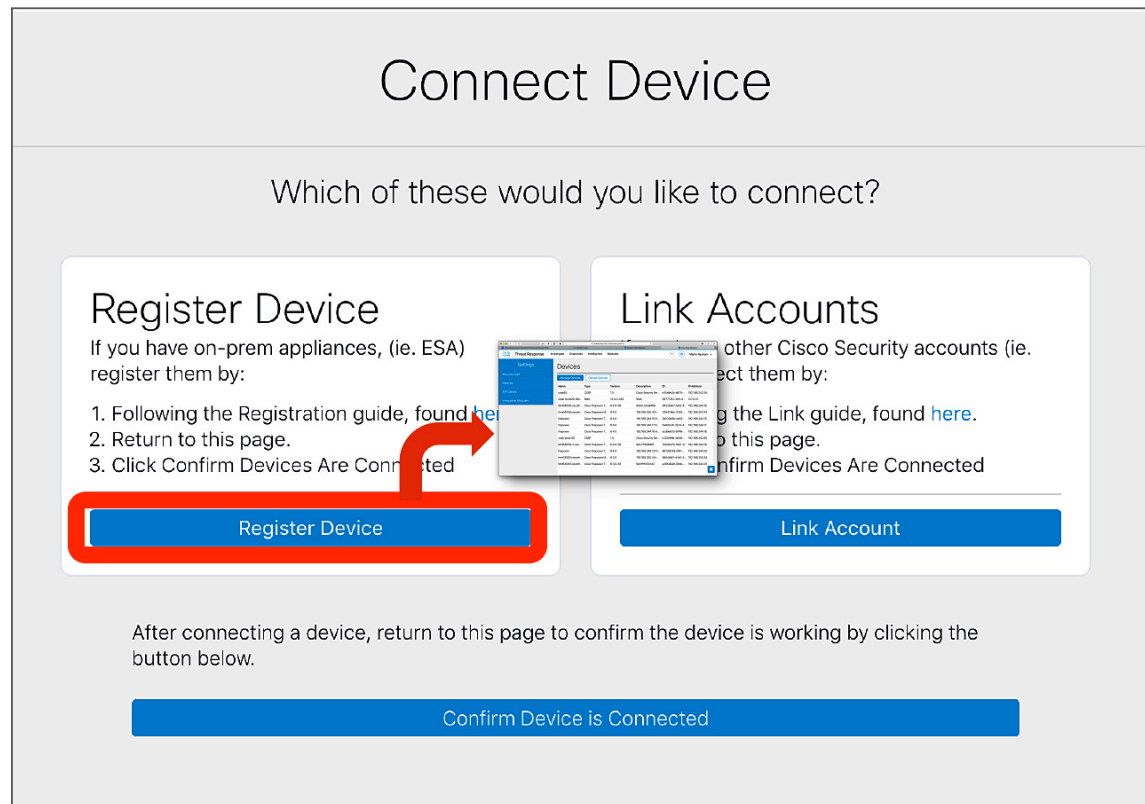
Step 2: Configure modules

Step 3: Start investigating

B. Confirm Threat Response has been enabled and that the device is ready to accept a registration token. Your device is now ready to be linked to Threat Response.



C. If you've completed Step 1, you should have a tab open with the screen below. Select Register Device. A new tab will open where you can connect your device. Come back to this tab to confirm the device is connected.



Contents

Step 1: Access Cisco Threat Response

Step 2: Configure modules

Step 3: Start investigating

D. Click “Manage Devices” and log-in again to add your ESA or SMA. You may need to enable your browser to allow popups from <https://visibility.amp.cisco.com> or your regional portal.

Name	Type	Version	Description	ID	IP Address
cssp55	CSSP	1.0	Cisco Security Ser...	e35a9e2b-d875-...	192.168.242.55
sma1.hc2926-99.i...	SMA	12.0.0-452	SMA	837773f2-3f0f-4...	127.0.0.1
fdm64056.ciscoth...	Cisco Firepower T...	6.4.0-56	9AACJUQMOK	84228eb7-fa02-4...	192.168.244.16
fmc64056.ciscoth...	Cisco Firepower M...	6.4.0	192.168.250.43 f...	239434bc-5192-...	192.168.250.43
firepower	Cisco Firepower T...	6.4.0	192.168.244.15 fir...	0e533b5b-ec63-...	192.168.244.15
firepower	Cisco Firepower T...	6.4.0	192.168.244.17 fir...	5a9d7e3f-32c0-4...	192.168.244.17
firepower	Cisco Firepower T...	6.4.0	192.168.244.18 fir...	dcd9e633-8746-...	192.168.244.18
cssp-prod-60	CSSP	1.0	Cisco Security Ser...	b122e89d-b046-...	192.168.242.60
fdm64056-2.cisc...	Cisco Firepower T...	6.4.0-56	9ALPT9GB9RT	7b0d2a79-16b7-4...	192.168.244.19
firepower	Cisco Firepower T...	6.4.0	192.168.244.20 fir...	867d3039-0f61-...	192.168.244.20
fmc63083.ciscoth...	Cisco Firepower M...	6.3.0	192.168.250.44 f...	9654fb61-d7a0-4...	192.168.250.44
fdm63083.ciscoth...	Cisco Firepower T...	6.3.0-83	9A5HH0SXXAT	a385d0a8-08cb-...	192.168.244.25

E. In Cisco Services Exchange, add a new device or devices.

Devices for [redacted]

Filter by Status: --Show All--

[Refresh] [Add (+)] [Search: Device Name / ID]

	1/4	#	Name	Type	Version	Status	Description	Actions
<input type="checkbox"/>	>	1	[redacted]	[redacted]	[redacted]	Registered	[redacted]	[Edit] [Delete] [Refresh]

Contents

Step 1: Access Cisco Threat Response

Step 2: Configure modules

Step 3: Start investigating

F. Specify the token expiration time. The default is 1 hour.

Add Devices ✕

Number of devices

Up to 100

Token expiration time


1 hour

Cancel Generate Tokens

G. Copy the token generated. You will use this token on your ESA or SMA for registration.

Add Devices and Generate Tokens ✕

The following tokens have been generated and will be valid for 1 hour(s): ⓘ

Tokens
 ⓘ

Close Copy to Clipboard Save To File

Contents

Step 1: Access Cisco Threat Response

Step 2: Configure modules

Step 3: Start investigating

H. Confirm the device has been created.

Cisco Services Exchange

Devices Cloud Services Events

Devices for [redacted] ?

Filter by Status: --Show All--

	1/4	#	Name	Type	Version	Status	Description	Actions
<input type="checkbox"/>	>	1	New Device - 154869981141			Created		

I. Navigate to your ESA or SMA and insert the token and click Register.

Cloud Service Settings

Cloud Services

Threat Response: Enabled [Edit Settings](#)

Cloud Services Settings

Registration Token: ? [Register](#)

J. Confirm successful registration by reviewing the status in the Cisco Security Services Exchange. It should show as registered with the actual device name populated, IP address, and connector version.

Cisco Services Exchange

Devices Cloud Services Events

Devices for [redacted] ?

Filter by Status: --Show All--

	1/4	#	Name	Type	Version	Status	Description	Actions
<input type="checkbox"/>	>	1	[redacted]	[redacted]	[redacted]	Registered	[redacted]	
<input type="checkbox"/>	∨	2	[redacted]	SMA	12.0.0-322	Registered	SMA	

ID: [redacted] IP Address: [redacted] Connector Version: 1.3.34

Created: Jan 9, 2019, 4:32 PM

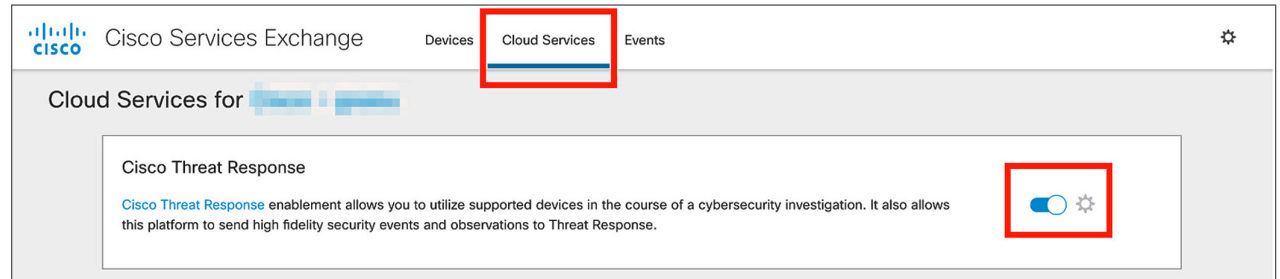
Contents

Step 1: Access Cisco Threat Response

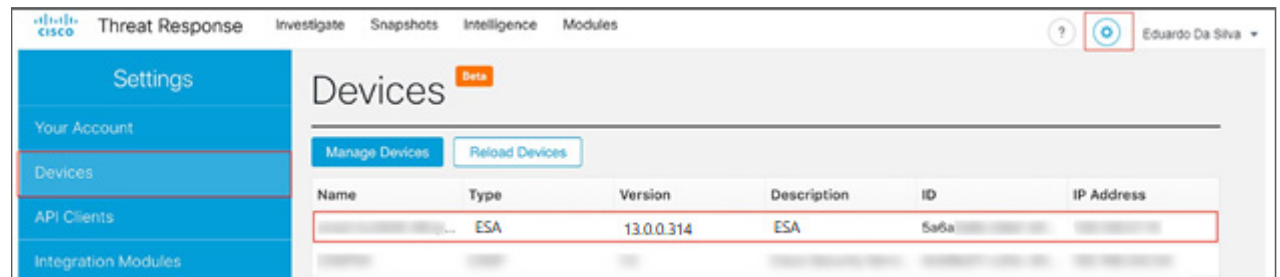
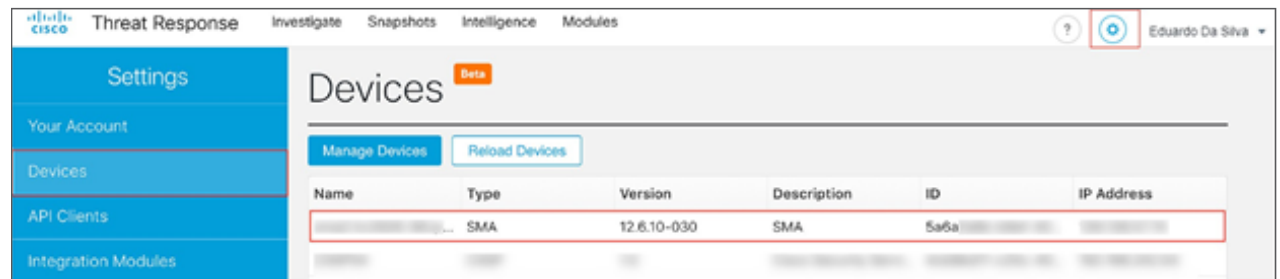
Step 2: Configure modules

Step 3: Start investigating

K. On the Cloud Services page, enable Cisco Threat Response.



L. In Threat Response, navigate to Settings > Devices via the gear icon in the upper right-hand corner. Check that the ESA or SMA has registered with Cisco Services Exchange.



Contents

Step 1: Access Cisco Threat Response

Step 2: Configure modules

Step 3: Start investigating

M. In Threat Response, navigate to Settings > Integration Modules > Add New Module. Find either the module type “Email Security Appliance” (if you have only the ESA) or “SMA Email” (if you have an SMA - including CES users), as appropriate, and click “Add New Module”.

The screenshot shows two module cards side-by-side. The left card is for 'Email Security Appliance' (ESA) with a purple 'Esa' icon. It includes a description: 'The Cisco Email Security Appliance (ESA) provides advanced threat protection capabilities to detect, block, and remediate threats faster,...' and buttons for 'Add New Module' and 'Learn More'. The right card is for 'SMA Email' with a purple 'Sma Email' icon. It includes a description: 'Cisco Content Security Management Appliance (SMA) centralizes management and reporting functions across multiple Cisco email and w...' and buttons for 'Add New Module', 'Learn More', and 'Free Trial'.

N. Type the module name, and then select a device under the registered device, and click Save. This completes the ESA or SMA module configuration.

The screenshot shows two configuration forms side-by-side. The left form is titled 'Add New Email Security Appliance Module'. It has a 'Module Name*' field with 'Email Security Appliance' entered, a 'Registered Device*' dropdown menu with 'my_esa' selected, and 'Save' and 'Cancel' buttons. The right form is titled 'Add New SMA Email Module'. It has a 'Module Name*' field with 'SMA Email' entered, a 'Registered Device*' dropdown menu with 'Search registered devices by name' selected, and 'Save' and 'Cancel' buttons.

Contents

Step 1: Access Cisco Threat Response

Step 2: Configure modules

Step 3: Start investigating

O. Once your ESA or SMA is connected, come back to this tab to confirm that the device is connected.

P. Click the “Start” button to go to the main page.

Contents

Step 1: Access Cisco Threat Response

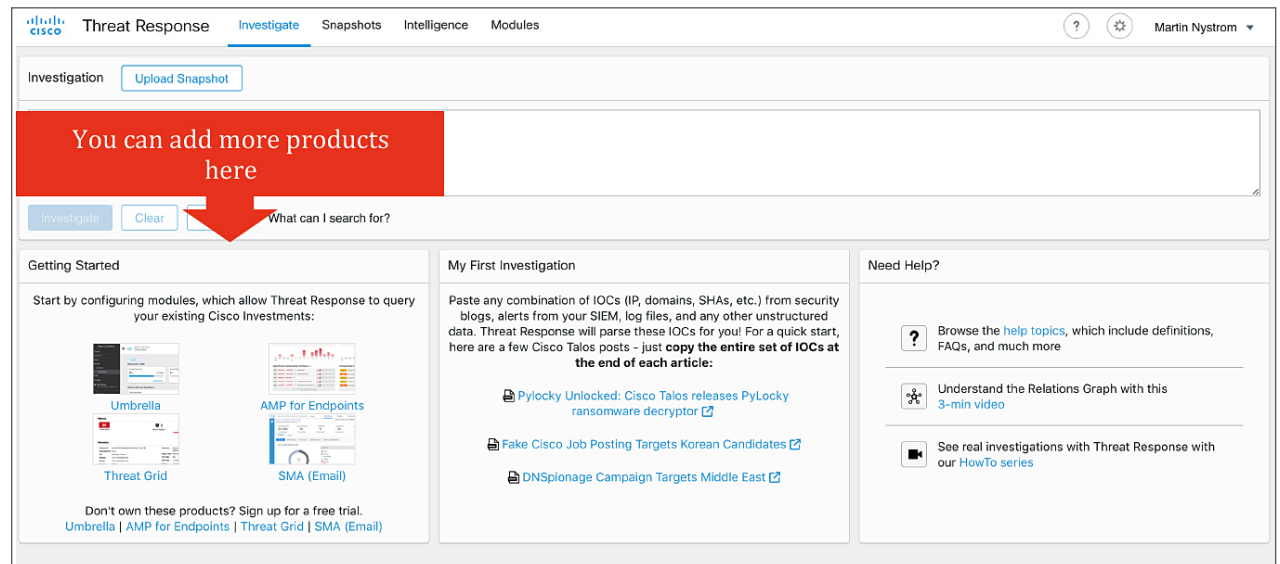
Step 2: Configure modules

Step 3: Start investigating

Configuring other modules

If you own AMP for Endpoints, Umbrella, Threat Grid, WSA, Stealthwatch Enterprise, or any of the other Threat Response integrated Cisco Security products, or supported 3rd party products or services like VirusTotal, you can also integrate them with Threat Response for greater intelligence, visibility, and enforcement capabilities.

Under the getting started tile, you can click on any other products you own for quick steps to configure them.



Contents

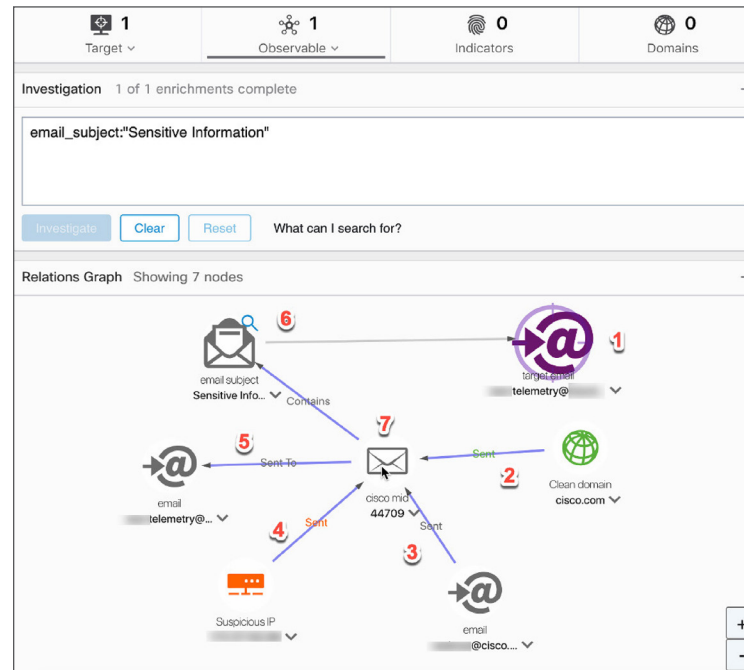
[Step 1: Access Cisco Threat Response](#)

[Step 2: Configure modules](#)

[Step 3: Start investigating](#)

Step 3: Start investigating

You can verify the ESA or SMA email module operation by investigating an email subject as an observable. The example in the picture below uses the subject “Sensitive Information.” The investigation syntax is **email_subject: “Sensitive Information”**.



From the graph output, we identify the following sighting elements associated with the investigation:

1. Message inbox(es) that have been targeted by the incoming message. This matches the email address that the message was sent to.
2. Incoming sender domain.
3. The sender's email address.
4. IP address of the sending host.
5. The email address that the message was sent to. This matches the target being identified.
6. The email subject observable that was investigated.
7. The Cisco Message ID (MID) that identifies the message.

Contents

Step 1: Access Cisco Threat Response

Step 2: Configure modules

Step 3: Start investigating

You can use the same syntax for other email observables as follows:

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

Besides the investigation of email elements, you can also copy IOCs (indicators of compromise) on the latest threats from [Talos' Weekly Threat Roundup](#).

The screenshot shows the Cisco Threat Response Investigate interface. At the top, there are navigation tabs: Threat Response, Investigate (selected), Snapshots, Intelligence, and Modules. A user profile 'Eduardo Da Silva' is visible in the top right. Below the navigation, there is an 'Investigation' section with an 'Upload Snapshot' button. The main content area displays a search result for domains: 'shirkeswitch[.]net' and 'guideofgeorgia[.]org'. Below the domains, it states: 'The following IP addresses have been observed to be associated with malware campaigns.' followed by a list of IP addresses: '112.213.89[.]40 67.23.254[.]61 62.212.33[.]98'. At the bottom of the search results, there are three buttons: 'Investigate', 'Clear', and 'Reset', and a search prompt 'What can I search for?'.

Paste any text that contains IOCs—domains, IP addresses, file hashes—and let Threat Response do the work for you. Or, use the browser plugins available from cs.co/CTR4Chrome and cs.co/CTR4Firefox.

Want to learn more?

Please visit our [Cisco Threat Response page](#) or talk with your Cisco account team. Still have questions? Check the FAQ at https://cs.co/ctr_faq and the documentation in the product at the help button.