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

![Email activation message]

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

**Connect a Device such as SMA Email**
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.

<table>
<thead>
<tr>
<th>Cloud Service Settings</th>
<th>Management Appliance</th>
<th>Email</th>
<th>Web</th>
<th>Centralized Services</th>
<th>Network</th>
<th>System Administration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cloud Services</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat Response:</td>
<td>Disabled</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Cloud Services Settings</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Status: Enable the Cloud Services on your appliance to use the Cisco Threat Response portal.</td>
</tr>
</tbody>
</table>
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.

Connect Device

Which of these would you like to connect?

Register Device
If you have on-prem appliances, (i.e. ESA) register them by:
1. Following the Registration guide, found here.
2. Return to this page.
3. Click Confirm Devices Are Connected

Link Accounts
If you have other Cisco Security accounts (i.e. ACI, AMP) connect them by:
1. Following the Link guide, found here.
2. Return to this page.
3. Click Confirm Devices Are Connected

After connecting a device, return to this page to confirm the device is working by clicking the button below.

Confirm Device is Connected
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.

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

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

**Step 1: Access Cisco Threat Response**

**Step 2: Configure modules**

**Step 3: Start investigating**

---

**H. Confirm the device has been created.**

![Image of Cisco Services Exchange](image)

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

![Image of Cloud Service Settings](image)

**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.**

![Image of Cisco Services Exchange](image)
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.
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”.

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.
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.

Thank You!

Your account has been activated.
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.
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.
You can use the same syntax for other email observables as follows:

<table>
<thead>
<tr>
<th>IP address</th>
<th>ip: &quot;4.2.2.2&quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>domain: &quot;cisco.com&quot;</td>
</tr>
<tr>
<td>Sender email address</td>
<td>email: &quot;<a href="mailto:noreply@cisco.com">noreply@cisco.com</a>&quot;</td>
</tr>
<tr>
<td>Email message header</td>
<td>email_messageid: &quot;<a href="mailto:123-abc-456@cisco.com">123-abc-456@cisco.com</a>&quot;</td>
</tr>
<tr>
<td>Email subject</td>
<td>email_subject: &quot;Invoice Due&quot;</td>
</tr>
<tr>
<td>Cisco Message ID (MID)</td>
<td>cisco_mid: &quot;12345&quot;</td>
</tr>
<tr>
<td>SHA256 filehash</td>
<td>sha256: &quot;sha256filehash&quot;</td>
</tr>
<tr>
<td>Email attachment file name</td>
<td>file_name: &quot;invoice.pdf&quot;</td>
</tr>
</tbody>
</table>

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

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.