

Quick Start Guide for Umbrella Customers

Unleash the power of our integrated security architecture

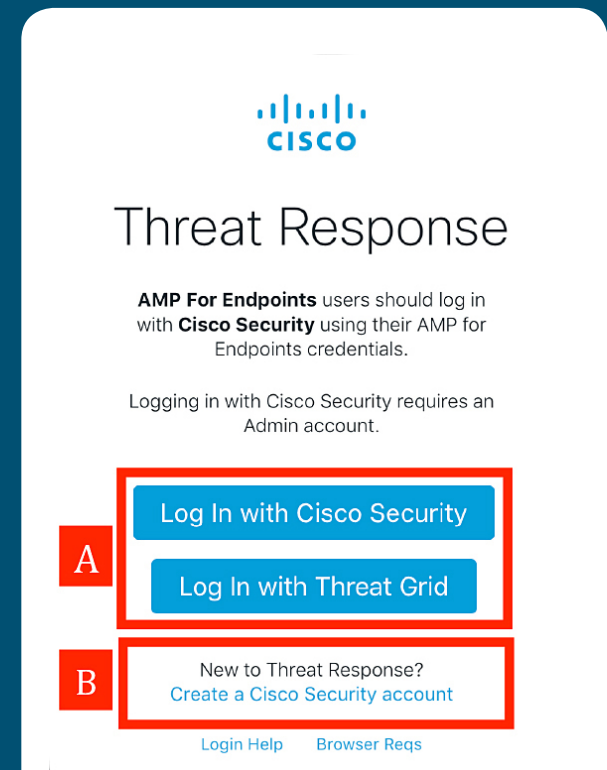
Extend the value of your Cisco Umbrella investment by leveraging Cisco Threat Response to accelerate key security operations functions: detection, investigation, and remediation. By aggregating threat intelligence, you can dramatically cut the time and manual effort required to investigate and remediate cybersecurity incidents.

Start investigating today in 3 steps

Step 1: Access Cisco Threat Response

As an Umbrella customer, 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 [AP cloud](#).

- 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 not yet available on the Asia Pacific cloud).



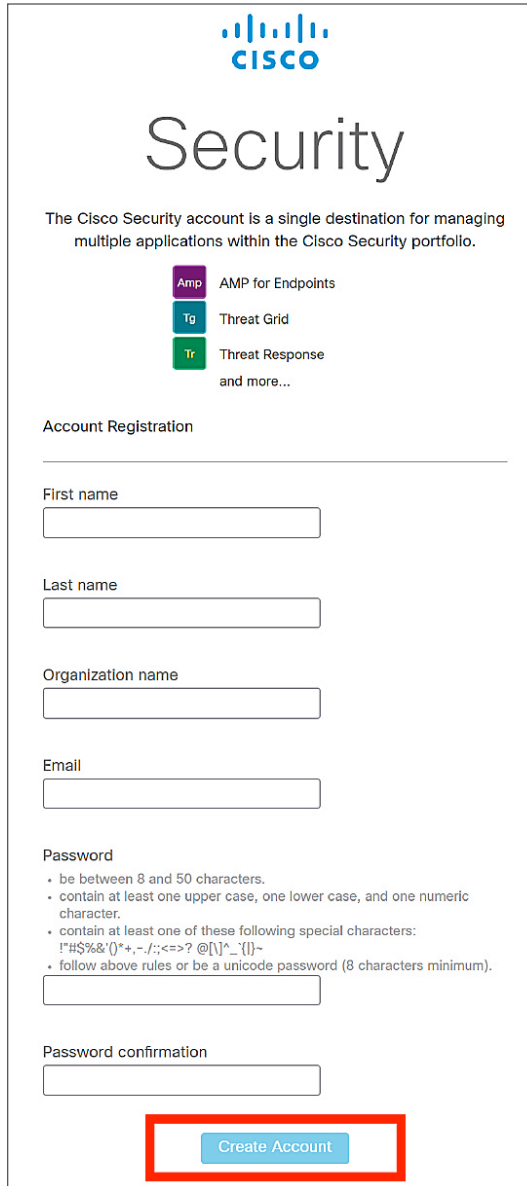
Contents

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).



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

- Amp** AMP for Endpoints
- Tg** Threat Grid
- Tr** 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

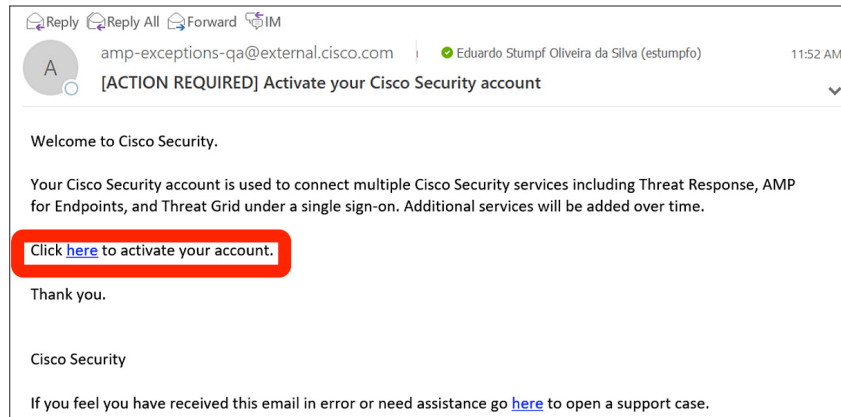
Contents

Step 1: Access Cisco Threat Response

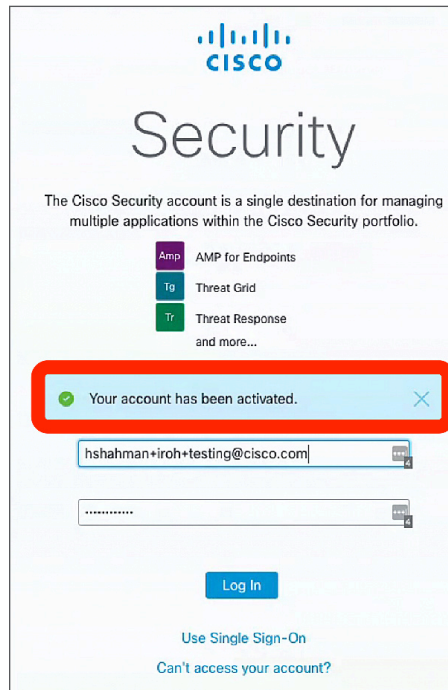
Step 2: Configure modules

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

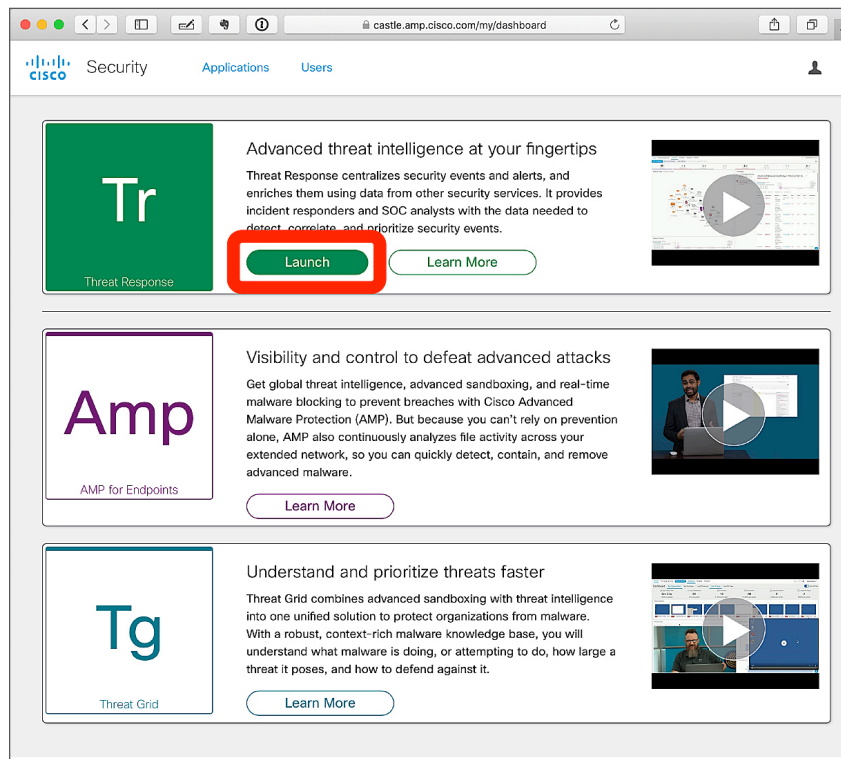
Step 1: Access Cisco Threat Response

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.** To activate your account, click on Configure under the section “Configure Umbrella or AMP for Endpoints.” Step 2 will guide you to configure your Umbrella module to finalize account activation.

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

If you've completed step 1, you will be directed to this screen. Click Add Module under the Umbrella tile. A new tab will open to configure the module by simply copy and pasting your API keys. Come back to this tab to confirm the module is working.

You can find detailed Umbrella module configuration steps [here](#).

Configure Module

Which of these modules do you currently have?

AMP for Endpoints

Advanced Malware Protection

Add Module


Umbrella

Cisco Umbrella Investigate

Add Module

After selecting and configuring one of the above options, return to this page to confirm the module is working by clicking the button below.

Confirm Module is Configured



Contents

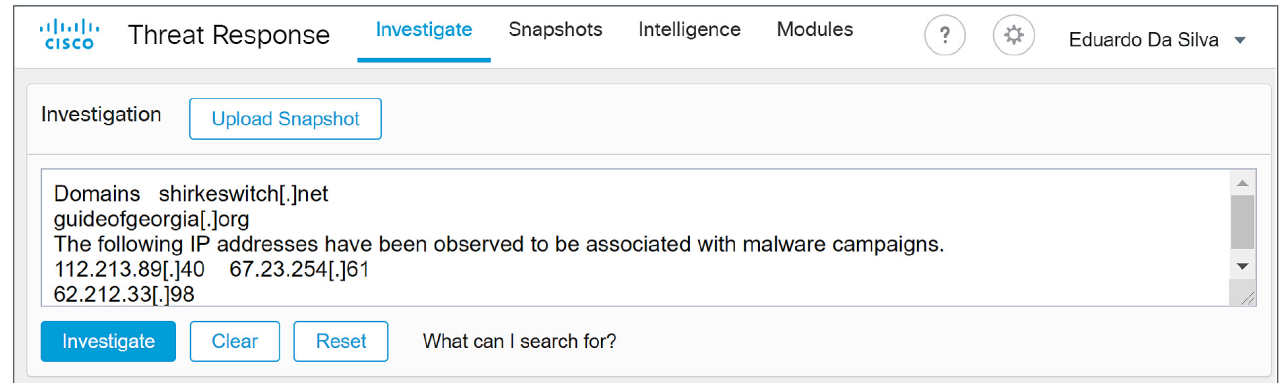
Step 1: Access Cisco Threat Response

Step 2: Configure modules

Step 3: Start investigating

Step 3: Start investigating

Paste any text that contains Indicators of Compromise (IOCs), including domains, IP addresses, and file hashes, and let Threat Response do the work for you.



The screenshot shows the Cisco Threat Response web interface. At the top, there's a navigation bar with the Cisco logo, 'Threat Response', and tabs for 'Investigate' (which is active), 'Snapshots', 'Intelligence', and 'Modules'. On the right of the navigation bar are icons for help and settings, and the user's name 'Eduardo Da Silva'. Below the navigation bar, the 'Investigate' section has a sub-header 'Investigation' and an 'Upload Snapshot' button. A text area contains the following text: 'Domains shirkesswitch[.]net', 'guideofgeorgia[.]org', 'The following IP addresses have been observed to be associated with malware campaigns.', '112.213.89[.]40 67.23.254[.]61', and '62.212.33[.]98'. At the bottom of the text area are three buttons: 'Investigate' (in blue), 'Clear', and 'Reset'. To the right of these buttons is a search prompt 'What can I search for?'.

You can copy IOCs on the latest threats from [Talos' weekly threat roundup](#). Spot a new threat? One click stops it.

Want to learn more? Please visit our [Cisco threat response page](#) or talk with your Cisco account team. Still have questions? Reach out to threat-response-early@cisco.com.