Quick Start Guide for Umbrella Customers
Unleash the power of our integrated security architecture

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).
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.

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.
**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.

<table>
<thead>
<tr>
<th>Account Activation</th>
</tr>
</thead>
<tbody>
<tr>
<td>To start using Threat Response, please configure your first product to activate your account.</td>
</tr>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configure Umbrella or AMP for Endpoints</th>
<th>Connect a Device such as SMA Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Configure]</td>
<td>[Connect]</td>
</tr>
</tbody>
</table>
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](#)
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.

You can copy IOCs on the latest threats from [Talos’ weekly threat roundup](https://www.talosintelligence.com/threat-roundup). Spot a new threat? One click stops it.

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