

思科威胁响应(CTR)和ESA集成

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[步骤1: 导航至网络\(Network\)>云服务设置\(Cloud Service Settings\)](#)

[步骤2. 点击Edit Settings](#)

[步骤3. 选中Enable和Threat Response Server复选框](#)

[步骤4. 提交并提交更改](#)

[步骤5. 登录CTR门户并生成ESA中请求的注册令牌](#)

[步骤6. 将注册令牌 \(从CTR门户生成\) 粘贴到ESA](#)

[步骤7. 验证ESA设备是否在SSE门户中](#)

[步骤8. 导航至CTR门户并添加新的ESA模块](#)

[验证](#)

[故障排除](#)

[CTR门户中未显示ESA设备](#)

[CTR调查未显示来自ESA的数据](#)

[ESA未请求注册令牌](#)

[由于无效或过期的令牌，注册失败](#)

[相关信息](#)

简介

本文档介绍将思科威胁响应(CTR)与邮件安全设备(ESA)集成的流程，以及如何验证此流程以执行某些CTR调查。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科威胁响应
- 邮件安全设备

使用的组件

本文档中的信息基于以下软件和硬件版本：

- CTR帐户

- 思科安全服务交换
- 软件版本13.0.0-392上的ESA C100V

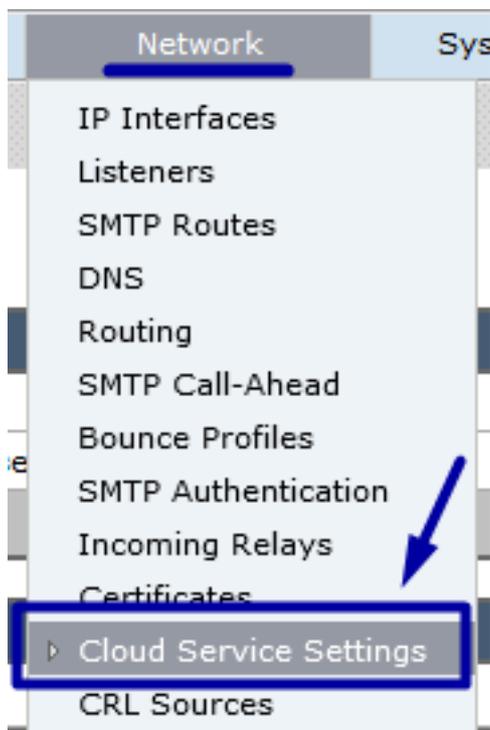
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

要配置集成CTR和ESA，请登录邮件安全虚拟设备并执行以下快速步骤：

步骤1: 导航至网络(Network)>云服务设置(Cloud Service Settings)

进入ESA后，导航至情景菜单Network > Cloud Service Settings，以查看当前威胁响应状态（禁用/启用），如图所示。



步骤2. 点击Edit Settings

到目前为止，ESA中的威胁响应功能已禁用，要启用此功能，请点击编辑设置（如图所示）：



步骤3.选中Enable和Threat Response Server复选框

选中复选框启用，然后选择威胁响应服务器，请查看下图：

Cloud Service Settings

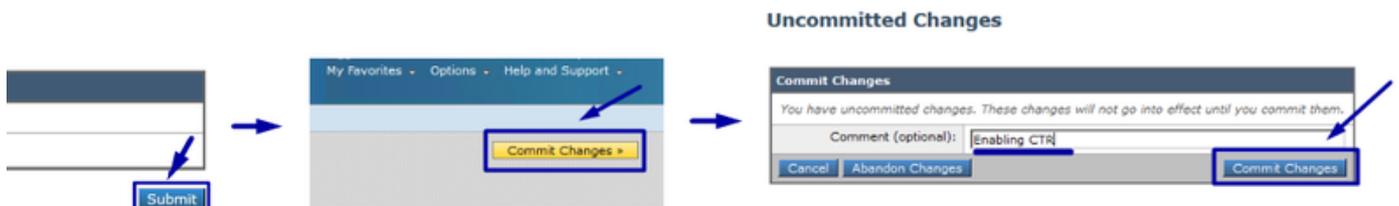


注意：威胁响应服务器URL的默认选择是AMERICAS(api-sse.cisco.com)。对于欧洲企业，单击下拉菜单并选择EUROPE(api.eu.sse.itd.cisco.com)

步骤4.提交并提交更改

必须提交并提交更改，才能保存并应用任何更改。现在，如果刷新ESA接口，将请求注册令牌以注册集成，如下图所示。

注意：您可以看到“成功”消息：您的更改已提交。



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	

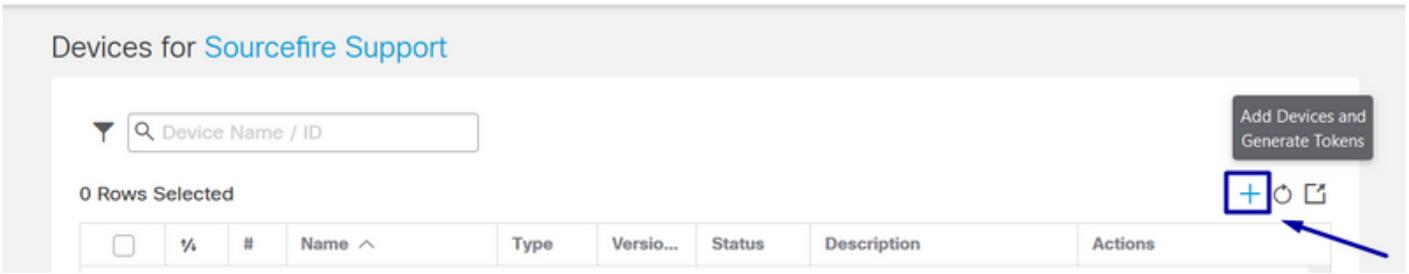
Cloud Services Settings	
Registration Token: ?	<input type="text"/>
Register	

步骤5.登录CTR门户并生成ESA中请求的注册令牌

1. — 进入CTR门户后，导航至Modules > Devices > Manage Devices，请查看下一个映像。

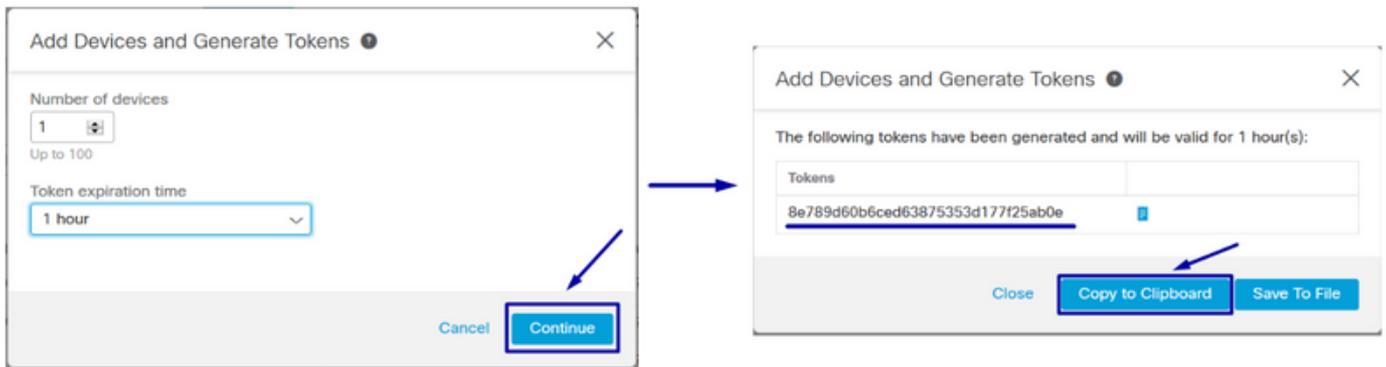
The screenshot shows a web browser at the URL <https://visibility.amp.cisco.com/settings/devices>. The navigation menu includes Threat Response, Investigate, Snapshots, Incidents (Beta), Intelligence, and Modules. The 'Modules' link is highlighted with a blue box and an arrow. Below the navigation, the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

2.- Manage Devices链接将您重定向到安全服务交换(SSE)，一旦到达，点击图标Add Devices and Generate Tokens，如图所示。



3. — 单击“继续”以生成令牌，一旦生成令牌，单击“复制到剪贴板”，如图所示。

提示：您可以选择要添加的设备数量（从1到100），并选择令牌到期时间（1小时、2小时、4小时、6小时、8小时、12小时、01天、02天、03天、04天和05天）。



步骤6.将注册令牌（从CTR门户生成）粘贴到ESA

生成注册令牌后，将其粘贴到ESA的“云服务设置”部分，如下图所示。

注意：您可以看到“成功”消息：向思科威胁响应门户注册设备的请求已发起。稍后导航回此页面以检查设备状态。

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.
---------	--

步骤7.验证ESA设备是否在SSE门户中

您可以导航至SSE门户(CTR > Modules > Devices > Manage Devices)，在Search选项卡中查看ESA设备，如图所示。

Security Services Exchange Audit Log Brenda Marquez

Devices for Sourcefire Support

Search:

0 Rows Selected

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

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

步骤8.导航至CTR门户并添加新的ESA模块

1. — 进入CTR门户后，导航至Modules > Add New Module，如图所示。

Threat Response Investigate Snapshots Incidents Intelligence Modules Brenda Marquez

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. — 选择模块类型，在本例中，模块是邮件安全设备模块，如下图所示。

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 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](#)

Esa 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. — 输入字段：模块名称、注册设备（选择之前注册的设备）、请求时间范围（天）和保存，如图所示。

Threat Response Investigate Snapshots Incidents Beta Intelligence Modules

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

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.

验证

为了验证CTR和ESA集成，您可以发送测试电子邮件，您也可以从ESA查看该电子邮件，导航至监控(Monitor)>邮件跟踪(Message Tracking)，然后查找测试电子邮件。在本例中，我按邮件主题过滤为下图。

Cisco C100V
Email Security Virtual Appliance

Monitor | Mail Policies | Security Services | Network | System Administration

Message Tracking

Search

Available Time Range: 14 May 2020 12:44 to 14 May 2020 13:41 (GMT +00:00) Data in time range: 100.0% complete

Envelope Sender: ? Begins With []

Envelope Recipient: ? Begins With []

Subject: Begins With [test test]

Message Received: Last Day Last Week Custom Range

Start Date: [05/13/2020] Time: [13:00] and End Date: [05/14/2020] Time: [13:42] (GMT +00:00)

Advanced Search messages using advanced criteria

Clear Search

Generated: 14 May 2020 13:42 (GMT +00:00) Export All... | Export...

Results

Items per page 20

Displaying 1 — 1 of 1 items.

1	14 May 2020 13:23:57 (GMT +00:00)	MID: 8	Show Details
---	-----------------------------------	--------	--------------

SENDER: mgmt01@cisco.com
RECIPIENT: testingBren@cisco.com
SUBJECT: test test
LAST STATE: Message 8 to testingBren@cisco.com received remote SMTP response 'ok: Me:

Displaying 1 — 1 of 1 items.

现在，从CTR门户，您可以执行调查，导航至调查，并使用一些可观察电子邮件，如图所示。

The screenshot shows the Cisco Threat Response Investigate interface. At the top, there are navigation tabs: Threat Response, Investigate, Snapshots, Incidents, Intelligence, and Modules. The user is logged in as Brenda Marquez. The interface displays search results for the query 'email_subject:'test test'. A callout box indicates that the 'esa03' module enriched this investigation with 1 sighting and 0 judgements. The sightings table shows one sighting from the 'Email Security Appliance' module, observed 9 hours ago, with a description of an incoming message (Delivered) and a confidence of High and severity of Low. The relations graph shows connections between various entities like IP, Domain, Email Address, and Email Subject.

提示：您可以对其他可观察电子邮件使用相同的语法，如图所示。

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"

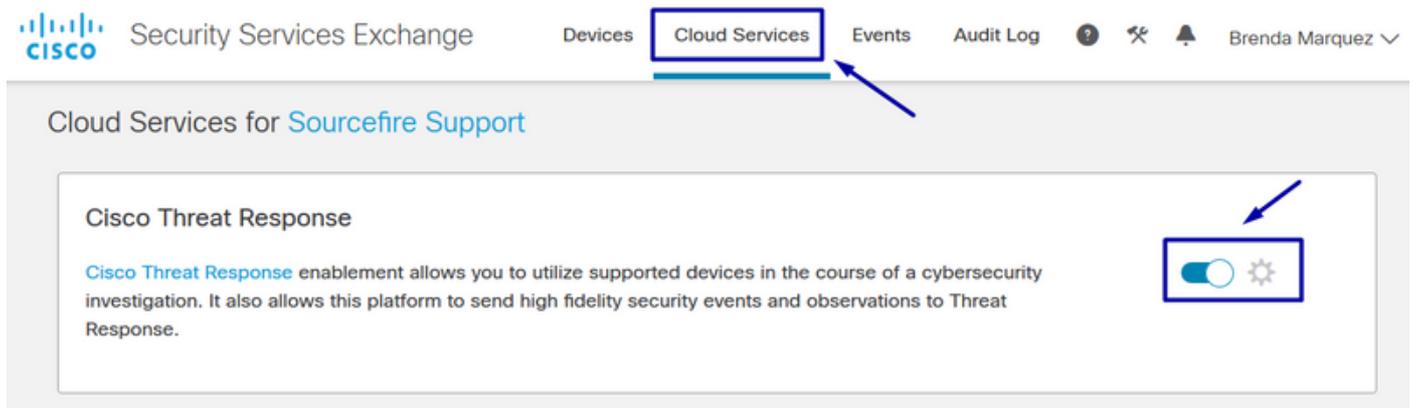
故障排除

如果您是CES客户，或者如果您通过SMA管理ESA设备，则只能通过SMA连接到威胁响应。请确保您的SMA运行AsyncOS 12.5或更高版本。如果不使用SMA管理ESA，而直接集成ESA，请确保其为AsyncOS版本13.0或更高版本。

CTR门户中未显示ESA设备

如果在CTR门户中添加ESA模块时ESA设备未显示在下拉注册设备中，请确保已在SSE中启用

CTR，在CTR中导航至Modules > Devices > Manage Devices，然后在SSE门户中导航至Cloud Services并启用CTR，如下图所示：



CTR调查未显示来自ESA的数据

请确保：

- 调查的语法正确，邮件可观察项如上“验证”部分所示。
- 您已选择适当的威胁响应服务器或云（美洲/欧洲）。

ESA未请求注册令牌

请确保在启用威胁响应后提交更改，否则，更改将不会应用到ESA的“威胁响应”部分。

由于无效或过期的令牌，注册失败

请确保令牌是从正确的云生成的：

如果将欧洲（欧盟）云用于ESA，请从以下位置生成令牌：<https://admin.eu.sse.itd.cisco.com/>

如果将美洲(NAM)云用于ESA，请从以下位置生成令牌：<https://admin.sse.itd.cisco.com/>

另请记住，注册令牌有过期时间（选择最方便的时间及时完成集成）。

相关信息

- 您可以在思科威胁响应和ESA集成视频中[找到本文包含的信息](#)。
- [技术支持和文档 - Cisco Systems](#)