

# Cisco Threat Response (CTR) e integração ESA

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Etapa 1. Navegue até Network > Cloud Service Settings](#)

[Etapa 2. Clique em Editar configurações](#)

[Etapa 3. Marque a caixa de seleção Habilitar e o Servidor de resposta a ameaças](#)

[Etapa 4. Enviar e confirmar alterações](#)

[Etapa 5. Faça login no portal CTR e gere o token de registro solicitado no ESA](#)

[Etapa 6. Cole o token de registro \(gerado a partir do portal CTR\) no ESA](#)

[Passo 7. Verifique se o dispositivo ESA está no portal SSE](#)

[Etapa 8. Navegue até o portal CTR e adicione um novo módulo ESA](#)

[Verificar](#)

[Troubleshoot](#)

[O dispositivo ESA não é exibido no portal CTR](#)

[A investigação CTR não está mostrando dados do ESA](#)

[O ESA não está solicitando o token de registro](#)

[Falha no registro devido a um token inválido ou expirado](#)

[Informações Relacionadas](#)

## Introduction

Este documento descreve o processo de integração do Cisco Threat Response (CTR) com o Email Security Appliance (ESA) e como verificar isso para realizar algumas investigações do CTR.

## Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Threat Response
- Dispositivo de segurança de e-mail

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Conta CTR

- Cisco Security Services Exchange
- ESA C100V na versão de software 13.0.0-392

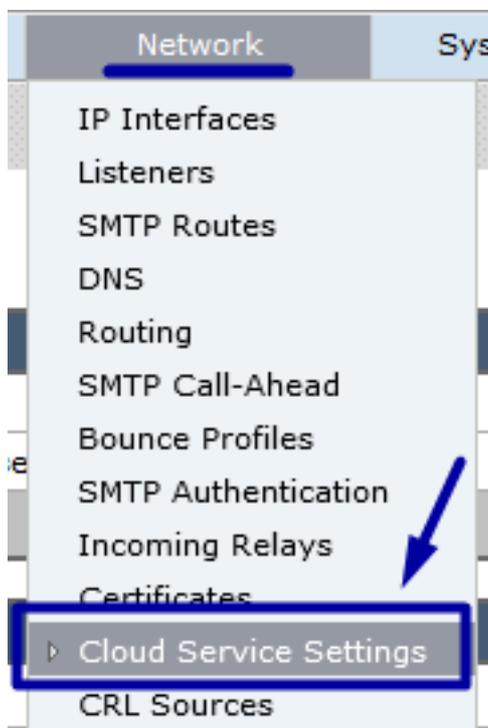
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Configurar

Para configurar o CTR e o ESA de integração, faça login no Email Security Virtual Appliance e siga estas etapas rápidas:

### Etapa 1. Navegue até Network > Cloud Service Settings

No ESA, navegue até o menu de contexto Network > Cloud Service Settings (Rede > Configurações de serviço de nuvem) para ver o status atual da resposta à ameaça (Desabilitado / Habilitado) como mostrado na imagem.



### Etapa 2. Clique em Editar configurações

Até agora, o recurso Resposta a ameaças no ESA está desabilitado. Para habilitar o recurso, clique em Editar configurações, conforme mostrado na imagem:



### Etapa 3. Marque a caixa de seleção Habilitar e o Servidor de resposta a ameaças

Marque a caixa de seleção Enable (Habilitar) e escolha o Threat Response Server. Consulte a imagem abaixo:

#### Cloud Service Settings

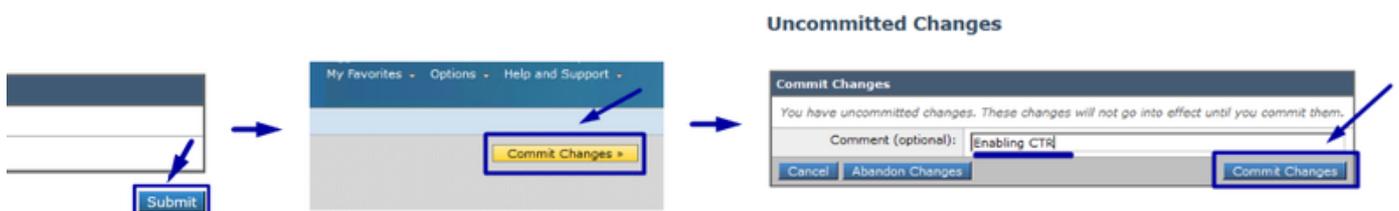


**Note:** A seleção padrão para a URL do Threat Response Server é AMERICAS (api-sse.cisco.com). Para empresas EUROPE, clique no menu suspenso e escolha EUROPE (api.eu.sse.itd.cisco.com)

### Etapa 4. Enviar e confirmar alterações

É necessário enviar e confirmar as alterações para salvar e aplicar qualquer alteração. Agora, se a interface ESA for atualizada, um token de registro será solicitado para registrar a Integração, como mostrado na imagem abaixo.

**Note:** Você pode ver uma mensagem de êxito: Suas alterações foram confirmadas.



## Cloud Service Settings

Success — Your changes have been committed.

Cloud Services	
Threat Response:	Enabled
Threat Response Server:	AMERICAS (api-sse.cisco.com)
<a href="#">Edit Settings</a>	

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)
<a href="#">Edit Settings</a>	

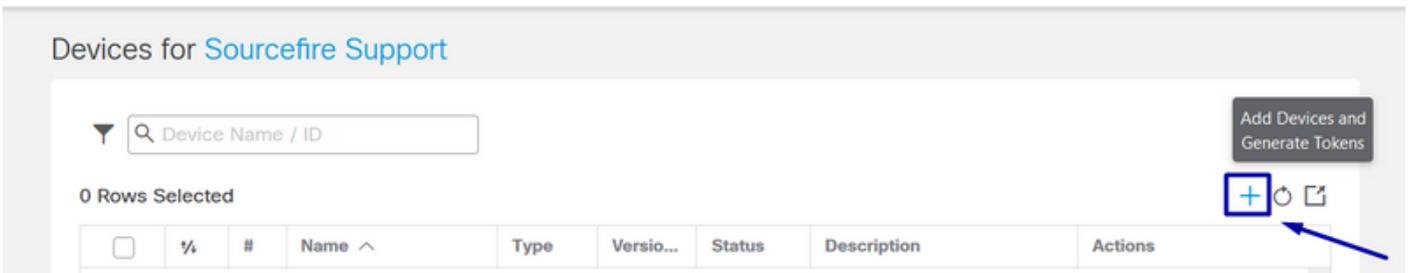
Cloud Services Settings	
Registration Token: ?	<input type="text"/>
<a href="#">Register</a>	

### Etapa 5. Faça login no portal CTR e gere o token de registro solicitado no ESA

1.- No portal CTR, navegue até Modules > Devices > Manage Devices (Módulos > Dispositivos > Gerenciar dispositivos). Consulte a próxima imagem.

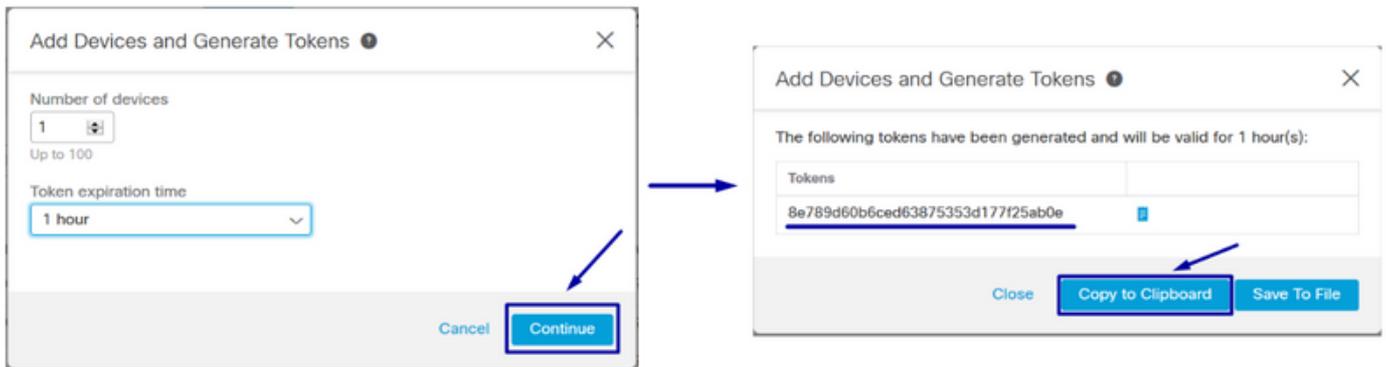
The screenshot shows the Cisco Threat Response portal interface. The browser address bar displays <https://visibility.amp.cisco.com/settings/devices>. The navigation menu includes Threat Response, Investigate, Snapshots, Incidents, Intelligence, and Modules. The 'Modules' link is highlighted with a blue box and an arrow. Below the navigation menu, the breadcrumb path is 'Settings > Devices'. The 'Devices' section is active, showing a 'Manage Devices' button and a 'Reload Devices' button. The 'Manage Devices' button is highlighted with a blue box and an arrow. The left sidebar menu is also visible, with 'Devices' highlighted and an arrow pointing to it.

2.- O link Gerenciar dispositivos o redireciona para o Security Services Exchange (SSE), quando estiver lá, clique no ícone Adicionar dispositivos e Gerar tokens, como mostrado na imagem.



3.- Clique em Continuar para gerar o Token, depois de gerá-lo, clique em Copiar para a Área de Transferência, conforme mostrado na imagem.

**Tip:** Você pode selecionar o número de dispositivos a serem adicionados (de 1 e até 100) e também selecionar o tempo de expiração do token (1h, 2h, 4h, 6h, 8h, 12h, 01 dias, 02 dias, 03 dias, 04 dias e 05 dias).



### Etapa 6. Cole o token de registro (gerado a partir do portal CTR) no ESA

Quando o Token de registro for gerado, cole-o na seção Cloud Services Settings do ESA, como a imagem abaixo.

**Note:** Você pode ver uma mensagem de êxito: Uma solicitação para registrar seu dispositivo no portal Cisco Threat Response é iniciada. Volte para esta página depois de algum tempo para verificar o status do aplicativo.

### 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.
---------	----------------------------------------------------------------------------------------------------------------------

## Passo 7. Verifique se o dispositivo ESA está no portal SSE

Você pode navegar até o portal SSE (CTR > Modules > Dispositivos > Gerenciar dispositivos) e, na guia Pesquisar, veja o dispositivo ESA, como mostrado na imagem.

Security Services Exchange Audit Log Brenda Marquez

### Devices for Sourcefire Support

Search:

0 Rows Selected

	%	#	Name ^	Type	Versio...	Status	Description	Actions
<input type="checkbox"/>	<input type="checkbox"/>	1	esa03.mex-amp.inl...	ESA	13.0.0	Registered	ESA	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Refresh</a>

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

## Etapa 8. Navegue até o portal CTR e adicione um novo módulo ESA

1.- Quando estiver no portal CTR, navegue até Modules > Add New Module (Módulos > Adicionar novo módulo), conforme mostrado na imagem.

Threat Response Investigate Snapshots Incidents Intelligence **Modules** Brenda Marquez

Settings > Modules

### 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** 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.- Escolha o tipo de módulo, nesse caso, o módulo é um módulo do Email Security Appliance como a imagem abaixo.

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.- Insira os campos: Nome do módulo, Dispositivo registrado (selecione o registrado anteriormente) e Prazo da solicitação (dias) e Salvar, como mostrado na imagem.

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

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.

Verificar

Para verificar a Integração CTR e ESA, você pode enviar um e-mail de teste, que também pode ser visto em seu ESA, navegar até Monitor > Message Tracking e encontrar o e-mail de teste. Nesse caso, filtrei por assunto do e-mail como a imagem abaixo.

**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.

Agora, no portal do CTR, você pode executar uma investigação, navegar até Investigar e usar alguns e-mails observáveis, como mostrado na imagem.

The screenshot shows the Cisco Threat Response Investigate interface. At the top, there are navigation tabs: Threat Response, Investigate (selected), Snapshots, Incidents, Intelligence, and Modules. Below the navigation, there are filters for 1 Target, 1 Observable, 0 Indicators, 0 Domains, 0 File Hashes, 0 IP Addresses, 0 URLs, and 1 Module. The search bar contains the query `email_subject:'test test'`. Below the search bar, there are buttons for 'Investigate', 'Clear', and 'Reset'. The main area is divided into three sections: 'Relations Graph' showing a network of nodes (IP, Target Email, Email Subject, Cisco Message ID, Domain, Email Address), 'Sightings' showing a graph of sightings over time, and 'Observables' showing details for the search query. A table in the 'Observables' section lists sightings, with one entry highlighted in a blue box:

Module	Observed	Description	Confidence	Severity	Details
esa03 ----- Email Security Appliance	9 hours ago	Incoming m essage (Del ivered)	High	Low	

**Tip:** Você pode usar a mesma sintaxe para outros observáveis de e-mail da seguinte forma na imagem.

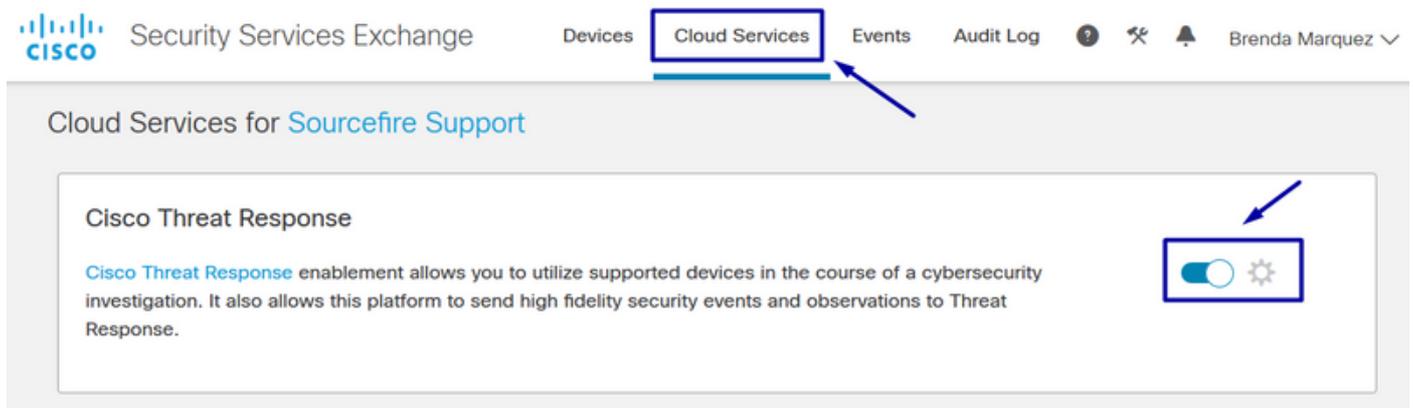
IP address	<code>ip:"4.2.2.2"</code>	Email subject	<code>email_subject:"Invoice Due"</code>
Domain	<code>domain:"cisco.com"</code>	Cisco Message ID (MID)	<code>cisco_mid:"12345"</code>
Sender email address	<code>email:"noreply@cisco.com"</code>	SHA256 filehash	<code>sha256:"sha256filehash"</code>
Email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

## Troubleshoot

Se você for um cliente CES ou se gerenciar seus dispositivos ESA por meio de um SMA, poderá se conectar somente à resposta a ameaças por meio do SMA. Certifique-se de que o seu SMA execute o AsyncOS 12.5 ou posterior. Se você não gerenciar seu ESA com um SMA e integrar o ESA diretamente, verifique se ele está na versão 13.0 do AsyncOS ou superior.

## O dispositivo ESA não é exibido no portal CTR

Se o dispositivo ESA não for exibido na lista suspensa Dispositivo registrado enquanto o módulo ESA for adicionado ao portal CTR, certifique-se de que o CTR tenha sido ativado no SSE, no CTR, navegue para Módulos > Dispositivos > Gerenciar dispositivos e, em seguida, no portal SSE, navegue para Serviços de nuvem e ative o CTR, como a imagem abaixo:



## A investigação CTR não está mostrando dados do ESA

Certifique-se de que:

- A sintaxe da investigação está correta, os observáveis de e-mail são mostrados acima na Seção Verificar.
- Você selecionou o servidor de resposta a ameaças ou a nuvem (Américas/Europa) apropriados.

## O ESA não está solicitando o token de registro

Certifique-se de confirmar as alterações, quando a resposta à ameaça for ativada, caso contrário, as alterações não serão aplicadas à seção Resposta à ameaça no ESA.

## Falha no registro devido a um token inválido ou expirado

Certifique-se de que o token seja gerado a partir da nuvem correta:

Se você usar a nuvem da Europa (UE) para ESA, gere o token a partir de:

<https://admin.eu.sse.itd.cisco.com/>

Se você usar o NAM (Americas) Cloud para ESA, gere o token de:

<https://admin.sse.itd.cisco.com/>

Além disso, lembre-se de que o token Registration tem um tempo de expiração (selecione o horário mais conveniente para concluir a Integração no tempo).

## Informações Relacionadas

- Você pode encontrar as informações contidas neste artigo no vídeo [Cisco Threat Response and ESA Integration](#).
- [Suporte Técnico e Documentação - Cisco Systems](#)