Cisco Threat Response (CTR) e integração ESA

Contents

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

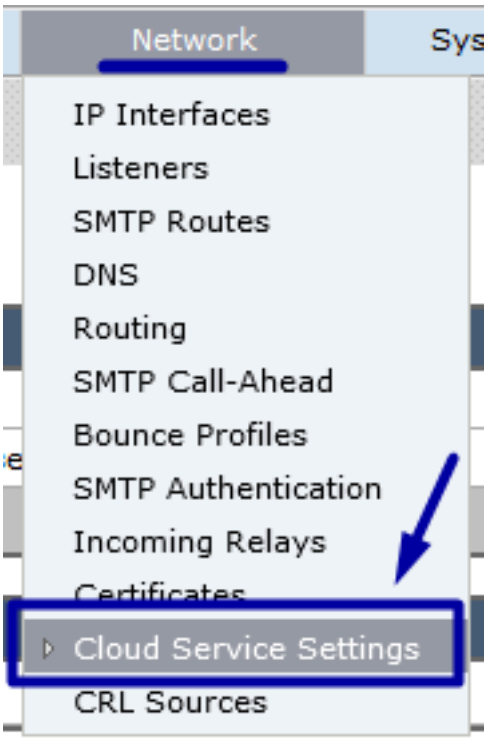
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

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

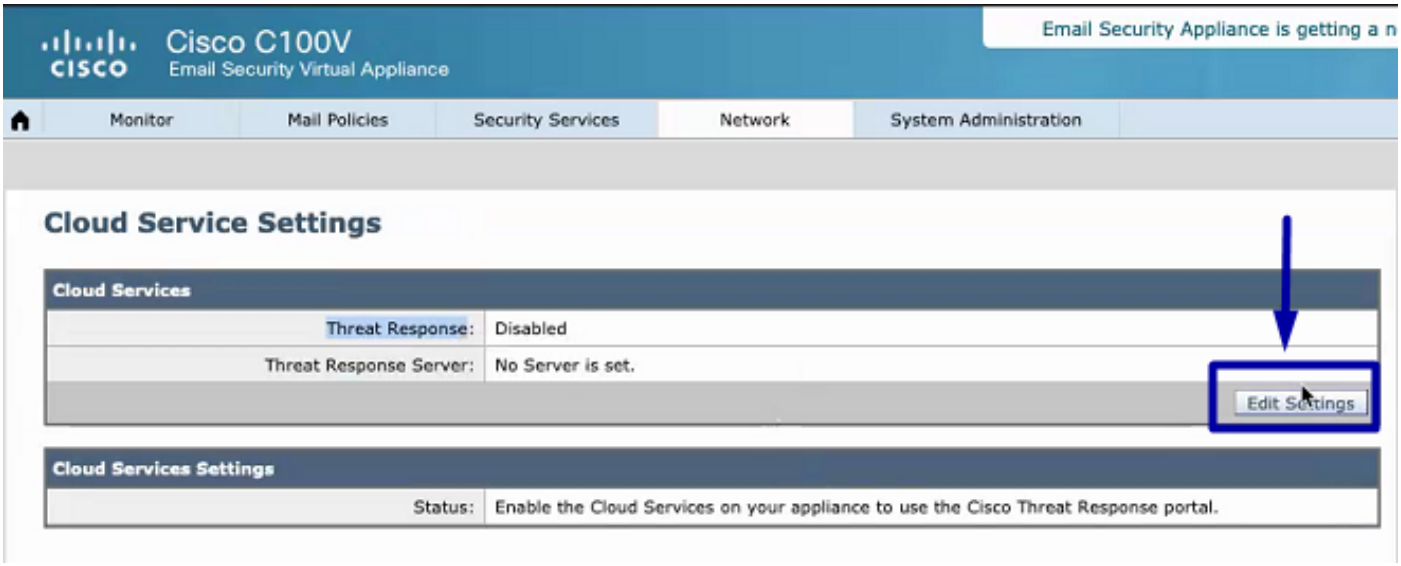
Etapa 1. Navegue até Network > Cloud Service Settings

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

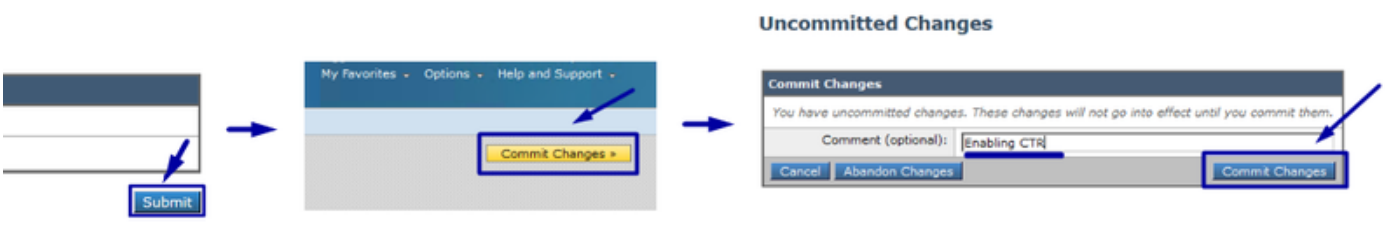
Marque a caixa de seleção Enable (Habilitar) e escolha o Threat Response Server. Consulte a imagem abaixo:

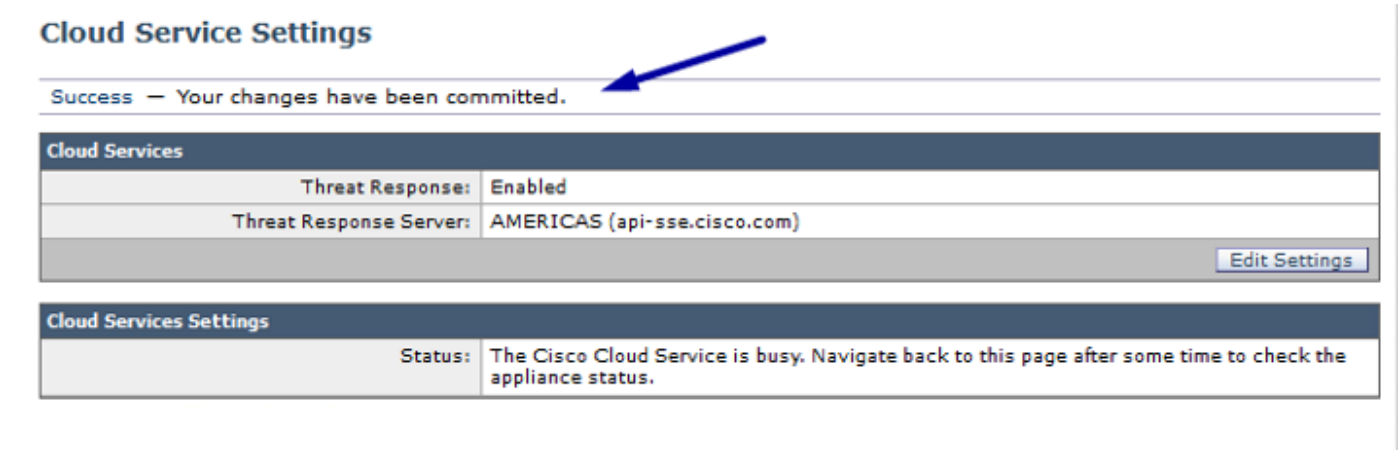
Note: A seleção padrão para a URL do Threat Response Server é AMERICAS (api-sse.cisco.com). Para empresas EUROPE, clique no menu suspenso e escolha EUROPE (api.eu.sse.itd.cisco.com)

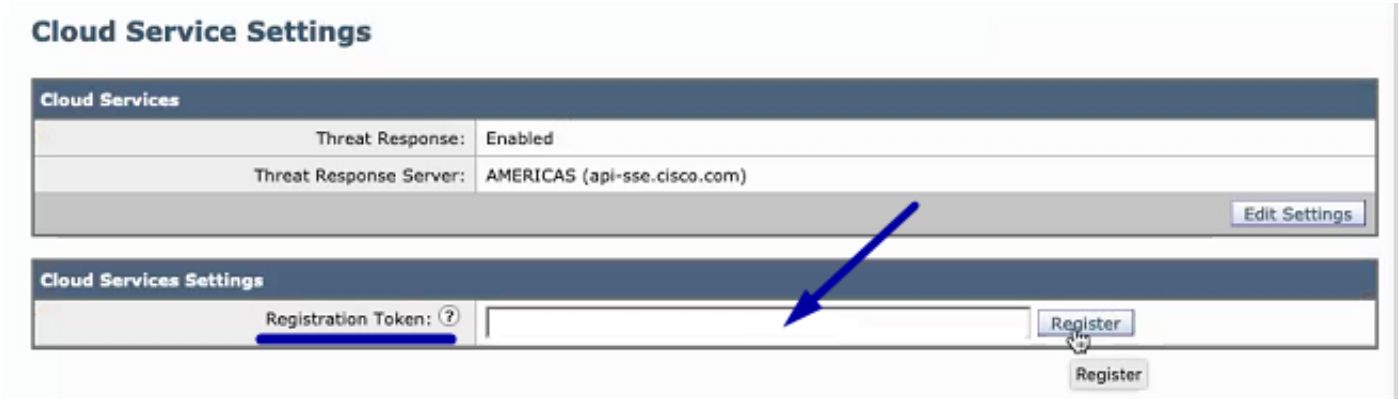
Etapa 4. Enviar e confirmar alterações

Énecessário 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.

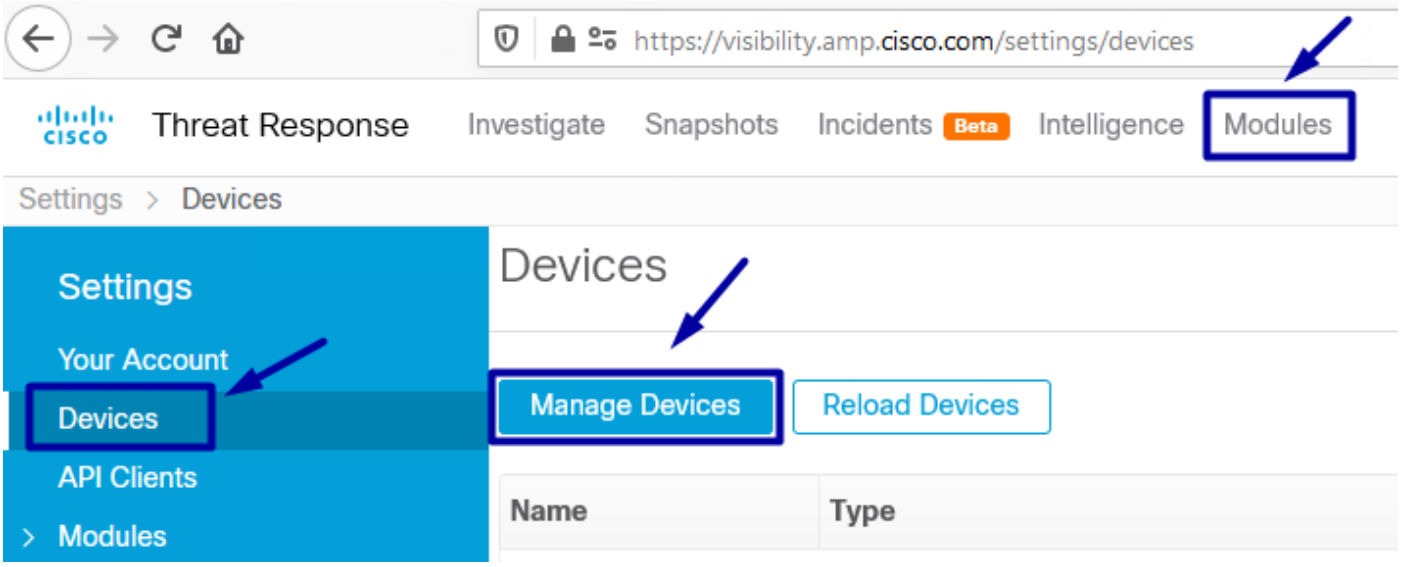




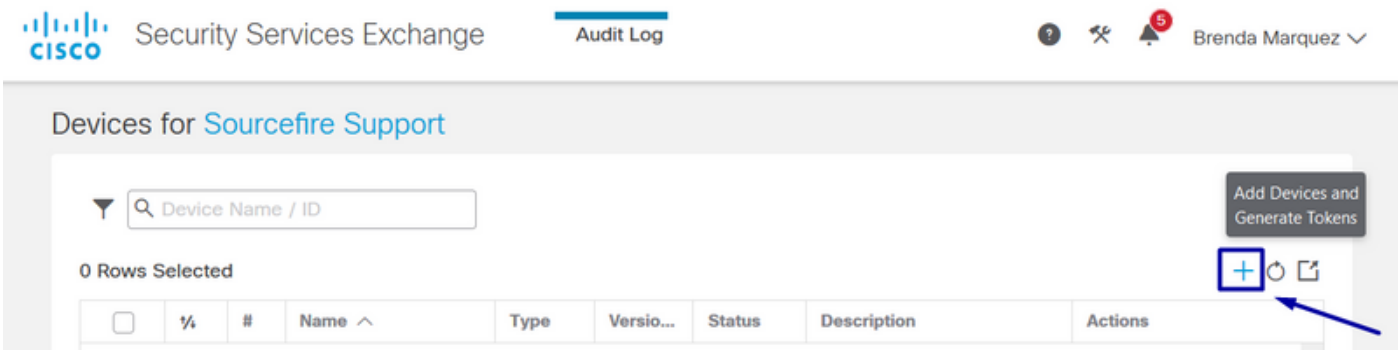


Etapa 5. Faça login no portal CTR e gere o token de registro solicitado no ESA

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

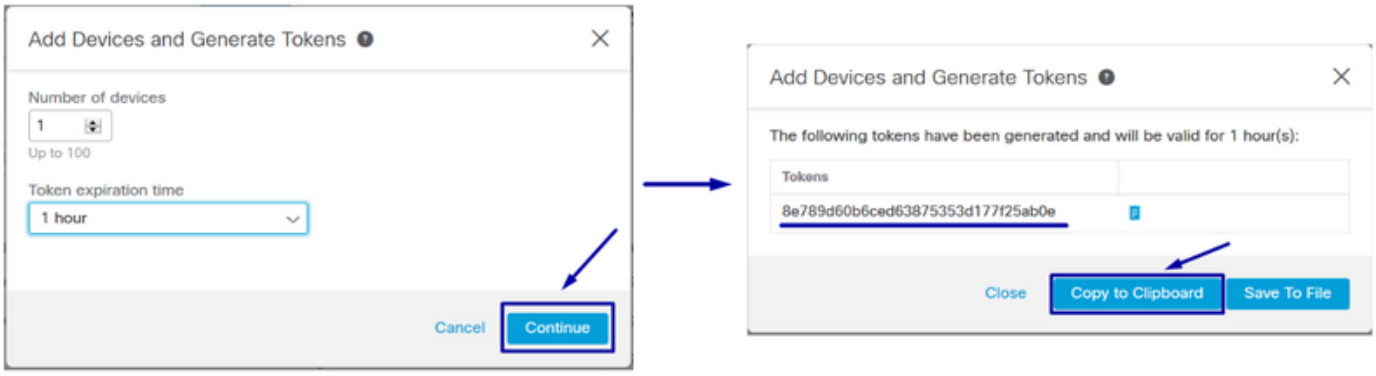


2.- O link Gerenciar dispositivos o redireciona para o Security Services Exchange (SSE), quando estiver lá, clique no ícone Adicionar dispositivos e Gerar tokens, como mostrado na imagem.



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

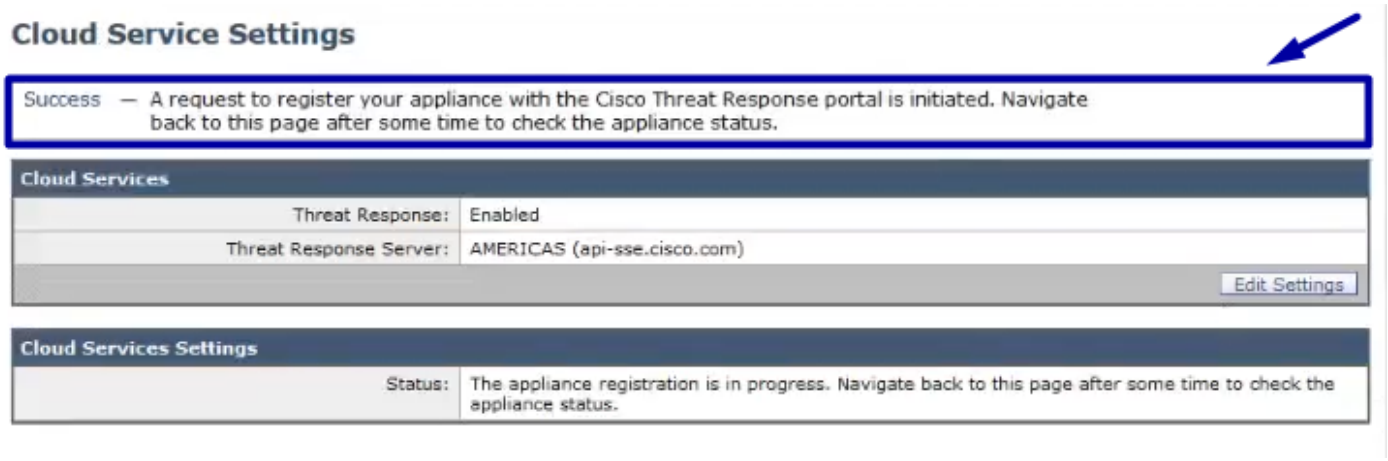
> **Tip**: Você pode selecionar o número de dispositivos a serem adicionados (de 1 e até 100) e também selecionar o tempo de expiração do token (1h, 2h, 4h, 6h, 8h, 12h, 01 dias, 02 dias, 03 dias, 04 dias e 05 dias).



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

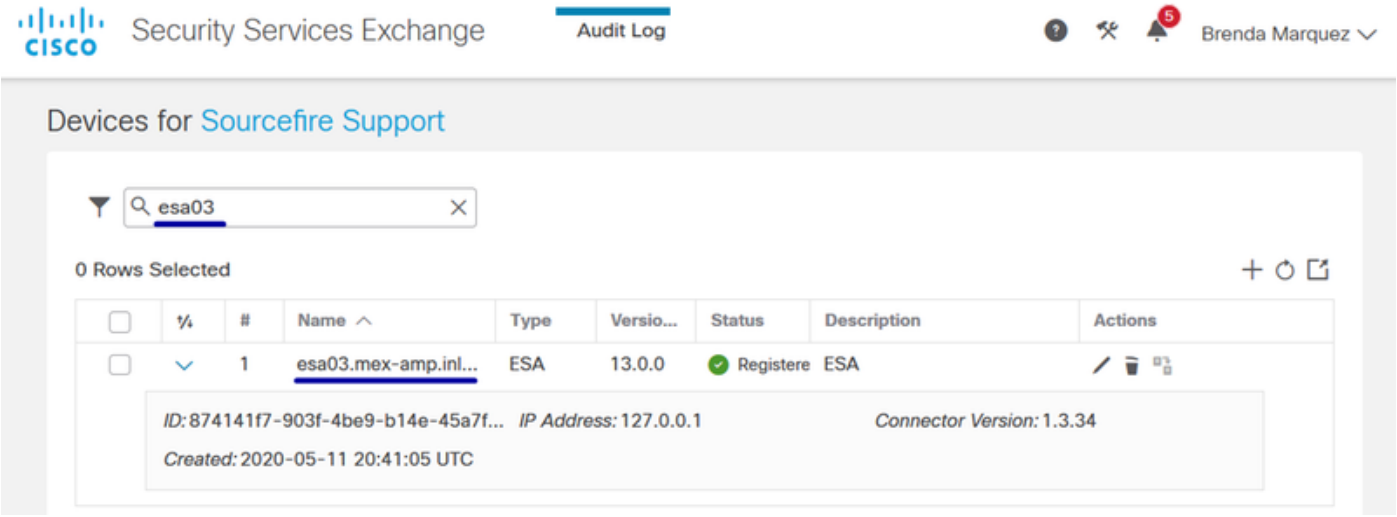
Quando o Token de registro for gerado, cole-o na seção Cloud Services Settings do ESA, como a imagem abaixo.

> **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.



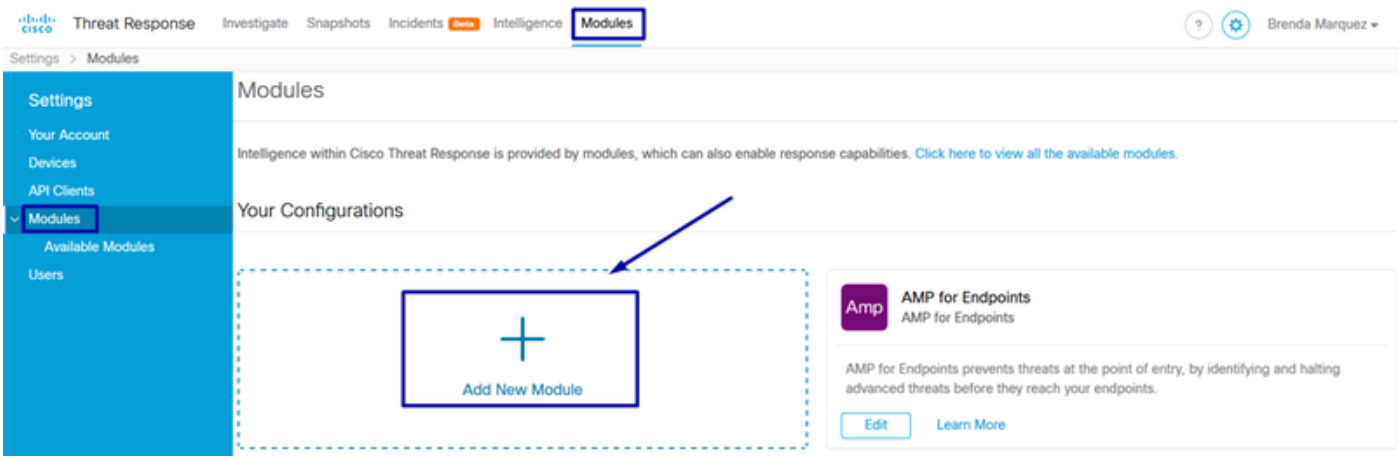
Passo 7. Verifique se o dispositivo ESA está no portal SSE

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

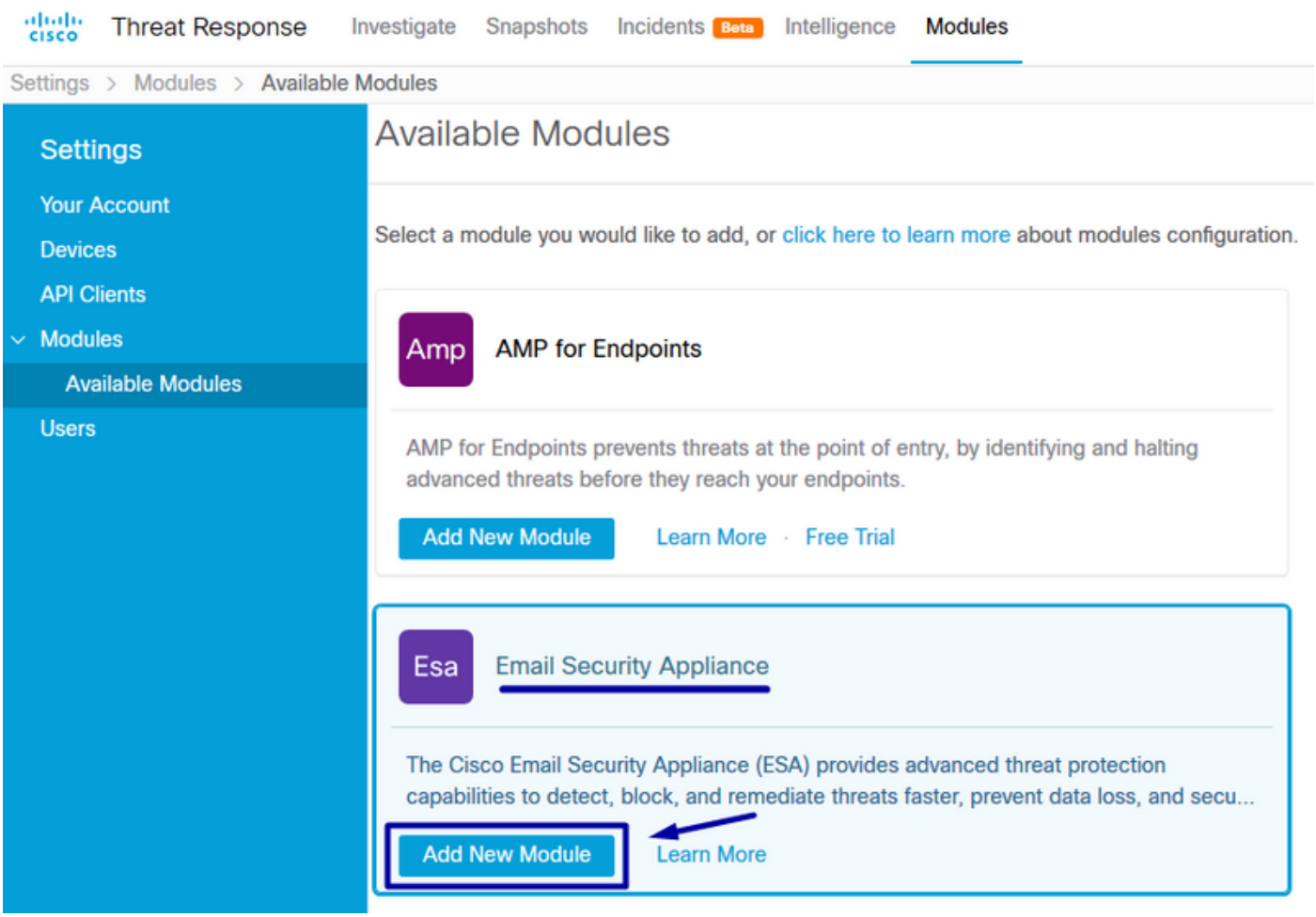


Etapa 8. Navegue até o portal CTR e adicione um novo módulo ESA

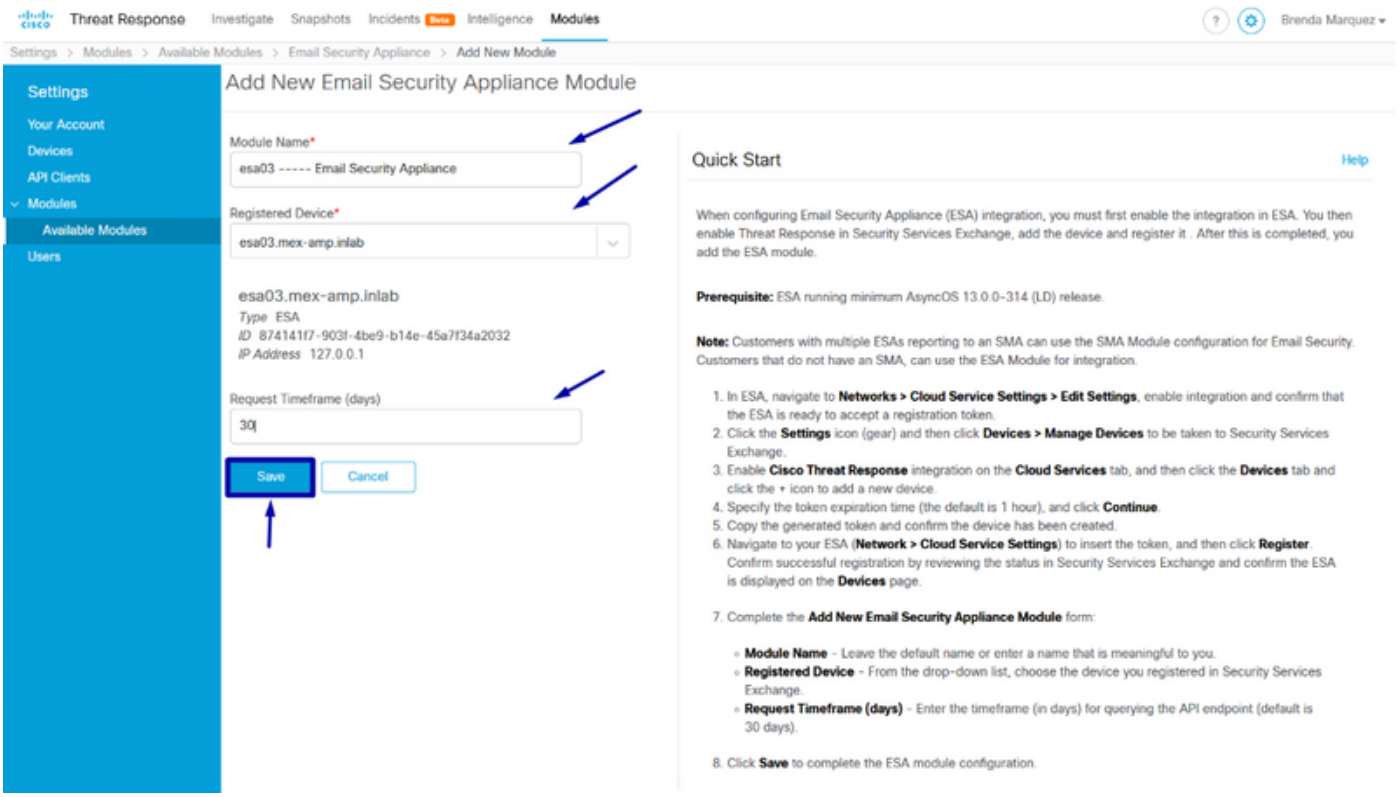
1.- Quando estiver no portal CTR, navegue até Modules > Add New Module (Módulos > Adicionar novo módulo), conforme mostrado na imagem.



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

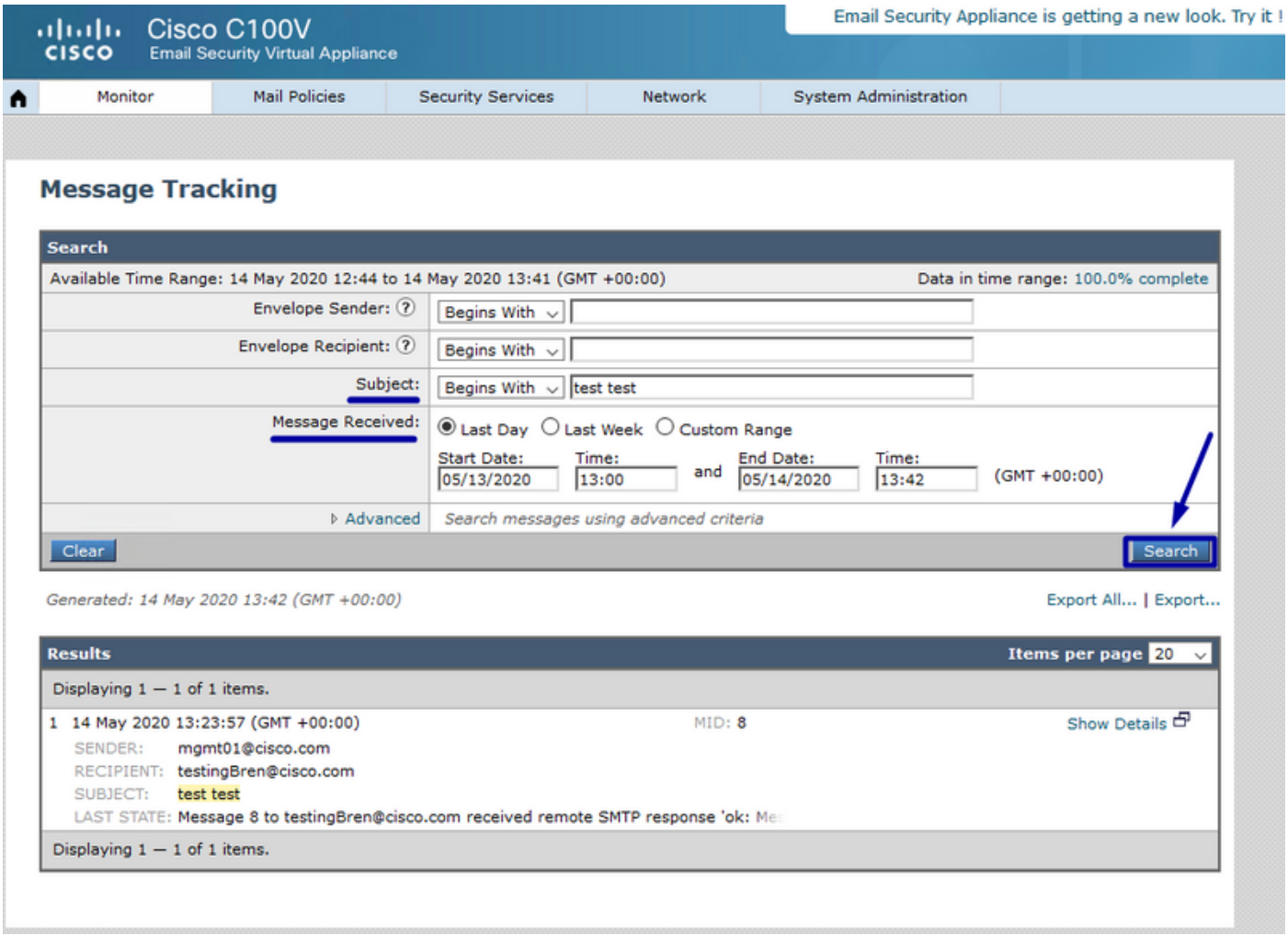


3.- Insira os campos: Nome do módulo, Dispositivo registrado (selecione o registrado anteriormente) e Prazo da solicitação (dias) e Salvar, como mostrado na imagem.

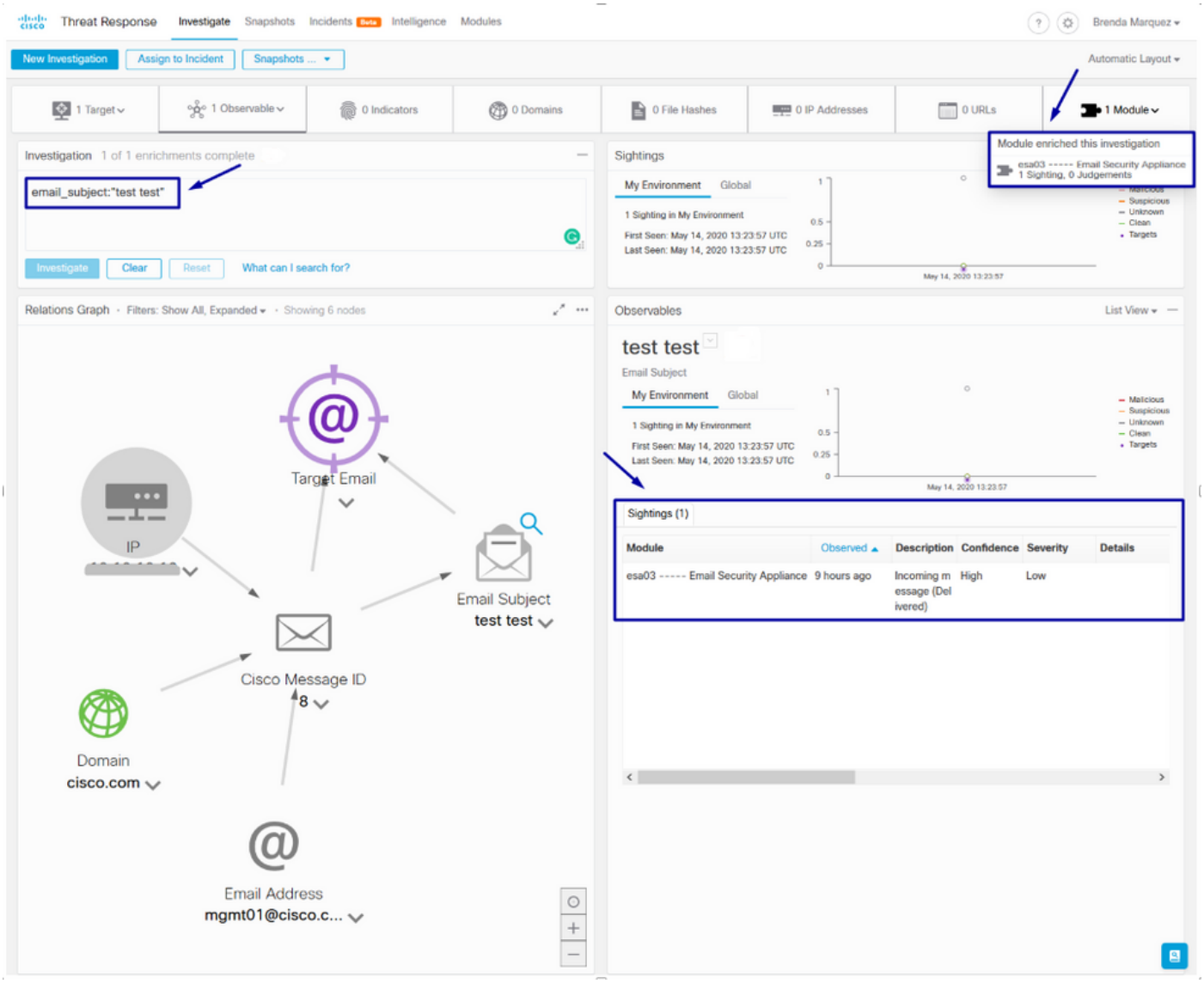


Verificar

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.



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



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

IP address	ip:"4.2.2.2"
Domain	domain:"cisco.com"
Sender email address	email:"noreply@cisco.com"
Email message header	email_messageid:"123-abc-456@cisco.com"

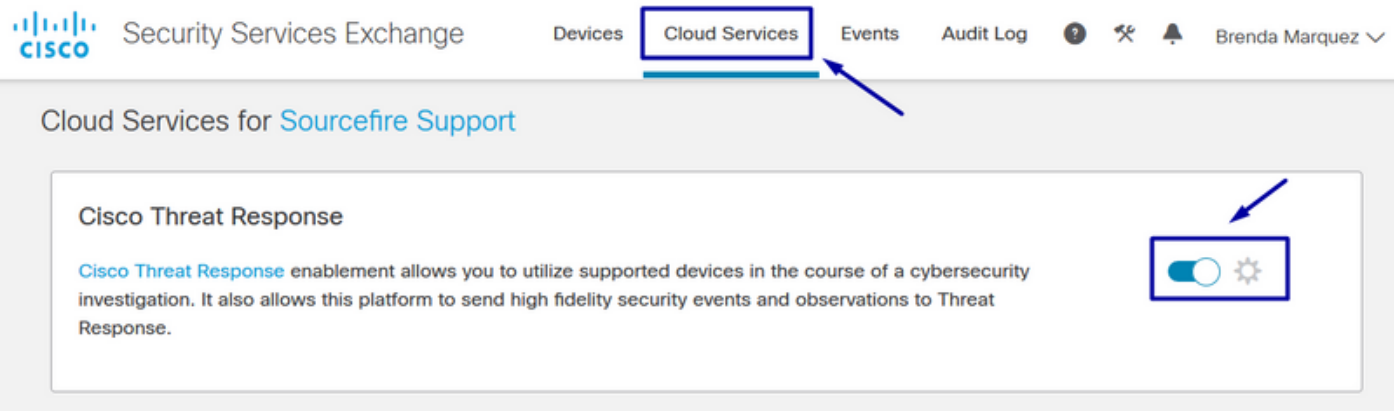
Email subject	email_subject:"Invoice Due"
Cisco Message ID (MID)	cisco_mid:"12345"
SHA256 filehash	sha256:"sha256filehash"
Email attachment file name	file_name:"invoice.pdf"

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