Integrar WSA com CTR

Contents

Introduction

Este documento descreve as etapas para integrar o Web Security Appliance (WSA) ao portal Cisco Threat Response (CTR).

Contribuído por Shikha Grover e editado por Yeraldin Sanchez Engenheiros do TAC da Cisco.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- acesso WSA
- acesso ao portal CTR
- Conta de segurança da Cisco

Componentes Utilizados

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

- Async Operating System versão 12.x ou posterior

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

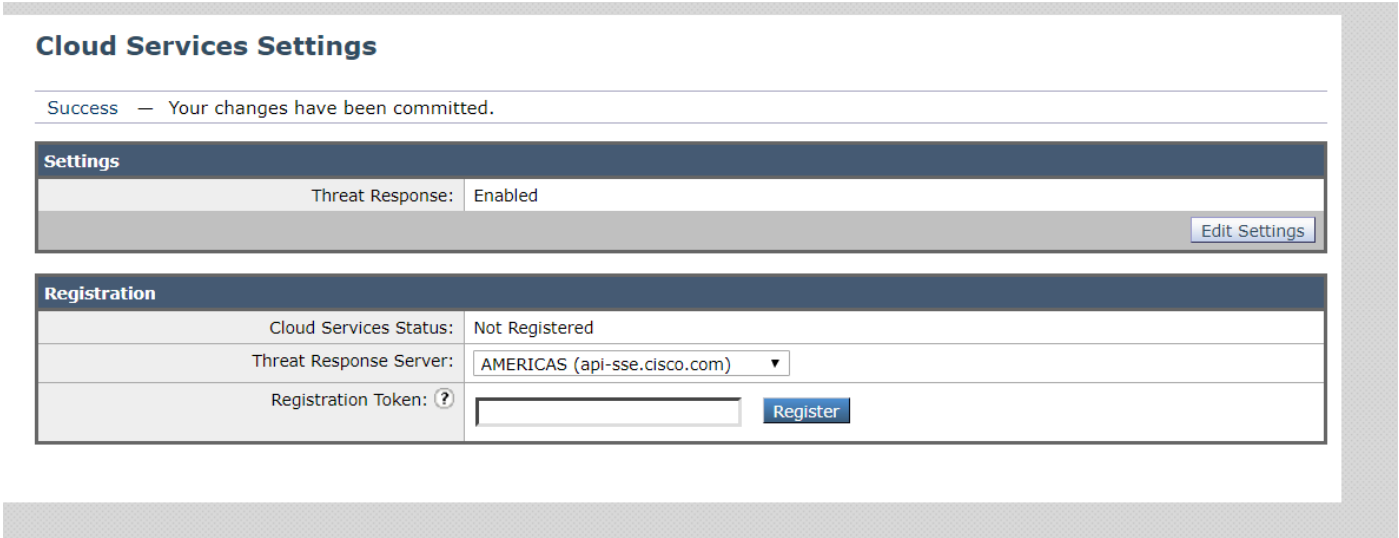
> **Caution**: Se você acessa o CTR com um URL regional do Pacífico Asiático, Japão e China (https://visibility.apjc.amp.cisco.com/), a integração com seu dispositivo não é suportada no momento.

Etapa 1. Ative **CTROBSERVABLE** em REPORTINGCONFIG na CLI e confirme as alterações, como mostrado na imagem.

```
WSA-12-0-1-173.COM> reportingconfig


hoose the operation you want to perform:
 COUNTERS - Limit counters recorded by the reporting system.
 WEBTRACKINGQUERYTIMEOUT - Timeout value for Webtracking Queries.
 AVERAGEOBJECTSIZE - Average HTTP Object Size used for Bandwidth Savings
alculation.
 WEBEVENTBUCKETING - Enable or Disable web transaction event bucketing.
 CTROBSERVABLE - Enable or Disable CTR observable based indexing.
 CENTRALIZED - Enable/Disable Centralized Reporting for this WSA appliance.
]> ctrobservable

TR observable indexing currently Enabled.
re you sure you want to change the setting? [N]> y


hoose the operation you want to perform:
 COUNTERS - Limit counters recorded by the reporting system.
 WEBTRACKINGQUERYTIMEOUT - Timeout value for Webtracking Queries.
 AVERAGEOBJECTSIZE - Average HTTP Object Size used for Bandwidth Savings Calculation.
 WEBEVENTBUCKETING - Enable or Disable web transaction event bucketing.
 CTROBSERVABLE - Enable or Disable CTR observable based indexing.
 CENTRALIZED - Enable/Disable Centralized Reporting for this WSA appliance.
```

Etapa 2. Configure o portal de nuvem do Security Service Exchange (SSE), navegue até **Network >Cloud Services Settings > Edit settings**, clique em **Enable** e **Submit**, conforme mostrado na imagem.

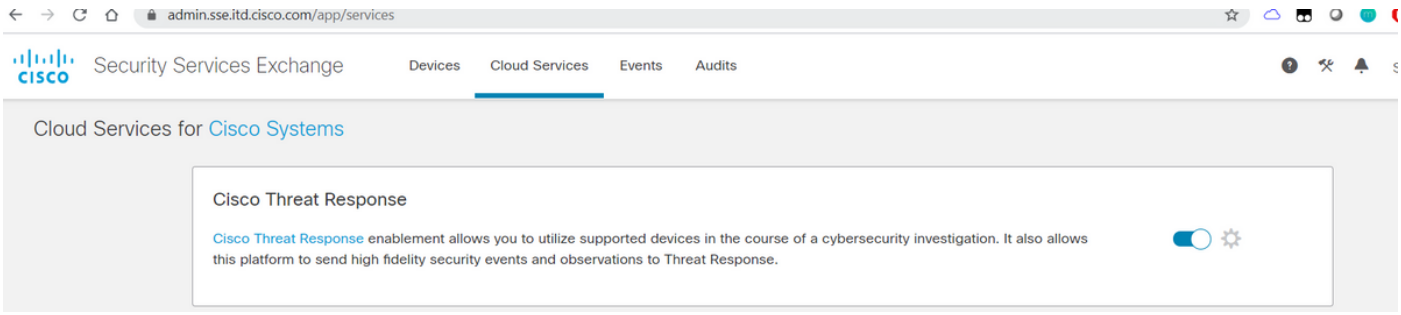
Escolha a nuvem conforme o local, como mostrado na imagem.



Etapa 3. Se você não tiver uma conta do Cisco Security, poderá criar uma conta de usuário no portal Cisco Threat Response com direitos de acesso de administrador.

Para criar uma nova conta de usuário, navegue até a página de login do portal Cisco Threat Response.

Etapa 4. Ative o Cisco Threat Response em serviços de nuvem no portal SSE, como mostrado na imagem.



Etapa 5. Verifique se o WSA tem acessibilidade na porta 443 para o portal SSE:

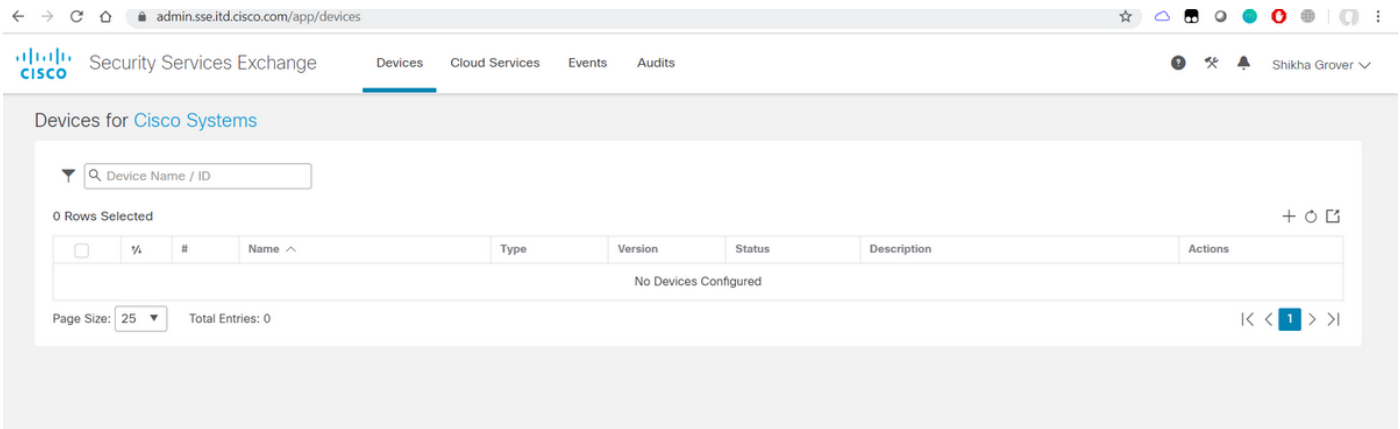
- api.eu.sse.itd.cisco.com (Europa)
- api-sse.cisco.com (América)

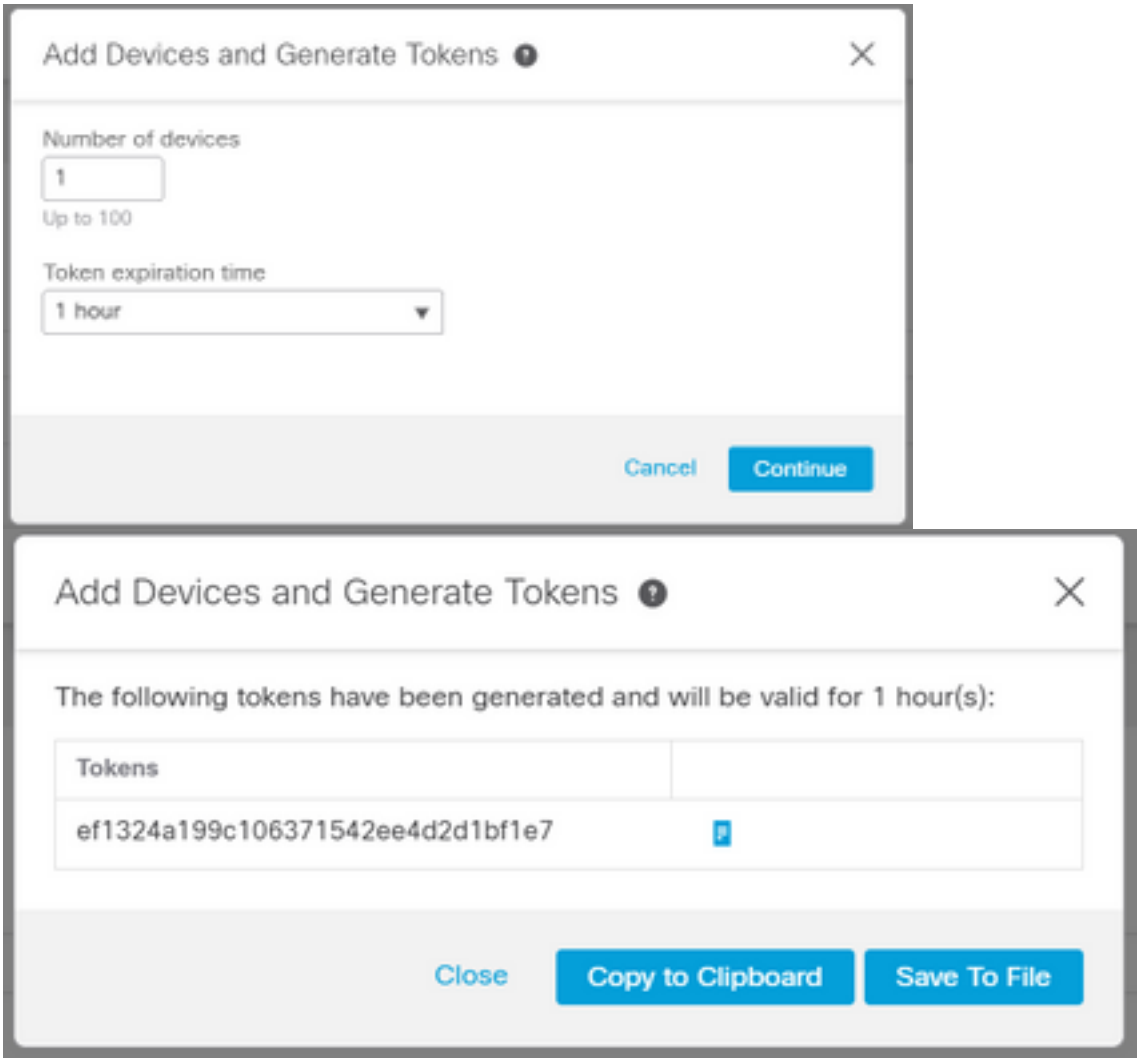
Registrar o aplicativo

Etapa 1. Obtenha um token de registro no portal do Security Services Exchange (SSE) para registrar seu dispositivo no portal do Security Services Exchange.

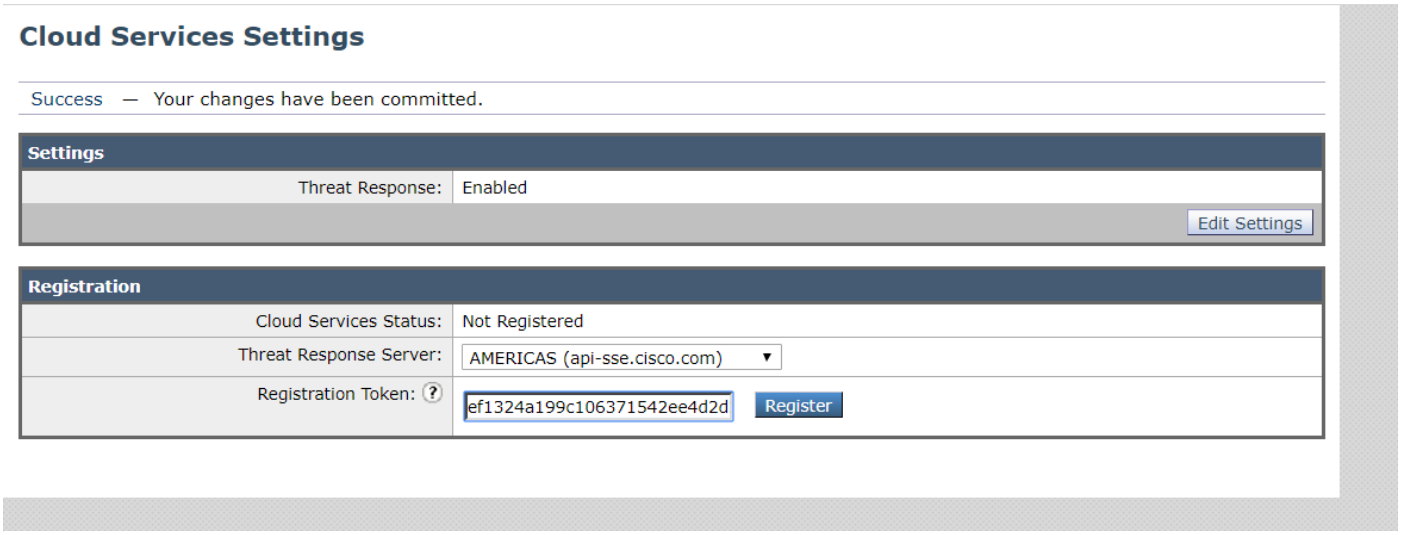
O link do portal SSE é https://admin.sse.itd.cisco.com/app/devices.

> **Note**: Use credenciais de conta CTR para fazer login no portal SSE.



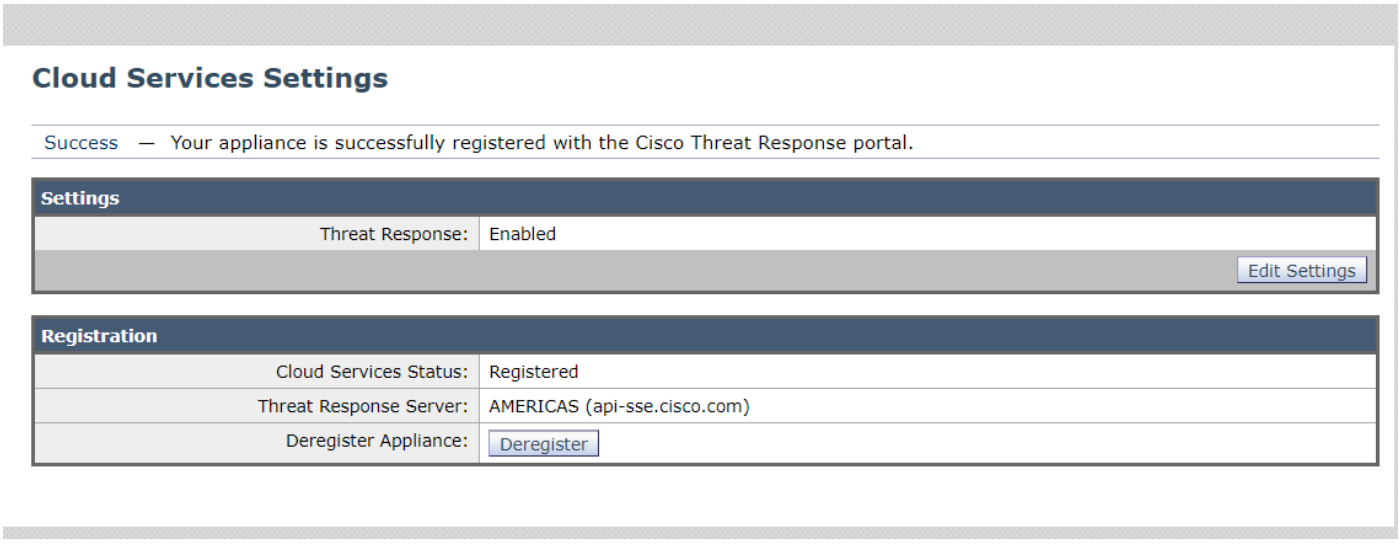


Etapa 2. Insira o token de registro obtido do portal do Security Services Exchange no WSA e clique em **Registrar**, como mostrado na imagem.

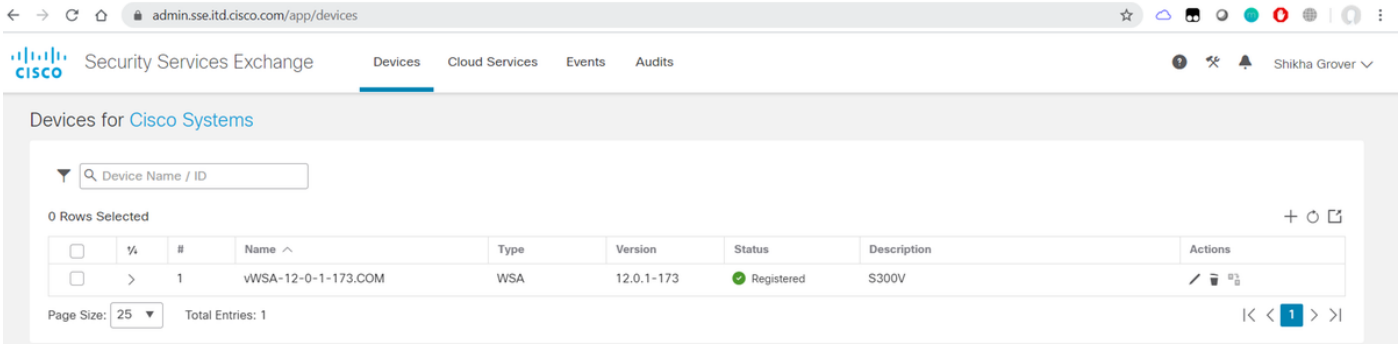


Etapa 3. Após alguns segundos, você verá que o registro foi bem-sucedido.

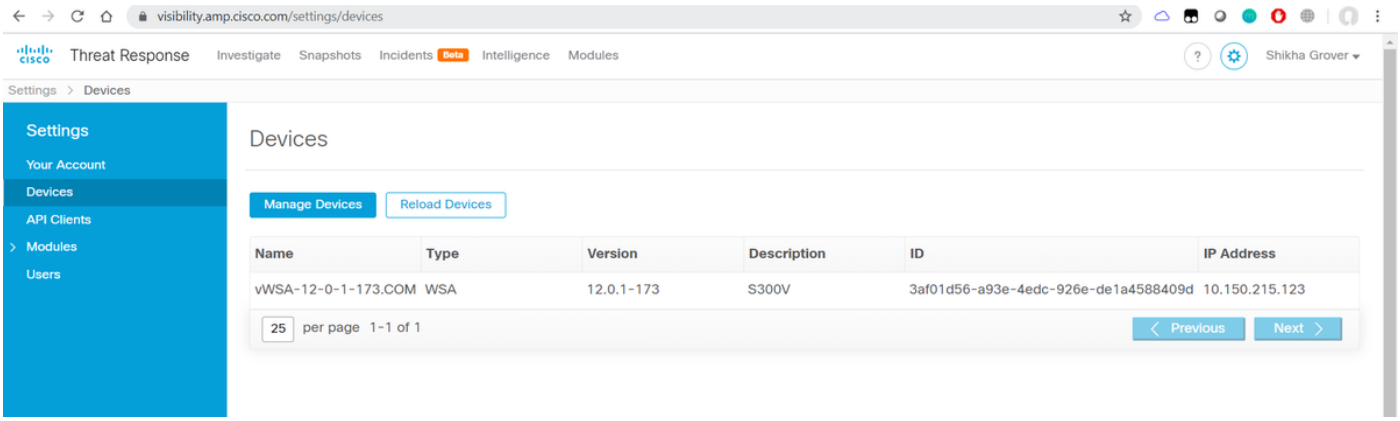
Caution: Verifique se o token gerado é usado antes de expirar.



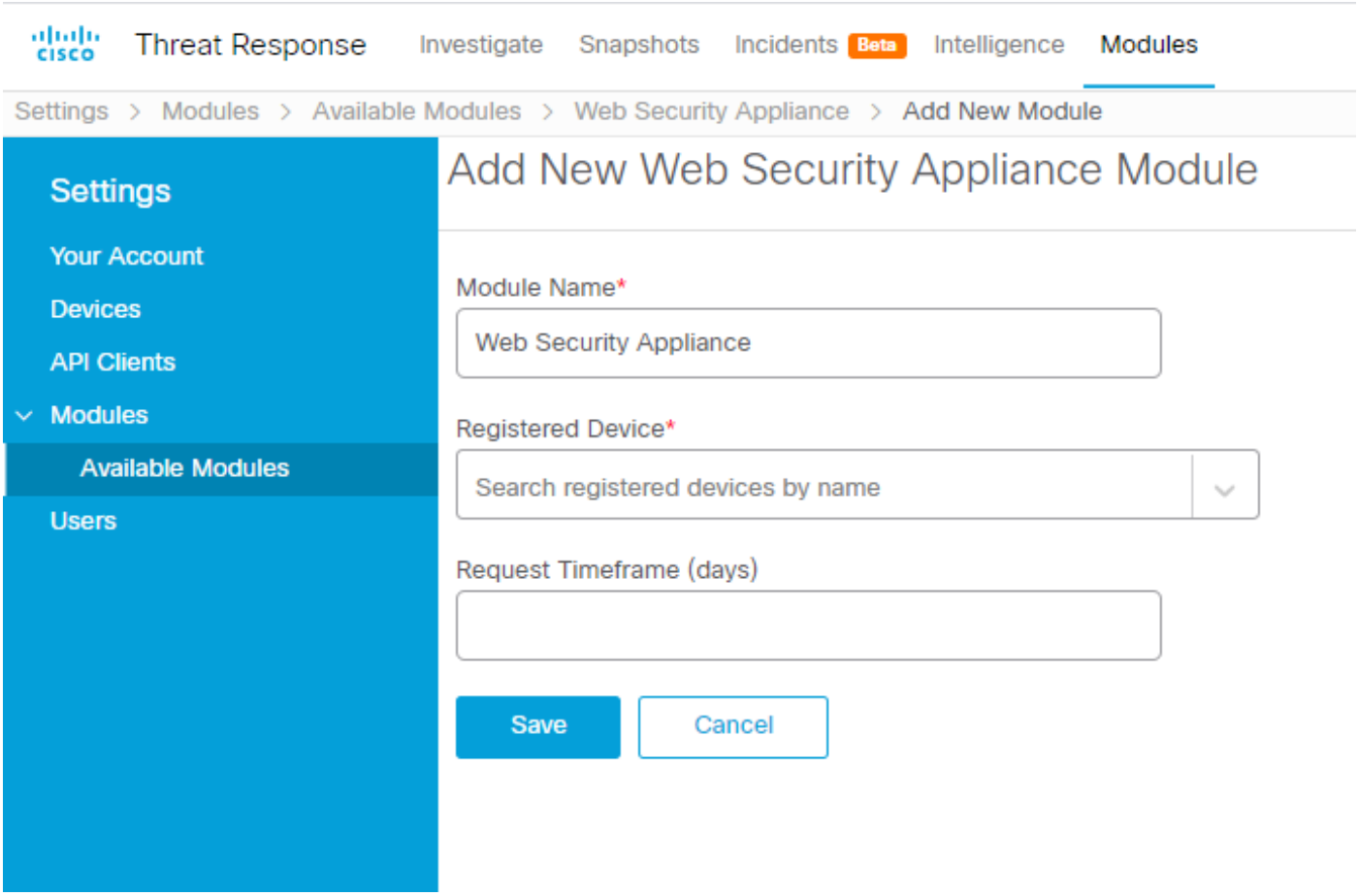
Etapa 4. No portal SSE, você pode ver o status do dispositivo.



Etapa 5. No portal CTR, o dispositivo está registrado.



Você pode associar esse dispositivo a um módulo, navegar para **Módulos > Adicionar novo módulo > Web Security Appliance**, como mostrado na imagem.



O dispositivo agora está integrado. Você pode passar pelo tráfego do WSA e investigar ameaças no portal CTR.

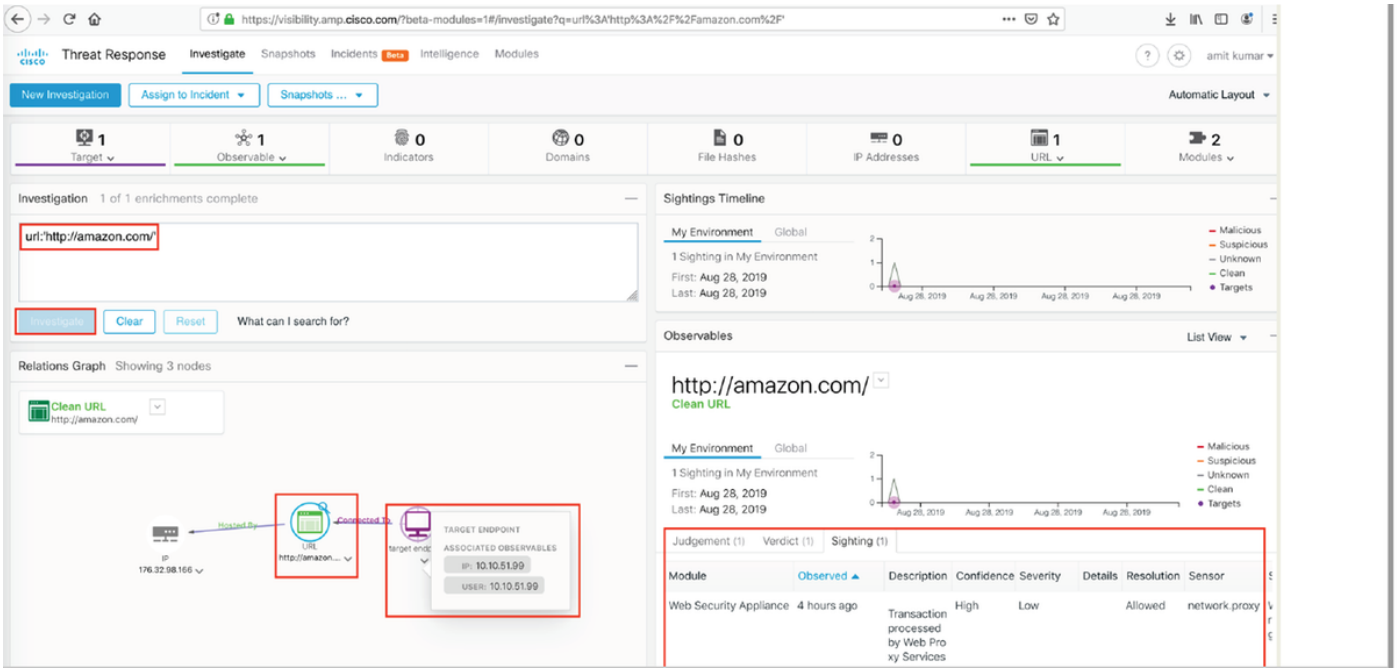
Verificar

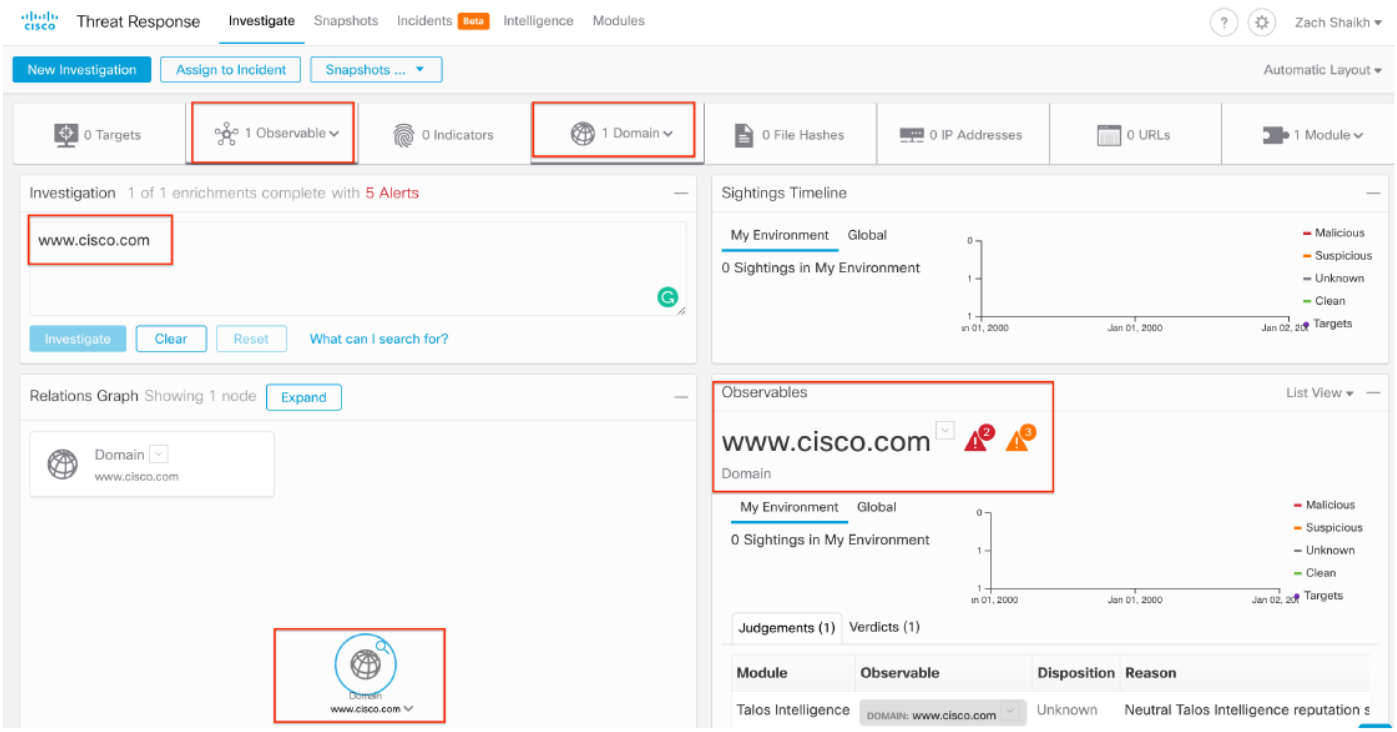
Use esta seção para confirmar se a sua configuração funciona corretamente.

Enrichments(Consultando os registros WSA) disponíveis para o módulo WSA e seu formato suportado para executar a consulta no portal CTR:

- Domínio - domínio:"com"
- URL - url:"http://www.neverssl.com"
- SHA256 - sha256:"8d3aa8badf6e5a38e1b6d59a254969b1e0274f8fa120254ba1f7e0291872379"
- IP - ip:"172.217.26.164"
- Nome do arquivo - nome_do_arquivo:"test.txt"

Enriquecimentos em uso como exemplo:





Sinta-se à vontade para me informar se perdi algo que deveria ser incluído. Sinta-se à vontade para me informar se perdi algo que deveria ser incluído. Sinta-se à vontade para me informar se perdi algo que deveria ser incluído. Sinta-se à vontade para me informar se perdi algo que deveria ser incluído.