Integración de WSA con CTR

Contenido

Introducción

Este documento describe los pasos para integrar Web Security Appliance (WSA) con el portal Cisco Threat Response (CTR).

Colaborado por Shikha Grover y editado por Yeraldin Sanchez Ingenieros del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- acceso WSA
- acceso al portal CTR
- Cuenta de seguridad de Cisco

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Async Operating System versión 12.x o 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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

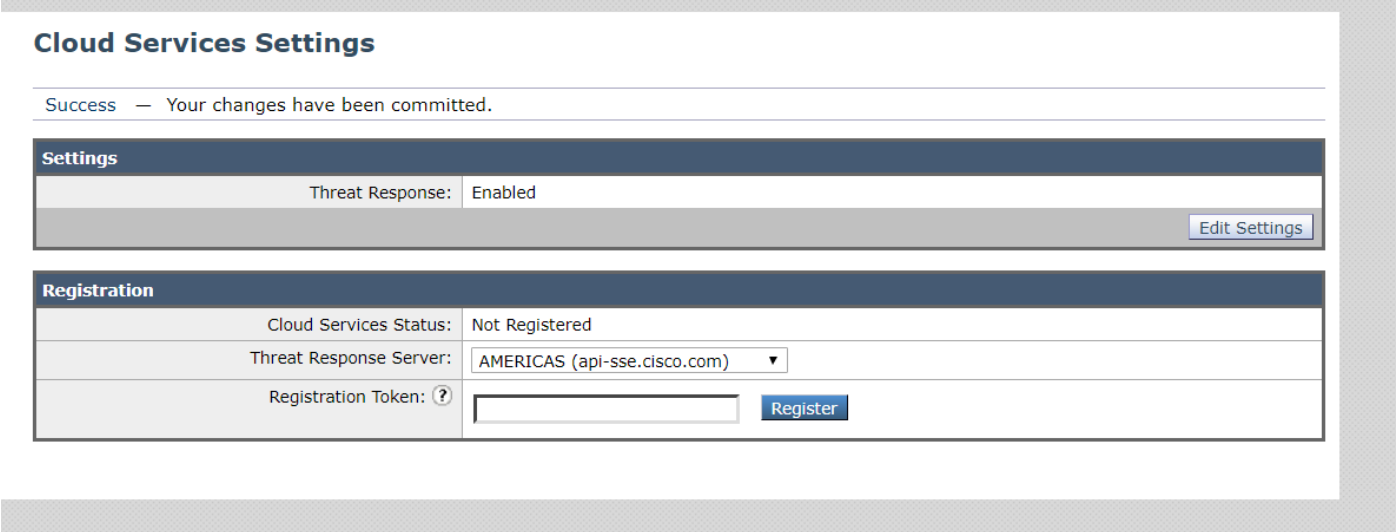
> **Precaución:** Si tiene acceso a CTR con una URL regional de Asia Pacífico, Japón y China (https://visibility.apjc.amp.cisco.com/), la integración con su dispositivo no es compatible actualmente.

Paso 1. Habilite **CTROBSERVABLE** en REPORTINGCONFIG en la CLI y realice los cambios, como se muestra en la imagen.

```
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.
```

Paso 2. Configure el portal en la nube de Security Service Exchange (SSE), navegue hasta **Red > Configuración de servicios en la nube > Editar configuración**, haga clic en **Habilitar** y **Enviar**, como se muestra en la imagen.

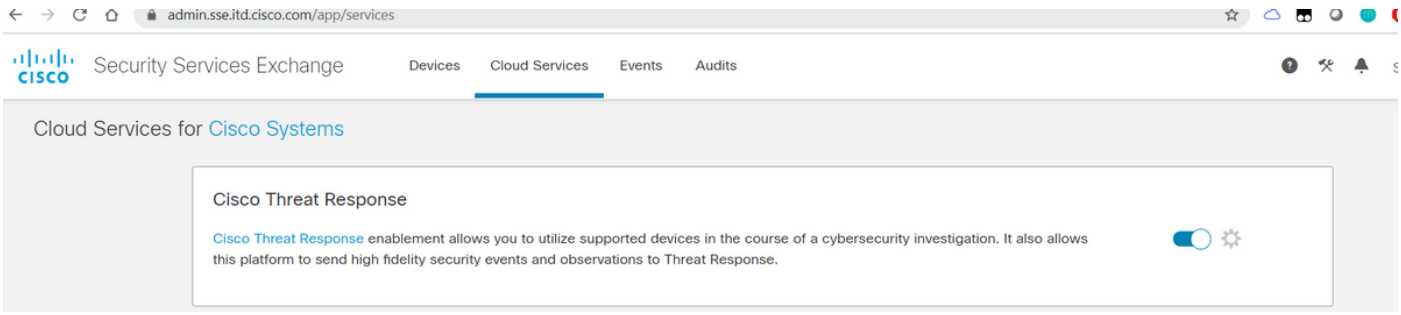
Elija la nube según su ubicación, como se muestra en la imagen.



Paso 3. Si no tiene una cuenta de Cisco Security, puede crear una cuenta de usuario en el portal de Cisco Threat Response con derechos de acceso de administrador.

Para crear una nueva cuenta de usuario, navegue a la página de inicio de sesión del portal de respuesta a amenazas de Cisco.

Paso 4. Habilite Cisco Threat Response en Cloud Services en el portal SSE, como se muestra en la imagen.



Paso 5. Asegúrese de que WSA tenga disponibilidad en el puerto 443 al portal SSE:

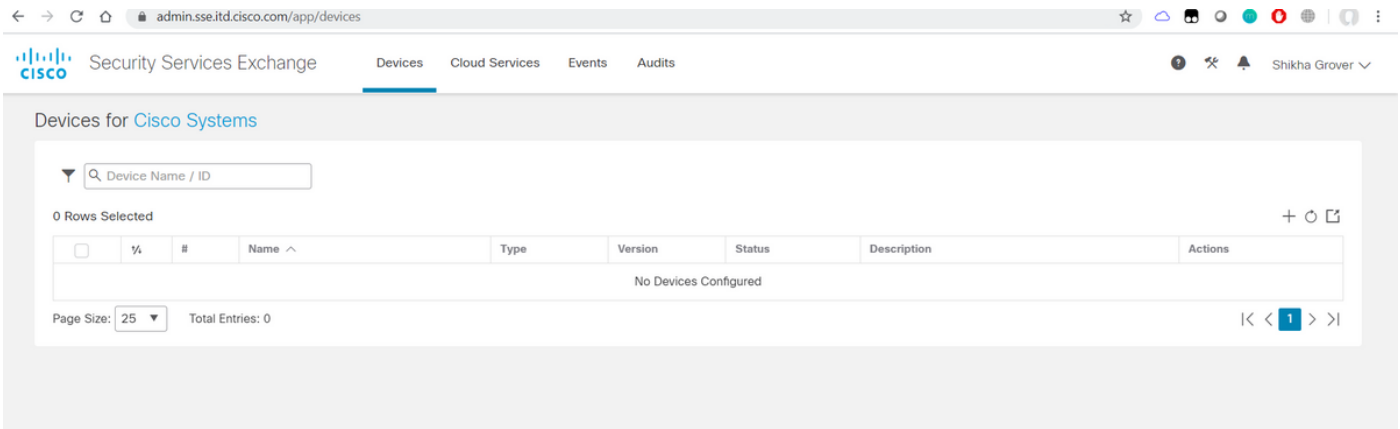
- api.eu.sse.itd.cisco.com (Europa)
- api-sse.cisco.com (América)

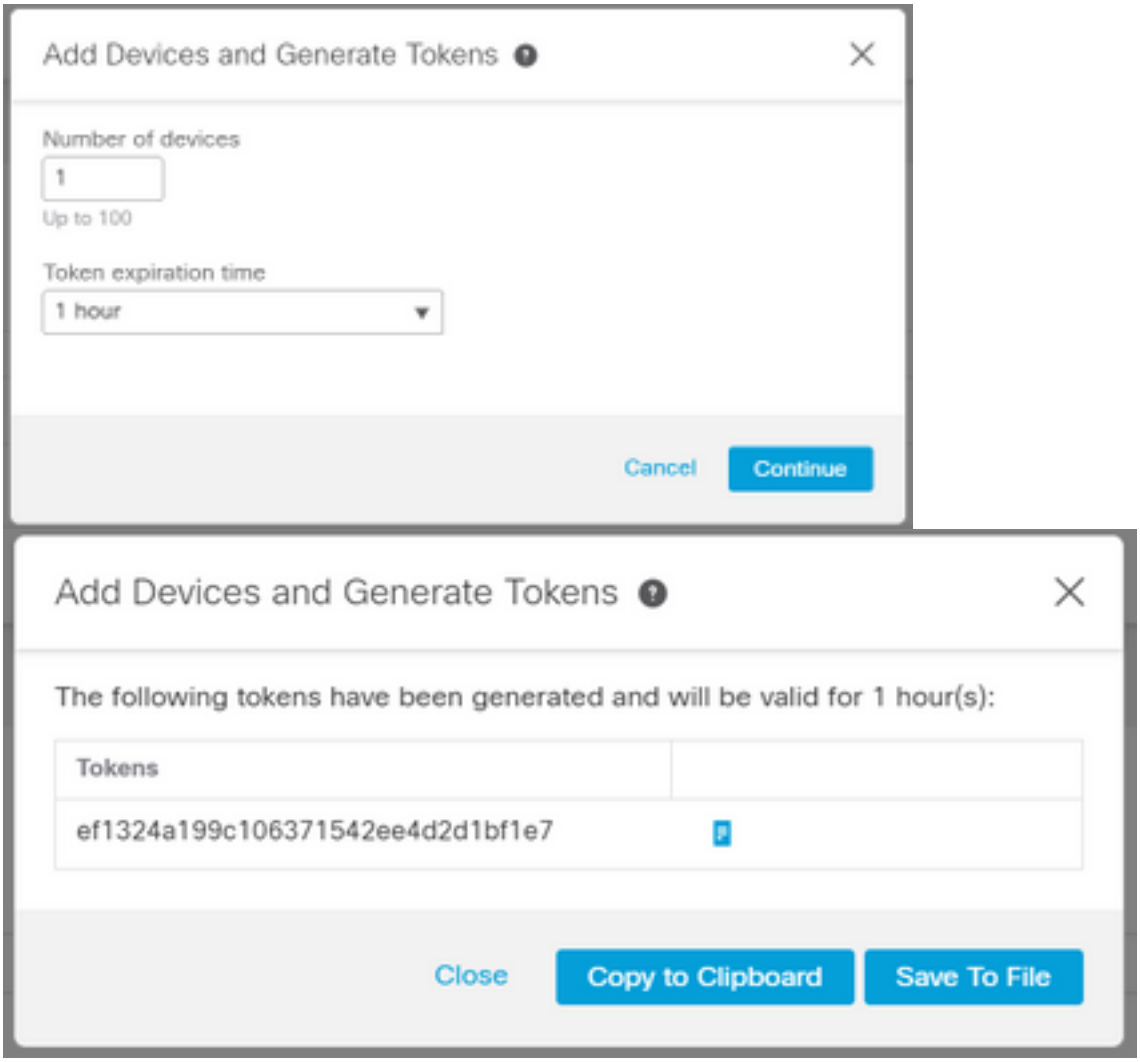
Registrar el dispositivo

Paso 1. Obtenga un token de registro del portal Security Services Exchange (SSE) para registrar su dispositivo en el portal Security Services Exchange.

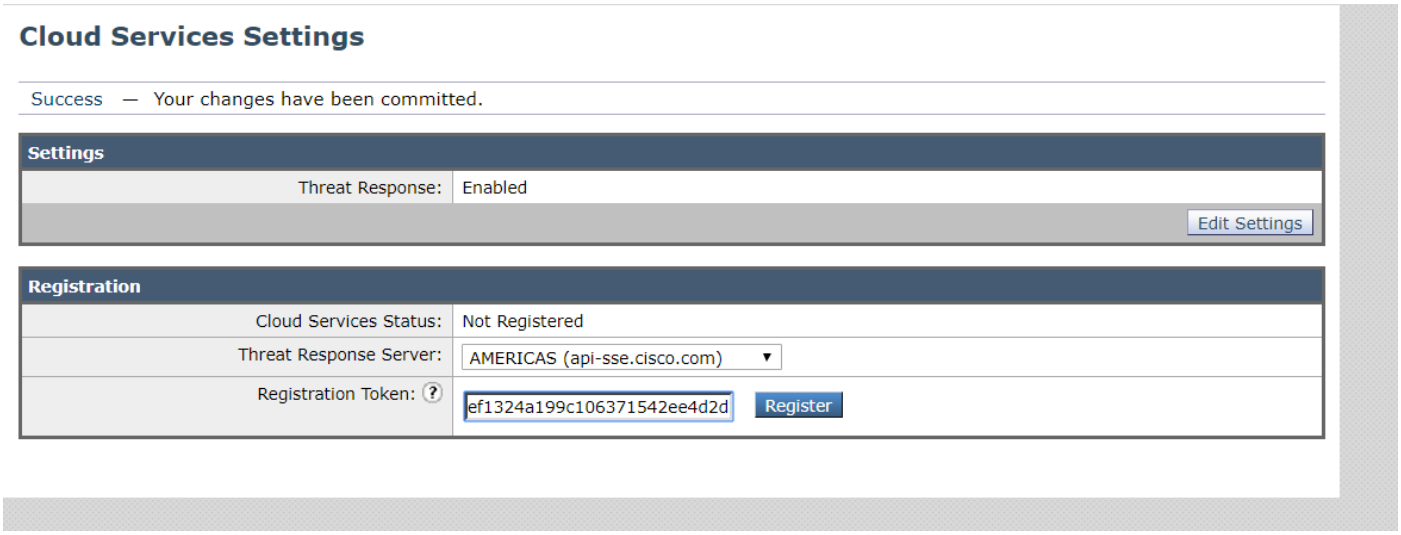
El enlace del portal SSE es https://admin.sse.itd.cisco.com/app/devices.

> **Nota:** Utilice las credenciales de la cuenta CTR para iniciar sesión en el portal SSE.



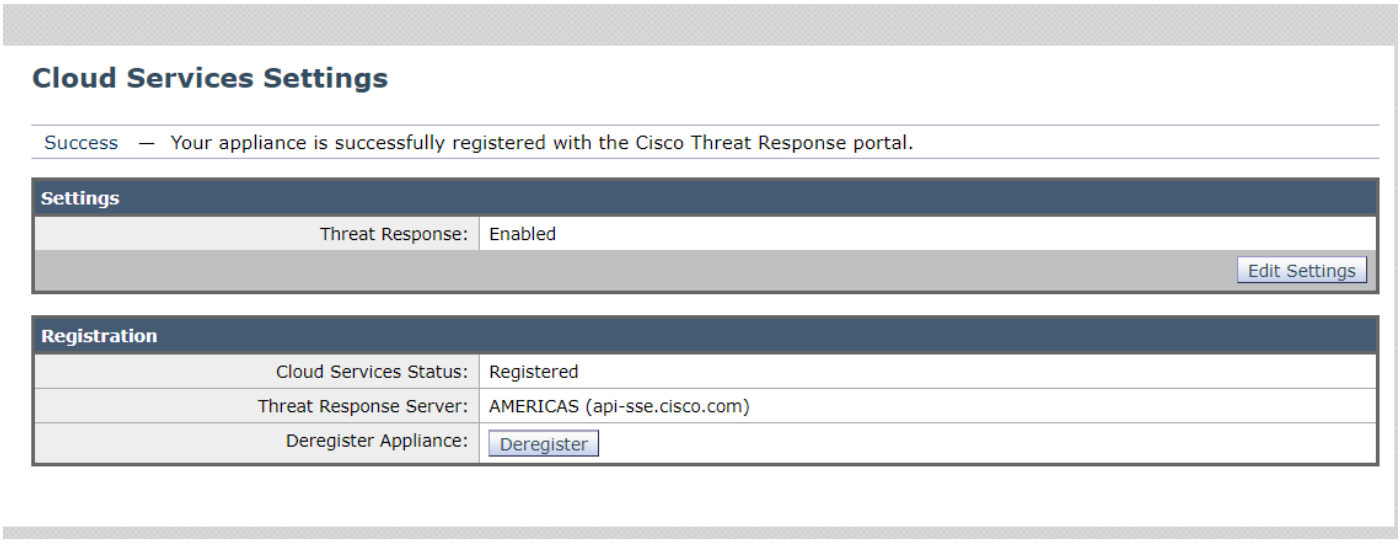


Paso 2. Ingrese el token de registro obtenido del portal Security Services Exchange en WSA y haga clic en **Register**, como se muestra en la imagen.

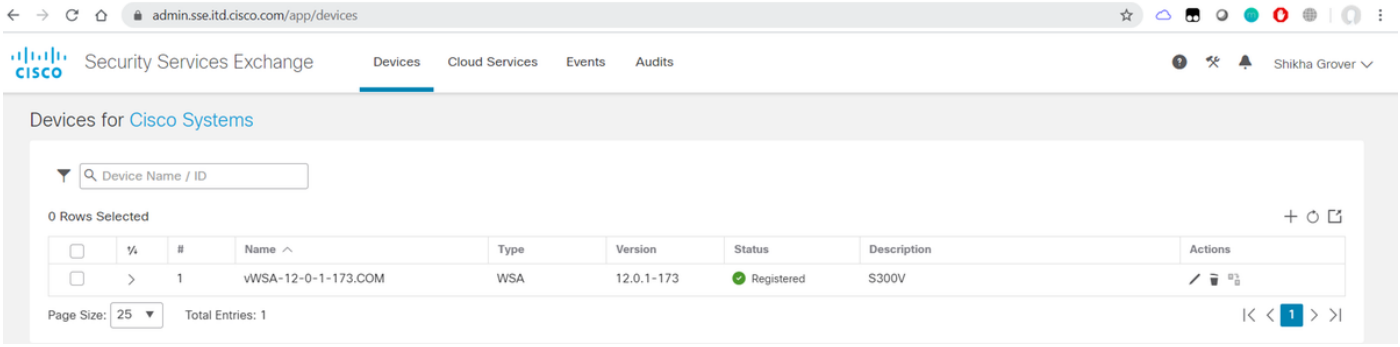


Paso 3. Después de unos segundos, verá que el registro se realiza correctamente.

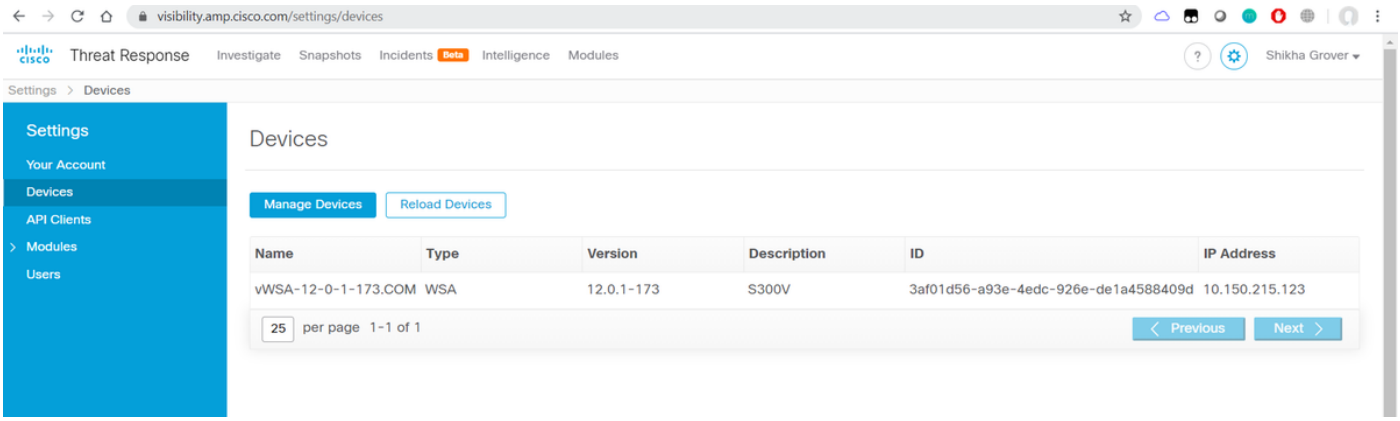
Precaución: Asegúrese de que el token generado se utiliza antes de que caduque.



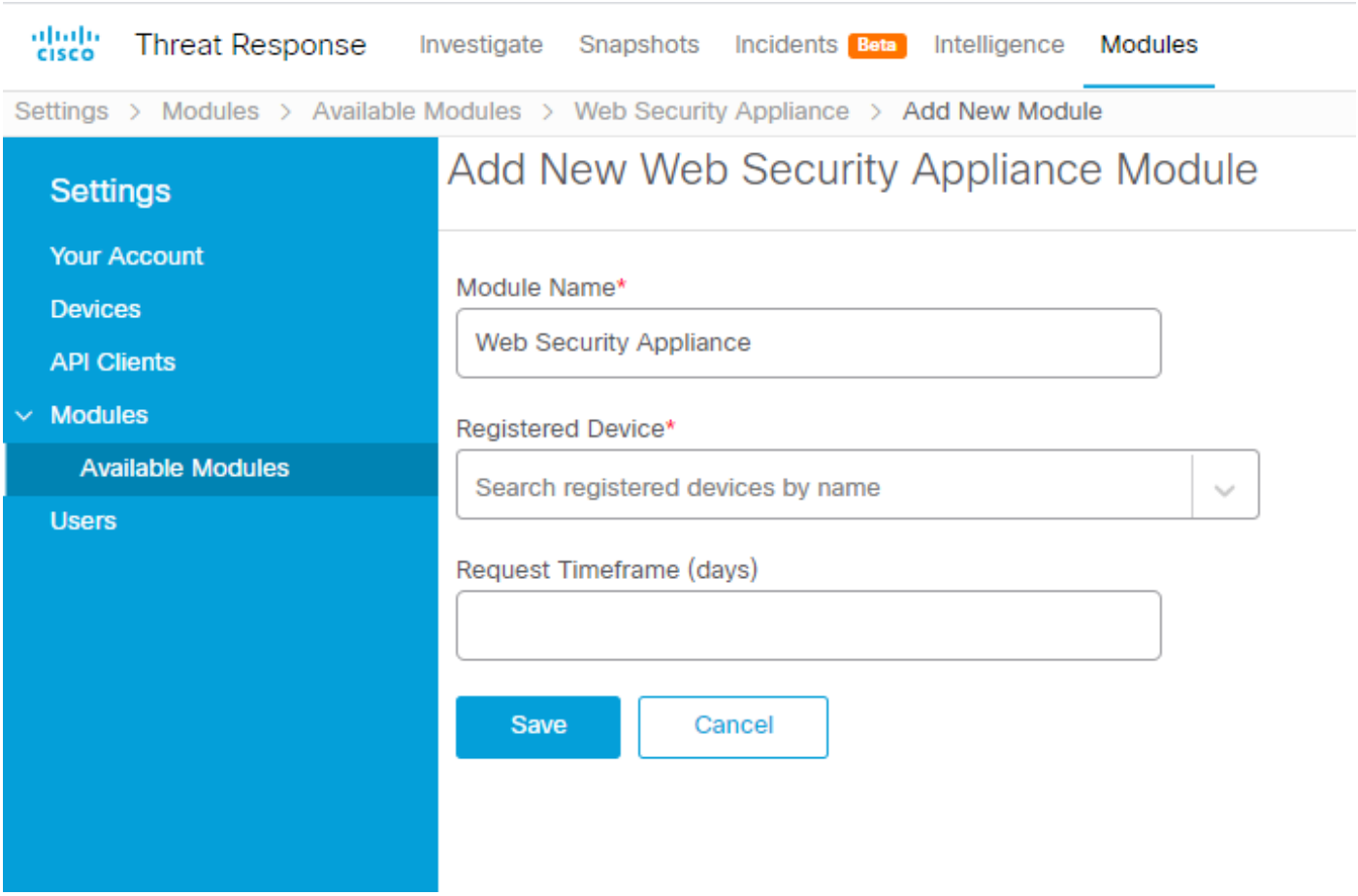
Paso 4. En el portal SSE, puede ver el estado del dispositivo.



Paso 5. En el portal CTR aparece el dispositivo registrado.



Puede asociar este dispositivo a un módulo, navegue hasta **Módulos > Agregar nuevo módulo > Dispositivo de seguridad web**, como se muestra en la imagen.



El dispositivo ya está integrado. Puede pasar el tráfico desde WSA e investigar las amenazas en el portal CTR.

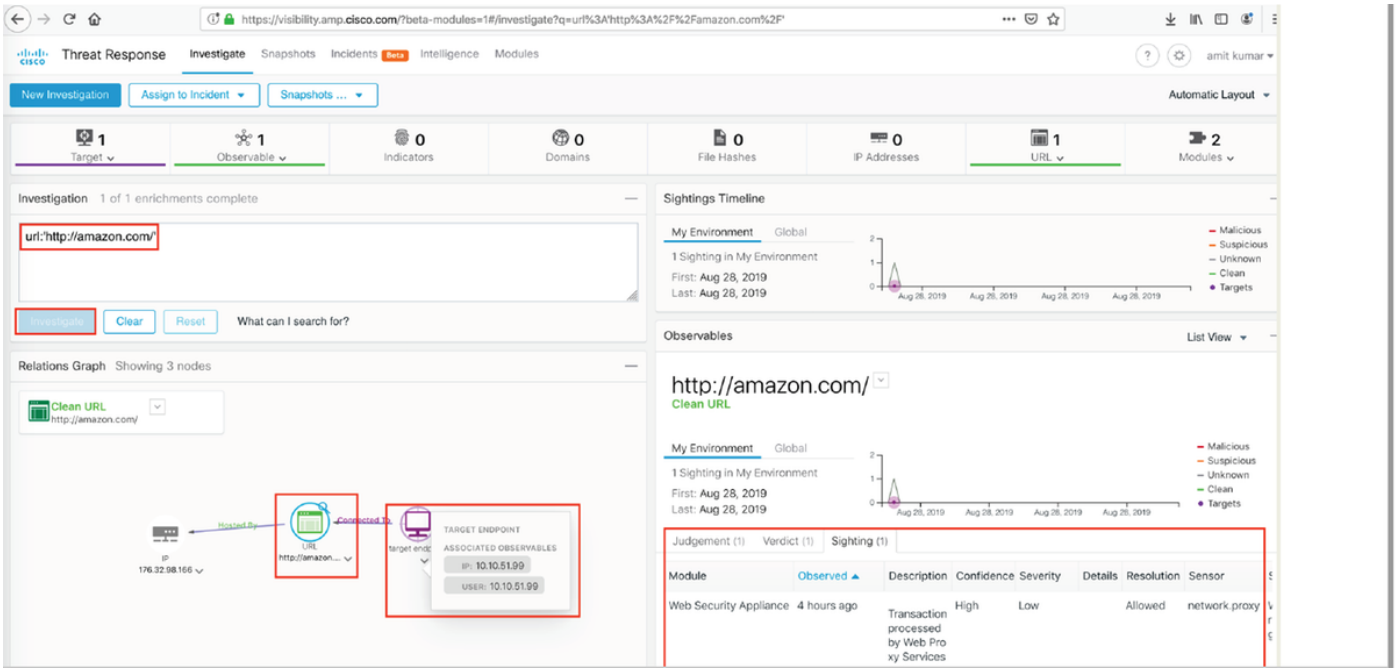
Verificación

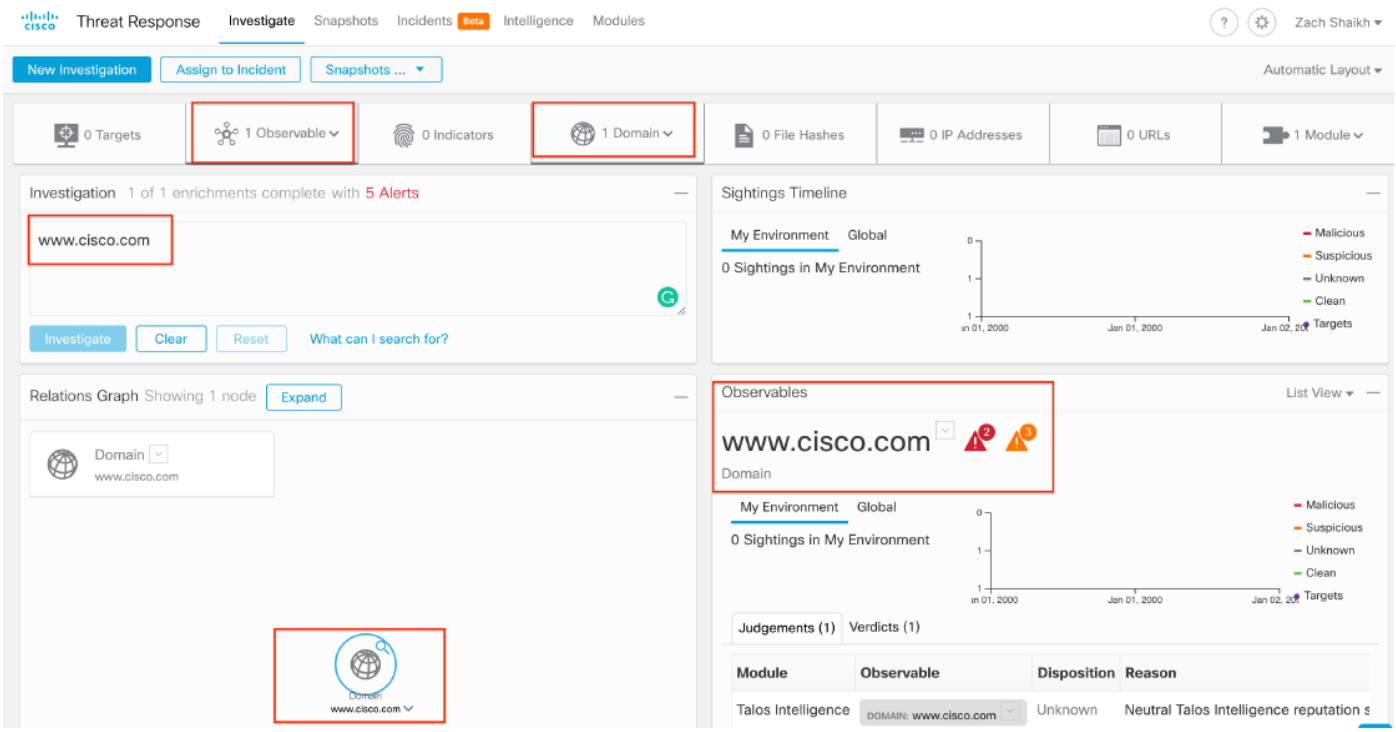
Use esta sección para confirmar que su configuración funciona correctamente.

Enrichamientos(Consultar los registros WSA) disponibles para el módulo WSA y su formato admitido para ejecutar la consulta desde el portal CTR:

- Dominio - dominio:"com"
- URL - url:"http://www.neverssl.com"
- SHA256 - sha256:"8d3aa8badf6e5a38e1b6d59a254969b1e0274f8fa120254ba1f7e02999 1872379"
- IP - ip:"172.217.26.164"
- Nombre - nombre_archivo:"test.txt"

Enriquecimientos en uso como ejemplo:





No dude en decirme si me he perdido algo que debería incluirse. No dude en decirme si me he perdido algo que debería incluirse. No dude en decirme si me he perdido algo que debería incluirse. No dude en decirme si me he perdido algo que debería incluirse.