

# Integración de WSA con CTR

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Registrar el dispositivo](#)

[Verificación](#)

## 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

Choose 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

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

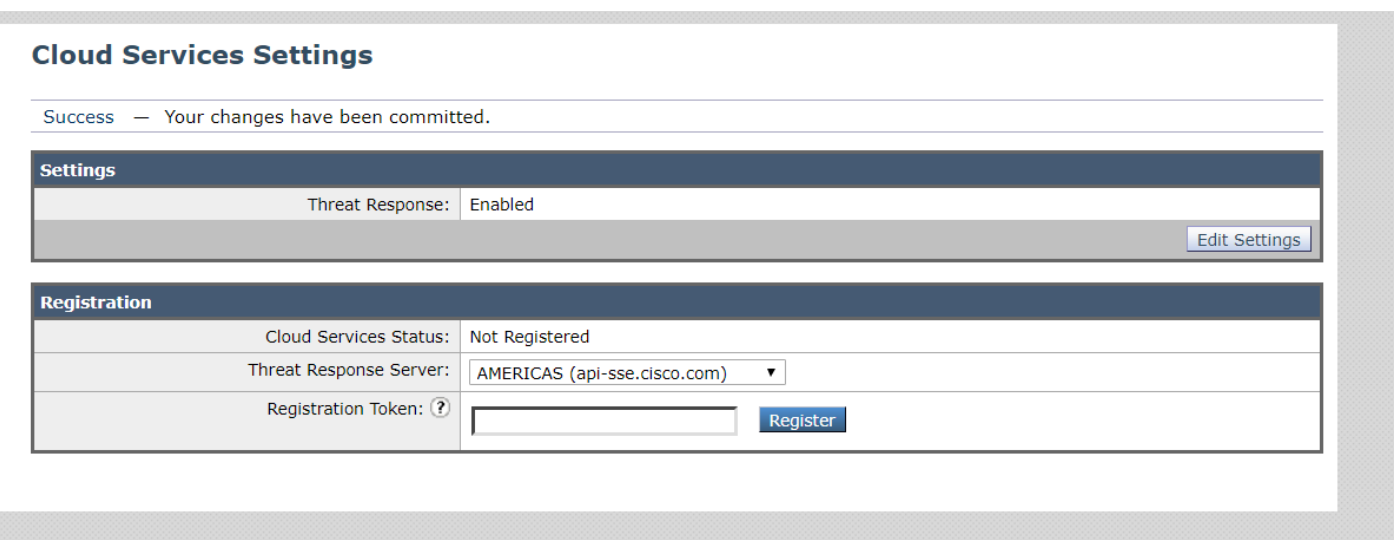
Choose the operation you want to perform:
COUNTERS - Limit counters recorded by the reporting system.
WEBTRACKINGQUERYTIMEOUT - Timeout value for Webtracking Queries.
AVERAGEOBJECTSIZE - Average HTTP Object Size used for Bandwidth Savings Calculation.
WEBEVENTBUCKETING - Enable or Disable web transaction 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.

### Cloud Services Settings



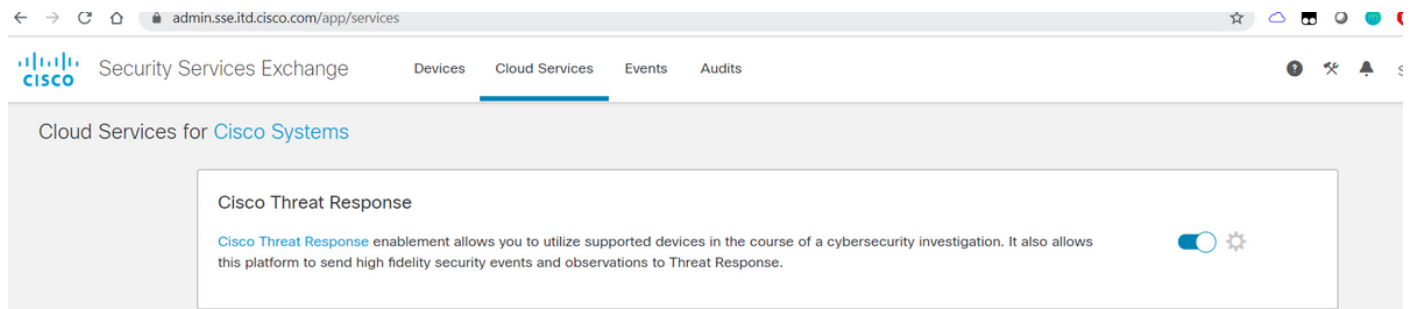
Elija la nube según su ubicación, como se muestra en la imagen.



**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:

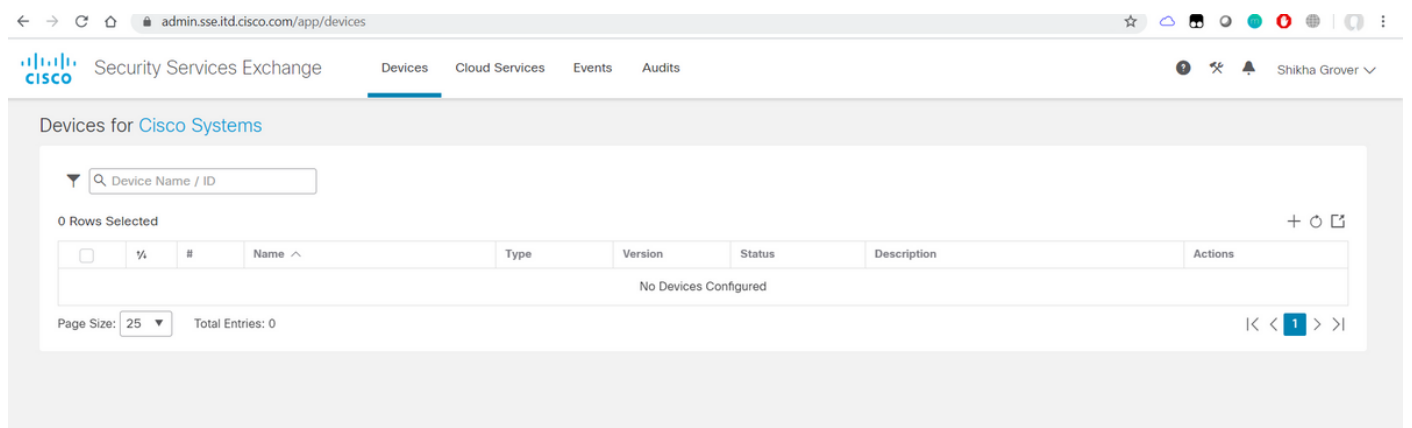
- [api.eu.sse.itd.cisco.com](https://api.eu.sse.itd.cisco.com) (Europa)
- [api-sse.cisco.com](https://api-sse.cisco.com) (América)

## 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.



### Add Devices and Generate Tokens ? ✕

Number of devices  
  
Up to 100

Token expiration time

[Cancel](#) [Continue](#)

### Add Devices and Generate Tokens ? ✕

The following tokens have been generated and will be valid for 1 hour(s):

Tokens
ef1324a199c106371542ee4d2d1bf1e7 <span>📄</span>

[Close](#) [Copy to Clipboard](#) [Save To File](#)

**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.

## Cloud Services Settings

Success — Your changes have been committed.

Settings	
Threat Response:	Enabled
<a href="#">Edit Settings</a>	

Registration	
Cloud Services Status:	Not Registered
Threat Response Server:	AMERICAS (api-sse.cisco.com) ▼
Registration Token: <span>?</span>	<input type="text" value="ef1324a199c106371542ee4d2d"/> <a href="#">Register</a>

**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.

## Cloud Services Settings

Success — Your appliance is successfully registered with the Cisco Threat Response portal.

### Settings

Threat Response:	Enabled
------------------	---------

[Edit Settings](#)

### Registration

Cloud Services Status:	Registered
Threat Response Server:	AMERICAS (api-sse.cisco.com)
Deregister Appliance:	<a href="#">Deregister</a>

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

admin.sse.itd.cisco.com/app/devices

Security Services Exchange

Devices for Cisco Systems

0 Rows Selected

Name	Type	Version	Status	Description	Actions
vWSA-12-0-1-173.COM	WSA	12.0.1-173	Registered	S300V	<a href="#">/</a> <a href="#">🗑️</a> <a href="#">🔍</a>

Page Size: 25 Total Entries: 1

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

visibility.amp.cisco.com/settings/devices

Threat Response

Settings > Devices

Manage Devices Reload Devices

Name	Type	Version	Description	ID	IP Address
vWSA-12-0-1-173.COM	WSA	12.0.1-173	S300V	3af01d56-a93e-4edc-926e-de1a4588409d	10.150.215.123

25 per page 1-1 of 1

[Previous](#) [Next](#)

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



**Settings**  
Your Account  
Devices  
API Clients  
▼ Modules  
    **Available Modules**  
Users

## Add New Web Security Appliance Module

Module Name\*

Registered Device\*

Request Timeframe (days)

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:"8d3aa8badf6e5a38e1b6d59a254969b1e0274f8fa120254ba1f7e029991872379"
- IP - ip:"172.217.26.164"
- Nombre - nombre\_archivo:"test.txt"

Enriquecimientos en uso como ejemplo:

Threat Response Investigate Snapshots Incidents **Beta** Intelligence Modules

New Investigation Assign to Incident Snapshots ... Automatic Layout

1 Target 1 Observable 0 Indicators 0 Domains 0 File Hashes 0 IP Addresses 1 URL 2 Modules

Investigation 1 of 1 enrichments complete

url: http://amazon.com/

Investigate Clear Reset What can I search for?

Relations Graph Showing 3 nodes

Clean URL http://amazon.com/

Hosted By URL http://amazon.com/ Connected To Target endpoint IP: 10.10.51.99 USER: 10.10.51.99

Sightings Timeline

My Environment Global 1 Sighting in My Environment First: Aug 28, 2019 Last: Aug 28, 2019

Observables

http://amazon.com/ Clean URL

My Environment Global 1 Sighting in My Environment First: Aug 28, 2019 Last: Aug 28, 2019

Judgement (1) Verdict (1) Sighting (1)

Module	Observed	Description	Confidence	Severity	Details	Resolution	Sensor
Web Security Appliance	4 hours ago	Transaction processed by Web Proxy Services	High	Low	Allowed	network proxy	

Threat Response Investigate Snapshots Incidents **Beta** Intelligence Modules

New Investigation Assign to Incident Snapshots ... Automatic Layout

0 Targets 1 Observable 0 Indicators 1 Domain 0 File Hashes 0 IP Addresses 0 URLs 1 Module

Investigation 1 of 1 enrichments complete with 5 Alerts

www.cisco.com

Investigate Clear Reset What can I search for?

Relations Graph Showing 1 node Expand

Domain www.cisco.com

Sightings Timeline

My Environment Global 0 Sightings in My Environment

Observables

www.cisco.com Domain

My Environment Global 0 Sightings in My Environment

Judgements (1) Verdicts (1)

Module	Observable	Disposition	Reason
Talos Intelligence	DOMAIN: www.cisco.com	Unknown	Neutral Talos Intelligence reputation s

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.