

# Integrate WSA with CTR

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Register the Appliance](#)

[Verify](#)

## Introduction

This document describes the steps to integrate Web Security Appliance (WSA) with Cisco Threat Response (CTR) portal.

Contributed by Shikha Grover and Edited by Yeraldin Sanchez Cisco TAC Engineers.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- WSA access
- CTR portal access
- Cisco Security Account

### Components Used

The information in this document is based on these software and hardware versions:

- Async Operating System version 12.x or later

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. If your network is live, ensure that you understand the potential impact of any command.

## Configure

**Caution:** If you access to CTR with a regional Asia Pacific, Japan, and China URL (<https://visibility.apjc.amp.cisco.com/>), the integration with your appliance is not currently supported.

**Step 1.** Enable **CTROBSERVABLE** under REPORTINGCONFIG in the CLI and commit the changes, as shown in the image.

```
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.
```

**Step 2.** Configure the Security Service Exchange (SSE) cloud portal, navigate to **Network >Cloud Services Settings > Edit settings**, click **Enable** and **Submit**, as shown in the image.

### Cloud Services Settings

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

Chose the cloud as per your location, as shown in the image.

### Cloud Services Settings

Success — Your changes have been committed.

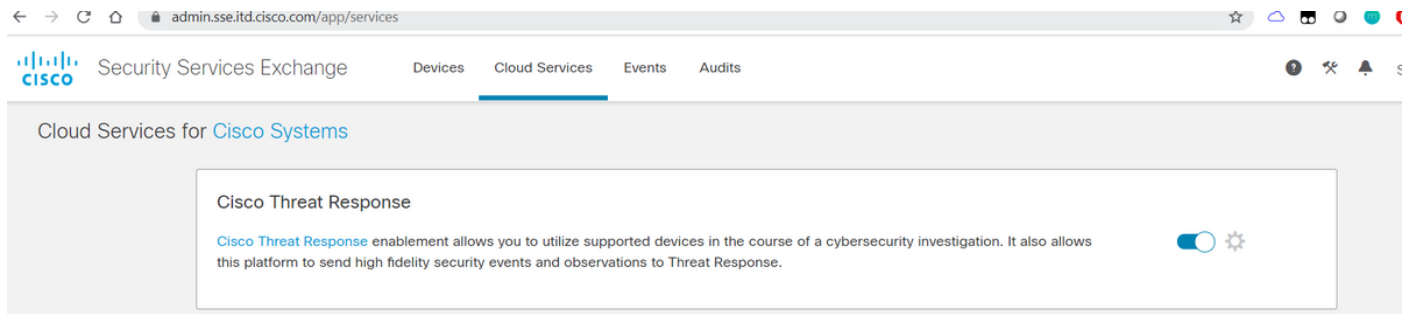
Settings	
Threat Response:	Enabled
<a href="#">Edit Settings</a>	

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

**Step 3.** If you do not have a Cisco Security account, you can create a user account in the Cisco Threat Response portal with admin access rights.

In order to create a new user account, navigate to the Cisco Threat Response portal [login page](#).

**Step 4.** Enable Cisco Threat Response under Cloud Services on the SSE portal, as shown in the image.



**Step 5.** Make sure WSA has reachability on port 443 to the SSE portal:

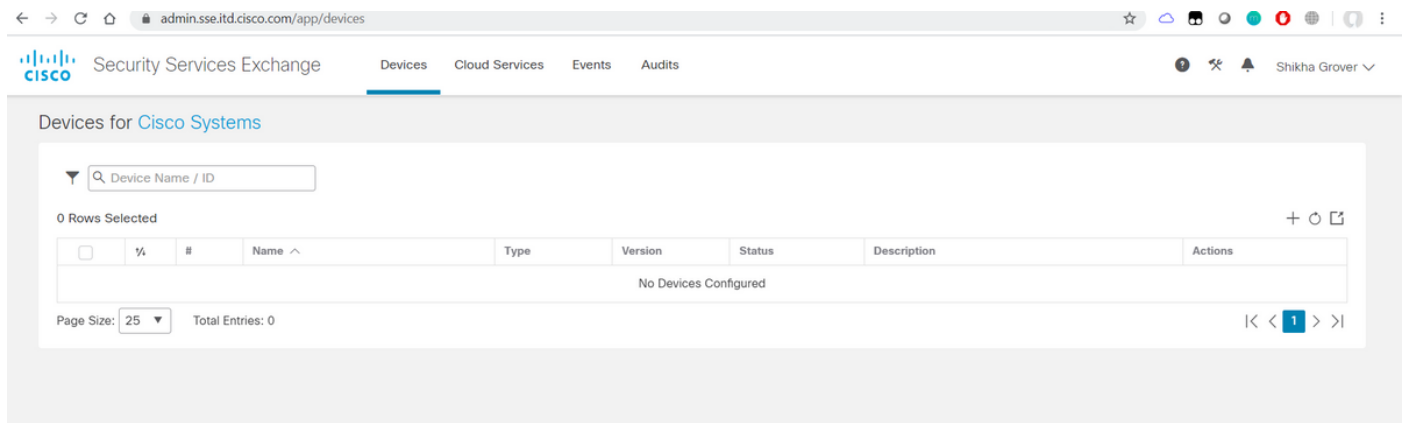
- api.eu.sse.itd.cisco.com (Europe)
- api-sse.cisco.com (America)

## Register the Appliance

**Step 1.** Obtain a registration token from the Security Services Exchange (SSE) portal to register your appliance with the Security Services Exchange portal.

SSE portal link is <https://admin.sse.itd.cisco.com/app/devices>.

**Note:** Use CTR account credentials to login to SSE portal.



**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	

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

**Step 2.** Enter the registration token obtained from the Security Services Exchange portal in WSA and click **Register**, as shown in the image.

### Cloud Services Settings

Success — Your changes have been committed.

#### Settings

Threat Response: Enabled

[Edit Settings](#)

#### Registration

Cloud Services Status: Not Registered

Threat Response Server: AMERICAS (api-sse.cisco.com) ▼

Registration Token: ?

ef1324a199c106371542ee4d2d

[Register](#)

**Step 3.** After a few seconds, you would see registration is successful.

**Caution:** Make sure the token generated is used before it expires.

## 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: [Deregister](#)

**Step 4.** On the SSE portal, you can see the device status.

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

Security Services Exchange | Devices | Cloud Services | Events | Audits

Devices for Cisco Systems

0 Rows Selected

	%	#	Name ^	Type	Version	Status	Description	Actions
<input type="checkbox"/>	>	1	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

**Step 5.** On the CTR portal appears the device registered.

visibility.amp.cisco.com/settings/devices

Threat Response | Investigate | Snapshots | Incidents **Total** | Intelligence | Modules

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

You can associate this device to a module, navigate to **Modules > Add New Module > Web Security Appliance**, as shown in the image.



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

## Add New Web Security Appliance Module

Module Name\*

Registered Device\*  
 ▼

Request Timeframe (days)

The device is now integrated. You can pass through traffic from the WSA and investigate threats on the CTR portal.

## Verify

Use this section to confirm that your configuration works properly.

Enrichments( Querying the WSA logs ) available for the WSA module and their supported format for running the query from the CTR portal:

- Domain – domain:"[com](#)"
- URL – url:"<http://www.neverssl.com>"
- SHA256 –  
    sha256:"8d3aa8badf6e5a38e1b6d59a254969b1e0274f8fa120254ba1f7e02991872379"
- IP – ip:"172.217.26.164"
- Filename – file\_name:"test.txt"

Enrichments in use as an example:

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

Feel free to let me know if I have missed something that should be included. Feel free to let me know if I have missed something that should be included. Feel free to let me know if I have missed something that should be included. Feel free to let me know if I have missed something that should be included.