

Intégrer WSA à CTR

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[Enregistrer l'appareil](#)

[Vérification](#)

Introduction

Ce document décrit les étapes à suivre pour intégrer le dispositif de sécurité Web (WSA) au portail Cisco Threat Response (CTR).

Contribué par Shikha Grover et édité par Yeraldin Sanchez Ingénieurs du TAC Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Accès WSA
- Accès au portail CTR
- Compte de sécurité Cisco

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Système d'exploitation asynchrone version 12.x ou ultérieure

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 votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configuration

Attention : Si vous accédez à CTR avec une URL Asie-Pacifique, Japon et Chine (<https://visibility.apjc.amp.cisco.com/>), l'intégration avec votre appareil n'est pas prise en charge actuellement.

Étape 1. Activez **CTROBSERVABLE** sous **REPORTINGCONFIG** dans l'interface de ligne de commande et validez les modifications, comme indiqué dans l'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

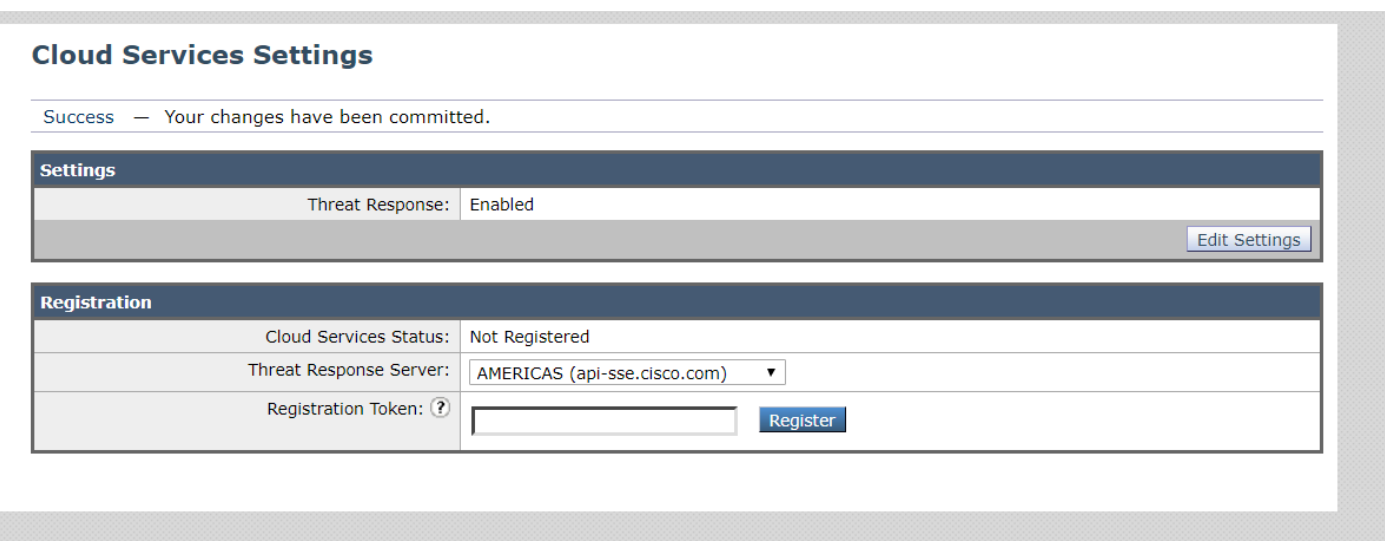
Choose the operation you want to perform:
COUNTERS - Limit counters recorded by the reporting system.
WEBTRACKINGQUERYTIMEOUT - Timeout value for Webtracking Queries.
AVERAGEOBJECTSIZE - Average HTTP Object Size used for Bandwidth Savings Calculation.
WEBEVENTBUCKETING - Enable or Disable web transaction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

Étape 2. Configurez le portail cloud Security Service Exchange (SSE), accédez à **Network >Cloud Services Settings > Edit settings**, cliquez sur **Enable** and **Submit**, comme illustré dans l'image.

Cloud Services Settings



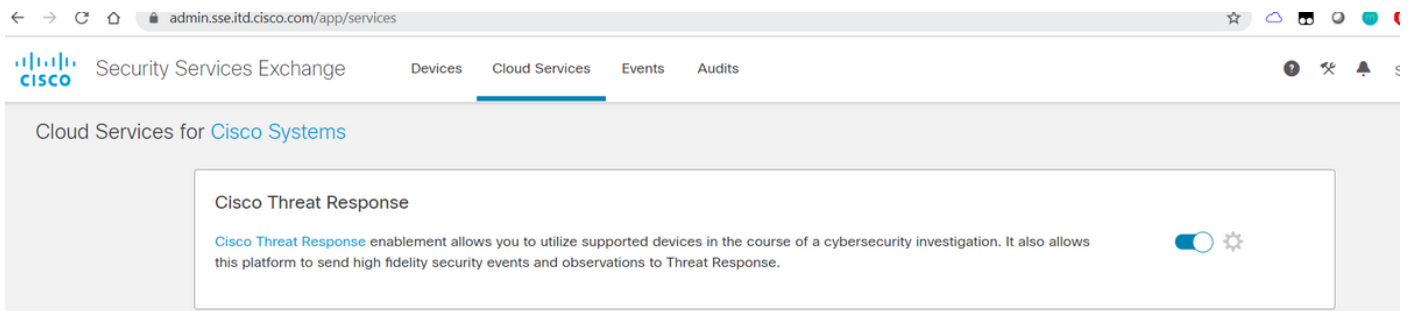
Choisissez le cloud en fonction de votre emplacement, comme l'illustre l'image.



Étape 3. Si vous ne disposez pas d'un compte Cisco Security, vous pouvez créer un compte utilisateur dans le portail Cisco Threat Response avec des droits d'accès administrateur.

Afin de créer un nouveau compte d'utilisateur, accédez à la [page de connexion](#) du portail Cisco Threat Response.

Étape 4. Activez Cisco Threat Response sous Cloud Services sur le portail SSE, comme l'illustre l'image.



Étape 5. Assurez-vous que WSA est accessible sur le port 443 au portail SSE :

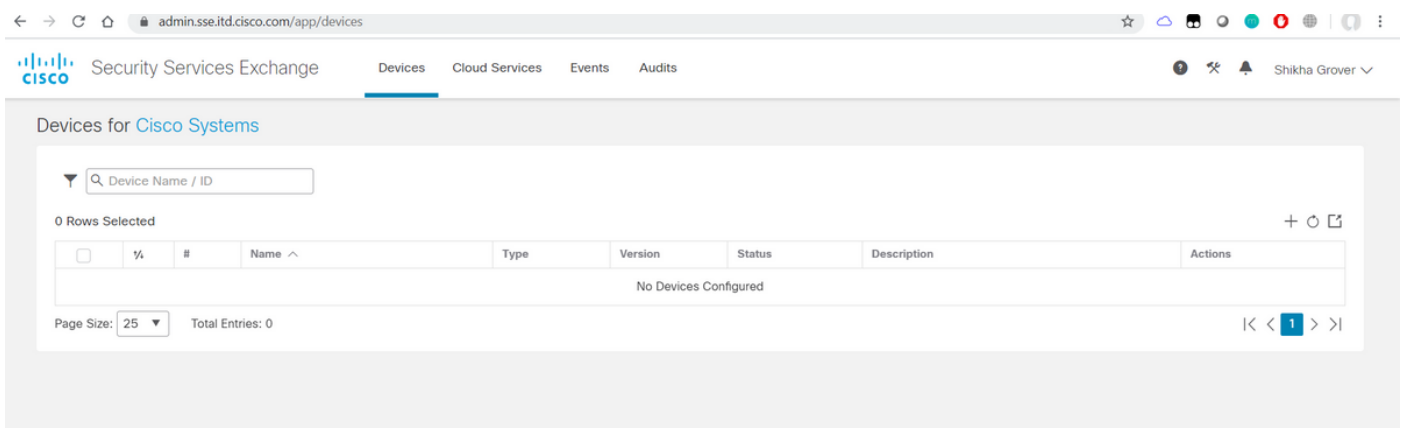
- api.eu.sse.itd.cisco.com (Europe)
- api-sse.cisco.com (Amérique)

Enregistrer l'appareil

Étape 1. Obtenez un jeton d'inscription à partir du portail Security Services Exchange (SSE) pour enregistrer votre appliance auprès du portail Security Services Exchange.

Le lien du portail SSE est <https://admin.sse.itd.cisco.com/app/devices>.

Note: Utilisez les informations d'identification du compte CTR pour vous connecter au portail 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	

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

Étape 2. Entrez le jeton d'enregistrement obtenu à partir du portail Security Services Exchange dans WSA et cliquez sur **Register**, comme indiqué dans l'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](#)

Étape 3. Au bout de quelques secondes, l'enregistrement a réussi.

Attention : Assurez-vous que le jeton généré est utilisé avant son expiration.

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](#)

Étape 4. Sur le portail SSE, vous pouvez voir l'état du périphérique.

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

Security Services Exchange

Devices for Cisco Systems

0 Rows Selected

	%	#	Name ^	Type	Version	Status	Description	Actions
<input type="checkbox"/>	>	1	WSA-12-0-1-173.COM	WSA	12.0.1-173	Registered	S300V	/ 🗑️ 🔍

Page Size: 25 Total Entries: 1

Étape 5. Sur le portail CTR apparaît le périphérique enregistré.

visibility.amp.cisco.com/settings/devices

Threat Response

Settings > Devices

Devices

Manage Devices Reload Devices

Name	Type	Version	Description	ID	IP Address
WSA-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

Vous pouvez associer ce périphérique à un module, accéder à **Modules > Ajouter un nouveau module > Appareil de sécurité Web**, comme illustré dans l'image.



Settings
Your Account
Devices
API Clients
▼ Modules
Available Modules
Users

Add New Web Security Appliance Module

Module Name*

Registered Device*

Request Timeframe (days)

Le périphérique est désormais intégré. Vous pouvez passer par le trafic à partir du WSA et enquêter sur les menaces sur le portail CTR.

Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Enrichments(Interrogation des journaux WSA) disponibles pour le module WSA et leur format pris en charge pour exécuter la requête à partir du portail CTR :

- Domaine - domaine : " [com](#) "
- URL - url : " <http://www.neverssl.com> "
- SHA256 - sha256 : " 8d3aa8badf6e5a38e1b6d59a254969b1e0274f8fa120254ba1f7e029
"1872379 "
- IP - ip : " 172.217.26.164 "
- Nom de fichier - nom_fichier : " test.txt "

Enrichissements utilisés comme exemple :

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

N'hésitez pas à me faire savoir si j'ai raté quelque chose qui devrait être inclus. N'hésitez pas à me faire savoir si j'ai raté quelque chose qui devrait être inclus. N'hésitez pas à me faire savoir si j'ai raté quelque chose qui devrait être inclus. N'hésitez pas à me faire savoir si j'ai raté quelque chose qui devrait être inclus.