

Integration der WSA mit CTR

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Appliance registrieren](#)

[Überprüfen](#)

Einführung

Dieses Dokument beschreibt die Schritte zur Integration von Web Security Appliance (WSA) in das Cisco Threat Response (CTR)-Portal.

Verfasst von Shikha Grover und herausgegeben von Yeraldin Sanchez Cisco TAC Engineers.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- WSA-Zugriff
- CTR-Portalzugriff
- Cisco Security Account

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Async Operating System, Version 12.x oder höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Vorsicht: Wenn Sie über eine regionale URL für den Asien-Pazifik-Raum, Japan und China (<https://visibility.apjc.amp.cisco.com/>) auf CTR zugreifen, wird die Integration mit Ihrer Appliance derzeit nicht unterstützt.

Schritt 1: Aktivieren Sie **CTROBSERVABLE** unter **REPORTINGCONFIG** in der CLI, und bestätigen Sie die Änderungen, wie im Bild gezeigt.

```
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

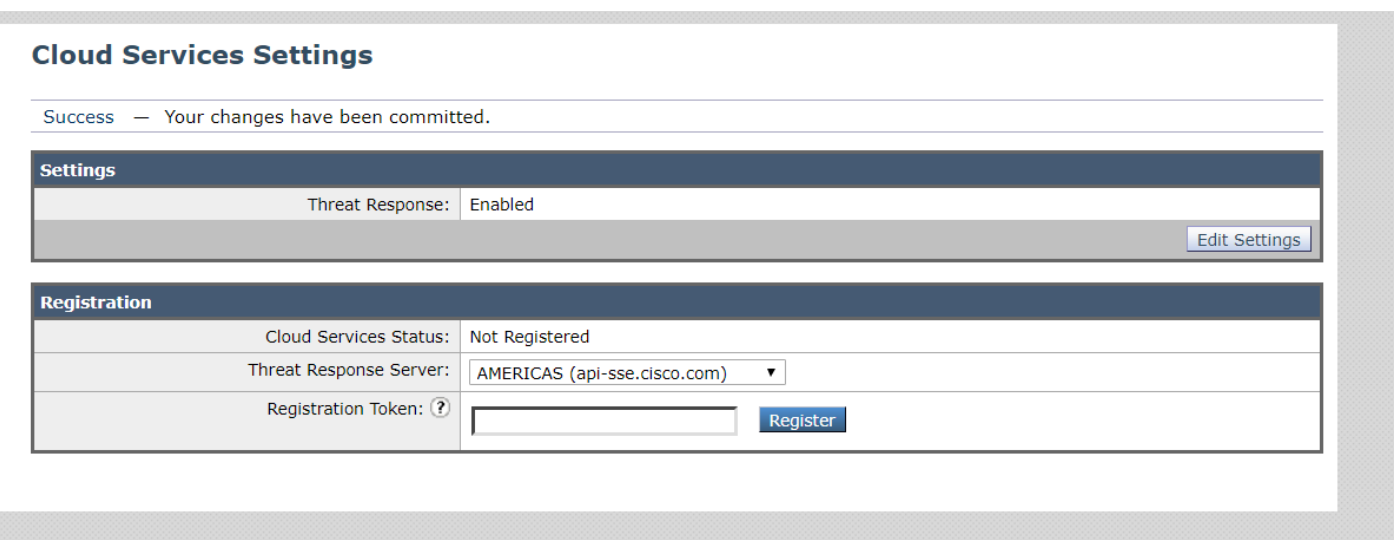
Choose the operation you want to perform:
COUNTERS - Limit counters recorded by the reporting system.
WEBTRACKINGQUERYTIMEOUT - Timeout value for Webtracking Queries.
AVERAGEOBJECTSIZE - Average HTTP Object Size used for Bandwidth Savings Calculation.
WEBEVENTBUCKETING - Enable or Disable web transaction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

Schritt 2: Konfigurieren Sie das Cloud-Portal von Security Service Exchange (SSE), navigieren Sie zu **Network > Cloud Services Settings > Edit settings**, und klicken Sie auf **Enable** and **Submit** (**Netzwerk > Cloud Services Settings > Edit settings**), wie im Bild gezeigt.

Cloud Services Settings



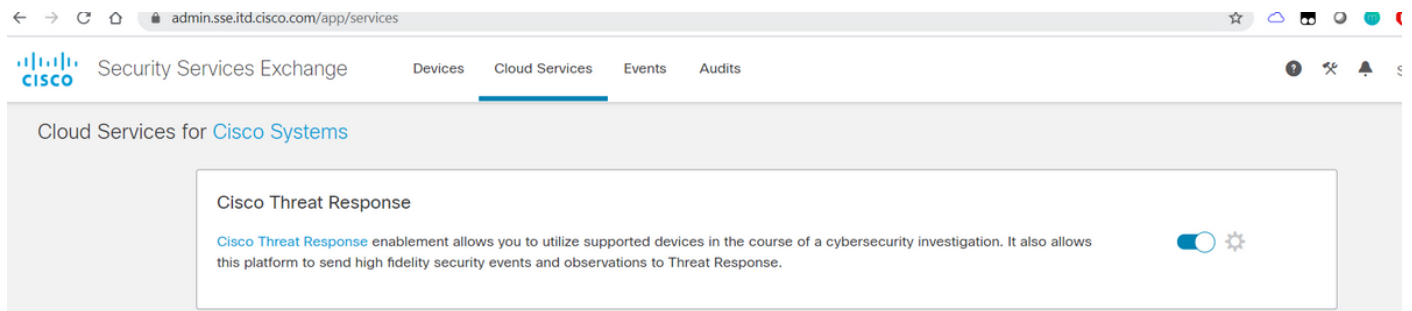
Wählen Sie die Cloud nach Ihrem Standort aus, wie im Bild gezeigt.



Schritt 3: Wenn Sie kein Cisco Security-Konto haben, können Sie im Cisco Threat Response-Portal ein Benutzerkonto mit Administratorrechten erstellen.

Um ein neues Benutzerkonto zu erstellen, navigieren Sie zur [Anmeldeseite](#) des Cisco Threat Response-Portals.

Schritt 4: Aktivieren Sie Cisco Threat Response unter Cloud-Services im SSE-Portal, wie im Bild gezeigt.



Schritt 5: Stellen Sie sicher, dass die WSA für Port 443 zum SSE-Portal erreichbar ist:

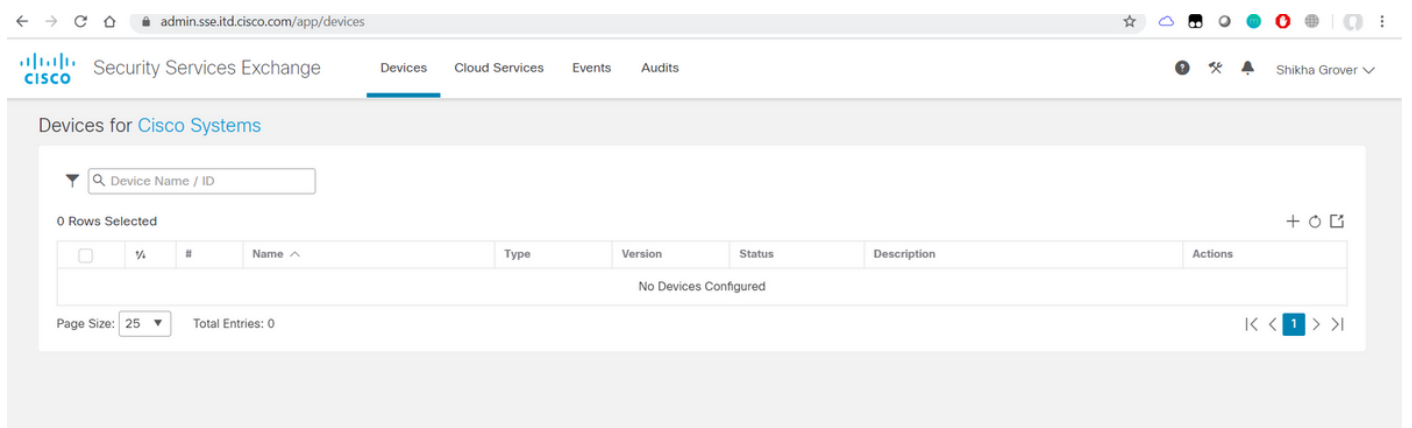
- api.eu.sse.itd.cisco.com (Europa)
- api-sse.cisco.com (Amerika)

Appliance registrieren

Schritt 1: Rufen Sie ein Registrierungstoken vom Security Services Exchange-Portal (SSE) ab, um Ihre Appliance beim Exchange-Portal für Sicherheitsdienste zu registrieren.

Der SSE-Portal-Link lautet <https://admin.sse.itd.cisco.com/app/devices>.

Hinweis: Verwenden Sie CTR-Kontoanmeldeinformationen, um sich beim SSE-Portal anzumelden.



Add Devices and Generate Tokens ?
✕

Number of devices

Up to 100

Token expiration time

1 hour ▼

Cancel
Continue

Add Devices and Generate Tokens ?
✕

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

Tokens	
ef1324a199c106371542ee4d2d1bf1e7	P

Close
Copy to Clipboard
Save To File

Schritt 2: Geben Sie das im Security Services Exchange-Portal in WSA abgerufene Registrierungstoken ein, und klicken Sie auf **Registrieren**, wie im Bild gezeigt.

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](#)

Schritt 3: Nach einigen Sekunden wird die Registrierung erfolgreich durchgeführt.

Vorsicht: Stellen Sie sicher, dass das generierte Token verwendet wird, bevor es abläuft.

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](#)

Schritt 4: Im SSE-Portal wird der Gerätestatus angezeigt.

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

Schritt 5: Im CTR-Portal wird das registrierte Gerät angezeigt.

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

Sie können dieses Gerät einem Modul zuordnen. Navigieren Sie zu **Module > Neues Modul hinzufügen > Websicherheits-Appliance**, wie im Bild gezeigt.



Settings
Your Account
Devices
API Clients
▼ Modules
Available Modules
Users

Add New Web Security Appliance Module

Module Name*

Registered Device*
 ▼

Request Timeframe (days)

Das Gerät ist nun integriert. Sie können Datenverkehr von der WSA durchlaufen und Bedrohungen im CTR-Portal untersuchen.

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Enrichments (Abfragen der WSA-Protokolle), verfügbar für das WSA-Modul und das unterstützte Format für die Ausführung der Abfrage vom CTR-Portal aus:

- Domäne - Domäne: "[com](#)"
- URL - url: "<http://www.neverssl.com>"
- SHA256 - sha256: "8d3aa8badf6e5a38e1b6d59a254969b1e0274f8fa120254ba1f7e02991872379"
- IP - IP: "172.217.26.164"
- Dateiname - Dateiname: "test.txt"

Als Beispiel werden Anreicherungen verwendet:

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

Bitte lassen Sie mich wissen, wenn ich etwas verpasst habe, das eingeschlossen werden sollte.
 Bitte lassen Sie mich wissen, wenn ich etwas verpasst habe, das eingeschlossen werden sollte.
 Bitte lassen Sie mich wissen, wenn ich etwas verpasst habe, das eingeschlossen werden sollte.
 Bitte lassen Sie mich wissen, wenn ich etwas verpasst habe, das eingeschlossen werden sollte.