

Integrazione di WSA con CTR

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Registrazione dell'accessorio](#)

[Verifica](#)

Introduzione

In questo documento viene descritta la procedura per integrare Web Security Appliance (WSA) con il portale Cisco Threat Response (CTR).

Contributo di Shikha Grover e modificato da Yeraldin Sanchez Cisco TAC Engineers.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- accesso WSA
- Accesso portale CTR
- Account di sicurezza Cisco

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Async Operating System versione 12.x o successiva

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Attenzione: Se si accede a CTR con un URL regionale per Asia Pacifico, Giappone e Cina (<https://visibility.apjc.amp.cisco.com/>), l'integrazione con l'accessorio non è attualmente supportata.

Passaggio 1. Abilitare **CTROBSERVABLE** in **REPORTINGCONFIG** nella CLI ed eseguire il commit delle modifiche, come mostrato nell'immagine.

```
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

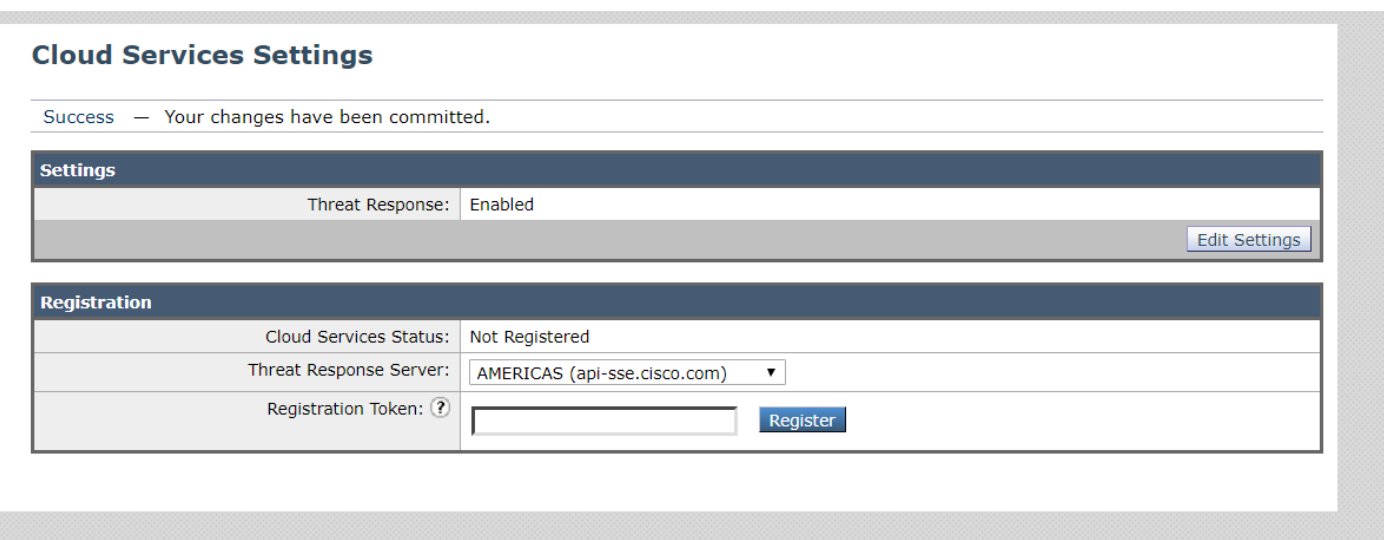
Choose the operation you want to perform:
COUNTERS - Limit counters recorded by the reporting system.
WEBTRACKINGQUERYTIMEOUT - Timeout value for Webtracking Queries.
AVERAGEOBJECTSIZE - Average HTTP Object Size used for Bandwidth Savings Calculation.
WEBEVENTBUCKETING - Enable or Disable web transaction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

Passaggio 2. Configurare il portale cloud di Security Service Exchange (SSE), passare a **Rete > Impostazioni servizi cloud > Modifica impostazioni**, fare clic su **Abilita** e **invia**, come mostrato nell'immagine.

Cloud Services Settings



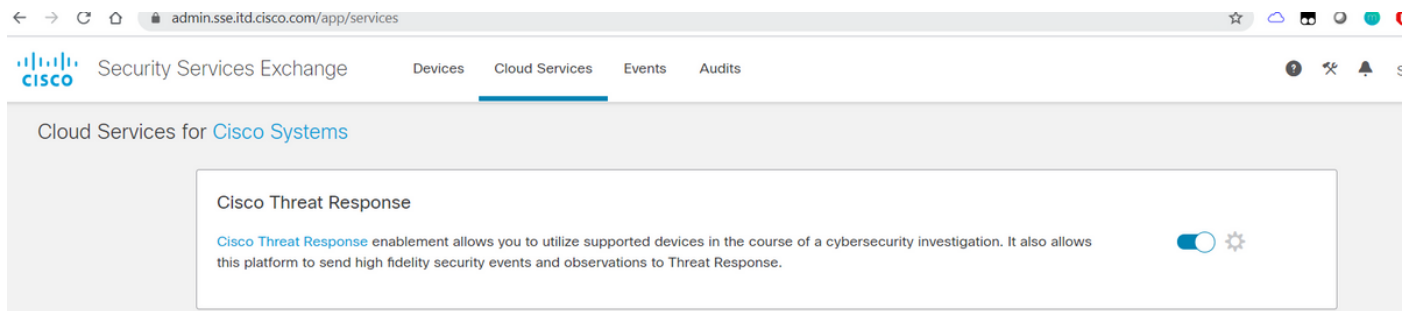
Scegliere il cloud in base alla posizione, come mostrato nell'immagine.



Passaggio 3. Se non si dispone di un account Cisco Security, è possibile creare un account utente nel portale Cisco Threat Response con diritti di accesso di amministratore.

Per creare un nuovo account utente, accedere alla [pagina di accesso del](#) portale Cisco Threat Response.

Passaggio 4. Abilitare Cisco Threat Response in Cloud Services sul portale SSE, come mostrato nell'immagine.



Passaggio 5. Verificare che WSA sia raggiungibile sulla porta 443 al portale SSE:

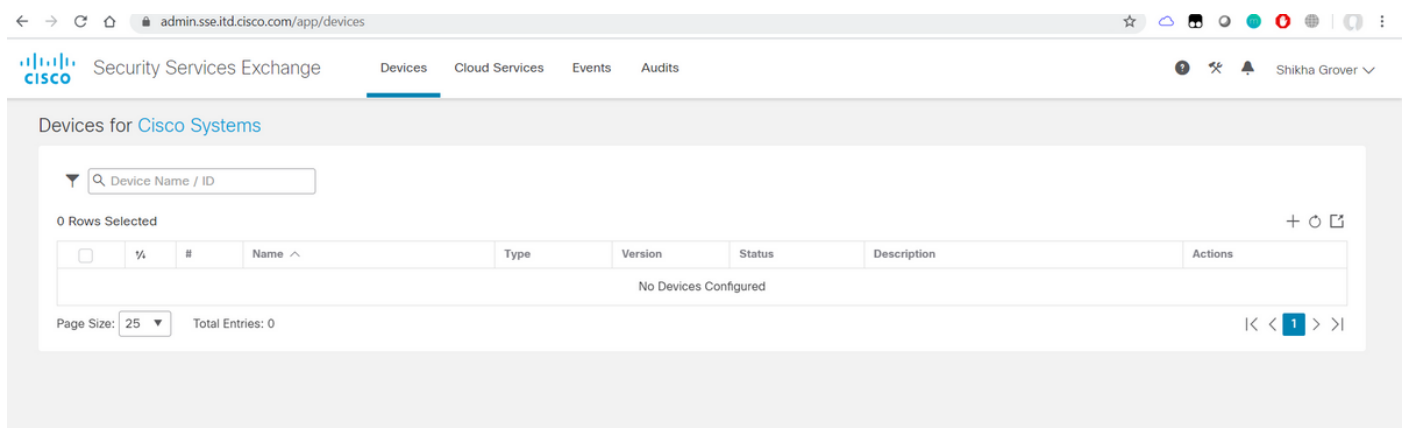
- api.eu.sse.itd.cisco.com (Europa)
- api-sse.cisco.com (America)

Registrazione dell'accessorio

Passaggio 1. Ottenere un token di registrazione dal portale SSE (Security Services Exchange) per registrare l'appliance nel portale Exchange dei servizi di sicurezza.

Il collegamento al portale SSE è <https://admin.sse.itd.cisco.com/app/devices>.

Nota: Usa le credenziali dell'account CTR per accedere al portale 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](#)

Passaggio 2. Immettere il token di registrazione ottenuto dal portale Security Services Exchange in WSA e fare clic su **Registra**, come mostrato nell'immagine.

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: ?	<input type="text" value="ef1324a199c106371542ee4d2d"/> Register

Passaggio 3. Dopo alcuni secondi, la registrazione è riuscita.

Attenzione: Assicurarsi che il token generato sia utilizzato prima della scadenza.

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](#)

Passaggio 4. Sul portale SSE è possibile visualizzare lo stato del dispositivo.

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

Security Services Exchange

Devices Cloud Services Events Audits

Shikha Grover

Devices for Cisco Systems

Device Name / ID

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	/ 🗑️ 🔍

Page Size: 25 Total Entries: 1

Passaggio 5. Sul portale CTR appare il dispositivo registrato.

visibility.amp.cisco.com/settings/devices

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

Shikha Grover

Settings > Devices

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](#)

È possibile associare il dispositivo a un modulo, selezionare **Moduli > Aggiungi nuovo modulo > Web Security Appliance**, come mostrato nell'immagine.



Settings
Your Account
Devices
API Clients
▼ Modules
Available Modules
Users

Add New Web Security Appliance Module

Module Name*

Registered Device*
 ▼

Request Timeframe (days)

Il dispositivo è ora integrato. Puoi passare attraverso il traffico dalla WSA e indagare sulle minacce sul portale CTR.

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Enrichments(Query sui log WSA) disponibili per il modulo WSA e il formato supportato per l'esecuzione della query dal portale CTR:

- Dominio - dominio:"[com](#)"
- URL - url:"<http://www.neverssl.com>"
- SHA256 -
sha256:"8d3aa8badf6e5a38e1b6d59a254969b1e0274f8fa120254ba1f7e02991872379"
- IP - ip:"172.217.26.164"
- Nome file - nome_file:"test.txt"

L'esempio dell'arricchimento utilizzato è il seguente:

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

Sentitevi liberi di farmi sapere se mi sono perso qualcosa che dovrebbe essere incluso. Sentitevi liberi di farmi sapere se mi sono perso qualcosa che dovrebbe essere incluso. Sentitevi liberi di farmi sapere se mi sono perso qualcosa che dovrebbe essere incluso. Sentitevi liberi di farmi sapere se mi sono perso qualcosa che dovrebbe essere incluso.