

Integrar WSA com CTR

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Registrar o aplicativo](#)

[Verificar](#)

Introduction

Este documento descreve as etapas para integrar o Web Security Appliance (WSA) ao portal Cisco Threat Response (CTR).

Contribuído por Shikha Grover e editado por Yeraldin Sanchez Engenheiros do TAC da Cisco.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- acesso WSA
- acesso ao portal CTR
- Conta de segurança da Cisco

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Async Operating System versão 12.x ou 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Caution: Se você acessa o CTR com um URL regional do Pacífico Asiático, Japão e China (<https://visibility.apjc.amp.cisco.com/>), a integração com seu dispositivo não é suportada no momento.

Etapa 1. Ative **CTOBSERVABLE** em **REPORTINGCONFIG** na CLI e confirme as alterações, como mostrado na imagem.

```
WSA-12-0-1-173.COM> reportingconfig

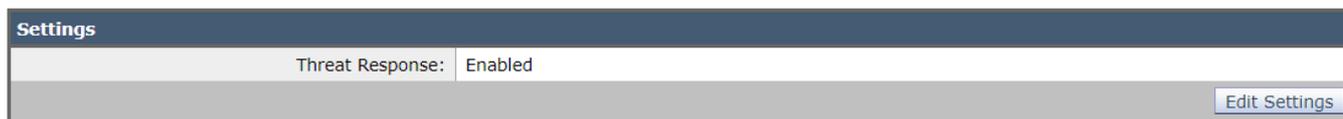
Choose the operation you want to perform:
COUNTERS - Limit counters recorded by the reporting system.
WEBTRACKINGQUERYTIMEOUT - Timeout value for Webtracking Queries.
AVERAGEOBJECTSIZE - Average HTTP Object Size used for Bandwidth Savings
alculation.
WEBEVENTBUCKETING - Enable or Disable web transaction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

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

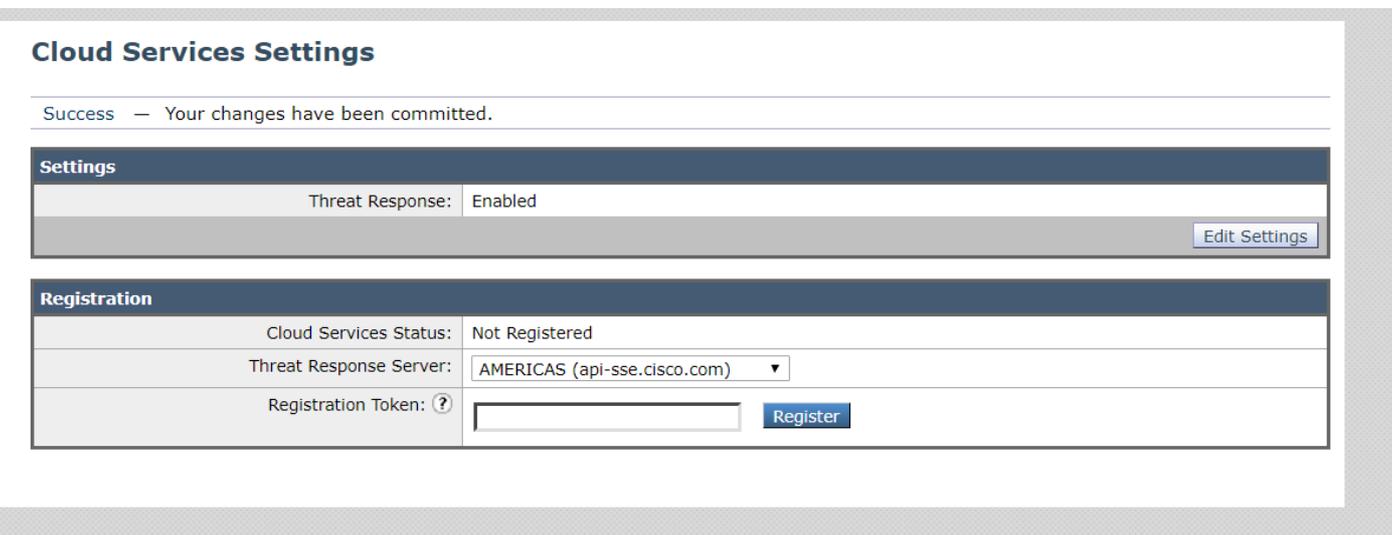
Choose the operation you want to perform:
COUNTERS - Limit counters recorded by the reporting system.
WEBTRACKINGQUERYTIMEOUT - Timeout value for Webtracking Queries.
AVERAGEOBJECTSIZE - Average HTTP Object Size used for Bandwidth Savings Calculation.
WEBEVENTBUCKETING - Enable or Disable web transaction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

Etapa 2. Configure o portal de nuvem do Security Service Exchange (SSE), navegue até **Network > Cloud Services Settings > Edit settings**, clique em **Enable** e **Submit**, conforme mostrado na imagem.

Cloud Services Settings



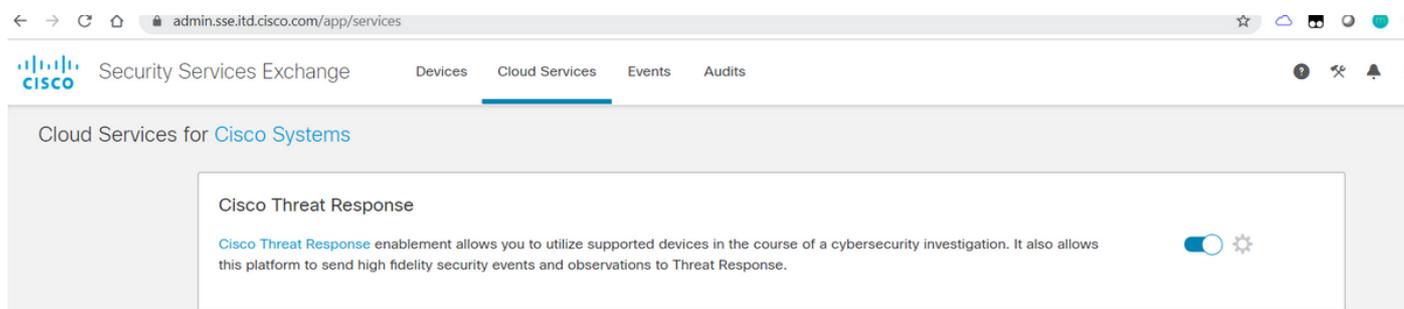
Escolha a nuvem conforme o local, como mostrado na imagem.



Etapa 3. Se você não tiver uma conta do Cisco Security, poderá criar uma conta de usuário no portal Cisco Threat Response com direitos de acesso de administrador.

Para criar uma nova conta de usuário, navegue até a [página de login](#) do portal Cisco Threat Response.

Etapa 4. Ative o Cisco Threat Response em serviços de nuvem no portal SSE, como mostrado na imagem.



Etapa 5. Verifique se o WSA tem acessibilidade na porta 443 para o portal SSE:

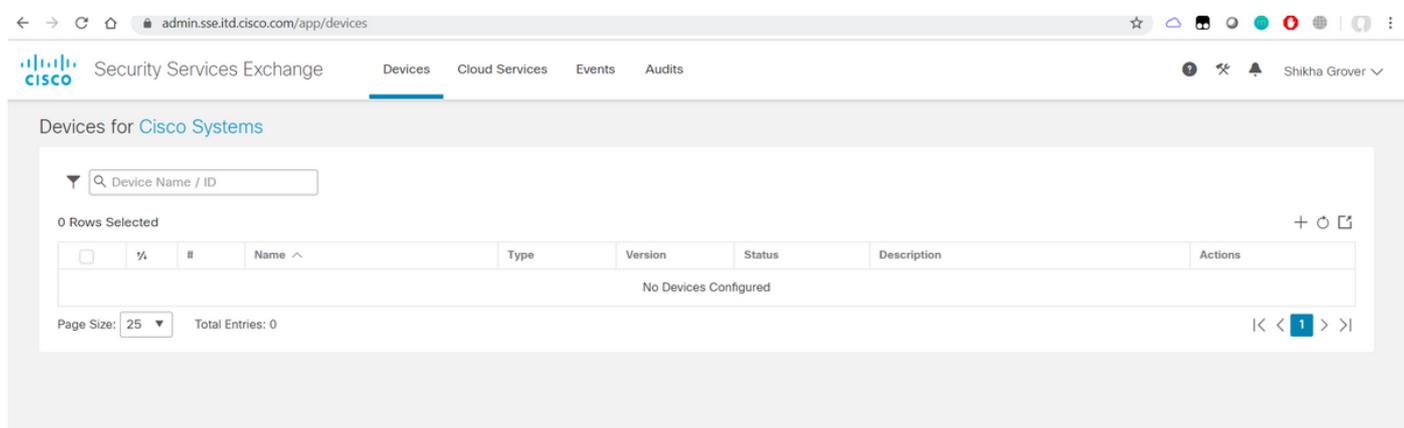
- api.eu.sse.itd.cisco.com (Europa)
- api-sse.cisco.com (América)

Registrar o aplicativo

Etapa 1. Obtenha um token de registro no portal do Security Services Exchange (SSE) para registrar seu dispositivo no portal do Security Services Exchange.

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

Note: Use credenciais de conta CTR para fazer login no 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 P

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

Etapa 2. Insira o token de registro obtido do portal do Security Services Exchange no WSA e clique em **Registrar**, como mostrado na imagem.

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

Etapa 3. Após alguns segundos, você verá que o registro foi bem-sucedido.

Caution: Verifique se o token gerado é usado antes de expirar.

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

Etapa 4. No portal SSE, você pode ver o status do dispositivo.

Name	Type	Version	Status	Description	Actions
vWSA-12-0-1-173.COM	WSA	12.0.1-173	Registered	S300V	/ 🗑️ 🔍

Etapa 5. No portal CTR, o dispositivo está registrado.

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

Você pode associar esse dispositivo a um módulo, navegar para **Módulos > Adicionar novo módulo > Web Security Appliance**, como mostrado na imagem.



Settings
Your Account
Devices
API Clients
▼ Modules
 Available Modules
Users

Add New Web Security Appliance Module

Module Name*

Registered Device*
 ▼

Request Timeframe (days)

O dispositivo agora está integrado. Você pode passar pelo tráfego do WSA e investigar ameaças no portal CTR.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Enrichments(Consultando os registros WSA) disponíveis para o módulo WSA e seu formato suportado para executar a consulta no portal CTR:

- Domínio - domínio:"[com](#)"
- URL - url:"<http://www.neverssl.com>"
- SHA256 - sha256:"8d3aa8badf6e5a38e1b6d59a254969b1e0274f8fa120254ba1f7e0291872379"
- IP - ip:"172.217.26.164"
- Nome do arquivo - nome_do_arquivo:"test.txt"

Enriquecimentos em uso como exemplo:

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

Sinta-se à vontade para me informar se perdi algo que deveria ser incluído. Sinta-se à vontade para me informar se perdi algo que deveria ser incluído. Sinta-se à vontade para me informar se perdi algo que deveria ser incluído. Sinta-se à vontade para me informar se perdi algo que deveria ser incluído.