

# عم اه حال صا و هئاطخأ فاشك ت سا و SecureX جم د (WSA) بيولا نامأ زا هج

## تا يوت حمل ا

[عم دق م ل ا](#)

[قي س اس أ ل ا ت ا ب ل ط ت م ل ا](#)

[ت ا ب ل ط ت م ل ا](#)

[عم د خ ت س م ل ا ت ا ن و ك م ل ا](#)

[ن ي و ك ت ل ا](#)

[SecureX ل ق ط ن م ل ك ل ق ب و ل ط م ل ا URL ن ي و ا ن ع](#)

[SSE ل ي ج س ت ل WSA دا د ع](#)

[SecureX عم ك ي د ل زا ه ج ل ا جم د](#)

[ق ح ص ل ا ن م ق ق ح ت ل ا](#)

[اه حال ص ا و ا ط خ أ ل ا ف ا ش ك ت س ا](#)

[CLI ن م زا ه ج ل ا ل ي ج س ت ن م ق ق ح ت ل ا](#)

[وي دي ف ل ا](#)

## عم دق م ل ا

ق ق ح ت ل ا و (WSA) بيولا نامأ زا هج عم SecureX لم ا ك ت ل ق ب و ل ط م ل ا ت ا و ط خ ل ا د ن ت س م ل ا ا ذ ه ف ص ي  
اه حال ص ا و ل م ا ك ت ل ا ا ذ ه ا ط خ أ ف ا ش ك ت س ا و ه ن م

## قي س اس أ ل ا ت ا ب ل ط ت م ل ا

### ت ا ب ل ط ت م ل ا

قي ل ا ت ل ا ع ي ض ا و م ل ا ب ق ر ع م ك ي د ل ن و ك ت ن ا ب Cisco ي ص و ت:

- (WSA) بيولا نامأ زا هج
- ر و ص ل ل ق ي ر ا ي ت خ ل ا ل ا ق ي ض ا ر ت ف ا ل ا ا ك ا ح م ل ا

### عم د خ ت س م ل ا ت ا ن و ك م ل ا

- (WSA) بيولا نامأ زا هج
- (SSE) نام أ ل ا ت ا م د خ ل د ا ب ت
- SecureX ق ب ا و ب

ق ص ا خ ق ي ل م ع م ق ي ب ي ف ق د و ج و م ل ا ق ز ه ج أ ل ا ن م د ن ت س م ل ا ا ذ ه ي ف ق د ر ا و ل ا ت ا م و ل ع م ل ا ع ا ش ن ا م ت  
ت ن ا ك ا ذ ا. (ي ض ا ر ت ف ا) ح و س م م ن ي و ك ت ب د ن ت س م ل ا ا ذ ه ي ف ق م د خ ت س م ل ا ق ز ه ج أ ل ا ع ي م ج ت ا د ب  
ر م أ ي أ ل ل م ت ح م ل ا ر ي ث ا ت ل ل ك م ه ف ن م د ك ا ت ف، ل ي غ ش ت ل ا د ي ق ك ت ك ب ش

## نيوكتلا

SecureX ل قطنم لكل ةبولطملا URL نيوانع

443 ذفنملا ىلع URL نيوانع ىلا لوصولا ةينام هيدل WSA زاهج نأ نم ققحت

ةيكييرملا ةقطنملا

- api-sse.cisco.com

يپوروالا داخاتالا ةقطنم

- api.eu.sse.itd.cisco.com

ئداهلا طيحمل او ايسآل URL ناو نع مادختساب SecureX ىلا لوصولا ناك اذا: ةظالم موعدم ريغ زاهجلا عم جمدا نإف، (<https://visibility.apjc.amp.cisco.com/>) نصل او نابايلا او ايلاح.

SSE ليحستل WSA دادع

1.- ةزيمملا زومرلا عاشن او ةزهجالا ةفاضلا (+) قوف رقنا م ةزهجالا ىلا لقتنا: SSE ةبواب ىلع -1، ةروصللا يف حضورم وه امك،

### Add Devices and Generate Tokens ?

Number of devices

  
Up to 100

Token expiration time



Cancel Continue

2.- ةروصللا يف حضورم وه امك، WSA ل زيمملا زومرلا عاشن م تيوعباتم قوف رقنا -2.

## Add Devices and Generate Tokens ?



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


Tokens	
 7120c58e1b4	

Close

Copy to Clipboard

Save To File

3.- كنكمي Reportingconfig تحت، WSA (CLI) رم اوأ رطس ةهجاوي ف Ctobservable نيكمتب مق - 3.  
ةروصلال في حضورم وه امك، Ctobservable نيكمتل راخالال لىل ع روثعلا:

```
WSA-.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.
j> 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.
```

4.- ةكبشلال لىل ل قننلالاو (SSE) نامأل تامدخ لدابتب ةصخالال ةباحسلا ةباب نيكمت - 4.  
في حضورم وه امك، لاسراو نيكمت قوف رقنا، تادادعال ريرحت > ةباحسلا تامدخ تادادع>  
ةروصلال:

### Cloud Services Settings

Settings
Threat Response: Enabled

[Edit Settings](#)

5.- اهب لاصتالال ديرت يتللا ةباحسلا دح :-

### 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"/> <a href="#">Register</a>

6.- اءاتنا تقو لبق زيملال زمرا مادختسا نم دكأت (SEE) لىل عهأشنا يذلا زيملال زمرا لخدأ :-  
(ةيحالصل):

### 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"/> <a href="#">Register</a>

7.- حاجنب زاھللا ليجست لىل ريشة لاسر رتس، زيملال زمرا ليجست درجم :-

### 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:	<a href="#">Deregister</a>

8.- ةباوب لىل لجملا زاھللا رت، كلذ دعب :-

Security Services Exchange

Devices Cloud Services Events Audit Log

Devices for Sourcefire Support

WSA

0 Rows Selected

	%	#	Name	Type	Version	Status	Description	Actions
<input type="checkbox"/>	>	1	lft-wsa.mohsoni.lab	WSA	12.5.0-569	Registered	S300V	
<input type="checkbox"/>	>	2	wsa02.mex-amp.lab	WSA	12.0.1-268	Registered	S100V	

ID: 363f1b56-e9e5-4dba-888a-640868b6ae54  
Created: 2020-05-28 04:55:38 UTC

IP Address: 10.10.10.19  
Connector Version:

## SecureX عم كيديل زاهجلا جدم

ددح وديج ةي طمن ةدحو ةفاضلا مكال تايلمع يلا لقتنا، SecureX عم WSA جدم 1. ةوطخلا وه امك، ظفح قوف رقنا م، بلطلل ينمزل راطلا دادعاب مقو، كزاهج ددح م، بيولا نامأ زاهج ةروصلال يف حضورم.

CISCO SecureX

Dashboard Integrations **Orchestration Beta** Administration

Settings

Your Account

Devices

API Clients

Integrations

**Available Integrations**

Users

### Add New Web Security Appliance Module

Module Name\*

Web Security Appliance

Registered Device\*

wsa02.mex-amp.lab

wsa02.mex-amp.lab

Type WSA

ID [REDACTED] 8a-640868b6ae54

IP Address [REDACTED] 0.19

Request Timeframe (days)

60

Save Cancel

ددح، ةديج تامولعم ةحول + ةنوقيأ قوف رقنا، كب ةصاخلا تامولعملا ةحول عاشنإل 2. ةوطخلا تامولعملا ةحولل امه مادختسا ديرت ابناجتو امسا.

## Web Security Appliance

### Incoming Files Analyzed by AMP

A set of metrics summarizing incoming files analyzed by AMP



### HTTPS Reports

A set of metrics summarizing web transactions for HTTP and HTTPS traffic



### Top Domains

A set of metrics summarizing top domains in web transactions



### Top Malware Categories

A set of metrics summarizing Top Malware Categories in web transactions



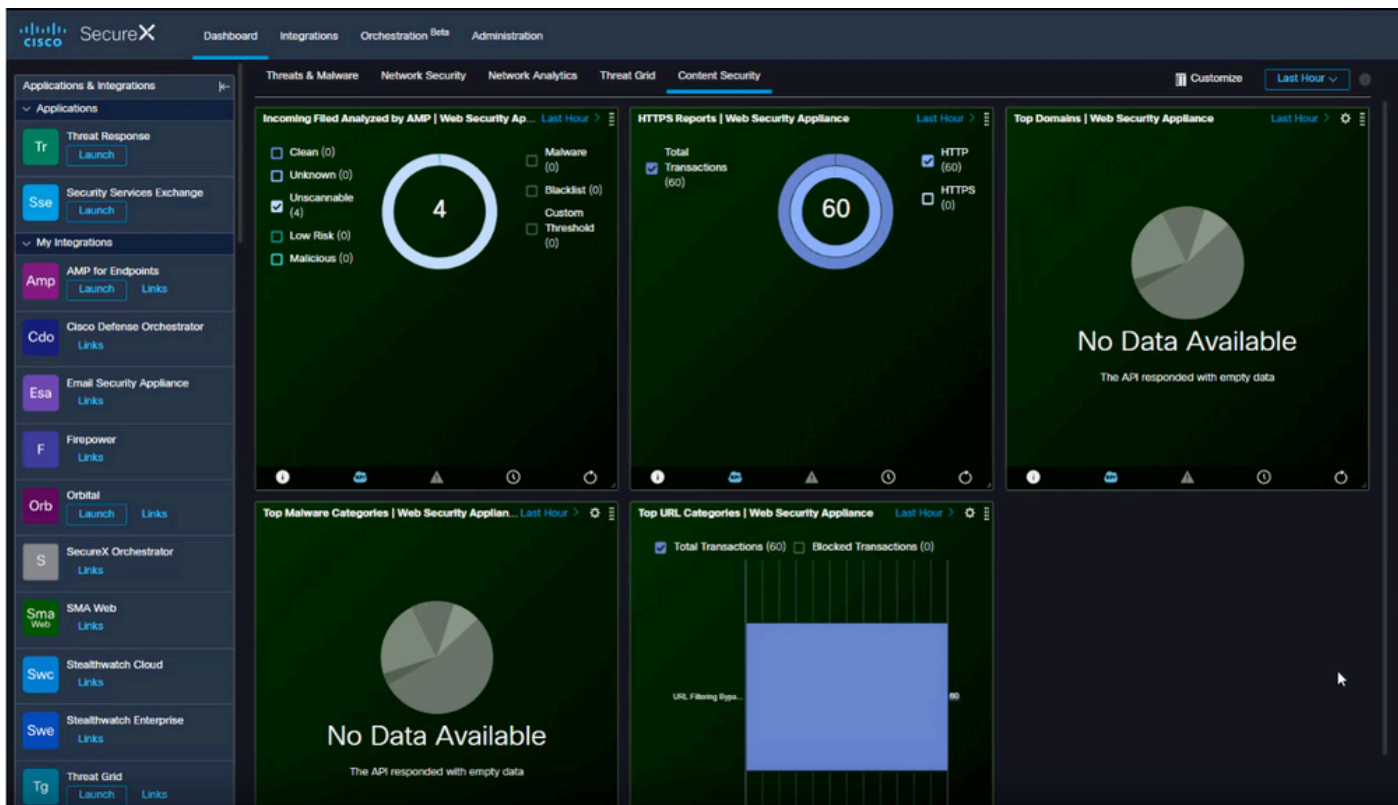
### Top URL Categories

A set of metrics summarizing Top URL Categories in web transactions



## ةحصللا نم ققحتلا

SSE جذومن يف اهرشن مت يتلا تامولعمللا ةحول تامولعم ةدهاشم كنكمي لمكتلا ءارجإ دعب عم SSE ةباوب لئغشت متيو اهنع فشكلا مت يتلا تاديدهتلا نم ي أ قوف رقنلا كنكمي اهيلع ثدحلا عون ةيفصت لماع.



## اه حالص او عاطخال فاشكتسا

نم زاخال ليجست نم ققحتل

نع ثحبا. لاصلتال اولاح نم ققحتلل ةيفللخال ةهجال يف curl رمألا ليغشتب مق 1. ةوطخال لهؤملا لاجملا مسا FQDN لثم لوقحلال عم قفاوتملا جارخال نم لدابتلا تحت ةلاخال لوقح: ةلجسمللا ةلاخال يف لجملا زاخال. ليجستلا، (لمكالب):

```
<#root>
```

```
/usr/local/bin/curl -XGET -v
```

```
http://localhost:8823/v1/contexts/default
```

```
"exchange": [
  {
    "type": "registration",
    "status": "Enrolled"
  },
  {
    "name": "",
    "description": "Device has been enrolled."
  }
]
```

لصوملا نم اهؤارچا مت يتيلا تامالعستسالا نم ققحتلا اضيا كنكمي، جارخال اذ نم 2. ةوطخال

```
type": "administration",
  "statistics": {
    "transactionsProcessed": 20,
    "failedTransactions": 0,
    "lastFailedTransaction": "0001-01-01T00:00:00Z",
    "requestFetchFailures": 0,
    "responseUploadFailures": 0,
    "commandsProcessed": 20,
    "commandsFailed": 0,
    "lastFailedCommand": "0001-01-01T00:00:00Z"
```

SSE (5) إلى لصوملا نم اهل مع مت يتل بلقلا تاض بن نم ققحتلا اضيأ كنكمي 3. ةوطخلا (يضارتفا لكش ب قئاقد):

```
refresh": {
  "registration": {
    "timestamp": "2010-06-29T03:51:45Z",
    "timeTaken": 1.387869786,
    "successCount": 6,
    "failureCount": 0
```

إلى لقننتلا كمزلي WSA. إلى لصوملا تالجس نم ققحتلل 4. ةوطخلا:

<#root>

/data/pub/sse\_connectord\_logs/sse\_connectord\_log.current

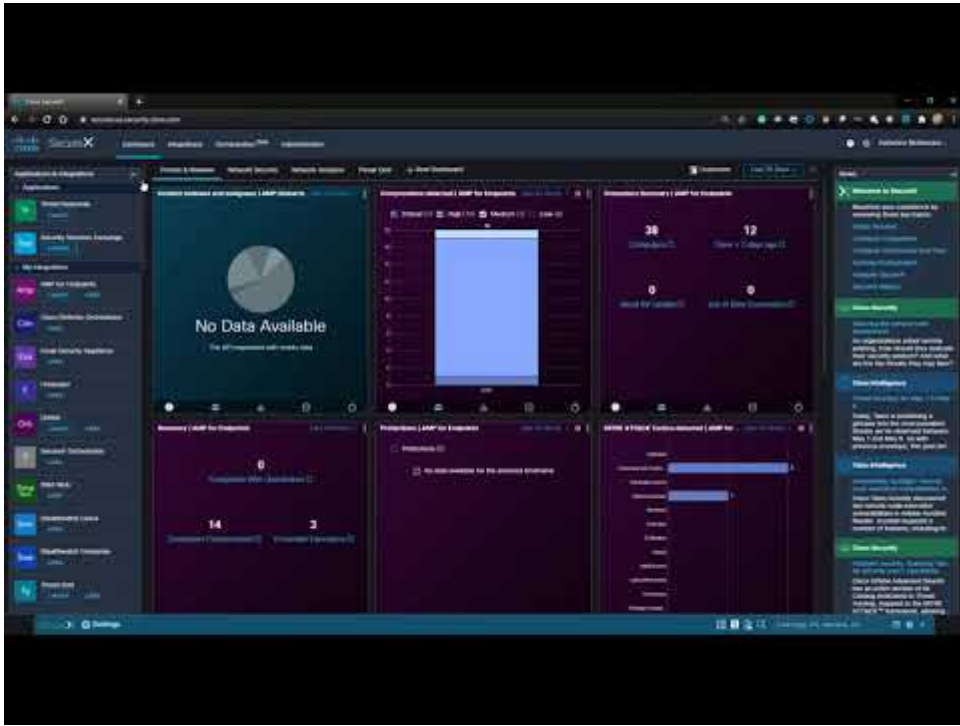
sse\_connectord\_log.current في اهلي ع روثلع نكمي يتلا تامولعمل

- SSE عم ليجستلا ةكرح
- ءارثإل مالعتسا تالجس
- SSE ةبواب في ليجستلا ءاغلل تالجس

## ويديفلا

ويديفلا اذه في دنتملا اذه في ةدراول تامولعمل إلى ع روثلع كنكمي





ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت  
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او  
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب  
Cisco ةللخت. فرتمة مچرت مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او  
ىل إلمءءاد ءوچرلاب ةصوء و تاملرتل هذه ةقء نء اهءل وئس م Cisco  
Systems (رفوتم طبارل) ةلصلأل ةزىلچنلأل دن تسمل