

اهال صا وهئاطخأ فاشكتساو Cisco XDR جمد نمألا ةيامحل رادج مادختساب

تايوتحمل

[ةمدقملا](#)

[ةيساسال تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[نيوكتلا](#)

[صيخرتلا](#)

[ةزهجال لفس SSE بكتاباسح طبارأ](#)

[تاقيقحتلا ءارثا: \(لمأكتلا فصن\) 1 ةقيرطلا](#)

[SSE يف ةزهجال لفس](#)

ةمدقملا

فاشكتساو متحصنم ققحتلاو نمألا ةيامحل رادج عم Cisco XDR جمدل قبولطملا تاوطخلا دنتسملا اذه فصوي
اهال صا وهئاطخأ.

ةفلتخم جئاتن رفوي جمد لكو، XDR و Secure Firewall جمدل ناتقيرط لكانه.

نمألا قباحس يف مكحتلاو، (SSX) نامألا تامدخ لدابتو، نمألا ةيامحل رادج جمد ةيفيك ىلوالا ققيرطلا فصت
تاقيقحتلا ءارثا XDR و XDR تاليلحتو.

و SAL Cloud و XDR-A و نمألا قباحس يف مكحتلاو SSX و نمألا ةيامحل رادج جمد ةيفيك ةيناثلا ققيرطلا فصت
ثداوخل ءارثا XDR.

ةيساسال تابلطتملا

تابلطتملا

ةيلاتلا عيضاوملاب ةفرعم لكيدل نوكت نأب Cisco يصوصت:

- Firepower (FMC) قراد زكرم
- نمألا ةيامحل رادج
- روصلل ةيرايختخالا ةيضارتفال ةاكاحملا
- Cisco Defense Orchestrator
- نامألا تامدخ لدابت
- نامألا قباحس يف مكحتلا

ةمدختسملا تانوكملا

- 7.2 - نمآل اقيامحل رادج
- 7.2 Firepower (FMC) قراد زكرم
- (SSX) نامآل تامدخ لدابت
- Cisco نم XDR
- Smart صيخرتل اقبوب
- Cisco Defense Orchestrator
- نامآل اقباسح سيف مكحتل

قرهجال اعيماج تادب. قصاخ ايلمعم ائيبي يف قنوجومل قرهجال نم دنسمل اذه يف قنراول تامولعمل اءاشن مت كمهف نم دكأتف، ليغشتل دي قكتكبش تناك اذ. (يضا رتفا) حوسمم نيوكتب دنسمل اذه يف قمدختسمل رم آل لمحتحمل ريثأتلل

نيوكتل

صيخرتل

يرهامل باسحل راودا:

يكل باسحل طبر زايتم اب يكل باسحل لوؤسم و ايرهامل باسحل لوؤسم طقف عتمتي SSE باسح.

عمئاق تحتو software.cisco.com لىلق تنا، يكل باسحل رود حص نم ققحتلل. 1. عوطخل يكل باسحل قراد دح، قرادل



Download & Upgrade

Software Download
Download new software or updates to your current software

eDelivery
Get fast electronic fulfillment of software, licenses, and documentation

Product Upgrade Tool (PUT)
Order major upgrades to software such as Unified Communications

Upgradeable Products
Browse a list of all available software updates.



Network Plug and Play

Plug and Play Connect
Device management through Plug and Play Connect portal

Learn about Network Plug and Play
Training, documentation and videos



License

Traditional Licensing
Generate and manage PAK-based and other device licenses, including demo licenses

Smart Software Licensing
Track and manage Smart Software Licenses.

Enterprise Agreements
Generate and manage licenses from Enterprise Agreements.

View My Consumption
View all my customers based on smart accounts



Order

Buy Directly from Cisco
Configure, price, and order Cisco products, software, and services Available to partners and to customers with a direct purchasing agreement.

End User License and SAAS Terms
Cisco software is not sold, but is licensed to the registered end user. The terms and conditions provided govern your use of that software. Read them here.



Administration

All Users:

Request a Smart Account
Get a Smart Account for your organization or initiate it for someone else

Request Access to an Existing Smart Account
Submit a request for access to a Smart Account

Manage Smart Account
Review the properties of your Smart Accounts and associate individual Cisco Accounts with Smart Accounts.

Learn about Smart Accounts
Access documentation and training.

Additional for Partners:

Request a Partner Holding Account
Allows Cisco Partners to request a Holding Smart Account

Manage Pending Smart Accounts
View the properties of Smart Accounts in 'Pending' status requested on behalf of Customers and take actions to activate the Smart Accounts

نبيعت نم ققحتو، نيمدختسم الى لقتنا، مدختسم الى رود ةحص نم ققحتلل 2. ةوطخل
 ةروصل الى ف حضوم وه امك، يرهاظ باسح لوؤسم الى راودال تحت تاباسحل

Cisco Software Central > Manage Smart Account > Users

TAC Cisco Systems, Inc. Help

Account Properties | Virtual Accounts | **Users** | Custom Tags | Requests | Account Agreements | Event Log

Users

Users | User Groups

Add Users... Remove Selected... Export Selected...

User	Email	Organization	Account Access	Role	User Group	Actions
☐ danielbenj						
☐ Daniel Benitez danielben	danielben@cisco.com	Cisco Systems, Inc.	All Virtual Accounts Mex-AMP TAC	Smart Account Administrator Virtual Account Administrator	-	Remove...

1 User

صيخرت الى ليوتحي SSE الى طابتراللدحم ال "يرهاظل باسحل" نأ نم دكأت 3. ةوطخل
 نامال ةزهجأو SSE الى نامال صيخرت الى ليوتحي ال باسح طابتراللاح في نامال ةزهجأل
 SSE. ةبابو الى ليوتحي ال ثدحل او

Cisco Software Central > Smart Software Licensing

TAC Cisco Systems, Inc. Feedback Support Help

Alerts | Inventory | Convert to Smart Licensing | Reports | Preferences | On-Prem Accounts | Activity

Virtual Account: **Mex-AMP TAC** 13 Minor Hide Alerts

General | **Licenses** | Product Instances | Event Log

Available Actions Manage License Tags License Reservation...

Search by License

License	Billing	Purchased	In Use	Balance	Alerts	Actions
☐ FPR1010 URL Filtering	Prepaid	10	0	+ 10		Actions
☐ FPR4110 Threat Defense Malware Protection	Prepaid	1	0	+ 1		Actions
☐ FPR4110 Threat Defense Threat Protection	Prepaid	1	0	+ 1		Actions
☐ FPR4110 Threat Defense URL Filtering	Prepaid	1	0	+ 1		Actions
☐ HyperFlex Data Platform Enterprise Edition Subscription	Prepaid	2	0	+ 2		Actions
☐ ISE Apex Session Licenses	Prepaid	1	0	+ 1		Actions
☐ ISE Base Session Licenses	Prepaid	10	0	+ 10		Actions
☐ ISE Plus License	Prepaid	10	0	+ 10		Actions
☐ Threat Defense Virtual Malware Protection	Prepaid	10	1	+ 9		Actions
☐ Threat Defense Virtual Threat Protection	Prepaid	10	1	+ 9		Actions

10 Showing Page 5 of 7 (85 Records)

صيخارت الى لقتنا، حيصل ال يرهاظل باسحل في FMC ليچست نم ققحتلل 4. ةوطخل
 يكلذل صيخرتل اظنل

Smart License Status

Cisco Smart Software Manager

Usage Authorization:	✓ Authorized (Last Synchronized On Jun 10 2020)
Product Registration:	✓ Registered (Last Renewed On Jun 10 2020)
Assigned Virtual Account:	Mex-AMP TAC
Export-Controlled Features:	Enabled
Cisco Success Network:	Enabled ⓘ
Cisco Support Diagnostics:	Disabled ⓘ

Smart Licenses

License Type/Device Name	License Status
> Firepower Management Center Virtual (1)	✓
> Base (1)	✓
> Malware (1)	✓
> Threat (1)	✓
> URL Filtering (1)	✓
> AnyConnect Apex (1)	✓
> AnyConnect Plus (1)	✓
AnyConnect VPN Only (0)	

Note: Container Instances of same blade share feature licenses

ةزهجال لچسو SSE ب ك تاباسح طبرأ

SSE باسح ب ي كذل ك تاباسح طبر كيلي ع بچي، SSE باسح ىل ل لوخدل ليحست دن ع 1. ةوطخل تاباسحل طبر ديحتو تاودال زمر قوف رقلل ىل لجاتحت كذل



Daniel Benitez ▾

Link Smart/Virtual Accounts

Link CDO Account

Downloads

ةيره اظلال تاباسحلا ةفاك ىلع يوتحي يذلا بكذلا باسحلا ىرتس ،باسحلا طبر درجمب هيلع ةدوجوملا

تاقىقحتلا ءارثا : (لماكلال فصن) 1 ةقىرطلال

SSE فى ةزهجال لىجست

كتئيب ىلع اهب حومسم هذه URL نىوانع نأ نم دكأت 1. ةوطخل

ةكىرمالال ةقطنملا

- api-sse.cisco.com
- eventing-ingest.sse.itd.cisco.com
- mx*.sse.itd.cisco.com
- dex.sse.itd.cisco.com
- eventing-ingest.sse.itd.cisco.com
- registration.us.sse.itd.cisco.com

ىبوروالال داحتالال ةقطنم

- api.eu.sse.itd.cisco.com
- mx*.eu.sse.itd.cisco.com
- dex.eu.sse.itd.cisco.com
- eventing-ingest.eu.sse.itd.cisco.com
- registration.eu.sse.itd.cisco.com

نالكبأ مىلقا

- api.apj.sse.itd.cisco.com
- mx*.apj.sse.itd.cisco.com
- dex.apj.sse.itd.cisco.com
- eventing-ingest.apj.sse.itd.cisco.com
- registration.apj.sse.itd.cisco.com

هده URL ناونع مادختساب SSE ةبابوب ىلإ لوخدلا لىجس 2. ةوطخل <https://admin.sse.itd.cisco.com>، وه امك Cisco XDR response و Eventing نىرايخلال الك نىكمتب مقو ،ةباسحلال تامدخ ىلإ لقتنا ةقطنملا ةروصلال فى حضورم

Cisco XDR

Cisco XDR enablement allows you to utilize supported devices in the course of a cybersecurity investigation. It also allows this platform to send high fidelity security events and observations to Threat Response.



Eventing

Eventing allows you to collect and view events in the cloud.



SSE: في ةلجسم ال ةزهجآلا ةيؤر نآلا كنكمي هنأ نم ققحتل كنكمي 3. ةوطخل

Security Services Exchange

Devices Cloud Services Events Audit Log

Devices for Sourcefire Support

0 Rows Selected

	%	#	Name	Type	Version	Status	Description
☐		1	Responder	Cisco Firepower Threat Defense for VMWare	6.5.0	Registered	27 Responder (FMC managed)
			Created 2020-08-10 19:51:48 UTC	IP Address: 10.10.10.27			Connector Version:
☐		2	MEX-AMP-FMC	Cisco Firepower Management Center for VMWare	6.5.0	Registered	24 MEX-AMP-FMC
			Created 2020-08-10 20:17:37 UTC	IP Address: 10.10.10.24			Connector Version:

Page Size: 25 Total Entries: 2

ةباوب ىلع ةدوجوم ال ةادحآلا ىلإ لقتنا ،ةنمآلا ةيماحل راج ةزهجآ ةطساوب ةادحآلا لاسرا متي
في حضوم وه امك ،SSX ىلإ ةزهجآلا ةطساوب اهل لاسرا متي ةادحآلا نم ققحتل ل SSX
ةروصل:

Security Services Exchange

Devices Cloud Services Events Audit Log

Event Stream for Sourcefire Support

0 Rows Selected

Enter filter criteria

08/04/2020, 18:50 - 08/05/2020, 18:50

	Talos Disposition	Incident	Destination IP	Event Time	Ingest Time	Message	Protocol	Reporting Device ID	Source IP
☐	Neutral	No	10.10.10.252	2020-08-05 18:48:50 UTC	2020-08-05 18:48:51 UTC		tcp	09d441eedce5	100
☐	Neutral	No	10.10.10.145	2020-08-05 18:47:38 UTC	2020-08-05 18:47:38 UTC		tcp	09d441eedce5	100
☐	Unknown	No	10.10.10.100	2020-08-05 18:47:30 UTC	2020-08-05 18:47:30 UTC		tcp	09d441eedce5	100
☐	Neutral	No	10.10.10.252	2020-08-05 18:46:50 UTC	2020-08-05 18:46:50 UTC		tcp	09d441eedce5	100

(SCC/CDO) نامآلا ةباحس في مكحتل في ةزهجآلا ليحست

كتئيپ ىلع اهب حومسم هذه [URL نيوانع](#) نأ نم دكأت 1. ةوطخل

ةيكي رملال ةقطنم:

- defenseorchestrator.com
- edge.us.cdo.cisco.com

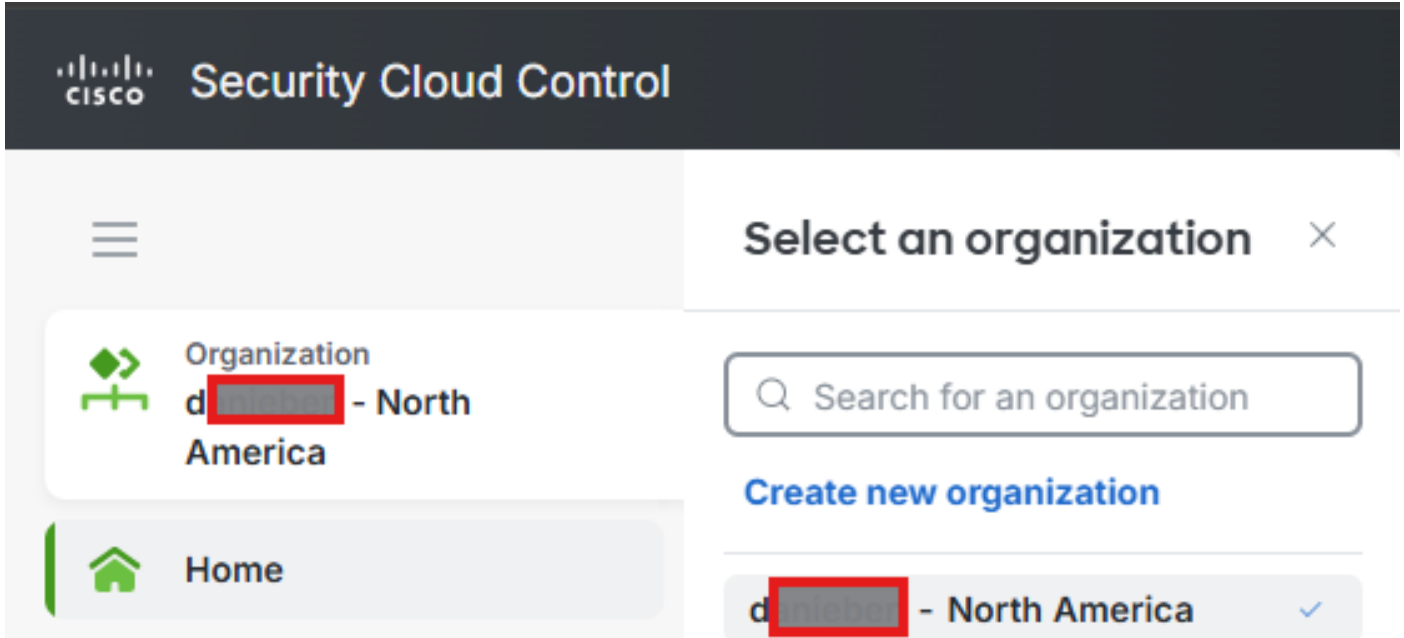
يبوروال داخالا ةقطنم

- defenseorchestrator.eu
- edge.eu.cdo.cisco.com

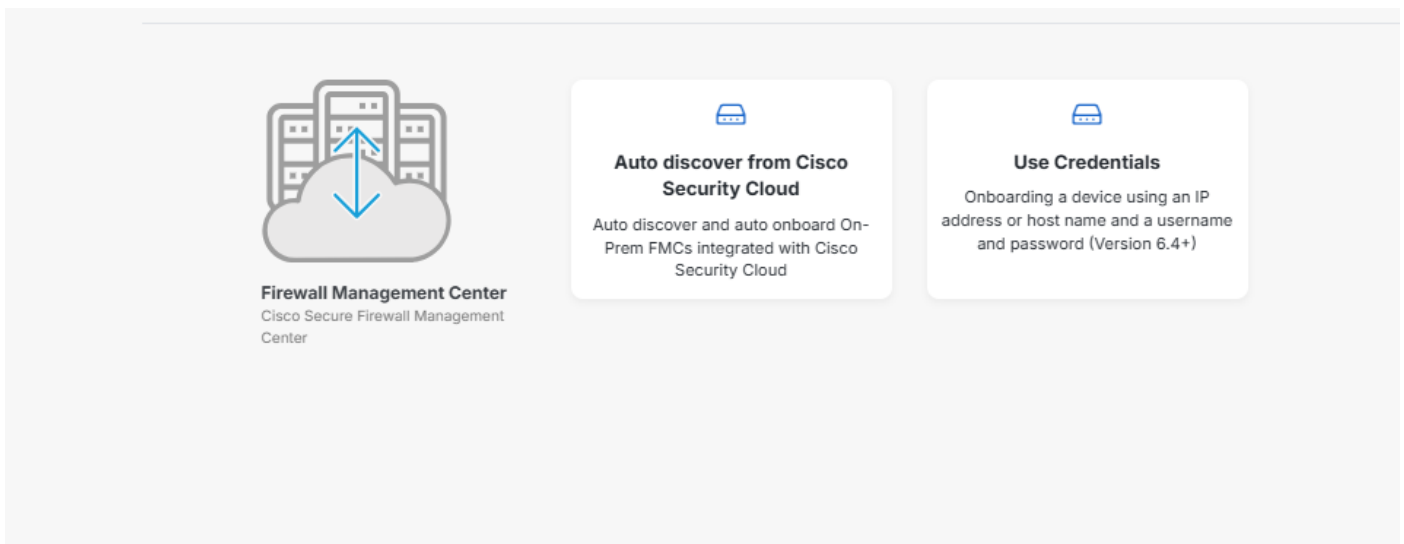
ناكبأ مليقإ

- apjc.cdo.cisco.com
- edge.apjc.cdo.cisco.com

(كثقتنم بسح طابترالا فلتخي نأ نكمي) [نامألا ةكبش يف مكحتلا](#) ىلإ لقتنا 2. ةوطخل
نامألا ةباحس يف مكحتلا ةسسؤم ديدحتل كهجوي اذهو.



ناك اذا امم ققحت، Products>Firewall ىلإ لقتنا، ةبسانملا ةسسؤملا ديدحت درجم 3. ةوطخل
ةباحس يف مكحتلا ىلإ هنيمضت كنكمي ف، ادوجوم نكي مل نإ، لعفلاب ادوجوم كي دل زاهجلا
عيمج ديدحت قوف رقنا، ةماعلا درجال ةمئاق نمض، اذهل، (Cisco Defense Orchestrator) نامألا
ةزهجال.



FMC ةمظنأب ةمئاق مي دقت متي، ةيماجل راج ةرادإ زكرم Administration ىلإ لقتنا 4. ةوطخل
Plus. زمر ىلع رقنا، ةيماجل راج ةرادإ زكرم ىرت مل اذا، SCC يف ةجمدملا

كذلك رمألا نكي مل اذا، ةحوللا ىلع ايئاقلت ةنمألا ةيماجل ناردرج جاردا متي، ةداع 4.1. ةوطخل
لوخدلا ليجست بولسأو (FTD عضو يف) ةحوللا ىلع همادختسا ديرت يذلا زاهجال ددح
كي دل لصفملا.

يُلع نمآلآةي امحل رادج زاهج ددح ،دئاز ةنوقي قوف رقنا نامآلآةزهجأ مسق تحت 4.2 ةوطخلل ةحولل

Security Devices

Devices Templates Search by Device Name, IP Address, or Serial Number Displaying 4 of 4 results

All FTD

Onboard FTD Device

Follow the steps below

Firewall Threat Defense

Important: After you onboard the threat defense device to cdFMC or the Firewall Management Center using the zero-touch provisioning method, the device will be managed by the corresponding manager it is onboarded to. Note that the firewall device manager will no longer manage the device, and all existing policy configurations on the device will be lost except for the basic interface configurations. Therefore, you must configure the policies from the corresponding manager.

- Use CLI Registration Key**
Onboard a device using a registration key generated from SCC and applied on the device using the Command Line Interface. (FTD 7.0.3+ & 7.2+)
- Use Serial Number**
Onboard a factory-shipped FTD 7.2+ device to cdFMC or to a 7.4+ On-Prem FMC using zero-touch provisioning.
- Deploy an FTD to a cloud environment**
Deploy a device to supported cloud platforms: AWS, GCP, and Azure.
- Bulk Onboard using CSV File**
Use this method for adding multiple devices by uploading a .csv file, with template assignment. (FTD 7.4+)

كنكمي ،"نامآلآةباحس يف مكحتل" يف كتزهجأ لىل لوصولل ليحست درجمب 5 ةوطخلل نوزملم يف اهروصت.

لقتنا ،ببسل اذهل ،كب ةصاخل SSX ةسسؤمب ةطبترم CDO ةسسؤم نأ نم دكأت 6 ةوطخلل CDO باسح طابترل قوف رقناو ،"تاودأ" ةمئاقل زمر قوف رقناو ،"نامآلآةامدخ لدابت" لىل

Security Services Exchange Devices Cloud Services Events Audit Log

Devices for XDR BETA - TAC Org

Device Name / ID

- Link Smart/Virtual Accounts
- Unlink Smart/Virtual Accounts
- Link CDO Account
- Downloads

Cisco XDR عم 7.2.x نمآلآةي امحل رادج جم د

SecureX > جم دل لىل لقتنا ،نمآلآةي امحل رادج ةرادل زكرم يف 1 ةوطخلل

Firewall Management Center Integration / SecureX

Overview Analysis Policies Devices Objects Integration

SecureX Setup

This feature allows Secure Firewall Management Center to integrate with other SecureX services via SecureX ribbon.

SecureX	Intelligence
Security Analytics & Logging	Incidents
Other Integrations	Sources

SecureX نيكم ت قوف رقناو ،ةبسانملم ةقطنملم رتخأ 2 ةوطخلل



SecureX Integration

SecureX Setup

This feature allows Secure Firewall Management Center to integrate with other SecureX services via SecureX ribbon. [Learn more](#)

1

Cloud Region

This setting determines where events are sent to, if configured to send to the cloud, as well as data generated by the Cisco Success Network and Cisco Support Diagnostics tools.

Current Region

us-east-1 (US Region)

2

SecureX Enablement

After completing this configuration, the SecureX ribbon will show up at the bottom of each page. [Learn more](#)

[Enable SecureX](#)

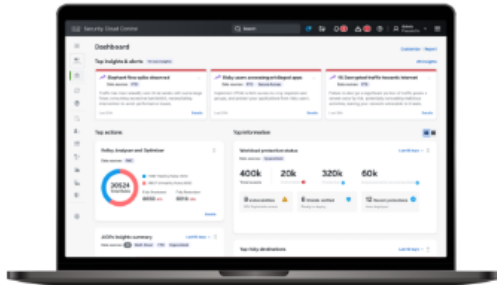
Cisco قد اصبحت حصة إلى كهي جوت دي عي هناف SecureX، نيكمت قوف رقننلا دعب 3. ةوطخلا إلى ةعباتم قوف رقنا، (نامألا ةباحس لوخد ليجست نم ديفتست يتلا) Cisco Defense Orchestrator إلى ةعباتم قوف رقنا، (نامألا ةباحس لوخد ليجست نم ديفتست يتلا) Cisco SSO.



Welcome to the Cisco Security Cloud

Delivered through Security Cloud Control (SCC)

Staying on top of security is easier than ever. Security Cloud Control helps you consistently manage policies across your Cisco security products. It is a cloud-based application that cuts through complexity to save time and keep your organization protected against the latest threats.



SCC complements FMC by allowing you to:

- Drive consistent policy through shared object management with FMCs
- Enable Zero-Touch Provisioning of FTDs
- View events in the cloud
- Get a centralized view of inventory across FMCs
- Leverage cloud CSDAC and Cloud Delivered FMC
- and [more](#)

To continue with cloud registration of your FMC, you will need a Cisco Security Cloud Sign On (SSO) user account.

If you don't already have a Cisco SSO account, please proceed below and Sign Up for free. Note that you will need to restart the cloud registration from your FMC after your new SSO account is created.

If you already have a Cisco SSO account, please proceed below to choose or create a free SCC account to register your FMC.

Let's get started!

1

Sign Up/Sign In with Cisco SSO

2

Register FMC with a SCC Tenant

[Continue to Cisco SSO](#)

ءاشنإ وأ اقبس م دووم نام ةباحس يف مكحت رصنع رجاتسم ديدحت اما كنكمي 4. ةوطخل ديدج رجاتسم

قباطي ةحفصل هذه يف هاقلتت يذلا زمرلا نأ نم دكأتو بسانم رجاتسم لدح 5. ةوطخل FMC ليفوخت قوف رقنا ،قباطم ناك اذا ،FMC يف هاقلتت يذلا زمرلا

Please verify the code provided by SecureX.

9C1FEC52

Close

Grant Application Access

Compare the code below to the authorization code shown in the FMC tab. If the codes match, authorize the FMC to complete the registration.

If the codes do not match, [cancel registration](#).

9C1FEC52

FMC would like access to your SCC tenant **danieben**.

- **Users:** All internal users in FMC will have read-only access to this SCC tenant.
- **Data:** FMC will be able to collect data using SCC APIs.

The FMC will be registered with tenant **danieben**

Authorize FMC

ههلامتك ادرج بم، جم دلا لى وخت و نام ألال اعباحس ىل ل وخذلا لى جست دامت عا تانايب لخدأ. 6 ةوطخلال، Cisco نام ألال اعباحس عم لى جست لل اهل وخت مت دق FMC نأ لى لكأت مي دقت متي.



Welcome to Security Cloud Control

You have successfully authorized your FMC to register with Cisco Security Cloud, you may now close this tab.

ديرت يتي لثا دحلأا دي دحتو، FMC ب لاصتال ا دإعإ كنكمي، ضيوفتال لامتكا دعب 7. ةوطخل ظفح قوف رقنا، كلذ نم ءهانتال درجمبو ءارظنل ةومجم ىلإ اهل اسرا

SecureX (XDR ةتمتأ) نمازت نيكمت دي دحت كنكمي 8. ةوطخل

2

SecureX Enablement

After completing this configuration, the SecureX ribbon will show up at the bottom of each page. [Learn more](#)

▲ SecureX is enabled for US Region. You will need to save your configuration for this change to take effect.

[Enable SecureX](#)

3

Event Configuration

☒ Send events to the cloud

☒ Intrusion events

☒ File and malware events

☒ Connection Events

☐ Security

☒ All

● View your Cisco Cloud configuration

View your Events in SecureX

4

Orchestration

Enable SecureX orchestration to allow SecureX users to build automated workflows that interact with various resources in the Secure Firewall Management Center. [Learn more](#)

☒ Enable SecureX Orchestration

Specify the Firewall Management Center user role you want to assign to the SecureX orchestration workflows.

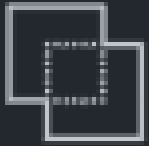
Assigned Role

Access Admin

Save

كتزهجأ نع ثحباو On Premises زاهال >(XDR ةرادا) XDR>Administration ىلإ لقتنا 9. ةوطخل اياقلا ل اهل لجست متي نأ بجي

نمآلا ةيامحل رادج لماكت نيكمتو لماكتال تاي لمع XDR> ةرادا ىلإ لقتنا 10. ةوطخل



Secure Firewall

powered by
CISCO

Cisco Managed

Secure Firewall (formerly Firepower) provides complete and unified management over firewalls, application control, intrusion prevention, URL filtering, and advanced malware protection.

Free Trial

Get Started

ةفاضل+ قوف رقنا ،كب صاخلا لماكتلل مسا نبيعتب مق 10.1 ةوطخلا

ADD INTEGRATION

Integration Name *

Secure Firewall CDO Integration

Manage On-Premises Appliances

Check for New Appliances

Name	Version	Status	Description	IP Address
AMP 	7.2.5-208	✓ Registered	JMX2716X2M1	10.
MexAmp-FTD	7.2.0	✓ Registered	10. MexAmp-FTD (FMC managed)	10.
mexMEX-AMP-FMCMex	7.2.0.1	✓ Registered	10. mexMEX-AMP-FMCMex	10.

Rows per page

30

1-3 of 3

<

1

>

☒ Create Dashboard

Create a dashboard of the tiles associated with this integration, which can be shared by all members of your organization.

+ Add

XDR. لخاد تاقىقحتلل ءارثل جمدل اذه كل حيتي

XDR في شادحأل اءارثا: (لمالكال لمالكال) 2 ةقيرطال

ءءاعإل لىءسئل او نامأل الال لىءل ءىءرء لىء ءىءل CDO باسء لىءءىء نأ بءى 1. ةوطءال Cisco XDR لىء شادحأل الال لىءءو.

فى مكءال او SSX فى ءءزهء لىءسئل اقباى ءءضوءال الال ماءءسإ لىءى 2. ةوطءال نامأل الال باءس.

طبر بلطو لىءصافءال الال الال ماءءسإ اب TAC لىءل لوصووال لىءى، ءاءءنالال ءرءمب 3. ةوطءال XDR الال لىءلءءب SAL/نامأل الال باءس فى مكءال الال.

- CDO رءأسم فرعم
- CDO مسا
- XDR Org ID
- SSE رءأسم فرعم
- SSE مسا
- SCA ةسسؤم فرعم

XDR الال لىءلءءب ةباوبب ءب صاءال CDO باسء طابءرا نم ءءأء 4. ةوطءال

:لىءى امء وءبى، XDR الال لىءلءءب CDO ةباوب طبر لبق

Dashboard

Multicloud Defense

Monitor

Insights & Reports

Events & Logs

Events & Logs

Events

Event Logging

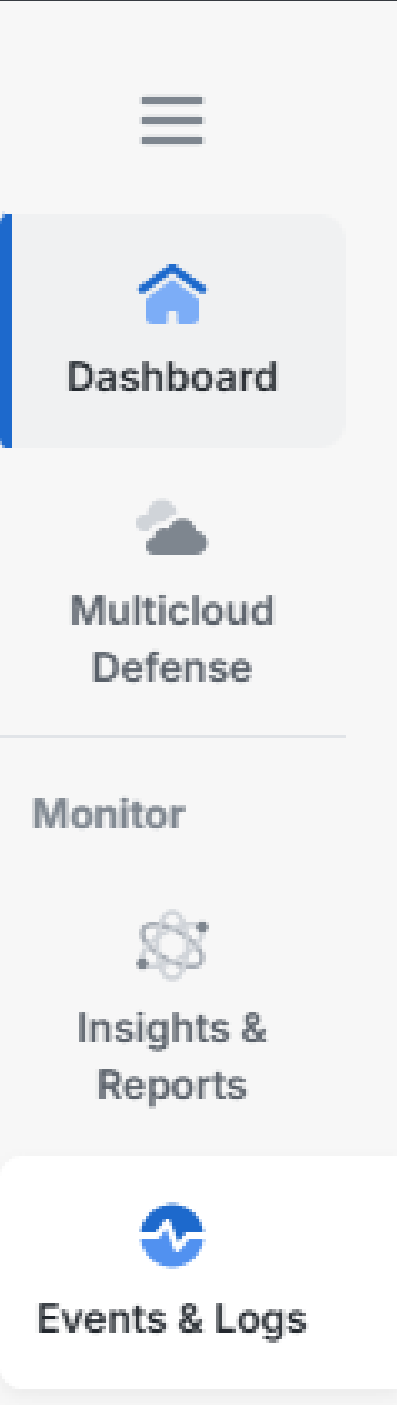
Jobs

Logs

Change Log

Firewall Threat Defense

XDR. تاليلحت لخدم ىلإ لاقتنالل رايلال ةيؤركنكمي ،طابتالالامتكادعب



Event Logging

Jobs

Secure Cloud Analytics

Change Log

Firewall Threat Defense

Security Cloud Control Portal ب ك ب صاخال XDR تاليلحت باسح طبرم تي ن ا م 5. ةوطخال XDR، تاليلحت ي ف ،اذهل، XDR عم ةجم دم XDR تاليلحت ن ا نم دكأت ال ال جاتحت، (CDO) ن ا نم ورضخا ققحت دوجو نم دكأتو XDR لم اكن نع ثحبا ، Settings>Integration>XDR ال لقتنا ةححصال XDR ةسسؤم ال ريشت لم اكن ةدحو.



✓ Cisco XDR Integration ✓

Status: Enabled

The integration module for **XDR BETA - TAC Org** Cisco XDR organization has been active since 2 de mayo de 2023, 10:37 a.m. GMT-6.

If you remove this integration, the Secure Cloud Analytics module will no longer be available in your Cisco XDR portal.

Remove

ةحصنل نم ققحتل

للستل ثادلأو، (قارتخأ وأ ةراض جمارب) ثادلأ عاشنإب موقت ةنمألآ ةياملل نارنج نأ نم ققحتل
ىلإ لقتنا، لفظتل ثادلأ، ةراضل جمارب لل ثادلأ ةلافلملل ةلئلل لقتنا
لفظتل ثادلأ Analysis>

ةزهألآ ليجست 4 ةوطخل ي ف روكذم وه امك SSE ةبابو ىل ع ةلجسمل ثادلأ ةحص نم ققحتل
SSE مسق ىل ع.

ةهجاو تالجس نم ققحتل وأ Cisco XDR تامولعم ةحول ىل ع تامولعمل هذه ضرع ةحص نم ققحتل
تاقببطل ةجمرب ةهجاو لشف ببس ىل ع ةالطال كنكمي ىل ع (API) تاقببطل ةجمرب
لحمل (API).

حتفا، لكاشم كيدل تناك اذا، حيحص لكشب اعم نوطبترم ني رجاتسمل اعم نم ققحتل
ةيلاتل لىصافتل ريفوتب مقو ةينفل ةدعاسمل زكرم ةلاح:

- رجأتسم فرع م CDO
- مسا CDO
- XDR Org ID
- رجأتسم فرع م SSE
- مسا SSE
- سسؤم فرع م SCA

اهالصلإو ةاطخلأ فاشكتسا

لاصتال لكاشم فاشكتسا

لشفل تالاح ي ف action_queue.log فلم نم ةماعل لاصتال لكاشم نع فشكل كنكمي

فلملالي ف ةدوچومل تالچسل هذه ةيؤر كنكمي:

```
ActionQueueScrape.pl[19094]: [SF::SSE::Enrollment] canConnect: System (/usr/bin/curl -s --connect-timeout
```

لاصتالا نم ققحتلا بجيو ةيلمعلا ةلهم ءاهتنا 28 جورخلا زمرينعي، ةلاحلا هذه في
DNS ةقد في لكاشم ينعي يذلا 6 جورخلا زمر اضيا ىرت نا بجي. تنرتنللاب

DNS ةقد ببسب لاصتالا تالكشم

جحص لكشب لمعي لاصتالا نا نم دكأت 1. ةوطخل

```
root@ftd01:~# curl -v -k https://api-sse.cisco.com
* Rebuilt URL to: https://api-sse.cisco.com/
* getaddrinfo(3) failed for api-sse.cisco.com:443
* Couldn't resolve host 'api-sse.cisco.com'
* Closing connection 0
curl: (6) Couldn't resolve host 'api-sse.cisco.com'
```

هذه فيو، URL <https://api-sse.cisco.com> ناو نع لىل رداق ريغ زاوجل نا جارخالا اذه حضوي
محص نم ققحتلا كنميو، بسانملا DNS مداخل نيوكت نم ققحتلا لىل جاتحن، ةلاحلا
ريخل (CLI) رماوالا رطس ةهجاو نم NSLOOKUP مادختساب

```
root@ftd01:~# nslookup api-sse.cisco.com
;; connection timed out; no servers could be reached
```

DNS، تادادع ديكأتل، هنيوكت مت يذلا DNS لىل لوصولا متي مل هنا جارخالا اذه حضوي
show network رمالا مدختسا:

```
> show network
===== [ System Information ] =====
Hostname           : ftd01
DNS Servers        : x.x.x.10
Management port    : 8305
IPv4 Default route
Gateway            : x.x.x.1

===== [ eth0 ] =====
State              : Enabled
Link               : Up
Channels           : Management & Events
Mode               : Non-Autonegotiation
MDI/MDIX           : Auto/MDIX
MTU                : 1500
MAC Address        : x:x:x:x:9D:A5
```

```

-----[ IPv4 ]-----
Configuration      : Manual
Address            : x.x.x.27
Netmask            : 255.255.255.0
Broadcast          : x.x.x.255
-----[ IPv6 ]-----
Configuration      : Disabled

===== [ Proxy Information ] =====
State              : Disabled
Authentication     : Disabled

```

رّمألا اذه مَادخِتسَاب DNS تَادَادِعْ رِي غِت كَن كَمِي ،أَطْخَلَا DNS مَادَا مَادخِتسَا مِت ،لَا ثَمَلَا اذه يَف:

```
> configure network dns x.x.x.11
```

اِحْجَان لَاصِتَالَا نَوَكِي ،ةَرْمَلَا هَذَوَى رْخَا قَرْم لَاصِتَالَا اذه رَابِتْخَا دَعَب

```

root@ftd01:~# curl -v -k https://api-sse.cisco.com
* Rebuilt URL to: https://api-sse.cisco.com/
* Trying x.x.x.66...
* Connected to api-sse.cisco.com (x.x.x.66) port 443 (#0)
* ALPN, offering http/1.1
* Cipher selection: ALL:!EXPORT:!EXPORT40:!EXPORT56:!aNULL:!LOW:!RC4:@STRENGTH
* successfully set certificate verify locations:
* CAfile: none
Cpath: /etc/ssl/certs
* TLSv1.2 (OUT), TLS header, Certificate Status (22):
* TLSv1.2 (OUT), TLS handshake, Client hello (1):
* TLSv1.2 (IN), TLS handshake, Server hello (2):
* TLSv1.2 (IN), TLS handshake, Certificate (11):
* TLSv1.2 (IN), TLS handshake, Server key exchange (12):
* TLSv1.2 (IN), TLS handshake, Request CERT (13):
* TLSv1.2 (IN), TLS handshake, Server finished (14):
* TLSv1.2 (OUT), TLS handshake, Certificate (11):
* TLSv1.2 (OUT), TLS handshake, Client key exchange (16):
* TLSv1.2 (OUT), TLS change cipher, Client hello (1):
* TLSv1.2 (OUT), TLS handshake, Finished (20):
* TLSv1.2 (IN), TLS change cipher, Client hello (1):
* TLSv1.2 (IN), TLS handshake, Finished (20):
* SSL connection using TLSv1.2 / ECDHE-RSA-AES128-GCM-SHA256
* ALPN, server accepted to use http/1.1
* Server certificate:
* subject: C=US; ST=California; L=San Jose; O=Cisco Systems, Inc.; CN=api -sse.cisco.com
* start date: 2019-12-03 20:57:56 GMT
* expire date: 2021-12-03 21:07:00 GMT
* issuer: C=US; O=HydrantID (Avalanche Cloud Corporation); CN=HydrantID S SL ICA G2
* SSL certificate verify result: self signed certificate in certificate chain (19), continuing anyway.
> GET / HTTP/1.1
> Host: api-sse.cisco.com
> User-Agent: curl/7.44.0
> Accept: */*
>

```

```
< HTTP/1.1 403 Forbidden
< Date: Wed, 08 Apr 2020 01:27:55 GMT
< Content-Type: text/plain; charset=utf-8
< Content-Length: 9
< Connection: keep-alive
< Keep-Alive: timeout=5
< ETag: "5e17b3f8-9"
< Cache-Control: no-store
< Pragma: no-cache
< Content-Security-Policy: default-src 'self'
< X-Content-Type-Options: nosniff
< X-XSS-Protection: 1; mode=block
< Strict-Transport-Security: max-age=31536000; includeSubdomains;
```

SSE ةبأوب ىلإ ليحستلا لكاشم

ةصاخلا ةرادإلا ةهجاو ىلع SSE URL ناوئعب لاصتا ىلإ نمآلا ةيماحل رادجو FMC نم لك جاتحي رذجلا لوصول عم Firepower CLI ىلع رماوآلا هذه لخدا ، لاصتالا رابتخال ، امه

<#root>

```
curl -v https://api-sse.cisco.com/providers/sse/services/registration/api/v2/clients --cacert /ngfw/etc/
```

```
curl -v https://est.sco.cisco.com --cacert /ngfw/etc/ssl/connectorCA.pem
```

```
curl -v https://eventing-ingest.sse.itd.cisco.com --cacert /ngfw/etc/ssl/connectorCA.pem
```

```
curl -v https://mx01.sse.itd.cisco.com --cacert /ngfw/etc/ssl/connectorCA.pem
```

رمألا اذهب ةداهشلا نم ققحتلا زواجت نكمي:

```
root@ftd01:~# curl -v -k https://api-sse.cisco.com
* Rebuilt URL to: https://api-sse.cisco.com/
* Trying x.x.x.66...
* Connected to api-sse.cisco.com (x.x.x.66) port 443 (#0)
* ALPN, offering http/1.1
* Cipher selection: ALL:!EXPORT:!EXPORT40:!EXPORT56:!aNULL:!LOW:!RC4:@STRENGTH
* successfully set certificate verify locations:
* CAfile: none
Cpath: /etc/ssl/certs
* TLSv1.2 (OUT), TLS header, Certificate Status (22):
* TLSv1.2 (OUT), TLS handshake, Client hello (1):
* TLSv1.2 (IN), TLS handshake, Server hello (2):
* TLSv1.2 (IN), TLS handshake, Certificate (11):
* TLSv1.2 (IN), TLS handshake, Server key exchange (12):
* TLSv1.2 (IN), TLS handshake, Request CERT (13):
```

```
* TLSv1.2 (IN), TLS handshake, Server finished (14):
* TLSv1.2 (OUT), TLS handshake, Certificate (11):
* TLSv1.2 (OUT), TLS handshake, Client key exchange (16):
* TLSv1.2 (OUT), TLS change cipher, Client hello (1):
* TLSv1.2 (OUT), TLS handshake, Finished (20):
* TLSv1.2 (IN), TLS change cipher, Client hello (1):
* TLSv1.2 (IN), TLS handshake, Finished (20):
* SSL connection using TLSv1.2 / ECDHE-RSA-AES128-GCM-SHA256
* ALPN, server accepted to use http/1.1
* Server certificate:
* subject: C=US; ST=California; L=San Jose; O=Cisco Systems, Inc.; CN=api-sse.cisco.com
* start date: 2019-12-03 20:57:56 GMT
* expire date: 2021-12-03 21:07:00 GMT
* issuer: C=US; O=HydrantID (Avalanche Cloud Corporation); CN=HydrantID S SL ICA G2
* SSL certificate verify result: self signed certificate in certificate chain (19), continuing anyway.
> GET / HTTP/1.1
> Host: api-sse.cisco.com
> User-Agent: curl/7.44.0
> Accept: */*
>
< HTTP/1.1 403 Forbidden
< Date: Wed, 08 Apr 2020 01:27:55 GMT
< Content-Type: text/plain; charset=utf-8
< Content-Length: 9
< Connection: keep-alive
< Keep-Alive: timeout=5
< ETag: "5e17b3f8-9"
< Cache-Control: no-store
< Pragma: no-cache
< Content-Security-Policy: default-src 'self'
< X-Content-Type-Options: nosniff
< X-XSS-Protection: 1; mode=block
< Strict-Transport-Security: max-age=31536000; includeSubdomains;
```

 تسيّل رابتخالا نم ققحتم الام لعمال نأل قروطحمال 403 قلاسرلا ىلع لصحت: قظحالما لاصتالا نم ققحتلل قيافكلا هي فامب تبثي اذه نكلو SSE هعقوتي ام

SsecConnector ققحتالا

حضم وه امك لصومال صئاصخ نم ققحتالا كنكمي

```
# more /ngfw/etc/sf/connector.properties
registration_interval=180
connector_port=8989
connector_fqdn=api-sse.cisco.com
```

لاثم اذه، رمالا اذه مادختسا كنكمي يذل EventHandler و SScontor ني لاصتالا نم ققحتلل
ئيس لاصتالا ىلع

```
root@firepower:/etc/sf# netstat -anlp | grep EventHandler_SSEConnector.sock
```

```
unix 2 [ ACC ] STREAM LISTENING 3022791165 11204/EventHandler /ngfw/var/sf/run/EventHandler_SSEConnector.sock
```

ةلصتم قفدلا ةلاح نأ ىرت نأ كنكمي ،تباث لاصتا ىلع لاثم يف

```
root@firepower:/etc/sf# netstat -anlp | grep EventHandler_SSEConnector.sock
unix 2 [ ACC ] STREAM LISTENING 382276 7741/EventHandler /ngfw/var/sf/run/EventHandler_SSEConnector.sock
unix 3 [ ] STREAM CONNECTED 378537 7741/EventHandler /ngfw/var/sf/run/EventHandler_SSEConnector.sock
```

SSE و CTR ةباوب ىلإ ةلسرمل تانايبلا نم ققحتلا

عم TCP لاصتا عاشنإ ةجاح ىلع عالطال نمآلا ةيامحل رادج زاهج نم ثادحألا لاسرل
SSE لخدم نيي هؤاشنإ متي مل لاصتا ىلع لاثم اذه <https://eventing-ingest.sse.itd.cisco.com>
نمآلا ةيامحل رادجو:

```
root@firepower:/ngfw/var/log/connector# lsof -i | grep conn
connector 60815 www 10u IPv4 3022789647 0t0 TCP localhost:8989 (LISTEN)
connector 60815 www 12u IPv4 110237499 0t0 TCP firepower.cisco.com:53426->ec2-100-25-93-234.compute-1.amazonaws.com
```

تالچسلا لصوملا يف

```
time="2020-04-13T14:34:02.88472046-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:connect] failed to connect to https://eventing-ingest.sse.itd.cisco.com:443"
time="2020-04-13T14:38:18.244707779-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:connect] failed to connect to https://eventing-ingest.sse.itd.cisco.com:443"
time="2020-04-13T14:42:42.564695622-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:connect] failed to connect to https://eventing-ingest.sse.itd.cisco.com:443"
time="2020-04-13T14:47:48.484762429-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:connect] failed to connect to https://eventing-ingest.sse.itd.cisco.com:443"
time="2020-04-13T14:52:38.404700083-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:connect] failed to connect to https://eventing-ingest.sse.itd.cisco.com:443"
```

 <https://eventing-ingest.sse.itd.cisco.com> ىلإ يمتنت 1x.x.246 و x.x.x.246 ةضورع مل IP نيوانع نأ ظحال :ةظحالم
ةكرحل حامسلا يه ةيصوتلا نإف ببسلا اذهلو ،ريغتت نأ بجي و <https://eventing-ingest.sse.itd.cisco.com>
IP نيوانع نم الدب URL ىلإ ادانتسا SSE ةباوب تانايبلا رورم.

لاصتا ىلع لاثم اذه SSE ةباوب ىلإ ثادحألا لاسرل متي نلف ،لاصتالا اذه عاشنإ متي مل اذا
SSE لخدمو نمآلا ةيامحل رادج نيي تباث

```
root@firepower:# lsof -i | grep conn
connector 13277 www 10u IPv4 26077573 0t0 TCP localhost:8989 (LISTEN)
connector 13277 www 19u IPv4 26077679 0t0 TCP x.x.x.200:56495->ec2-35-172-147-246.compute-1.amazonaws.com
```

نامأل ةباحس في مكحتل رصنع في (FTD) زاهل ليجست نكمي ال

رجأتسم لب لاصتا رفوت نم دكأتف، "نامأل ةباحس في مكحتل" في كزاهل ليجست رذعت اذا بسانمل CDO.

Cloud ددح، ةيامحل رادج ةرادا زكرم >Administration لى لقتنا، حيحصل ال URL ناو نع نم ققحتل Delivered FMC، كتشاش نم يولعل رسيأل بانجل في.

```
admin@MexAmpFTD:~$ nc -vz xxxxxxxx.app.us.cdo.cisco.com 443
Connection to xxxxxxxx.app.us.cdo.cisco.com 443 port [tcp/https] succeeded!
```

يلع لاثم اذه، 8305 ذفنملا حتف نم دكأتف، CDO ب لاصتال لكاشم هجاوت لازت ال تنك اذا لاصتا ةلكشم.

```
admin@AMP-DMZ-FPR:~$ sudo tail /ngfw/var/log/messages
Jan 25 18:48:56 AMP-DMZ-FPR SF-IMS[20448]: [1465] sftunneId:sf_peers [INFO] Peer xxxxxxxx.app.us.cdo.ci
Jan 25 18:48:56 AMP-DMZ-FPR SF-IMS[20448]: [1465] sftunneId:sf_ssl [INFO] Connect to xxxxxxxx.app.us.cd
Jan 25 18:48:56 AMP-DMZ-FPR SF-IMS[20448]: [1465] sftunneId:sf_ssl [INFO] Initiate connection using res
Jan 25 18:48:56 AMP-DMZ-FPR SF-IMS[20448]: [1465] sftunneId:sf_ssl [INFO] Initiate IPv6 type connection
Jan 25 18:48:56 AMP-DMZ-FPR SF-IMS[20448]: [1465] sftunneId:sf_ssl [INFO] Initiate IPv4 type connection
Jan 25 18:48:56 AMP-DMZ-FPR SF-IMS[20448]: [1465] sftunneId:sf_ssl [INFO] Initiate IPv4 connection from
Jan 25 18:48:56 AMP-DMZ-FPR SF-IMS[20448]: [1465] sftunneId:sf_ssl [INFO] Initiating IPv4 connection to
Jan 25 18:48:56 AMP-DMZ-FPR SF-IMS[20448]: [1465] sftunneId:sf_ssl [INFO] Wait to connect to 8305 (IPv4
Jan 25 18:48:56 AMP-DMZ-FPR SF-IMS[20448]: [1465] sftunneId:sf_ssl [INFO] Connect to x.x.x.51 failed on
```

ئطاخ SSX رجأتسم لى زاهل ليجست مت

كب صاخال FMC في لجسم SSX رجأتسم يا نم ققحتل كنكمي.

```
admin@fmc01:~$ curl localhost:8989/v1/contexts/default/tenant
```

```
{"registeredTenantInfo":{"companyId":"689xxxxx-eaxx-5bxx-b1xx-a7662axxxx","companyName":"XDR BETA - TA
```

SSX في ةزهأل ليجستل تاوطخل ذيفنت ةداعا لى جاتحت، حيحص ريغ SSX رجأتسم ناك اذا

ةبسانمل SSX ةسسؤمب طبترم ريغ CDO رجأتسم نكلو، احيحص SSX رجأتسم ناك اذا، لىصافتال هذه عم TAC ب لاصتال عاجل:

- SSX رجأتسم فرع م
- CDO رجأتسم فرع م

ةمچرتل هذه ل و ح

ةل آل ا ت ا ي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت م ل ا ع ل ا ا ح ن ا ع ي م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و ا م ك ة ق ي ق د ن و ك ت ن ل ة ل آل ا ة م چ ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب Cisco ي ل خ ت . ف ر ت ح م م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا