

ىلع Azure Entra في ةديقملا ةباوبلا نيوكت نمآلا ةيامحلا راج

تايوتحملا

[قمدملا](#)

[قيساسلا تابلطتلا](#)

[تابلطتلا](#)

[قمدختسلا تانوكملا](#)

[قيساسا تامولعم](#)

[يطيختلا مسرلا](#)

[Azure Entra و FTD و ةياهنلا ةطقن نيوكت ةديقملا ةباوبلا](#)

[نيوكتلا](#)

[ىلوالأ DNS و FMC نيوكت: ىلوالأ ةلخرملا](#)

[Cisco نم \(CSDAC\) ةيكيما نيوللا تامسلا لوصوم نيوكت: 1 ةوطخلا](#)

[FTD لخدم ةهجاول لمكلااب لهؤم لاجم مسالا ةكبش نيوكت لثمم عاش ناب مق: 2 ةوطخلا](#)

[DNS لچس نيوكت: 3 ةوطخلا](#)

[ماعلا خاتملا قيساسلا ةيكنبلا نيوكت: ةيكنبلا ةلخرملا](#)

[FMC ىللا ةيلخادلا CA ةداهش داريتسا: 1 ةوطخلا](#)

[قدصملا عجرملا عم ةمدخلا دوزم ةداهش عيقتوت: 2 ةوطخلا](#)

[FTD ىللا SP ةداهش ريشن: 3 ةوطخلا](#)

[Azure نيوكت: ةئلالاتلا ةلخرملا](#)

[SAML تاودأ ةعومجمل Entra Enterprise قيبطت عاشنا: 1 ةوطخلا](#)

[ارتنالا فرعم قيبطت تاليجست نيوكت: 2 ةوطخلا](#)

[لىچستلا Microsoft Graph ل \(API\) تاقيبطتلا ةجمرب ةهجاو تانودأ نيوكت: 3 ةوطخلا](#)

[\(EH\) شادجالا عزم مسالا ةحاسم نيوكت: 4 ةوطخلا](#)

[شادجالا عزم مسالا ةحاسم يف اهؤاشنا وأ كرتشملا لوصولا جهن رايخلا: 5 ةوطخلا](#)

[مسالا ةحاسم نم اهتظالمو \(SAS\) كرتشملا لوصولا عيقتوت تامولعم عيقتوت: 6 ةوطخلا](#)

[EH](#)

[شادجالا عزم مسالا ةحاسم لخد شادجالا عزم لىثم عاشنا: 7 ةوطخلا](#)

[شادجالا عزم مسالا ةحاسم لخد شادجالا عزم لىثملا ةيكنبلا ةعومجمل عاشنا: 8 ةوطخلا](#)

[ةعومجمل ميقلا نم ققحتلا: 9 ةوطخلا](#)

[شادجالا زكرم ىللا ارتنالا فرعم قيبطت لچس قفد نيوكت: 10 ةوطخلا](#)

[FMC/FTD و Azure ل ةطشنلا ةقداصملا نيوكت جم: 4 ةوطخلا](#)

[FMC جللا عم مادتستاب Azure SAML/Entra فرعم قاطن نيوكت: 1 ةوطخلا](#)

[Azure قيبطت يف FMC ل ةنوكملا SAML SP فيرعت تانايي ذيفنت: 2 ةوطخلا](#)

[Enterprise](#)

[\(عبات\) FMC جللا عم مادتستاب Azure SAML/Entra فرعم قاطن نيوكت: 3 ةوطخلا](#)

[مولىزنت مت نيوكتلا نيومدختسلا نم ققحتلا: 4 ةوطخلا](#)

[FMC يف تاسايسلا نيوكت: 5 ةوطخلا](#)

[ريفشنتلا كف جهن نيوكت: 1 ةوطخلا](#)

[ريفشنتلا كف ةسايس دعاوق نيوكت: 2 ةوطخلا](#)

[ةيوهلا ةسايس عاشنا: 3 ةوطخلا](#)

[ةيوهلا جهن دعاوق نيوكت: 4 ةوطخلا](#)

[لوصولا يف مكحتلا ةسايس نيوكت: 5 ةوطخلا](#)

[Cisco نم ةنوكملا ةيامحلا راج ةهجاو ىللا تانايي نيوكتلا ريشن: 6 ةوطخلا](#)

[قجصللا نم ققحتلا](#)

[قيموسرلا مدختسملا قهجاو](#)

[CLI](#)

[امجالص او عا طخألا فاشكتسا](#)

[ديقملا قباوبلا عا طخألا حيحصت](#)

[مدختسملا قيوه غيرفت](#)

[قلمتحملا اي اضقلا](#)

[رسألا يف دوجوملا لخدملل قفورعم ريغ تاداهش قطللس](#)

[مداخلا اىلع روثعلا متي مل قديقملا قباوبلا](#)

[قلىص تاذ تامولعم](#)

قم دقمل

قديقملا قباوبلا عم مادختسالا Microsoft Azure Entra فرعم نيوكت دنتسملا اذه فصق Cisco نم نمآلا قيامحل رادج ىلع (قطنللا ققداصل)

قيساسالا تابلطتملا

تابلطتملا

قيلاللا تاعوضوملا قفرعمب Cisco قيصوت

- (SAML) نامالا ديكأت زيمرت قغل
- Microsoft Azure
- Cisco نم (FMC) نمآلا قيامحل رادج قراذ زكرم
- Cisco نم (FTD) قيامحل رادج ديدعت نع نمآلا عافدل

ثادخال زكرم عاشنال Azure قف قرفوتمل قساقلال ريعستلا ققبط كيدل نوكي نا بقق منيكم متي ذلا "قكذلا صيخرتللا" مادختساب قزهأالا طيشنت بقق، كلذىل قفاضللابو ريدصتللا قطساوب اهي ق مكحتللا متي قتللا قئاظولا عم

قم دختسملا تانوكمل

قيلاللا قيدامل تانوكمل او جماربلا تارادصلال دنتسملا اذه قف قذراوال تامولعمللا دنتست

- Cisco Secure FTD، رادصلالا 10.0
- Cisco Secure FMC، رادصلالا 10.0

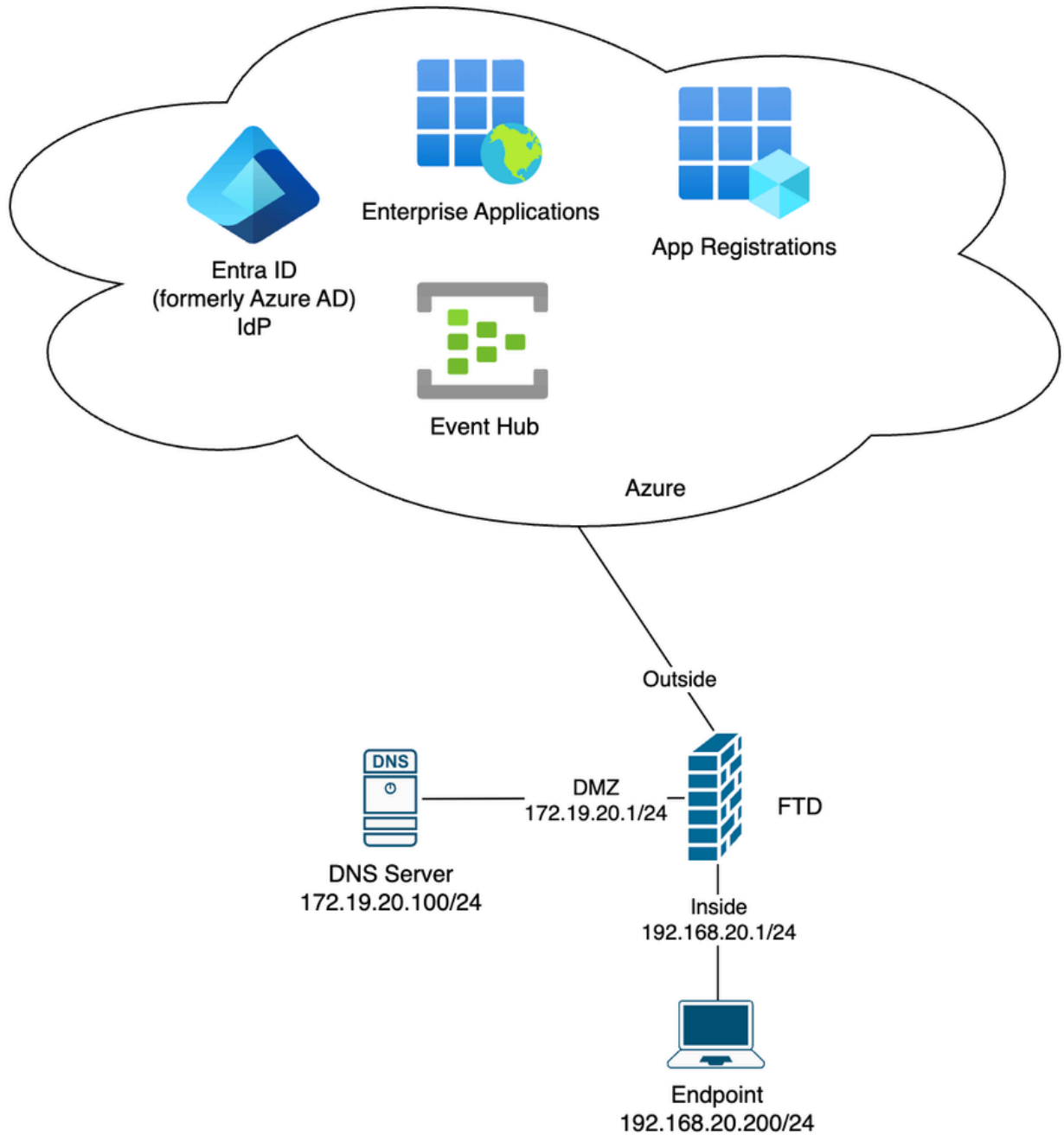
صاخ ةي لم عم ةئي ب ي ف ةدوجوم ل ةزهجال نم دنتسمل اذه ي ف ةدراول تامولعمل عاشنإ مت
تناك اذا . (يضا رتفا) حوسم م نيوكتب دنتسمل اذه ي ف ةمدختسمل ةزهجال عي مج تادب
رمأ يأل لم تحمل ريثأتلل كمهف نم دكأتف ، ليغشتل دي ق ك تكبش

ةيساسأ تامولعم

(IP) تنرتنإل لوكونورب ىلع ةمئاقلا ةيديلقنل نامأل ىنب هي ف عراضت يذلا تقولا ي ف
نمأل ةيامل رادجل ةطشنل ةقداصلم رفوت ، نيجهل او ةيكيما ني دل لمعل تائي ب ةبك او مل
Microsoft فرعم نم ةدافتسال لال خ نم . ةي وه ل ىلع زكتر ي ا يوق الح SAML جم د عم Cisco نم
دعاوق زواجت ةيناكمإ ني لوؤسمل ل نيوكتل اذه حيتي ، يزكرم ةي وه رفومك (Azure AD) Entra
ةي وه ىلإ ادانتسا تايوتسمل ددعت لموصول ي ف مكحتل صرفو ةتباثل ةكبشل
ىلع جم دل اذه لمعي . ةبلقنم ل ةكبشل نيوانع نم الدب اهنم ققحتل مت ي تل مدختسمل
ةقداصلم او (SSO) ةمات ةسالسب ي داخال لوخل دل ليحست لال خ نم مدختسمل ةبرجت لي هست
ةيؤر ةيناكمإ ىلع ظفاحي دحوم نامأ عضو رفوت نامض عم ، (MFA) ةيمازلإ لم اوعل ةددعت
قياطن يأل ل اجاتحت ال ةكبش ربع تاسايسال ذافن او ةقئاف

ي طي طختل مسرل

Azure Entra و FTD و ةي اهنل ةطقن ني ب ةديقم ل ةباوبل



Entra و Azure EndPoint نې ې ډي قم لال ې او ې لال

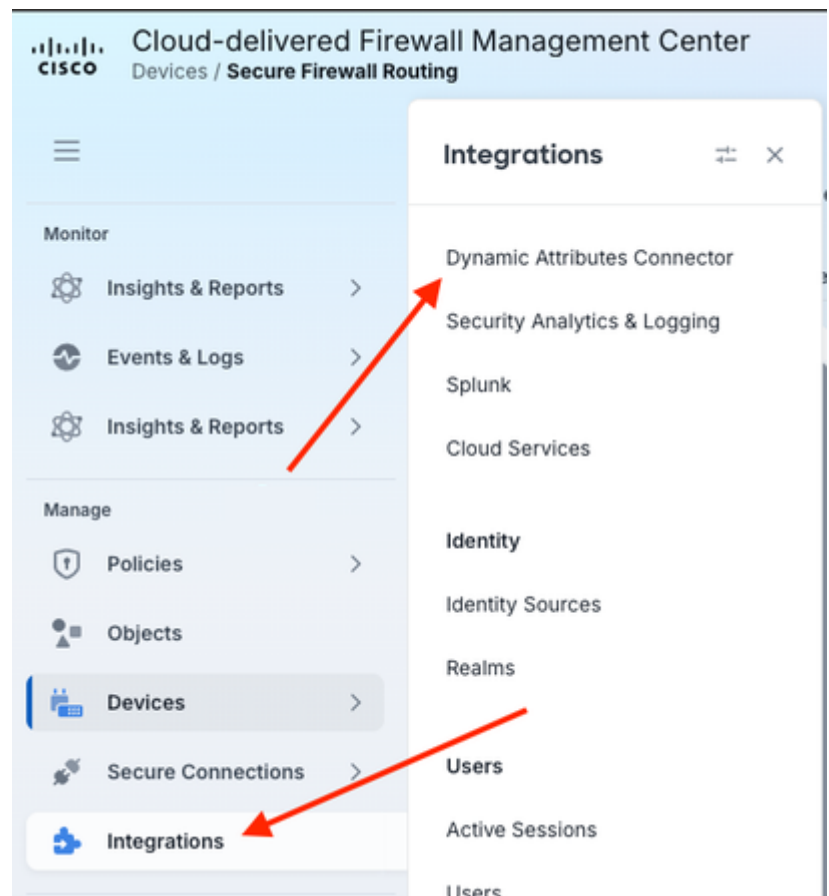
نې وک تال

ې ل و ال DNS و FMC نې وک ت : ې ل و ال ې ل حر م لال

ې با ح س لال ر ب ع ه لې ص و ت م ت ې ذ لال ې ا م ح لال ر ا د ج ې ر ا د ا ز ک ر م ر ب ت خ م لال ا ذ ه م د خ ت سې : ې ط ح لال م ې ل ح ل م لال FMC ل ې س ن لال ا ې س ف ن ت ا و ط خ لال ې ق ب ت ، ک ل ذ ع م و : (CDfmc)

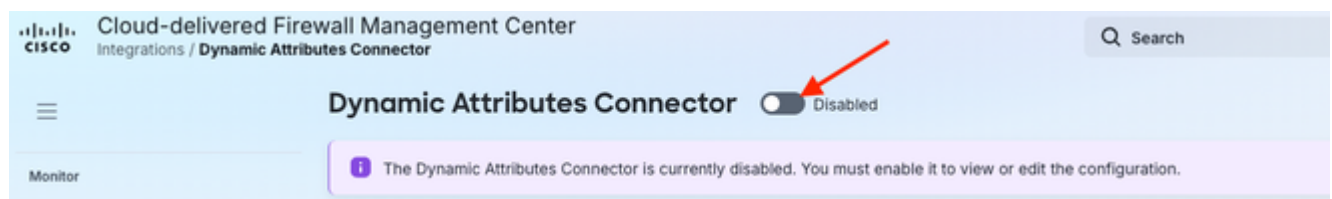
Cisco نم (CSDAC) ةيكيما نيدلا تامسلا لصوم نيكمت 1: ةوطخلا

ةيكيما نيدلا تامسلا لصوم > لمكتلا تاي لمع رتخأ 1)



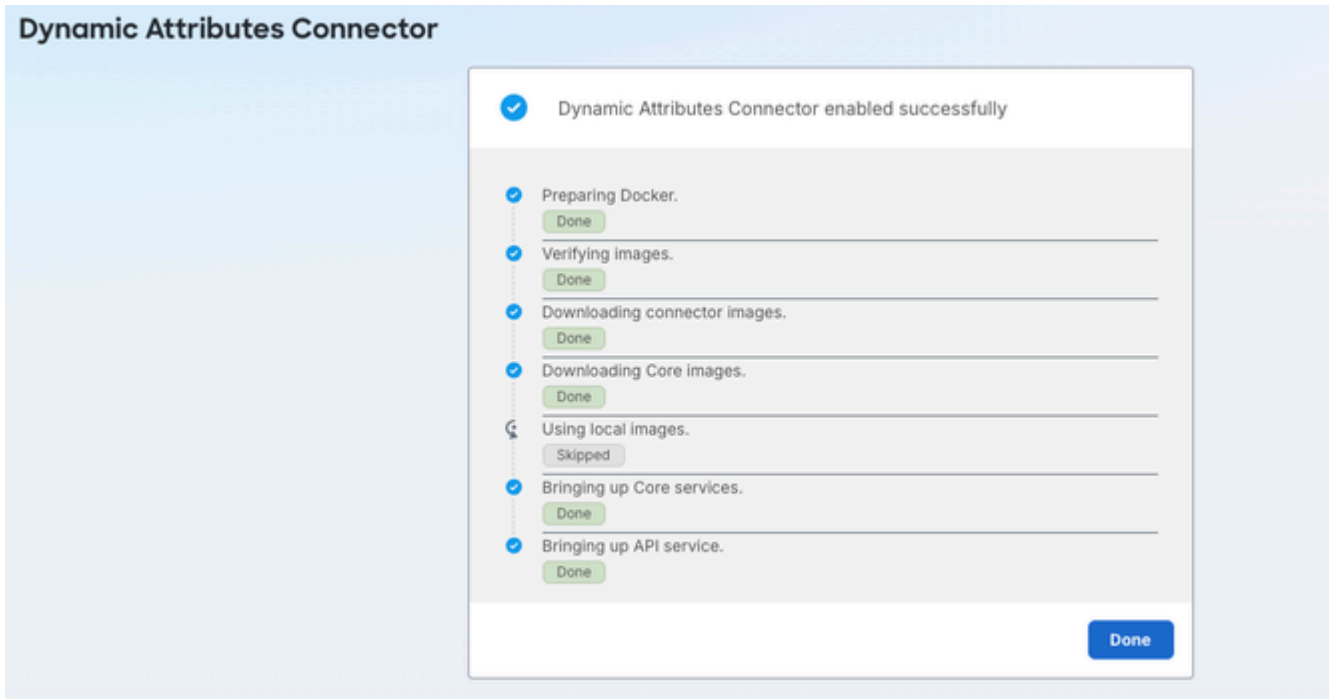
لمكتلا تاي لمع ةيكيما نيدلا تامسلا لصوم رتخأ

CSDAC. نيكمتل لطم ةلسلسل رواجم لكحتلا رصنع قوف رقنا 2)



Cisco نم ةيكيما نيدلا تامسلا لصوم نيكمت

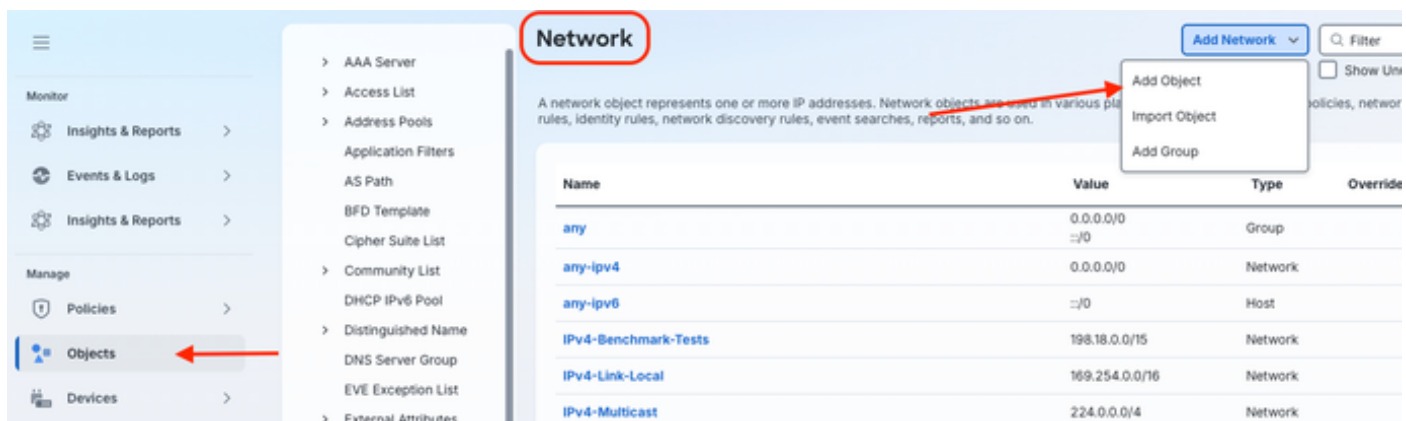
CSDAC. نيكمت لامتك درجمب مت قوف رقنا ج)



Cisco نم ةيكي ماني دل تامس لل لصوم ة لاج ني كمت

FTD لخدم ةه جاول لم اكلا ب لهؤم لاجم مسا ةكبش نئاك لثمم عاشناب مق 2: ةوطخل

نئاك ةفاضل > ةكبش ةفاضل > تانئاك رتخأ 1)



يديج لم اكلا ب لهؤم لاجم مسا ةكبش نئاك عاشناب

لم اكلا ب لهؤم لاجم مسا ماديختساب هنيوكت مت يذلا ةكبش لل نئاك ةي مستب مق 2)
يلدابتل رزلا قوف رقلاب FQDN عونك ةكبش لل نئاك نييعتب مقو، FQDN لخدأ (FQDN).
ظفح قوف رقنا .بس انملا

②

active_auth_fqdn

○ Host

☐ Range

○ Network

 FQDN

ftd-inside.example.com

Note:

You can use FQDN network objects in access, prefilter and translated destination in NAT rules only.

Resolve within IPv4 and IPv6

☐ Allow Overrides

Cancel

Save

FQDN ةكېش نىاك تاريغتم نيوكت

DNS لجس نيوكت : 3 ةوطخلا

ةصاخلا قئاثولا عجار؛ Windows Server 2025 لي غشتلا ماضن مدختسي انه نيبملا لاثملا 1)
ةعاجلا بسح ددحملا مسالا عق دماخپ



لح ىل ع ارداق ع طشننللا ع قداصملا ذى فنن ب موقى ي ذلا لىمعل نوكتى نأ بجى :ع ظحالما
اذه A DNS لجس

ماعلا حاتفم لل عىساسأللا عىنبلل نىوكت :عىنائللا علحرملا

نىوكتل (PKI) ماعلا حاتفم لل عىساسأللا عىنبلللا (CA) لىلخاد عداش عجرم مادختسا نكمى
لىلخادللا ماعلا CA حاتفم لىمحت FTD و Cisco FMC نم لك بلطتى .ع طشننللا ع قداصملا
ع رورضللا SSL ضارتنلا تاىلمع ذى فننل لىلخاد CA نئاكل هب نرتقملا صاغللا حاتفملاو
ي ذلا لىمعللا ضرعتسم لىلخادللا CA ب قوثلل بجى ،كلذى لىل عفاضللاب .اهرىفش ت كفو
ع فىكى نم ققحتلل لىمعللا ضرعتسم قئاثو عجار .هنم ع طشننللا ع قداصملا عارجل مئى
عداشللا فى قئى ضرعتسملا نأ دىكأت

FMC لىل عىلخادللا CA عداش دارىتسا :1 عوطخللا

قدصم عجرم دارىتسا لىل ع رقنا .عىلخادللا (CAs) لوصوللا تادصم > PKI > تانئاكللا رتخأ 1)



FMC لىل ع رشابم لىلخادللا قدصملا عجرملا عاشن نكمى امك :ع ظحالما

Import Internal Certificate Authority

Name:

Certificate Data or, choose a file:

-----BEGIN CERTIFICATE-----

-----END PRIVATE KEY-----

Key or, choose a file:

-----BEGIN CERTIFICATE-----

-----END PRIVATE KEY-----

☒ Encrypted, and the password is:



لقحلل ميقي طغي يذلل ضيبألل غارفلل رهظي ،دنتسملل اذه ىوتحم نمض :ةظحالل ميقلل ساكعنا متي .دنتسملل اذهل رشن لكك دوصقم وهو روصلل ي ف ةفلتخملل .نيوكتلل ةيلمع ءانثأ كئيبلىل ةيلعللل

قدصملل عجرملل عم ةمدخلل دوزم ةداهش عيقتوت :2 ةوطخلل

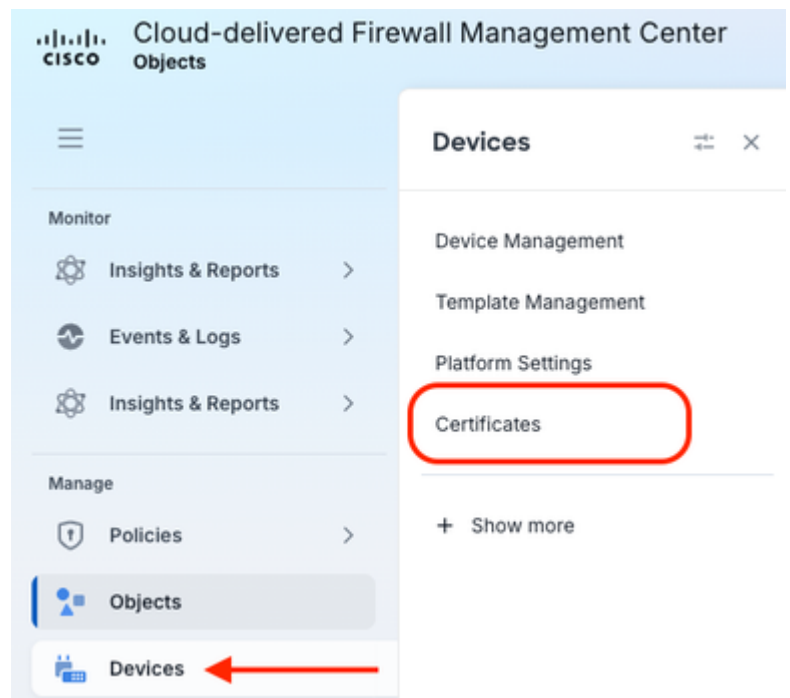
اهتداعلو (CA) هب قوئوم قدصم عجرم لبق نم (SP) ةمدخلل دوزم ةداهش عيقتوت بجي 1) (p12). PKCS#12 قيسنتب



عجرملل نأ وه ديحولل هيبنتلل .ايلخاد قدصملل عجرملل اذه عيقتوت نكمي :ةظحالل .للمعلل زاهج ةطساوب هب اقوئوم نوكلل نأ بجي يلخادلل قدصملل

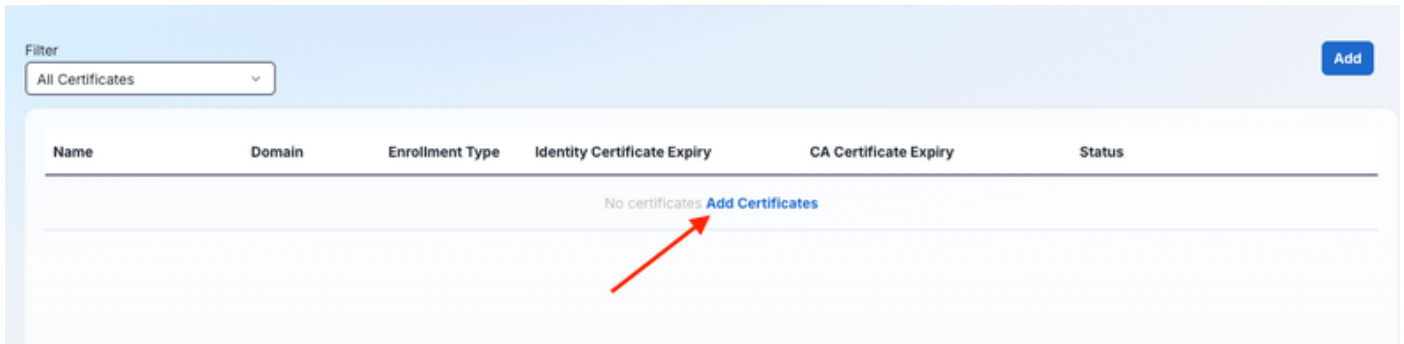
FTD ىلإ SP ةداهش رشن :3 ةوطخلل

تاداهش > ةزهجأ رتخأ 1)



تاداهشللو ةزهجألل ىلإ لقتنا

تاداهش ةفاضل رقنا 2)



ةديج زاهج ةداهش ةفاضإ

رقنأ م ث ،ةطشننلا ةقداصملا ذيفنتب موقت يتلا ةلدسنملا ةمئاقلا نم زاهجلا ىلع رقنأ 3)
ديج ةداهش ليجست ءاشنإل + ةنوقيأ ىلع

ديج ةداهش ليجست فضأو FTD ددح

فلم رتخأ ،ليجستلا عون ةلدسنملا ةمئاقلا نمو ،ةداهشلا ليجست ةيمستب مق 4)
PKCS12.

Add Certificate Enrollment

Name*
FTD-SP-Cert

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type: SCEP

Enrollment URL:*

Challenge Password:

Confirm Password:

Retry Period:

Retry Count: 10 (Range 0-100)

Fingerprint: Ex: e6f7d542 e355586c a758e7...

Validation Usage: ☒ IPsec Client ☒ SSL Client ☐ SSL Server

Cancel Save

عونلاو ةداهشلا ليجست تادادع

رورملا ةرابع لخدأو PKCS12 فلم ضارعتسا ىلع رقنلاب PKCS#12 فلم داري تساب مق (5)
ظفح قوف رقنا . ةبولطملا

Add Certificate Enrollment

?

Name*

Description

CA Information
Certificate Parameters
Key
Revocation

Enrollment Type:

PKCS12 File
▼

PKCS12 File*:

SP.p12

Browse PKCS12 File

Passphrase*:

.....

Validation Usage:

☒ IPsec Client
 ☒ SSL Client
 ☐ SSL Server

☐ Skip Check for CA flag in basic constraints of the CA Certificate

☒ Allow Overrides

> Override (0)

Cancel
Save

PKCS12 فلم داري ت سا و ضا ر ع ت سا

ة ف ا ض ا ق و ف ر ق ن ا و ة ح ي ح ص ل ي ج س ت ل ا ل ي ص ا ف ت ن ا ن م د ك ا ت 6)

Add New Certificate

?

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*:

FTD
▼

Certificate Enrollment*:

FTD-SP-Cert

▼
+

Certificate Enrollment Details:

Name:	FTD-SP-Cert
Enrollment Type:	PKCS12 file
Enrollment URL:	N/A

Cancel
Add

ة د ا ه ش ل ل ي ج س ت ل ي ص ا ف ت د ي ك ا ت

7) مدقتا ديقتا داريتسا سالسا كعي

FTD				
FTD-SP-Cert	Global	PKCS12 file	In progress	  

فرع الم زمروقوف رقنلاب SP ةداهش تامولعم نم ققحتللكمي ،داريتسالامتكك اءرءمب .اهنيوكك مك يكل ةداهشلاب صااال

Filter

All Certificates

Add

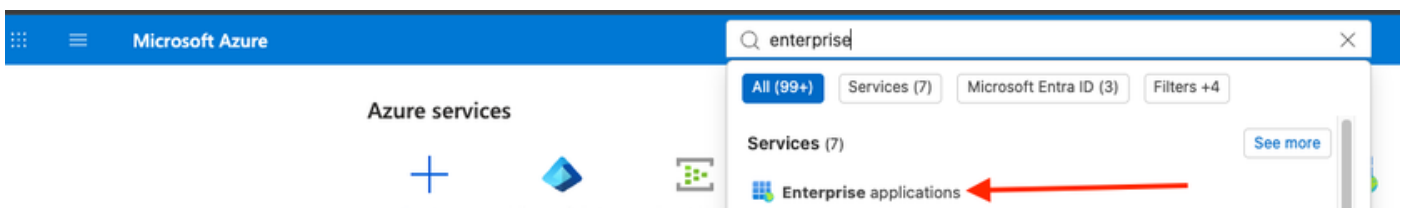
Name	Domain	Enrollment Type	Identity Certificate Expiry	CA Certificate Expiry	Status
FTD					
FTD-SP-Cert	Global	PKCS12 file	Dec 18, 2028	Sep 12, 2036	CA ID

مدقتال دي ق ةداهشال داري تسال

Azure نيوكت :ةثلاثال ةلحرمل

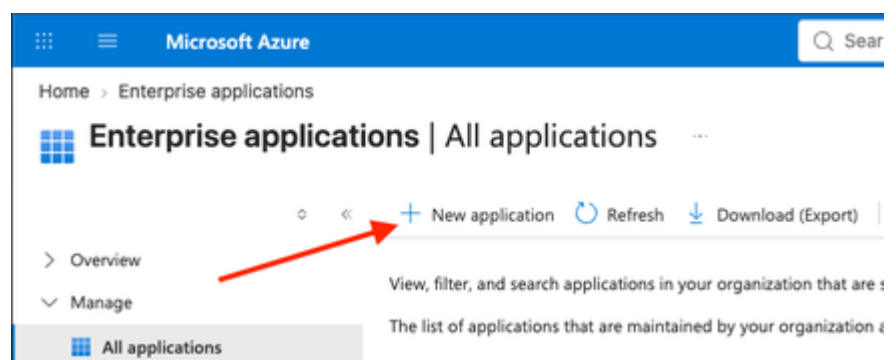
SAML تاولدأ ةوممءل Entra Enterprise قيبطت ءاشنإ: 1 ةوطءلا

1) اهقوق ورقناو تاسسؤملا تاقيبطت نع ثحبا



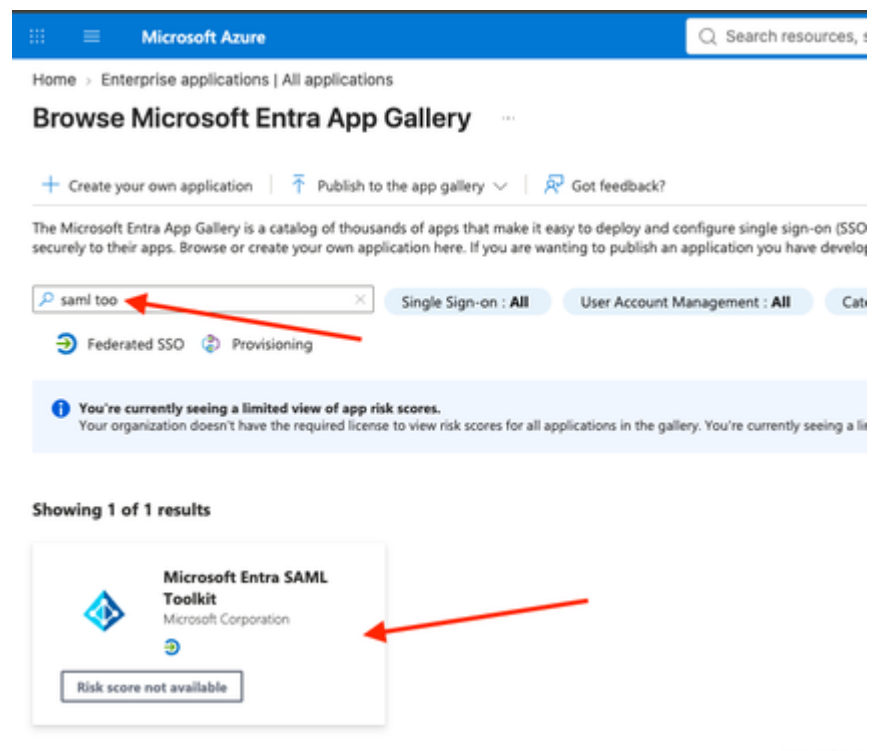
ةسسؤملا تاقيبطت ىلإ لوصولاو ثحبلا

2) ديدج قيبطت + قوف رقنا



ةسسؤملا تاقيبطت نمض اديج اقبطت ددح

3) هل ةرغصملا ةروصلال قوف رقن او Microsoft Entra SAML Toolkit نع شحبا



Microsoft Entra SAML Toolkit دي دحتو شحب

4) عاشن ا قوف رقن او Microsoft Entra SAML Toolkit Enterprise قيبطتل مسا صيصختب مق (ةوطخ Microsoft Entra SAML Toolkit اودا ةعومجم لماكتل سوردمل انمىلعت ارقى Microsoft: نم عجرم) (ةوطخب).

Microsoft Entra SAML Toolkit

Get feedback?

Logo  Name *

Publisher Provisioning

Single Sign-On Mode
SAML-based Sign-on
Linked Sign-on

URL

[Read our step-by-step Microsoft Entra SAML Toolkit integration tutorial](#)

This is the sample SAML app which customers can use to test the SAML single sign-on integration with Microsoft Entra ID.

Create

SAML تاوداً ةومجم قيبطتل مسا نييعت

قيبطت الى ةنيعم تاومجمو ني ددحم ني مدختسم نييعتب مق ، ةماعلا ةرطنلا ةحفص في 5) في اوضع (Captive-Portal-user) رابخال باسح دعي ، لاثملا اذه في SAML Toolkit Enterprise. ةومجم Active-Auth-lab.

 **1. Assign users and groups**

Provide specific users and groups access to the applications

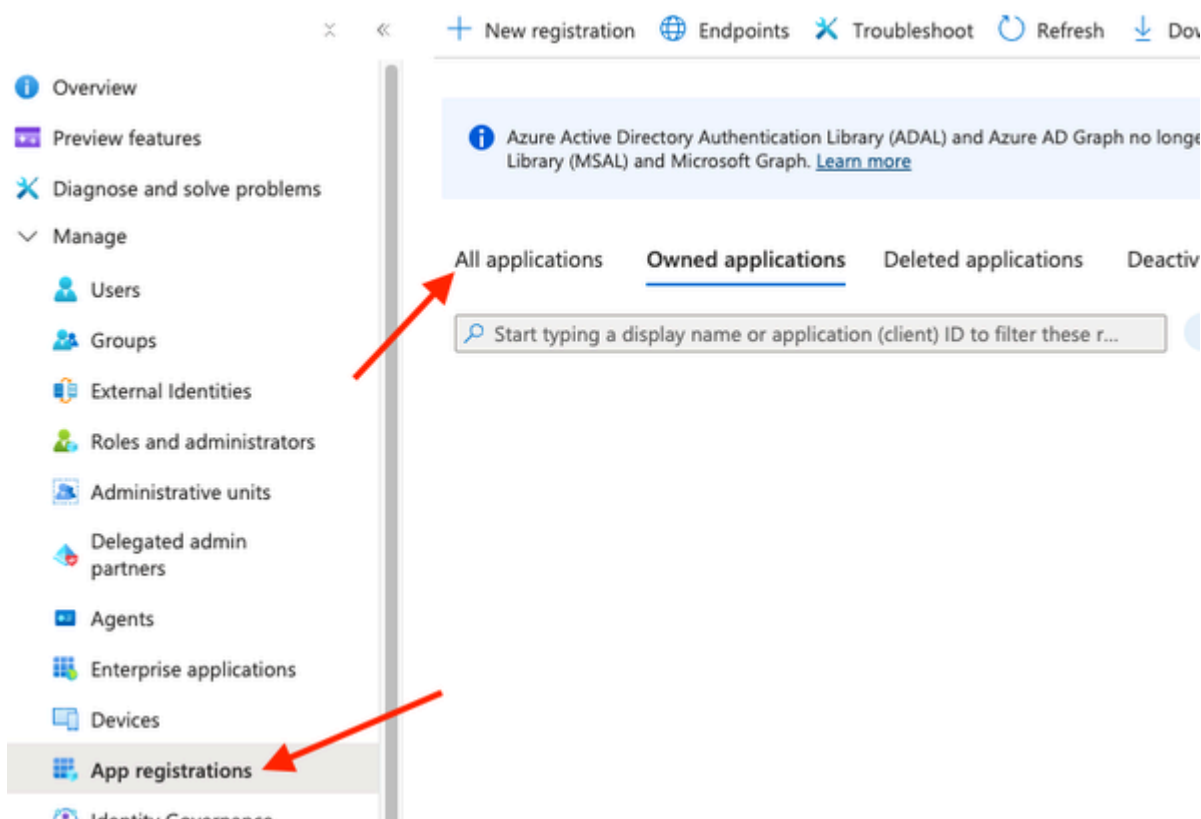
[Assign users and groups](#)

قيبطتل تاومجمو ني مدختسم نييعت

ةخالل تاوطلخا في اذه ةسسؤملا قيبطت نيوكت رمتسي 6)

ارتداد فرع قيبطت تاليجست نيوك 2: ةوطخل

قيبطت تاليجست رتخأ، ىرسى لال قننتال ةمئاق نمو Entra فرع ىل فلخلل لقتنا 1)
ةسسؤم لال قيبطت لىطعم لال مسالال نع ثحابو تاليجستال عىمجة ةيفصت لماع قوف رقال
بسانم لال قيبطتال قوف رقال



تاليجستال عىمجة و تاليجستال تاليجست ىل لقتنا

ةسسؤم لال تاليجست لىطعم لال مسالال ةمئاق و ةمئاق لىطعم لال مسالال عىمجة 2)

تحت ميقال عىمجة و ةمئاق لىطعم لال مسالال ةمئاق لىطعم لال مسالال عىمجة
ةمئاق ةمئاق لىطعم لال مسالال ةمئاق لىطعم لال مسالال عىمجة

- ضرع لال مسالال
- (للمعم لال قيبطتال فرع
- (رجأتسم لال لىلدل فرع

Captive-Auth-SAML

Search

Deactivate Delete Endpoints

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Authentication (Preview)

Certificates & secrets

Got a second? We would love your feedback on Microsoft identity platform (previous)

Essentials

Display name : [Captive-Auth-SAML](#)

Application (client) ID :

Object ID :

Directory (tenant) ID :

Supported account types : [My organization only](#)

ليدل الفرع موقيت بطال او ضرع الميق عيحت

ي.رس يبعشت طبار وأداهش فاضا إلى رونا 3)

Captive-Auth-SAML

Search

Deactivate Delete Endpoints

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Authentication (Preview)

Certificates & secrets

Got a second? We would love your feedback on Microsoft identity platform (previous Azure AD for developer). →

Essentials

Display name : [Captive-Auth-SAML](#)

Application (client) ID :

Object ID :

Directory (tenant) ID :

Supported account types : [My organization only](#)

Client credentials : [Add a certificate or secret](#)

Redirect URIs : [1 web, 0 spa, 0 public client](#)

Application ID URI : [Add an Application ID URI](#)

Managed application in : [Captive-Auth-SAML](#)

State : [Activated](#)

ي.رس يبعشت طابرا وأداهش فاضا

دي.دج ليمع رس + قوف رونا 4)

Captive-Auth-SAML | Certificates & secrets

Search

Got feedback?

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Authentication (Preview)

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable (scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) Client secrets (0) Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
No client secrets have been created for this application.			

دي.دج ليمع رس فاضا

(Add) فاضا قوف رونا. ةرورضال بسح ةيصالصا اءاتنا طبضو رسلل فصوري فوت 5)

Add a client secret

Description: **saml-secret**

Expires: Recommended: 180 days (6 months)

Add **Cancel**

ليمعل رسل فصول ري فوت

6) رسال خسننا

ةظفاحل الى ةخوسنملا ةيرسللا ةميقللا ظحال :ماه

Captive-Auth-SAML | Certificates & secrets

Search: Got feedback?

Overview
Quickstart
Integration assistant
Diagnose and solve problems
Manage
Branding & properties
Authentication (Preview)
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (1)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

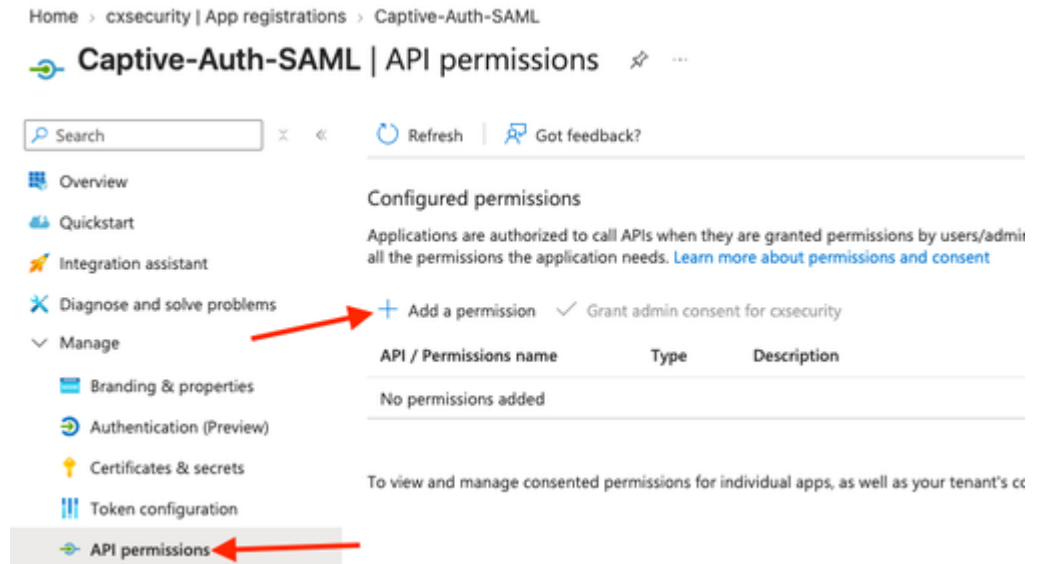
Description	Expires	Value	Secret ID
saml-secret	3/14/2027		

ليمعلل ةيرسللا ةميقللا خسن

ليجستل Microsoft Graph ل (API) تاقيبطتلا ةجررب ةهجاو تانودأ نيوك ت. 3 ةوطخل

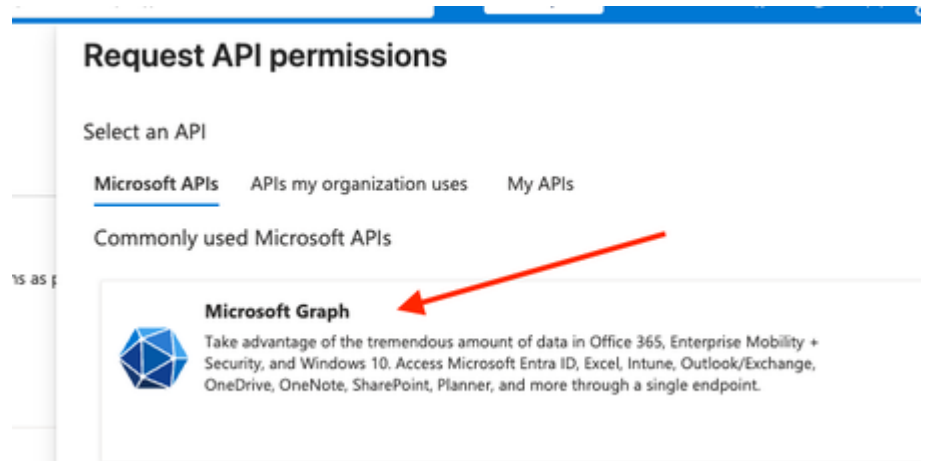
قېبىتىل

ەفاىز + قوف رىنا م، رىسالى لىقنىلى ەمئاق نى تاقىبىتىلى ەجرىب ەجاو تانودا رىخ (1) نى.



تاقىبىتىلى ەجرىب ەجاو تانودا نىوكىت

Microsoft Graph تاقىبىتىلى ەجرىب ەجاو قوف رىنا (2)



Microsoft Graph تاقىبىتىلى ەجرىب ەجاو دىدەت

تانودا ەفاىز قوف رىنا م، ەعارقىلى. صوفىلى مدخستىلى تانودا حنىم (3)

Request API permissions

[← All APIs](#)

 Microsoft Graph
<https://graph.microsoft.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

Permission	Admin consent required
> AgentIdUser	
> IdentityRiskyUser	
▼ User (1)	
☒ User.Read ⓘ Sign in and read user profile	No
☐ User.Read.All ⓘ Read all users' full profiles	Yes
☐ User.ReadBasic.All ⓘ Read all users' basic profiles	No

[Add permissions](#) [Discard](#)

مدخست سمل لة ضوفم لة عارق لة تانوذأ حنم

(رايتخال لة نأخ ددح) قيبطت لة تانوذأل User.Read.All حنم 4)

Request API permissions



< All APIs



Microsoft Graph

<https://graph.microsoft.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Permission	Admin consent required
User.Read.All	
IdentityRiskyUser	
User (1)	
☒ User.Read.All ⓘ Read all users' full profiles	Yes

تانوڈال ءفاك ءءارق قيبطتلل حنم

ءءارقلا تانوڈا حنمل راي تخالا ءناخ هذه ددحو (ءومجمل) Group.Read.All راي تخالا ءناخ نع شحبا 5) نودا ءفاضا قوف رقنا. اضيا ءومجملل

Permission	Admin consent required
Group.Read.All	
Group (1)	
☒ Group.Read.All ⓘ Read all groups	Yes

[Add permissions](#) [Discard](#)

تاقيبطتلل ءمرب ءءاو تانوڈا ظفح

اهل ءيرادلل ءقفاومل حنم او، اهنويوك مت يتلل تانوڈال قفاوت نم دكات 6)

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission

✓ Grant admin consent for

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (3)				
Group.Read.All	Application	Read all groups	Yes	⚠ Not granted for ***
User.Read	Delegated	Sign in and read user profile	No	***
User.Read.All	Application	Read all users' full profiles	Yes	⚠ Not granted for ***

تاندؤالل ةق فاولملا حنم

ل.وؤسملا ةق فاولملا حنم درجمب جتانلا ضرع متي 7)

+ Add a permission

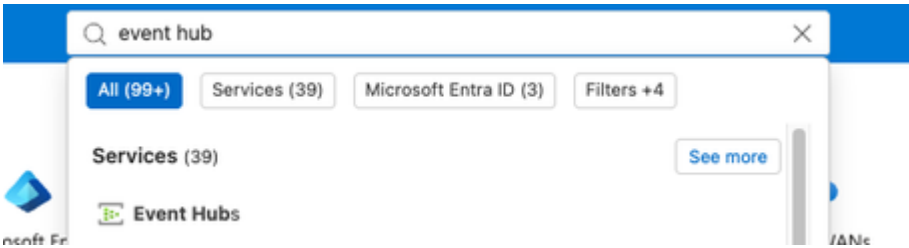
✓ Grant admin consent for

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (3)				
Group.Read.All	Application	Read all groups	Yes	✔ Granted for ***
User.Read	Delegated	Sign in and read user profile	No	✔ Granted for ***
User.Read.All	Application	Read all users' full profiles	Yes	✔ Granted for ***

ةق فاولملا ج اءلال حنم م

(EH) ءااءالا عزوم مسا ةحاسم نيوكا : 4 ةوطءلا

اهاقوف رقناو ءااءالا زكارم نع ءءبا 1)



ءءبلا ءااءأ عزوم نيوكا

EH ةءءء مسا ةحاسم عاشنا 2)



No event hubs namespaces to display

An Event Hubs namespace is a management container for event hubs which provides DNS-integrated network endpoints and a range of access control and network integration management.



[Learn more about Event Hubs](#)

شادحأل عزوم مسا ةحاسم عاشنإ

EH. مسا ةحاسم نيوكتب مق 3)



ريعتستال ةقبط عنمت. ىلعأ وأ ةيسايقلا ريعستال ةقبط رايتخإ بجي: ةظحالم
قاطنل مادختسا ةيساسأل

ةيلباقو ةمدقتمل تادادعلل ميعيقتل نم ديزم ىلع لوصحلل [Azure](#) شادحأ زكرم قئاثو عجار
ةنيعم تاجايتحال اقفو قيبتل

عاشنإ + ةعجارم قوف رقنا



Create Namespace

Event Hubs

[Basics](#) [Advanced](#) [Networking](#) [Tags](#) [Review + create](#)

Project Details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Resource group *

[Create new](#)

Instance Details

Enter required settings for this namespace, including a price tier and configuring the number of units (capacity).

Namespace name * ☒ .servicebus.windows.net

Region * ☒
i The region selected supports Availability zones. Your namespace will have Availability Zones enabled. [Learn more](#).

Pricing tier * ☒
[Browse the available plans and their features](#)

Throughput Units *

Enable Auto-inflate ☐

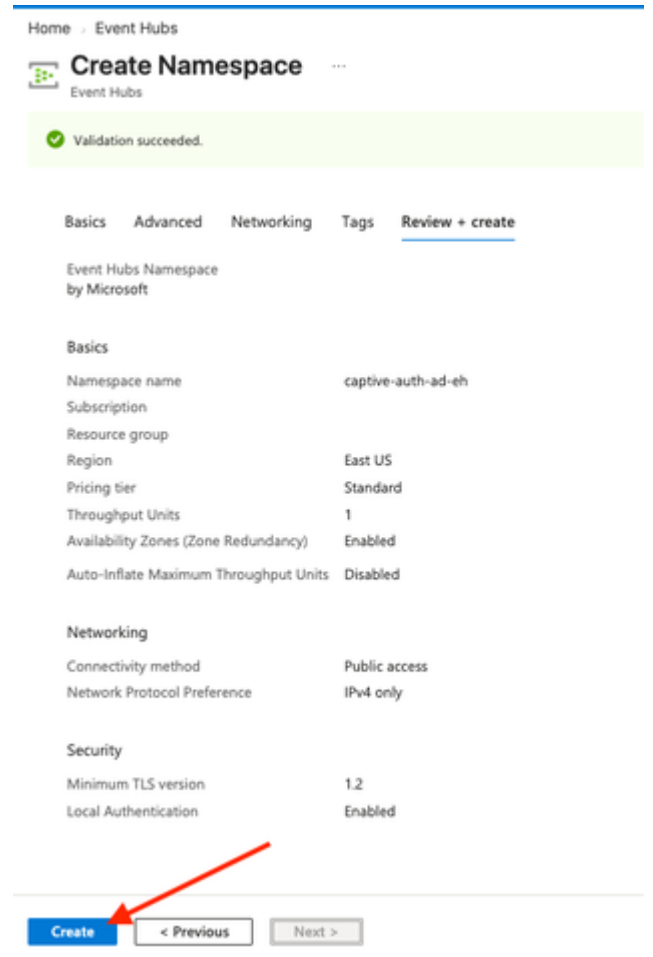
[Review + create](#)

< Previous

Next: Advanced >

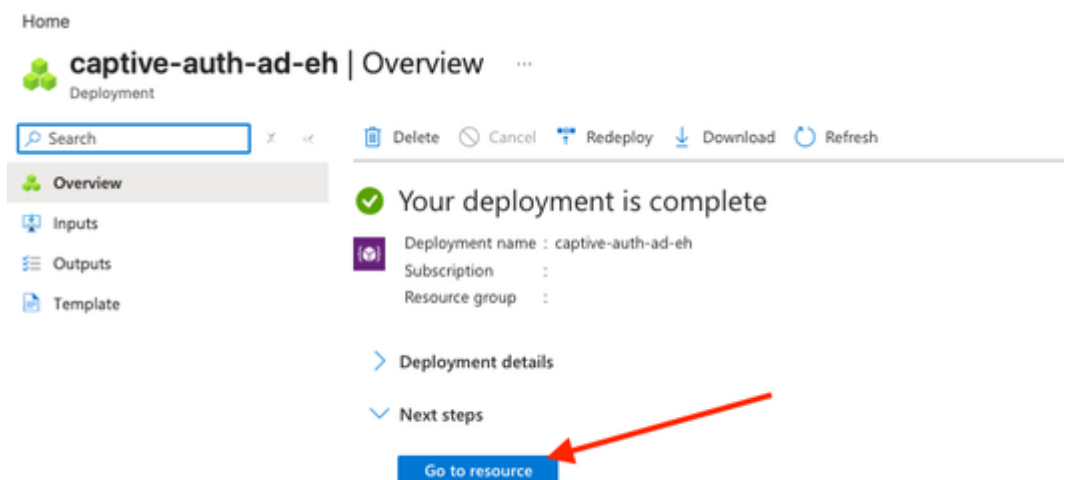
شادأل عزوم مسآةحاسم تادادع| نيوكت

ءاشن| قوف رقنا،ةحصلال نم ققحتال حاجن درجم ب 4)



شادحأل عزوم مسا ةحاسم رشن عاشنإ

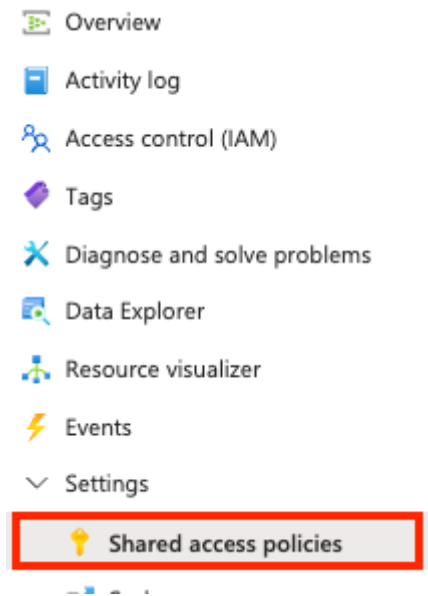
دروم إلإ لاقتنا قوف رقنا مث ،رشنلإ لامتك نم دكأت 5)



شادحأل عزوم مسا ةحاسم دروم إلإ لاقتناإلإ

شادحأل عزوم مسا ةحاسم يف اهؤاشنإ وأ كرتشم لوصولا جهن رايخإ: 5 ةوطخلا

كترشم لوصول تاسايس > تادادعإ رتخأ، یرسې لال قننتال ةمئاق نم 1)



كترشم لوصول تاسايس ىل ل قننتا

ف "عاشنإ قوف رقنا. ةرادا رایتخالال ةناخ ددحو، ديدجلال جهنللا مسا لخدأو ةفاضإ + قوف رقنا 2)
ةسايس ةفاضإ ةمئاق ةحول لفسأ



ديدج كترشم لوصول جهن ةفاضإ



كترشم لوصول جهن عاشنإ

EH مسا ةحاسم نم اهتظالمو (SAS) كترشم لوصول عي قوت تامولعم عي مجت: 6 ةوطخلال

ةحولللا ف EH SAS ةسايس رهظت؛ ديدجلال كترشم لوصول ةسايس قوف رقنا 1)

نمي لي إلية بنال

[Regenerate primary key](#) [Regenerate secondary key](#) [Delete](#)

Event Hubs access control with Shared Access Signatures [Learn more](#)

Claims

☒ Manage

☒ Send

☒ Listen

Primary key

Secondary key

Primary connection string

Secondary connection string

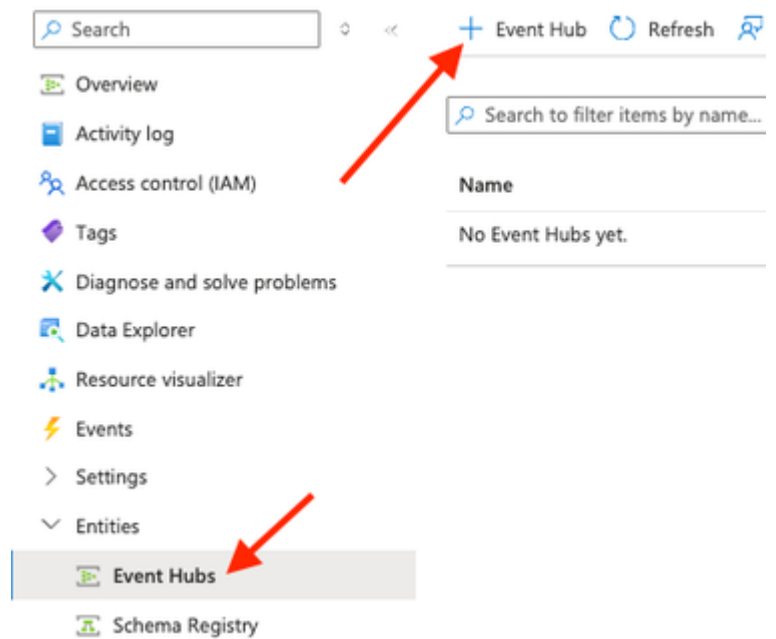
CAC Admin ADM ID

ةيساسألا لاصتالا ةلسلس خسن

اهتظالم وةيساسألا لاصتالا ةلسلس خسن ب مق :ماه

ثادأالا عزوم مسا ةحاسم لخاد ثادأا عزوم ليثم عاشنا : 7 ةوطخال

ليثم عاشناإل Event Hub + قوف رقنا .ثادأالا رواحم > تانايك رتخأ ،مسالا ةحاسم ةمئاق نم (1)
ديج EH



دېج شادحاً عزوم لېښم عاشن

عاشن + ةعجارم قوف رقنا مټ ،دېجل EH لېښم ل مسا نېي عتب مق 2)

Home > Event Hubs > captive-auth-ad-eh | Event Hubs

Create Event Hub

Event Hubs

Basics Capture Review + create

Event Hub Details

Enter required settings for this event hub, including partition count and message retention.

Name *

captive-auth-ad-eh-1

Partition count

1

Retention

Configure retention settings for this Event Hub. [Learn more](#)

Cleanup policy

Delete

Retention time (hrs) *

1

min. 1 hour, max. 168 hours (7days)

Review + create

< Previous

Next: Capture >

شادحأل عزوم لي ثمل مسا نبيعت

شادحأل زكرم لي ثمل ريفوتل عاشنا قوف رقنا ،ةحصلال نم ققحتال ةيلمع حاجن درجمب 3)

Create Event Hub

Event Hubs

✓ Validation succeeded.

Basics Capture Review + create

Event Hubs Instance by Microsoft

Basics

Name	captive-auth-ad-eh-1
Partition count	1

Retention

Cleanup policy	Delete
Retention time (hrs)	1

Capture

Capture Status	Off
----------------	-----

Create

< Previous

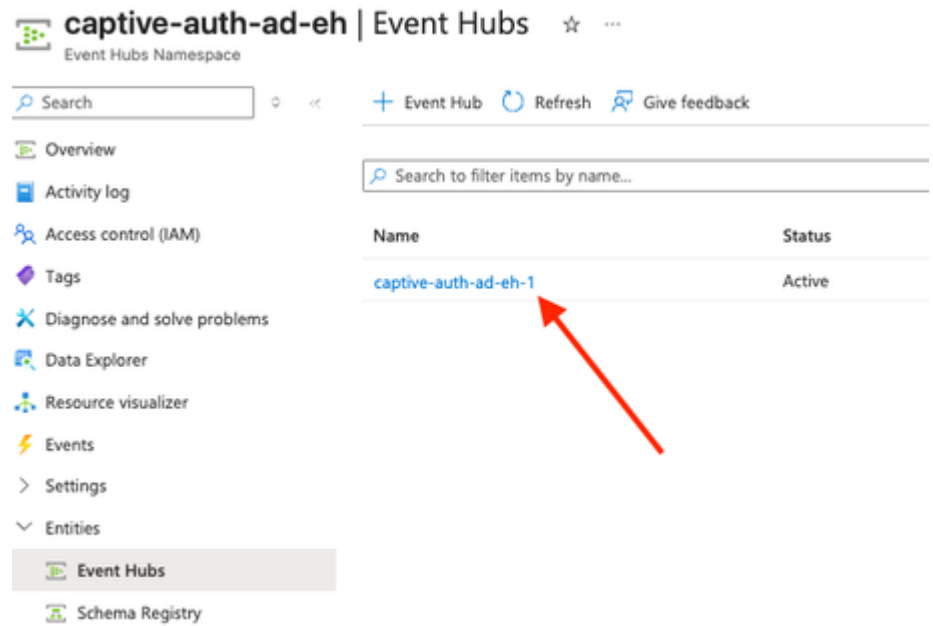
Next >

Provision Event Hub لي ثمل

هتظحالامو Event Hub لي ثمل مسا خسنب مق :ماه

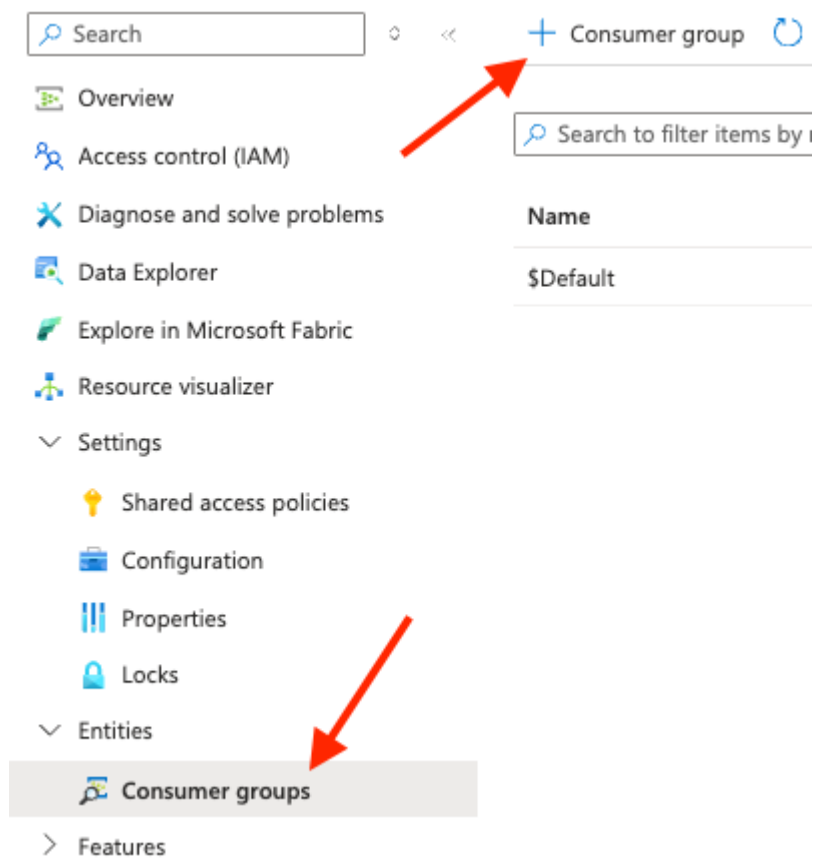
شادحأل عزوم مسا ةحاسم لخاد شادحأل عزوم لي ثمل ةيكالاهتسا ةومجم عاشنا : 8 ةوطخال

ةقباسال ةوطخال يف نوكمال دي دل EH لي ثمل قوف رقنا 1)



Access Event Hub لي ثم نيوكت

نيكلهتسم ةعومجم ءاشناب مقو، نيكلهتسم لا تاومجم > تاناياك لا رتخأ، EH لا ثم نم 2) ةديج.



نيكلهتسم ةعومجم ءاشناب

ءاشناب قوف رقاو نيكلهتسم لا ةعومجم ةيمستب مق 3)

Create

نيكلهت سملاة و مچمل مسا نيي عت

هتظحالمو Event Hub لي ثمل نيك له تسمل العومجم مسا خسنب مق :ماه

ةعمجملا ميقلاب نم ققحتلا : 9 ةوطخلا

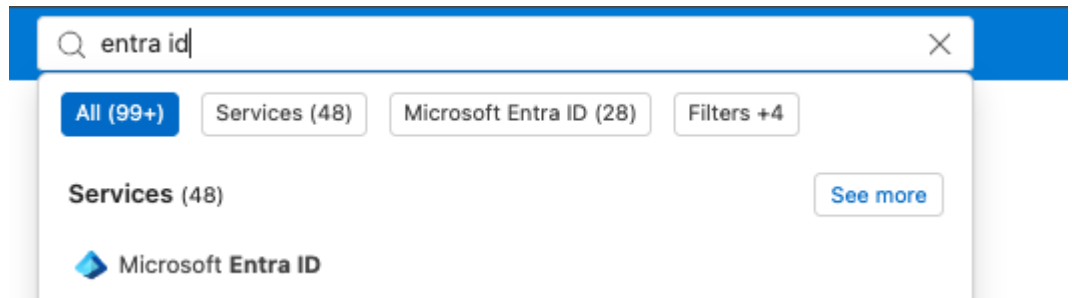
١) ةقبا سلا تاوطخلا نم اهيلع لوصحلا مت يتلا ميقلل هذه ةظحالم نيعتي ،ةلحرمل هذه يف
:اهيعمجت متي شيح ةيراسلا ةوطخلا عجارف ،ةميقي أليجست متي مل اذا

- هذه هؤاشنإ مت يذلا ةسسؤملا قيبطتل) قيبطتلا ليجست - 2 ةوطخلا 3 ةلحرمل
- (هعيمجت مت يذلا ضرعل مسا ةطساوب هيلإ راشملا ،ةيلمعل
- 2 ةيعرفلا ةوطخلا ، 2 ةوطخلا
- ضرعل مسا
- (ليمعل) قيبطتلا فرعم
- (رجأتسملا) ليلدل فرعم
- 6 ةيعرفلا ةوطخلا ، 2 ةوطخلا
- لليمعل رس
- ثادحلأ زكرم - 6 ةوطخلا ةثلاثلا ةلحرمل
- 1 ةيعرفلا ةوطخلا ، 6 ةوطخلا
- EH مسا ءحاسم
- ةيساسلأا لاصتالا ةلسلس

- 3 ةيعرفلا ةوطخل، 7 ةوطخل
- EH (Event Hub) ليثم مسا
- 3 ةيعرفلا ةوطخل، 8 ةوطخل
- EH يكلهتسم ةعومجم مسا

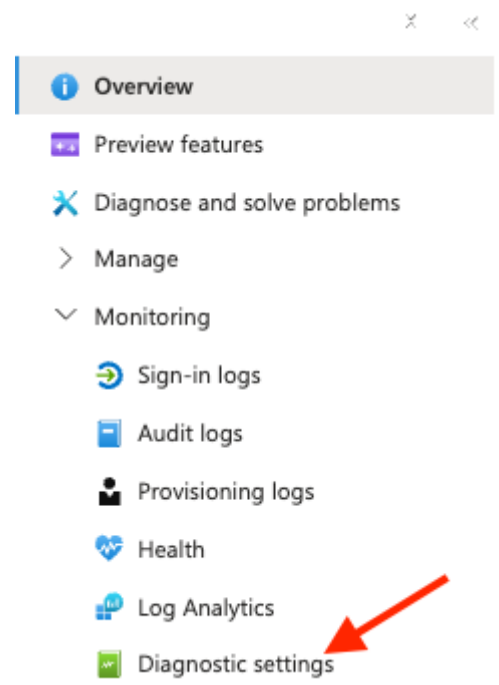
ثادحألا زكرم ىلا ارتنإلا فرعم قيقدت لجس قفد نيوكت: 10 ةوطخل

ارتنإلا فرعم رجأتسم نيوكت ىلا فلخلل لقننتلاب مق 1)



ارتنإلا فرعم رجأتسم نيوكت ىلا لاقننتالاول شحبالا

صيخشنتلا تاداعإ > ةبقارم رتخأ، ىرسىلا ةمئاقلا نم 2)



صيخشنتلا تاداعإ ةبقارم

صيخشنت داعدإ ةفاضإ + قوف رقناو ماع > صيخشنتلا تاداعإ رتخأ 3)

Diagnostic settings | General



Can you explain how to send diagnostic logs?



Refresh



Feedback

Diagnostic settings



General



Custom security attributes

Diagnostic settings are used to configure streaming export of platform logs.

Diagnostic settings

Name	Storage account
	-
	-
	-

+ Add diagnostic setting

دېج صېخشت دادع | ؤفاض|

لېجسټل AuditLog رايټخاله ۀناخ ددحو، صېخشتل دادع | ۀل بولطم ال مسال نييغت ب مق 4) نم اهتظالم تمت يټل ميق ل عچار. ټاډح زكرم ۀل قفدت رايټخاله ۀناخ ددحو، لوڅدل ل.امتكال دن ع ظفح قوف رقناو، ۀقباسل تانيوكتل.

Diagnostic setting

Save Discard Delete Feedback

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more about the different log categories and contents of those logs](#)

Diagnostic setting name *

captive-portal-auth

Logs

Categories

- ☒ AuditLogs
- ☐ SignInLogs
- ☐ NonInteractiveUserSignInLogs
- ☐ ServicePrincipalSignInLogs
- ☐ ManagedIdentitySignInLogs
- ☐ ProvisioningLogs
- ☐ ADFSSignInLogs
- ☐ RiskyUsers
- ☐ UserRiskEvents
- ☐ NetworkAccessTrafficLogs

Destination details

☐ Send to Log Analytics workspace

☐ Archive to a storage account

☒ Stream to an event hub

For potential partner integrations, [click to learn more about event hub integration](#).

Subscription

Event hub namespace *

captive-auth-ad-eh

Event hub name (optional) ⓘ

captive-auth-ad-eh-1

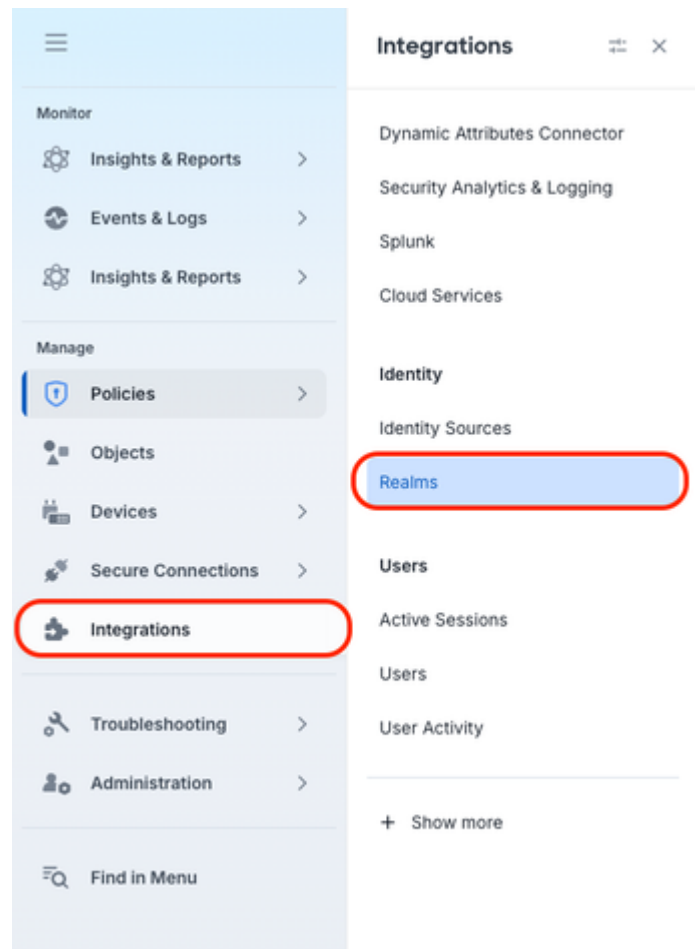
Event hub policy name

☐ Send to partner solution

FMC/FTD و Azure ل ةطشنلا ةقداصملا نيوكت جم د: 4 ةلحرمل

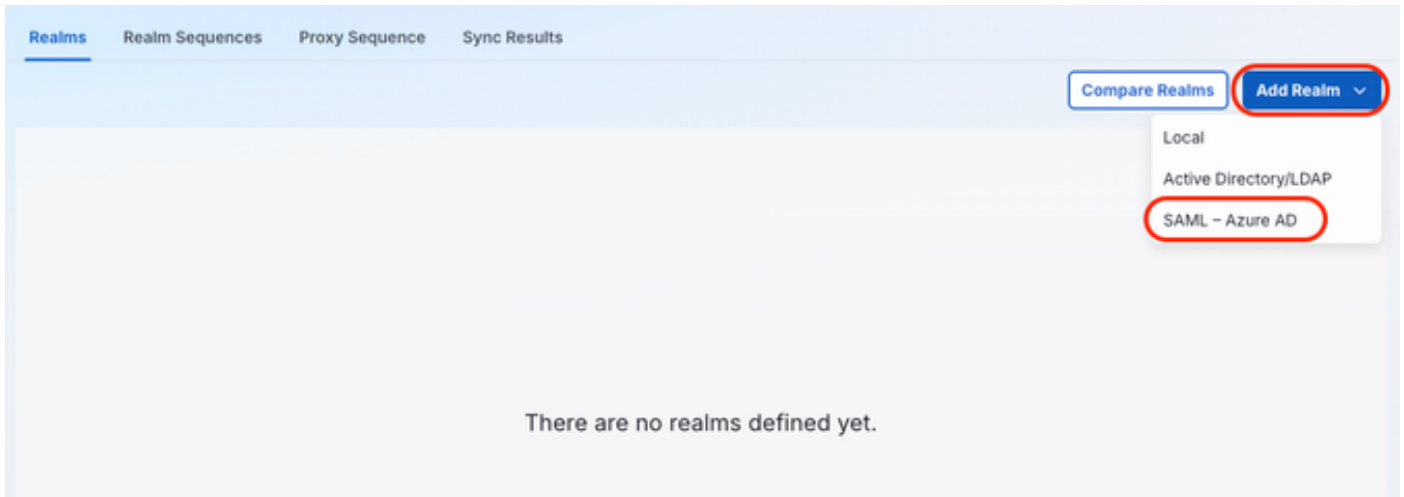
FMC جلاعم مادختساب Azure SAML/Entra فرعم قاطن نيوكت: 1 ةوطخلا

طباورلا > ةيوهلا > لماكتلا تايلمع رتخأ، FMC نمض 1)



ةيوهلا تالاجم نيوكت

SAML - Azure AD. رتخاو، لاجم ةلدسنملا ةمئاقلا ةفاضل قوف رقنا 2)



إضافة SAML Azure AD Realm

- 3) إعدادات الرايتم الرايتم رايتخا نم دكأتو، همادختسا فصول Azure لقحل فصول مسان يي عتب مق 3) عم رايسا لخدم مادختسا وأ Azure AD مادختساب يبلس لكشب (يلالات) Next قوف رونا. نيوكتال عون قدس نمل

Azure AD قاطن تادادع نيوكت

- 4) نايكل فرعم لخدأ. ياساسال URL ناووع نوكل اقبسم هنيوكت مت يذل FQDN نئاك رتخا 4) حضومال قدسلسلال قيسنتب

https://<fqdn-base-url>/<uniqueSuffix>

- نيوكتال لاثم في رضخألاب اهتحت متي يتي (SAML) نايف فرع مةقحال نيوكت دنع بجي .ةئيبلا لخاد رخأال SSO ذيفنت تايلمع نيب ةديرف ةقحال نا نم دكأت ،(يالات لال خ وه امك يساسأال URL يقبي .اضيأ Azure SAML نيوكت عم ةميقل هذه قباطت نا نيوكتال .
- ربيغتلل لباق ريغ وهو ايئاقلت (ACS) ةدكؤمل عالمعل تامدخل URL ناونع علم متي تحت FMC في ةقباسل لمعل ريس تاوطخ في ةلجسمل (SP) ةمدخل دوزم ةداهش رتخأ .تاداهشل > ةزهأال .
- ةيلمع ليهستل ةمدخل رفوم فيرعت تانايب لي زنت قوف رقنا ،ميقل هذه لخاد دعب Azure. إلاتباتك تمت دق ةقوتمل ميقلا نا يلع ديكأتال نيوكتال .

Add SAML – Azure AD Realm

1

Realm Details

Name

azure-entra-saml

Description

Active Authentication IdP

Identity Provider

Azure AD

Configuration Type

Authenticate passively with Azure AD or using captive portal with Azure AD

2

SAML Service Provider (SP) Metadata

Base URL *

active_auth_fqdn

Must resolve to the interface(s) of source security zones used in an identity policy.

Entity ID *

https://ftd-inside.example.com/saml/sp/metadata/activeAuthEntID

Unique, alphanumeric identifier for a SAML entity.

Assertion Consumer Services (ACS) URL *

https://ftd-inside.example.com/+CSCOE+/saml/sp/acs?tname=azure-entra

URL at which the service provider receives SAML assertions from Azure AD.

Service Provider Certificate *

FTD-SP-Cert

Certificate used for SAML authentication and TLS/SSL communication with the secure threat defense device. The certificate must have the value you specify for Base URL that must match the Common Name (CN) or Subject Alternative Name (SAN). The certificate, which must be in PKCS12 format, must be trusted by clients.

Download Service Provider Metadata

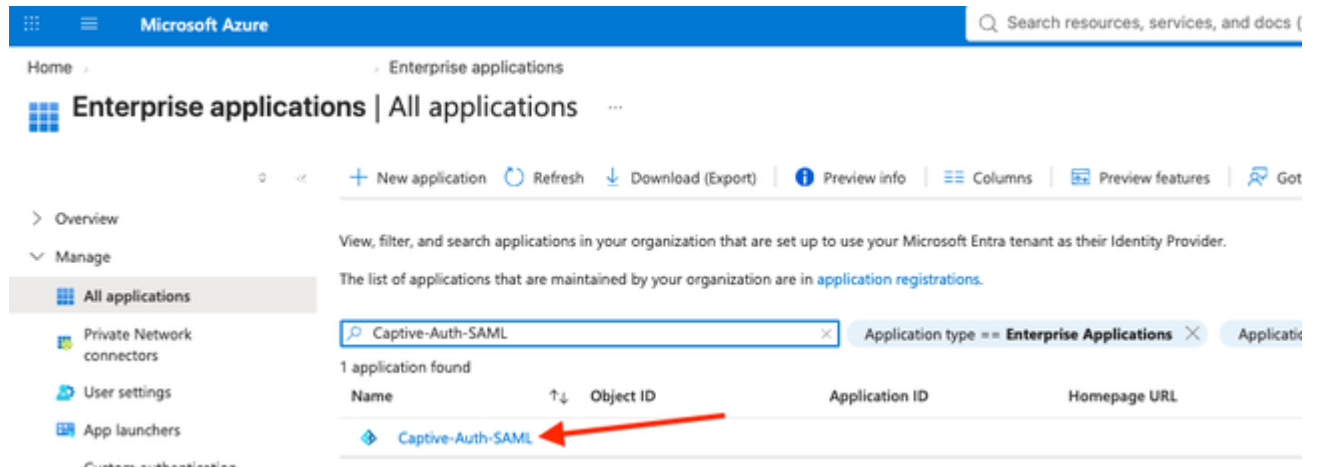
Next

SAML فيرعت تانايب لي زنت و ةدحو لا فرع مو يساسأال URL ناونع نيوكت

ق.اطنل نيوكت نم 3 لسلسلتال إلالاقتنالل يلاتال قوف رقنا 5)

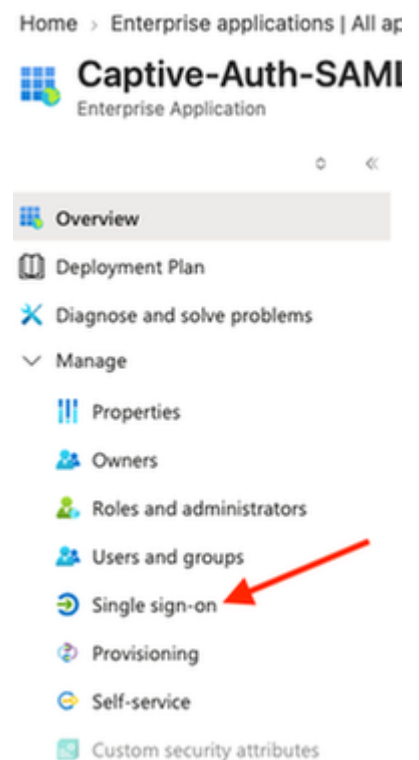
Azure Enterprise قىبطت في FMC لة نوكم ال SAML SP في رعت تاناي ب ذي فنت 2: ة واخل

ن ع ثح با .ة سؤم ال ا قىبطت > ة راد ا > Entra فرعم رتخاو Azure لى لى فلل ل لقتنا 1)
Microsoft Entra SAML Toolkit Enterprise قىبطت ل اق بسم هؤاشن ا مت ي ذل ل لى ثم ال



Microsoft Entra SAML Toolkit قىبطت ع قوم دي دحت

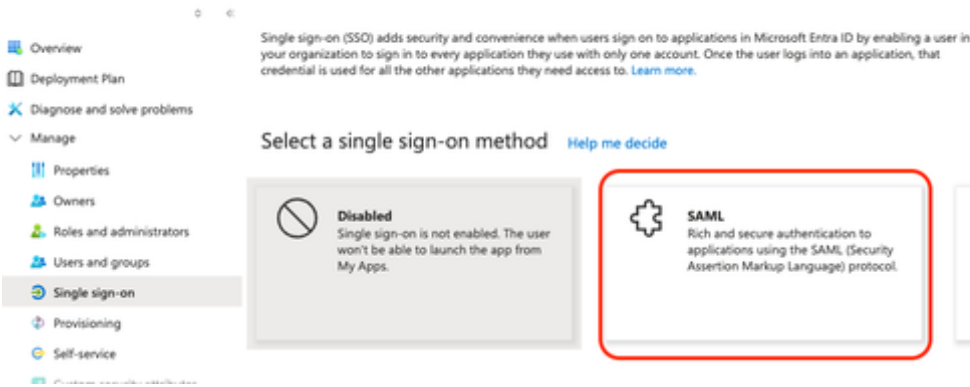
ي داح ال ل واخل لى ج ست > ة راد ا رتخا ، ي ب ن ا ل ل قنت ال ة مئاق نم 2)



ي داح ال ل واخل لى ج ست ني وكت ة راد ا

SAML (SSO). ي داح ال ل واخل لى ج ست ع ضو لى ع ر قنا 3)

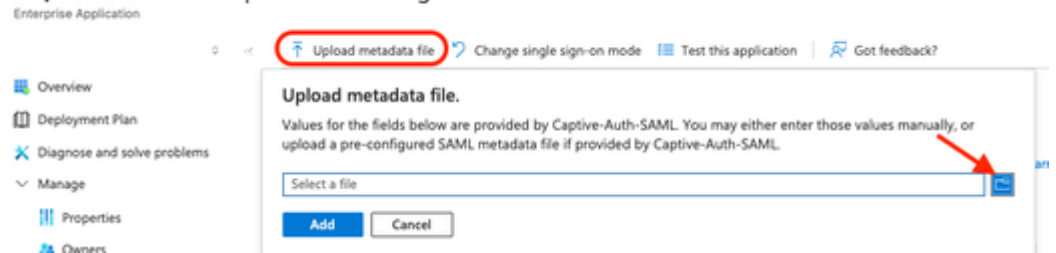
Captive-Auth-SAML | Single sign-on



SAML يداخل لولوج ليجست عضو ديت

ضارعت سال قرزال دلجم الة نوقي قوف رقناو فيرعت التاناي ب فلم ليجست قوف رقنا 4) هليزنت مت يذل SAML فيرعت تاناي ب فلم يلا لوصول ك صاخل ليجست التافلماظن FMC.

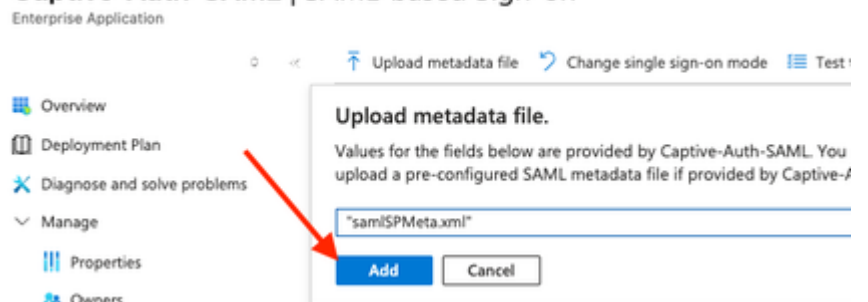
Captive-Auth-SAML | SAML-based Sign-on



ةيامل رادج راد زكرم نم فيرعت التاناي ب فلم ليجست

ةافاضا قوف رقنا، ليجست التاناي ب درجب 5)

Captive-Auth-SAML | SAML-based Sign-on



SAML نيوكت قيبطت ةافاضا

فرعم) فرعم لثم مي ق جارختسإ متي و، يساس ال SAML نيوكت لة يبنال الة حول رهظت 6) مت يذل او FMC ةطساوب هؤاشنإ مت يذل ي فيرعت التاناي ب فلم نم ACS URL ناو نو (ةدحول بولطم هو لولوج ليجست URL ناو نو علم متي مل، ك لذ عمو. ايئاقلت هقيبطت و هليجست ظفحل لبق

Basic SAML Configuration

Save | Got feedback?

Identifier (Entity ID) * ⓘ

The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

Default

https://ftd-inside.example.com/saml/sp/metadata/activeAuthEntID ✓



Add identifier

Patterns: https://samltoolkit.azurewebsites.net

Reply URL (Assertion Consumer Service URL) * ⓘ

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

Index

Default

https://ftd-inside.example.com/+CSCOE+/saml/sp/acs?tgname=azure-entra-saml ✓

0



Add reply URL

Patterns: https://samltoolkit.azurewebsites.net/SAML/Consume

Sign on URL *

Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

*

Enter a sign on URL

Patterns: https://samltoolkit.azurewebsites.net/

- ✗ Please enter a valid URL starting with "https://". If your URL has query parameters, ensure that there is a slash preceding the question mark (i.e. /?)
- ✗ This field is required

Relay State (Optional) ⓘ

The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application.

Enter a relay state

Logout Url (Optional)

This URL is used to send the SAML logout response back to the application.

Enter a logout url ✓

يساس ال SAML نيوكت جارختسا

رقنوا، اهقصلو ەمېقلا خسنب مقو، حونم مالم لوخدلا ليجستل URL ناو نع طمن مدختسا 7)

Basic SAML Configuration

 Save  Got feedback?

Identifier (Entity ID) *

The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

Default

[Add identifier](#)

Patterns: <https://samltoolkit.azurewebsites.net>

Reply URL (Assertion Consumer Service URL) *

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

Index

Default

0

[Add reply URL](#)

Patterns: <https://samltoolkit.azurewebsites.net/SAML/Consume>

Sign on URL *

Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

*

Patterns: <https://samltoolkit.azurewebsites.net/>

Relay State (Optional)

The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application.

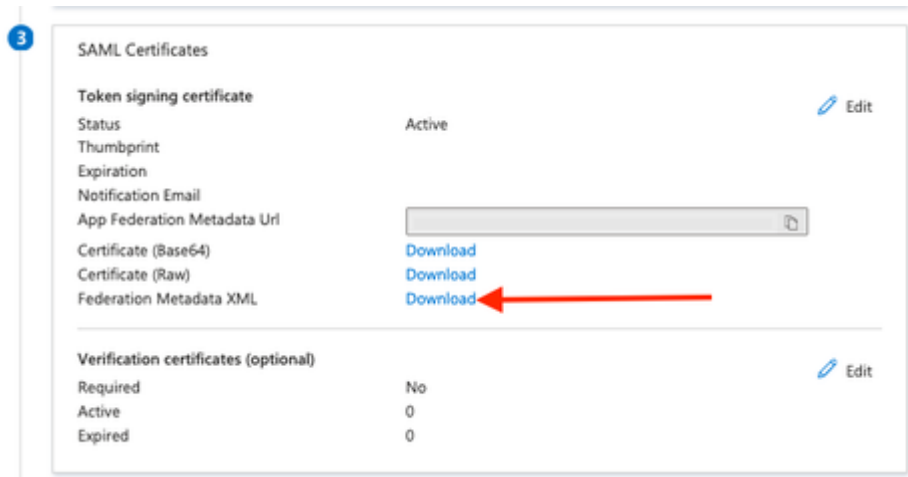
Logout Url (Optional)

This URL is used to send the SAML logout response back to the application.

URL نويوكت لاخذإلى لىل لوخذل لىجست

مت يذل داحتال فيرعت تانايبل XML فلم ردصأو، SAML تاداهش لىل لفسأل ريرمتلاب مق

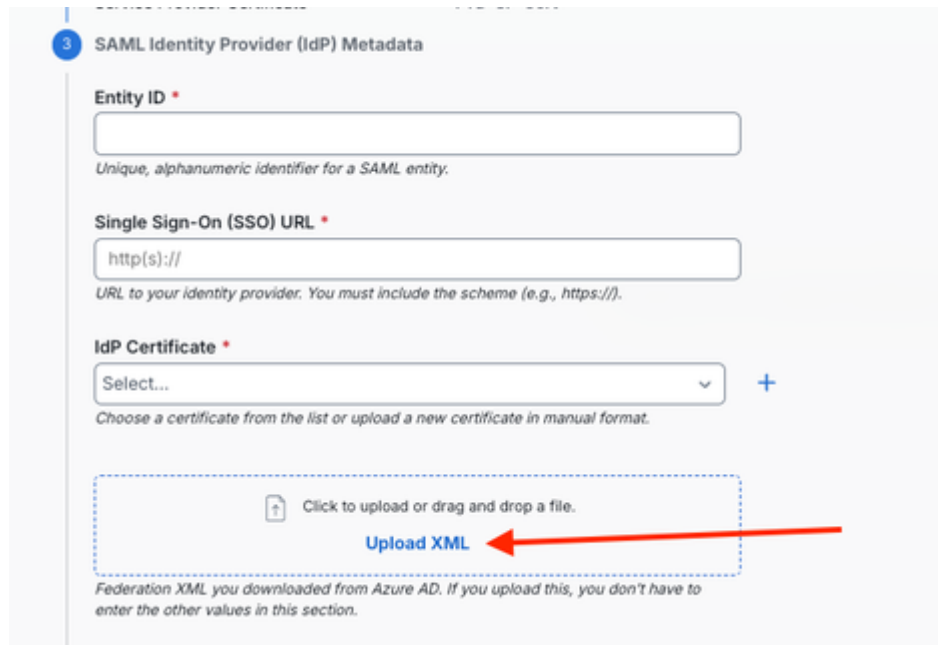
Cisco. نم نم آال FMC ىلى هداريتسال Azure لبق نم هؤاشنإ



داحتالال فيرعت تانايب ل XML فلم ريصت

(عبات) FMC جالعام م ادختساب Azure SAML/Entra فرع قاطن نيوكت: 3 ةوطخلال

3، لسلسلتال تحت (FMC) ةساسأال ةحوللإ ةرادإ في مكحتلال ةدحو ىلى فلخلل لقتنا (1) يذل XML داحتالال فيرعت تانايب فلم لي محتب مق، SAML (IdP) ةي وه رفوم فيرعت تانايب اياقلا ةرورضلال ميقلال فلمل FMC ىلى Azure نم هريصت مت



داحتالال فيرعت تانايب ل XML فلم لي محت

حضورم وه امك ميقلال مي ممتي، اهل ممت درجمب (2)

3 SAML Identity Provider (IdP) Metadata

Entity ID *

Unique, alphanumeric identifier for a SAML entity.

Single Sign-On (SSO) URL *

URL to your identity provider. You must include the scheme (e.g., https://).

IdP Certificate *

Choose a certificate from the list or upload a new certificate in manual format.

 Click to upload or drag and drop a file.

Upload XML

Federation XML you downloaded from Azure AD. If you upload this, you don't have to enter the other values in this section.

 **Next**

ايئاقلت اهتئبعت مت يئالت SAML ةي وه رفوم ميقي

ةروصلال ي في ئئزلال جارخإل ضرع متي :ةظحال م

ةطقنللا هذ يئح ذئ فنئلل ةئل م ع لال خ ةعمم لال مئقلا لالخا 3)

- قئب طئلل لئجست
- (لئ م لال) قئب طئلل فرعم
- لئ م لال رس
- (رأئ س لال) لئ ل دلل فرعم
- ئاأال زكرم
- EH م س ا ةحاس م ل فيض م ل م س ا
- EH م س ا ةحاس م ل ةئ ساسأل لاصئال ةل س ل س
- EH (Event Hub) لئ ئ م س ا
- EH ئك ل هئ س م ةعومم م س ا

Add SAML – Azure AD Realm

4 Azure AD Details

Client ID *

851607f9-969f-4fed-90ec-829607c1c

Application ID (also referred to as client ID you created in Azure AD).

Client Secret *

.....

Secret string that the application uses to prove its identity when requesting a token.

Tenant ID *

af42bac0-52aa-429f-92db-9258199f

Microsoft Entry ID entity that typically encompasses an organization. Displayed in Azure Entra ID → Properties.

Event Hubs Host Name *

captive-auth-ad-eh.servicebus.windo

Hostname of the Event Hub Namespace. Displayed in Event Hubs → Event Hubs Namespace.

Event Hub Name *

captive-auth-ad-eh

Name of your event hub. Displayed in Event Hubs Name Space → Overview.

Consumer Group Name *

captive-auth-ad-eh-cg

A view of an entire event hub. Consumer groups enable consuming applications to each have a separate view of the event stream.

Event Hub Connection String *

Endpoint=sb://captive-auth-ad-eh.servicebus.windows.net;/SharedAccessKeyNi

Event Hub Connection String: Unique identifier for the event hub (also referred to as topic or endpoint). It is displayed on the Azure AD portal in Event Hubs → (name of your event hub) → Shared access policies → (name of policy).

USER GROUPS ☒

☐ Excluded User Groups

☒ Included User Groups

Enter each group name on a separate line

active-auth-lab

Enter one or more groups from which to download users for identity control. Users in these groups will be available for use in access control policies.

Test Test connection succeeded

Next

شادحألا زكرم وقيبطتلا تامولعم لاخدا

Azure إلى لوصولو ةيئناكم نم دكأت و لاصتالا نم ققحتلل Test قوف رقنا ، Azure لاخدا درجمب ةرفوتملا تامولعمل مادختساب

قفاوتت ةنمضمل/ةدعبتسملا نيمدختسملا تاومجم نأ نم دكأت ، نكمأ نإ :ةطحالـم
خسنلل نيوكت عم

SAML لخدم نيمدختسم ةلهم نيوكت ةيئناكم لجالعملل ةريخألا ةوطخلال كل حيتت 4)
ةقيقد 1440 وه يضارتفالا .نيروسأالا

5 User Session Timeout

SAML Captive Portal Users

1440 Minutes Range 0-35791394

لقننتم ال لخدملة لهم نيوكت

عبارات لليلالات قوف رقنا 5)

After the timeout is exceeded, the user's session ends; if the user continues to access the network without logging in again, the user is seen by the management center as Unknown (except for Failed Captive Portal Users).

Next

Azure AD Realm نيوكت عم مدقتال

صخلملة ياهن في ظفح قوف رقنا. هذيفنت مت يذال نيوكت لل اصخلم لجالعمل مدقي 6)
اهديكأت واهلإخدا مت يتال ميقلأ حص نم ققحتال دعب

5 User Session Timeout Edit

SAML Captive Portal Users	1440 Minutes
ISE Users	1440 Minutes

Cancel Save

قاطنل نيوكت صخلم ظفح رز

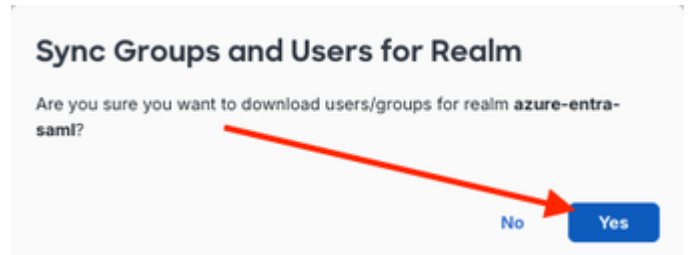
مهليزنت مت نيلذل نيمدختسمل نم ققحتال 4: ةوطخال

نمض نآل ليزنتال رز مادختساب Azure Entra نم نيمدختسمل ليزنتة يانكإ نم دكأت 1)
RealMS. لمع ريس > ةيوهال > لملكالتا يلمع

Name	Type	Description	Proxy	Status	Value	
azure-entra-saml	SAML - Azure AD (captive portal)	Active Authentication IdP	Not Applicable	Ok	tenant-id: af42bac0-5	Enabled Download Now

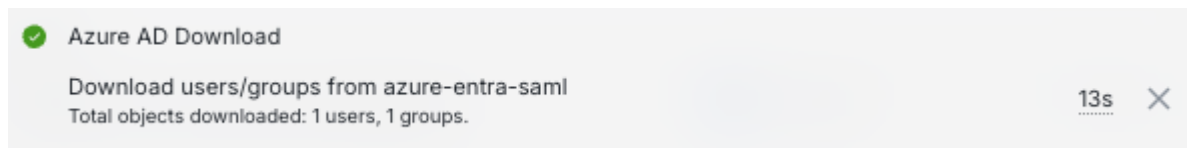
Azure AD نيمدختسمل ليزنت

راوخال عبرم ةبلالطمل ةباجتسا معن قوف رقنا 2)



Azure AD نم نېم دځتسم لالېزنت دېكأت

نمض دكؤم وه امك ،اهلېزنت مت ؤدحاو ؤعومجمو دحاو مځتسم لالېزنتال ؤمهم نع چتني (3)
م.اهم > تامالعا

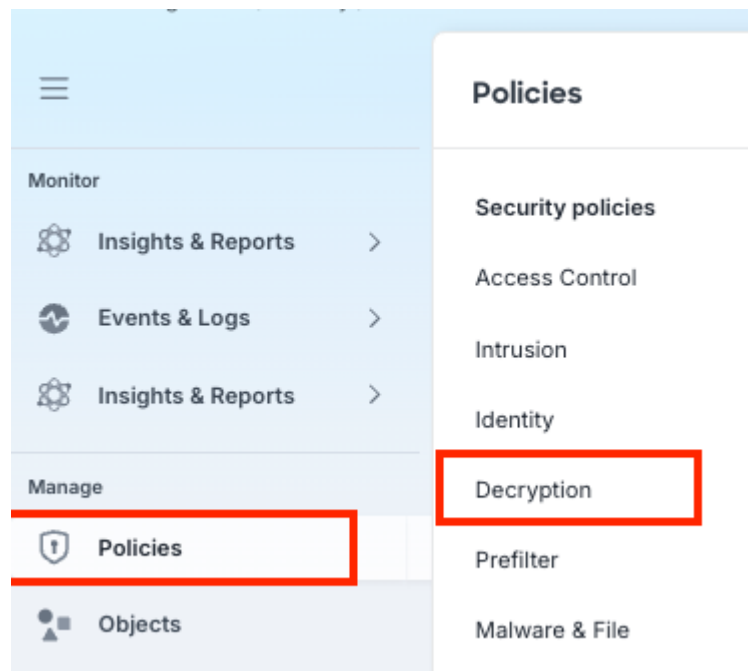


Azure AD نم نېم دځتسم لالېزنتال مالعلا لاد

FMC ف تاسايسال نيوكت :5 ؤلحرمل

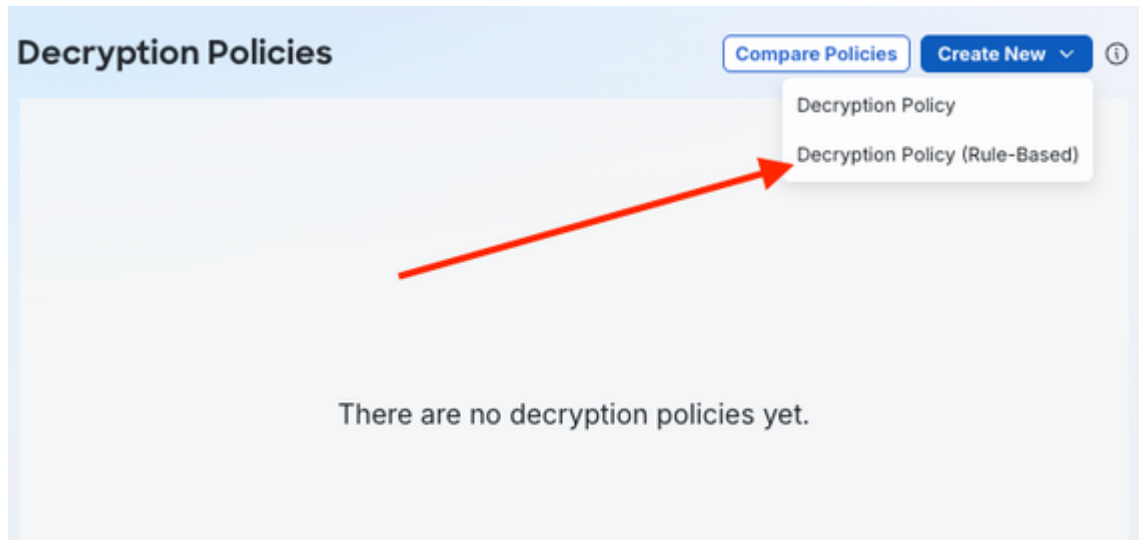
رېفشتلال ك ف هه نيوكت :1 ؤوطخال

رېفشتلال ك ف > نېمأتال تاسايس > تاسايس رتخأ ،FMC ف (1)



رېفشتلال ك ف هه نېم لالاقنتال

يلع ٤مئاق) ريفشتلا كف ؤسايس رتخاو ؤيڊج ؤلڊسنم ؤمئاق عاشنإ قوف رقنا 2)
(ؤعاقولال.



ؤعاقولال ؤل ؤنئسي ؤيڊج ريفشت كف ؤن عاشنإ

ؤيڊجال ريفشتلا كف ؤسايسل فصو، اٲولطم كلذ ناك اذإ، مسا نييؤتب مق 3)
ؤيماح) ؤرؤاصلال تالاصتالال بيوبتلال ؤمالع رايع قوف رقناو، ؤعاقولال ال ؤنئسمال
ؤاٲالال ؤقؤاصلال ؤٲولطمال ؤلاقئسالال ريفشتلا كف ؤفيظو ذيئفل (مؤخئسمال
(ؤئشنال ؤقؤاصلال) ؤيڊمال

ؤرؤاصلال تالاصتالال ؤسايس ليصافت ذيئفل

4) ةيراسلا ةلدسنملا ةمئاقلا نم اقبس م هقيبطت مت يذلا يلخادلا قدصملا عجرملا رتخأ (يلالاتلا) Next قوف رقنا .راوحلا سفن يف هب ةصاخلا

5) عیاجال بسح تارایخل صیصخت

Create Decryption Policy

1 Policy Details

2 Blocking

3 Decryption Exclusions

Enter name, description, choose policy type and certificates.

(Optional) Configure blocking based on TLS version and certificate status

(Optional) Configure exclusions for outbound connections.

☐ Block inbound and outbound connections based on TLS version

We recommend blocking the following because they are not secure.

SSL v3.0 X TLS v1.0 X TLS v1.1 X

[Reset to default](#)

☐ Block inbound and outbound connections based on server certificate status

We recommend blocking the following because they are not secure.

Invalid Signature X Expired X Not Yet Valid X

[Reset to default](#)

Cancel

Skip

Back

Next

ريفتلار ك ف جهن تاراخي صي صخت

6) **ةب ول ط لم ة سا ي س لا لي ص ا ف ت ء ا ن ث ت س ا ب ت ا ي ض ا ر ت ف ا لا م ا د خ ت س ا م ت ي ، ل ا ث م لا ا ذ ه ي ف 6) ج ه ن ء ا ش ن ا ق و ف ر ق ن ل ا ب ن ي و ك ت ل ج ل ا ع م ل م ك ا**

Create Decryption Policy

1 Policy Details
Enter name, description, choose policy type and certificates.

2 Blocking
(Optional) Configure blocking based on TLS version and certificate status

3 Decryption Exclusions
(Optional) Configure exclusions for outbound connections.

Decryption Exclusions

☐ **Bypass decryption for sensitive URL categories**
 In many environments, certain categories of websites are not inspected for regulatory, compliance or privacy reasons. Customize the list below to bypass inspection for designated categories.
 Note: **URL License is Required**
 URL Categories: Finance Online Trading Health and Medicine + Add

☒ **Bypass decryption for undecryptable distinguished names**
 Bypass decryption based on Cisco's list of known undecryptable distinguished names.
 Note: **This option is selected by default to allow traffic which cannot be decrypted to remain encrypted. Disabling this option might cause decryption to fail for unsupported distinguished names.**
56 Distinguished names included

☒ **Bypass decryption for undecryptable applications**
 Certain applications are not supported for decryption due to a variety of reasons (certificate pinning, client certificate authentication, and so on). This option bypasses decryption based on Cisco's list of known undecryptable applications.
 Note: **This option is selected by default to allow traffic which cannot be decrypted to remain encrypted. Disabling this option might cause decryption to fail for unsupported applications.**
59 Applications included

Intelligent Decryption Bypass

☐ **Bypass decryption for very low-risk connections** New
 Bypass decryption for very low-risk clients connecting to trusted servers.
 Note: **Do not decrypt traffic for very low-risk clients connecting to trusted servers, based on the threat confidence levels of clients**

Cancel Skip Back Create Policy

يئاهنل زيمرتل ك ف چن عاشن

ريفشتل ك ف سايس دعاوق نيوك ت: 2 ةوطخل

ةكرح .انه دعاوق ىلا ةدنتسمل زيمرتل ك ف سايسل يضارتال طيطختال ضرع متي (1 ةمئاق ىلا ريفشت يتال) 3 ةدعاقال لثم ،ةنكممل ةيضارتال دعاوقال قباطتال يتال رورمل تاقيبطتال ىلا ريفشت يتال) 6 ةدعاقالو (ةرفشمل ريغ تالاجمل امامسأل اقبسمةصمخ - ريفشتال اغلل - ريفشتال ك ف ارجال عرضت ،(ةرفشم ريغك اهيلع ةمالع عوضومت يتال ارجال ىلا ةفاضالاب ،تايضارتالال هذه ليدعت نكمي .7 ةدعاقال بجومب ريفشتال اغلل يا عم قباطتال يتال رورمل ةكرح نيوك متي ،يضارتالال كشب .ةجاجل بسح ،يضارتالال ريفشتال ك ف موقتال اهنأ ىلعل رخأ ةدعاق

ةدعاق عاشن متي كلذل ،صفحلل Azure ةقداصم ةمدخ رورم ةكرح ريفشت ك ف مدع بجي .عبدلل ةدعاق ةفاضل + قوف رقنا .اهل ةصصمخ

active-auth-decrypt-policy Save Cancel

Decryption Policy for Active Authentication

[Rules](#) [Trusted CA Certificates](#) [Undecryptable Actions](#) [Advanced Settings](#)

[+ Add Category](#) [+ Add Rule](#)

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicatio...	Source Ports	Dest Ports	Categories	SSL	Action
Administrator Rules													
This category is empty													
Standard Rules													
1	Auto-Rule-Certificate-Stz (Disabled)	any	any	any	any	any	any	any	any	any	any	3 Cert Status s	Block with reset
2	Auto-Rule-TLS-Versions (Disabled)	any	any	any	any	any	any	any	any	any	any	3 Protocol Vers	Block with reset
3	Auto-Rule-Undecrypt	any	any	any	any	any	any	any	any	any	any	1 DN selection	Do not decrypt
4	Auto-Rule-Low-Risk-Con (Disabled)	any	any	any	any	any	any	any	any	any	Any (Except L	1 Client Threat	Do not decrypt
5	Auto-Rule-URL-Categoric (Disabled)	any	any	any	any	any	any	any	any	any	Finance (Any Health and M	any Online Tradin	Do not decrypt
6	Auto-Rule-Undecryptabl	any	any	any	any	any	any	Tags: undecry	any	any	any	any	Do not decrypt
7	Auto-Rule-Internal-La	any	any	any	any	any	any	any	any	any	any	any	Decrypt - Resign
Root Rules													
This category is empty													
Default Action													Do not decrypt

ةيضا رتفا ةءءاق لى دننسم ريفشت ك ف طي طخا رهاظو ةءءاق ةفاضا

ريفشت ل ك ف مدع رتخاو ، ةديءل ريفشت ل ك ف ةسايس ةءءاق لاءل م سا نبيعت ب مق 2) م تي امك . اءيءل ل ءاوقل لى لءا ف ةءءاق ل ءضوو ، "ءاءل" ةلءسنم ل ءمئل ل نم ركب ل كشب ةءءاق ل قبيضتل ةءءول/رءصم ل قطانم ءيفنت

Add Rule

Name: ☒ Enabled

Action:

Insert:

[Zones](#) [Networks](#) [VLAN Tags](#) [Users](#) [Client Threat](#) [Applications](#) [Ports](#) [Category](#) [Certificate](#) [DN](#) [Cert Status](#) [Cipher Suite](#) [Version](#) [Logging](#)

Available Zones

- Inside_Zone
- Outside_Zone
- DMZ_Zone

Source Zones (1):

Destination Zones (1):

ريفشت ل ك ف مدع ةءءاق نيوكا

ءمءل قبيبط نء ءءابا ، ءاقيبطا بيوبتا ءمءل ءوف رقنا ، ةءءاق ل ءفاضا لبق 3)

ةفاضل قوف رقنا م ث ،ةدعاقلا لة فاضل قوف رقناو Azure ةقداصم

Add Rule

Name: Azure-Auth-Service-DND ☒ Enabled Insert: above rule 3

Action:

Zones Networks VLAN Tags Users Client Threat **Applications** Ports Category Certificate DN Cert Status Cipher Suite Version Logging

Application Filters Available Applications (2)

Risks (Any Selected)

- ☐ Very Low 809
- ☐ Low 715
- ☐ Medium 2239
- ☐ High 1823
- ☐ Very High 609

Business Relevance (Any Selected)

- ☐ Very Low 609

Available Applications (2)

All apps matching the filter

- Azure Arc
- Azure Authentication Service**

Selected Applications and Filters (0)

any

Azure ةقداصم ةمدخ قيبطت ةدعاق ةفاضل

ظفح قوف رقنا 4)

active-auth-decrypt-policy

Decryption Policy for Active Authentication

You have unsaved changes

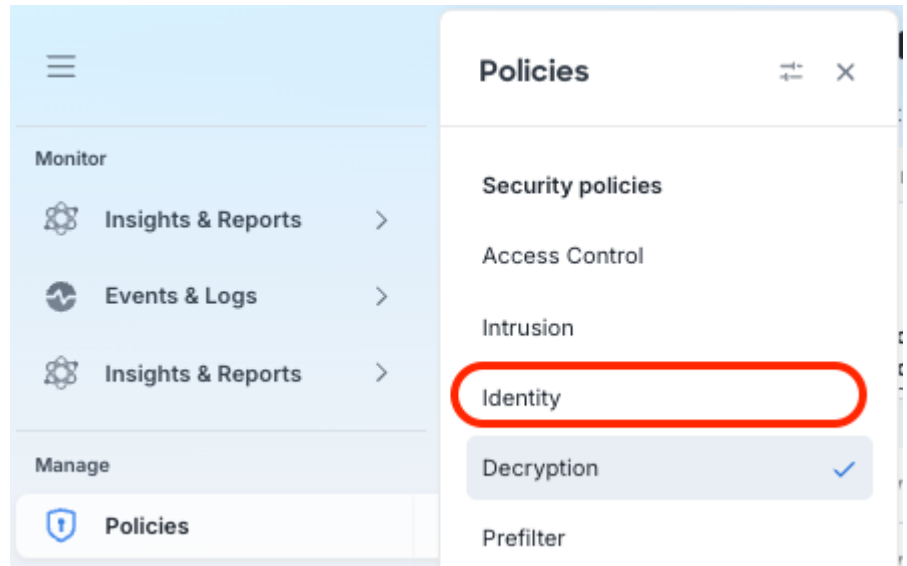
Rules Trusted CA Certificates Undecryptable Actions Advanced Settings

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Application...	Source Ports	Dest Ports	Categories	SSL	Action
Standard Rules													
1	Auto-Rule-Certificate-St (Disabled)	any	any	any	any	any	any	any	any	any	any	3 Cert Status s	Block with reset
2	Auto-Rule-TLS-Versions (Disabled)	any	any	any	any	any	any	any	any	any	any	3 Protocol Vers	Block with reset
3	Azure-Auth-Service-	Inside_Zone	Outside_Zon	any	any	any	any	Azure Authen	any	any	any	any	Do not decrypt

ريفشلتال كف جهن ظفح

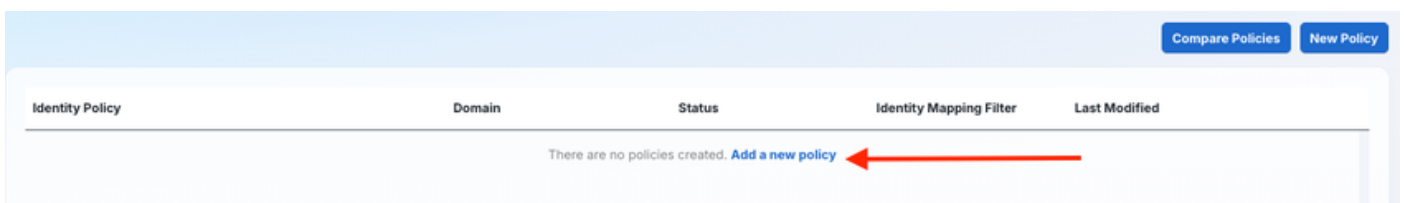
ةيوهلا ةسايس عاشنل 3 ةوطخلال

ةيوه ةسايس عاشنل ةيوهلا > ني مأتال تاسايس > تاسايس رتخأ 1)



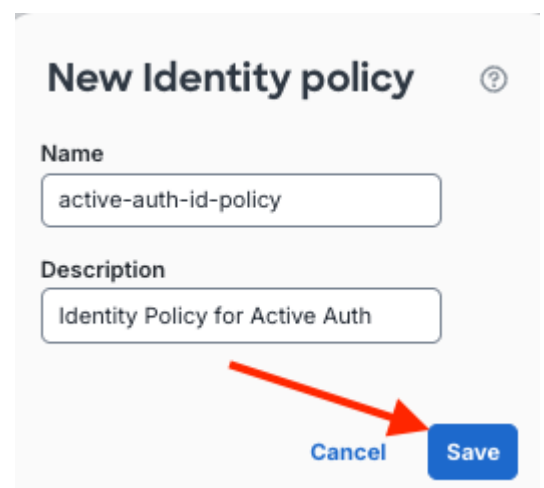
ئۆيۈرلەش سىياسىتىنى

2) ئۆيۈرلەش سىياسىتىنى قۇرۇش ۋە ئۆيۈرلەش سىياسىتىنى قۇرۇش.



ئۆيۈرلەش سىياسىتىنى قۇرۇش

3) ئۆيۈرلەش سىياسىتىنى قۇرۇش. ئۆيۈرلەش سىياسىتىنى قۇرۇش، ئۆيۈرلەش سىياسىتىنى قۇرۇش، ئۆيۈرلەش سىياسىتىنى قۇرۇش.



ئۆيۈرلەش سىياسىتىنى قۇرۇش

ئۆيۈرلەش سىياسىتىنى قۇرۇش: 4 ئۆيۈرلەش سىياسىتىنى قۇرۇش

١) ةءءاق فاضل + قوف رقنلاب ةءىء ةءءاق فاضل

active-auth-id-policy

Save

Cancel

Identity Policy for Active Auth

Identity Mapping Filter

None

+

How it works

Rules

Active Authentication

+ Add Category

+ Add Rule

Search Rules

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Source Ports	Dest Ports	Realm	Action	Auth Protocol
Administrator Rules											
This category is empty											
Standard Rules											
This category is empty											
Root Rules											
This category is empty											

ەدىج ەيۈە جەن ەدەاق ەفاضا

٢) عارج الة لدس نم المة ئاق ال نم ة طشن ال ة قدا صم ل رتخاو ، ة د د ج ل ة د عاق ال ة م س ت ب م ق ة قدا صم ل ذ ي ف ن ت ل ة د عاق ال ق با ط ت ن ا ب ج ي ت ل ة د د ح م ل ت ا ك ب ش ل / ق ط ا ن م ل ق ي ي ض ت و ة ط ش ن ل .

Add Rule

Name: **Active Auth ID Rule** ☒ Enabled Insert: into Category Standard Rules

Action: **Active Authentication** Realm: No realm Authentication Protocol: HTTP Basic Exclude HTTP User-Agents: None

Zones Networks VLAN Tags Ports

Available Zones

- Inside_Zone
- Outside_Zone**
- DMZ_Zone

Add to Source Add to Destination

Source Zones (1): **Inside_Zone**

Destination Zones (1): **Outside_Zone**

Cancel Add

ةطشنلا ةقداصلما ةدعاق تادادعإ نيوكت

دع اوقلا رحم نمض تادادع اوقا طنل بي وبت لة مالع قوف رونا ،ةفاضل قوف رونا لبق (3)
 رونا مث ،ةقداصل لاقحك ةقباصل اواطخل ي ف هنيوكت مت يذل قاطنل رايخا نم دكا
 ةفاضل قوف

Add Rule

Name: Active Auth ID Rule ☒ Enabled Insert into Category: Standard Rules

Action: Active Authentication **Realm:** azure-entra-saml (S... **Authentication Protocol:** SAML **Exclude HTTP User-Agents:** None

Zones Networks VLAN Tags Ports [Realm & Settings](#)

Authentication Realm *
azure-entra-saml (SAML)

☐ Use passive identity if available.
Active identity realm is going to be used as a passive identity realm.

Authentication Protocol
SAML

▶ HTTP User Agent Exclusions

[Cancel](#) [Add](#)

ةي وه ل ةدع اق ل تاد ادع ا ل او قاطن ل ن ي و ك ت

ظ ف ح ق و ف ر ق ن ا . ا ه ن ي و ك ت و ة د ع ا ق ل ة ف ا ض ا م ت ت 4)

active-auth-id-policy

Identity Policy for Active Auth

Identity Mapping Filter: None [How it works](#)

[Rules](#) [Active Authentication](#)

[+ Add Category](#) [+ Add Rule](#)

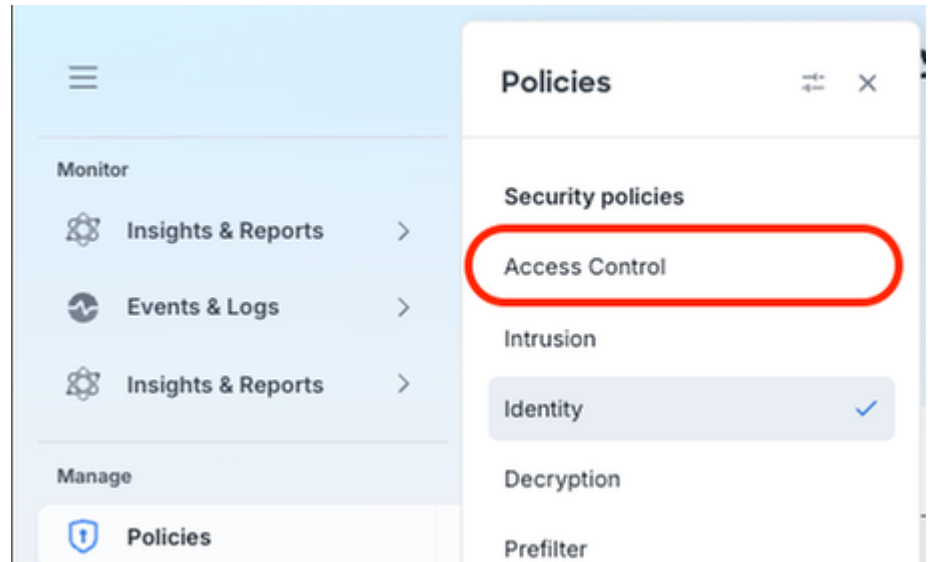
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Source Ports	Dest Ports	Realm	Action	Auth Protocol
Administrator Rules											
This category is empty											
Standard Rules											
1	Active Auth ID Rule	Inside_Zone (Ro	Outside_Zone (F	any	any	any	any	any	azure-entra-san	Active Authentication	SAML
Root Rules											
This category is empty											

[Save](#) [Cancel](#)

ةي وه ل ة س ا ي س ة د ع ا ق ن ي و ك ت ظ ف ح

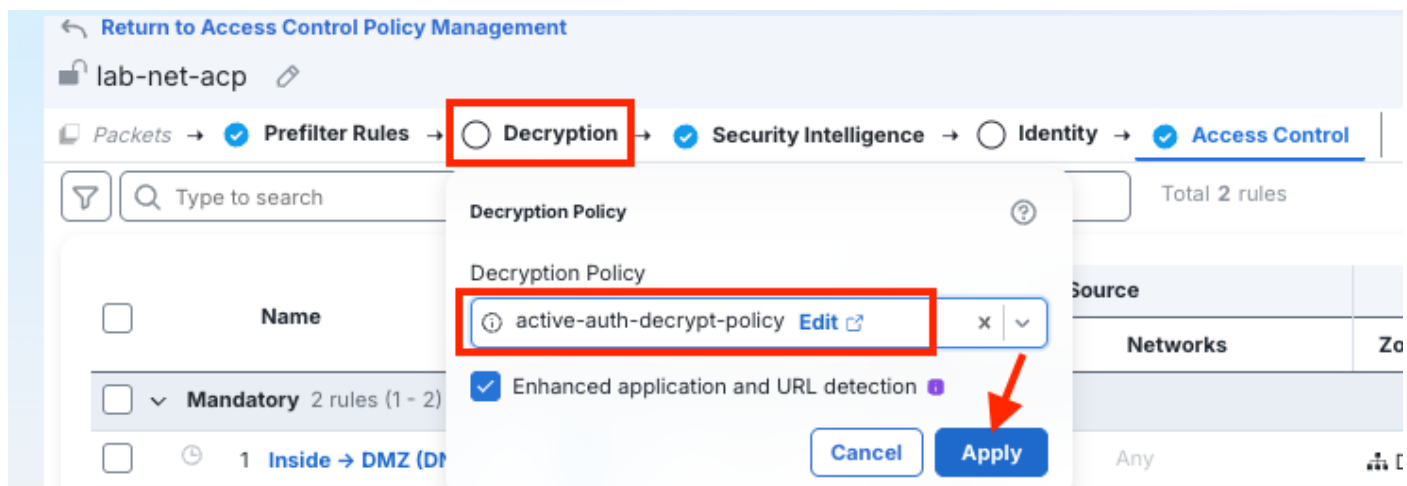
ل و ص و ل ا ي ف م ك ح ت ل ة س ا ي س ن ي و ك ت : 5 ة و ط خ ل ا

ي ف م ك ح ت ل ة س ا ي س ق و ف ر ق ن ا و ، ل و ص و ل ا ي ف م ك ح ت ل > ن ا م أ ل ا ت ا س ا ي س > ت ا س ا ي س ر ت خ أ 1)
ا ه ل F T D ن ي ي ع ت م ت ي ت ل ل و ص و ل ا



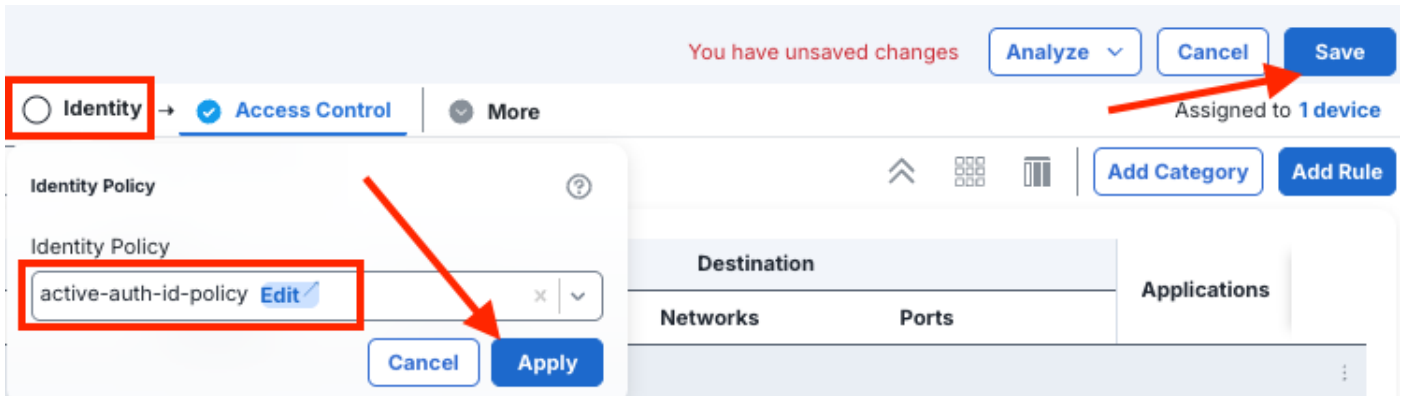
لوصول الى مكدحتال ةسايس نيوكت

2) لىل ةقباال تاوطخال في اهنىوكت متي تال ريفشتال ك ةسايس قيبطت نم دكأت 2) لوصول الى مكدحتال جن.



لوصول الى مكدحتال لىل ريفشتال ك ةسايس قيبطت

3) جن لىل اضيأ ةقباال تاوطخال في اهنىوكت متي تال ةيوهال ةسايس قيبطت نم دكأت 3) جهنال تاريغت ظفح. لوصول الى مكدحتال



لوصول اليف مكحتل الى عةوهال عسايس قيبطت

نمآل ةيامحل راج لال خ نم ليمعل تانايب يوتسم رورم ةكرحل حمست دعاوق دوجو نم دكأت 4) ةئيبي ف عسوأ دعاوق ةعومجم انه حضومل لاثمل مدختسي . ةحجانل ةطشنل ةقداصل مدعب لمعمل.

	Name	Action	Source		Destination			Applications
			Zones	Networks	Zones	Networks	Ports	
Mandatory 2 rules (1 - 2)								
1	Inside → DMZ (DNS)	Allow	Inside_Zone	Any	DMZ_Zone	Any	Application Default	DNS
2	DMZ-Inside → Outside	Allow	DMZ_Zone	Any	Outside_Zone	Any	Any	Any
Default (No rules)								

مدختسمل تانايب يوتسم رورم ةكرحل دعاوق ةعومجم

Cisco نم ةنمآل ةيامحل راج ةزهجأ الى تانايبوكتل رشن : 6 ةوطخل

مادختساب تانايب رورم ةكرحل لاسراب نوموقي نيذل عالعمل ةبلاطم متت ، رشنل درجمب Azure Entra مادختساب ةطشنل ةقداصل عارجل Microsoft الى لوخدل ليجستل بيو ةحفص

[Microsoft Azure AD قاطن عاشن](#) عجار ، انه ةقثومل ةيلمعل الى عةيفاضا قاييس الى لوصولل FMC 10.x زاهج نيوكت ليلد : لصفال - (ريسأ لخدم) ةطشنل ةقداصلل (SAML)

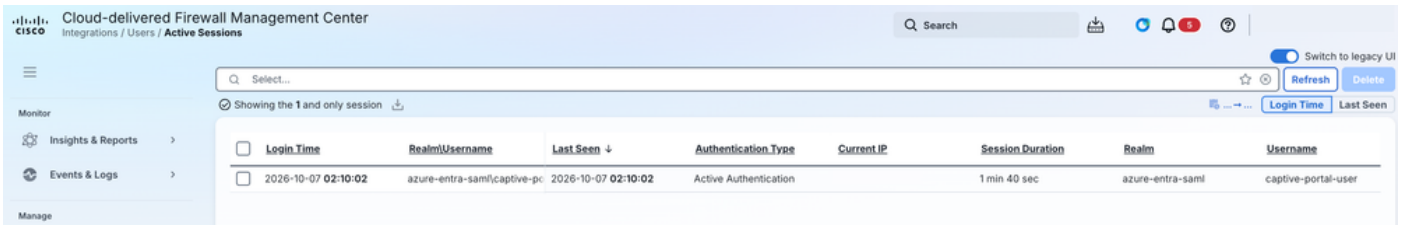
ةحصلال نم ققحتل

ححص لكشب لمعي نيوكتل نأ نم دكأتل يف ةدعاسملل مسقلل اذه مدختسأ

ةيموسرل مدختسمل ةهجاو

FMC: في طاشننل او مدختسمل لمع تاسلج ةحص نم ققحتلا

- ةطشنل لمعل تاسلج > نيمدختسمل > لمككتل تاي لمع رتخأ



☐	Login Time	Realm/Username	Last Seen ↓	Authentication Type	Current IP	Session Duration	Realm	Username
☐	2026-10-07 02:10:02	azure-entra-saml/captive-pc	2026-10-07 02:10:02	Active Authentication		1 min 40 sec	azure-entra-saml	captive-portal-user

FMC ل ةطشنل لمعل تاسلج جارخا

- .مدختسمل طاشن > نيمدختسمل > لمككتل تاي لمع رتخأ



☐	Time ↓	Username	Event	Realm	Discovery Application	Authentication Type	IP Address	Start Port
☐	2026-10-07 02:10:02	captive-portal-user	User Login	azure-entra-saml	Microsoft Azure	Active Authentication		
☐	2026-10-07 02:10:01	captive-portal-user	User Login	azure-entra-saml	Microsoft Azure	Active Authentication		

FMC مدختسمل طاشن جارخا

Microsoft Entra ةرادإ زكرم ىلإ لقتنا ، Azure في

- لباقلا قيبطتلا قوف رقن/نع ثحبا ، تاسسؤمل تاقيبطت ةيفصتب مق قيبطتلل

Microsoft Entra admin center

Home > Enterprise applications

Enterprise applications | All applications

Overview

- Overview
- Diagnose and solve problems

Manage

- All applications
- Private Network connectors
- User settings
- App launchers
- Custom authentication extensions

Security

- Conditional Access
- Consent and permissions
- Application policies

Home

Favorites

Entra ID

Overview

Users

Groups

Devices

Agents

Enterprise apps

App registrations

Roles & admins

Delegated admin partners

Tenant governance

Search resources, services

« + New application ↻ R

View, filter, and search applica

The list of applications that are

Search captive-

Name	↑↓	Obj
Captive-Auth...		efda

Enterprise تاقىبطت لقننت Azure Entra زكرمل

• لوخدلا ليجست تالچس > طاشن رتخأ

Home > Enterprise applications | All applications > Captive-Auth-SAML

Captive-Auth-SAML | Sign-in logs

Enterprise Application

«

Download

Export data Settings

Troubleshoot

Refresh

Manage view

Got feedback?

Diagnose and solve problems

Manage

Properties

Owners

Roles and administrators

Users and groups

Single sign-on

Provisioning

Self-service

Custom security attributes

Security

Conditional Access

Permissions

Token encryption

Activity

Sign-in logs

Usage & insights

Want to switch back to the legacy sign-in logs experience? Click here to leave the preview.

Add filter

Show dates as: UTC

Date range: 10/7/2026 - 10/7/2026

Application contains

User sign-ins (interactive)

User sign-ins (non-interactive)

Service principal sign-ins

Managed identity sign-ins

Date ↓	Request ID	User principal name	Application	Status
2026-10-07T06:10:02Z		captive-portal-user@...	Captive-Auth-SAML	Success
2026-10-07T06:10:01Z		captive-portal-user@...	Captive-Auth-SAML	Success
2026-10-07T06:10:01Z		captive-portal-user@...	Captive-Auth-SAML	Success
2026-10-07T06:10:00Z		captive-portal-user@...	Captive-Auth-SAML	Success
2026-10-07T06:09:59Z		captive-portal-user@...	Captive-Auth-SAML	Success
2026-10-07T06:09:58Z		captive-portal-user@...	Captive-Auth-SAML	Interrupted
2026-10-07T06:09:52Z		captive-portal-user@...	Captive-Auth-SAML	Success
2026-10-07T06:09:51Z		captive-portal-user@...	Captive-Auth-SAML	Interrupted
2026-10-07T06:09:29Z		captive-portal-user@...	Captive-Auth-SAML	Interrupted

Azure Enterprise قىببط لولخ لىجست طاشن تالچس

CLI

- ةقلىعتمل تاىئاصحلإا ةىؤر كنكمى (FTD) رماوالا رطس ةهجاو (CLI) رماوا رطس ةهجاو ىف فووقومل لخدملاو SAML لخدم تاباجتساب

<#root>

>

debug menu captive-portal 6

```
SAML passed requests captive-portal 14
SAML failed requests captive-portal 0
SAML passed responses captive-portal 4
SAML failed responses captive-portal 0
Total captive-portal bee-client messages processed 4
Total captive-portal bee-client messages successful 4
Total captive-portal bee-client messages failed 0
Total bee-client reconnects 0
```

اهال صإو اءاطخأل فاشكسا

ديقمال ةبوابل اءاطخأ حيحصت

- جارخال حضوي FTD ىل ع system support captive-portal-debug رمال مادختسا نكمي
ف ةدعاسملل جارخال ةيساسأل اءالاضى اءال وءاطخأل حيحصت نيكم ةيفي
نمضمال لخدمال قفدت مهف

<#root>

>

system support captive-portal-debug

Enable firewall-debug too? [n]:

y

Enable identity-debug too? [n]:

y

Please specify an IP protocol:

tcp

Please specify a client IP address:

192.168.20.200

Please specify a client port:

Please specify a server IP address:

Please specify a server port:

Enable daq-debug too? (WARNING: current packet debug configs and logs will be overwritten) [n]:

Monitoring captive_portal and firewall and identity debug messages

!---

Baseline output pending user Captive Portal authentication

...

192.168.20.200 53650 -> 198.51.100.1 443 6 AS=0 ID=1 GR=1-1 match rule order 1, id 1 action Captive por

192.168.20.200 53650 -> 198.51.100.1 443 6 AS=0 ID=1 GR=1-1 didn't find active binding, initiating capt

192.168.20.200 53650 -> 198.51.100.1 443 6 AS=0 ID=1 GR=1-1 captive portal authentication started

192.168.20.200 53650 -> 198.51.100.1 443 6 AS=0 ID=1 GR=1-1 defer trust until captive portal redirect i

192.168.20.200 53650 -> 198.51.100.1 443 6 AS=0 ID=1 GR=1-1 Current state = S_INIT, Event = EVT_CP_RULE

...

!---

Captive Portal probe intercepted and redirected to SAML IdP (generate_204)

```

...
192.168.20.200 53659 -> 198.51.100.2 80 6 AS=0 ID=1 GR=1-1 AppID session with service_id: 676, url: http
192.168.20.200 53659 -> 198.51.100.2 80 6 AS=0 ID=1 GR=1-1 Current state = S_PENDING_USER, Event = EVT_
192.168.20.200 53659 -> 198.51.100.2 80 6 AS=0 ID=1 GR=1-1 app event changes: service, client, host, ur
192.168.20.200 53659 -> 198.51.100.2 80 6 AS=0 ID=1 GR=1-1 using ipv4 address 192.168.20.1 for redirect
192.168.20.200 53659 -> 198.51.100.2 80 6 AS=0 ID=1 GR=1-1 encrypted redirect url: https://ftd-inside.e
192.168.20.200 53659 -> 198.51.100.2 80 6 AS=0 ID=1 GR=1-1 Current state = S_REDIRECTING, Event = EVT_F
...
!---

SAML authentication completes, identity binding created

...

192.168.20.200 54023 -> 198.51.100.2 80 6 AS=0 ID=2 GR=1-1 looked for user_id with realm_id 2 auth_type
192.168.20.200 54023 -> 198.51.100.280 6 AS=0 ID=2 GR=1-1 found active binding for user_id 0 usernames
192.168.20.200 54023 -> 198.51.100.2 80 6 AS=0 ID=2 GR=1-1 IdentityFlowSetupEventHandler Retrieved iden
192.168.20.200 54023 -> 198.51.100.2 80 6 AS=0 ID=2 GR=1-1 New firewall session
192.168.20.200 54023 -> 198.51.100.2 80 6 AS=0 ID=2 GR=1-1 allow action
...
!---

Authenticated binding persists across subsequent, unrelated destinations (no further redirects)

...

192.168.20.200 54024 -> 198.51.100.2 80 6 AS=0 ID=2 GR=1-1 found active binding for user_id 0 usernames
192.168.20.200 54025 -> 198.51.100.1 443 6 AS=0 ID=1 GR=1-1 found active binding for user_id 0 usernam
192.168.20.200 54026 -> 198.51.100.2 80 6 AS=0 ID=1 GR=1-1 found active binding for user_id 0 usernam
192.168.20.200 54027 -> 198.51.100.3 443 6 AS=0 ID=1 GR=1-1 found active binding for user_id 0 usernam
192.168.20.200 19935 -> 198.51.100.4 443 6 AS=0 ID=1 GR=1-1 found active binding for user_id 0 usernam
...

```

مدخستسمال ةي وه غي رقت

- system رمأل ل غش تب مق FTD، ل ع ةي لال ال مدخستسمال ةي وه ةل ا تاناي بل ة ط ق ل ذأل
ب ة صاأل (CLI) رماوأل رطس ةه جاو ل ع support firewall-engine-dump-user-identity-data
FTD:

```
> system support firewall-engine-dump-user-identity-data
```

```
Successfully commanded snort.
```

>

- تانايب مادختساب لوخدلا ليچست ءانثأ، ريبلخال عضو في (CLI) رماوأل رطس ةهجاو في في لمهمال فلملا تايوتحم ضرعا، FTD زاهجل يلحمل لوؤسملا دامتعا /ngfw/var/sf/user_enforcement/user_identity.dump

<#root>

>

expert

admin@ftd:~\$

sudo su

Password:

root@ftd:/home/admin#

root@ftd:/home/admin#

ls -lah /ngfw/var/sf/user_enforcement/user_identity.dump

-rw----- 1 root root 5.6K Oct 7 07:51 /ngfw/var/sf/user_enforcement/user_identity.dump

root@ftd:/home/admin#

root@ftd:/home/admin#

less /ngfw/var/sf/user_enforcement/user_identity.dump

...

IP:USER

!--- Host IP is aligned with the user authenticated via Captive Portal/Active Authentication

Host ::ffff:192.168.20.200

::ffff:192.168.20.200:0 realm 2 type 8, username azure-entra-saml\captive-portal-user@onmicrosoft.example

::ffff:192.168.20.200: SXP initialized 0 sgt 0

ABP values: None

SXP MAPPING:

...

ةلمتحملا اياضقلا

رسأل في دوجوم للخدمة فورع ريغ تاداهش عطلس

عقداصم للوادم دنع فورع ريغ ردصم أطخ عاجراب ليمعلا ضرعتسم موقوي: لكشملا

ليمعلا ضرعتسم لخاد هب قووم ريغ يلخادلا قدصملا عجرملا: لمحمل ببسلا

نأ انه رهاظلا لاثملا دكؤي. ضرعتسملا لخاد هب قووم قدصملا عجرملا نأ نم دكأت: قدلا
اهب قووم يلخادلا CA عدهاش

مداخللا لعل روثعلا متي مل عديقملا عباوبلا

ريغ مداخللا "عجري هناف، عديقملا عباوبلا ليمحت ليمعلا ضرعتسم لواحي ام دنع: لكشملا
هباش ام وأيساسلا URL لىل لوصوللا لواحم ءانثأ يساسلا URL ناونعل "دوجوم

ححص ريغ DNS نيوكت وأ DNS لىل لوصوللا ةيناكم: لمحمل ببسلا

نم دكأت A. لجسلا لحل هنيوكت مت يذلا بسانملا DNS مداخل هيدل ليمعلا نأ نم دكأت: قدلا
عجاتسالا لوصوللا لباق هناف أو FQDN لعل هنييعة مت لجس هيدل مداخل نأ

قلمص تاذا تامولعم

- [ليلد - \(ريسا لخدم\) عطشنلا عقداصم لل Microsoft Azure AD \(SAML\) قاطن ءاشن](#)
- [FMC 10.x زاهج نيوكت](#)
- [Azure Event Hub قئاثو](#)
- [Cisco Systems - تادنتسملا وينقتلا معدلا](#)

ةمچرتل هذه ل و ح

ةيلآل ا تاي 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 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 ا و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ 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