

يلع ةقث نود دعب نع لوصولا رشن نيوكت نمآلة ةيامحل راج

تايوتحمل

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسأ تامولعم](#)

[نيوكتلا](#)

[ةكبش ليل طي طختلا مسرلا](#)

[يساسأ بيلطتم نيوكت](#)

[ةمعاللة ةيسهتلا تايلمع](#)

[تاقى بيلطتملا ةعومجم نيوكت](#)

[ك IDP duo مادختسا: 1 تاقى بيلطتملا ةعومجم](#)

[فرعمك Microsoft Entra \(Azure AD\) فرعم مادختسا: 2 تاقى بيلطتملا ةعومجم](#)

[تاقى بيلطتملا نيوكت](#)

[1 تاقى بيلطتملا ةعومجم يف وضع FMC بيو مدختسم ةهجاو رابتخا: 1 تاقى بيلطتملا](#)

[2 تاقى بيلطتملا ةعومجم يف وضع CTB بيو مدختسم ةهجاو: 2 تاقى بيلطتملا](#)

[ةحصلا نم ققحتلا](#)

[ةشاشلا](#)

[اهجالص او عا طخألا فاشكتسا](#)

[ةلص تاذا تامولعم](#)

ةمدقملا

راج يلع Zero Trust يل ةقث نودب دعب نع لوصولا رشن نيوكت ةيلمع دنتسملا اذه فصوي نمآة ةيامح.

ةيساسألا تابلطتملا

تابلطتملا

ةيلاتلا عيضاوملاب ةفرعم كي دل نوكت ناب Cisco ي صوت:

- Firepower (FMC) ةرادا زكرم
- ةيساسألا ZTNA ةفرعم
- (SAML) ةيساسألا نامألا دي كأت زييمت ةغل ةفرعم

ةمدختسملا تانوكملا

قيبطت الالكلذب ةصاخال SNI عم رقص ةقثال قيبطت نيوكتل يچراخال

- هجولم اعضولا ي ف طقف موعدم
- (مبيقتل اعضو ي ف لمعي ال) ي كذ صيخرت رفوت مزلي

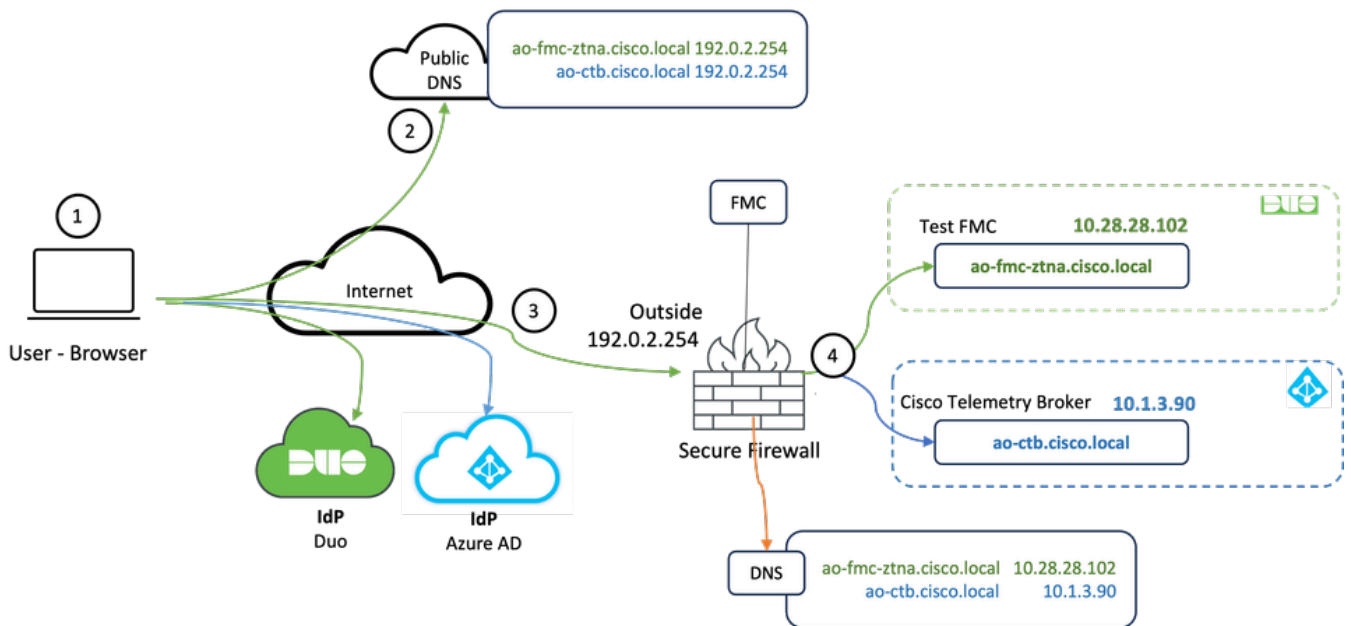
ةيماحل اراج ي ف ةقث نوب لوصول لوج ليصافتل او تامولعملال نم ديزم يلعل لوصول
7.4 رادصال Cisco نم نمالا ةيماحل اراج قرادا زكرم زاخ نيوكتل ليلا ل ا عجرا، نمالا

نيوكتل

ZTNA ل "دعب نع لوصول" رشن يلعل دنننسمال اذه زكري

(UI) بيولم مدختسم تاهجاو يل لوصول نيديعبال نومدختسمال بلطتي، ويرانيسلال اذه ي
اهتفاضتسا مبي يتل Cisco (CTB) تانايب عبتت تانايب طيسوو FMC رابتاب ةصاخال
Duo: ني فلل تخم ني فرعم ةطساوب تاقيبطتال هذه يل لوصول حنم مبي. نم ةيماحل اراج فلخ
يلال ططخمال ي ف حضورم وه امك، يللاوتل يلعل Microsoft Entra ID و

ةكبشلل يطيختل مسرلا



ايچولوبوطال ططخم

1. راج فلخ ةفاضتسمال تاقيبطتال يل لوصول نيديعبال نومدختسمال اجاتحي
نمالا ةيماحل
2. ةماعال DNS مداخي ي ف DNS ل اخل يلعل قيبطت لك يوتحي نأ بچي.
3. ةيچراخال نمالا ةيماحل اراج ههجاوب صاخال IP ناوع يل هذه تاقيبطتال عامسا ل بچي.
4. مدختسم لك قداصي و تاقيبطتال ل ل قيقحل IP نيوانع يل نمالا ةيماحل اراج ل مبي
SAML ةقداصم مادختساب قيبطت لك يلعل

يساسا بلطتم نيوكتل

(DNS) ل اجمال مسامداخو (IDp) ةيوهال رفوم

- Duo لثم SAML (IDp) ةيوه رفوم ي ف تاقىببطلتال تاعومجم و ا تاقىببطلتال نيوكت بچي .تافرع مك Microsoft Entra فرعمو Duo مادختسا متي ،لاثلما اذه ي ف Azure AD و OKTA و نيوكت دنع IdPs ةطساوب اهواشن ا مت ي تال ف ي رعتال تانايب و ةداهشال مادختسا متي نم آال ةيامحل رادج ىلع قىببطلتال

ةيخرال او ةيلخادال DNS مداوخ

- لاد ا ىلع (دعب نع نومدختسمل ا هم دختسي ي تال) ةيخرال DNS مداوخ يوتحت ن ا بچي ةهجاو لل IP ناو نع چراخ نم آال ةيامحل رادج ىل لحت ن او ، تاقىببطلتال صاخال FQDN لاد ا ىلع (نم آال ةيامحل رادج لبق نم ةمدختسمل) ةيلخادال DNS مداوخ يوتحت ن ا بچي قىببطلتال قىقيلل IP ناو نع ىل لحت ن او ، تاقىببطلتال صاخال FQDN

تاداهشال

ZTNA: جهن نيوكتل ةبولطم ةيلتال تاداهشال

- تاقىببطلتال عيملتال نم آال ةيامحل رادج ةطساوب مدختست :ليكول/ةيوهال ةداهش ل دب فرح ةداهشال هذه نوكت ن ا بچي . SAML (SP) ةمدخ رفومك انه نم آال ةيامحل رادج لمعي ةداهش) ةصاخال تاقىببطلتال FQDN قباطت (SAN) عوضوملل لي دب مسا ةداهش و (ةقداصملا لبق ام ةلحرم ي ف ةصاخال تاقىببطلتال عيملتال ةكرتشم قىببطلتال ةعومجم و ا قىببطلتال ل كل ةداهش ةقداصملا مدختسمل فرعمال رفوي IDP: ةداهش ةيامحل رادج نيما متي ىتحت ةداهشال هذه نيوكت بچي . ةفرعم ةعومجم اذه فيرعت مت اذا) ةراوال SAML تاديكات ىلع IDP عيقتو نم ققحتال نكمي (اهل مك ا ب تاقىببطلتال ةعومجم ل ةداهشال س فن مادختسا متي ، تاقىببطلتال مدختسمل نم ةرفشمال تانايبال رورم ةكرح ريفشت ك ف مزلي : قىببطلتال ةداهش ةلسلس ةفاضا بچي ، يلاتلابو ، نم آال ةيامحل رادج ةطساوب قىببطلتال ىل ديعلال نم آال ةيامحل رادج ىل قىببطلتال ل كل صاخال حاتفملاو تاداهشال

ةماعال ةئيهتال تاي لمع

ةيلتال تاوطخال ذي فننتب مق ، ديدج ةيرفص ةقت قىببطلتال نيوكتل:

1. قوف رقاو ةقتال مادعنا قىببطلتال > لوصول ي ف مكحتال > تاسايسال ىل لقتنا . ةسايس ةفاضا
2. ةبولطملا لوقحال لمك أ:

ةسايسال فصولو مسا لخدأ :ماع أ)

عافدل ةرابع ةهجاو ىل هلح بچي و DNS ىل هتفاضا متت يذل مسالا وه اذه : لاجملا مسا ب) . تاقىببطلتال ىل لوصول متي شيح نم ديدتال نع

 تاقىببطلتال عيملتال ACS ل URL ناو نع ءاشنال لاجملا مسا مادختسا متي : ةظحال تاقىببطلتال ةعومجم ي ف ةصاخال

لبق ام ةلحرم يف ةصاخلا تاقببطلال عيجم لثمت ةماع ةداهش هذه :ةيوهلا ةداهش ج) ةقداصملا.

يتلا (SAN) ليدبلا عوضوملا مسا ةداهش وأ لدب فرح ةداهشلا هذه نوكت نأ بجي :ةظالم ةصاخلا تاقببطلالاب صاخلا FQDN قباطت

ميظنت اهلالخ نم متي يتلا لخال و /أو هيخراخلا قطانملا رايخا :ةينملا قطانملا د) ةصاخلا تاقببطلال

صاخ قيببطلال لكل عمجتلا اذه نم ديرف ذفنم صيصخت متي :ةيملال ذفانملا عمجت ه)

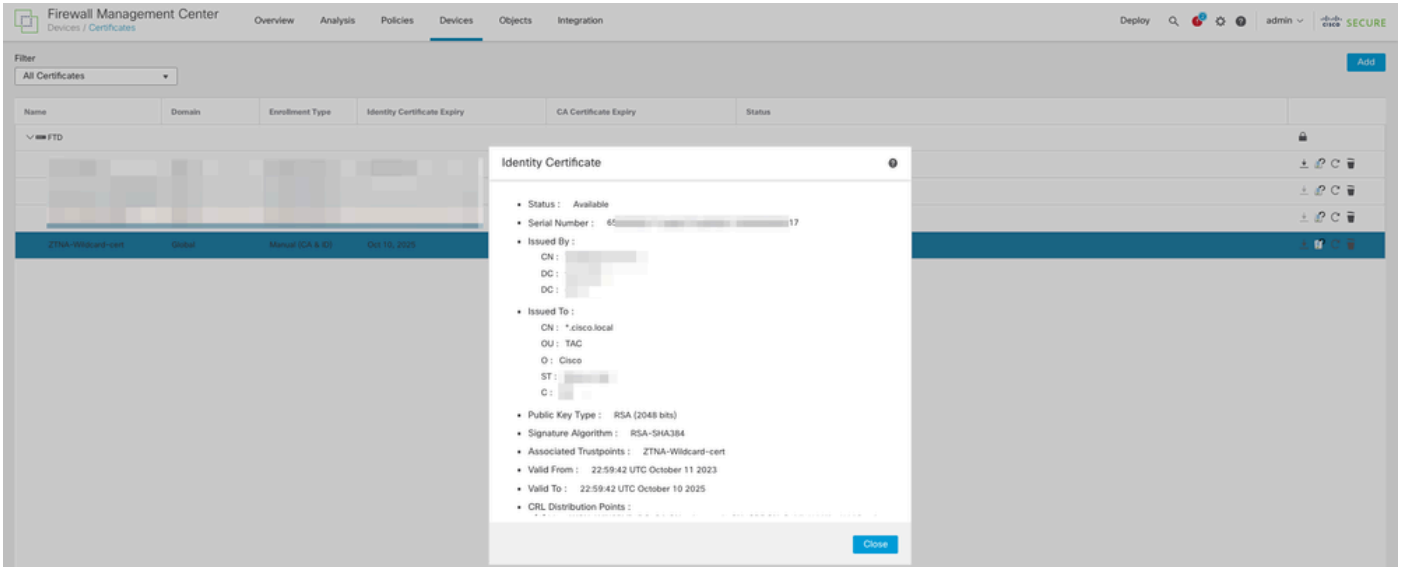
عضخت ةصاخلا تاقببطلال تناك اذا ام ددح:(يرايخا) نيملتال مكحت رصانع و) شيتفتلل

ةيلاتل تامولعملال لخال مت ، اذه نيوكتلال جذومن يف

The screenshot shows the 'Add a Zero Trust Application Policy' configuration page in the Firewall Management Center. The page is divided into several sections:

- General:** Name* (ZTNA-TAG), Description.
- Domain Name:** Domain Name* (with a note: 'Ensure that the domain name is added to the DNS. The domain name resolves to the threat defense gateway interface from where the application is accessed. The domain name is used to generate the ACS URL for all private applications in an Application Group.')
- Identity Certificate:** Certificate* (ZTNA-Wildcard-cert, with a note: 'This certificate must be a wildcard or Subject Alternative Name (SAN) certificate that matches the FQDN of the private applications.')
- Security Zones:** Security Zones* (Outside, with a note: 'This is the default setting for all private applications. It can be overridden at an Application or Application Group level.')
- Global Port Pool:** Port Range* (20000-22000, Range: {1024-65535}, with a note: 'Ensure a sufficient range is provided to accommodate all private applications. Do not share these ports in NAT or other configurations.')
- Security Controls (Optional):** Intrusion Policy (None), Variable Set (None), Malware and File Policy (None, with a note: 'These are default settings for all private applications. It can be overridden at an Application or Application Group level.')

FQDN ةقباطملا لدب فرح ةداهش يه ةلخال هذه يف ةمدختسملا ليكول/ةيوهلا ةداهش ةصاخلا تاقببطلال



3. ةسايس لظافح.

4. ةديج تاقيبطت وأ/و ةديج تاقيبطت تاعومجم ءاشناب مق:

- ةهجاو لا لوصول او SAML ةقداصم هب صاخ بي و قيبطت تاقيبطت ل دحأ ددحي تافل ل تاسايس و ةراض ل امارب ل لاصلت او.
- ةكرتشم تادادع اكراشم و ةددعتم تاقيبطت عيمجتب تاقيبطت ل ةعومجم كل حمست نام ال ي فم كحتل تادادع او ةهجاو لا لوصول او SAML ةقداصم لثم.

امه دحأ: نيفل لتخم ني قيبطت و ني فلتخم تاقيبطت يت عومجم ني وكت مت، لاثم لا اذه ي دارم ل قيبطت ل ل رخال او (FMC Web UI رابتخا) Duo ةطساوب هتقداصم دارم ل قيبطت ل ل Microsoft Entra (CTB Web UI) فرعم ةطساوب هتقداصم.

تاقيبطت ل ةعومجم ني وكت

IDP ك duo مادختسا: 1 تاقيبطت ل ةعومجم

SAML (SP) ةمدخ رفوم فيرعت تانايب ل ل قوف رقاو تاقيبطت ل ةعومجم مسا لخدأ أ. اهضرع بولطم ل.

Add Application Group



An Application Group allows you to group multiple Applications and share authentication, security zone, and threat configurations.

1 Application Group

Name External_Duo

Edit

2 SAML Service Provider (SP) Metadata

The service provider's metadata for the Application Group are dynamically generated and cannot be modified. Copy or download the SP metadata file as required for use in your IdP.

Entity ID

https://.../External_Duo/saml/sp/metadata

Copy

Assertion Consumer Service (ACS) URL

https://.../External_Duo/+CSCOE+/saml/sp/acs?tgname=

Copy

Download SP Metadata

Next

3 SAML Identity Provider (IdP) Metadata

4 Re-Authentication Interval

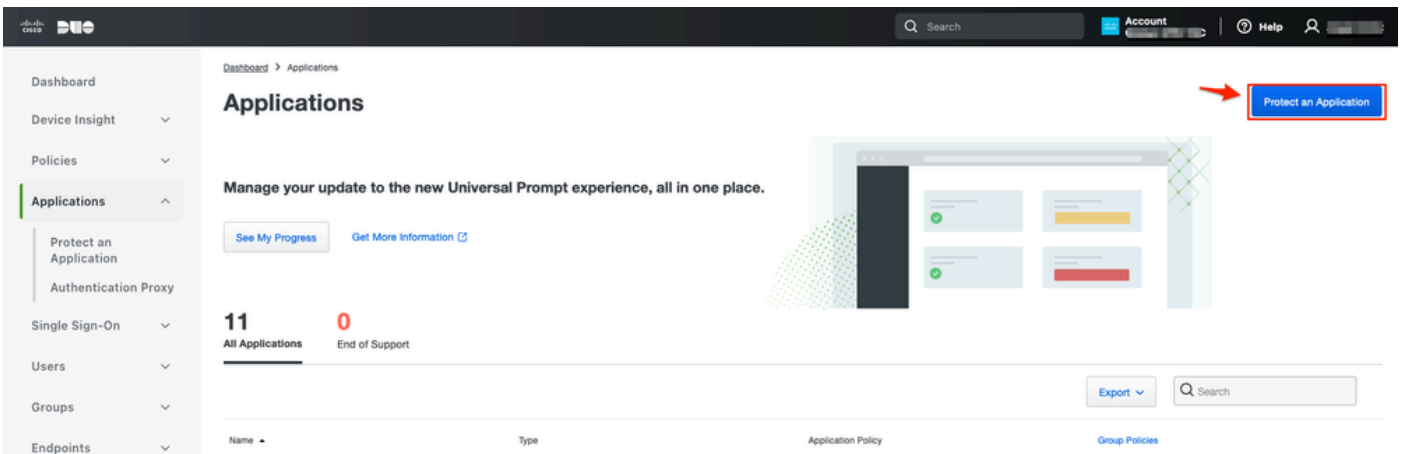
5 Security Zones and Security Controls

Cancel

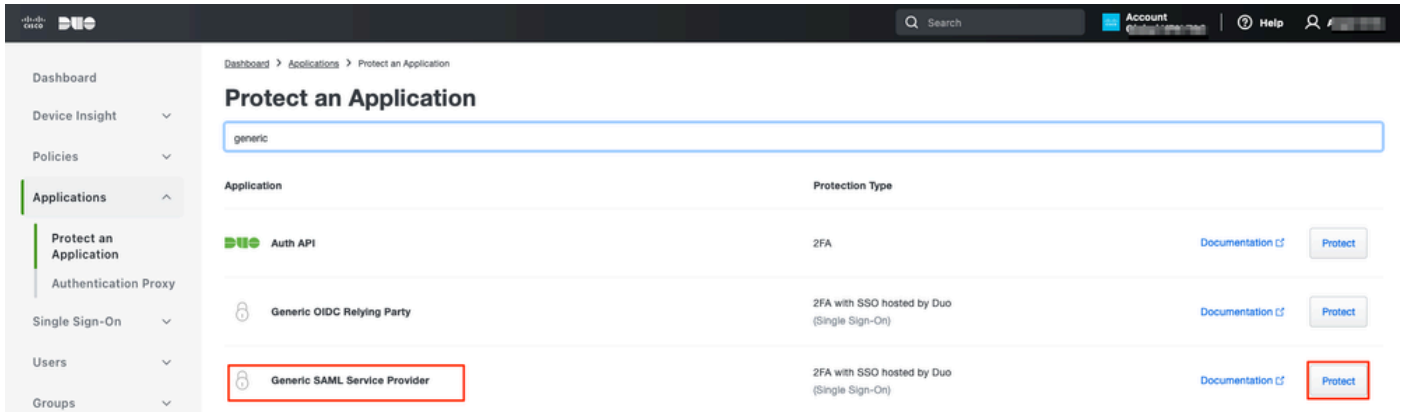
Finish

ب. قېبېت سAML SSO قېبېت نېوكېتې م قو IdP ىل لقتنا، SAML SP فيرعت تانا ب ضرع درج م ب. دى دى.

ج. قېبېت ةي امح > تاقېبېت ىل لقتنا و ةيئانثلا ىل لوخدلا ل ج س.



د. ة.امح قوف رقناو ماع SAML ةمدخ رفوم نع ثحبا .



ه. رادج ىلع نيوكتللا ةعباتمل بولطم وه امك IDp نم SAML فيرعت تانايبو ةداهشلا ليزنت .

ف. تاقيبطت ةومجم نم (ACS) ةدكؤملا ءالمعلا ةمدخو نايلكلا فرعم ب صاخلا URL ناو نع لخدأ .

(A) ةوطخلال يف اهؤاشنإ مت (ZTNA).

Generic SAML Service Provider - Single Sign-On 1

See the [Generic SSO documentation](#) to integrate Duo into your SAML-enabled service provider.

Metadata

Entity ID	<input type="text" value="https://sso-.../metadata"/>	Copy
Single Sign-On URL	<input type="text" value="https://sso-8.../sso"/>	Copy
Single Log-Out URL	<input type="text" value="https://sso-i.../slo"/>	Copy
Metadata URL	<input type="text" value="https://sso-8.../metadata"/>	Copy

Certificate Fingerprints

SHA-1 Fingerprint	<input type="text" value="9E:5...5C"/>	Copy
SHA-256 Fingerprint	<input type="text" value="7:85:...E9:52"/>	Copy

Downloads

Certificate	Download certificate	Expires: 01-19-2038
SAML Metadata	Download XML	

Service Provider

Metadata Discovery

[Early Access](#)

Entity ID *

The unique identifier of the service provider.

Assertion Consumer Service (ACS) URL *

[+ Add an ACS URL](#)

- Dashboard
- Device Insight
- Policies
- Applications**
- Protect an Application
- Authentication Proxy
- Single Sign-On
- Users
- Groups
- Endpoints
- 2FA Devices
- Administrators
- Trusted Endpoints
- Trust Monitor
- Reports
- Settings
- Billing

You're using the new Admin Panel menu and left-side navigation.

- [Provide feedback](#)
- [Temporarily switch to the old experience](#)

قېبىتلىلى لىل لوصول قىچىنم اۇە صاخلا كىتابلىلىم لاقى قىبىتلىلى رىرتىب قىز. ظفح قوف رقىن او طقف نىدوص قىم لى نىمدىختىم لىل

Type Generic SAML Service Provider - Single Sign-On

Name **External Applications ZTNA**
Duo Push users will see this when approving transactions.

Self-service portal Let users remove devices, add new devices, and reactivate Duo Mobile
See [Self-Service Portal documentation](#).
To allow Duo to notify users about self-service portal activity, select [Settings > Notifications](#)

Username normalization Username normalization for Single-Sign On applications is controlled by the enabled authentication source. Please visit your [authentication source](#) to modify this configuration.
Controls if a username should be altered before trying to match them with a Duo user account.

Voice greeting
Specify the message read to users who use phone callback, followed by authentication instructions. Maximum 512 characters.

Notes
For internal use. Maximum 512 characters.

Administrative unit

Permitted groups Only allow authentication from users in certain groups

When unchecked, all users can authenticate to this application.

Allowed Hostnames Since this application is using Frameless Duo Universal Prompt, configuring allowed hostnames is no longer supported.
[Get more information](#)

h. ،تاقىبطت الة عومجم الى SAML IDp فى رعت تاناىب فضاؤ FMC الى لى رةم لقتنا .
IdP. نم اهل يزنت مت لى تال تافل مل مادختساب

An Application Group allows you to group multiple Applications and share authentication, security zone, and threat configurations.

1 Application Group Edit

Name External_Duo

2 SAML Service Provider (SP) Metadata Edit

Entity ID https://[redacted]External_Duo/saml/sp/metadata
Assertion Consumer Service (ACS) URL https://[redacted]External_Duo/+CSCOE+/saml/sp/acs?tname=D...

3 SAML Identity Provider (IdP) Metadata

Import or enter the IdP metadata. If IdP metadata is not currently available, you can skip this step and configure it later.

- Import IdP Metadata
- Manual Configuration
- Configure Later

Import IdP Metadata

Drag and drop your file here
[or select file](#)
External Applications ZTNA - IDP Metadata.xml

Entity ID*

https://sso-8[redacted] N

Single Sign-On URL*

https://sso-8[redacted] N

IdP Certificate

MIIDDTC[redacted]yDQYJKoZI
[redacted]
[redacted]
[redacted]

Next

Cancel

Finish

عجارتا بلطتمل اقبط مكحت نم أول صاف reauthentication ل تل كشو كلذ دعب تقطوط. انأ
ءاهن قوف رقناو صللم لا نيوكت.

Add Application Group



An Application Group allows you to group multiple Applications and share authentication, security zone, and threat configurations.

1	Application Group	Name	External_Duo	Edit
2	SAML Service Provider (SP) Metadata	Entity ID	https://[redacted] External_Duo/saml/sp/metadata	Edit
		Assertion Consumer Service (ACS) URL	https://[redacted] External_Duo/+CSCOE+/saml/sp/acs?tgname=D...	
3	SAML Identity Provider (IdP) Metadata	Entity ID	https://ssc [redacted]	Edit
		Single Sign-On URL	https://ssc [redacted]	
		IdP Certificate	External_Duo-1697063490514	
4	Re-Authentication Interval	Timeout Interval	1440 minutes	Edit
5	Security Zones and Security Controls	Security Zones	Inherited: (Outside)	Edit
		Intrusion Policy	Inherited: (None)	
		Variable Set	Inherited: (None)	
		Malware and File Policy	Inherited: (None)	

Cancel

Finish

فرعك Microsoft Entra (Azure AD) فرع م ادخ تس | 2: تاق ي ب ط ل ا ة و م ج م

ة م د خ ر ف و م ف ي ر ع ت ت ا ن ا ي ب ل ي ل ا ت ل ا ق و ف ر ق ن ا و ت ا ق ي ب ط ل ا ة و م ج م م س ا ل خ د ا . أ . ا ه ض ر ع ب و ل ط م ل ا

Add Application Group



An Application Group allows you to group multiple Applications and share authentication, security zone, and threat configurations.

- Application Group** Edit
Name: **Azure_apps**
- SAML Service Provider (SP) Metadata**
The service provider's metadata for the Application Group are dynamically generated and cannot be modified. Copy or download the SP metadata file as required for use in your IdP.
Entity ID: `https://[redacted]/Azure_apps/saml/sp/metadata` Copy
Assertion Consumer Service (ACS) URL: `https://[redacted]/Azure_apps/+CSCOE+/saml/sp/acs?tname=[redacted]` Copy
Download SP Metadata Next
- SAML Identity Provider (IdP) Metadata**
- Re-Authentication Interval**
- Security Zones and Security Controls**

Cancel

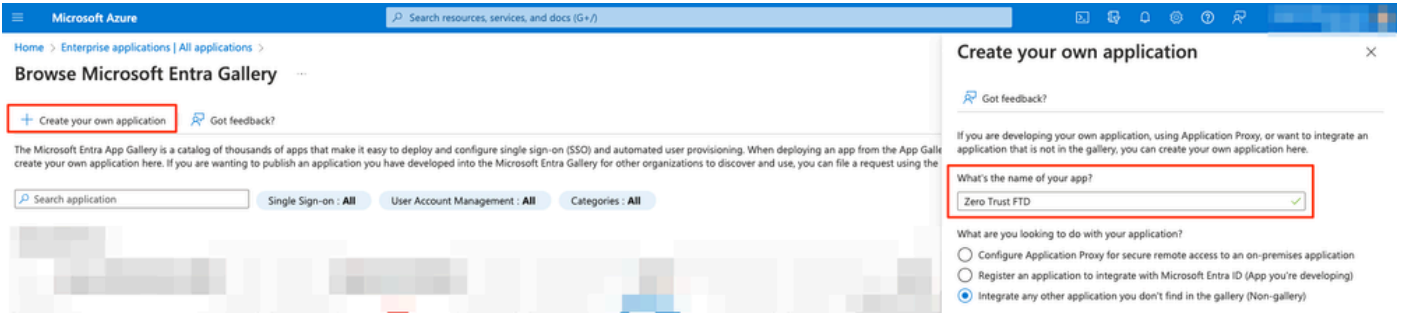
Finish

ب. ڊيڊج SAML SSO قىيىبىت نىيوىك تىب مقو IdP لىلى لقتنا ، SAML SP فىرعت تاناىب ضرع درجم ب. ڊيڊج.

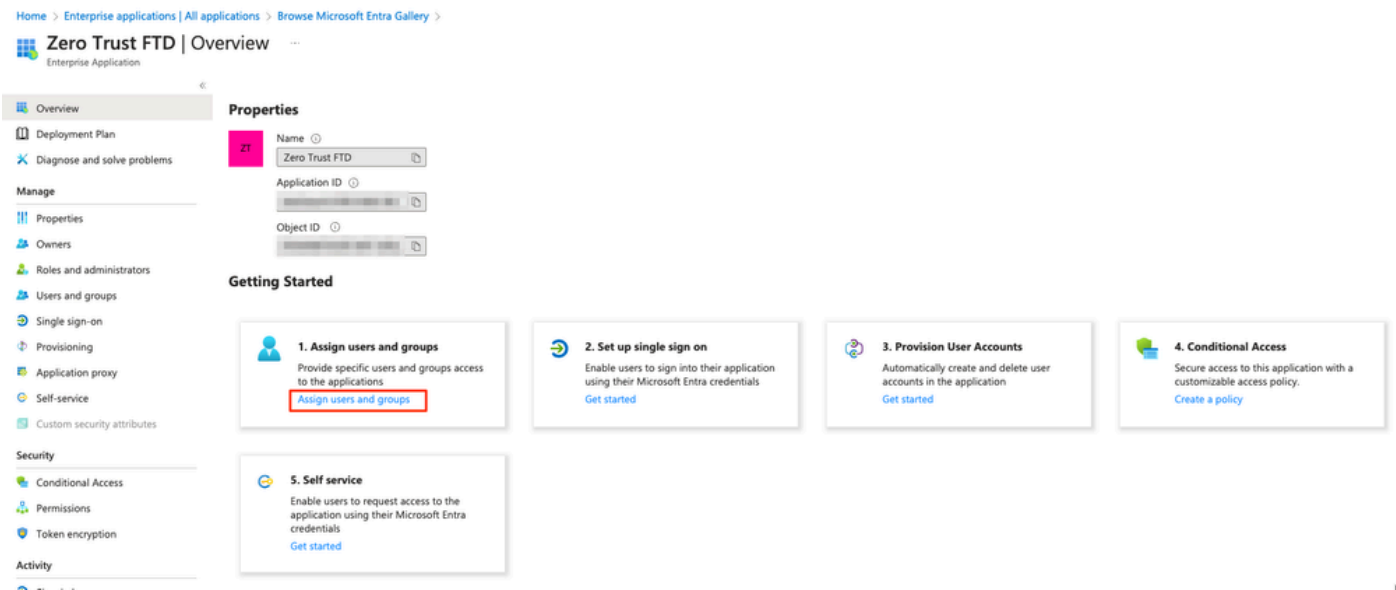
ڊيڊج قىيىبىت Enterprise > تاقىيىبىت لىلى لقتناو Microsoft Azure لىلى لوخذلا لچس ج.

The screenshot shows the Microsoft Azure portal interface for managing Enterprise applications. The top navigation bar includes the Microsoft Azure logo and a search bar. The main heading is "Enterprise applications | All applications". Below this, there are several action buttons: "+ New application" (highlighted with a red box), "Refresh", "Download (Export)", "Preview info", "Columns", "Preview features", and "Got feedback?". The left sidebar contains a navigation menu with "Overview" and "Manage" sections. Under "Manage", "All applications" is highlighted with a red box. The main content area displays a list of 77 applications found, with columns for Name, Object ID, Application ID, Homepage URL, and Created on. The "Application type" filter is set to "Enterprise Applications".

د. عاشن | > قيبطتال مسال خدأ > صاخلال كقيبطت عاشن | قوف رقنا .د



ه. وأو ني مدختسالم في رعتل تاعومجم وني مدختسم ني عت قوف رقنا و قيبطتال حتفا .ه
قيبطتال إلى لوصولاب اهل حومسالم تاعومجمالم



ن. ني عت > ة رورضال تاعومجمالم/ني مدختسالمال دي دحت > ةومجم/مدختسم ةفاضل قوف رقنا .و
يدألال لوخدلال ليجست قوف رقنا ، ةحاصلال تاعومجمالم/ني مدختسالمال ني عت درجمب

Zero Trust FTD | Users and groups

Enterprise Application

Overview
Deployment Plan
Diagnose and solve problems

Manage

Properties
Owners
Roles and administrators
Users and groups
Single sign-on

+ Add user/group 1

Edit assignment Remove Update credentials Columns Got feedback?

The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this. →

Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the [application registration](#).

First 200 shown, to search all users & gro...

Display Name	Object Type
<input type="checkbox"/> AO Angel	
<input type="checkbox"/> FG Fernando	

g. SAML على رقمنا، يداحألا لوخدلا ليحست مسق في فدحاو ةرم.

Zero Trust FTD | Single sign-on

Enterprise Application

Overview
Deployment Plan
Diagnose and solve problems

Manage

Properties
Owners
Roles and administrators
Users and groups
Single sign-on
Provisioning
Application proxy

Select a single sign-on method [Help me decide](#)

Single sign-on (SSO) adds security and convenience when users sign on to applications in Microsoft Entra ID by enabling a user in your organization to sign in to every application they use with only one account. Once the user logs into an application, that credential is used for all the other applications they need access to. [Learn more](#).

Disabled
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Password-based
Password storage and replay using a web browser extension or mobile app.

رادج) ةمدخلا دوزم نم هليزنت مت يذلا XML فلم ددحو فيرعتلا تانايب فلم ليحت قوف رقنا نم (ACS) ةدكؤملا كلهتسملا ةمدخل URL ناونعو ةدحول فرعم ايودي لخدأ وأ (نمآلا ةياملال A) ةوطخلال في اهؤاشنإ مت (ZTNA) تاقيبطت ةعومجم

يدرف لكشب ةداهشلا ليزنت وأ داحتالال فيرعت تانايب ل XML ليزنت نم دكأت: ةطحالم لوخدلا ليحستل URL نيوانع) IDp تافرعم نم SAML فيرعت تانايب خسنو (64 ةدعاق) على نيوكتلا ةعباتمل ةبولطم هذه إن شيح (Microsoft Entra) تافرعم وجرخلال ليحستو نمآلا ةياملال رادج

Zero Trust FTD | SAML-based Sign-on

Enterprise Application

« [Upload metadata file](#) [Change single sign-on mode](#) [Test this application](#) | [Got feedback?](#)

- Overview
- Deployment Plan
- Diagnose and solve problems

Manage

- Properties
- Owners
- Roles and administrators
- Users and groups
- Single sign-on**
- Provisioning
- Application proxy
- Self-service
- Custom security attributes

Security

- Conditional Access
- Permissions
- Token encryption

Activity

- Sign-in logs
- Usage & insights
- Audit logs
- Provisioning logs
- Access reviews

Troubleshooting + Support

- New support request

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. [Learn more.](#)

Read the [configuration guide](#) for help integrating Zero Trust FTD.

- Basic SAML Configuration** [Edit](#)

Identifier (Entity ID)	https://[redacted]/Azure_apps/saml/sp/metadata
Reply URL (Assertion Consumer Service URL)	https://[redacted]/Azure_apps/+CSCOE+/saml/sp/acs?tname=DefaultZeroTrustGroup
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	Optional
- Attributes & Claims** [Edit](#)

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname
- SAML Certificates**

Token signing certificate	Active	Edit
Status	Active	
Thumbprint	[redacted]	
Expiration	[redacted]	
Notification Email	[redacted]	
App Federation Metadata Url	[redacted]	Download
Certificate (Base64)	[redacted]	Download
Certificate (Raw)	[redacted]	Download
Federation Metadata XML	[redacted]	Download
Verification certificates (optional)		Edit
Required	No	
Active	0	
Expired	0	
- Set up Zero Trust FTD**

You'll need to configure the application to link with Microsoft Entra ID.

Login URL	https://[redacted]	Download
Microsoft Entra Identifier	https://[redacted]	Download
Logout URL	https://[redacted]	Download

2. اتفق بطلالة عومجم الى SAML IDp فيرعت تانايب داريتساب مقو FMC الى ىرخأ ةرم لقتنا i. تانايب الل لاخدا ب مق و IdP نم هل يزن ت مت يذلا فيرعت الل تانايب فلم مادختساب 2، ايودي ةبولطالم.

Add Application Group



An Application Group allows you to group multiple Applications and share authentication, security zone, and threat configurations.

1 Application Group

Name Azure_apps

Edit

2 SAML Service Provider (SP) Metadata

Entity ID https://[redacted]/Azure_apps/saml/sp/metadata
Assertion Consumer Service (ACS) URL https://[redacted]/Azure_apps/+CSCOE+/saml/sp/acs?tname=Def...

Edit

3 SAML Identity Provider (IdP) Metadata

Import or enter the IdP metadata. If IdP metadata is not currently available, you can skip this step and configure it later.

Import IdP Metadata

Manual Configuration

Configure Later

Import IdP Metadata

Drag and drop your file here
or select file
Zero Trust FTD.xml

Entity ID*

https://[redacted]

Single Sign-On URL*

https://[redacted]

IdP Certificate

MIIc8DCCAdigAwIBAgIQdTT7Lwlj7aRGm1m212dU/DANBgkqhkiG9w0B

[redacted]

Next

4 Re-Authentication Interval

5 Security Zones and Security Controls

Cancel

Finish

عجارتا بابل طتمل اقبط مكحت نم اول صاف reauthentication ل ت لك شو كلذ دع ب تق طقط ي.
ءاهن ا قوف ر قن او ص خ لم ل ن ي وكت

ة) لادلا تاداهشلل > PKI > تانئلكل ةرادا

نم ردصم ال IP ناو نع ةم جرت متت : (يراي تخ) IPv4 لوكوتورب ربع (NAT) ةكبش ردصم ه) معد متي ال) قي ببطتلا الى مزحلل هيجوت ةداع لبق ةدحملل نيوانعل الى ديعلل مدختسمل الى ويوتحت يتلل تانئلكل تاعومجم/قاطنل او فيضمل عون نم ةكبشلل تانئلكل يوس الى رخأ ةرم راسم يلع تاقيبطتلا لوصح نامضل اذه نيوكت نكمي . (IPv4 نيوانعل نم آلا ةيامحلل رادج لال خ نم نيديعلل ني مدختسمل

ةومجم الى هتفاضل تمت دق قي ببطتلا اذه ناك اذا ام دح: (يراي تخ) تاقيبطتلا ةومجم و) هل انه نيوكت مت يتلل تاداعلال مادختسال ةدوجوم تاقيبطت

رابتخا ةباتمب ZTNA مادختساب اهلي لوصولل متي يتلل تاقيبطتلا دعت ، لاثملا اذه يف نم آلا ةيامحلل رادج فلخ ةدوجوم ال CTB ل بيومدختسم ةهجاوو FMC بيومدختسم ةهجاول

ة) لادلا تاداهشلل > PKI > تانئلكل ةرادا > تانئلكل يف تاقيبطتلا صيخارت ةفاضل بجي

Add Known Internal Certificate



Name:

ao-fmc-ztna.cisco.local

Certificate Data or, choose a file:

Browse..

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

T
G
AY

Key or, choose a file:

Browse..


-----BEGIN RSA PRIVATE KEY-----

Encrypted, and the password is:

.....

Cancel

Save

 مادختساب هيل لوصولا متيل قيبطت لكل تاداهشلا ةفاك ةفاضل نم دكأت :ةظحالم
ZTNA.

قبتم دادع ةلمعل لكشي نأ اورمتسا ،يلخاد نوكي يقلتي تاداهشلا تفضأ نإ ام

يه لاثملا اذهل اهنوكت متي تال قيبطتلا تاداعل

(1 تاقيبطتلا ةومجم يف وضع) FMC بيومدختسم ةهجاو رابتخا :1 قيبطتلا

Add Application



Enabled

Edit

1 Application Settings

Application Name	FMC
External URL	https://ao-fmc-ztna.cisco.local
Application URL	https://ao-fmc-ztna.cisco.local
IPv4 NAT Source	-
Application Certificate	ao-fmc-ztna.cisco.local
Application Group	External_Duo

2 SAML Service Provider (SP) Metadata

Configurations are derived from Application Group 'External_Duo'

3 SAML Identity Provider (IdP) Metadata

Configurations are derived from Application Group 'External_Duo'

4 Re-Authentication Interval

Configurations are derived from Application Group 'External_Duo'

5 Security Zones and Security Controls

Security Zones	Inherited: (Outside)
Intrusion Policy	Inherited: (None)
Variable Set	Inherited: (None)
Malware and File Policy	Inherited: (None)

Edit

Cancel

Finish

2) تاقىب طتال ةومجم يف وضع CTB بىو مدختسم ةهجاو: 2 قىب طتال

ىلالتال وه قىب طتال اذهل نىوكتال صخلم نوكل

Enabled

1 Application Settings Edit

Application Name: CTB
 External URL: https://ao-ctb.cisco.local
 Application URL: https://ao-ctb.cisco.local
 IPv4 NAT Source: ZTNA_NAT_CTBB
 Application Certificate: ao-ctb.cisco.local
 Application Group: Azure_apps

2 SAML Service Provider (SP) Metadata
 Configurations are derived from Application Group 'Azure_apps'

3 SAML Identity Provider (IdP) Metadata
 Configurations are derived from Application Group 'Azure_apps'

4 Re-Authentication Interval
 Configurations are derived from Application Group 'Azure_apps'

5 Security Zones and Security Controls Edit

Security Zones: Inherited: (Outside)
 Intrusion Policy: Inherited: (None)
 Variable Set: Inherited: (None)
 Malware and File Policy: Inherited: (None)

Cancel Finish

✎ "ZTNA_NAT_CTBB" كڤش نئاك نيوكت مت، قيبطتلا اذهل ڤس نلاب هنأ طحال: طحال ال ىل اذع نع نيلمعت سمل نم ناونع رصملا تمجرت، لڤكشت اذه عم IPv4 ل nat رصمك قيبطتلا ىل اذع رل لسري نأ لبق نئاك لكشي لا نمض ناونع رادج ريغ ىرخأ ڤاوب ىل اذع ريشي (CTB) قيبطتلا لىضارتالا راسملا نأ اذه نيوكت مت نڤديع بل نيلمعت سمل ىل اذع رل رورم ڤكرح لاسرا متي مل ىلات لابلو، نمآلا ڤامحلا ڤي عرفلا كڤش ل قيبطتلا لىع تباث راسم نيوكت مت، اذع NAT نيوكت عم نمآلا ڤامحلا رادج لالخ نم اهل لوصول نكمي ىل ZTNA_NAT_CTBB.

ڤلابا قمل "تاقيبطتلا ڤومجم" نمض نألا اهضرع متي، تاقيبطتلا نيوكت دعب

ZTNA-TAC Targeted: 1 device

Applications Settings Groups: 3 Applications:

Bulk Actions Add Application Group Add Application

Name	External URL	Application URL	SAML Entity ID	Security Zones	Intrusion Policy	Malware and File Policy	Enabled
<input checked="" type="checkbox"/> Azure_apps (1 Application)			https://sts.v...	Outside (Inherited)	None (Inherited)	None (Inherited)	
<input type="checkbox"/> CTB	https://ao-ctb.cisco.local	https://ao-ctb.cisco.local		Outside (Inherited)	None (Inherited)	None (Inherited)	True
<input checked="" type="checkbox"/> External_Duo (1 Application)			https://sso-...	Outside (Inherited)	None (Inherited)	None (Inherited)	
<input type="checkbox"/> FMC	https://ao-fmc-ztna.cisco.local	https://ao-fmc-ztna.cisco.local		Outside (Inherited)	None (Inherited)	None (Inherited)	True

نيوكتلا رشنو تاريغىغتلا ظفح بق، اريخأ

ةحصلا نم ققحتلا

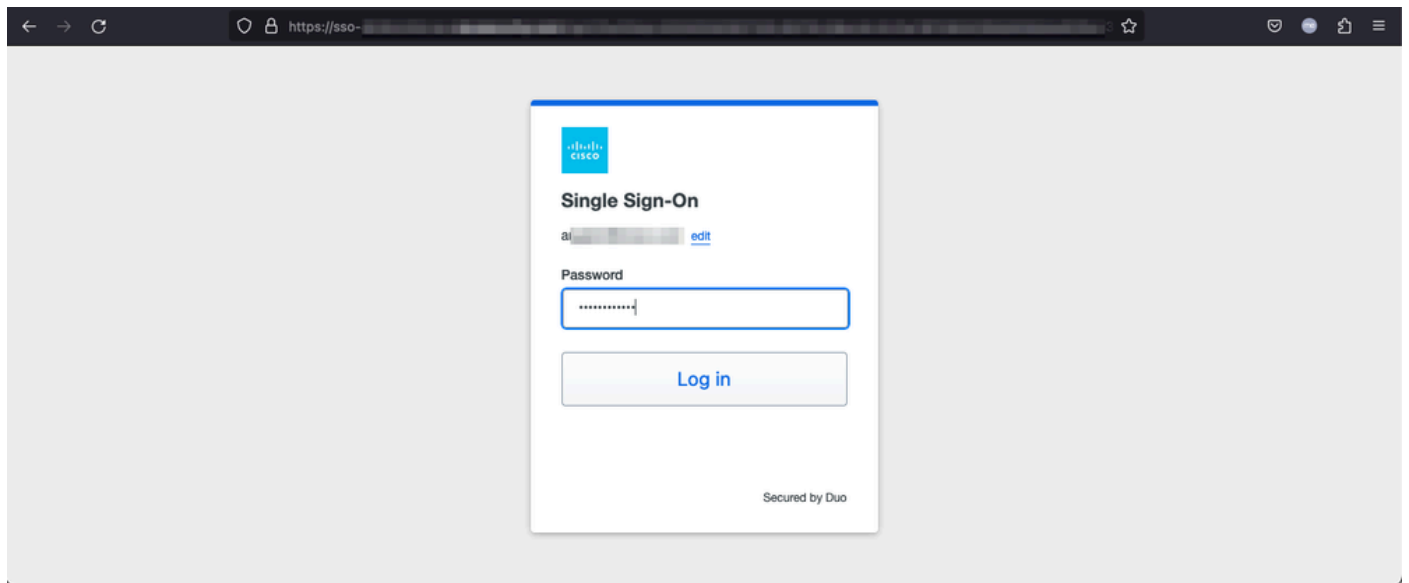
تاقببطللا ىلإ لوصولا دعب نع نيمدختسملل نكمي ،هعضوم ي ف نيوكتلل نوكي نأ درجم ب قح مهيدلف ،قباطملا IDp فرعم ةطساوب اهب احوومسم ناك اذا ويحراخلل URL ناووع لالخنم اه ىلإ لوصولا

1 قيببطللا

1. قيببطللاب صاخلل يحيراخلل URL ناووع ىلإ هجوتلاو بيو ضرعتسم حتفب مدختسملل موقبي .
1. <https://ao-fmc-ztna.cisco.local/> وه يحيراخلل طبرلا ناووع ،ةلاجل هذه في .

✎ نمآلة يامحلا رادج ةهجاوب صاخلل IP ناووع ىلإ يحيراخلل URL ناووع مسال ح بجي :ةظحالم (192.0.2.254) ةيحراخلل ةهجاولل IP ناووع ىلإ لجال متي ،لاثلما اذه في .اهنيوكت مت يتلا

2. IdP ىلإ لوخدلا ليحست ةباوب ىلإ مدختسملل هيجوت ةداع مت ،ديج لوصولو وه اذه نأل ارظن .
قيببطللل اهنيوكت مت يتلا .

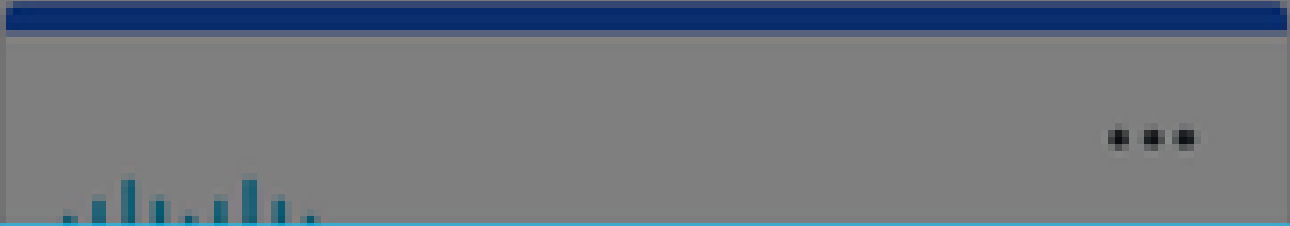


3. ىلع هنيوكت مت يذلا MFA بولسأ ىلع اذه دمتعي (MFA ل مدختسملل ةفدل لاسرا متي .
IdP).



Accounts

Add



Are you logging in to **External Applications ZTNA?**

 Global VPN TAC

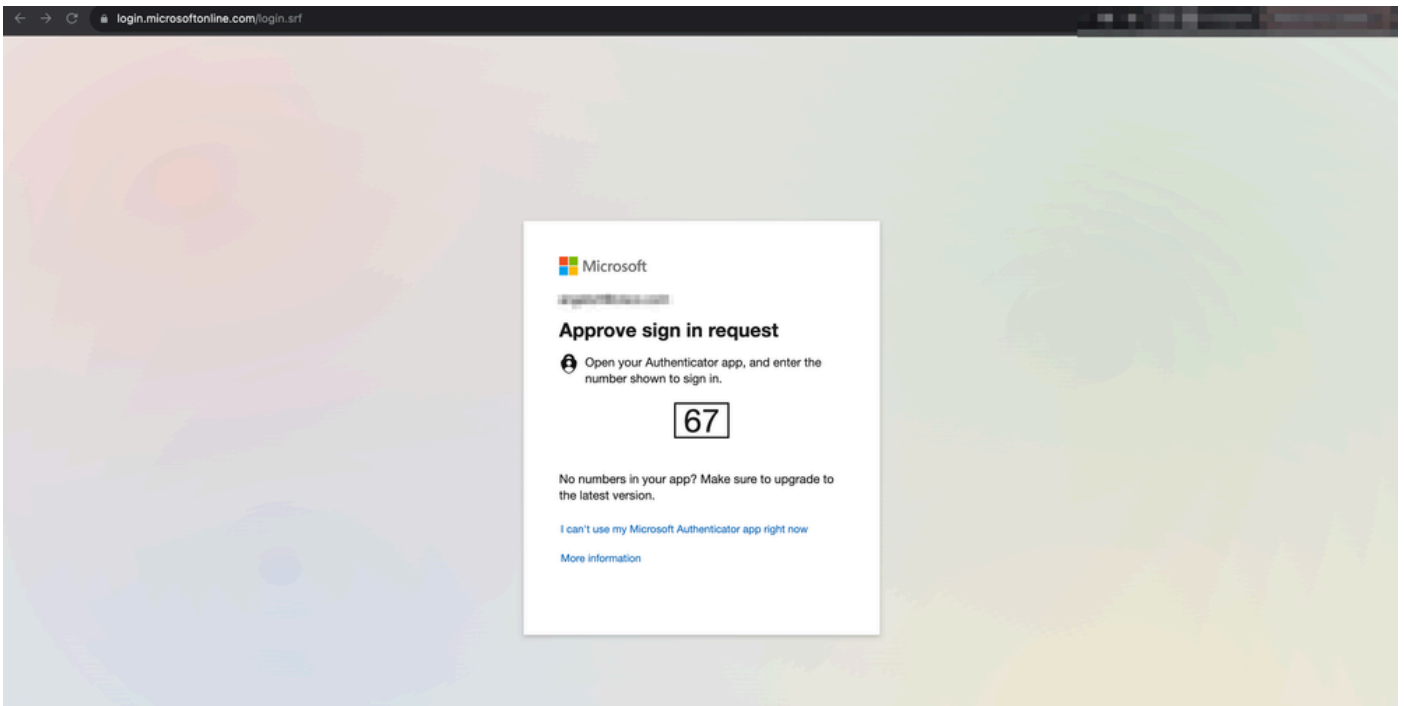
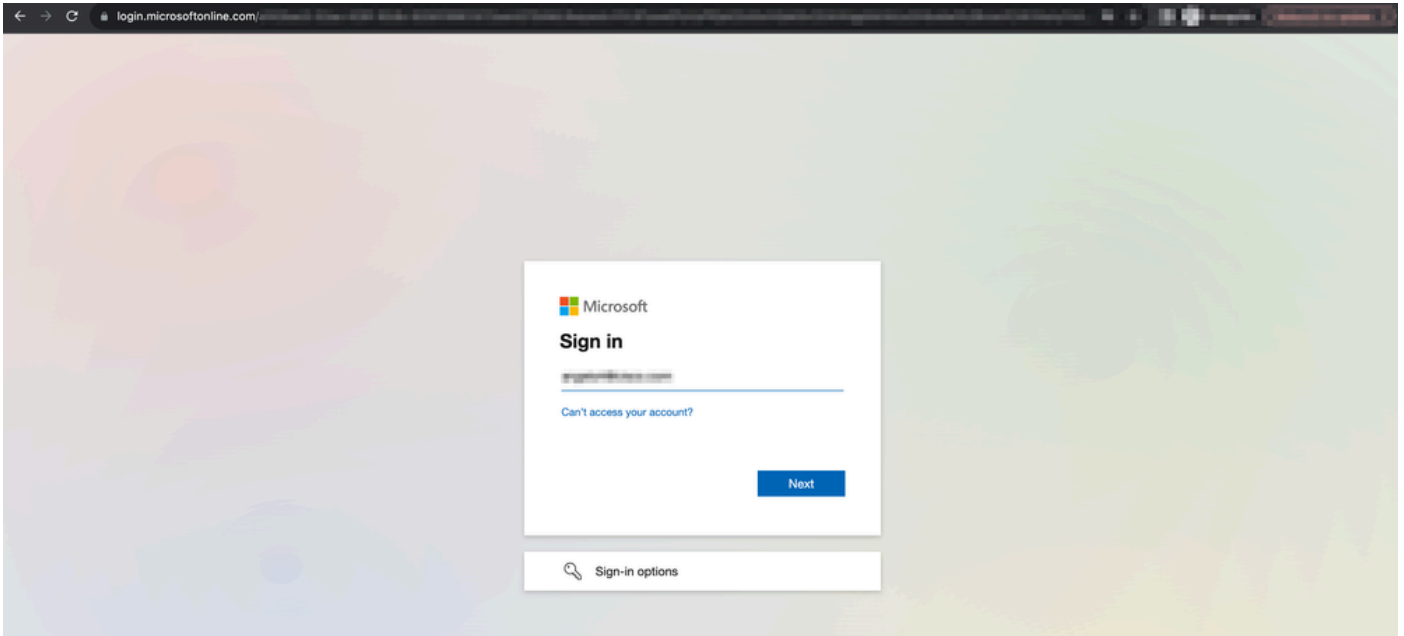
 [Redacted]

 1:13 p.m.

 [Redacted]

✎ ناونع ىل لىل حل متي، لاثملا اذه في. اهنىوكت مت يتي لتلا نمآلا ةي امحل رادج ةهجاوب صاخلا
ةجراخل ةهجاولل IP (192.0.2.254)

2. IdP ىل لوخدلا لىجست ةباوب ىل م دختس م لا هي جوت ةداع مت، ديدج لوصو وه اذه نأل ارظن.
قىبطلل اهنىوكت مت يتي لتلا.

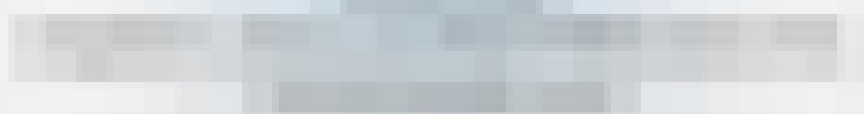


3. ىل هنىوكت مت يتي لىل MFA بولسأ ىل اذه دمتعي) MFA ل م دختس م لىل ةع ف د لاسرا متي.
IdP).

4:24



Are you trying to sign in?



Enter the number shown to sign in.

Enter number

No, it's not me

Yes

- ةي لى صفت تال جس عمجتو (ال م أ ق ف اوم) الماش اليلحت صيخشتل تاي لمع رفوت تالكشمل ل حل اه ليلحت نكمي

فاشتكال قي بطتلاب ة صاخلا تا صيخشتل مادختسا متي:

- DNS ماظنب ة قلعتملا لكاشملا
- دعاوقو، لي صوتلا ذم حتف متي مل، لاثملا لى بس لىع، حىحص ريغ نيوكت nat دعاوقو، في نصتلا
- ةيرفصللا ةقثلا لىل لوصولا جهن في لكاشملا
- ةهجالا نأ أو، ةهجالا نيوكت متي مل، لاثملا لى بس لىع، ةهجالا ب ة قلعتملا لكاشملا ةلطم

نع فشك لل ةماعلا تا صيخشتل:

- يوق ري فشت صيخرت ني كمت متي مل اذ
- ةحلاص ريغ قي بطتلا ةداهش تناك اذ
- ةيضا رتفالا قافنأل ةومجم في SAML لىل ةقداصملا بولسا ةئيهت مت مل اذ
- ةقائل ةرفوملا و ةومجملا ةمجملا ةنمازملا تالكشم
- ة قلعتملا كلت لثم، تالكشملا صيخشتل snort تادادع نم لىل لوصحلا ري فشتلا ك ف أو ةزيمملا تامالعالاب
- ةمجت ردصم في رادصا كالهتسا ةكرب برص.

تا صيخشتل لي غشتل:

1. ZTNA قي بطت لك ل ةدوجوملا صيخشتل ةنوي لىل لقتنا.

Name	External URL	Application URL	SAML Entity ID	Security Zones	Intrusion Policy	Malware and File Policy	Enabled
Azure_apps (1 Application)				Outside (Inherited)	None (Inherited)	None (Inherited)	
CTB				Outside (Inherited)	None (Inherited)	None (Inherited)	True
External_Duo (1 Application)				Outside (Inherited)	None (Inherited)	None (Inherited)	
FMC				Outside (Inherited)	None (Inherited)	None (Inherited)	True

2. لي غشت قوف رقنا وازاهج ددح.

Select Device

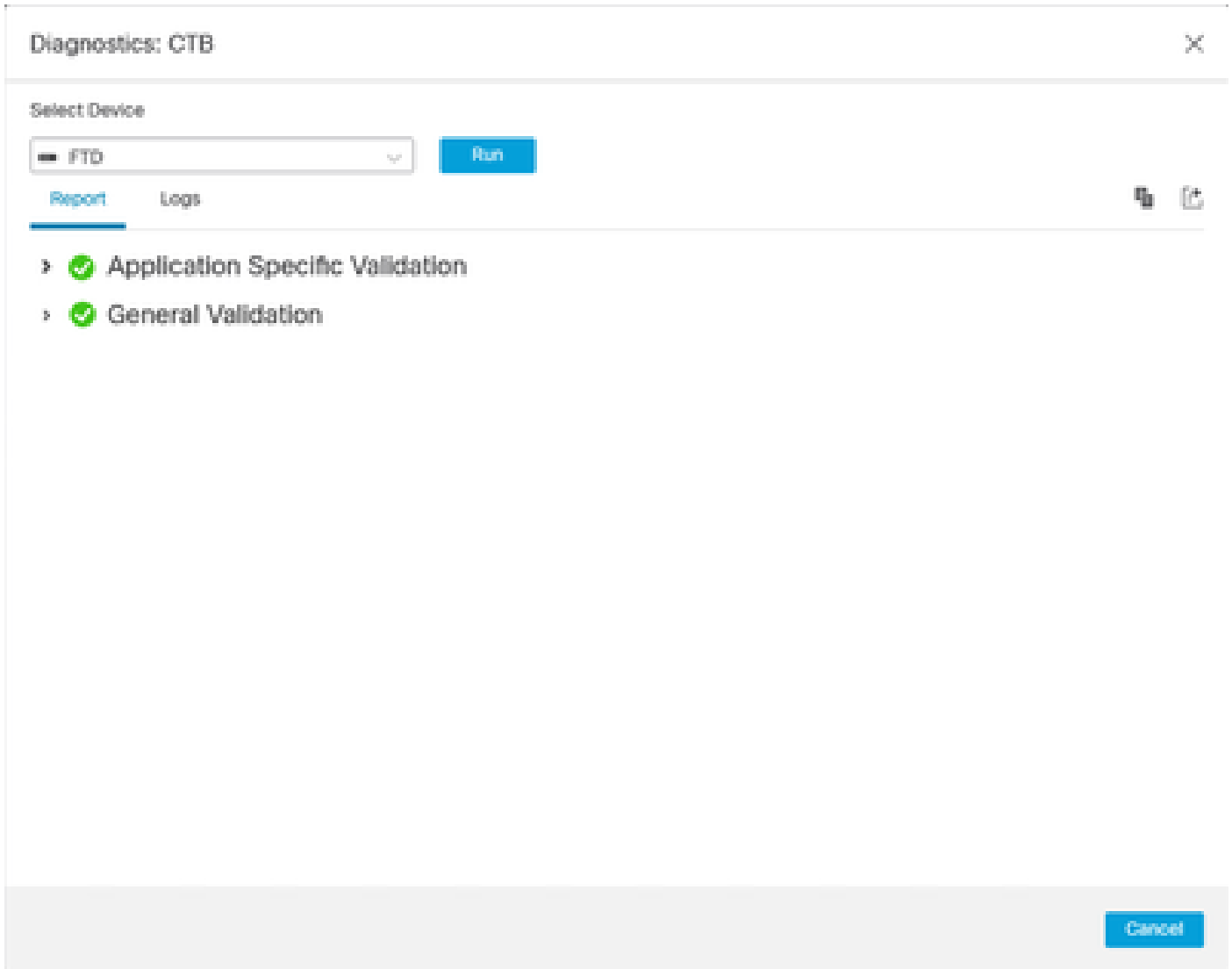
Select...

FTD

Run

Cancel

3. ريرقتلا في جئاتنلا ضرع.



تايئاصحإلإ ضرعوو ةقثلا مدع نيوكت ضرعل FTD CLI يف حوضولواو ضرعلال رمأوا رفوتت
ةسلجلال تامولعمو.

```
<#root>
```

```
firepower# show running-config zero-trust
```

```
application      Show application configuration information  
application-group Show application group configuration  
|                Output modifiers  
<cr>
```

```
firepower# show zero-trust
```

```
sessions  Show zero-trust sessions  
statistics Show zero-trust statistics
```

```
firepower# show zero-trust sessions
```

```
application      show zero-trust sessions for application
application-group show zero-trust sessions for application group
count            show zero-trust sessions count
user             show zero-trust sessions for user
detail           show detailed info for the session
|               Output modifiers
<cr>
```

```
firepower# clear zero-trust
```

```
sessions  Clear all zero-trust sessions
statistics Clear all zero-trust statistics
```

```
firepower# clear zero-trust sessions
```

```
application Clear zero-trust sessions for application
user         Clear zero-trust sessions for user
<cr>
```

في فة لالتل رم اوأل مدختسأ ، WebVPN و Zero-trust ة طمنل لدحول اءاطخأ ححصت ني كم تل
ة بل لاطم Lina:

- Firepower# debug zero-trust 255
- Firepower# ءاطخأ ححصت WebVPN 255
- Firepower# debug webVPN response 255
- Firepower# debug webVPN saml 255

ة ل ص ت ا ذ ت ا م و ل ع م

- مزل ي (TAC) ة نقتل ة دعاسم ل زكرم ب لاصتال ا جري ، ة فاضا ة دعاسم ل ع لوصحل ل
Cisco نم ة م ل ا ع ل ا م ع د ل ا ل ا ص ت ا ت ا ه ج : ح ل ا ص م ع د د ق ع
- [ا ن ه](#) Cisco VPN ع م ت ج م ة ر ا ي ز ا ض ي ا ك ن ك م ي

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت
ملاعلاء انءمچي فني مدختسمل معدى وتحم مي دقتل یرشبل او
امك ةقيقد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاخل مه تبلب
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه
ىل إأمئاد ةوچرلاب يصوت وتامچرتل هذه ةقد نع اهتيلوئسم Cisco
Systems (رفوتم طبارل) يلصلأل يزي لچنل دن تسمل