

مادختساب ةددعتم لق فنل اتاعومجم نيوكت ASA ىلع SAML

تايوتحملا

[ةمدقملا](#)

[ةيساسال اتابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسا تامولعم](#)

[SAML-Sp-Initiated SSO](#)

[تانويكتلا](#)

[ضدعمللا نم Cisco Secure Firewall - Secure Client ةفاضلا](#)

[قيبطتلل Azure AD ىمدختسم نييعت](#)

[CLI ربع ASA نيوكت](#)

[فحصللا نم ققحتلا](#)

[اوحالصال وءاطخال افاشكتسا](#)

[قلص تاذا تامولعم](#)

ةمدقملا

Cisco ىلع ةددعتم لق فنل اتاعومجم ل Azure Identity Provider عم SAML ةقداصم ةقيثو اذه فصلي ASA.

ةيساسال اتابلطتملا

تابلطتملا

ةيلالتل اتاعوضوملا ةفرعمب Cisco ىصوت:

- (ASA) ةلدعملل نامال ةزهجأ
- (SAML) نامال ديكأت زيمرت ةغل
- (SSL) ةنمال ليصوتل ذخأم ةقبط تاداهش
- Microsoft Azure

ةمدختسملا تانوكملا

ةيلالتل ةيدامل تانوكملا وجماربلل تارادصل ىل دنننسملا اذه يف ةدراول تامولعملل دننست:

- ASA 9.22(1)1
- Microsoft Azure Entra ID عم SAML 2.0

- Cisco Secure Client 5.1.7.80

ةصاخ ةي لمعم ةئي ب ي ف ةدوجومل ةزهجال نم دنتسمل اذه ي ف ةدراول تامولعمل عاشن ا مت تناك اذا .(يضا رتفا) حوسمم نيوكتب دنتسمل اذه ي ف ةمدختسمل ةزهجال عي مج تادب رما يال لمحتمل ريثاتلل كمهف نم دكاتف ،ليغشتل دي ق كتكبش

ةيساسا تامولعمل

قيبطت لك بلطتي .هسفن نايلك ل فرعمل ةددعتم تاقيبطت Microsoft Azure معددي نا نكمي تاعومجم نيوكتب نكمي ASA، ي ف .ةديرف ةداهش (ةفلتخم قفن ةعومجم لىل هنييغت مت) ةزيم ببسب (IDp) زواجتل ةي وه رفومل ةي محم ةفلتخم تاقيبطت مادتسسال ةددعتم قافنا م داخ نئاك ي ف ةيساسال IdP ةداهش زواجتب ني لووسملل ةزيمل هذه حمست .IdP ةداهش ةزيمل هذه لاخدا مت .قافنا ةعومجم لكل ةني عم IdP ةداهشب (SSO) ي داخال لوخدل ليحست ادعاصف 9.17.1 رادصال نم ASA لىل

SAML-Sp-Initiated SSO

كولس رمتسي ASA، لىل لوصول قيرط نع لوخدل ليحست يئاهنل م دختسمل ادبي ام دنع يلاتل وحنل لىل لوخدل ليحست:

1. ةداعل متت ،هرايخا و ا ةنكمم SAML قافنا ةعومجم لىل VPN ةكبش م دختسمل لوصول دنع .1. مقى مل ام م دختسمل ةبل اطم متت .ةقداصلل SAML فرعم لىل يئاهنل م دختسمل هيجوت ةداعل نوكت ةالحال هذه ي فو ،ةرشابم ةعومجملاب صاخال URL ناو نع لىل لوصولاب م دختسمل ةتماص هيجوتل
2. فرعم لىل هيجوت ةداعل ب ضرعتسمل موقى يذلاو ،SAML ةقداصلم بلط عاشناب ASA موقى .SAML
3. بجي .لوخدل يئاهنل م دختسمل لچسي و دامتعال تانايل بل يئاهنل م دختسمل IdP يدحتي .IdP ةقداصلم نيوكتب ةلخدمال دامتعال تانايل يفت نا
4. ليحستل URL ناو نع لىل اهرشن متي و ضرعتسمل لىل ىرخا ةرم IdP ةباجتسل لاسرا متي .لوخدل ليحست لامكال ةباجتسال نم ASA ققحتي .ASA لوخد

تانويوكتل

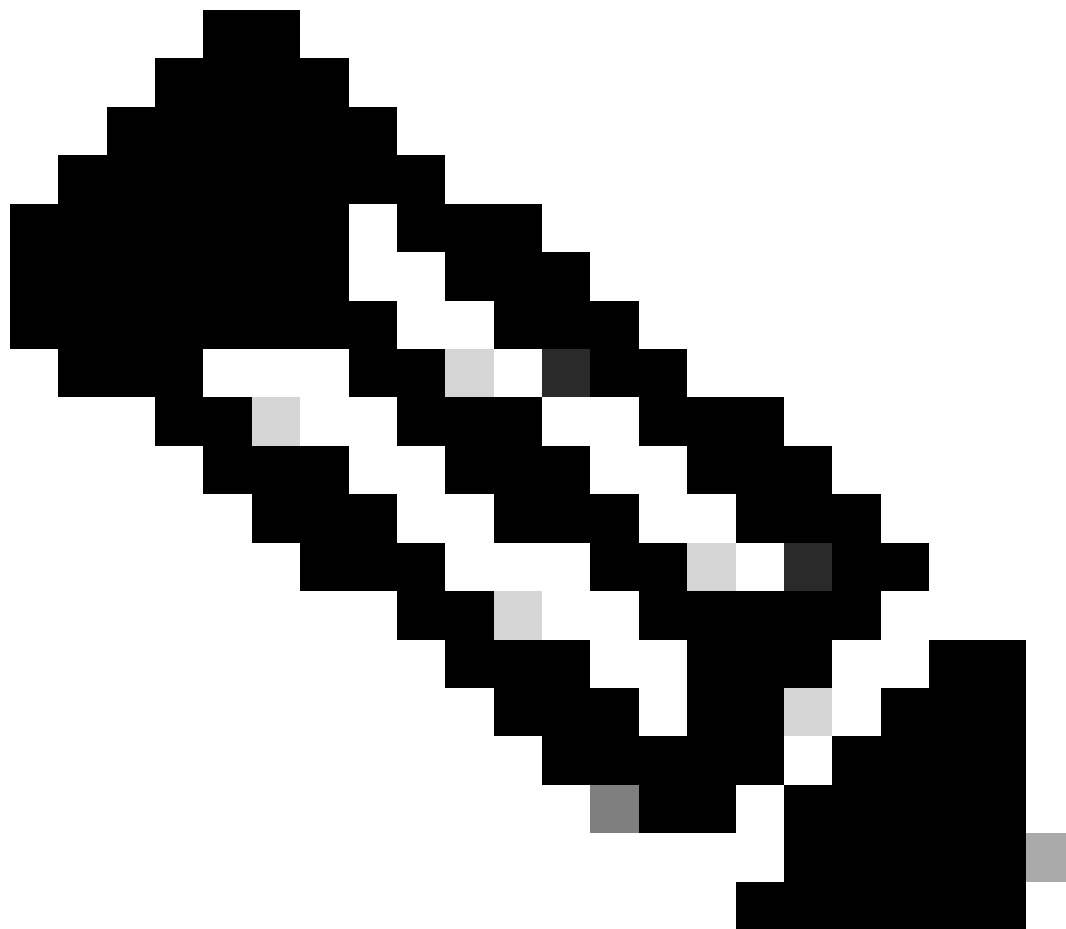
ضرعمل نم Cisco Secure Firewall - Secure Client ةفاضل

متي - نمال Cisco ةي امح رادج عم Microsoft Entra SSO لم اكت ةفاضل متت ،لاثمل اذه ي ف ASA لىل اهنيوكت مت ي تال قافنال تاعومجم Azure لىل "نم آلي مع" ةفاضل

- SAML1
- SAML2

Microsoft Entra ةقاطب فرعم ي ف نمال لي عمل - Cisco نم نمال ةي امحال رادج لم اكت نيوكتل SAAs تاقيبطت ةمئاق لىل ضرعمل نم نمال لي عمل - Cisco Secure Firewall ةفاضل كمزلي

ةرادملا



ىلإ Cisco Secure Firewall - Secure Client ةفاضل وه تاوطخل هذه نم ضرغل :ةطحالم
SAML1، لوال قفنة ةومجب صاخلا ضرعملا

Microsoft Entra فرع رتخاو Azure لخدم ىلإ لوخدلا لجس 1. ةوطخل

Azure services



Create a
resource



Microsoft Entra
ID



All resources



Security



Quickstart
Center



Azure AI
services



Kubernetes
services



Virtual machines



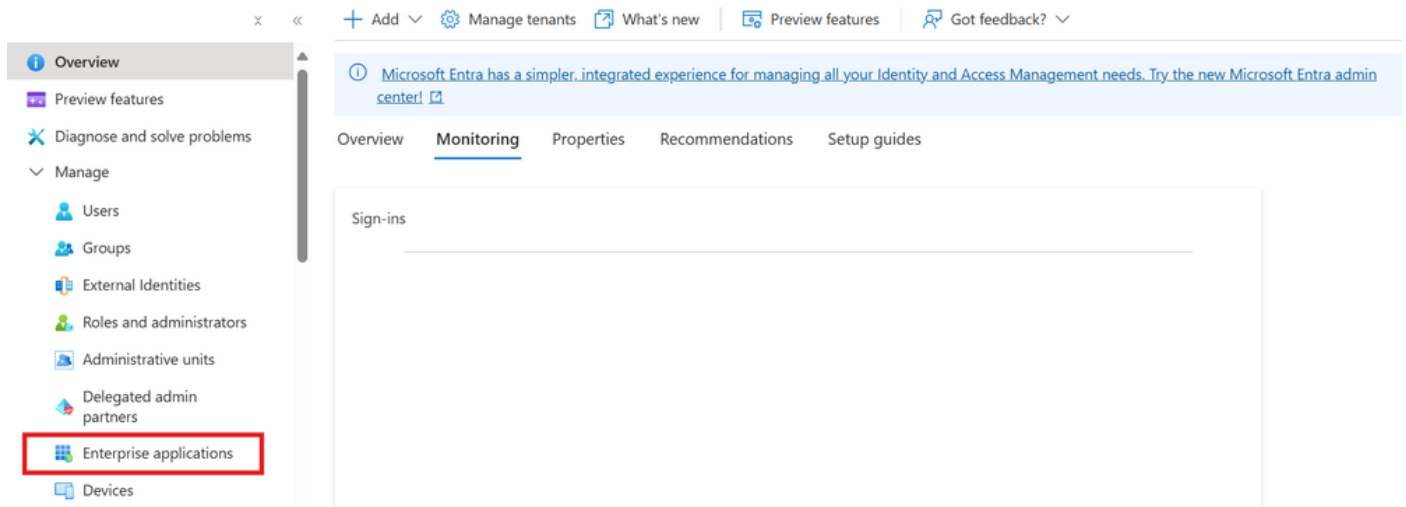
App Services



More services

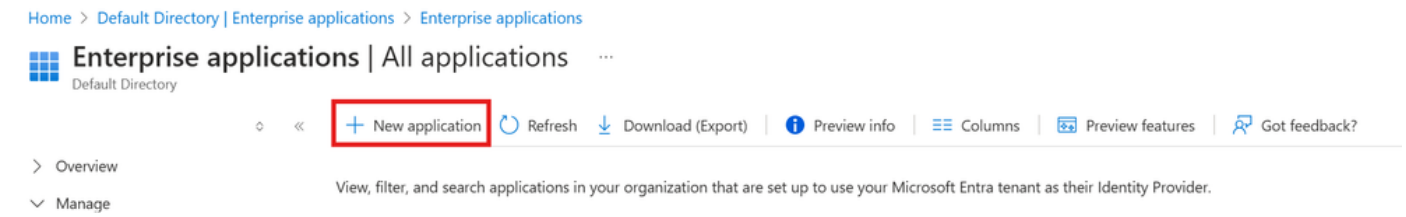
Microsoft Entra فرع

تاسسؤم ال تاقىبطت رتخأ، ةروصلال هذه يف حضوم وه امك 2. ةوطخلال



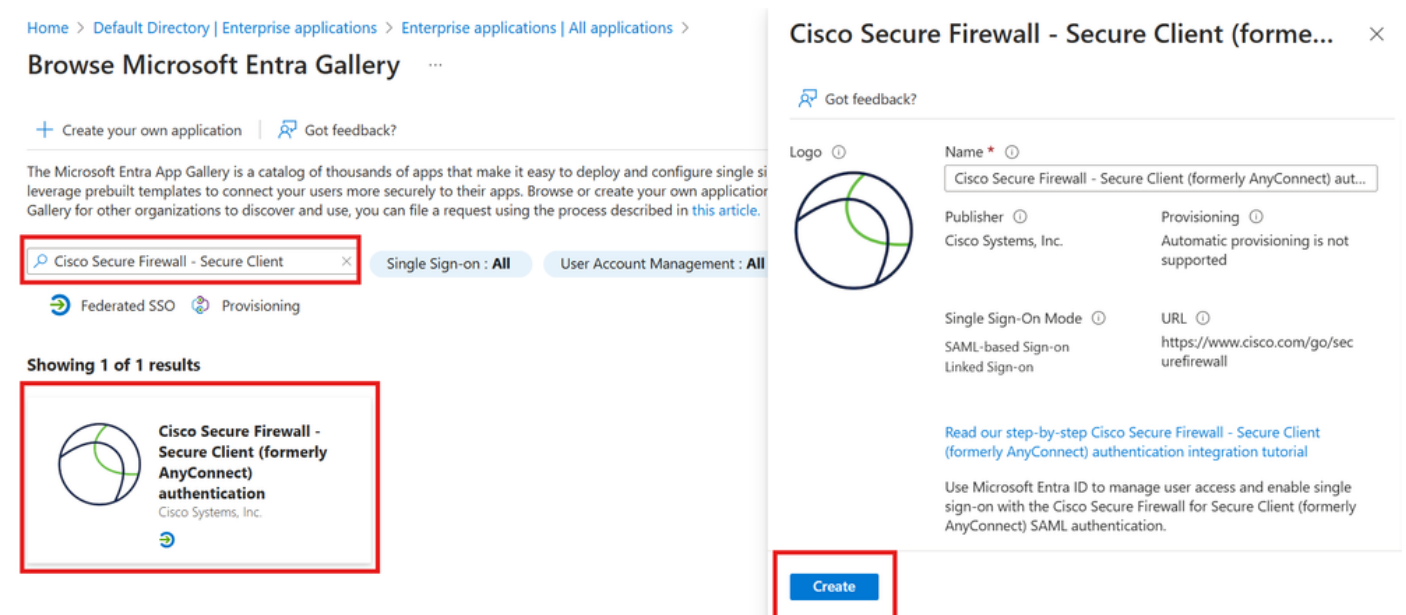
تاسسؤم ال تاقىبطت

ةروصلال هذه يف حضوم وه امك ،ديج قىبطت رتخأ، نآال 3. ةوطخلال



ديج قىبطت

يف Cisco Secure Firewall - Secure Client بتكا، ضرعمل نم ةفاضلال مسق يف 4. ةوطخلال ةفاضلا م ث، جئاتنلال ةحول نم Cisco Secure Firewall - Secure Client رتخاو، ثحالب ع برم قىبطتلال.



ةروصل هذه في حضورم وه امك ،يداحأ لوخد ليجست ةمئاق رصنع رتخأ 5. ةوطخل

Cisco Secure Firewall - Secure Client (formerly AnyConnect) authentication | Overview ...

Enterprise Application

Overview

Deployment Plan

Diagnose and solve problems

Manage

Security

Activity

Troubleshooting + Support

Properties

Name ⓘ
Cisco Secure Firewall - Secu...

Application ID ⓘ
098b5489-4aec-4c73-8de1-...

Object ID ⓘ
584f4478-7571-4361-9453-...

Getting Started

1. Assign users and groups
Provide specific users and groups access to the applications
[Assign users and groups](#)

2. Set up single sign on
Enable users to sign into their application using their Microsoft Entra credentials
[Get started](#)

يداحأال لوخدال ليجست دادعإ

ةوطخل Select a Single Sign-on MethodPage في SAML رتخأ 6. ةوطخل

Cisco Secure Firewall - Secure Client (formerly AnyConnect) authentication | 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

Self-service

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.](#)

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

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.

لماس

ةنوقيأ لىلع رقنا ،SAML مادختساب يداحأال لوخدال ليجست دادعإ ةحفص في 7. ةوطخل
تادادعإال ريرحتل يساسأل SAML نيوكت ملق/ريرحت

Basic SAML Configuration



Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	<i>Optional</i>
Relay State (Optional)	<i>Optional</i>
Logout Url (Optional)	<i>Optional</i>

يُساسأل SAML نيوكت

هذه بة صاخال ميقل لخدأ، SAML مادختساب يداخال لوخدلا ليحست دادعإ ةحفص ي ف 8. ةوطخال لوقخال:

طمنلا اذه مادختساب URL ناوع بتكا، فرعما صنلا عبرم ي ف أ:

`https://<VPN URL>/saml/sp/metadata/<tunnel_group_name>`

طمنلا اذه مادختساب URL ناوع بتكا، درلاب صاخال URL ناوع صن عبرم ي ف ب:

`https://<VPN URL>/+CSCOE+/saml/sp/acs?tgname=<tunnel_group_name> [tunnel_group_name = SAML1]`



طاقون ىلع ةميقلال يوتحت الأ بجيو فرحالأ ةلاحل ساسح Tunnel_group_name :ةطحال م
'/' عطقتو '!'.

عيقوت ةداهش مسق ي ف SAML، مادختساب يداخالأ لوخدلا ليچست دادعإ ةحفص ي ف 9. ةوطخال
ىلع هظفو ةداهشلا فلم ليزنت لجأ نم ليزنت رتخاو (Base64) ةداهشلا نع ثحبا، SAML،
رتوي بمكلا.

SAML Certificates

Token signing certificate

 Edit

Status

Active

Thumbprint

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100

Expiration

2/4/2028, 4:33:14 PM

Notification Email

msal@ashruba.com

App Federation Metadata Url

https://

Certificate (Base64)

[Download](#)

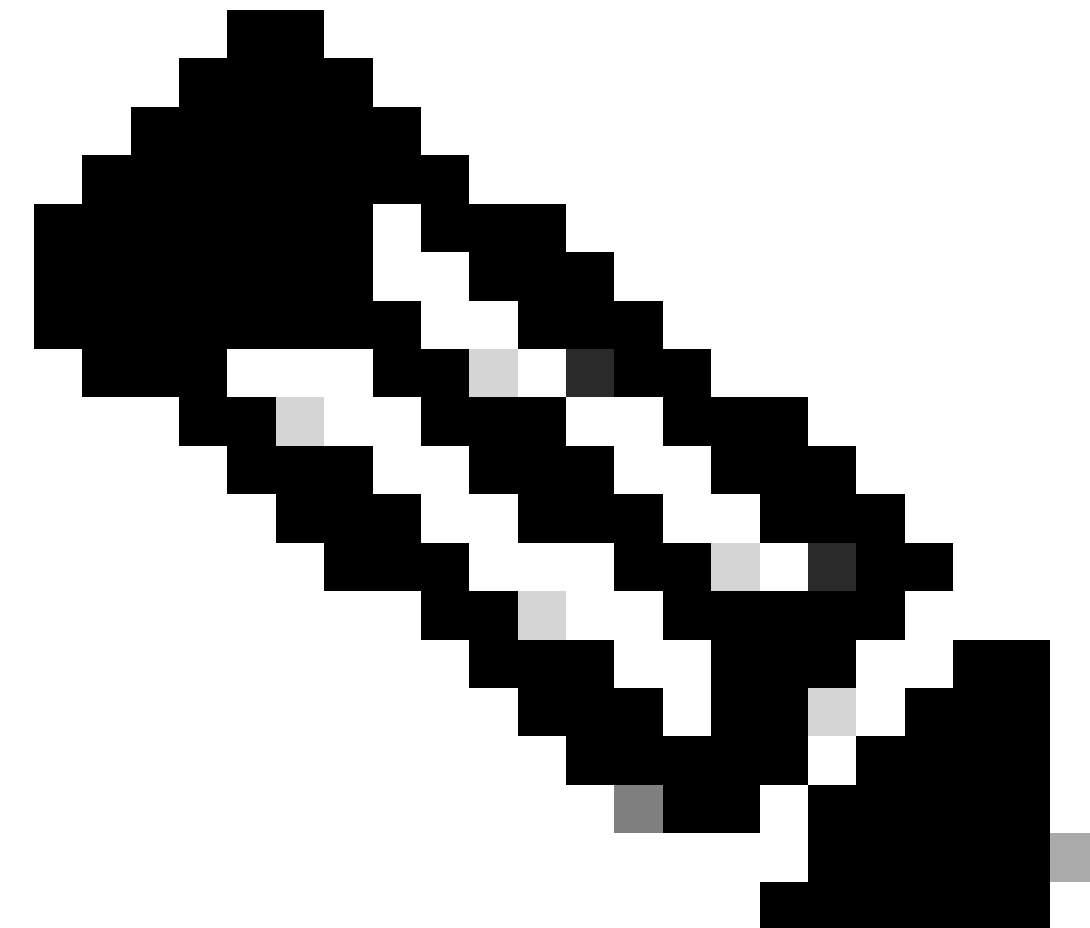
Certificate (Raw)

[Download](#)

Federation Metadata XML

[Download](#)

عداهشال ليزنت (Base64)



ASA TrustPoint AzureAD-AC-SAML1 إلی اهل ليزنت مت ي التل عداهشال هذه داريتسإ مت :ةطحال م ليصافتال نم ديزم يل عل لوصحلل ASA نيوكت مسق يلإ عرا .

(نېوانع) ناونع خسنا، نمال ليمعلا - Cisco نم نمال اةامحل رادج دادعإ مسق ي ف 10 ةوطخل نيوكتل هذه URL (نېوانع) ناونع مادختسا متي. كئابلطتم ىلإ ادانتسا بسانملا URL ASA ىلع SSO مداخ نئاك

- Microsoft Entra Identifier - وه اذه VPN نيوكت ي ف SAML IDP
- URL لوخد ليجست وه اذه - لوخدلا ليجستل URL ناونع
- URL جورخ ليجست وه اذه - جورخلا ليجستل URL ناونع

Set up Cisco Secure Firewall - Secure Client (formerly AnyConnect) authentication

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

Login URL

<https://login.microsoftonline.com/65d917a5-74a4...>

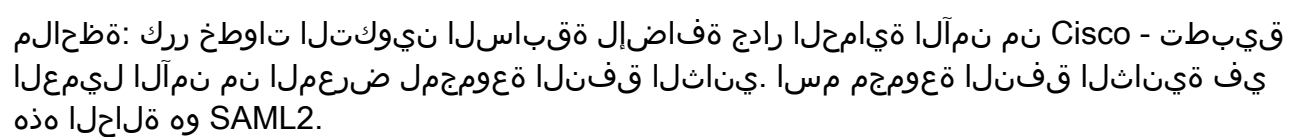
Microsoft Entra Identifier

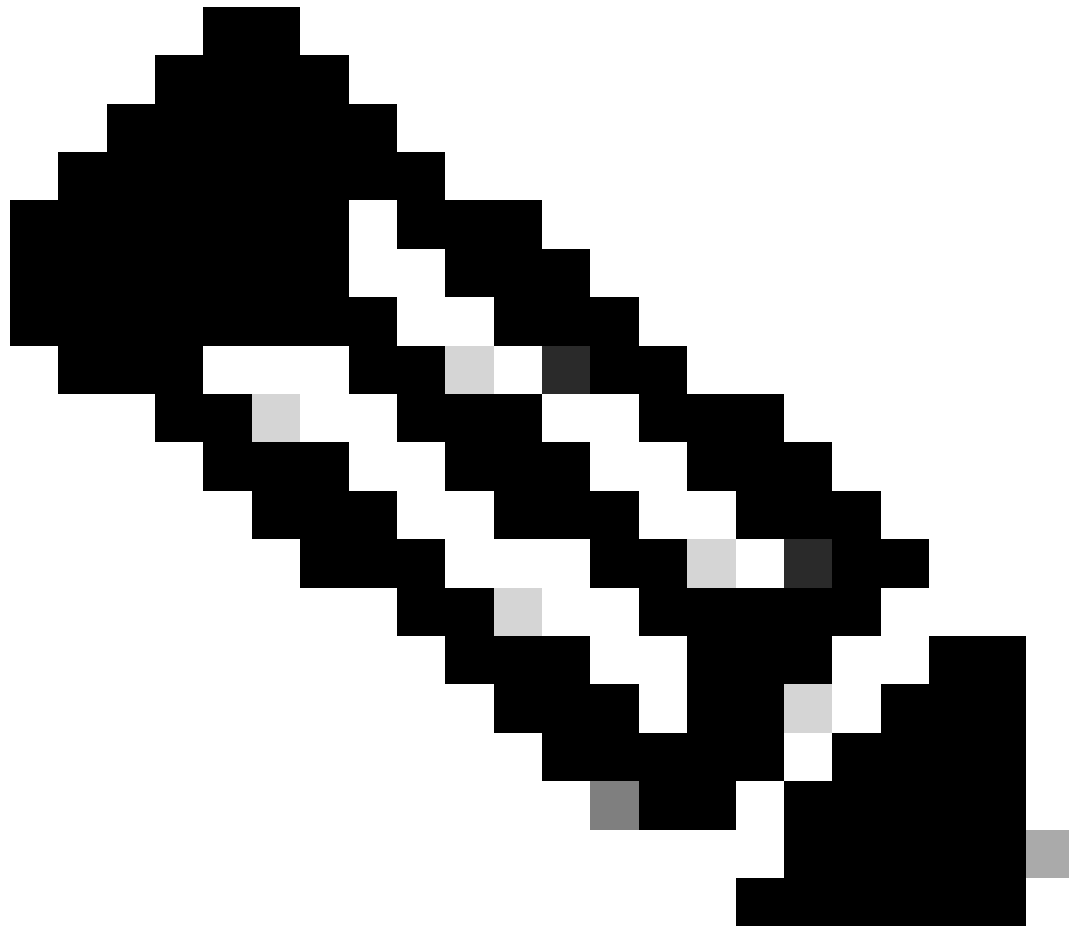
<https://sts.windows.net/65d917a5-74a4-42aa-8e3...>

Logout URL

<https://login.microsoftonline.com/65d917a5-74a4...>

SSO ب صاغل URL





ةومجم ل نمآلا ليمعلا قيبطت - Cisco نم نمآلا ةيامحلا راج ةفاضإ ءانثأ :ةطحال م
ةوطخلا يف اهليزنت مت يتلا Azure ةداهش داريئسإ متي ، (SAML 2) ةيناثلا قفنلا
8. إلى ASA TrustPoint AzureAD-AC-SAML2.

قيبطت لل Azure AD يمدختسم نييعت

لوصولا حنمت كنأل ارظن ، Azure SSO م ادختسالا Test1 و Test2 نيكت متي ، مسقلا اذه يف
Cisco Secure Client قيبطت إلى

لؤلألا IDp قيبطتل

م ث ، تاعومجم و نيمدختسم رتخأ ، لؤلألا IDp قيبطت إلى ةماعلا ةرظنلا ءحفص يف 1. ةوطخلا
امدختسم فضا

Cisco SAML 1 | Users and groups ...
Enterprise Application

◁ << **+ Add user/group** ✎ Edit assignment 🗑 Remove assignment 🔍 Update credential ↻ Refresh ⚙ Manage view ▾ | 🗨 Got feedback?

Overview
Deployment Plan
Diagnose and solve problems
Manage
Properties
Owners
Roles and administrators
Users and groups ☆
Single sign-on

📘 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, search all users & groups

Display name	Object type
No application assignments found	

تاعومچم لاول مدختسم ل

ةمهم ةفاضل راوح عبرم ي ف تاعومچم و اني مدختسم رتخا 2. ةوطخل

Add Assignments
Default Directory

📘 Try changing or adding filters if you don't see what you're looking for.

Search
🔍
4 results found

All Users

Users
None Selected
Select a role
Default Access

 Test1	User
---	------

ةمهم ةفاضل 1

نيي عت زلا قوف رقنا ،ةمهم ةفاضل راوح ل عبرم ي ف 3. ةوطخل

Add Assignment ...

Default Directory

Users

1 user selected.

Select a role

Default Access

Assign

Test1 مَدْخُتْ سَم نِي يِعْت

نِي نَاثِل IDp قِي بَطَل

رُوصِلَا هَذِهِ فِي حُضُوم وَهُ امَك نِي حَزَانِل نِي نَاثِل قِي بَطَل لَلْ قَبَاسِلَا تَاوْطَخِلَا رَرَكْ.

Add Assignment ...

Default Directory

Users

1 user selected.

Select a role

Default Access

Assign

2 مهم ة فاضا

Home > Default Dir

Add Assignment

Default Directory

Users

Try changing or adding filters if you don't see what you're looking for.

Search



4 results found

All Users

	Name	Type	Details
☐	 Test2	User	

Selected (0)

Reset

No items selected

Assign

Select

Test2 مدختسم نييغت

Test1: مدختسم نييغت

Cisco SAML 1 | Users and groups ...

Enterprise Application

« + Add user/group Edit assignment Remove assignment Update credential Refresh Manage view Got feedback?

Overview
Deployment Plan
Diagnose and solve problems
Manage
Properties
Owners
Roles and administrators
Users and groups ☆
Single sign-on
Provisioning
Self-service

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, search all users & groups

Display name	Object type
☐  Test1	User

دخاومدختسم نييعت رابتخا

Test2: مدختسم لا نييعت

Cisco SAML 2 | Users and groups ...

Enterprise Application

« + Add user/group Edit assignment Remove assignment Update credential Refresh Manage view Got feedback?

Overview
Deployment Plan
Diagnose and solve problems
Manage
Properties
Owners
Roles and administrators
Users and groups ☆
Single sign-on
Provisioning
Self-service

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, search all users & groups

Display name	Object type
☐  Test2	User

مدختسم نييعت 2 رابتخا

ASA نيوكت CLI ربع

SAML. تاداهش داري تساو ةقث طاقن ءاشن 1. ةوطخل

قفن ةومجم لكب ةصاخ لا SAML تاداهش داري تساو ةقث يتطقن نيوكتب مق

<#root>

config t

crypto ca trustpoint

AzureAD-AC-SAML1

```

revocation-check none
no id-usage
enrollment terminal

```

```
no ca-check
crypto ca authenticate
```

AzureAD-AC-SAML1

```
-----BEGIN CERTIFICATE-----
```

```
...
```

```
PEM Certificate Text you downloaded from AzureAD goes here
```

```
...
```

```
-----END CERTIFICATE-----
```

```
quit
```

```
!
```

```
crypto ca trustpoint
```

AzureAD-AC-SAML2

```
revocation-check none
no id-usage
enrollment terminal
no ca-check
crypto ca authenticate
```

AzureAD-AC-SAML2

```
-----BEGIN CERTIFICATE-----
```

```
...
```

```
PEM Certificate Text you downloaded from AzureAD goes here
```

```
...
```

```
-----END CERTIFICATE-----
```

```
quit
```

SAML. فرع م نيوكتب مق 2. ةوطخل

SAML. فرع م تادادع! ري فوتل رم اوأل هذه مدختسأ

webvpn

```
saml idp https://xxx.windows.net/xxxxxxxxxxxxx/ - [Azure AD Identifier]
url sign-in https://login.microsoftonline.com/xxxxxxxxxxxxxxxxxxxxx/saml2 - [Login URL]
url sign-out https://login.microsoftonline.com/xxxxxxxxxxxxxxxxxxxxx/saml2 - [Logout URL]
trustpoint idp AzureAD-AC-SAML1 - [IdP Trustpoint]
trustpoint sp ASA-EXTERNAL-CERT - [SP Trustpoint]
no force re-authentication
no signature
base-url https://asa.example.com
```

ىل وأل VPN ق فن ةومجم ىل ع SAML ةقداصم ق ىب طت 3. ةوطخل

AzureAD-AC-SAML1 IdTrustPoint م ادختس اب SAML1 ق فن ةومجم نيوكتب مق

<#root>

```
tunnel-group SAML1 webvpn-attributes
authentication saml
group-alias SAML1 enable
saml identity-provider https://xxx.windows.net/xxxxxxxxxxxxx/
```

saml idp-trustpoint AzureAD-AC-SAML1 <---- Overrides the primary IDP certificate in the Single Sign-On (SSO) configuration.

ة. VPN ق فن ةومجم ىل ع SAML ةقداصم قيب ط ت 4. ةوطخال

ق فن ةومجم نيوك ت ب مق SAML2 IdTrustPoint. م ادخت ساب AzureAD-AC-SAML2

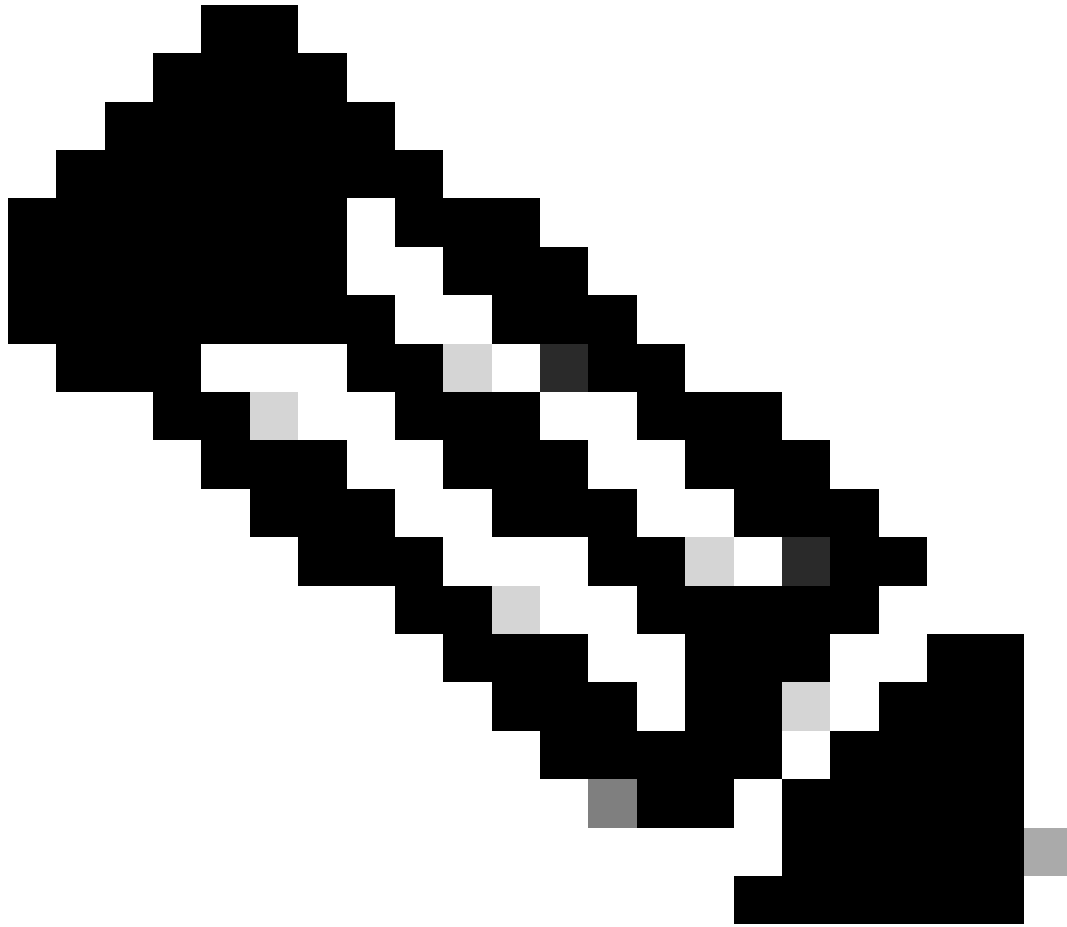
<#root>

```
tunnel-group SAML2 webvpn-attributes
authentication saml
group-alias SAML2 enable
saml identity-provider https://xxx.windows.net/xxxxxxxxxxxxx/
```

saml idp-trustpoint AzureAD-AC-SAML2 <---- Overrides the primary IDP certificate in the Single Sign-On (SSO) configuration.

ن. نيوك ت ل ظ ف ح 5: ةوطخال

write memory



هذه الرسوم توضح كيفية عمل IdP، وهي توضح كيفية عمل SAML. هذه الرسوم توضح كيفية عمل SAML. هذه الرسوم توضح كيفية عمل SAML.

مراحل العمل

1. إعداد SAML في AnyConnect.

2. إعداد URL في AnyConnect.

3. إعداد SAML في AnyConnect.

4. إعداد SAML في AnyConnect.

اهحال صإو ءاطخألا فاشك تسا

هيلع روثلعلا نكمي حيحص ريغ نيوكت اءحال صإو SAML ءاطخأ فاشك تسأ تاودأ مظعم نمضتت
debug webVPN مءءختسا نكمي .ءاطخألا حيحصت ليغشت وأ ،SAML نيوكت نم ققءتلا دنع
ال يءلا تاءوي راني سالا ي ف ،كلذ عمو ،اهحال صإو لكاشملا مظعم ءاطخأ فاشك تسالا 255 saml
ءاطخألا حيحصت نم ديزملا ليغشت نكمي ،ءديفم تامولعم اءه ءاطخألا حيحصت اءي ف رفوي

```
debug webvpn saml 255
debug webvpn 255
debug webvpn session 255
debug webvpn request 255
```

ءلص تاذا تامولعم

- [ءءءتم ءقءاصملا عم ASA AnyConnect نم \(ءصااالا ءيضا رءافالا ءكبشلا\) VPN نيوكت](#)
(نامألا ءيكاأء زيمرت ءغل) SAML لالاا نم Microsoft Azure نم لمءاوللا
- [Cisco Systems - ءاءنء سءملا ويءقءلا مءءلا](#)

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