

# Microsoft Azure Active Directory REST API فرعون نويوك

## تايي وتحمل

[قمدق ملنا](#)

[قيس اس اس اتمولع](#)

[قيس اس اس الاتاب لطتملنا](#)

[تابل طتملنا](#)

[قمدخلت سملنا تان وكملا](#)

[نويوك تلنا](#)

[هوت سمل ايلاع قفدت لايلاع قماع قرطن](#)

[لماكتللا نويوك](#)

[لماكتللا ISE نويوك](#)

[فلبت خم مادخت سات الاحل ISE قس اي اس قلثما](#)

[قحص لابنم ققحتلنا](#)

[اهحالص او عاطخ الا فاش كتسا](#)

[وق داصم قمدخ عم لكاشم REST](#)

[فرعم وق داصم يف لكاشم REST](#)

[لجه سلات افال مادخت ساب لمعلنا](#)

## ةمدق ملنا

ةيوهه قمدخ لالخ نم هذيفنت مت يذلا Cisco ISE 3.0 ع Microsoft Azure AD دنات سملنا اذه فصي دروملا كلام رورم ظملك دامتعا تان اي ب مادخت ساب.

## قيس اس اس اتمولع

ةي وهلا تامدخ كرحم لماكت نويوك ةيفيك دنات سملنا اذه فصي Microsoft (MS) Azure Active Directory (AD) لقون ةيوهه قمدخ لالخ نم اهحالص او هئاطخ افash كتس او (ROPC) دروملا كلام رورم ظملك دامتعا تان اي ب ةدعاسم ب (ID).

## قيس اس اس الاتاب لطتملنا

[تابل طتملنا](#)

ةيلاتلا عيضا وملاب ةيس اس اس فرعون كيدل نوك نأب Cisco يصوت:

- ةي وهلا فشك تامدخ كرحم (ISE)

روزا ةديسلا

طاب ترالا: هيلع ةضور فمل دويقلا او ROPC لوك ورب ذيفنت مهف

ةمـدـخـتـسـمـلـاـ تـانـوـكـمـلـا

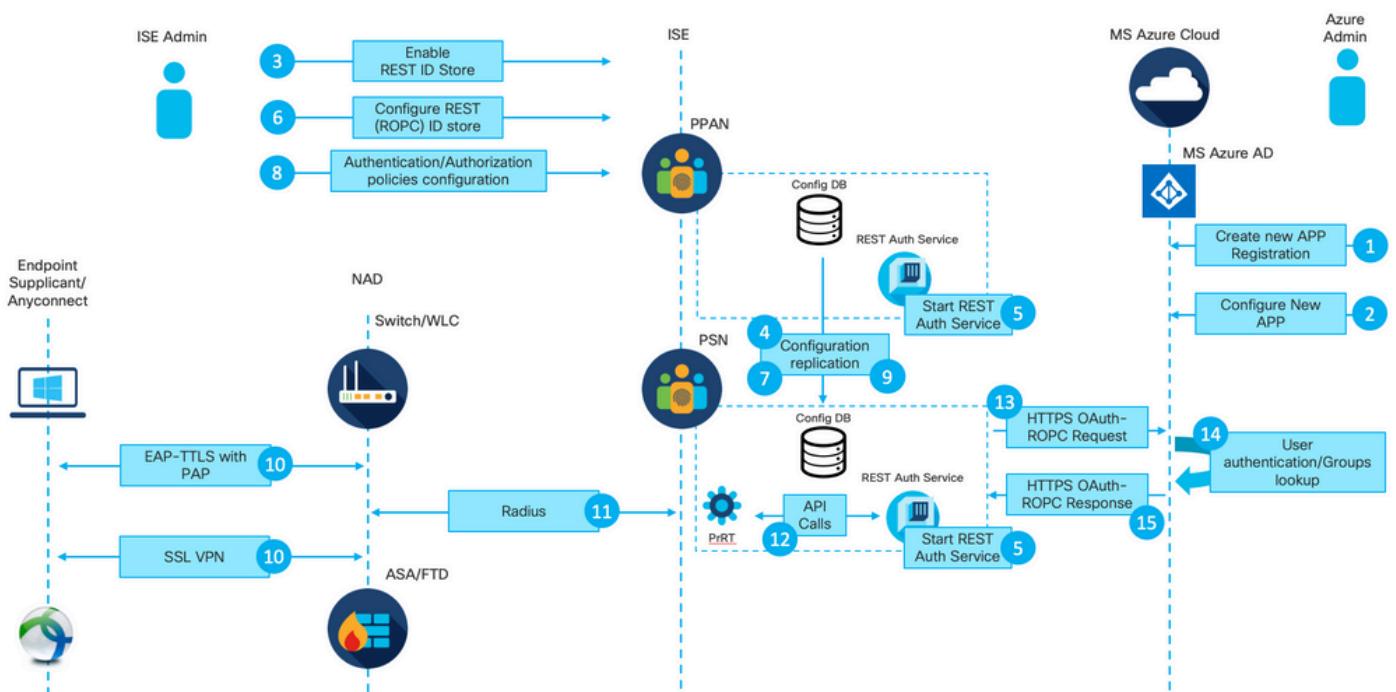
ڦيلاتلا ڦي داملا تانو ڪملا وجمارپلا تارادصا ىلإ دنتسملا اذه ڀف ڦدراولما تامولعملا دنتست

- Cisco 3.0 نم رادص إلـا ISE
  - روزا ةديسـلـا
  - WS-C3850-24P مـع S/W 16.9.2
  - ASA v مـع 9.10 (1)
  - Windows 10.0.18363

ڦڻا خ ڦيلم ڻا يف ڦدوجو ڻا ڦزه ج ڻا نم دن ت س ڻا اذه يف ڦدراو ڻا تام و لع ڻا عاش نا م ڻا ت ناک اذا . (ي ضارتفا) حوس م ڻا ن ي و ڪ ت ب دن ت س ڻا اذه يف ڦدم دخت س ڻا ڦزه ج ڻا ع ي مج ت أد ب رمأ ي ڦل ل م ڻا م ت ح ڻا ر ڻا ي ث ڦل ل ل ڻا كم ه ڻا نم دك أ ت ف ، ل ڻا ي غ ش ڻا د ڻا ي ق ك ڻا ت ك ڻا بش

نیوکل

## یوتسملایل اع قفتلا یل ع ۆماع ۆرظن



لیصافت مادختس امتي . ديدج قیبٹت لیچسٹ عاشناب Azure ۋېھسەم موقىي . 1. عەم لاصتا عاشنال ISE ىلۇق اچال قیبٹتلا اذە

2. مادختس اب قیبٹتلا نیوکت Azure ۋېھسەم ىلۇق بجى:

- لیمۇر رس عاشناب
- ROPC نیكەت
- ۋەنمەمەلە تاپلەاطم ۋەفاضا
- تاقىبٹتلا ۋەجمىرىب ۋەھجاو تانۋەذا فيرعت (API)

3. ئارجا يأ ذىفنت لبىق كىلذب مايىقلاب جى . REST ۋەقداصلەم ۋەمدەخ لىغشىتبا ISE ۋېھسەم موقىي . رخآ

4. لەماكلاب ISE رشن ربىع اھىسنۇن نیوكتىلا تانايىب ۋەدعاق يىف تارىيىغىتلا ۋېباتك مەتت.

5. دىقىعلا عېمەج ىلۇق ۋەحارىلا ۋەقداصلەم ۋەمدەخ أدبىت.

6. 2. ۋەوطخلانم لىصافتىب REST فەرمۇن نزەم نیوكتىب ISE ۋېھسەم موقىي .

7. لەماكلاب ISE رشن ربىع اھىسنۇن نیوكتىلا تانايىب ۋەدعاق يىف تارىيىغىتلا ۋېباتك مەتت.

8. دەۋەمەلە لىسلىسىتلا لىدىغىتىب موقىي وا ديدج ۋېھىنە نزەم لىسلىسىت عاشناب ISE ۋېھسەم موقىي . ضىوفتىلا/ۋەقداصلەملا تاسايىس نیوكتىب موقىي و لۇغۇلاب

9. لەماكلاب ISE رشن ربىع اھىسنۇن نیوكتىلا تانايىب ۋەدعاق يىف تارىيىغىتلا ۋېباتك مەتت.

10. بجى، ROPC لوكوتورب تافىصا اوەملەقىفو . ۋەقداصلەملا ۋېھىتىب ۋېھىنەلە ۋەطقۇن موقۇت . ربىع حەضارىسىنى يىف Microsoft ۋېھىنەلە يىسا سالا ماظۇنلارىدا مەدختىسىملا رورم ۋەملەك رىفۇت ئەمەم دەمىلە ۋەحاتملا ۋەدىھولە ۋەقداصلەملا تارايانىخ نەف ، ۋەقىقەلە ھەذەل ارظانو ئەرفىشەم HTTP لەاصتا يە: ISE لبىق نم

- ئەم (EAP-TTLS) يىقىنلى لقىنلى ۋەقىقەلە ۋەقداصلەملا لوكوتورب
- ۋەقىقەلە خاد ۋەقىرطىك (PAP) رورملا ۋەملەك ۋەقداصلەم لوكوتورب
- AnyConnect SSL VPN مادختس اب PAP ۋەقداصلەم

11. ربع ISE (PSN) ةس اي س ةمدخ ةدقع عم لدابتلا.

مدى تطبيق REST API في تطبيقات RESTful، بما في ذلك طلب (PrRT) ورد (PrRJ)، وذلك لتحسين الكفاءة والمتانة.

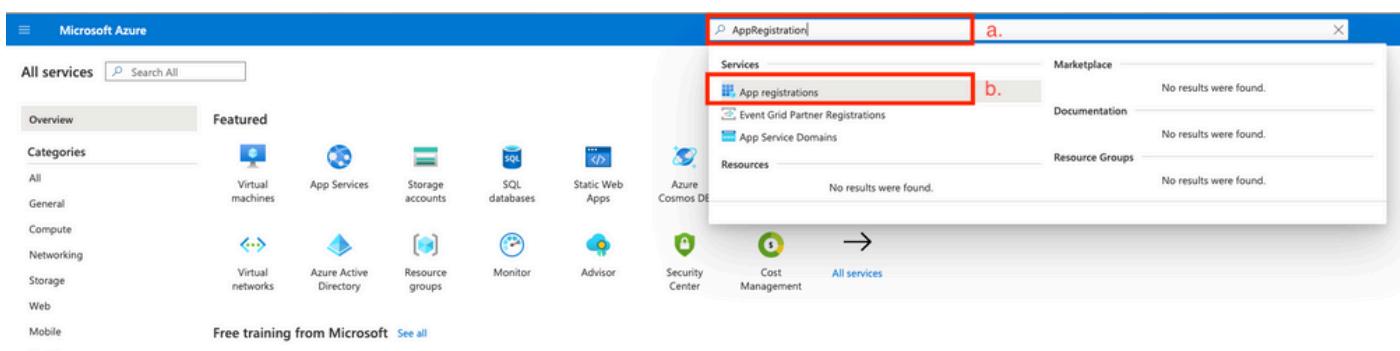
13. صنلا لقن لوکوتورب رب REST ID OAuth ROPC ایل Azure AD بلط ڦمداخ لس رت نمآلا (HTTPS) په عشتل.

14. موقی اب Azure AD عارج اس اوق دا صم ملا سمل دخت سمل ا و موجم ب لجو تاع می دنی.

15. ISE-م. عاجراً تجيئن وختلاً داصصالاً ملأا خليلاً.

## لماکتلل Azure AD نیوکت

روصلایف حضووم وہ امک AppRegister ۃمدخ عقووم ددح 1.

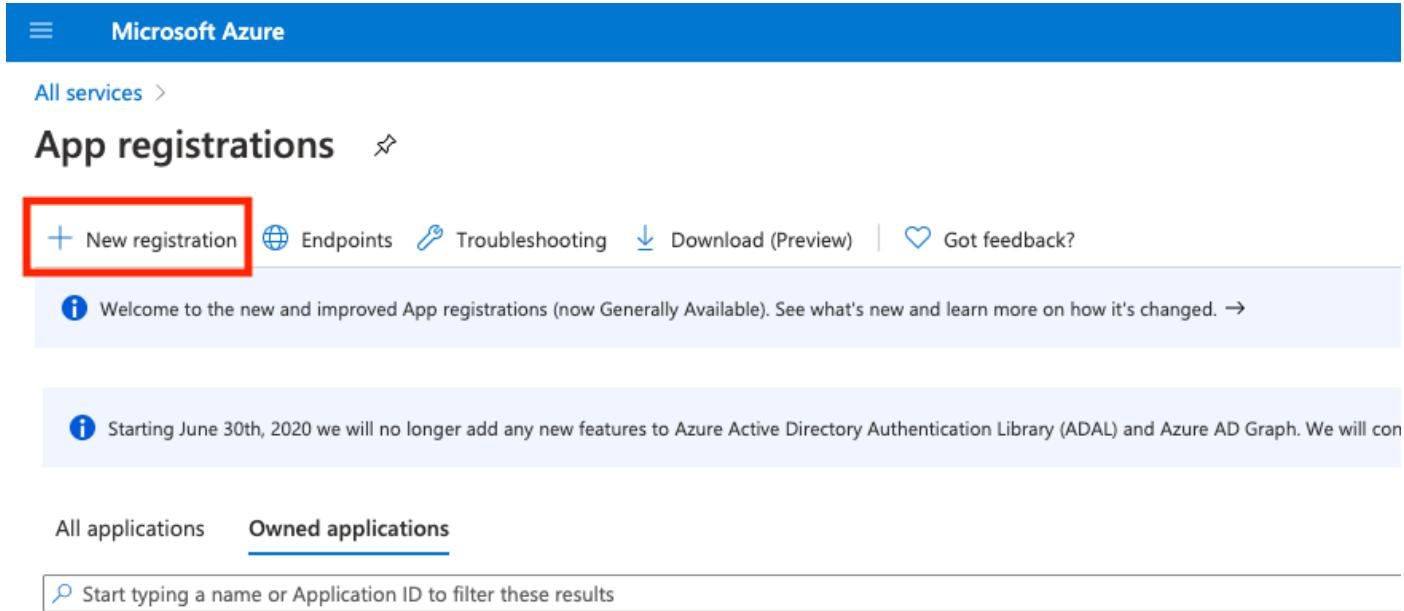


## لکش 2.

یوم عمل اثجبلا طیرش یف AppRegister بتکا.

بـ. قـيـبـطـلـا لـيـجـسـت ةـمـدـخـ قـوـفـ رـقـنـا

دی دج قیب طت لی جست عاشن ا.



## Register an application

\* Name

The user-facing display name for this application (this can be changed later).

Azure-AD-ISE-APP



a.

### Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (DEMO only - Single tenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- Personal Microsoft accounts only

b.

[Help me choose...](#)

### Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web



e.g. https://myapp.com/auth

[By proceeding, you agree to the Microsoft Platform Policies](#)

[Register](#)

C.

يـفـ ةـحـاـتـمـلـاـ تـافـرـعـمـلـاـ نـزـاخـمـ ةـمـئـاـقـ يـفـ مـسـالـاـ اـذـهـ ضـرـعـ مـتـيـ اـمـكـ .ـلـيـوـخـتـلـاـ جـهـنـ نـيـوـكـ دـنـعـ نـزـخـمـ لـسـلـسـتـ نـيـوـكـ يـفـ ةـحـاـتـمـلـاـ تـافـرـعـمـلـاـ نـزـاخـمـ ةـمـئـاـقـ يـفـوـ ةـقـدـاصـمـلـاـ جـهـنـ تـادـادـعـاـ ةـيـوـهـلـاـ.

نـيـوـكـ مـسـقـ نـمـ 8ـ ـةـوـطـخـلـاـ يـفـ Azure ADـ لـيـمـعـلـاـ فـرـعـمـ رـيـفـوـتـبـ مـقـ .ـبـ

جـ لـمـاـكـتـ نـيـوـكـ مـسـقـ نـمـ 7ـ ـةـوـطـخـلـاـ يـفـ Azure ADـ لـيـمـعـلـاـ رـسـ رـيـفـوـتـ جـ

دـ لـمـاـكـتـ نـيـوـكـ مـسـقـ نـمـ 8ـ ـةـوـطـخـلـاـ يـفـ Azure ADـ رـجـأـتـسـمـلـاـ فـرـعـمـ رـيـفـوـتـ .ـدـ

مـتـ مـدـخـتـسـمـلـاـ مـسـاـ نـيـوـكـتـ 5ـ مـدـخـتـسـمـلـاـ مـسـاـ نـيـوـكـtـ ISE PSNـ مـدـخـتـسـمـلـاـ مـسـاـ نـيـوـكـtـ sAMAccountNameـ قـيـسـنـتـ يـفـ هـرـيـفـوـتـ مـتـيـ يـذـلـاوـ ،ـيـئـاهـنـلـاـ مـدـخـتـسـمـلـاـ لـبـقـ نـمـ هـرـيـفـوـتـ لـ نـكـمـيـ الـ ،ـةـلـاحـلـاـ هـذـهـ لـثـمـ يـفـ ؛ـبـوبـ ،ـلـاثـمـلـاـ لـيـبـسـ ىـلـعـ ،ـرـصـتـخـمـلـاـ مـدـخـتـسـمـلـاـ مـسـاـ)ـ يـذـلـاـ مـدـخـتـسـمـلـاـ مـسـاـ ىـلـاـ ـةـفـاـضـمـلـاـ ةـمـيـقـلـاـ يـهـ .ـمـدـخـتـسـمـلـاـ عـقـوـمـ دـيـدـحـتـ ADـ ـقـيـسـنـتـ ىـلـاـ مـدـخـتـسـمـلـاـ مـسـاـ رـاضـحـاـلـ مـدـخـتـسـمـلـاـ هـمـدـقـيـ UPNـ.

 مـدـخـتـسـمـلـاـ مـسـاـ ةـمـسـ ىـلـعـ دـمـتـعـيـ هـنـأـلـ مـدـخـتـسـمـلـاـ ـةـقـدـاصـمـ ىـلـعـ ROPCـ رـصـتـقـيـ :ـةـظـحـاـلـمـ مـدـخـتـسـمـلـاـ مـسـاـ تـامـسـ ىـلـعـ Azure ADـ يـفـ زـاـجـلـاـ تـانـئـاـكـ يـوـتـحـتـ الـ .ـقـدـاصـمـلـاـ عـاـنـثـأـ

قـيـبـطـتـلـاـ لـيـصـاـفـتـلـ ISEـ مـاـدـخـتـسـاـ ةـيـنـاـكـمـاـ نـمـ دـكـأـتـلـلـ رـابـتـخـاـلـاـ لـاـصـتـاـ ىـلـعـ طـغـضـاـ .ـوـ

ىـلـاـ Fـرـعـمـ نـزـخـمـ يـفـ ةـرـفـوـتـمـلـاـ تـاعـوـمـجـمـلـاـ ـةـفـاـضـاـلـ لـيـمـحـتـلـاـ تـاعـوـمـجـمـ ىـلـعـ طـغـضـاـ .ـلـوـؤـسـمـلـاـ ـةـبـرـجـتـ رـوـهـظـ ةـيـفـيـكـ يـلـاـتـلـاـ لـاـشـمـلـاـ حـضـوـيـ RESTـ.

 Cisco CSCvx00345ـ نـمـ ءـاطـخـأـلـاـ حـيـحـصـتـ فـرـعـمـ يـفـ لـلـخـلـاـ ىـلـاـ هـاـبـتـنـاـلـاـ ـيـجـرـيـ :ـةـظـحـاـلـمـ ةـمـزـحـ يـفـ لـلـخـلـاـ حـاـلـصـاـ مـتـ دـقـوـ .ـتـاعـوـمـجـمـلـاـ لـيـمـحـتـ مـدـعـ يـفـ بـبـسـتـيـ هـنـأـلـ ISE 3.0 2ـ.

## Groups

Load Groups

cel

Save

HR-Azure-Users

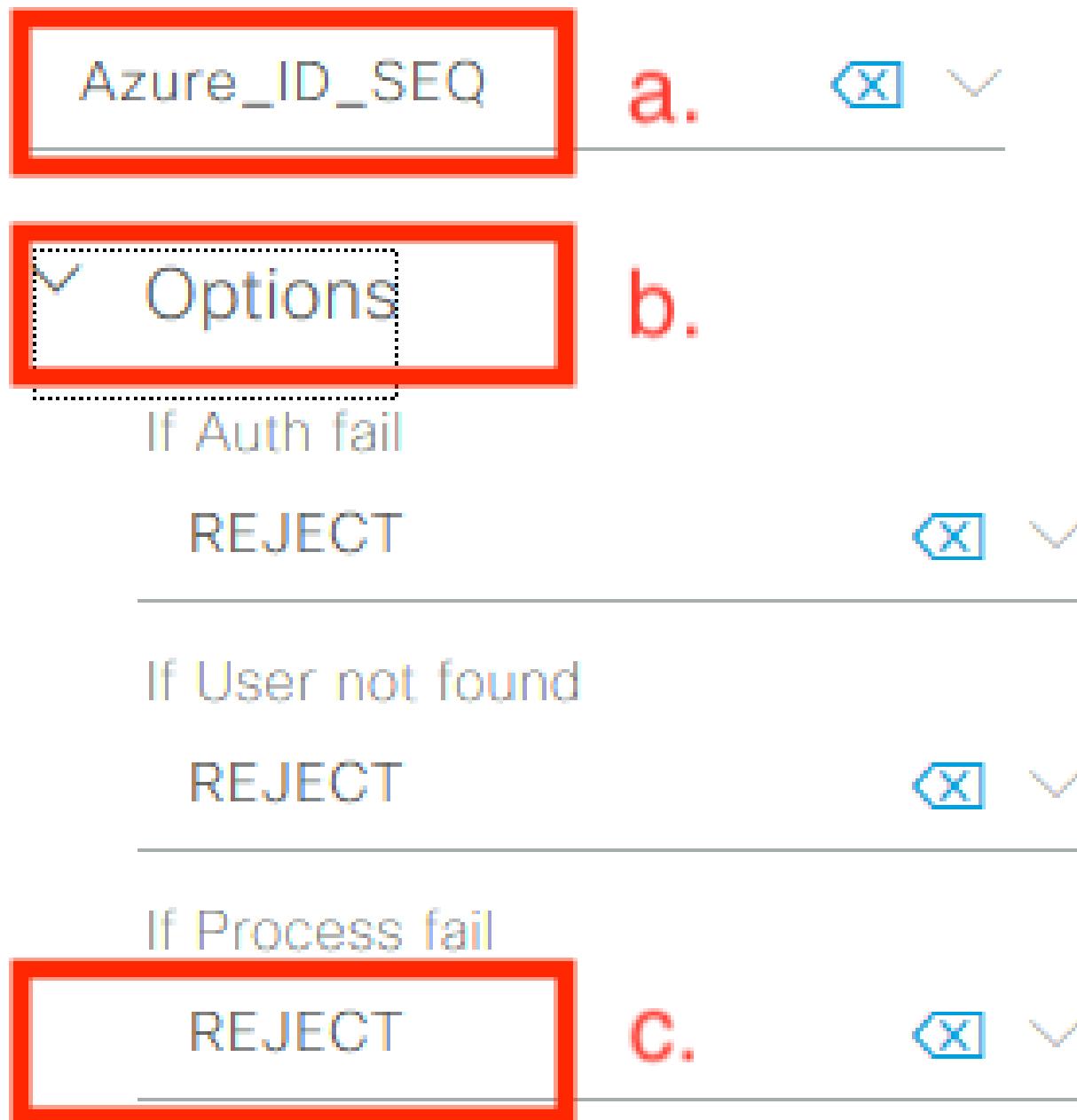
Finance-Azure-Users

IT-Azure-Users

ك ب ة ص ا خ ل ا تار ي ي غ ت ل ا ل ا س را ج.

فرع م نزخ م نم ض ت ي ، د ي د ج ة ي و ه نزخ م ل س ل س ت ع ا ش ن ا راب ت ع ال ا ي ف ع ض ، ة و ط خ ل ا ه ذ ه ي ف . 5. ا ث ي د ح ه ف ا ش ن ا م ت ي ذ ل ا REST.

ي ذ ل ا تاي و ه ل ا نزخ م و أ فرع م نزخ م ل س ل س ت ن ي ي ع ت ا ه ي ف م ت ي ي ت ل ا ة ظ حل ل ل ا ي ف . 6. ى ل ا D R O P ن م ة ي ل م ع ل ا ل ش ف ل ي ض ا ر ت ف ال ا ء ا ر ج ال ا ر ي ي غ ت ب م ق ، ة ق دا ص م ل ا ج ه ن ى ل ع ي و ت ح ي ر و رص ل ا ي ف ح ض و م و ه ا م ك REJECT.



ل ك ش 24.

أ . فرع م نزخ م م د خ ت س ي ي ذ ل ا ة ق دا ص م ل ا ج ه ن ع ق و م د ي د ح ت . REST.

ب . ئ د س ن م ل ا تار اي خ ل ا ة م ئ ا ق ح ت ف .

ن م ئيلمعلل يضارتفالا رئيغتلا ئارج ا لش ف ج DROP ئلإ REJECT.

تالاح هيـف ثـدحت تـقوـيف NAD بـنـاجـىـلـعـتـيـمـعـكـPSNـمـالـعـعـضـوـبـنـجـتـلـاـذـهـعـارـجـاـمـزـلـىـلـثـمـRـEـSـTـIDـنـزـخـمـلـخـادـةـنـيـعـمـلـشـفـ:

- يـفـعـوـمـجـمـيـأـيـفـاوـضـعـسـيـلـمـدـخـتـسـمـلـاـAzure ADـ.
- مـدـخـتـسـمـلـاـرـوـرـمـقـمـلـكـرـئـيـغـتـبـجـيـ.

7. لـيـوـخـتـلـاـجـهـنـىـلـإـفـرـعـمـنـزـخـمـسـوـمـاـقـةـفـاـصـاـ.

Editor

Dictionary	Attribute	ID	Info
All Dictionaries	Aire-Data-Bandwidth-Aver...	7	
Airespace	Aire-Data-Bandwidth-Aver...	13	
Alcatel-Lucent	Aire-Data-Bandwidth-Burs...	9	
Aruba	Aire-Data-Bandwidth-Burs...	15	
Azure_AD	Aire-Real-Time-Bandwidth...	8	
Brocade	Aire-Real-Time-Bandwidth...	14	
CERTIFICATE	Aire-Dat-Times-Bandwidth	16	
CWA			
Cisco-BBSM			
Cisco-VPN3000			
Cisco			
DEVICE			
EXAMPLE			
EndPoints			
Guest			
H3C			
HP			
IdentityGroup			
InternalUser			
Juniper			

لـكـشـ25ـ.

أـسـوـمـاـقـلـلـلـقـلـدـسـنـمـلـاـمـئـاـوـقـلـاـةـفـاـكـحـتـفـ.

بـكـبـصـاخـلـاـRـEـSـTـIDـنـزـخـمـقـقـيـرـطـسـفـنـبـىـمـسـمـلـاـسـوـمـاـقـلـاـنـاـكـمـدـدـحـ.

نـزـخـمـسـوـمـاـقـيـفـةـرـفـوـتـمـلـاـةـدـيـحـوـلـاـةـمـسـلـاـ،ـIـSـE~3~.~0ـ،ـيـتـحـ(ـيـجـرـاخـةـيـوـهـتـاعـوـمـجـمـةـفـاـصـاـ).ـيـجـرـاخـةـعـوـمـجـمـيـهـFـRـUـMـ

## Editor

The screenshot shows the Cisco ISE Policy Editor interface. A configuration step is open, titled "Azure\_AD·ExternalGroups". The condition "Equals" is selected, and the target field "Choose from list or type" contains the placeholder text "Finance-Azure-Users", "HR-Azure-Users", and "IT-Azure-Users". Below the list are "Duplicate" and "Save" buttons. To the left, a dashed box indicates a previous configuration step involving "Dot1x-PEAP" and "Dot1x-Wireless-Wired".

لکش 26.

### فلت خم مادختس ا تالاحل ISE اس اي س ڈلثما

ڈک بشلا یل ا لوصولا سوماق نم EAP ڈفن طرش مادختس ا نکمی، ڈقداصم ڈلاح یف ڈروصل ا یف حضوم وہ امک تالواح ڈقباطمل.

The screenshot shows the Cisco ISE Policy Editor interface. It displays two policy conditions: "Dot1x-PEAP" and "Dot1x-TTLS". The "Dot1x-PEAP" condition has an "AND" clause with "Dot1x-Wireless-Wired" and "Network Access-EapAuthentication EQUALS EAP-MSCHAPv2". The "Dot1x-TTLS" condition also has an "AND" clause with "Dot1x-Wireless-Wired" and "Network Access-EapTunnel EQUALS EAP-TTLS". A red box highlights the "Dot1x-TTLS" condition. To the right, a dropdown menu for "All\_User\_ID\_Stores" is shown, with "a." and "b." pointing to specific items: "a." points to "Dot1x-TTLS" and "b." points to "Azure\_AD\_REST\_ID\_Sto...".

لکش 27.

یل ا ہھیجوت ڈداع ا مزلي یتل ا تالواح مل ا ڈقباطمل EAP-TTLS ل یواس مل ا EAP ڈفن دیدھت ا فرعم نزخم REST.

دومع یف ہيلع یوتحي یذلا ، تایوہلا نزخم لسلست و ا ڈرشابم REST فرعم نزخم یف ددھ ب "مادختس ال".

عون ع م Azure AD نم ڈیجراخ ل ا تاعومجملا مادختس ا نکمی ، ڈیدرفل ا ل یوخت ل ا تاس اس اس لخاد ڈفن EAP:

✓ Dot1X-TTLS-Azure-Finance	AND	Dot1x-Wireless-Wired
		Network Access-EapTunnel EQUALS EAP-TTLS
		Azure_AD-ExternalGroups EQUALS Finance-Azure-Users
✓ Dot1X-TTLS-Azure-HR	AND	Dot1x-Wireless-Wired
		Network Access-EapTunnel EQUALS EAP-TTLS
		Azure_AD-ExternalGroups EQUALS HR-Azure-Users
✓ Dot1X-TTLS-Azure-IT	AND	Dot1x-Wireless-Wired
		Network Access-EapTunnel EQUALS EAP-TTLS
		Azure_AD-ExternalGroups EQUALS IT-Azure-Users

لکش 28.

زیممک قفن ۋە وەجەم مس ا مادختسإ كنكمي، ئەكپىش ىلى دىتسەلە قىفتىلى ئەپسەنلىپ: ۋەقىداصەملا جەن:

Status	Rule Name	Conditions	Action	Use
Green	Cisco-VPN3000-CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS skuchere	Azure-AD	Azure_AD_REST_ID_Sto...	Options

لېوختلا جەن:

✓ VPN-Azure-Finance	AND	Cisco-VPN3000-CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS skuchere
		Azure_AD-ExternalGroups EQUALS Finance-Azure-Users
✓ VPN-Azure-HR	AND	Cisco-VPN3000-CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS skuchere
		Azure_AD-ExternalGroups EQUALS HR-Azure-Users
✓ VPN-Azure-IT	AND	Cisco-VPN3000-CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS skuchere
		Azure_AD-ExternalGroups EQUALS IT-Azure-Users

لکش 29.

## ۆحصىلا نەم ققحتلا

حىحص لەكش بىيوكىتلا لەم دىكأتلى مىسىقىلا اذە مەختىسا.

1. REST دەقۇرىلىع ئەقداشىم ئەمدىخ لېغشت نەم دىكأت.

نامالا ئەقبەط ئەقبەط يەف show application status ise رەمألا ذىفنت كەمزلەي، كەلذ نەم ققحتلى.

فدهل ا ise ةدقع نم (SSH):

<#root>

```
skuchere-ise30-1/admin# show application status ise
```

ISE PROCESS NAME	STATE	PROCESS ID
Database Listener	running	101790
Database Server	running	92 PROCESSES
Application Server	running	39355
Profiler Database	running	107909
ISE Indexing Engine	running	115132
AD Connector	running	116376
M&T Session Database	running	107694
M&T Log Processor	running	112553
Certificate Authority Service	running	116226
EST Service	running	119875
SXP Engine Service	disabled	
Docker Daemon	running	104217
TC-NAC Service	disabled	
pxGrid Infrastructure Service	disabled	
pxGrid Publisher Subscriber Service	disabled	
pxGrid Connection Manager	disabled	
pxGrid Controller	disabled	
PassiveID WMI Service	disabled	
PassiveID Syslog Service	disabled	
PassiveID API Service	disabled	
PassiveID Agent Service	disabled	
PassiveID Endpoint Service	disabled	
PassiveID SPAN Service	disabled	
DHCP Server (dhcpd)	disabled	
DNS Server (named)	disabled	
ISE Messaging Service	running	104876
ISE API Gateway Database Service	running	106853
ISE API Gateway Service	running	110426
Segmentation Policy Service	disabled	
REST Auth Service	running	63052
SSE Connector	disabled	

نم مسق .تاوطلخلا نم ققحت) ةقداصملاتقويف REST فرعم نزخم مادختسا نم ققحت 2. يليصفتلا ةقداصملاريرقت).

### 15013 Selected Identity Source - Azure\_AD

- 25103 Perform plain text password authentication in external REST ID store server - Azure\_AD a.
- 25100 Connecting to external REST ID store server - Azure\_AD b.
- 25101 Successfully connected to external REST ID store server - Azure\_AD (⌚ Step latency=1660 ms) c.
- 25104 Plain text password authentication in external REST ID store server succeeded - Azure\_AD d.
- 25107 REST ID store server respond with groups - Azure\_AD e.
- 25110 User groups inserted to session cache - Azure\_AD f.

22037 Authentication Passed

ددحملـا REST فـرعـم نـزمـعـم يـداعـلـا صـنـلـا ظـقـدـاصـمـا أـدبـيـاـ.

بـ. عـم أـشـنـمـلـا لـاصـتـالـا اـشـنـمـلـا Azure Cloud.

ةـهـجـاـوـمـ ةـلـاحـ يـفـ. اـنـهـ ةـضـورـمـلـا لـاقـتـنـالـا نـمـزـ ةـمـيـقـ ئـلـا هـبـتـنـاـ - ةـيـلـعـفـلـا ةـقـدـاصـمـلـا ةـوـطـخـ جـ اـنـاـ قـفـدـتـ ئـلـعـ اـذـهـ رـثـؤـيـ، رـيـبـكـ لـوـصـوـنـمـزـl Aure اـنـمـزـ عـمـ كـبـ ةـصـاخـلـا تـاـقـدـاصـمـلـا عـيـمـ جـ رـقـتـسـمـ رـيـغـ لـمـاـكـلـابـ ISE اـنـمـزـ عـجـارـ، كـلـذـلـ ةـجـيـتـنـوـ، رـخـآـلـا.

ةـقـدـاصـمـلـا حـاجـنـ دـيـكـأـتـ - دـ.

كـلـذـ ئـلـعـ اـدـرـ ةـمـدـقـمـلـا ةـعـوـمـجـمـلـا تـانـاـيـبـ دـيـكـأـتـ - ٥ـ.

لـوـحـ لـيـصـاـفـتـلـا نـمـ دـيـزـمـلـ. نـيـمـدـخـتـسـمـلـا ةـعـوـمـجـمـ تـانـاـيـبـبـ لـوـهـأـمـلـا لـمـعـلـا ةـسـلـجـ قـاـيـسـ - وـ طـابـتـراـ - لـاقـمـلـا اـذـهـ ةـعـجـارـمـ عـجـارـ، ISE اـنـمـزـ ةـسـلـجـ ةـرـادـاـ ةـيـلـمـ.

ةـرـظـنـلـا نـمـ قـقـحـتـلـاـ "ـمـسـقـلـ"ـ ةـعـقـوـتـمـلـا لـيـوـخـتـلـاـ/ـةـقـدـاصـمـلـا تـاسـاـيـسـ دـيـدـحـتـ نـمـ دـكـأـتـ. يـلـيـصـفـتـلـا ةـقـدـاصـمـلـا رـيـرـقـتـ يـفـ اـذـهـ "ـةـمـاعـلـاـ".

## Overview

Event	5200 Authentication succeeded
Username	bob
Endpoint Id	ED:37:E1:08:57:15 
Endpoint Profile	
Authentication Policy	SPRT-Policy-Set >> Azure-AD
Authorization Policy	SPRT-Policy-Set >> Azure-Finance
Authorization Result	PermitAccess

لکش 30.

## اھالص او ئاطخاً فاشكتسا

اھالص او نيوكتل اھالص ئاطخاً فاشكتسا اھم ادختسا كىنكمى يىتلا تامولعملا مسقىلا اذه رفوي.

## ۋەقىداصم ئەمدەخ بۇقلىعىتمەل لەكاشمىلدا REST

ئەجارمۇب عىدبىلا كەمزلىي ،اھالص او REST ۋەقىداصم ئەمدەخ بۇقلىعىتمەت لەكاشىم ئەم ئاطخاً فاشكتسا اھم ADE.log. / adeos/ade فەلم.

يىف مەكھىتلا - يە REST ۋەقىداصم ئەمدەخ بۇقلىعىتمەل لەكاشمىلدا.

ۋەقىداصم ئەمدەخ لېغشت ئەدب ئەي فيك لاثىملا اذه حضورى:

```
2020-08-30T11:15:38.624197+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] S
2020-08-30T11:15:39.217794+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] i
2020-08-30T11:15:39.290301+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] I
2020-08-30T11:15:39.291858+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] D
2020-08-30T11:15:39.293768+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] L
2020-08-30T11:15:39.359490+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] E
2020-08-30T11:15:42.789242+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] L
2020-08-30T11:15:42.830411+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] D
2020-08-30T11:15:42.832131+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] S
2020-08-30T11:15:42.844051+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] i
2020-08-30T11:15:53.479968+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] C
2020-08-30T11:15:55.325973+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] C
2020-08-30T11:15:57.103245+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] C
2020-08-30T11:15:57.105752+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] C
2020-08-30T11:15:57.278374+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] C
```

نم ، عقوتم ریغ لکشب ضفختن و ادبلا یف ۆمدخلە اھیف لشفت یتلا تالاحلا یف لکاش ملل ریثم ینمز راطا لوح ADE.Log ۆعجارم لالخ نم عدبلا امئاد یقطنەملە.

## فرعم ۆقاداصم لکاشم REST

ریرقەت نم عدبلا امئاد کەمزلی، فرعم نزخم مادختسە دنەن ۆقاداصم لاشف ۆللاح یف عطقەم ۆیور کەنکەمی، "ىرخألا تامسلا" ۆقطنم یف RestAuthErrorMsg ۆباجس لباق نم ھەعاجرا مت أطخىلە یوتحىي Azure:

Error Key - invalid\_client | Error Description -  
AADSTS7000218: The request body must contain the  
following parameter: 'client\_assertion' or 'client\_secret'. Trace  
ID: e33912ff-18af-4f81-acc9-efda91873900 Correlation ID:  
519641db-a8ea-49df-85aa-ddd2b53a0c28 Timestamp:  
2020-09-13 19:11:47Z | Error Codes - [7000218] | Error URI  
- <https://login.microsoftonline.com/error?code=7000218>

لکش 31.

## لجسلا تافلم مادختساب لمعلا

اھل ئاطخألا حیحصت نیکەمەت مەتی، REST ID ۆزىمەل ھەمەكتەملا مەيەقتىلا بېسپ 3.0 یف تافلم یف فرعمب ۆقلۇتمەلە تالجسلا عېمەج نېزخەت مەتی. يىضاارتىفا لکشب (رماؤلا رەتس ۆچجاو) CLI ربۇع اھضرۇن نكەمی یتلا:

```
skuchere-ise30-1/admin# sh logging application | i ropc  
755573 Oct 04 2020 09:10:29 ropc/ropc.log
```

```
skuchere-ise30-1/admin# sh logging application ropc/ropc.log  
23:49:31.449 [http-nio-9601-exec-6] DEBUG c.c.i.r.c.ROPCController - Starting ROPC auth flow  
23:49:31.788 [http-nio-9601-exec-6] DEBUG c.c.i.r.u.ScimUtility - Found user and pass in the SCIM filter
```

سېلىو ropc.log ۋە فەلمەلە مەسا نأ ظحال، تېبىتمەلە حیحصەتلىعا عم 3.0 یف rest-id-store.log. رېغتى مل دلجمەلە مەسا نألى ھەرىفوت مەت يىذلە قېباشلا ثىحبلا لاثم لمعىي.

ةمۇزەنەد ISE لە نم تىجىختىسا تىنەن عېطتىسى دربم اذە نأ وە.

ةفلتىخەم لەم رېغولەم تاھويرانىس رەھەت یتلا لجسلا ۆلثەمأ ضۇب يىلى امېف:

ةظحالىم نكەمی ISE. ۆدقۇع لباق نم اھب قۇۋۇم Azure Graph نوكتىلە امدىن ۆداھاشلە یف أطخىلە 1. فرعم نزخم دادۇيىف تاھۇمچەمەلە لېمەت مەتى امدىن ۆداھاشلە یف أطخىلە اذە REST.

```
20:44:54.805 [http-nio-9601-exec-7] ERROR c.c.i.r.p.a.AzureIdentityProviderFacade - Couldn't fetch application certificate
javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: No trusted certificate found
at sun.security.ssl.Alerts.getSSLError(Alerts.java:192)
at sun.security.ssl.SSLSocketImpl.fatal(SSLocketImpl.java:1946)
at sun.security.ssl.Handshaker.fatalSE(Handshaker.java:316)
at sun.security.ssl.Handshaker.fatalSE(Handshaker.java:310)
at sun.security.ssl.ClientHandshaker.serverCertificate(ClientHandshaker.java:1639)
```

نم اهب قووثوم ریغ تاقيب طت ةجمرب ةهج او ةداهش نأ ئلإ ئلكشملا هذه ريشت  
يف تبثم DigiCert نم يمومع رذج G2 قدصم عجرم ىلع ISE 3.0.0.458 يوتحي الـ ISE.  
لخلالا يف قووثوم اذهو. بـ قووثوملا نزخملـا

عجرمـلا تـيـبـثـتـ كـمـزـلـيـ، ئـلـكـشـمـلـاـ هـذـهـ ئـجـلـاعـمـلـ Ciscoـ نـمـ ئـاطـخـأـلـاـ حـيـحـصـتـ فـرـعـمـ -  
بـ قـوـثـومـكـ قـمـالـعـهـ عـضـوـوـ لـ ISEـ لـ بـ قـوـثـومـلـاـ نـزـخـمـلـاـ يـفـ G2ـ قدـصـمـلـاـ تـامـدـخـلـ Ciscoـ.

2. ئـطـاخـ قـيـبـطـتـ فـرـعـمـ - اـنـهـ نـمـ ئـدـاهـشـلـاـ لـيـزـنـتـ نـكـمـيـ <https://www.digicert.com/kb/digicert-root-certificates.htm>

3. حـيـحـصـ رـيـغـ قـيـبـطـتـ فـرـعـمـ.

```
10:57:53.200 [http-nio-9601-exec-1] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with truststore
10:57:54.205 [http-nio-9601-exec-1] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Status code: 401
10:57:54.206 [http-nio-9601-exec-1] ERROR c.c.i.r.c.ROPCController - Request related Error
com.cisco.ise.ROPC.entities.exceptions.InvalidApplicationAuthException: AADSTS7000215: Invalid client secret
Trace ID: 99cc29f7-502a-4aaa-b2cf-1daeb071b900
Correlation ID: a697714b-5ab2-4bd1-8896-f9ad40d625e5
Timestamp: 2020-09-29 09:01:36Z - Error Codes: [7000215]
at com.cisco.ise.ROPC.providers.azure.AzureIdentityProviderFacade.authenticateApplication(AzureIdentityProviderFacade.java:100)
```

4. مـدـخـتـسـمـلـاـ ىـلـعـ روـثـعـلـاـ مـتـيـ مـلـ.

```
21:34:36.090 [http-nio-9601-exec-4] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with truststore
21:34:36.878 [http-nio-9601-exec-4] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Status code: 401
21:34:36.879 [http-nio-9601-exec-4] ERROR c.c.i.r.c.ROPCController - Request related Error
com.cisco.ise.ROPC.entities.exceptions.InvalidApplicationAuthException: AADSTS700016: Application with identifier '6dbd0fdd-0128-4ea8-b06a-5e78f37c0100' was not found
Trace ID: 6dbd0fdd-0128-4ea8-b06a-5e78f37c0100
Correlation ID: eced0c34-fcc1-40b9-b033-70e5abe75985
Timestamp: 2020-08-31 19:38:34Z - Error Codes: [700016]
```

5. مـدـخـتـسـمـلـاـ ىـلـعـ روـثـعـلـاـ مـتـيـ مـلـ.

```
10:43:01.351 [http-nio-9601-exec-2] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Status code: 401
10:43:01.352 [http-nio-9601-exec-2] ERROR c.c.i.r.c.ROPCController - Request related Error
com.cisco.ise.ROPC.entities.exceptions.ROPCResponseErrorException: {"error": "invalid_grant", "error_description": "The provided grant token is invalid."}
at com.cisco.ise.ROPC.providers.azure.AzureIdentityProviderFacade.authenticateUser(AzureIdentityProviderFacade.java:100)
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.authenticateUser(AzureROPCFlow.java:100)
```

```
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.doEntireFlow(AzureROPCFlow.java:69)
at com.cisco.ise.ROPC.controllers.ROPCCController.ROPCAuthFlow(ROPCCController.java:168)
at com.cisco.ise.ROPC.controllers.ROPCCController.get(ROPCCController.java:85)
at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:62)
at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
at java.lang.reflect.Method.invoke(Method.java:498)
```

هؤاشن! مت يذلا مدخلت سملل ثدحي نأ نكمي ام ظداع - مدخلت سملل رورم ظملك ئيجالص تهتنا.  
تقو يف اهرييغت بجي Azure لوؤسم ئطس اووب اهفييرعت مت يتلل رورملل ظملك نأ ئيچ اثيدح  
تىل لوخدلل ليجسـت Office365.

```
10:50:55.096 [http-nio-9601-exec-4] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Sta
10:50:55.097 [http-nio-9601-exec-4] ERROR c.c.i.r.c.ROPCCController - Request related Error
com.cisco.ise.ROPC.entities.exceptions.ROPCResponseException: {"error":"invalid_grant","error_desc
at com.cisco.ise.ROPC.providers.azure.AzureIdentityProviderFacade.authenticateUser(AzureIdentityProvide
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.authenticateUser(AzureROPCFlow.java:100)
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.doEntireFlow(AzureROPCFlow.java:69)
at com.cisco.ise.ROPC.controllers.ROPCCController.ROPCAuthFlow(ROPCCController.java:168)
at com.cisco.ise.ROPC.controllers.ROPCCController.get(ROPCCController.java:85)
at sun.reflect.GeneratedMethodAccessor53.invoke(Unknown Source)
at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
at java.lang.reflect.Method.invoke(Method.java:498)
```

6. ئەھيچىص رىغ API تان وذا ببىسب تاعومجمـلـا ليـمـحـتـ نـكـمـيـ الـ.

```
12:40:06.624 [http-nio-9601-exec-9] ERROR c.c.i.r.u.RestUtility - Error response in 'GET' request. Sta
"error": {
"code": "Authorization_RequestDenied",
"message": "Insufficient privileges to complete the operation.",
"innerError": {
"date": "2020-08-30T10:43:59",
"request-id": "da458fa4-cc8a-4ae8-9720-b5370ad45297"
}
}
}'
```

7. بـنـاجـىـلـعـ ROPC بـحـامـسـلـاـ مـتـيـ الـ اـمـدـنـعـ ئـقـدـاصـمـلـاـ لـشـفـتـ.

```
11:23:10.824 [http-nio-9601-exec-2] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tr
11:23:11.776 [http-nio-9601-exec-2] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Sta
11:23:11.777 [http-nio-9601-exec-2] ERROR c.c.i.r.c.ROPCCController - Request related Error
com.cisco.ise.ROPC.entities.exceptions.ROPCResponseException: {"error":"invalid_client","error_desc
at com.cisco.ise.ROPC.providers.azure.AzureIdentityProviderFacade.authenticateUser(AzureIdentityProvide
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.authenticateUser(AzureROPCFlow.java:100)
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.doEntireFlow(AzureROPCFlow.java:69)
at com.cisco.ise.ROPC.controllers.ROPCCController.ROPCAuthFlow(ROPCCController.java:168)
at com.cisco.ise.ROPC.controllers.ROPCCController.get(ROPCCController.java:85)
```

```
at sun.reflect.GeneratedMethodAccessor53.invoke(Unknown Source)
at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
at java.lang.reflect.Method.invoke(Method.java:498)
```

8. بناجىل عوومجم يألىا يمتنى ال مدخل سملانأ ارظن قداصملالشافت Azure.

```
21:54:55.976 [http-nio-9601-exec-5] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tr
21:54:57.312 [http-nio-9601-exec-5] ERROR c.c.i.r.p.a.AzureROPCFlow - Missing claims in the id token: "
21:54:57.313 [http-nio-9601-exec-5] ERROR c.c.i.r.c.ROPCController - Server Error
com.cisco.ise.ROPC.entities.exceptions.JsonParseException: Json exception: Missing claims in the id tok
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.validateIdTokenPayload(AzureROPCFlow.java:93)
```

9. عوومجملا داعتس او حجانلا مدخل سملانأ قداصم.

```
11:46:03.035 [http-nio-9601-exec-7] DEBUG c.c.i.r.c.ROPCController - Starting ROPC auth flow
11:46:03.037 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.ScimUtility - Found user and pass in the SCIM filter
11:46:03.037 [http-nio-9601-exec-7] DEBUG c.c.i.r.c.ROPCController - Getting the right ROPC handler for
11:46:03.037 [http-nio-9601-exec-7] DEBUG c.c.i.r.c.ROPCController - Getting user groups from handler
11:46:03.038 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Start building http client
11:46:03.039 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Start proxy load for URI 'https://
11:46:03.039 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Start check if host is bypass
11:46:03.039 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Iterating bypass hosts '192.168.1.1
11:46:03.040 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Proxy server found with address
11:46:03.040 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Start adding proxy credentials
11:46:03.040 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - No credentials found for proxy
11:46:03.040 [http-nio-9601-exec-7] DEBUG c.c.i.r.e.c.CertificateCache - Created SSLContext with TLSv1.3
11:46:03.041 [http-nio-9601-exec-7] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tr
11:46:04.160 [http-nio-9601-exec-7] DEBUG c.c.i.r.c.ROPCController - The ROPCHandlerResponse is: {
"schemas" : [ "urn:ietf:params:scim:schemas:core:2.0:User" ],
"userName" : "username",
"name" : {
"formatted" : "bob"
},
"displayName" : "bob",
"groups" : [ {
"value" : "17db2c79-fb87-4027-ae13-88eb5467f25b"
} ],
"roles" : [ ]
}
```

## هـ لـ وـ لـ جـ رـ تـ لـ اـ هـ ذـ هـ

ةـ يـ لـ آـ لـ اـ تـ اـ يـ نـ قـ تـ لـ اـ نـ مـ مـ جـ مـ وـ عـ مـ اـ دـ خـ تـ سـ اـ بـ دـ نـ تـ سـ مـ لـ اـ اـ ذـ هـ تـ مـ جـ رـ تـ  
لـ اـ عـ لـ اـ ءـ اـ حـ نـ اـ عـ يـ مـ جـ يـ فـ نـ يـ مـ دـ خـ تـ سـ مـ لـ لـ مـ عـ دـ ئـ وـ تـ حـ مـ يـ دـ قـ تـ لـ ةـ يـ رـ شـ بـ لـ اـ وـ  
اـ مـ كـ ةـ قـ يـ قـ دـ نـ وـ كـ تـ نـ لـ ةـ يـ لـ آـ ةـ مـ جـ رـ تـ لـ ضـ فـ اـ نـ اـ ةـ ظـ حـ اـ لـ مـ ئـ جـ رـ يـ .ـ صـ اـ خـ لـ اـ مـ هـ تـ غـ لـ بـ  
يـ لـ خـ تـ .ـ فـ رـ تـ حـ مـ مـ جـ رـ تـ مـ اـ هـ دـ قـ يـ يـ تـ لـ اـ ةـ يـ فـ اـ رـ تـ حـ اـ لـ اـ ةـ مـ جـ رـ تـ لـ اـ عـ مـ لـ اـ حـ لـ اـ وـ  
ىـ لـ إـ أـ مـ ئـ اـ دـ عـ وـ جـ رـ لـ اـ بـ يـ صـ وـ تـ وـ تـ اـ مـ جـ رـ تـ لـ اـ هـ ذـ هـ ةـ قـ دـ نـ عـ اـ هـ تـ يـ لـ وـ ئـ سـ مـ  
(رـ فـ وـ تـ مـ طـ بـ اـ رـ لـ اـ)ـ يـ لـ صـ أـ لـ اـ يـ زـ يـ لـ جـ نـ إـ لـ اـ دـ نـ تـ سـ مـ لـ اـ).