

AnyConnect عالم عمل AD ةقداصم نيوكت

تايوت حمل

[قم دق م ل](#)

[ةيساس أ ل تابل ط م ل](#)

[تابل ط م ل](#)

[ةمدخت س م ل تانوك م ل](#)

[ةيساس أ تامول عم](#)

[نيوك ت ل](#)

[ويراني س ل او ةكبش ل ل يطي طخ ت ل م س ر ل](#)

[Active Directory تان يوك ت](#)

[ةعوم حمل ل DN و ي س اس أ ل LDAP DN دي دخت](#)

[FTD باسح عاش ن](#)

[\(يراي تخا\) تانال عا تاعوم حمل ل ني مدخت س م ة فاض او تانال عا تاعوم حمل عاش ن](#)

[STARTTLS و LDAPs ل طوق ف بولطم\) LDAP ب صاخ ل SSL ةداهش رذخ سن](#)

[FMC تان يوك ت](#)

[صيخر ت ل نم ق قحت ل](#)

[دادع ل م ل](#)

[AD ةقداصم ل AnyConnect نيوك ت](#)

[مدخت س م ل ةي وول نام أ ل تاس ايس نيوك ت و ةي وول ا جهن نيوك ت](#)

[NAT عانثت س ل نيوك ت](#)

[رش ت ل](#)

[ةحص ل نم ق قحت ل](#)

[يئا ه ت ل بي ت ر ت ل](#)

[AAA نيوك ت](#)

[AnyConnect نيوك ت](#)

[لن نم ق قحت ل او AnyConnect نم ل وول ا ي ف م كحت ل ةس ايس دع او ق ب ل اص ت ل](#)

[FMC ل اص ت ل ا دج ا ما دخت س ا ب ق قحت ل](#)

[اهال ص او عا طخ أ ل فاش ك ت س ا](#)

[عا طخ أ ل احي حص ت](#)

[ةلماع ل LDAP عا طخ أ ل احي حص ت](#)

[LDAP مداخ ب ل اص ت ل عاش ن رذعت](#)

[ةحي حص ريغ رور م ل ةملك و أ و DN ي ف طب ر ل ل جس](#)

[مدخت س م ل م س ا ي ل ع روث ع ل LDAP مداخ ي ل ع رذعت](#)

[مدخت س م ل م س ا ل ةحي حص ريغ رور م ل ةملك](#)

[AAA راب ت خا](#)

[منحل ا طاق ت ل تاي ل مع](#)

[Windows Server ا دج ا ض راع تال جس](#)

ةمدق م ل

AnyConnect عالم عمل Active Directory (AD) ةقداصم نيوك ت ةي ف ي ك دن ت س م ل اذه حضوي FirePOWER (FTD) دي ده ت ي عاف دب ةل ص ت م ل

نيت وعومجم ونيمدختسم تاباسح ةثالث عاشنإ متي ، اذه نيوكتال

نيمدختسمال تاباسح

- مداخ ب طابترالاب FTD ل حامس لل ليلد باسحك باسحلا اذه مادختسإ متي FTD لوؤسم Active Directory.
- مدختسملا ةيوه راهظال رابتخالال لوؤسم باسح مدختسي : تامولعملال ةينقت لوؤسم
- مدختسملا ةيوه راهظال مدختسي رابتخال مدختسم باسح : رابتخالال مدختسم

تاعومجمال

- راهظال اهليل تامولعملال ةينقت لوؤسم ةفاضل متت رابتخال ةعومجم AnyConnect Admins: RDP لوصول اهيدل ةعومجمال اذه . مدختسملا ةيوه
- مدختسملا ةيوه ضرعل مدختسمال رابتخال ةعومجم ةفاضل متت AnyConnect ومدختسم . طقف Windows Server ل HTTP لوصول اهيدل ةعومجمال اذه

Active Directory تانويكت

ليلق ددع رفوت مزلي ، FTD لعل بسانم لكش ب مدختسملا ةيوهو AD ةقداصم نيوكت لجا نم ميقال نم

لعل نيوكتال ءارجل لبق Microsoft Server لعل اهيعمجت وأ ليلصافال اذه عيمج عاشنإ بجي FMC . يه ةسيسيرل ميقال

- لجال مسال :

لجال مسال وه example.com نوكي ، اذه نيوكتال ليلدي . مداخال لجال مسال وه اذه

- مداخال IP/FQDN ناوع :

بجبي ف FQDN مادختسإ مت اذا . Microsoft مداخال لوصول مدختسمال FQDN وأ IP ناوع FQDN لجل FTD و FMC لخال DNS مداخال نيوكت

لجل لجال متي يذال) win2016.example.com يه ةميقال اذه ، اذه نيوكتال ليلدي (192.168.1.1).

- مداخال ذفنم :

ذفنم STARTTLS و LDAP مدختسي ، يضا رتفا لكش ب . ةمدخ LDAP ل ب لمعتسي ءانيمال TCP 636 ذفنم SSL (LDAPs) ربع LDAP و ، LDAP ل TCP 389

- رذجال قداصم ال عجرمال :

عيقوتل مدختسمال رذجال قداصم ال عجرمال نوكي ، STARTTLS وأ LDAP مادختسإ لاج بي . ابولطم LDAPs ةطساوب ةمدختسمال SSL ةداهش

- رورمال ةملك و ليلدل مدختسمال مسال :

نيمدختسمال ةقداصم و LDAP مداخ ب طبرلل FTD و FMC لبق نم مدختسمال باسحلا وه اذه تاعومجمال او نيمدختسمال نع ثحبل او

ض.رغلا اذهل "FTD لوؤسم" مساب باسح عاشنإ مت

- (DN) ةومجمل او ةءاقلل زيمملا مسالا:

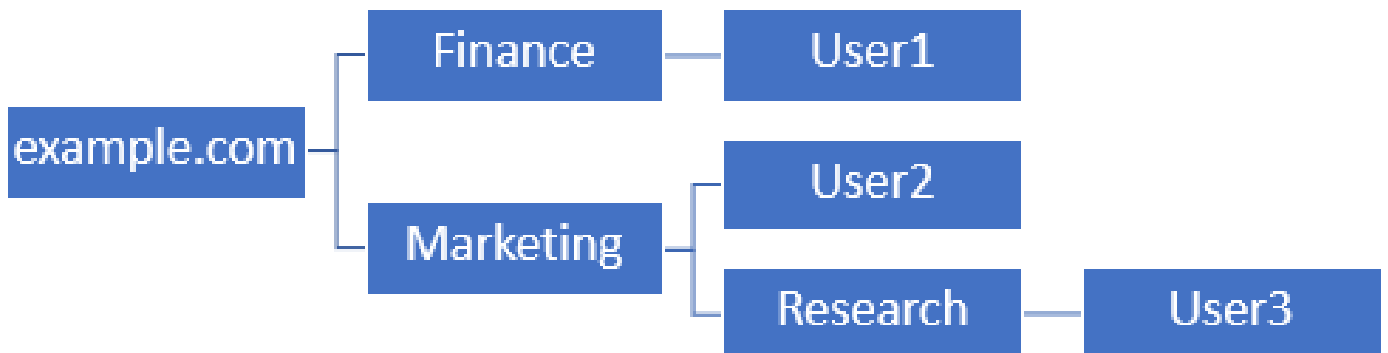
نع شحبل اءبب Active Directory مالعاب FTD موقيو FMC ةءبال ةطقن يه يساسألا DN م.مهتقءاصم ونيمءخسمل

ءءبال ناك مب Active Directory ملعت يتلا FMC ةءبال ةطقن يه ةومجمل DN نإف، لثملا بو مءخسمل ةيوهل ءاعومج نع شحبل يف

DN ءكبش هنا ىلع example.com رءال لءملا مءخسإ متي، اذه نيوكءتلا لئل يف ةومجملاب ةصاخلا DN ءكبشو يساسألا

ءرءتلا لءاء رءكأ يساسألا DN و DN مءخسإ نوئي، ءاءنإلا ةئيبلا ءبسئلاب، كلذ عمو لءفألا وه LDAP ل مءرهل

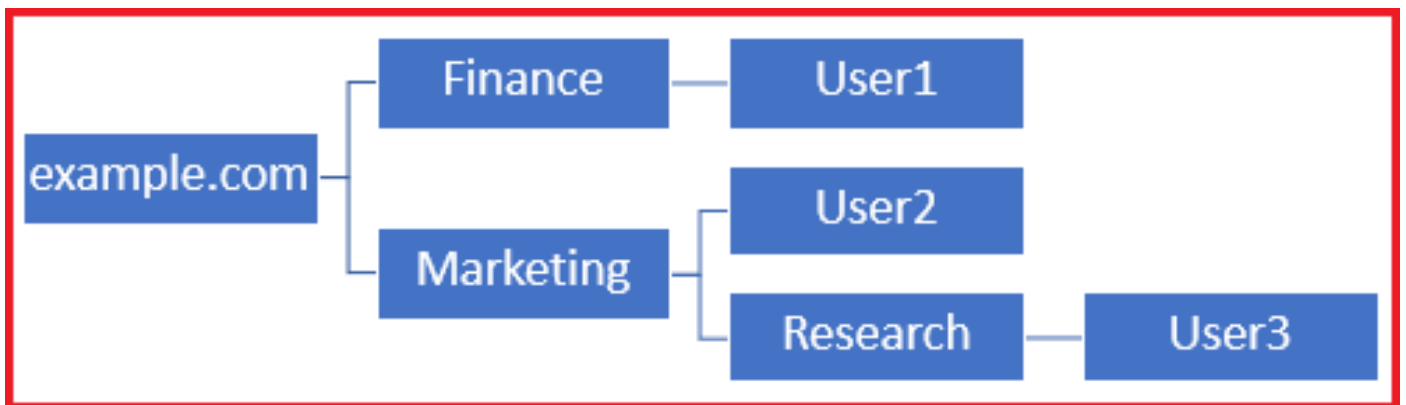
LDAP ل مءرهل ءرءتلا اذه، لءملا لئيبس ىلع



DN ءقءاصم نم قيوستلا ءسسؤم ءءو لءاء نومءخسمل نكمءي نأ ءيري لوؤسملا ناك اءا (example.com) رءال ىلع انه نيءعت نكمي، يساسألا

اضئأ لوءءلا لئءسءب ءيلاءملا ءيميظنءلا ءءوولا نمض User1 ل اضئأ اذه ءمسي، كلذ عمو قيوستلا ءيلاءملا نوؤشلا ىلإ لءقءنئو رءال نم ءءبي مءخسمل نع شحبل نأ شء شءبل او

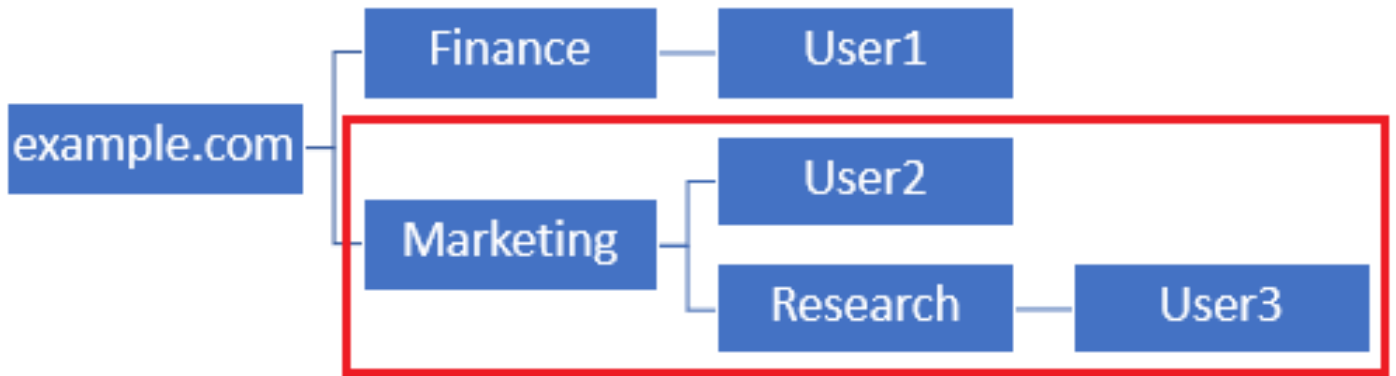
example.com ىلع ءيساسألا DN ءكبش نيءعت مت



ءلبق امو قيوستلا ءسسؤم ءءو يف ءءوولا مءخسمل ىلإ لوءءلا لئءسءب ءيقت لءأ نم قيوستلا ىلع يساسألا DN نيءعت كلذ نم ءءب لوؤسملل نكمي

قويوستلا يف أدبي شحبالا نأل ةقداصملا طقف User2 و User3 ل نأل نكمي.

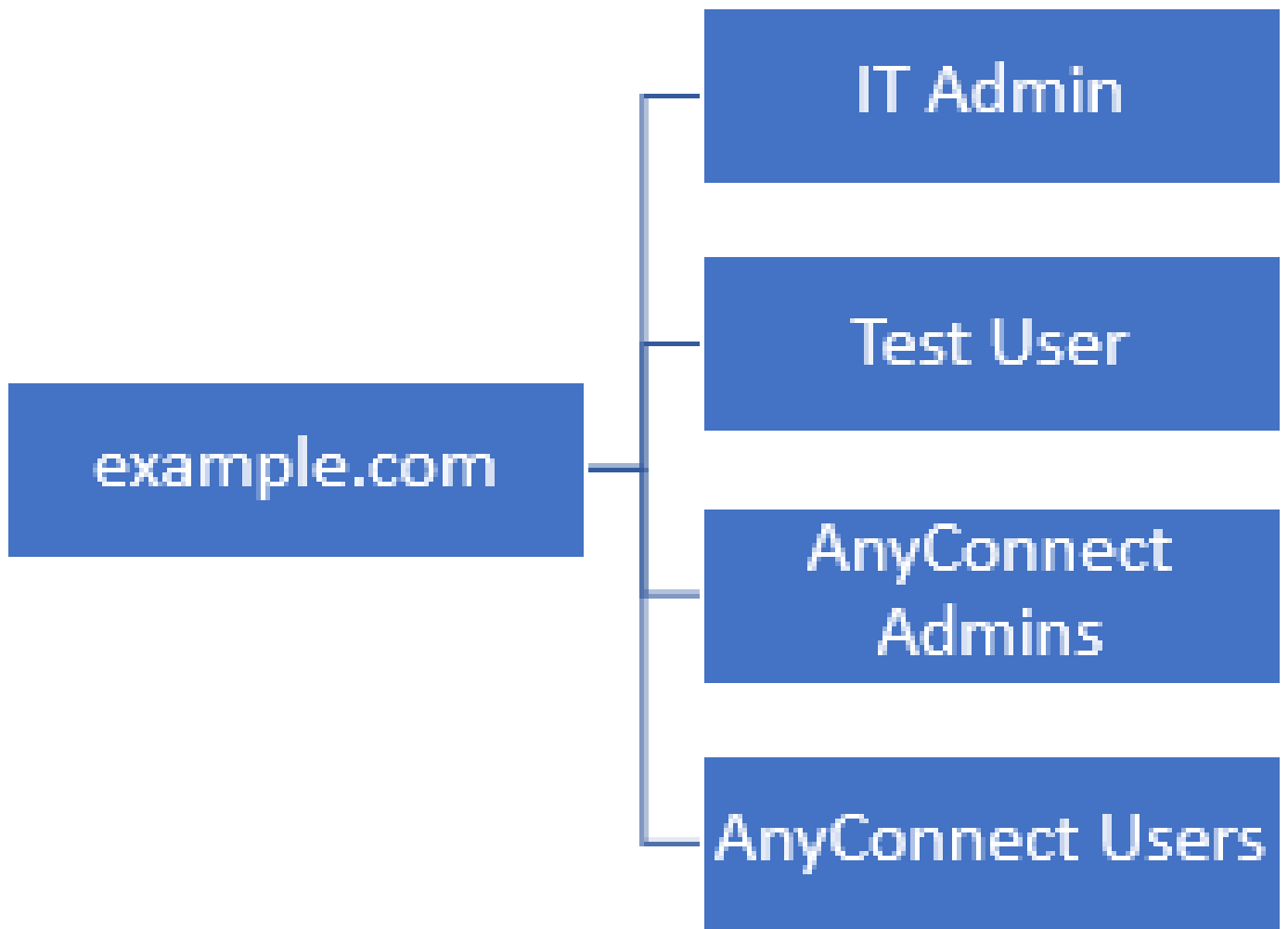
قويوستلا يلع ياساسأل DN نييعت



نيمدختسملل حمسي يذلاو FTD لخاد تايوتسملل ددعت م كحتلا نم ديزمل هنا ظحال، مهبة صاخلا AD تامس يلا اذانتسا نيمدختسملل فلتخم ضيوفت نييعت وأ ليصوتب LDAP. ضيوفت ةطيخ نيوكت مزلي

AnyConnect LDAP [طيطخت نيوكت](#): انه رمألا اذه لوح تامولعملل نم ديزم يلع روثعل نكمي [FirePOWER \(FTD\) ديهت دضع افدلا يلع](#).

DN مادختسا متي و اذه نيوكتلا ليلد ي ف طسبملا LDAP ل يمرهلا جردتلا اذه مادختسا متي ةومجملل DN و ياساسأل DN نم لك ل example.com روجلل



ةوعومجملل DN و يساسأل LDAP DN ديحت

رتوي بمكلا ةزهجأو Active Directory يمدختسمحت ف 1.



Best match



Active Directory Users and Computers

Desktop app



Settings



Edit local users and groups



Change User Account Control settings



User Accounts



Select users who can use remote desktop



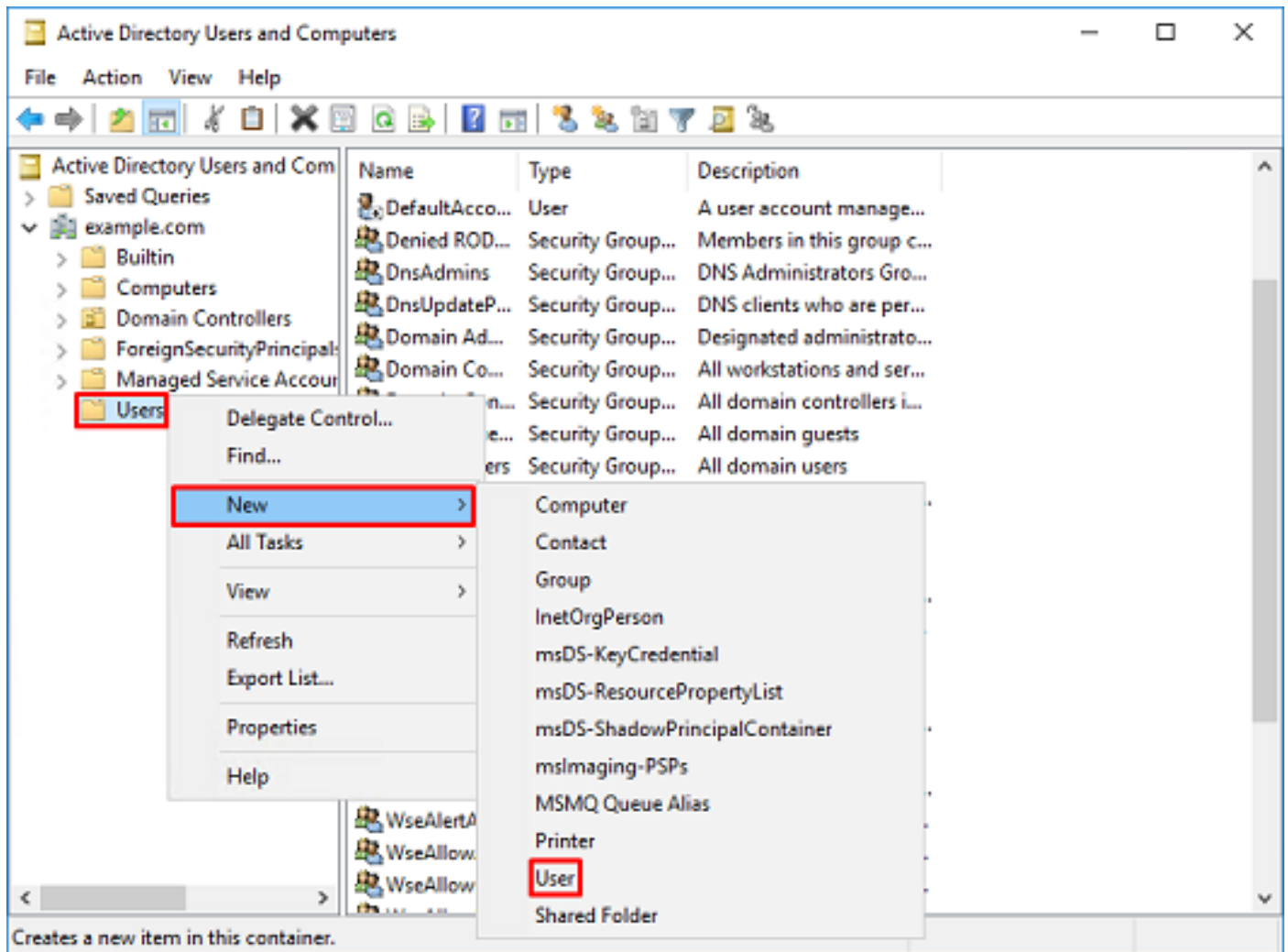
تانايب قارتخأ مت اذا ةكبشلا لخاد رخأ ناكم إلى هب حرصملا ريغ لوصولا عنم وه لصف نم
طب رلل ةمدختسملا دامتعالا

ةومجملاب صاخلا DN وأ يساسألا DN قاطن نمض باسحلا اذه نوكتي نأ مزلي ال

1. ةمظنملا/ةيواحلا قوف نميألا سواملا رزب رقنا، Active Directory User and Computers في ف
اهي لإ FTD باسح ةفاضلا تمت يتلا

مدختسملا مسال فسأ نومدختسملا ةيواح نمض FTD باسح ةفاضلا تمت، نيوكتلا اذه في
ftd.admin@example.com.

مدختسم > ديدج إلى لقتنا م، نيومدختسملا قوف نميألا سواملا رزب رقنا



2. مدختسم - ديدج نئاك جلاعم إلى لقتنا.

New Object - User



Create in: example.com/Users

First name:

FTD

Initials:

Last name:

Admin

Full name:

FTD Admin

User logon name:

ftd.admin

@example.com



User logon name (pre-Windows 2000):

EXAMPLE\

ftd.admin

< Back

Next >

Cancel

New Object - User



Create in: example.com/Users

Password:

●●●●●●●●

Confirm password:

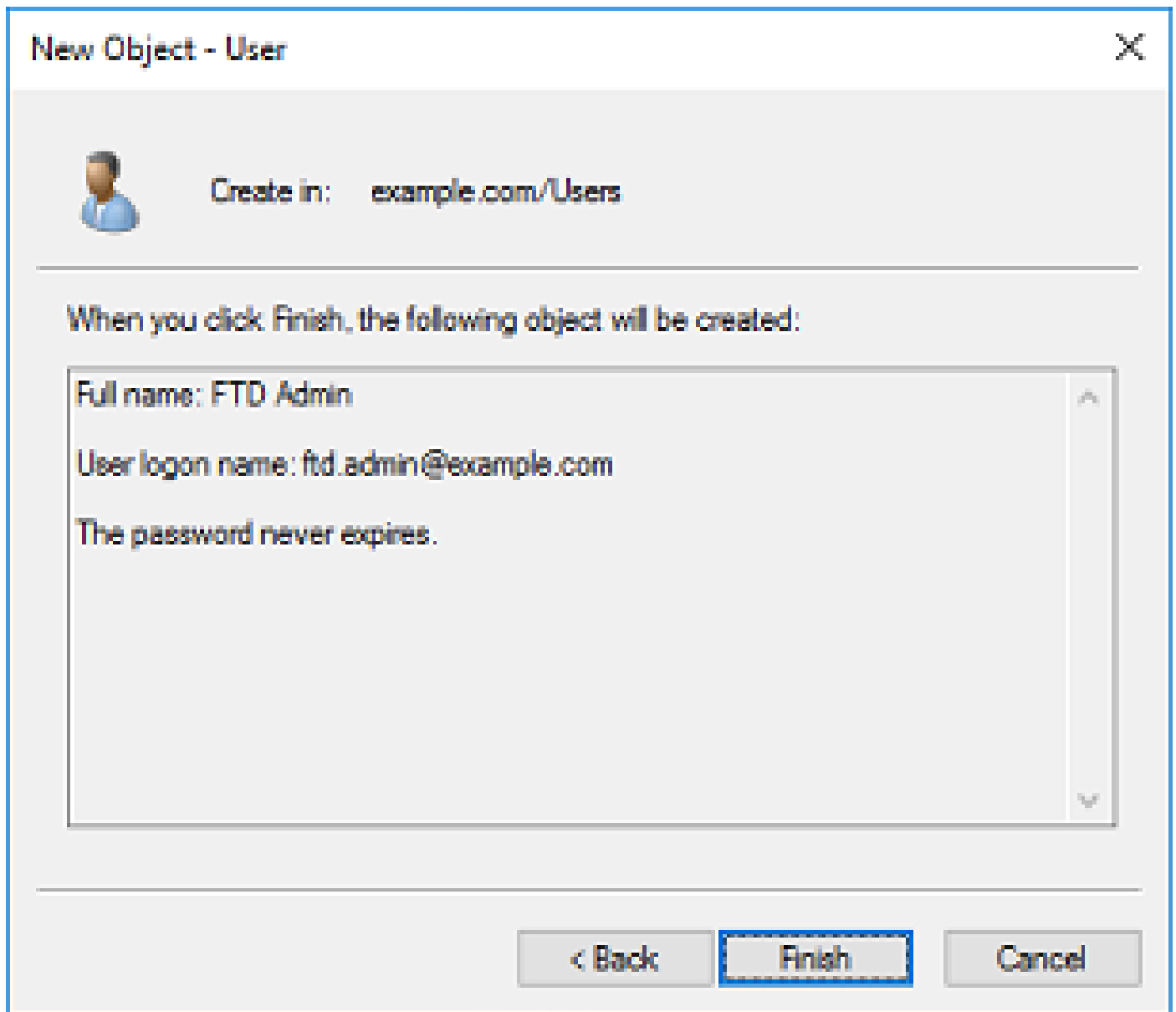
●●●●●●●●

- User must change password at next logon
- User cannot change password
- Password never expires
- Account is disabled

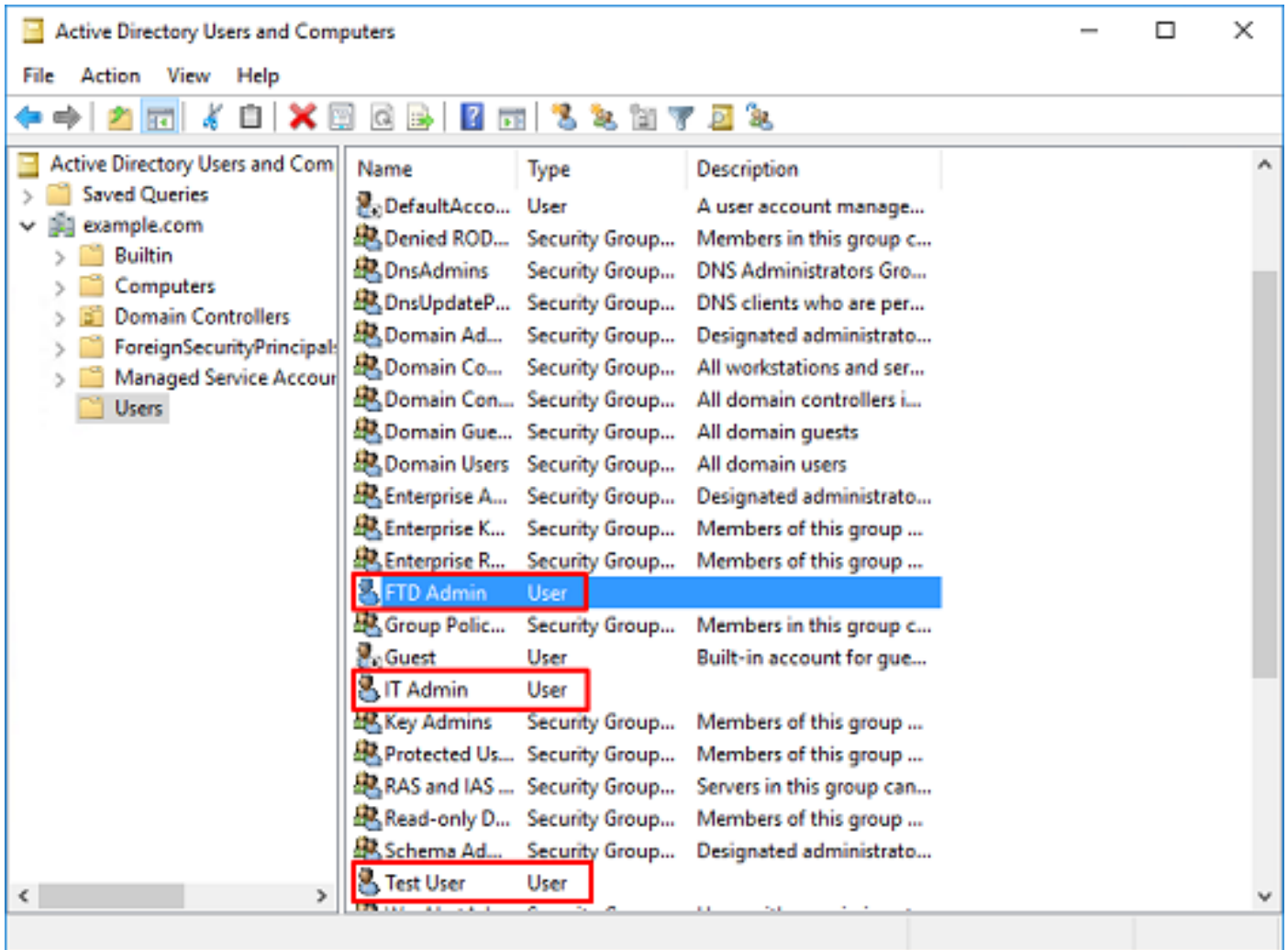
< Back

Next >

Cancel



3. قېنقت لوؤسم امه و ، نېي فاضا نې باسح عاشن ا مت FTD باسح عاشن ا نم ققحت . رابتخال ا مدختسم و تامول عمل ا



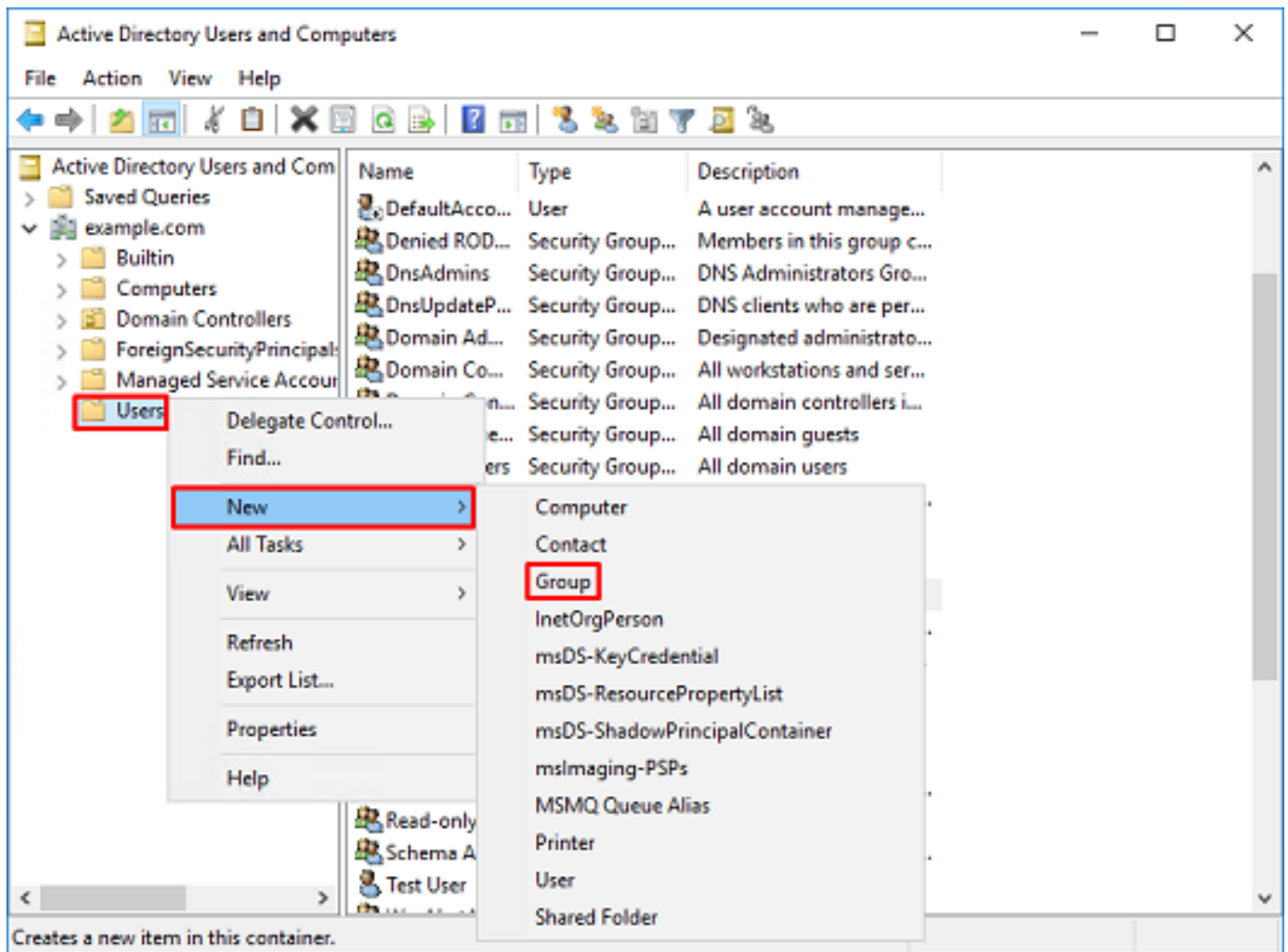
(يراي تخ) تانال ع تاعومجم لى لى نى م د خ ت س م ة فاض او تانال ع تاعومجم عاش ن

ق ي ب ط ت ل ي ه س ت ل تاعومجم لى م ا د خ ت س ل ن ك م ي ، ة ق د ا ص م ل لى لى ة ج ا ح ل م د ع ن م م غ ر ل لى لى و و LDAP. ض ي و ف ت لى لى ة فاض ل ا ب نى م د خ ت س م ة د ع لى لى ل و ص و ل ا ت ا س ا ي س

ل و ص و ل ا ب م ك ح ت ل ل ج ه ن ت ا د ا د ع لى ق ي ب ط ت ل تاعومجم لى م ا د خ ت س ل م ت ي ، ا ذ ه ن ي و ك ت ل ل لى لى د ي ف FMC. ل خ ا د م د خ ت س م ل ل ة ي و ه ل ل ا ل خ ن م ا ق ح ا ل


1. ة د ح و ل و ا ة ي و ا ح ل ق و ف ن م ي ا ل س و ا م ل ر ز ب ر ق ن ا ، Active Directory User and Computers. م ت ي ت م ل ل ة ي م ي ظ ن ت ل ل ا ه ل ل ة د ي د ج ل ل ة و م ج م ل ل ة فاض ل ت م ت ي ت ل ل ة ي م ي ظ ن ت ل ل

ن و م د خ ت س م ة ي و ا ح ل ن م ض ة و م ج م ل ل ي ف AnyConnect لى ل و و س م ة فاض ل م ت ت ، ل ا ث م ل ا ذ ه ي ف ة و م ج م > د ي د ج لى لى ل ق ت ن ا م ت ، نى م د خ ت س م ل ق و ف ن م ي ا ل س و ا م ل ر ز ب ر ق ن ا



2. عموم جم - ديدج نئاك جلاعم يلا لقتنا.

New Object - Group X

 Create in: example.com/Users

Group name:

Group name (pre-Windows 2000):

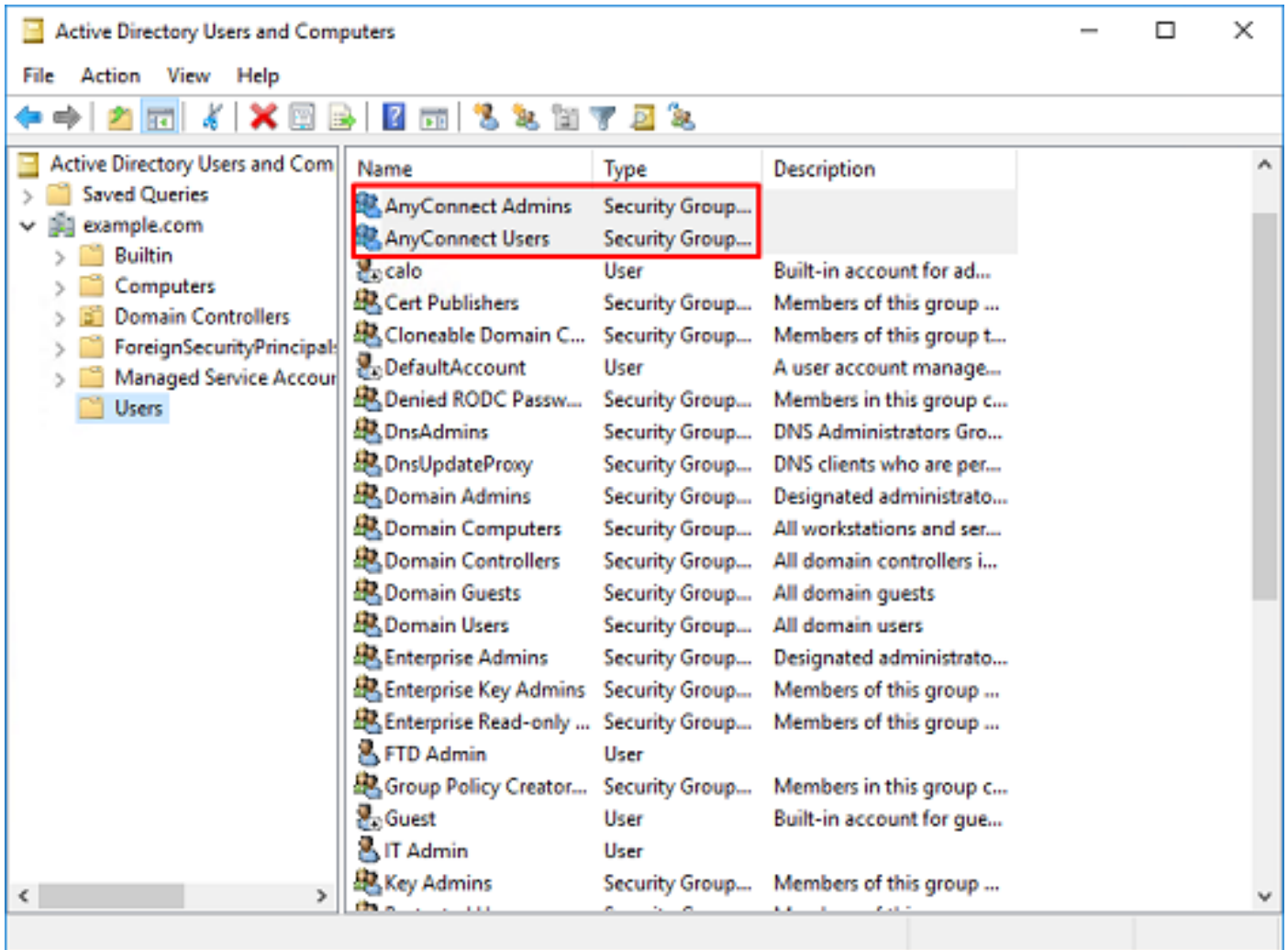
Group scope

Domain local
 Global
 Universal

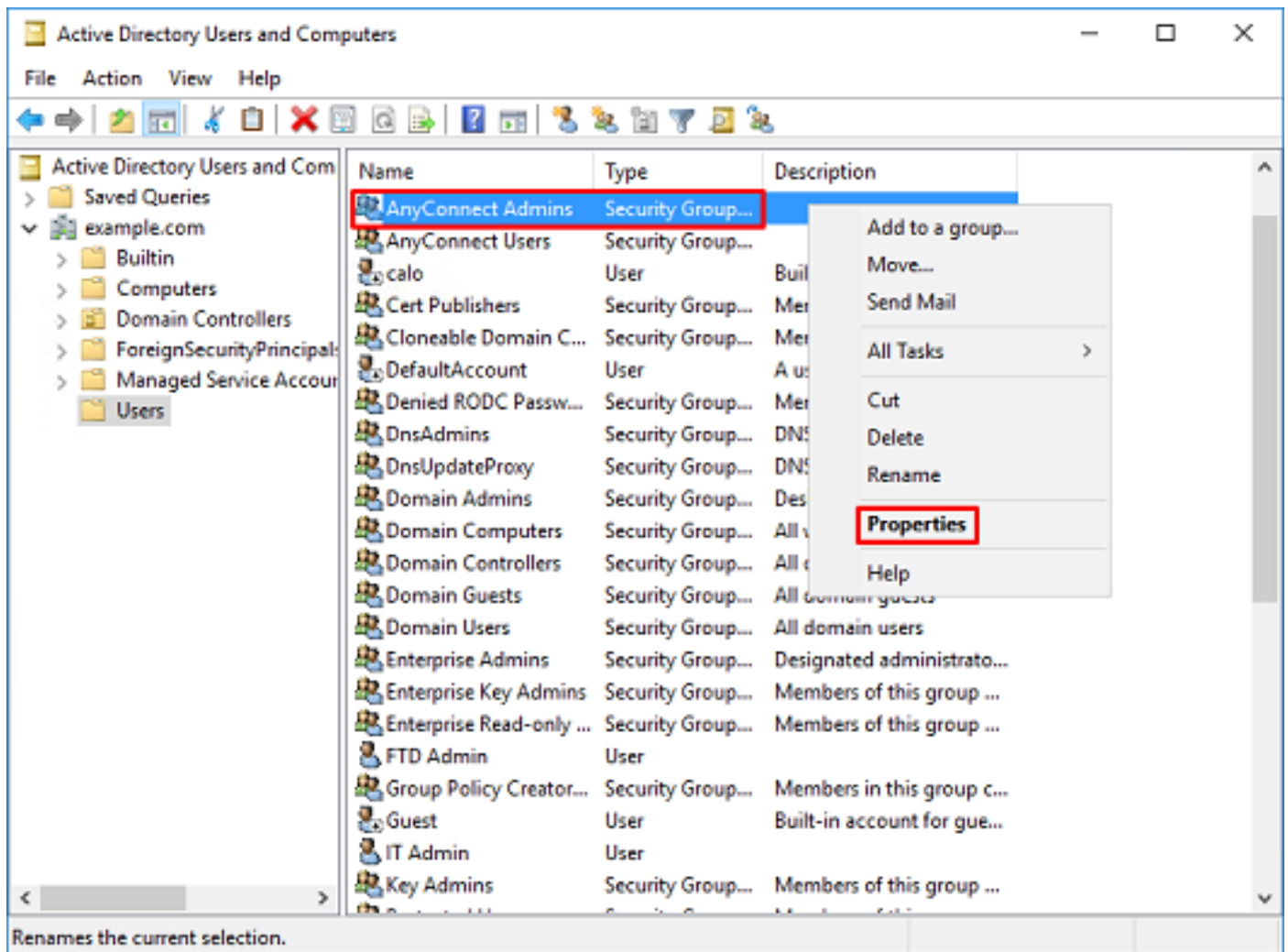
Group type

Security
 Distribution

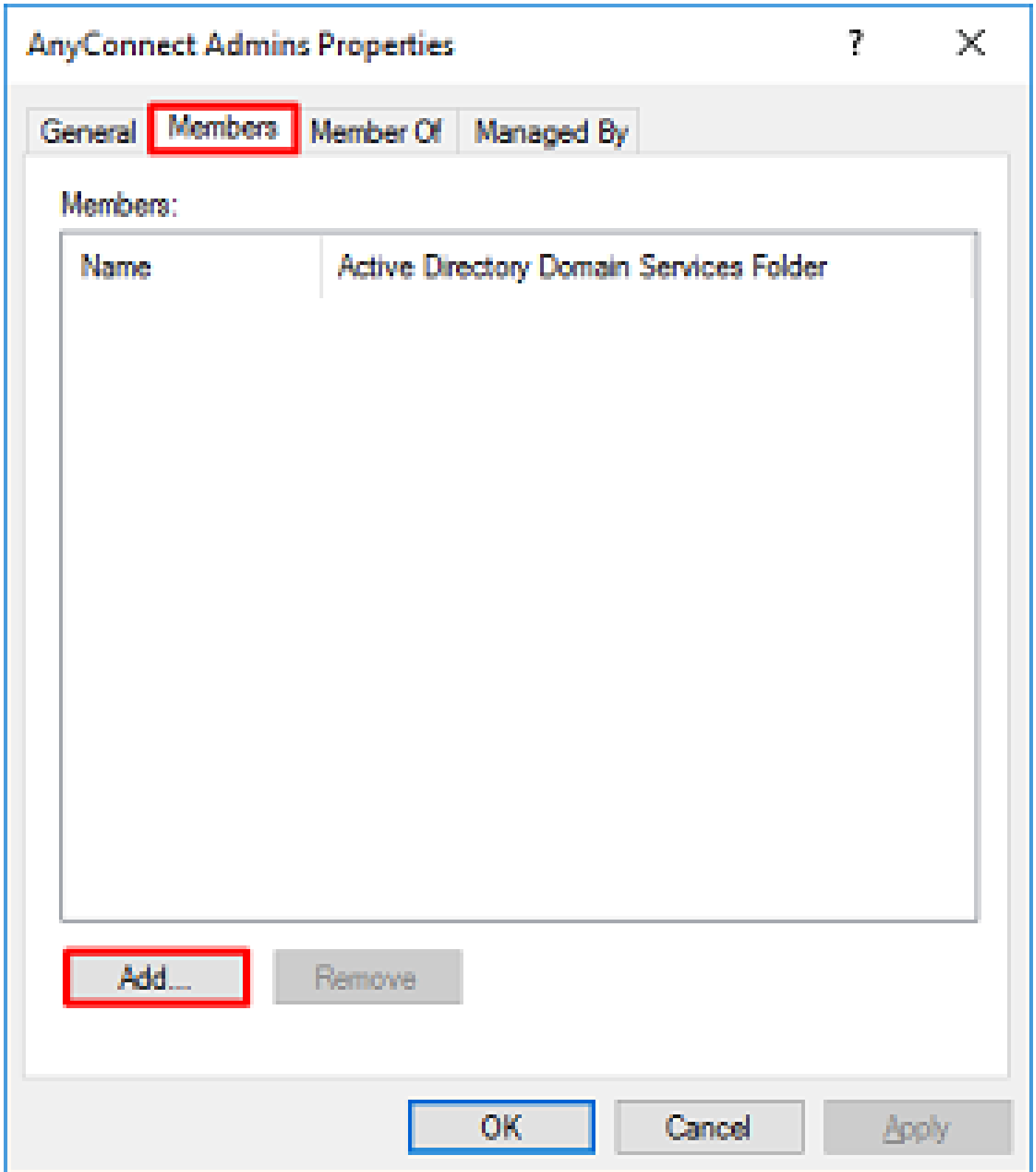
3. AnyConnect يمدختم سم ةعومجم ءاشنإ اضيأ متي . ةعومجملا ءاشنإ نم ققحت .



4. نبيوكتلا اذه يف .صئاصخ رتخأ مئ (نئمدختسملا) ةعومجملا قوف نميال سواملا رزب رقنا .متتو AnyConnect لئوؤسم ةعومجم لئ مدختسم لئ تامولعملل ةينقت لوؤسم ةفاضل مت AnyConnect .مئمدختسم ةعومجم لئ مدختسملا رابتخا مدختسم ةفاضل



5. أفاضاً قوف رقنا ،أاضعأ بيوبتللا ةمالع تحت .



ىل ع روٲعلا نم ققحتلل ءامسألأ نم ققحتلا قوف رقناو لقحلا ف مدختسملا لخدأ
ok. تقطقط ،ققحتلا مت نإ ام .مدختسملا

Select Users, Contacts, Computers, Service Accounts, or Groups

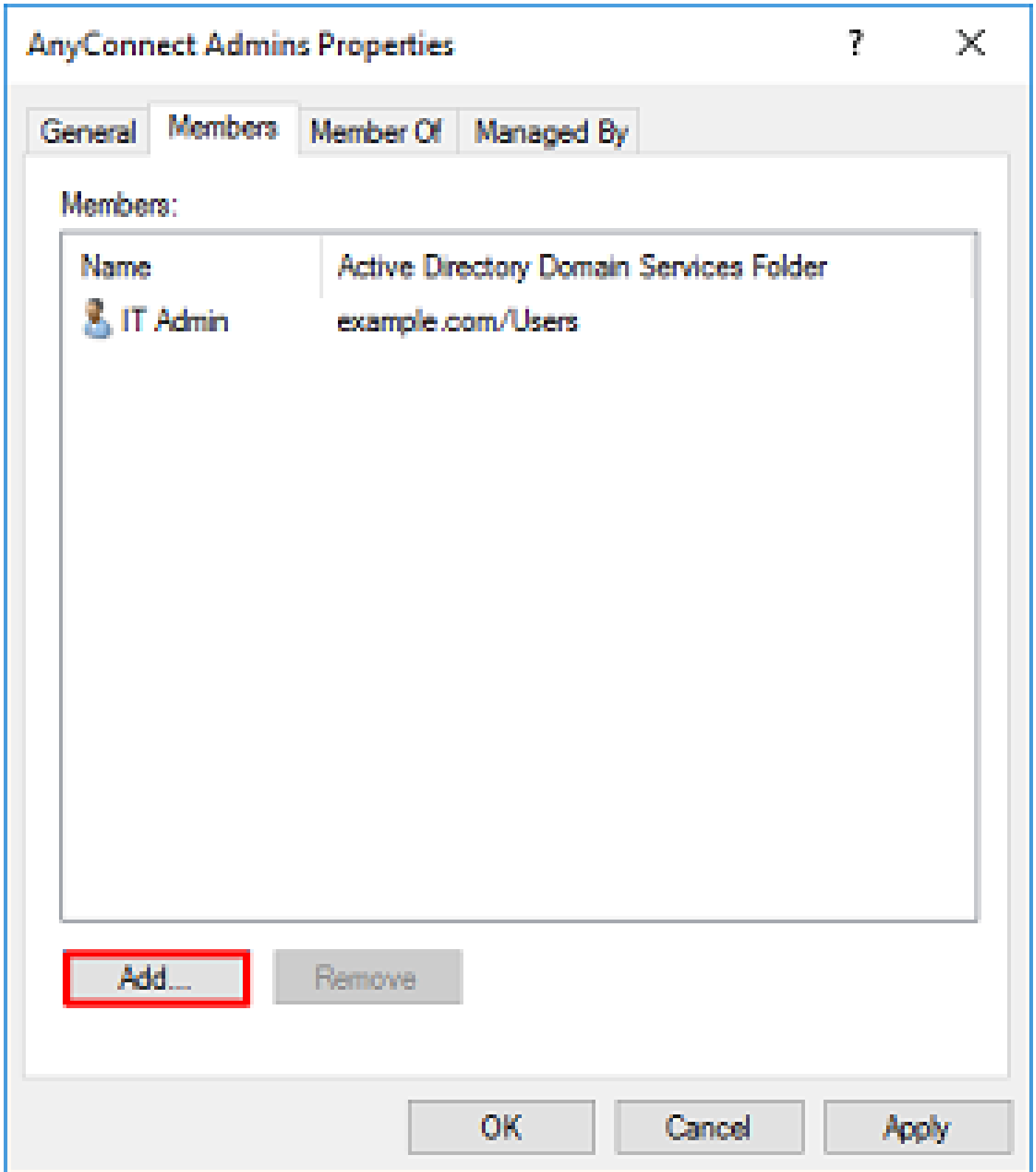
Select this object type:
Users, Service Accounts, Groups, or Other objects Object Types...

From this location:
example.com Locations...

Enter the object names to select (examples):
IT Admin (it.admin@example.com) Check Names...

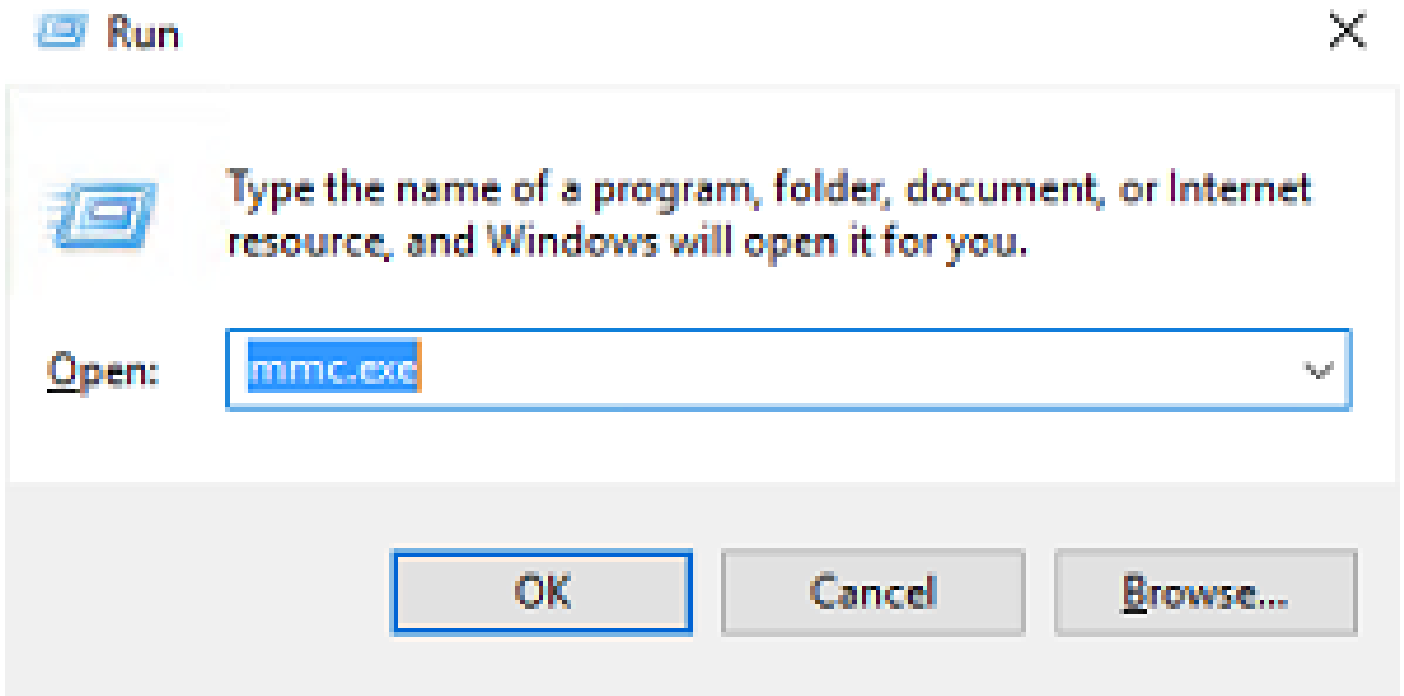
Advanced... OK Cancel

رابطه | مَدْخَلِ سَمِ ةِ فَا ضِ | مَت تِ امِ كِ . قِ فَا وِ مِ قِ وِ فِ رِقْ نَا مِ ثِ حِ حِ صِ لِ مَدْخَلِ سَمِ ةِ فَا ضِ | نِ مِ قِ قِ حِ تِ
اِ هِ سِ فِ نِ تَا وِ طِ خِ لِ مَادِ خِ تِ سِ اِ بِ AnyConnect يِ مَدْخَلِ سَمِ ةِ فَا وِ مِ جِ مِ يِ لِ مَدْخَلِ سَمِ ةِ فَا ضِ |

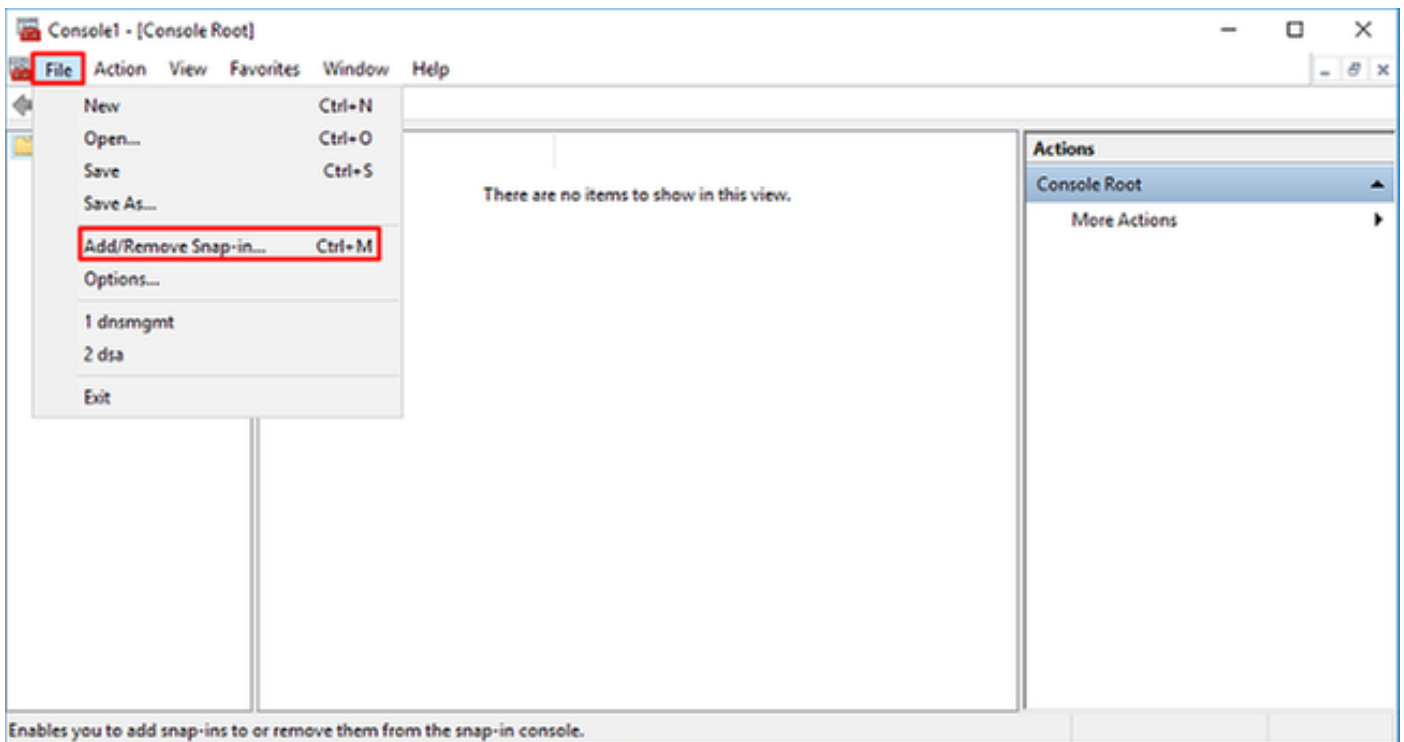


(STARTTLS أو LDAPs ل نطاق بولطم) LDAP ب صاا ل SSL ةداهش رذج خسن

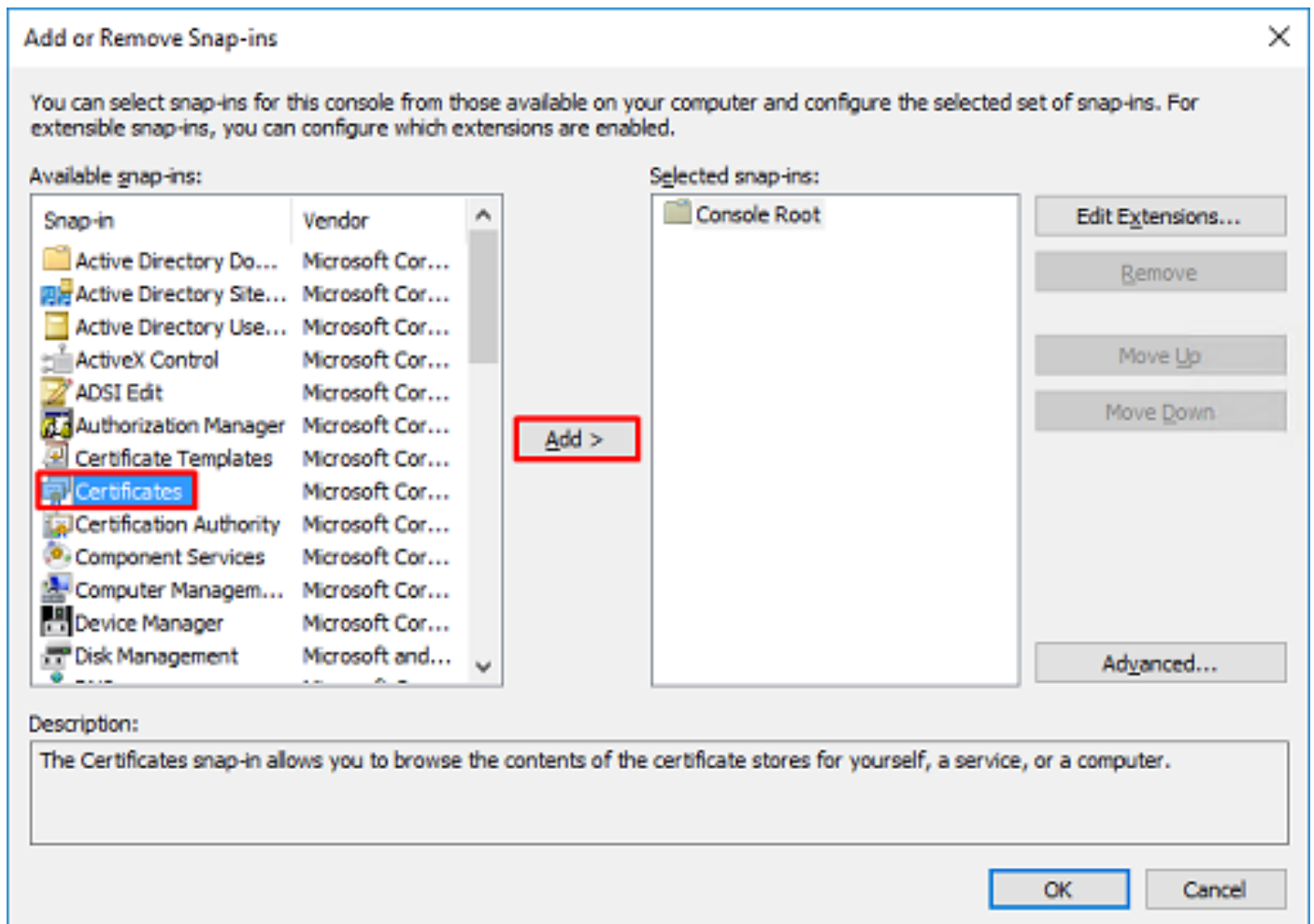
1. OK قوف رقنا مث .mmc.exe لخدأو Win+R لىع طغضا .



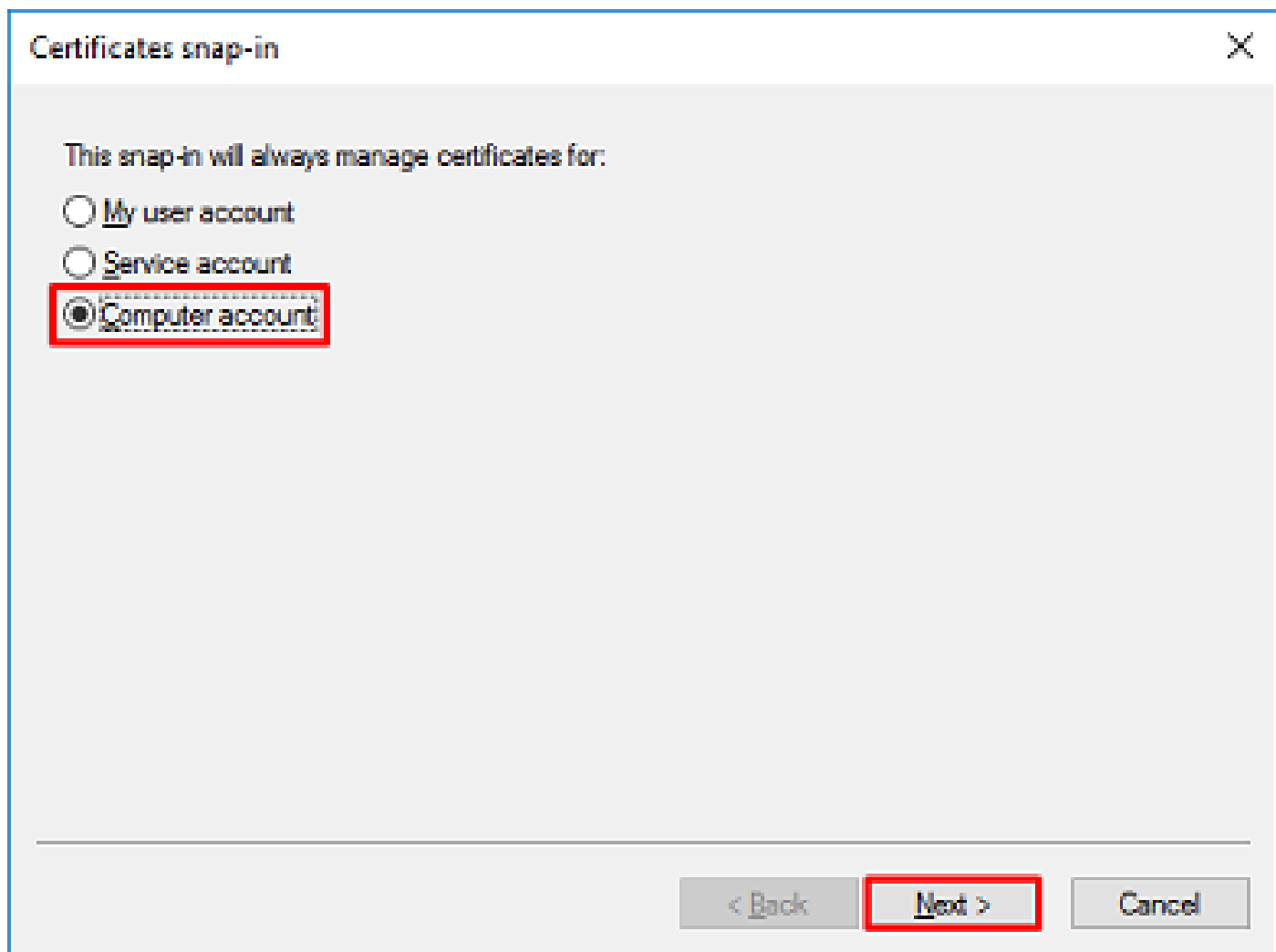
2. في فضاء الإدارة أذلة/إزالة فضاء > فلم إلى لقتنا.



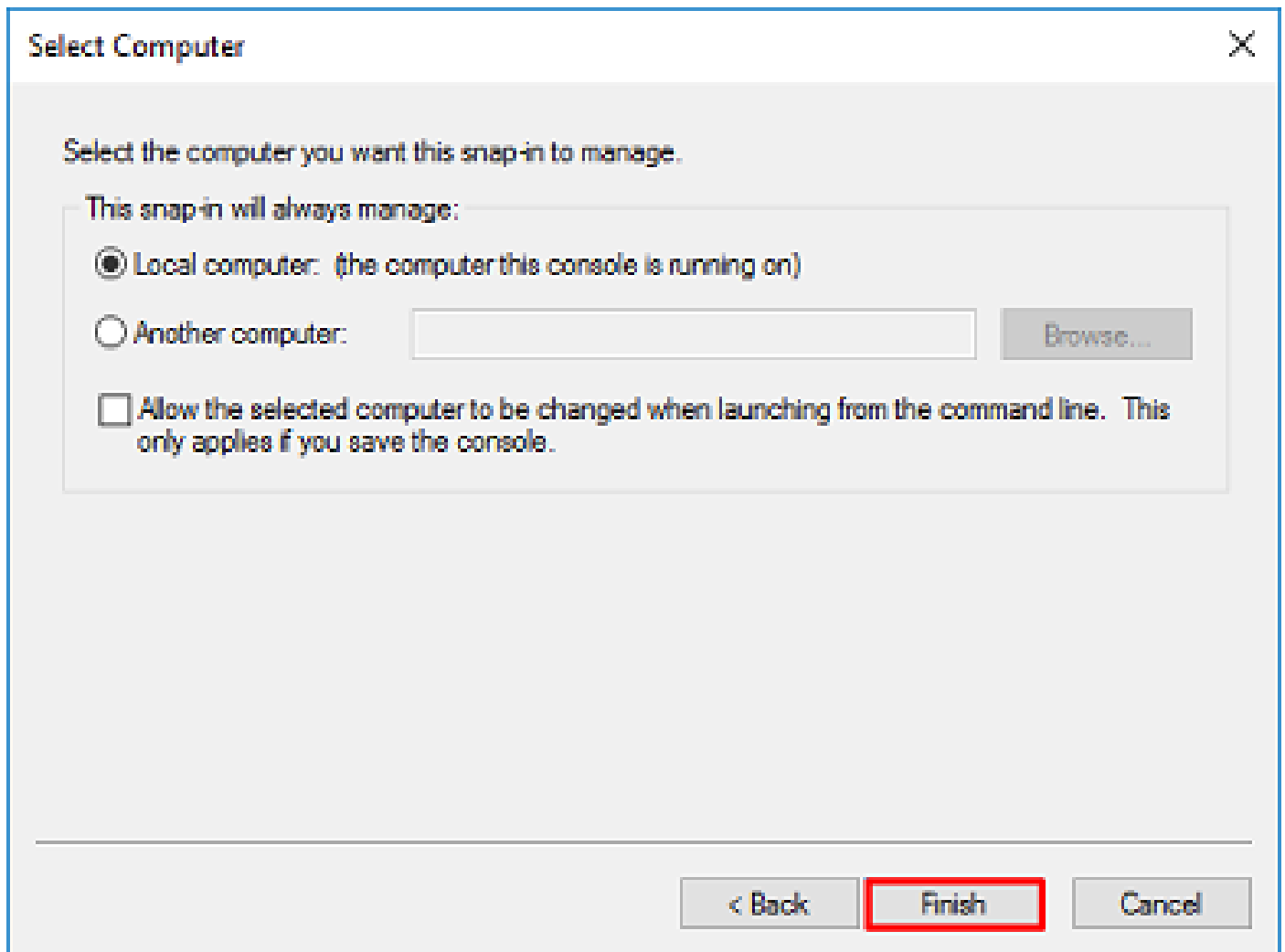
3. فضاء إلى لقتنا مث تاداهشلا دح، عحاتملا في فضاء الإدارة تاوأل تحت.



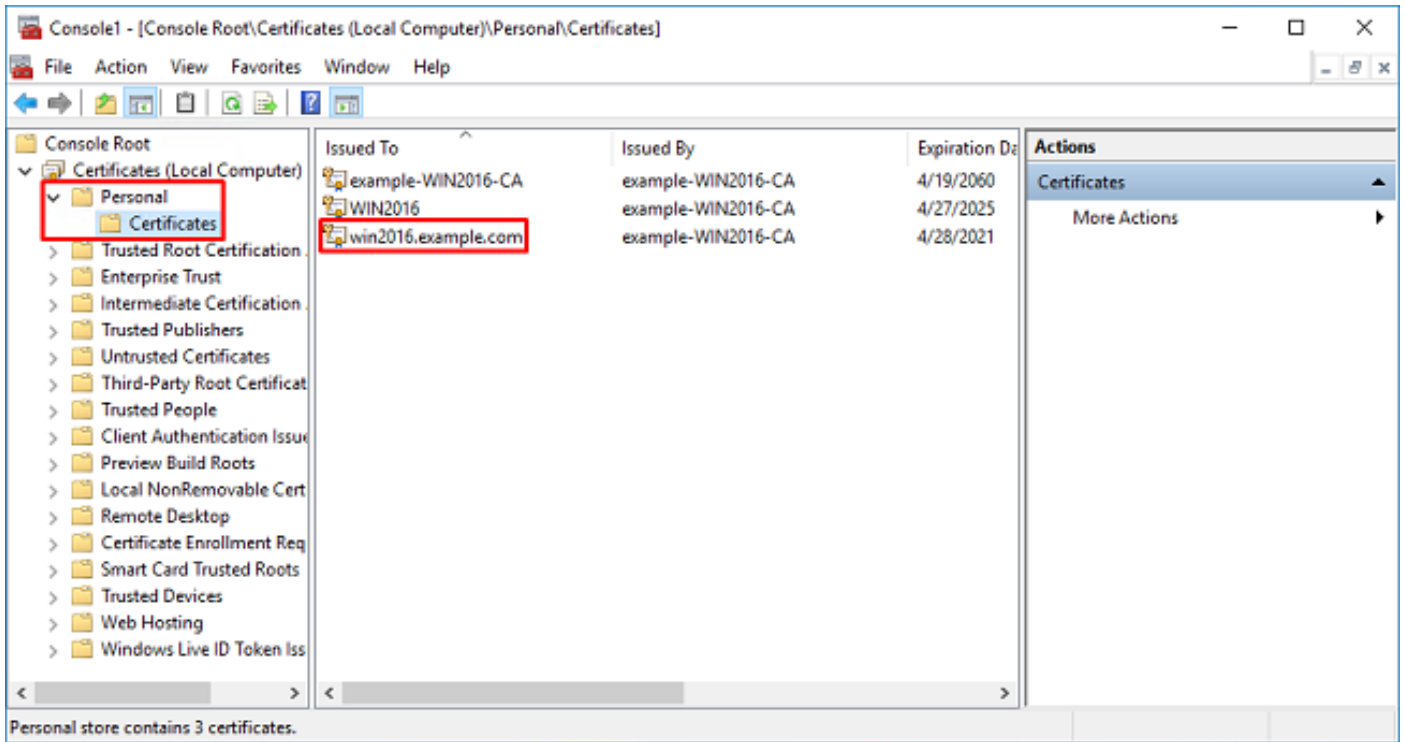
4. يلاتال قوف رقنا م ث رتوي بمكلا باسح دح.



ءاهن| قوف رقنا



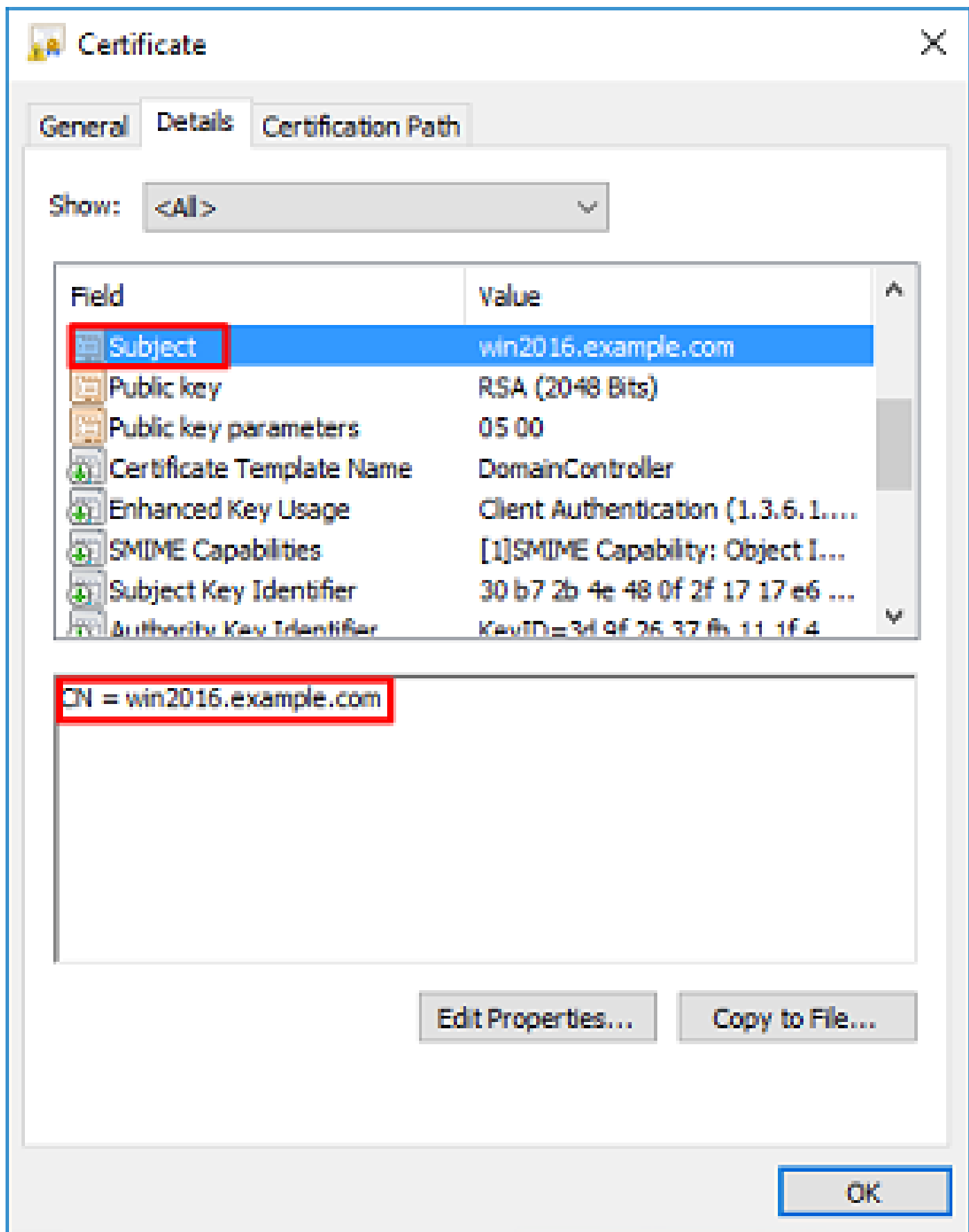
5. قوف رونا OK.



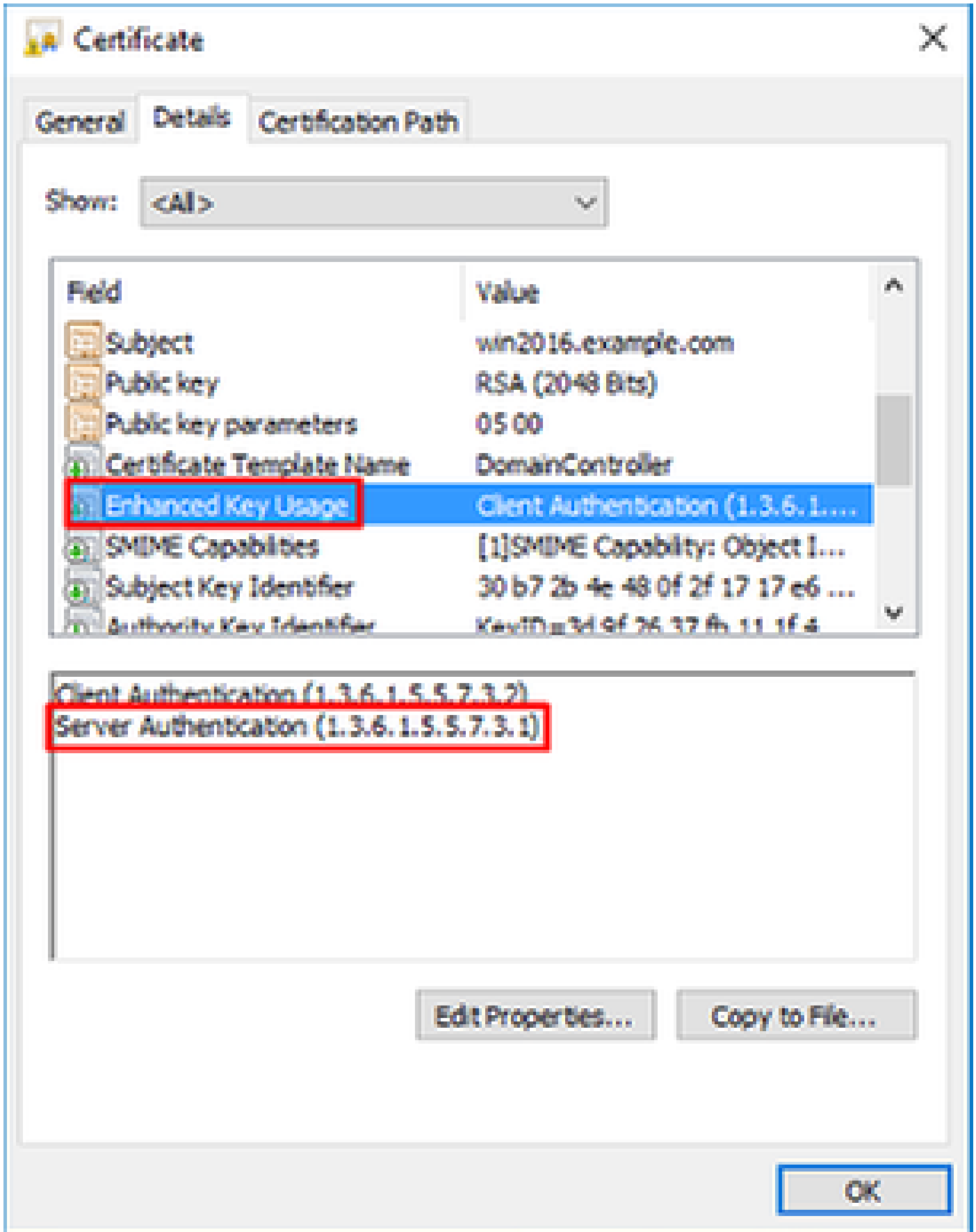
7. تابلطتم لاهذه ةداهش لاي فووتست نأ بجي ، LDAPS ل SSL ةداهشك اهم ادختسا متي يكل :

- مداخل صاخال FQDN عم DNS عوضومل ليدبل مسالا وأ عئاشلال مسالا قباطتي Windows.
- نسمح لاحتفم لادختسا لقح نمض مداخل اقداصم لىع ةداهش لايوتحت .

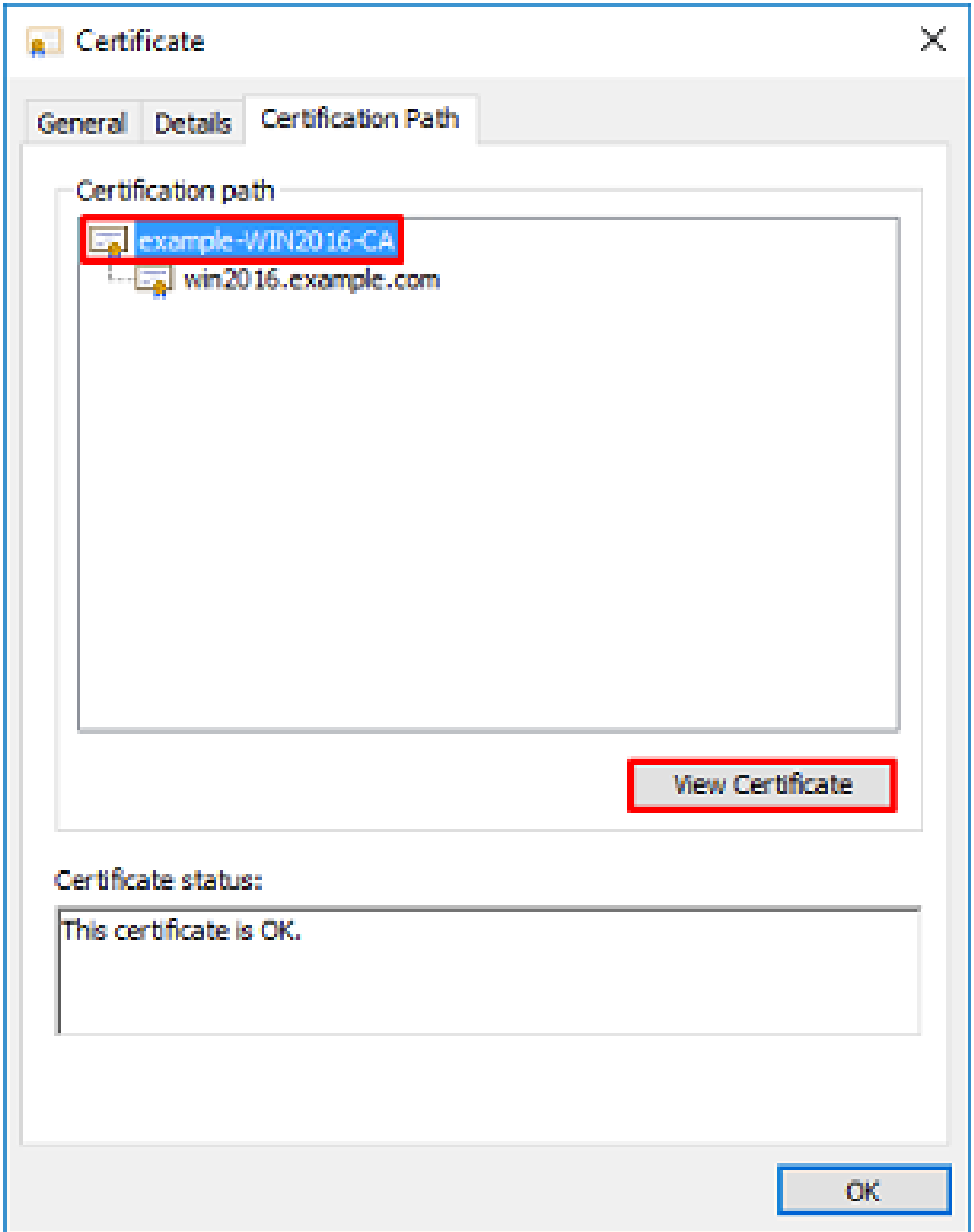
فQDN دجوي ، ليدبل عوضومل مساو عوضومل دح ، ةداهش لاي صافات بيوبتلال ةمالع تحت win2016.example.com.



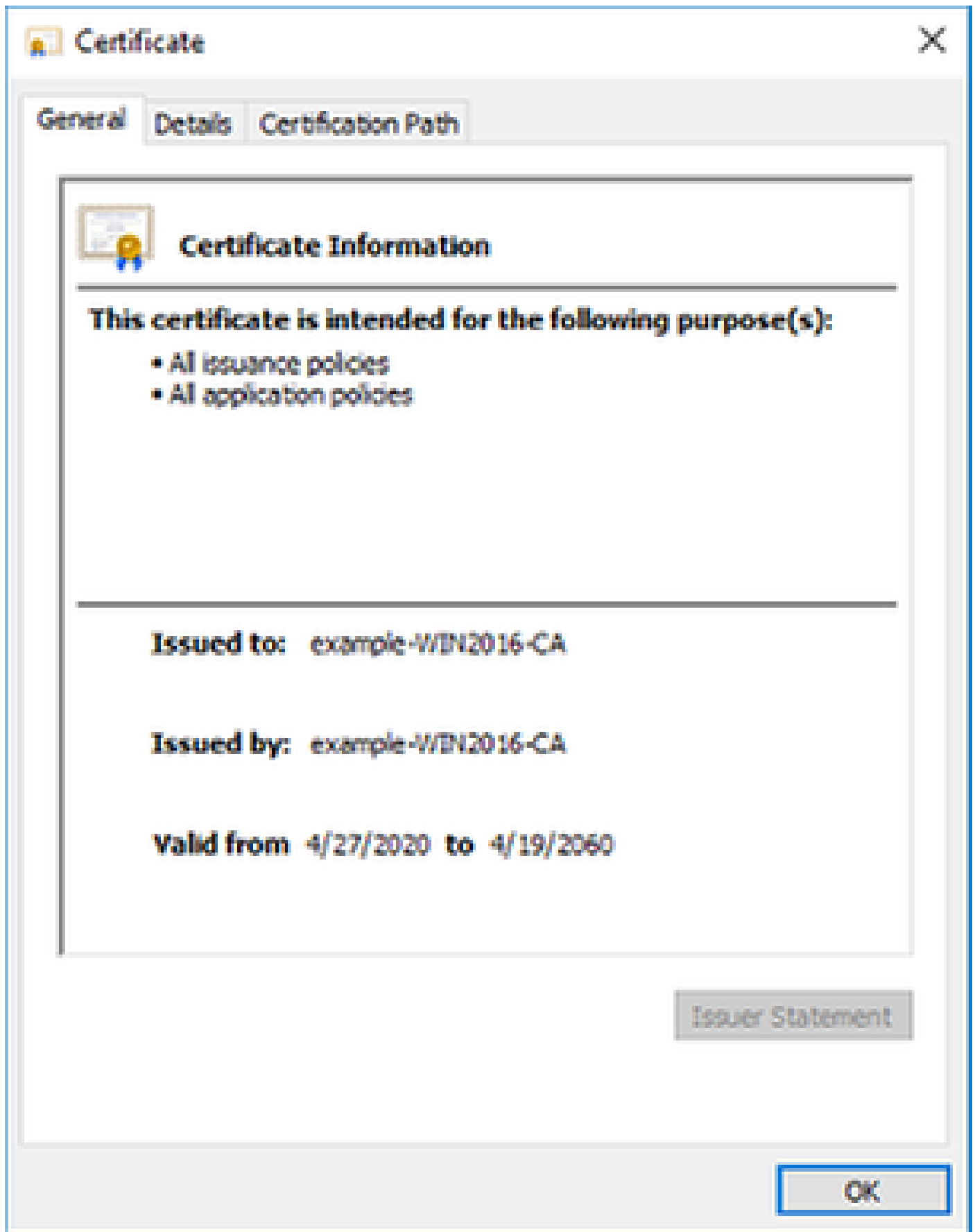
مداخله قداصم دجوت، حيت افم لل نس حمل ما دخت ساله تحت



8. يه يتل ايلعل اءاهشلل دء، اءاهشلل راسم بيوبتلل اءالء ءء، كلذ نم ءكأءل ءرءم ب. اءاهشلل ضرء قوف رءنا مء، رءءل قءصمءل اءرءمءل اءاهش.



9. رذجل ا قدصملا عجرملا ةداهشل تاداهشلا لي صافات حتف ىلا كلذ ي دؤي .



فلم ىلا خسن قوف رقنا ،لصافات بىوبتلا ةمالع تحت



←  Certificate Export Wizard

Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.


A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Next

Cancel

خ.509 زم رمل ال Base-64 ددح

←  Certificate Export Wizard ✕

Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

DER encoded binary X.509 (.CER)

Base-64 encoded X.509 (.CER)

Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

Include all certificates in the certification path if possible

Personal Information Exchange - PKCS #12 (.PFX)

Include all certificates in the certification path if possible

Delete the private key if the export is successful

Export all extended properties

Enable certificate privacy

Microsoft Serialized Certificate Store (.SST)

هري دصت متي ني او فللملا مسا ددح.

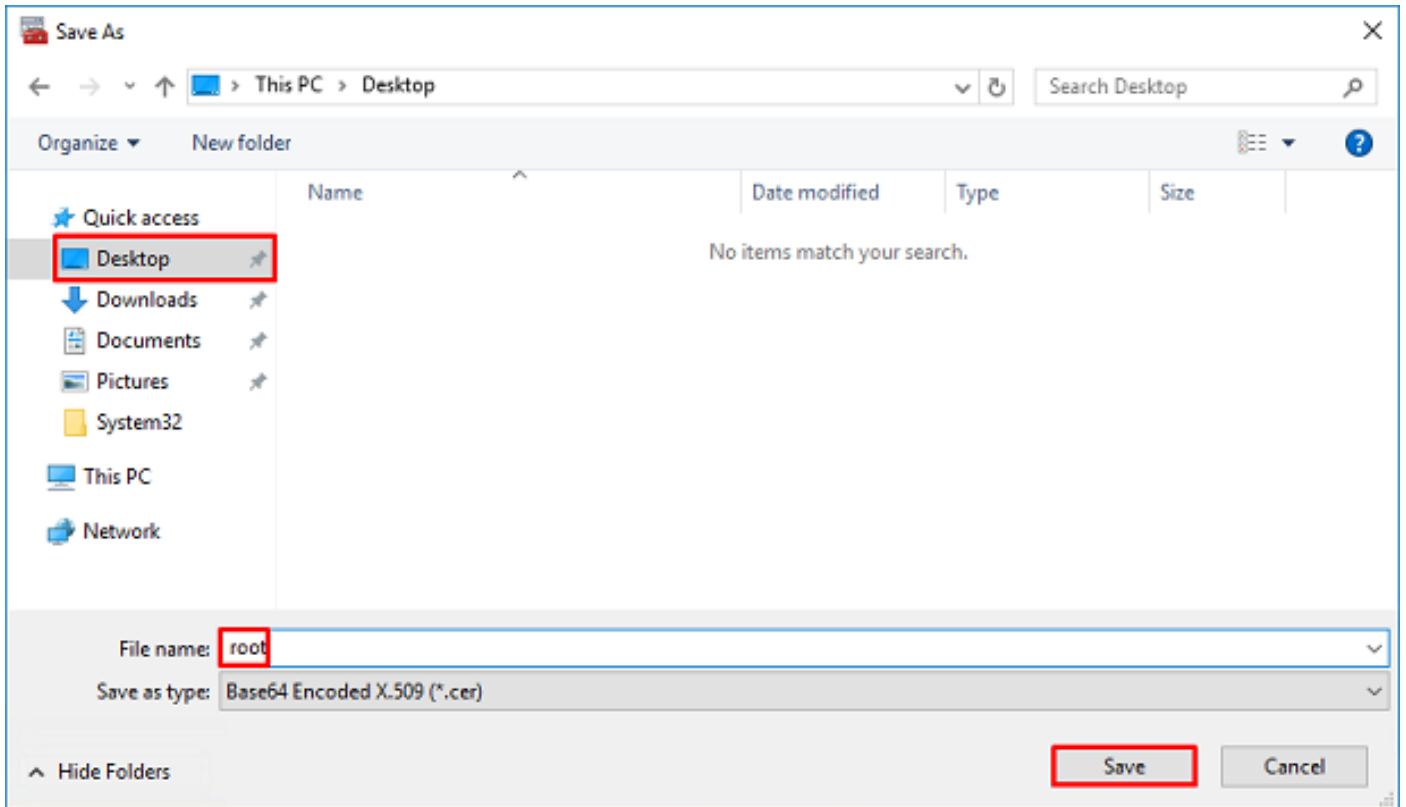


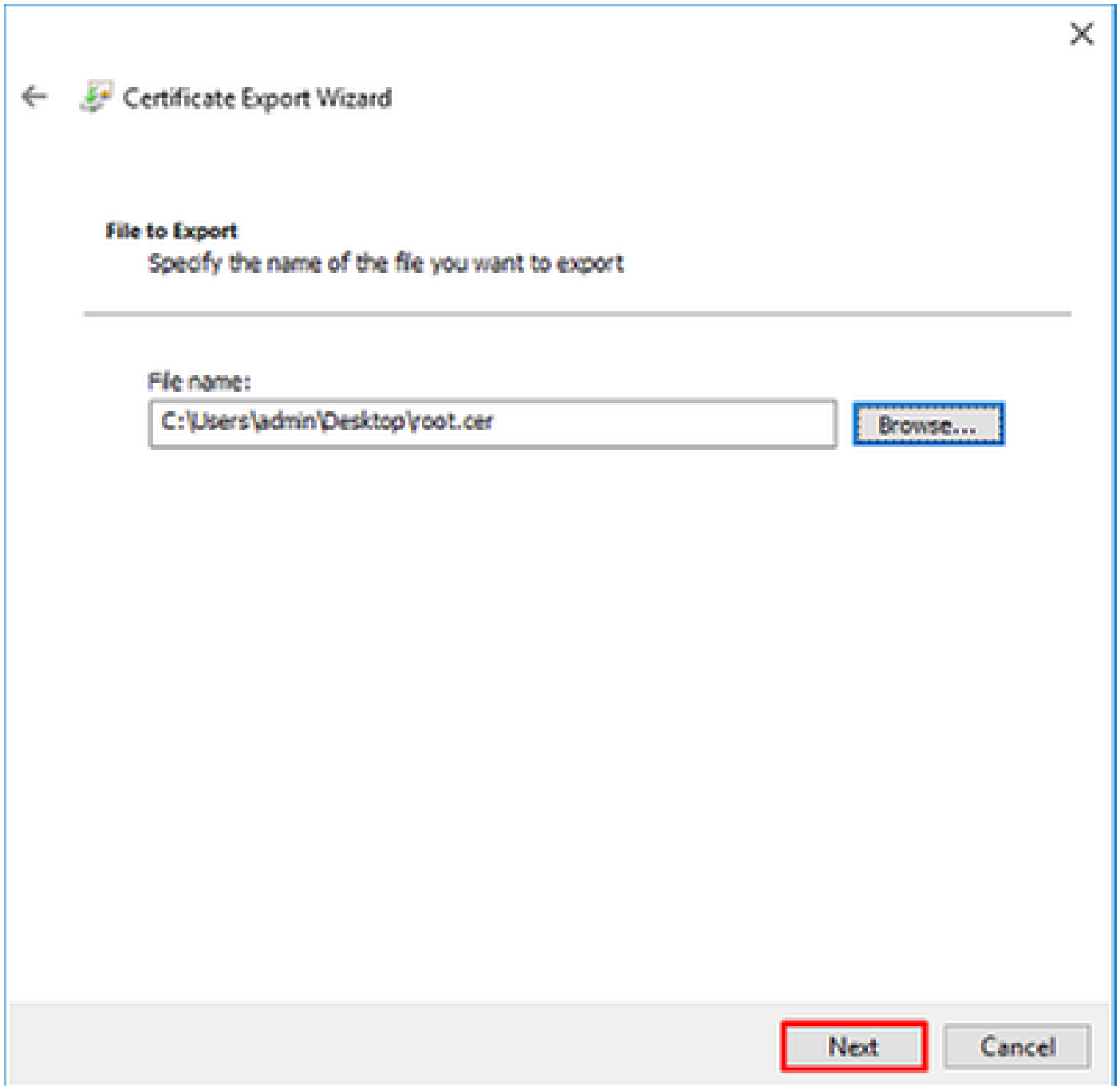
←  Certificate Export Wizard

File to Export

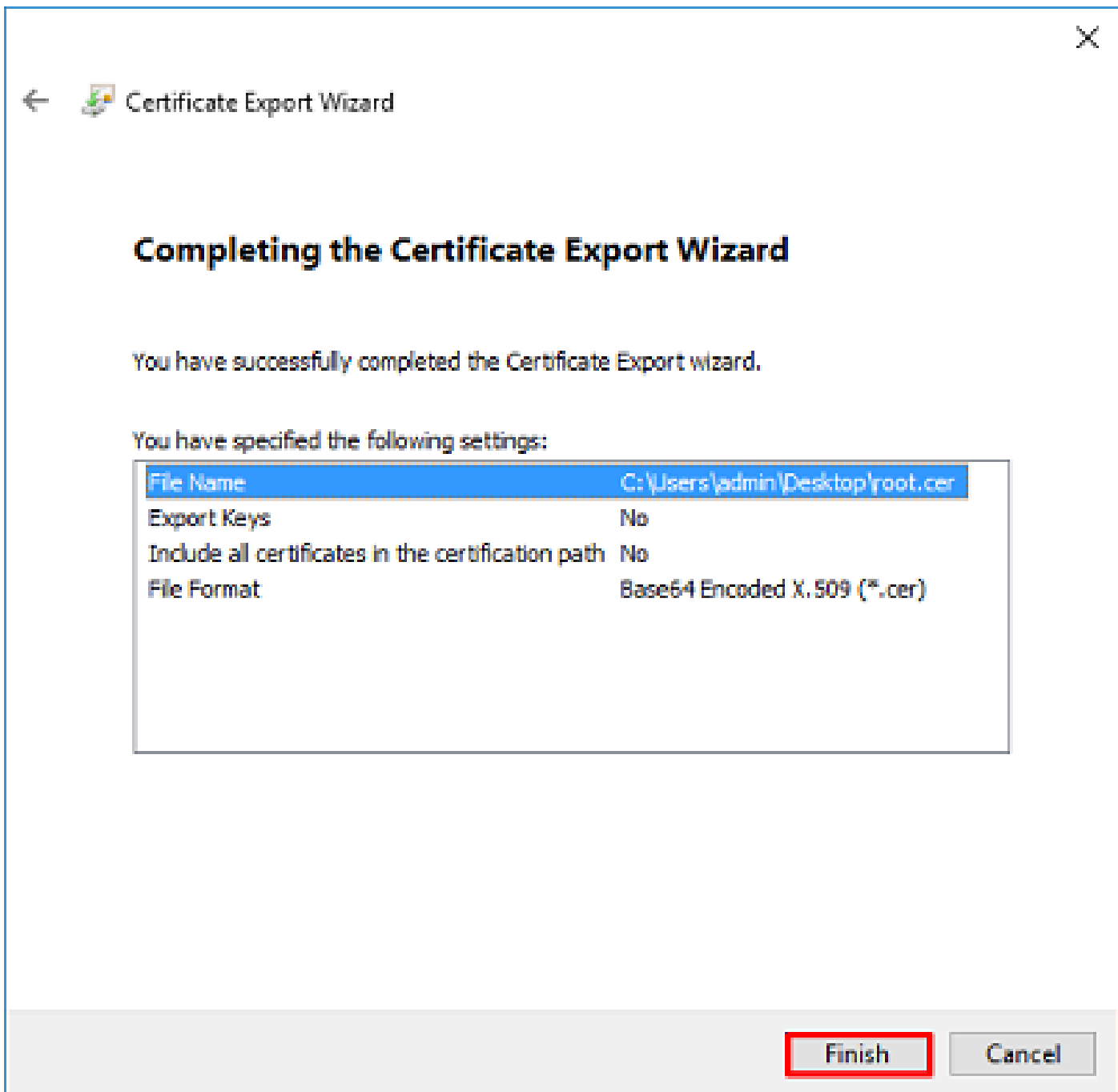
Specify the name of the file you want to export

File name:





ءاهنإ قوف رقنا نألأ



11. اذه ضرعي . رخآ صوصن ررحم ي وأ ةركفم مادختساب ةداهشلا حتفاوع قوملا ىلإ لقتنا . قحجال تقول اذه ظفحإ . PEM قيسنت ةداهش

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

```
MIIDCCCAfCgAwIBAgIQE4ZG5Z1wT61ONTjooEQyMTANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDExJleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YUw1bW1wGUtV01OMjAxNi1DQTCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAI8ghT719NzSQpoQPh0YT67b
Ya+PngsxMyvkewP33QLTAww1HW1Tb9Mk5BDW0ItTaVsgHwPBfd++m+bLn3AiZnHV
00+k6dVVY/E5qVkeKSGoY+v940S23161zdwReMOFhgbc2qMertIoficrRihonuU
Cjyeub3C0+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpNO7KEMkfa1LPuM
aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHW1RnUIQBUaLdQaabhipD/
sVs5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKqOL7N86HFPfkMA3u8C
AwEAAaNCMEAwDgYDVR0PAQH/BAQDAgGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0O
BBYEFD2fJjf7ER9EM/HCxCVFN5QzqEdvMA0GCSqGSIb3DQEBCwUAA4IBAQB31ZJo
```

```
vzwVD3c5Q1nrNP+6Mq620FpYH91k4Ch9S5g/CE0emhcg8MDIoxW2dTsjenAEt7r  
phFIHZoCoSyjBjMgK3xybmoSeg8vBjCXseYNGEmOc9KW1oFmT0vdNVib7Xp11IVa  
6tALTt3ANRNgrREtxPA6yQbthKGavW0Anfsojk9IcDr2vp0MTj1BCxsTscubR1+D  
dLEFKQqmMeYvkVf+a7a64mqPZsG3Uxo0rd6cZxAPkq/y1cdwNSJFfQV3DgZg+R96  
9WLCR30big6xyo9Zu+1ixcWpdrbAD06zMhbEYEhkh00jBrUEBBI6Cy83iTZ9ejsk  
KgwBJXEu33Pp1W6E  
-----END CERTIFICATE-----
```

12. LDAPs لبق نم اهم ادختسإ نكمي يتلا ةيوهلا تاداهش نم ديدعل دوجو ةلاح ي (يرايخإ).
نم، LDAP، مداخل لوصو دوجو مدع وأ، مدختسمل ةيهامب قلعتي اميف نيقي مدع كانه ناك و
مدع ب FTD وأ Windows مداخل يلع مت ةمزح طاقتل نم يردجل عجرمل جارختسإ نكمملا

FMC تانويك

صخيخرتل نم ققحتل

قبيطت بجيو، يكدل صخيخرتل مداخل عم FTD ليجست مزلي، AnyConnect نيوكت رشنل
طقف زاهجلا يلع حلصا VPN وأ Apex وأ Plus صخيخرت

1. يكدل صخيخرتل > صخيخرتل > ماظنل يلقنا.



2. صخيخرت مادختساب زاهجلا ليجست نم دكأت. حاجنب ةلجسمو ةقفاوتم ةزهجالا نأ نم دكأت.
طقف VPN، Plus، وأ Apex AnyConnect

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help admin

Configuration Users Domains Integration Updates Licenses Smart Licenses Health Monitoring Tools

Smart License Status Cisco Smart Software Manager

Usage Authorization:	Authorized (Last Synchronized On May 03 2020)
Product Registration:	Registered (Last Renewed On Mar 03 2020)
Assigned Virtual Account:	SEC TAC
Export-Controlled Features:	Enabled
Cisco Success Network:	Disabled
Cisco Support Diagnostics:	Disabled

Smart Licenses Filter Devices... Edit Licenses

License Type/Device Name	License Status	Device Type	Domain	Group
Firepower Management Center Virtual (2)	✓			
Base (2)	✓			
Malware (1)	✓			
Threat (2)	✓			
URL Filtering (2)	✓			
AnyConnect Apex (1)	✓			
FTD-2 192.168.1.17 - Cisco Firepower Threat Defense for VMWare - v6.3.0	✓	Cisco Firepower Threat Defense for VMWare	Global	N/A
AnyConnect Plus (0)				
AnyConnect VPN Only (0)				

Note: Container Instances of same blade share feature licenses

دادعإلا ملع

1. لمكئلا > ماضنلا إلى إلقئنا.

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help admin

Configuration Users Domains Integration Updates Licenses Health Monitoring Tools

2. New Realm قوف رقنا مئ، Realms ئئئ.

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help admin

Configuration Users Domains Integration Updates Licenses Health Monitoring Tools

Cloud Services Realms Identity Sources eStreamer Host Input Client Smart Software Satellite Compare realms New realm

Name	Description	Domain	Type	Base DN	Group DN	Group Attribute	State
------	-------------	--------	------	---------	----------	-----------------	-------

3. مئ Microsoft مءاخ نم اءعئمئ مئ ئئلا ئامولءملا إلى اءانئسا ءبسانملا لوقءلا ألاما. OK قوف رقنا

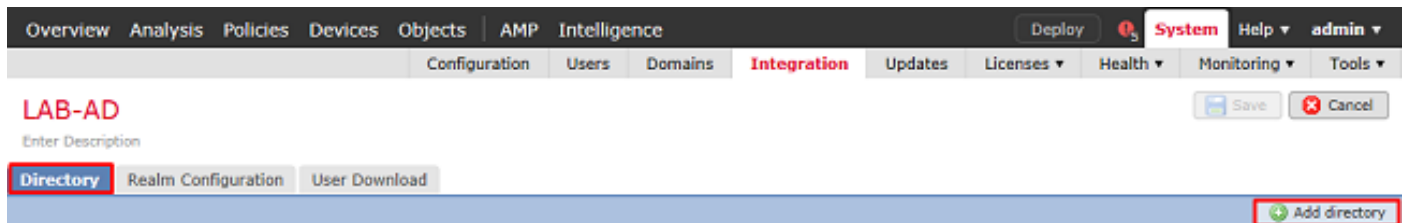
Add New Realm



Name *	<input type="text" value="LAB-AD"/>	
Description	<input type="text"/>	
Type *	<input type="text" value="AD"/>	
AD Primary Domain *	<input type="text" value="example.com"/>	ex: domain.com
AD Join Username	<input type="text"/>	ex: user@domain
AD Join Password	<input type="password"/>	<input type="button" value="Test AD Join"/>
Directory Username *	<input type="text" value="ftd.admin@example.com"/>	ex: user@domain
Directory Password *	<input type="password" value="*****"/>	
Base DN *	<input type="text" value="DC=example,DC=com"/>	ex: ou=user,dc=cisco,dc=com
Group DN *	<input type="text" value="DC=example,DC=com"/>	ex: ou=group,dc=cisco,dc=com
Group Attribute	<input type="text" value="Member"/>	

* Required Field

4. ليلد ةفاضل قوف رونا، لعف لاب هراي تخم دق نكي مل اذا ليلد ددح، ديدجل راطالال ي ف.





طبرللا FTD و FMC ل نكمي ال، FQDN مادختس ةلاح ي ف هنا طحال. AD مداخل ليصافات الم
ب FQDN لحل DNS نيوكت متي مل ام حاجن ب

ةرادال تاهجاو ددحو نيوكت > ماظن لىل لقتنا، FMC ل DNS دادع ل

ةسايس عاشن اب مق و، ياساس ال ماظن لادادع > ةزهجال لىل لقتنا، FTD ل DNS دادع لجا نم
ب DNS لىل لقتنا مثة للاح ةسايس ررح و، ةديج

Add directory



Hostname / IP Address	<input type="text" value="win2016.example.com"/>
Port	<input type="text" value="389"/>
Encryption	<input type="radio"/> STARTTLS <input type="radio"/> LDAPS <input checked="" type="radio"/> None
SSL Certificate	<input type="text"/>  

امسا صيخرتل طعأو، رضخألا (دئاز) + زمر رقنا، ةمدختسم STARTTLS وأ LDAPs تناك اذا ظفح قوف رقنا مث. PEM قي سننل رذجال قدصملا عجرملا ةداهش خسن او

Import Trusted Certificate Authority



Name:	<input type="text" value="LDAPS_ROOT"/>
Certificate Data or, choose a file:	<input type="button" value="Browse.."/>
<pre>-----BEGIN CERTIFICATE----- MIIDCCCAFgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhkiG9w0BAQsFADAd MRswGQYDVQQDEExleGFtZXIwLWVudC50d35tUvo/FEHGGXJFaJS1se2UrpNO7KEMkFA1LPuM aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWIRnUIQBUaLdQaabhipD/ sVs5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKqOL7N86HFPFkMA3u8C AwEAAaNCMEAwDgYDVR0PAQH/BAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0O BBYEFD2fj7ER9EM/HcXCVFN5QzqEdvMA0GCSqGSIb3DQEBCwUAA4IBAQB31ZJo vzwVD3c5Q1nrNP+6Mq62OFpYH91k4Ch9S5g/CEOemhcgw8MDIoxW2dTsjenAET7r phFIHZoCoSyjBjMgK3xybmoSeg8vBjCXseYNGEmOc9KW1oFmTOvdNVib7Xpl1IVa 6tALTt3ANRNREtPA6yQbthKGavW0Anfsojk9ICDr2vp0MTjBCxsTscubRI+D dLEFKQqmMeYvkVf+a7a64mqPZsG3Uxo0rd6cZxAPkq/ylcdwNSJFFQV3DgZg+R96 9WLCR3Obig6xyo9Zu+lixwPdrbADO6zMHbEYehkhOOjBrUEBBI6Cy83iTZ9ejsk KgwBJXEu33PplW6E -----END CERTIFICATE-----</pre>	
<input type="checkbox"/> Encrypted, and the password is:	<input type="text"/>

ةداهشل ةرواجملا ةلدسنملا ةمئاقلا نم اثيدح هتفاضلا تمت يذلا رذجال قدصملا عجرملا دح LDAPs و STARTTLS قوف رقنا و SSL.

Edit directory



Hostname / IP Address	<input type="text" value="win2016.example.com"/>
Port	<input type="text" value="636"/>
Encryption	<input type="radio"/> STARTTLS <input checked="" type="radio"/> LDAPS <input type="radio"/> None
SSL Certificate	<input type="text" value="LDAPS_ROOT"/>

رورم الة م لكو ليل دلل مدختسم مساب حاجنب FMC طبر ة ني ناكم ا نم دك ا تلل رابتخا قوف رقنا ة ق باسلا ة و طخلال ي ف ني ر فوملا

سي لو (FMC) ة ي س اس ا ل ة ح و ل ل ا ة ر ا د ا ي ف م ك ح ت ل ل ا ة د ح و ن م ا ه و د ب م ت ي ت ا ر ا ب ت خ ا ل ا ه ذ ه ن ا ل ا ر ط ن و ة ي ل خ ا د ل ل ا ت ا ه ج ا و ل ا ل م (FTD) ل ع ا ه ن ي و ك ت م ت ي ت ل ل ا ه ي ج و ت ل ل ة ل ب ا ق ل ل ا ت ا ه ج ا و ل ا ي د ح ا ل ل ا ل خ ن م ة ج ي ت ن ل ل س ف ن ن م ض ي ال (ل ش ا ف ل ا و ا) ح ج ا ن ل ل ل ا ص ت ا ل ا ن ا ف ، (DMZ) ة ط ق ن ل ل ا و ة ي ج ر ا خ ل ا و FTD ت ا ه ج ا و ي د ح ا ن م ا ه و د ب م ت ي AnyConnect LDAP ة ق د ا ص م ت ا ب ل ط ن ا ل AnyConnect ة ق د ا ص م ل ا ه ي ج و ت ل ل ة ل ب ا ق ل ل ا

ة ق د ا ص م ل ا ر ا ب ت خ ا م س ق ع ج ا ر ، FTD ن م LDAP ت ا ل ا ص ت ا ر ا ب ت خ ا ل و ح ت ا م و ل ع م ل ا ن م د ي ز م ل ا ط ا خ ا ل ا ف ا ش ك ت س ا ة ق ط ن م ي ف م ز ح ل ا ط ا ق ت ل م س ق و (AAA) ة ب س ا ح م ل ا و ض ي و ف ت ل ا و ا ه ج ا ل ص ا و

Status



Test connection succeeded

OK

5. مدختسم الة ي وهل اهم ادختسا م ت ي ت ل ل ا ت ا ع و م ج م ل ا ل ي ز ن ت ب م ق ، مدختسم الة ل ي ز ن ت ت ح ت . ة ق ح ا ل ل ا ت ا و ط خ ل ا ل ي ف

ة ح ا ت م ل ا ت ا ع و م ج م ل ا ب ص ا خ ل ا د و م ع ل ا و ت ا ع و م ج م ل ا و ن ي م د خ ت س م ل ا ل ي ز ن ت ب ص ا خ ل ا ع ب ر م ل ا د ح Active Directory ن م ض ا ه ن ي و ك ت م ت ي ت ل ل ا ت ا ع و م ج م ل ا ب ا ه ت ئ ب ع ت م ت ي ت ل ل ا

م ت ي ت ل ل ا ت ا ع و م ج م ل ا ع ي م ج ن ي م ض ت م ت ي ك ل ذ ع م و ، ا ه د ا ع ب ت س ا و ا ت ا ع و م ج م ل ا ن ي م ض ت ن ك م ي ي . ي ض ا ر ت ف ا ل ك ش ب ة ع و م ج م ل ا ب ة ص ا خ ل ا DN ن م ض ا ه ي ل ع ر و ث ع ل ا

نمضم تاعومجم ياً رفوتت .كلذك مهءاعب تسإ وأ نيددجم نيدمءتسم نيمضت نكمي امك قءال تقوي ف مءءتسم الة يوهل مهءيدءت مءيل نيدمءتسم و

ظفء قوف رقنا ،ءاءءنالا دنء

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help admin

Configuration Users Domains **Integration** Updates Licenses Health Monitoring Tools

LAB-AD You have unsaved changes Save Cancel

Directory Realm Configuration **User Download**

Download users and groups

Begin automatic download at 8 PM America/New York Repeat Every 24 Hours

Download Now

Available Groups

Search by name

- AnyConnect Admins
- DnsUpdateProxy
- WseRemoteAccessUsers
- WseInvisibleToDashboard
- Allowed RODC Password Replication Group
- Enterprise Key Admins
- Domain Admins
- WseAlertAdministrators
- Event Log Readers
- Replicator
- Domain Guests
- Windows Authorization Access Group
- Account Operators
- Hyper-V Administrators
- System Managed Accounts Group

Groups to Include (2)

- AnyConnect Admins
- AnyConnect Users

Groups to Exclude (0)

None

Add to Include Add to Exclude

Enter User Inclusion Add Enter User Exclusion Add

6. ديدءال لاءم ال نيمءمء

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help admin

Configuration Users Domains **Integration** Updates Licenses Health Monitoring Tools

Cloud Services **Realms** Identity Sources eStreamer Host Input Client Smart Software Satellite

Compare realms New realm

Name	Description	Domain	Type	Base DN	Group DN	Group Attribute	State
LAB-AD		Global	AD	DC=example,DC=com	DC=example,DC=com	member	<input checked="" type="checkbox"/>

7. فءءس او ب رءءال ءا قءي نأ اضيأ مزليءس ف ،STARTTLS وأ LDAPs مءءءتسإ مء اءا .ءاءاءشال > ءزهءال ال لءقءنا ،الوأ اءء مءيقلل

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT VPN QoS Platform Settings FlexConfig **Certificates**

نيمي لءءال ي ف فيضي ءقءق

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT VPN QoS Platform Settings FlexConfig **Certificates** Add

(ءئاز) + زم رقوف رقنالا ال LDAP نيوءء ءافاضإ مءء فءء

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-2

Cert Enrollment*:

Select a certificate enrollment object

Add

Cancel

ليجستال عون ةلدسنم المة ئاقول نم يوديلا ليجستال رتخأ م ث لاصتال ةطقنل مساحنم ظفح يل عرقنا م ث ، انه PEM رذج قي دصت عجرم ةداهش قصلال

Add Cert Enrollment



Name*

LDAPS_ROOT

Description

CA Information

Certificate Parameters

Key

Revocation

Enrollment Type:

Manual

CA Certificate:*

```
-----BEGIN CERTIFICATE-----
MIIDCDCCAfCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhki
G9w0BAQsFADAd
MRswGQYDVQQDEExleGFtcG9uLWVudC51b3R0eS1uYXZlbnQ0
3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTIaMB0xGzAZBgNVBAMTEmV4YW1wbGU
tv0lOMjAxNi1DQTCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAI8ghT719N
zSQpoQPh0YT67b
Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOITaVsgHwPbf
d++M+bLn3AiZnHV
OO+k6dVVY/E5qvKEKSGoY+v940S2316lzdwrEMOFhgbc2qMertIo
ficrRihonuU
Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFa3S1se2UrpN
O7KEMkfa1LPuM
aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWlRnUIQBU
aLdQaabhipD/
sVs5PneYJX8YKma821uYI6j90YuytmsHBTcIevC062a8BKqOL7N86
```

Allow Overrides

Save

Cancel

ةفاضل قوف رقنا م ث ؤاشنل م ث يذل TrustPoint دي دحت نم ققحت

Add New Certificate



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

Device*:

Cert Enrollment*:

Cert Enrollment Details:

Name: LDAPS_ROOT

Enrollment Type: Manual

SCEP URL: NA

Add

Cancel

يوهل اءءاهش ءاريتس انا ركذي هنا نم مغرلا يلع . FTD نمض ءءيءال ءقثلا ءطقن رهظت ءلذل . LDAP مءاخ نم ءلسرمل ال SSL ءءاهش ءقءاصم FTD نم اءولطم سئل هنا الء ءولطم ءللسرللا هءه لهاءء نءمئ

Name	Domain	Enrollment Type	Status
FTD-1			
FTD-1-PKCS12	Global	PKCS12 file	CA, ID
FTD-2			
FTD-2-PKCS12	Global	PKCS12 file	CA, ID
FTD-2-Selfsigned	Global	Self-Signed	CA, ID
LDAPS_ROOT	Global	Manual	CA, ID, Identity certificate import required

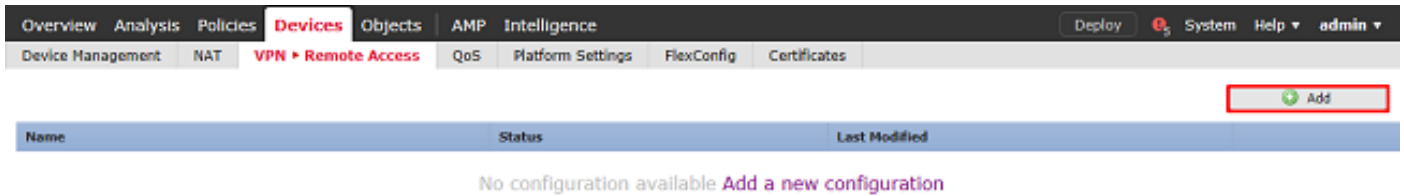
AD ءقءاصم ال AnyConnect نئوكء

ءاشن اءل ءلءلاب ءءب نع لوصولل VPN ءهن ءاشن اءل مءئ مل هنا ءا وءءل هءه ضرءءء 1. 3. ءوءءل ءطءءو ءهن ال اءهل "رئءء" رءلا ءوف رءناف ءءاو

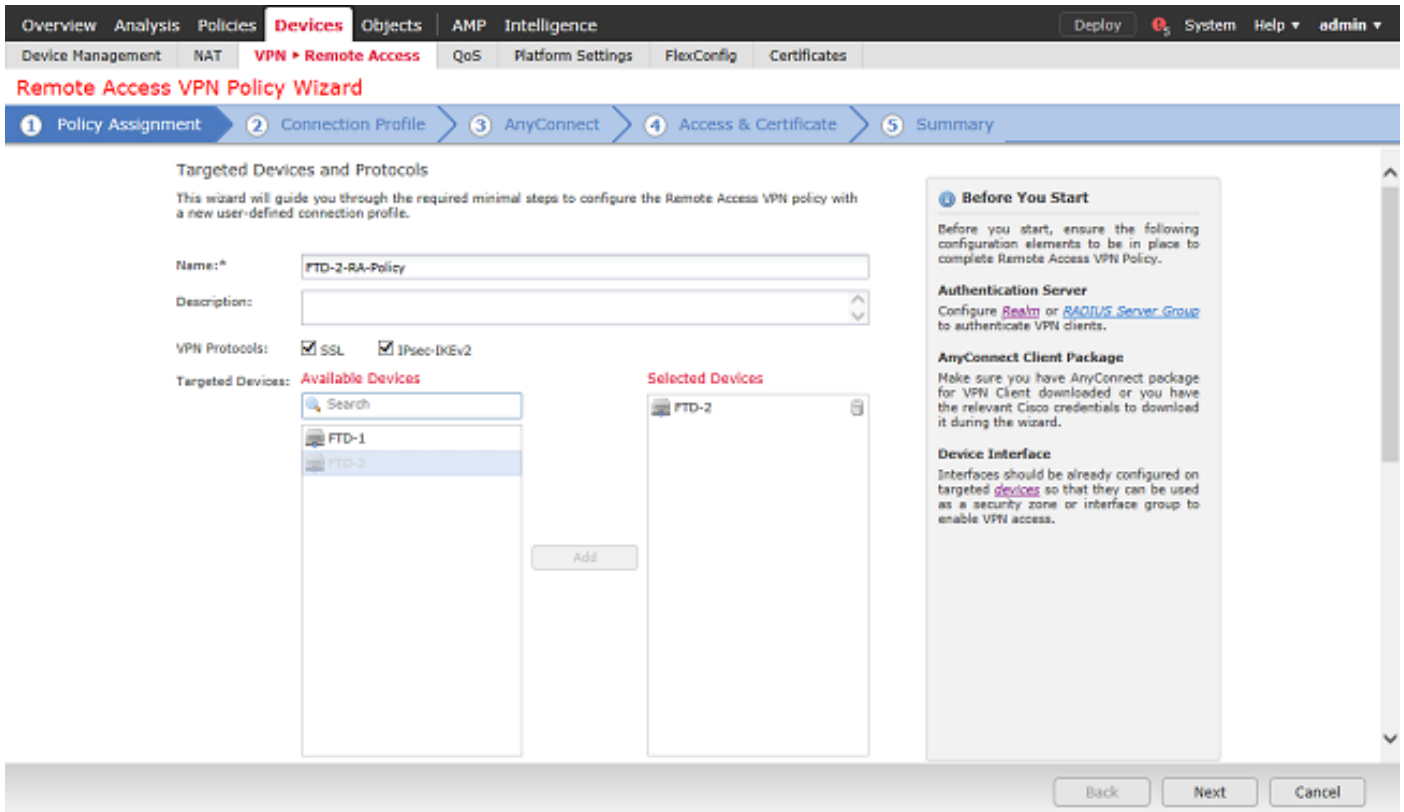
ءءب نع لوصولل > VPN > ءزهءال ال لءلقءنا

Device Management	NAT	VPN	QoS	Platform Settings	FlexConfig	Certificates
		Site To Site				
		Remote Access				
		Troubleshooting				

ءءب نع لوصولل ءئء VPN ءهن ءاشن ال ءفاضا ءوف رءنا



2. عه اوجهن لل امسا دح، جهن لل نيي عت تحت. دع ب نع لوصول VPN جهن جلا عم لامك اب مق. اه لعل جهن لل قيبطت متي يتي لل



راع تس م ساك اضي ا مدختسي يذلا لي صوت لل في صوت مسا دح، لي صوت لل في صوت تحت م. هل صوت دنع AnyConnect وم دختسم هاري ع وم جمل لل

ع. قدا صملا مداخ تحت اقبسم هؤاشن ا مت يذلا قاطن لل دح.

AnyConnect. اءالم عمل IP نيوانع نيي عت اه ب متي يتي لعل قيرطال دح

اذه لاصلتاللا في رعت فل مل مدختسم ل ا يضارت فالال ع وم جمل جهن دح

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT **VPN > Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 **Connection Profile** 3 AnyConnect 4 Access & Certificate 5 Summary

Connection Profile:
 Connection Profiles specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itself, how AAA is accomplished and how addresses are assigned. They also include user attributes, which are defined in group policies.

Connection Profile Name: *
This name is configured as a connection alias, it can be used to connect to the VPN gateway

Authentication, Authorization & Accounting (AAA):
 Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.

Authentication Method:
 Authentication Server: * (Realm or RADIUS)
 Authorization Server: (RADIUS)
 Accounting Server: (RADIUS)

Client Address Assignment:
 Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

Use AAA Server (RADIUS only) ⓘ
 Use DHCP Servers
 Use IP Address Pools

IPv4 Address Pools:
 IPv6 Address Pools:

Group Policy:
 A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy: * ⓘ
[Edit Group Policy](#)

Back Next Cancel

مزال هذه دي دحت و اهم ادختس! متي يتل AnyConnect مزح لي محتب مق AnyConnect نمض.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT **VPN > Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 **AnyConnect** 4 Access & Certificate 5 Summary

AnyConnect Client Image
 The VPN gateway can automatically download the latest AnyConnect package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download AnyConnect Client packages from [Cisco Software Download Center](#).

Show Re-order buttons ⓘ

<input checked="" type="checkbox"/>	AnyConnect File Object Name	AnyConnect Client Package Name	Operating System
<input checked="" type="checkbox"/>	anyconnect-linux64-4.7.03052-we...	anyconnect-linux64-4.7.03052-webdeploy-k9...	Linux
<input checked="" type="checkbox"/>	anyconnect-win-4.7.00136-webde...	anyconnect-win-4.7.00136-webdeploy-k9.pkg	Windows

Back Next Cancel

لجأ نم اهيلي لوصول AnyConnect يمدختس مل نكمي يتل هه اول دح، داهش لاول لوصول تحت AnyConnect.

حفاصم ءانثأ FTD لبق نم اهم ادختس! متي يتل داهش ل دي دحت وأ و ءاشن اب مق

كف مت يتل رورملا ءكرحل يفافتلال لوصول اب مكحتل ءسايسل رايتخال ءناخ نأ نم دكأت اهؤاشن مت يتل ممدختس مل ءي وه حبصت شيح ب ددحم ريغ (sysopt allowed-vpn) اهري فشت RAVPN. تالاصتال لوعفملا ءذفان اقحال

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT **VPN > Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 **Access & Certificate** 5 Summary

Network Interface for Incoming VPN Access
 Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

Interface group/Security Zone: * +

Enable DTLS on member interfaces

Device Certificates
 Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment: * +

Enroll the selected certificate object on the target devices

Access Control for VPN Traffic
 All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

Bypass Access Control policy for decrypted traffic (syntax permit-vpn)
This option bypasses the Access Control Policy inspection, but VPN filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.

Back Next Cancel

ءاهن إ قوف رقنا نيوكتلا عجار، صخلم تحت

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT **VPN > Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 **Access & Certificate** 5 Summary

Remote Access VPN Policy Configuration

Firepower Management Center will configure an RA VPN Policy with the following settings

Name: FTD-2-RA-Policy

Device Targets: FTD-2

Connection Profile: General

Connection Alias: General

AAA:

- Authentication Method: AAA Only
- Authentication Server: LAB-AD
- Authorization Server: -
- Accounting Server: -

Address Assignment:

- Address from AAA: -
- DHCP Servers: -
- Address Pools (IPv4): AnyConnect-Pool
- Address Pools (IPv6): -

Group Policy: DfltGrpPolicy

AnyConnect Images:

- anyconnect-linux64-4.7.03052-webdeploy-k9.pkg
- anyconnect-win-4.7.00136-webdeploy-k9.pkg

Interface Objects: outside-zone

Device Certificates: FTD-2-Selfsigned

Device Identity Certificate Enrollment

Certificate enrollment object 'FTD-2-Selfsigned' is not installed on one or more targeted devices. Certificate installation will be initiated on the targeted devices on finishing the wizard. Go to the [Certificates](#) page to check the status of the installation.

Additional Configuration Requirements

After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets.

- Access Control Policy Update**
An [Access Control](#) rule must be defined to allow VPN traffic on all targeted devices.
- NAT Exemption**
If NAT is enabled on the targeted devices, you must define a [NAT Policy](#) to exempt VPN traffic.
- DNS Configuration**
To resolve hostname specified in AAA Servers or CA Servers, configure DNS using [FlexConfig Policy](#) on the targeted devices.
- Port Configuration**
SSL will be enabled on port 443. IPsec-IKEv2 uses port 500 and Client Services will be enabled on port 443 for Anyconnect image download. NAT-Traversal will be enabled by default and will use port 4500. Please ensure that these ports are not used in [NAT Policy](#) or other services before deploying the configuration.

Network Interface Configuration
 Make sure to add interface from targeted devices to SecurityZone object 'outside-zone'

Back Finish Cancel

توقياً قوف رقنا، دع بع لوصول ةسايس > (VPN) ةيرهاطلا ةصاخلا ةكبشلا نمض 3.
 بسانملا لاصلتالا فيرعت فلم يلع لوصولل (صاصر ملق) ريرحت

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT **VPN Remote Access** QoS Platform Settings FlexConfig Certificates

FTD-2-RA-Policy Save Cancel

Enter Description Policy Assignments (1)

Connection Profile Access Interfaces Advanced

Name	AAA	Group Policy
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	DfltGrpPolicy
General	Authentication: LAB-AD (AD) Authorization: None Accounting: None	DfltGrpPolicy

اقبس م هؤاشنإ مت يذلا قاطنلا ىلع ةقداصلما م داخ نييعت نم دكأت

اورغي نأ ني مدختسملل حامسلل رورملا ةملك ةرادإ قيقدت نكمي ، ةمدقتم تادادعإ تحت اهتيجالصل يهتنت نأ لقبق وأ ام دنع مه رورم ةملك

قوف رقنا ، تاريغت ي أ عارجإ مت اذا LDAPs قاطنلا مدختسي نأ بلطتي دادعإلا اذه نأ ريغ ظفح

Edit Connection Profile ? X

Connection Profile:* General

Group Policy:* DfltGrpPolicy [Edit Group Policy](#)

Client Address Assignment **AAA** Aliases

Authentication

Authentication Method: AAA Only

Authentication Server: LAB-AD (AD)

Use secondary authentication

Authorization

Authorization Server:

Allow connection only if user exists in authorization database

Accounting

Accounting Server:

Advanced Settings

Strip Realm from username

Strip Group from username

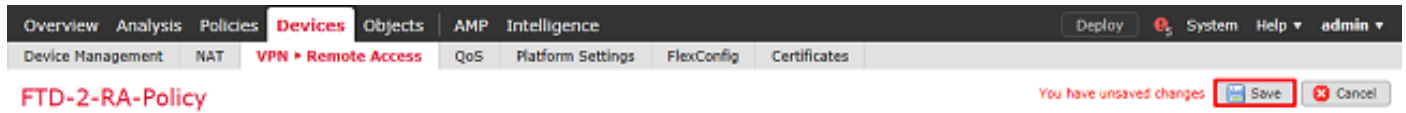
Enable Password Management

Notify User 14 days prior to password expiration

Notify user on the day of password expiration

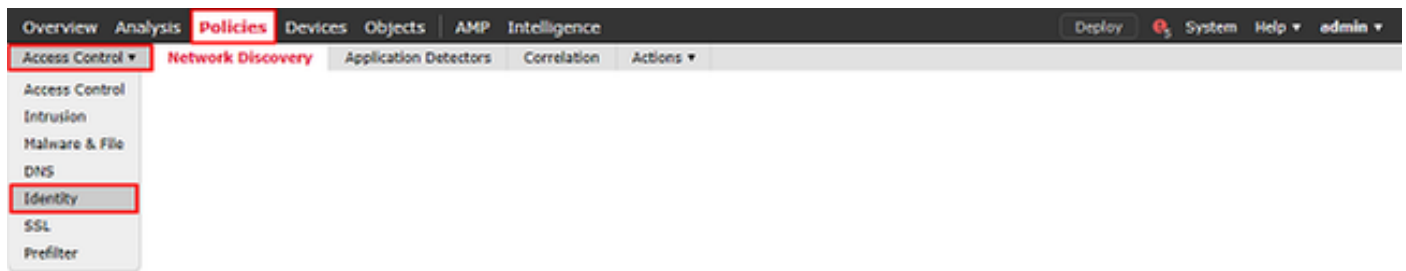
Save Cancel

ظفح قوف رقنا،ءاهتالال دنع



مدختسمل ءيول نامأل تاسايس نيوكتو ءيولال جهن نيكمتم

ءيولال > لوصولل ءي مكلحتلل > تاسايسلل ءلل لقتنا 1.



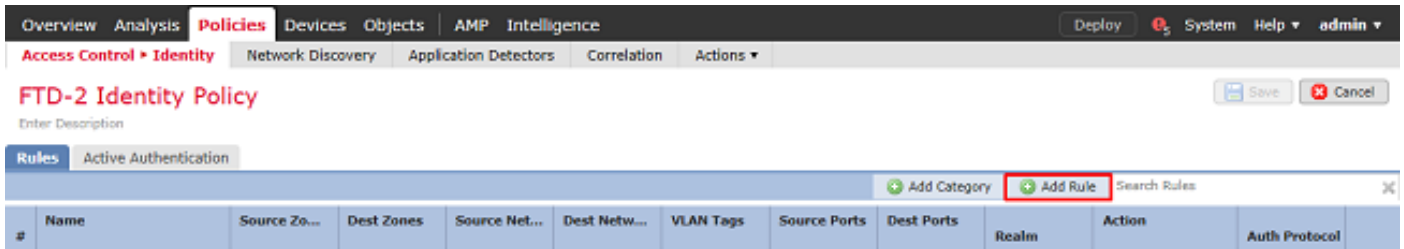
ءي ءيولال ءاشنل



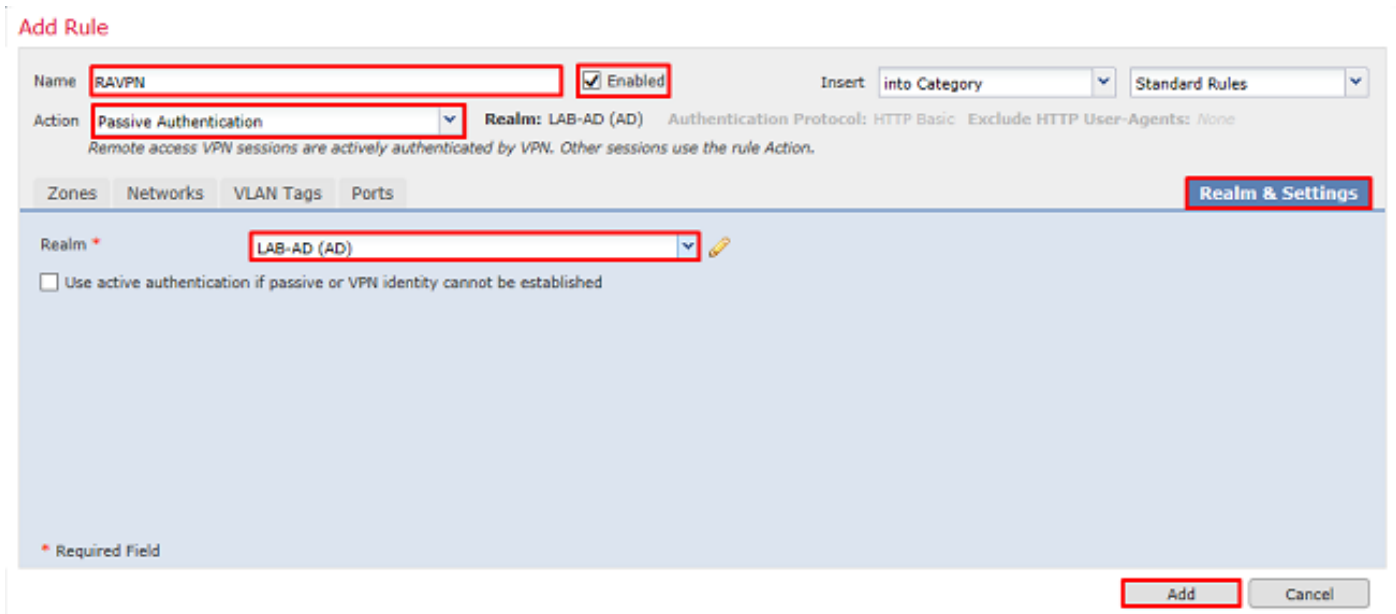
ءي ءل ءيولال جهنل امسا ءء



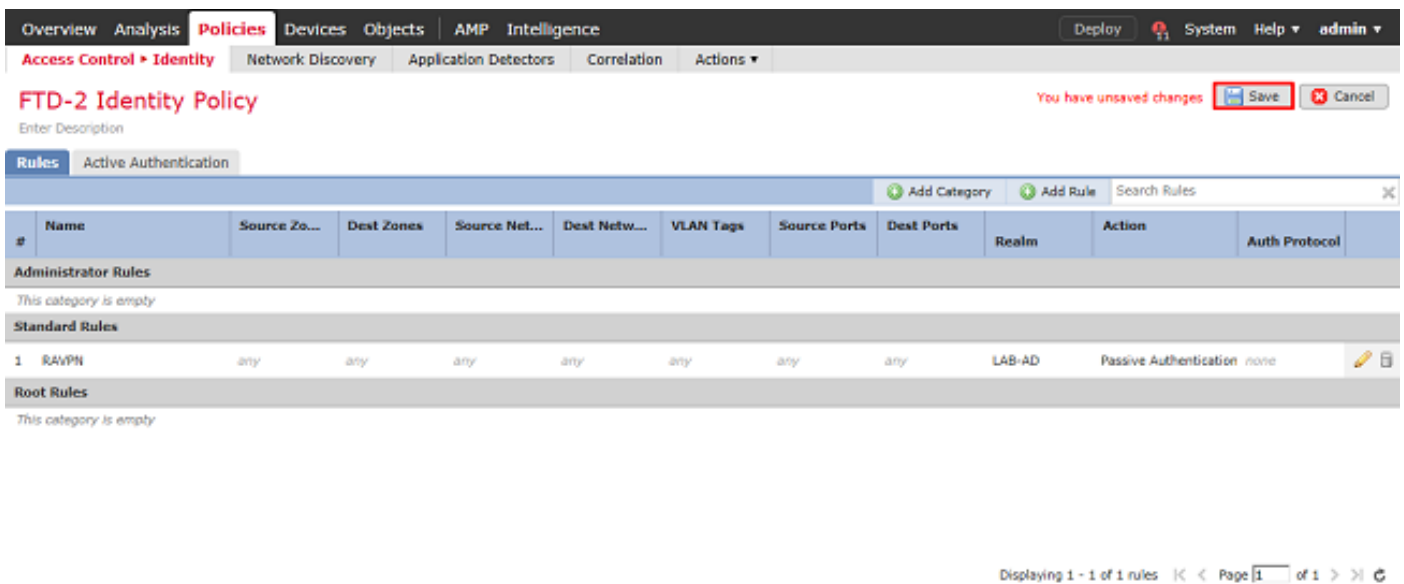
ءءاق ءفاضا قوف رقنا 2.



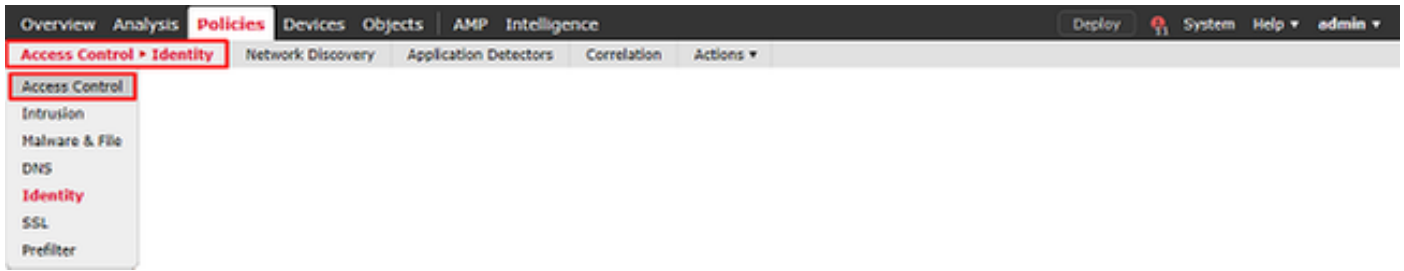
3. قلم الخالفة قداصلم الى ل ع ارجال ني عت مت واهني كمت نم دكأت .ةديجل الة دة اقلل امسا دح .
هؤاشنإ مت يذل قاطنل ددحو (تادادعإل او قاطنل) Realm & Settings بيوبتل الة مالع قوف رقنا
عاهتال دن عة فاضإ قوف رقنا .اقبسم



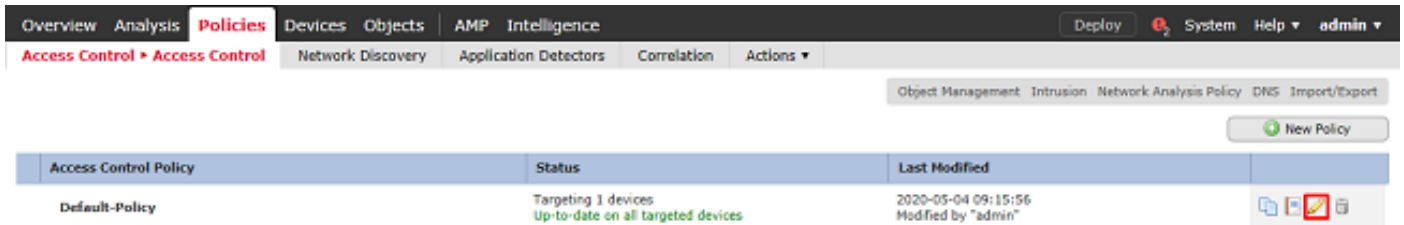
4. ظفح قوف رقنا .



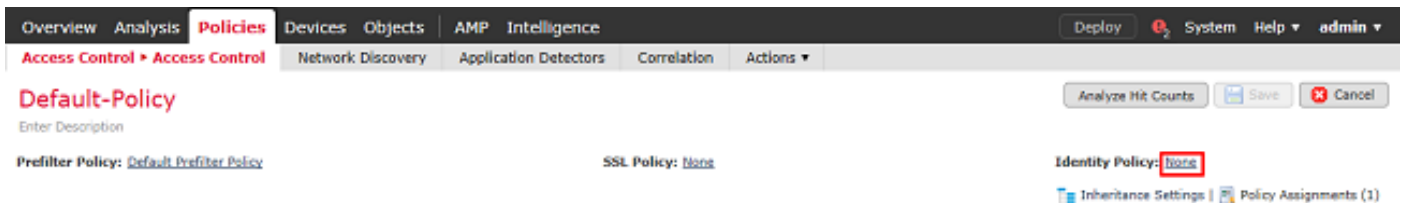
5. لوصولي ف مكحتل > لوصولي ف مكحتل > تاسايسل الى لقتنا .



6. اہب صاخال FTD نيوكوت مت يتلا لوصولو ي ف مكحتلا ةسايس ريحت .



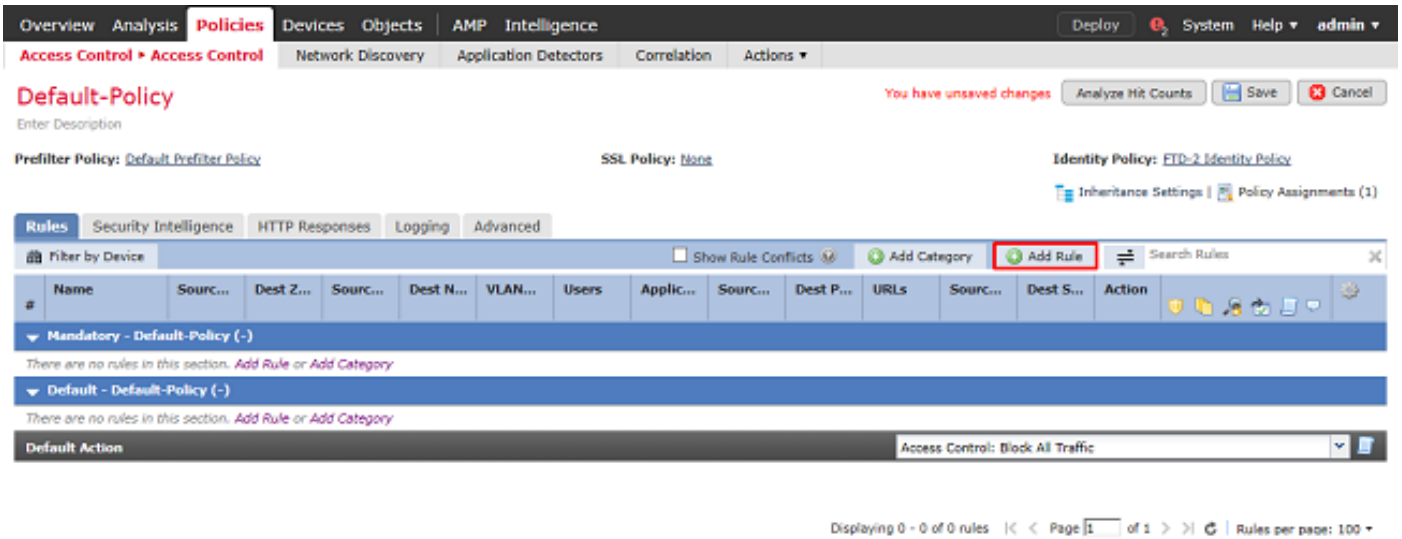
7. ةيوهلا جهنل ةرواجملا ةميقلال قوف رقنا .



قفاوم قوف رقنا م اقبسم هؤاشنإ مت يذلا ةيوهلا جهن دح.



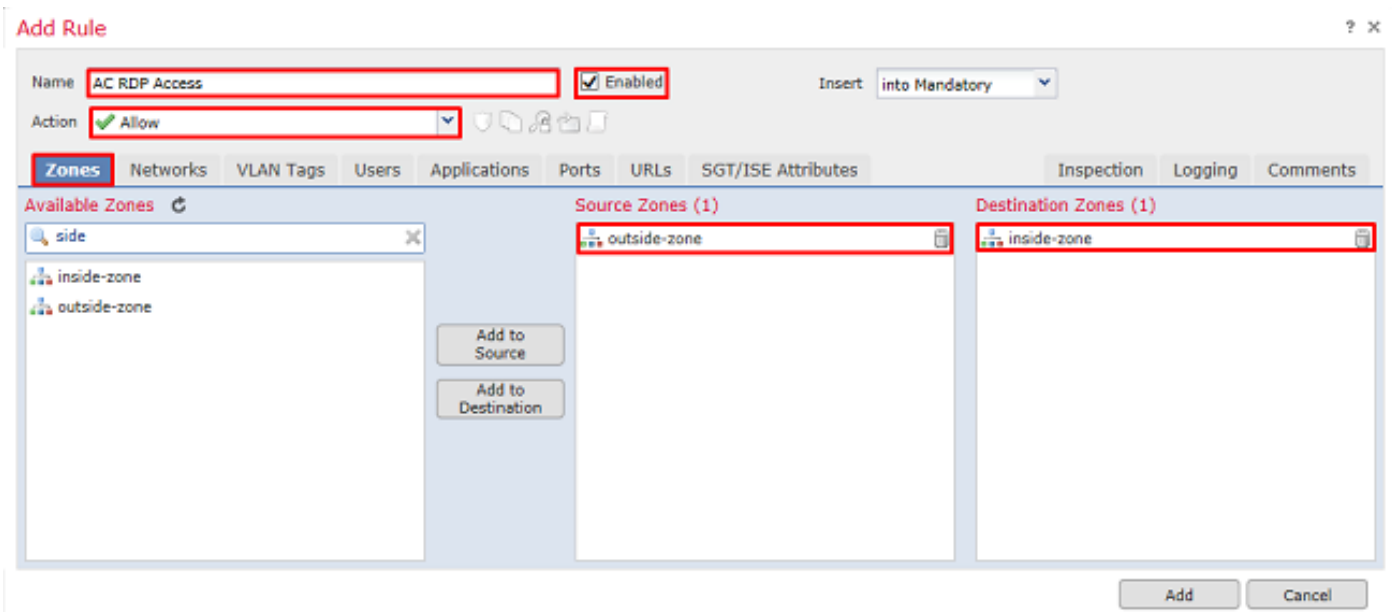
8. ةدعاق عاشنإ يلع تاوطخلا هذه لمعت . ةديج ACP ةدعاق عاشنإل ةدعاق ةفاضل قوف رقنا . ةكبشلا لخاد ةزهجأ لاصتالاب AnyConnect يلوؤسم ةعومجم نمض مدختسملل حامسلل RDP مادختساب .



بـسانـمـلـا عـارـجـإـلـا رـفـوت نـم و ؤـعـاقـلـال نـيـكـمـت نـم دـكـأت . ؤـعـاقـلـل اـمـسـا دـح .

ةـدـيـفـمـلـا رـورـمـلـا ؤـكـرـحـل ؤـبـسـانـمـلـا قـطـانـمـلـا دـح ، قـطـانـم بـيـوـبـتـلـا ؤـمـالـع تـحـت .

ةـيـجـرـاـخـالـل ؤـقـطـنـمـلـا ؤـهـجـا و نـم اـهـرـدـصـمـلـا FTD يـلـى و نـومـدـخـتـسـمـلـا اـهـأـب يـتـلـال RDP رـورـم ؤـكـرـح يـتـأت ؤـيـلـخـادـلـال ؤـقـطـنـمـلـا نـم جـرـخـت و .



ةـهـجـولـا و رـدـصـمـلـا تـاـكـبـش فـيـرـعـتـب مـق ، تـاـكـبـشـلـا تـحـت .

AnyConnect . ؤـمـالـعـلـا اـهـنـيـيـعـت مـتـي يـتـلـال IP نـيـوانـع AnyConnect_POOL نـئـاـكـلـال نـمـضـتـي .

ةـيـلـخـادـلـال ؤـيـعـرـفـالـال ؤـكـبـشـلـال inside_net نـئـاـكـلـال نـمـضـتـي .

Add Rule

Name: AC RDP Access Enabled Insert: into Mandatory

Action: Allow

Zones: **Networks** VLAN Tags Users Applications Ports URLs SGT/ISE Attributes Inspection Logging Comments

Available Networks: Search by name or value

- Inside_Net
- IPv4-Benchmark-Tests
- IPv4-Link-Local
- IPv4-Multicast
- IPv4-Private-10.0.0.0-8
- IPv4-Private-172.16.0.0-12
- IPv4-Private-192.168.0.0-16
- IPv4-Private-All-RFC1918
- IPv6-IPv4-Mapped

Source Networks (1):

Source	Original Client
AnyConnect_Pool	

Destination Networks (1):

Inside_Net

Enter an IP address Add

Enter an IP address Add

Add Cancel

قوف رقنا مٲ، ءحاتم ال RealMs نمض اق بسم هؤاشنإ مٲ يذلا قاطنل قوف رقنا، Users تحت ءءاقلا إل ءافاضا قوف رقنا مٲ، Available Users نمض بسانم الم ءءءس الم/ءءومءم الم.

مايق نم ءكأءف، نءءءم الم نءءءءس الم مسق نمض ءءومءم وأ نءءءءس م يأ رفوءء مءل إءا نمض ءءومءم الم او نءءءءس الم لءزنءب (FMC) ءءءس أال ءءولل ءراءا ف مءءءل ءءو بسانم الم ءءءس الم/ءءومءم الم نءمضء نم و قاطنل مسق.

رءص الم روظنم نم انه ءءءم الم ءءومءم الم/نءءءءس الم نم ققءءل مءء.

ءءء نأ FTD مءقء، نأل ءءءءاقلا هءء فءفءرءء مءءم ءءءءس اب، لءءم لءب س ءل مءءو، ءءءءل ءءنم الم إل اءءءءو مءءو ءءءءءل ءءنم الم نم اءءل ءل و صءل مءء رورم الم فء ءءبءل إل اءءءءو مءءو و AnyConnect_Pool نءء فء ءءبءل نم اءءل ءل و صءل الم AnyConnect ءءومءم فء ءءءس م نم رورم ل ءءءءل ءل و صءل مءءو، Inside_Net نءءء Admins.

Add Rule

Name: AC RDP Access Enabled Insert: into Mandatory

Action: Allow

Zones: Networks VLAN Tags **Users** Applications Ports URLs SGT/ISE Attributes Inspection Logging Comments

Available Realms: Search by name or value

- Special Identities
- LAB-AD

Available Users: Search by name or value

- LAB-AD/*
- AnyConnect Admins
- AnyConnect Users
- it.admin
- test.user

Selected Users (1):

LAB-AD/AnyConnect Admins

Add to Rule

Add Cancel

هنأ طءال 3389 ءانءم UDP و TCP ءم سء نأ ءءفضأ نءءءك RDP صصءم ءنءء، ءانءم ءءء نم ققءءل مءء، ءءاسبلا لءأ نم نءل و ءاقءبءل م مسق نمض RDP ءافاضا نءمء.

طاقف ذفانملا

Add Rule ? x

Name: AC RDP Access Enabled Insert: into Mandatory

Action: Allow

Zones Networks VLAN Tags Users Applications **Ports** URLs SGT/ISE Attributes Inspection Logging Comments

Available Ports: Search by name or value

- AOL
- BitTorrent
- DNS_over_TCP
- DNS_over_UDP
- FMC-HTTPS
- FMC-SSH
- FTD-3-FDM
- FTD-3-SSH
- FTP
- HTTP

Selected Source Ports (0): any

Selected Destination Ports (2): RDP-TCP, RDP-UDP

Protocol: TCP (6) Port: Enter a Add

Add Cancel

ققحتلل لاصتالا ةياهن يف لجسلا نم ققحتلا متي ،لجسلا تحت هنا نم دكات ،اريأ عاهتتالا دنع ةفاضل قوف رقنا . قجال تقوي يف فاضالا

Add Rule ? x

Name: AC RDP Access Enabled Insert: into Mandatory

Action: Allow

Zones Networks VLAN Tags Users Applications Ports URLs SGT/ISE Attributes Inspection **Logging** Comments

Log at Beginning of Connection

Log at End of Connection

File Events:

Log Files

Send Connection Events to:

Event Viewer

Syslog Server (Using default syslog configuration in Access Control Logging) Show Overrides

SNMP Trap Select an SNMP Alert Configuration...

Add Cancel

ةومجمل نمض ني مدختسملل حامس لل HTTP لوصول ةفاضل ةدعاق عاشنإ متي 9. ظفح قوف رقنا . بېولا ىلع Windows Server IIS عقوم ىلإ مدختسملا لوصول AnyConnect

Default-Policy

Enter Description

Prefilter Policy: [Default Prefilter Policy](#) SSL Policy: [None](#) Identity Policy: [FTD-2 Identity Policy](#)

Inheritance Settings | Policy Assignments (1)

Rules Security Intelligence HTTP Responses Logging Advanced

Filter by Device Show Rule Conflicts Add Category Add Rule Search Rules

#	Name	Source Zo...	Dest Zones	Source Networks	Dest Netwo...	V...	Users	A...	S...	Dest Ports	U...	S...	D...	Action
▼ Mandatory - Default-Policy (1-2)														
1	AC RDP Access	outside-zone	inside-zone	AnyConnect_Pool	Inside_Net	Any	LAB-AD/AnyConnect Admins	Any	Any	RDP-TCP RDP-UDP	Any	Any	Any	Allow
2	AC HTTP Access	outside-zone	inside-zone	AnyConnect_Pool	Inside_Net	Any	LAB-AD/AnyConnect Users	Any	Any	HTTP	Any	Any	Any	Allow
▼ Default - Default-Policy (-)														
There are no rules in this section. Add Rule or Add Category														

Default Action: Access Control: Block All Traffic

Displaying 1 - 2 of 2 rules | Page 1 of 1 | Rules per page: 100

NAT انثتسإ نيوكت

نأ م مهم وه ،ةدعاق برض تنرتنإ لثم ،رورم ةكرح AnyConnect لىل ع رثؤي نأ ةدعاق nat كانه نإ رثأتى nat ال رورم ةكرح AnyConnect so that ةدعاق انثتسإ nat لكشي.

1. NAT > ةزهجالا لىل لقتنا.

Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management **NAT** VPN QoS Platform Settings FlexConfig Certificates

Deploy System Help admin

New Policy

FTD لىل قبطم ال NAT جهن دح

Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management **NAT** VPN QoS Platform Settings FlexConfig Certificates

Deploy System Help admin

NAT Policy	Device Type	Status
FTD-2-NAT-Policy	Threat Defense	Targeting 1 devices Up-to-date on all targeted devices

2. امب) رورم ةكرح لك رثؤي برض يآ ةياهنلا ي ف يكييمانيد برض كانه ،هذه NAT ةسايس ي ف .يچراخ نراقلا لىل يچراخ نراقلا زرفي نأ (رورم ةكرح AnyConnect كلذ ي ف

ةدعاق ةفاضل قوف رقنا ،NAT لىل AnyConnect رورم ةكرح ريثأت عنمل

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management **NAT** VPN QoS Platform Settings FlexConfig Certificates

FTD-2-NAT-Policy

Enter Description

Show Warnings Save Cancel

Policy Assignments (1)

Rules

Filter by Device Add Rule

#..	Direction	Type	Original Packet		Translated Packet		Options
			Source Interface Object	Destination Interface Object	Original Sources	Original Destinations	
NAT Rules Before							
Auto NAT Rules							
=	→	Dynamic	any	outside-zone	obj-any	Interface	Dns: false
NAT Rules After							

Displaying 1-1 of 1 rows Page 1 of 1 Rows per page: 100

عونلا عم ةيودي NAT ةدعاق يه ةدعاقلا نأ نم دكأتو، NAT ءانثتسا ةدعاق نيوكتب مق 3. AnyConnect رورم ةكرح ىلع قبطنت هاجتإلا ةيئانث NAT ةدعاق اذه. يكيئاتسا نكاس

ناونع ىلإ ةهجومو Inside_Net نم ةردصم رورم ةكرح FTD فشتك يامدنع، تادادعإلا هذه عم ةميقلال سفن ىلإ ردصملا ةمچرت متت، (AnyConnect_POOL ةطساوب فرعملال) AnyConnect_IP رورم ةكرح لوصو دنع (AnyConnect_POOL) ةميقلال سفن ىلإ ةهجوملا ةمچرت متتو (Inside_Net) متي امدنع NAT ياساسا لكشب اذه زواجتي. zone_جراخ ليحستتو inside_zone تانايبلا طورشللا هذه ءافيتسا.

Add NAT Rule

NAT Rule: Manual NAT Rule Insert: In Category NAT Rules Before

Type: Static Enable

Description:

Interface Objects Translation PAT Pool Advanced

Available Interface Objects

zone

inside-zone
outside-zone

Add to Source
Add to Destination

Source Interface Objects (1)

inside-zone

Destination Interface Objects (1)

outside-zone

OK Cancel

Add NAT Rule ? x

NAT Rule: Manual NAT Rule Insert: In Category NAT Rules Before

Type: Static Enable

Description:

Interface Objects **Translation** PAT Pool Advanced

Original Packet	Translated Packet
Original Source:* Inside_Net	Translated Source: Address
Original Destination: Address	Translated Destination: Inside_Net
Original Source Port: <input type="text"/>	Translated Source Port: <input type="text"/>
Original Destination Port: <input type="text"/>	Translated Destination Port: <input type="text"/>
Original Source Port: <input type="text"/>	Translated Source Port: <input type="text"/>
Original Destination Port: <input type="text"/>	Translated Destination Port: <input type="text"/>

OK Cancel

ARP سيو هذه رورملا ةكرح راسم نع شحب ءارجإل FTD نيني عت متي ،كلذ يلى ءفاضا لابلو م ام دنع ok ةق قوط .للي كولل

Add NAT Rule ? x

NAT Rule: Manual NAT Rule Insert: In Category NAT Rules Before

Type: Static Enable

Description:

Interface Objects Translation PAT Pool **Advanced**

Translate DNS replies that match this rule

Falthrough to Interface PAT(Destination Interface)

IPv6

Net to Net Mapping

Do not proxy ARP on Destination Interface

Perform Route Lookup for Destination Interface

Unidirectional

OK Cancel

4. ظفح قوف رونا .

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

FTD-2-NAT-Policy You have unsaved changes Show Warnings Save Cancel

Enter Description Policy Assignments (1)

Rules Filter by Device Add Rule

#	Direction	Type	Source Interface Object	Destination Interface Object	Original Packet		Translated Packet			Options
					Original Sources	Original Destinations	Orig... Services	Translated Sources	Translated Destinations	
▼ NAT Rules Before										
1	↔	Static	inside-zone	outside-zone	Inside_Net	AnyConnect_Pool	Inside_Net	AnyConnect_Pool		Dns:false route-lookup no-proxy-arp
▼ Auto NAT Rules										
=	↔	Dynamic	any	outside-zone	obj-any		Interface			Dns:false
▼ NAT Rules After										

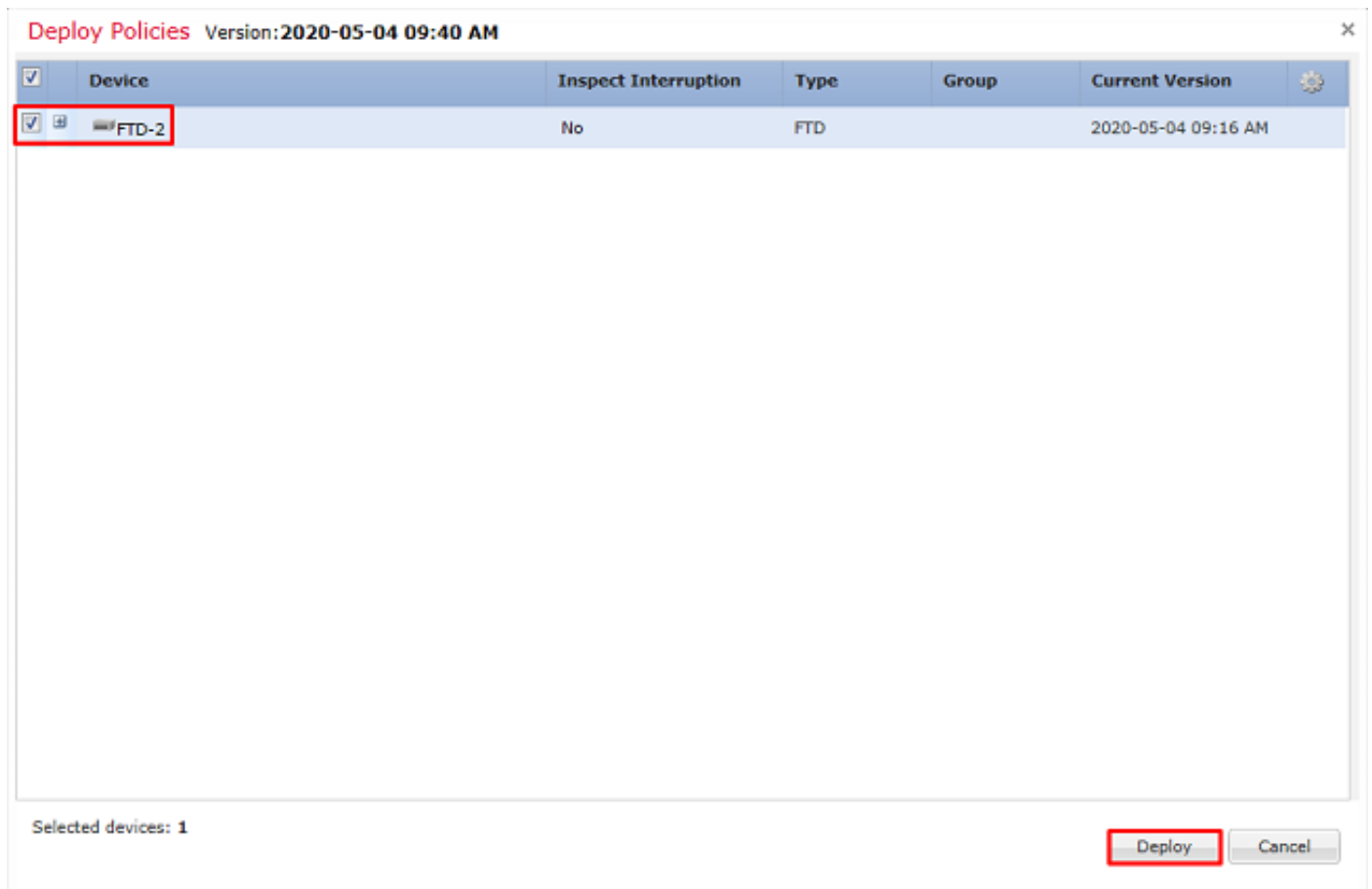
Displaying 1-2 of 2 rows Page 1 of 1 Rows per page: 100

رشنال

1. رشن قوف رقنا، نيوكتال اءاتنا دنع.

Deploy System Help admin

2. قوف رقنا مٲ اهيلع نيوكتال قيبطت مٲي شيح FTD ل ةرواجمل رايتخالال ةناخ قوف رقنا رشن.



ةحصل ال نم ققحت ال

يئاهن ال بيترت ال

نيوكت AAA

```
> show running-configuration aaa-server
aaa-server LAB-AD protocol ldap
max-failed-attempts 4
realm-id 5
aaa-server LAB-AD host win2016.example.com
server-port 389
ldap-base-dn DC=example,DC=com
ldap-group-base-dn DC=example,DC=com
ldap-scope subtree
ldap-naming-attribute samaccountname
ldap-login-password *****
ldap-login-dn ftd.admin@example.com
server-type microsoft
```

نيوكت AnyConnect

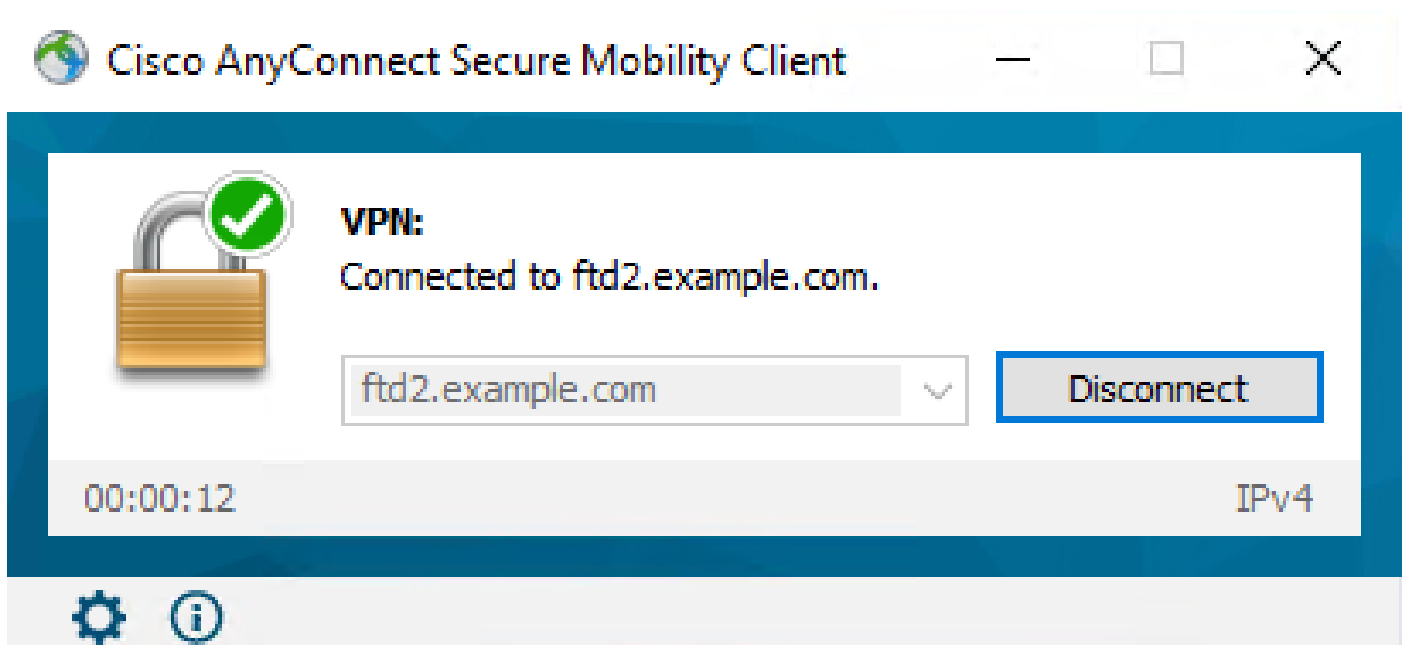
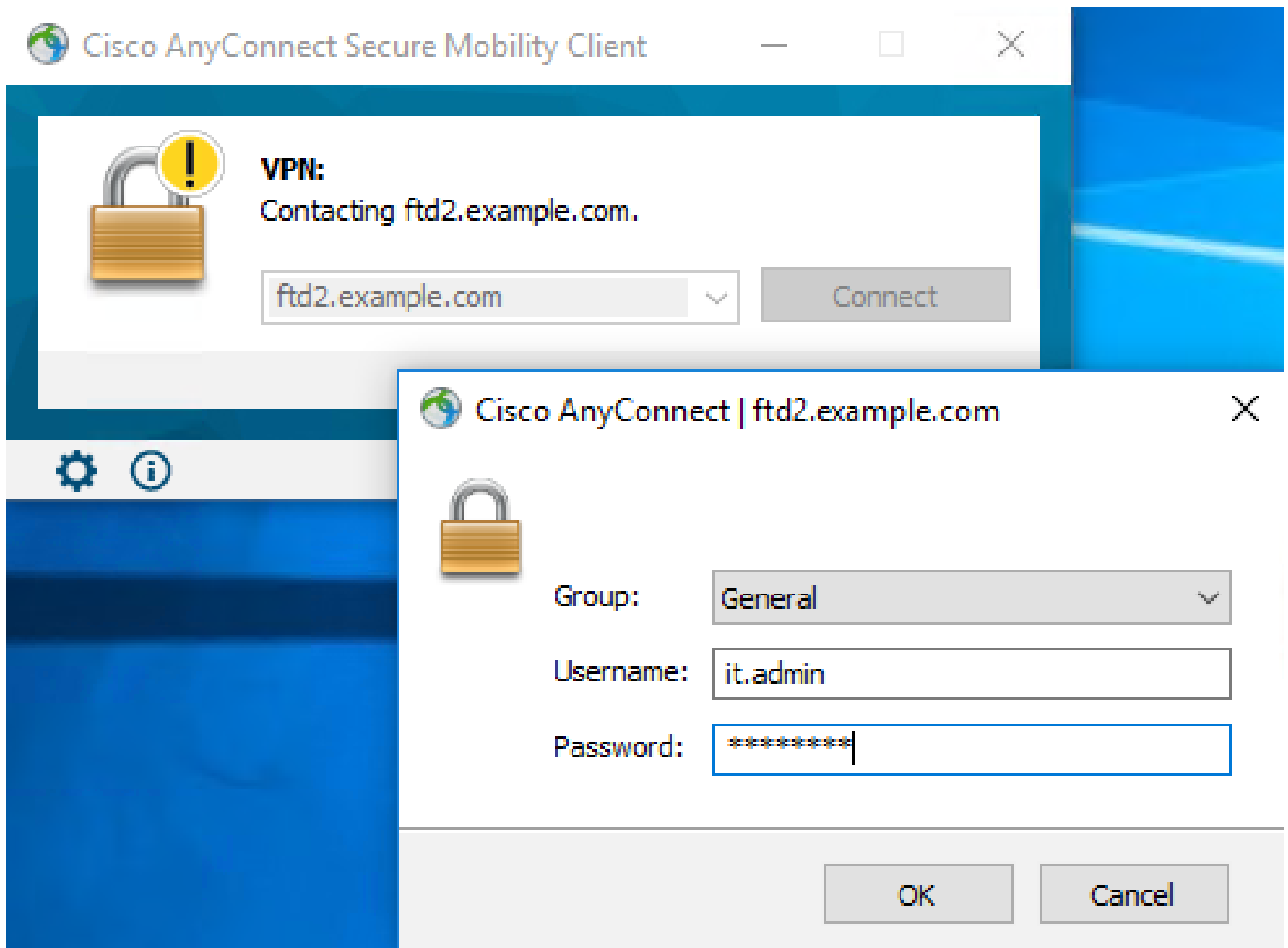
```
> show running-config webvpn
webvpn
  enable Outside
  anyconnect image disk0:/csm/anyconnect-linux64-4.7.03052-webdeploy-k9.pkg 1 regex "Linux"
  anyconnect image disk0:/csm/anyconnect-win-4.7.00136-webdeploy-k9.pkg 2 regex "Windows"
  anyconnect profiles Lab disk0:/csm/lab.xml
  anyconnect enable
  tunnel-group-list enable
  cache
    no disable
  error-recovery disable

> show running-config tunnel-group
tunnel-group General type remote-access
tunnel-group General general-attributes
  address-pool AnyConnect-Pool
  authentication-server-group LAB-AD
tunnel-group General webvpn-attributes
  group-alias General enable

> show running-config group-policy
group-policy DfltGrpPolicy attributes
  vpn-simultaneous-logins 10
  vpn-tunnel-protocol ikev2 ssl-client
  split-tunnel-policy tunnelspecified
  split-tunnel-network-list value Lab
  user-authentication-idle-timeout none
webvpn
  anyconnect keep-installer none
  anyconnect modules value dart
  anyconnect ask none default anyconnect
  http-comp none
  activex-relay disable
  file-entry disable
  file-browsing disable
  url-entry disable
  deny-message none
  anyconnect ssl df-bit-ignore enable

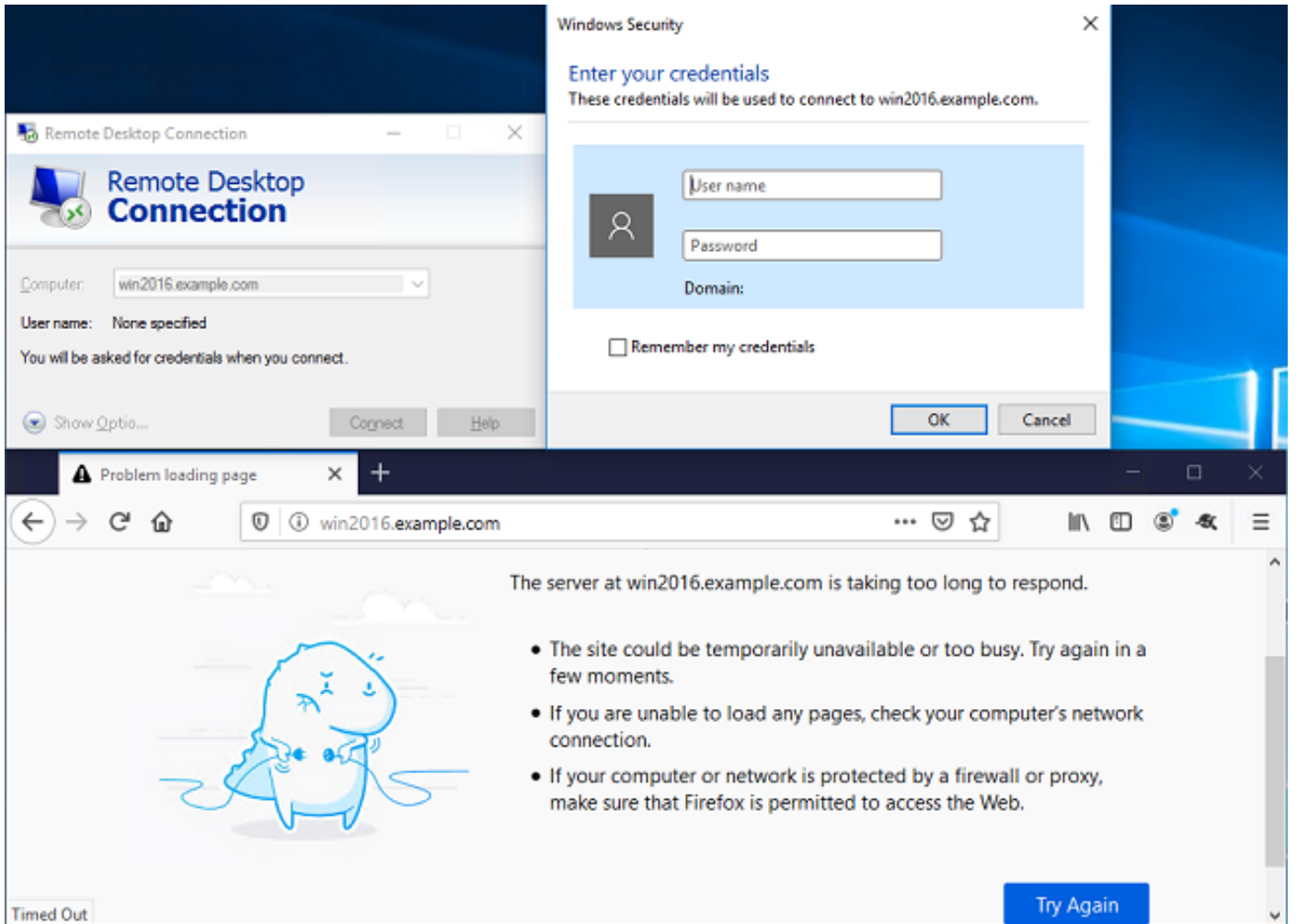
> show running-config ssl
ssl trust-point FTD-2-SelfSigned outside
```

اهنم ققحتلالو AnyConnect نم لوصولا يف مكحتلالا ةسايس دعاوقب لاصتالا

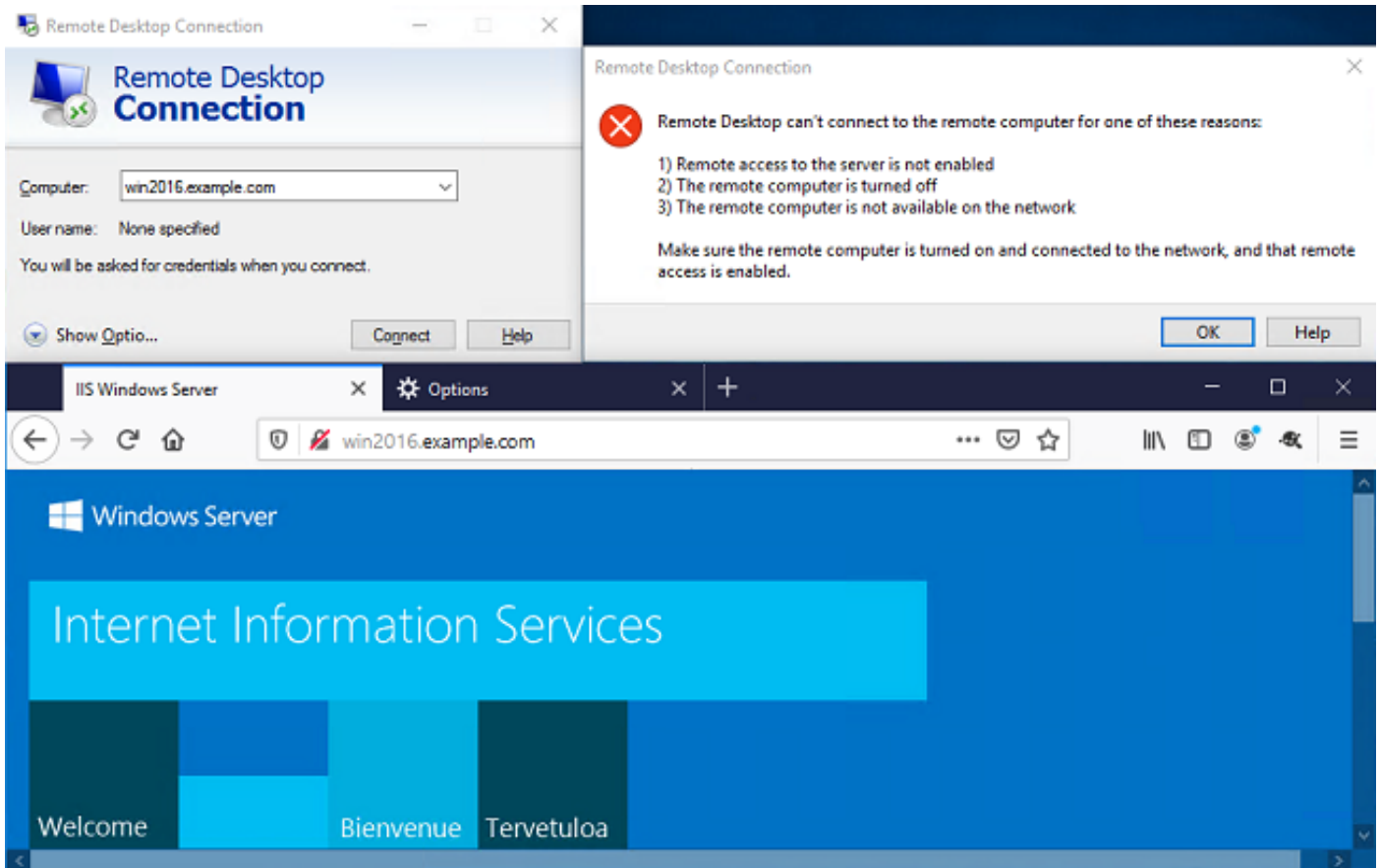


مداخل إلى RDP لوصول واهي دل يتال AnyConnect Admins ةومجمل ي ف دوجوم User IT Admin
Windows. HTTP. إلى لوصول ق هيدل سيل، كلذ عم و.

إلى لوصول هنكمي مدختسمل اذه نأ نم ققحتي مداخل اذهل Firefox و RDP لم ةسلج حتف نإ
طوق RDP ربع مداخل.



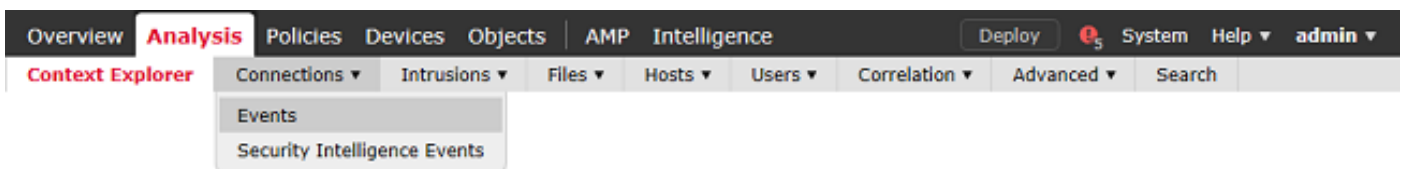
ة وومج م ي ف دوچوم ل ا "مدختسم ل ا راب تخ ا مدختسم" مادختساب ل وخذل ا ل ي ج ست ة ل ا ح ي ف ققحتل ا كنكم ي ، RDP ل ا س ي ل و HTTP ل ا ل وصولا مهنكم ي ن ي ذل ا AnyConnect ي مدختسم ل و ع ف م ل ا ة ي راس ت ح ب ص ا ل وصولا ي ف م ك ح ت ل ا ج ه ن د ع ا و ق ن ا ن م .



FMC لاصتا اداخا مادختساب ققحتال

اداخا نم ققحتال نكمي، لوصولاب مكحتال سايس دعاوق يي ليچستال نيكم تل ارظنو دعاوقال هذه قباطت رورم ةكرح يال لاصتال.

Analysis (ليحتال) > Connections > Events.



لوؤسمل لاصتال اداخا ضرعل تالچسالا ةيفصت متت، لاصتال اداخال لودجال ضرع تحت طقف تامولعملال ةينقت.

رسي، امهم، (TCP و UDP 3389) مداخلال لىل RDP رورم ةكرح حمسي نأ تققد عيطتسي تنأ، انه تنعم نوكي رورم ةكرح 80.

Action	Initiator IP	Initiator User	Responder IP	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code
Allow	10.10.10.1	it_admin (LAB-AD\it_admin, LDAP)	192.168.1.1	outside-zone	inside-zone	62473 / tcp	3389 / tcp
Block	10.10.10.1	it_admin (LAB-AD\it_admin, LDAP)	192.168.1.1	outside-zone	inside-zone	62474 / tcp	80 (http) / tcp
Block	10.10.10.1	it_admin (LAB-AD\it_admin, LDAP)	192.168.1.1	outside-zone	inside-zone	62475 / tcp	80 (http) / tcp
Block	10.10.10.1	it_admin (LAB-AD\it_admin, LDAP)	192.168.1.1	outside-zone	inside-zone	62476 / tcp	80 (http) / tcp

مدخال الى RDP رورم ة كرح رطح نم ققحت ال كنكمي ،مدخت سمل رابتخ |مدخت سمل ة بس نلاب 80 ذفنم ال رورم ة كرح ب حامس ل او

Action	Initiator IP	Initiator User	Responder IP	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code
Block	10.10.10.1	test user (LAB-AD\test.user, LDAP)	192.168.1.1	outside-zone	inside-zone	62493 / tcp	3389 / tcp
Allow	10.10.10.1	test user (LAB-AD\test.user, LDAP)	192.168.1.1	outside-zone	inside-zone	62494 / tcp	80 (http) / tcp

اه حال ص او ا ط خ ال فاش ك ت سا

ا ط خ ال ح ي ح ص ت

LDAP ة ق د اص م ا ط خ ا فاش ك ت س ال ي ص ي خ ش ت CLI ي ف ا ذه ا ط خ ال ح ي ح ص ت ل ي غ ش ت ن ك م ي ا ه حال ص او : debug ldap 255.

ل ي غ ش ت ن ك م ي ، ا ه حال ص او م د خ ت س م ل ا ة ي و ه ل ل و ص و ل ا ي ف م ك ح ت ل ا ة س ا ي س ا ط خ ا فاش ك ت س ال رورم ال ة ك رح ب حامس ل ب بس د ي ح ت ل م ك ح ت ل ا ة م ئ ا ق ي ف م ا ط ن ل ا م ع د ة ي ا م ح ر ا د ج ا ط خ ا ح ي ح ص ت ع ق و ت م ر ي غ ل ك ش ب ا ه ع ن م و ا

ة ل م ا ع ال LDAP ا ط خ ا ح ي ح ص ت

```
[53] Session Start
[53] New request Session, context 0x00002b1d13f4bbf0, reqType = Authentication
[53] Fiber started
[53] Creating LDAP context with uri=ldap://192.168.1.1:389
[53] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[53] supportedLDAPVersion: value = 3
[53] supportedLDAPVersion: value = 2
[53] LDAP server 192.168.1.1 is Active directory
[53] Binding as ftd.admin@example.com
```



```
[53] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[53] LDAP Search:
      Base DN = [DC=example,DC=com]
      Filter  = [sAMAccountName=it.admin]
      Scope   = [SUBTREE]
[53] User DN = [CN=IT Admin,CN=Users,DC=example,DC=com]
[53] Talking to Active Directory server 192.168.1.1
[53] Reading password policy for it.admin, dn:CN=IT Admin,CN=Users,DC=example,DC=com
[53] Read bad password count 6
[53] Binding as it.admin
[53] Performing Simple authentication for it.admin to 192.168.1.1
[53] Processing LDAP response for user it.admin
[53] Message (it.admin):
[53] Authentication successful for it.admin to 192.168.1.1
[53] Retrieved User Attributes:
[53]   objectClass: value = top
[53]   objectClass: value = person
[53]   objectClass: value = organizationalPerson
[53]   objectClass: value = user
[53]   cn: value = IT Admin
[53]   sn: value = Admin
[53]   givenName: value = IT
[53]   distinguishedName: value = CN=IT Admin,CN=Users,DC=example,DC=com
[53]   instanceType: value = 4
[53]   whenCreated: value = 20200421025811.0Z
[53]   whenChanged: value = 20200421204622.0Z
[53]   displayName: value = IT Admin
[53]   uSNCreated: value = 25896
[53]   memberOf: value = CN=AnyConnect Admins,CN=Users,DC=example,DC=com
[53]   uSNChanged: value = 26119
[53]   name: value = IT Admin
[53]   objectGUID: value = &...J..0..2w...c
[53]   userAccountControl: value = 512
[53]   badPwdCount: value = 6
[53]   codePage: value = 0
[53]   countryCode: value = 0
[53]   badPasswordTime: value = 132320354378176394
[53]   lastLogoff: value = 0
[53]   lastLogon: value = 0
[53]   pwdLastSet: value = 132319114917186142
[53]   primaryGroupID: value = 513
[53]   objectSid: value = .....{I...;.....}j...
[53]   accountExpires: value = 9223372036854775807
[53]   logonCount: value = 0
[53]   sAMAccountName: value = it.admin
[53]   sAMAccountType: value = 805306368
[53]   userPrincipalName: value = it.admin@example.com
[53]   objectCategory: value = CN=Person,CN=Schema,CN=Configuration,DC=example,DC=com
[53]   dSCorePropagationData: value = 16010101000000.0Z
[53]   lastLogonTimestamp: value = 132319755825875876
[53] Fiber exit Tx=515 bytes Rx=2659 bytes, status=1
[53] Session End
```

LDAP مداخل لاصتا عاشن | رذعت

<#root>

[-2147483611] Session Start

```
[-2147483611] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483611] Fiber started
[-2147483611] Creating LDAP context with uri=ldap://171.16.1.1:389
[-2147483611]
```

Connect to LDAP server: ldap://172.16.1.1:389, status = Failed

```
[-2147483611] Unable to read rootDSE. Can't contact LDAP server.
[-2147483611] Fiber exit Tx=0 bytes Rx=0 bytes, status=-2
[-2147483611] Session End
```

قمة محتوم لولول:

- LDAP مداخل نم ةباجتسإ ىقلى تي FTD نأ نم دكأت و هيجوتل نم ققحت
- اه ب قووم ةحيجصلل رذل ال CA ةداهش نأ نم دكأت ، STARTTLS و LDAP مادختسإ ةلاحي في
- حاجنب SSL ةحفاصم لامكإ نكمي شيحي
- نم ققحت في ، فيضم ال مسامادختسإ مت اذا . جحص ءانيمو ناونع ال لمعتسي نأ تققد
- جحص ال IP ناونع ال هلى حلى لى DNS ةردق

ةححص ريغ رورم ال ةملك و/و DN في طبرل لاجس

<#root>

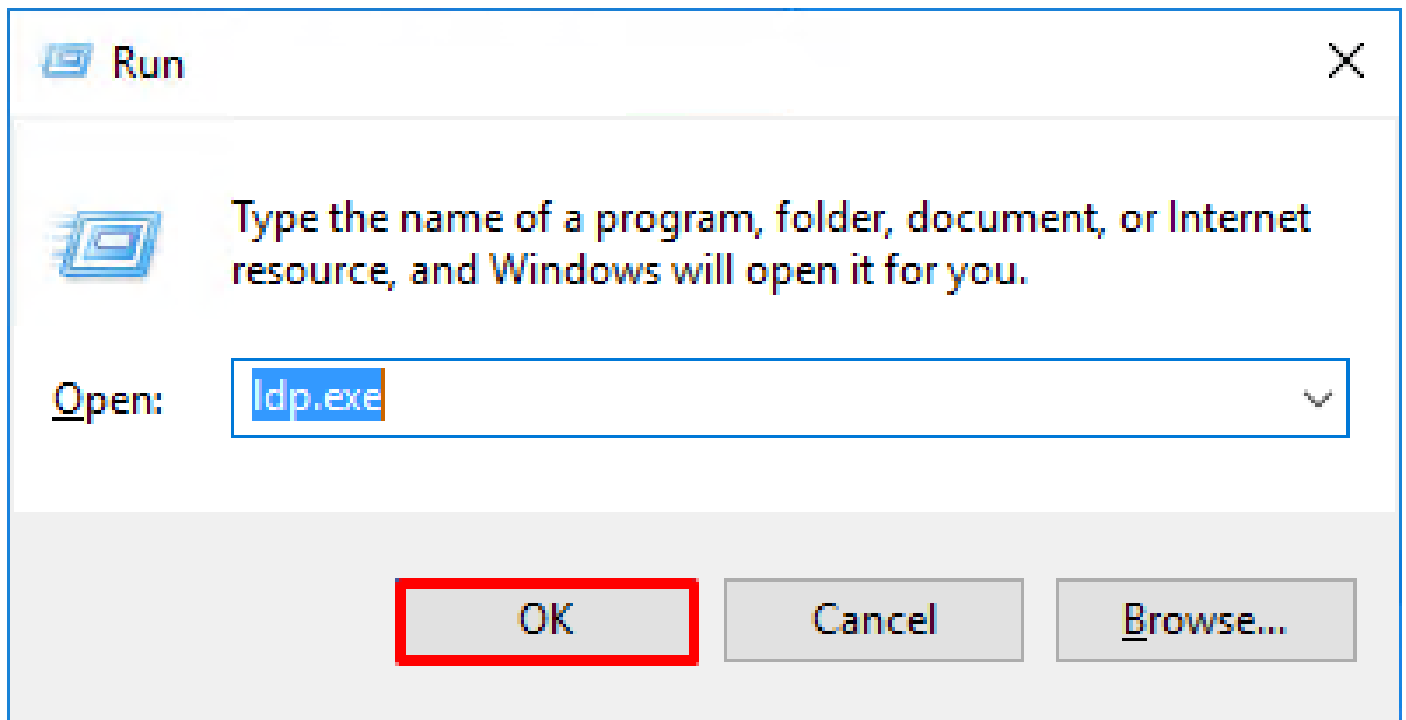
```
[-2147483615] Session Start
[-2147483615] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483615] Fiber started
[-2147483615] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483615] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483615] defaultNamingContext: value = DC=example,DC=com
[-2147483615] supportedLDAPVersion: value = 3
[-2147483615] supportedLDAPVersion: value = 2
[-2147483615] LDAP server 192.168.1.1 is Active directory
[-2147483615] supportedSASLMechanisms: value = GSSAPI
[-2147483615] supportedSASLMechanisms: value = GSS-SPNEGO
[-2147483615] supportedSASLMechanisms: value = EXTERNAL
[-2147483615] supportedSASLMechanisms: value = DIGEST-MD5
[-2147483615] Binding as ftd.admin@example.com
[-2147483615] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[-2147483615] Simple authentication for ftd.admin@example.com returned code (49) Invalid credentials
[-2147483615]
```

Failed to bind as administrator returned code (-1) Can't contact LDAP server

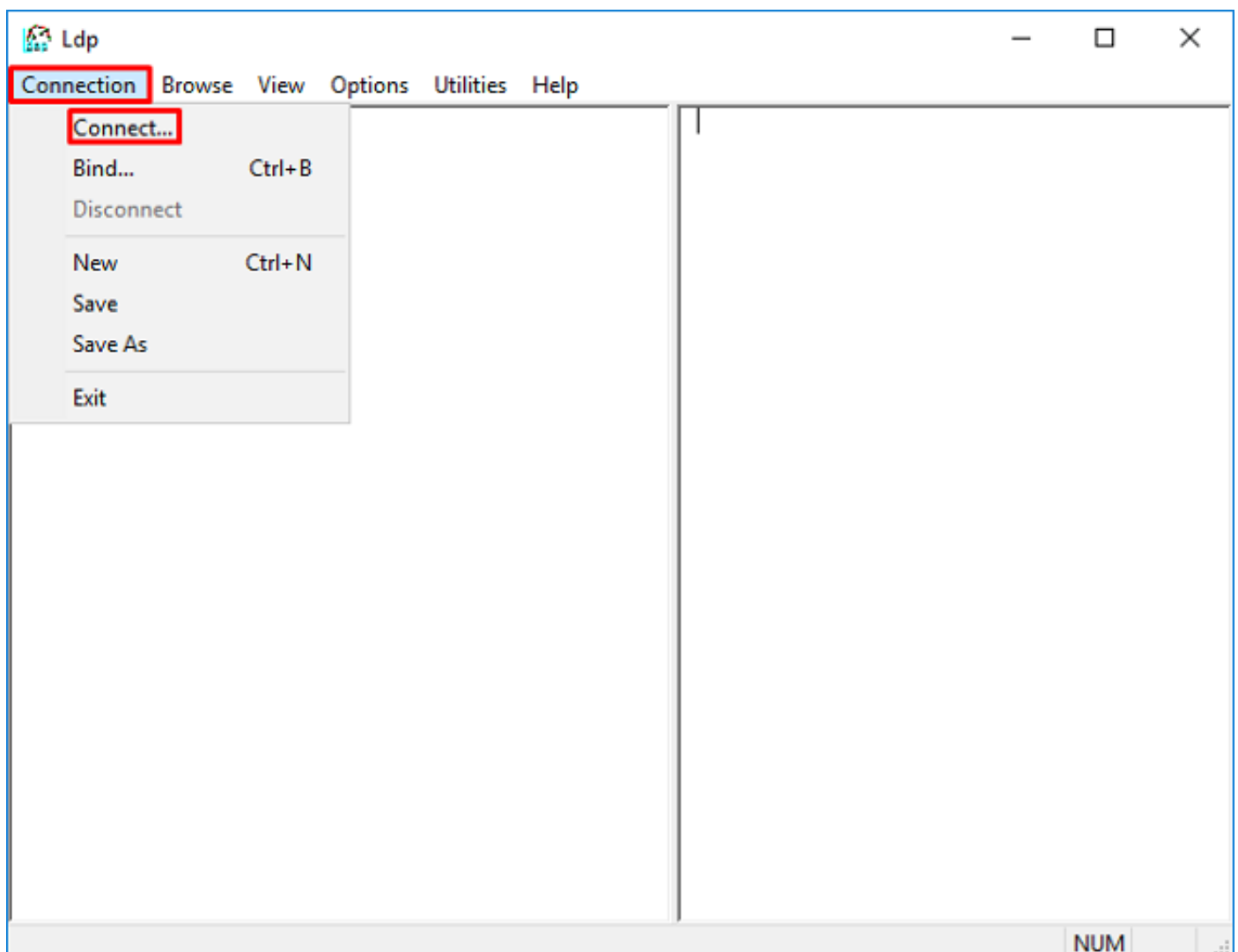
```
[-2147483615] Fiber exit Tx=186 bytes Rx=744 bytes, status=-2
[-2147483615] Session End
```

لكشب لوخدل ليجست و DN لى لوخدل ليجست رورم ةملك نيوكت نم ققحت :لم محتوم لولول
ةينام نم ققحت لل ldp.exe مادختساب AD مداخل لى ءارجإ اذه نم ققحتل نكمي . جحص
ةيلال تاوطل ال عبتا ، LDP مادختساب حاجنب باسح طبر :

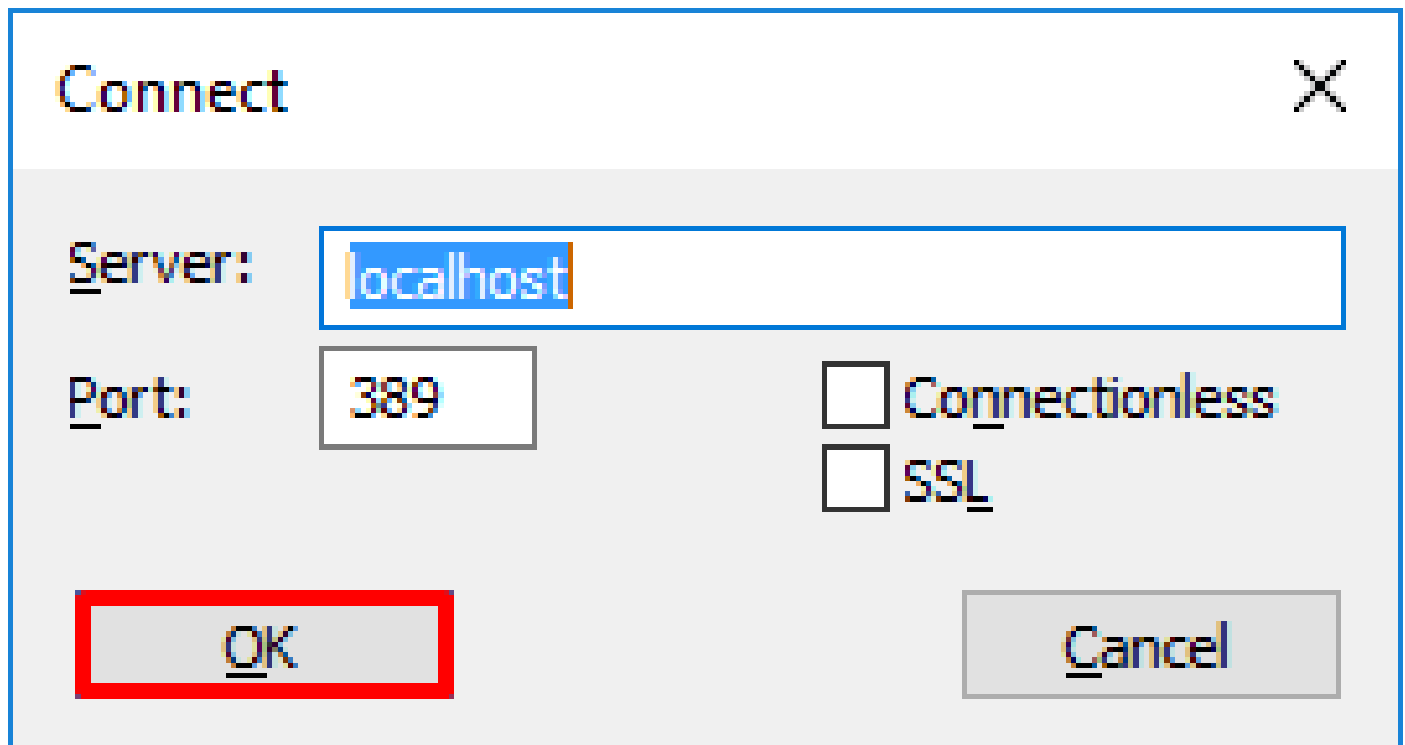
1. AD مداخل لى لdp.exe نع شحل و Win+R لى طغضا .



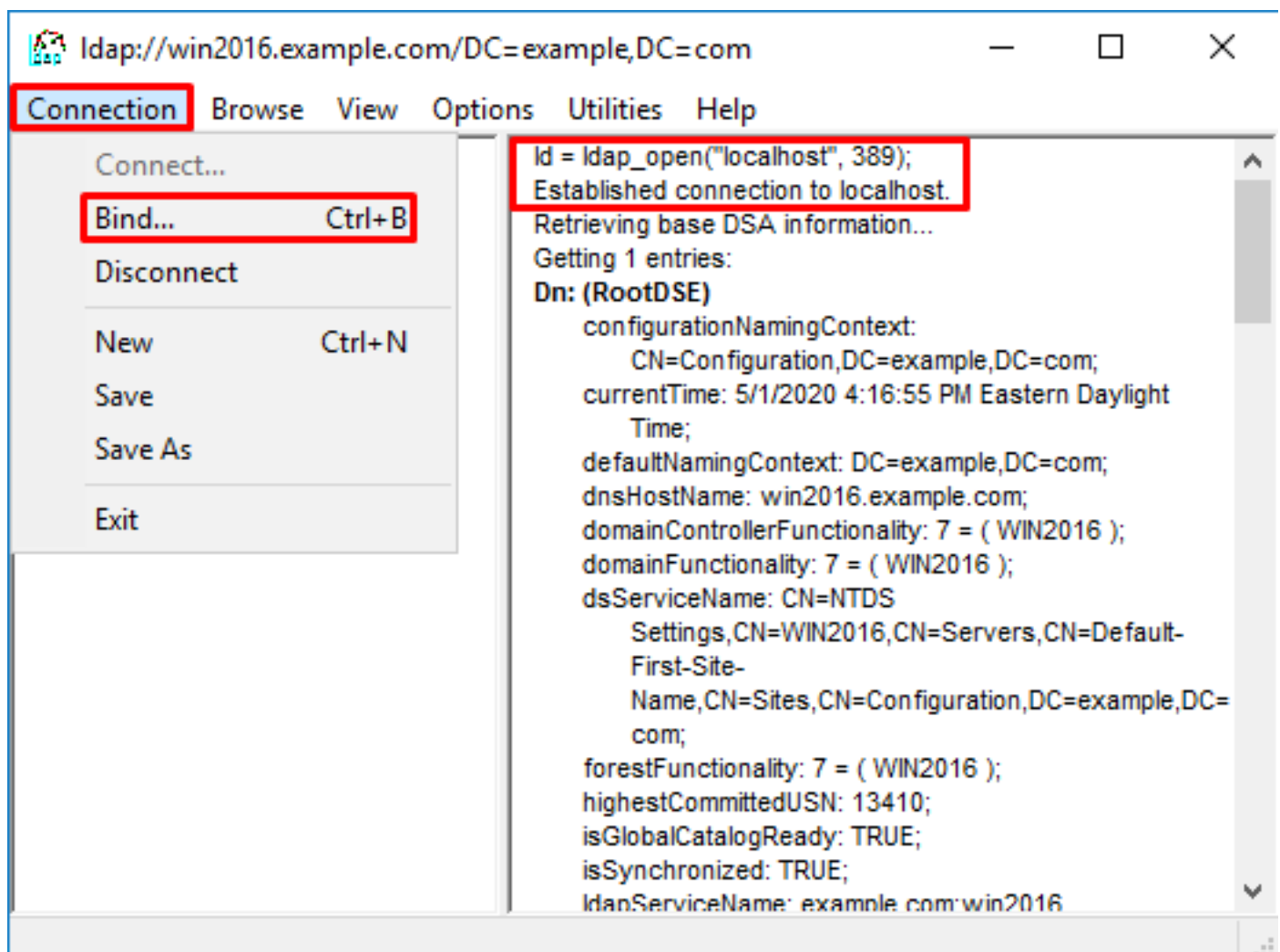
2. Connect ددج، لاصتالال تحت.



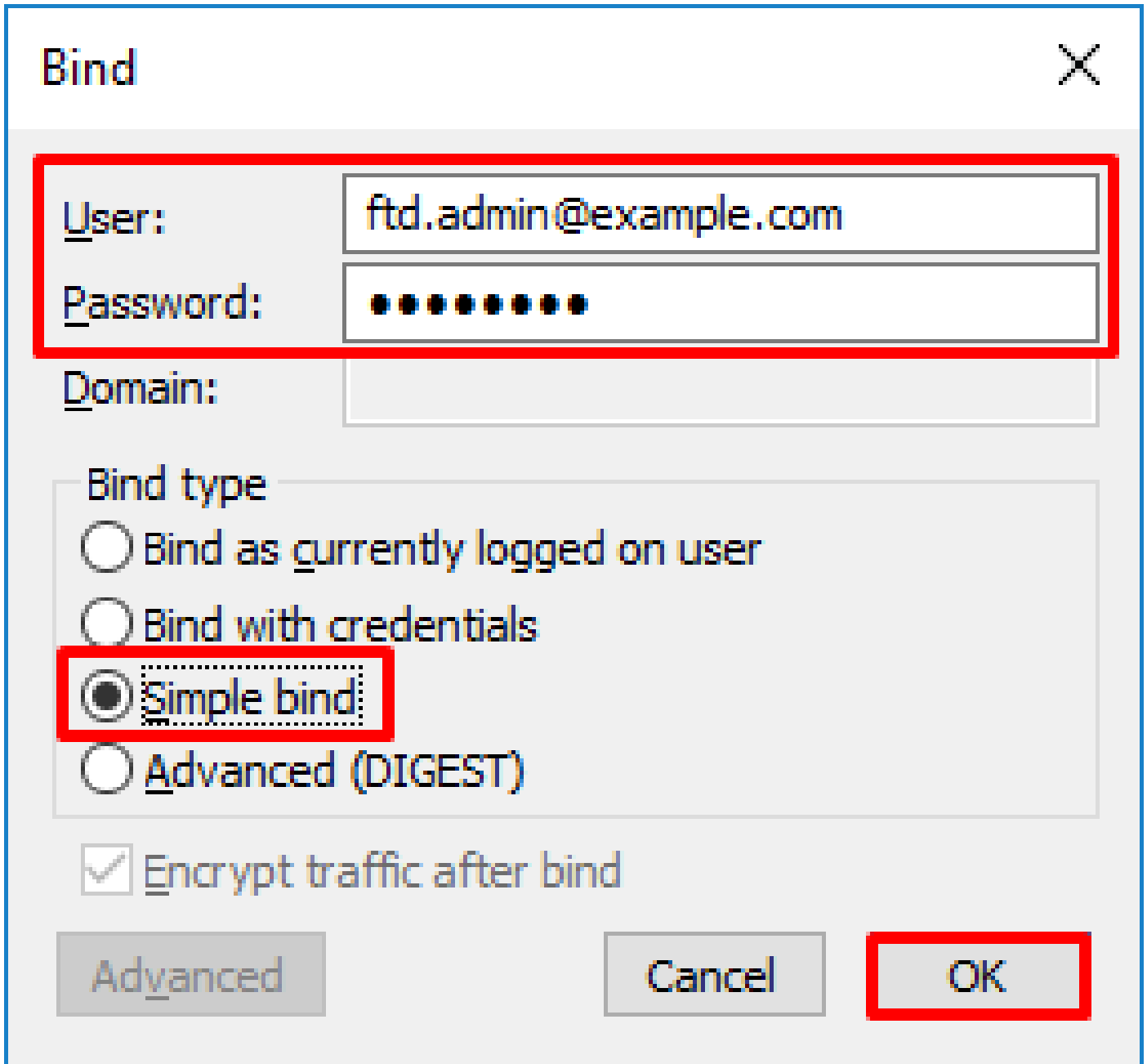
3. قفاوم قوف رقنا مٲ بسانملا ذفنملاو مداخلل يلحم فيضم ددح.



4. طبر > لاصتا ىل لقتنا. حجنا لاصتا ىل ريشي اصن نميال دومعلا رهظي.



5. OK قوف رقناو. رورملا ةملاك و ليلدلا باسح مدختسم ددح م ث طيسب طبر ددح.



Bind [X]

User: ftd.admin@example.com

Password: ●●●●●●●●

Domain:

Bind type

Bind as currently logged on user

Bind with credentials

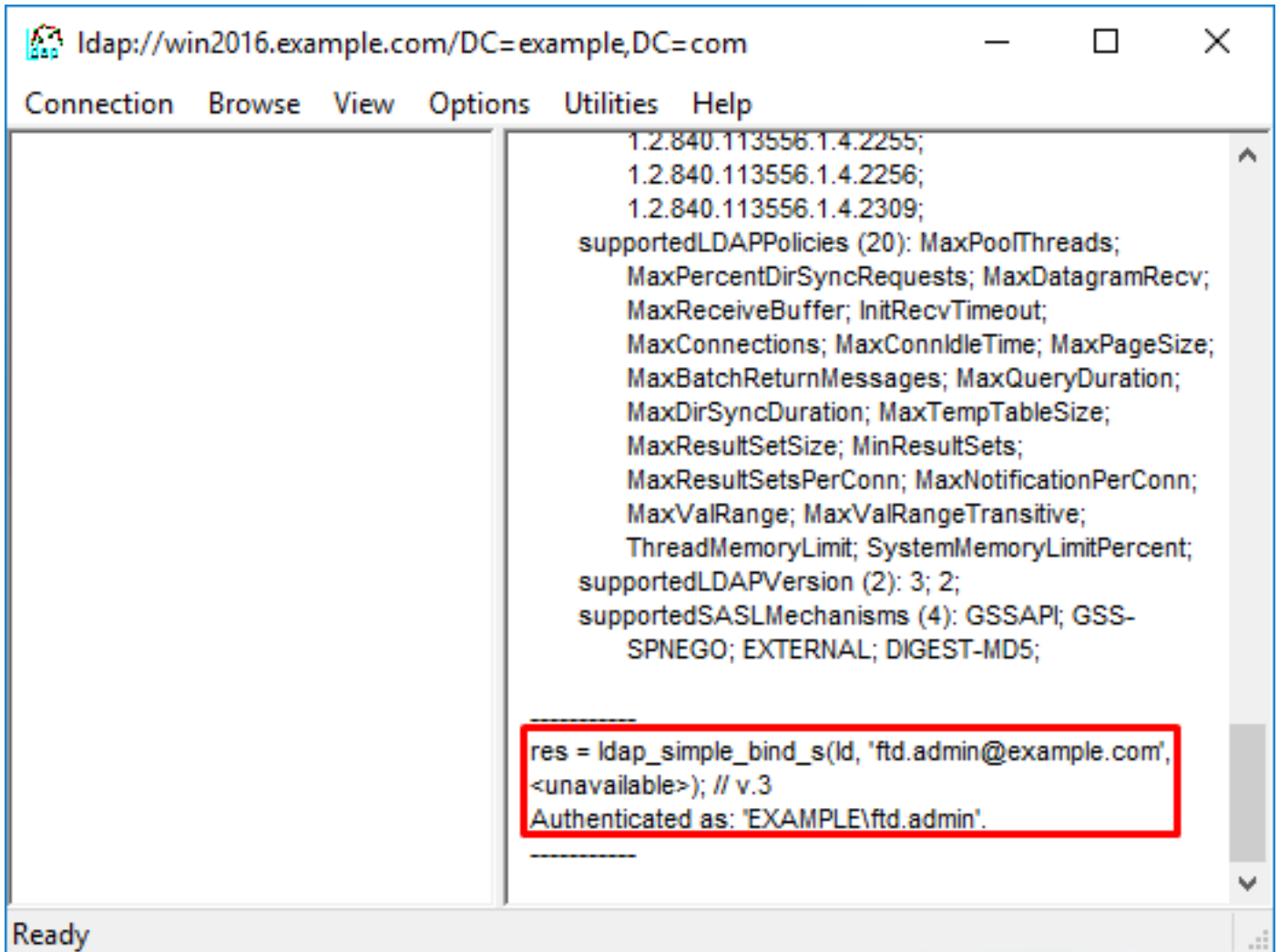
Simple bind

Advanced (DIGEST)

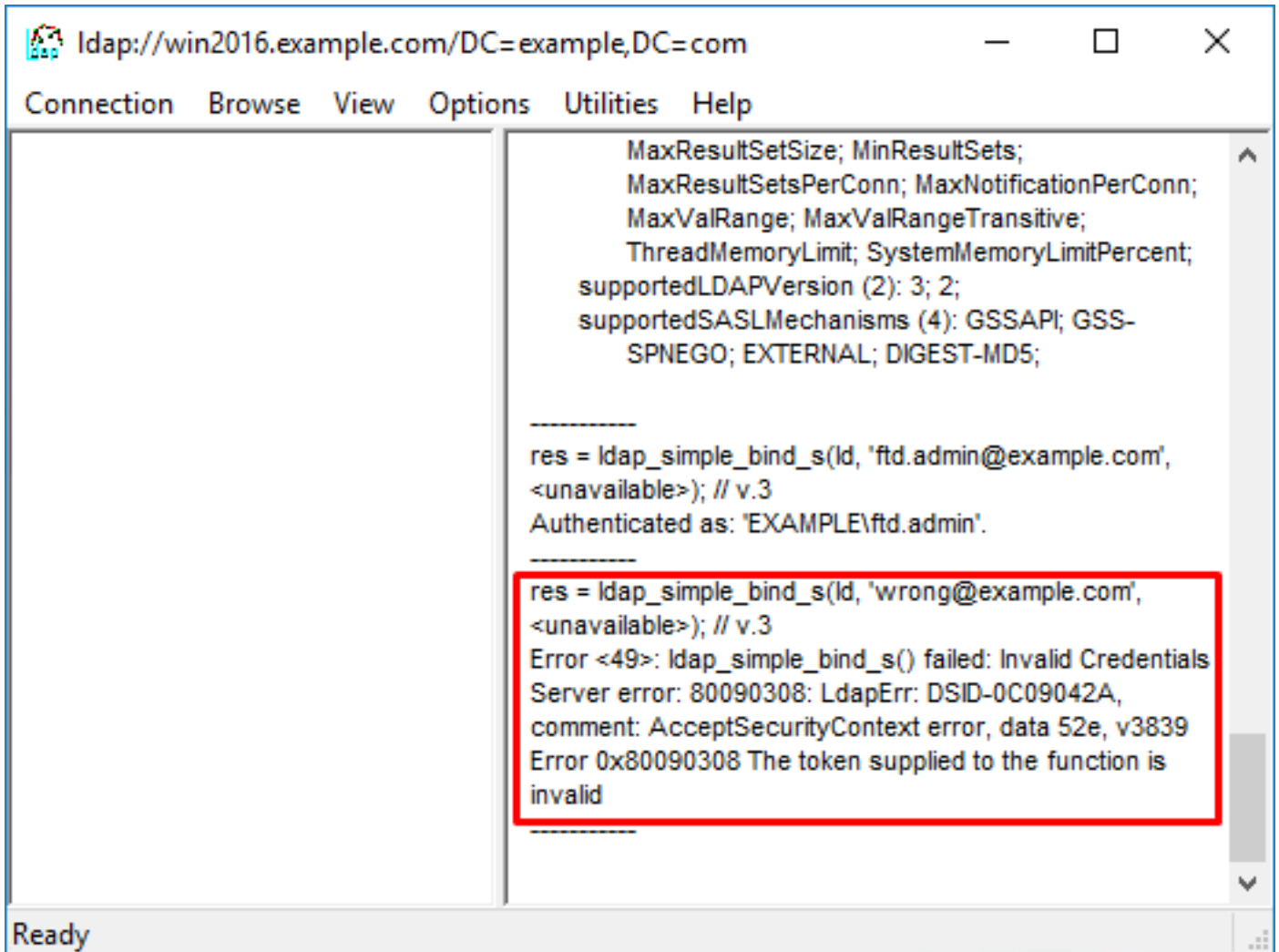
Encrypt traffic after bind

Advanced Cancel **OK**

DOMAIN\username : ك قدصم LDP رهظي ،حجان طبر مادختساب



لثم لشف ةححص ريغ رورم ةملك وأحل اص ريغ مدختسم مساب طبرلا ةلواحم نع جتني
انه امهارة نيدللا نينثاللا



مدخست مسال مسال روئع ال LDAP مداخ ال رذعت

<#root>

```
[-2147483612] Session Start
[-2147483612] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483612] Fiber started
[-2147483612] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483612] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483612] supportedLDAPVersion: value = 3
[-2147483612] supportedLDAPVersion: value = 2
[-2147483612] LDAP server 192.168.1.1 is Active directory
[-2147483612] Binding as ftd.admin@example.com
[-2147483612] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[-2147483612] LDAP Search:
    Base DN = [dc=example,dc=com]
    Filter = [samaccountname=it.admi]
    Scope = [SUBTREE]
[-2147483612]

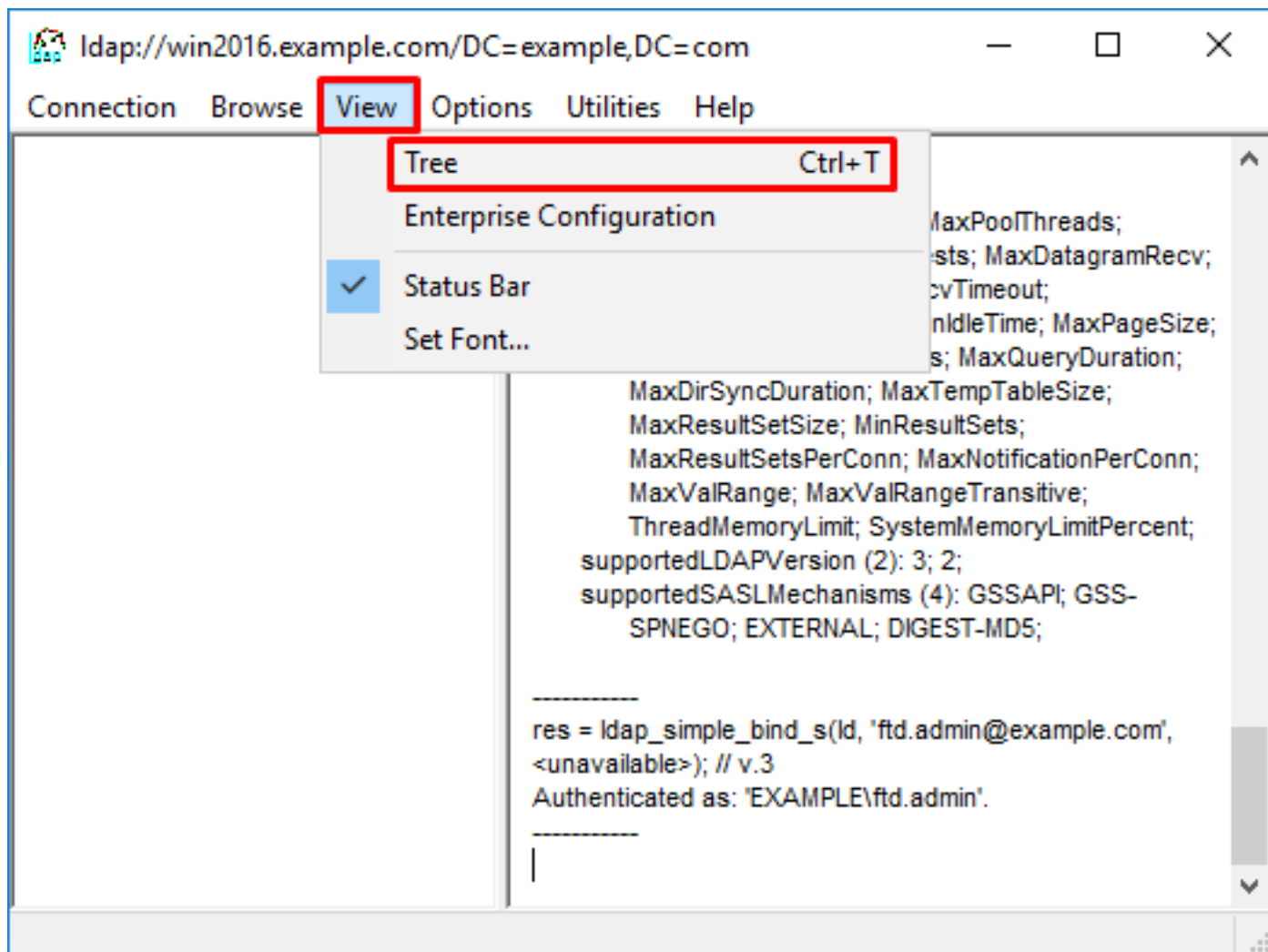
Search result parsing returned failure status

[-2147483612] Talking to Active Directory server 192.168.1.1
[-2147483612] Reading password policy for it.admi, dn:
[-2147483612] Binding as ftd.admin@example.com
[-2147483612] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
```

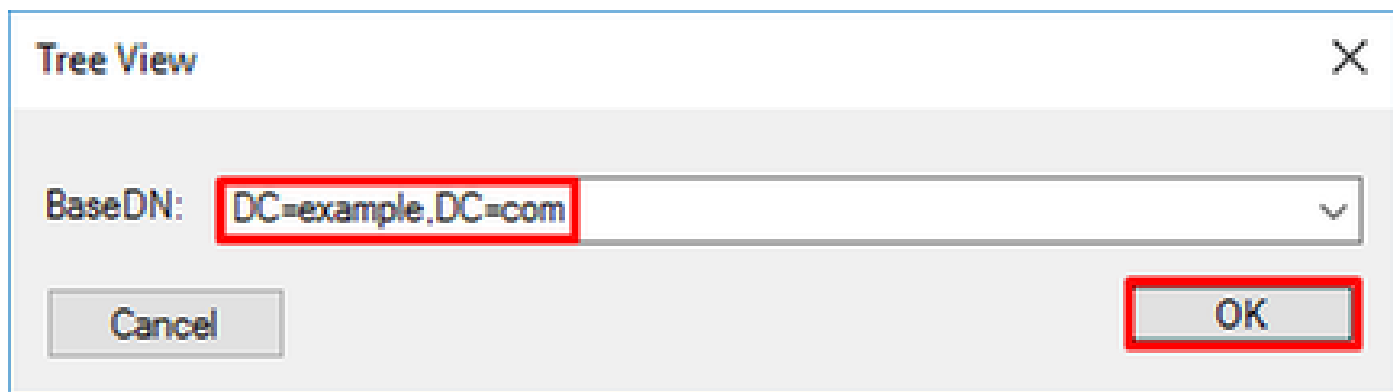
[-2147483612] Fiber exit Tx=456 bytes Rx=1082 bytes, status=-1
[-2147483612] Session End

ةطساوب مت يذلا ثحبلا عم مدختسملا ىلع روثلعل هنكمي AD نأ نم ققحت :لمتحملا لجل
اض ي ldp.exe عم اذه متي نأ نكمملا نمو .FTD.

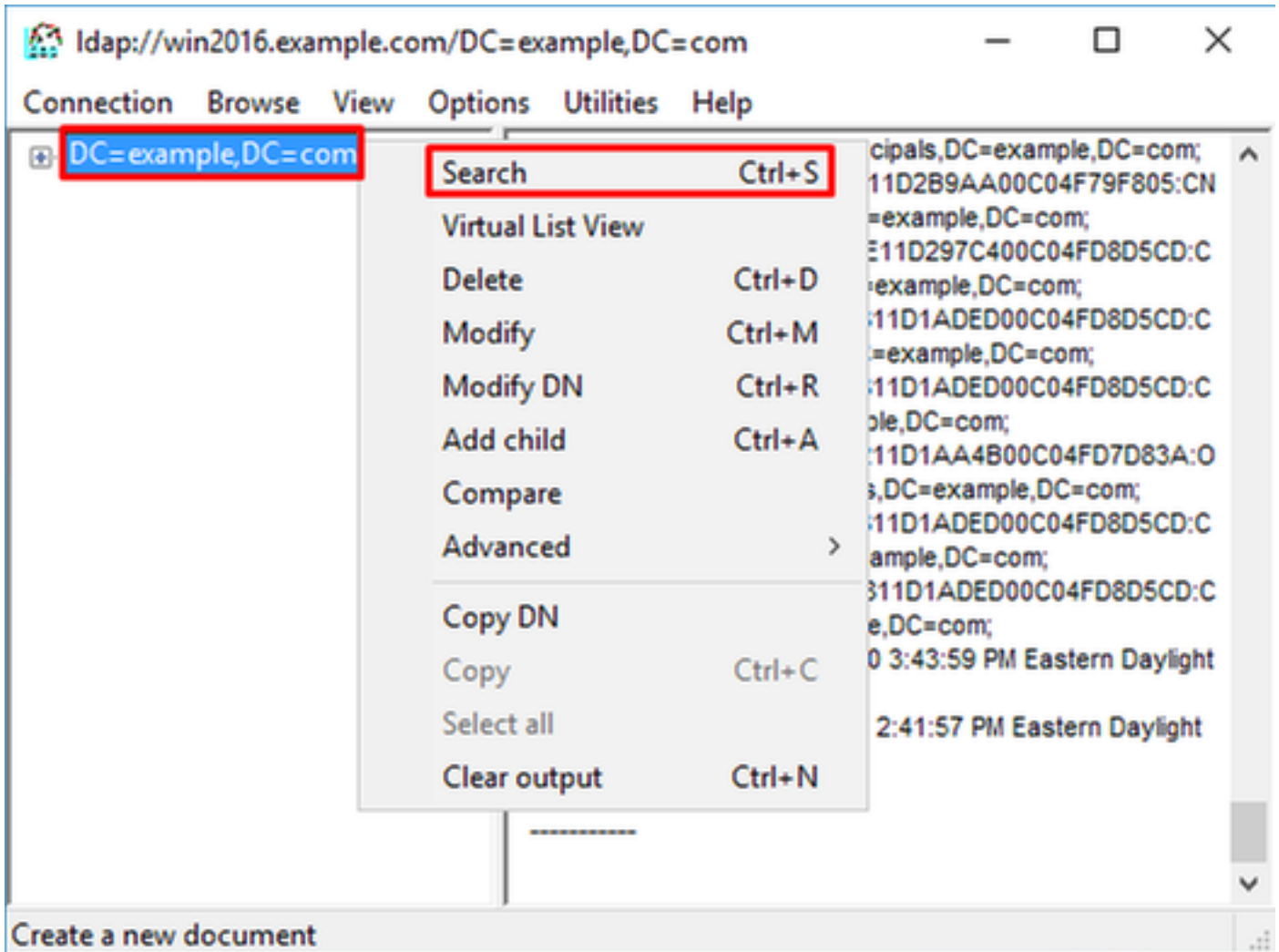
1. ةرغش > ضرع ىلإ لقتنا ،هالعلأ حضوم وه امك حاجنب طبرلا دع ب .



2. قفاوم قوف رقنا مٲ FTD ىلع هن يوكت مت يذلا يساسأل DN ددح .



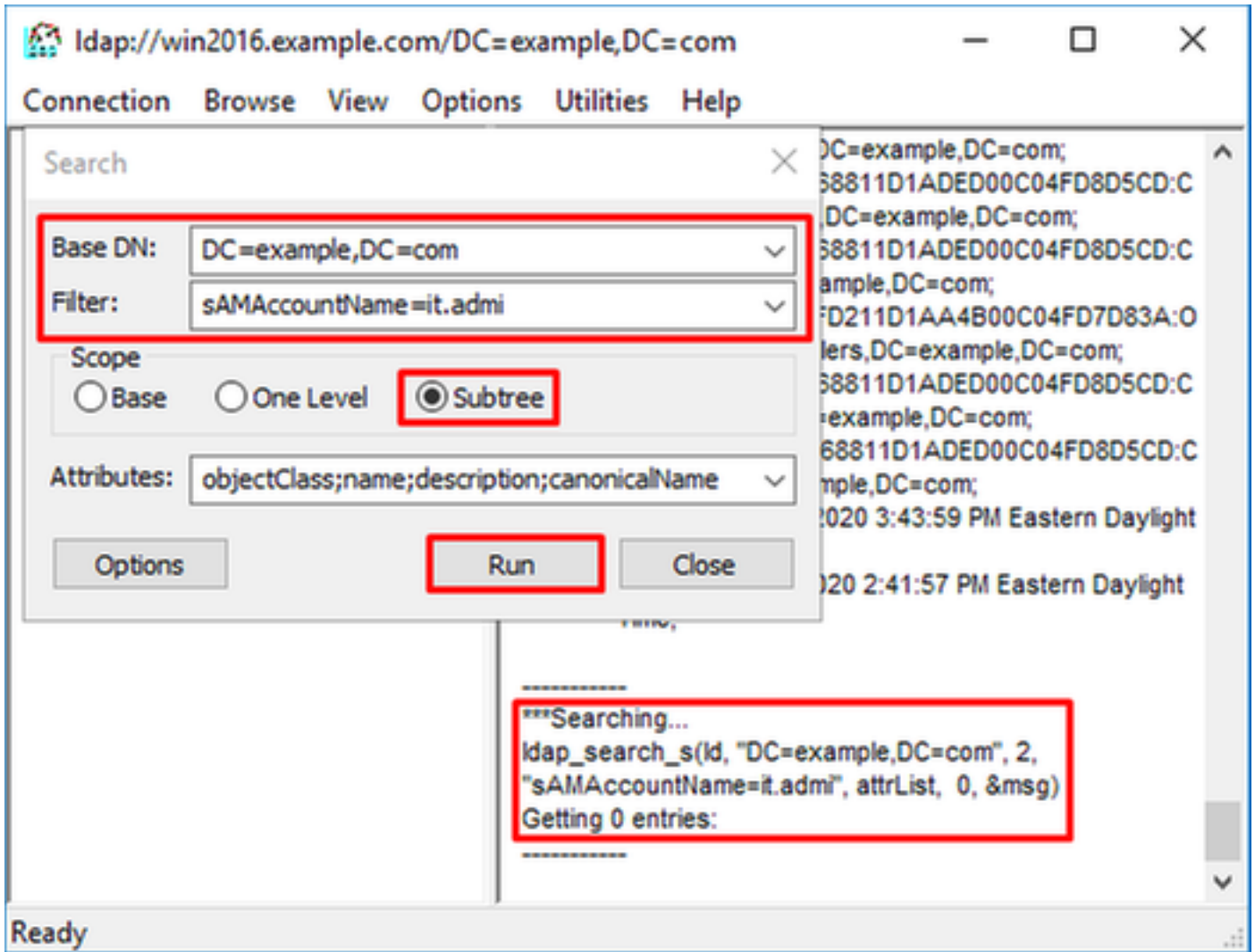
3. ثحب قوف رقنا مٲ يساسأل DN قوف نم يأل سواملا رزب رقنا .



4. إعطاء ألقاب خاصة في فروع مختلفة من نطاق، و Filter، و Scope، أساس الـ DN مرقوم في صفحة 4.

هذه، لثمة الأذى في:

- أساس الـ DN مرقوم: `dc=example.dc=com`
- أساس الـ Filter: `samaccountname=it.admi`
- أساس الـ Scope: `ou=example.com`



لفسأ SAMAccountName it.admi عم مدختسم باسح دوجو مدعل ارطن تالادخا 0 نع LDP شحبى
 DN=example,dc=com.

لادخا 0 نع LDP شحبى. ةفلتخم ةجيتن ححص ل SAMAccountName it.admin عم ىرخأ ةلواجم رهظت
 مدختسم ل ل DN=example, dc=com عبطىو ىساسأل DN=example, dc=com تحت دحاو.

LDAP Search Configuration:

- Base DN: DC=example,DC=com
- Filter: sAMAccountName=it.admin
- Scope: Subtree
- Attributes: objectClass;name;description;canonicalName

Search Results:

```

***Searching...
ldap_search_s(ld, "DC=example,DC=com", 2,
"sAMAccountName=it.admin", attrList, 0, &msg)
Getting 1 entries:
Dn: CN=IT Admin,CN=Users,DC=example,DC=com
   canonicalName: example.com/Users/IT Admin;
   name: IT Admin;
   objectClass (4): top; person; organizationalPerson;
   user;

```

مدخست مسال ةححص ريغ رورمال ةملك

<#root>

```

[-2147483613] Session Start
[-2147483613] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483613] Fiber started
[-2147483613] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483613] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483613] supportedLDAPVersion: value = 3
[-2147483613] supportedLDAPVersion: value = 2
[-2147483613] LDAP server 192.168.1.1 is Active directory
[-2147483613] Binding as ftd.admin@example.com
[-2147483613] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[-2147483613] LDAP Search:
      Base DN = [dc=example,dc=com]
      Filter  = [samaccountname=it.admin]
      Scope   = [SUBTREE]
[-2147483613] User DN = [CN=IT Admin,CN=Users,DC=example,DC=com]
[-2147483613] Talking to Active Directory server 192.168.1.1

```

```
[-2147483613] Reading password policy for it.admin, dn:CN=IT Admin,CN=Users,DC=example,DC=com
[-2147483613] Read bad password count 0
[-2147483613] Binding as it.admin
[-2147483613] Performing Simple authentication for it.admin to 192.168.1.1
[-2147483613]
```

Simple authentication for it.admin returned code (49) Invalid credentials

```
[-2147483613] Message (it.admin): 80090308: LdapErr: DSID-0C09042A, comment: AcceptSecurityContext error
[-2147483613]
```

Invalid password for it.admin

```
[-2147483613] Fiber exit Tx=514 bytes Rx=2764 bytes, status=-1
[-2147483613] Session End
```

ءاهتنا مدع نم ووححص لكشب مدختسمل رورم ةملك نيوكت نم ققحت :لمتحملا لجال
مادختساب AD طبرب FTD موقوي ،لوخدلا ليجستب صاخلا DN عم لجال وه امك و. اهتيخالص
مدختسمل دامتعا تانايب

سفن لىل فرعتلا لىل رداق AD نأ نم ققحتلل ldp في طبرلا اذهب مايقلا نكمي امك
DN في LDP في ةدوجوملا تاوطلخال ضرع متي .رورملا ةملك و مدختسمل مسا دامتعا تانايب
ةحص ريغ رورملا ةملك وأ/و مسقلا طبرل لوخد ليجست

لمتحم لشف ببسل Microsoft مداخل شادحأ ضراع تالجسة عجارم نكمي ،كلذ لىل ةفاضلاب

رابتخا AAA

مدختسم مسا مادختساب FTD نم ةقداصم ةلواجم ةاكاحم test aaa-server رمألا مادختسا نكمي
وه رمألا .ةقداصملا وأ لاصلتالا لشف تالاح رابتخال اذه مادختسا نكمي .نيددحم رورم ةملك و
[AD IP/hostname] فيضملا [AAA-server] aaa مداخل ةقداصم رابتخا

```
<#root>
```

```
> show running-configuration aaa-server
aaa-server LAB-AD protocol ldap
  realm-id 7
aaa-server
```

LAB-AD

host

win2016.example.com

```
server-port 389
ldap-base-dn DC=example,DC=com
ldap-scope subtree
ldap-login-password *****
ldap-login-dn ftd.admin@example.com
server-type auto-detect
```

```
> test aaa-server authentication
```

LAB-AD

host

win2016.example.com

Username: it.admin

Password: *****

INFO: Attempting Authentication test to IP address (192.168.1.1) (timeout: 12 seconds)

INFO: Authentication Successful

مرحّل طاقّات اّي لمع

LDAP مزح ترداغ اذا AD مداخل لوصول اّي نكّم نم ققحتل مزحل تاومجم مادختسا نكمي هيچوتل اّي فةلكشم لى لكذريشي دقف، ةباجتسا دجوتال نكلو، FTD.

هاجتال اّي ئانث LDAP رورم ةكرح طاقّاتال رهظي.

```
> show route 192.168.1.1
```

```
Routing entry for 192.168.1.0 255.255.255.0
```

```
Known via "connected", distance 0, metric 0 (connected, via interface)
```

```
Routing Descriptor Blocks:
```

```
* directly connected, via inside
```

```
Route metric is 0, traffic share count is 1
```

```
> capture AD interface inside match tcp any host 192.168.1.1 eq 389
```

```
> show capture
```

```
capture AD type raw-data interface inside [Capturing - 0 bytes]
```

```
match tcp any host 192.168.1.1 eq ldap
```

```
> test aaa-server authentication LAB-AD host win2016.example.com username it.admin password *****
```

```
INFO: Attempting Authentication test to IP address (192.168.1.1) (timeout: 12 seconds)
```

```
INFO: Authentication Successful
```

```
> show capture
```

```
capture AD type raw-data interface inside [Capturing - 10905 bytes]
```

```
match tcp any host 192.168.1.1 eq ldap
```

```
> show capture AD
```

```
54 packets captured
```

```
1: 23:02:16.770712      192.168.1.17.61960 > 192.168.1.1.389: S 3681912834:3681912834(0) win 32768 .
2: 23:02:16.772009      192.168.1.1.389 > 192.168.1.17.61960: S 491521506:491521506(0) ack 36819128
3: 23:02:16.772039      192.168.1.17.61960 > 192.168.1.1.389: . ack 491521507 win 32768 <nop,nop,ti
4: 23:02:16.772482      192.168.1.17.61960 > 192.168.1.1.389: P 3681912835:3681912980(145) ack 4915
5: 23:02:16.772924      192.168.1.1.389 > 192.168.1.17.61960: P 491521507:491522141(634) ack 368191
6: 23:02:16.772955      192.168.1.17.61960 > 192.168.1.1.389: . ack 491522141 win 32768 <nop,nop,ti
7: 23:02:16.773428      192.168.1.17.61960 > 192.168.1.1.389: P 3681912980:3681913024(44) ack 49152
8: 23:02:16.775030      192.168.1.1.389 > 192.168.1.17.61960: P 491522141:491522163(22) ack 3681913
9: 23:02:16.775075      192.168.1.17.61960 > 192.168.1.1.389: . ack 491522163 win 32768 <nop,nop,ti
```

```
[...]
```

```
54 packets shown
```

Windows Server ءادأ ضراع ءالأس

ءوآ ببس لول الیصفء رءكأ ءامولعم AD مءاخ یلع ءادأال ضراع ءالأس رفوء نأ نكمی لشف.

1. هءاءء فاول ءادأال ضراع نع ءحبلال.



Best match



Event Viewer

Desktop app

Settings



View event logs



ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا ذه Cisco ت مچرت
م ل ا ل اء ان ا ع مچ ي ف ن ي م دخت س م ل ل م عد ي و ت ح م م ي دقت ل ة ي ر ش ب ل و
امك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ال 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 مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ال ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م اء ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا هذه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
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 دن ت س م ل ا