

EAP-TLS و PEAP ل APs ىل ع 802.1X ت لكش عم LSC

تايوت حمل

[عمدقم](#)

[عم ساس الابل طتم](#)

[تابل طتم](#)

[عمدخت سمل تانوك](#)

[عم ساس ا تامول عم](#)

[ك بشل ل ل يطى طخ ت ل م س ر ل](#)

[ن يوك ت ل](#)

[Windows Server 2016 SCEP CA](#)

[هل چ س ت و ع داهش ل ل بل اق ن يوك ت](#)

[9800 ىل ع LSC ن يوك ت](#)

[LSC AP ل \(GUI\) عم م س ر ل م دخت س م ل ع و ج او ن يوك ت تاوطخ](#)

[LSC AP ل \(CLI\) رم او ال رط س ع و ج او ن يوك ت تاوطخ](#)

[AP LSC ن م ق ق ج ت ل](#)

[ا ح ال ص او LSC داد ع ا ط خ ا ف اش ك ت س ا](#)

[LSC مادخت س اب 802.1X ع داص م ع ك ل س ل ل لوص و ل ا ط ق ت](#)

[لوص و ل ا ط ق ت ل ع ك ل س ل ل 802.1X ع داص م ن يوك ت تاوطخ](#)

[802.1X ع داص م ل \(GUI\) عم م س ر ل م دخت س م ل ع و ج او ن يوك ت ع ك ل س ل ل لوص و ل ا ط ق ت](#)

[ل ي ك ش ت CLI ع و ه ع ح ص AP Wired 802.1X](#)

[ل ي ك ش ت ح ات ف م ع و ه ع ح ص 802.1X ع ك ل س ل](#)

[RADIUS م داخ ع داهش ت ي ت](#)

[ع ك ل س ل ل 802.1X ع داص م ن م ق ق ج ت ل لوص و ل ا ط ق ت](#)

[ا ح ال ص او 802.1X ع داص م ع ا ط خ ا ف اش ك ت س ا](#)

[ق ل ص ت ا ذ ت امول عم](#)

عمدقم

802.1X لم عت س ي switchport م ه ىل ع ط ق ن ذ ف ن م cisco ق داص ي ن ا ف ي ك ع ق ي ت و ا ذ ه ف ص ي ع ق ي ر ط EAP-TLS و PEAP.

عم ساس الابل طتم

تابل طتم

عم ي ل ال ع ي ض او م ل اب ع فر عم ك ي دل نوك ت ن ا ب Cisco ي ص وت:

- عم ك ل س ل ل م ك ح ت ل ا ع د ح و

- لوصولو ةطقن
- ليدبت
- مداخل ISE
- ةداهشل حنم ةهج

ةمدختسمل تانوكملا

ةيلاتلا ةيداملا تانوكملا وجماربال تارادصا إىلا دنن تسمل اذ ه ي ةدراولا تامولعمل دنن تست

- 17.09.02 رادصإلا لغشت يتلا C9800-40-K9: ةيكلساللا مكحتلا ةدحو
- لوصولو ةطقن: C9117AXI-D
- 17.06.04 ضكري C9200L-24P-4G: لوجل
- 3.1.0.518 لغشي يذلا ISE-VM-K9 AAA: مداخل
- ةداهشل حنم ةهج: Windows Server 2016

ةصاخ ةيلمعم ةئيب ي ةدوجوملا ةزهجال نم دنن تسمل اذ ه ي ةدراولا تامولعمل عاشنإ مت تناك اذا. (يضا رتفا) حوسمم نيوكتب دنن تسمل اذ ه ي ةمدختسمل ةزهجال عيمج تادب رمأ يال لمحتملا ريثأتلل كمهف نم دكأتف، ليعشتلا ديق كتكتبش

ةيساسا تامولعم

اهنإف، 802.1X مادختساب اهب صاخلا switchport عم قداصت نا (APs) لوصولو طاقن تدرأ اذا ل تنأ ديرى نإ. تاداهش بلطتي ال يذلا EAP-FAST ةقداصم لوكوتورب اضا رتفا مدختست ريغ بناج ap لىل ع تاغوسم لمعتسي ي (أ) ةقيرط PEAP-MSCHAPV2 ل لمعتسي نا APs تنأ، (بناج الك لىل ع ةداهش لمعتسي ي (أ) ةقيرط EAP-TLS ل وأ (بناج RADIUS لىل ع ةداهش ةطقن لىل ع رذج/اهب قوثوم ةداهش ريفوتل ةديجولا ةقيرطال ي هو. ال أو LSC لكشي نا رطضي لهاجتو PEAP ءارجإ لوصولو ةطقنل نكمي ال. (EAP-TLS ةلاحي ي ف زاهج ةداهش كلذكو) لوصولو 802.1X نيوكتب بناج مث LSC نيوكتب ال أو دنن تسمل اذ ه ي طغي. مداخل بناج نم ققحتلا

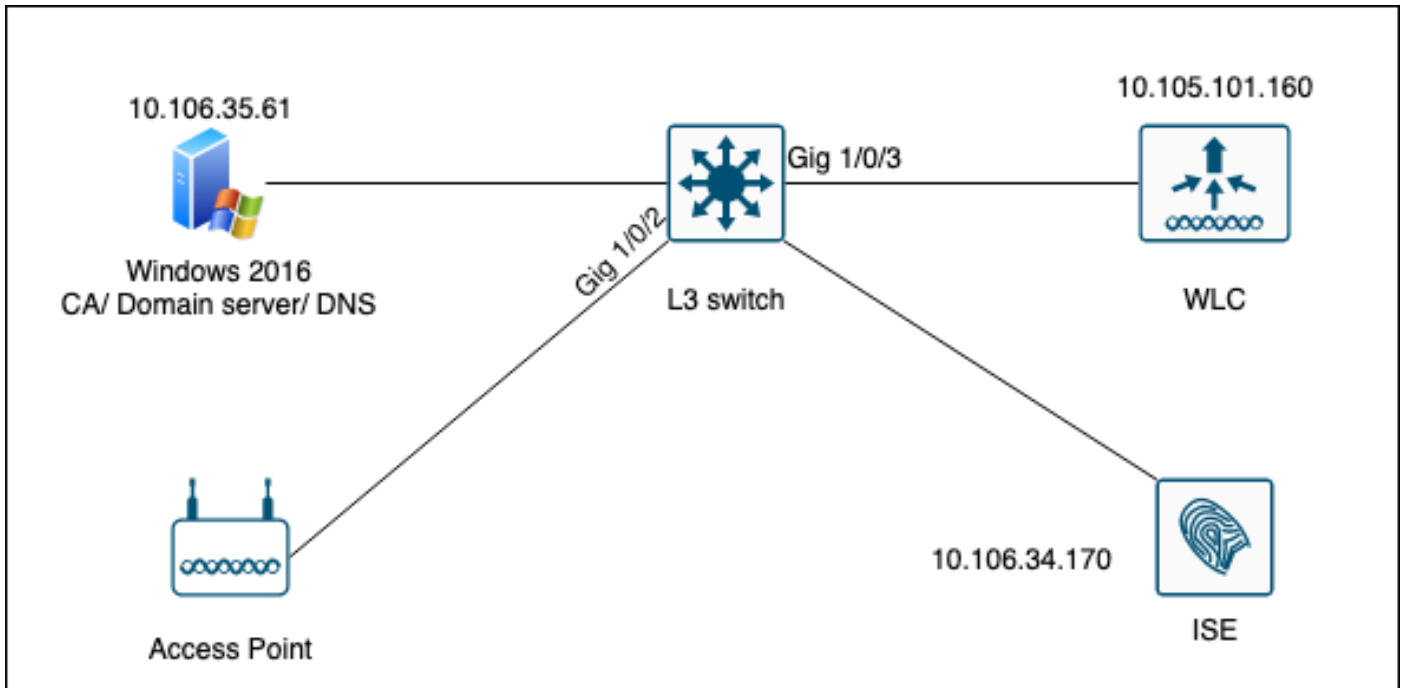
ددحتو، (CA) صيخرتلا عجرم ي ف مكحتو، لضافا نيميأت PKI رفوت نا ديرت تنك اذا LSC مدختسا اهواشنإ مت يتلا تاداهشلا لىل ع تامادختسالو، دويقلاو، تاسايسلا

لوصولو ةطقن لصتت ال CA. نع ةرداص ةداهش لىل ع مكحتلا زاهج لصحي، LSC مادختساب (WLC) ةيكلساللا ةيلحملا ةكبشل ي ف مكحتلا ةدحو بلطتت نكلو CA مداخل ةرشابم لىل ع CA مداخل لىل ع صافت نيوكتب بحج. مضمنت يتلا (APs) لوصولو طاقن نع ةباين تاداهش اهيل لوصولو بحجيو مكحتلا ةدحو.

تابللطا لهيجوت ةداعإل (SCEP) طيسبال ةداهشلا ليحست لوكوتورب مكحتلا ةدحو مدختست تاداهشلا لىل ع لوصولل ىرخأ ةرم SCEP مدختستو CA لىل ع ةزهجال لىل ع اهواشنإ مت يتلا CA نم ةعقوملا

ةداهشلا ليحست معدل CA مداوخو PKI ءالمع هم مدختسي تاداهش ةرادإ لوكوتورب وه SCEP ي ف CA مداوخ نم ديدعلا لبق نم معدمو Cisco ي ف عساو قاطن لىل ع مدختسم وه. اهلاطباو لوكوتورب نم يساسال فدهل. PKI لئاسرل لوقن لوكوتوربك HTTP مادختسا متي، SCEP ةكبشل ةزهجا إىلا تاداهشلل نم آال رادصإل وه SCEP.

ةكبشلال يطيختلا مسرلا



نيوكتالا

اساساً لكوكتال نيارم كانه SCEP CA و 9800 WLC.

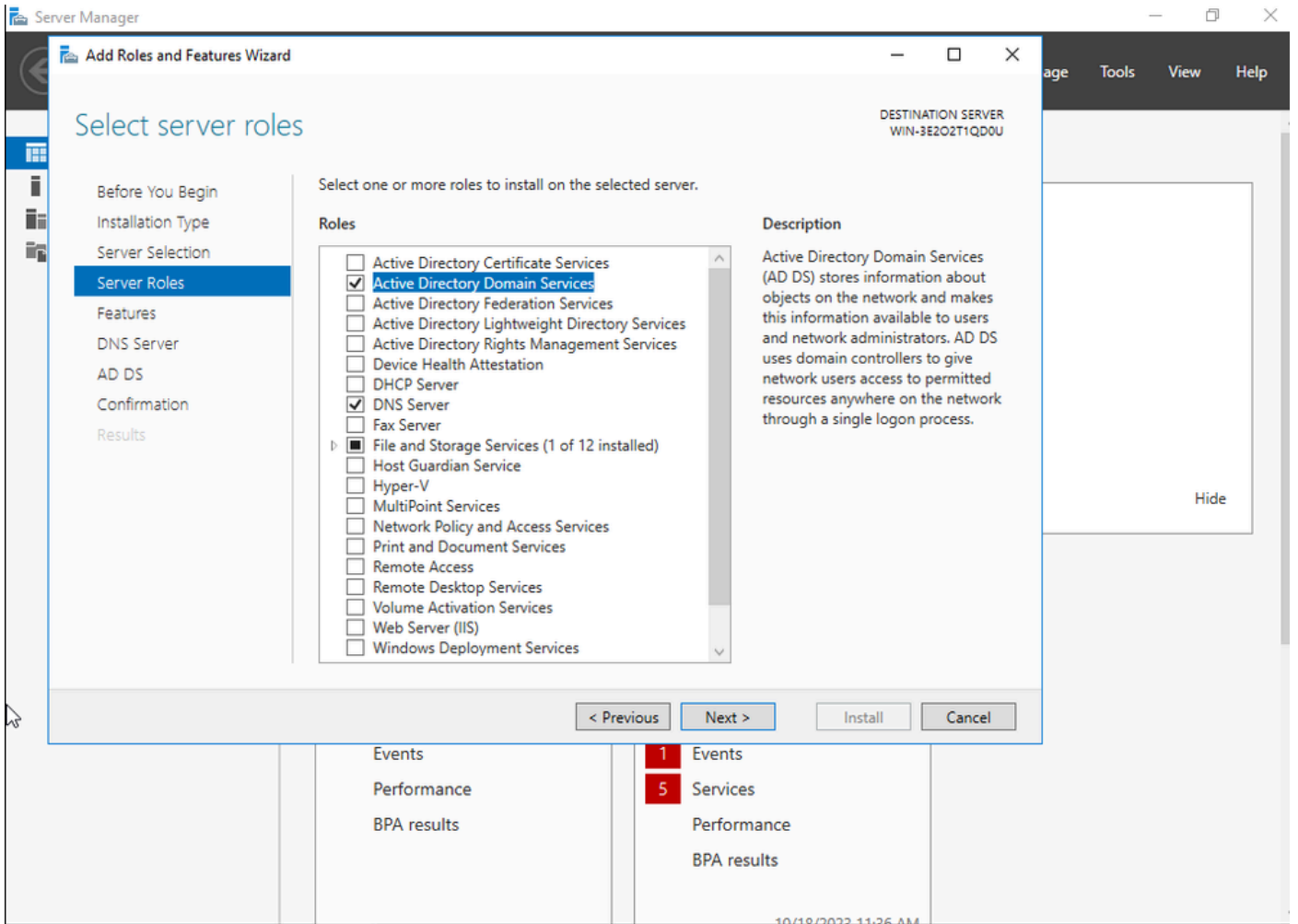
Windows Server 2016 SCEP CA

ل Windows Server SCEP لوصولو لكوكتال نيارم كانه SCEP CA و 9800 WLC. لكوكتال نيارم كانه SCEP CA و 9800 WLC. لكوكتال نيارم كانه SCEP CA و 9800 WLC. لكوكتال نيارم كانه SCEP CA و 9800 WLC.

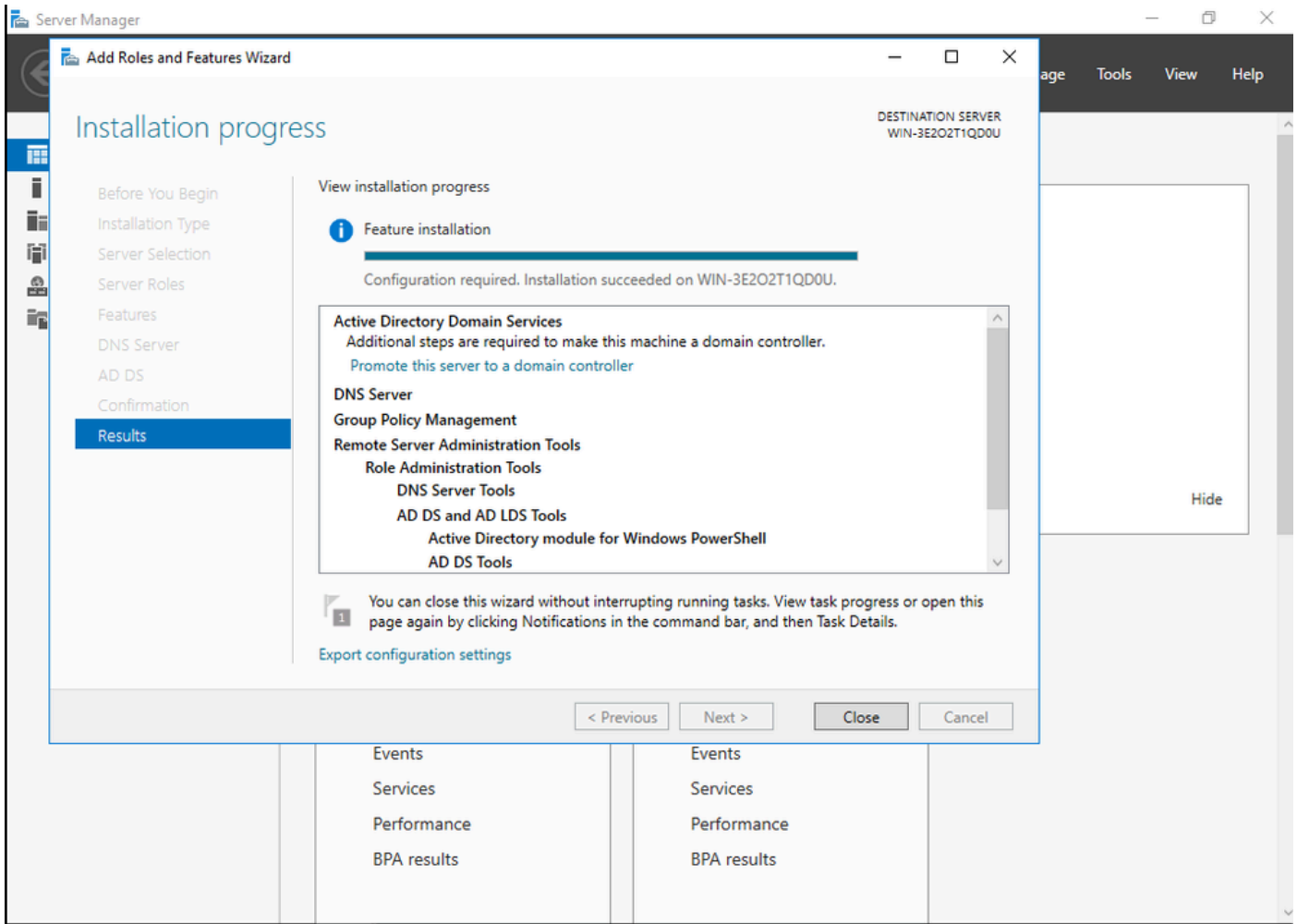
1. لكوكتال نيارم كانه SCEP CA و 9800 WLC.

2. لكوكتال نيارم كانه SCEP CA و 9800 WLC.

3. لكوكتال نيارم كانه SCEP CA و 9800 WLC.

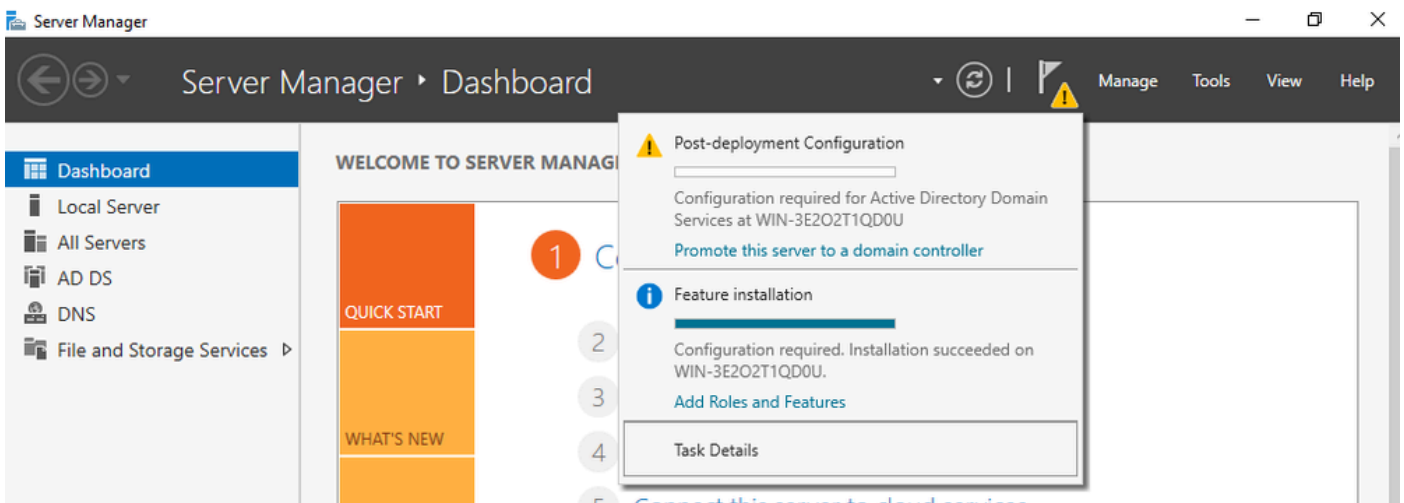


Active Directory تېپىش



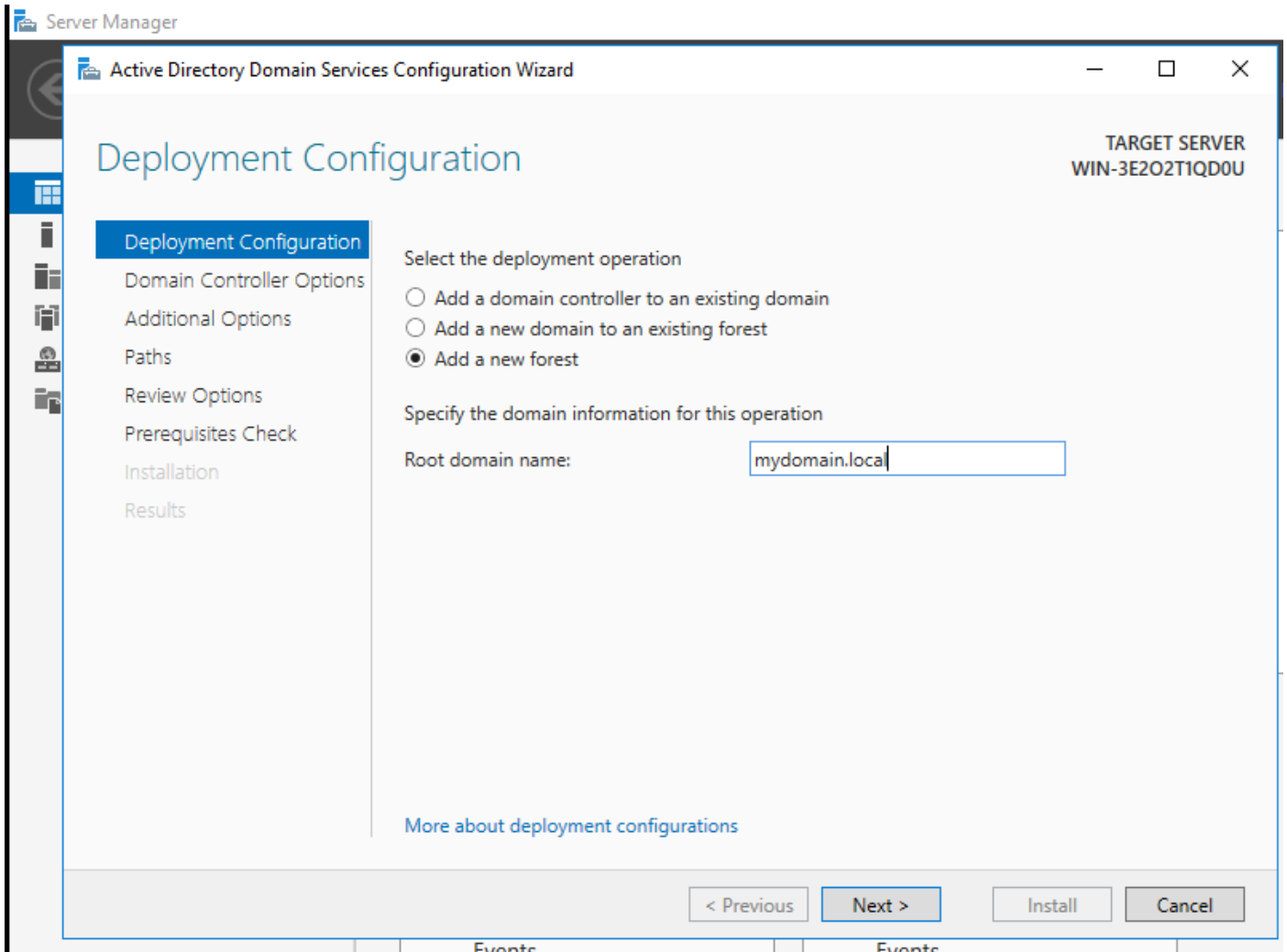
AD تېپتت عاهت نا

ةدحو لىل مدخال اذه ةيقرتب ةصاخلا تامولعمل ةحول قوف رقنا ،عاهت ناال درجم ب .4 ةوطخال لاجم لاب مكحت



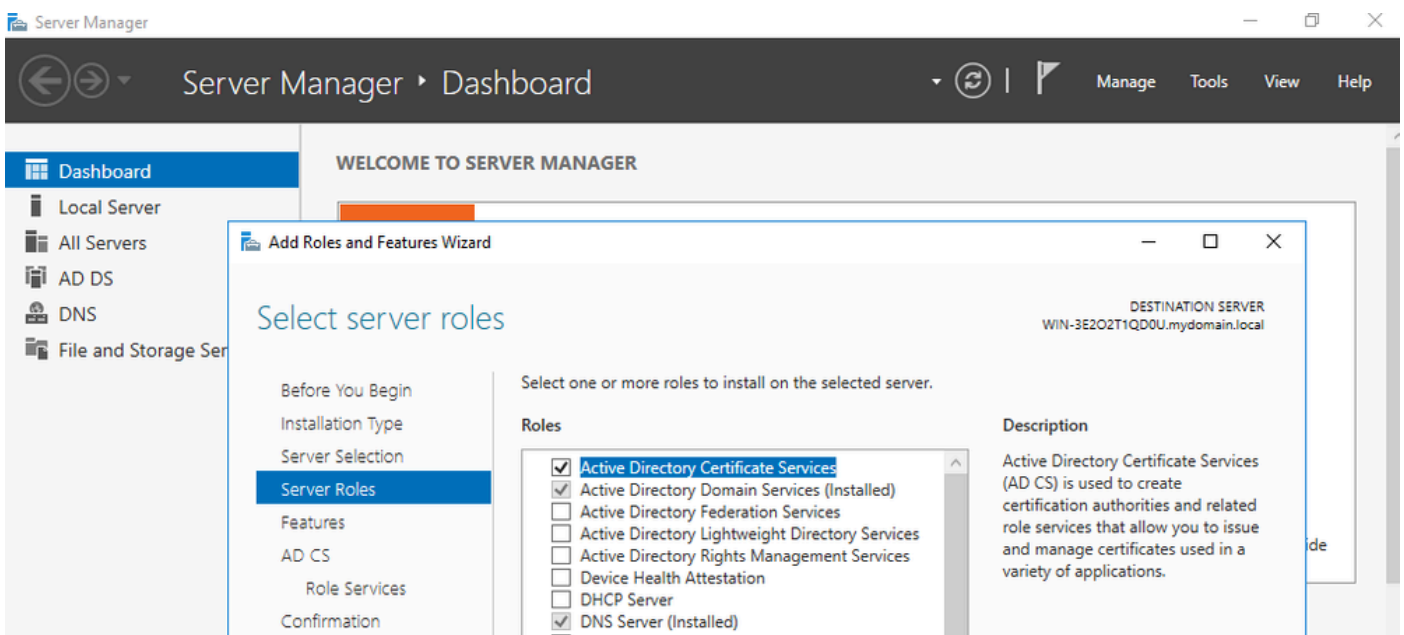
AD تامدخ نيوكت

لاجم مسا رتخاو ةديج ةباغ عاشن اب مق .5 ةوطخال

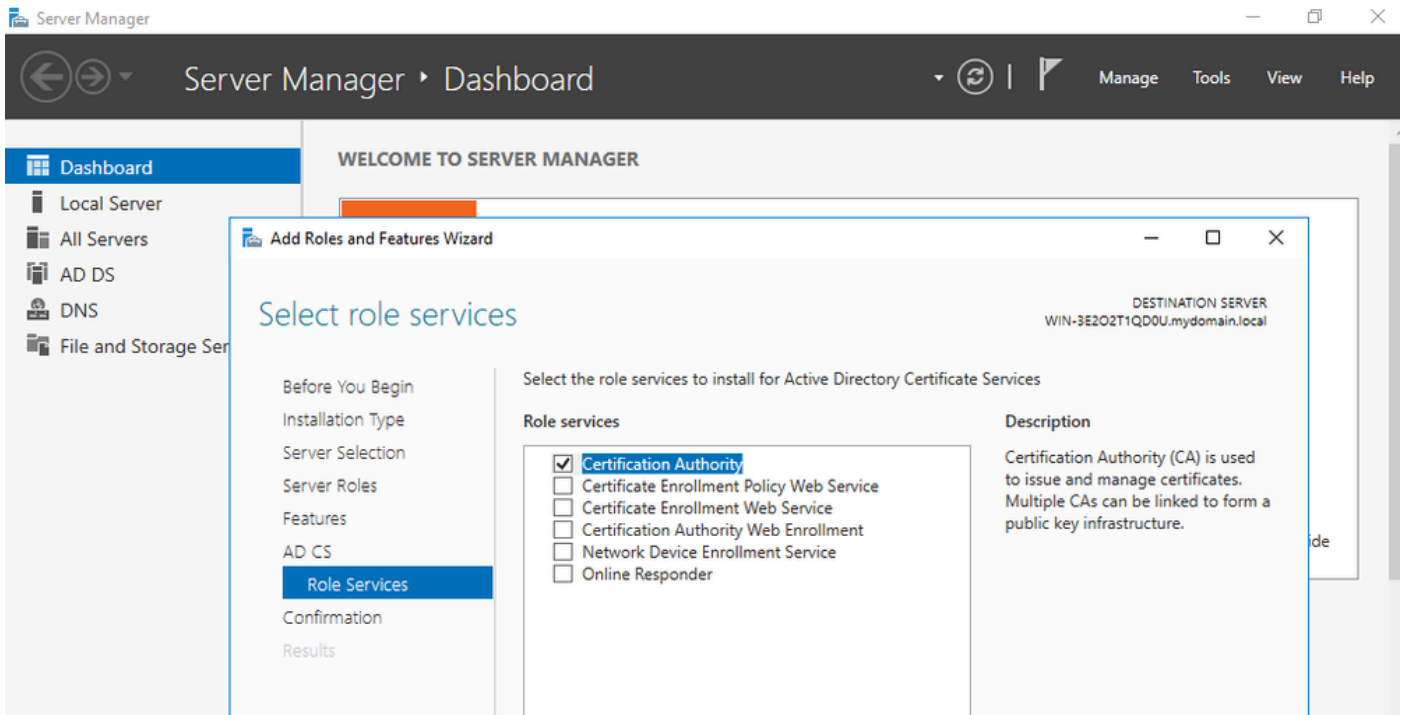


ةبأغ مسا رايتخا

مدخال اللى اتاداهش لل تامدخ رود فضا 6. ةوطخلا

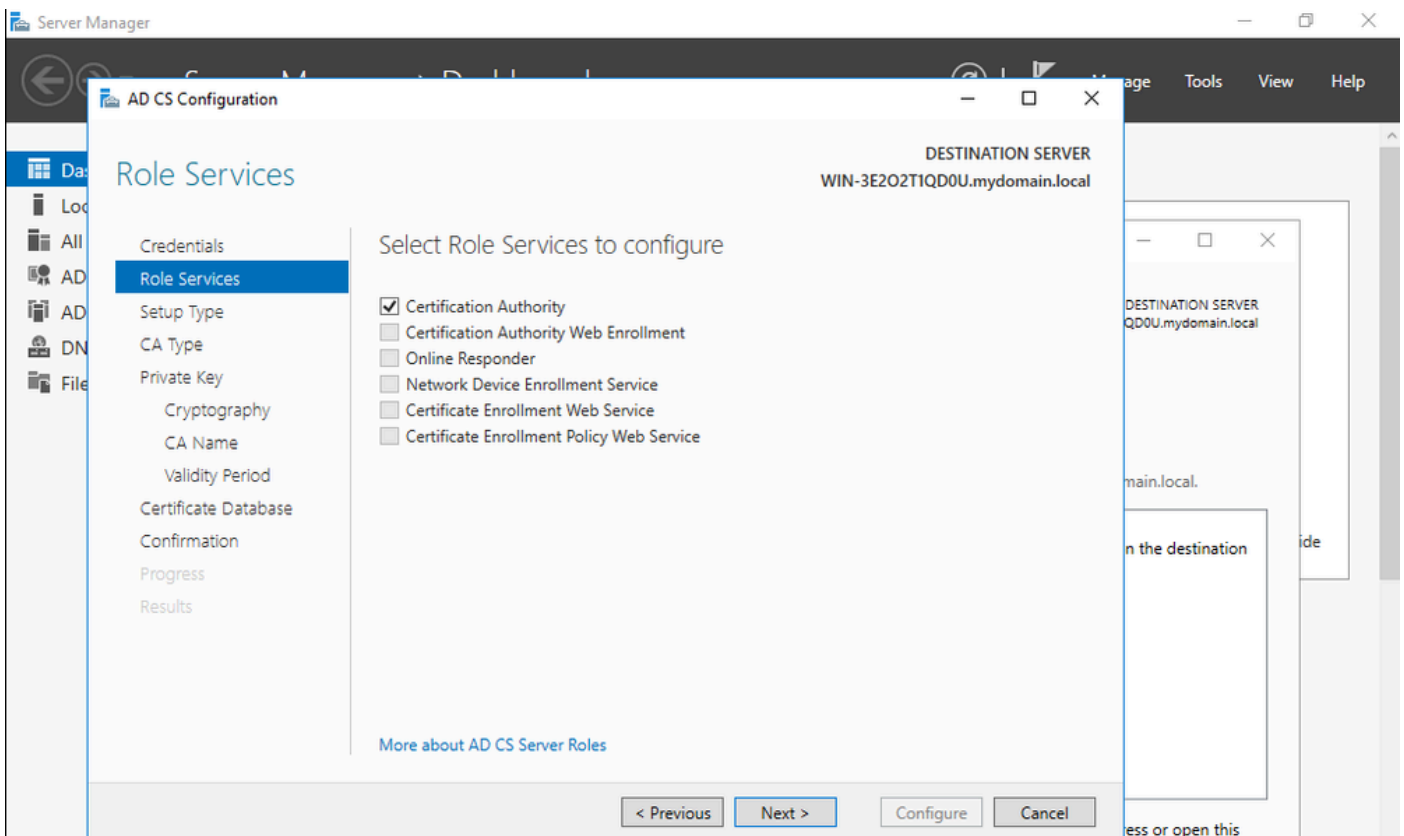


تاداهش تامدخ ةفاض

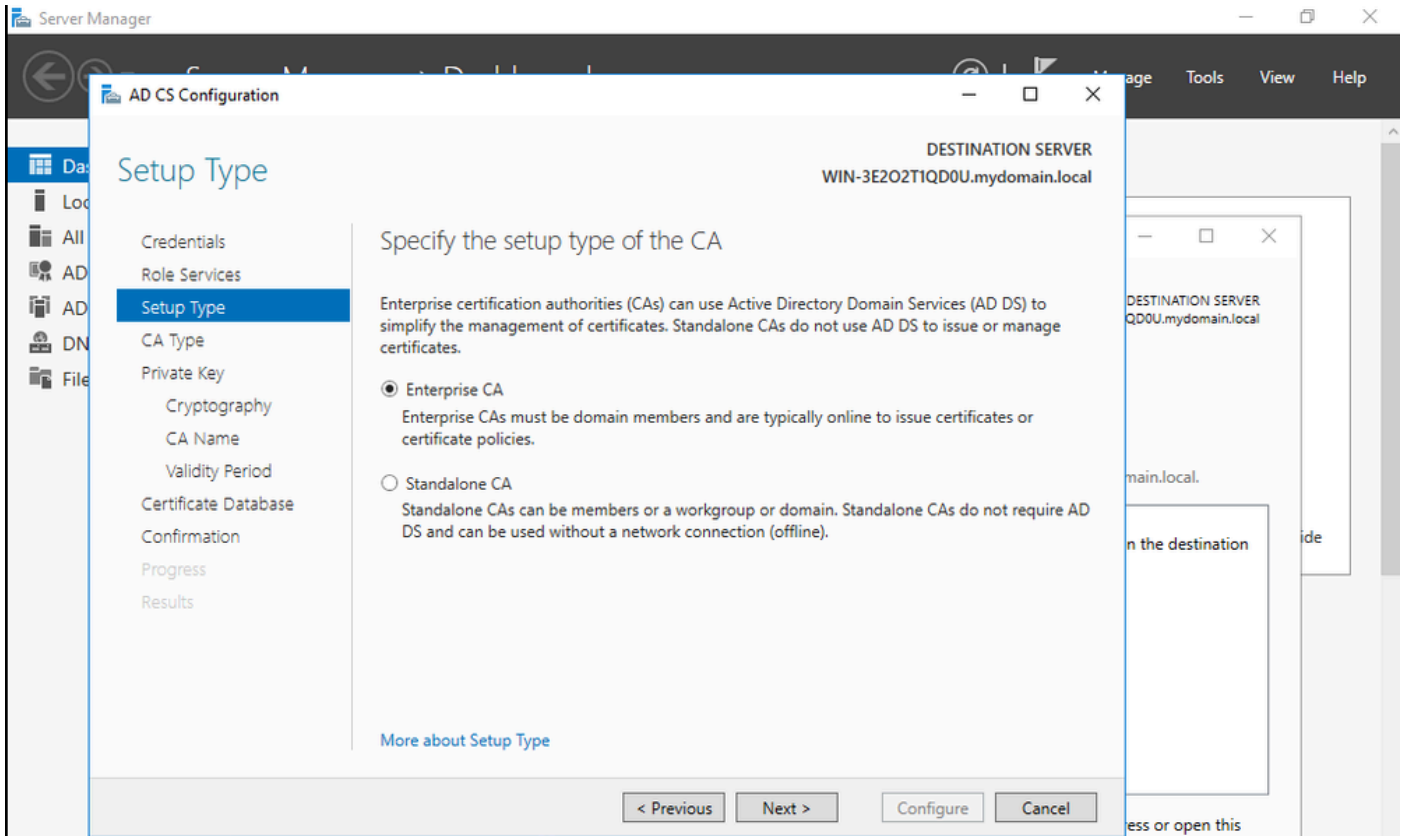


طبق قديم المجرم الافاضا

كب صاخلا قديم المجرم نيوكتب مق، اءتال درجم 7. ةوطخال

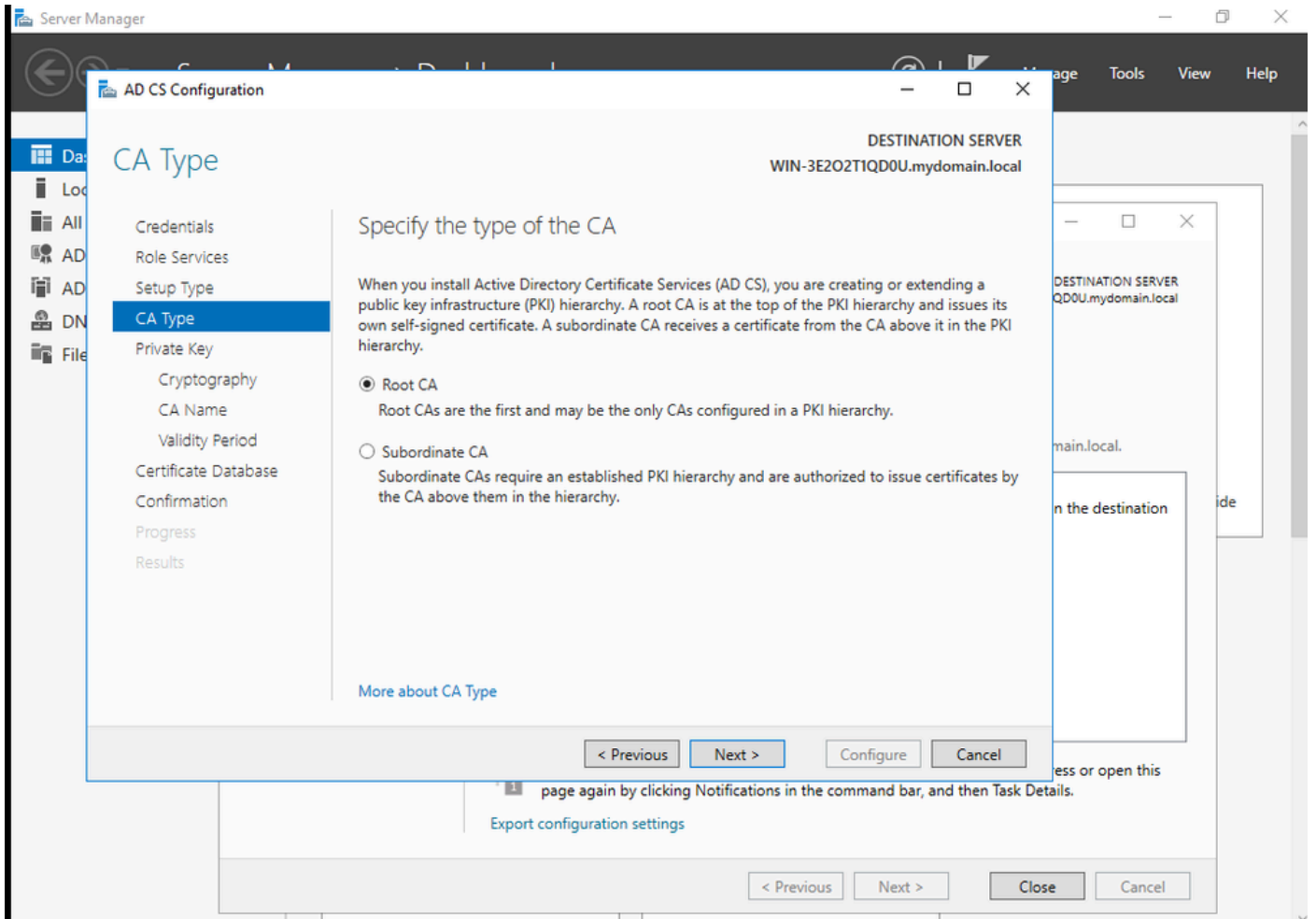


Enterprise CA. رتخأ 8. ةوطخال



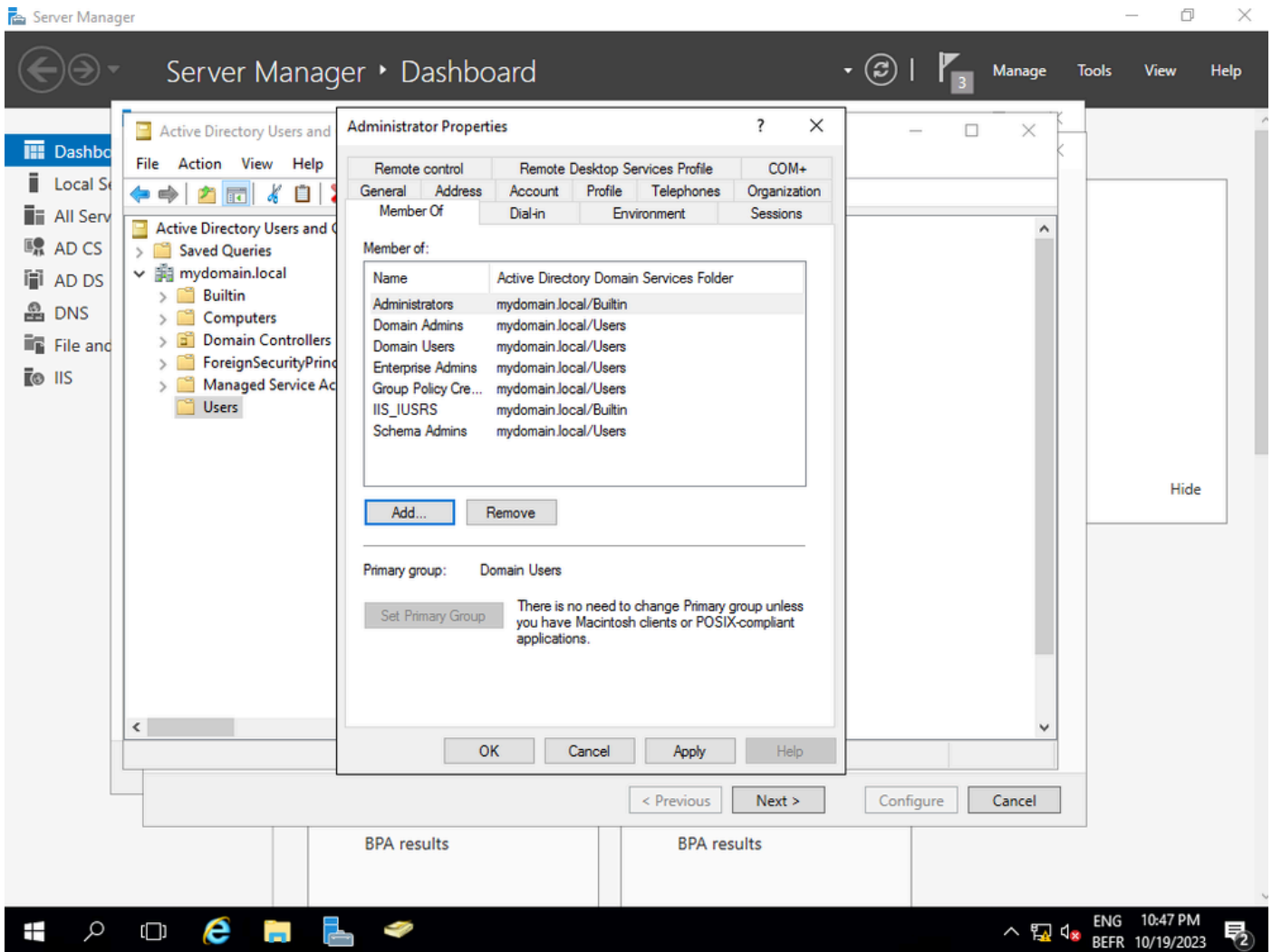
ةسسؤم لل ق دصم عجرم

LSC ل ةعبات ال CAs م عد م تي ، Cisco IOS XE 17.6 ذنم . رذل ال ق دصم ال عجرم ال هل عأ 9. ةوطخ ال



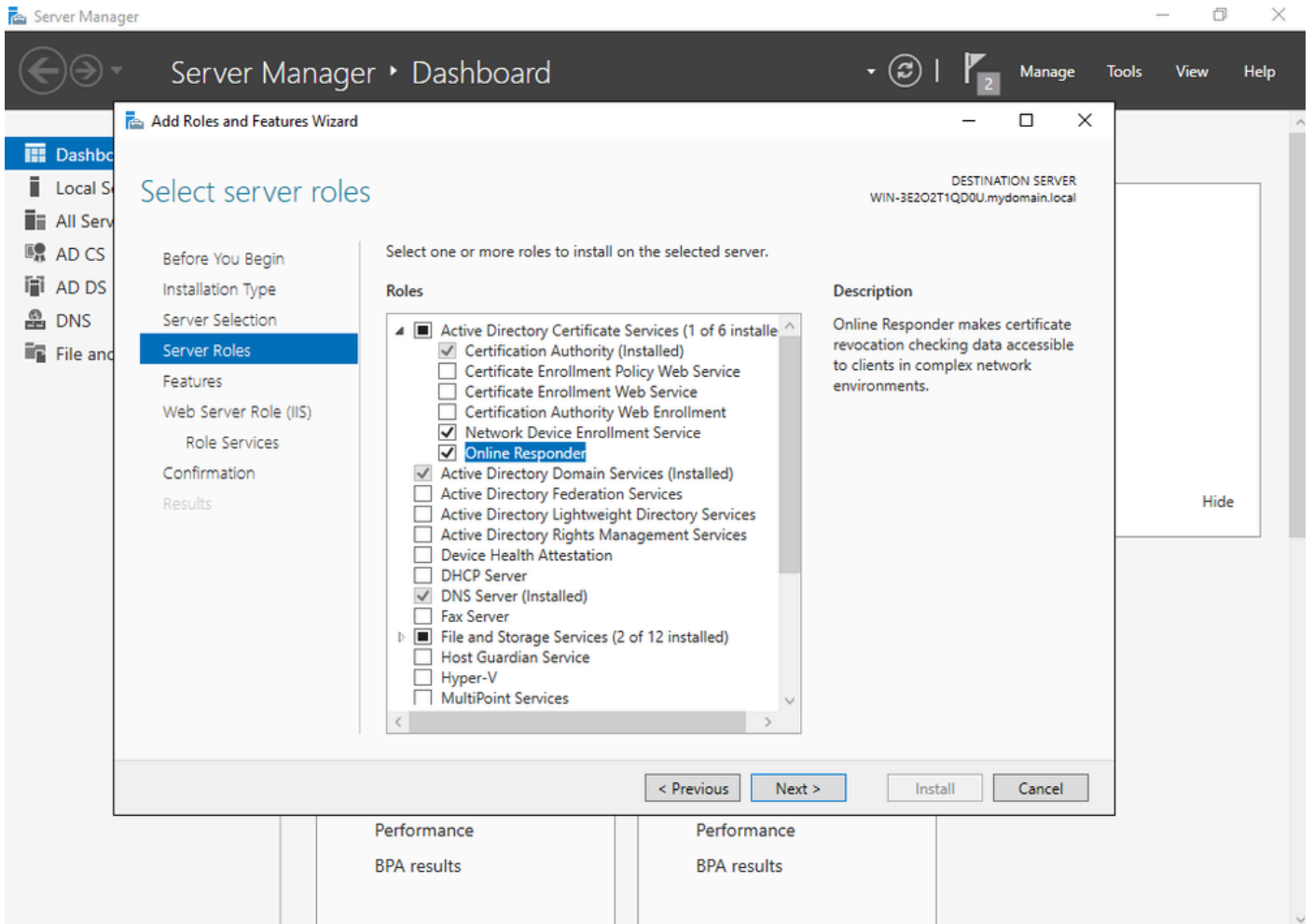
يُرجى قِدم صم عِج رِم راي تِخا

ة عومِج م نم اعزج قِدم صم ل عِج رِم ل نو كِ ي ي كل هم دِخ ت س ت ي ذل ا با س ح ل ل كِ ي د ل نو كِ ي ن ا م هم ل ا نم
ة م ئ ا ق ل ل ا ل ل ا ق ت ن ا ل ا و Administrator با س ح م ا دِخ ت س ا ك ن ك م ي ، ل ا ث م ل ا ا ذ ه ي ف . IIS_IUSRS
ة عومِج م ل ل ا ن ي ل و و س م ل ا ن ي م دِخ ت س م ل ا ة ف ا ص ا ل Directory Users and Computers . IIS_IUSRS .



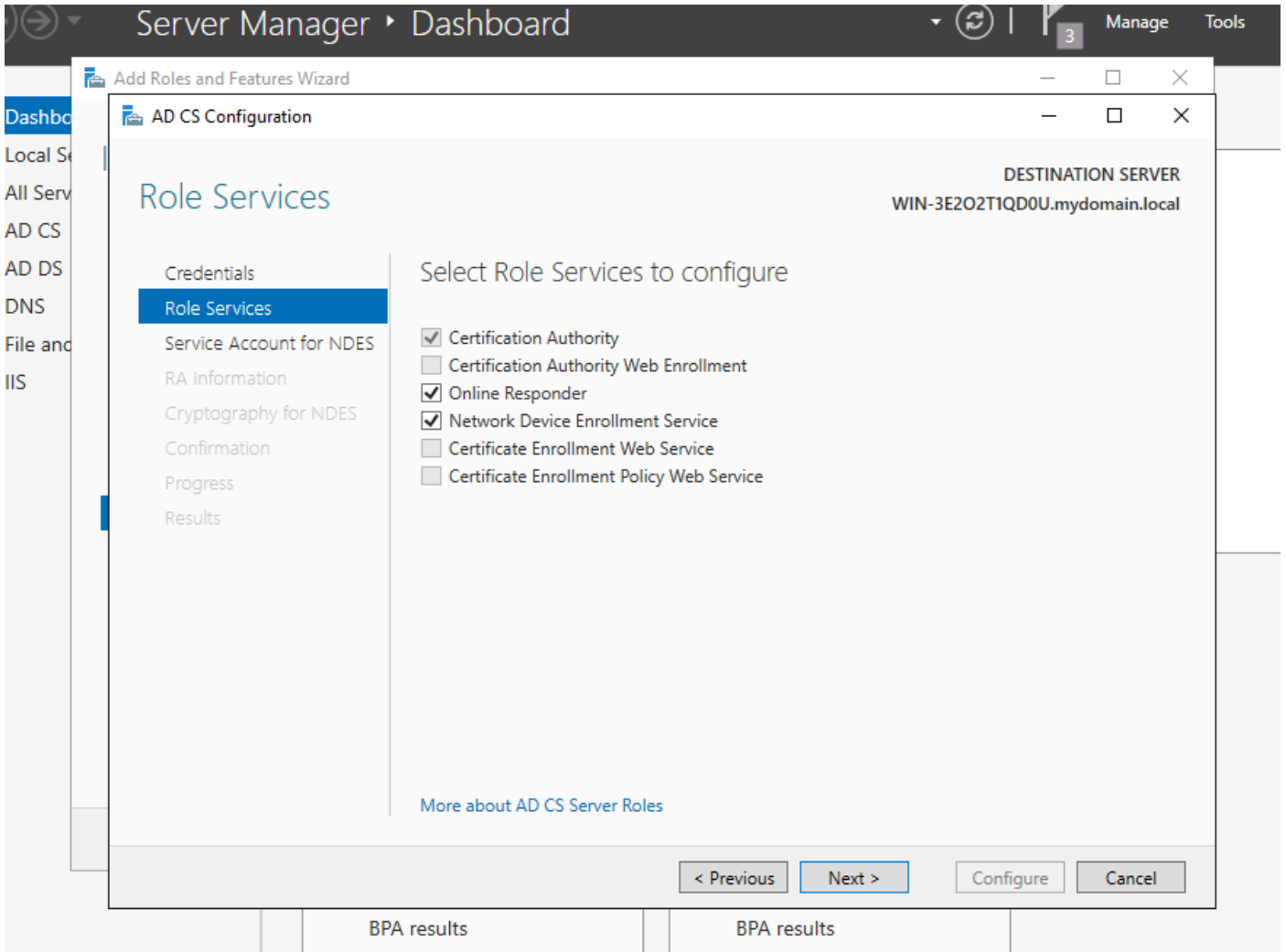
إدخال IIS_USER في كيبوردك لإدخاله في قائمة المستخدمين

رأودالاً فإضاب مق، ةححصلا IIS ةومجم يف مدختسم كيدل نوكي نأ درجم ب. 10 ةوطخلا
 كيبوردك في دصتلا عجم لإ NDES و Online Responder تامدخ فضا م. تامدخلاو



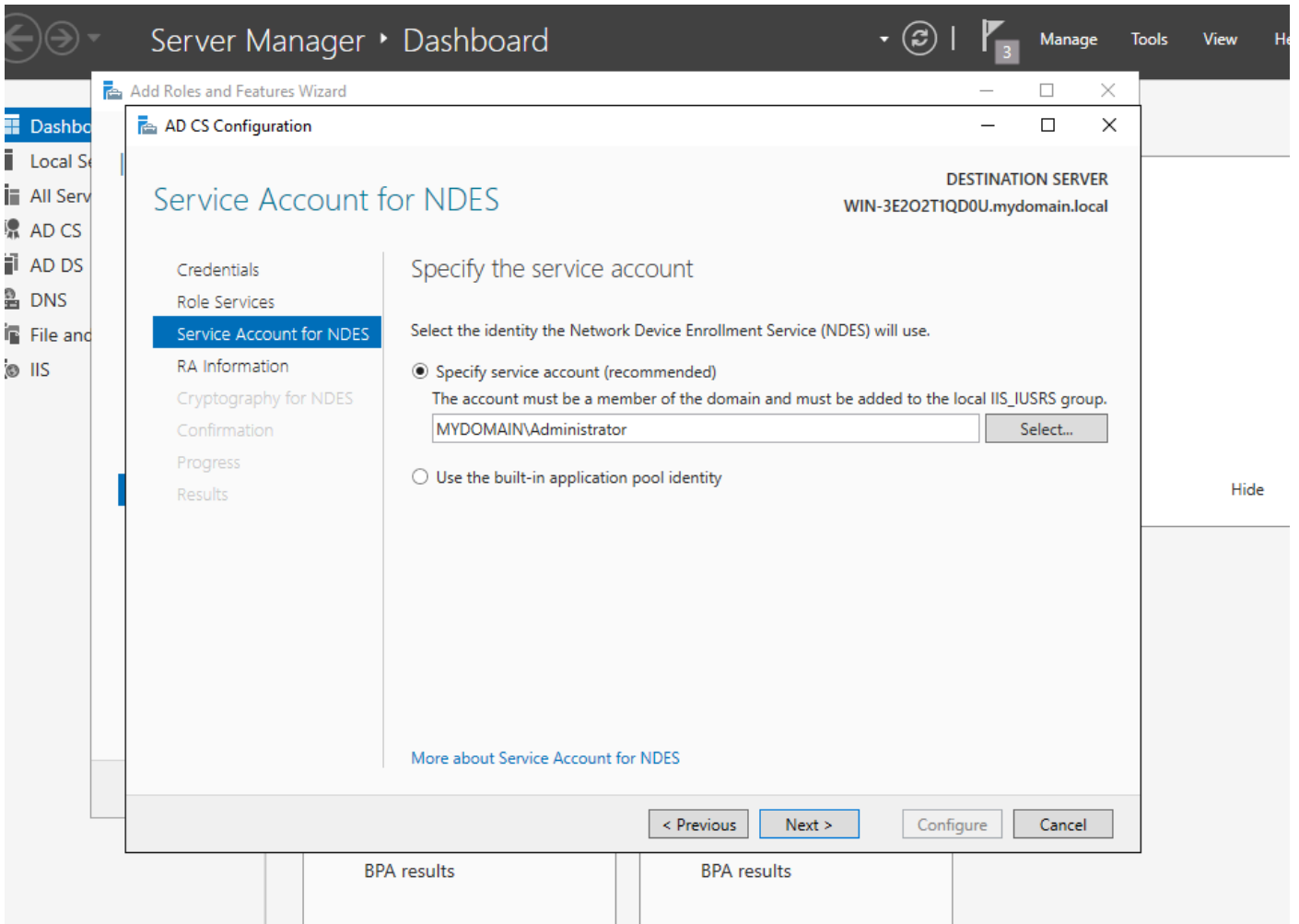
تنترتن ال رعب بي جتس الم الامدخو NDES تي ت

امدخال هذه نيوكت ب مق ،كلذب مايق ل ا درجم ب . 11 ةوطخال



تثبيت Online Responder و NDES

يتم إدخال اسم الخادم في حقل 'الخادم المستهدف' في صفحة 'الخدمات الأدوار'. يتم تحديد الخدمات التي سيتم تثبيتها في حقل 'الخدمات الأدوار'. يتم تحديد 'Online Responder' و 'Network Device Enrollment Service' في حقل 'الخدمات الأدوار'.



IIS ةومومج ىل ا هتفضأ ىذلا مدختسم ل اءاقتنا

تېبثت اضيأ كمزلي، 802.1X ةقداصم قيقحتل نكلو، SCEP تاي لمعل يفكي اذه. 13 ةوطخل ا ىتح ةلوهسب اهنوكوتو بېولا ليجست ةمدختېبثت ب مق، كذلذ. RADIUS مداخ ىلع ةداهش Windows مداخ ىلع ISE ةداهش بلط قصلوخسن نم نكمتت

Select server roles

DESTINATION SERVER
WIN-3E202T1QD0U.mydomain.local

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select one or more roles to install on the selected server.

Roles

- Active Directory Certificate Services (3 of 6 installed)
 - Certification Authority (Installed)
 - Certificate Enrollment Policy Web Service
 - Certificate Enrollment Web Service
 - Certification Authority Web Enrollment
 - Network Device Enrollment Service (Installed)
 - Online Responder (Installed)
- Active Directory Domain Services (Installed)
- Active Directory Federation Services
- Active Directory Lightweight Directory Services
- Active Directory Rights Management Services
- Device Health Attestation
- DHCP Server
- DNS Server (Installed)
- Fax Server
- File and Storage Services (2 of 12 installed)
 - Host Guardian Service
 - Hyper-V
 - MultiPoint Services

Description

Certification Authority Web Enrollment provides a simple Web interface that allows users to perform tasks such as request and renew certificates, retrieve certificate revocation lists (CRLs), and enroll for smart card certificates.

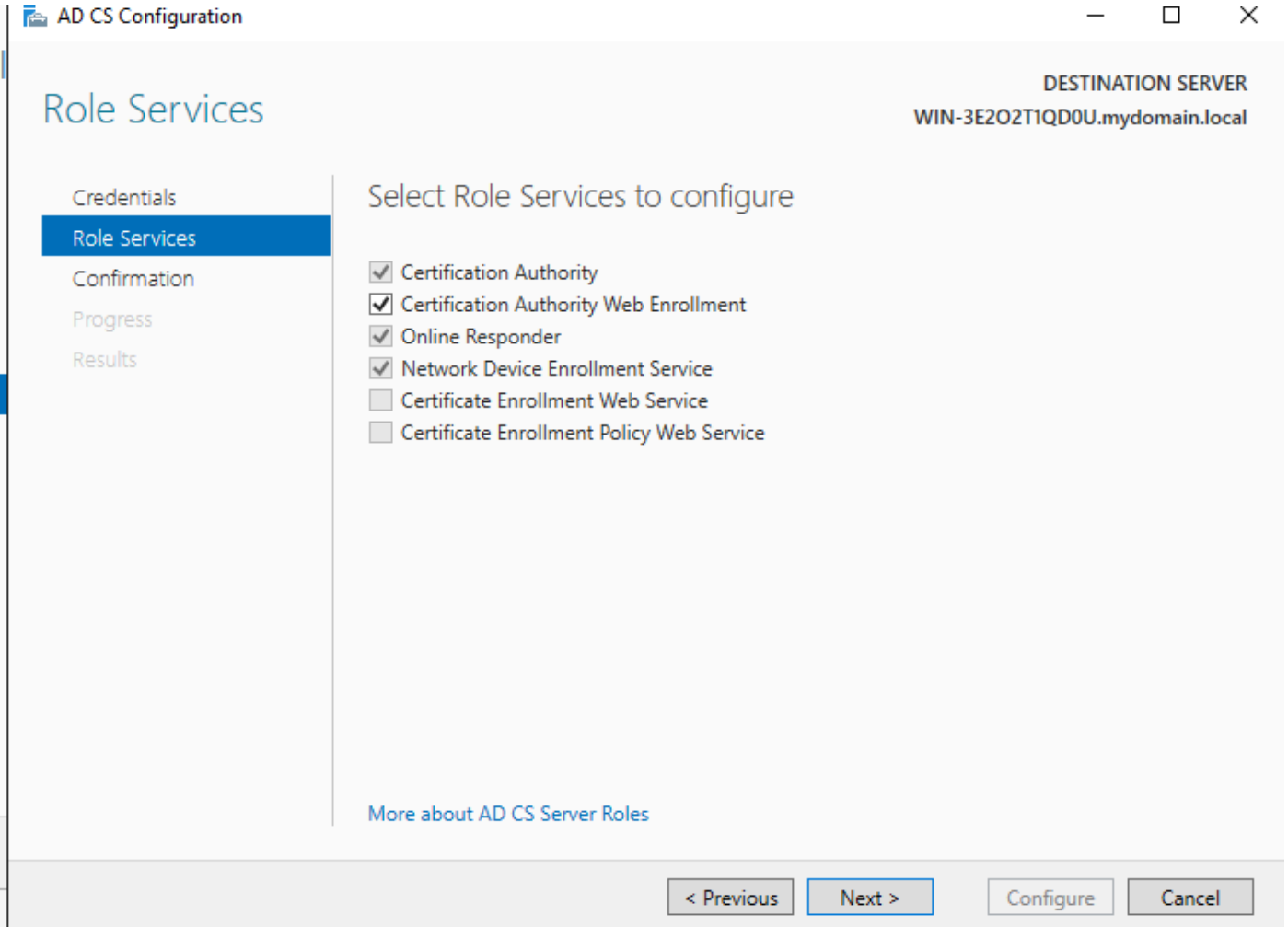
< Previous

Next >

Install

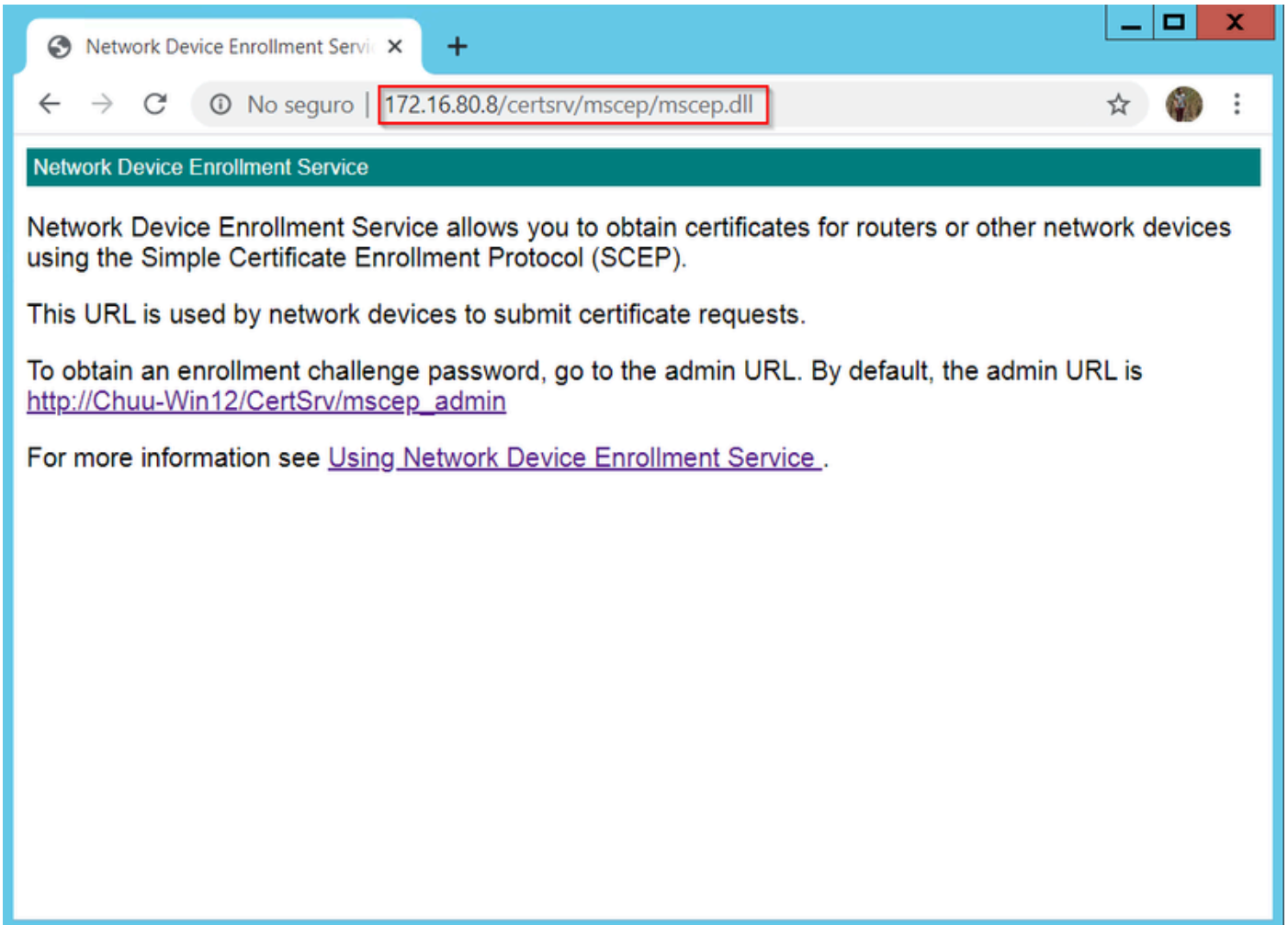
Cancel

بېولال لېجست ډمځ تېښت



بېولو ليجست ؤمدخ نيوكت

قرايز لالځ نم حيص ل كشب SCEP ؤمدخ ليجشت نم ققحت لال كنكمي .14 ؤوطخل
<http://<serverify>/certsrv/mscep/mscep.dll> :



SCEP لخدم نم ققحتل

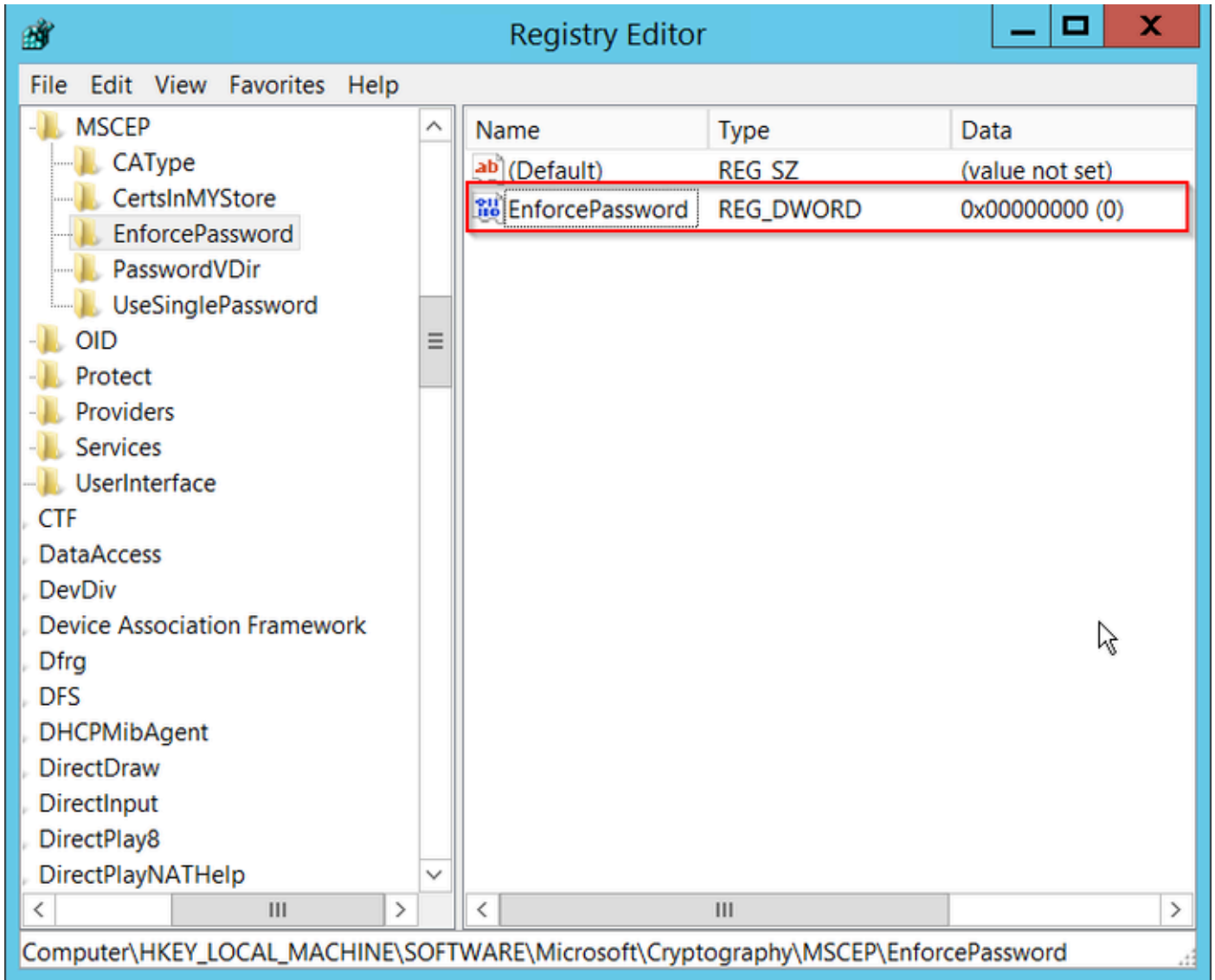
15 ةوطخل

تابلطة قداصل "يكي مانيدي دحت" رورم ةم لك Windows مداخل مدختسأ، يضارتفا لكشبو باسح اذه بلطتي. Microsoft SCEP (MSCEP) لخاد ليجستل لبقة ةياهنلا ةطقنول ليمعلا بسح رورم ةم لك ءاشنإل بيولل (GUI) ةيموسرلا مدختسمل ةهجاوإل حفصت لل لوؤسم ني مضت مكحتل ةدحو لىل رذعتي. (بلطلال نمض رورملا ةم لك ني مضت بجي) بلط لك بلطلال ليدعت مزلي، ةزيملا هذه ةلازال. مداخلإل اهل سرت يتل تابلطلال نمض هذه رورملا ةم لك NDES: مداخلىل دوجوملا ليجستل حاتفم

Start. ةمئاقلا نمض Regedit نع ثحبا، "ليجستل ررحم" حتفا

MSCEP > ريفشت > Microsoft > جم انرب > HKEY_LOCAL_MACHINE > رتوي بمكلا لىل لقتنا > EnforcementPassword

يه امك اهكرتاف، لعفلاب 0 تناك اذا 0 لىل EnforcementPassword ةميقي ريفيغب مق



ديحتال ضرر ةملك ةميقي نييعت

اهلجست و ةداهشال بلاق نيوكت

ضارغال ةددعتم تاهوييرانيس يف اهب ةنرتقمال حيتافملاو تاداهشال مادختسا نكمي جهن نيذخت متي. قدصملا عجرملا مداخ لخد قيبطتال جهن ةطساوب اهديحت مت ةفلتخم لقحلا اذه ليلحت متي. ةداهشال "EKU" عسوملا حاتفملا مادختسا لقح يف قيبطتال نم دكأتلل. هنم دوصقمال ضرغلل ليمعلا لبق نم همادختسا نم ققحتلل قدصملا ةطساوب بسانملا ةداهشال بلاق عاشناب مق، AP و WLC تاداهشال ةبسانملا قيبطتال ةسايس جمد NDES لجس يلى هنييعتب مقو

قدصملا عجرملا > ةيرادا تاودا > ادبا يلى لقنتا. 1. ةوطخل

قوف نميال سواملا رزب رقنا، قدصملا عجرملا مداخ دلجم ةرجش عيسوتب مق. 2. ةوطخل ةرادا ددحو صيخرتال بلاوق تادلجم

يف بلاقال راركت ددح م، نيمدختسملا ةداهش بلاق قوف نميال سواملا رزب رقنا. 3. ةوطخل قيايسال ةمئاق

بسح ةيصالصلا ةرتفو بلاقال مسا رييعتب مقو، ماع بيوبتال ةمالع يلى لقنتا. 4. ةوطخل

ديدحت نودب ىرخأل تاراىخلا لك كرتأ ،ةبغرلا

رذج ةداهش ةيخالص نم ربكأ تسيل اهنأ نم دكأت ،ةيخالصلا ةرتف ليدعت دنع :ريذحت
قدصملا عجرملا

Properties of New Template



Subject Name	Server	Issuance Requirements		
Superseded Templates		Extensions		Security
Compatibility	General	Request Handling	Cryptography	Key Attestation

Template display name:

Template name:

Validity period:
 years

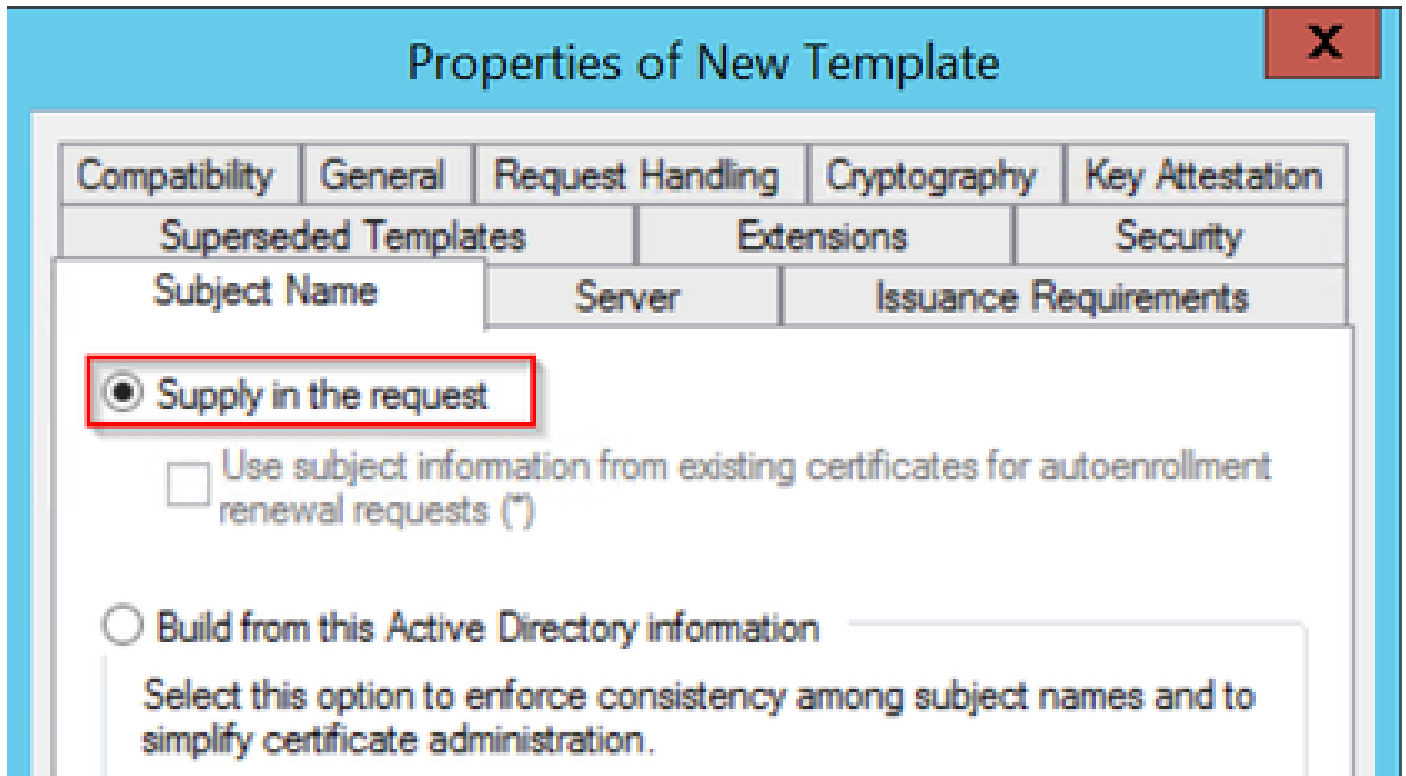
Renewal period:
 weeks

Publish certificate in Active Directory

Do not automatically reenroll if a duplicate certificate exists in Active Directory

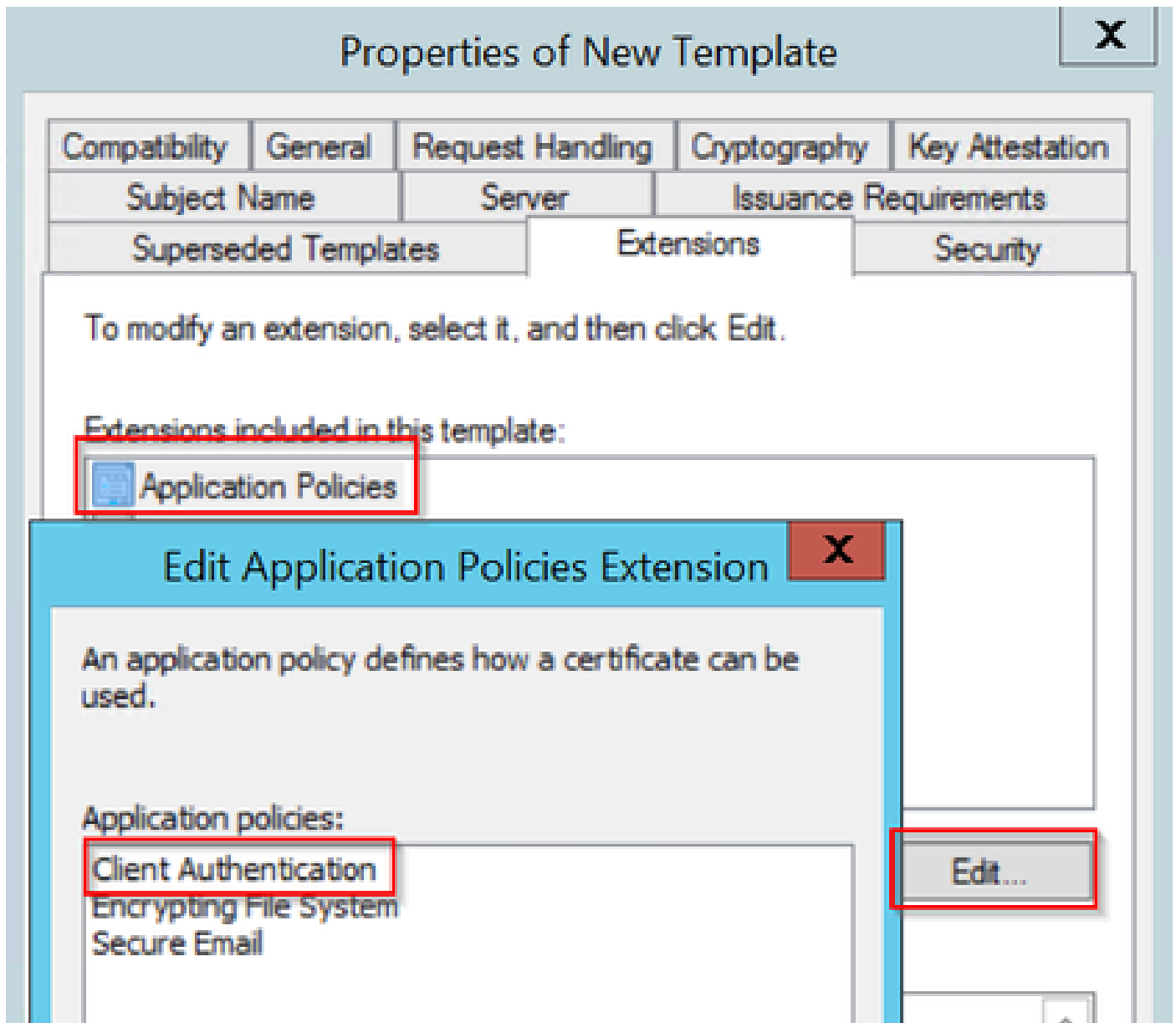
OK Cancel Apply Help

بطلال ي ف ديروتال دي دحت نم دكأت و، عوضومال مسا بيوبتال عمال عى لى لقتنا 5. ةوطخال لى لى لوصحلل لوؤسمال ةقفاومل نوجاتحي ال نيمدختسمال نأ لى لى ريشي قثب نم نأ ودي بي قفاوم ددح، ةداهشال لى لى مهع يقوت.



بطلال ي ف ديروتال

رزل ددحو تاقى بطلال جهن راىخ ددح م ث، تاقحل ملال بيوبتال عمال عى لى لقتنا 6. ةوطخال ةفاضا ددح، ال او، قى بطلال تاسايس ةذفان ي ف ةدوجوم لى م عمل ةقداصم نأ نم دكأت ريرحت هفضاو.



تاقحلملا نم ققحتلا

نم 6 ةوطخلال ي ف ددحلملا ةمدخلال باسح نأ نم دكأتو، نامأ بيوبتلا ةمالع ىلإ لقتنا 7. ةوطخلال م ث، بلالاقلا ب ةصاخلا لمالكلا مكحتلا تانودأ هي دل Windows Server في SCEP تامدخ ني كمت قفاومو قي ببطت ددح.

Properties of New Template



Compatibility	General	Request Handling	Cryptography	Key Attestation
Subject Name		Server	Issuance Requirements	
Superseded Templates		Extensions		Security

Group or user names:

- Authenticated Users
- Administrator**
- Domain Admins (CHUU-DOMAIN\Domain Admins)
- Domain Users (CHUU-DOMAIN\Domain Users)
- Enterprise Admins (CHUU-DOMAIN\Enterprise Admins)

Add... Remove

Permissions for Administrator

	Allow	Deny
Full Control	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Enroll	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Autoenroll	<input checked="" type="checkbox"/>	<input type="checkbox"/>

For special permissions or advanced settings, click Advanced.

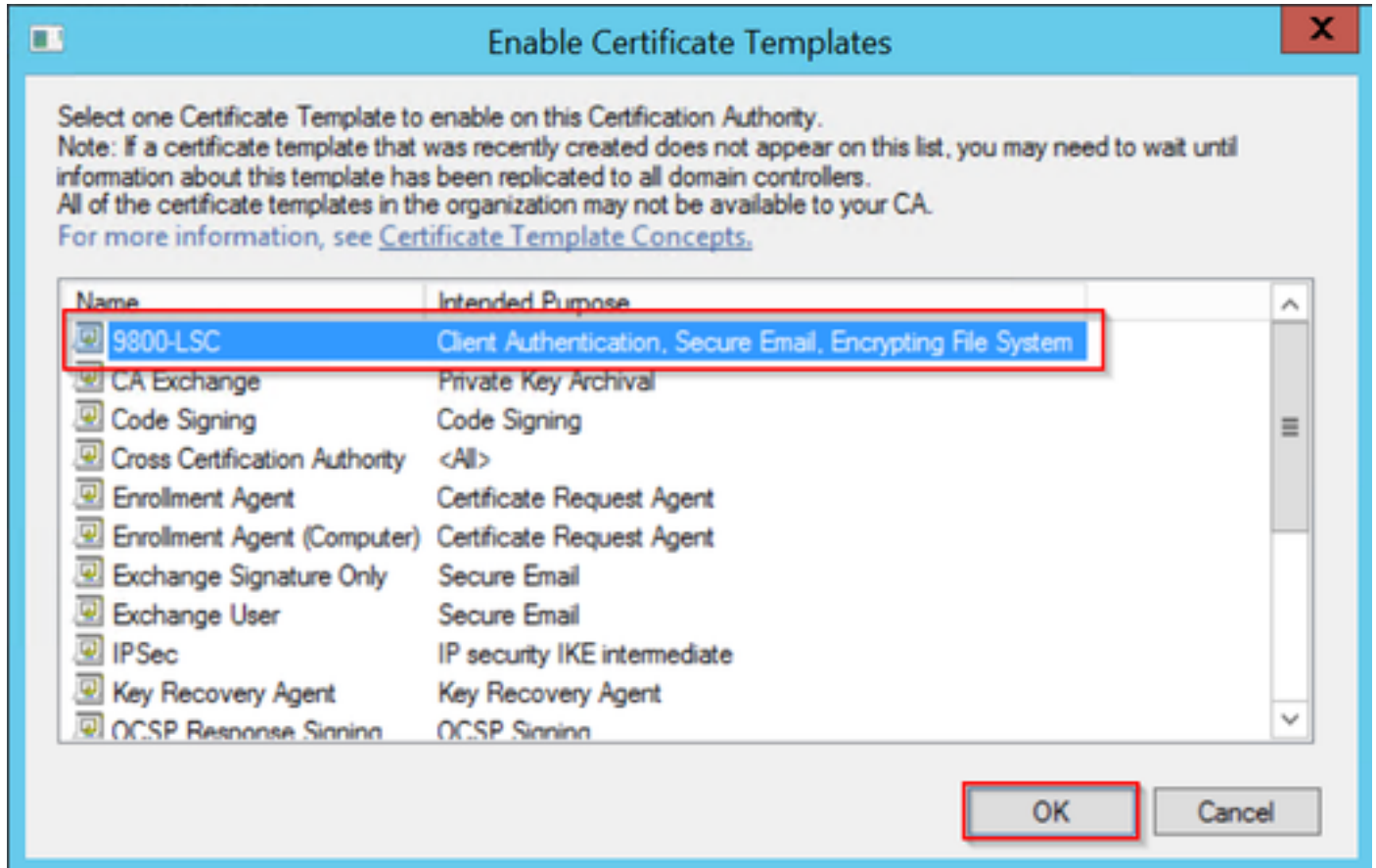
Advanced

OK Cancel **Apply** Help

بلاوق دلچملا يف نميألسواملا رزب رقن او، قدصملا عجرملا ةذفان إل عجرا 8. ةوطخل
ه.رادصإ دارملا ةداهشلا بلاق > دي دح و ةداهشلا

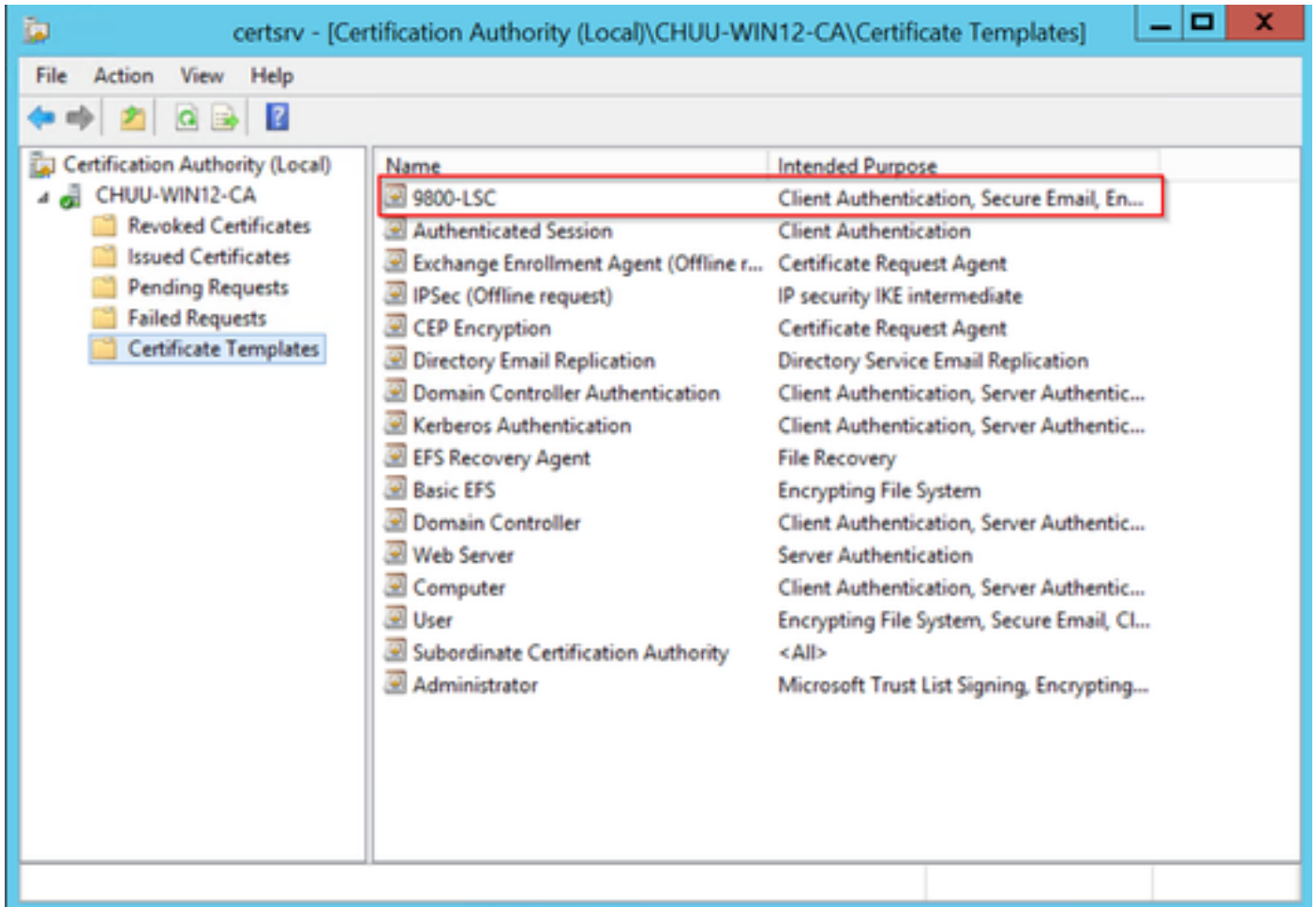
قفاوم دحو، 9800-LSC لاثملا اذه يف، اق بسم هؤاشنإ مت يذلا ةداهشلا بلاق دح. 9. ةوطخل

✎ يف جاردإلل لوطاً اتقو اتي دح هؤاشنإ مت يذلا ةداهشلا بلاق قرغتسي نأ نكمي: ةظحالم
مداوخل ةفاك يلع لثامتملا خسنلا إل جاتحي هنأل ةددعتم مداوخ رشن تايلمع



بلاقلا راي تخا

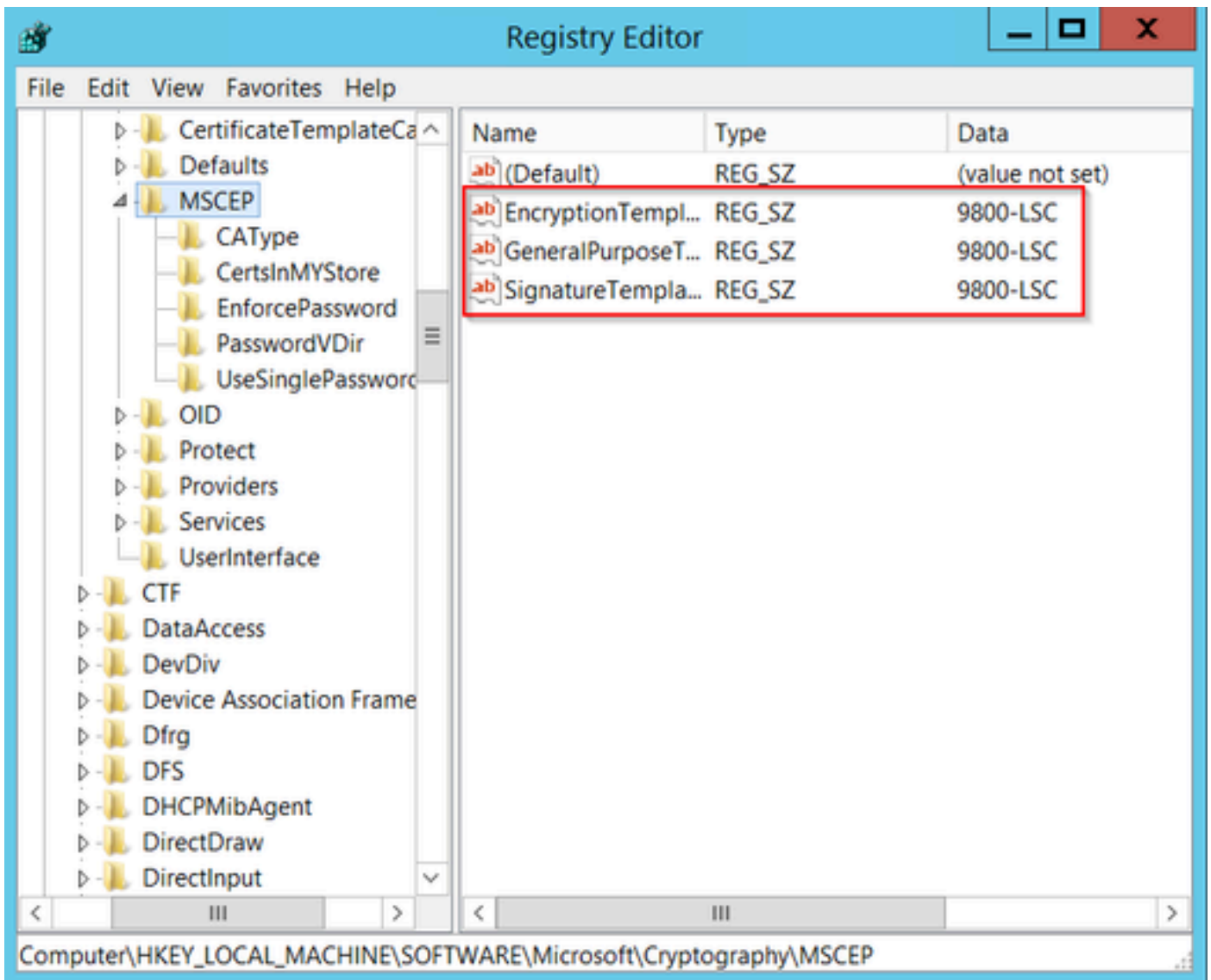
تاداهشلا بلاوق دلچم يوتحم نمض نألا دي دجل ةداهشلا بلاق درس متي



دد LSC

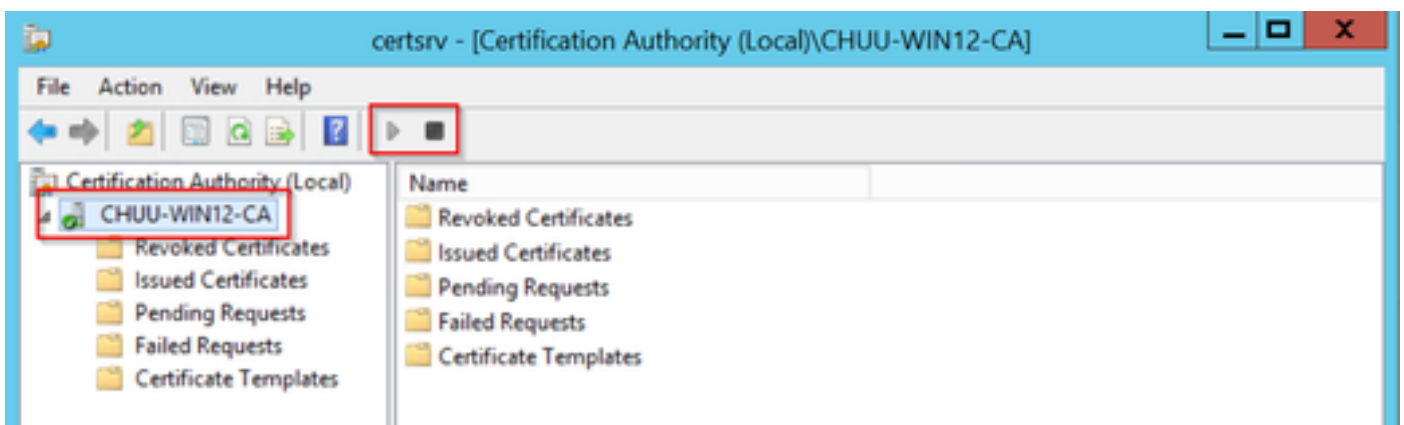
Computer > HKEY_LOCAL_MACHINE > Software > Microsoft > Cryptography > MSCEP.

EncryptionTemplate و GeneralPurposeTemplate تالچس ريرحتب مق 11. ةوطخل
ا.ثيدج هؤاشنإ مت يذلا ةداهشلا بلق اىل ريرشت شىحب SignatureTemplate و



لجسلا في بلالقا ربيغت

مداخل مسا ددحو، قددصملا عجرملا ةذفان ىلا عجرا كلذل، NDES مداخل ليغشت دعأ 12 ةوطخلا، حاجنب ليغشت وفاقيا رز ددحو.



9800 ىل ع LSC نيوكت

WLC في ap ل LSC لكشي ل لسلسلست في steps لانه

1. PKI TrustPoint ل احوال حات فملا اذه مادختسا متي RSA حات فم عاشن اب مق .
2. هؤاشن مت يذلا RSA حات فم نييعتو عتو ةقث ةطقن عاشن اب مق .
3. TrustPoint نييعتو لوصولو طاقنل LSC دادع| نيكم تب مق .
 1. ةمضنملا لوصولو طاقن عيمجل LSC نيكم تب مق .
 2. ريفوتل ةمئاق ربع ةدحمل لوصولو طاقنل LSC نيكم تب مق .
4. LSC ةقث ةطقن ل رشأو ةيكل لساللا ةرادلا ةقث ةطقن ريغت تب مق .

AP LSC ل (GUI) ةيموسرللا مدختسمللا ةهجاو نيوكت تاوطلخ

حيتا فملا جوز عاشن | > PKI ةراد | > نامأل | > نيوكتلا ل لقتنا . 1. ةوطخللا

1. بسانم مسا هي طعيو فيضي ةقطق .
2. RSA حات فم مجح ةفاض اب مق .
3. ريصدت ديتر تنك اذ طقف بولطم اذه . يراي تخ | ريصدت لل لباقل حات فملا رايخ | .
عبرملا جراخ حات فملا .
4. عاشن ادح .

ةقثلا طاقن | > PKI ةراد | > نامأل | > نيوكتلا ل لقتنا . 2. ةوطخللا

1. بسانم مسا هي طعيو فيضي ةقطق .
2. وه انه URL ناوع) ليجستلل URL ناوع لخدأ .
<http://10.106.35.61:80/certsrv/mscep/mscep.dll>
3. 1. ةوطخللا ي هؤاشن مت يذلا RSA حيتا فم جاوزا ادح .
4. ةقداصملا لعل رقنا .
5. رورم ةملك لخدأو TrustPoint ليجست قوف رقنا .
6. زاهجلا لعل قي ببطت قوف رقنا .

Configuration > Security > PKI Management

Add Trustpoint

Label* Enrollment Type SCEP Terminal

Subject Name

Country Code State

Location Domain Name

Organization Email Address

Enrollment URL Authenticate

Key Generated Available RSA Keypairs

Enroll Trustpoint

Password*

Re-Enter Password*

دحو لفسأل ريرمتلاب مق .لوصولا طاقن > يكلسال > نيوكتلا ىلا لقتنا.3 ةوطخلال ريفوت LSC.

1. اذه WLC. اذى تطبر نوكي نأ all the APs ل LSC نكمي اذه .ةنكممكة لجال ديحت
2. ةوطخلال في هانأشنأ يذلا TrustPoint مسادح

ك.تاجايتحال اقفوليصافتلا ةيقبألم

Configuration > Wireless > Access Points

All Access Points

Total APs: 1

AP Name	AP Model	Slots	Admin Status	Up Time	IP Address	Base Radio MAC	Ethernet MAC	AP Mode	Power Derate Capable	Operation Status	Config Status
AP000-F89A-8E0	C9117AX-D	2	✓	0 days 0 hrs 26 mins 42 secs	10.105.101.198	d0ec.3579.0300	0cd0.f89a.45a0	Local	Yes	Registered	Health

Misconfigured APs: Tag: 0, Country Code: 0, LSC Fallback: 0

6 GHz Radios

5 GHz Radios

2.4 GHz Radios

Dual-Band Radios

Country

LSC Provision

Status

Trustpoint Name

Number of Join Attempts

Key Size

Certificate chain status: Not Available

Subject Name Parameters

Country

State

City

Organization

ةدحو لمعة سلج في .ديهتم دعأو WLC قي رطنع ةداهشلا تبلج APs، LSC تنأ نكمي نألم

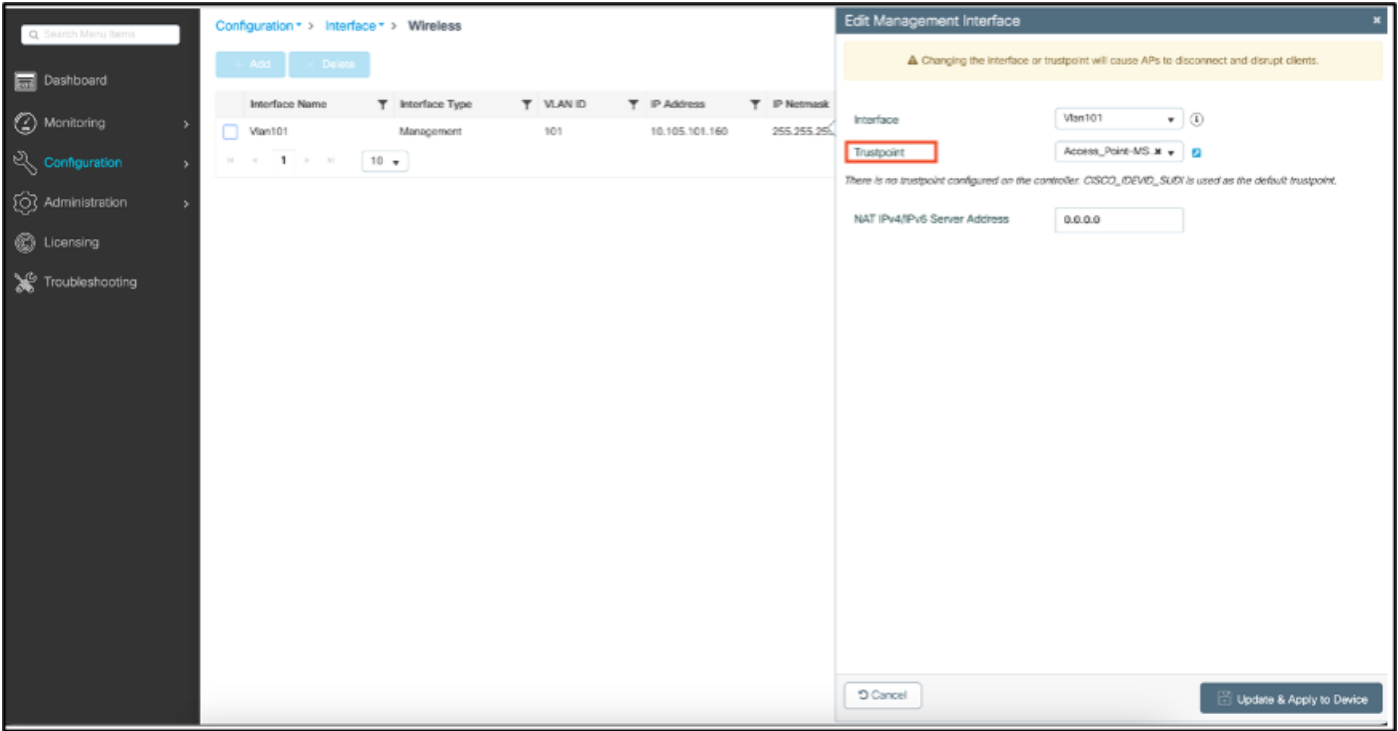
ةصاقللا هذه لثم ائيش ىرتس ،لوصولا ةطقنب مكحتلا

```
[*09/25/2023 10:03:28.0993] .....+
[*09/25/2023 10:03:28.7016] .....+
[*09/25/2023 10:03:28.7663] writing new private key to '/tmp/lsc/priv_key'
[*09/25/2023 10:03:28.7666] -----
[*09/25/2023 10:03:28.9212] LSC_ENABLE: saving ROOT_CERT
[*09/25/2023 10:03:28.9212]
[*09/25/2023 10:03:28.9293] LSC_ENABLE: saving DEVICE_CERT
[*09/25/2023 10:03:28.9293]
[*09/25/2023 10:03:28.9635] LSC certs and private key verified
[*09/25/2023 10:03:28.9635]
[*09/25/2023 10:03:29.4997] LSC private key written to hardware TAM
[*09/25/2023 10:03:29.4997]
[*09/25/2023 10:03:29.5526] A[09/25/2023 10:03:29.6099] audit_printk_skb: 12 callbacks suppressed
```

TrustPoint قباطل ةيكلساللا ةرادإلا ةداهش ربيغت كنكمي ،LSC نيكم تدرجم 4 ةوطخلل AP ل ةداهش LSC وه لمعتسي WLC ل او ةداهش LSC مه عم ىقالتي APs ل عجي اذه .LSC لوصولا طاقنل 802.1X ةقداصم لمعب طقف امتهم تنك اذا ةيراي تخا ةوطخ هذه .ىقالتي كبةصاخلا

1. ةهجاو قوف رقن او Wireless > Interface (ةهجاو) > Configuration (نيوكتلا) لىل لقتنا ةرادإلا.
2. ةوطخلل في هاناشنأ يذلا TrustPoint قباطل TrustPoint ربيغت ب مق .

لوصولا طاقن نوكت نأ بجي .LSC ل (GUI) ةيموسرلا مدختسملا ةهجاو نيوكت عزج متتخي اذهو مادختساب (WLC) ةيكلساللا ةيلحمللا ةكبشلا في مكحتلا رصنع لىل امامضنالا لىل ةرداق نألا LSC ةداهش



LSC AP ل (CLI) رماوألارطس ةهجاو نيوكت تاوطخ

1. رمالا اذه مادختساب RSA حاتفم عاشناب مق .

```
9800-40(config)#crypto key generate rsa general-keys modulus 2048 label AP-SCEP
```

```
% You already have RSA keys defined named AP-SCEP.
% They will be replaced
% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)
Sep 27 05:08:13.144: %CRYPTO_ENGINE-5-KEY_DELETED: A key named AP-SCEP has been removed from key storage
Sep 27 05:08:13.753: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named AP-SCEP has been generated or imported
```

2. ليجستلاب صاخال URL ناونع لخدأ RSA حيتافم جوز نييعتو PKI ةقث ةطقن ءاشنإ ل. ليجستلاب صاخال ليجستلاب.

```
9800-40(config)#crypto pki trustpoint Access_Point-MS-CA
9800-40(ca-trustpoint)#enrollment url http://10.106.35.61:80/certsrv/mscep/mscep.dll
9800-40(ca-trustpoint)#subject-name C=IN,L=Bengaluru,ST=KA,O=TAC,CN=TAC-LAB.cisco.local,E=mail@tac-lab.
9800-40(ca-trustpoint)#rsaakeypair AP-SCEP
9800-40(ca-trustpoint)#revocation none
9800-40(ca-trustpoint)#exit
```

3. crypto pki authenticate رمأل مادختساب CA مداخ عم اهل ليجستو PKI ةقث ةطقن ةقداصم <trustPoint>. رورم ل ةمك ةبل اطم يف رورم ةمك لخدأ.

```
9800-40(config)#crypto pki authenticate Access_Point-MS-CA
Certificate has the following attributes:
Fingerprint MD5: C44D21AA 9B489622 4BF548E1 707F9B3B
Fingerprint SHA1: D2DE6E8C BA665DEB B202ED70 899FDB05 94996ED2
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
9800-40(config)#crypto pki enroll Access_Point-MS-CA
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.
Password:
Sep 26 01:25:00.880: %PKI-6-CERT_ENROLL_MANUAL: Manual enrollment for trustpoint Access_Point-MS-CA
Re-enter password:
% The subject name in the certificate will include: C=IN,L=Bengaluru,ST=KA,O=TAC,CN=TAC-LAB.cisco.local
% The subject name in the certificate will include: 9800-40.cisco.com
% Include the router serial number in the subject name? [yes/no]: yes
% The serial number in the certificate will be: TTM244909MX
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose Access_Point-MS-CA' command will show the fingerprint.
Sep 26 01:25:15.062: %PKI-6-CSR_FINGERPRINT:
CSR Fingerprint MD5 : B3D551528B97DA5415052474E7880667
CSR Fingerprint SHA1: D426CE9B095E1B856848895DC14F997BA79F9005
CSR Fingerprint SHA2: B8CEE743549E3DD7C8FA816E97F2746AB48EE6311F38F0B8F4D01017D8081525
Sep 26 01:25:15.062: CRYPTO_PKI: Certificate Request Fingerprint MD5 :B3D55152 8B97DA54 15052474 E78806
Sep 26 01:25:15.062: CRYPTO_PKI: Certificate Request Fingerprint SHA1 :D426CE9B 095E1B85 6848895D C14F9
Sep 26 01:25:15.063: CRYPTO_PKI: Certificate Request Fingerprint SHA2 :B8CEE743 549E3DD7 C8FA816E 97F27
```

```
Sep 26 01:25:30.239: %PKI-6-CERT_INSTALL: An ID certificate has been installed under
Trustpoint : Access_Point-MS-CA
Issuer-name : cn=sumans-lab-ca,dc=sumans,dc=tac-lab,dc=com
Subject-name : e=mail@tac-lab.local,cn=TAC-LAB.cisco.local,o=TAC,l=Bengaluru,st=KA,c=IN,hostname=9800-4
Serial-number: 5C0000001400DD405D77E6FE7F000000000014
End-date : 2024-09-25T06:45:15Z
9800-40(config)#
```

4. LSC. ةداهش مادختساب لوصولال ةطقن مامضنا نيوكتب مق .

```
9800-40(config)#ap lsc-provision join-attempt 10
9800-40(config)#ap lsc-provision subject-name-parameter country IN state KA city Bengaluru domain TAC-L
9800-40(config)#ap lsc-provision key-size 2048
9800-40(config)#ap lsc-provision trustpoint Access_Point-MS-CA
9800-40(config)#ap lsc-provision
In Non-WLANCC mode APs will be provisioning with RSA certificates with specified key-size configuration
Are you sure you want to continue? (y/n): y
```

5. اهؤاشنإ مت يتل TrustPoint قباطتل ةيكلسالل ةرادإلاب ةصاخال TrustPoint رييغت تب مق . هالعأ

```
9800-40(config)#wireless management trustpoint Access_Point-MS-CA
```

AP LSC نم ققحتل

LSC. ل ققدي نأ WLC ىلع رمأ اذه تضكر

```
#show wireless management trustpoint
#show ap lsc-provision summary
#show ap name < AP NAME > config general | be Certificate
```

```

9800-40#sho ap lsc-provision summ
AP LSC-provisioning : Enabled for all APs
Trustpoint used for LSC-provisioning : Access_Point-MS-CA
Certificate chain status : Available
Number of certs on chain : 2
Certificate hash      : b7f12604ffe66b4d4abe01e32c92a417b5c6ca0c
LSC Revert Count in AP reboots : 10

AP LSC Parameters :
Country : IN
State : KA
City : Bengaluru
Orgn : TAC
Dept : TAC-LAB.cisco.local
Email : mail@tac-lab.local
Key Size : 2048
EC Key Size : 384 bit

AP LSC-provision List :

Total number of APs in provision list: 0

Mac Addresses :
-----

9800-40#sho wire
9800-40#sho wireless man
9800-40#sho wireless management tru
9800-40#sho wireless management trustpoint
Trustpoint Name : Access_Point-MS-CA
Certificate Info : Available
Certificate Type : LSC
Certificate Hash : b7f12604ffe66b4d4abe01e32c92a417b5c6ca0c
Private key Info : Available
FIPS suitability : Not Applicable

9800-40#

```

```

9800-40#sho ap name AP@CD0.F89A.46E0 config general | begin Certificate
AP Certificate type : Locally Significant Certificate
AP Certificate expiry-time : 09/25/2024 06:48:23
AP Certificate issuer common-name : sumans-lab-ca
AP Certificate Policy : Default
AP CAPWAP-OTLS LSC Status
Certificate status : Available
LSC fallback status : No
Issuer certificate hash : 611255bc69f565af537be59297f453593e432e1b
Certificate expiry time : 09/25/2024 06:48:23
AP 002.lx LSC Status
Certificate status : Not Available
AP LSC authentication state : CAPWAP-OTLS

```

ةطقنل (CLI) رم اوألا رطس ةهجاو ىلإ لوخدلا ليحستب مق ، لوصول طاقن ليحت ةداعإ درجمب LSC نيوكت نم ققحتلل رم اوألا هذه ليغشتب مق مث لوصول

```

#show crypto | be LSC
#show capwap cli config | in lsc
#show dtls connection

```

```

AP@CD0.F89A.46E0#sho crypto | be LSC
LSC: Enabled
----- Device Certificate -----
Certificate:
Data:
  Version: 3 (0x2)
  Serial Number:
    5c:00:00:00:18:18:14:ed:da:85:f9:bf:d1:00:00:00:00:00:18
  Signature Algorithm: sha256WithRSAEncryption
  Issuer: DC = com, DC = tac-lab, DC = sumans, CN = sumans-lab-ca
  Validity
    Not Before: Sep 28 04:15:28 2023 GMT
    Not After : Sep 27 04:15:28 2024 GMT
  Subject: C = IN, ST = KA, L = Bengaluru, O = TAC, CN = ap1g6-0CD0F89A46E0 emailAddress = mail@tac-lab.local
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public-Key: (2048 bit)
    Modulus:

```

```

AP0CD0.F89A.46E0#sho crypto | in LSC
LSC: Enabled
AP0CD0.F89A.46E0#sho capwap cli config | in lsc
AP lsc enable : 1
AP lsc reboot cnt : 0
AP lsc max num of retry : 10
AP lsc mode : 0x1
AP lsc dtls fallback state : 0
AP0CD0.F89A.46E0#
Read timed out

```

```

AP0CD0.F89A.46E0#sho dtls connections

```

```

Number of DTLS connection = 1

```

```

[ClientIP]:ClientPort <=> [ServerIP]:ServerPort Ciphersuit Version
-----

```

```

[10.105.101.168]:5256 <=> [10.105.101.160]:5246 0xc02f 1.2

```

```

Current connection certificate issuer name: sumans-lab-ca

```

اهحال صإو LSC دادعإ ءاطخأ فاشكتسأ

يتللا ءءاهشللا نم ققحتلل AP وأ WLC لىصوت لوحم ذفنم نم EPC طاقتللا ذخأ كنكمي DTLS قفن ءاشنإ مت اذإ PCAP نم ققحت . CAPWAP قفن نيوكتل لوصوللا ءطقن اهمدختست حاجنب .

```

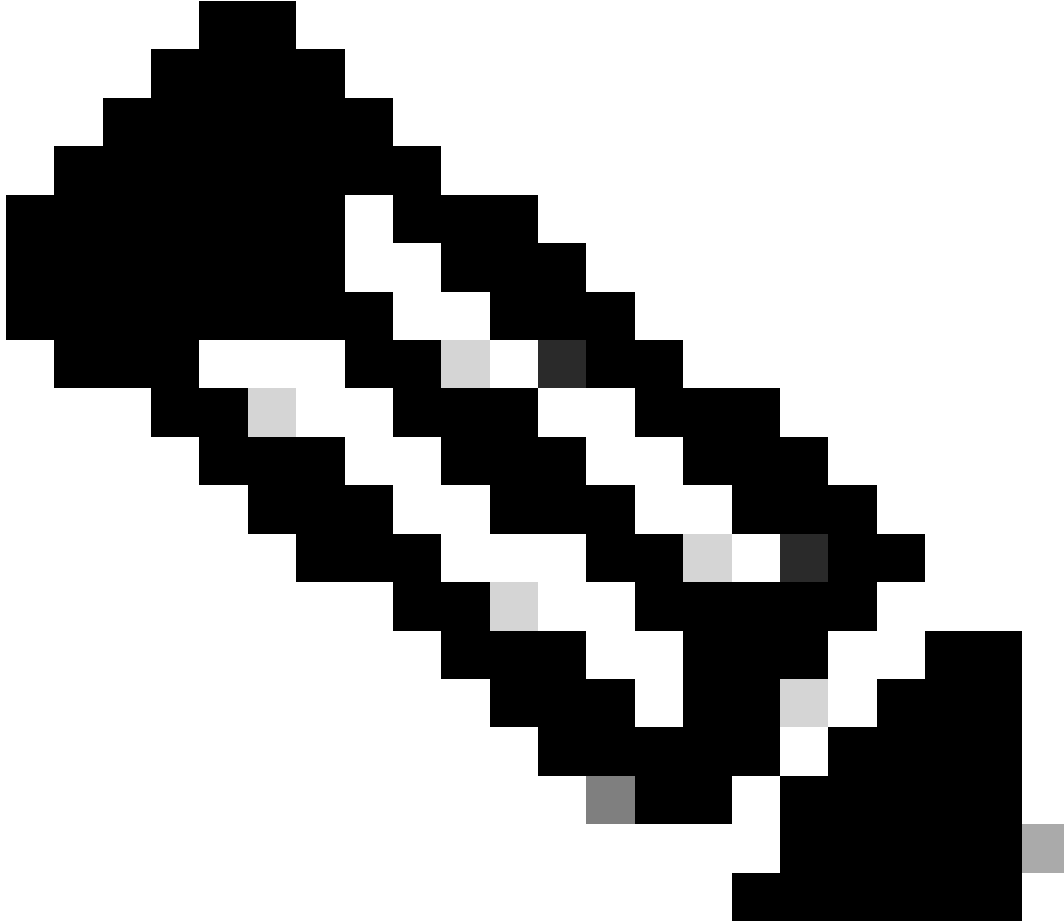
v Datagram Transport Layer Security
  v DTLSv1.2 Record Layer: Handshake Protocol: Certificate (Reassembled)
    Content Type: Handshake (22)
    Version: DTLS 1.2 (0xfefd)
    Epoch: 0
    Sequence Number: 5
    Length: 82
  v Handshake Protocol: Certificate (Reassembled)
    Handshake Type: Certificate (11)
    Length: 1627
    Message Sequence: 2
    Fragment Offset: 1557
    Fragment Length: 70
    Certificates Length: 1624
  v Certificates (1624 bytes)
    Certificate Length: 1621
  v Certificate: 3082065130820539a00302010202135c000000181814edda85f9bfd100000000018300d. (pkcs-9-at-emailAddress@mail@tac-lab.local,id-at-commonName=
  v signedCertificate
    version: v3 (2)
    serialNumber: 0x5c000000181814edda85f9bfd1000000000018
    v signature (sha256WithRSAEncryption)
      Algorithm Id: 1.2.840.113549.1.1.11 (sha256WithRSAEncryption)
    v issuer: rdnSequence (0)
      v rdnSequence: 4 items (id-at-commonName=sumans-lab-ca,dc=sumans,dc=tac-lab,dc=com)
        v RDNSequenc item: 1 item (dc=com)
          v RelativeDistinguishedName item (dc=com)
            Object Id: 0.9.2342.19200300.100.1.25 (dc)
            IA5String: com
          v RDNSequenc item: 1 item (dc=tac-lab)
            v RelativeDistinguishedName item (dc=tac-lab)
              Object Id: 0.9.2342.19200300.100.1.25 (dc)
              IA5String: tac-lab
            v RDNSequenc item: 1 item (dc=sumans)
              v RelativeDistinguishedName item (dc=sumans)
                Object Id: 0.9.2342.19200300.100.1.25 (dc)
                IA5String: sumans
              v RDNSequenc item: 1 item (id-at-commonName=sumans-lab-ca)
                v RelativeDistinguishedName item (id-at-commonName=sumans-lab-ca)
                  Object Id: 2.5.4.3 (id-at-commonName)
                  v DirectoryString: printableString (1)
                    printableString: sumans-lab-ca
                v validity
                  v notBefore: utcTime (0)
                    utcTime: 2023-09-28 04:15:28 (UTC)
                  v notAfter: utcTime (0)
                    utcTime: 2024-09-27 04:15:28 (UTC)
                v subject: rdnSequence (0)

```

ءءاهشللا ءلكشم مهفل AP و WLC لىل DTLS ءاطخأ حيحصت لىغشت نكمي .

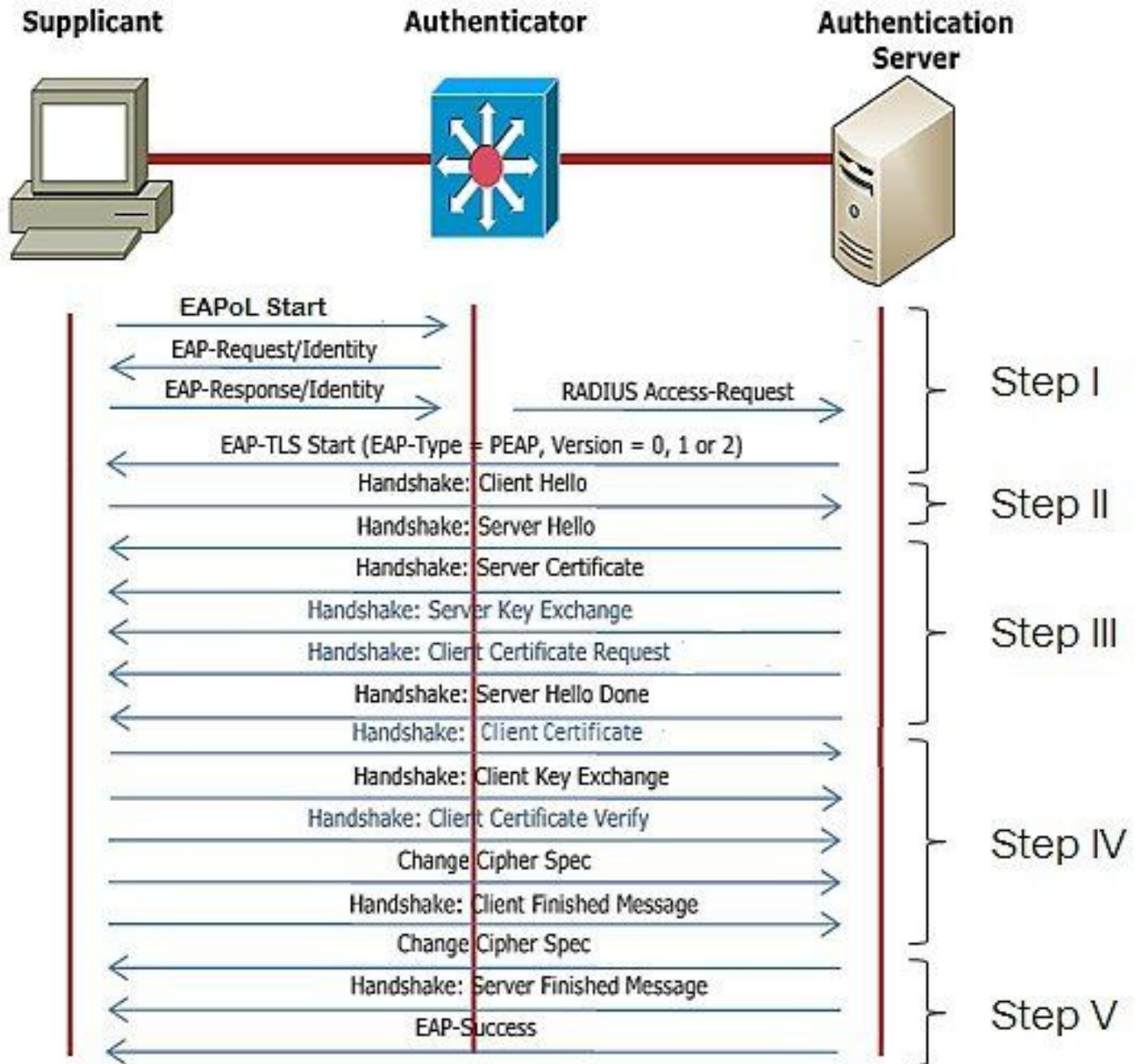
LSC مادختساب 802.1X ةقداصم ةيكلسلا لوصولا ةطقن

لمعت .اهسفن ىلع ةقداصم لل LSC ةداهش سفن مادختسال لوصولا ةطقن نيوكت مت
مداخ ثدحتي .ISE مداخ لباقم لوحملا ةطساوب اهتقداصم متي و 802.1X هجومك لوصولا ةطقن
ةشاشلا ةرؤم يف نالعالا ىلإ ISE



طاقنل نكمي ال ، AP ليصوت لوحم ذفنم ىلع dot1x ةقداصم نيكمت درجمب :ةظحالم
دادرتسال .ةقداصملا ريرمت متي ىتح رورم ةكرح ي ا لباقتسا ا و ا هيحوت ةداع ا لوصولا
ةقداصم لي طعتب مق ، AP ا لوصولا و ةحجان ريغ ةقداصمب (AP) لوصولا طاقن
لوصولا ةطقنل يكلسلا لوحملا ذفنم ىلع dot1x .

لائسارلا لدابتو EAP-TLS ةقداصم لمع ريس

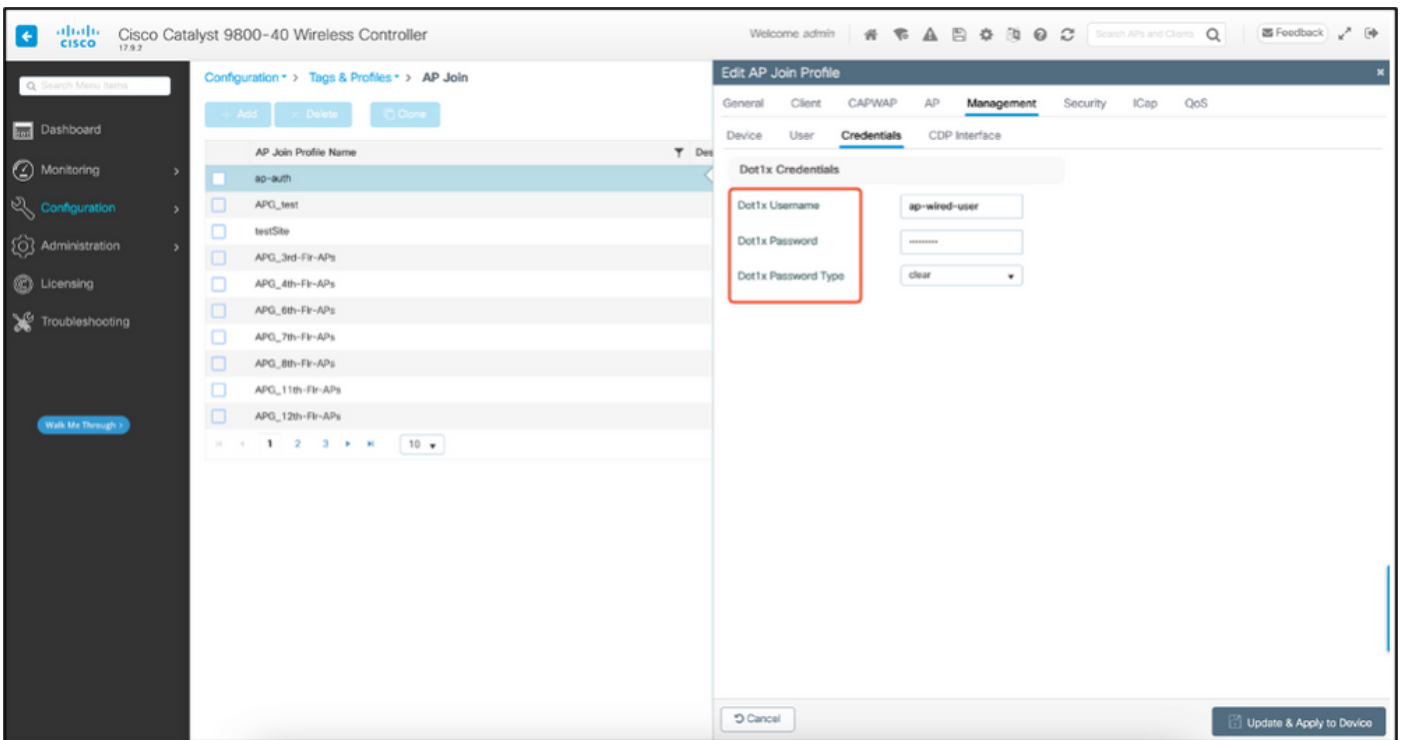
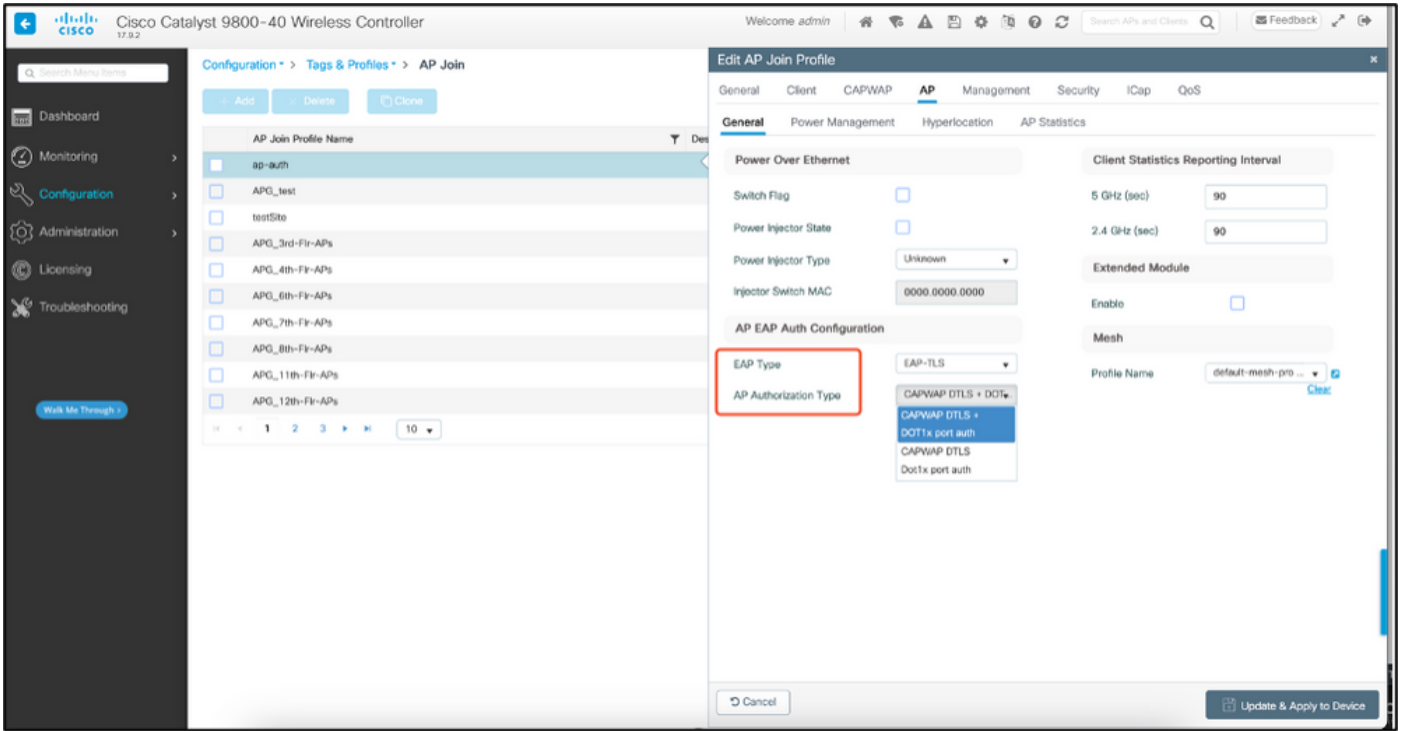


لوصول ةطقنل ةيكلسلل 802.1x ةقداصم نيوكت تاوطخ

1. EAP. عون ددحو CAPWAP ل DTLS عم dot1x ذفنملا ةقداصم نيوكت مق.
2. لوصول طاقنل dot1x دامتعا تانايب عاشناب مق.
3. ءانم حاتفملا يلع dot1x تننكم.
4. RADIUS مداخل يلع اهب قوئوم ةداهش تيبتت.

ةقداصم (GUI) ةيموسرلا مدختسمل ةهجاو نيوكت ةيكلسلل لوصول ةطقن 802.1x

1. فيرعتلا فلم يلع رقناو لوصول ةطقن طبر فيرعت فلم يلل لقتنا.
 1. CAPWAP DTLS + dot1x Port auth" ك AP ليوخت عونو EAP عون ددحو. ماع > لوصول ةطقن يلع رقنا.
 2. ةطقنل رورم ةملاك و مدختسمل مسا عاشناب مقو دامتعا تانايب > ةرادا يلل لقتنا. لوصول dot1x auth.



ليكشنت CLI ةيوه ءحص AP Wired 802.1x

ءقءاصم ال نيكمت ل ال اءه يءؤي ال . CLI ل نم APs ل dot1x نكمي نأ رماً اءه تلمعتسا نيعم ال طبرل ا فيصوت مءءتست يت ال لوصول طاقنل ةيكلسل ال .

```
#ap profile ap-auth
#dot1x eap-type eap-tls
#dot1x lsc-ap-auth-state both
#dot1x username ap-wired-user password 0 cisco!123
```

```
9808-40(config)#ap profile ap-auth
9808-40(config-ap-profile)#dot1x cap-type cap-tls
9808-40(config-ap-profile)#dot1x lsc-ap-auth-state both
9808-40(config-ap-profile)#
```

لېكشت حالات فم ټي ووه ټحص 802.1x يكل س ap

كلنك مې. ټيكل س ل AP ټق داصم نېكل م تل LAB ي ف هذو لو حمل ا تاني وكت ما دخت سا م ټي م صتل ا ل ا ادان ت سا ټق ل تخم ټي هت ل ل و ص ح ل ا

```
aaa new-model
dot1x system-auth-control
aaa authentication dot1x default group radius
aaa authorization network default group radius
radius server ISE
address ipv4 10.106.34.170 auth-port 1812 acct-port 1813
key cisco!123
!
interface GigabitEthernet1/0/2
description "AP-UPLINK-PORT-AUTH-ENABLED"
switchport access vlan 101
switchport mode access
authentication host-mode multi-host
authentication order dot1x
authentication priority dot1x
authentication port-control auto
dot1x pae authenticator
end
```

RADIUS م داخ ټ دا ه س ټ ب ټ ت

ل ك ق ټ ي ن ا ب ج ي . RADIUS م داخ و (س م ت ل م ك ل م ع ت ي ت ل ا) ل و ص و ل ا ټ ط ق ن ن ي ب ټ ق د ا ص م ل ا ټ د ح ت م داخ ټ دا ه س ي ف ل و ص و ل ا ټ ط ق ن ا ه ب ق ټ ت ي ت ل ا ټ د ي ح و ل ا ټ ق ي ر ط ل ا . ر خ ا ل ا ټ دا ه س ي ف ا م ه ن م AP ټ دا ه س ر د ص ا ي ذ ل ا SCEP CA ع ج ر م ن م ټ ر د ا ص ټ دا ه س RADIUS م داخ م د خ ت س ي ن ا ي ه RADIUS ا ض ي ا .

ټ ا د ا ه س ع ي ق و ت ټ ا ب ل ط ا ه س ن ا > ټ ا د ا ه س > ټ ر ا د ا ل ا ل ا ل ا ل ق ت ن ا ، ISE ي ف

ك ب ټ ص ا خ ل ا ISE ټ د ق ع ټ ا م و ل ع م ب ل و ق ح ل ا ټ ب ع و ت و CSR ا ه س ن ا ب م ق .

Certificate Management

- System Certificates
- Trusted Certificates
- OCSP Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Se...

Certificate Authority

Certificate Signing Request

Certificate types will require different extended key usages. The list below outlines which extended key usages are required for each certificate type:

ISE Identity Certificates:

- Multi-Use (Admin, EAP, Portal, pxGrid) - Client and Server Authentication
- Admin - Server Authentication
- EAP Authentication - Server Authentication
- DTLS Authentication - Server Authentication
- Portal - Server Authentication
- pxGrid - Client and Server Authentication
- SAML - SAML Signing Certificate
- ISE Messaging Service - Generate a Signing Certificate or generate a brand new Messaging Certificate.
- Data Connect Certificate - Connect to Oracle Database

ISE Certificate Authority Certificates:

- ISE Root CA - This is not a signing request, but an ability to generate a brand new Root CA certificate for the ISE CA functionality.
- ISE Intermediate CA - This is an Intermediate CA Signing Request.
- Renew ISE OCSP Responder Certificates - This is not a signing request, but an ability to renew the OCSP responder certificate that is signed by the ISE Root CA/ISE Intermediate CA.

Usage

Certificate(s) will be used for **EAP Authentication**

Allow Wildcard Certificates

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
<input checked="" type="checkbox"/> ISE99	ISE99#EAP Authentication

Subject

Common Name (CN)

Organizational Unit (OU)

Organization (O)

City (L)

State (ST)

اضيفاً صنفك اهقصل خسنو اهري دصت كنكمي ،اهدولوت متي نأ درجمب

URL ناووع ىلإ /certsrv/ فضاو Windows CA ب صاخلا IP ناووع ىلإ لقتنا

ةداهش بلط ىلع رقنا

← → ↻ Non sécurisé | 192.168.1.98/certsrv/

Microsoft Active Directory Certificate Services - mydomain-WIN-3E202T1QD0U-CA

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with. You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request. For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

base-64 ... م ادختساب ةداهش بلط لاسرا ىلع رقنا

Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

[Create and submit a request to this CA.](#)

[Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.](#)

ب.ي.و.ل.ا م.د.ا.خ. ة.د.ا.ه.ش. ب.ل.ا.ق. ر.ت.خ.ا. ص.ن.ل.ا. ع.ب.ر.م. ي.ف. C.S.R ص.ن. ق.ص.ل.ل.

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

Certificate Template:

(No templates found) ▾

Additional Attributes:

Attributes:

ة.د.ا.ه.ش.ل.ا ع.ي.ق.و.ت. ب.ل.ط. ة.م.ئ.ا.ق. ي.ل.ا. ة.و.ج.ر.ل.ا.ب. I.S.E ي.ل.ع. ة.د.ا.ه.ش.ل.ا. ه.ذ.ه. ت.ي.ب.ث.ت. ك.ل.ذ. د.ع.ب. ك.ن.ك.م.ي. Windows ن.م. اه.ي.ل.ع. ت.ل.ص.ح. ي.ت.ل.ل.ا. ة.د.ا.ه.ش.ل.ل.ا. ل.ي.م.ح.ت. ك.ل.ذ. د.ع.ب. ك.ن.ك.م.ي. ة.د.ا.ه.ش.ل.ل.ا. ط.ب.ر. ق.و.ف. ر.ق.ن.ل.ا. و. C.

Certificate Management	▼
System Certificates	
Trusted Certificates	
OCSP Client Profile	
Certificate Signing Requests	
Certificate Periodic Check Se...	
Certificate Authority	>

Certificate Signing Requests

Generate Certificate Signing Requests (CSR)

A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click "export" to download one or more CSRs so that they may be signed by an external authority. After a request has been signed, click this list.

🔍 View 📄 Export 🗑️ Delete 🔗 Bind Certificate

<input type="checkbox"/>	Friendly Name	Certificate Subject	Key Length	Portal gro...	Timestamp	Host
<input checked="" type="checkbox"/>	ISE99#EAP Authentication	CN=ISE99.mydomain.local	4096		Mon, 30 Oct 2023	ISE99

ة.ي.ك.ل.س.ل.ل. 802.1x ة.ق.د.ا.ص.م. ن.م. ق.ق.ح.ت.ل.ل.ا. :ل.و.ص.و.ل.ا. ة.ط.ق.ن.

ر.م.أ.ل. ل.ي.غ.ش.ت.ب. م.ق.و. ل.و.ص.و.ل.ا. ة.ط.ق.ن. ي.ل.ا. م.ك.ح.ت.ل.ل.ا. ة.د.ح.و. ل.و.ص.و. ي.ل.ع. ل.ص.ح.ا.

#show ap authentication status

:ل.و.ص.و.ل.ا. ة.ط.ق.ن. ة.ق.د.ا.ص.م. ن.ي.ك.م.ت. م.ت.ي. م.

```
AP0CD0.F89A.46E0#sho ap authentication status
AP dot1x feature is disabled.
AP0CD0.F89A.46E0#
```

AP: ةقداصم نيكمتم دعب AP نم مكحتلا ةدحو تالجس

```
AP0CD0.F89A.46E0#[*09/26/2023 08:57:40.9154]
[*09/26/2023 08:57:40.9154] Restart for both CAPWAP DTLS & 802.1X LSC mode
[*09/26/2023 08:57:40.9719] AP Rebooting: Reset Reason - LSC mode ALL
```

حاجنب AP ةقداصم تمتم

```
AP0CD0.F89A.46E0#sho ap authentication status
vty mgmt-IEEE 802.1X (no WPA)
wpa state=COMPLETED
address=0c:d0:f8:9a:46:e0
supplicant PAK state=AUTHENTICATED
supplicantStatus=Authorized
EAP state=SUCCESS
selectedMethod=13 (EAP-TLS)
EAP TLS version=15v1.2
EAP TLS cipher=ECDHE-RSA-AES256-GCM-SHA384
tls_session_reused=0
EAP session_id=0d7b91a744885a6e8e460d49fee7d2d5604ca2bdd11f40494a4325dc98d1919af48b9f33ce526f18eda11effcb2ea0238cf95244aaf5f17decf336ad11e88121
AP0CD0.F89A.46E0#
```

WLC نم ققحتلا

```
9800-40#sho ap name AP0CD0.F89A.46E0 config general | begin Certificate
AP Certificate type : Locally Significant Certificate
AP Certificate Expiry-time : 09/25/2024 06:48:23
AP Certificate issuer common-name : sumans-lab-ca
AP Certificate Policy : Default
AP CAPWAP-DTLS LSC Status
Certificate status : Available
LSC fallback status : No
Issuer certificate hash : 611255bc69f565af537be59297f453593e432e1b
Certificate expiry time : 09/25/2024 06:48:23
AP 802.1x LSC Status
Certificate status : Available
Issuer certificate hash : 611255bc69f565af537be59297f453593e432e1b
Certificate expiry time : 09/25/2024 06:48:23
AP LSC authentication state : CAPWAP-DTLS and 802.1x authentication
```

ةحجانلا ةقداصم ال دعب Switchport ةهجاو ةلحاج

```
Switch#sho authentication sessions interface gigabitEthernet 1/0/2
Interface MAC Address Method Domain Status Fg Session ID
Gi1/0/2 0cd0.f89a.46e0 dot1x DATA Auth 9765690A0000005CCEED0FBF
```

ةحجان ةقداصم ال ريشت لوصولا ةطقن مكحت ةدحو تالجس نم ةنيح هذه

```
[*09/26/2023 07:33:57.5512] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.5513] hostapd:EAP: Status notification: started (param=)
[*09/26/2023 07:33:57.5513] hostapd:EAP: EAP-Request Identity
[*09/26/2023 07:33:57.5633] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.5634] hostapd:EAP: Status notification: accept proposed method (param=TLS)
[*09/26/2023 07:33:57.5673] hostapd:dot1x: CTRL-EVENT-EAP-METHOD EAP vendor 0 method 13 (TLS) selected
[*09/26/2023 07:33:57.5907] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.5977] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6045] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6126] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6137] hostapd:dot1x: CTRL-EVENT-EAP-PEER-CERT depth=1 subject='/DC=com/DC=tac-lab
[*09/26/2023 07:33:57.6145] hostapd:dot1x: CTRL-EVENT-EAP-PEER-CERT depth=0 subject='/C=IN/ST=KA/L=BLR/
[*09/26/2023 07:33:57.6151] hostapd:EAP: Status notification: remote certificate verification (param=su
[*09/26/2023 07:33:57.6539] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6601] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6773] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.7812] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.7812] hostapd:EAP: Status notification: completion (param=success)
[*09/26/2023 07:33:57.7812] hostapd:dot1x: CTRL-EVENT-EAP-SUCCESS EAP authentication completed successf
[*09/26/2023 07:33:57.7813] hostapd:dot1x: State: ASSOCIATED -> COMPLETED
[*09/26/2023 07:33:57.7813] hostapd:dot1x: CTRL-EVENT-CONNECTED - Connection to 01:80:c2:00:00:03 compl
```


اه حال ص او 802.1X ة ق داصم عاطخا فاشك تسأ

ة حجانلا ة ق داصم ل نم ع ج ي لي امي ف . RADIUS ة ق داصم نم ق قحت و AP ة ل ص و ي ل ع PCAP ذخ

479..	07:47:17.192983	Cisco_9a:46:e0	Nearest-non-TP..	EAP			Response, Identity(Packet size limited during capture)
479..	07:47:17.200205	10.100.34.170	10.100.101.151	RADIUS	1812	55431	Access-Challenge id=251
479..	07:47:17.205983	Cisco_9a:46:e0	Nearest-non-TP..	TLV1.2			Encrypted Handshake Message
479..	07:47:17.210904	10.100.34.170	10.100.101.151	RADIUS	1812	55431	Access-Challenge id=244
479..	07:47:17.216975	Cisco_9a:46:e0	Nearest-non-TP..	EAP			Response, TLS EAP (EAP-TLS)(Packet size limited during capture)
479..	07:47:17.220975	10.100.34.170	10.100.101.151	RADIUS	1812	55431	Access-Challenge id=240
479..	07:47:17.227976	Cisco_9a:46:e0	Nearest-non-TP..	EAP			Response, TLS EAP (EAP-TLS)(Packet size limited during capture)
479..	07:47:17.274979	Cisco_9a:46:e0	Nearest-non-TP..	EAP			Response, TLS EAP (EAP-TLS)(Packet size limited during capture)
479..	07:47:17.277982	10.100.34.170	10.100.101.151	RADIUS	1812	55431	Access-Challenge id=247
479..	07:47:17.311988	Cisco_9a:46:e0	Nearest-non-TP..	EAP			Response, TLS EAP (EAP-TLS)
479..	07:47:17.314974	10.100.34.170	10.100.101.151	RADIUS	1812	55431	Access-Challenge id=246
479..	07:47:17.318968	Cisco_9a:46:e0	Nearest-non-TP..	EAP			Response, TLS EAP (EAP-TLS)
479..	07:47:17.322976	10.100.34.170	10.100.101.151	RADIUS	1812	55431	Access-Challenge id=248
479..	07:47:17.324988	Cisco_9a:46:e0	Nearest-non-TP..	TLV1.2			Encrypted Handshake Message, Encrypted Handshake Message, Encrypted Handshake Message, Change Cipher Spec, Encrypted Handshake Message
479..	07:47:17.342969	Cisco_9a:46:e0	Nearest-non-TP..	EAP			Response, TLS EAP (EAP-TLS)(Packet size limited during capture)
479..	07:47:17.378979	10.100.34.170	10.100.101.151	RADIUS	1812	55431	Access-Accept id=251

ة ق داصم ل طاق ت ل ال ISE نم TCPdump ع م ج ي

80	07:47:18.177107	10.100.34.170	10.100.101.151	RADIUS	1812	55431	Access-Challenge id=245
87	07:47:18.177802	10.100.34.170	10.100.101.151	RADIUS	1812	55431	Access-Request id=244
88	07:47:18.182802	10.100.34.170	10.100.101.151	RADIUS	1812	55431	Access-Challenge id=244
89	07:47:18.183000	10.100.34.170	10.100.101.151	RADIUS	1812	55431	Access-Request id=240
90	07:47:18.183983	10.100.34.170	10.100.101.151	RADIUS	1812	55431	Access-Challenge id=240
91	07:47:18.184000	10.100.34.170	10.100.101.151	RADIUS	1812	55431	Access-Request id=240
92	07:47:18.184012	10.100.34.170	10.100.101.151	RADIUS	1812	55431	Access-Challenge id=240
93	07:47:18.184018	10.100.34.170	10.100.101.151	RADIUS	1812	55431	Access-Request id=247
94	07:47:18.184022	10.100.34.170	10.100.101.151	RADIUS	1812	55431	Access-Challenge id=247
95	07:47:18.184028	10.100.34.170	10.100.101.151	RADIUS	1812	55431	Access-Challenge id=248
96	07:47:18.184037	10.100.34.170	10.100.101.151	RADIUS	1812	55431	Access-Challenge id=248
97	07:47:18.184040	10.100.34.170	10.100.101.151	RADIUS	1812	55431	Access-Request id=248
98	07:47:18.184050	10.100.34.170	10.100.101.151	RADIUS	1812	55431	Access-Challenge id=248
99	07:47:18.184058	10.100.34.170	10.100.101.151	RADIUS	1812	55431	Access-Request id=251
82	07:47:01.945978	10.100.34.170	10.100.101.151	RADIUS	1812	55431	Access-Accept id=251

نم نم ازتم لك شب مزجل طاق ت ل مز ل ي س ف ، ة ق داصم ل ا ن ث ا ط ح ال ت ة لك شم ك ان ه ت ن ا ك ا ذ ا ISE ب ن ا ج و ة ي ك ل س ل ال AP ة ل ص و

ال AP ل عاطخا ل ا ج ي ح ص ت رم ا

```
#debug ap authentication packet
```

ة ل ص ت ا ذ ت ا م و ل ع م

- [Cisco نم ت ال ي ز ن ت ل ا و ي ن ق ت ل ا م ع د ل ا](#)
- [AireOS م ا د خ ت س ا ب ال AP ل ع 802.1X ن ي و ك ت](#)
- [LSC ل 9800 ن ي و ك ت ل ا ل ي ل د](#)
- [LSC ل ل ا ث م ل ي ك ش ت](#)
- [9800 ل ع ل و ص و ل ا ط ا ق ن ل 802.1X ن ي و ك ت](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذه Cisco تچرت
ملاعلاء انءمچ يف نيمدختسمل معدى وتحم مي دقتل ةيرشبلاو
امك ةقيد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچرئ. ةصاغل مهتغب
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه
ىل إامئاد ةوچرلاب يصوت وتامچرتل هذه ةقد نع اهتيلوئسم Cisco
Systems (رفوتم طبارل) يلصلأل يزلچنل دن تسمل