

ةيهمهألا تاذ تاداهشلا دادم إل SCEP نيوكت 9800 WLC

تاي وتحمل

ةمدقملا

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكمل](#)

[ةيساسأتامولعم](#)

[نيوكتل](#)

[ةكبشلل يطي طختلا مس رلا](#)

[مداخن يف SCEP تامدخ نيكمت Windows](#)

[ليجست يدحت رورم قملك تابلطتم ليطبع SCEP](#)

[اهليجست و ظاهشلا بلاق نيوكت](#)

[TrustPoint زاهجل 9800 نيوكت](#)

[قرادال ل ثيدحت ولوصولا ظقون ليجست تاملعم ديدهت TrustPoint](#)

[ةحصلا نم ققحتلا](#)

[مكحتلا ةدحو ظاهش تيبثت نم ققحتلا](#)

[9800 WLC LSC نيوكت نم ققحتلا](#)

[لوصلولا ظقون ظاهش تيبثت نم ققحتلا](#)

[اهمالص او عاطخألا فاشكتسا](#)

[ةعياشلا تالكشملا](#)

[لجرسل او عاطخألا حيحصت رماوا](#)

[ةحجان ليجست قلوا حم ئيلع لاثم](#)

ةمدقملا

ةيكلساللا ةيلحمل ةكبشلا يف مكحتلا ةدحو نيوكت ةيفيك دنتسملا اذه حضوي نم مامضنالا ضارغل (AP) لوصلولا ظقونل (LSC) ايلاح ظمهالا ظاهشلا ليجستل 9800 زارت ظاهشلا ليجست لوكوتورب و (NDES Microsoft) ةكبش ةزهجأ ليجست ةمدخ تازيم لالخ يسيقلala Windows Server 2012 R2 طيسبلala.

ةيساسألا تابلطتملا

ةكبشلا يف مكحتلا رصنع يفوتست نأ بجي Windows Server، عاجنب يفوتست ئارجا لجأ نم ةيلاتلا تابلطتملا 9800 زارت (WLC) ةيكلساللا ةيلحمل:

- مداخل او مكحتلا ةدحو نيب لوصلولا ةيناكما رفوت بجي.
- ةقطنملاو خيراتلا سفن ةكراشم وأ ، مداخ سفن ع ةدحو ةنمازم مرت.
- ةطقن نإف ، لوصلولا ظقون نم تقولا او CA مداخ نيب افلتخم تقولا ناك اذا) ةينمزلا (اهتيبيثتو ظاهشلا ةحص نم ققحتلا يف للكاشم اهب لوصلولا.
- اهنيكمت مت يتلا (IIS) تمنرتنالا تامولعم تامدخ ئيلع Windows Server يوتحي نأ بجي اقبسم.

تابل طتملا

تاي نقطلا هذهب ةفرعم كيدل نوكـت نـأب Cisco يصوت

- 9800 Wireless LAN Controller، رادصـلا 16.10.1.
- Microsoft Windows Server 2012 Standard.
- تـاداهـشـلـاـوـ (PKI) صـاخـلـاـ حـاتـفـمـلـلـ ةـيـسـاسـأـلـاـ ةـيـنـبـلـاـ.

ةـمـدـخـتـسـمـلـاـ تـانـوـكـمـلـاـ

ـيـلـاتـلـاـ ةـيـدـامـلـاـ تـانـوـكـمـلـاـ وـجـمـارـبـلـاـ تـارـادـصـاـ ـىـلـاـ دـنـتـسـمـلـاـ اـذـهـ يـفـ ةـدـرـاـوـلـاـ تـامـوـلـعـمـلـاـ دـنـتـسـتـ

- 17.2.1. رادصـلا 9800-L WLC، جـمـانـربـاـ.
- Windows Server 2012 Standard R2.
- لـوـصـوـلـاـ طـاقـنـاـ 3802.

ـيـدـحـتـلـاـ هـجـوـ ـىـلـعـ WLC SCEP وـهـ دـنـتـسـمـلـاـ اـذـهـ يـفـ مـدـاـخـلـلـ يـبـنـاجـلـاـ نـيـوـكـتـلـاـ نـإـ:ـظـاحـالـمـ
ـىـلـاـ عـوـجـرـلـاـ يـجـرـيـ .ـتـادـاهـشـوـ ـةـنـمـآـوـ ـةـزـعـمـ مـدـاـخـلـلـ ةـيـفـاـضـاـ تـانـيـوـكـتـلـاـ ـىـلـعـ لـوـصـحـلـلـ
Microsoft TechNet.

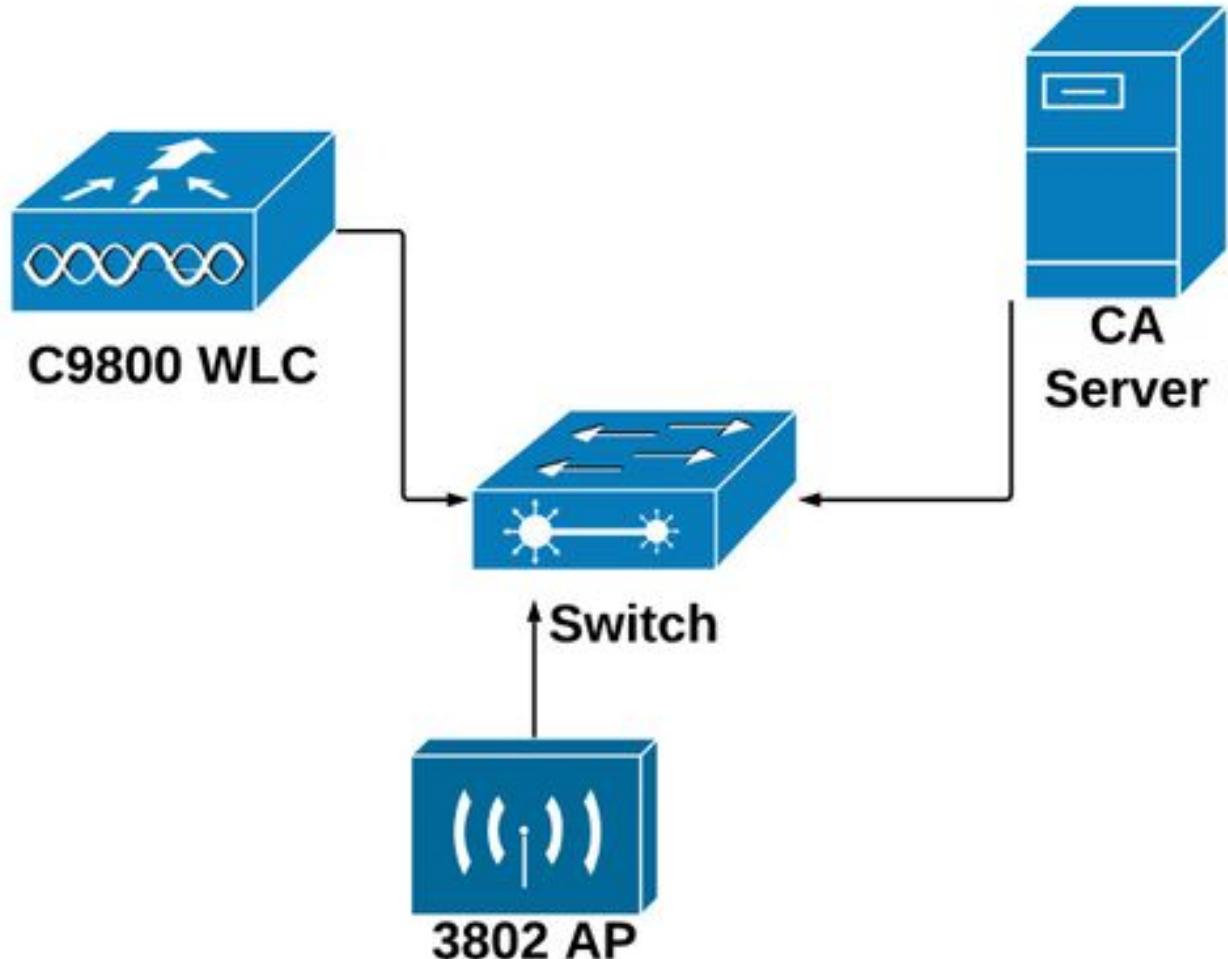
ةـيـسـاسـأـ تـامـوـلـعـمـ

ـقـدـصـمـلـاـ عـجـرـمـلـابـ ةـصـاخـلـاـ رـذـجـلـاـ ةـدـاهـشـلـاـ نـمـ لـكـ ،ـةـدـيـدـجـلـاـ LSCـ تـادـاهـشـ تـيـبـثـتـ بـجـيـ
ـمـاـخـتـسـابـ .ـفـاطـمـلـاـ ةـيـاهـنـ يـفـ لـوـصـوـلـاـ طـاقـنـاـ يـفـ اـهـلـيـزـنـتـلـ مـكـحـتـلـاـ ـدـحـوـ ـىـلـعـ ،ـزـاهـجـلـاـ ةـدـاهـشـ وـ
ـدـحـوـ يـفـ اـيـئـاـقـلـتـ اـقـحـاـلـ اـهـتـيـبـثـتـ مـتـيـوـ ،ـCـAـ مـدـاـخـ نـمـ زـاهـجـلـاـ تـادـاهـشـ وـCـAـ مـاـلـتـسـاـ مـتـيـوـ
ـمـكـحـتـلـاـ.

ـيـفـ مـكـحـتـلـاـ مـئـاوـقـعـمـ لـوـصـوـلـاـ طـاقـنـاـ رـيـفـوـتـ مـتـيـ اـمـدـنـعـ اـهـسـفـنـ دـامـتـعـاـلـاـ ةـيـلـمـعـ ـثـدـحـتـ
ـىـلـعـ لـوـصـحـلـاـ يـفـ دـعـاـسـتـوـ CAـ لـيـكـوـكـ مـكـحـتـلـاـ ـدـحـوـ لـمـعـتـ ،ـكـلـذـبـ مـاـيـقـلـلـ (LSCs)ـ لـوـصـوـلـاـ
ـلـوـصـوـلـاـ ةـطـقـنـلـ CAـ لـبـقـ نـمـ عـقـوـمـلـاـ (ـاـيـتـاـذـ ةـأـشـنـمـلـاـ)ـ ةـدـاهـشـلـاـ بـلـطـ.

نـيـوـكـتـلـاـ

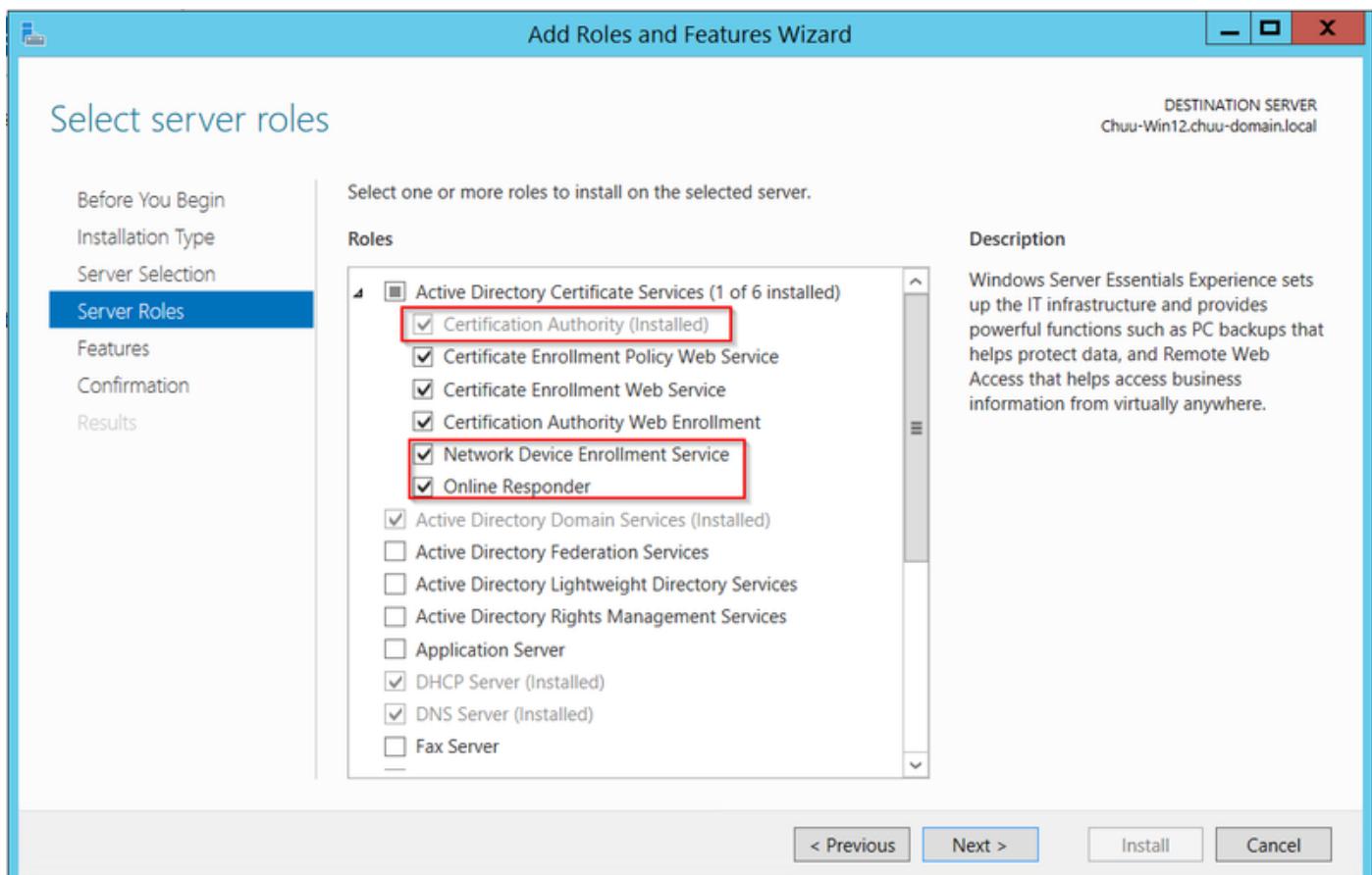
ةـكـبـشـلـلـ يـطـيـطـخـتـلـاـ مـسـرـلـاـ



Windows نیکمەن داخیف SCEP تامدھە

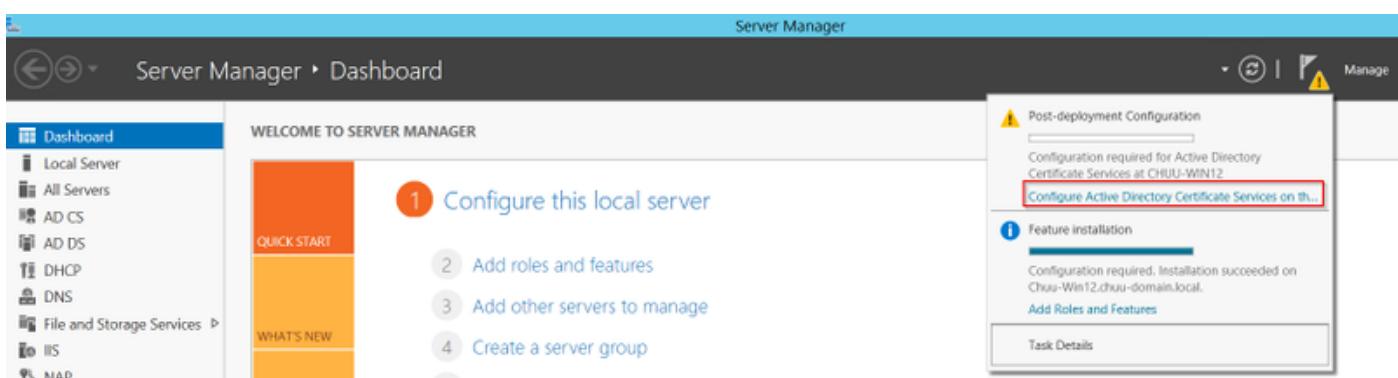
حەتھل تازىم و راودا ئەفاضى رايىخ دەھ مىث ۋەردىم ئەقلىا دەھ، مىداخلا رىدم قىبىطت يىف. 1. ۋەطخىلا لىجىستىل ھەمادختىس ام تى يىذلىا مىداخلا لىيىتم دەھ، كانه نەنم و. ئەفاضىلا رەددو تازىم نىيوكىت جىلاعەم SCEP.

بىچىتسەملەو ئەكېشلى زاھىج لىجىست ئەم دەخوقىدىصەملە عەرمەلە تازىم دىدھت نەم قىقىھت. 2. ۋەطخىلا يىلاتلىا دەھ مىث، تىنرتىن إلە رېب:



ةيلمع مدخل لـ AD CS. نـيوكـتـلـا جـلـاعـم عـاهـنـا مـثـ، نـيـتـرـمـ يـلـاتـلـا دـدـحـ 3. ـوـطـخـلـاـ جـلـاعـمـلـا قـالـغـإـلـ قـالـغـإـ دـدـحـ مـثـ، ـزـيـمـلـا تـيـبـثـ.

مـدخلـا رـيـدـمـ مـالـعـاـ "ـنـوـقـيـأـ" يـفـ رـيـذـحـتـ ـنـوـقـيـأـ رـهـظـتـ، تـيـبـثـتـلـا نـمـ عـاهـتـنـاـ درـجـمـبـ. 4. ـوـطـخـلـاـ جـلـاعـمـ ـقـمـئـاـقـ دـيـدـحـتـلـ ـهـجـوـلـاـ مـادـخـلـعـ Active Directory تـامـدـخـ نـيـوـكـتـ رـايـخـ طـابـتـرـاـ دـدـحـ وـهـدـدـ حـ نـيـوـكـتـ AD CS.



مـتـيـسـ يـتـلـاـ تـنـرـتـنـاـ رـبـعـ بـيـجـتـسـمـلـاـ رـاوـدـاـ تـامـدـخـ وـ ـكـبـشـلـاـ زـاهـجـ لـيـجـسـتـ ـمـدـخـ دـدـحـ 5. ـوـطـخـلـاـ يـلـاتـلـاـ دـدـحـ مـثـ، ـقـمـئـاـقـلـاـ يـفـ اـهـنـيـوـكـتـ.

وـأـنـمـضـمـلـاـ تـاقـيـبـطـتـلـاـ عـمـجـتـ نـيـبـ نـيـرـايـخـلـاـ نـمـ يـأـ دـدـحـ NDESـ لـ ـمـدـخـلـاـ بـاسـحـ يـفـ. 6. ـوـطـخـلـاـ يـلـاتـلـاـ دـدـحـ مـثـ، ـقـمـدـخـلـاـ بـاسـحـ.

ـعـوـمـجـمـ نـمـ عـزـجـ بـاسـحـلـاـ نـأـ نـمـ دـكـأـتـفـ، ـقـمـدـخـلـاـ بـاسـحـ نـاـكـ اـذـاـ: ـظـحـاـلـمـ IIS_IUSRS.

AD CS Configuration

Service Account for NDES

DESTINATION SERVER
Chuu-Win12.chuu-domain.local

Credentials
Role Services
Service Account for NDES
RA Information
Cryptography for NDES
CA for CES
Authentication Type for C...
Service Account for CES
Authentication Type for C...
Server Certificate
Confirmation
Progress
Results

Specify the service account

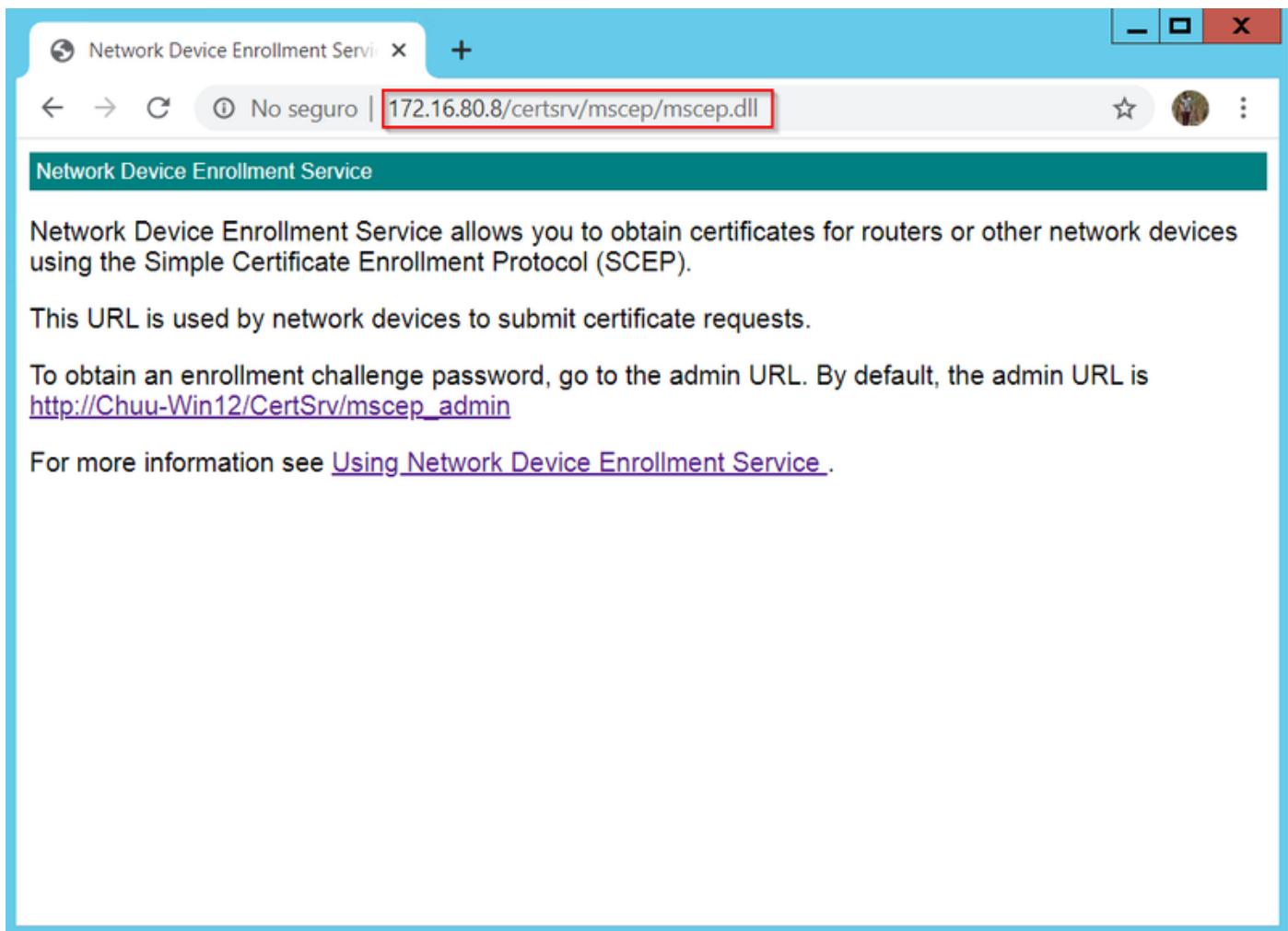
Select the identity the Network Device Enrollment Service (NDES) will use.

Specify service account (recommended)
The account must be a member of the domain and must be added to the local IIS_IUSRS group.

Use the built-in application pool identity

[More about Service Account for NDES](#)

تىېبىتلىلا دىعە. يەتىنەت تىېبىتلىلا ئېلىمكىرىتىمۇ، ئېلىاتلىلا تاشاشلىلىلىاتلىدا دەح 7. ۋەطخىل، ناونىع ئىلى لىقىتىنا. بىيەمداخ يىأعەم SCEP URL <http://<server ip>/certsrv/mscep/mscep.dll> ناونىع رفوتى.



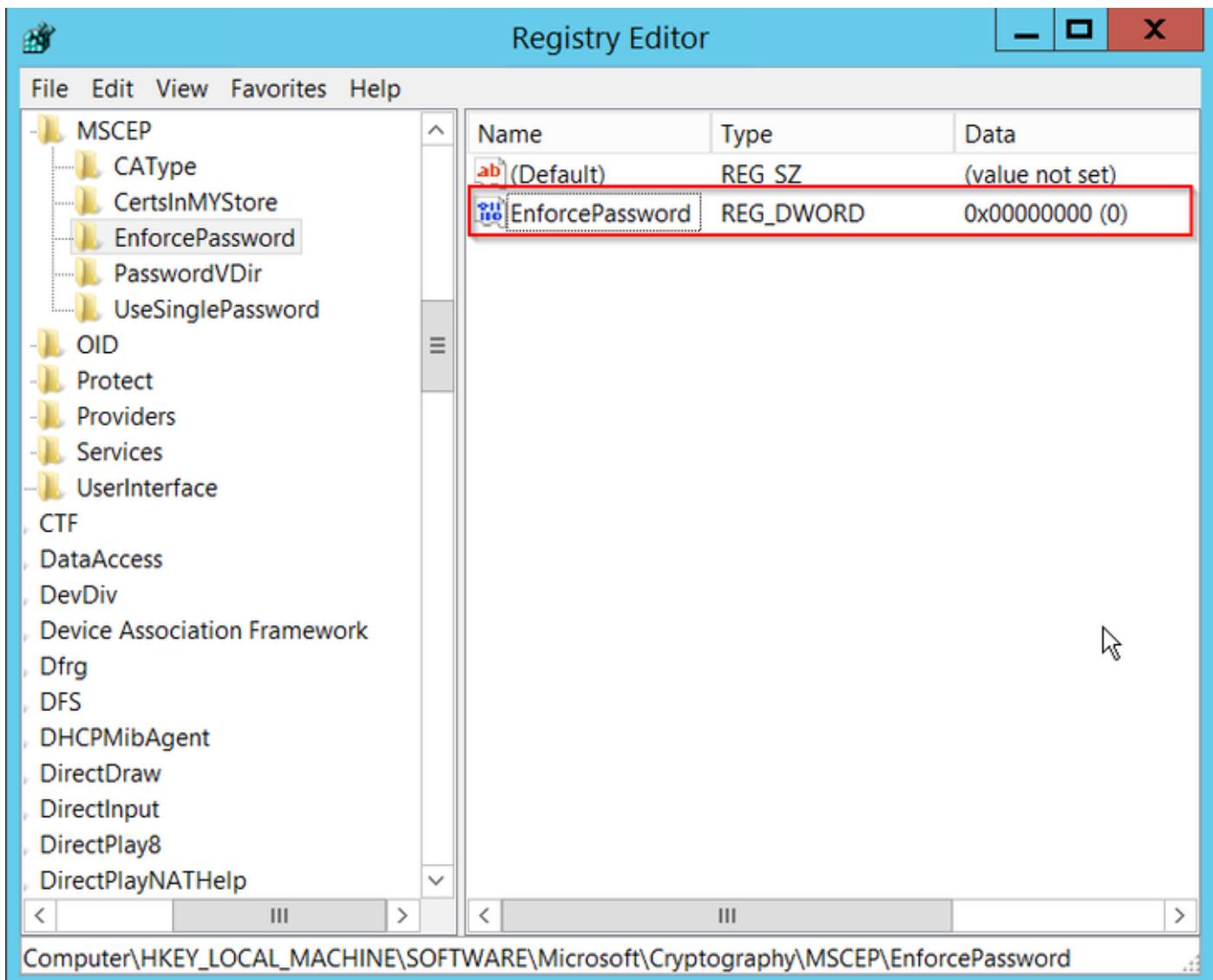
لیجسٽ یدحت رورم ۃملک تابلطتم لیطبعت

تابلط ۃقادصل "یکیمانید یدحت" رورم ۃملک Windows مداخ مدختساً، یضارتفا للكشبو باسح اذه ببلطتی. Microsoft SCEP (MSCEP) لخاد لیجستلا لباق ۃیاهنلا ۃطقنولیمعالا بسح رورم ۃملک عاشنال بیولل (GUI) ۃیموسرلا مدخلتسملما ۃھج اویلا حفصتلل لوؤسم نیمضت مکحتلا ۃدھویل عرذعتی. (بلطلا نمض رورملا ۃملک نیمضت بجی) بلط لکل ببلطلا لیدعٽ مزلي، ۃزملا هذه ۃلازال. مداخلالیا اهلسرت یتلاتابلطلا نمض هذه رورملا ۃملک NDES: مداخ یل ع دوجوملا لیجستلا حاتفم

أدبا ۃمائقلانمض Regedit نع ثحبا، "لیجستلا ریحٽ" حتفا 1. ۃوطخلالا

ریفشت > جمانرب > Microsoft > HKEY_LOCAL_MACHINE > MSCEP > EnforcementPassword > رتویبمکلا یل ا لقتنا 2. ۃوطخلالا

امک اهکرتاف، لعفلاب 0 تناناک اذإ 0. یل ا EnforcementPassword ۃمیق رییغتب مق 3. ۃوطخلالا ی.



اهليجست و ئاداھشلا بلاق نېوكت

ضارغآل ئەدۇتەم تاھويرانىس يف اھب ئەنرتقىملە حىتافمىل او تاداھشلا مادختسا نكىمىي جەن نىزخت مەتى. قىدىمىلە عجرمىلە مداخ لخاد قىبىطتلە جەن ۋەتساوب اھدىحەت مەت ئەفلىتەخەم لقىحلا اذە ليلىخت مەتى. ئاداھشلىل (EKU) عسومىلە حاتفەملە مادختسا لقىح يف قىبىطتلە نم دكأتلىل. ھنم دوصقىملە ضرغلل لىيمۇلە لېقىن نم ھمادختسا نم ۋەققىحتىلىل قىدىمىلە ۋەتساوب بىسانملا ئاداھشلا بلاق ئاشناب مۇق، WLC و AP ئاداھشلىل ئابسانملا قىبىطتلە ئاسايىس جەمد لىجس ئىلەن يىعىت بىمۇق و NDES:

قىدىمىلە عجرمىلە > ئيرادا تاودا > أدبا ئىلەن لقىتنىا 1. ئەوطخلە.

قوف نمياڭلا سواڭلا رزب رقنىا، قىدىمىلە عجرمىلە دلچىم ئەرجىش عىسىوت بىمۇق. 2. ئەوطخلە ئيرادا ددھو صىخىرتلىل ئادلەنلىق تادلەنلىق.

يىف بلاقلا راركىت ددھ مەت، نىيەمدىختىسىملا ئاداھش بلاق قوقۇم ئەنلا سواڭلا رزب رقنىا. 3. ئەوطخلە قايسىلا ۋەمىئاپ.

بىسح ئىچالىصلە ئەرتىفو بلاقلا مىسرا رىيغىت بىمۇق، ماع بىيوبتلىل ئەرمالىع ئىلەن لقىتنىا 4. ئەوطخلە دىحەت نودب ئىرخالا تارايىخلىل كىرتا، ئەبغىرلىل.

رۇزج ئاداھش ئىچالىص نم ربکا تىسىل اھنأ نم دكأت، ئىچالىصلە ئەرتىف لىيدىعەت دىنەن: رىيذەت قىدىمىلە عجرمىلە.

Properties of New Template

X

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

Template display name:

9800-LSC

Template name:

9800-LSC

Validity period:

2 years ▾

Renewal period:

6 weeks ▾

Publish certificate in Active Directory

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

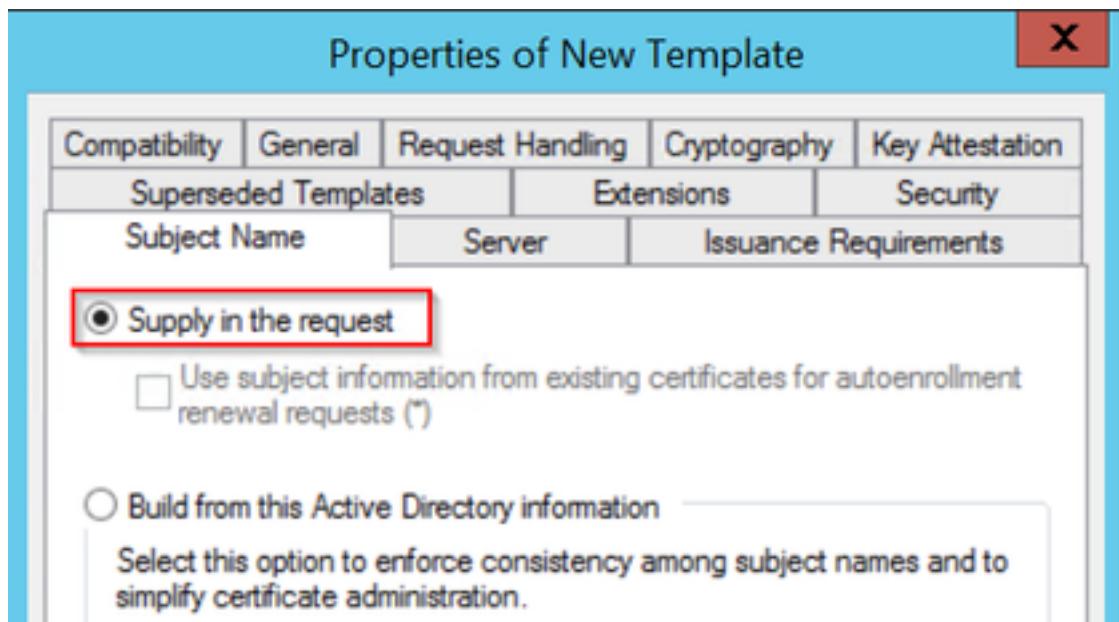
OK

Cancel

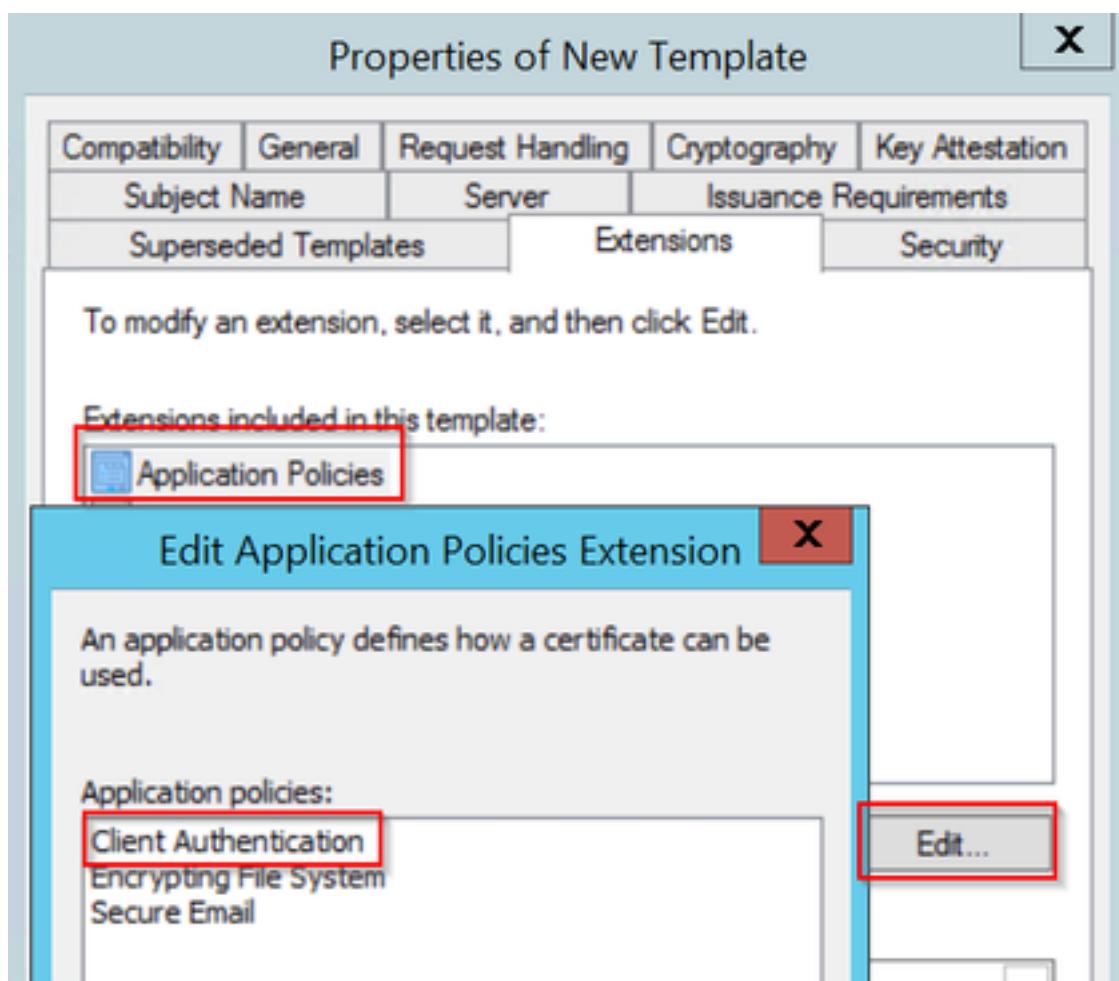
Apply

Help

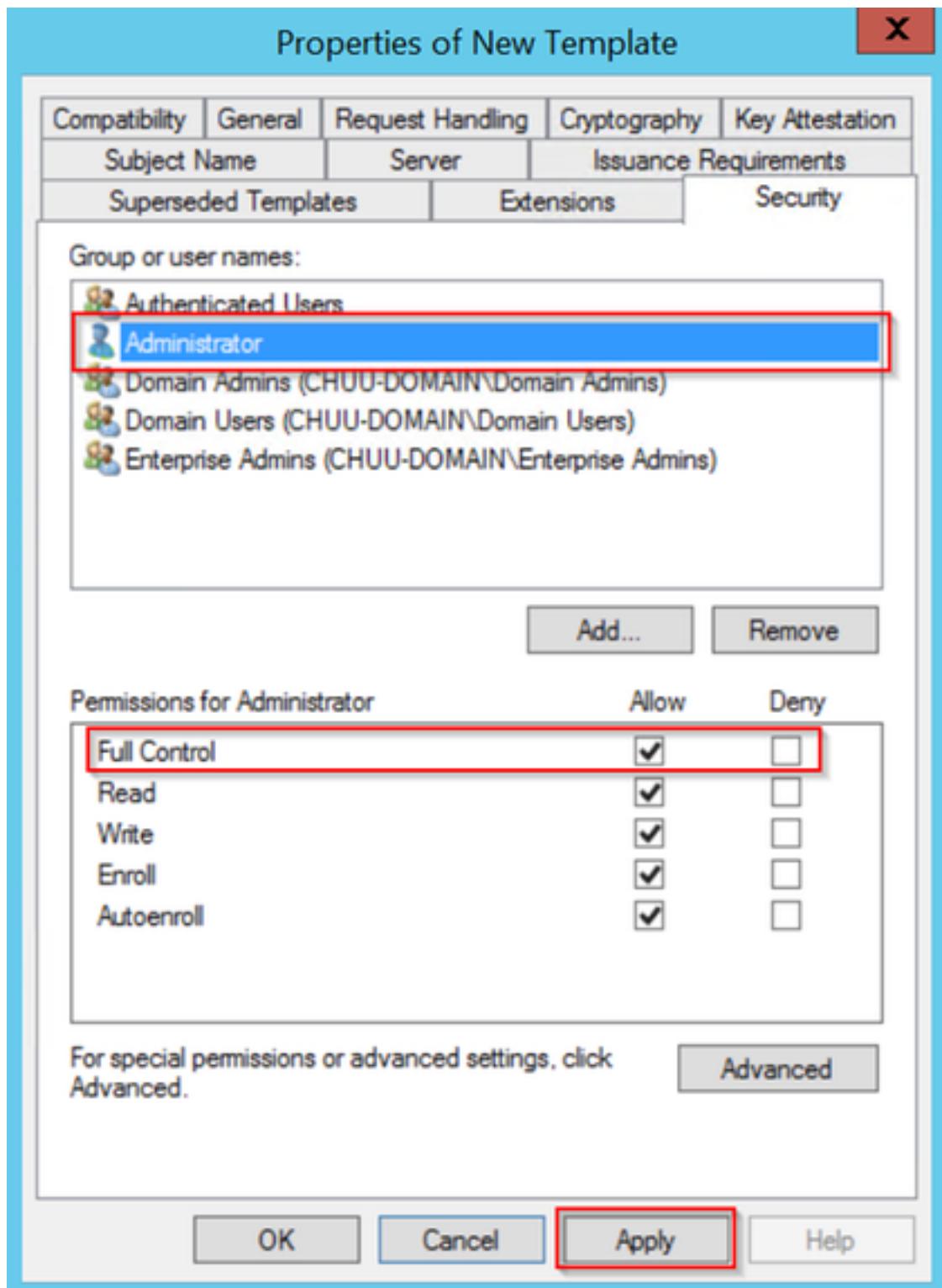
بـلـطـلـا يـف دـيـرـوـتـلـا دـيـدـحـتـ نـم دـكـأـتـو، عـوـضـوـمـلـا مـسـا بـيـوـبـتـلـا ظـمـالـعـ ىـلـا لـقـتـنـا. 5. ؤـوـطـخـلـا لـلـعـ لـوـصـحـلـلـ لـوـفـسـمـلـا ؤـقـفـاـوـمـلـا نـوـجـاتـحـيـ الـ نـيـمـدـخـتـسـمـلـا نـأـىـلـا رـيـشـيـ قـثـبـنـمـ نـأـ وـدـبـيـ قـفـاـوـمـ دـدـحـ، ؤـدـاهـشـلـا لـلـعـ مـعـهـيـقـوـتـ.



رزلـا دـدـح و تـاقـيـبـطـتـلـا جـهـنـ رـايـخـ دـدـحـ مـثـ ، تـاقـحـلـمـلـا بـيـوـبـتـلـا قـمـالـعـ إـلـا لـقـتـنـا 6. وـطـخـلـا ظـفـاضـا دـدـحـ ، إـلـاـوـ ، قـيـبـطـتـلـا تـاسـاـيـسـ ةـذـفـانـ يـفـ ةـدـوـجـوـمـ لـيـمـعـلـا ةـقـدـاصـمـ نـأـ نـمـ دـكـأـتـ ...ـرـيـحـتـ هـفـضـأـوـ.



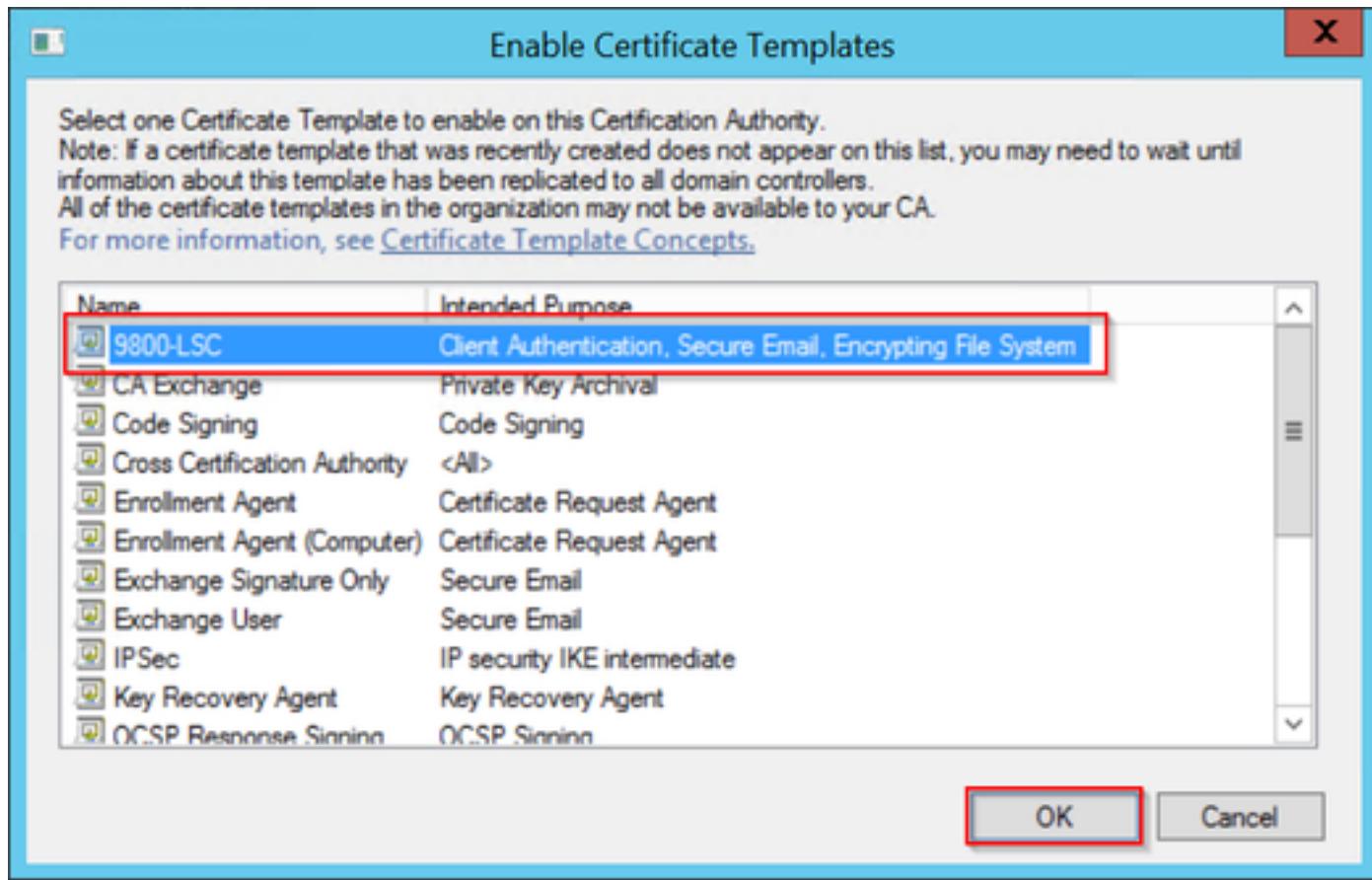
نـمـ 6 وـطـخـلـا يـفـ دـدـحـمـلـا قـمـدـخـلـا بـاـسـحـ نـأـ نـمـ دـكـأـتـوـ ، نـامـأـ بـيـوـبـتـلـا قـمـالـعـ إـلـا لـقـتـنـا 7. وـطـخـلـا مـثـ ، بـلـاـقـلـابـ ةـصـاخـلـا لـمـاـكـلـا مـكـحـتـلـا تـانـوـذـاـ هـيـدـلـ Windows Server يـفـ SCEP تـامـدـخـ نـيـكـمـتـ قـفـاـوـمـ وـقـيـبـطـتـ دـدـحـ.



بلاوق دلجملا يف نميألا سواملارزب رقناو، قدصملا عجرملما ڈفان ىلا عجرا. 8. ۋوطخلما رادصى دارملما ڈداحشلا بلاق > ديدج ددح و ڈداحشلا.

قفاوم ددح 9800-LSC لاثملا اذه يف، اقبسم ھواشنى مت يذلا ڈداحشلا بلاق ددح. 9. ۋوطخلما

يى جاردىلل لوطاً اتقىو اثىدح ھواشنى مت يذلا ڈداحشلا بلاق قرغتسىي دق: ۋوطخلما مداخىلما ڈفاك ىلۇ لىثامتمىلا خسنىلا ىلى جاتحىي ھنأىل ڈدەتەم داوخىشنى تايىلمۇ.



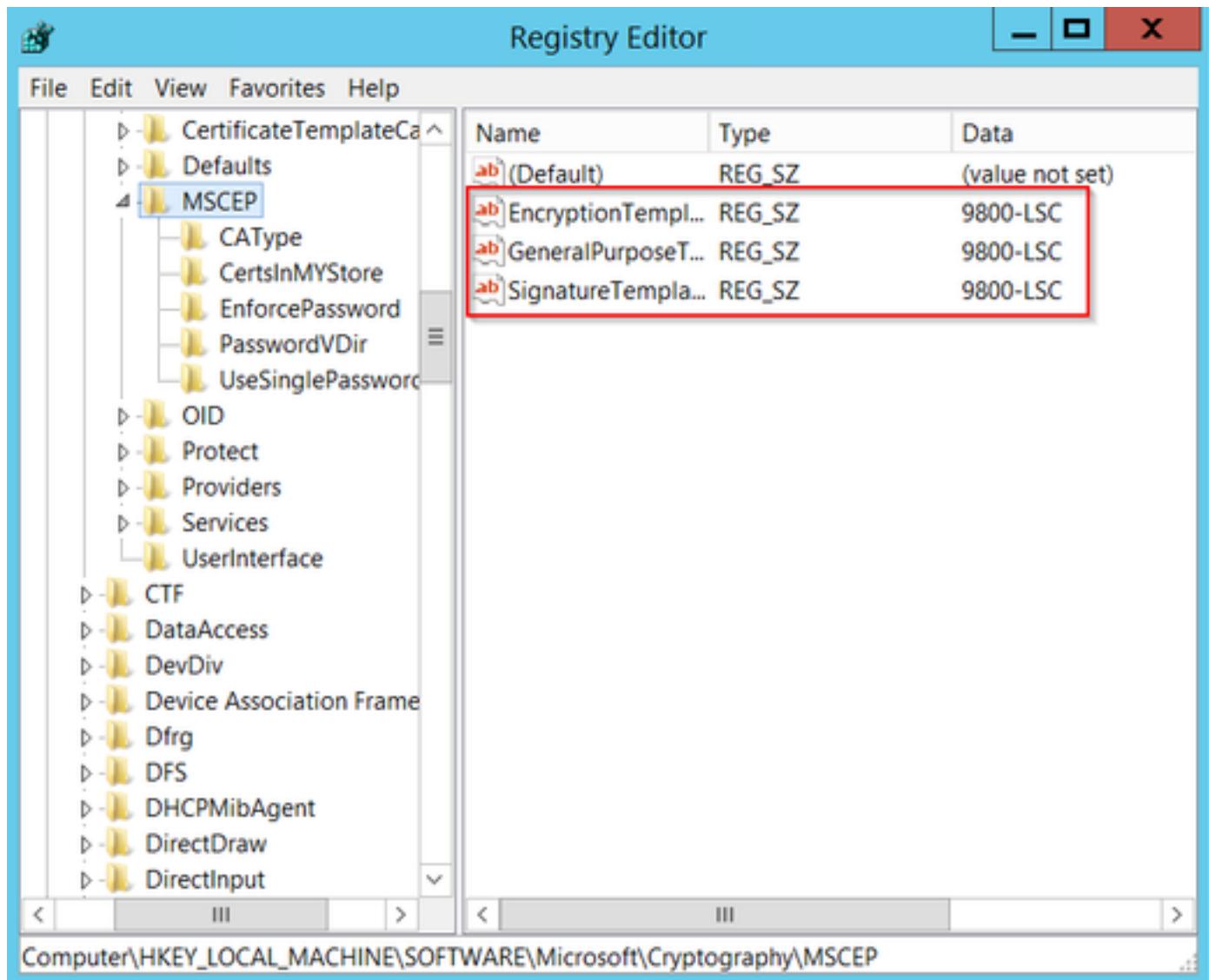
تاداهشلا بـلـاـوـق دـلـجـمـىـوـتـحـمـنـمـضـنـآـلـاـدـيـدـجـلـاـةـدـاهـشـلـاـبـلـاـقـدـرـسـمـتـيـ.

Name	Intended Purpose
9800-LSC	Client Authentication, Secure Email, En...
Authenticated Session	Client Authentication
Exchange Enrollment Agent (Offline r...)	Certificate Request Agent
IPSec (Offline request)	IP security IKE intermediate
CEP Encryption	Certificate Request Agent
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authentic...
Kerberos Authentication	Client Authentication, Server Authentic...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
Domain Controller	Client Authentication, Server Authentic...
Web Server	Server Authentication
Computer	Client Authentication, Server Authentic...
User	Encrypting File System, Secure Email, Cl...
Subordinate Certification Authority	<All>
Administrator	Microsoft Trust List Signing, Encrypting...

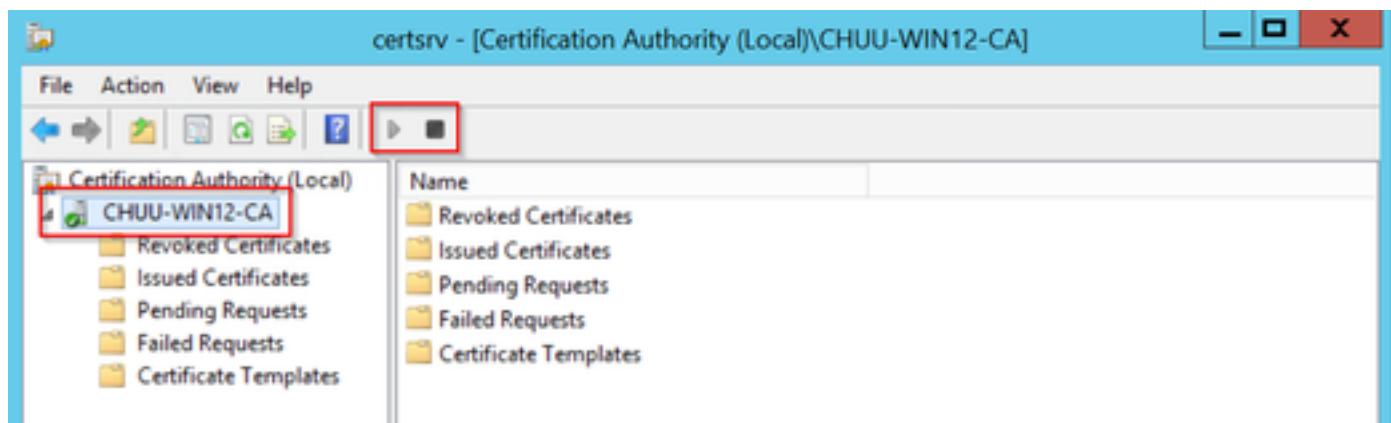
ىـلـىـلـقـتـنـأـوـلـجـسـلـاـرـحـمـةـذـفـانـىـلـاـعـجـرـاـ10ـوـطـخـلـاـComputer > HKEY_LOCAL_MACHINE >

Software > Microsoft > Cryptography > MSCEP.

تالجس ريرحتب مق. 11 ۋوطخىل EncryptionTemplate و GeneralPurposeTemplate و SignatureTemplate اثىدح هواشنى مىت يىذلا ۋداھشلى بلاقلى رىشتىچىب.



مداخلا مسا ددح و، قدصىملار عجمىلار ئەذفانلىكىنچى دىعى 12 ۋوطخىل، NDES مداخلىيغىشىت دىلەن كەلدىل، عجرا كەلدىل، حاجنب لىيغىشىتوفاقيا رىز ددح و.



زاهجىل TrustPoint 9800 نىوكت

درجهب (AP) لوصولى طاقىن ئەقادىمىل ئەفرۇم ئەققى ئەطقىن يىلۇ مەكھىتلا ددھو يوتخت نأ بېجى

لوصح لامت يتلـا CA رذج ئـدـاهـشـىـلـا ئـفـاـضـىـلـاـبـ، 9800 زـاهـجـةـدـاهـشـىـلـاـبـ نـمـصـىـتـتـ. اـهـدىـوـزـتـ يـفـ ئـدـاهـشـىـلـاـ تـيـبـثـتـ مـتـيـ يـكـلـ. (ـلـاـثـمـلـاـ اـذـهـ يـفـ CAـ Microsoft CAـ) مـدـاخـسـفـنـ نـمـ اـهـيـلـعـ مـتـيـوـ اـهـبـ ئـنـرـتـقـمـلـاـ حـيـتـافـمـ نـمـ جـوـزـعـمـ وـسـوـمـلـاـ تـامـسـ ئـلـعـ يـوـتـحـتـ نـأـ بـجـيـ، رـمـ اوـالـاـ رـطـسـ وـأـ بـيـوـلـاـ ئـهـجـاـوـلـاـ ئـلـخـ نـمـ اـمـاـ نـيـوـكـتـلـاـ ئـارـجـاـ.

حـيـتـافـمـ جـوـزـ عـاـشـنـاـ بـيـوـبـتـلـاـ ئـمـالـعـ دـدـحـوـ PKIـ ئـرـادـاـ > نـامـأـلـاـ > نـيـوـكـتـلـاـ ئـلـاـ لـقـتـنـاـ 1ـ. ئـوـطـخـلـاـ RSAـ + رـزـلـاـ دـدـحـ.

راـيـتـخـالـاـ ئـنـاـخـ دـيـدـحـتـ نـمـ دـكـأـتـوـ، حـيـتـافـمـلـاـ جـوـزـبـ ئـطـبـتـرـمـ ئـيـمـسـتـ دـيـدـحـتـبـ مـقـ. 2ـ. ئـوـطـخـلـاـ Exportableـ.

Key Label	Key Exportable	Zeroise RSA Key
TP-self-signed-1997188793	No	<input type="button" value="Zeroise"/>
AP-KEY	Yes	<input type="button" value="Zeroise"/>
chaincert.pfx	No	<input type="button" value="Zeroise"/>
TP-self-signed-1997188793.server	No	<input type="button" value="Zeroise"/>
CISCO_IDEVID_SUDI_LEGACY	No	<input type="button" value="Zeroise"/>
CISCO_IDEVID_SUDI	No	<input type="button" value="Zeroise"/>
SLA-KeyPair	Yes	<input type="button" value="Zeroise"/>
SLA-KeyPair2	Yes	<input type="button" value="Zeroise"/>

CLI ئـمـسـتـعـمـ لـاـ تـدـلـوـلـاـثـمـ لـيـكـشـتـ اـذـهـ يـفـ، 2ـ وـ 1ـ لـلـيـكـشـتـ AP-LSCـ وـ modulesـ تـبـ 2048ـ مجـ:

```
9800-L(config)#crypto key generate rsa exportable general-keys modulus
```

The name for the keys will be: AP-LSC

```
% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be exportable...
[OK] (elapsed time was 1 seconds)
```

رـزـلـاـ دـدـحـوـ بـيـوـبـتـلـاـ ئـمـالـعـ دـدـحـ، مـسـقـلـاـ سـفـنـ نـمـضـ. 3ـ. ئـوـطـخـلـاـ + Addـ.

زـاهـجـلـاـ ئـلـعـ قـيـبـطـتـ دـدـحـ مـثـ، زـاهـجـلـاـ تـامـوـلـعـمـبـ لـيـصـاـفـتـ أـلـمـاـ. 4ـ. ئـوـطـخـلـاـ

- طـبـتـرـمـلـاـ مـسـالـاـ وـ ئـيـمـسـتـلـاـ لـقـحـ trustPoint

نيـكـمـتـ نـمـ 7ـ ئـوـطـخـلـاـ يـفـ دـدـحـمـلـاـ نـاـونـعـلـاـ مـدـخـتـسـأـلـيـجـسـتـلـلـ URLـ نـاـونـعـلـاـ بـسـنـلـابـ •

SCEPـ مـدـاخـ "Windowsـ"

ئـدـاهـشـ لـيـزـنـتـ مـتـيـ ثـيـحـ بـقـدـاصـمـ رـاـيـتـخـالـاـ ئـنـاـخـ دـدـحـ CAـ

ئـدـاهـشـلـاـ بـلـطـلـ ئـمـاعـ مـسـاـ ئـاجـمـلـاـ مـسـاـ لـقـحـ عـضـوـمـتـيـ •

مـتـيـذـلـاـ حـيـتـافـمـلـاـ جـوـزـ دـدـحـ، ئـلـدـسـنـمـلـاـ ئـمـئـاـقـلـاـ رـهـظـتـوـ، حـاتـفـمـلـاـ ئـاـشـنـاـ رـاـيـتـخـالـاـ ئـنـاـخـ دـدـحـ •

2ـ ئـوـطـخـلـاـ يـفـ هـؤـاشـنـاـ

- اذه مدخلتسي .رورم ةملك بتکا ،رورم ةملک القيق رهظي ،Login TrustPoint رايي تخالا ةناخ ددج
قدصملأ عجرملأ ةداهش و زاهجلا ةداهشلأ حيتافم ليصوتل

تي بثتل تاقب طلا ةدعتم مداخلا لسالس 9800 مكحتلا ةدحو معادت ال :ريذحت LSC،
ةدحو نم ةداهشلأ تابلط ىلع عقوى يذلا وہ رذجلأ قدصملأ عجرملأ نوكی نأ بجي کل ذل
لوصلأا طاقن و مكحتلا (APs).

Add Trustpoint

Label*	9800-LSC	Enrollment URL	>certsrv/mscep/mscep.dll
Authenticate <input checked="" type="checkbox"/>			
Subject Name			
Country Code	MX	State	CDMX
Location	Juarez	Organisation	Wireless TAC
Domain Name	chuu-domain.local	Email Address	jesuherr@cisco.com
Key Generated <input checked="" type="checkbox"/> Available RSA Keypairs AP-LSC Enroll Trustpoint <input checked="" type="checkbox"/> Password <input type="password"/> ······ Re-Enter Password <input type="password"/> ······			
<input type="button" value="Cancel"/>		<input type="button" value="Apply to Device"/>	

ةعبارل او ةثلاثلأا تاوطلخلل CLI نيوكت:

متی نلف ال او LDAP، ةغایص یف عوضوملا مسا نیوکت رطس قیسنت بجي :ريذحت
مكحتلا ةدحو ةطساوب هلوبق.

```
9800-L(config)#crypto pki trustpoint
```

```
9800-L(ca-trustpoint)#enrollment url http://
```

```
9800-L(ca-trustpoint)#subject-name C=
```

```
9800-L(ca-trustpoint)#rsakeypair
```

```
9800-L(ca-trustpoint)#revocation-check none
```

```
9800-L(ca-trustpoint)#exit
```

```
9800-L(config)#crypto pki authenticate
```

Certificate has the following attributes:

```
    Fingerprint MD5: E630EAE6 FB824658 690EB0F5 638D7224
```

```
    Fingerprint SHA1: 97070ACD CAD03D5D 0C1A6085 19992E0D 6B8C4D8B
```

```
% Do you accept this certificate? [yes/no]: yes
```

Trustpoint CA certificate accepted.

```
9800-L(config)#crypto pki enroll <trustpoint name>
```

```
%
```

```
% 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:

Re-enter password:

```
% The subject name in the certificate will include: C=MX, ST=CDMX, L=Juarez, O=Wireless TAC,  
CN=9800-L.chuu-domain.local/emailAddress=jesuherr@cisco.com
```

```
% The subject name in the certificate will include: 9800-L.alzavala.local
```

```
% Include the router serial number in the subject name? [yes/no]: no
```

```
% 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 AP-LSC' command will show the fingerprint.
```

ةرادل TrustPoint لوصول اطقن ليجست تاملمع ديدحت

ليصافت ديدحت اقبسم ڏدجملا TrustPoint ليصافت لوصول اطقن ليجست مدخلتسى مكحتلما ڏدحو نا امب. اهيلما ڏداهشلا بلط هيچوت ڏداعاب مكحتلما ڏدحو موقت یتلا مداخلا عوضوملا تاملمع ملعيلىع نوکت نا یلما جاتحت اهناف، ڏداهشلا ليجستل ليکوك مدخلتسى رمأولا رطس وأ بيوولا ڦهجاولالخ نم اما نيوکتلما عارجا متیو. ڏداهشلا بلط یف ڦنمضم ملا.

ريفوتو ڦمياق عسو ولوصول اطقن > يكلسال < نيوکتلما یلما لقتنا 1. ڦوطخلما

لوصول اطقن ڏداهش تابلط یف ڦيئبعملما تامسلاب عوضوملا مسا تاملمع الـ 2. ڦوطخلما ڦيڪبطت ددھ مث.

Subject Name Parameters

Country	MX
State	CDMX
City	Juarez
Organisation	Cisco TAC
Department	Wireless TAC
Email Address	jesuherr@cisco.com

Apply

CLI steps 1 و 2:

```
9800-L(config)#ap lsc-provision subject-name-parameter country
```

امارت حا دلبلالا زمر لثم نيفرحب ةديقملاءوضوملا مسا تاملمع مارتحا بجي: ظحالم
ةحص نم ققحتي ال 9800 ةيكليساللا ةيلحملاءكبشلا يف مكحتلارصنعن نآل اقيقد
تامسلا هذه.
عجرمك [CSCvo72999](#) لللخلا عجار تامولعملانم ديزمل.

ددج و، ئلدسنملاءقمي اقلالا نم اقبسم ةددمحملاءTrustPoint ددج، ئقمي اقلالا سفن نمض. **3. ۋوطخلالا**
مدىختىت نأ لباق مامضنالا تالواجم ددع ددحي اذه) لوصولاءطقن طبرتالواجم ددع
قىبطةت قوف رقنا، كلذ دعب. ئداهشلا حاتفم مجح نىييعتب مقو، (ىرخأ ئرم نوفوركيمىملا

Status	Disabled	Subject Name Parameters	Apply
Trustpoint Name	AP-LSC	Country	MX
Number of Join Attempts	10	State	CDMX
Key Size	2048	City	Juarez
Add APs to LSC Provision List		Organization	Cisco TAC

CLI steps 3:

```
9800-L(config)#ap lsc-provision join-attempt
```

```
9800-L(config)#ap lsc-provision trustpoint
```

```
9800-L(config)#ap lsc-provision key-size
```

ةدحو ىلإ ةمضنملا لوصولا طاقن عيمجل AP LSC دادع ا ليغشت نكمي (يرايتخا). **4. ووطخلا**، ةمئاقلا سفن نمض. MAC نيوانع ةمئاق يف ةفرعم ةنيعم لوصو طاقن ىلأ وأ ،مكحتلا .ةمئاق + ةقطق طولاجم صنلا يف xxx.xxxx.xxxx قيسنت يف ناوونع كام تينرثا AP لـ تلخد فلملا ددحو ،لوصولا ةطقنل MAC نيوانع ىلع يوتحي csv فلم ليمحتب مق ،كلذ نم الدب .**فلملا ليمحت ددح مث**.

ةمئاق نم هيلع فرعتي ال CSV فلم يف MAC ناوونع يأ مكحتلا زاهج ئطختي :**ةظحالم بـ ةطبترملـ لوصولا طاقن**.

Add APs to LSC Provision List

Select File

Select CSV File

Upload File

AP MAC Address

+

APs in Provision List :

1	
286f.7fcf.53ac	✖

CLI 4: ووطخـ لـ ليـ كـ شـ تـ

```
9800-L(config)#ap lsc-provision mac-address
```

مث ٥ لاحل ا ئيمس ت ٽرواجمل ا ٽلسنمل ا ٽمه اق و انيكمت ددح . ٥ ٽوطخل ا
ليجست ليغشت قيبطت قوف رقنا AP LSC.

تيبيثت متي نا ام .اهتيبيثت و اهليزن ت و ٽدادهش للا بـلـط أدـبـتـ لـوصـولـاـ طـاقـنـ :ـٽـظـاحـالـمـ
ـٽـداـهـشـلـابـ طـبـرـلـاـ ـٽـيـلـمـعـ أـدـبـتـ وـ دـيـهـمـتـ دـيـعـتـ لـوـصـولـاـ ـٽـطـقـنـ نـافـ ،ـلـمـاـكـلـابـ ـٽـداـهـشـلـاـ
ـٽـدـيـدـجـلـاـ.

عـمـ اـهـمـ اـدـخـتـسـ اـمـتـيـ قـبـسـمـلـاـ جـاتـنـاـلـلـ مـكـحـتـ ـٽـدـحـوـلـاـلـخـ نـمـ AP LSC رـيـفـوـتـ مـتـ اـذـاـ حـيـمـلـتـ
ـلـاوـ ،ـاـذـهـ مـتـ نـاـ .ـٽـدـادـهـشـلـاـ رـيـفـوـتـ درـجـمـبـ AP تـالـاخـدـاـ ـٽـلـاـزـابـ مـقـتـ الـفـ ،ـرـيـفـوـتـلـاـ ـٽـمـهـ اـقـ
ـوـحـمـيـ تـادـاهـشـ LSC ،ـجـاتـنـاـلـاـ لـبـقـ مـكـحـتـ زـاهـجـ هـسـفـنـ لـاـ ـىـلـاـ مـامـضـنـالـاـوـ MIC ـىـلـاـ يـطاـيـتـحـاـ.



5: ٽوطخل لـيـكـشـتـ CLI:

```
9800-L(config)#ap lsc-provision
```

In Non-WLANCC mode APs will be provisioning with RSA certificates with specified key-size configuration. In WLANCC mode APs will be provisioning with EC certificates with a 384 bit key by-default or 256 bit key if configured.

Are you sure you want to continue? (y/n): y If specific AP list provisioning is preferred then use: 9800-L(config)#ap lsc-provision provision-list

ددـحـ لـقـحـ يـفـ .ـٽـرـادـاـلـاـ ـٽـهـجـاـوـ دـدـحـوـ يـكـلـسـاـلـ >ـٽـيـوـكـتـ ـىـلـاـ لـقـتـنـاـ 6. ٽوطخل
ـزـاهـجـلـاـ ـىـلـعـ قـيـبـطـتـوـ ثـيـدـحـتـ قـوـفـ رـقـنـاـوـ ـٽـلـسـنـمـلـاـ ـٽـمـهـ اـقـلـاـ نـمـ دـيـدـجـلـاـ.

ـمـاـمـضـنـالـاـ تـالـواـحـمـلـ مـهـنـيـوـكـتـ مـتـ يـذـلـاـ دـدـعـلـلـ LSC ـىـلـاـ مـامـضـنـالـاـ لـوـصـولـاـ طـاقـنـ لـواـحـتـ
ـنـأـ اـمـبـ نـأـ رـيـغـ ،ـٽـيـنـاثـ مـامـضـنـالـاـوـ MIC ـىـلـاـ ،ـٽـلـواـحـمـ يـصـقـأـلـاـ دـحـلـاـ غـلـبـيـ نـاـ
ـمـدـاـخـ مـوـقـيـ ثـيـحـ يـقـلـحـ رـارـكـتـ ـىـلـاـ يـدـؤـيـ اـذـهـوـ .ـدـيـدـجـ بـلـطـ APs ـلـاـ رـيـفـوـتـ تـنـكـ CA
ـبـلـطـ-ـطـبـرـ ـقـلـحـ يـفـ قـصـتـلـاـ APs وـ APs سـفـنـلـ رـاـرـمـتـسـابـ تـادـاهـشـلـاـ عـيـقـوـتـبـ reboot.

ـٽـاـقـنـلـ نـكـمـيـ اـلـ ،ـٽـدـادـهـشـ مـادـخـتـسـاـلـ Management TrustPoint ثـيـدـحـتـ درـجـمـبـ :ـٽـظـاحـالـمـ
ـمـعـ دـاـيـلـاـجـ دـجـوـيـ اـلـ .ـنـوـفـورـكـيـمـ مـادـخـتـسـاـبـ مـكـحـتـلـاـ ـٽـدـحـوـلـاـ ـٽـلـاـ مـامـضـنـالـاـ ـٽـدـيـدـجـلـاـ لـوـصـولـاـ
ـاـقـبـاـسـ تـدـوـزـ نـوـكـيـ نـأـ جـاتـحـيـ مـهـ ،ـدـيـدـجـ APs بـكـرـيـ نـأـ تـنـأـ جـاتـحـيـ نـاـ .ـرـيـفـوـتـ ـٽـذـفـانـ حـتـفـلـ
ـٽـطـقـنـ قـيـثـوـتـ ـرـادـاـلـاـ يـفـ دـحـاـوـلـاـ نـأـ CA هـسـفـنـ لـاـ نـمـ عـيـقـوـتـ عـمـ LSC.

Edit Management Interface

Interface	Vlan2622
Trustpoint	AP-LSC
NAT Status	DISABLED

Cancel

Update & Apply to Device

6: ۋەطخىلى لېكىشتىرۇنىڭ:

```
9800-L(config)#wireless management trustpoint
```

مەھىنە قىقىتلىرىنىڭ

مەھىنە قىقىتلىرىنىڭ تىبىتىنىڭ

9800 WLC TrustPoint show crypto pki certificates verbose <trustPoint name>, اهۋاشنى مەت يىتلە ب نىيتداھش طېرىمىتى، LSC تامولۇم دوجۇنەم قىقىتلىرىنىڭ trustPoint مەسما نوکىي، لاثىملا اذە يىف. Microsoft-ca" وە " microsoft-ca" رىفوقۇتلىرىنىڭ

طقف ةلصلأا يذ جارخ إالا:

```
9800-L#show crypto pki certificates verbose microsoft-ca
Certificate
  Status: Available
  Version: 3
  Certificate Usage: General Purpose
  Issuer:
    cn=CHUU-WIN12-CA
    dc=chuu-domain
    dc=local
  Subject:
    Name: 9800-L.alzavala.local
    cn=9800-L.chuu-domain.local/emailAddress=jesuherr@cisco.com
    o=Wireless TAC
    l=Juarez
    st=CDMX
    c=MX
    hostname=9800-L.alzavala.local
  CRL Distribution Points:
    ldap:///CN=CHUU-WIN12-CA,CN=Chuu-
    Win12,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Coint
  Validity Date:
    start date: 04:25:59 Central May 11 2020
    end date: 04:25:59 Central May 11 2022 Subject Key Info: Public Key Algorithm: rsaEncryption RSA
    Public Key: (2048 bit) Signature Algorithm: SHA256 with RSA Encryption [...] Authority Info
    Access: CA ISSUERS: ldap:///CN=CHUU-WIN12-
    CA,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=chuu-
    domain,DC=local?cACertificate?base?objectClass=certificationAuthority [...] CA Certificate
      Status: Available
      Version: 3
      Certificate Serial Number (hex): 37268ED56080CB974EF3806CCACC77EC
      Certificate Usage: Signature
      Issuer:
        cn=CHUU-WIN12-CA
        dc=chuu-domain
        dc=local
      Subject:
        cn=CHUU-WIN12-CA
        dc=chuu-domain
        dc=local
      Validity Date:
        start date: 05:58:01 Central May 10 2019
        end date: 06:08:01 Central May 10 2024 Subject Key Info: Public Key Algorithm: rsaEncryption RSA
        Public Key: (2048 bit) Signature Algorithm: SHA256 with RSA Encryption
```

نويوكـت نـم قـقـحتـلـا 9800 WLC LSC

رـمـأـلـا لـيـغـشـتـبـ مـوـقـتـ بـ لـوـحـ لـيـصـافـتـلـا نـم قـقـحتـلـلـ Wireless Management TrustPoint show يـوـتـحـتـ يـتـلـا ةـطـقـنـلـا) حـيـحـصـلـا TrustPoint نـم دـكـأـتـفـ. اـهـنـأـ يـلـعـ اـهـيـلـعـ اـهـيـلـعـ ـمـالـعـ عـضـوـمـتـيـوـ مـاـدـخـتـسـالـا دـيـقـ (ـلـاـثـمـلـا اـذـهـ يـفـ LSCـ AP-LSCـ لـيـصـافـتـ. ـةـحـاتـمـ:

```
9800-L#show wireless management trustpoint

Trustpoint Name : AP-LSC
Certificate Info : Available
Certificate Type : LSC
Certificate Hash : 9e5623adba5307facf778e6ea2f5082877ea4beb
Private key Info : Available
```

تتمت يېتل لوصول ا طاقن ۋە مىاھىق بناجىپ، AP LSC دادعا نىيوكىت لوحلىيىص افتلا نم ققحتلى نم دكأت رمألا لىغشتىب مق، ريفوتلار مىاھىقلى اهتىفاضا: حىحصىلار ريفوتلار ئەلەح راهظى:

```
9800-L#show ap lsc-provision summary
AP LSC-provisioning : Enabled for all APs
Trustpoint used for LSC-provisioning : AP-LSC
LSC Revert Count in AP reboots : 10
```

AP LSC Parameters :

```
Country : MX
State : CDMX
City : Juarez
Orgn : Cisco TAC
Dept : Wireless TAC
Email : josuvill@cisco.com
Key Size : 2048
EC Key Size : 384 bit
```

AP LSC-provision List :

```
Total number of APs in provision list: 2
```

```
Mac Addresses :
-----
xxxx.xxxx.xxxx
xxxx.xxxx.xxxx
```

لوصول ا طاقن ۋە داھش تىبىت نم ققحتلى

ةجىاو نم **show crypto** رمألا لىغشت لوصول ا طاقن يىف ئەتبىتمىلا تاداھشلى نام ققحتلى ۋە داھش و قىدىمىلار جىرمىلا رىزج ۋە داھش نم لىك دوجو نم دكأت، لوصول ا طاقنل (CLI) رمأولا رطس (طقف ئەلصلار تاذ تانايىبلالا جارخىلا ضرعى) زاھىجىلار:

```
AP3802#show crypto
[...]
----- LSC: Enabled
----- Device Certificate -----
Certificate:
Data:
    Version: 3 (0x2)
    Serial Number:
        73:00:00:00:0b:9e:c4:2e:6c:e1:54:84:96:00:00:00:00:0b
Signature Algorithm: sha256WithRSAEncryption
    Issuer: DC=local, DC=chuu-domain, CN=CHUU-WIN12-CA
    Validity
        Not Before: May 13 01:22:13 2020 GMT
        Not After : May 13 01:22:13 2022 GMT
    Subject: C=MX, ST=CDMX, L=Juarez, O=Cisco TAC, CN=ap3g3-
286F7FCF53AC/emailAddress=josuvill@cisco.com
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        Public-Key: (2048 bit)

----- Root Certificate -----
Certificate:
Data:
    Version: 3 (0x2)
    Serial Number:
```

```

32:61:fb:93:a8:0a:4a:97:42:5b:5e:32:28:29:0d:32
Signature Algorithm: sha256WithRSAEncryption
Issuer: DC=local, DC=chuu-domain, CN=CHUU-WIN12-CA
Validity
Not Before: May 10 05:58:01 2019 GMT
Not After : May 10 05:58:01 2024 GMT
Subject: DC=local, DC=chuu-domain, CN=CHUU-WIN12-CA
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)

```

تنكم نا تقاد عيطة سيا تنأ ap لانم، ةيوه وحص تلمعتسا dot1x ءانيم حاتفمل LSC نا رسيا وحص.

```
AP3802#show ap authentication status
AP dot1x feature is disabled.
```

دامتع انان اياب فيرعت مزلي، ذفنملاب لوصول ا طاقن نيكمل: **ةظحال**
هسفن لوصول ا ظقون نيكوت وأ لوصول ا ظقون فيرعت فلم يف لوصول ا طاقنل
ةفياز ميقب.

اهالص او عاطخألا فاشكتسا

ةعئاشلا تالكشملا

1. بـلـطـتـي مـداـخـلـا نـاكـ اـذـا وـأـ مـداـخـلـا لـجـسـ يـفـ حـيـحـصـ لـكـشـبـ بـلـاوـقـلـا نـيـيـعـتـ مـتـيـ مـلـ اـذـاـ هـضـفـرـ مـتـيـ لـوـصـوـلـا طـاقـنـلـ وـأـ 9800ـLـ اـمـاـ ةـدـاهـشـلـاـ بـلـطـ نـافـ،ـ رـورـمـ ةـمـلـكـ ضـارـعـاـ
 2. نـكـمـيـ اـلـ كـلـذـلـ،ـ اـضـيـأـ SCEPـ ةـمـدـخـ لـيـطـعـتـ مـتـيـ،ـ IISـ لـ ةـيـضـارـتـفـالـاـ عـقـاـوـمـلـاـ لـيـطـعـتـ مـتـ اـذـاـ ةـكـبـشـلـاـ يـفـ مـكـحـتـلـاـ رـصـنـعـ مـوـقـيـ الـوـ TrustPointـ يـفـ دـدـحـمـلـاـ URLـ نـاـوـنـعـ ىـلـاـ لـوـصـوـلـاـ
 3. ةـدـاهـشـ بـلـطـ يـأـ لـاسـرـابـ 9800ـZـارـطـ (WLC)ـ ةـيـكـلـسـالـلـاـ ةـيـلـحـمـلـاـ ةـيـلـحـمـلـاـ ةـكـبـشـلـاـ يـفـ مـكـحـتـلـاـ رـصـنـعـ وـمـداـخـلـاـ نـيـبـ تـقـوـلـاـ ةـنـمـازـمـ مـدـعـ ةـلـاحـ يـفـ
- ةـحـصـ نـمـ قـقـحـتـلـاـ لـشـفـلـ اـرـظـنـ تـادـاهـشـلـاـ تـيـبـثـتـ مـتـيـ اـلـ،ـ 9800ـZـارـطـ (WLC)ـ ةـيـكـلـسـالـلـاـ تـقـوـلـاـ

لـجـسـ او عـاطـخـأـلاـ حـيـحـصـ رـمـ اوـأـ

اهـالـصـ اوـأـ 9800ـMـكـحـتـلـاـ ةـدـحـوـ ةـدـاهـشـ لـيـجـسـتـ عـاطـخـأـ فـاشـكـتـسـالـ رـمـ اوـأـلـاـ هـذـهـ مـدـخـتـسـاـ

```
9800-L#debug crypto pki transactions
9800-L#debug crypto pki validation
9800-L#debug crypto pki scep
```

ةـيـلـاتـلـاـ رـمـ اوـأـلـاـ مـدـخـتـسـاـ،ـ اـهـالـصـ اوـأـهـتـبـقـارـمـ وـلـوـصـوـلـاـ ةـطـقـنـ لـيـجـسـتـ عـاطـخـأـ فـاشـكـتـسـالـ

```
AP3802#debug capwap client payload
AP3802#debug capwap client events
```

يف تـالـكـشـمـ اـهـبـ لـوـصـوـلـاـ ةـطـقـنـ تـنـاكـ اـذـاـ اـمـ **show logging**ـ رـهـظـيـ،ـ لـوـصـوـلـاـ ةـطـقـنـ رـمـ اوـأـ رـطـسـ نـمـ
ةـدـاهـشـلـاـ تـيـبـثـتـ مـدـعـ بـبـسـ لـوـحـ لـيـصـاـفـتـ مـدـقـيـوـ،ـ ةـدـاهـشـلـاـ تـيـبـثـتـ:

[...]

Mar 19 19:39:13 kernel: *03/19/2020 19:39:13.3429] AP has joined controller 9800-L Mar 19

```
19:39:13 kernel: 03/19/2020 19:39:13.3500] SELinux: initialized (dev mtd_inodefs, type
mtd_inodefs), not configured for labeling Mar 19 19:39:13 kernel: *03/19/2020 19:39:13.5982]
Generating a RSA private key Mar 19 19:39:14 kernel: *03/19/2020 19:39:13.5989]
..... Mar 19 19:39:15 kernel: *03/19/2020 19:39:14.4179] .. Mar 19 19:39:15
kernel: *03/19/2020 19:39:15.2952] writing new private key to '/tmp/lsc/priv_key' Mar 19
19:39:15 kernel: *03/19/2020 19:39:15.2955] ----- Mar 19 19:39:15 kernel: *03/19/2020
19:39:15.5421] cen_validate_lsc: Verification failed for certificate: Mar 19 19:39:15 kernel:
*03/19/2020 19:39:15.5421] countryName = MX Mar 19 19:39:15 kernel: *03/19/2020 19:39:15.5421]
stateOrProvinceName = CDMX Mar 19 19:39:15 kernel: *03/19/2020 19:39:15.5421] localityName =
Juarez Mar 19 19:39:15 kernel: *03/19/2020 19:39:15.5421] organizationName = cisco-tac Mar 19
19:39:15 kernel: *03/19/2020 19:39:15.5421] commonName = ap3g3- Mar 19 19:39:15 kernel:
*03/19/2020 19:39:15.5421] emailAddress = jesuherr@cisco.com Mar 19 19:39:15 kernel: *03/19/2020
19:39:15.5427] LSC certificates/key failed validation! Mar 19 19:39:15 kernel: *03/19/2020
19:39:15.5427]
```

ةحجان ليجست ۋە لاحم ئىلۇم

مكحىتلار ئەدۇن مىكىل حجغانلى ليجستلى لېپقەر كۈزىت ئەذلى ئاطخالا حىيىھىچىت نەم جىنخىملا وە اذە
اھب ئەنرتقىملا (APs) لوصۇلما طاقىن و.

رازج ئەدەش دارىتىسا CA ئىلە 9800 WLC:

```
[...]
Certificate has the following attributes: Fingerprint MD5: E630EAE6 FB824658 690EB0F5 638D7224
Fingerprint SHA1: 97070ACD CAD03D5D 0C1A6085 19992E0D 6B8C4D8B % Do you accept this certificate?
[yes/no]: yes CRYPTO_PKI_SCEP: Client sending GetCACert request CRYPTO_PKI: Sending CA
Certificate Request: GET /certsrv/mscep/mscep.dll/pkiclient.exe?operation=GetCACert&message=AP-
LSC HTTP/1.0 User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI) Host: 172.16.80.8
CRYPTO_PKI: locked trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: http connection opened
CRYPTO_PKI: Sending HTTP message CRYPTO_PKI: Reply HTTP header: HTTP/1.0 User-Agent: Mozilla/4.0
(compatible; MSIE 5.0; Cisco PKI) Host: 172.16.80.8 CRYPTO_PKI: unlocked trustpoint AP-LSC,
refcount is 0 CRYPTO_PKI: locked trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: Header length
received: 192 CRYPTO_PKI: parse content-length header. return code: (0) and content-length :
(3638) CRYPTO_PKI: Complete data arrived CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 0
CRYPTO_PKI: Reply HTTP header: HTTP/1.1 200 OK Content-Type: application/x-x509-ca-ra-cert
Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Tue, 19 May 2020 21:47:34 GMT Connection:
close Content-Length: 3638 Content-Type indicates we have received CA and RA certificates.
CRYPTO_PKI_SCEP: Client received CA and RA certificate
CRYPTO_PKI:crypto_process_ca_ra_cert(trustpoint=AP-LSC) The PKCS #7 message contains 3
certificates. CRYPTO_PKI:crypto_pkcs7_extract_ca_cert found cert CRYPTO_PKI: Bypassing SCEP
capabilities request 0 CRYPTO_PKI: transaction CRYPTO_REQ_CA_CERT completed CRYPTO_PKI: CA
certificate received. CRYPTO_PKI: CA certificate received. CRYPTO_PKI:
crypto_pki_get_cert_record_by_cert() CRYPTO_PKI: crypto_pki_authenticate_tp_cert() CRYPTO_PKI:
trustpoint AP-LSC authentication status = 0 Trustpoint CA certificate accepted.
```

رازج ليجست 9800 WLC:

```
[...]
CRYPTO_PKI: using private key AP-LSC for enrollment CRYPTO_PKI_SCEP: Client sending GetCACert
request CRYPTO_PKI: Sending CA Certificate Request: GET
/certsrv/mscep/mscep.dll/pkiclient.exe?operation=GetCACert&message=AP-LSC HTTP/1.0 User-Agent:
Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI) Host: 172.16.80.8 CRYPTO_PKI: locked trustpoint
AP-LSC, refcount is 1 CRYPTO_PKI: http connection opened CRYPTO_PKI: Sending HTTP message
CRYPTO_PKI: Reply HTTP header: HTTP/1.0 User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco
PKI) Host: 172.16.80.8 CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 0 CRYPTO_PKI: locked
trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: Header length received: 192 CRYPTO_PKI: parse
content-length header. return code: (0) and content-length : (3638) CRYPTO_PKI: Complete data
arrived CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 0 CRYPTO_PKI: Reply HTTP header:
HTTP/1.1 200 OK Content-Type: application/x-x509-ca-ra-cert Server: Microsoft-IIS/8.5 X-Powered-
By: ASP.NET Date: Tue, 19 May 2020 21:48:33 GMT Connection: close Content-Length: 3638 Content-
Type indicates we have received CA and RA certificates. CRYPTO_PKI_SCEP: Client received CA and
```

RA certificate CRYPTO_PKI:crypto_process_ca_ra_cert(trustpoint=AP-LSC) The PKCS #7 message contains 3 certificates. CRYPTO_PKI:crypto_pkcs7_insert_ra_certs found RA certs CRYPTO_PKI:crypto_pkcs7_insert_ra_certs found RA certs CRYPTO_PKI_SCEP: Client Sending GetCACaps request with msg = GET /certsrv/mscep/mscep.dll/pkiclient.exe?operation=GetCACaps&message=AP-LSC HTTP/1.0 User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI) Host: 172.16.80.8 CRYPTO_PKI: locked trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: http connection opened CRYPTO_PKI: Sending HTTP message CRYPTO_PKI: Reply HTTP header: HTTP/1.0 User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI) Host: 172.16.80.8 CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 0 CRYPTO_PKI: locked trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: Header length received: 171 CRYPTO_PKI: parse content-length header. return code: (0) and content-length : (34) CRYPTO_PKI: Complete data arrived CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 0 CRYPTO_PKI: Reply HTTP header: HTTP/1.1 200 OK Content-Type: text/plain Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Tue, 19 May 2020 21:48:33 GMT Connection: close Content-Length: 34 CRYPTO_PKI: HTTP header content length is 34 bytes CRYPTO_PKI_SCEP: Server returned capabilities: 92 CA_CAP_RENEWAL CA_CAP_S alz_9800(config)#HA_1 CA_CAP_SHA_256 CA_CAP_SHA_512 CRYPTO_PKI: transaction CRYPTO_REQ_CERT completed CRYPTO_PKI: status: %PKI-6-CSRFINGERPRINT: CSR Fingerprint MD5 : 9BFBA438303487562E888087168F05D4 CSR Fingerprint SHA1: 58DC7DB84C632A7307631A97A6ABCF65A3DEFEEF CRYPTO_PKI: Certificate Request Fingerprint MD5: 9BFBA438 30348756 2E888087 168F05D4 CRYPTO_PKI: Certificate Request Fingerprint SHA1: 58DC7DB8 4C632A73 07631A97 A6ABCF65 A3DEFEEF PKI:PKCS7 to issuer cn=CHUU-WIN12-CA,dc=chuu-domain,dc=local serial 18 00 00 00 38 DB 68 64 C0 52 C0 OF 0E 00 00 00 00 00 38 CRYPTO_PKI: Deleting cached key having key id 65 CRYPTO_PKI: Attempting to insert the peer's public key into cache CRYPTO_PKI:Peer's public inserted successfully with key id 66 CRYPTO_PKI: Expiring peer's cached key with key id 66 PKI: Trustpoint AP-LSC has no router cert PKI: Signing pkcs7 with AP-LSC trustpoint temp self-signed cert CRYPTO_PKI_SCEP: Client sending PKCSReq CRYPTO_PKI: locked trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: http connection opened CRYPTO_PKI: Sending HTTP message CRYPTO_PKI: Reply HTTP header: HTTP/1.0 Host: 172.16.80.8 CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 0 CRYPTO_PKI: locked trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: locked trustpoint AP-LSC, refcount is 2 CRYPTO_PKI: Header length received: 188 CRYPTO_PKI: parse content-length header. return code: (0) and content-length : (2807) CRYPTO_PKI: Complete data arrived CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: received msg of 2995 bytes CRYPTO_PKI: Reply HTTP header: HTTP/1.1 200 OK Content-Type: application/x-pki-message Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Tue, 19 May 2020 21:48:33 GMT Connection: close Content-Length: 2807 CRYPTO_PKI: Prepare global revocation service providers CRYPTO_PKI: Deleting cached key having key id 66 CRYPTO_PKI: Attempting to insert the peer's public key into cache CRYPTO_PKI:Peer's public inserted successfully with key id 67 CRYPTO_PKI: Expiring peer's cached key with key id 67 CRYPTO_PKI: Remove global revocation service providers The PKCS #7 message has 1 verified signers. signing cert: issuer cn=CHUU-WIN12-CA,dc=chuu-domain,dc=local serial 1800037A239DF5180C0672C0000037 Signed Attributes: CRYPTO_PKI_SCEP: Client received CertRep - GRANTED (AF58BA9313638026C5DC151AF474723F) CRYPTO_PKI: status = 100: certificate is granted The PKCS #7 message contains 1 certs and 0 crls. Newly-issued Router Cert: issuer=cn=CHUU-WIN12-CA,dc=chuu-domain,dc=local serial=1800043245DC93E1D943CA70000043 start date: 21:38:34 Central May 19 2020 end date: 21:38:34 Central May 19 2022 Router date: 21:48:35 Central May 19 2020 %PKI-6-CERT_INSTALL: An ID certificate has been installed under Trustpoint : AP-LSC Issuer-name : cn=CHUU-WIN12-CA,dc=chuu-domain,dc=local Subject-name : cn=9800-L.chuu-domain.local/emailAddress=jesuherr@cisco.com,o=Wireless TAC,l=Juarez,st=CDMX,c=MX,hostname=alz_9800.alzavalala.local Serial-number: 1800000043245DC93E1D943CA700000000043 End-date : 2022-05-19T21:38:34Z Received router cert from CA CRYPTO_PKI: Not adding alz_9800.alzavalala.local to subject-alt-name field because : Character allowed in the domain name. Calling pkiSendCertInstallTrap to send alert CRYPTO_PKI: All enrollment requests completed for trustpoint AP-LSC

ةدع جارخ إلأ اذه راركت متي ،مكحتلأا ةدح و بناج نم لوصولأا ةطقن ليجسٌت عاطخأ حيحصٌت جارخا ئيكلس إللأ ةيلحملأا ةكبشلا يف مكحتلأا رصبع إلأ مامضنالا متي لوصولٌةطقن لـكل تارم (WLC) زارت 9800:

[...]

CRYPTO_PKI: (A6964) Session started - identity selected (AP-LSC) CRYPTO_PKI: Doing re-auth to fetch RA certificate. CRYPTO_PKI_SCEP: Client sending GetCACert request CRYPTO_PKI: Sending CA Certificate Request: GET /certsrv/mscep/mscep.dll/pkiclient.exe?operation=GetCACert&message=AP-LSC HTTP/1.0 User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI) Host: 172.16.80.8 CRYPTO_PKI: locked trustpoint AP-LSC, refcount is 2 CRYPTO_PKI: http connection opened CRYPTO_PKI: Sending HTTP message CRYPTO_PKI: Reply HTTP header: HTTP/1.0 User-Agent: Mozilla/4.0

```

(compatible; MSIE 5.0; Cisco PKI) Host: 172.16.80.8 CRYPTO_PKI: unlocked trustpoint AP-LSC,
refcount is 1 CRYPTO_PKI: locked trustpoint AP-LSC, refcount is 2 CRYPTO_PKI: Header length
received: 192 CRYPTO_PKI: parse content-length header. return code: (0) and content-length :
(3638) CRYPTO_PKI: Complete data arrived CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 1
CRYPTO_PKI: Reply HTTP header: HTTP/1.1 200 OK Content-Type: application/x-x509-ca-ra-cert
Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Tue, 19 May 2020 21:51:03 GMT Connection:
close Content-Length: 3638 Content-Type indicates we have received CA and RA certificates.
CRYPTO_PKI_SCEP: Client received CA and RA certificate
CRYPTO_PKI:crypto_process_ca_ra_cert(trustpoint=AP-LSC) The PKCS #7 message contains 3
certificates. CRYPTO_PKI:crypto_pkcs7_insert_ra_certs found RA certs
CRYPTO_PKI:crypto_pkcs7_insert_ra_certs found RA certs CRYPTO_PKI: Capabilites already obtained
CA_CAP_RENEWAL CA_CAP_SHA_1 CA_CAP_SHA_256 CA_CAP_SHA_512 PKCS10 request is compulsory
CRYPTO_PKI: byte 2 in key usage in PKCS#10 is 0x5 May 19 21: alz_9800(config)#51:04.985:
CRYPTO_PKI: all usage CRYPTO_PKI: key_usage is 4 CRYPTO_PKI: creating trustpoint clone Proxy-AP-
LSC8 CRYPTO_PKI: Creating proxy trustpoint Proxy-AP-LSC8 CRYPTO_PKI: Proxy enrollment request
trans id = 7CBB299A2D9BC77DBB1A8716E6474C0C CRYPTO_PKI: Proxy forwading an enrollment request
CRYPTO_PKI: using private key AP-LSC for enrollment CRYPTO_PKI: Proxy send CA enrollment request
with trans id: 7CBB299A2D9BC77DBB1A8716E6474C0C CRYPTO_PKI: No need to re-auth as we have RA in
place CRYPTO_PKI: Capabilites already obtained CA_CAP_RENEWAL CA_CAP_SHA_1 CA_CAP_SHA_256
CA_CAP_SHA_512 CRYPTO_PKI: transaction CRYPTO_REQ_CERT completed CRYPTO_PKI: status: PKI:PKCS7
to issuer cn=CHUU-WIN12-CA,dc=chuu-domain,dc=local serial 18 00 00 00 38 DB 68 64 C0 52 C0 0F 0E
00 00 00 00 00 38 CRYPTO_PKI: Deleting cached key having key id 67 CRYPTO_PKI: Attempting to
insert the peer's public key into cache CRYPTO_PKI:Peer's public inserted successfully with key
id 68 CRYPTO_PKI: Expiring peer's cached key with key id 68 PKI: Trustpoint Proxy-AP-LSC8 has no
router cert and loaded PKI: Signing pkcs7 with Proxy-AP-LSC8 trustpoint temp self-signed cert
CRYPTO_PKI_SCEP: Client sending PKCSReq CRYPTO_PKI: locked trustpoint Proxy-AP-LSC8, refcount is
2 CRYPTO_PKI: http connection opened CRYPTO_PKI: Sending HTTP message CRYPTO_PKI: Reply HTTP
header: HTTP/1.0 Host: 172.16.80.8 CRYPTO_PKI: unlocked trustpoint Proxy-AP-LSC8, refcount is 1
CRYPTO_PKI: locked trustpoint Proxy-AP-LSC8, refcount is 2 CRYPTO_PKI: locked trustpoint Proxy-
AP-LSC8, refcount is 3 CRYPTO_PKI: Header length received: 188 CRYPTO_PKI: parse content-length
header. return code: (0) and content-length : (2727) CRYPTO_PKI: Complete data arrived
CRYPTO_PKI: unlocked trustpoint Proxy-AP-LSC8, refcount is 2 CRYPTO_PKI: received msg of 2915
bytes CRYPTO_PKI: Reply HTTP header: HTTP/1.1 200 OK Content-Type: application/x-pki-message
Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Tue, 19 May 2020 21:51:03 GMT Connection:
close Content-Length: 2727 CRYPTO_PKI: Prepare global revocation service providers CRYPTO_PKI:
Deleting cached key having key id 68 CRYPTO_PKI: Attempting to insert the peer's public key into
cache CRYPTO_PKI:Peer's public inserted successfully with key id 69 CRYPTO_PKI: Expiring peer's
cached key with key id 69 CRYPTO_PKI: Remove global revocation service providers The PKCS #7
message has 1 alz_9800(config)# verified signers. signing cert: issuer cn=CHUU-WIN12-CA,dc=chuu-
domain,dc=local serial 1800037A239DF5180C0672C0000037 Signed Attributes: CRYPTO_PKI_SCEP: Client
received CertRep - GRANTED (7CBB299A2D9BC77DBB1A8716E6474C0C) CRYPTO_PKI: status = 100:
certificate is granted The PKCS #7 message contains 1 certs and 0 crls. Received router cert
from CA CRYPTO_PKI: Enrollment poroxy callback status: CERT_REQ_GRANTED CRYPTO_PKI: Proxy
received router cert from CA CRYPTO_PKI: Rcvd request to end PKI session A6964. CRYPTO_PKI: PKI
session A6964 has ended. Freeing all resources. CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount
is 0 CRYPTO_PKI: Cleaning RA certificate for TP : AP-LSC CRYPTO_PKI: All enrollment requests
completed for trustpoint Proxy-AP-LSC8. CRYPTO_PKI: All enrollment requests completed for
trustpoint Proxy-AP-LSC8. CRYPTO_PKI: unlocked trustpoint Proxy-AP-LSC8, refcount is 1
CRYPTO_PKI: All enrollment requests completed for trustpoint Proxy-AP-LSC8. CRYPTO_CS: removing
trustpoint clone Proxy-AP-LSC8

```

لوصول ا Outlet بناءً على طرق لوصول ا Outlet حي حصلت جارخاً!

```

[DEC] CAPWAP_CONFIGURATION_UPDATE_REQUEST(7) seq 40 len 407
..Vendor Type: SPAM_VENDOR_ID_PAYLOAD(104) vendId 409600
...Vendor SubType: CERTIFICATE_PARAMETER_PAYLOAD(63) vendId 409600
LSC set retry number from WLC: 1

```

```

Generating a RSA private key
...
writing new private key to '/tmp/lsc/priv_key'
-----

```

```
[ENC] CAPWAP_WTP_EVENT_REQUEST(9)
...Vendor SubType: LSC_CERTIFICATE_PAYLOAD(64) Len 1135 Total 1135
[ENC] CAPWAP_CONFIGURATION_UPDATE_RESPONSE(8)
(Msg Elem Type: CAPWAP_MSGELE_RESULT_CODE(33) Len 8 Total 8
[DEC] CAPWAP_CONFIGURATION_UPDATE_REQUEST(7) seq 41 len 20
..Vendor Type: SPAM_VENDOR_ID_PAYLOAD(104) vendId 409600
...Vendor SubType: LSC_CERTIFICATE_PAYLOAD(64) vendId 409600
LSC_CERT_ENROLL_PENDING from WLC

[ENC] CAPWAP_CONFIGURATION_UPDATE_RESPONSE(8)
.Msg Elem Type: CAPWAP_MSGELE_RESULT_CODE(33) Len 8 Total 8
Received Capwap watchdog update msg.
[DEC] CAPWAP_CONFIGURATION_UPDATE_REQUEST(7) seq 42 len 1277
..Vendor Type: SPAM_VENDOR_ID_PAYLOAD(104) vendId 409600
...Vendor SubType: LSC_CERTIFICATE_PAYLOAD(64) vendId 409600
LSC_ENABLE: saving ROOT_CERT

[ENC] CAPWAP_CONFIGURATION_UPDATE_RESPONSE(8)
.Msg Elem Type: CAPWAP_MSGELE_RESULT_CODE(33) Len 8 Total 8
[DEC] CAPWAP_CONFIGURATION_UPDATE_REQUEST(7) seq 43 len 2233
..Vendor Type: SPAM_VENDOR_ID_PAYLOAD(104) vendId 409600
...Vendor SubType: LSC_CERTIFICATE_PAYLOAD(64) vendId 409600
LSC_ENABLE: saving DEVICE_CERT
```

SC private key written to hardware TAM

root: 2: LSC enabled
AP Rebooting: Reset Reason - LSC enabled
و اذه و متتخی الام نم لایخ SCEP LSC نیوکتل ایجستل.

هـ لـ وـ لـ جـ رـ تـ لـ اـ هـ ذـ هـ

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