

LSCを使用したPEAPまたはEAP-TLS用のAPでの802.1Xの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[ネットワーク図](#)

[設定](#)

[Windows Server 2016 SCEP CA](#)

[証明書テンプレートとレジストリの設定](#)

[9800でのLSCの設定](#)

[AP LSC GUIの設定手順](#)

[AP LSC CLIの設定手順](#)

[AP LSCの検証](#)

[LSCプロビジョニングのトラブルシューティング](#)

[LSCを使用したAP有線802.1X認証](#)

[AP有線802.1X認証の設定手順](#)

[APの有線802.1X認証GUI設定](#)

[APの有線802.1X認証のCLI設定](#)

[AP有線802.1X認証スイッチの設定](#)

[RADIUSサーバ証明書のインストール](#)

[AP有線802.1X認証の検証](#)

[802.1X認証のトラブルシューティング](#)

[関連情報](#)

はじめに

このドキュメントでは、802.1X PEAPまたはEAP-TLS方式を使用して、スイッチポートでシスコのアクセスポイントを認証する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ワイヤレス コントローラ

- アクセスポイント
- 最大 300 のアクセスポイントグループ
- ISEサーバ
- 認証局.

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ワイヤレスコントローラ：17.09.02を実行するC9800-40-K9
- アクセスポイント：C9117AXI-D
- スイッチ：17.06.04が稼働するC9200L-24P-4G
- AAAサーバ：3.1.0.518を実行するISE-VM-K9
- 認証局：Windows Server 2016

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

アクセスポイント(AP)を802.1Xを使用してスイッチポートで認証する場合、デフォルトでは、証明書を必要としないEAP-FAST認証プロトコルが使用されます。APでPEAP-mschapv2方式（AP側ではクレデンシャルを使用するが、RADIUS側では証明書を使用）またはEAP-TLS方式（両側で証明書を使用）を使用する場合、最初にLSCを設定する必要があります。これは、信頼できるルート証明書をアクセスポイント（およびEAP-TLSの場合はデバイス証明書）にプロビジョニングする唯一の方法です。APがPEAPを実行して、サーバ側の検証を無視することはできません。このドキュメントでは、最初にLSCの設定について説明し、次に802.1Xの設定側について説明します。

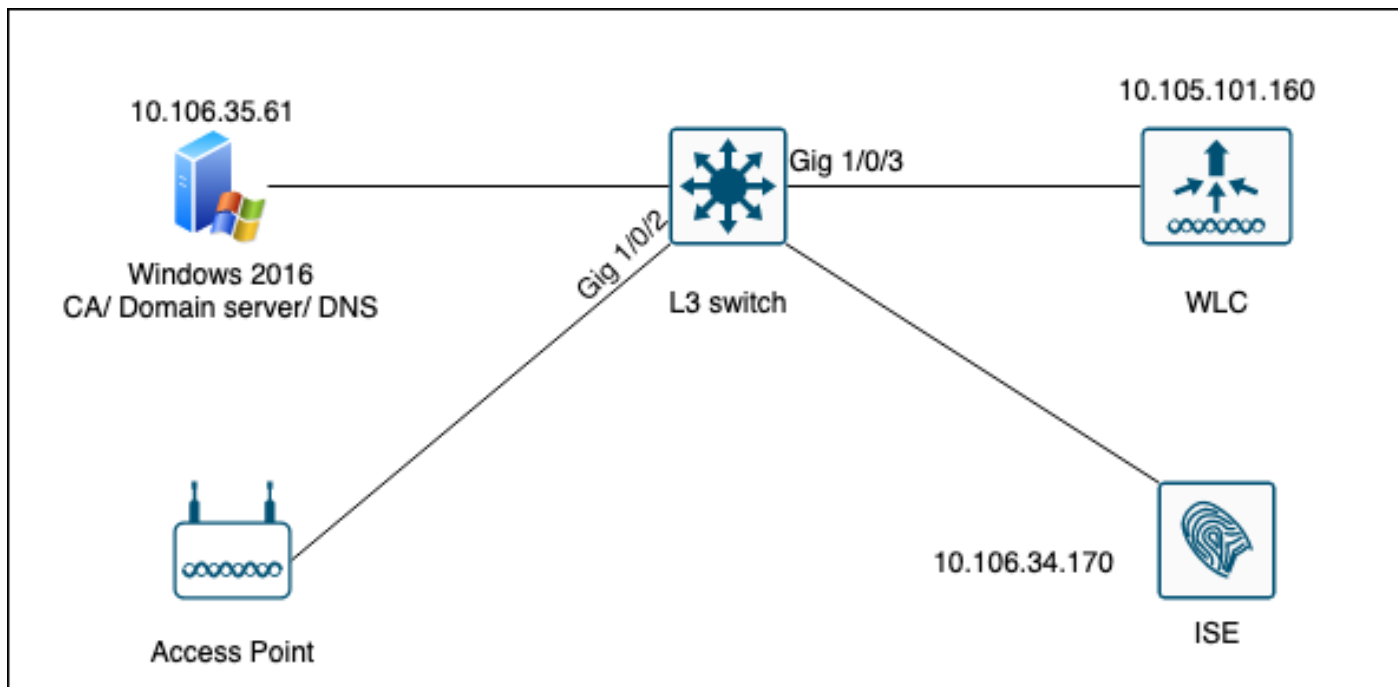
PKIでセキュリティを強化し、認証局(CA)を制御し、生成された証明書に対してポリシー、制限、および使用法を定義する場合は、LSCを使用します。

LSCを使用すると、コントローラはCAによって発行された証明書を取得します。APはCAサーバと直接通信しませんが、WLCは参加しているAPに代わって証明書を要求します。CAサーバの詳細は、コントローラ上で設定し、アクセス可能である必要があります。

コントローラは、Simple Certificate Enrollment Protocol(SCEP)を使用して、デバイスで生成されたcertReqsをCAに転送し、再度SCEPを使用してCAから署名付き証明書を取得します。

SCEPは、PKIクライアントとCAサーバが証明書の登録と失効をサポートするために使用する証明書管理プロトコルです。これはシスコで広く使用されており、多くのCAサーバでサポートされています。SCEPでは、PKIメッセージのトランスポートプロトコルとしてHTTPが使用されます。SCEPの主な目標は、ネットワークデバイスへの証明書のセキュアな発行です。

ネットワーク図



設定

主に設定する項目は、SCEP CAと9800 WLCの2つです。

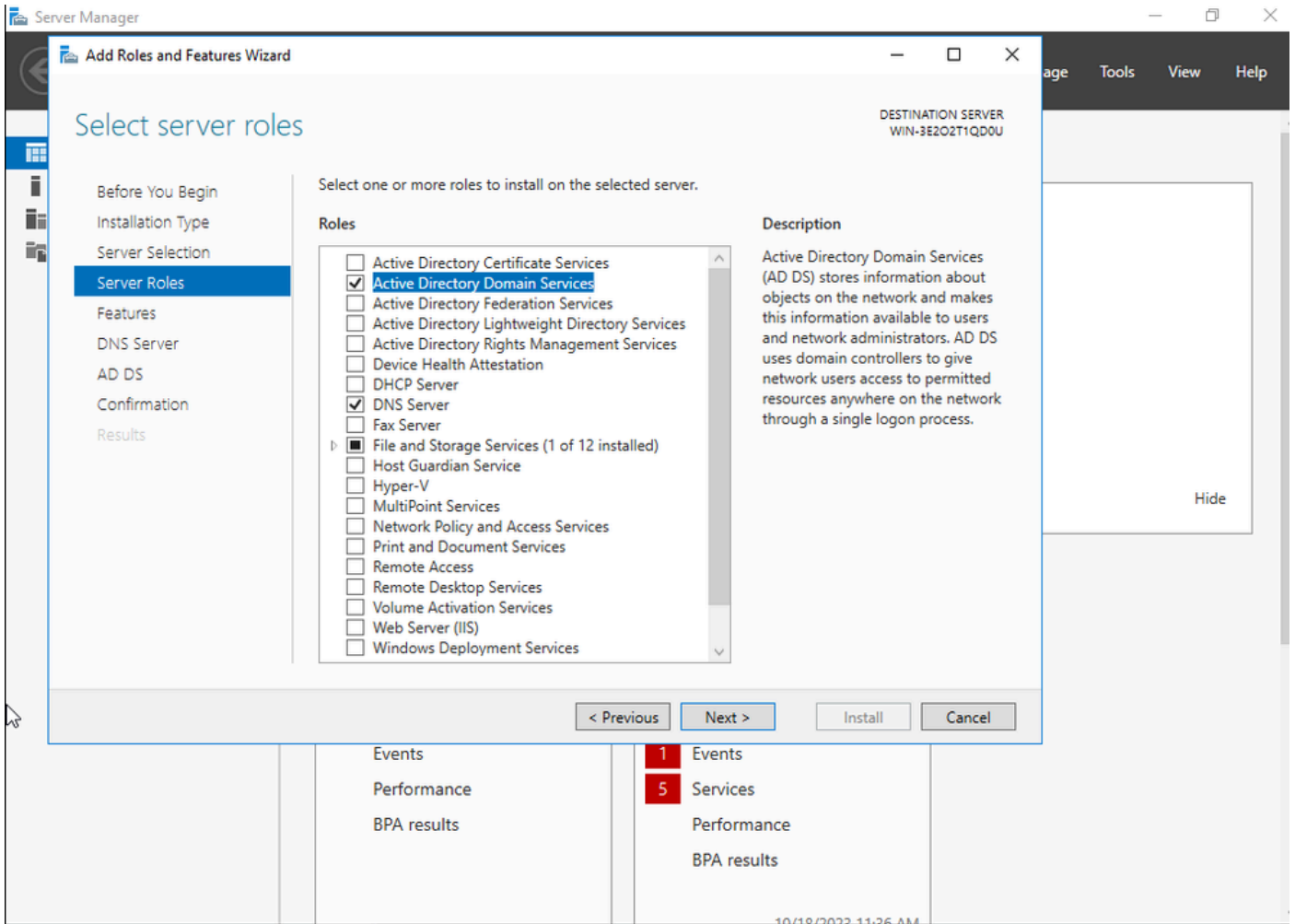
Windows Server 2016 SCEP CA

このドキュメントでは、ラボでのWindows Server SCEP CAの基本的なインストールについて説明します。実際の実稼働グレードのWindows CAは、企業運用に合わせて安全かつ適切に設定する必要があります。このセクションは、ラボでテストし、この設定を機能させるために必要な設定から着想を得ることを目的としています。内容は次のとおりです。

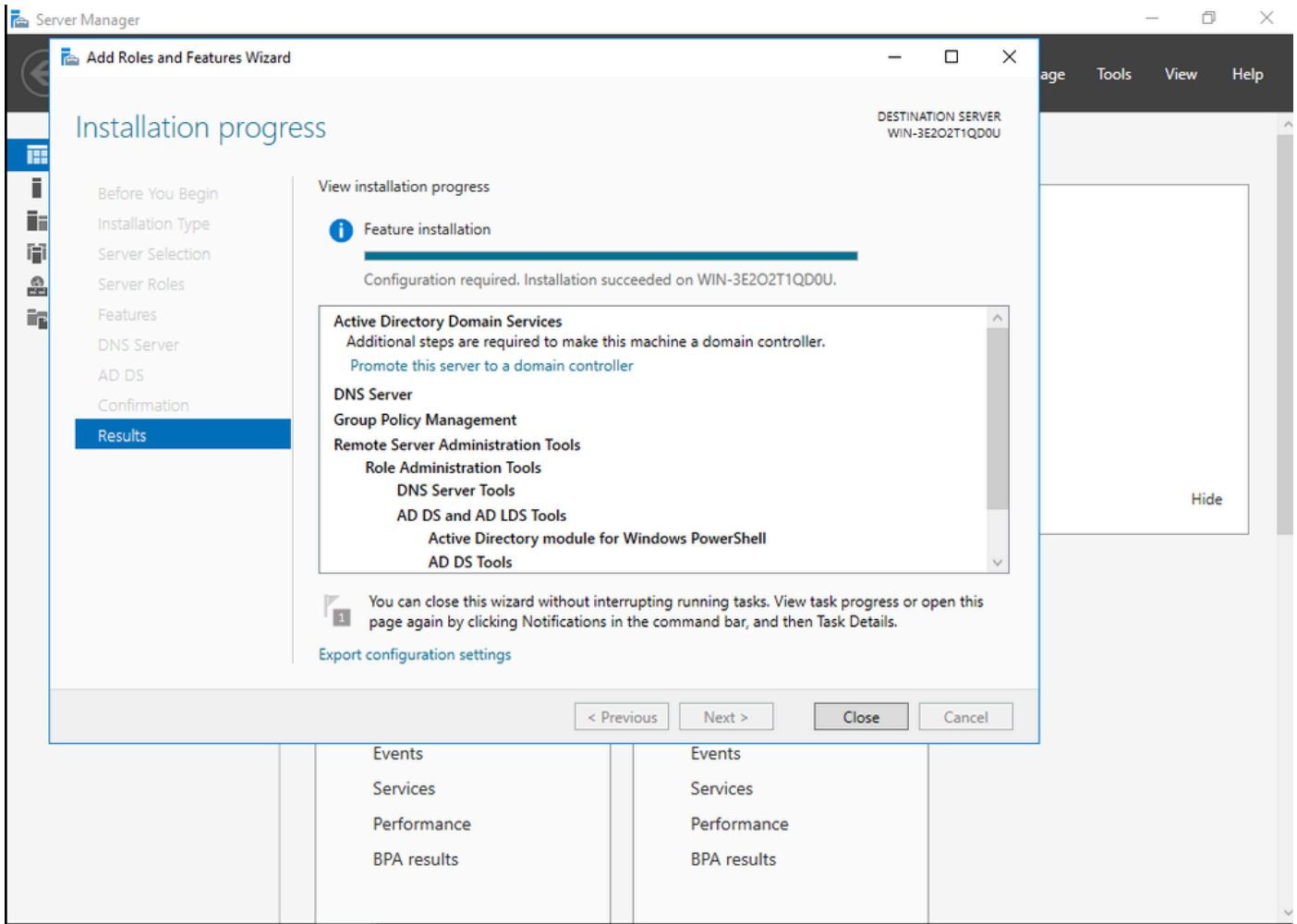
ステップ1:新しいWindows Server 2016デスクトップエクスペリエンスをインストールします。

ステップ2:サーバにスタティックIPアドレスが設定されていることを確認します。

手順3:新しい役割とサービスをインストールし、Active DirectoryドメインサービスとDNSサーバから開始します。

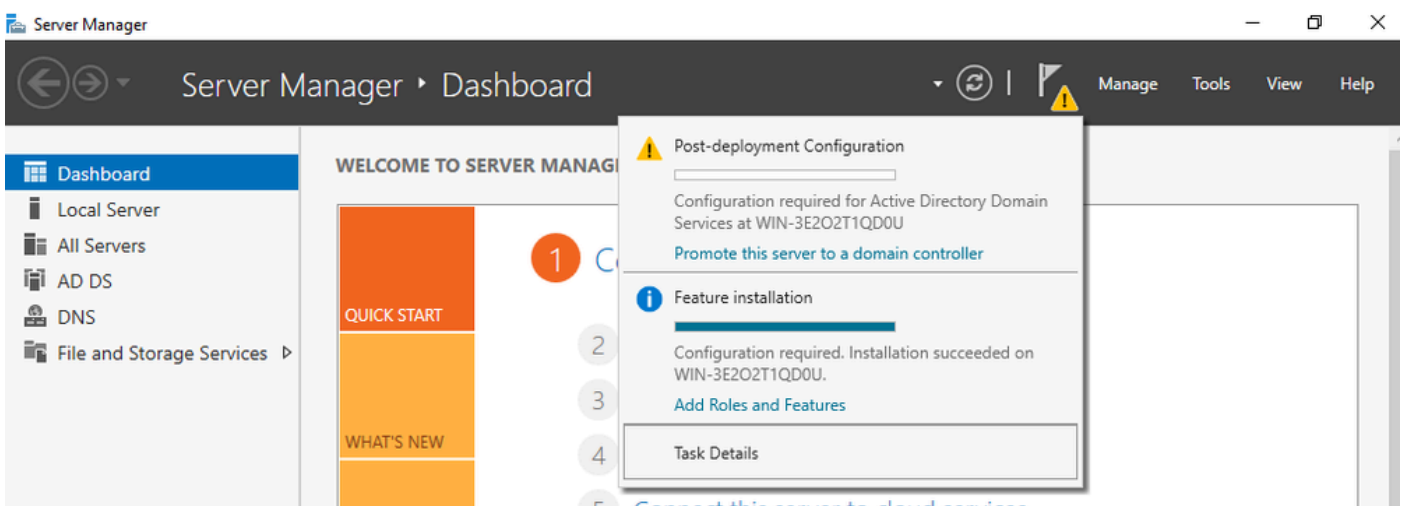


Active Directoryのインストール



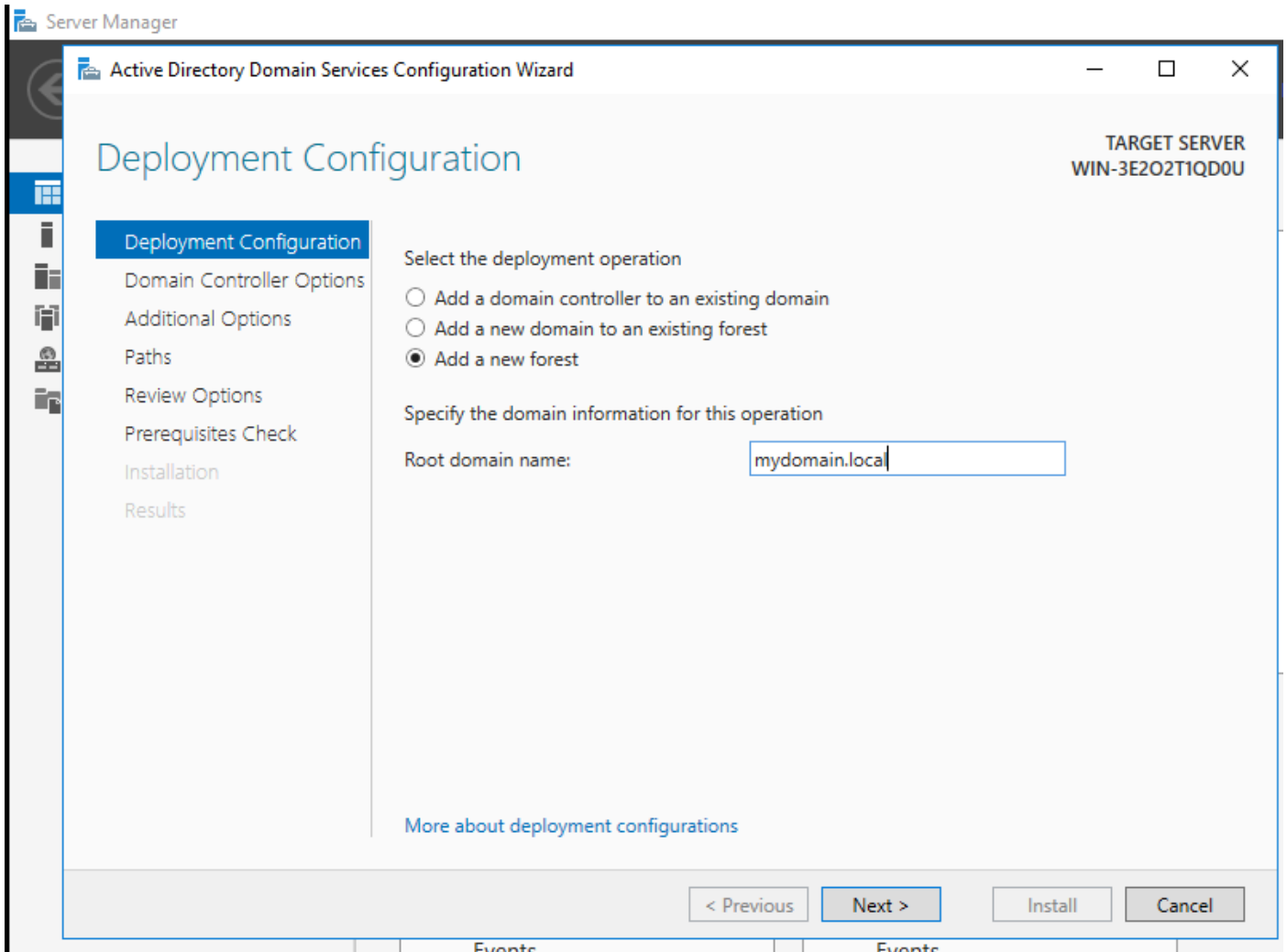
ADインストールの終了

ステップ4:完了したら、「Promote this server to a domain controller(このサーバをドメインコントローラに昇格させる)」のダッシュボードをクリックします。



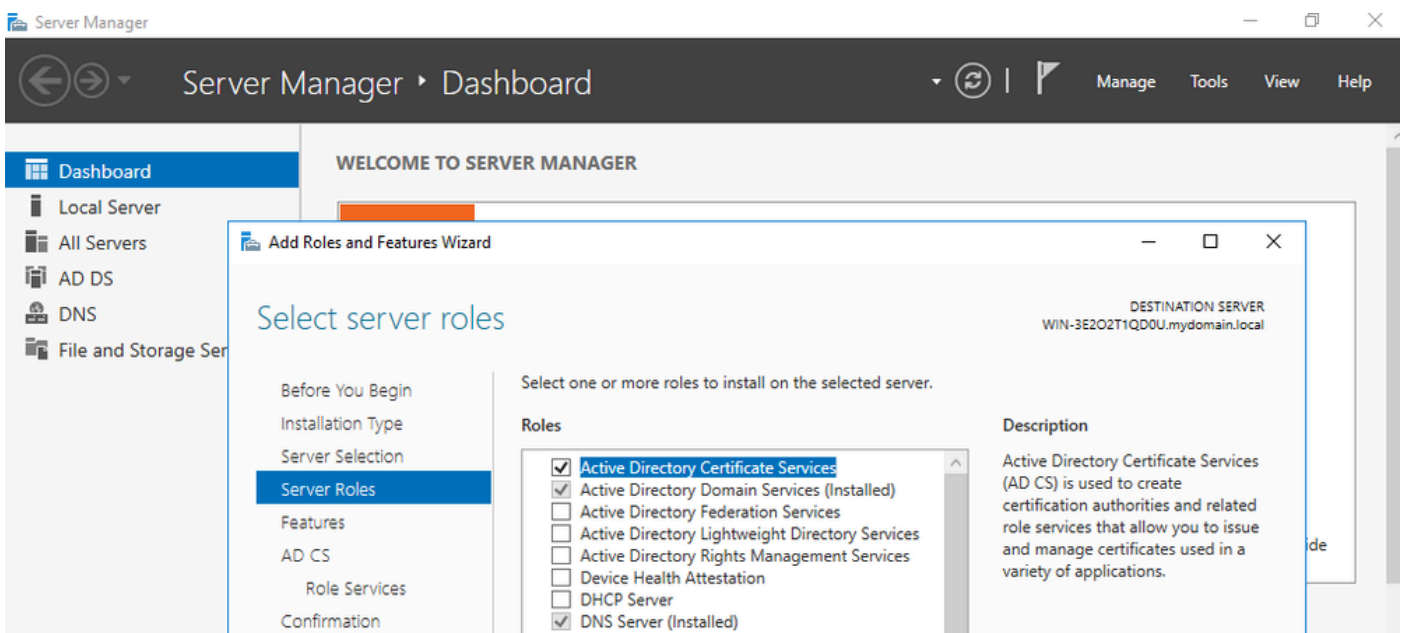
ADサービスの設定

ステップ5:新しいフォレストを作成し、ドメイン名を選択します。

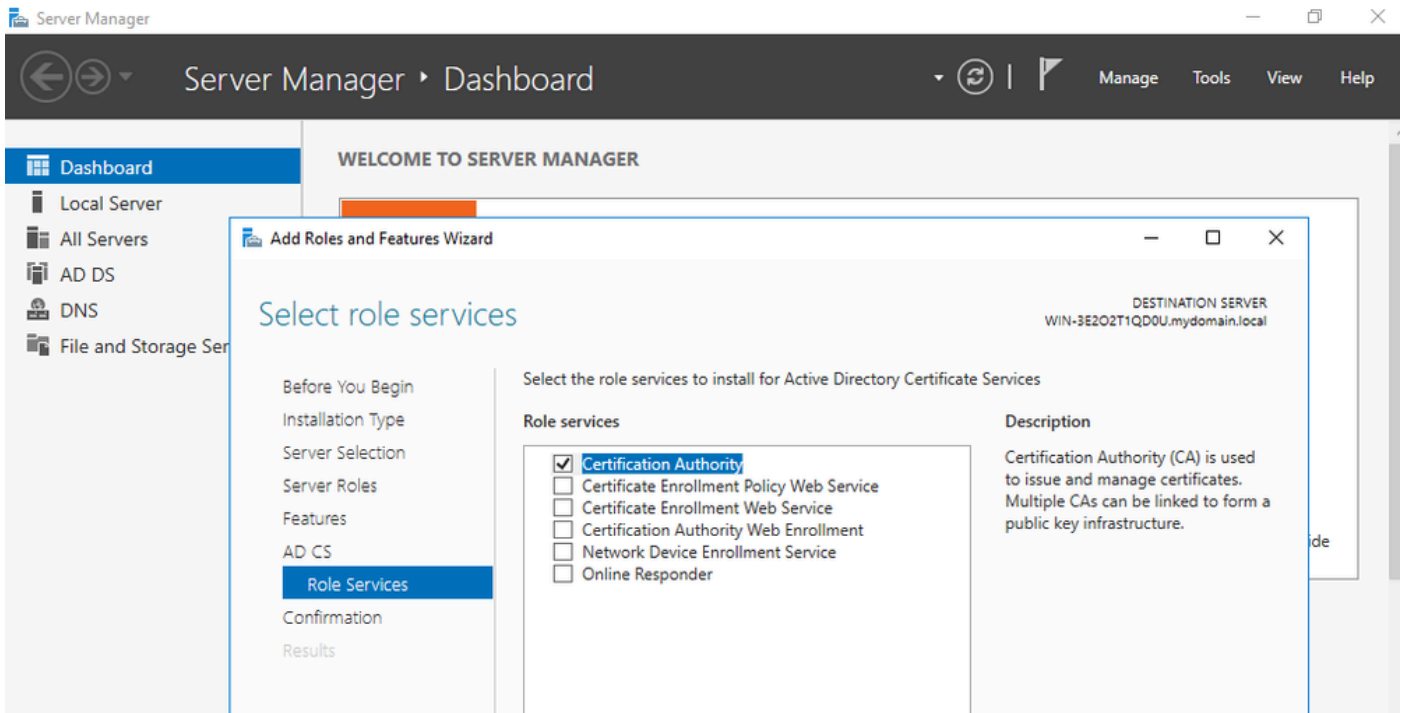


フォレスト名を選択してください

ステップ6:証明書サービスの役割をサーバに追加します。

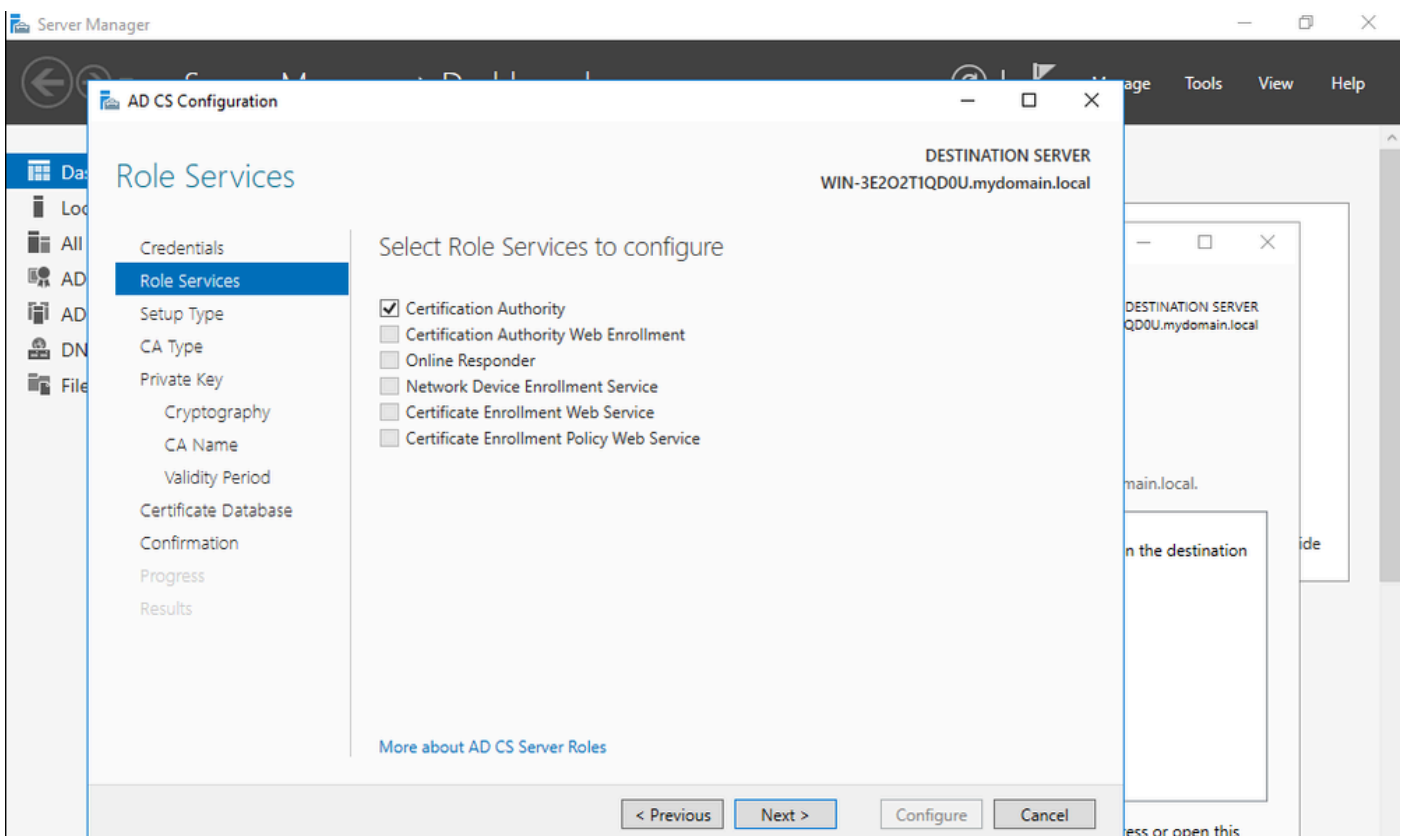


証明書サービスの追加

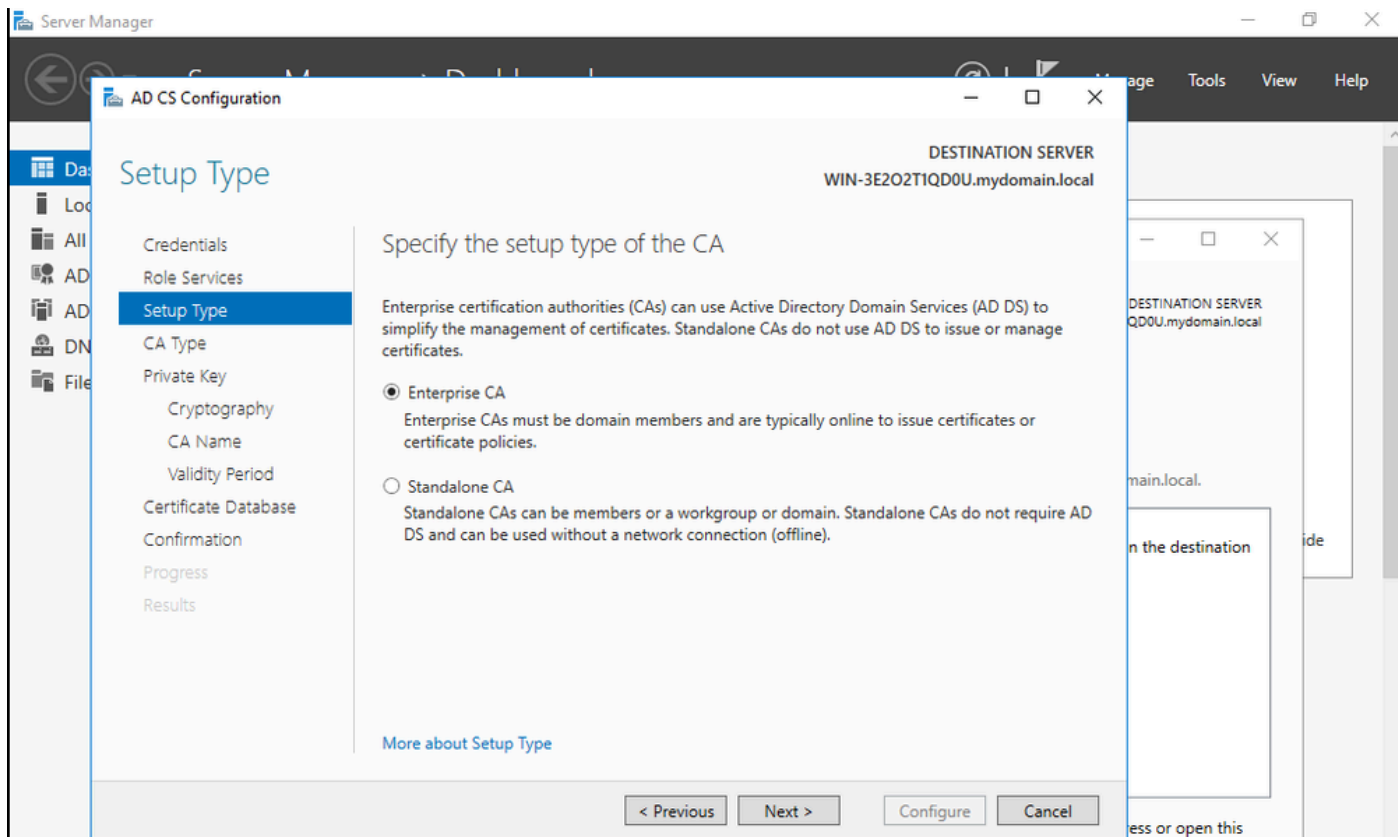


証明機関だけを追加する

ステップ7:設定が完了したら、認証局を設定します。

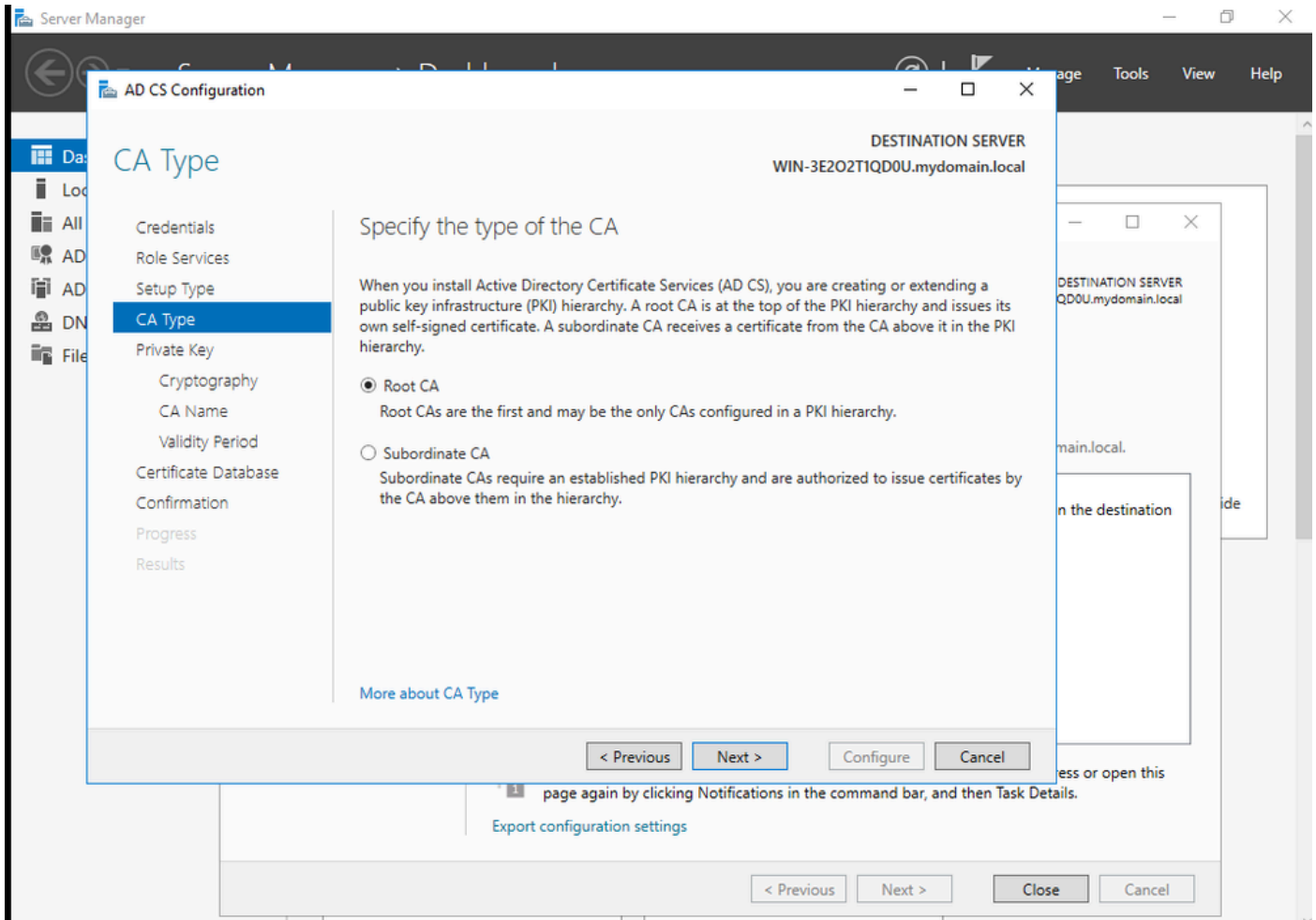


ステップ8:エンタープライズCAを選択します。



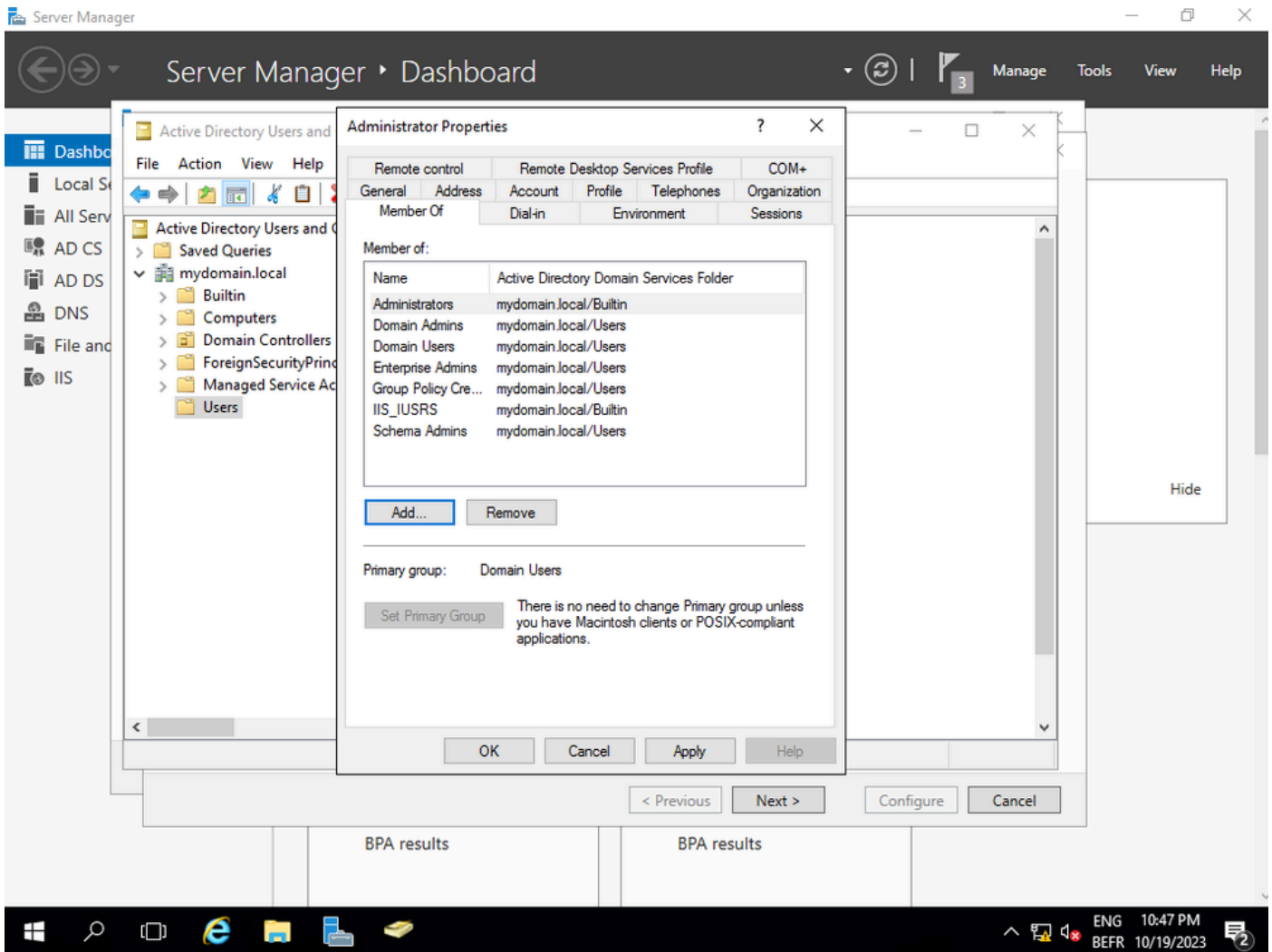
エンタープライズ CA

ステップ9:ルートCAにする。Cisco IOS XE 17.6以降、下位CAはLSCでサポートされています。



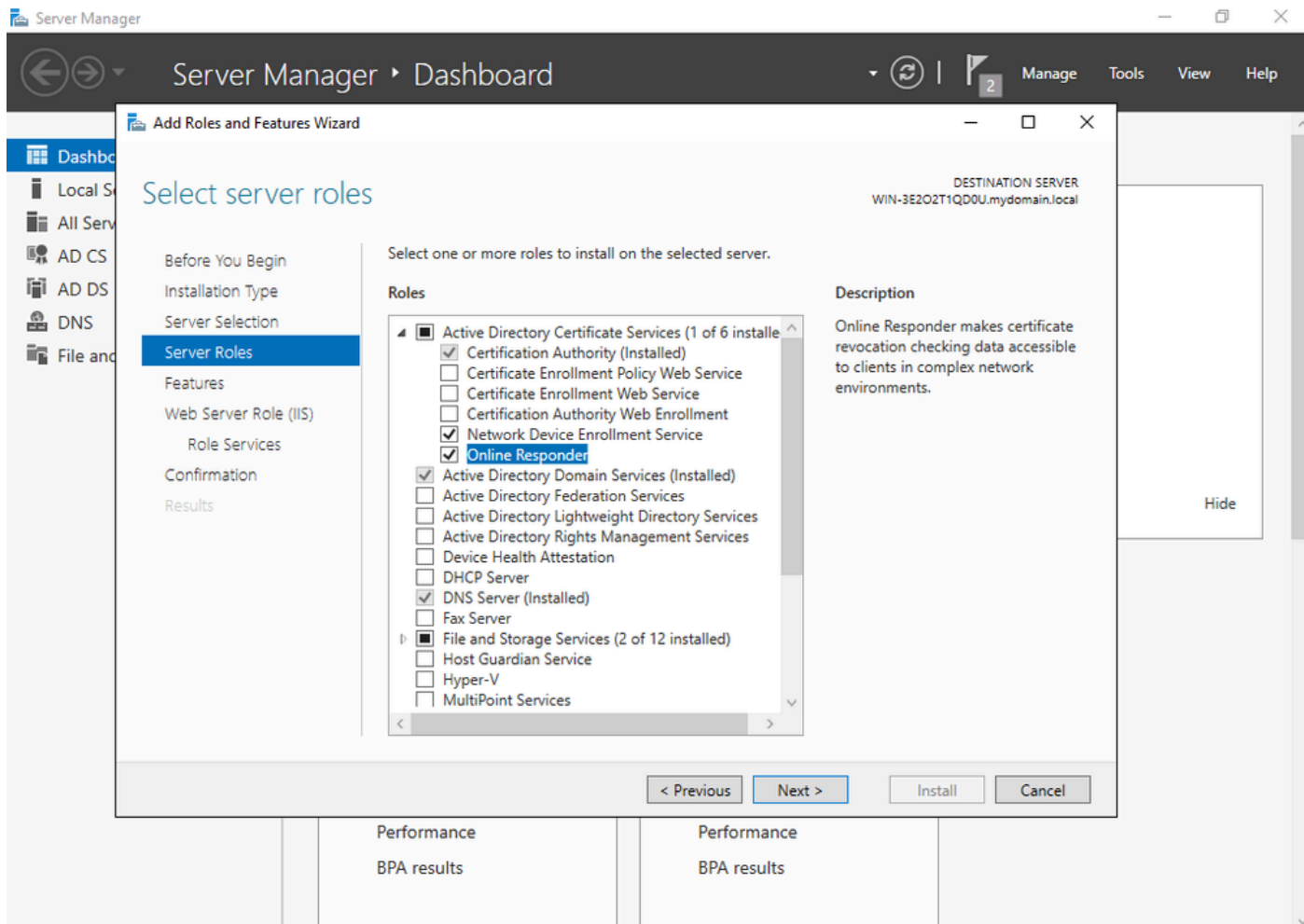
ルートCAの選択

IIS_IUSRSグループに属するCAに使用するアカウントを持つことが重要です。この例では、Administratorアカウントを使用してActive Directory Users and Computersメニューに移動し、AdministratorユーザをIIS_IUSRSグループに追加します。



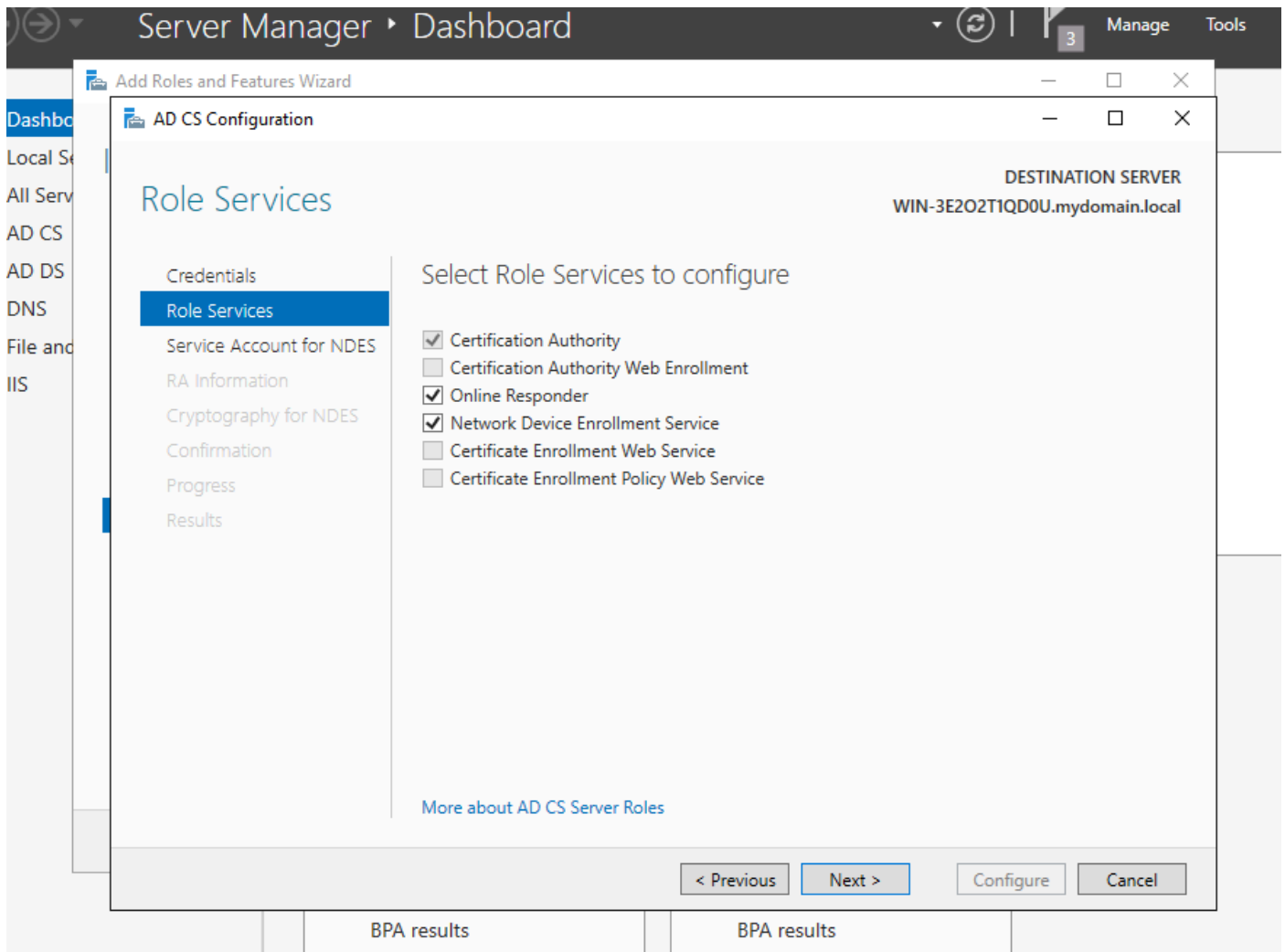
管理者アカウントをIIS_USERグループに追加します

ステップ10:適切なIISグループにユーザを追加したら、ロールとサービスを追加します。次に、オンラインレスポндаとNDESサービスを認証局に追加します。



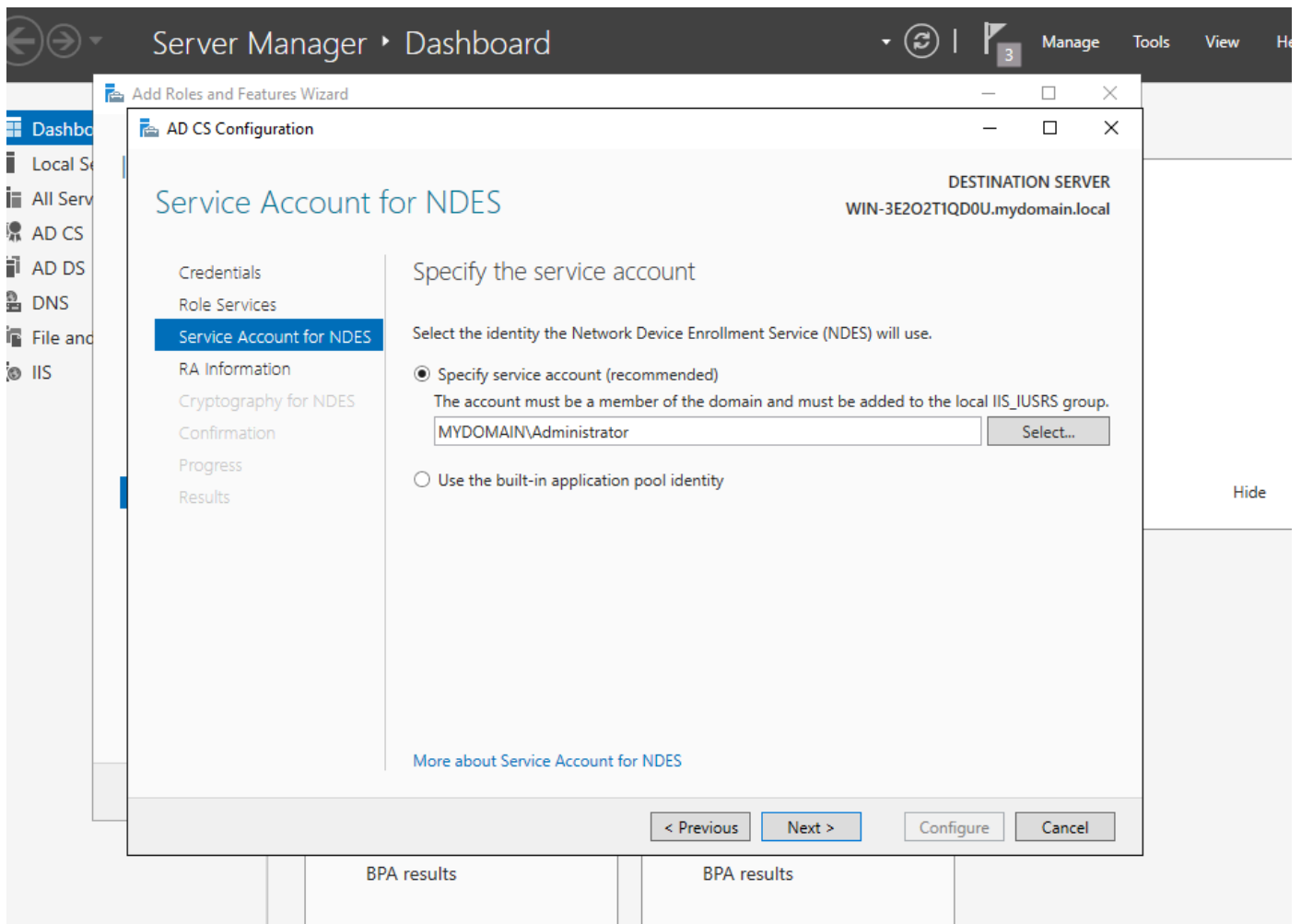
NDESおよびオンラインレスポナーサービスのインストール

ステップ11:完了したら、それらのサービスを設定します。



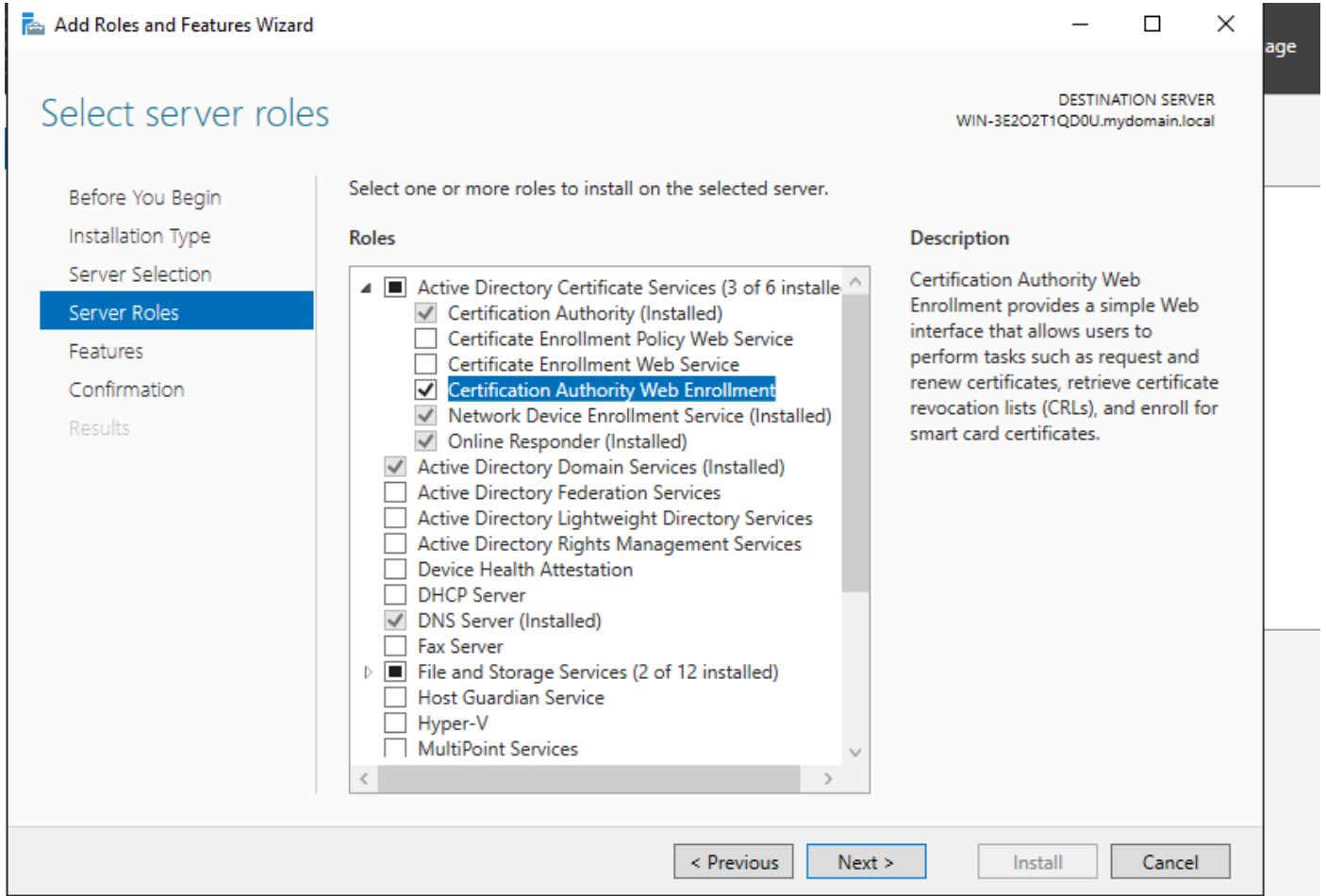
オンラインレスポンドとNDESサービスのインストール

ステップ12: サービスアカウントを選択するように求められます。これは、以前にIIS_IUSRSグループに追加したアカウントです。

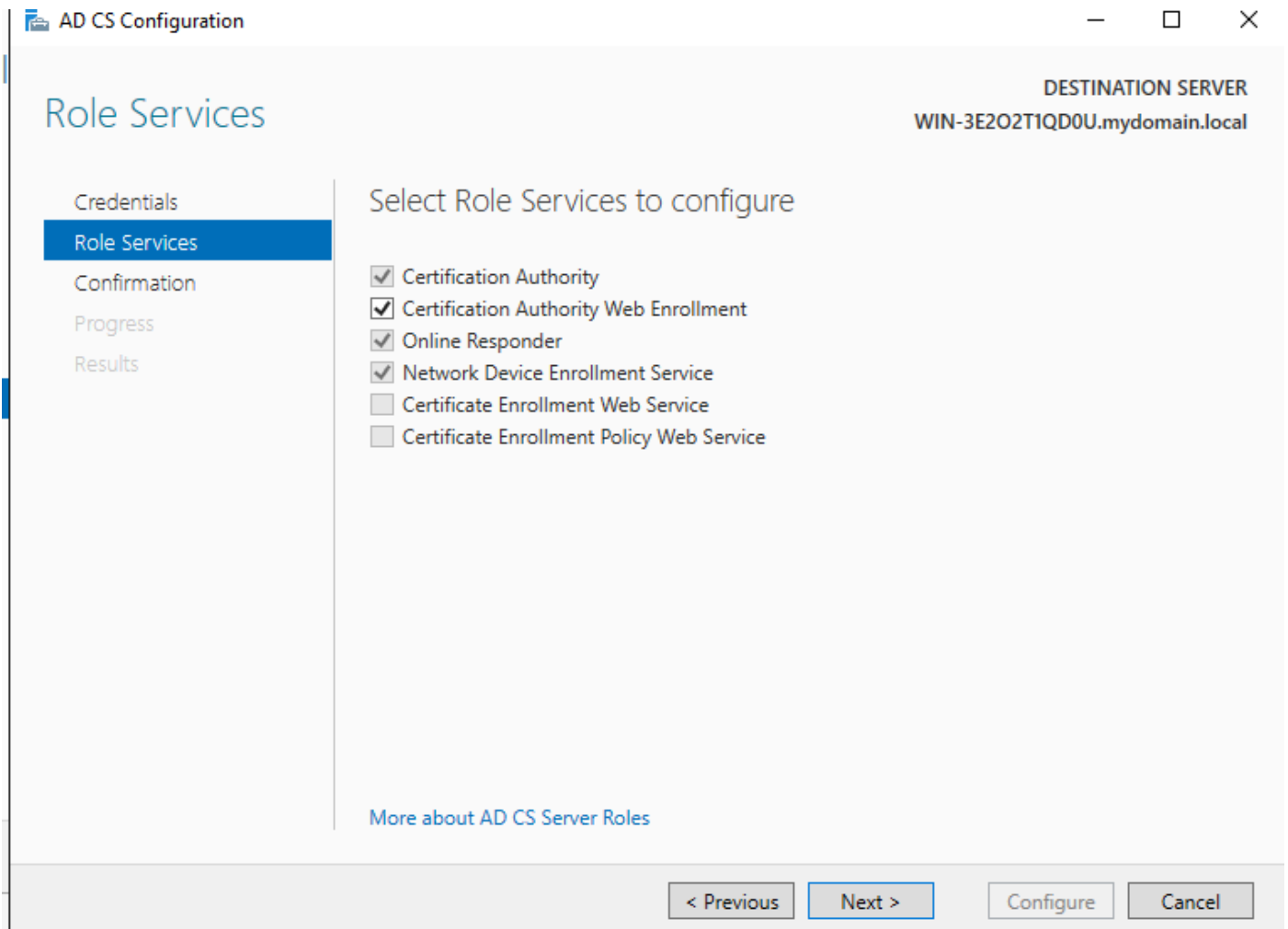


IISグループに追加したユーザを選択します

ステップ13：これはSCEP操作には十分ですが、802.1X認証を実現するには、RADIUSサーバに証明書をインストールする必要もあります。したがって、簡単にWeb登録サービスをインストールして設定し、ISE証明書要求をWindows Serverに簡単にコピーして貼り付けられるようにします。

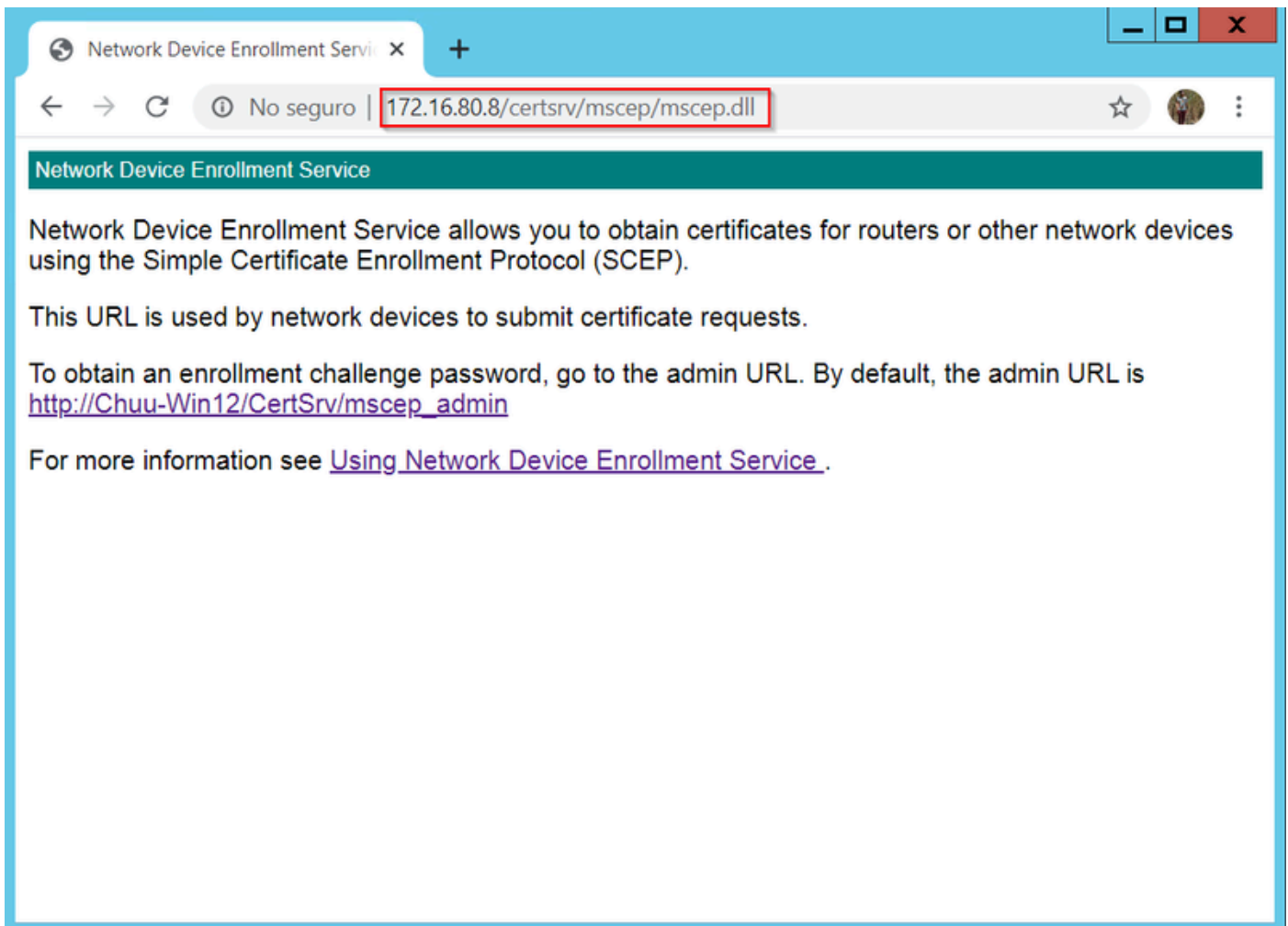


Web登録サービスのインストール



web登録サービスの設定

ステップ 14 : SCEPサービスが正常に動作していることを確認するには、
<http://<serverip>/certsrv/mscep/mscep.dll>にアクセスします。



SCEPポータルを検証

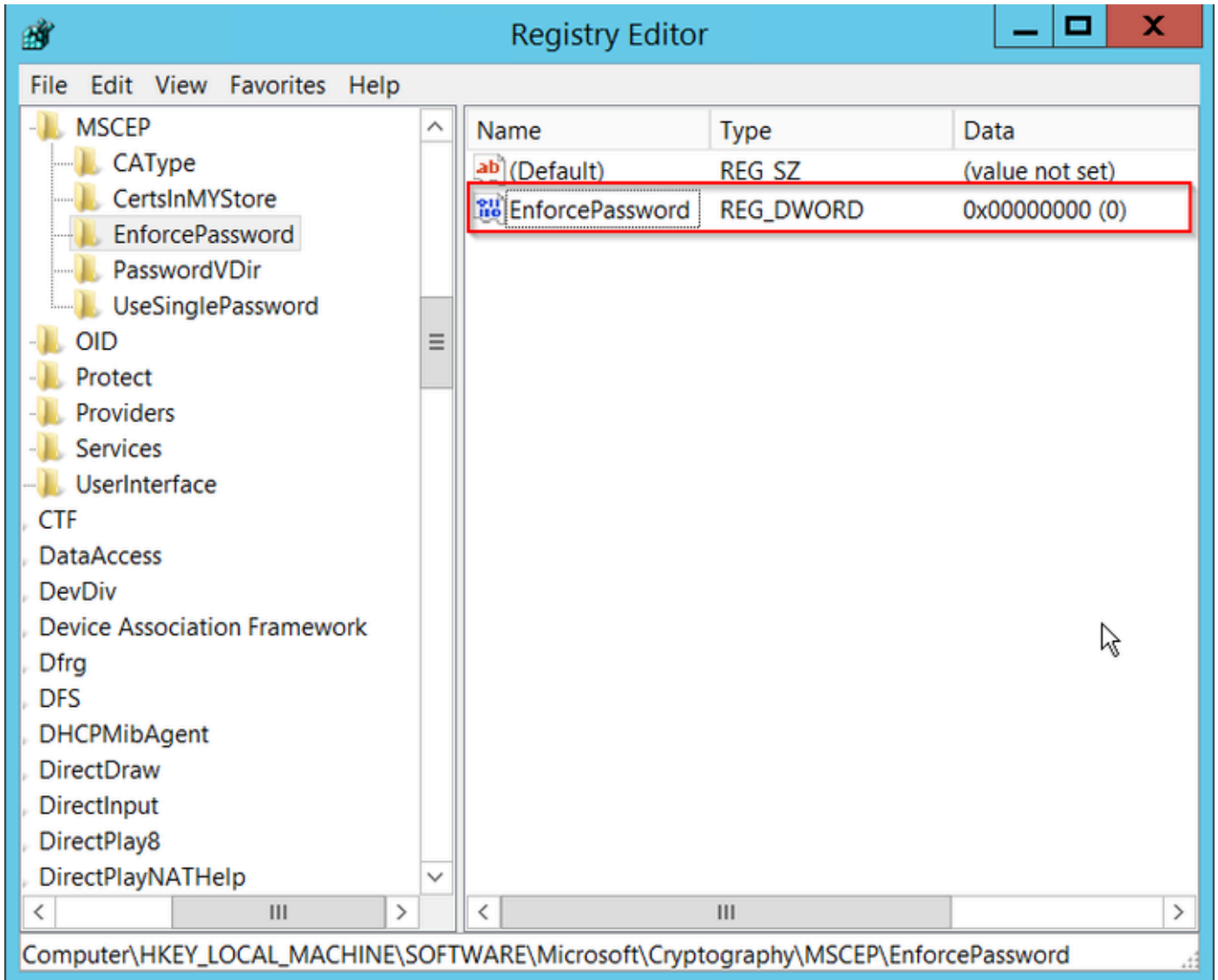
ステップ 15 :

デフォルトでは、Windows Serverは、Microsoft SCEP(MSCEP)に登録する前に、動的チャレンジパスワードを使用してクライアントおよびエンドポイントの要求を認証します。これには、管理者アカウントがWeb GUIを参照して要求ごとにオンデマンドパスワードを生成する必要があります (パスワードは要求内に含める必要があります)。コントローラは、サーバに送信する要求にこのパスワードを含めることはできません。この機能を削除するには、NDESサーバのレジストリキーを変更する必要があります。

レジストリエディタを開き、StartメニューでRegeditを検索します。

Computer > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptography > MSCEP > EnforcePasswordの順に移動します。

EnforcePasswordの値を0に変更します。すでに0の場合は、そのままにしておきます。



Enforcepassword値の設定

証明書テンプレートとレジストリの設定

証明書および証明書に関連付けられたキーは、CAサーバ内のアプリケーションポリシーで定義されたさまざまな目的で、複数のシナリオで使用できます。アプリケーションポリシーは、証明書の拡張キー使用法(EKU)フィールドに保存されます。このフィールドは、オーセンティケータによって解析され、クライアントが目的の目的で使用していることを確認します。適切なアプリケーションポリシーがWLCとAPの証明書に確実に統合されるようにするには、適切な証明書テンプレートを作成し、NDESレジストリにマッピングします。


ステップ 1 : Start > Administrative Tools > Certification Authorityの順に移動します。

ステップ 2 : CA Serverフォルダツリーを展開し、Certificate Templatesフォルダを右クリックして、Manageを選択します。

ステップ 3 : Users証明書テンプレートを右クリックし、コンテキストメニューからDuplicate Templateを選択します。

ステップ 4 : Generalタブに移動し、必要に応じてテンプレート名と有効期間を変更し、他のすべ

でのオプションはオフのままにします。

 注意：有効期間を変更する場合は、認証局ルート証明書の有効期間を超えないようにしてください。

Properties of New Template



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

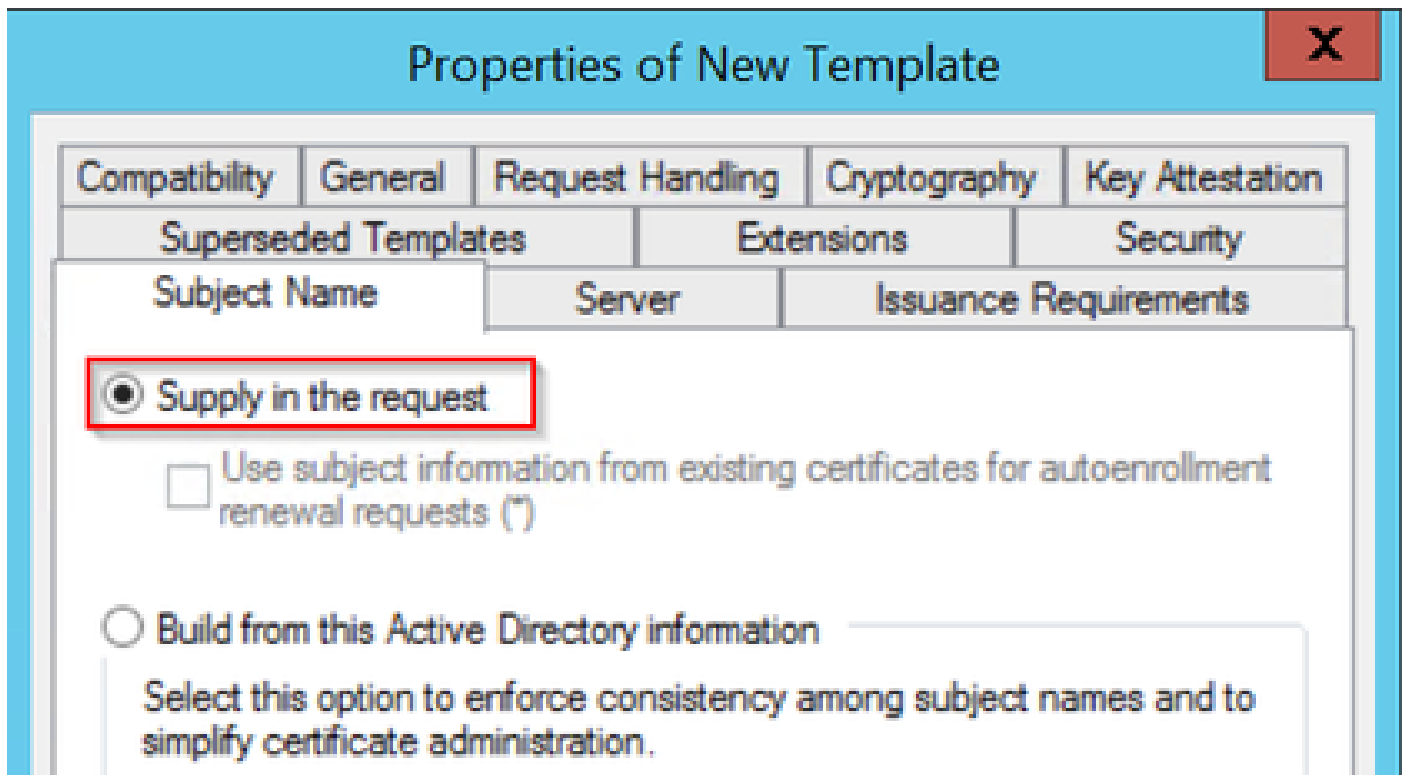
OK

Cancel

Apply

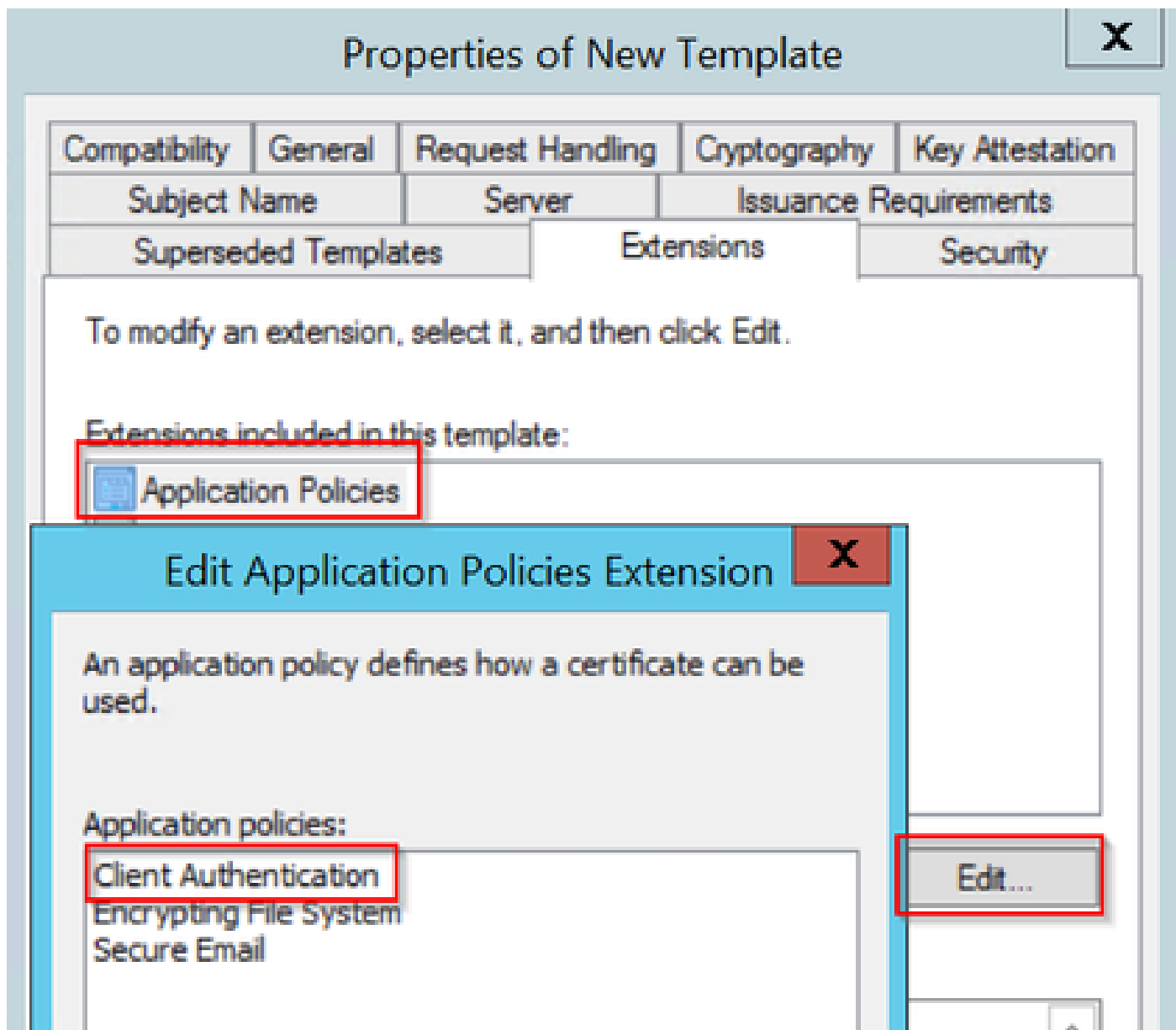
Help

ステップ 5 : Subject Nameタブに移動し、Supply in the requestが選択されていることを確認します。ポップアップが表示され、ユーザが証明書に署名するために管理者の承認を必要としていないことを示し、OKを選択します。



要求への入力

手順 6 : Extensionsタブに移動し、Application Policiesオプションを選択して、Edit...ボタンを選択します。Client AuthenticationがApplication Policiesウィンドウにあることを確認します。そうでない場合は、Addを選択して追加します。



内線番号の確認

手順 7 : Securityタブに移動し、Enable SCEP Services in the Windows Serverのステップ6で定義したサービスアカウントにテンプレートのFull Control権限が付与されていることを確認し、ApplyおよびOKを選択します。

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

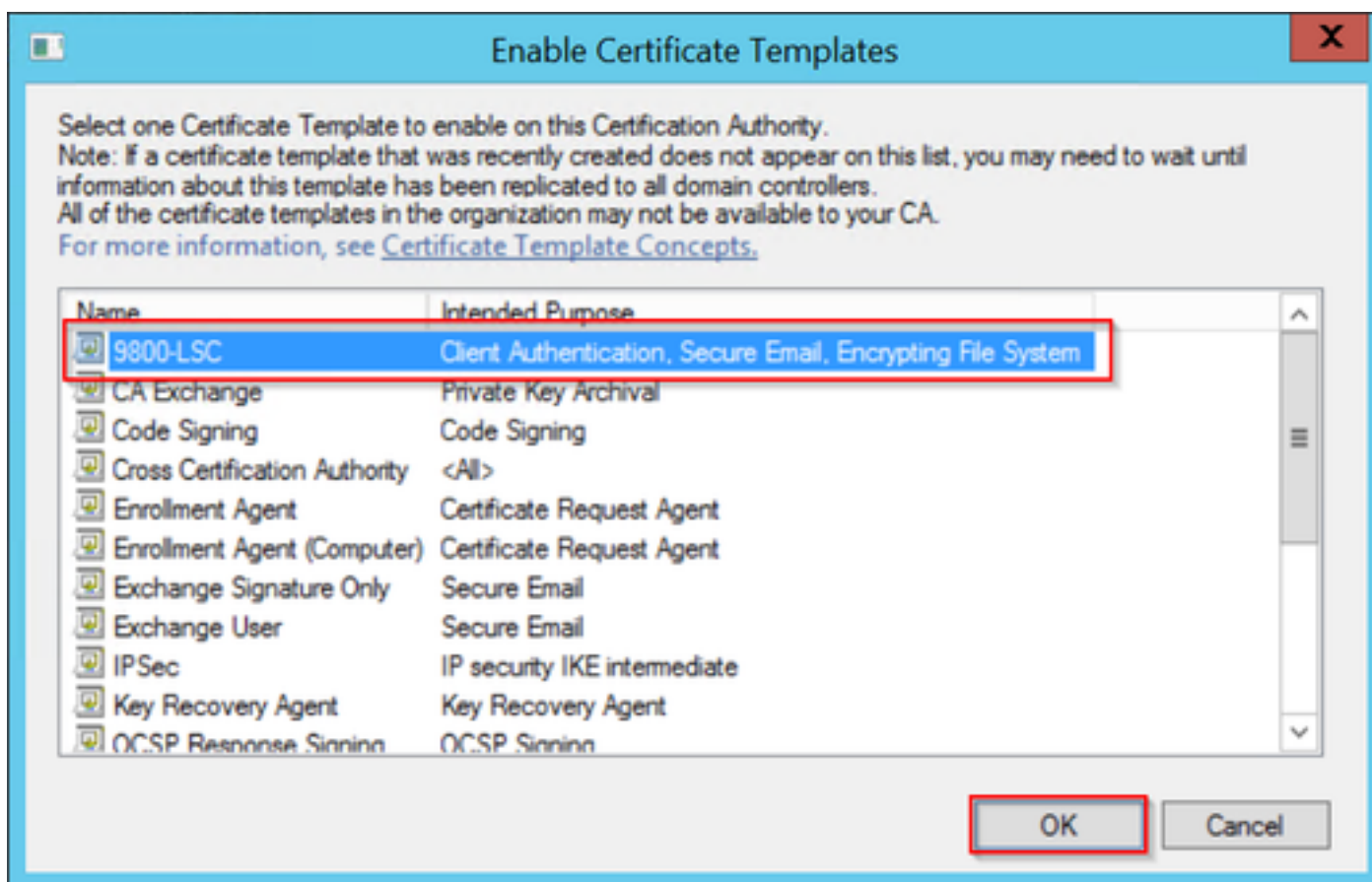
OK Cancel **Apply** Help

完全に制御する

ステップ 8 : Certification Authority ウィンドウに戻り、Certificate Templates フォルダを右クリックして、New > Certificate Template to Issue を選択します。

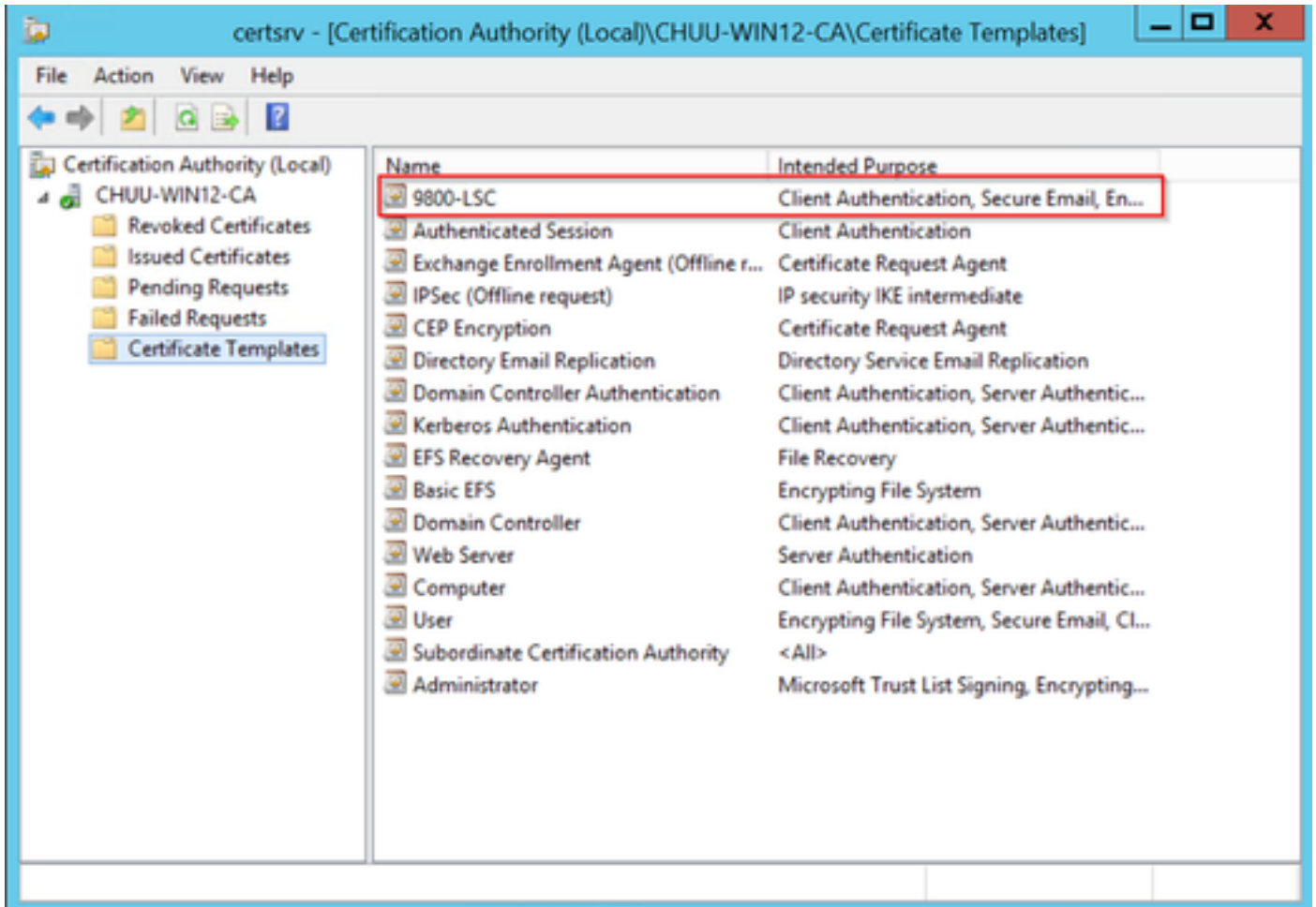
ステップ 9 : 以前に作成した証明書テンプレート (この例では 9800-LSC) を選択し、OK を選択します。

 注 : 新しく作成された証明書テンプレートは、すべてのサーバ間で複製する必要があるため、複数のサーバの展開にリストされるまでに時間がかかる場合があります。



テンプレートの選択

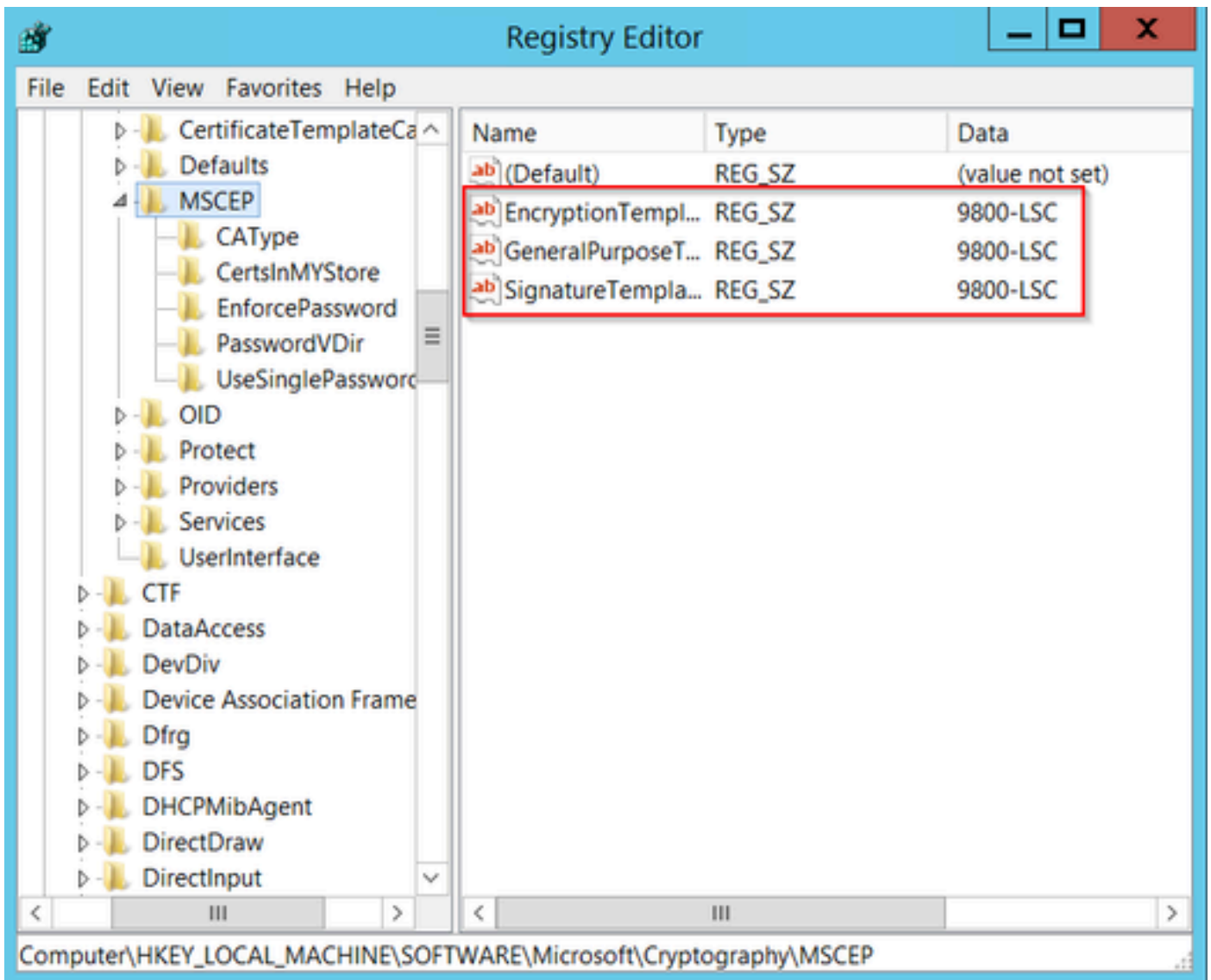
新しい証明書テンプレートがCertificate Templatesフォルダの内容にリストされます。



LSCの選択

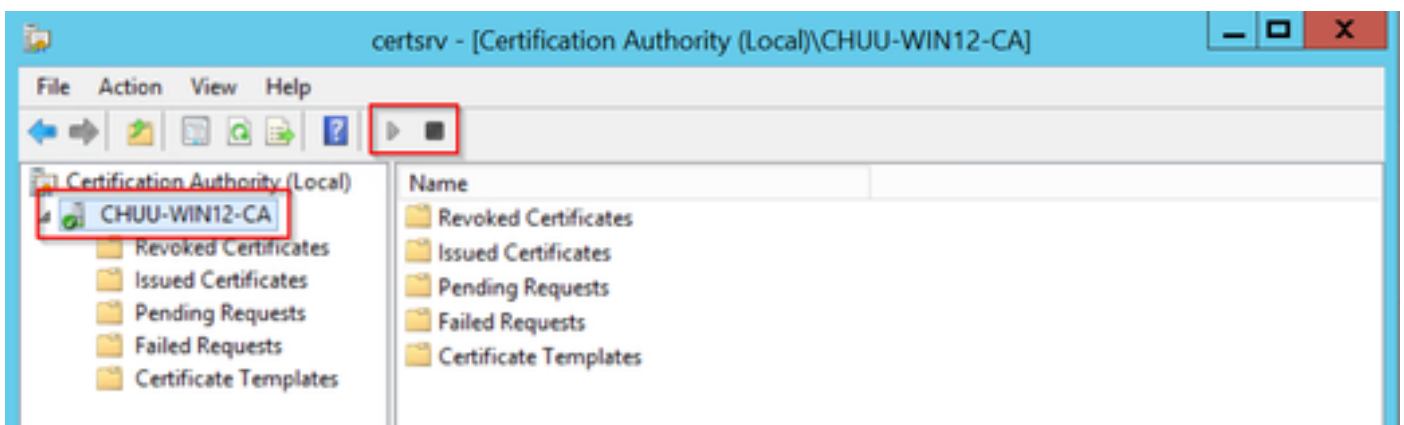
ステップ 10 : Registry Editorウィンドウに戻り、Computer > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptography > MSCEPの順に移動します。

ステップ 11 Encryption Template、General Purpose Template、および Signature Template レジストリを編集して、新しく作成された証明書テンプレートを指すようにします。



レジストリのテンプレートの変更

ステップ 12NDESサーバをリブートして、Certification Authorityウィンドウに戻り、サーバ名を選択し、StopとPlayボタンを続けて選択します。



9800でのLSCの設定

WLCでAPのLSCを設定する手順を次に示します。

1. RSAキーを作成します。このキーは、後でPKIトラストポイントに使用されます。
2. トラストポイントを作成し、作成したRSAキーをマッピングします。
3. APのLSCプロビジョニングを有効にし、トラストポイントのマッピングします。
 1. 加入しているすべてのAPでLSCを有効にします。
 2. プロビジョニングリストを使用して、選択したAPのLSCを有効にします。
4. ワイヤレス管理トラストポイントを変更し、LSCトラストポイントをポイントします。

AP LSC GUIの設定手順

ステップ1: Configuration > Security > PKI Management > Key Pair Generationの順に移動します。

1. Addをクリックし、適切な名前を付けます。
2. RSAキーサイズを追加します。
3. key exportableオプションはオプションです。これは、キーをエクスポートする場合にのみ必要です。
4. 生成の選択

Configuration > Security > PKI Management

Trustpoints CA Server **Key Pair Generation** Add Certificate Trustpool

+ Add

Key Name	Key Type	Key Exportable	Zeroize
TP-self-signed-2147029136	RSA	No	<input type="checkbox"/> Zeroize
9800-40.cisco.com	RSA	No	<input type="checkbox"/> Zeroize
TP-self-signed-2147029136.server	RSA	No	<input type="checkbox"/> Zeroize
CISCO_IDEVID_SUDI	RSA	No	<input type="checkbox"/> Zeroize
CISCO_IDEVID_SUDI_LEGACY	RSA	No	<input type="checkbox"/> Zeroize

1 - 5 of 5 items

Key Name* AP-SCEP

Key Type* RSA Key EC Key

Modulus Size* 2048

Key Exportable*

Cancel Generate

ステップ 2 : Configuration > Security > PKI Management > Trustpointsの順に移動します。

1. Addをクリックし、適切な名前を付けます。
2. 登録URL(URLは<http://10.106.35.61:80/certsrv/mscep/mscep.dll>)とその他の詳細を入力します。
3. ステップ1で作成したRSAキーペアを選択します。
4. Authenticateをクリックします。
5. Enroll trustpointをクリックし、パスワードを入力します。
6. Apply to Deviceをクリックします。

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*

ステップ3: Configuration > Wireless > Access Pointsの順に移動します。下にスクロールして、LSC Provisionを選択します。

1. ステータスとしてenabledを選択します。これにより、このWLCに接続されているすべてのAPに対してLSCが有効になります。
2. ステップ2で作成したトラストポイント名を選択します。

必要に応じて残りの詳細を入力します。

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-46E0	C9117AXI-D	2	●	0 days 0 hrs 26 mins 42 secs	10.105.101.158	80ec.3579.0300	0cd0.f99a.46e0	Local	Yes	Registered	Healthy

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

Subject Name Parameters

Country

State

City

Organization

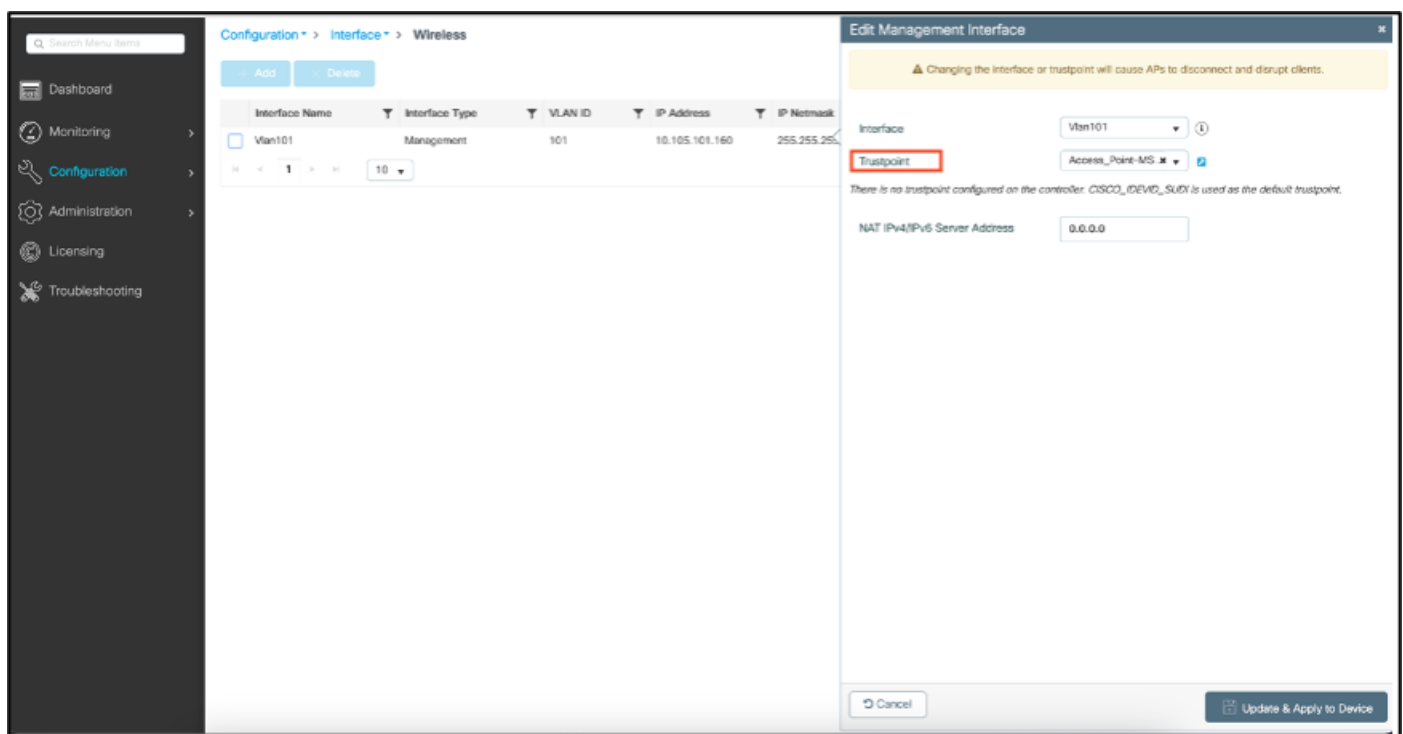
LSCを有効にすると、APはWLC経由で証明書をダウンロードし、レポートします。APコンソールセッションで、次のようなスニペットが表示されます。

```
[*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
```

ステップ4:LSCを有効にすると、LSCトラストポイントと一致するようにワイヤレス管理証明書を変更できます。これにより、APはLSC証明書を使用して加入し、WLCはAP加入にLSC証明書を使用します。APの802.1X認証のみを行う場合、これはオプションの手順です。

1. Configuration > Interface > Wirelessの順に選択し、Management Interfaceをクリックします。
2. トラストポイントを、手順2で作成したトラストポイントに一致するように変更します。

これで、LSC GUIの設定の部分は終了です。APは、LSC証明書を使用してWLCに参加できる必要があります。



AP LSC CLIの設定手順

1. 次のコマンドを使用してRSAキーを作成します。

```
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. PKIトラストポイントを作成し、RSAキーペアをマッピングします。登録URLと残りの詳細を入力します。

```
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)#rsakeypair AP-SCEP
9800-40(ca-trustpoint)#revocation none
9800-40(ca-trustpoint)#exit
```

3. コマンド `crypto pki authenticate <trustpoint>` を使用して、PKIトラストポイントを認証し、CAサーバに登録します。パスワードプロンプトにパスワードを入力します。

```
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証明書を使用してAP加入を設定します。

```
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. ワイヤレス管理トラストポイントを、上記で作成したトラストポイントと一致するように変更します。

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

AP LSCの検証

WLCで次のコマンドを実行して、LSCを確認します。

```
#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
FPS suitability : Not Applicable

9800-40#

```

```

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-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

```

APがリロードされたら、AP CLIにログインし、次のコマンドを実行してLSC設定を確認します。

```

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

```

```

AP0CD0.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
```

LSCプロビジョニングのトラブルシューティング

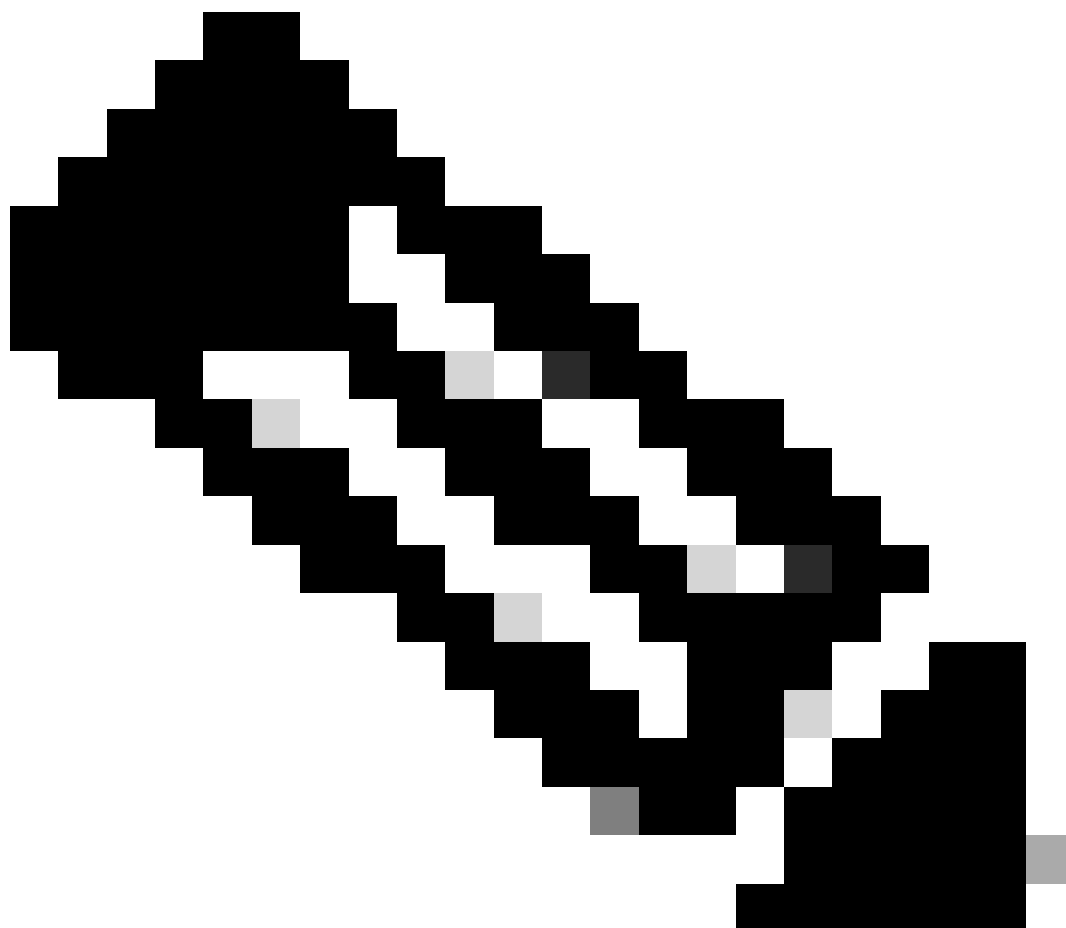
WLCまたはAPアップリンクスイッチポートからEPCキャプチャを取得して、APがCAPWAPトンネルを形成するために使用している証明書を確認できます。DTLSトンネルが正常に構築されたかどうかをPCAPから確認します。

```
▼ Datagram Transport Layer Security
  ▼ DTLSv1.2 Record Layer: Handshake Protocol: Certificate (Reassembled)
    Content Type: Handshake (22)
    Version: DTLS 1.2 (0xfefd)
    Epoch: 0
    Sequence Number: 5
    Length: 82
  ▼ Handshake Protocol: Certificate (Reassembled)
    Handshake Type: Certificate (11)
    Length: 1627
    Message Sequence: 2
    Fragment Offset: 1557
    Fragment Length: 70
    Certificates Length: 1624
  ▼ Certificates (1624 bytes)
    Certificate Length: 1621
  ▼ Certificate: 3082065130820539a00302010202135c000000181814edda85f9bfd100000000018300d_ (pkcs-9-at-emailAddress@mail@tac-lab.local,id-at-commonName=)
    ▼ signedCertificate
      version: v3 (2)
      serialNumber: 0x5c000000181814edda85f9bfd1000000000018
      ▼ signature (sha256WithRSAEncryption)
        Algorithm Id: 1.2.840.113549.1.1.11 (sha256WithRSAEncryption)
      ▼ issuer: rdnSequence (0)
        ▼ rdnSequence: 4 items (id-at-commonName=sumans-lab-ca,dc=sumans,dc=tac-lab,dc=com)
          ▼ RDNSequene item: 1 item (dc=com)
            ▼ RelativeDistinguishedName item (dc=com)
              Object Id: 0.9.2342.19200300.100.1.25 (dc)
              IA5String: com
            ▼ RDNSequene item: 1 item (dc=tac-lab)
              ▼ RelativeDistinguishedName item (dc=tac-lab)
                Object Id: 0.9.2342.19200300.100.1.25 (dc)
                IA5String: tac-lab
            ▼ RDNSequene item: 1 item (dc=sumans)
              ▼ RelativeDistinguishedName item (dc=sumans)
                Object Id: 0.9.2342.19200300.100.1.25 (dc)
                IA5String: sumans
            ▼ RDNSequene item: 1 item (id-at-commonName=sumans-lab-ca)
              ▼ RelativeDistinguishedName item (id-at-commonName=sumans-lab-ca)
                Object Id: 2.5.4.3 (id-at-commonName)
                ▼ DirectoryString: printableString (1)
                  printableString: sumans-lab-ca
          ▼ validity
            ▼ notBefore: utcTime (0)
              utcTime: 2023-09-28 04:15:28 (UTC)
            ▼ notAfter: utcTime (0)
              utcTime: 2024-09-27 04:15:28 (UTC)
        ▼ subject: rdnSequence (0)
```

DTLSデバッグをAPおよびWLCで実行すると、証明書の問題を理解できます。

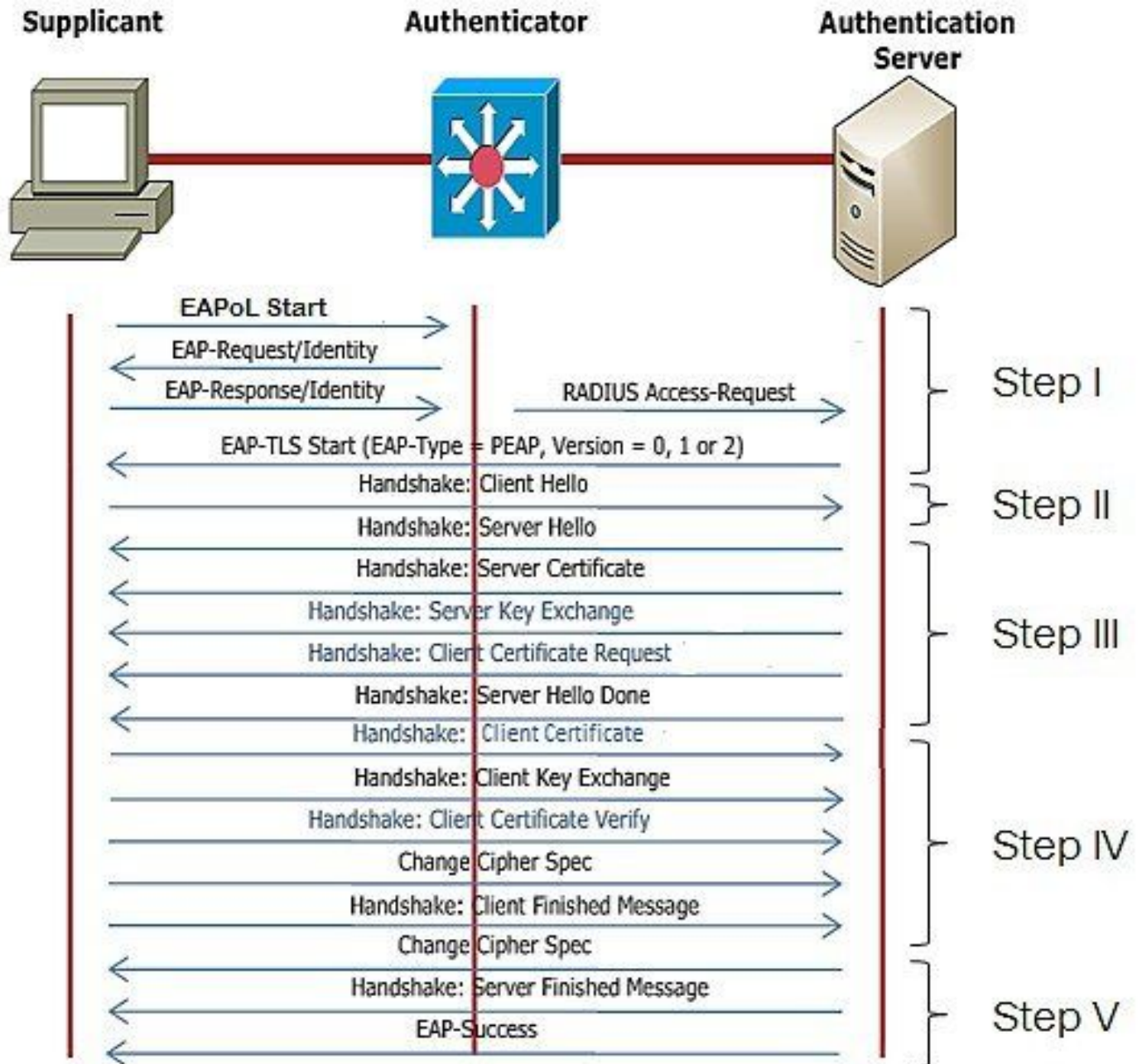
LSCを使用したAP有線802.1X認証

APは、同じLSC証明書を使用して自身を認証するように設定されています。APは802.1Xサブリカントとして機能し、ISEサーバに対してスイッチによって認証されます。ISEサーバはバックエンドでADと通信します。



注:APアップリンクスイッチポートでdot1x認証を有効にすると、認証が通過するまでAPはトラフィックを転送または受信できません。認証に失敗したAPを回復してAPにアクセスするには、APの有線スイッチポートでdot1x authを無効にします。

EAP-TLS認証のワークフローとメッセージ交換

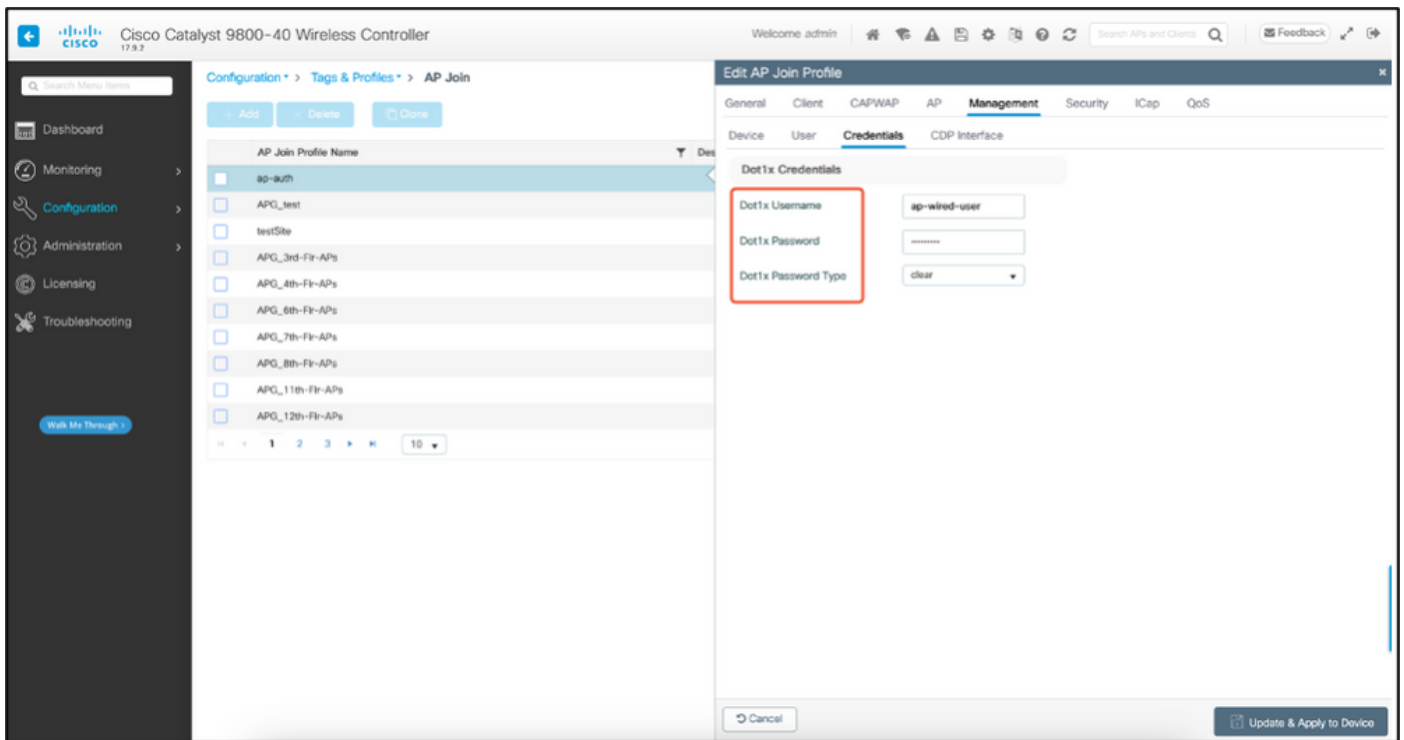
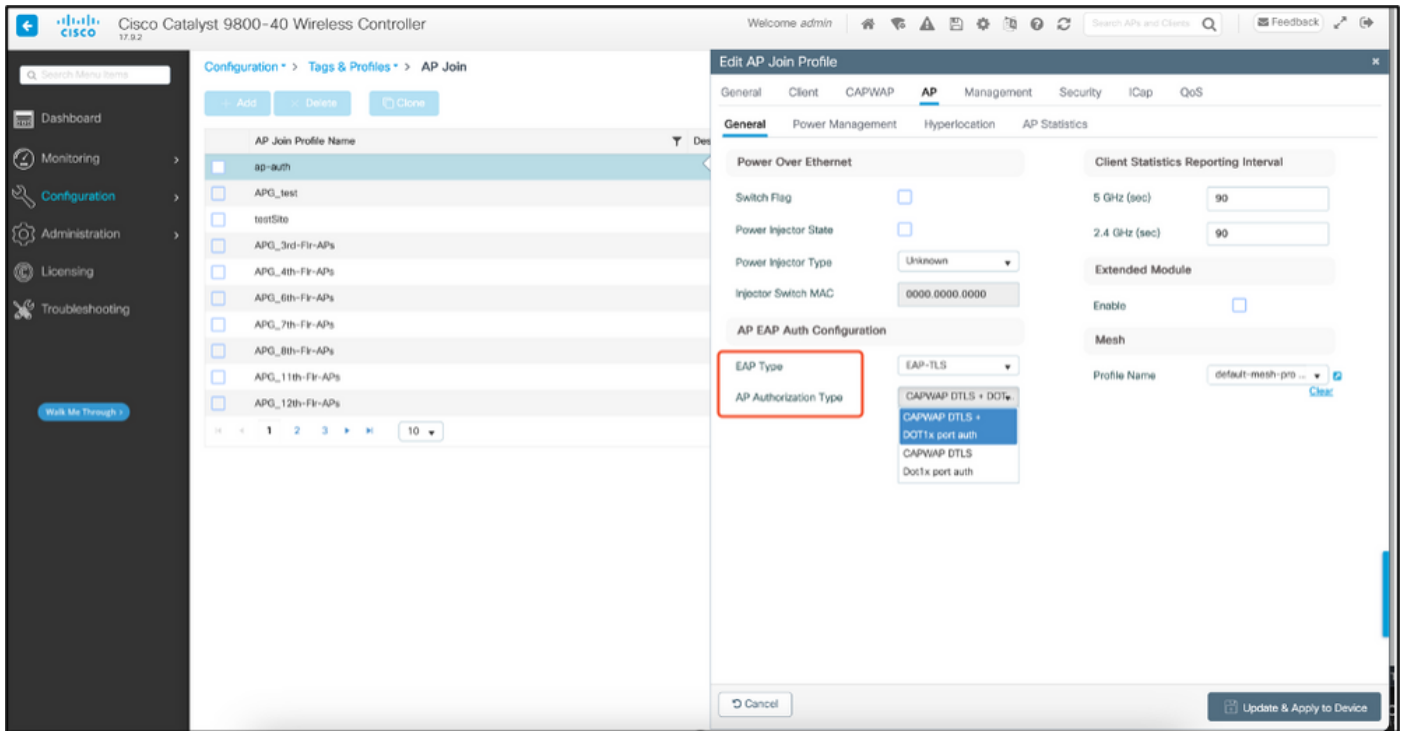


AP有線802.1x認証の設定手順

1. CAPWAP DTLSとともにdot1xポート認証を有効にし、EAPタイプを選択します。
2. AP用のdot1xクレデンシャルを作成します。
3. スイッチポートでdot1xを有効にします。
4. 信頼できる証明書をRADIUSサーバにインストールします。

APの有線802.1x認証GUI設定

1. AP加入プロファイルに移動し、プロファイルをクリックします。
 1. AP > Generalの順にクリックします。「CAPWAP DTLS + dot1x port auth」としてEAPタイプとAP認証タイプを選択します。
 2. Management > Credentialsの順に移動し、AP dot1x authのユーザ名とパスワードを作成します。



APの有線802.1x認証のCLI設定

CLIからAPのdot1xを有効にするには、次のコマンドを使用します。これは、特定の参加プロファイルを使用しているAPの有線認証のみを有効にします。

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

```
9800-40(config)#ap profile ap-auth
9800-40(config-ap-profile)#dot1x cap-type cap-tls
9800-40(config-ap-profile)#dot1x lsc-ap-auth-state both
9800-40(config-ap-profile)#
```

AP有線802.1x認証スイッチの設定

このスイッチ設定は、ラボでAP有線認証を有効にするために使用されます。設計に基づいて異なる設定を行うことができます。

```
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サーバ証明書のインストール

認証は、(サブリカントとして機能している) APとRADIUSサーバの間で行われます。両方が互いの証明書を信頼する必要があります。APにRADIUSサーバ証明書を信頼させる唯一の方法は、AP証明書を発行したSCEP CAによって発行された証明書をRADIUSサーバで使用させることです。

ISEで、Administration > Certificates > Generate Certificate Signing Requestsの順に選択します

CSRを生成し、フィールドにISEノードの情報を入力します。

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)

生成されたテキストは、エクスポートしたり、テキストとしてコピー&ペーストしたりできます

。

Windows CA IPアドレスに移動し、URLに/certsrv/を追加します

Request a certificateをクリックします

← → ↻ Non sécurisé | 192.168.1.98/certsrv/

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

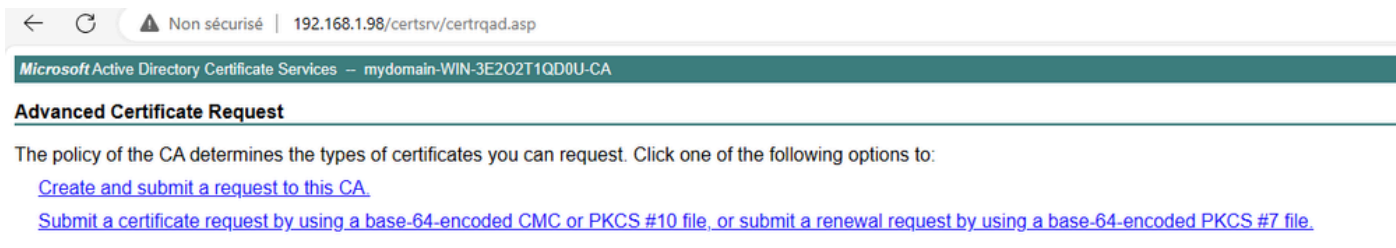
Welcome

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:

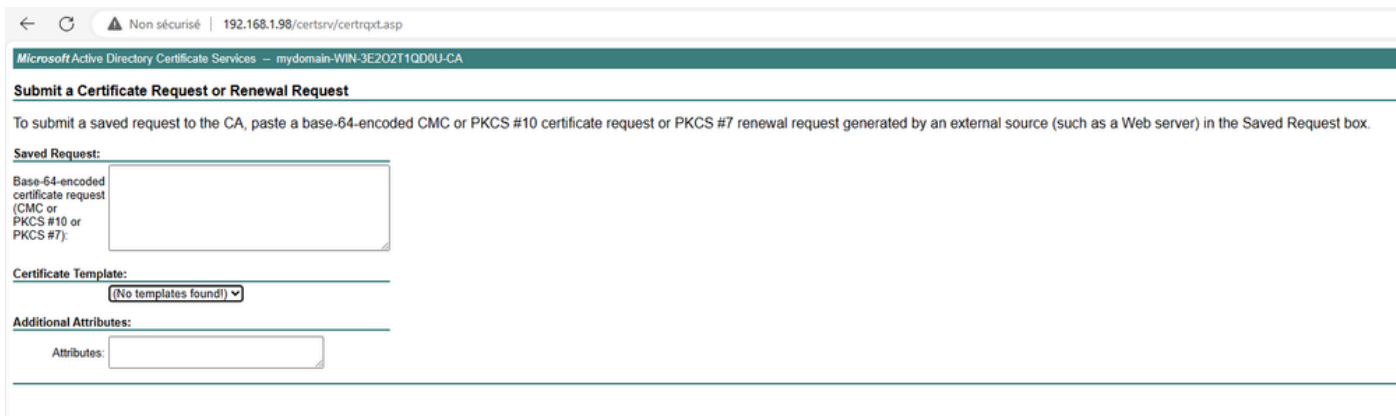
- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

Submit a certificate request by using a base-64をクリックします

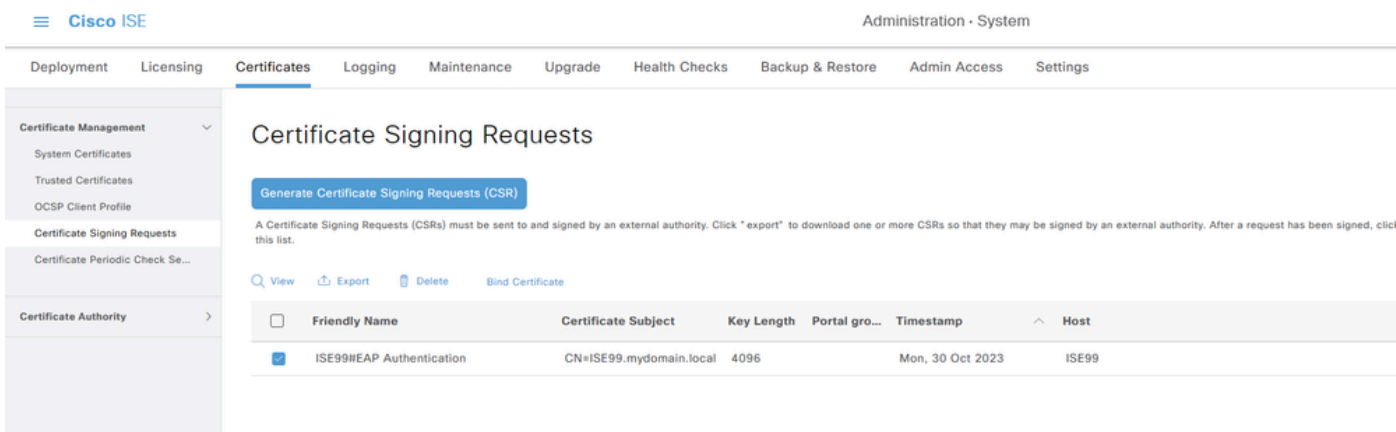


CSRテキストをテキストボックスに貼り付けます。Webサーバ証明書テンプレートを選択します

。



その後、Certificate Signing Requestメニューに戻り、Bind certificateをクリックして、この証明書をISEにインストールできます。その後、Windows Cから取得した証明書をアップロードできます。



AP有線802.1x認証の検証

コンソールからAPにアクセスし、次のコマンドを実行します。

```
#show ap authentication status
```

Ap認証が有効になっていない :

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

ap authを有効にした後のAPからのコンソールログ :

```
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
```

APが正常に認証されました :

```
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 pae state=AUTHENTICATED
supplicant status=authorized
EAP state=SUCCESS
selectedMethod=13 (EAP-TLS)
EAP TLS version=TLSv1.2
EAP TLS cipher=ECDHE-RSA-AES256-GCM-SHA384
tls_session_reused=0
eap_session_id=0d7b91a744885a6e8e460d49fee7d2d5604ca2bdd11f40494a4325dc98d1919af48b9f33ec526f18eda11effcb2ea0238cf95244aaf5f17decf336ad11e88121
AP0CD0.F89A.46E0#
```

WLCの検証 :

```
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
```

認証に成功した後のswitchportインターフェイスのステータス :

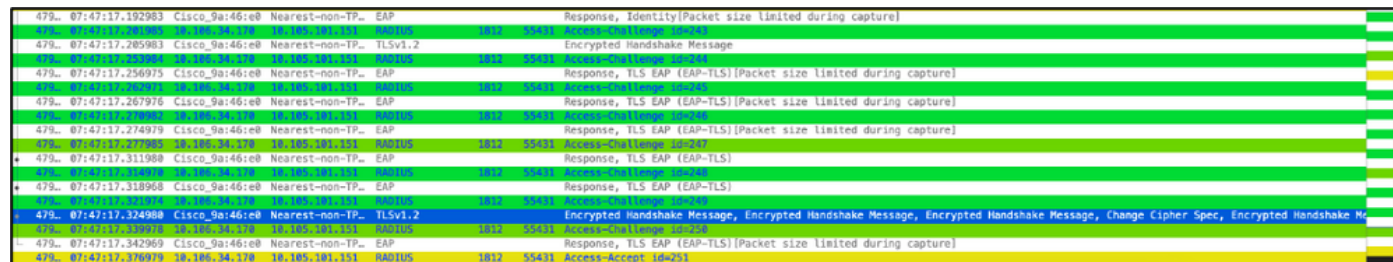
```
Switch#sho authentication sessions interface gigabitEthernet 1/0/2
Interface MAC Address Method Domain Status Fg Session ID
Gi1/0/2 0cd0.f89a.46e0 dot1x DATA Auth 9765690A0000005CCEED0FBF
```

次に、認証が成功したことを示すAPコンソールログの例を示します。

```
[*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
```

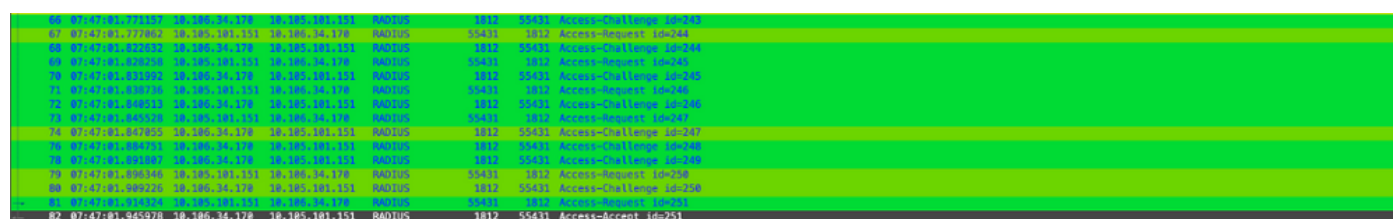
802.1X認証のトラブルシューティング

APアップリンクでPCAPを取得し、RADIUS認証を確認します。認証に成功した場合のスニペットを次に示します。



479.	07:47:17.192983	Cisco_9a:46:e0	Nearest-non-TP...	EAP		Response, Identity[Packet size limited during capture]	
479.	07:47:17.205983	Cisco_9a:46:e0	Nearest-non-TP...	TLV1.2		Encrypted Handshake Message	
479.	07:47:17.256975	Cisco_9a:46:e0	Nearest-non-TP...	EAP		Response, TLS EAP (EAP-TLS)[Packet size limited during capture]	
479.	07:47:17.267976	Cisco_9a:46:e0	Nearest-non-TP...	EAP		Response, TLS EAP (EAP-TLS)[Packet size limited during capture]	
479.	07:47:17.279983	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.	07:47:17.277983	Cisco_9a:46:e0	Nearest-non-TP...	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.	07:47:17.318968	Cisco_9a:46:e0	Nearest-non-TP...	EAP		Response, TLS EAP (EAP-TLS)	
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 M...	
479.	07:47:17.342969	Cisco_9a:46:e0	Nearest-non-TP...	EAP		Response, TLS EAP (EAP-TLS)[Packet size limited during capture]	
479.	07:47:17.376979	10.186.34.178	10.185.101.151	RADIUS	1812	55431	Access-Accept id=251

認証をキャプチャするISEからのTCPdump collect。



80	07:47:18.117893	10.186.34.178	10.185.101.151	RADIUS	1812	55431	Access-Request id=250
80	07:47:18.117893	10.186.34.178	10.185.101.151	RADIUS	1812	55432	Access-Request id=248
80	07:47:18.120338	10.186.34.178	10.185.101.151	RADIUS	1812	55431	Access-Request id=249
79	07:47:18.133002	10.186.34.178	10.185.101.151	RADIUS	1812	55432	Access-Challenge id=248
79	07:47:18.138576	10.186.34.178	10.185.101.151	RADIUS	1843	5821	Access-Request id=249
79	07:47:18.140812	10.186.34.178	10.185.101.151	RADIUS	1812	55432	Access-Challenge id=249
79	07:47:18.140812	10.186.34.178	10.185.101.151	RADIUS	1843	5821	Access-Request id=247
78	07:47:18.147803	10.186.34.178	10.185.101.151	RADIUS	1812	55432	Access-Challenge id=247
78	07:47:18.148062	10.186.34.178	10.185.101.151	RADIUS	1843	5840	Access-Challenge id=246
78	07:47:18.148062	10.186.34.178	10.185.101.151	RADIUS	1812	55431	Access-Challenge id=246
78	07:47:18.150516	10.186.34.178	10.185.101.151	RADIUS	1843	5821	Access-Request id=250
80	07:47:18.149826	10.186.34.178	10.185.101.151	RADIUS	1812	55431	Access-Challenge id=250
80	07:47:18.154524	10.186.34.178	10.185.101.151	RADIUS	1843	5821	Access-Request id=251
82	07:47:18.145978	10.186.34.178	10.185.101.151	RADIUS	1812	55431	Access-Accept id=251

認証中に問題が確認された場合は、APの有線アップリンクとISE側からの同時パケットキャプチャが必要になります。

APのdebugコマンド：

```
#debug ap authentication packet
```

関連情報

- [シスコテクニカルサポートおよびダウンロード](#)
- [AireOSを使用するAPでの802.1Xの設定](#)
- [LSC用の9800コンフィギュレーションガイド](#)
- [9800のLSC設定例](#)
- [9800上のAP用の802.1Xの設定](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。