ISE内部CAを使用した9800 WLCでのEAP-TLSの設定

内容

はじめに

このドキュメントでは、Identity Services Engine(ISE)の認証局を使用してユーザを認証するEAP-

TLS認証について説明します。

前提条件

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：17.09.04aを実行するC9800-40-K9
- Cisco ISE：バージョン3パッチ4の実行
- APモデル：C9130AXI-D
- スイッチ：9200-L-24P

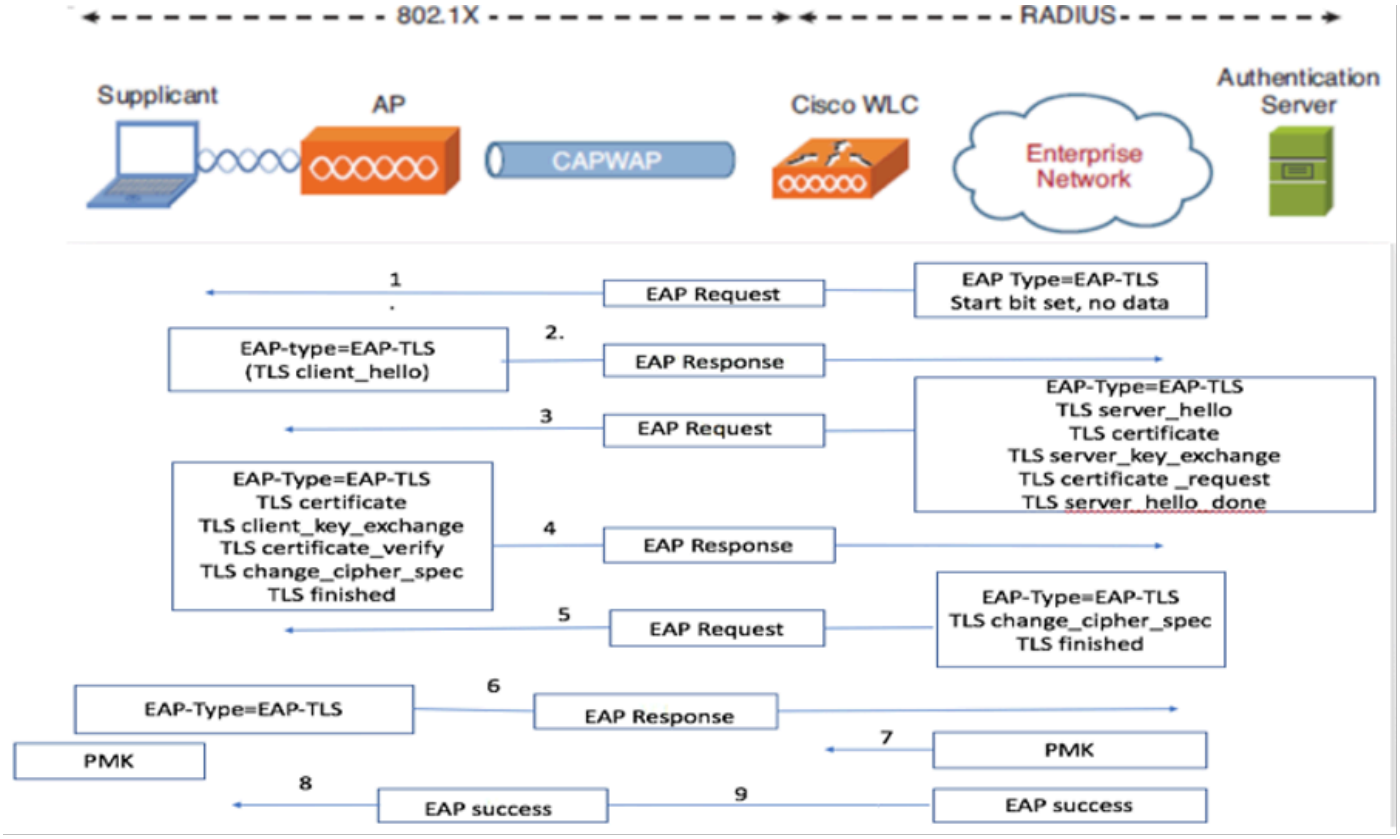
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

ほとんどの組織には、EAP-TLS認証のためにエンドユーザに証明書を発行する独自のCAがあります。ISEには、EAP-TLS認証で使用するユーザの証明書の生成に使用できる組み込みの認証局が含まれています。本格的なCAを使用できないシナリオでは、ユーザ認証にISE CAを使用するのが有利です。

このドキュメントでは、ISE CAを効果的に使用してワイヤレスユーザを認証するために必要な設定手順の概要を説明します。EAP-TLS認証フロー

EAP-TLS認証フロー



EAP-TLS認証フロー

EAP-TLSフローの手順

1. ワイヤレス クライアントはアクセス ポイント（AP）を関連付けます。
2. この段階では、APはデータ送信を許可せず、認証要求を送信します。
3. サプリカントとして動作するクライアントは、EAP応答IDで応答します。
4. ワイヤレスLANコントローラ(WLC)は、ユーザID情報を認証サーバに転送します。
5. RADIUSサーバは、EAP-TLS開始パケットでクライアントに応答します。
6. EAP-TLS通信はこの時点から開始されます。
7. クライアントは、暗号がNULLに設定されたclient_helloハンドシェイクメッセージを含むEAP-Responseを認証サーバに返信します。
8. 認証サーバは、次の内容を含むAccess-Challengeパケットで応答します。

```
TLS server_hello
Handshake message
Certificate
Server_key_exchange
Certificate request
Server_hello_done
```

9. クライアントは、次を含むEAP-Responseメッセージで応答します。

```
Certificate (for server validation)
Client_key_exchange
```

```
Certificate_verify (to verify server trust)
Change_cipher_spec
TLS finished
```

10. クライアント認証が成功すると、RADIUSサーバは次の内容を含むAccess-Challengeを送信します。

```
Change_cipher_spec
Handshake finished message
```

11. クライアントはハッシュを検証してRADIUSサーバを認証します。

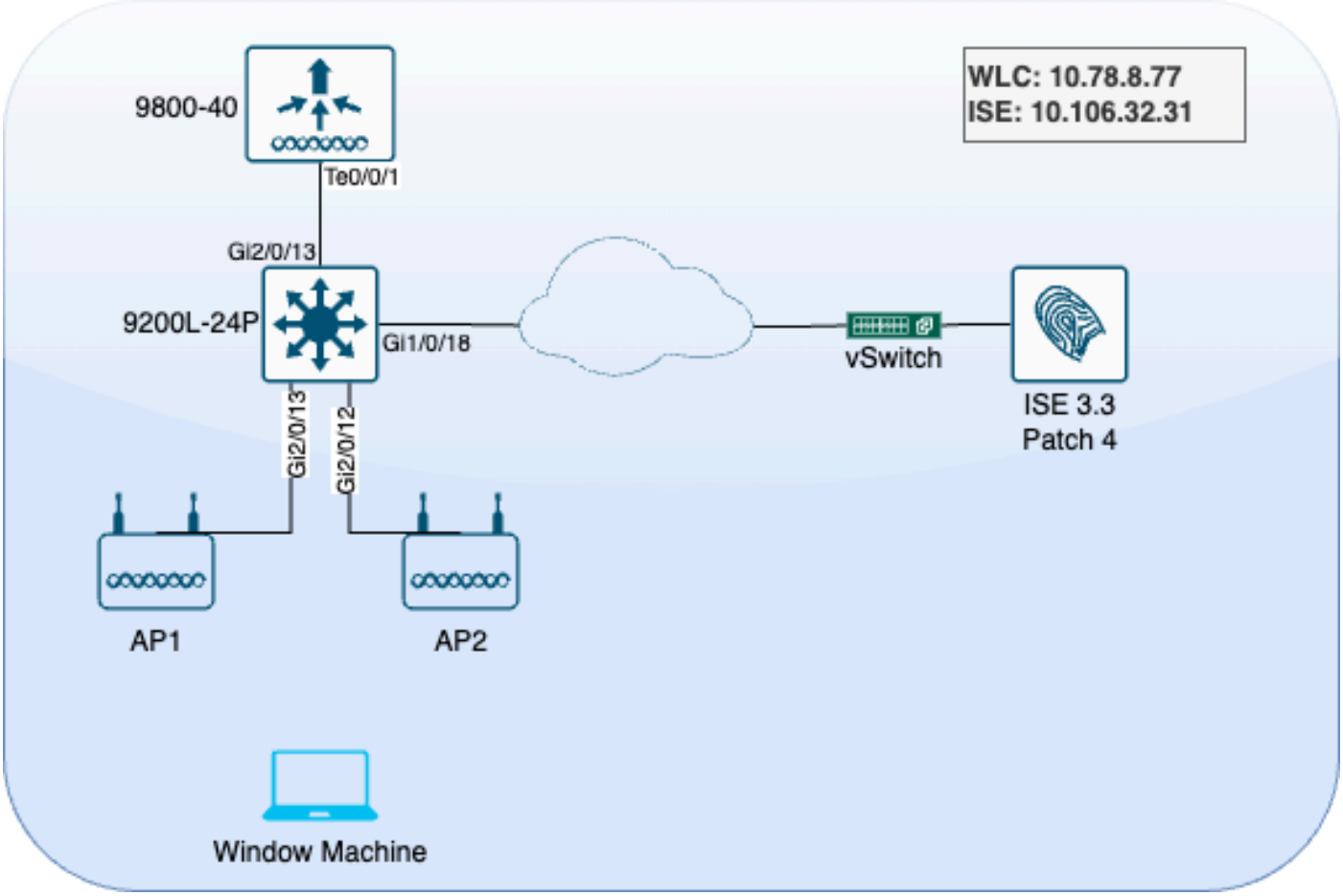
12. TLSハンドシェイク中に、新しい暗号キーがシークレットから動的に取得されます。

13. EAP-Successメッセージがサーバからオーセンティケータに送信され、次にサプリカントに送信されます。

14. EAP-TLSが有効なワイヤレスクライアントがワイヤレスネットワークにアクセスできるようになりました。

設定

ネットワーク図



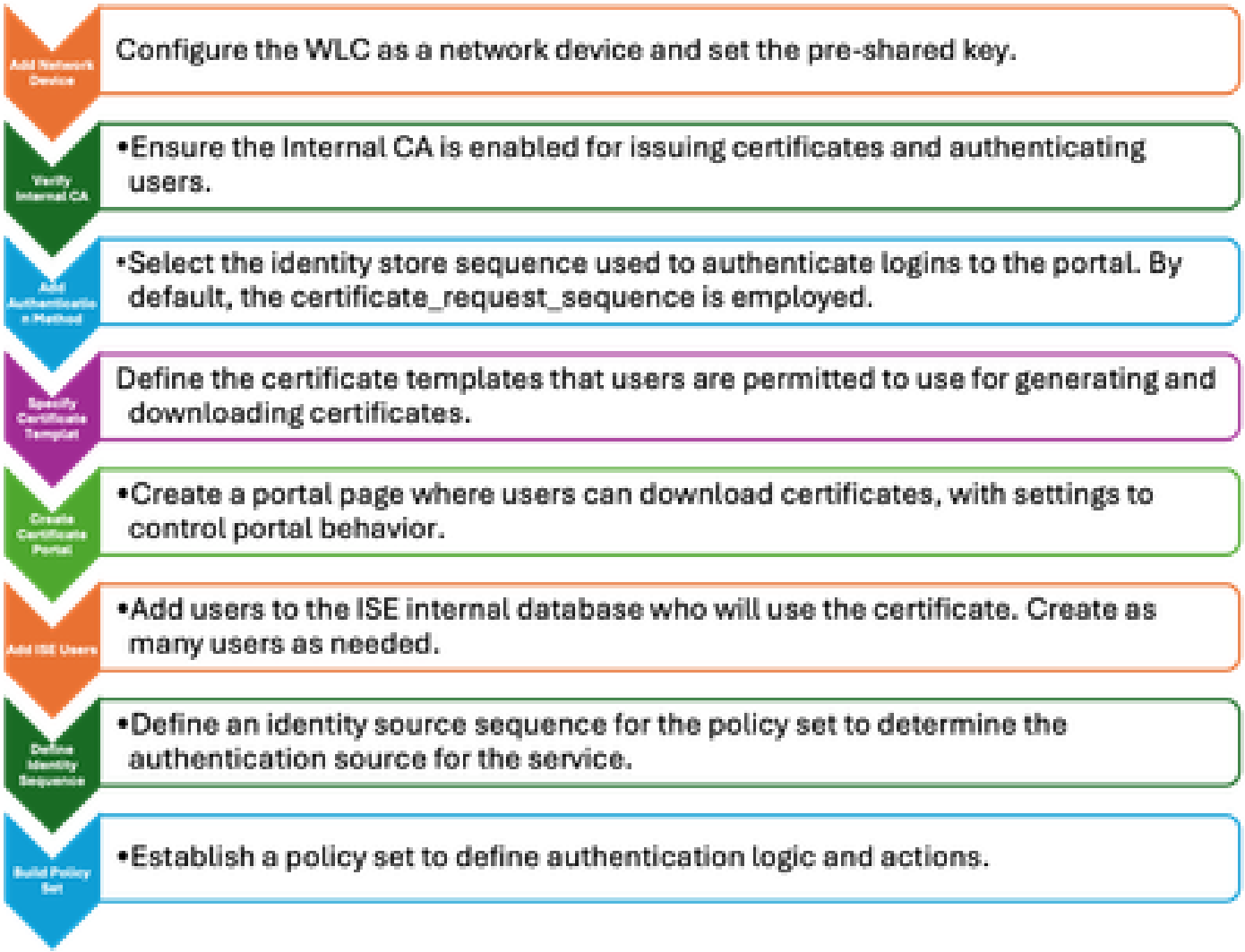
ラボのトポロジ

コンフィギュレーション

このセクションでは、ISEと9800 WLCの2つのコンポーネントを設定します。

ISE 設定

ISEサーバの設定手順を次に示します。 各ステップには、視覚的なガイダンスを提供するために、このセクションのスクリーンショットが添付されています。

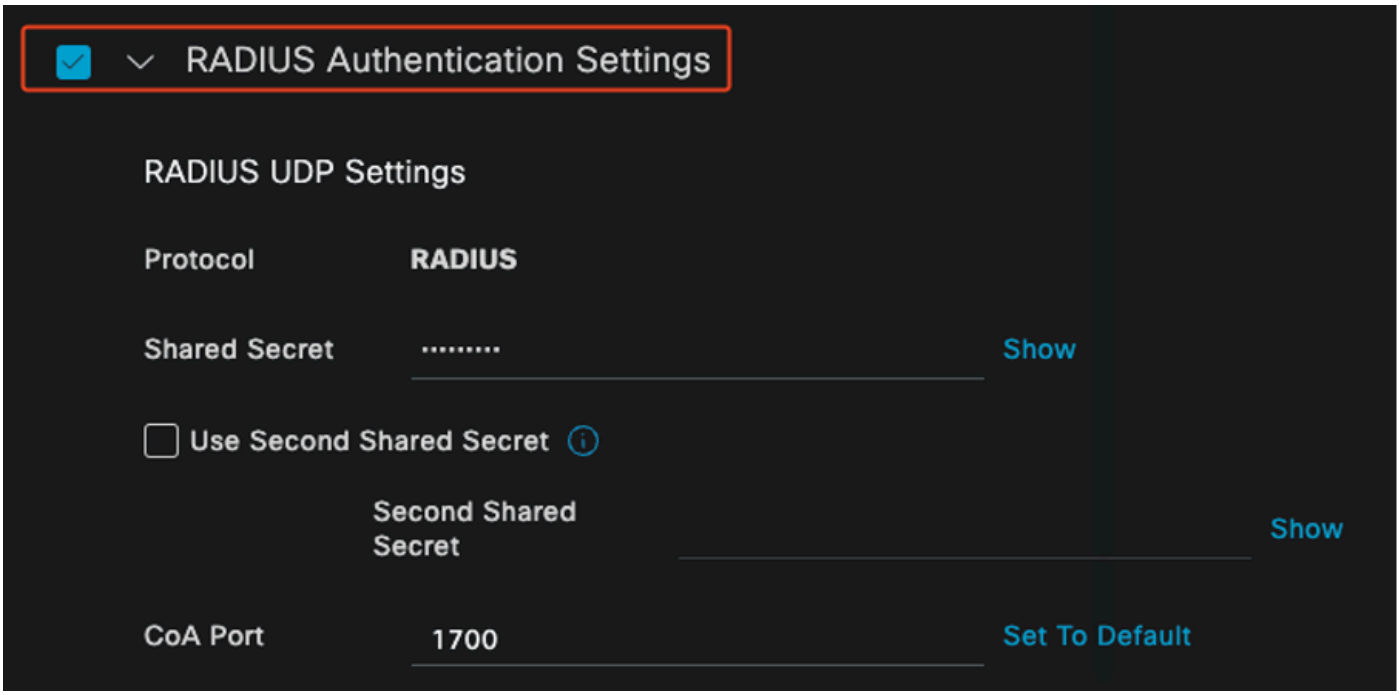


ISEサーバの設定手順

ネットワークデバイスの追加

ワイヤレスLANコントローラ(WLC)をネットワークデバイスとして追加するには、次の手順を使用します。

1. [管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワークデバイス（Network Devices）] に移動します。
2. +Addアイコンをクリックして、WLCの追加プロセスを開始します。
3. 適切な通信を有効にするために、事前共有キーがWLCとISEサーバの両方に一致していることを確認します。
4. すべての詳細を正しく入力したら、左下隅にあるSubmitをクリックして、設定を保存します

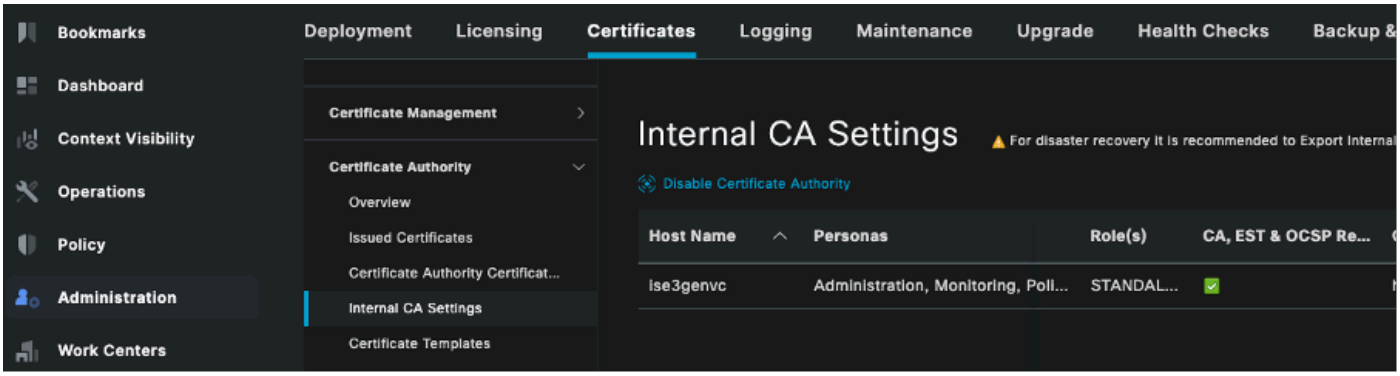


ネットワークデバイスの追加

内部CAの確認

内部認証局(CA)の設定を確認するには、次の手順を実行します。

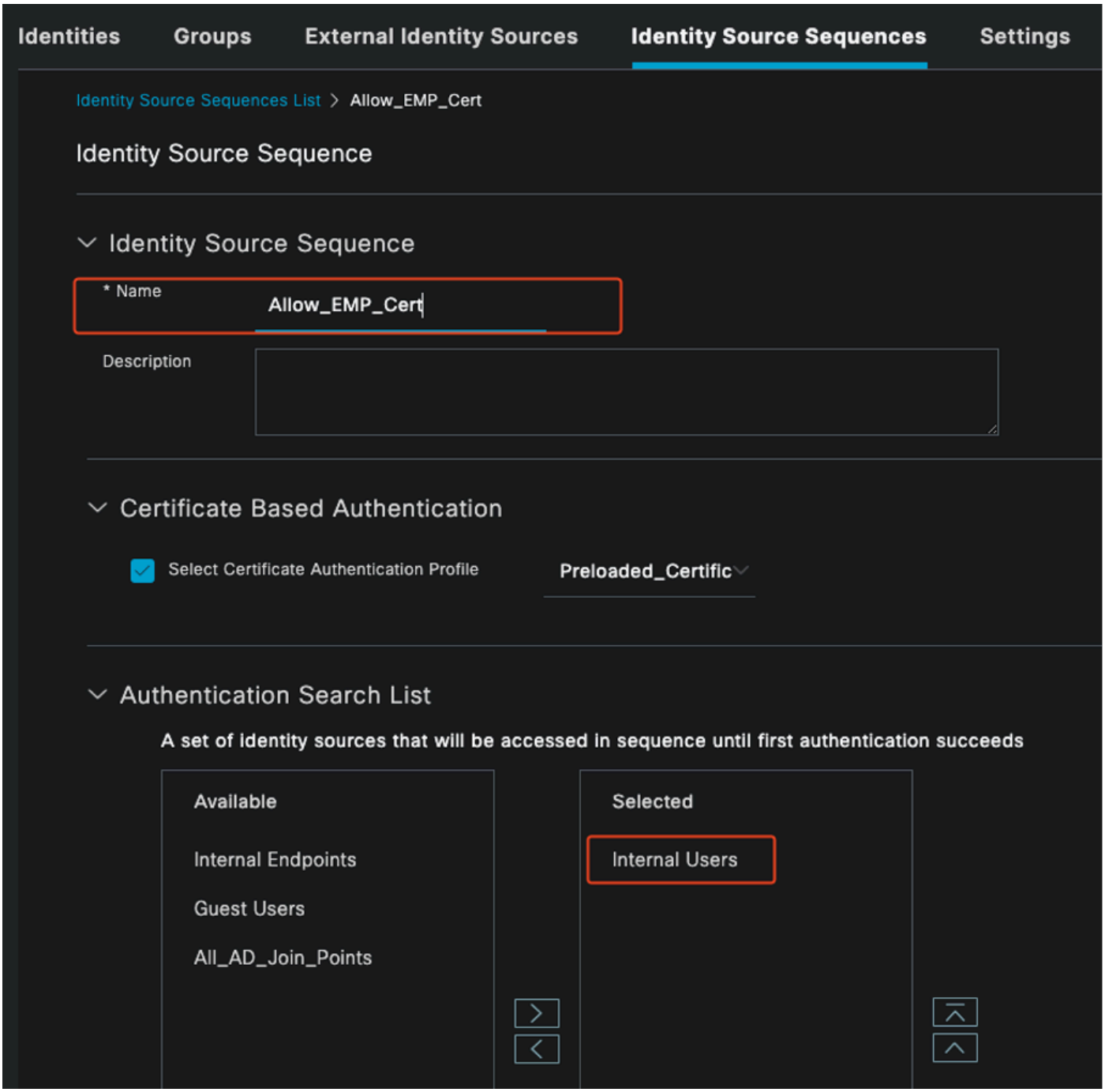
1. Administration > System > Certificates > Certificate Authority > Internal CA Settingsの順に選択します。
2. 内部CAがアクティブであることを確認するために、CA列が有効になっていることを確認します。



内部CAの確認

認証方法の追加

Administration > Identity Management > Identity Source Sequencesの順に移動します。ポータルログインソースを制御するカスタムIDシーケンスを追加します。



認証メソッド

証明書テンプレートの指定

証明書テンプレートを指定するには、次の手順を実行します。

ステップ 1：Administration > System > Certificates > Certificate Authority > Certificate Templatesの順に移動します。

ステップ 2：+Addアイコンをクリックして、新しい証明書テンプレートを作成します。

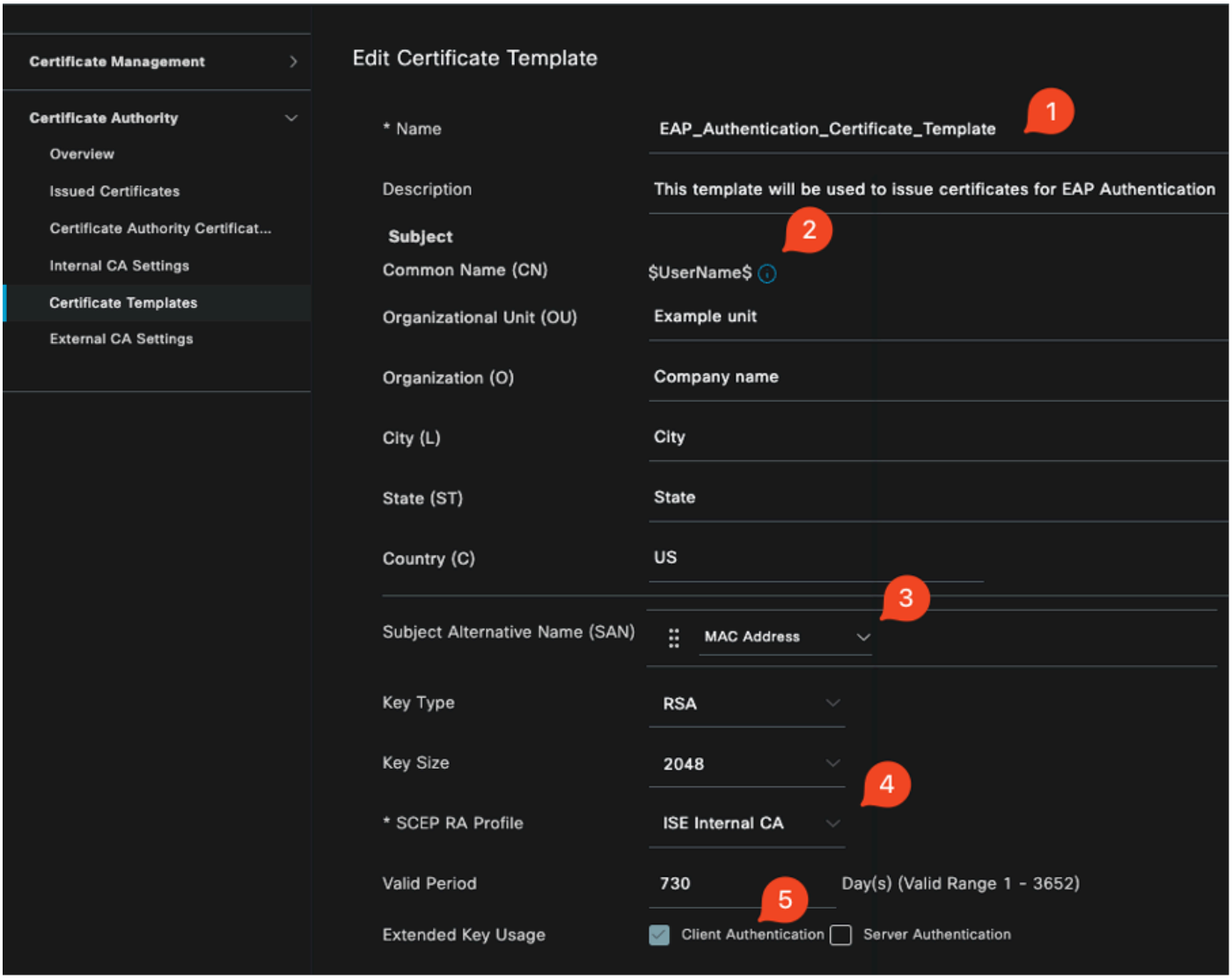
2.1テンプレートのISEサーバにローカルな一意の名前を指定します。

2.2共通名(CN)が$UserName$に設定されていることを確認します。

2.3サブジェクト代替名(SAN)がMACアドレスにマッピングされていることを確認する。

2.4 SCEP RAプロファイルをISE内部CAに設定します。

2.5拡張キーの使用セクションで、クライアント認証をイネーブルにします。



証明書テンプレート

証明書ポータルの作成

クライアント証明書生成用の証明書ポータルを作成するには、次の手順を使用します。

ステップ 1：Administration > Device Portal Management > Certificate Provisioningの順に移動します。

ステップ 2：Createをクリックして、新しいポータルページを設定します。

ステップ 3：ポータルを簡単に識別するための一意の名前を指定します。

3.1.動作させるポータルのポート番号を選択し、これを8443に設定します。

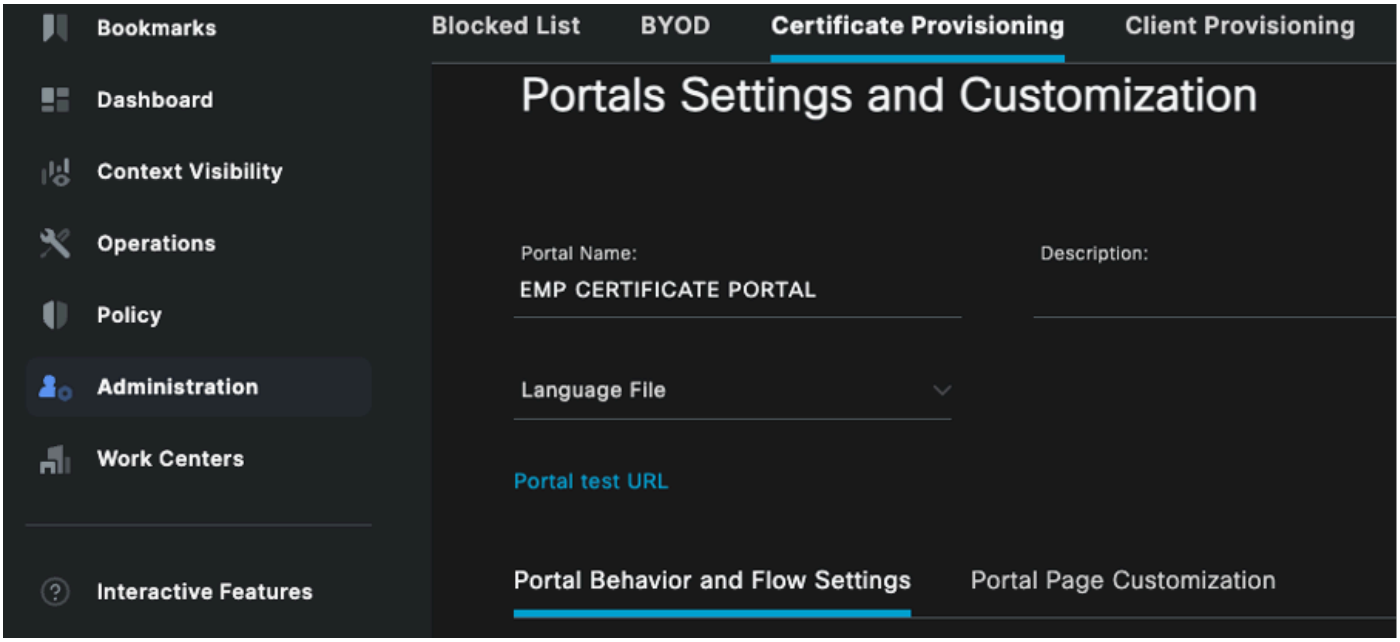
3.2. ISEがこのポータルをリッスンするインターフェイスを指定します。

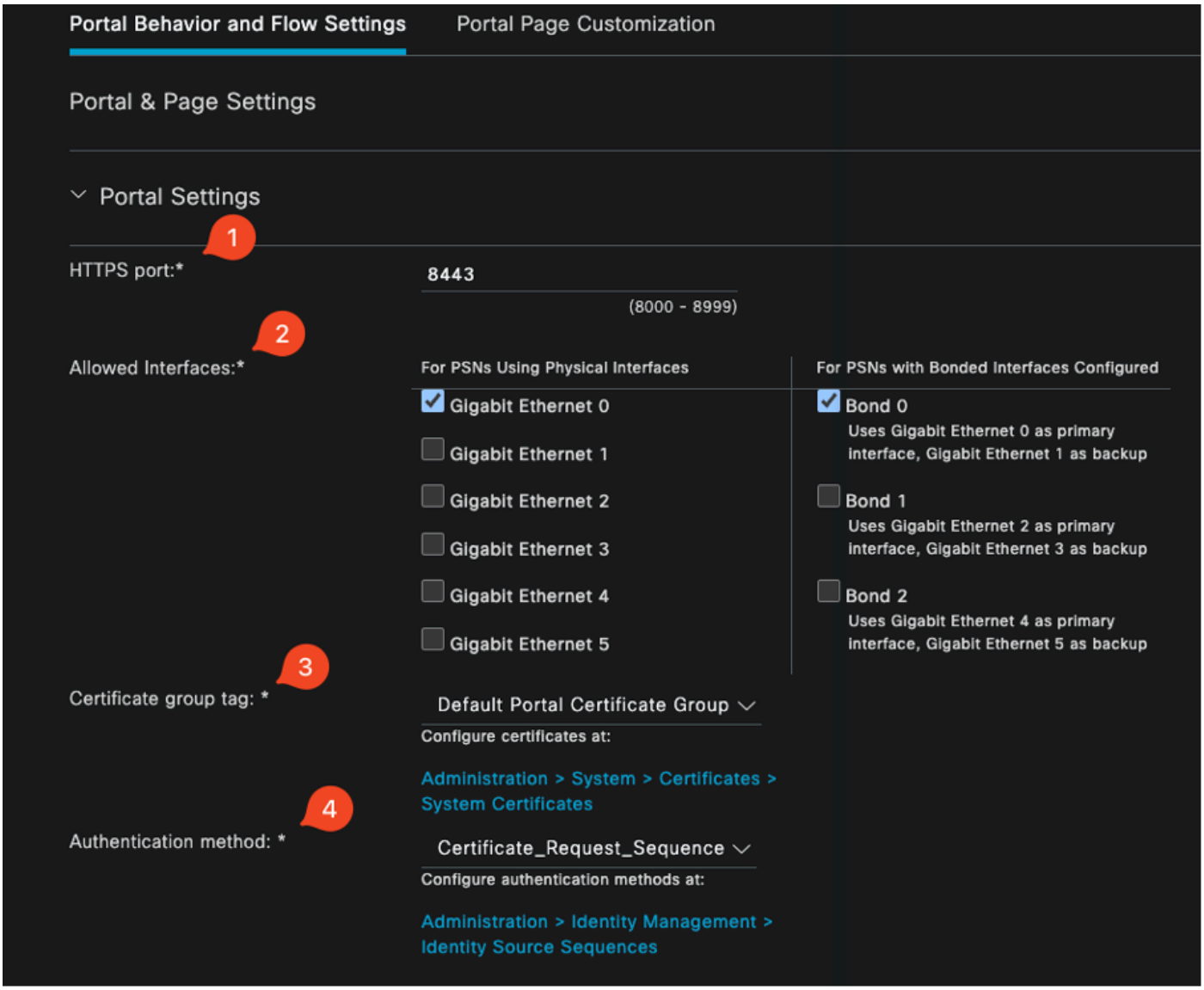
3.3.デフォルトポータル証明書グループとしてCertificate Group Tagを選択します。

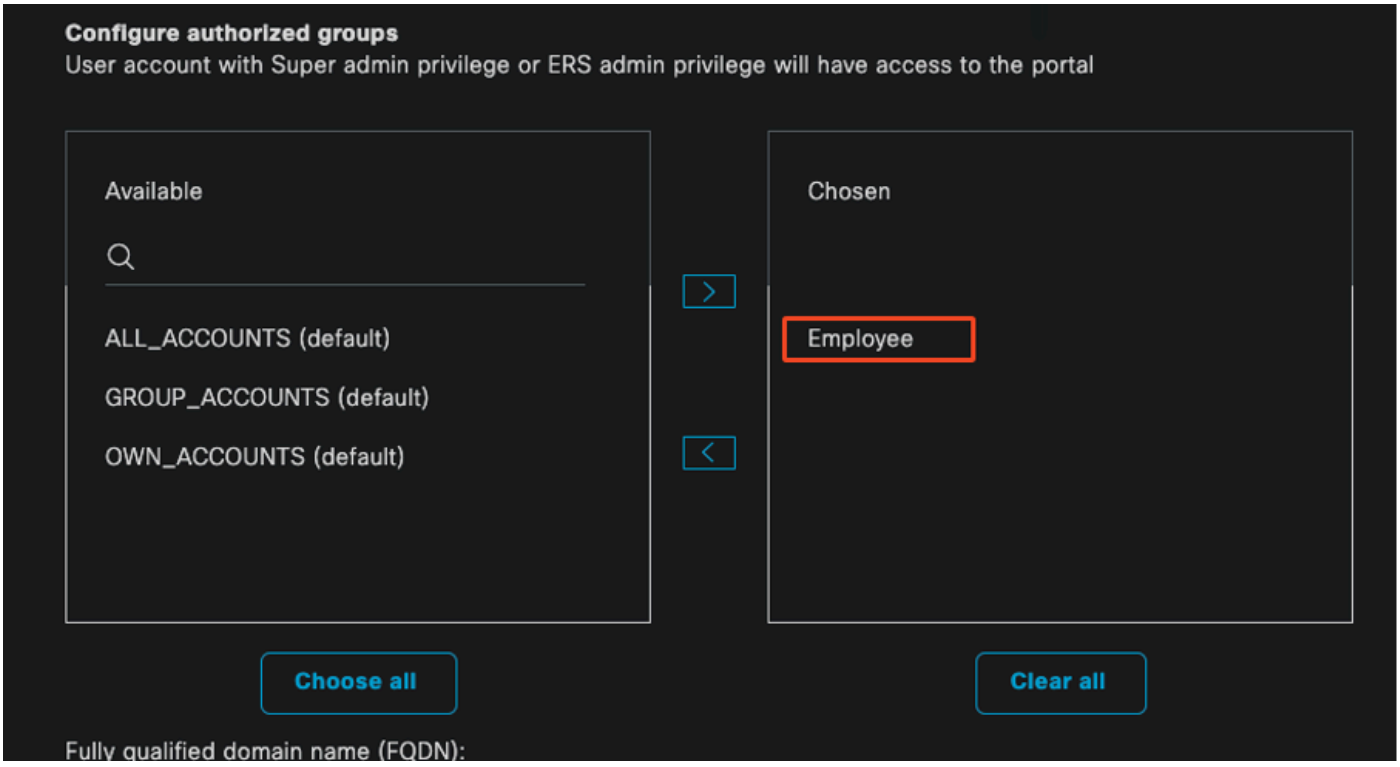
3.4.認証方式を選択します。これは、このポータルへのログインの認証に使用されるIDストアシーケンスを示します。

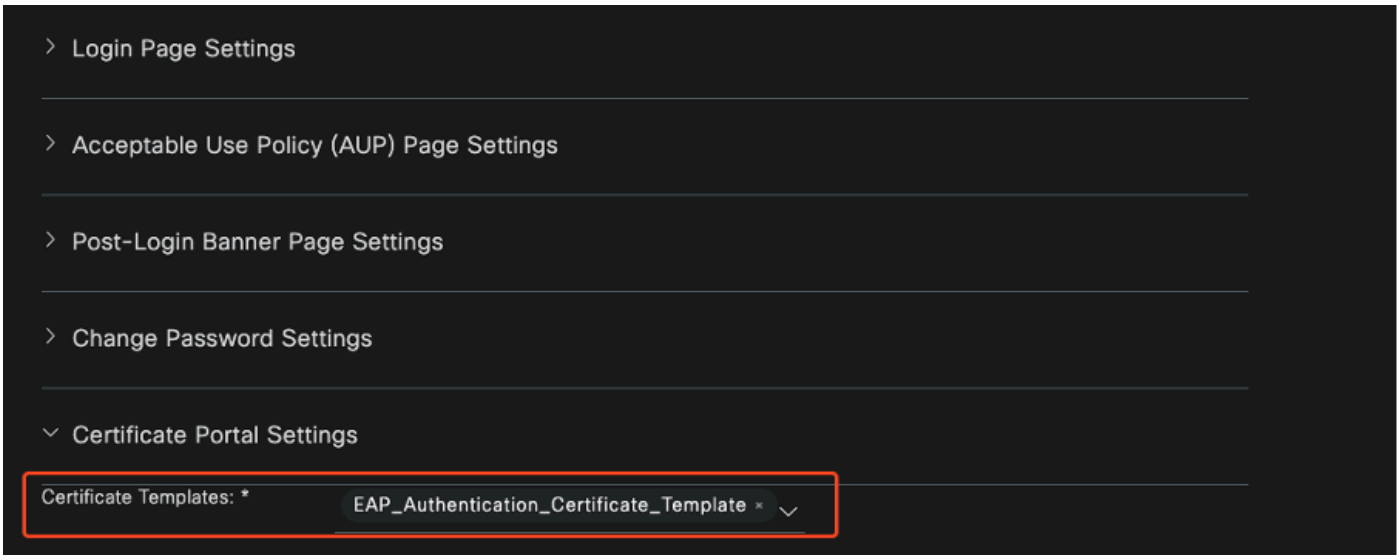
3.5.メンバーがポータルにアクセスできる許可されたグループを含める。たとえば、ユーザがこのグループに属している場合、Employeeユーザグループを選択します。

3.6.証明書プロビジョニング設定で許可される証明書テンプレートを定義する。



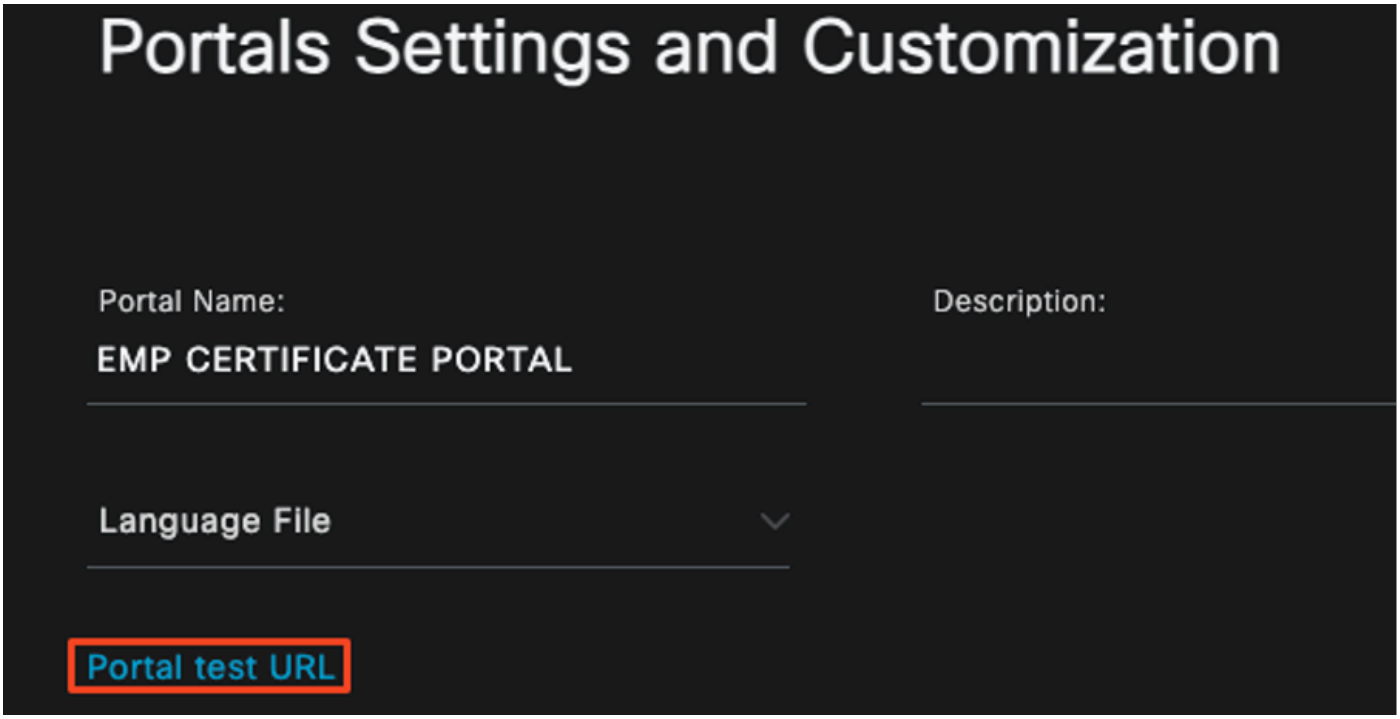

Portal Behavior and Flow Settings
Portal Page Customization
Portal & Page Settings
Portal Settings
1
HTTPS port:*
8443
(8000 - 8999)
2
Allowed Interfaces:*
For PSNs Using Physical Interfaces
Gigabit Ethernet 0
Gigabit Ethernet 1
Gigabit Ethernet 2
Gigabit Ethernet 3
Gigabit Ethernet 4
Gigabit Ethernet 5
For PSNs with Bonded Interfaces Configured
Bond 0
Uses Gigabit Ethernet 0 as primary interface, Gigabit Ethernet 1 as backup
Bond 1
Uses Gigabit Ethernet 2 as primary interface, Gigabit Ethernet 3 as backup
Bond 2
Uses Gigabit Ethernet 4 as primary interface, Gigabit Ethernet 5 as backup
3
Certificate group tag: *
Default Portal Certificate Group
Configure certificates at:
Administration > System > Certificates > System Certificates
4
Authentication method: *
Certificate_Request_Sequence
Configure authentication methods at:
Administration > Identity Management > Identity Source Sequences


Configure authorized groups
User account with Super admin privilege or ERS admin privilege will have access to the portal
Available
ALL_ACCOUNTS (default)
GROUP_ACCOUNTS (default)
OWN_ACCOUNTS (default)
Chosen
Employee
Choose all
Clear all
Fully qualified domain name (FQDN):

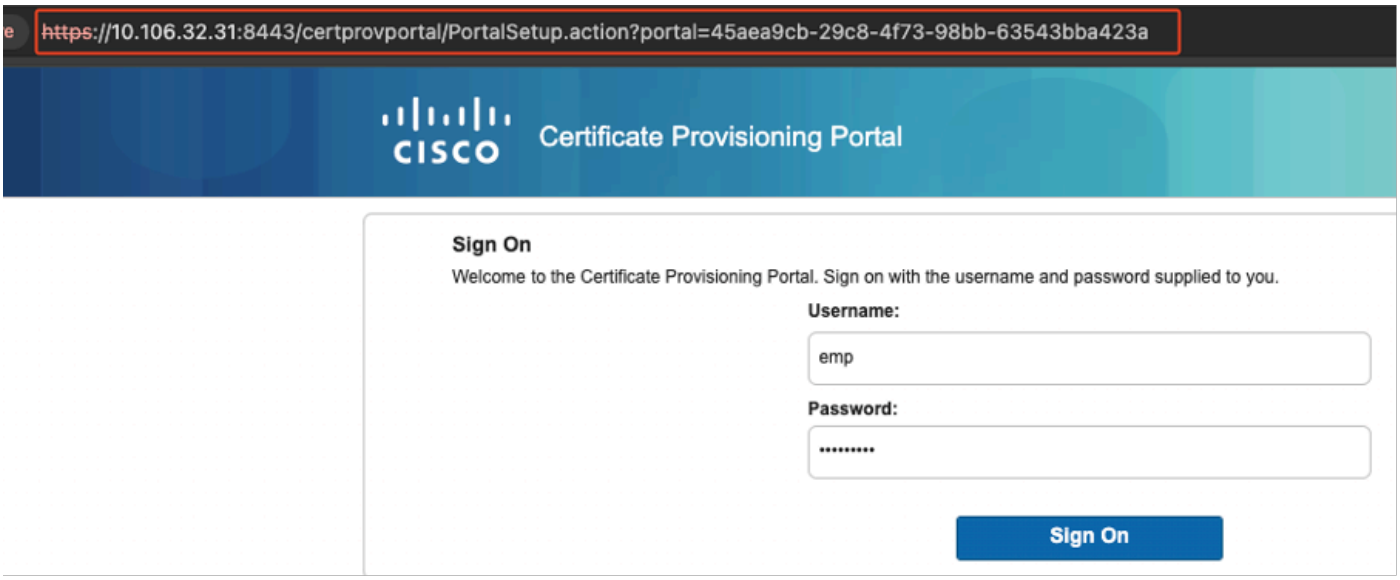


証明書ポータルの設定

このセットアップが完了したら、ポータルテストURLをクリックしてポータルをテストできます。この操作を実行すると、ポータルページが開きます。



テストポータルページのURL

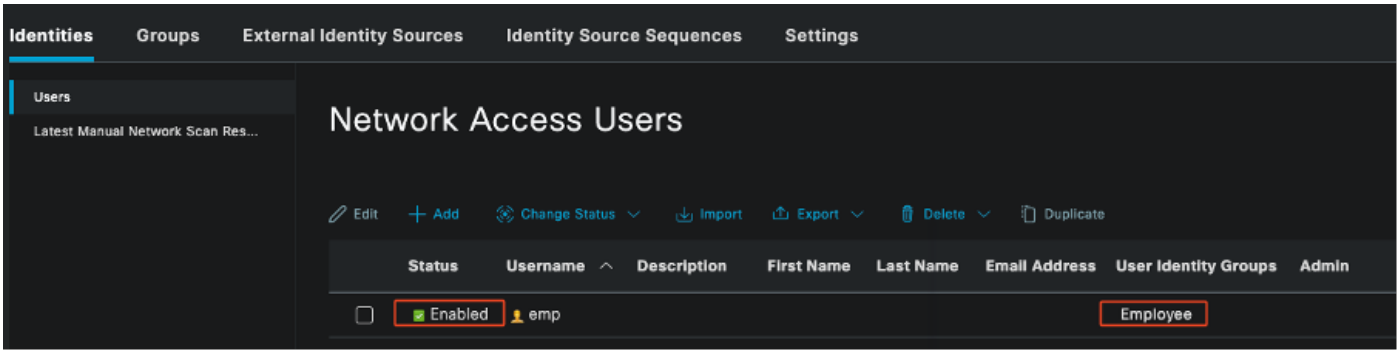


ポータル ページ

内部ユーザの追加

証明書ポータルで認証するユーザを作成するには、次の手順を実行します。

1. Administration > Identity Management > Identities > Usersの順に選択します。
2. システムにユーザを追加するオプションをクリックします。
3. ユーザが属するユーザIDグループを選択します。この例では、ユーザをEmployeeグループに割り当てます。



内部ユーザの追加

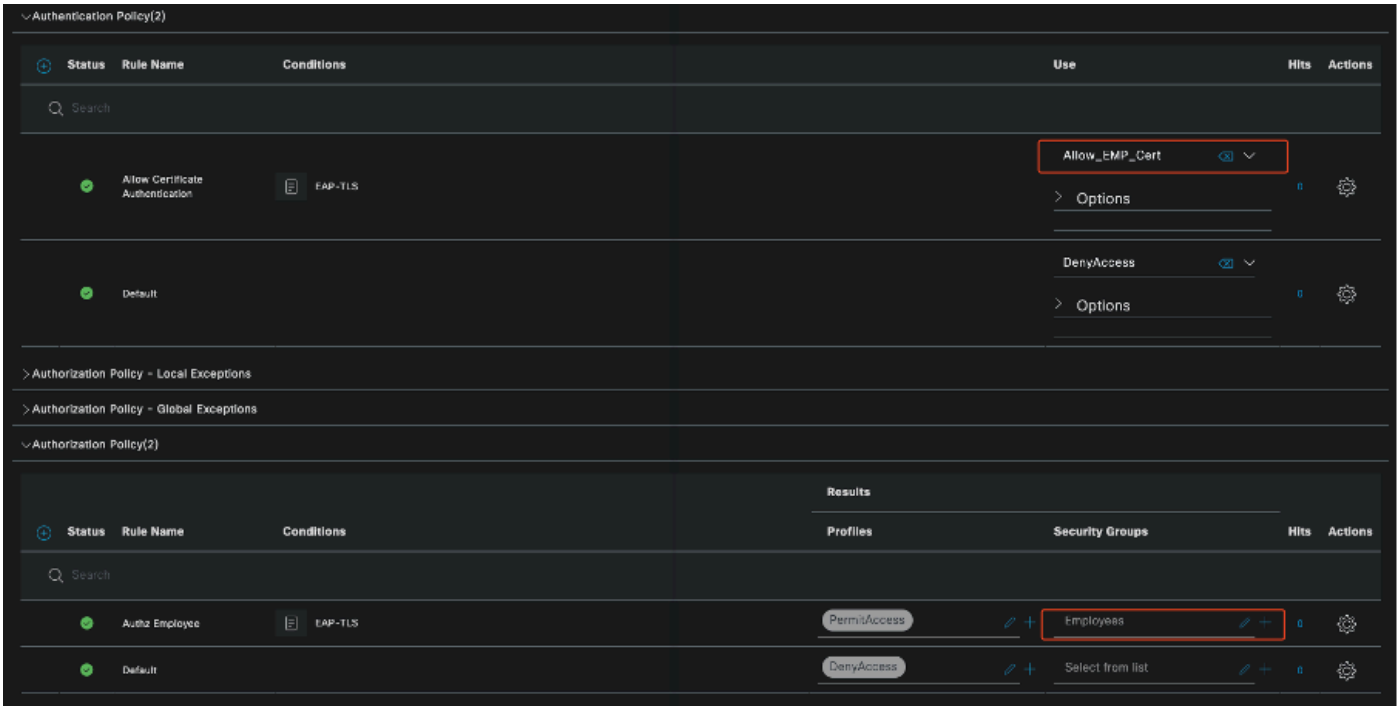
ISE証明書プロビジョニングポータルとRADIUSポリシーの設定

前のセクションでは、ISE証明書プロビジョニングポータルのセットアップについて説明しました。次に、ユーザ認証を許可するようにISE RADIUSポリシーセットを設定します。

1. ISE RADIUSポリシーセットの設定
2. Policy > Policy Setsの順に移動します。
3. プラス記号(+)をクリックして、新しいポリシーセットを作成します。

この例では、証明書を使用してユーザを認証するように設計された簡単なポリシーセットをセットアップします。

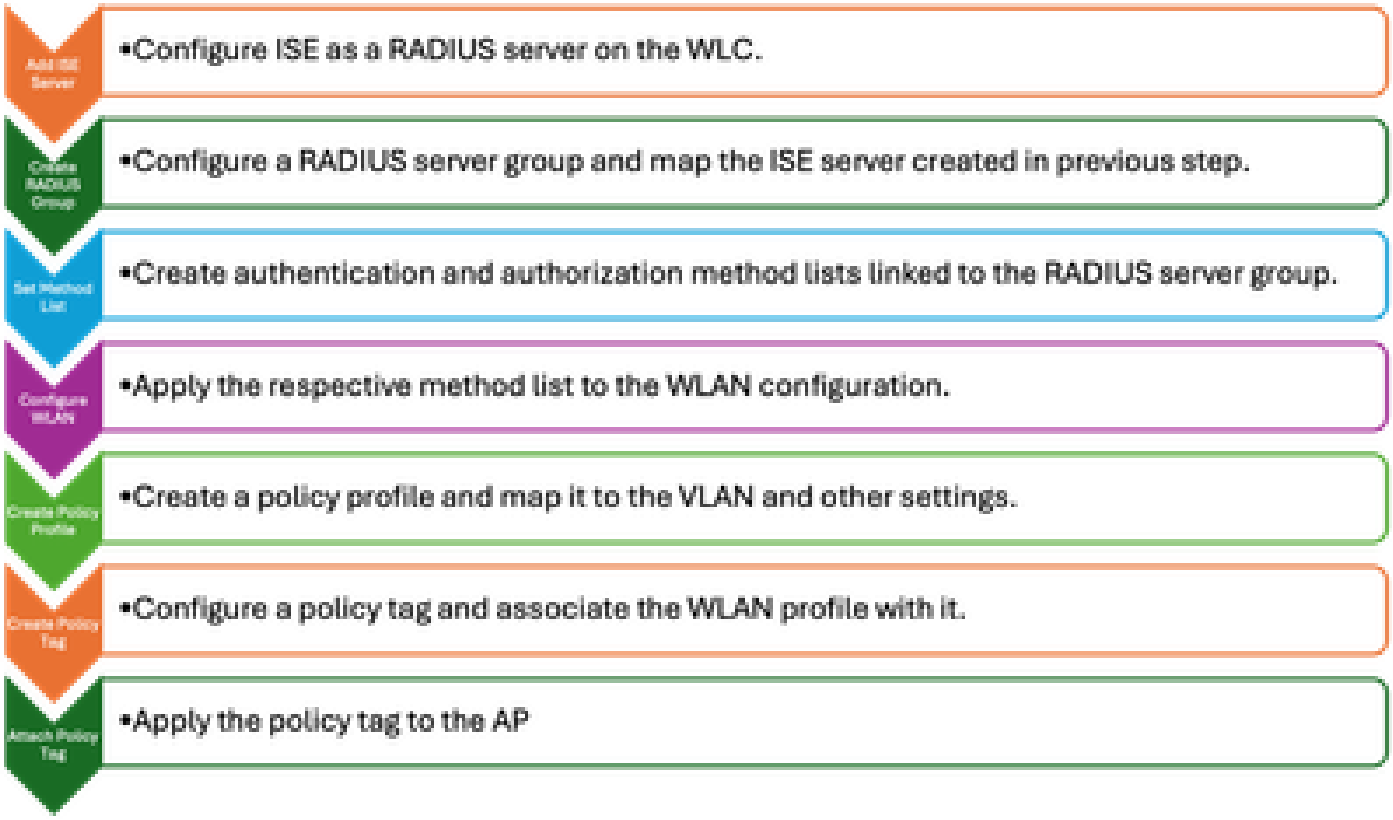
ポリシーセット



認証ポリシーと許可ポリシーを示すポリシーセット

9800 WLCの設定

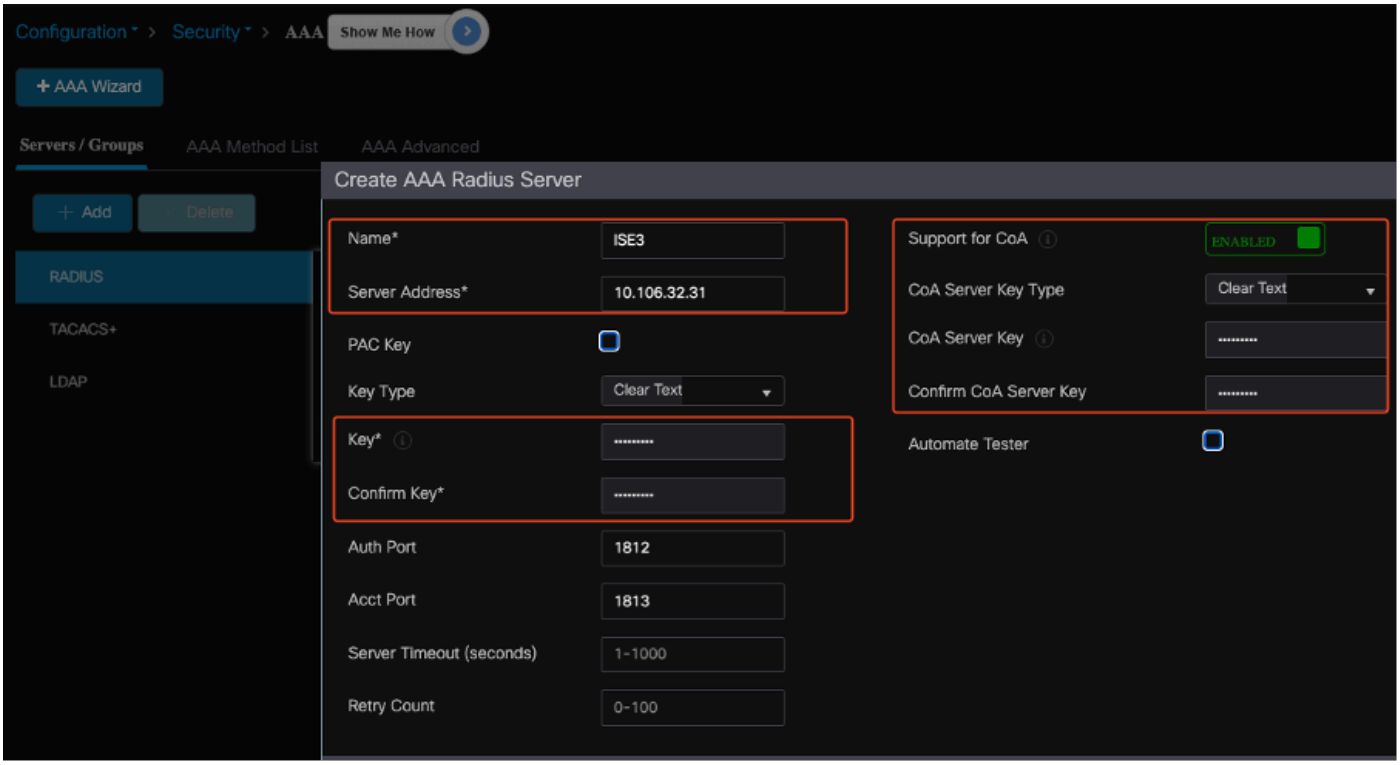
9800 WLCの設定手順を次に示します。 各ステップには、視覚的なガイダンスを提供するために、このセクションのスクリーンショットが添付されています。



WLCの設定手順

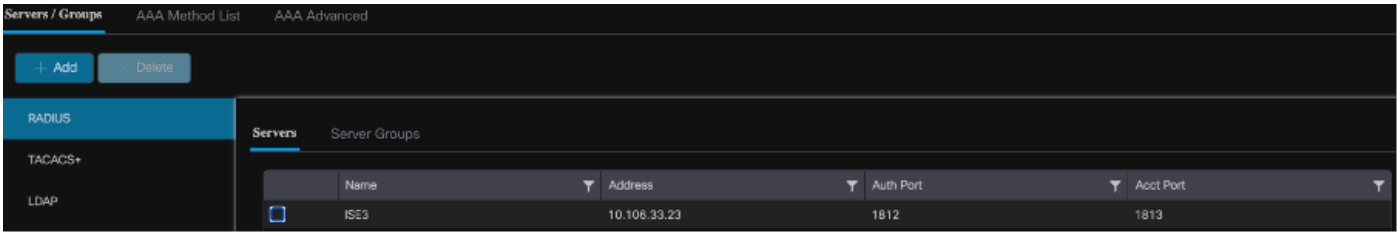
ISEサーバの9800 WLCへの追加

1. ISEサーバを9800ワイヤレスLANコントローラ(WLC)と統合するには、次の手順を使用します。
2. Configuration > Security > AAAの順に選択します。
3. Addボタンをクリックして、WLC設定にISEサーバを含めます。



WLCでのISEサーバの追加

サーバが追加されると、サーバのリストに表示されます。

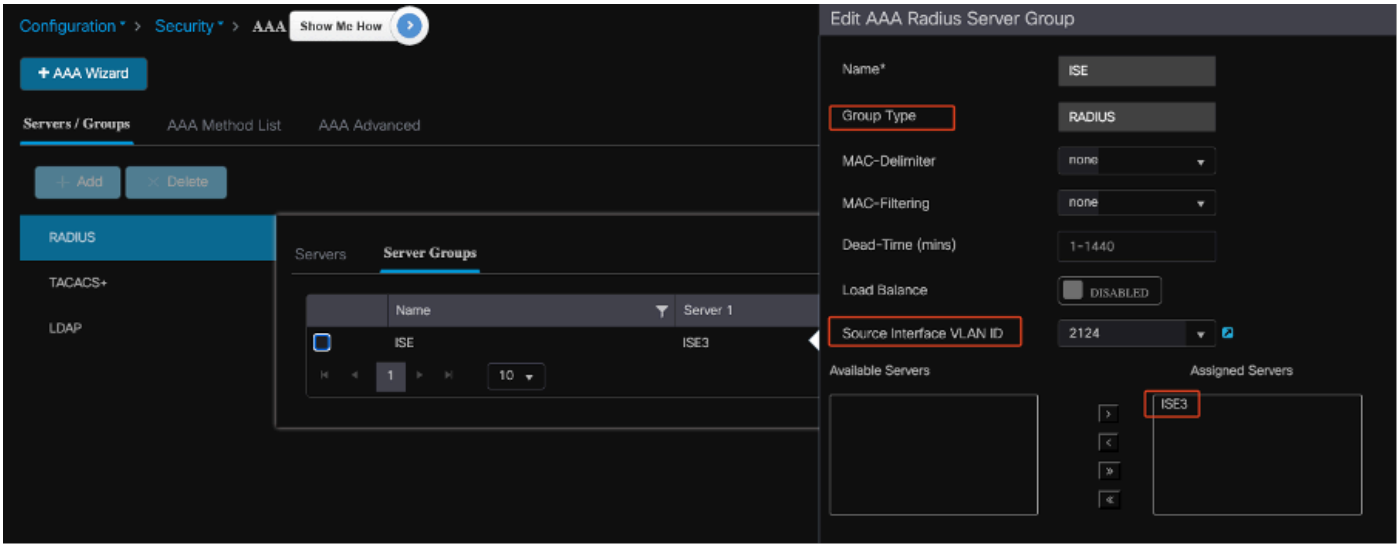


RADIUSサーバの表示

9800 WLCでのサーバグループの追加

9800ワイヤレスLANコントローラでサーバグループを追加するには、次の手順を実行します。

1. Configuration > Security > AAAの順に移動します。
2. Server Groupタブをクリックし、次にAddをクリックして新しいサーバグループを作成します。

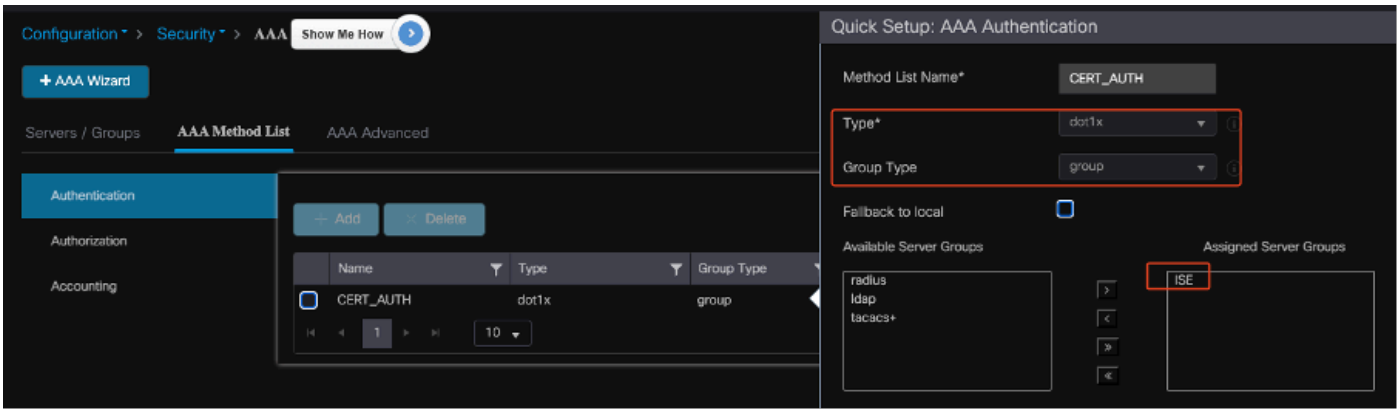


RADIUSサーバグループへのISEサーバのマッピング

9800 WLC上でのAAA方式リストの設定

サーバグループを作成した後、次の手順を使用して認証方式リストを設定します。

1. Configuration > Security > AAA > AAA Method Listの順に移動します。
2. Authenticationタブで、新しい認証方式リストを追加します。
3. タイプをdot1xに設定します。
4. グループタイプとしてgroupを選択します。
5. 先ほど作成したISEサーバグループをサーバグループとして含めます。

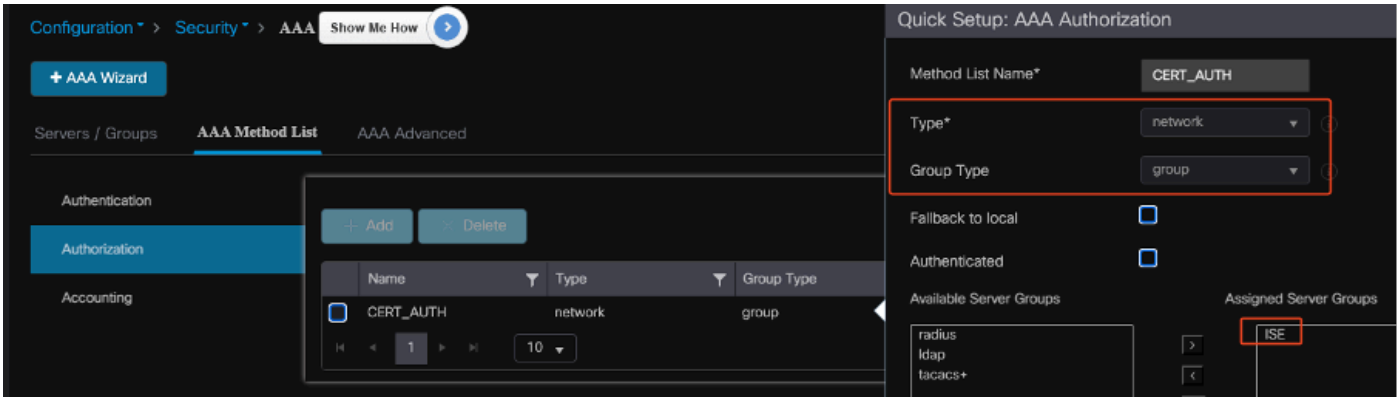


認証方式リストの作成

9800 WLC上での認証方式リストの設定

許可方式リストを設定するには、次の手順を使用します。

1. AAA Method Listセクション内のAuthorizationタブに移動します。
2. Addをクリックして、新しい許可方式リストを作成します。
3. タイプとしてnetworkを選択します。
4. グループタイプとしてgroupを選択します。
5. ISEサーバグループをサーバグループとして含めます。

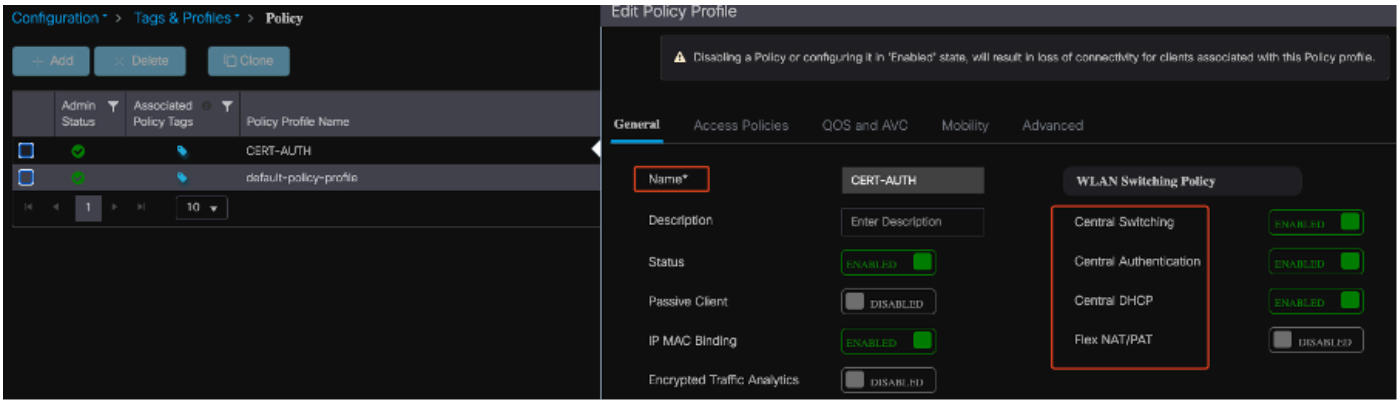


許可方式リストの追加

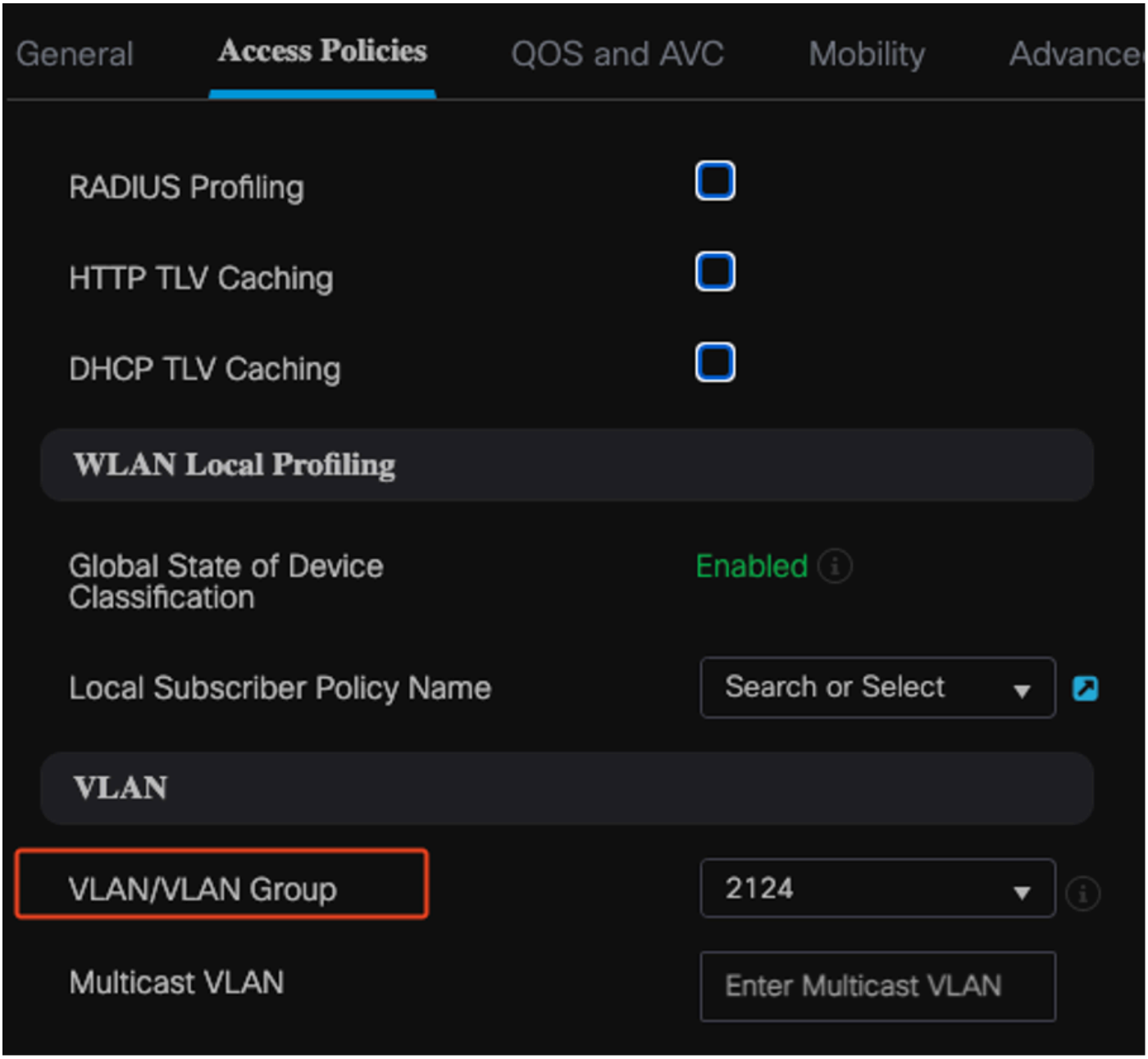
9800 WLC上でのポリシープロファイルの作成

RADIUSグループの設定が完了したら、ポリシープロファイルの作成に進みます。

1. [設定（Configuration）] > [タグとプロファイル（Tags & Profiles）] > [ポリシー（Policy）] に移動します。
2. Addをクリックして、新しいポリシープロファイルを作成します。
3. ポリシープロファイルに適したパラメータを選択します。この例では、すべてが中央VLANであり、LAB VLANがクライアントVLANとして使用されます。



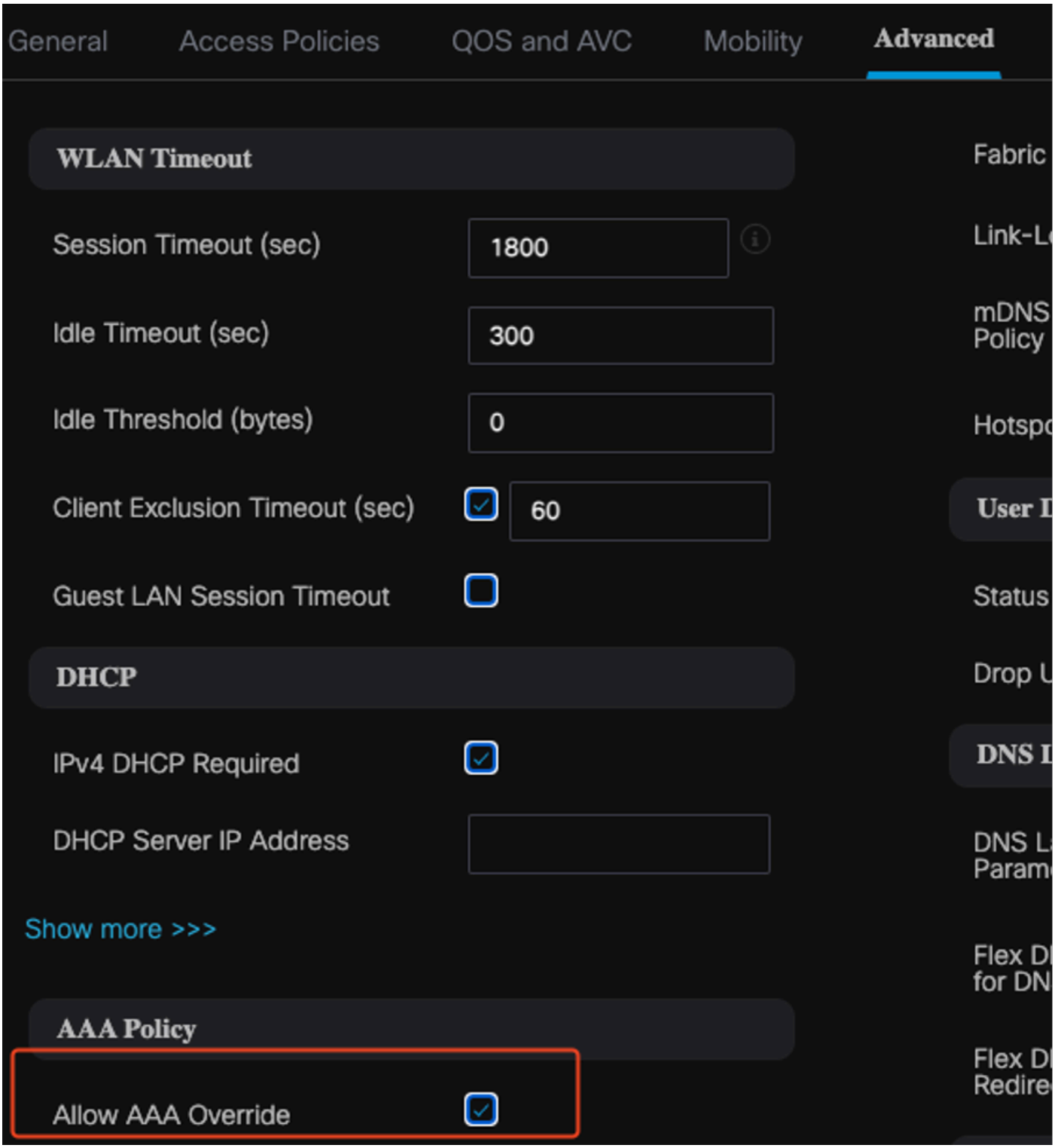
ポリシープロファイルの設定



VLANからポリシーへのマッピング

RADIUS認可を設定する場合は、ポリシープロファイル設定のadvancedタブでAAA Overrideオプションが有効になっていることを確認します。この設定により、ワイヤレスLANコントローラは

RADIUSベースの許可ポリシーをユーザとデバイスに適用できます。

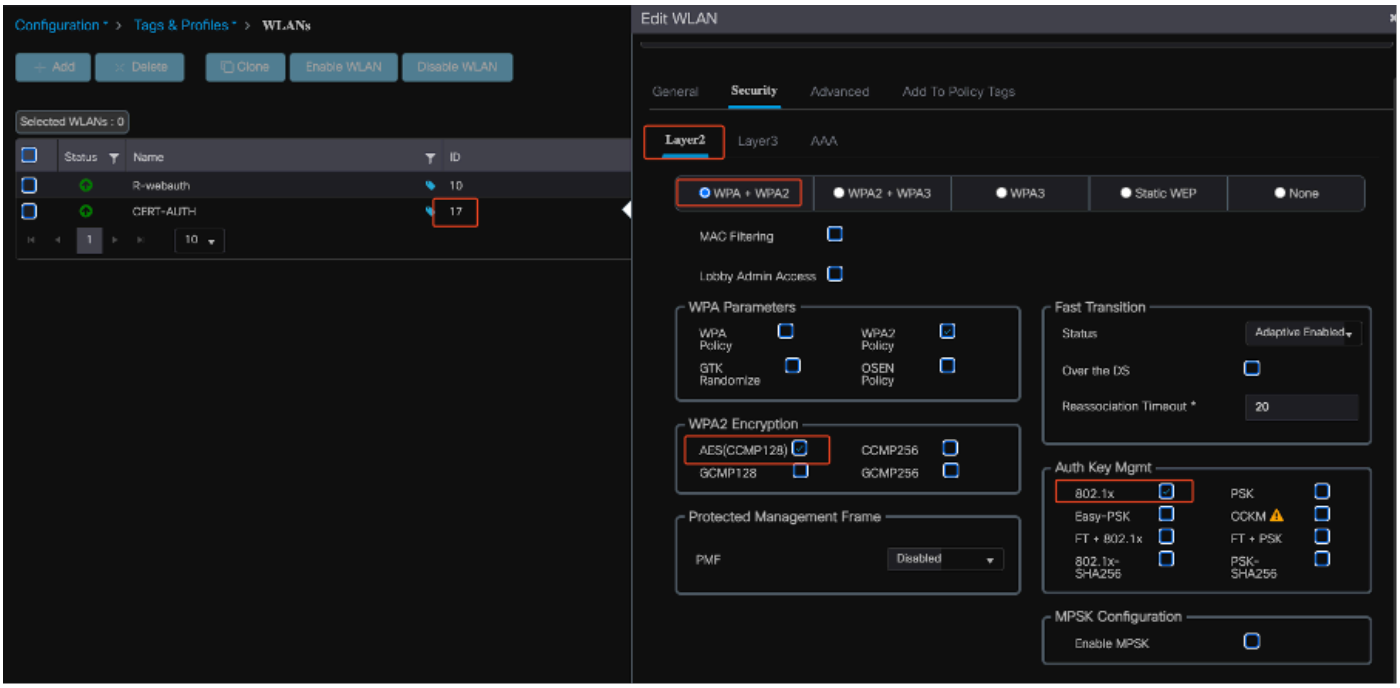


AAA オーバーライド

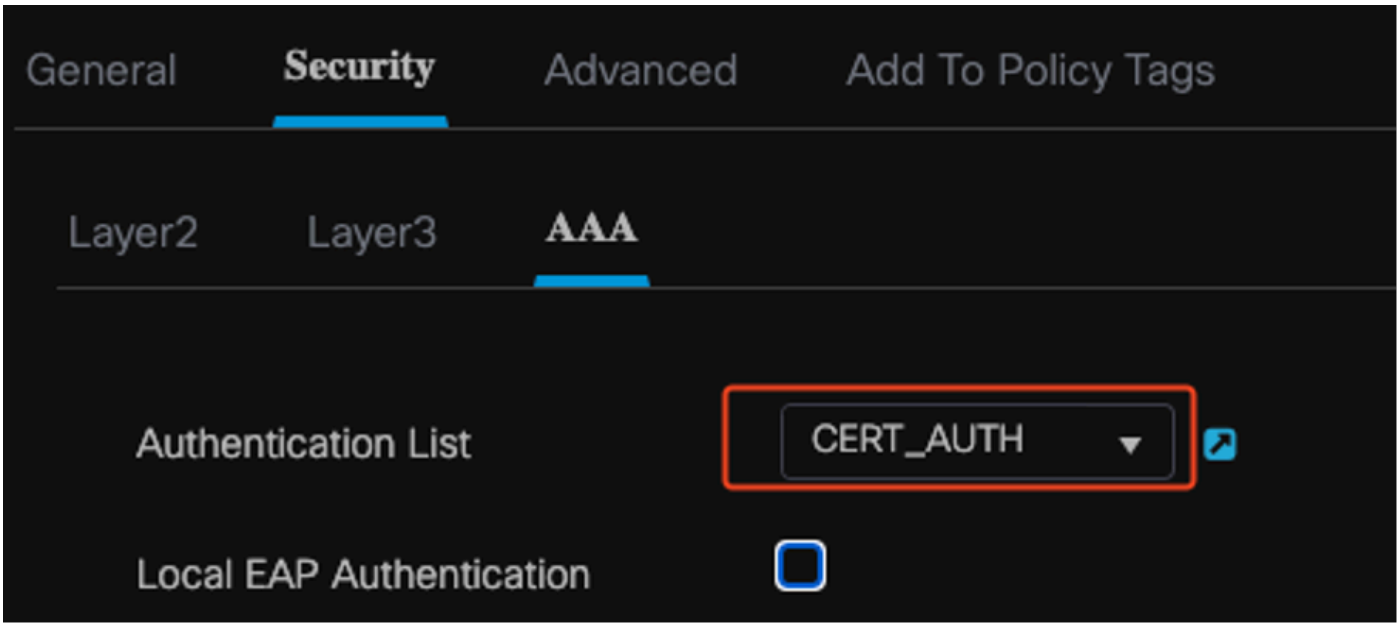
9800 WLCでのWLANの作成

802.1x認証を使用して新しいWLANを設定するには、次の手順を実行します。

1. Configuration > Tags & Profiles > WLANsの順に選択します。
2. Addをクリックして、新しいWLANを作成します。
3. レイヤ2認証設定を選択し、802.1x認証を有効にします。



WLAN プロファイルの設定

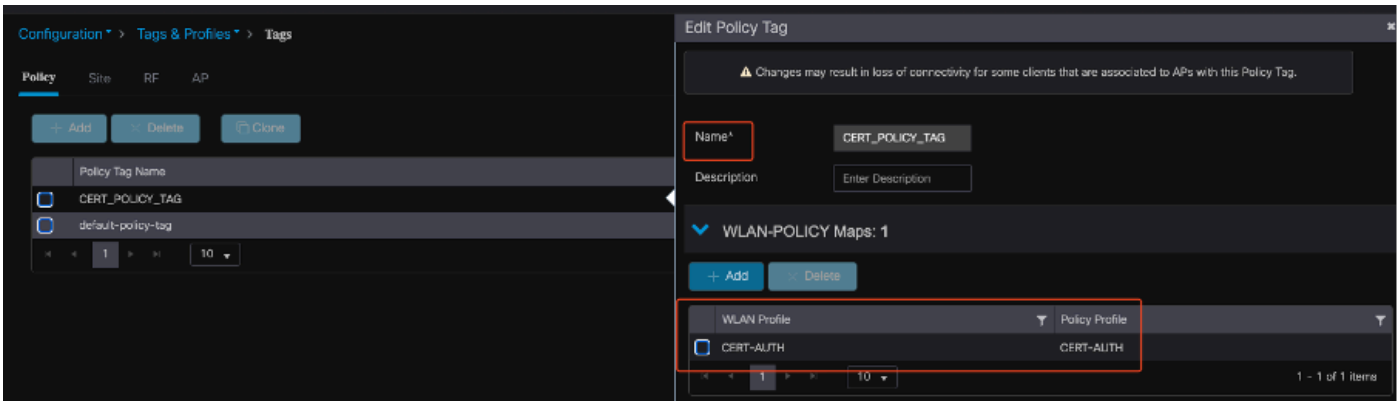


WLANプロファイルと方式リストマップ

WLANを9800 WLCのポリシープロファイルにマッピングする

WLANをポリシープロファイルに関連付けるには、次の手順を使用します。

1. Configuration > Tags & Profiles > Tagsの順に移動します。
2. Addをクリックして、新しいタグを追加します。
3. WLAN-POLICYセクションで、新しく作成したWLANを適切なポリシープロファイルにマッピングします。

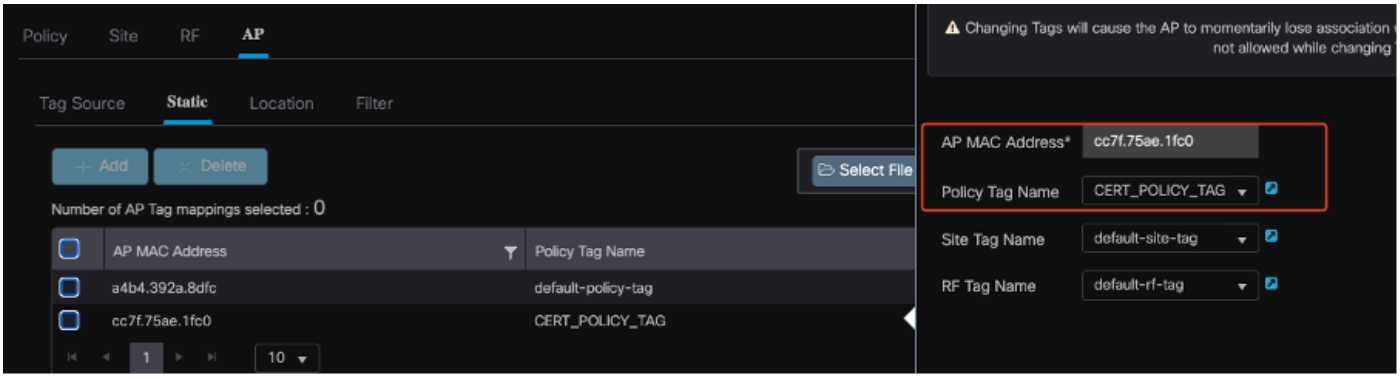


ポリシータグの設定

9800 WLC上のアクセスポイントへのポリシータグのマッピング

ポリシータグをアクセスポイント(AP)に割り当てるには、次の手順を実行します。

1. Configuration > Tags & Profiles > Tags > APの順に移動します。
2. AP設定のStaticセクションに移動します。
3. 設定する特定のAPをクリックします。
4. 作成したポリシータグを選択したAPに割り当てます。



APタグの割り当て

セットアップ完了後のWLCの実行コンフィギュレーション

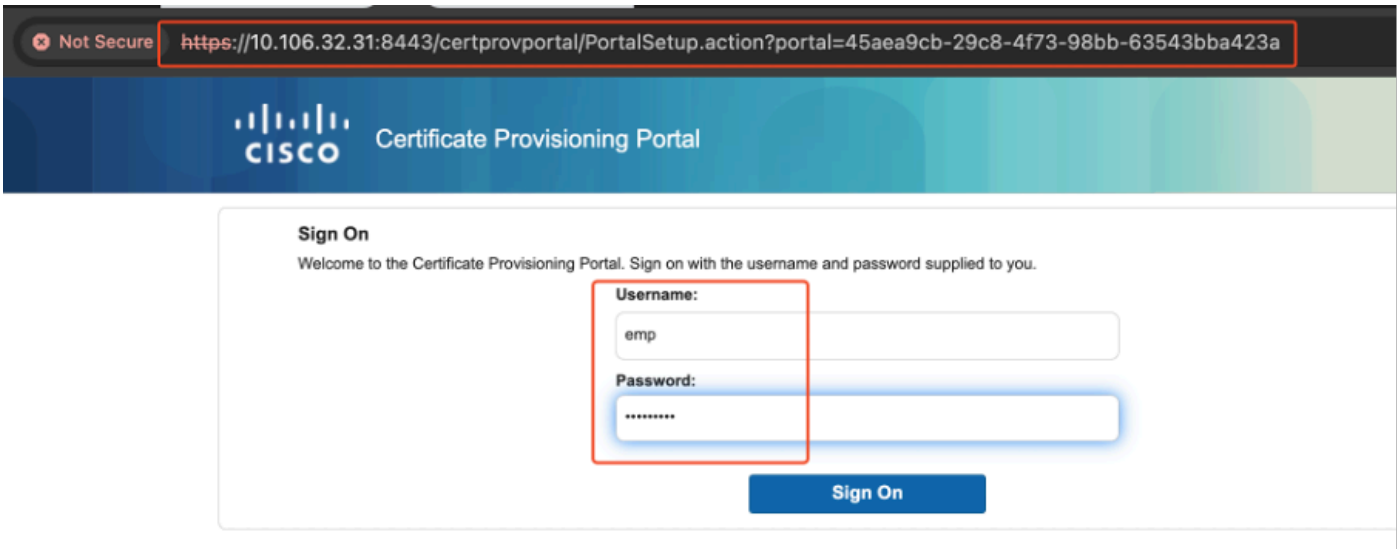
```
aaa group server radius ISE
 server name ISE3
 ip radius source-interface Vlan2124
aaa authentication dot1x CERT_AUTH group ISE
aaa authorization network CERT_AUTH group ISE
aaa server radius dynamic-author
 client 10.106.32.31 server-key Cisco!123
!

wireless profile policy CERT-AUTH
 aaa-override
 ipv4 dhcp required
 vlan 2124
 no shutdown
 wlan CERT-AUTH policy CERT-AUTH
wlan CERT-AUTH 17 CERT-AUTH
```

```
 security dot1x authentication-list CERT_AUTH
 no shutdown
!
wireless tag policy CERT_POLICY_TAG
 wlan CERT-AUTH policy CERT-AUTH
```

ユーザの証明書の作成とダウンロード

ユーザの証明書を作成およびダウンロードするには、次の手順を実行します。

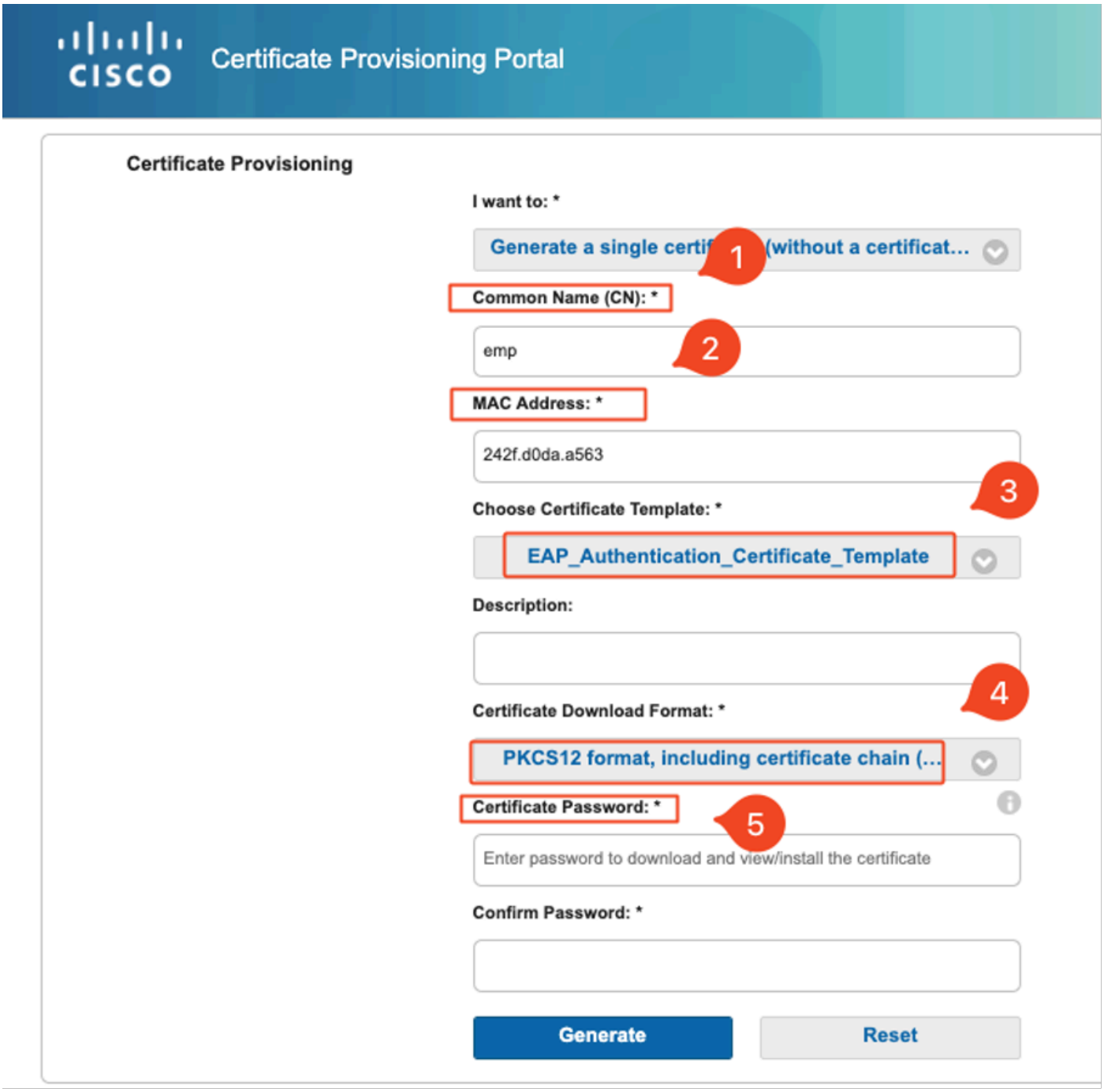
1. 以前にセットアップした証明書ポータルにユーザーをログインさせます。



証明書ポータルへのアクセス

2. アクセプタブルユースポリシー(AUP)に同意します。 ISEは証明書生成用のページを表示します。

3. Generate a single certificate (without a certificate signing request)を選択します。



証明書の生成中

証明書プロビジョニングポータルを使用して証明書を生成するには、次の必須フィールドに入力します。

- CN：認証サーバは、クライアント証明書のCommon Nameフィールドに表示される値を使用してユーザを認証します。Common Nameフィールドに、（証明書プロビジョニングポータルへのログインに使用した）ユーザ名を入力します。
- MACアドレス：サブジェクト代替名(SAN)は、さまざまな値をセキュリティ証明書に関連付けることができるX.509拡張です。Cisco ISEリリース2.0は、MACアドレスのみをサポートしています。したがって、SAN/MACアドレスフィールドに入力します。
    - 証明書テンプレート：証明書テンプレートは、要求の検証と証明書の発行時にCAが使用する一連のフィールドを定義します。Common Name（CN；共通名）などのフィールドは、要求の検証に使用されます（CNはユーザ名と一致する必要があります）。

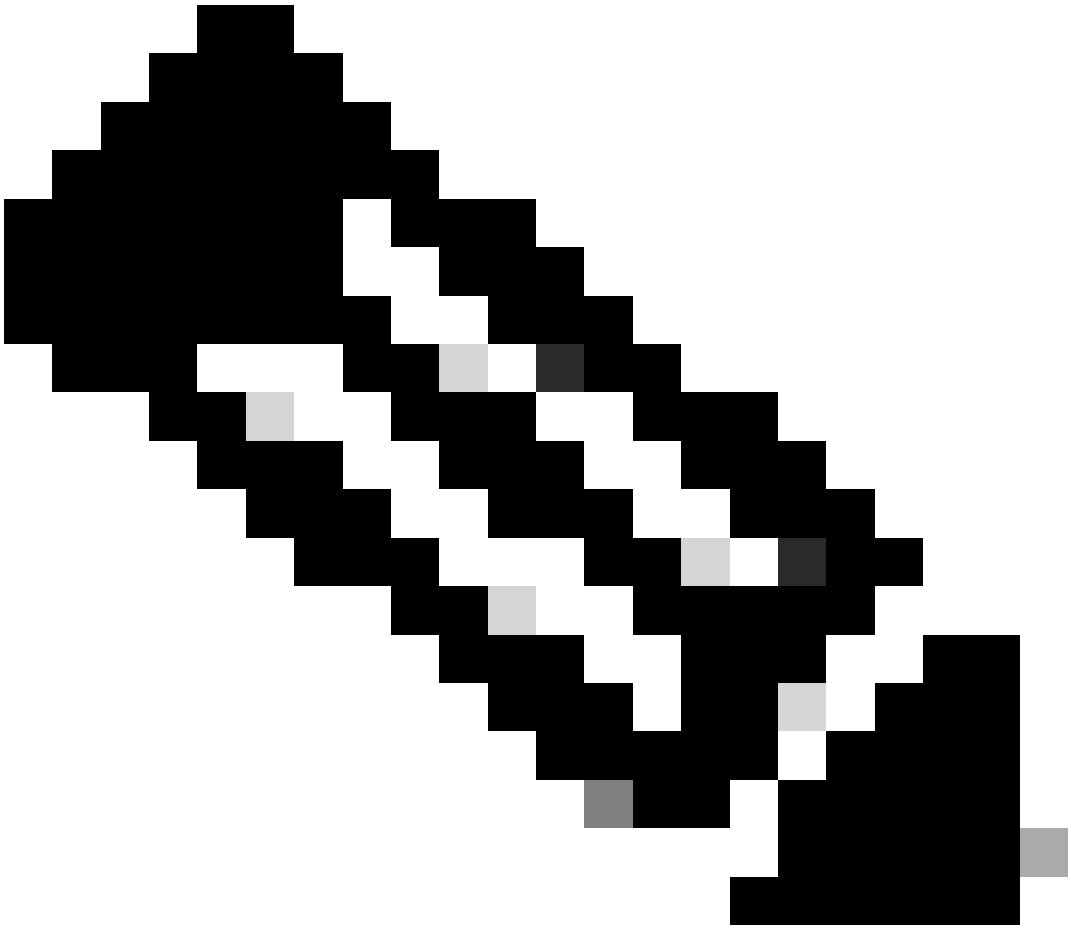
その他のフィールドは、証明書の発行時にCAによって使用されます。

- 証明書のパスワード：証明書を保護するには、証明書のパスワードが必要です。証明書の内容を表示したり、デバイスに証明書をインポートしたりするには、証明書のパスワードを入力する必要があります。
- パスワードは次の規則に従う必要があります。
- パスワードには、大文字1つ、小文字1つ、および数字1つ以上を含める必要があります
  - パスワードは8 ~ 15文字の長さにする必要があります
  - 使用できる文字は、A ~ Z、a ~ z、0 ~ 9、_、#です

すべてのフィールドに入力したら、Generateを選択し、証明書を作成してダウンロードします。

Windows 10マシンでの証明書のインストール

Windows 10マシンに証明書をインストールするには、次の手順に従ってMicrosoft管理コンソール(MMC)を開きます。

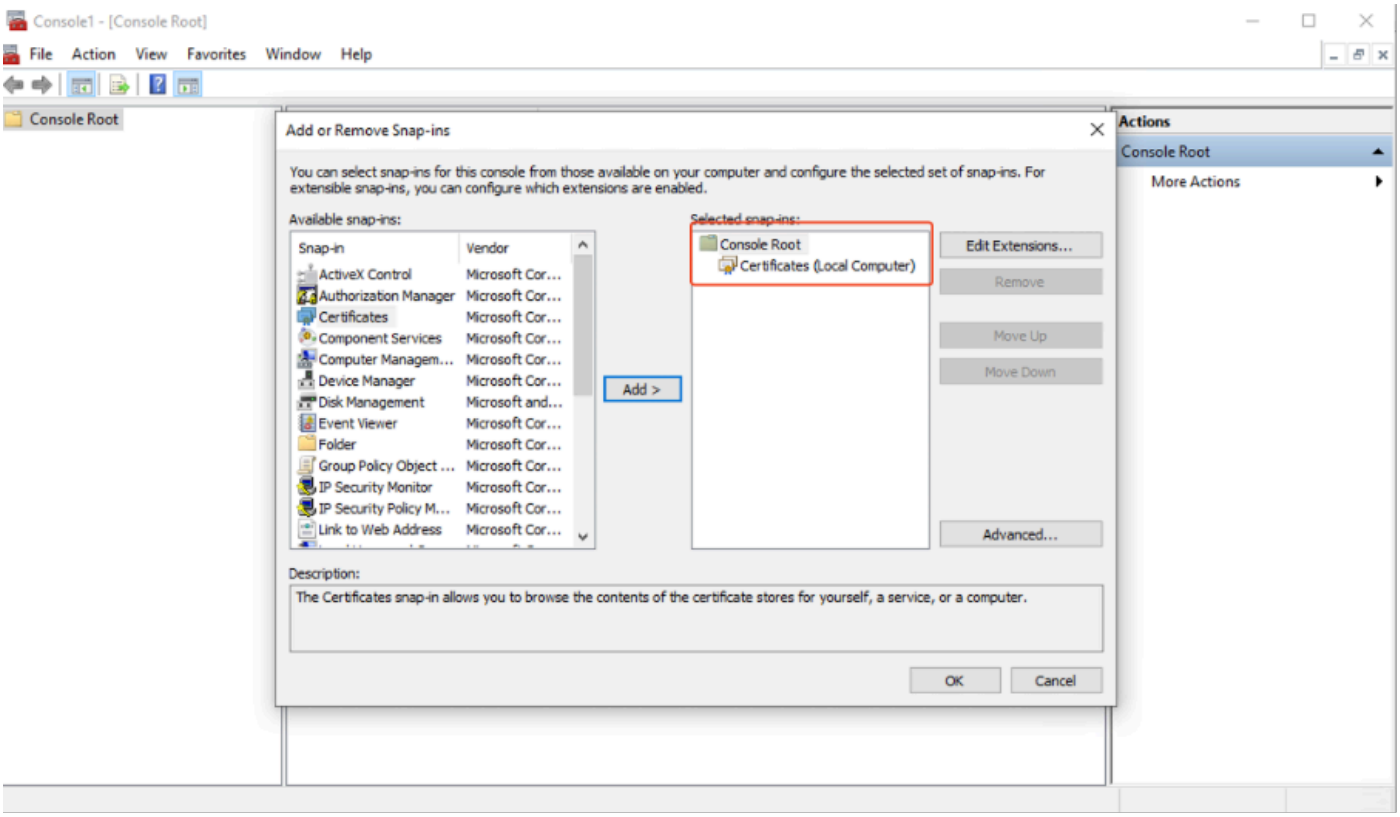


注：これらの手順はWindowsのセットアップによって異なる場合があるため、詳細につ

いてはMicrosoftのドキュメントを参照してください。

1. Start、Runの順にクリックします。
2. Runボックスにmmcと入力し、Enterキーを押します。Microsoft管理コンソールが開きます。
3. 証明書スナップインの追加：
4. File > Add/Remove Snap-Inの順に選択します。
5. Addを選択し、次にCertificatesを選択して、Addをクリックします。
6. Computer Account、Local Computerの順に選択し、Finishをクリックします。

次の手順を使用すると、ローカルコンピュータ上の証明書を管理できます。



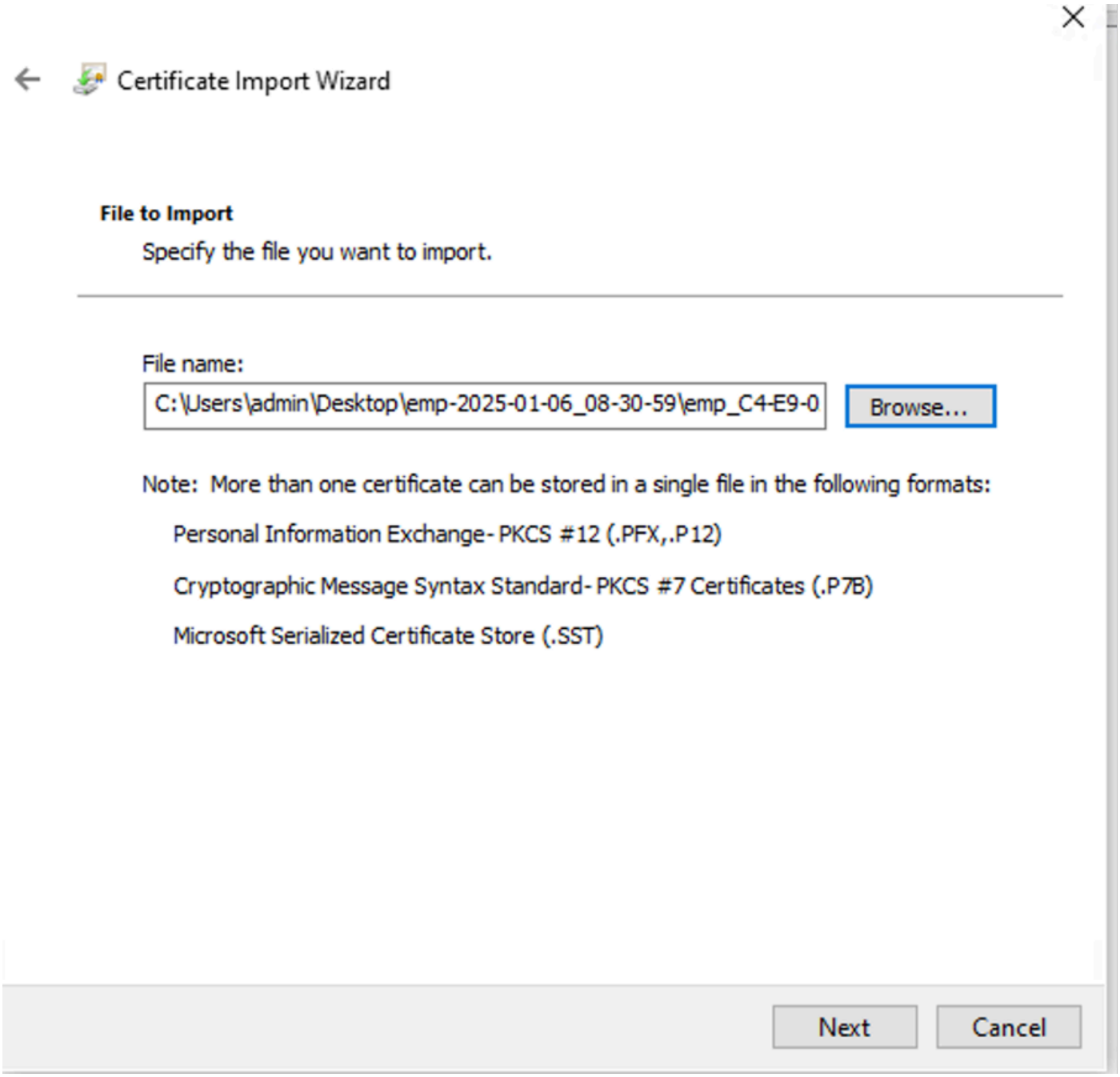
Windows MMCコンソール

ステップ 1：証明書をインポートします。

1.1.メニューでActionをクリックします。

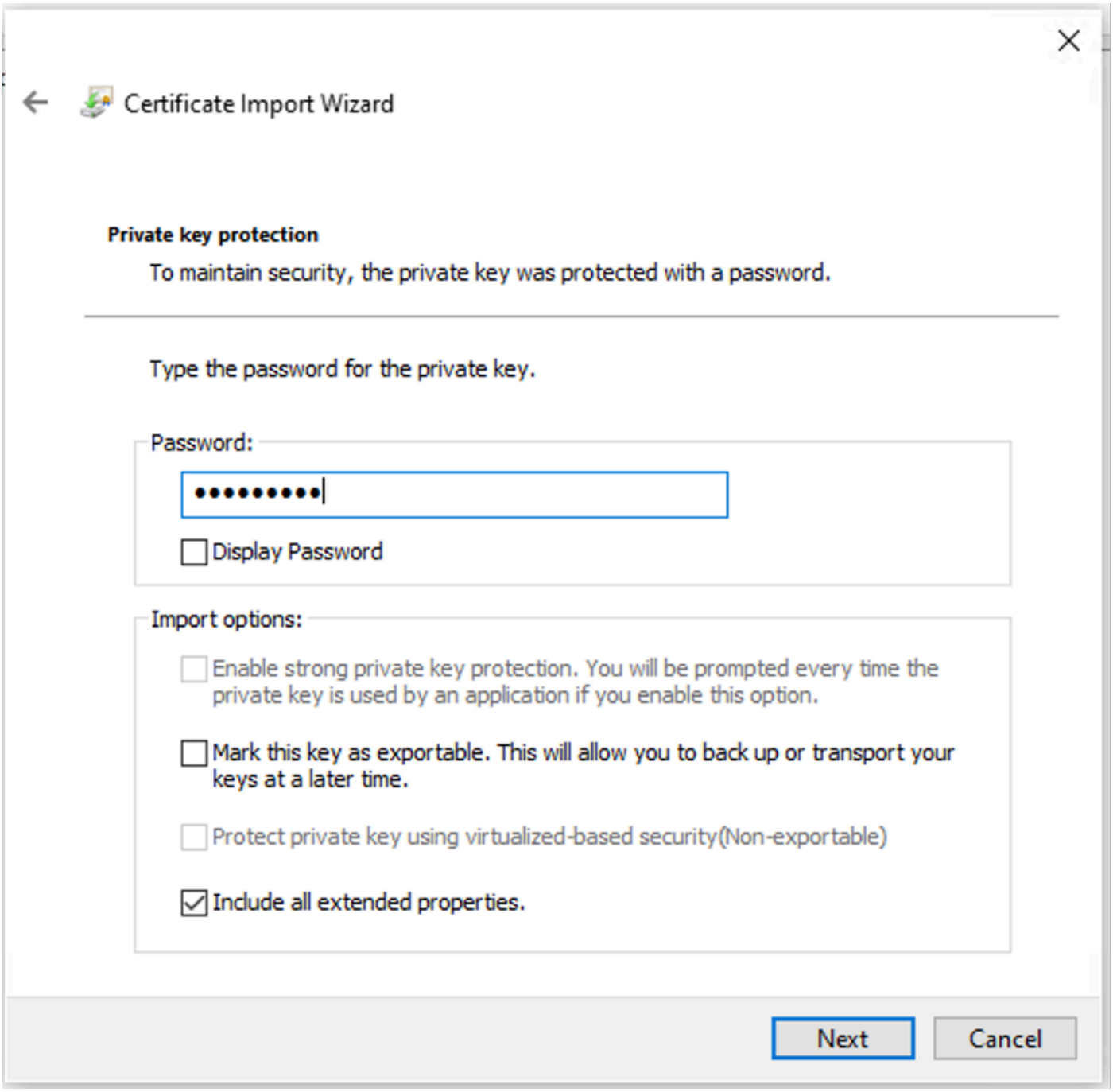
1.2. All Tasksに移動し、Importを選択します。

1.3.プロンプトに従って、マシンに保存されている証明書ファイルを検索して選択します。



証明書のインポート

証明書のインポートプロセス中に、ポータルで証明書を生成するときに作成したパスワードの入力を求められます。 このパスワードを正確に入力して、マシンに証明書を正常にインポートおよびインストールできることを確認してください。



証明書パスワードの入力

ステップ 2：証明書を適切なフォルダに移動します。

2.1. Microsoft管理コンソール(MMC)を開き、Certificates (Local Computer) > Personalフォルダに移動します。

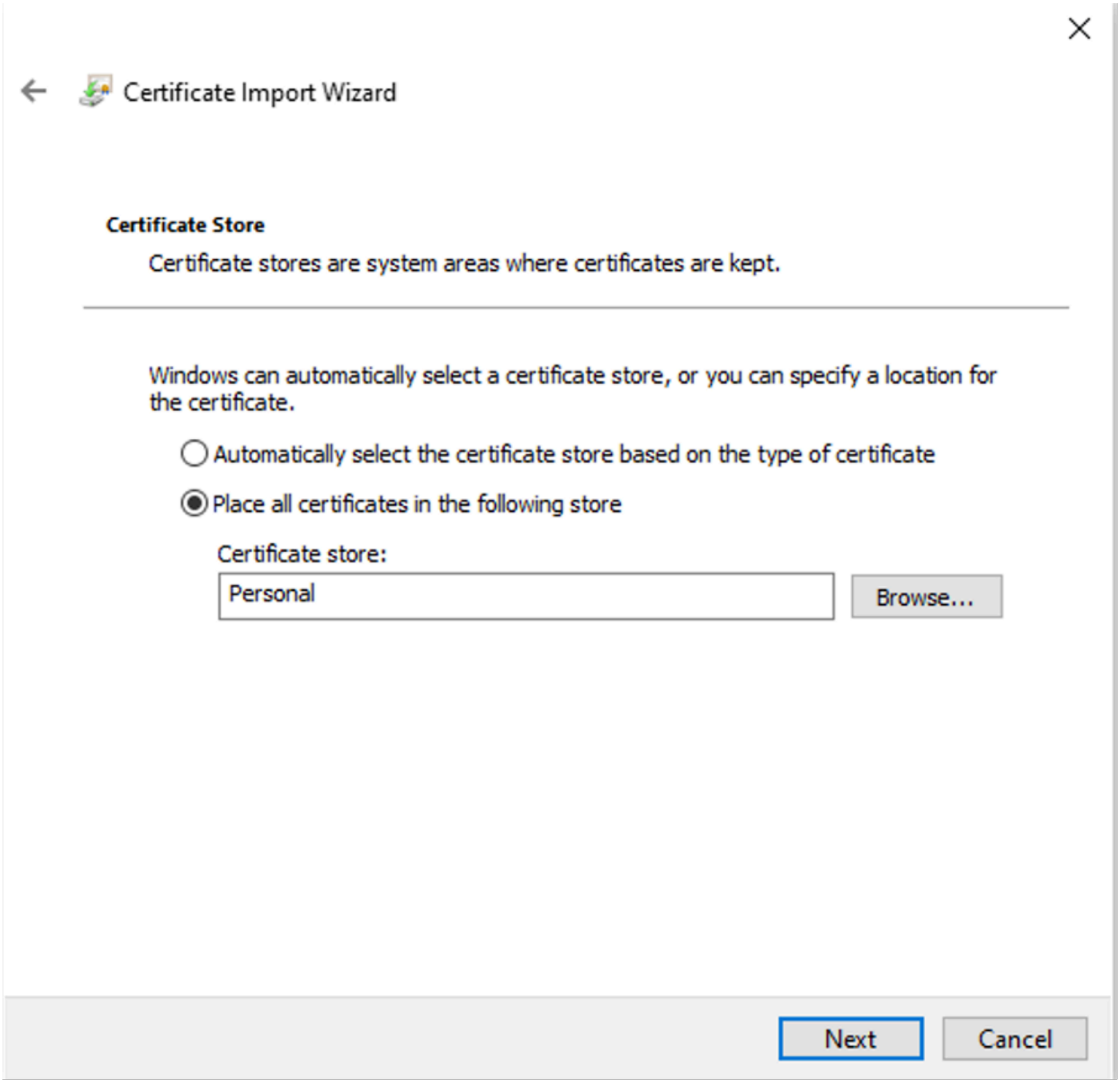
2.2.証明書を確認し、そのタイプ（ルートCA、中間CA、パーソナルなど）を決定する。

2.3.適切なストアへの各証明書の移動:

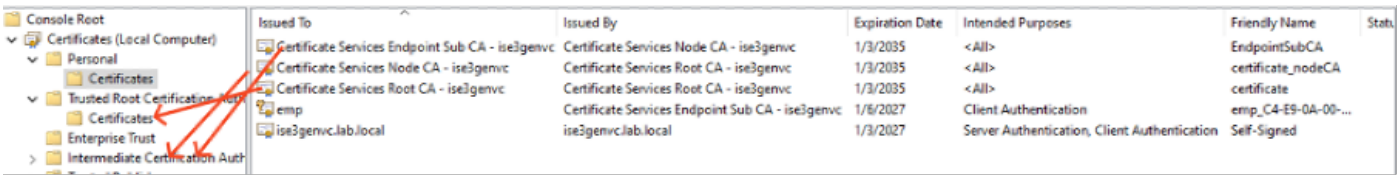
2.4.ルートCA証明書：信頼できるルート認証局への移動。

2.5.中間CA証明書：中間証明機関に移行する。

2.6.個人証明書：Personalフォルダ内に残ります。



個人用フォルダへの証明書の格納



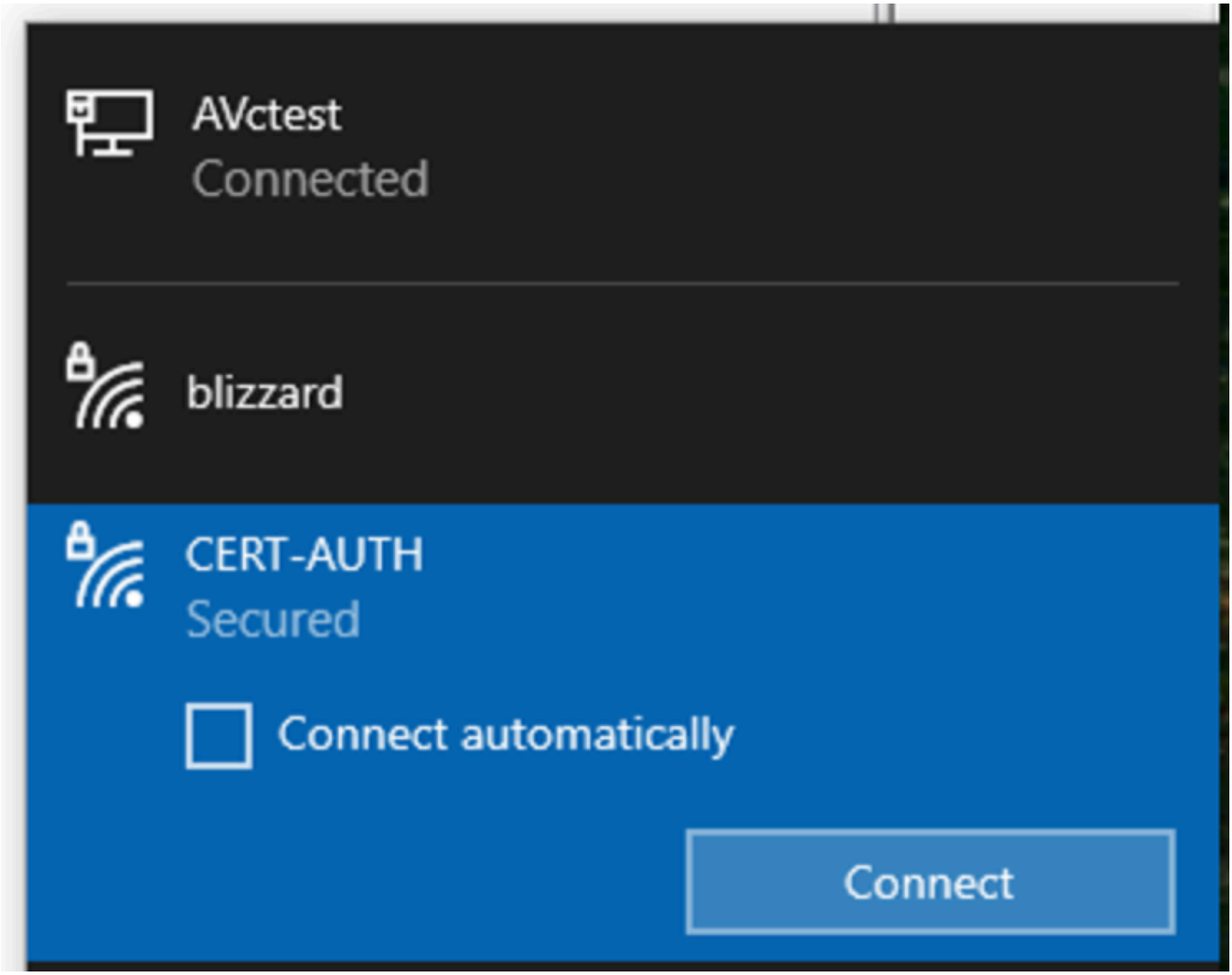
証明書をストア内で移動する

Windowsマシンの接続

証明書が正しいストアに移動されたら、次の手順を使用してWLANに接続します。

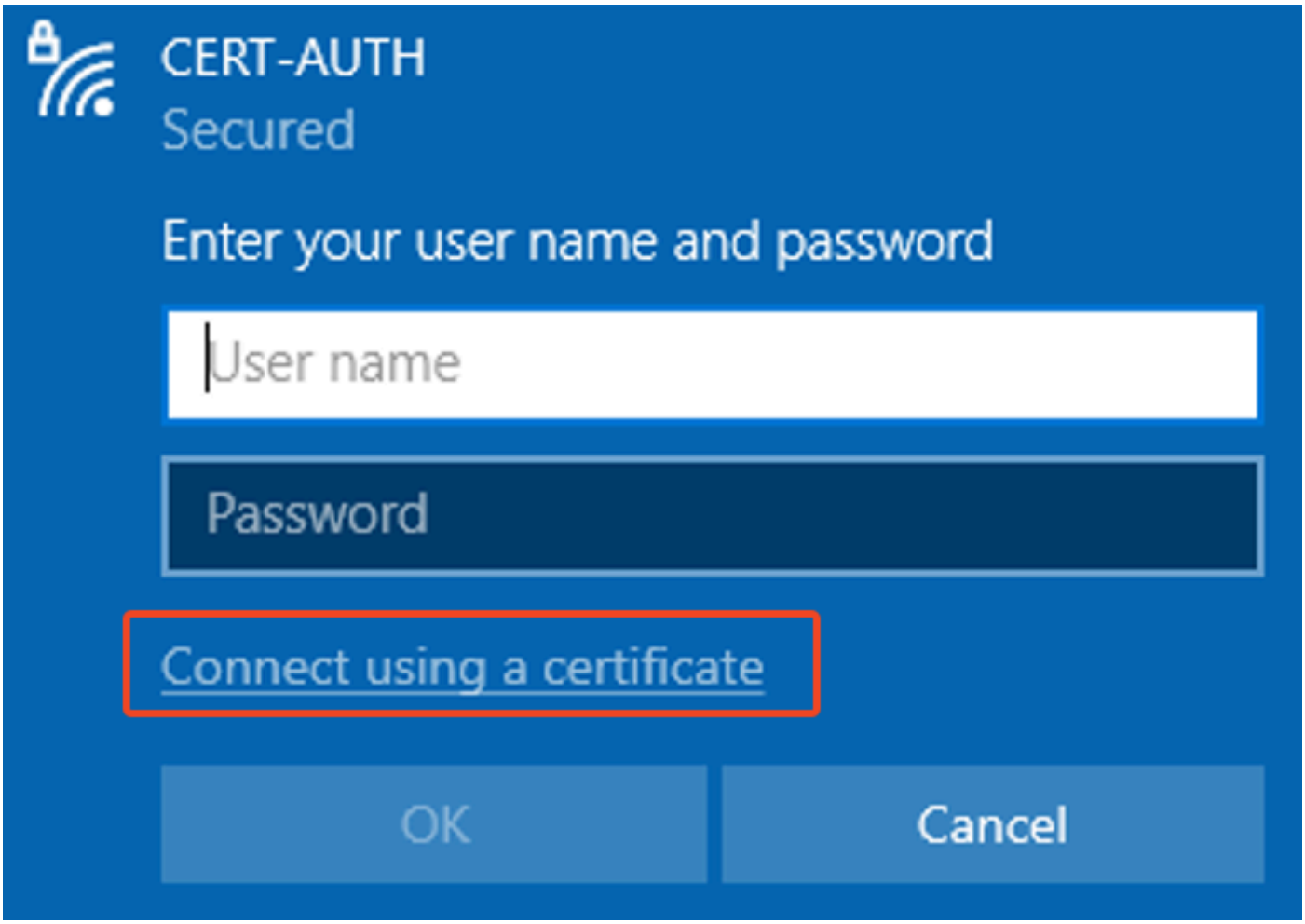
1. システムトレイのnetworkアイコンをクリックして、使用可能なワイヤレスネットワークを

表示します。
2. 接続するWLANの名前を探してクリックします。
3. Connectをクリックし、追加のプロンプトが表示されたら先に進み、認証に証明書を使用する接続プロセスを完了します。



ワイヤレスネットワークへの接続

WLANへの接続プロセス中にプロンプトが表示されたら、Connect using a certificateオプションを選択します。



クレデンシャルとしての証明書の使用

これにより、証明書を使用してワイヤレスネットワークに正常に接続できます。

```
C:\>netsh wlan  show interface

There is 1 interface on the system:

    Name                   : Wi-Fi 3
    Description            : TP-Link Wireless USB Adapter
    GUID                   : ee5d1c47-43cc-4873-9ae6-99e2e43c39ea
    Physical address       : 24:2f:d0:da:a5:63
    State                  : connected
    SSID                   : CERT-AUTH
    BSSID                  : a4:88:73:9e:8d:af
    Network type           : Infrastructure
    Radio type             : 802.11ac
    Authentication         : WPA2-Enterprise
    Cipher                 : CCMP
    Connection mode        : Profile
    Channel                : 36
    Receive rate (Mbps)    : 360
    Transmit rate (Mbps)   : 360
    Signal                 : 100%
    Profile                : CERT-AUTH

    Hosted network status  : Not available


C:\>netsh wlan show profiles CERT-AUTH | find "Smart"
    EAP type               : Microsoft: Smart Card or other certificate
```

ワイヤレスプロファイルの確認

確認

WLANがWLCによってブロードキャストされていることを確認します。

<#root>

```
POD6_9800#show wlan summ
Number of WLANs: 2
ID Profile Name SSID Status Security
-----------------------------------------------------------------------------------------------------------------
```

17

```
 CERT-AUTH
```

CERT-AUTH

```
 UP [WPA2][802.1x][AES]
```

APがWLCでアップしていることを確認します。

```
POD6_9800#show ap summ
Number of APs: 1
CC = Country Code
RD = Regulatory Domain
AP Name Slots AP Model Ethernet MAC Radio MAC CC RD IP Address State Location
-------------------------------------------------------------------------------------------------
AP1 3 C9130AXI-D cc7f.75ae.1fc0 a488.739e.8da0 IN -D 10.78.8.78 Registered default location
```

APがWLANをブロードキャストしていることを確認します。

<#root>

```
POD6_9800#show ap name AP1 wlan dot11 24ghz
Slot id : 0
WLAN ID BSSID
------------------------
17 a488.739e.8da0

POD6_9800#show ap name AP1 wlan dot11 5ghz
Slot id : 1
WLAN ID BSSID
------------------------
```

17

```
 a488.739e.8daf
```

EAP-TLSを使用して接続されたクライアント：

<#root>

```
POD6_9800#show wire cli summ
Number of Clients: 1
MAC Address AP Name Type ID State Protocol Method Role
-----------------------------------------------------------------------------------------------------
242f.d0da.a563 AP1 WLAN
```

17

```
 IP Learn 11ac
```

Dot1x

```
 Local

POD6_9800#sho wireless client mac-address 242f.d0da.a563 detail | in username|SSID|EAP|AAA|VLAN
```

Wireless LAN Network Name (SSID): CERT-AUTH

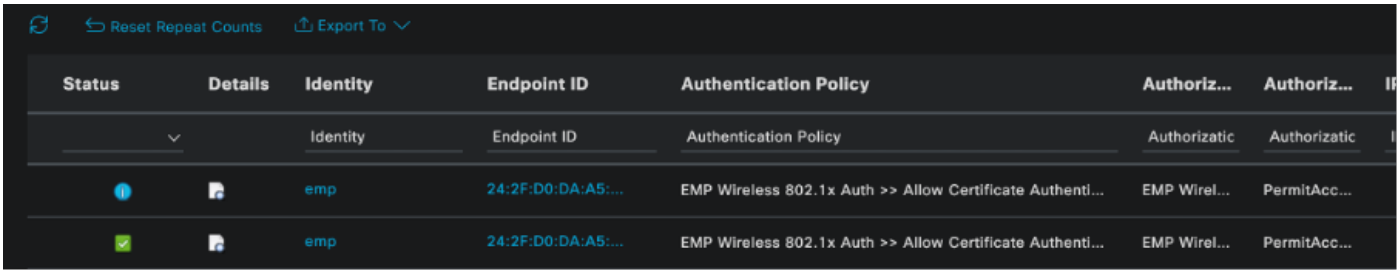
```
BSSID : a488.739e.8daf
```

EAP Type : EAP-TLS

```
VLAN : 2124
Multicast VLAN : 0
```

VLAN ： 2124

Cisco Radius ISEライブログ：

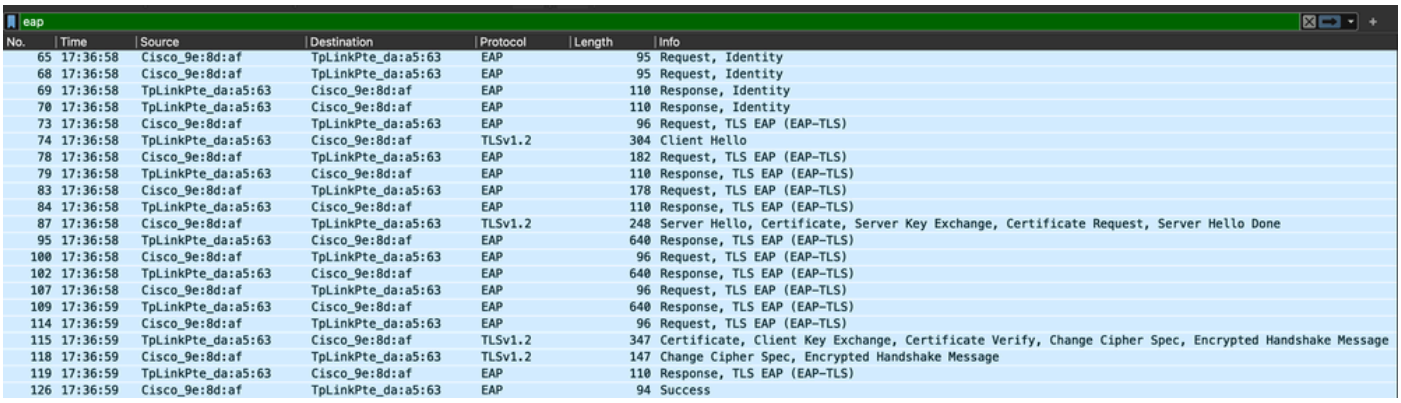


ISE Radiusライブログ

詳細な認証タイプ：

ISEの詳細ログ

EAP-TLSパケットを示すWLC EPCキャプチャ：



No.	Time	Source	Destination	Protocol	Length	Info
65	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	95	Request, Identity
68	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	95	Request, Identity
69	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, Identity
70	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, Identity
73	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)
74	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	TLSv1.2	304	Client Hello
78	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	182	Request, TLS EAP (EAP-TLS)
79	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, TLS EAP (EAP-TLS)
83	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	178	Request, TLS EAP (EAP-TLS)
84	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, TLS EAP (EAP-TLS)
87	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	TLSv1.2	248	Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
95	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	640	Response, TLS EAP (EAP-TLS)
100	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)
102	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	640	Response, TLS EAP (EAP-TLS)
107	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)
109	17:36:59	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	640	Response, TLS EAP (EAP-TLS)
114	17:36:59	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)
115	17:36:59	TpLinkPte_da:a5:63	Cisco_9e:8d:af	TLSv1.2	347	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
118	17:36:59	Cisco_9e:8d:af	TpLinkPte_da:a5:63	TLSv1.2	147	Change Cipher Spec, Encrypted Handshake Message
119	17:36:59	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, TLS EAP (EAP-TLS)
126	17:36:59	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	94	Success

EAPトランザクションを示すWLCキャプチャ

- パケット番号87は、このドキュメントの最初で説明したEAP-TLSフローのステップ8に対応します。
- パケット番号115は、このドキュメントの最初で説明したEAP-TLSフローのステップ9に対応します。
- パケット番号118は、このドキュメントの最初で説明したEAP-TLSフローのステップ10に対応します。

クライアント接続を示す無線アクティブ(RA)トレース：このRAトレースは、認証トランザクションのいくつかの関連行を表示するようにフィルタリングされます。

2025/01/08 11 58 20.816875191 {wncd_x_R0-2}{1} [ewlc-capwapmsg-sess] [15655] (debug)暗号化されたDTLSメッセージ送信。宛先IP 10.78.8.78[5256]、長さ499
2025/01/08 11 58 20.851392112 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Send Access-Request to 10.106.33.23 1812 id 0/25, len 390
2025/01/08 11 58 20.871842938 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Received from id 1812/25 10.106.33.23 0, Access-Challenge, len 123
2025/01/08 11 58 20.872246323 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005]送信されたEAPOLパケット – バージョン3、EAPOLタイプEAP、ペイロード長6、EAPタイプ= EAP-TLS
2025/01/08 11 58 20.881960763 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005]受信したEAPOLパケット – バージョン1,EAPOLタイプEAP、ペイロード長204、EAPタイプ= EAP-TLS
2025/01/08 11 58 20.882292551 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Send Access-Request to 10.106.33.23 1812 ID 0/26, len 663
2025/01/08 11 58 20.926204990 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Received from id 1812/26 10.106.33.23 0, Access-Challenge, len 1135
2025/01/08 11 58 20.927390754 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Sent EAPOL packet - Version 3,EAPOL Type EAP, Payload Length 1012, EAP-Type = EAP-TLS
2025/01/08 11 58 20.935081108 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005]受信したEAPOLパケット – バージョン1,EAPOLタイプEAP、ペイロード長6、EAPタイプ= EAP-TLS
2025/01/08 11 58 20.935405770 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Send Access-Request to 10.106.33.23 1812 ID 0/27, len 465
2025/01/08 11 58 20.938485635 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Received from

id 1812/27 10.106.33.23 0, Access-Challenge, len 1131
2025/01/08 11 58 20.939630108 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Sent EAPOL packet - Version 3,EAPOL Type EAP, Payload Length 1008, EAP-Type = EAP-TLS
2025/01/08 11 58 20.947417061 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005]受信したEAPOLパケット – バージョン1,EAPOLタイプEAP、ペイロード長6、EAPタイプ= EAP-TLS
2025/01/08 11 58 20.947722851 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Send Access-Request to 10.106.33.23 1812 id 0/28, len 465
2025/01/08 11 58 20.949913199 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Received from id 1812/28 10.106.33.23 0, Access-Challenge, len 275
2025/01/08 11 58 20.950432303 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Sent EAPOL packet - Version 3,EAPOL Type EAP, Payload Length 158, EAP-Type = EAP-TLS
2025/01/08 11 58 20.966862562 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Received EAPOL packet - Version 1,EAPOL Type EAP, Payload Length 1492, EAP-Type = EAP-TLS
2025/01/08 11 58 20.967209224 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Send Access-Request to 10.106.33.23 1812 id 0/29, len 1961
2025/01/08 11 58 20.971337739 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Received from id 1812/29 10.106.33.23 0, Access-Challenge, len 123
2025/01/08 11 58 20.971708100 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005]送信されたEAPOLパケット – バージョン3、EAPOLタイプEAP、ペイロード長6、EAPタイプ= EAP-TLS
2025/01/08 11 58 20.978742828 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Received EAPOL packet - Version 1,EAPOL Type EAP, Payload Length 1492, EAP-Type = EAP-TLS
2025/01/08 11 58 20.979081544 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Send Access-Request to 10.106.33.23 1812 id 0/30, len 1961
2025/01/08 11 58 20.982535977 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Received from id 1812/30 10.106.33.23 0, Access-Challenge, len 123
2025/01/08 11 58 20.982907200 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005]送信されたEAPOLパケット – バージョン3、EAPOLタイプEAP、ペイロード長6、EAPタイプ= EAP-TLS
2025/01/08 11 58 20.990141062 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Received EAPOL packet - Version 1,EAPOL Type EAP, Payload Length 1492, EAP-Type = EAP-TLS
2025/01/08 11 58 20.990472026 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Send Access-Request to 10.106.33.23 1812 ID 0/31, len 1961
2025/01/08 11 58 20.994358525 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Received from id 1812/31 10.106.33.23 0, Access-Challenge, len 123
2025/01/08 11 58 20.994722151 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005]送信されたEAPOLパケット – バージョン3、EAPOLタイプEAP、ペイロード長6、EAPタイプ= EAP-TLS
2025/01/08 11 58 21.001735553 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Received EAPOL packet - Version 1,EAPOL Type EAP, Payload Length 247,

EAP-Type = EAP-TLS
2025/01/08 11 58 21.002076369 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Send Access-Request to 10.106.33.23 1812 ID 0/32, len 706
2025/01/08 11 58 21.013571608 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Received from id 1812/32 10.106.33.23 0, Access-Challenge, len 174
2025/01/08 11 58 21.013987785 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Sent EAPOL packet - Version 3,EAPOL Type EAP, Payload Length 57, EAP-Type = EAP-TLS
2025/01/08 11 58 21.024429150 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005]受信したEAPOLパケット – バージョン1,EAPOLタイプEAP、ペイロード長6、EAPタイプ= EAP-TLS
2025/01/08 11 58 21.024737996 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Send Access-Request to 10.106.33.23 1812 ID 0/33, len 465
2025/01/08 11 58 21.057794929 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Received from id 1812/33 10.106.33.23 0, Access-Accept, len 324
2025/01/08 11 58 21.058149893 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] EAPメソッドEAP-TLSのID更新イベントが発生しました

トラブルシュート

一般的なワイヤレス802.1xのトラブルシューティング手順以外に、この問題に対する特定のトラブルシューティング手順はありません。

1. クライアントRAトレースデバッグを実行して、認証プロセスを確認します。
2. WLC EPCキャプチャを実行して、クライアント、WLC、およびRADIUSサーバ間のパケットを調べます。
3. ISEライブログを確認して、要求が正しいポリシーに一致していることを確認します。
4. Windowsエンドポイントで、証明書が正しくインストールされており、信頼チェーン全体が存在することを確認します。

参考資料

- 証明書プロビジョニングポータルFAQ、リリース3.2
- ISE内部認証局(CA)サービスについて
- WLCとISEを使用したEAP-TLSの理解および設定

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。