WLCとISEを使用したEAP-TLSの理解と設定

内容

概要

このドキュメントでは、802.1XとExtensible Authentication Protocol(EAP)EAP-TLSを使用してWireless Local Area Network(WLAN)を設定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。

- 802.1X認証プロセス
- 証明書

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。

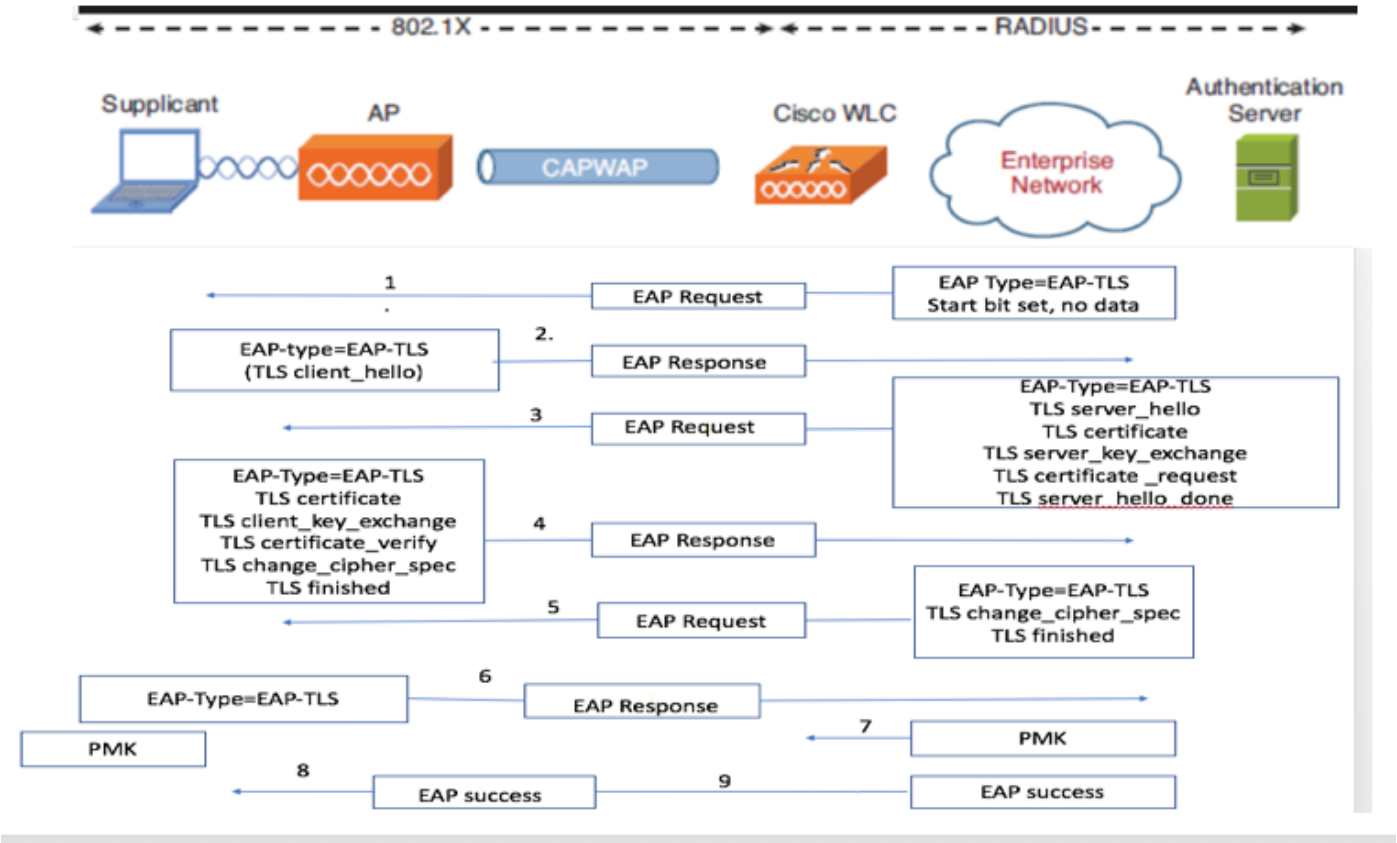
- WLC 3504 バージョン 8.10

- Identity Services Engine（ISE）バージョン 2.7

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、初期（デフォルト）設定の状態から起動しています。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

EAP-TLS フロー



EAP-TLS フローのステップ

1. ワイヤレスクライアントが、アクセスポイント（AP）に関連付けられます。APはこの時点ではクライアントによるデータの送信を許可せず、認証要求を送信します。サプリカントはEAP応答IDで応答します。WLC が、ユーザ ID 情報を認証サーバに送信します。RADIUS サーバが、EAP-TLS 開始パケットでクライアントに応答します。この時点で EAP-TLS カンバセーションが開始されます。
2. ピアは、NULLに設定された暗号である「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
3. 認証サーバが、次を含むアクセスチャレンジパケットで応答します。

```
TLS server_hello
handshake message
certificate
server_key_exchange
certificate request
server_hello_done.
```

4.クライアントは、次の内容を含むEAP-Responseメッセージで応答します。

```
Certificate ¬ Server can validate to verify that it is trusted.

client_key_exchange

certificate_verify ¬ Verifies the server is trusted

change_cipher_spec

TLS finished
```

5.クライアントが正常に認証されると、RADIUSサーバは「change_cipher_spec」と「handshake finished」メッセージを含むAccess-challengeで応答します。

6.これを受信すると、クライアントはRADIUSサーバを認証するためにハッシュを確認します。

7. 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る

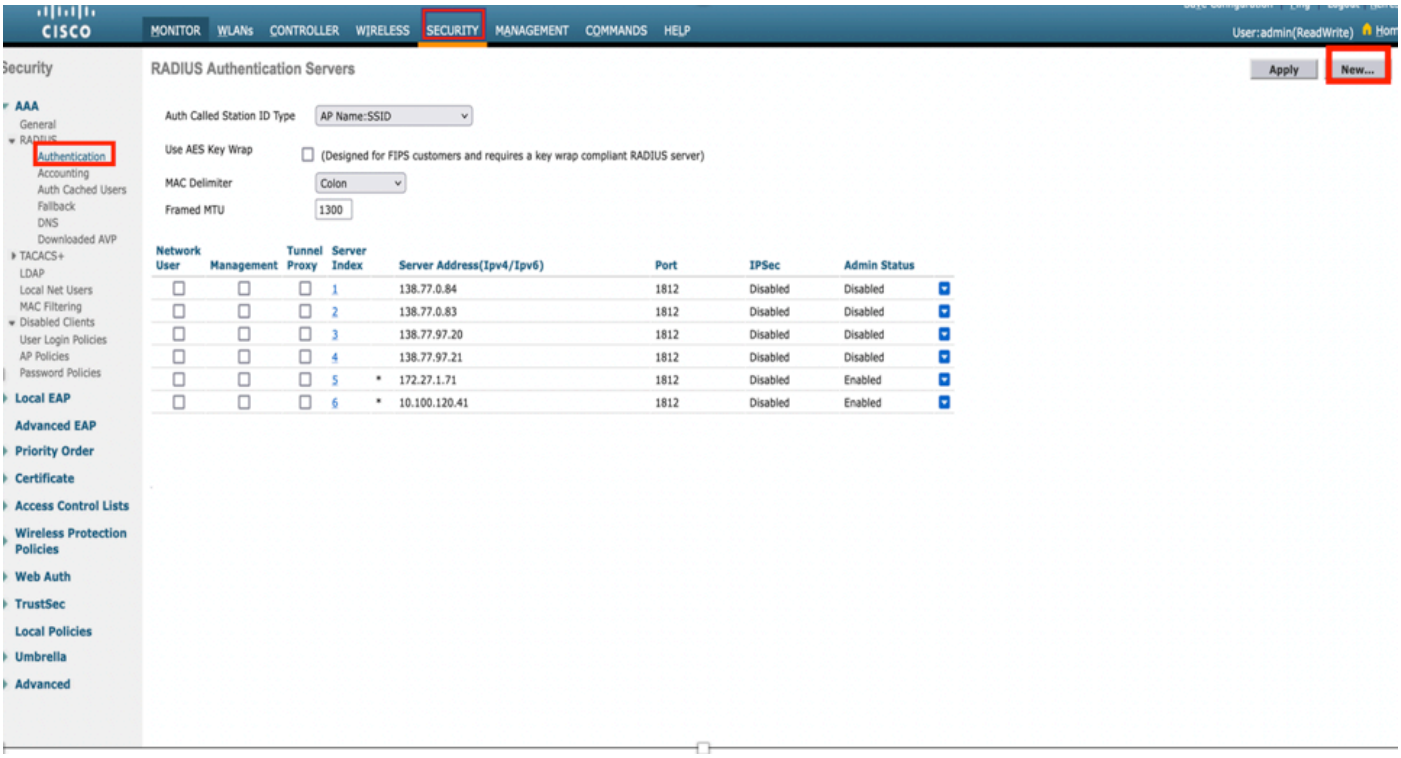
8/9.EAP：最終的にサーバからオーセンティケータに送信され、サプリカントに渡されます。

この時点で、EAP-TLS 対応の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ます。

設定

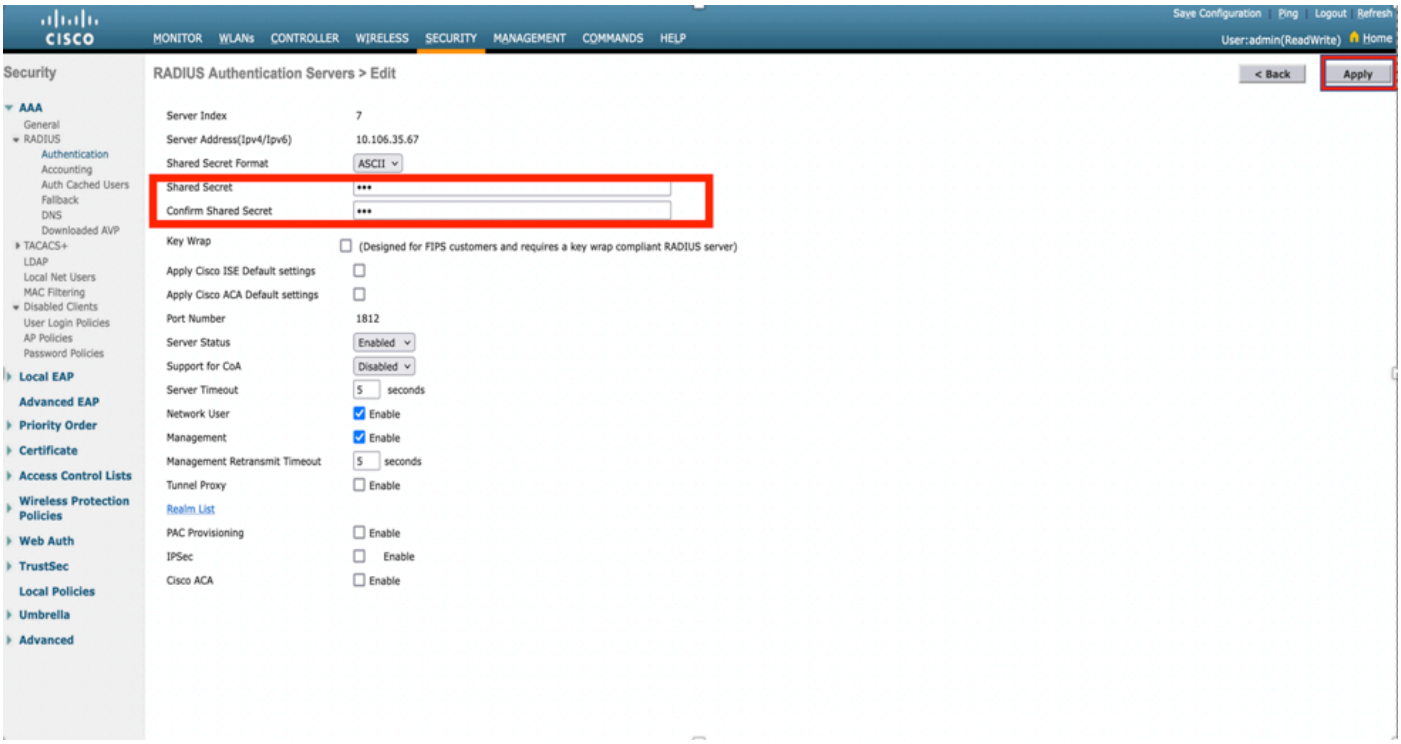
Cisco ワイヤレス LAN コントローラ

ステップ1：最初のステップでは、Cisco WLCでRADIUSサーバを設定します。RADIUS サーバを WLC に追加するには、[セキュリティ（Security）] > [RADIUS] > [認証（Authentication）] に移動します。図のように、[新規（New）] をクリックします。



ステップ2：ここで、ISE上のWLCを検証するために使用されるIPアドレスと共有秘密

<password>を入力する必要があります。図のように、[適用（Apply）] をクリックして続行します。

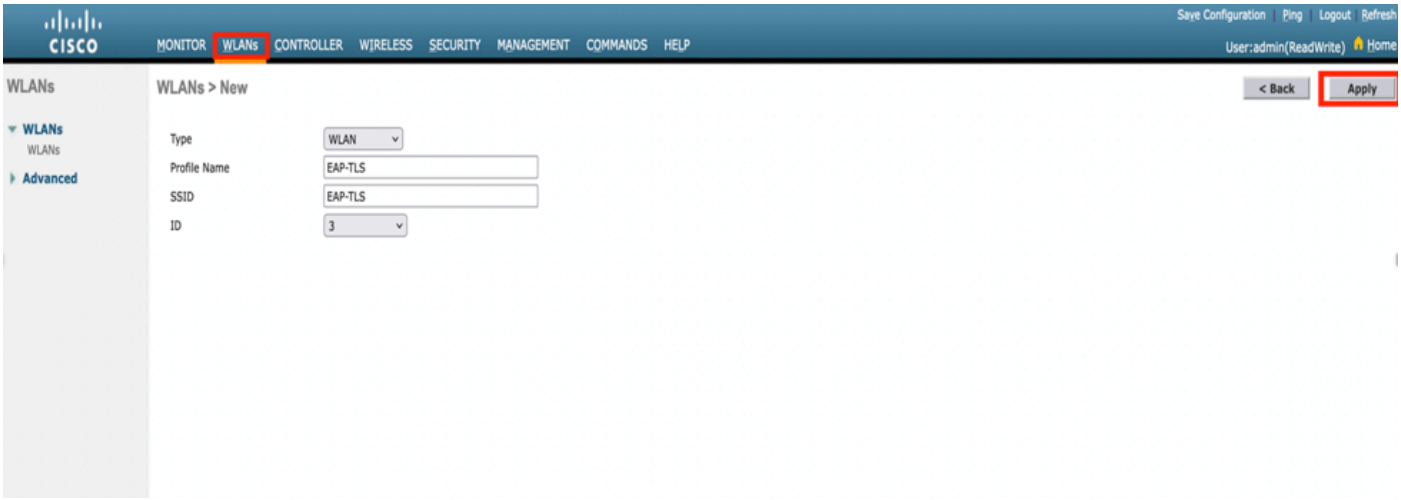


ステップ 3： RADIUS 認証用の WLAN を作成します。

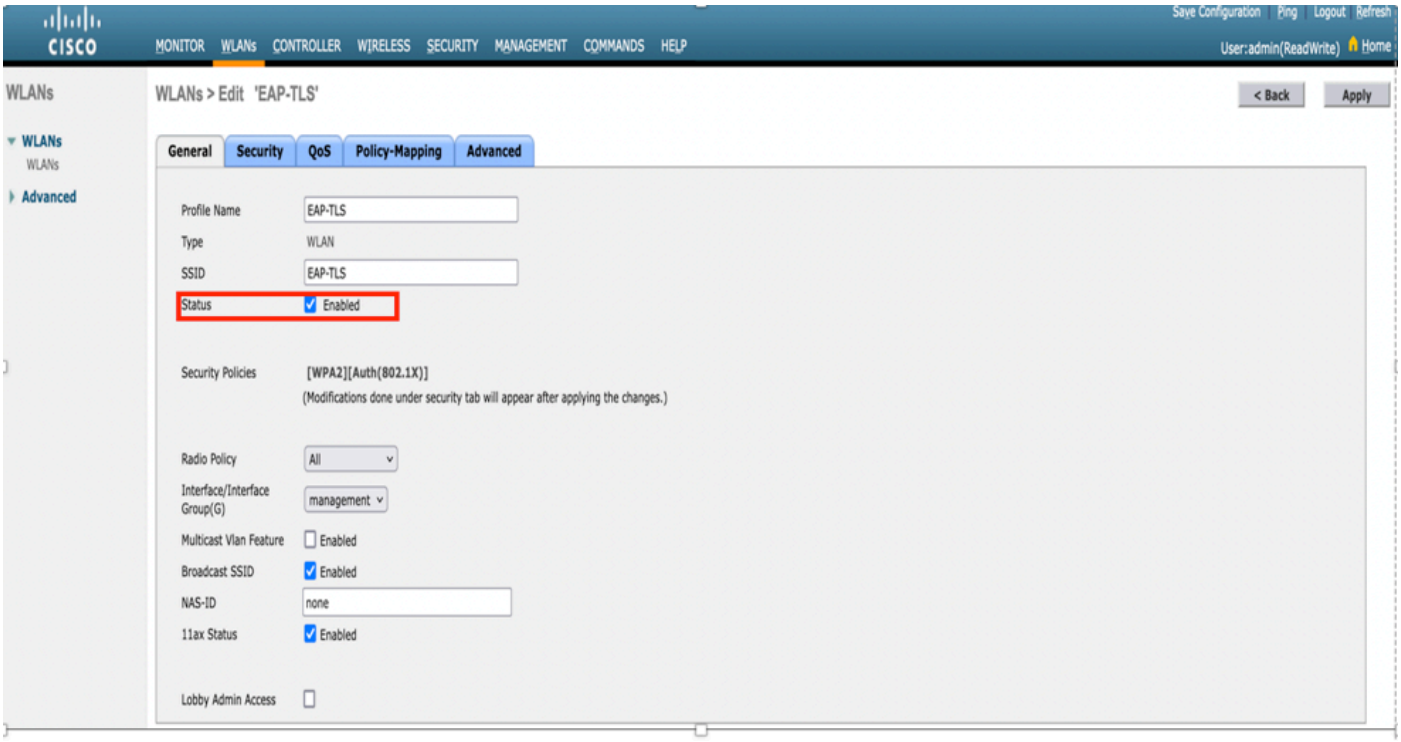
ここで、新しい WLAN を作成できます。この WLAN を、WPA-enterprise モードを使用するように設定することで、認証に RADIUS を使用できるようになります。

ステップ 4： 図のように、メインメニューから [WLAN（WLANs）] を選択し、[新規に作成（Create New）] を選択して、[実行（Go）] をクリックします。

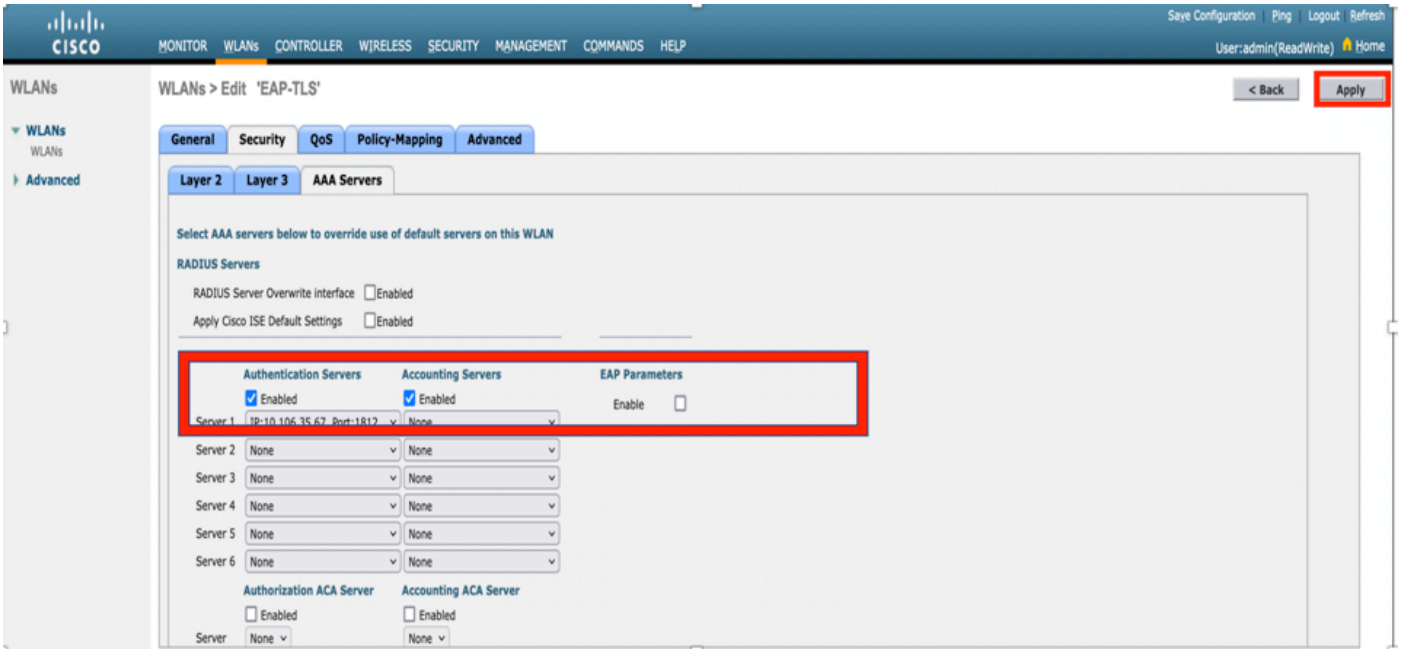
ステップ5：新しいWLANに**EAP-TLS**という名前を付けます。図のように、[適用（Apply）] をクリックして続行します。



ステップ 6： [全般（General）] をクリックし、[ステータス（Status）] が [有効（Enabled）] であることを確認します。図のように、デフォルトのセキュリティポリシーは 802.1X 認証と WPA2 です。



ステップ7：次に、[Security] > [AAA Servers] タブに移動し、図に示すように、設定した RADIUSサーバを選択します。



注：先に進む前に、WLC から RADIUS サーバに到達できることを確認することをお勧めします。RADIUS は UDP ポート 1812（認証用）を使用するため、このトラフィックがネットワークのどこにおいてもブロックされないようにする必要があります。

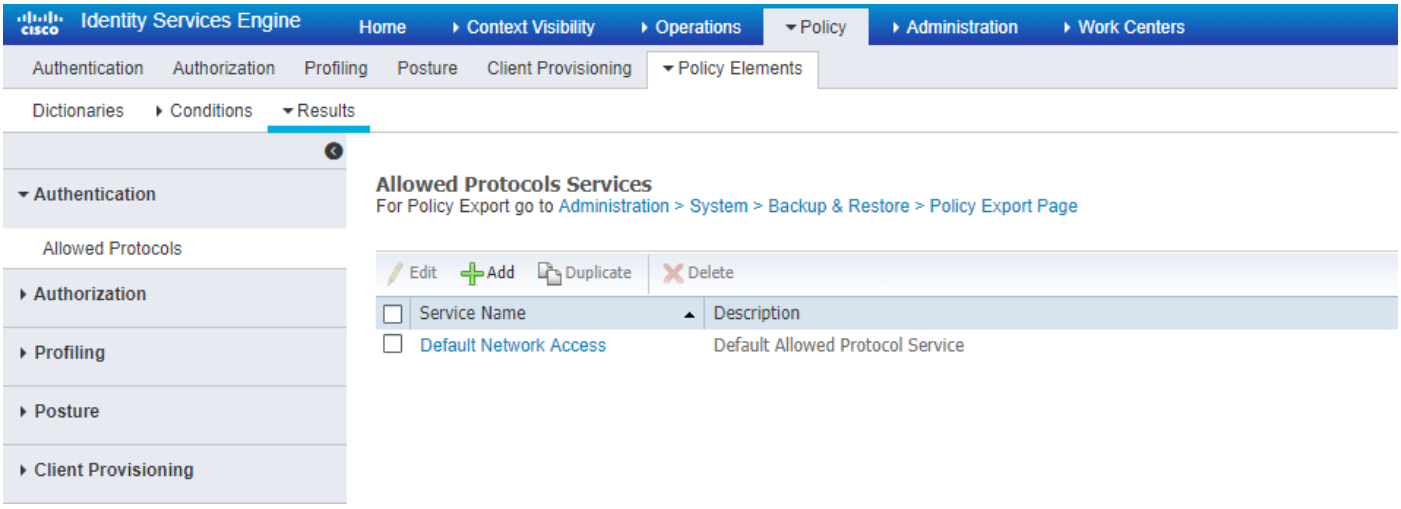
ISE と Cisco WLC

EAP-TLS 設定

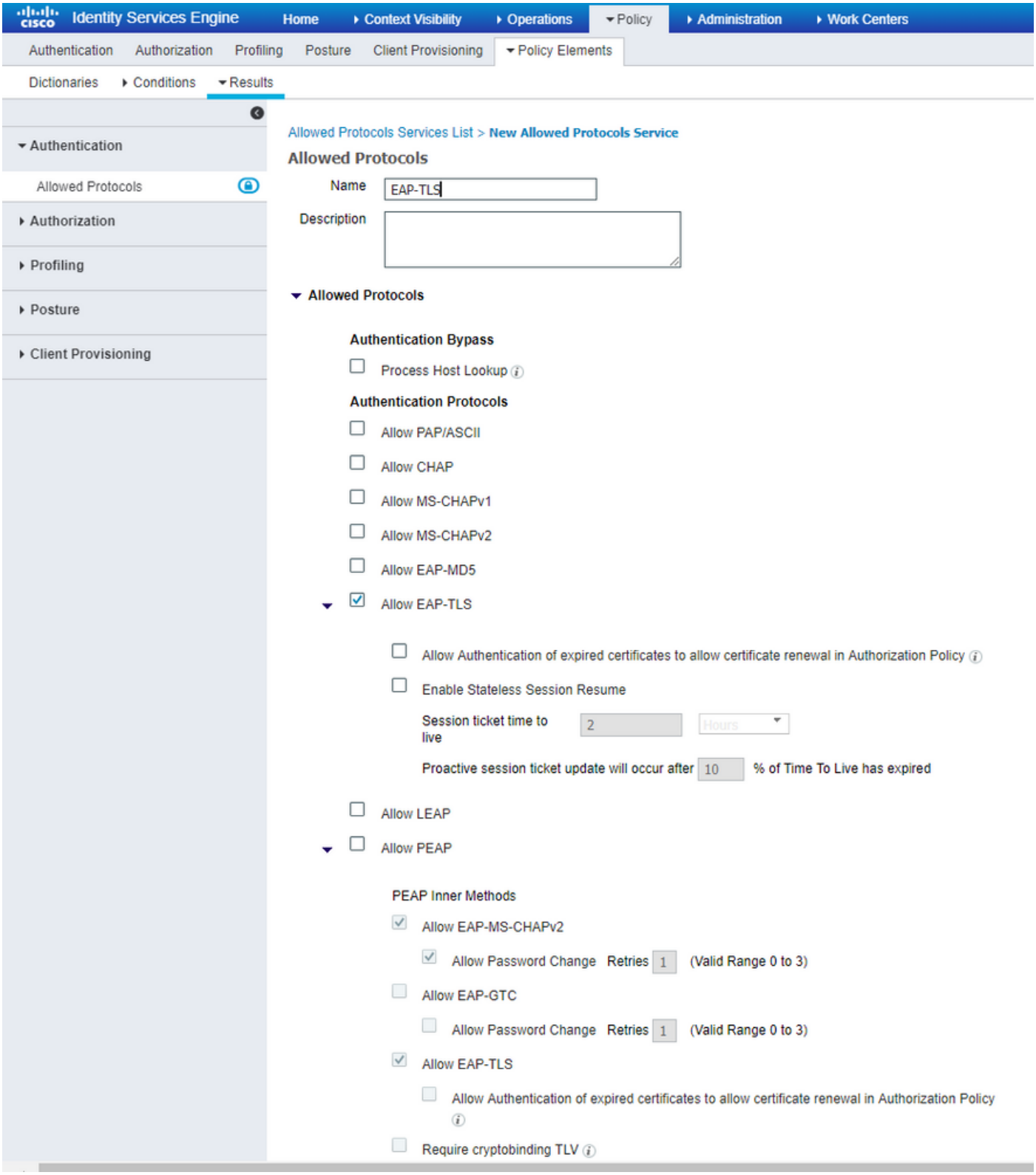
ポリシーを作成するために、ポリシーで使用する許可プロトコルリストを作成する必要があります。dot1x ポリシーを作成するため、ポリシーの設定方針に基づいて許可される EAP タイプを指定します。

デフォルトを使用すると、特定のEAPタイプへのアクセスをロックダウンする必要がある場合に推奨されない、ほとんどのEAPタイプを認証に使用できます。

ステップ 1： 図のように、[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [認証（Authentication）] > [許可されるプロトコル（Allowed Protocols）] に移動し、[追加（Add）] をクリックします。

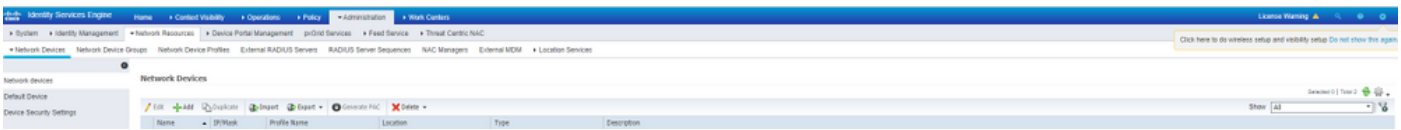


ステップ2：この[Allowed Protocol]リストで、リストの名前を入力できます。この場合、図のように、[EAP-TLSを許可（Allow EAP-TLS）] チェックボックスをオンにして、他のチェックボックスをオフにします。

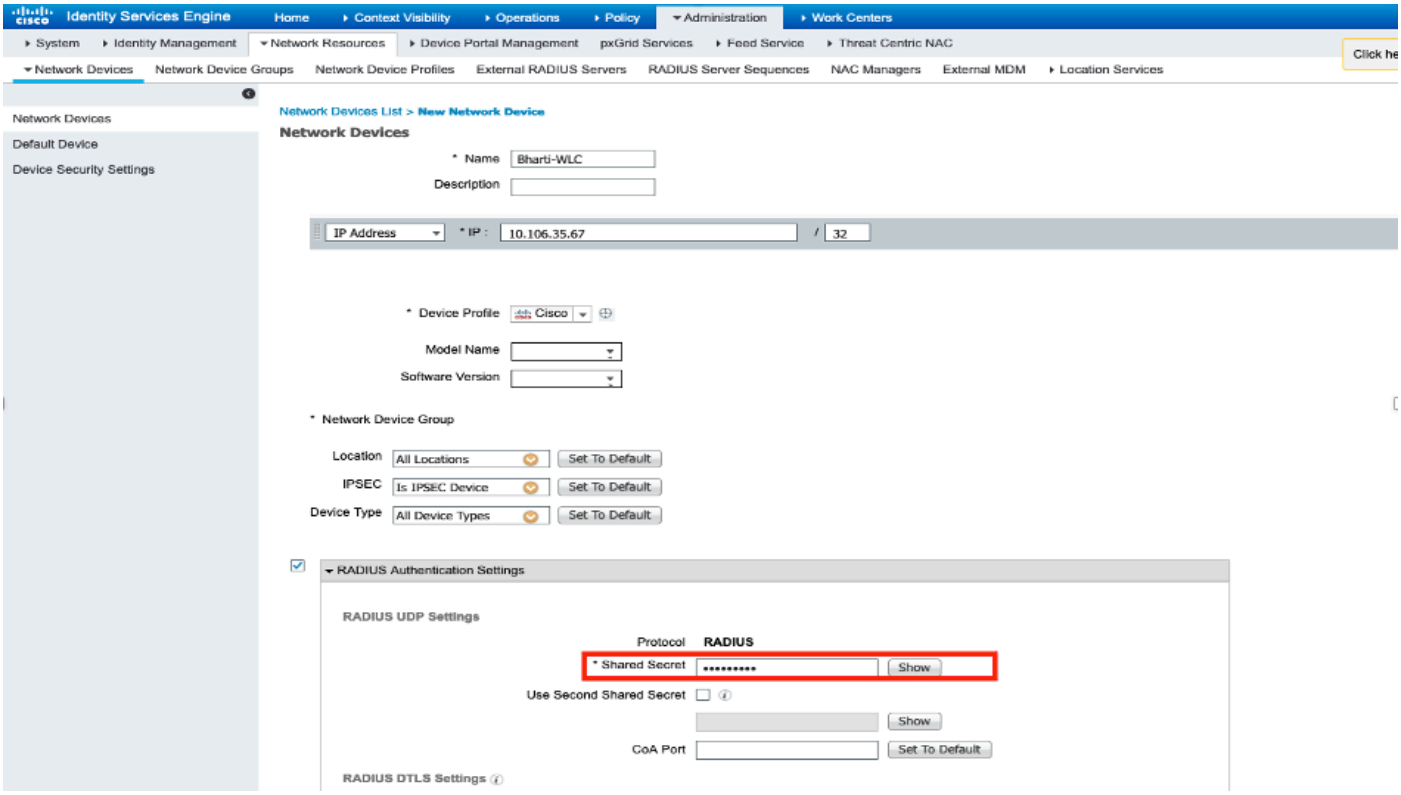


ISE での WLC の設定

ステップ 1： 図のように、ISE コンソールを開き、[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）] > [追加（Add）] に移動します。

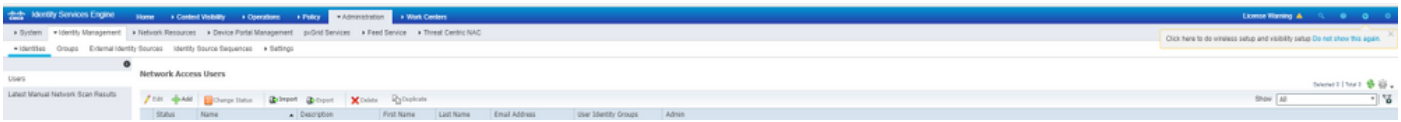


ステップ 2： 図にように、値を入力します。

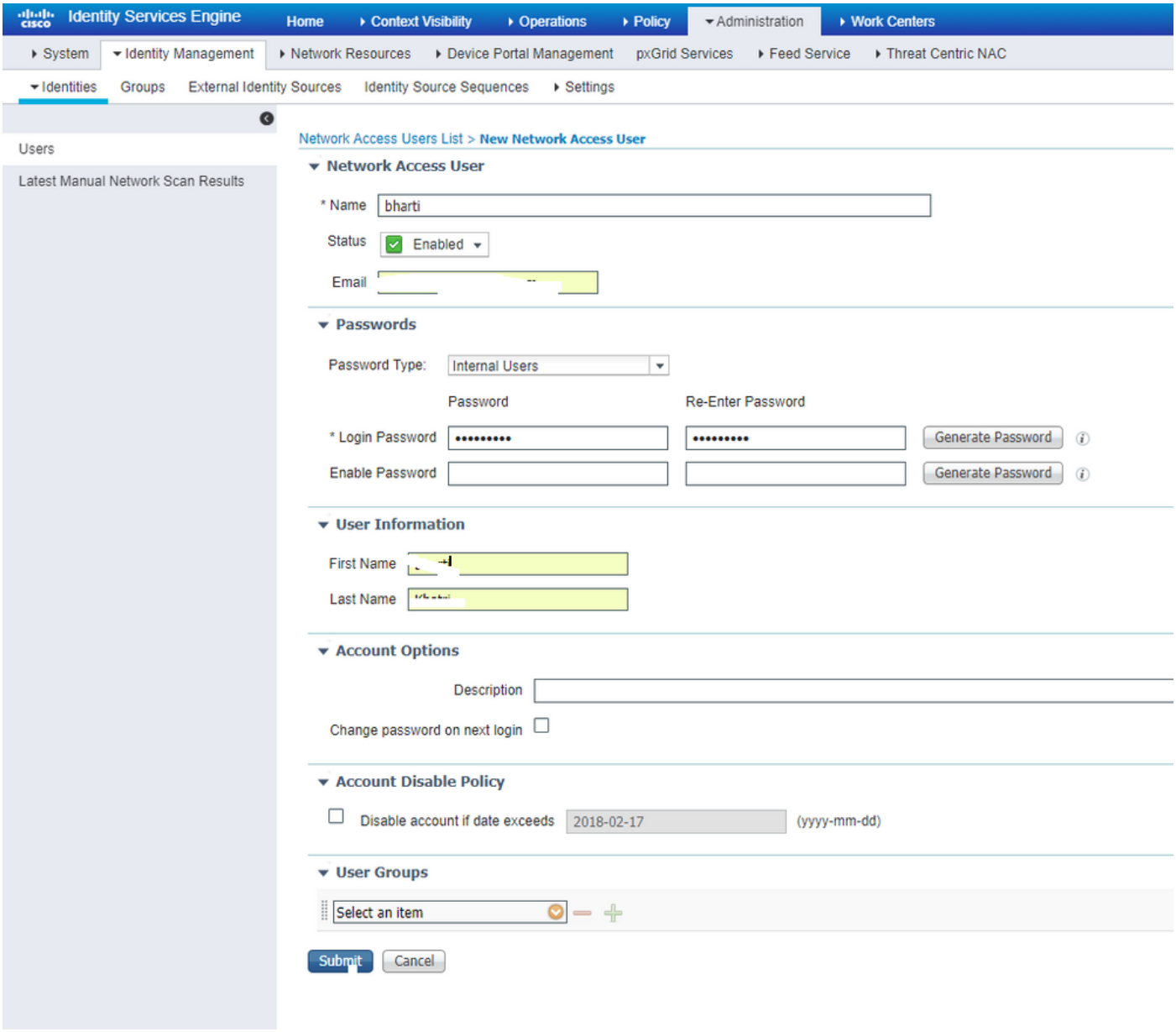


ISE での新しいユーザの作成

ステップ 1： 図のように、[管理（Administration）] > [IDの管理（Identity Management）] > [ID（Identities）] > [ユーザ（Users）] > [追加（Add）] に移動します。



ステップ 2： 図のように、情報を入力します。

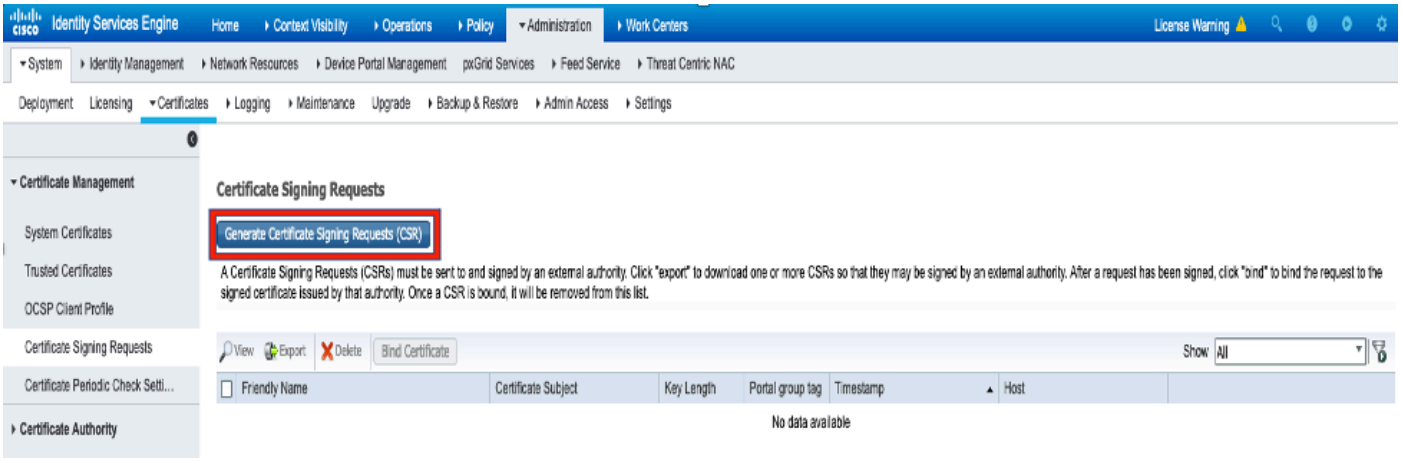


ISE での証明書の信頼確立

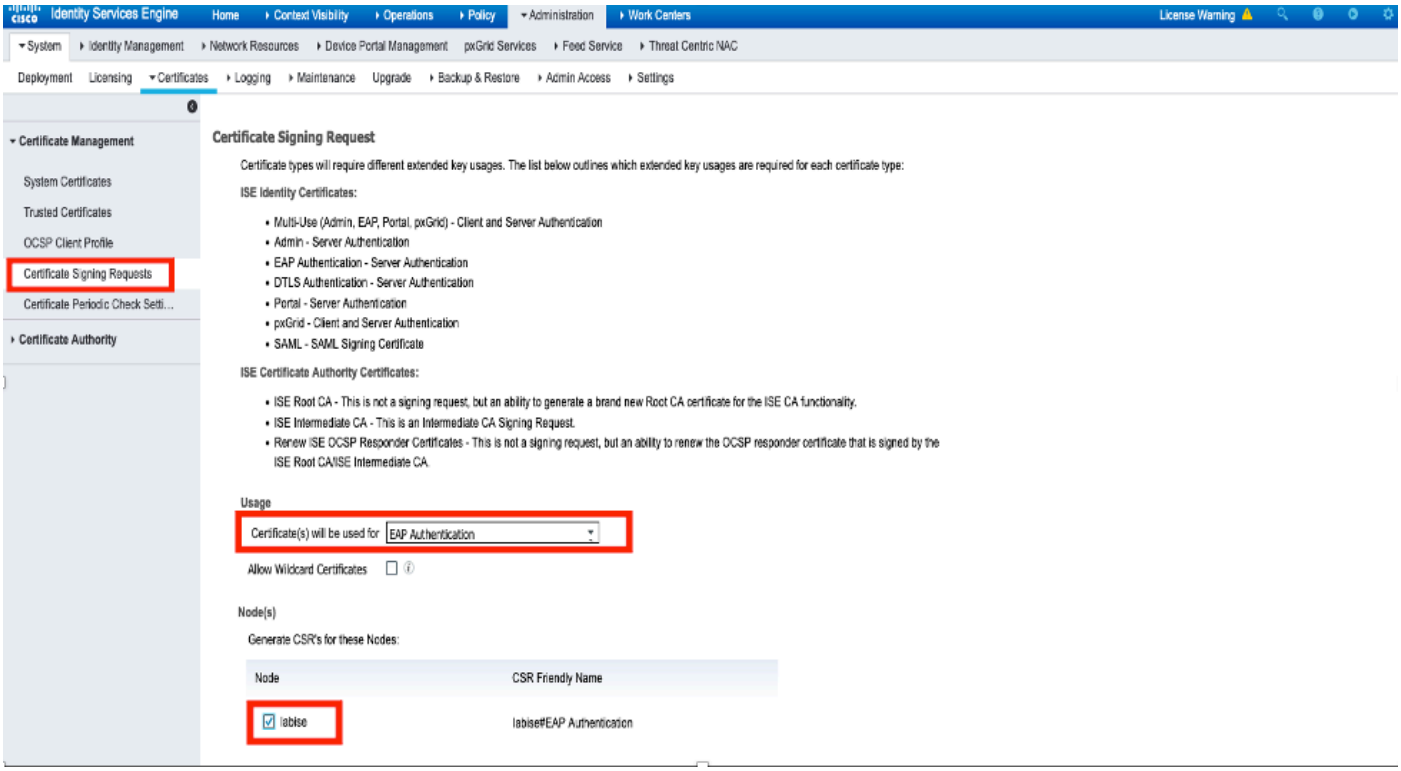
ステップ 1： [管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書の管理（Certificate Management）] > [信頼できる証明書（Trusted Certificates）] に移動します。

[インポート（Import）]をクリックして ISEに証明書をインポートします。WLC を追加し、ISE でユーザを作成したら、ISE で証明書の信頼を確立するという EAP-TLS の最も重要な部分を実行する必要があります。そのために、CSR を生成する必要があります。

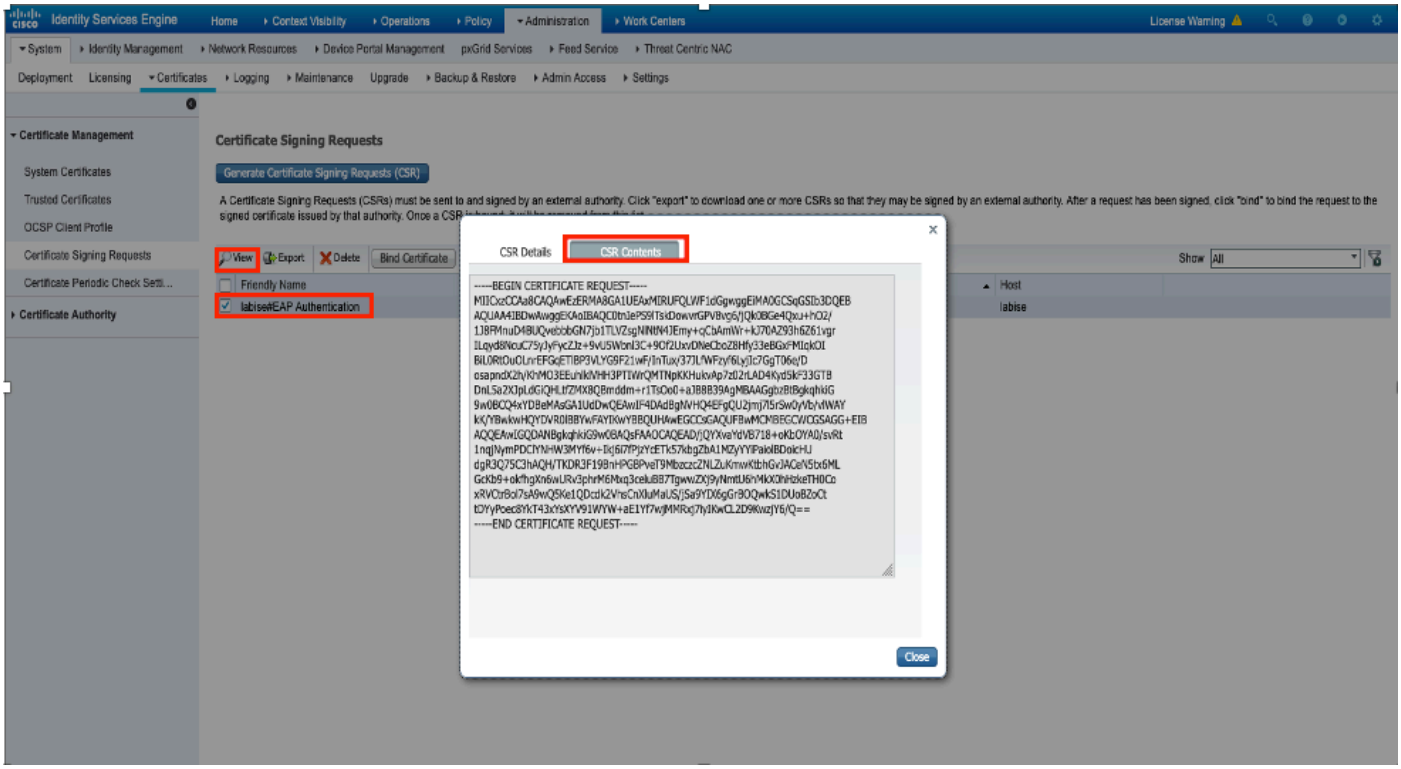
ステップ 2： 図のように、[管理（Administrauon）] > [証明書（Certificates）] > [証明書署名要求（Certificate Signing Requests）] > [証明書署名要求（CSR）の生成（Generate Certificate Signing Requests (CSR)）] に移動します。



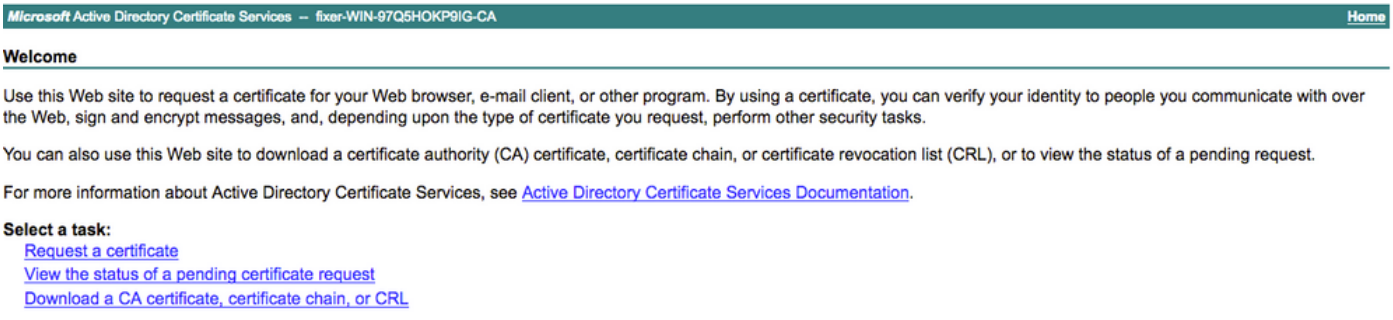
ステップ3:CSRを生成するには、[Usage] に移動し、[Certificate(s) are used for] ドロップダウンオプションから[EAP Authentication] を選択します（図を参照）。



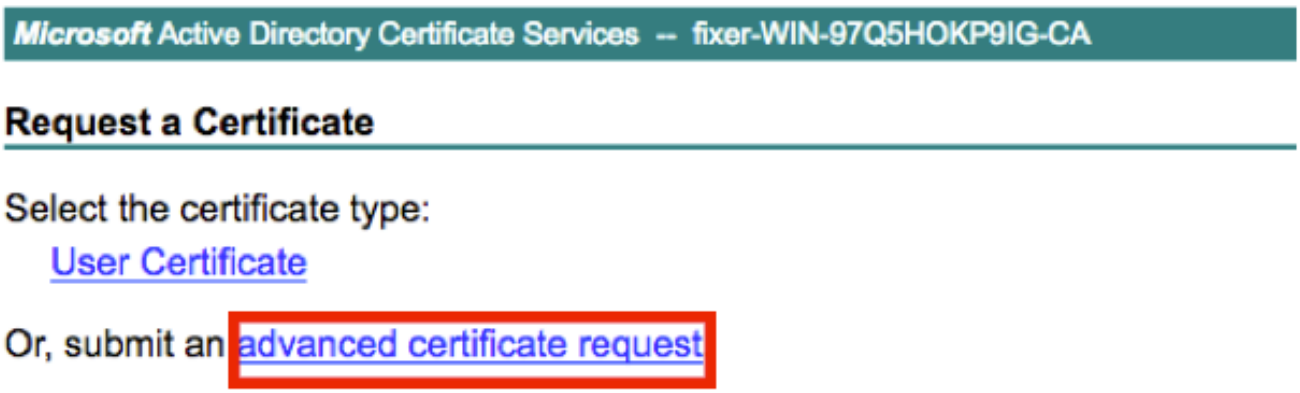
ステップ4:ISEで生成されたCSRを表示できます。図のように、[表示（View）] をクリックします。



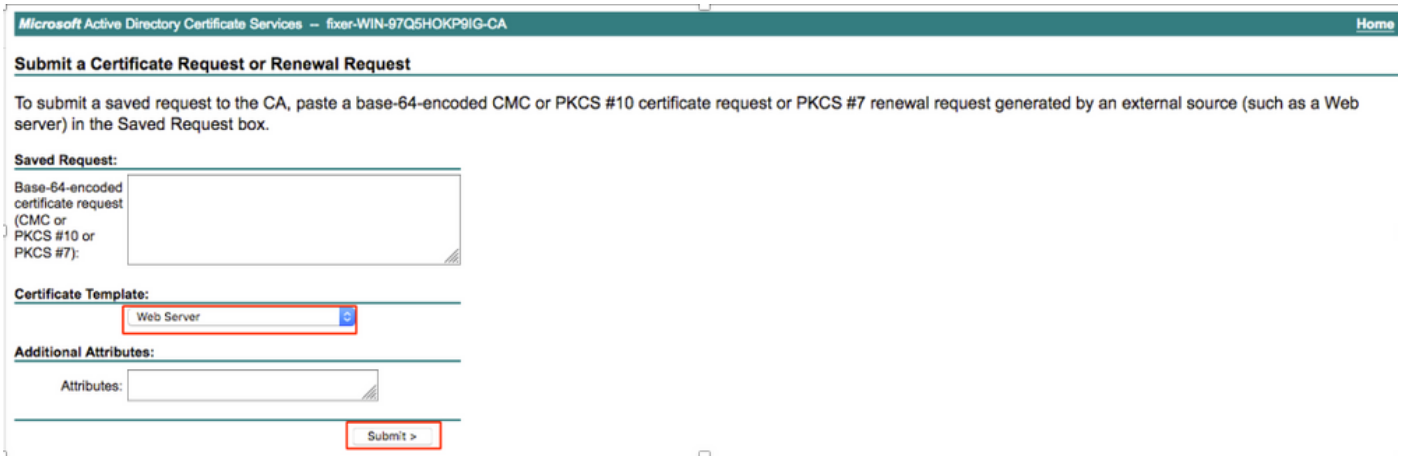
ステップ5:CSRが生成されたら、図に示すように、CAサーバを参照し、[Request a certificate] をクリックします。



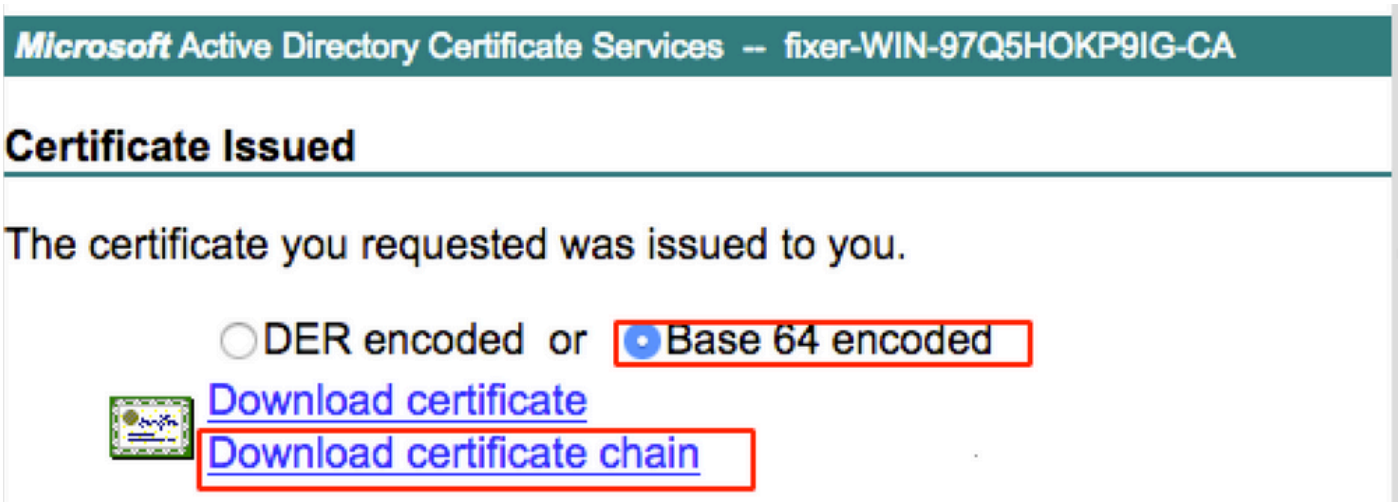
ステップ6：証明書を要求すると、[User Certificate] と[advanced certificate request] のオプションが表示されます。次の図に示すように、[advanced certificate request] をクリックします。



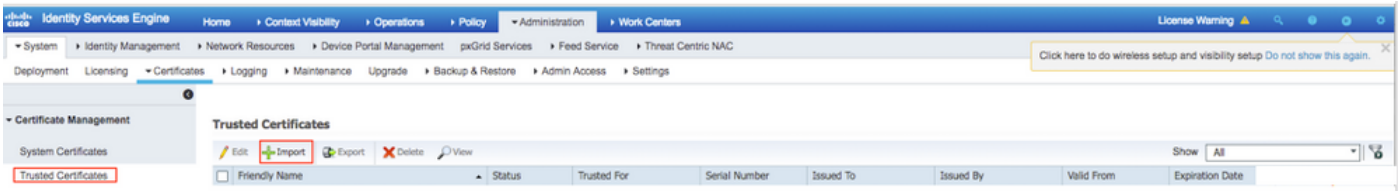
ステップ 7： 生成された CSR を [Base-64エンコード証明書要求（Base-64 encoded certificate request）] に貼り付けます。図のように、[証明書テンプレート：（Certificate Template:）] ドロップダウンオプションから [Webサーバ（Web Server）] を選択し、[送信（Submit）] をクリックします。

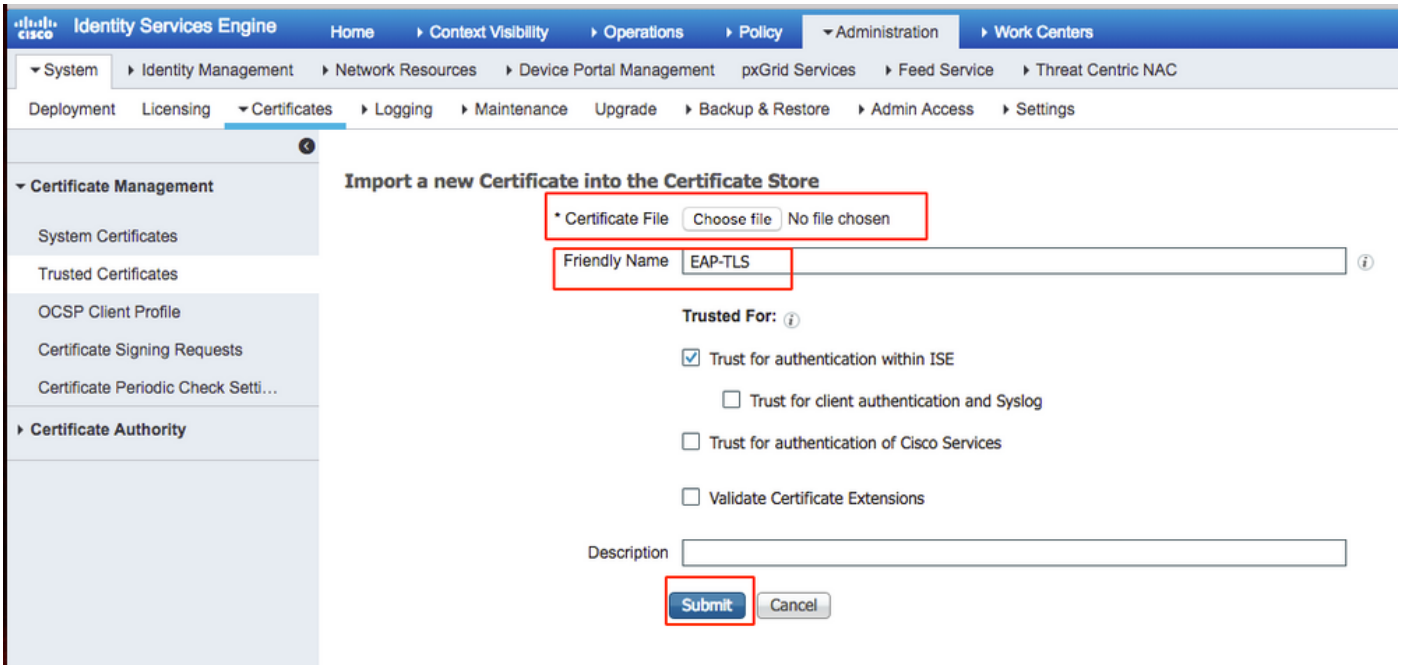


ステップ8:[Submit] をクリックすると、証明書のタイプを選択するオプションが表示されます。次に、[Base-64 encoded] を選択し、[Download certificate chain] をクリックします（図を参照）。

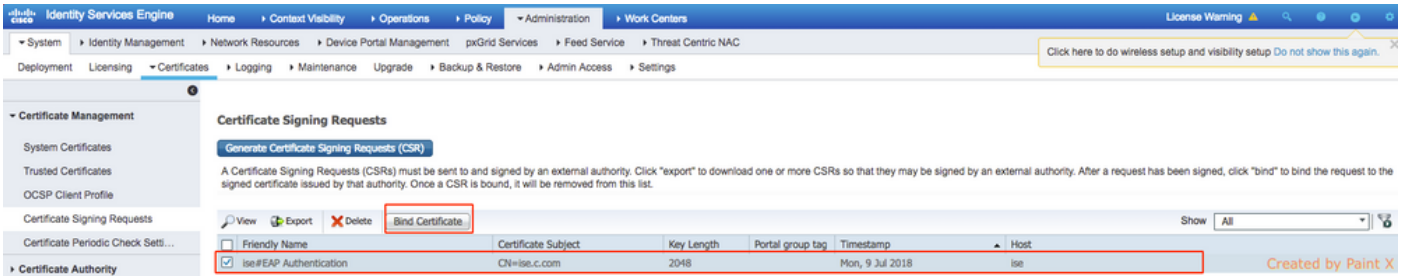


ステップ9:ISEサーバの証明書のダウンロードが完了します。証明書を抽出できます。証明書には、1つのルート証明書と他の中間証明書の2つの証明書が含まれています。ルート証明書は、図のように、[管理（Administration）] > [証明書（Certifictes）] > [信頼できる証明書（Trusted certificates）] > [インポート（Import）] を選択してインポートできます。

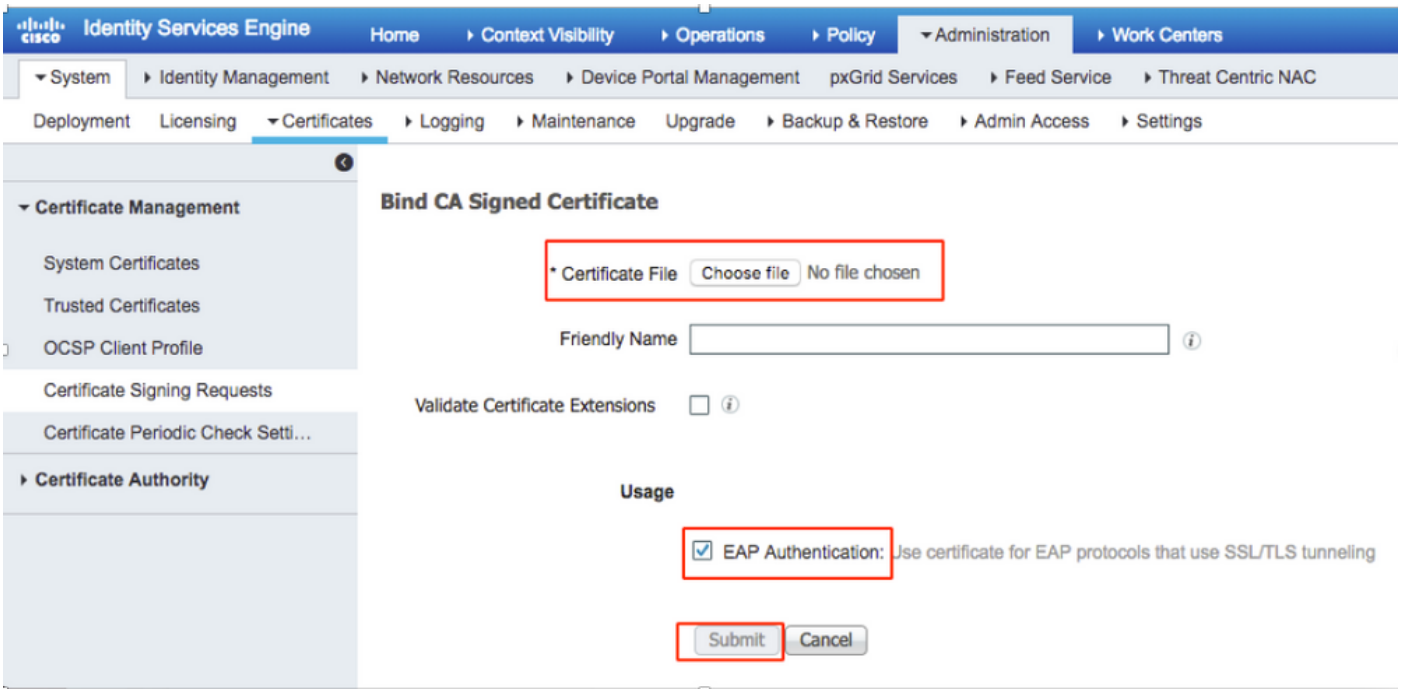




ステップ10:[Submit] をクリックすると、信頼できる証明書リストに証明書が追加されます。また、図のように、CSR にバインドするには中間証明書が必要です。

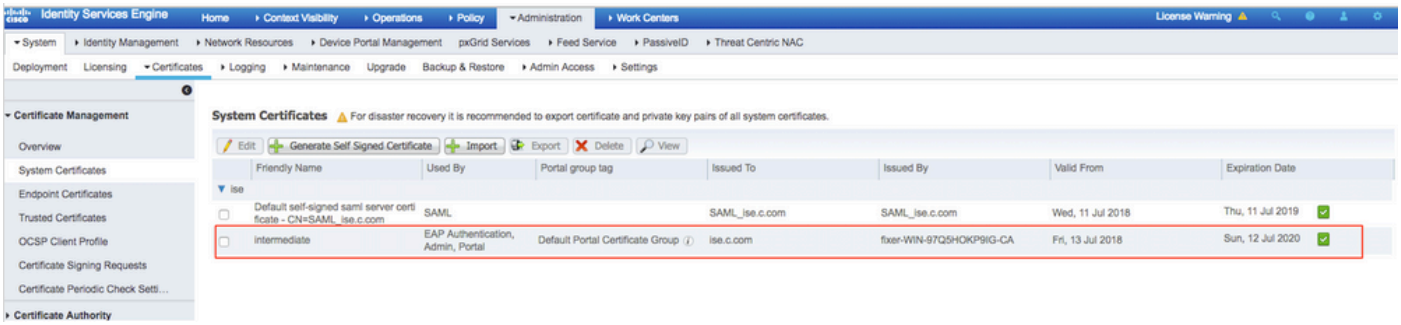


ステップ11:[Bind certificate] をクリックすると、デスクトップに保存されている証明書ファイルを選択するオプションがあります。図のように、中間証明書を選択し、[送信（Submit）] をクリックします。



ステップ12：証明書を表示するには、図に示すように、[Administration] > [Certificates] > [System

Certificates] に移動します。



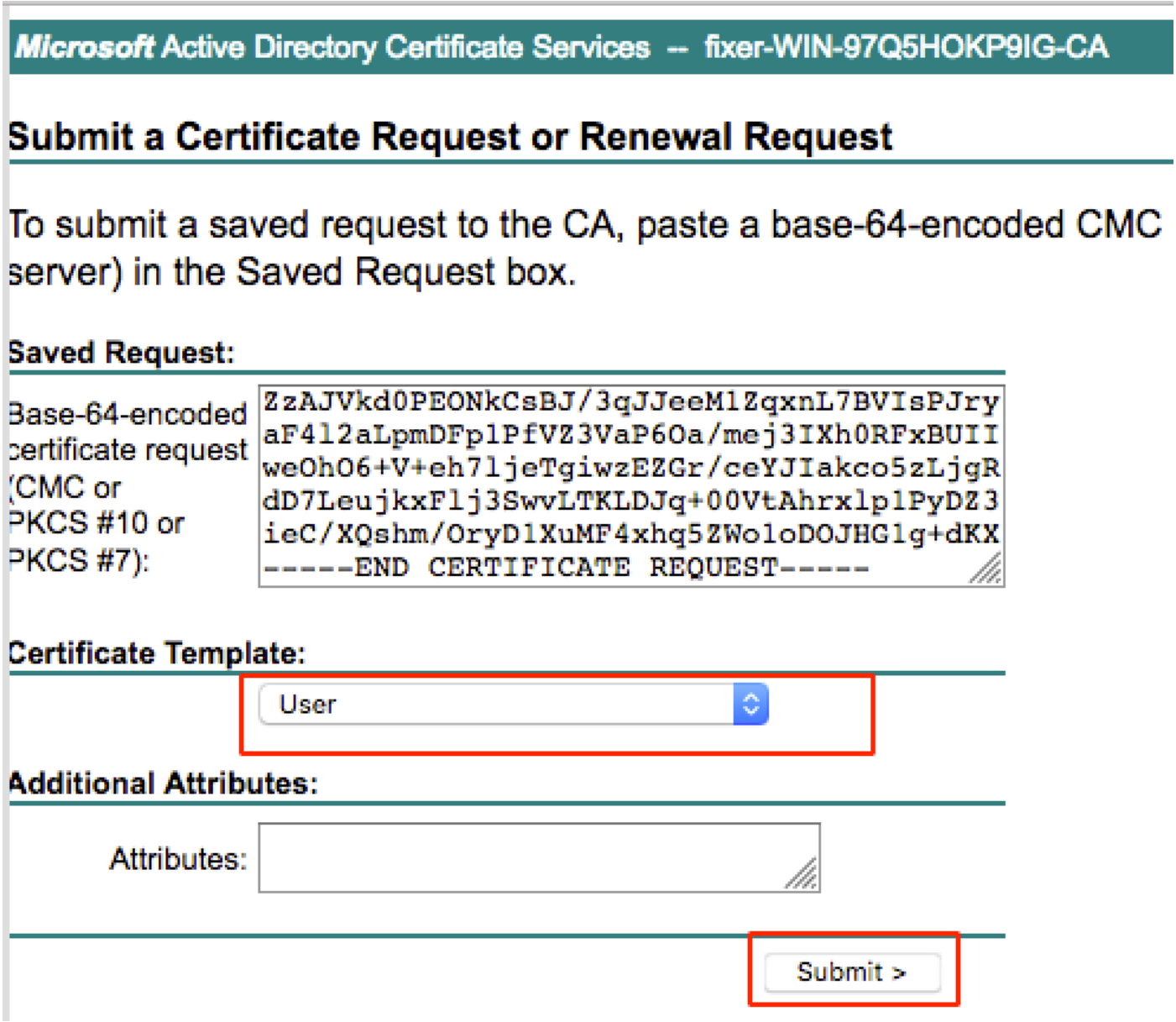
EAP-TLS 用のクライアント

クライアントマシン（Windows デスクトップ）へのユーザ証明書のダウンロード

ステップ 1： EAP-TLS を使用してワイヤレスユーザを認証するには、クライアント証明書を生成する必要があります。サーバにアクセスできるように、Windows コンピュータをネットワークに接続します。Web ブラウザを開き、次のアドレスを入力します：https://sever ip addr/certsrv:

ステップ2:CAは、ISE用に証明書をダウンロードしたCAと同じである必要があります。

そのために、サーバ用の証明書のダウンロードに使用した CA サーバにアクセスする必要があります。同じ CA で以前と同じように [証明書を要求する（Request a certificate）] をクリックしますが、今回は、図のように、[証明書テンプレート（Certificate Template）] で [ユーザ（User）] を選択する必要があります。



ステップ3：次に、先にサーバで行ったように、[download certificate chain] をクリックします。

証明書を取得したら、次の手順に従って証明書を Windows ラップトップにインポートします。

ステップ 4： 証明書をインポートするには、Microsoft 管理コンソール（MMC）から証明書にアクセスする必要があります。

1. MMC を開くには、[スタート（Start）] > [ファイル名を指定して実行（Run）] > [MMC] に移動します。
2. [ファイル（File）] > [スナップインの追加と削除（Add / Remove Snap In] に移動します。
3. [証明書（Certificates）] をダブルクリックします。
4. [コンピューターアカウント（Computer Account）] を選択します。
5. [ローカルコンピューター（Local Computer）] > [完了（Finish）] を選択します。
6. [OK] をクリックして[スナップイン（Snap-In）] ウィンドウを終了します。
7. [証明書（Certificates）] の横にある [+] をクリックし、[個人（Personal）] > [証明書（Certificates）] を選択します。
8. [証明書（Certificates）] を右クリックし、[すべてのタスク（All Tasks）] > [インポート（Import）] を選択します。
9. [next] をクリックします。

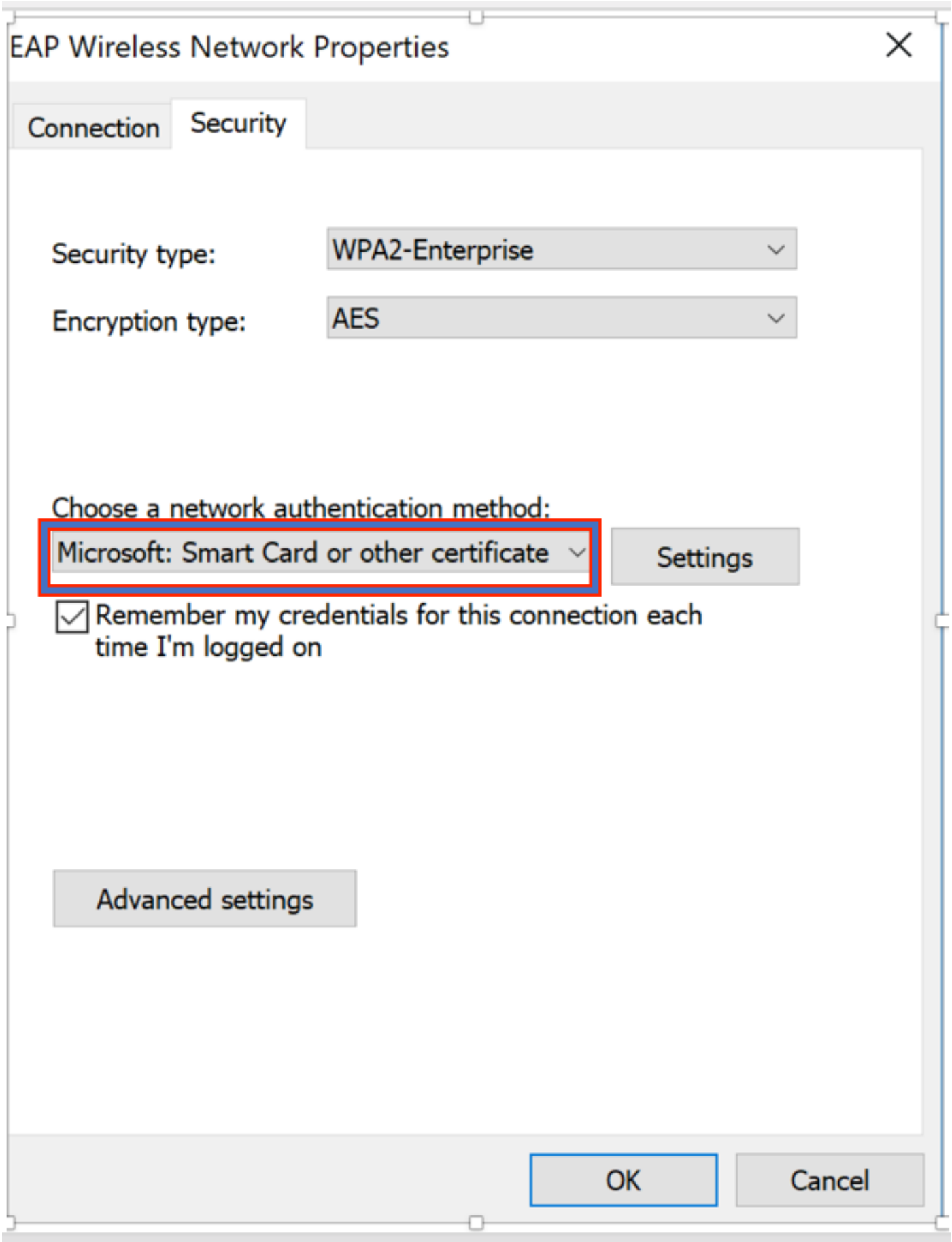
10. [Browse] をクリックします。
11. インポートする .cer、.crt、または .pfx ファイルを選択します。
12. [Open] をクリックします。
13. [next] をクリックします。
14. [証明書の種類に基づいて、自動的に証明書ストアを選択する（Automatically select the certificate store based on the type of certificate）] を選択します。
15. [完了（Finish）]、[OK] の順にクリックしてます。

証明書のインポートが完了したら、ワイヤレスクライアント（この例では Windows デスクトップ）を EAP-TLS 用に設定する必要があります。

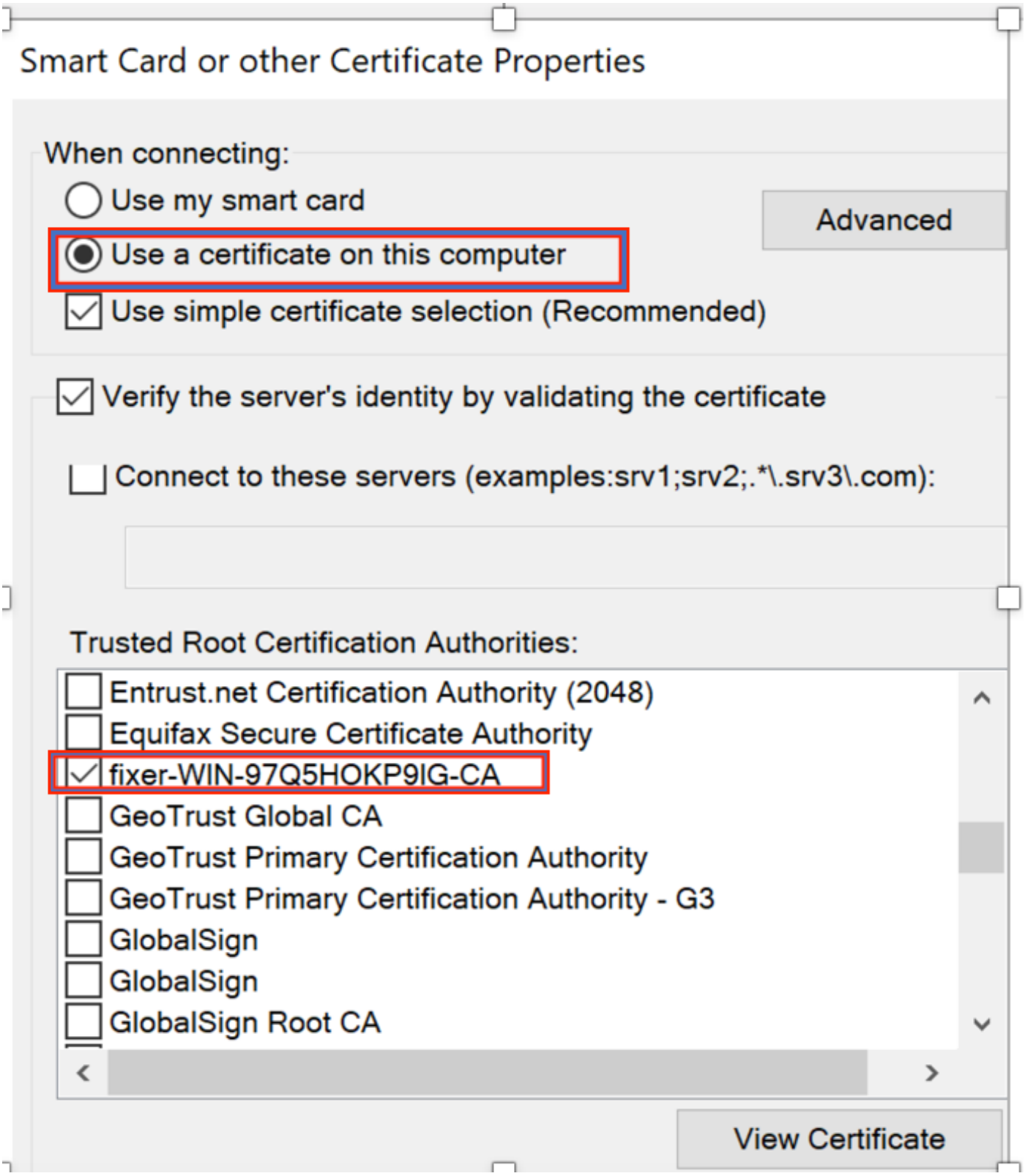
EAP-TLS のワイヤレスプロファイル

ステップ 1： Protected Extensible Authentication Protocol（PEAP）の代わりに EAP-TLS を使用するために、PEAP 用に以前に作成されたワイヤレスプロファイルを変更します。EAP ワイヤレスプロファイルをクリックします。

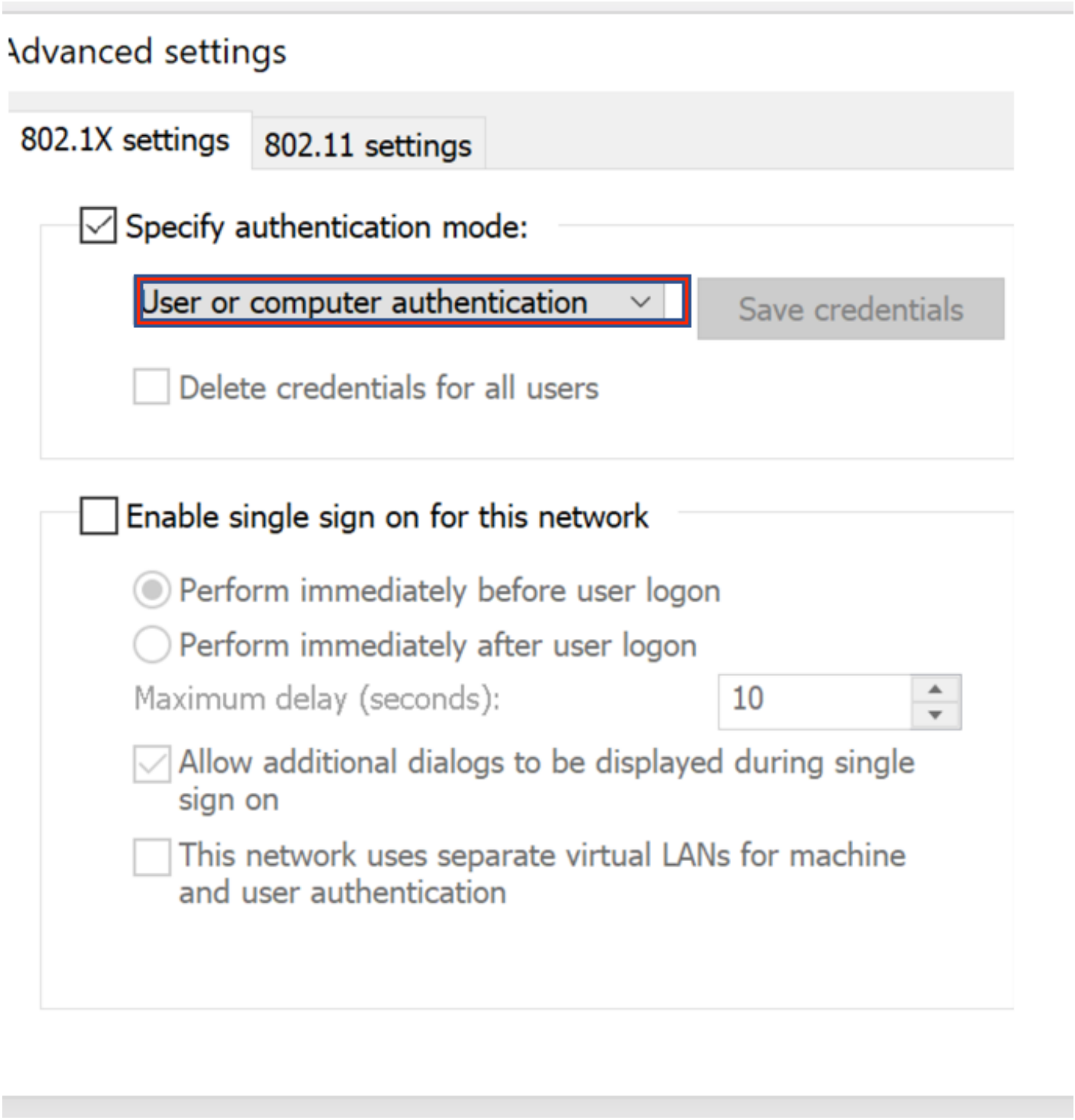
ステップ 2： 図のように、[Microsoft：**スマートカードまたはその他の証明書（Microsoft: Smart Card or other certificate）] を選択し、[OK] をクリックします。**



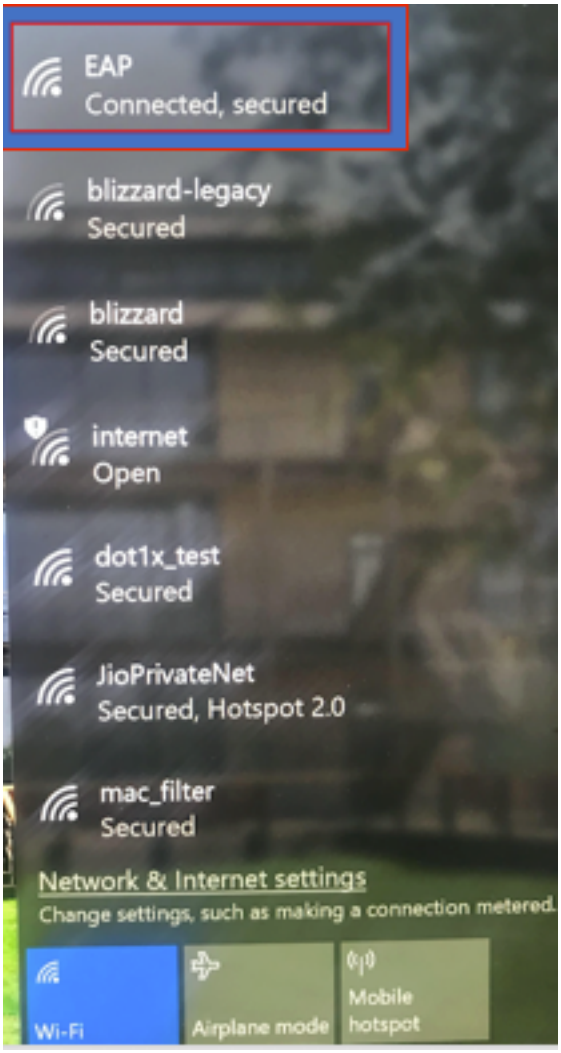
ステップ 3： [設定（Settings）] をクリックし、図のように、CA サーバから発行されたルート証明書を選択します。



ステップ 4： [詳細設定（Advanced Settings）] をクリックし、図のように、[802.1x設定（802.1x settings）] タブで [ユーザまたはコンピュータ認証（User or computer authentication）] を選択します。



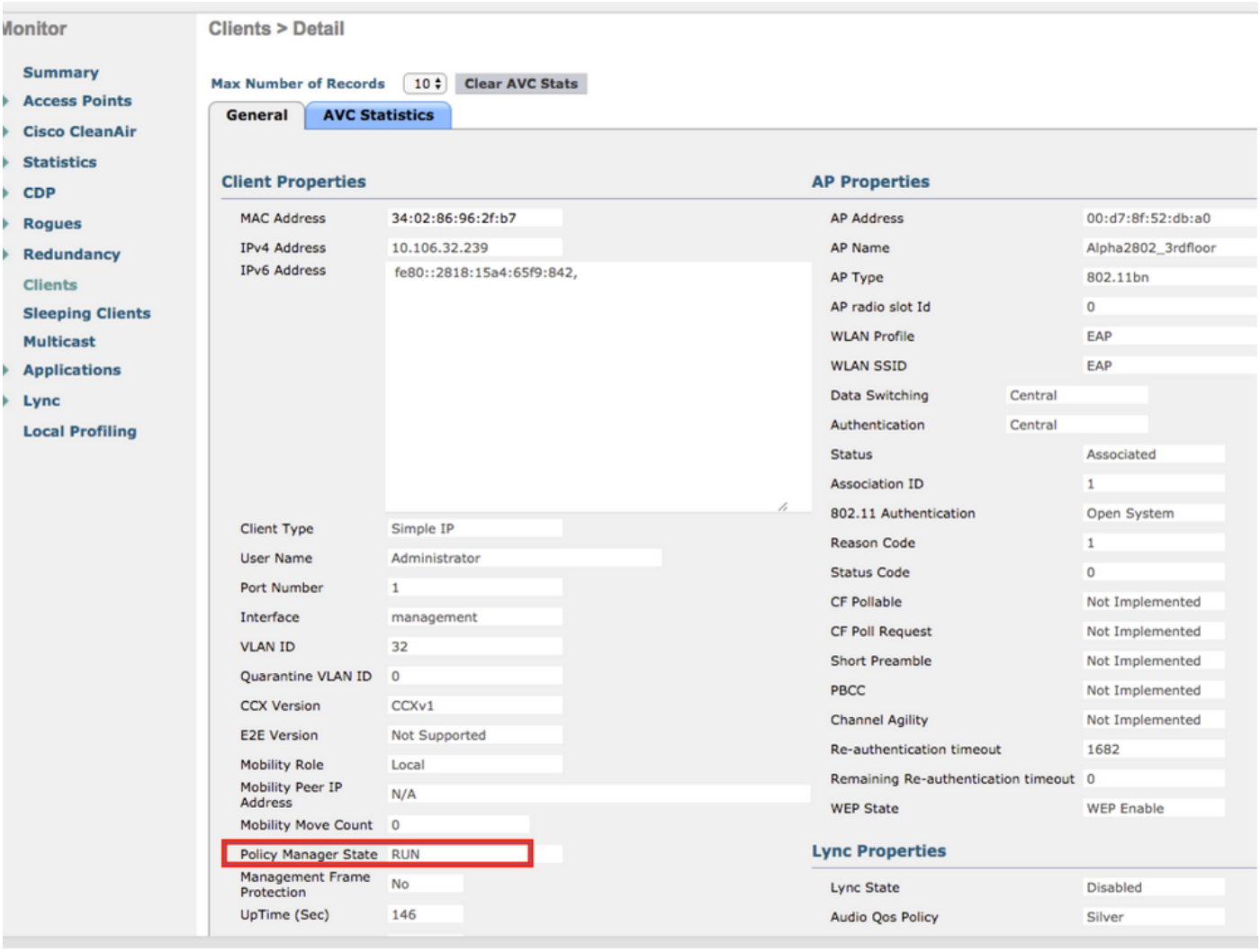
ステップ5：ここで、ワイヤレスネットワークへの接続を再試行し、正しいプロファイル（この例ではEAP）を選択して、**Connect**をクリックします。図のように、ワイヤレスネットワークに接続されます。



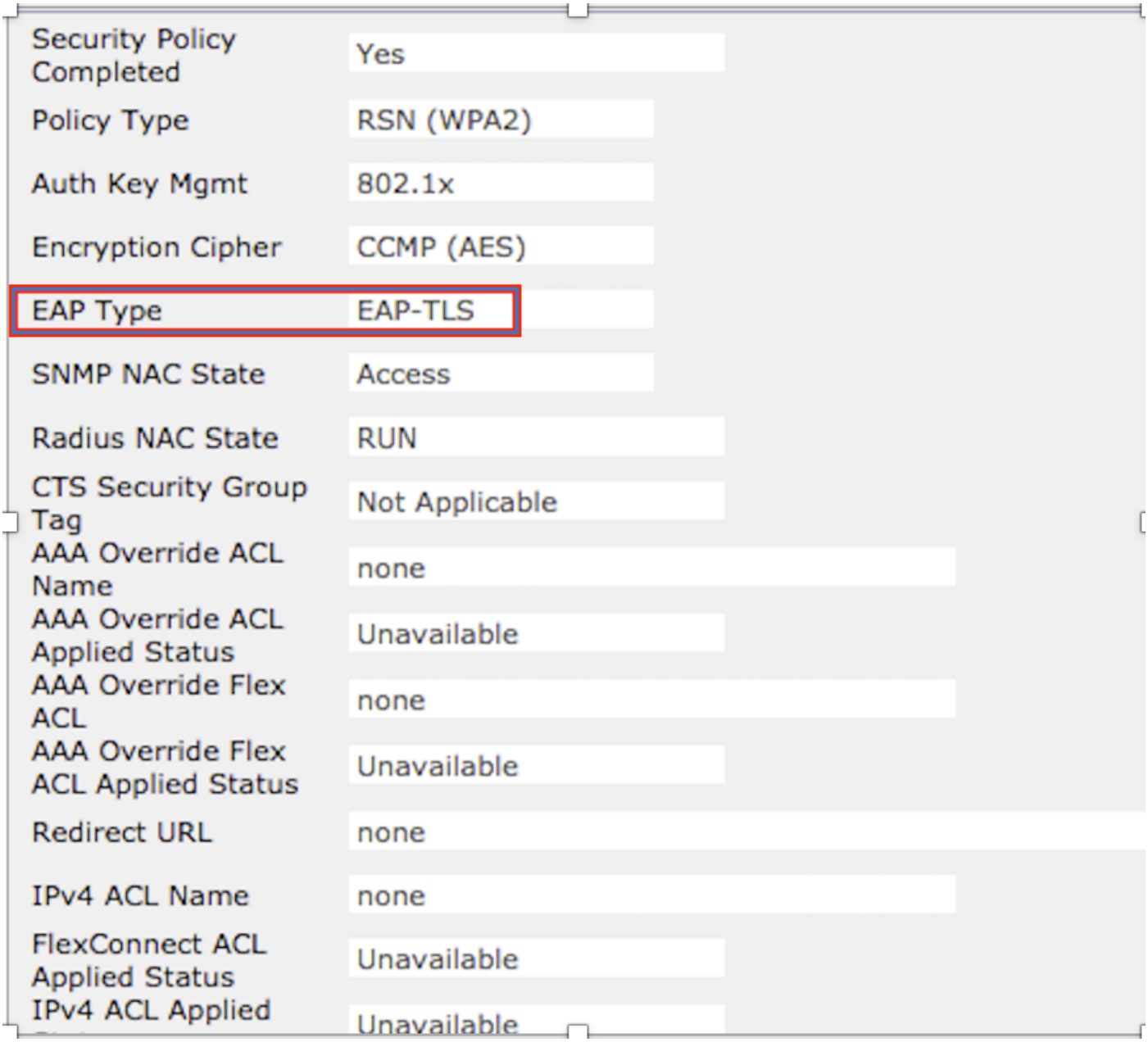
確認

ここでは、設定が正常に機能しているかどうかを確認します。

ステップ1：クライアントポリシーマネージャの状態がRUNと表示されている必要があります。これは、クライアントが、認証を完了し、IP アドレスを取得して、図に示されているトラフィックを渡す準備ができていることを意味します。



ステップ2：また、図に示すように、クライアントの詳細ページでWLCの正しいEAP方式を確認します。

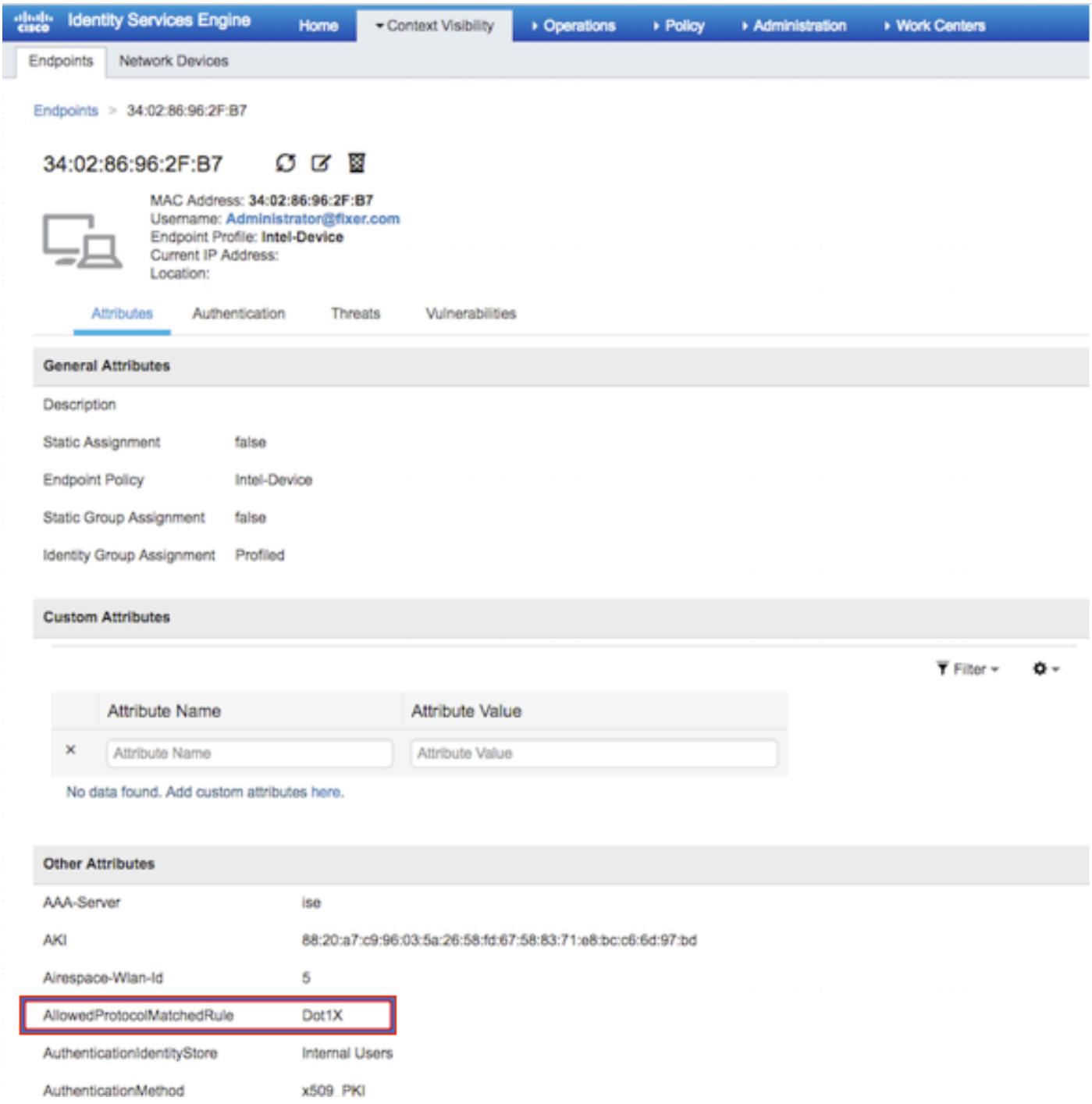


ステップ3：コントローラのCLIからのクライアントの詳細を次に示します（出力を省略）。

```
(Cisco Controller-Standby) >show client detail 34:02:86:96:2f:b7
Client MAC Address.............................. 34:02:86:96:2f:b7
Client Username ................................ Administrator
AP MAC Address.................................. 00:d7:8f:52:db:a0
AP Name.......................................... Alpha2802_3rdfloor
AP radio slot Id................................ 0
Client State.................................... Associated
Wireless LAN Id................................. 5
Wireless LAN Network Name (SSID)................ EAP
Wireless LAN Profile Name....................... EAP
Hotspot (802.11u)............................... Not Supported
BSSID........................................... 00:d7:8f:52:db:a4
Connected For .................................. 48 secs
Channel......................................... 1
IP Address...................................... 10.106.32.239
Gateway Address................................. 10.106.32.1
Netmask......................................... 255.255.255.0
Policy Manager State............................ RUN
Policy Type..................................... WPA2
Authentication Key Management................... 802.1x
```

```
Encryption Cipher.............................. CCMP-128 (AES)
Protected Management Frame ..................... No
Management Frame Protection..................... No
EAP Type....................................... EAP-TLS
```

ステップ4：図に示すように、ISEで[Context Visbility] > [End Points] > [Attributes] に移動します。



BYODRegistration	Unknown
Called-Station-ID	00-d7-8f-52-db-a0:EAP
Calling-Station-ID	34-02-86-96-2f-b7
Days to Expiry	363
DestinationIPAddress	10.106.32.31
DestinationPort	1812
DetailedInfo	Invalid username or password specified
Device IP Address	10.106.32.223
Device Port	32775
Device Type	Device Type#All Device Types
DeviceRegistrationStatus	NotRegistered
ElapsedDays	7
EnableFlag	Enabled
EndPointMACAddress	34-02-86-96-2F-B7
EndPointPolicy	Intel-Device
EndPointProfilerServer	ise.c.com
EndPointSource	RADIUS Probe
Extended Key Usage - Name	130, 132, 138
Extended Key Usage - OID	1.3.6.1.5.5.7.3.2, 1.3.6.1.5.5.7.3.4, 1.3.6.1.4.1.311.1
FailureReason	-
IdentityGroup	Profiled
InactiveDays	5
IsThirdPartyDeviceFlow	false
Issuer	CN=fixer-WIN-97Q5HOKP9IG-CA\,DC=fixer\,DC=c
Issuer - Common Name	fixer-WIN-97Q5HOKP9IG-CA
Issuer - Domain Component	fixer, com

Location	Location#All Locations
MACAddress	34:02:86:96:2F:B7
MatchedPolicy	Intel-Device
MessageCode	5200
NAS-IP-Address	10.106.32.223
NAS-Identifier	HA_Pri
NAS-Port	1
NAS-Port-Type	Wireless - IEEE 802.11
Network Device Profile	Cisco
NetworkDeviceGroups	Location#All Locations, Device Type#All Device Types
NetworkDeviceName	HA_Pri
NetworkDeviceProfileId	403ea8fc-7a27-41c3-80bb-27964031a08d
NetworkDeviceProfileName	Cisco
OUI	Intel Corporate
OpenSSLErrorMessage	SSL alert: code=0x230=560 \; source=local \; type=fatal \; message="Unknown CA - error unable to get issuer certificate locally"
OpenSSLErrorStack	140160653813504:error:140890B2:SSL routines:SSL3_GET_CLIENT_CERTIFICATE:no certificate returned:s3_srvr.c:3370:
PolicyVersion	0
PostureApplicable	Yes
PostureAssessmentStatus	NotApplicable
RadiusFlowType	Wireless802_1x
RadiusPacketType	AccessRequest
SSID	00-d7-8f-52-db-a0:EAP
SelectedAccessService	Default Network Access
SelectedAuthenticationIdentityStores	EAPTLS
SelectedAuthorizationProfiles	PermitAccess
Serial Number	10 29 41 78 00 00 00 00 00 11

トラブルシュート

現在、この設定のトラブルシューティングに使用できる特定の情報はありません。

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。