Mobility Expressおよび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、Mobility Express Controllerで802.1xセキュリティを使用するワイヤレスローカルエリアネットワーク(WLAN)をセットアップする方法について説明します。このドキュメントでは、特にExtensible Authentication Protocol(EAP)-Transport Layer Security(TLS)の使用についても説明します。

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。

- Mobility Expressの初期設定
- 802.1x 認証プロセス
- 証明書

使用するコンポーネント

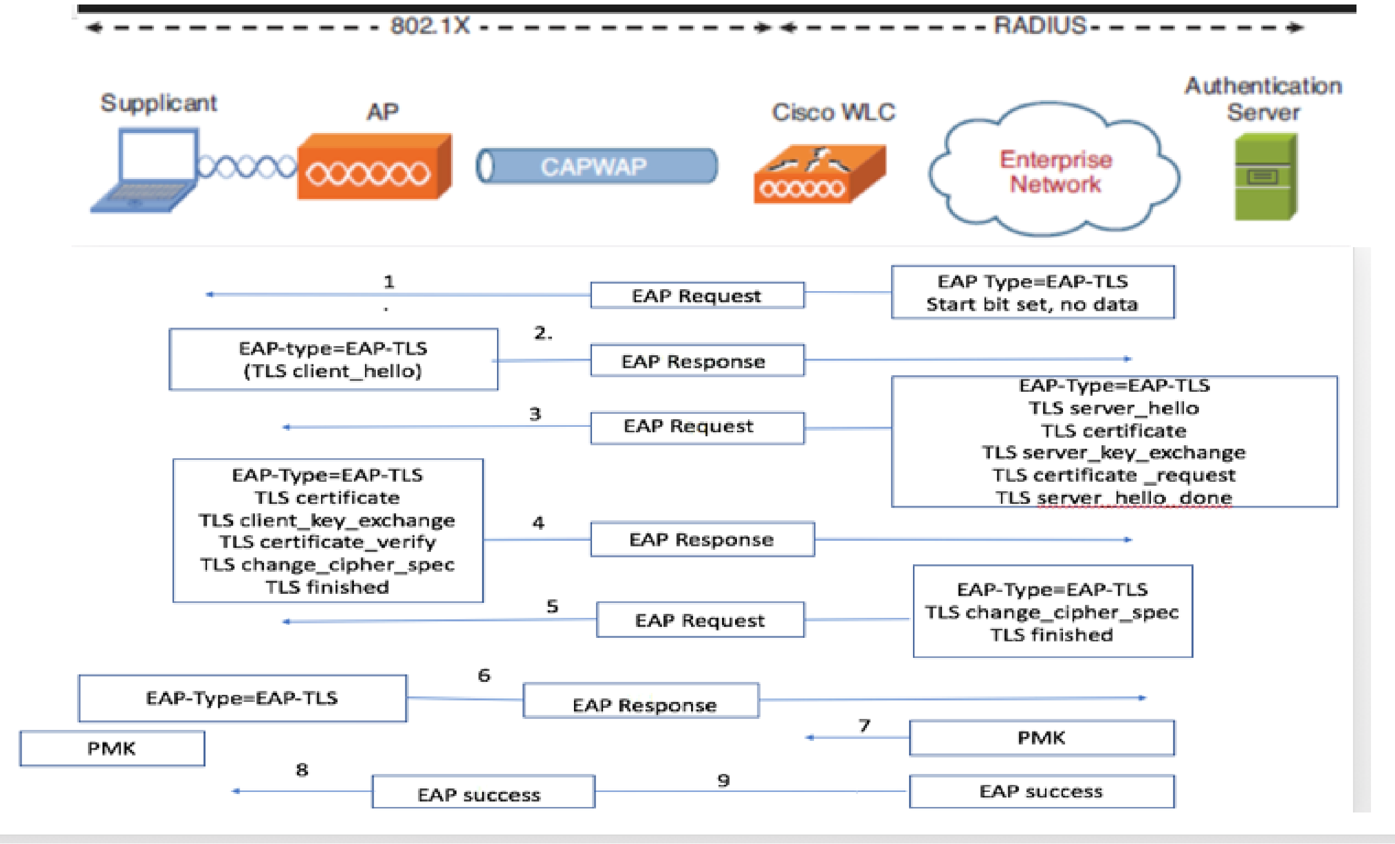
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- WLC 5508 バージョン 8.5
- Identity Services Engine（ISE）バージョン 2.1

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


802.1X
RADIUS
Supplicant
AP
CAPWAP
Cisco WLC
Enterprise Network
Authentication Server
1
EAP Request
EAP Type=EAP-TLS Start bit set, no data
2.
EAP-type=EAP-TLS (TLS client_hello)
EAP Response
3
EAP Request
EAP-Type=EAP-TLS TLS server_hello TLS certificate TLS server_key_exchange TLS certificate _request TLS server_hello_done
EAP-Type=EAP-TLS TLS certificate TLS client_key_exchange TLS certificate_verify TLS change_cipher_spec TLS finished
4
EAP Response
5
EAP Request
EAP-Type=EAP-TLS TLS change_cipher_spec TLS finished
6
EAP-Type=EAP-TLS
EAP Response
PMK
7
PMK
8
EAP success
9
EAP success

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。

2. AP は、クライアントがこの時点でデータを送信することを許可せず、認証要求を送信します。

3. サプリカントが、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。

4. 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。

5. ピアが、EAP 応答を認証サーバに返します。これには、「client_hello」ハンドシェイクメッセージ（NULL に設定された暗号）が含まれています。

6. 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.
```

7. クライアントが、次を含む EAP 応答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
```

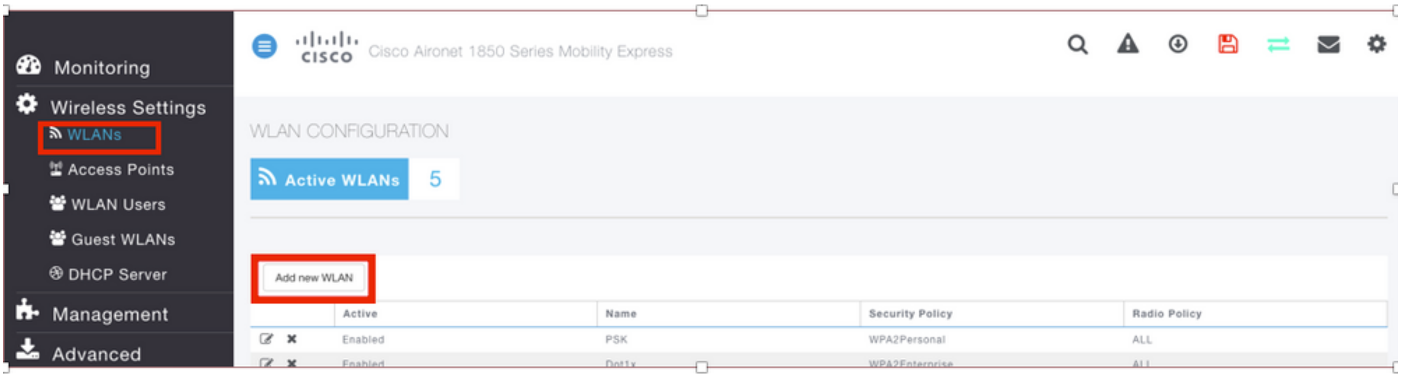
8. クライアントが正常に認証されると、RADIUS サーバが、「change_cipher_spec」およびハンドシェイク終了メッセージを含むアクセスチャレンジで応答します。これを受信したクライアントは、ハッシュを確認して RADIUS サーバを認証します。新しい暗号キーは、TLSハンドシェイク中にシークレットから動的に取得されます。

9. 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

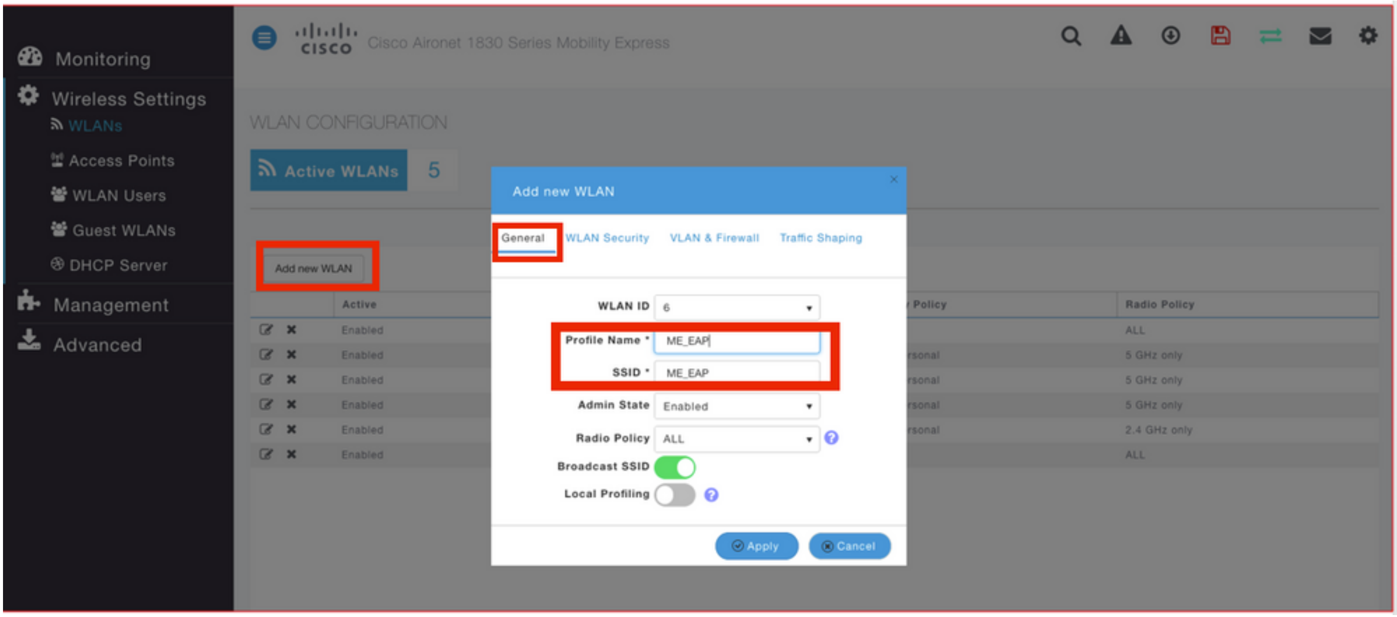
Cisco Mobility Express

ステップ1：最初のステップは、Mobility ExpressでWLANを作成することです。WLANを作成するには、図に示すように、**[WLAN] > [Add new WLAN]**に移動します。



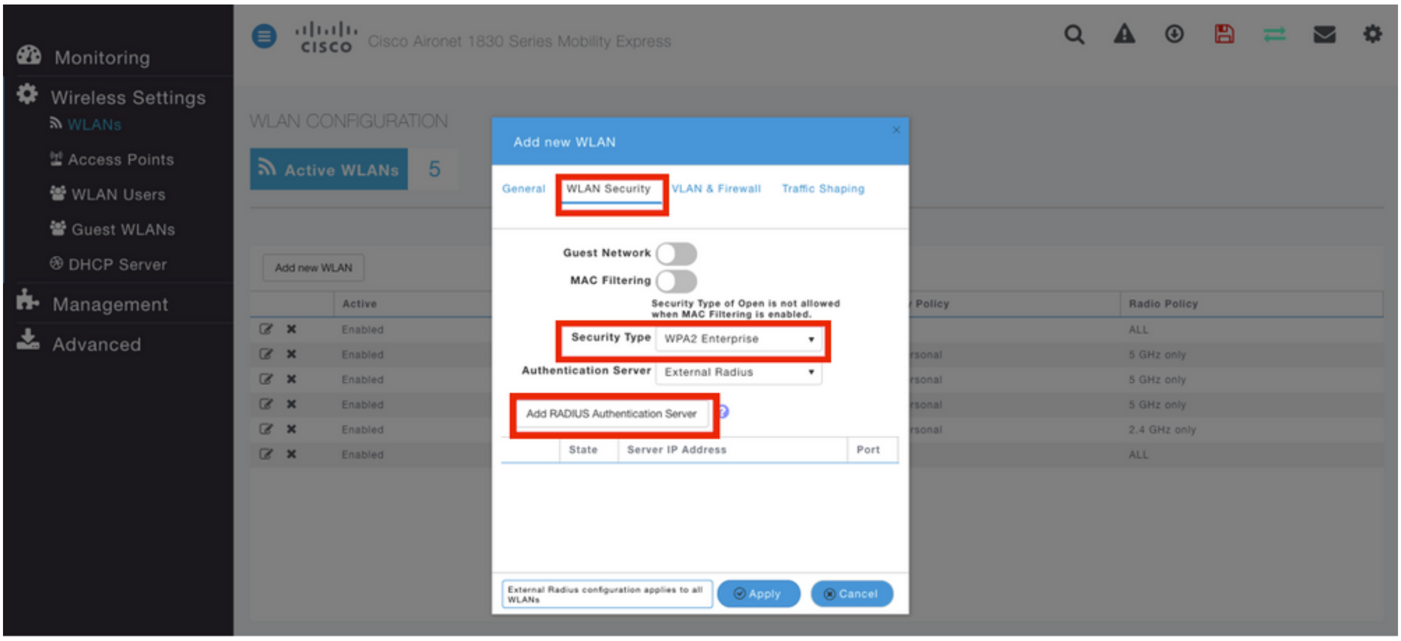
	Active	Name	Security Policy	Radio Policy
✎ ✖	Enabled	PSK	WPA2Personal	ALL
✎ ✖	Enabled	Dot1x	WPA2Enterprise	ALL

ステップ2:[Add new WLAN]をクリックすると、新しいポップアップウィンドウ**が表示されます。**プロファイル名を作成するには、図に示すように**[Add new WLAN] > [General]**に移動します。



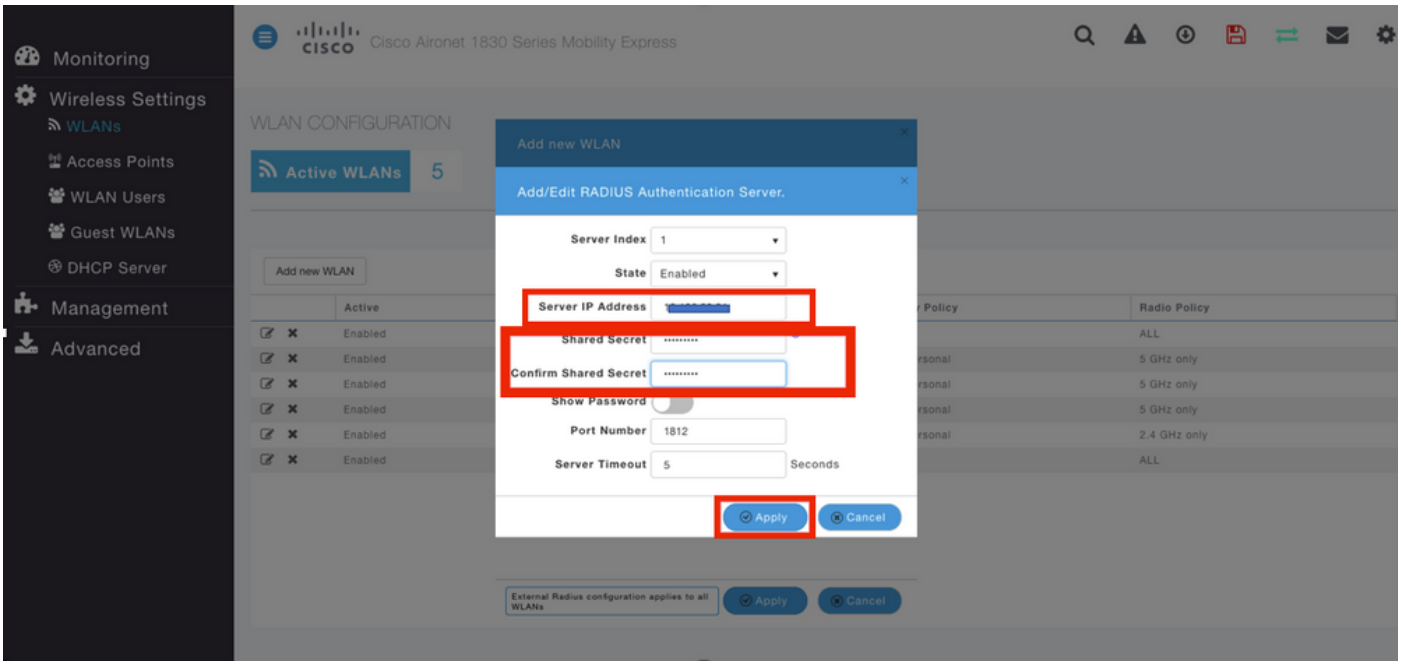
WLAN ID: 6
Profile Name *: ME_EAP
SSID *: ME_EAP
Admin State: Enabled
Radio Policy: ALL
Broadcast SSID: on
Local Profiling: off

ステップ3：図に示すように、802.1xの認証タイプをWPA Enterpriseに設定し、**[Add new WLAN] > [WLAN Security]でRADIUSサーバを設定します。**



Guest Network: off
MAC Filtering: off
Security Type of Open is not allowed when MAC Filtering is enabled.
Security Type: WPA2 Enterprise
Authentication Server: External Radius
External Radius configuration applies to all WLANs

ステップ4:**Add RADIUS Authentication Server**をクリックし、ISEで設定されている内容と正確に一致する必要があるRADIUSサーバと共有秘密のIPアドレスを指定し、図に示すように**Applyをクリックします。**



Add new WLAN

Add/Edit RADIUS Authentication Server.

Server Index: 1
State: Enabled
Server IP Address: [redacted]
Shared Secret: ••••••••••
Confirm Shared Secret: ••••••••••
Show Password
Port Number: 1812
Server Timeout: 5 Seconds

	Active	Policy	Radio Policy
	Enabled		ALL
	Enabled	rsonal	5 GHz only
	Enabled	rsonal	5 GHz only
	Enabled	rsonal	5 GHz only
	Enabled	rsonal	2.4 GHz only
	Enabled		ALL

External Radius configuration applies to all WLANs

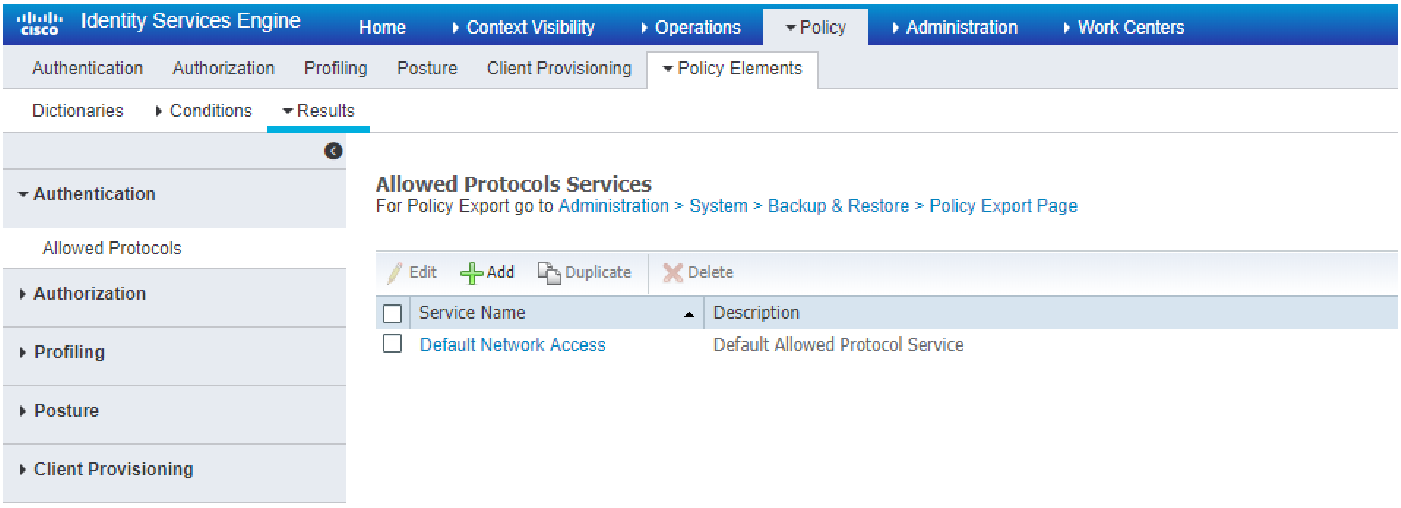
ISEとCisco Mobility Express

EAP-TLS 設定

ポリシーを作成するには、ポリシーで使用する許可された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認証でほとんどの EAP タイプが許可されますが、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、これは適していない可能性があります。

ステップ1：図に示すように、**[Policy] > [Policy Elements] > [Results] > [Authentication] > [Allowed Protocols]に移動**し、[Add]をクリックします。

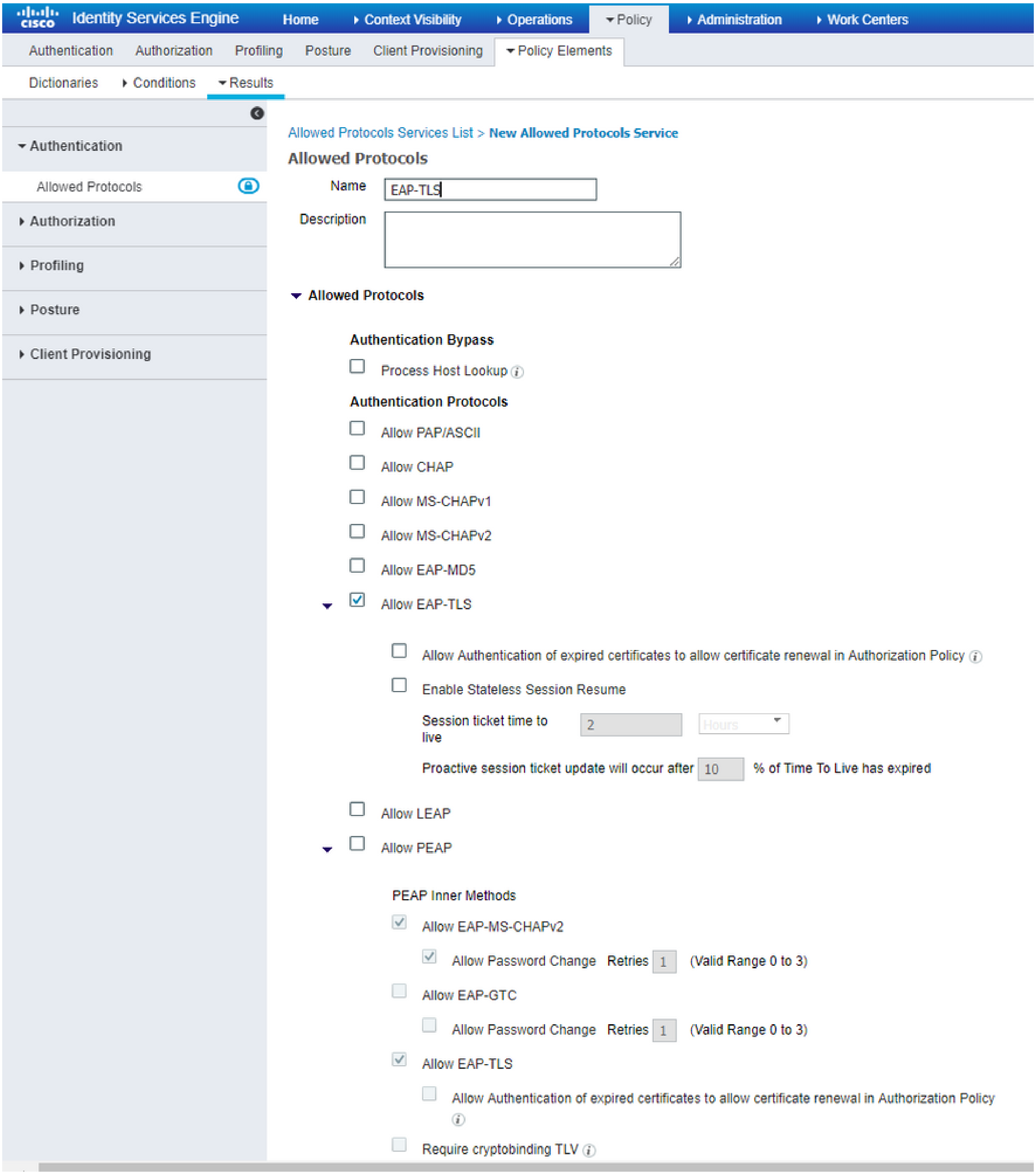


Allowed Protocols Services

For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

	Service Name	Description
□	Default Network Access	Default Allowed Protocol Service

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。



Allowed Protocols Services List > New Allowed Protocols Service

Allowed Protocols

Name: EAP-TLS

Description:

Allowed Protocols

Authentication Bypass

☐ Process Host Lookup

Authentication Protocols

☐ Allow PAP/ASCII

☐ Allow CHAP

☐ Allow MS-CHAPv1

☐ Allow MS-CHAPv2

☐ Allow EAP-MD5

☑ Allow EAP-TLS

☐ Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy

☐ Enable Stateless Session Resume

Session ticket time to live: 2 Hours

Proactive session ticket update will occur after 10 % of Time To Live has expired

☐ Allow LEAP

☐ Allow PEAP

PEAP Inner Methods

☑ Allow EAP-MS-CHAPv2

☑ Allow Password Change Retries 1 (Valid Range 0 to 3)

☐ Allow EAP-GTC

☐ Allow Password Change Retries 1 (Valid Range 0 to 3)

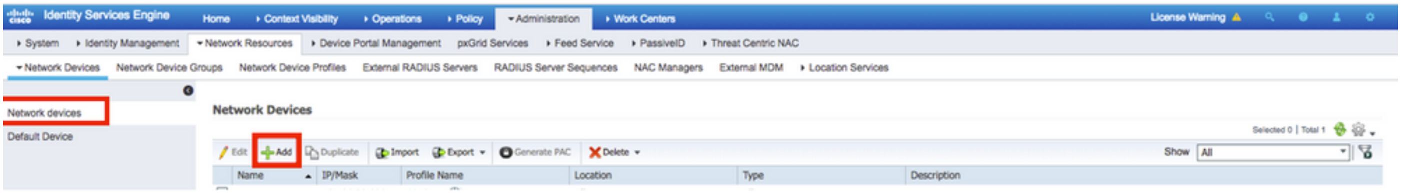
☑ Allow EAP-TLS

☐ Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy

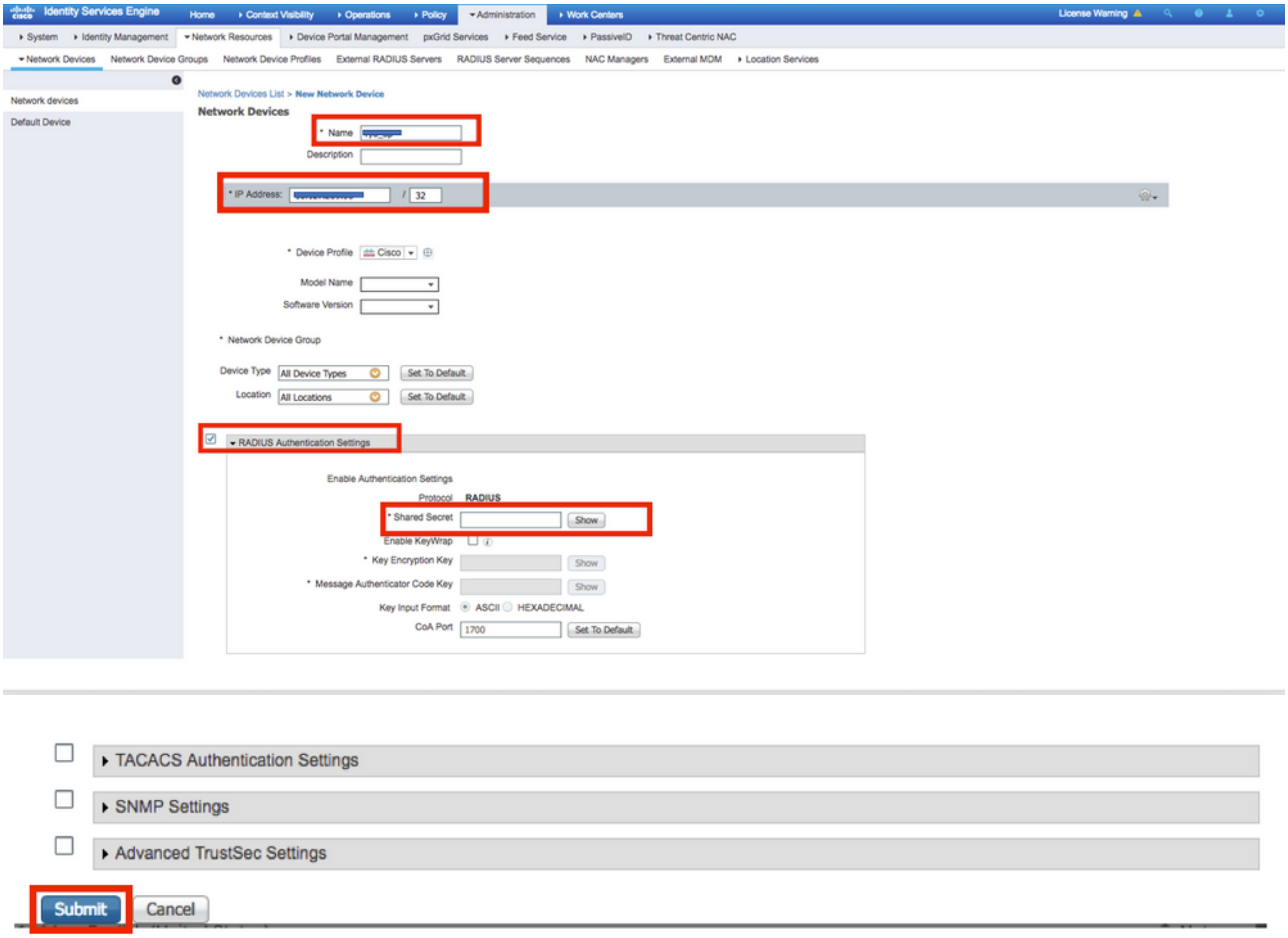
☐ Require cryptobinding TLV

ISEでのMobility Express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： 図のように、情報を入力します。



Network Devices

* Name [redacted]

Description

* IP Address: [redacted] / 32

* Device Profile Cisco

Model Name

Software Version

* Network Device Group

Device Type All Device Types Set To Default

Location All Locations Set To Default

☑ RADIUS Authentication Settings

Enable Authentication Settings

Protocol RADIUS

* Shared Secret Show

Enable KeyWrap □

* Key Encryption Key Show

* Message Authenticator Code Key Show

Key Input Format ● ASCII ○ HEXADECIMAL

CoA Port 1700 Set To Default

□ TACACS Authentication Settings

□ SNMP Settings

□ Advanced TrustSec Settings

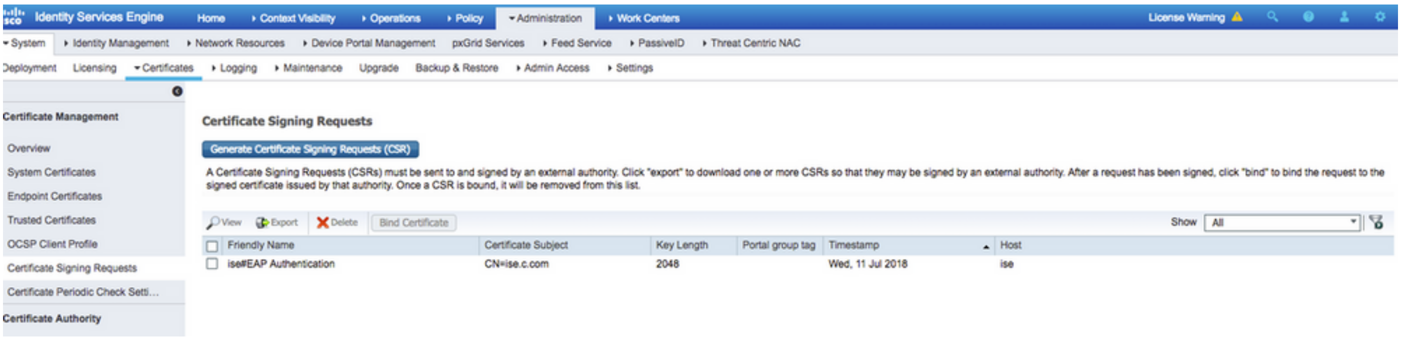
Submit Cancel

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。そのためには、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。

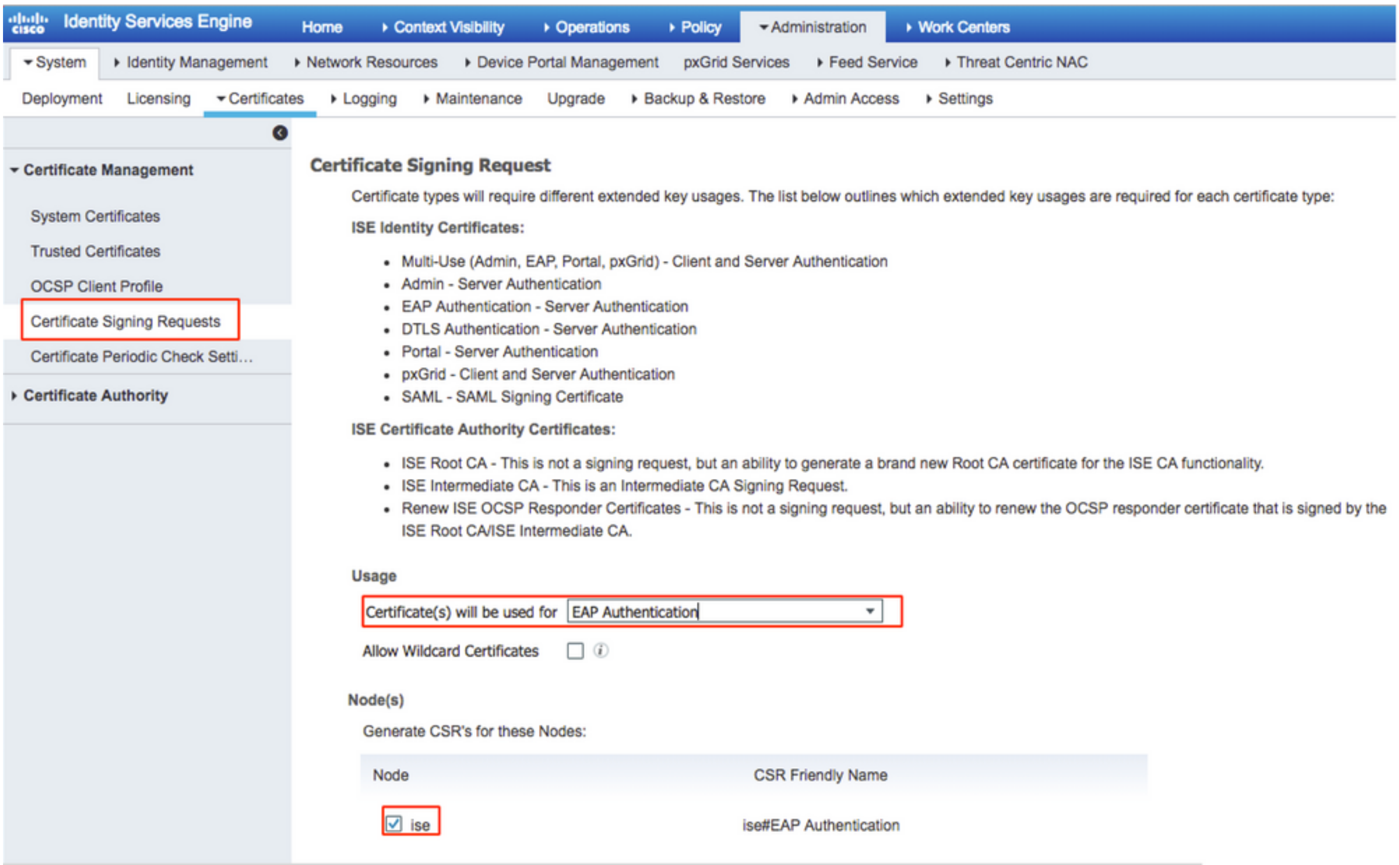


Certificate Signing Requests

A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click "export" to download one or more CSRs so that they may be signed by an external authority. After a request has been signed, click "bind" to bind the request to the signed certificate issued by that authority. Once a CSR is bound, it will be removed from this list.

	Friendly Name	Certificate Subject	Key Length	Portal group tag	Timestamp	Host
□	ise#EAP Authentication	CN=ise.c.com	2048		Wed, 11 Jul 2018	ise

ステップ 3： CSR を生成するには、図のように、[用途（Usage）] に移動し、[次の目的で証明書を使用（Certificate(s) will be used for）] ドロップダウンオプションから [EAP認証（EAP Authentication）] を選択します。



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 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

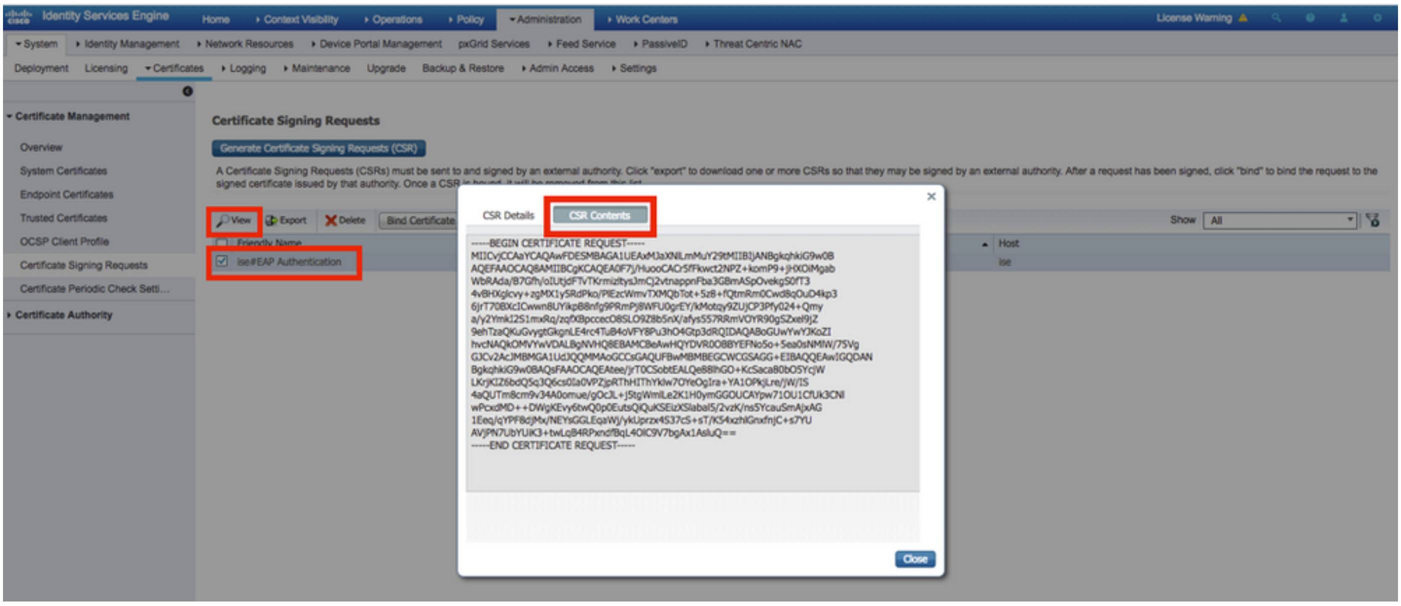
Allow Wildcard Certificates ☐

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
☑ ise	ise#EAP Authentication

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
。



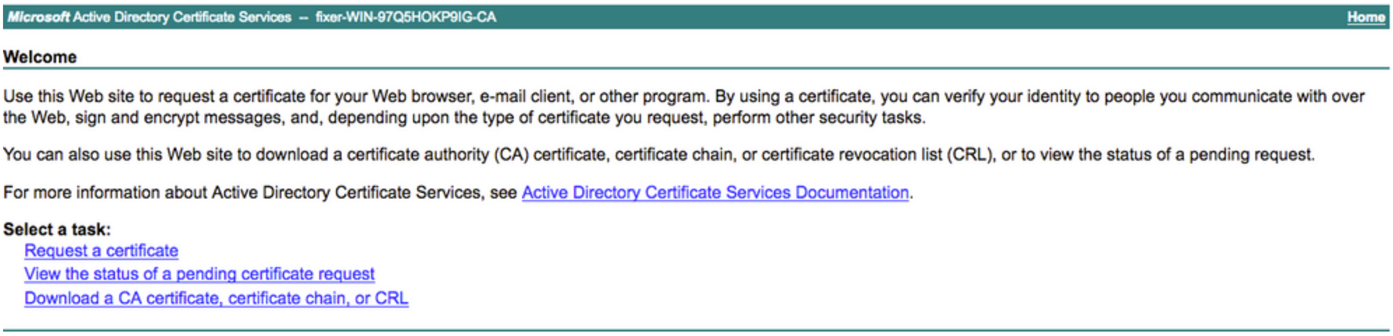
Certificate Signing Requests

A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click "export" to download one or more CSRs so that they may be signed by an external authority. After a request has been signed, click "bind" to bind the request to the signed certificate issued by that authority. Once a CSR is bound, it will be removed from this list.

	Friendly Name	Host
☑	ise#EAP Authentication	ise

```
-----BEGIN CERTIFICATE REQUEST-----
MIICvjCCAaYCAQAwFDESMBAGA1UEAxMJaXNlLmMuY29tMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEA0F7j/HuooCACr5fFkwct2NPZ+komP9+jHXOiMgab
WbRAda/B7Gfh/oIUtjdFTvTKrmizltysJmCj2vtnappnFba3GBmASpOvekgS0fT3
4vBHXglcvy+zgMX1y5RdPko/PlEzcWmvTXMQbTot+5z8+fQtmRm0Cwd8qOuD4kp3
6jrT70BXcICwwn8UYikpB8nfg9PRmPj8WFU0grEY/kMotqy9ZUjCP3Pfy024+Qmy
a/y2YmkI2S1mxRq/zqfXBpccecO8SLO9Z8b5nX/afys557RRmVOYR90gSZxel9jZ
9ehTzaQKuGvygtGkgnLE4rc4TuB4oVFY8Pu3hO4Gtp3dRQIDAQABoGUwYwYJKoZI
hvcNAQkOMVYwVDALBgNVHQ8EBAMCBeAwHQYDVR0OBBYEFNo5o+5ea0sNMIW/75Vg
GJCv2AcJMBMGA1UdJQQMMAoGCCsGAQUFBwMBMBEGCWCGSAGG+EIBAQQEAwIGQDAN
BgkqhkiG9w0BAQsFAAOCAQEAtee/jrT0CSobtEALQe8BlhGO+KcSaca80bO5YcjW
LKrjKIZ6bdQ5q3Q6cs0Ia0VPZjpRThHIThYklw7OYeOgIra+YA1OPkjLre/jW/IS
4aQUTm8cm9v34A0omue/gOcJL+j5tgWmlLe2K1H0ymGGOUCAYpw71OU1CfUk3CNI
wPcxdMD++DWgKEvy6twQ0p0EutsQiQuKSEizXSlabal5/2vzK/ns5YcauSmAjxAG
1Eeq/qYPF8djMx/NEYsGGLEqaWj/ykUprzx4S37cS+sT/K54xzhlGnxfnjC+s7YU
AVjPN7UbYUiK3+twLqB4RPxndfBqL40lC9V7bgAx1AsluQ==
-----END CERTIFICATE REQUEST-----
```

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



Microsoft Active Directory Certificate Services -- fixer-WIN-97Q5HOKP9IG-CA

Home

Welcome

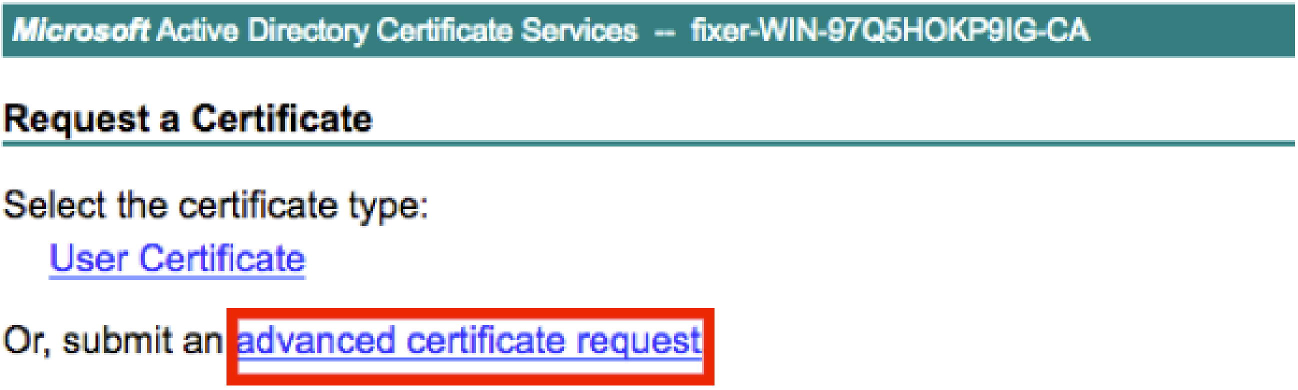
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

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

ステップ6：証明書を要求すると、ユーザ証明書と高度な証明書要求のオプションが表示さ**れ**、図に示すように**高度な証明書要求をクリ**ックします。



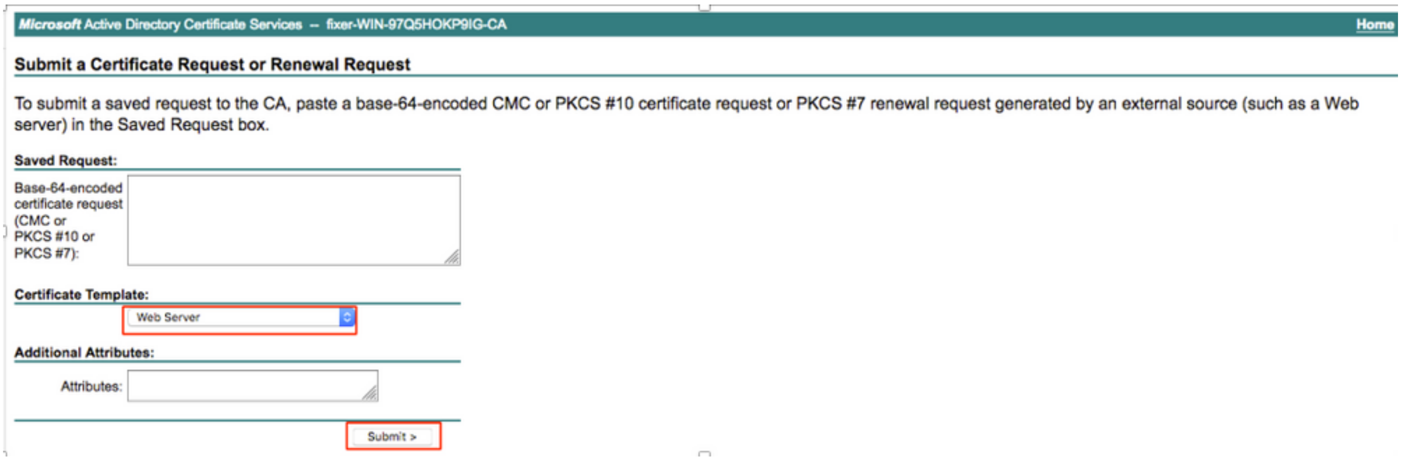
Microsoft Active Directory Certificate Services -- fixer-WIN-97Q5HOKP9IG-CA

Request a Certificate

Select the certificate type:
- User Certificate

Or, submit an advanced certificate request

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。[証明書テンプ**レート：]ドロップダ**ウンオプションから、**[Web Server]**を選択し、**[送信]**をクリックします（図を参照）。



Microsoft Active Directory Certificate Services -- fixer-WIN-97Q5HOKP9IG-CA

Home

Submit a Certificate Request or Renewal Request

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

Saved Request:

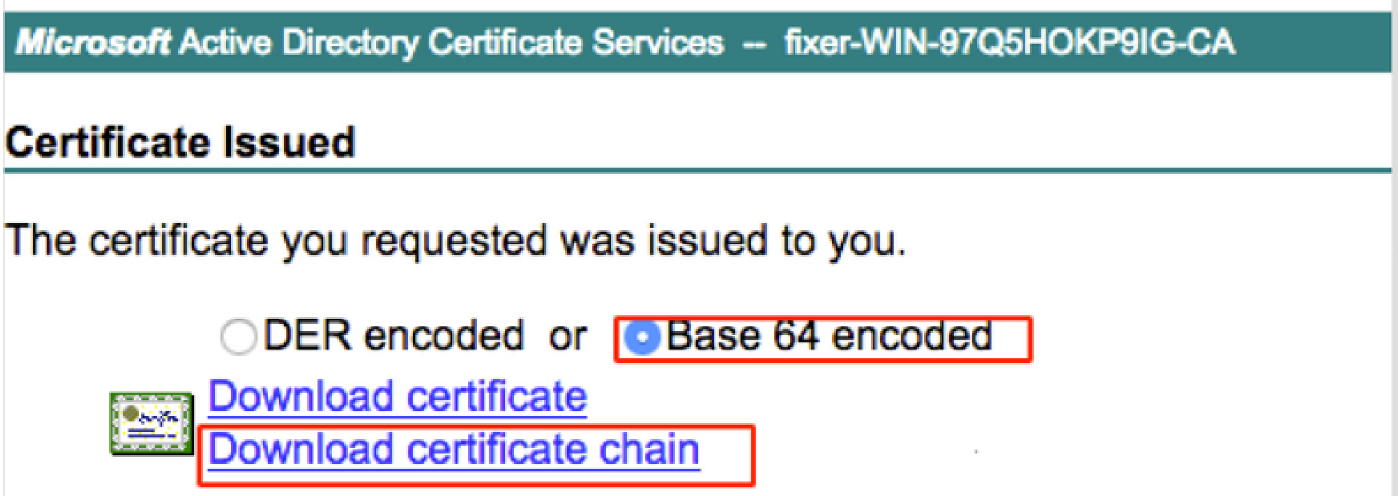
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

Certificate Template: Web Server

Additional Attributes:

Attributes:

ステップ8:[Submit]をクリックすると、証明書の種類を選択するオプションが表示され、**Base-64 encodedを選択**して、図に示すように**[Download certificate chain]**をクリックします。



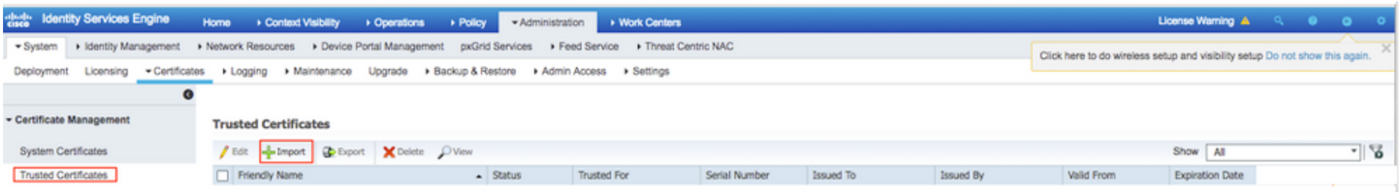
Microsoft Active Directory Certificate Services -- fixer-WIN-97Q5HOKP9IG-CA

Certificate Issued

The certificate you requested was issued to you.

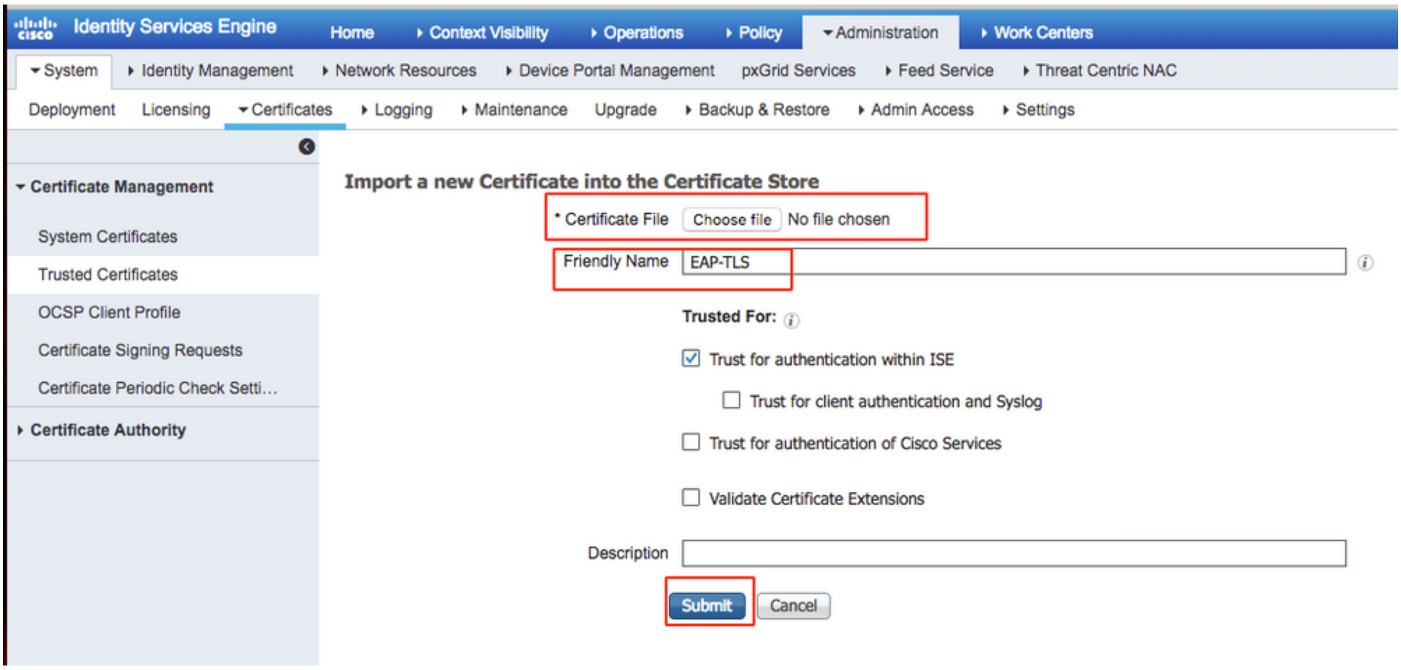
○ DER encoded or ● Base 64 encoded

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、ルート証明書と中間証明書の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。



Trusted Certificates

□ Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date



Import a new Certificate into the Certificate Store

* Certificate File Choose file No file chosen

Friendly Name EAP-TLS

Trusted For:

☑ Trust for authentication within ISE

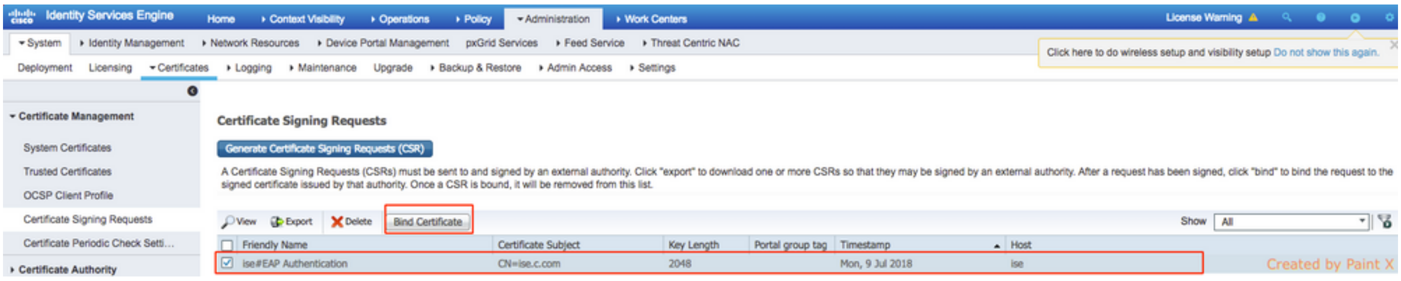
□ Trust for client authentication and Syslog

□ Trust for authentication of Cisco Services

□ Validate Certificate Extensions

Description

ステップ10:[Submit]をクリックすると、証明書が信頼できる証明書リストに追加されます。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。

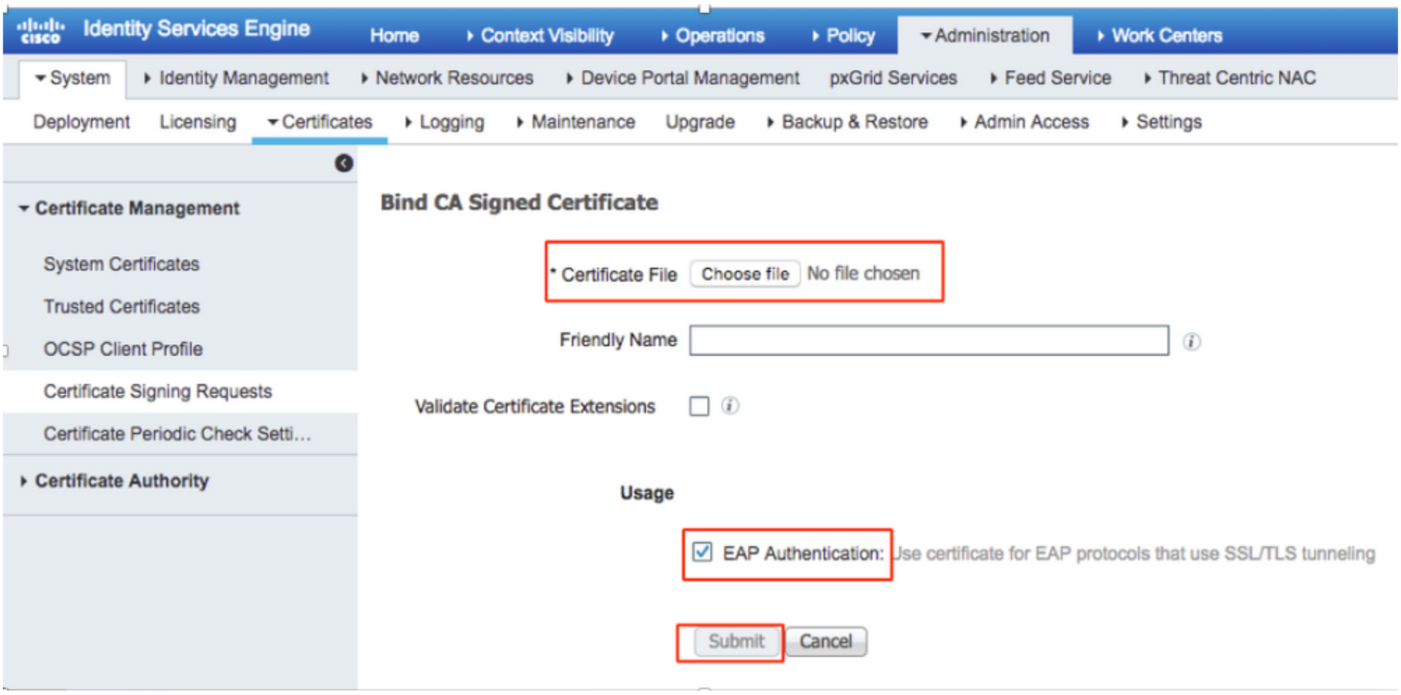


Certificate Signing Requests

A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click "export" to download one or more CSRs so that they may be signed by an external authority. After a request has been signed, click "bind" to bind the request to the signed certificate issued by that authority. Once a CSR is bound, it will be removed from this list.

□ Friendly Name	Certificate Subject	Key Length	Portal group tag	Timestamp	Host
☑ ise#EAP Authentication	CN=ise.c.com	2048		Mon, 9 Jul 2018	ise

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表示されます。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。



Bind CA Signed Certificate

* Certificate File Choose file No file chosen

Friendly Name

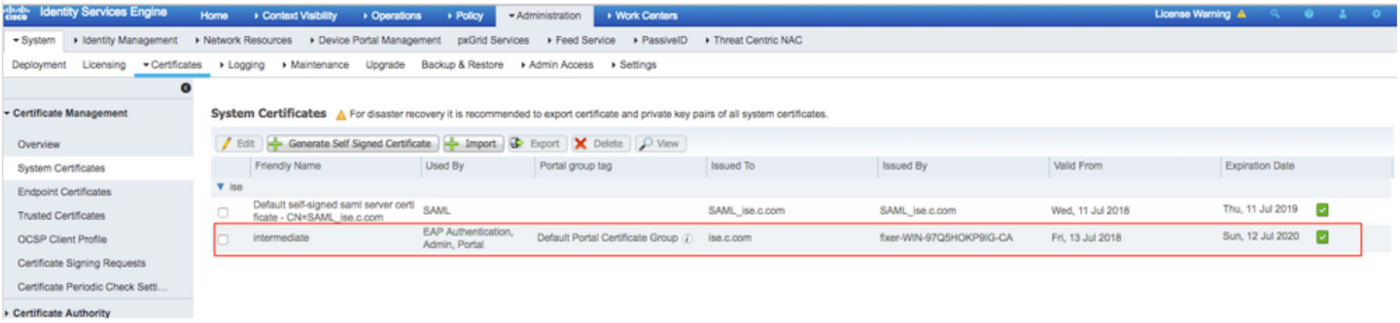
Validate Certificate Extensions □

Usage

☑ EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling

Submit Cancel

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。



System Certificates For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

	Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	
▼ ise								
□	Default self-signed saml server certificate - CN=SAML_ise.c.com	SAML		SAML_ise.c.com	SAML_ise.c.com	Wed, 11 Jul 2018	Thu, 11 Jul 2019	✓
□	intermediate	EAP Authentication, Admin, Portal	Default Portal Certificate Group	ise.c.com	fixer-WIN-97Q5HOKP9IG-CA	Fri, 13 Jul 2018	Sun, 12 Jul 2020	✓

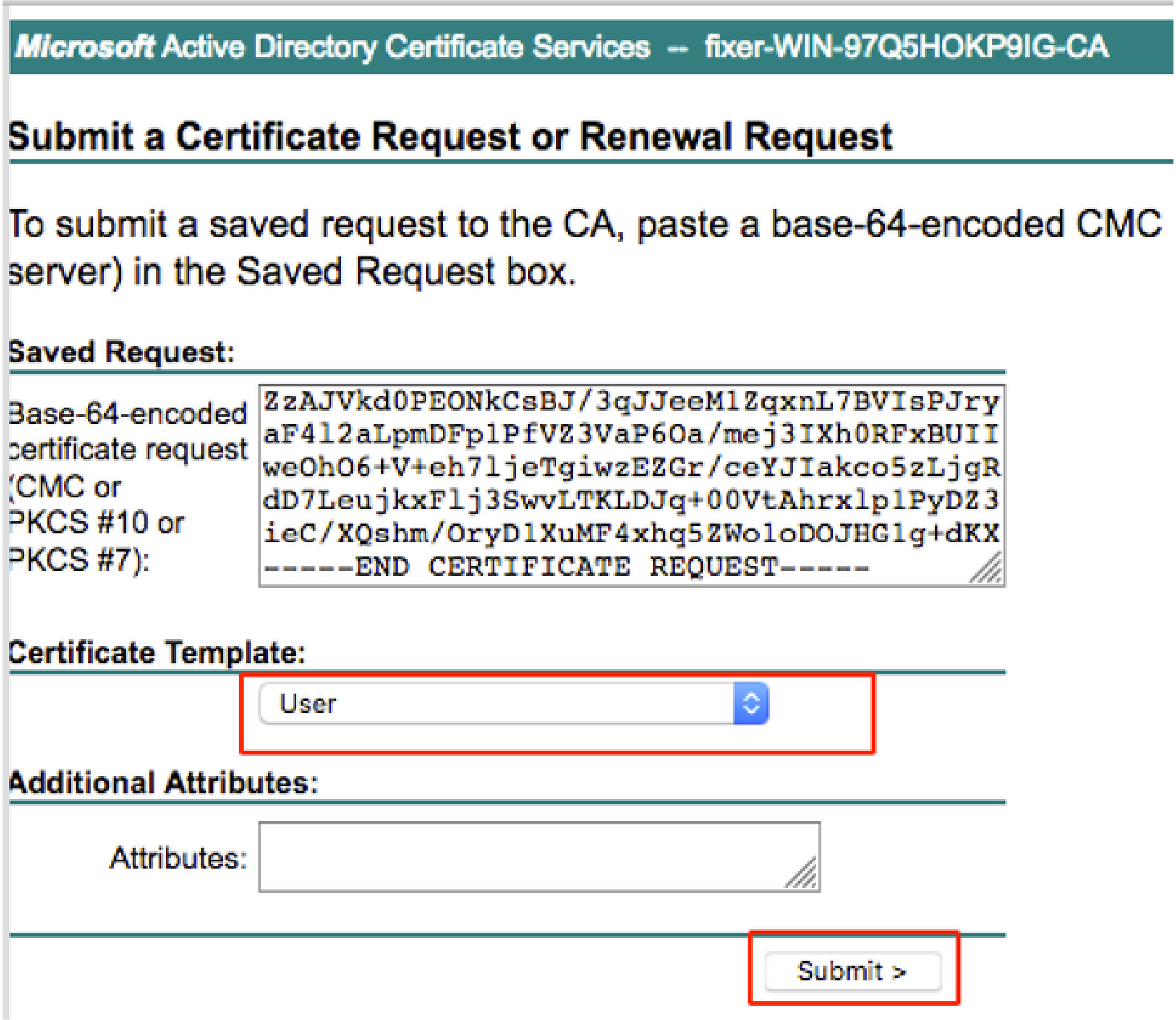
EAP-TLS 用のクライアント

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。



Microsoft Active Directory Certificate Services -- fixer-WIN-97Q5HOKP9IG-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC server) in the Saved Request box.

Saved Request:

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

```
ZzAJVkd0PEONkCsBJ/3qJJeeM1ZqxnL7BVIsPJry
aF412aLpmDFp1PfVZ3VaP6Oa/mej3IXh0RFxBUII
weOhO6+V+eh71jeTgiwzEZGr/ceYJIakco5zLjgR
dD7LeujkxF1j3SwvLTKLDJq+00VtAhrx1p1PyDZ3
ieC/XQshm/OryD1XuMF4xhq5ZWoloDOJHG1g+dKX
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

User

Additional Attributes:

Attributes:

ステップ3：次に、サーバに対して以前に行った**証明書チェーン**のダウンロードをクリックします。

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

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. [コンピュータア**カウント]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。

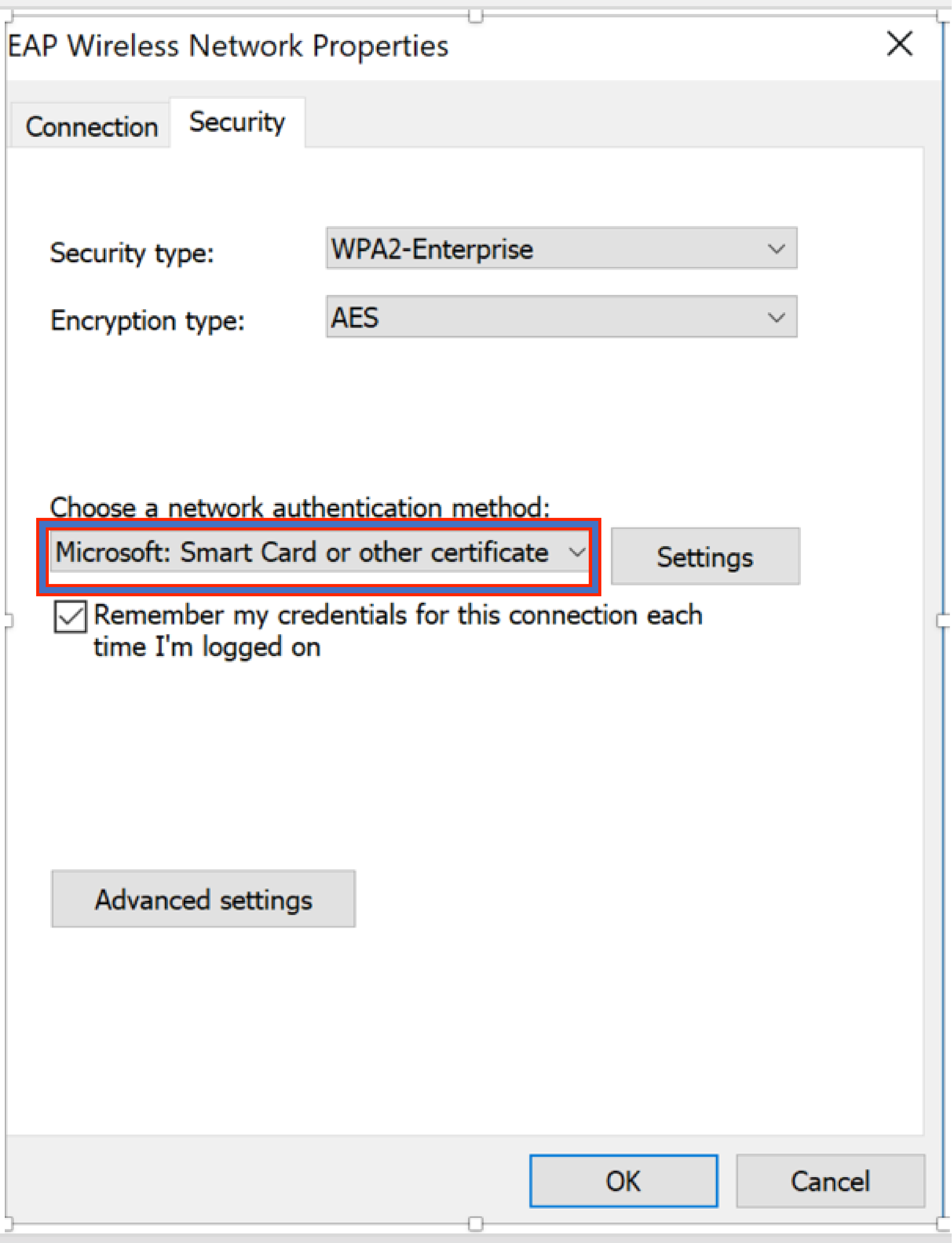
9. [next] をクリックします。
10. [Browse] をクリックします。
11. インポートする .cer、.crt、または .pfx ファイルを選択します。
12. [Open] をクリックします。
13. [next] をクリックします。
14. [証明書の種類に基づいて、自動的に証明書ストアを選択する（Automatically select the certificate store based on the type of certificate）] を選択します。
15. [完了（Finish）]、[OK] の順にクリックしてます。

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：代わりにEAP-TLSを使用するために、Protected Extensible Authentication Protocol(PEAP)用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：**図に示すように、スマートカードま**たは他の証明書**をクリック**し、[OK]をクリックします。



EAP Wireless Network Properties

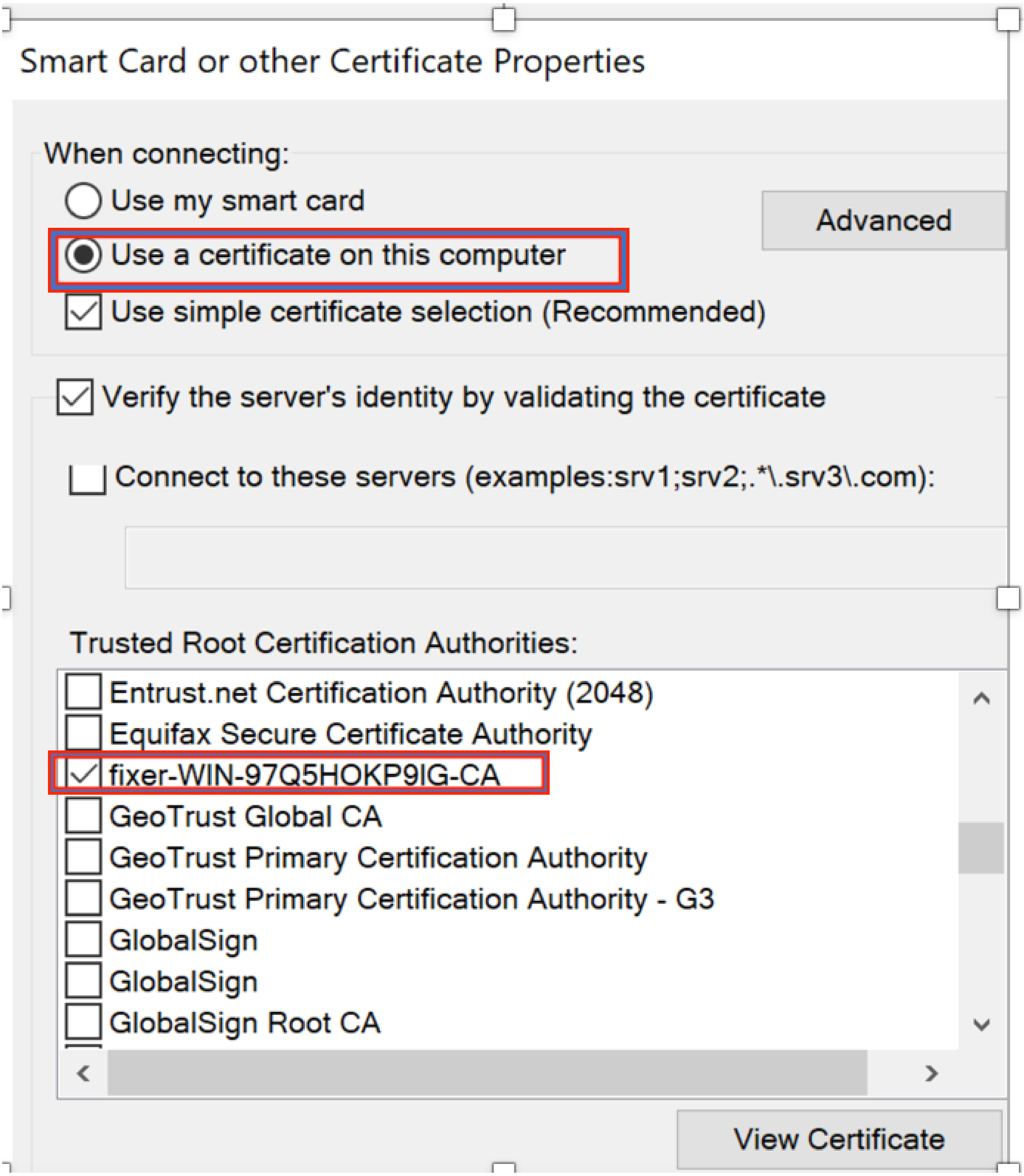
Security type: WPA2-Enterprise

Encryption type: AES

Choose a network authentication method:
Microsoft: Smart Card or other certificate

☑ Remember my credentials for this connection each time I'm logged on

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。



Smart Card or other Certificate Properties

When connecting:

○ Use my smart card

● Use a certificate on this computer

☑ Use simple certificate selection (Recommended)

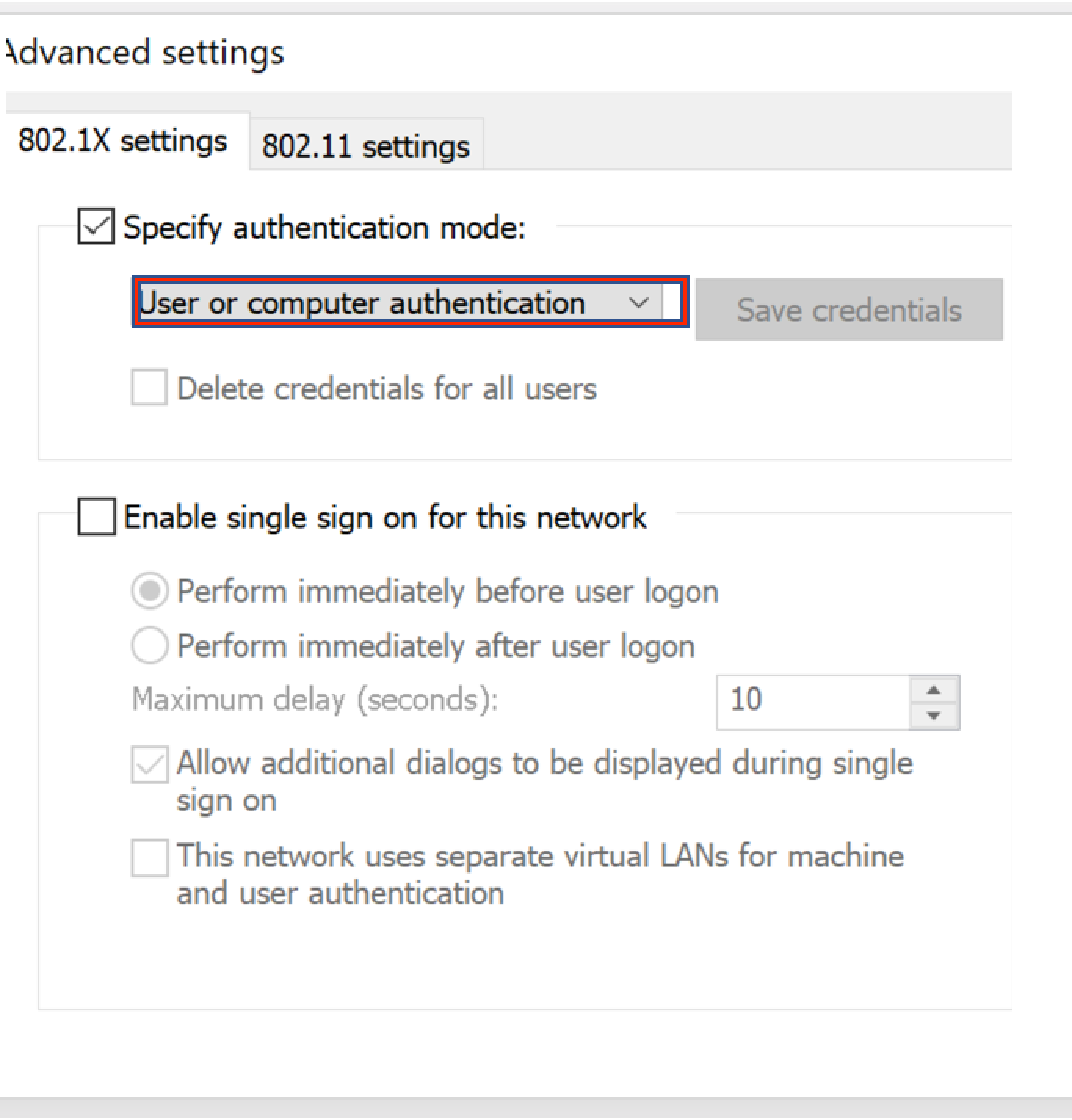
☑ Verify the server's identity by validating the certificate

□ Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):

Trusted Root Certification Authorities:

□ Entrust.net Certification Authority (2048)
□ Equifax Secure Certificate Authority
☑ fixer-WIN-97Q5HOKP9IG-CA
□ GeoTrust Global CA
□ GeoTrust Primary Certification Authority
□ GeoTrust Primary Certification Authority - G3
□ GlobalSign
□ GlobalSign
□ GlobalSign Root CA

ステップ4：図に示すように、[**Advanced Settings**]をクリックし、[802.1x settings]タブから[User or computer authentication]を選択します。



Advanced settings

802.1X settings | 802.11 settings

☑ Specify authentication mode:

User or computer authentication

□ Delete credentials for all users

□ Enable single sign on for this network

● Perform immediately before user logon

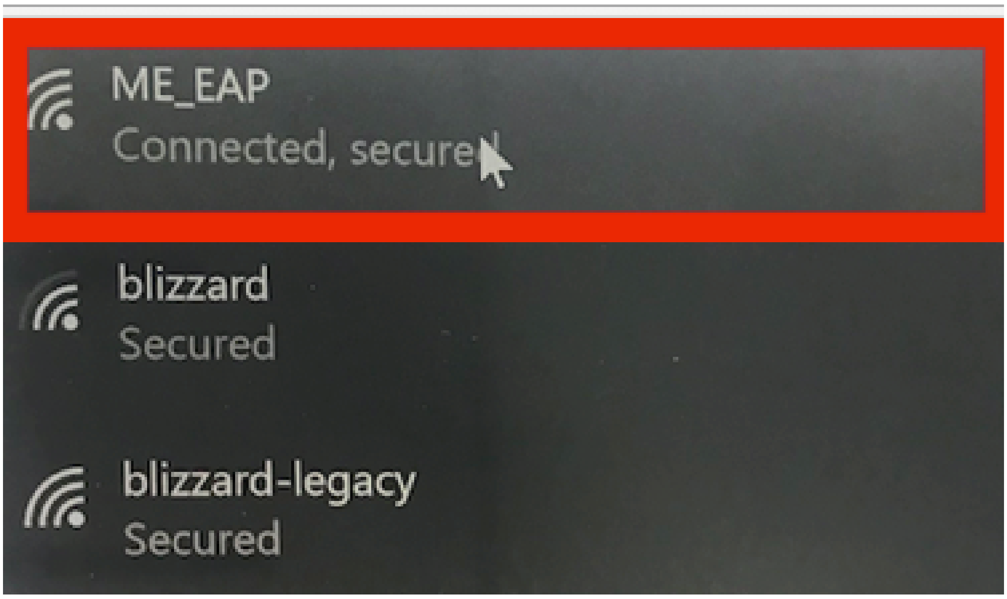
○ Perform immediately after user logon

Maximum delay (seconds): 10

☑ Allow additional dialogs to be displayed during single sign on

□ This network uses separate virtual LANs for machine and user authentication

ステップ5：次に、ワイヤレスネットワークに接続し直し、正しいプロファイル（この例ではEAP）を選択し、Connectを選択します。図のように、ワイヤレスネットワークに接続されます。



ME_EAP
Connected, secured

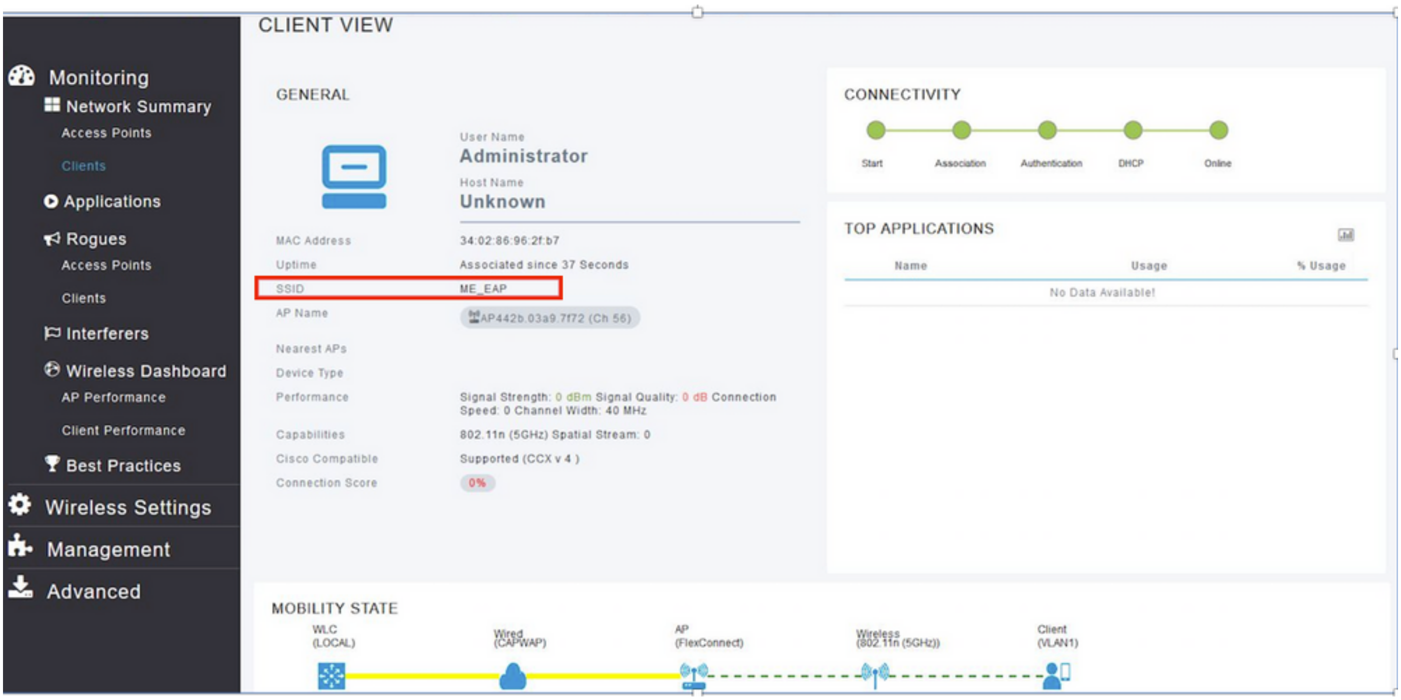
blizzard
Secured

blizzard-legacy
Secured

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。

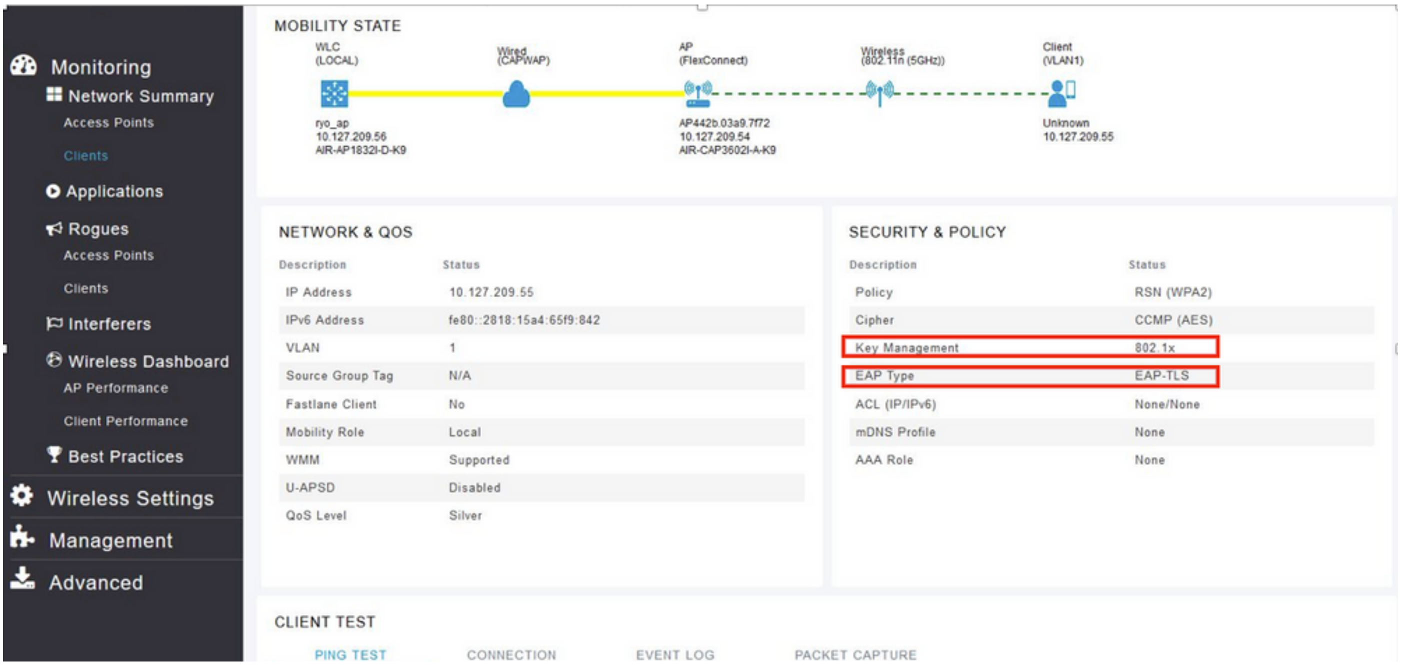
ステップ1：クライアントのEAP-TypeはEAP-TLSである必要があります。これは、クライアントがEAP-TLSを使用して認証を完了し、IPアドレスを取得し、図に示すようにトラフィックを渡す準備ができていることを意味します。



User Name
Administrator
Host Name
Unknown

MAC Address 34:02:86:96:2f:b7
Uptime Associated since 37 Seconds
SSID ME_EAP
AP Name AP442b.03a9.7f72 (Ch 56)
Nearest APs
Device Type
Performance Signal Strength: 0 dBm Signal Quality: 0 dB Connection Speed: 0 Channel Width: 40 MHz
Capabilities 802.11n (5GHz) Spatial Stream: 0
Cisco Compatible Supported (CCX v 4)
Connection Score 0%

No Data Available!



NETWORK & QOS

Description	Status
IP Address	10.127.209.55
IPv6 Address	fe80::2818:15a4:65f9:842
VLAN	1
Source Group Tag	N/A
Fastlane Client	No
Mobility Role	Local
WMM	Supported
U-APSD	Disabled
QoS Level	Silver

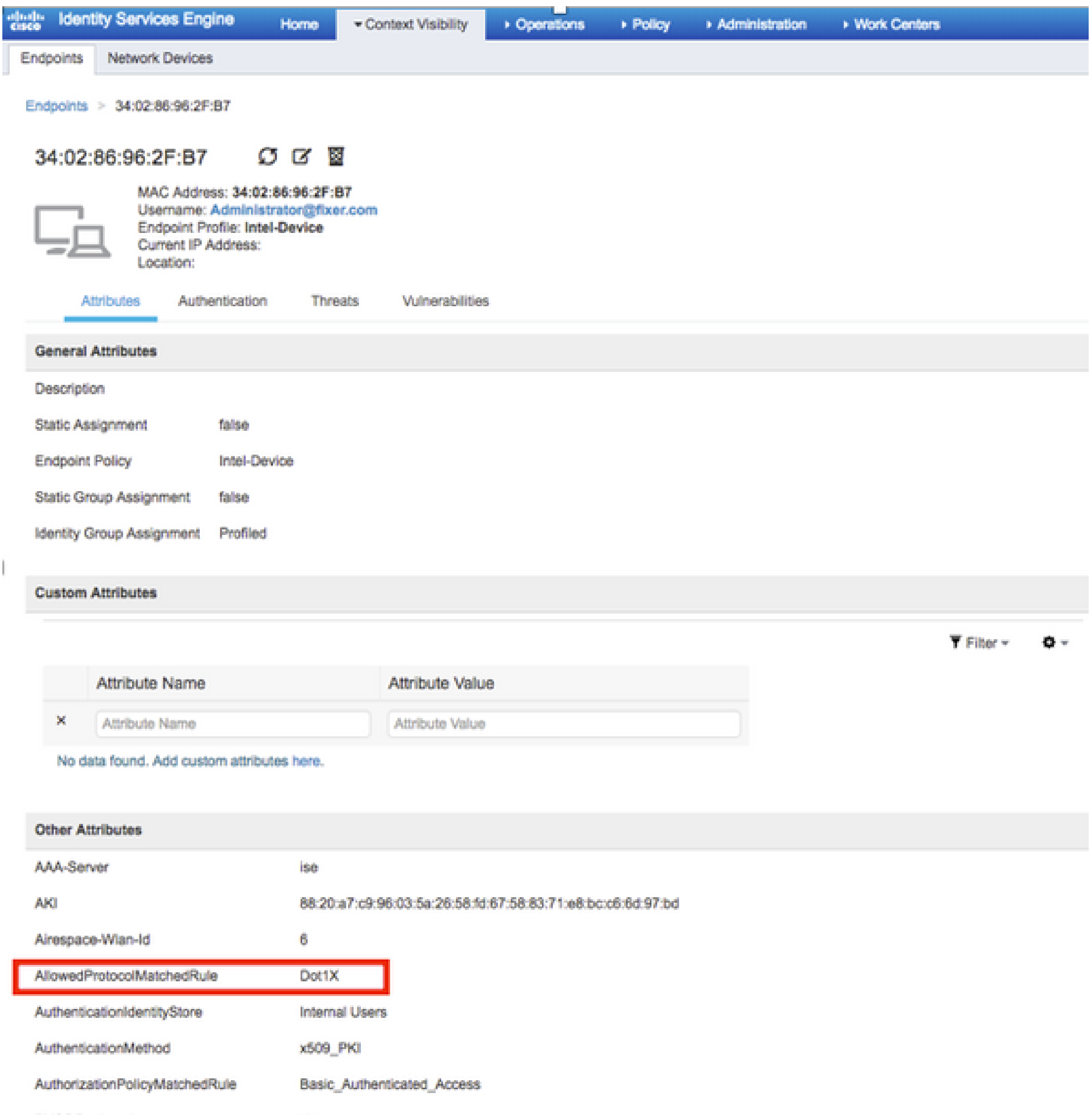
SECURITY & POLICY

Description	Status
Policy	RSN (WPA2)
Cipher	CCMP (AES)
Key Management	802.1x
EAP Type	EAP-TLS
ACL (IP/IPv6)	None/None
mDNS Profile	None
AAA Role	None

ステップ2：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) > show client detail 34:02:86:96:2f:b7
Client MAC Address............................... 34:02:86:96:2f:b7
Client Username ................................. Administrator
AP MAC Address................................... c8:f9:f9:83:47:b0
AP Name.......................................... AP442b.03a9.7f72
AP radio slot Id................................. 1
Client State..................................... Associated
Client User Group................................ Administrator
Client NAC OOB State............................. Access
Wireless LAN Id.................................. 6
Wireless LAN Network Name (SSID)................. ME_EAP
Wireless LAN Profile Name........................ ME_EAP
Hotspot (802.11u)................................ Not Supported
BSSID............................................ c8:f9:f9:83:47:ba
Connected For ................................... 18 secs
Channel.......................................... 56
IP Address....................................... 10.127.209.55
Gateway Address.................................. 10.127.209.49
Netmask.......................................... 255.255.255.240
IPv6 Address..................................... fe80::2818:15a4:65f9:842
--More-- or (q)uit
Security Policy Completed........................ Yes
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3：図に示すように、ISEで[Context Visbility] > **[End Points] > [Attributes]**に移動します。



34:02:86:96:2F:B7

MAC Address: **34:02:86:96:2F:B7**
Username: **Administrator@fixer.com**
Endpoint Profile: **Intel-Device**
Current IP Address:
Location:

General Attributes

Description	
Static Assignment	false
Endpoint Policy	Intel-Device
Static Group Assignment	false
Identity Group Assignment	Profiled

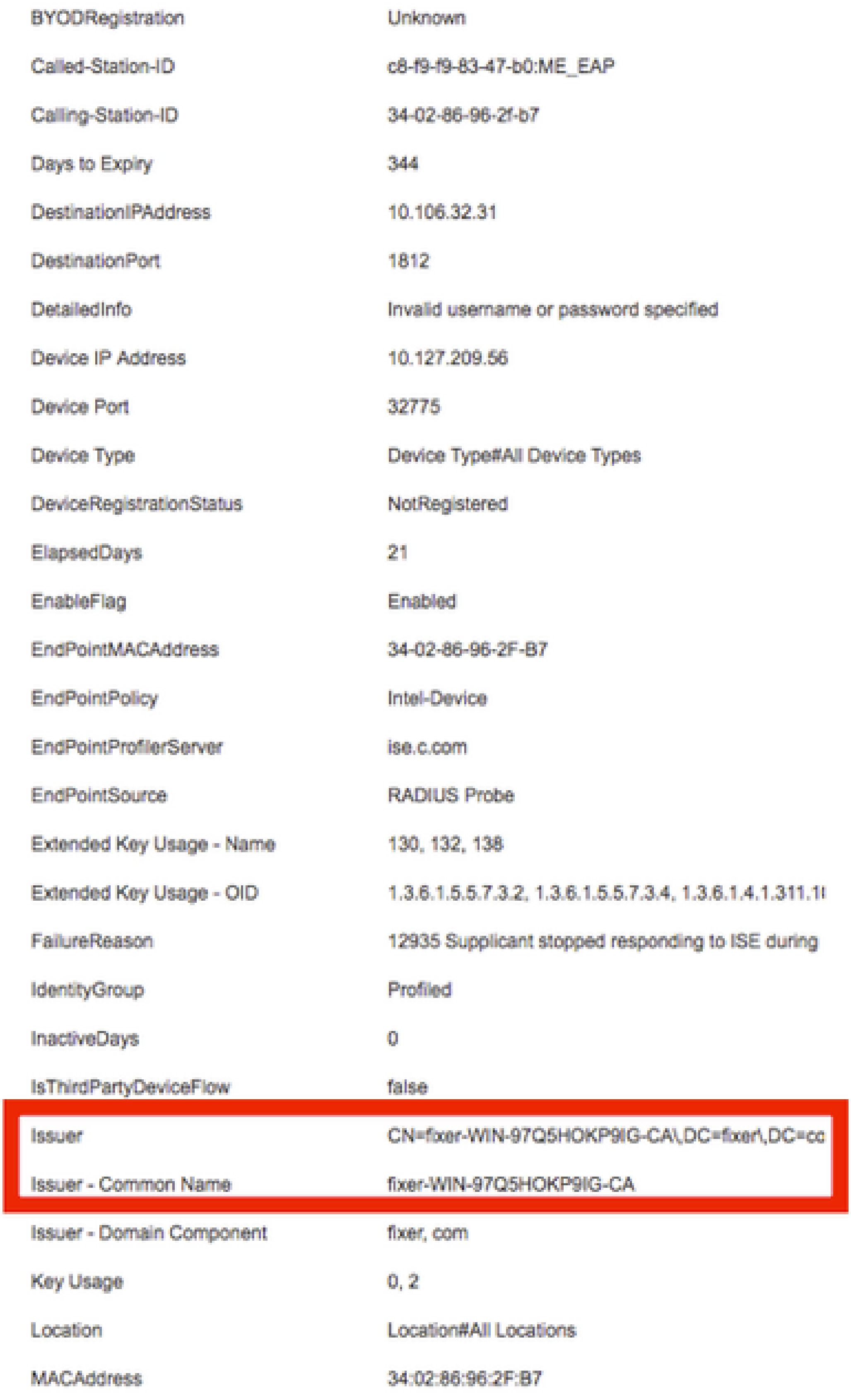
Custom Attributes

	Attribute Name	Attribute Value
×		

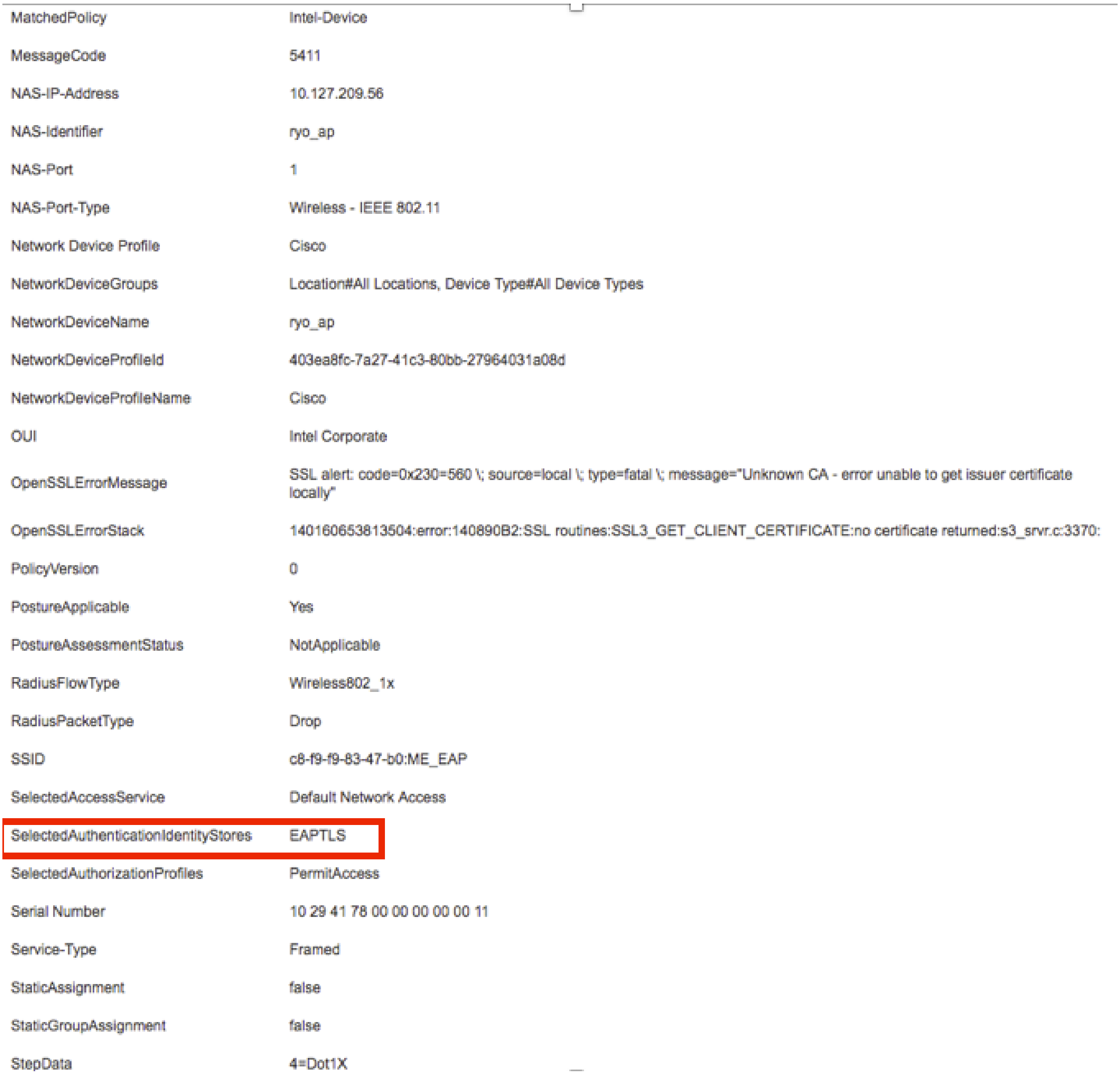
No data found. Add custom attributes here.

Other Attributes

AAA-Server	ise
AKI	88:20:a7:c9:96:03:5a:26:58:fd:67:58:83:71:e8:bc:c6:6d:97:bd
Airespace-Wlan-Id	6
AllowedProtocolMatchedRule	Dot1X
AuthenticationIdentityStore	Internal Users
AuthenticationMethod	x509_PKI
AuthorizationPolicyMatchedRule	Basic_Authenticated_Access



BYODRegistration	Unknown
Called-Station-ID	c8-f9-f9-83-47-b0:ME_EAP
Calling-Station-ID	34-02-86-96-2f-b7
Days to Expiry	344
DestinationIPAddress	10.106.32.31
DestinationPort	1812
DetailedInfo	Invalid username or password specified
Device IP Address	10.127.209.56
Device Port	32775
Device Type	Device Type#All Device Types
DeviceRegistrationStatus	NotRegistered
ElapsedDays	21
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	12935 Supplicant stopped responding to ISE during
IdentityGroup	Profiled
InactiveDays	0
IsThirdPartyDeviceFlow	false
Issuer	CN=fixer-WIN-97Q5HOKP9IG-CA\,DC=fixer\,DC=co
Issuer - Common Name	fixer-WIN-97Q5HOKP9IG-CA
Issuer - Domain Component	fixer, com
Key Usage	0, 2
Location	Location#All Locations
MACAddress	34:02:86:96:2F:B7



MatchedPolicy	Intel-Device
MessageCode	5411
NAS-IP-Address	10.127.209.56
NAS-Identifier	ryo_ap
NAS-Port	1
NAS-Port-Type	Wireless - IEEE 802.11
Network Device Profile	Cisco
NetworkDeviceGroups	Location#All Locations, Device Type#All Device Types
NetworkDeviceName	ryo_ap
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	Drop
SSID	c8-f9-f9-83-47-b0:ME_EAP
SelectedAccessService	Default Network Access
SelectedAuthenticationIdentityStores	EAPTLS
SelectedAuthorizationProfiles	PermitAccess
Serial Number	10 29 41 78 00 00 00 00 00 11
Service-Type	Framed
StaticAssignment	false
StaticGroupAssignment	false
StepData	4=Dot1X

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。