

# 802.1x WLAN + Mobility Express(ME)8.2およびISE 2.1でのVLANオーバーライド

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[ME の設定](#)

[ISE で ME を宣言する](#)

[ISE で新しいユーザの作成](#)

[認証ルールの作成](#)

[認証ルールの作成](#)

[エンド デバイスの設定](#)

[確認](#)

[ME の認証プロセス](#)

[ISE の認証プロセス](#)

## 概要

このドキュメントは、Wi-Fi Protected Access 2 ( WPA2 ) エンタープライズ セキュリティを備えた WLAN ( ワイヤレス LAN ) を Mobility Express コントローラおよび外部 Remote Authentication Dial-In User Service ( RADIUS ) サーバで設定する方法について説明します。Identity Service Engine ( ISE ) は外部 RADIUS サーバの例として使用されます。

このガイドで使用される Extensible Authentication Protocol ( EAP; 拡張可能認証プロトコル ) は Protected Extensible Authentication Protocol ( PEAP ) です。また、クライアントは特定の VLAN に割り当てられます ( デフォルトでは WLAN に割り当てられている VLAN 以外 ) 。

## 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
- PEAP
- 認証局 ( CA )
- 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。

MEv8.2

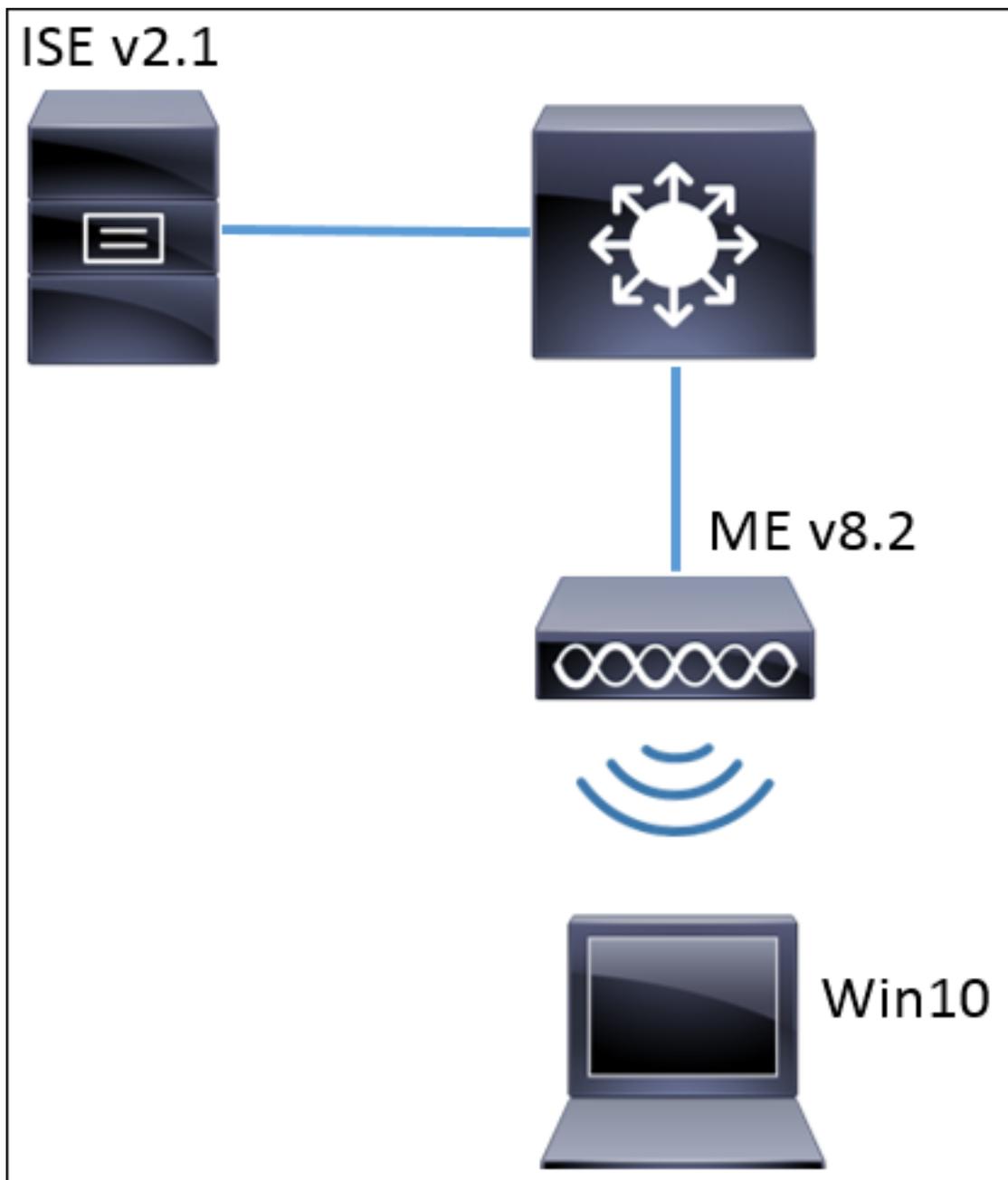
ISE v2.1

Windows 10 ラップトップ

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。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

## 設定

### ネットワーク図



## 設定

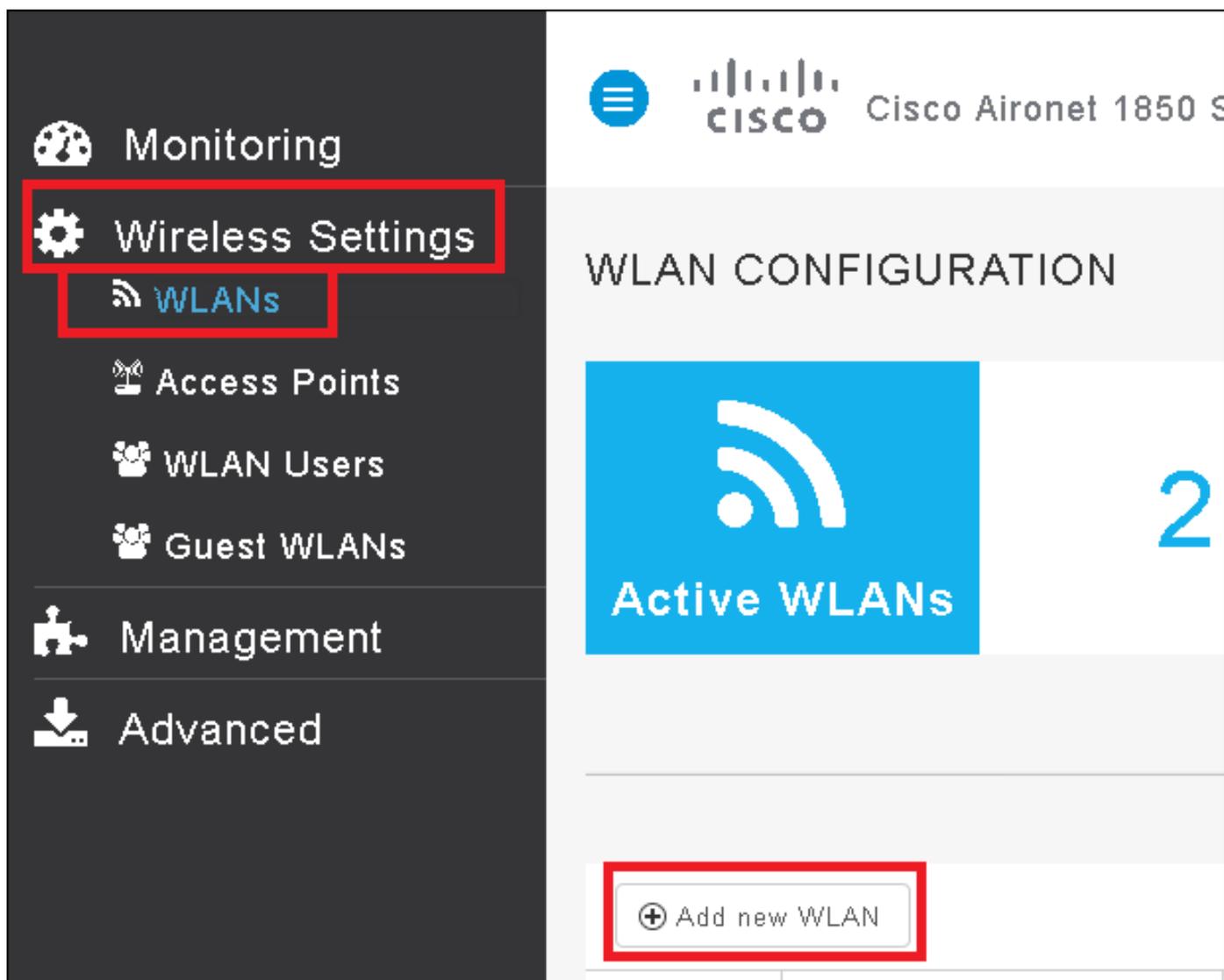
一般的な手順は以下のとおりです。

1. ME でサービス セット識別子 ( SSID ) を作成し、ME 上で RADIUS サーバ ( この例では ISE ) を宣言する
2. RADIUS サーバ ( ISE ) で ME を宣言する
3. ISE の認証ルール の作成
4. ISE の認可ルール の作成
5. エンドポイント の設定

## ME の設定

RADIUS サーバと ME 間の通信を可能にするには、RADIUS サーバを ME に登録し、その逆も登録する必要があります。この手順は RADIUS サーバを ME に登録する方法を示します。

ステップ1:MEのGUIを開き、 [Wireless Settings] > [WLANs] > [Add new WLAN]



ステップ 2 : WLAN の名前を選択します。

## Add New WLAN ✕

General **WLAN Security** VLAN & Firewall QoS

**WLAN Id** 3 ▼

**Profile Name \*** me-ise|

**SSID \*** me-ise

**Admin State** Enabled ▼

**Radio Policy** ALL ▼

✓ Apply ✕ Cancel

ステップ 3 : [WLAN Security] でセキュリティの設定を指定します。

[WPA2-Enterprise] を選択し、[Authentication Server] には [External RADIUS] を選択します。編集オプションをクリックして RADIUS の IP アドレスを追加し、[Shared Secret] キーを決めます。

# Add New WLAN



General WLAN Security VLAN & Firewall QoS

**Security** WPA2 Enterprise ▼

**Authentication Server** External Radius ▼

	Radius IP ▲	Radius Port	Shared Secret	
		1812	*****	▲
		1812	*****	▼

External Radius configuration applies to all WLANs

Apply

Cancel

Add New WLAN

General WLAN Security VLAN & Firewall QoS

Security WPA2 Enterprise ▼

Authentication Server External Radius ▼

Radius IP ▲	Radius Port	Shared Secret
a.b.c.d	1812	.....

ⓧ Please enter valid IPv4 address

External Radius configuration applies to all WLANs

Apply Cancel

<a.b.c.d> は、RADIUS サーバに対応しています。

ステップ 4 : SSID への VLAN の割り当て。

SSID を AP の VLAN に割り当てる必要がある場合は、この手順はスキップできます。

特定の VLAN ( AP の VLAN 以外 ) にこの SSID のユーザを割り当てるには、[Use VLAN Tagging] を有効にし、目的の VLAN ID を割り当てます。

Add New WLAN

General WLAN Security **VLAN & Firewall** QoS

Use VLAN Tagging Yes

VLAN ID \* 2400

Enable Firewall No

VLAN and Firewall configuration apply to all WLANs

Apply Cancel

注：VLAN タギングを使用する場合は、アクセス ポイントに接続されたスイッチ ポートが トランク ポートとして設定され、AP VLAN がネイティブに設定されていることを確認します。

ステップ 5：[Apply] をクリックして、設定を終了します。

**Add New WLAN**

General    WLAN Security    **VLAN & Firewall**    QoS

**Use VLAN Tagging** Yes ▼

**VLAN ID \*** 2400 ▼

**Enable Firewall** No ▼

VLAN and Firewall configuration apply to all WLANs

Apply    Cancel

ステップ6：オプションで、VLANオーバーライドを受け入れるようにWLANを設定します。

WLANでAAAオーバーライドを有効にし、必要なVLANを追加します。そのためには、ME管理インターフェイスへのCLIセッションを開き、次のコマンドを発行する必要があります。

```
>config wlan disable <wlan-id>
>config wlan aaa-override enable <wlan-id>
>config wlan enable <wlan-id>
>config flexconnect group default-flexgroup vlan add <vlan-id>
```

#### ISE で ME を宣言する

ステップ 1：ISE コンソールを開き、[Administration] > [Network Resources] > [Network Devices] > [Add] に移動します。

Identity Services Engine    Home    Context Visibility    Operations    Policy    **Administration**    Work

System    Identity Management    **Network Resources**    Device Portal Management    pxGrid Services    Feed Service

Network Devices    Network Device Groups    Network Device Profiles    External RADIUS Servers    RADIUS Server Sequences

Network devices    **Network Devices**

Default Device

Edit    **Add**    Duplicate    Import    Export    Generate PAC    Delete

ステップ 2：情報を入力します。

任意でモデル名、ソフトウェアバージョン、説明を指定し、デバイスタイプ、場所、WLC に基

づいてネットワーク デバイス グループを割り当てることができます。

a.b.c.d は ME の IP アドレスに対応します。

Network Devices List > **New Network Device**

### Network Devices

\* Name

Description

---

\* IP Address:  /

\* Device Profile

Model Name

Software Version

\* Network Device Group

Device Type

Location

WLCs

---

**▼ RADIUS Authentication Settings**

Enable Authentication Settings

Protocol **RADIUS**

\* Shared Secret

Enable KeyWrap  ⓘ

\* Key Encryption Key

\* Message Authenticator Code Key

Key Input Format  ASCII  HEXADECIMAL

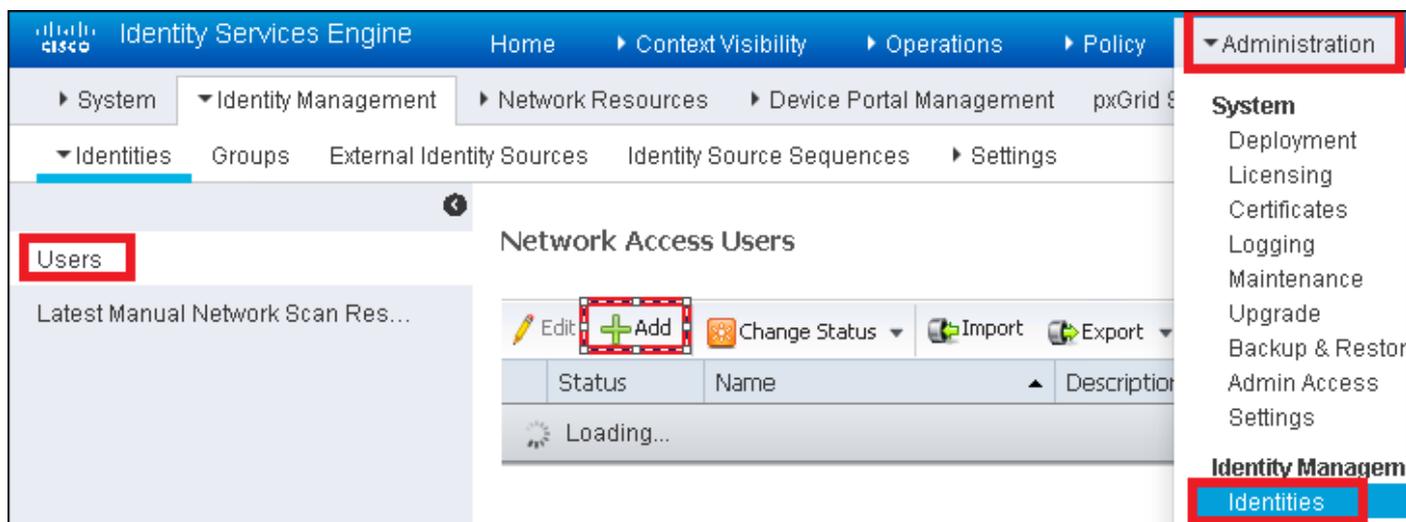
CoA Port

ネットワーク デバイス グループに関する詳細については以下のリンクを参照してください。

## [ISE:Network Device Groups](#)

### ISE で新しいユーザの作成

ステップ1: [Administration] > [Identity Management] > [Identities] > [Users] > [Add]を選択します。



ステップ2: 情報を入力します。

この例でこのユーザは ALL\_ACCOUNTS と呼ばれるグループに属していますが、必要に応じて調整できます。

▼ Network Access User

\* Name

Status  Enabled ▼

Email

▼ Passwords

Password Type:  ▼

Password

Re-Enter Passw

\* Login Password

Enable Password

▼ User Information

First Name

Last Name

▼ Account Options

Description

Change password on next login

▼ Account Disable Policy

Disable account if date exceeds

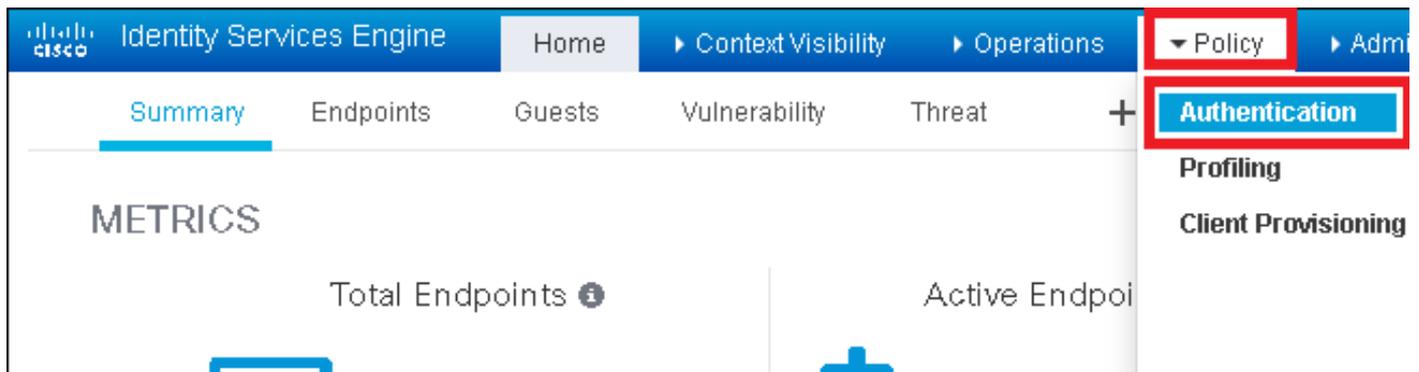
▼ User Groups

+

### 認証ルールの作成

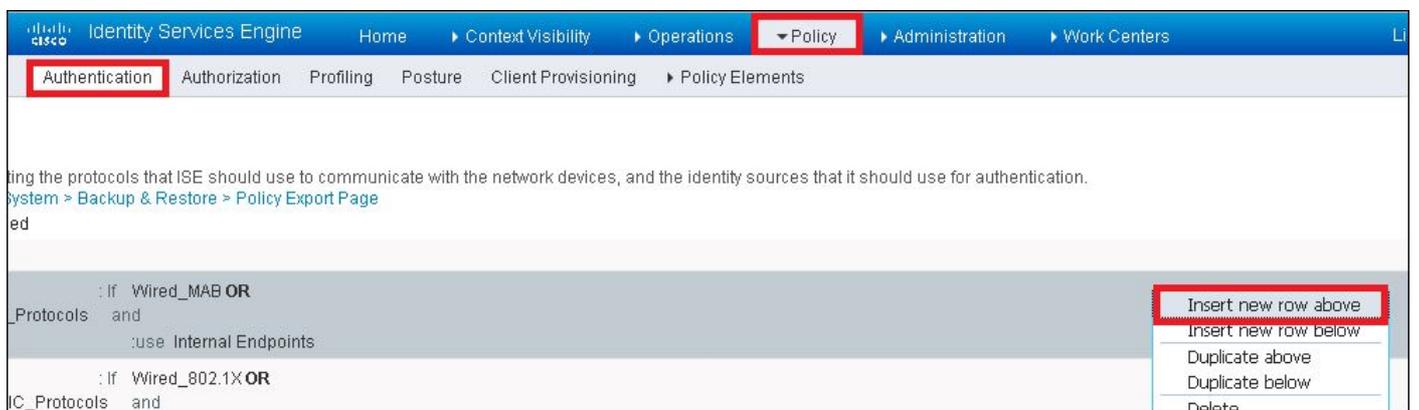
認証ルールはユーザのクレデンシャルが正しいか検証（ユーザ本当に本人かどうかの確認）し、それに使用する許可されている認証方法を制限するのに使用されます。

ステップ 1： ナビゲート [Policy] > [Authentication] に移動します。



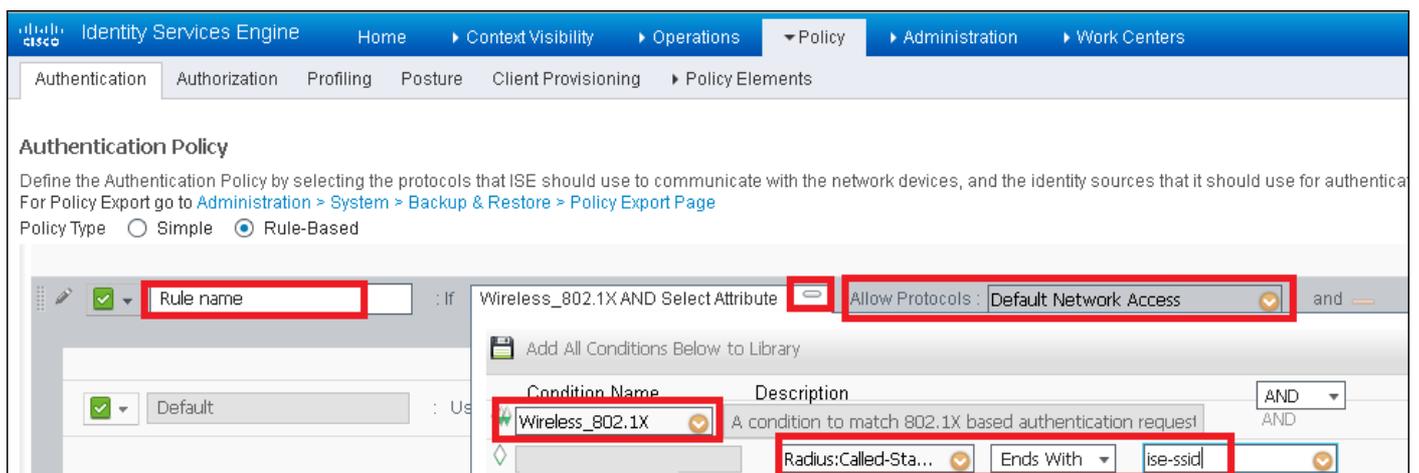
ステップ 2： 新しい認証ルールを挿入してください。

[Policy] > [Authentication] > [Insert] を選択して、下または上に新しい行を挿入します。

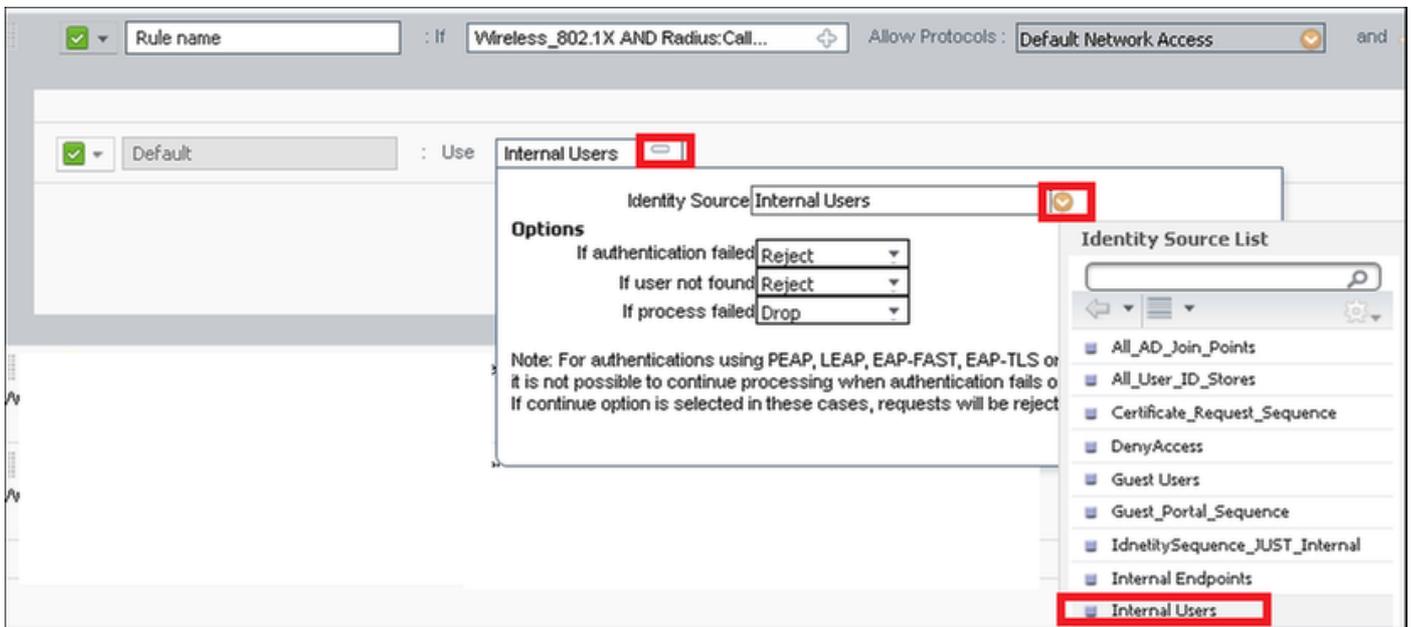


ステップ 3： 必要な情報を入力します。

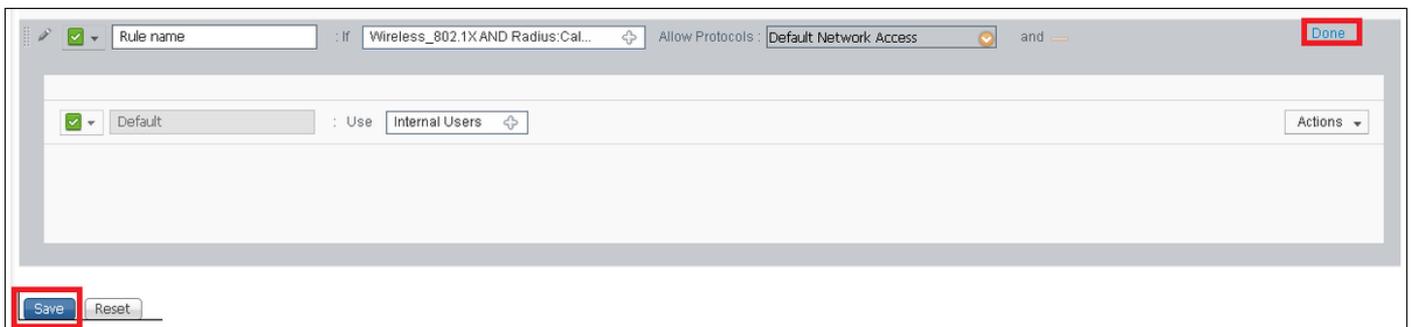
この認証ルールの例は、[Default Network Access] の一覧に記載されたすべてのプロトコルを許可します。この場合、Wireless 802.1x クライアント向けで Calling-Station-ID が *ise-ssid* で終了する認証要求に適用されます。



また、この認証ルールに一致するクライアントのアイデンティティソースを選択します。この例では、内部ユーザを使用します。



完了したら、[Done] と [Save] をクリックします。



許可されるプロトコルのポリシーに関する詳細については以下のリンクを参照してください。

[許可されるプロトコル サービス \( Allowed Protocols Service \)](#)

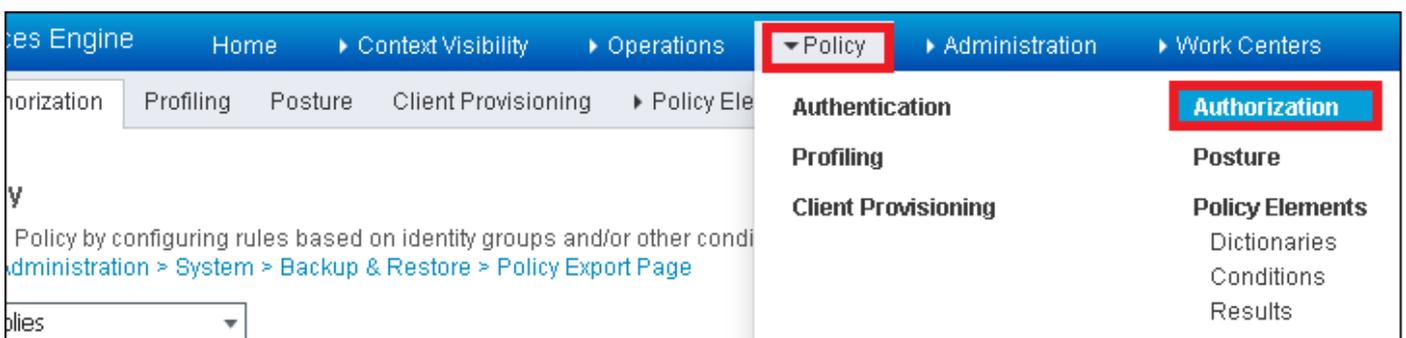
アイデンティティ ソースに関する詳細については以下のリンクを参照してください。

[ユーザ ID グループの作成](#)

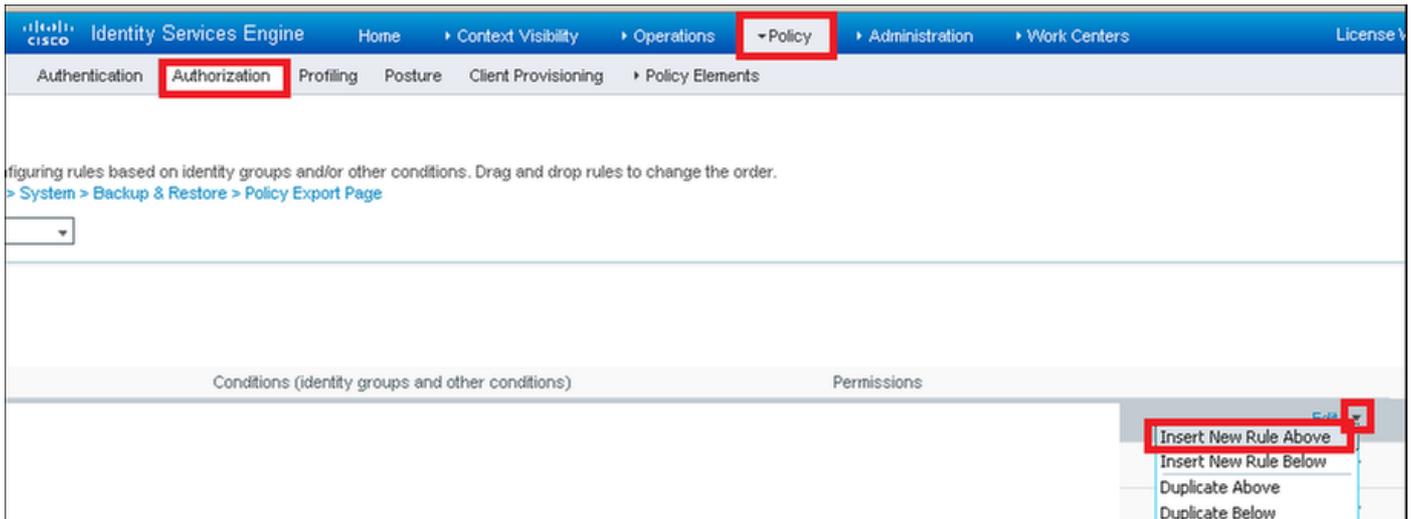
#### 認証ルールの作成

認証ルールはクライアントがネットワークに接続するかどうかの判断基準になります。

ステップ 1 : [Policy] > [Authorization] へ移動します。

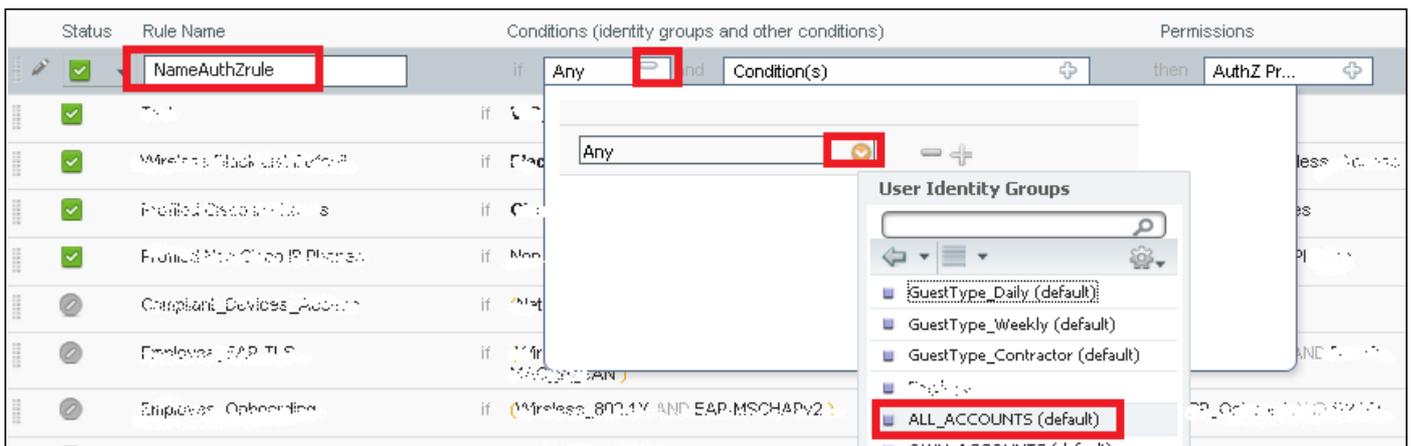


ステップ 2：新規ルールを追加します。[Policy] > [Authorization] > [Insert New Rule Above/Below]に進みます。

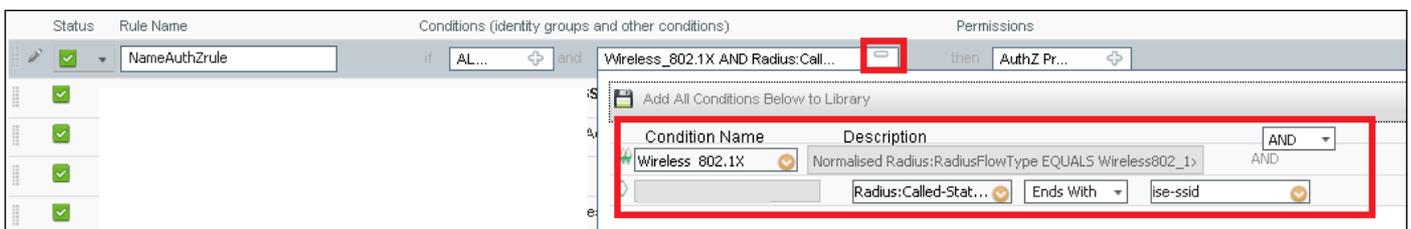


ステップ 3：情報を入力します。

まずルールの名前とユーザを保存する ID グループを選択します。この例では、ユーザは `ALL_ACCOUNTS` のグループに保存されます。



次に、承認プロセスがこのルールに当てはまるように、その他の条件を選択します。この例では、802.1x Wireless を使用した場合、承認プロセスはこのルールに当てはまり、局 ID は `ise-ssid` で終了します。



最後にクライアントがネットワークに参加できる認証プロファイルを選択して [Done]、[Save] をクリックします。



オプションで、ワイヤレスクライアントを別のVLANに割り当てる新しい許可プロファイルを作成します。



次の情報を入力します。

Add New Standard Profile

**Authorization Profile**

\* Name

Description

\* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

**Common Tasks**

DACL Name

ACL (Filter-ID)

VLAN Tag ID   IDName

Voice Domain Permission

**Advanced Attributes Settings**

Select an item  =

**Attributes Details**

Access Type = ACCESS\_ACCEPT  
Tunnel-Private-Group-ID = 1:vlan-id  
Tunnel-Type = 1:13  
Tunnel-Medium-Type = 1:6

## エンド デバイスの設定

PEAP/MS-CHAPv2 ( Challenge Handshake Authentication Protocol バージョン 2 の Microsoft 版 ) を使用して 802.1x 認証で SSID と接続するように Windows 10 のラップトップを設定します。

この設定例で ISE は自己署名証明書を使用して認証を実行します。

Windows のマシンで WLAN プロファイルを作成するには、次の 2 つのオプションがあります。

1. ISE サーバを有効にし、信頼するようにマシンに自己署名証明書をインストールし、認証を完成させる方法
2. RADIUS サーバの検証をバイパスし、認証に使用されるすべての RADIUS サーバを信頼する方法 ( 推奨されません )

これらのオプションの設定については、「[エンド デバイスの設定 - WLAN プロファイルの作成](#)」ステップ 7 で説明しています。

### エンド デバイスの設定 - ISE 自己署名証明書のインストール

ステップ 1 : ISE から自己署名証明書をエクスポートします。

ISE にログインし、[Administration] > [System] > [Certificates] > [System Certificates] に移動します。

EAP 認証に使用した証明書を選択し、[Export] をクリックします。

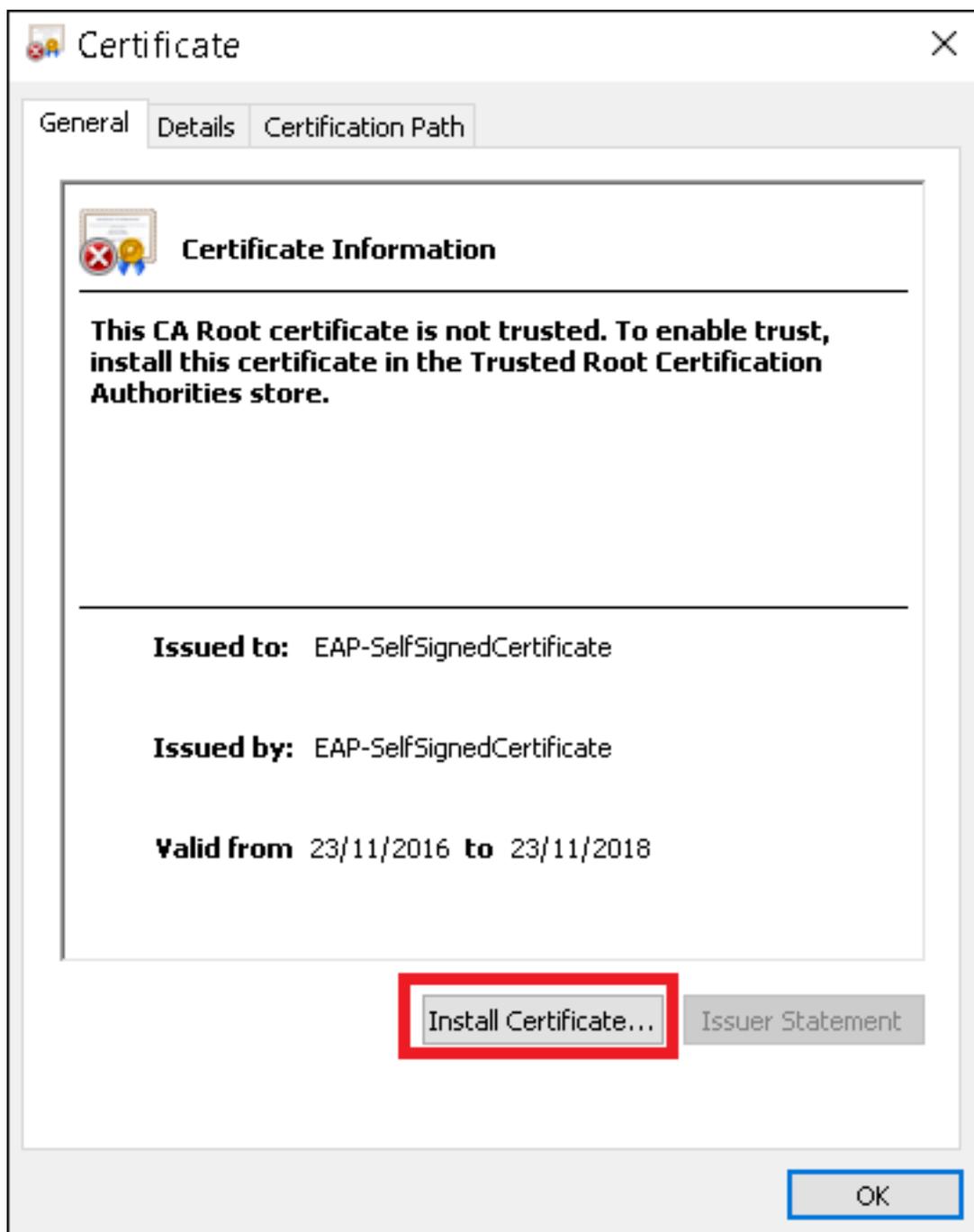
The screenshot shows the Cisco Identity Services Engine Administration interface. The navigation menu includes 'System', 'Administration', and 'Certificates'. The main content area is titled 'System Certificates' and features buttons for 'Edit', 'Generate Self Signed Certificate', 'Import', 'Export', and 'Delete'. Below these buttons is a table with columns for 'Friendly Name', 'Used By', and 'Portal group tag'. One certificate is selected and highlighted: 'EAP-SelfSignedCertificate#EAP-SelfSignedCertificate#00001' with 'EAP Authentication' as the portal group tag.

必要な場所に証明書を保存します。この証明書は Windows マシンにインストールされます。

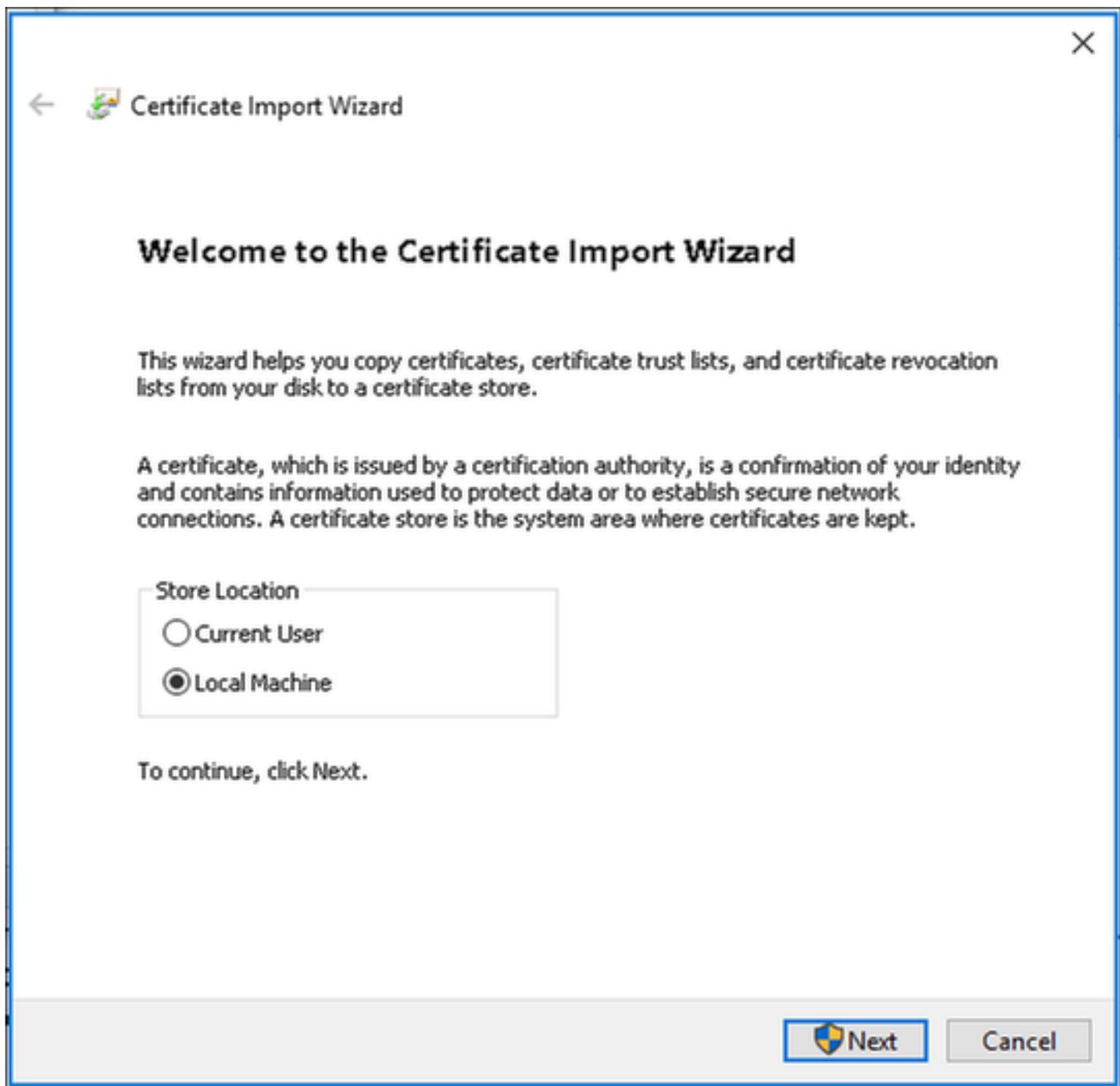
The dialog box is titled 'Export Certificate 'EAP-SelfSignedCertificate#EAP-SelfSignedCertificate#00001''. It contains two radio buttons: 'Export Certificate Only' (selected) and 'Export Certificate and Private Key'. Below these are two password input fields: '\*Private Key Password' and '\*Confirm Password'. A warning message states: 'Warning: Exporting a private key is not a secure operation. It could lead to possible exposure of the private key.' At the bottom right, there are 'Export' and 'Cancel' buttons.

ステップ 2 : Windows マシンに証明書をインストールします。

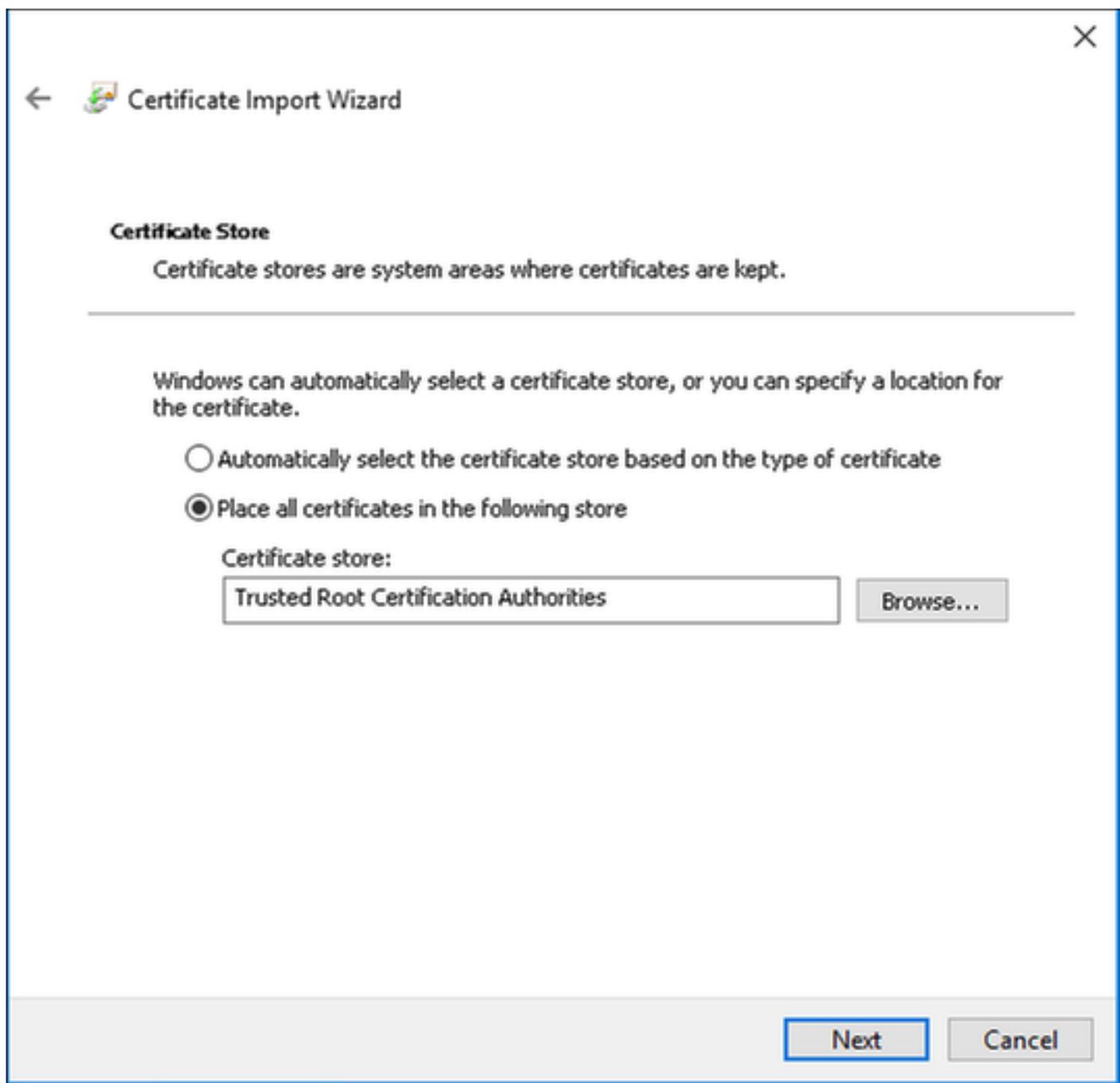
前にエクスポートした証明書をWindowsマシンにコピーし、ファイルの拡張子を.pemから.crtに変更します。その後、ダブルクリックして[証明書のインストール]を選択します。



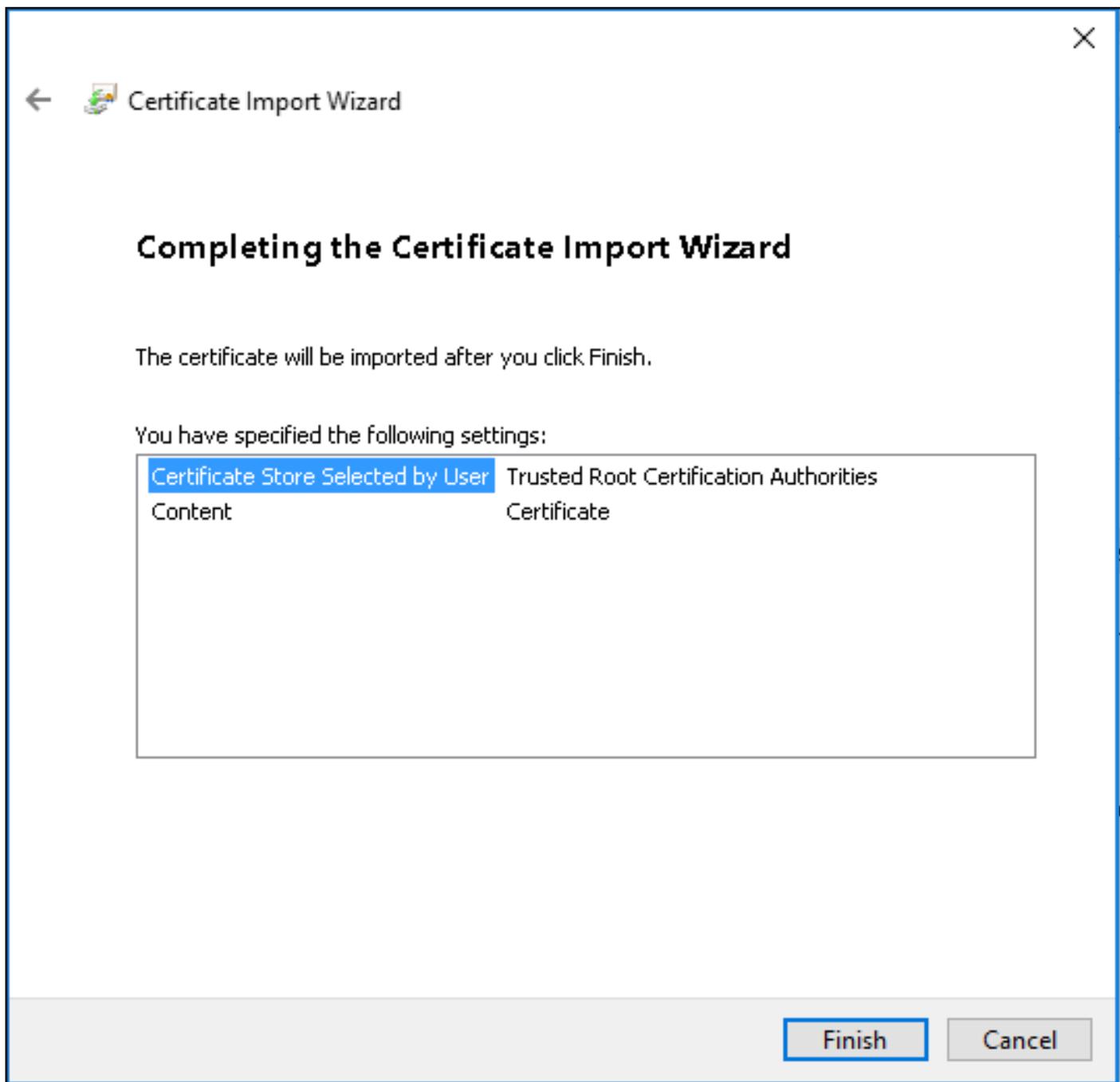
インストール場所で [Local Machine] を選択し、[Next] をクリックします。



[Place all certificates in the following store] を選択し、参照してから [Trusted Root Certification Authorities] を選択します。そのあと、[Next] をクリックします。



次に、[Finish] をクリックします。



最後に証明書のインストールを確認するには、[Yes] をクリックします。

## Security Warning



You are about to install a certificate from a certification authority (CA) claiming to represent:

EAP-SelfSignedCertificate

Windows cannot validate that the certificate is actually from "EAP-SelfSignedCertificate". You should confirm its origin by contacting "EAP-SelfSignedCertificate". The following number will assist you in this process:

Thumbprint (sha1): 011A193D 7007713D 0204E3D0 4759215D  
4E942137

### Warning:

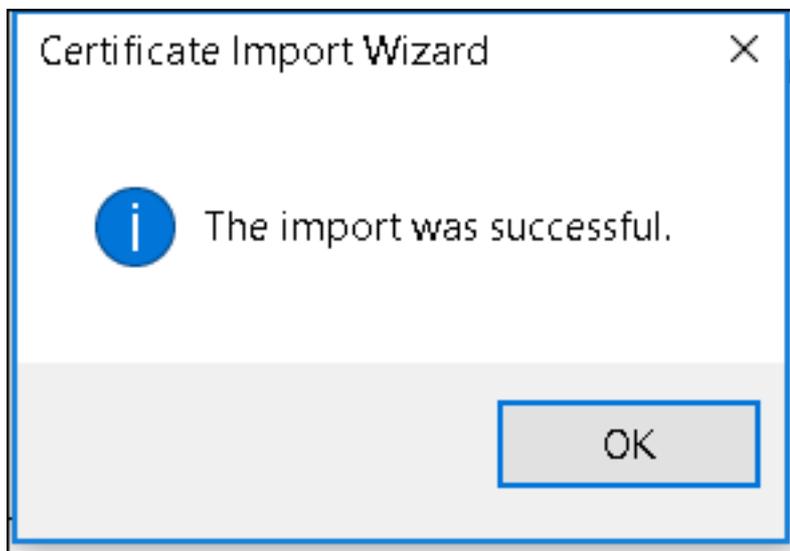
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

Yes

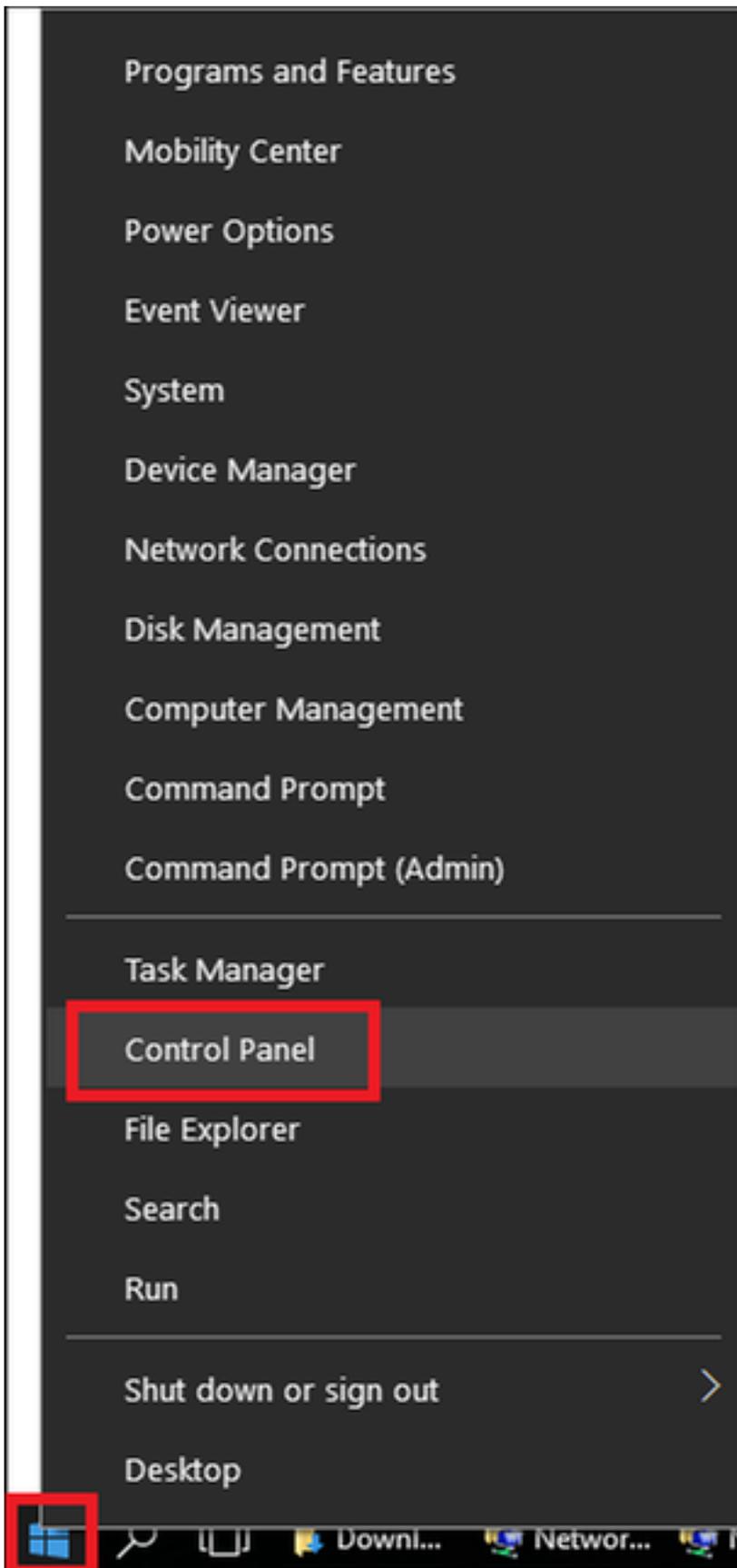
No

[OK] をクリックします。

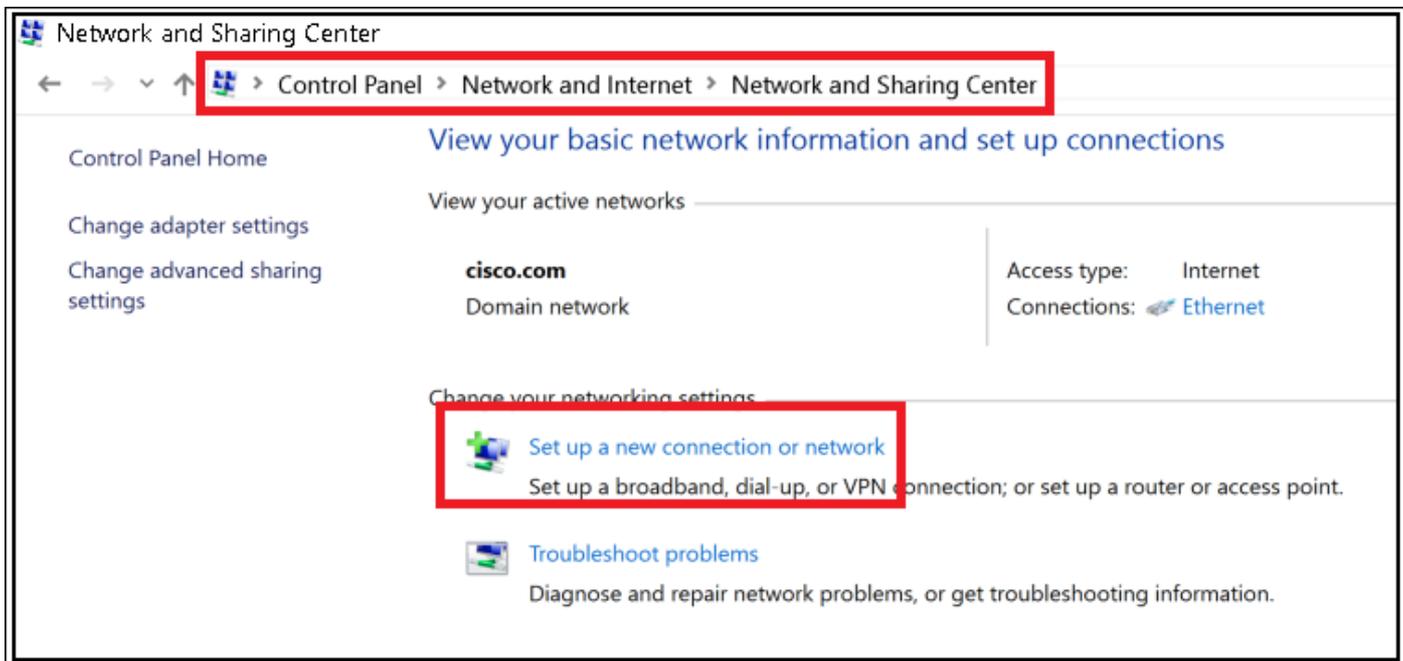


エンド デバイスの設定 : WLAN プロファイルの作成

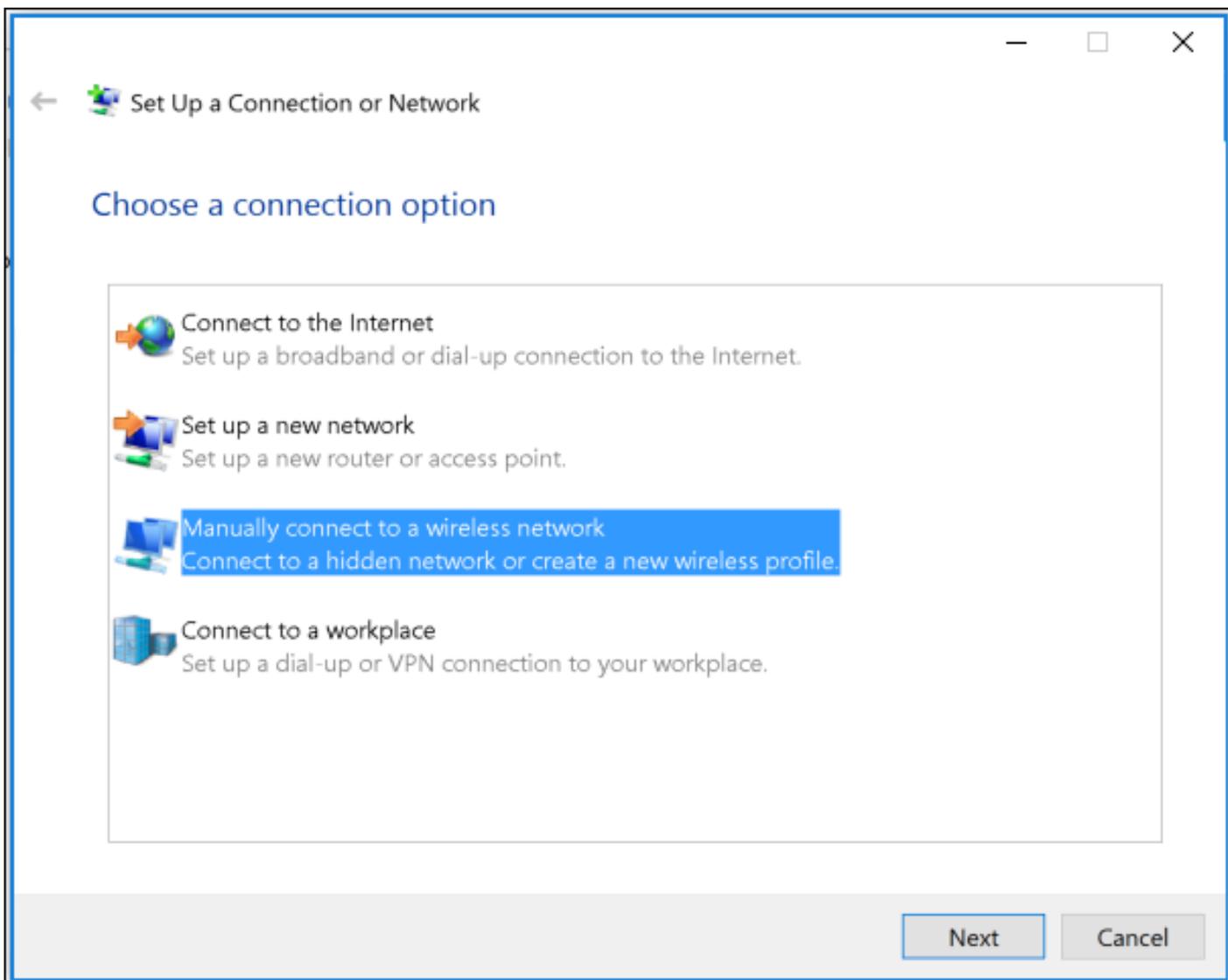
ステップ 1 : [Start] アイコンを右クリックし、[Control Panel] を選択します。



ステップ 2 : [Network and Internet] から [Network and Sharing Center] へ移動して、[Setup a new connection or network] をクリックします。



ステップ 3 : [Manually connect to a wireless network] を選択し、[Next] をクリックします。



ステップ 4 : SSID の名前および WPA2-Enterprise のセキュリティタイプの情報を入力し、[Next] をクリックします。

← Manually connect to a wireless network

Enter information for the wireless network you want to add

Network name:

Security type:

Encryption type:

Security Key:   Hide characters

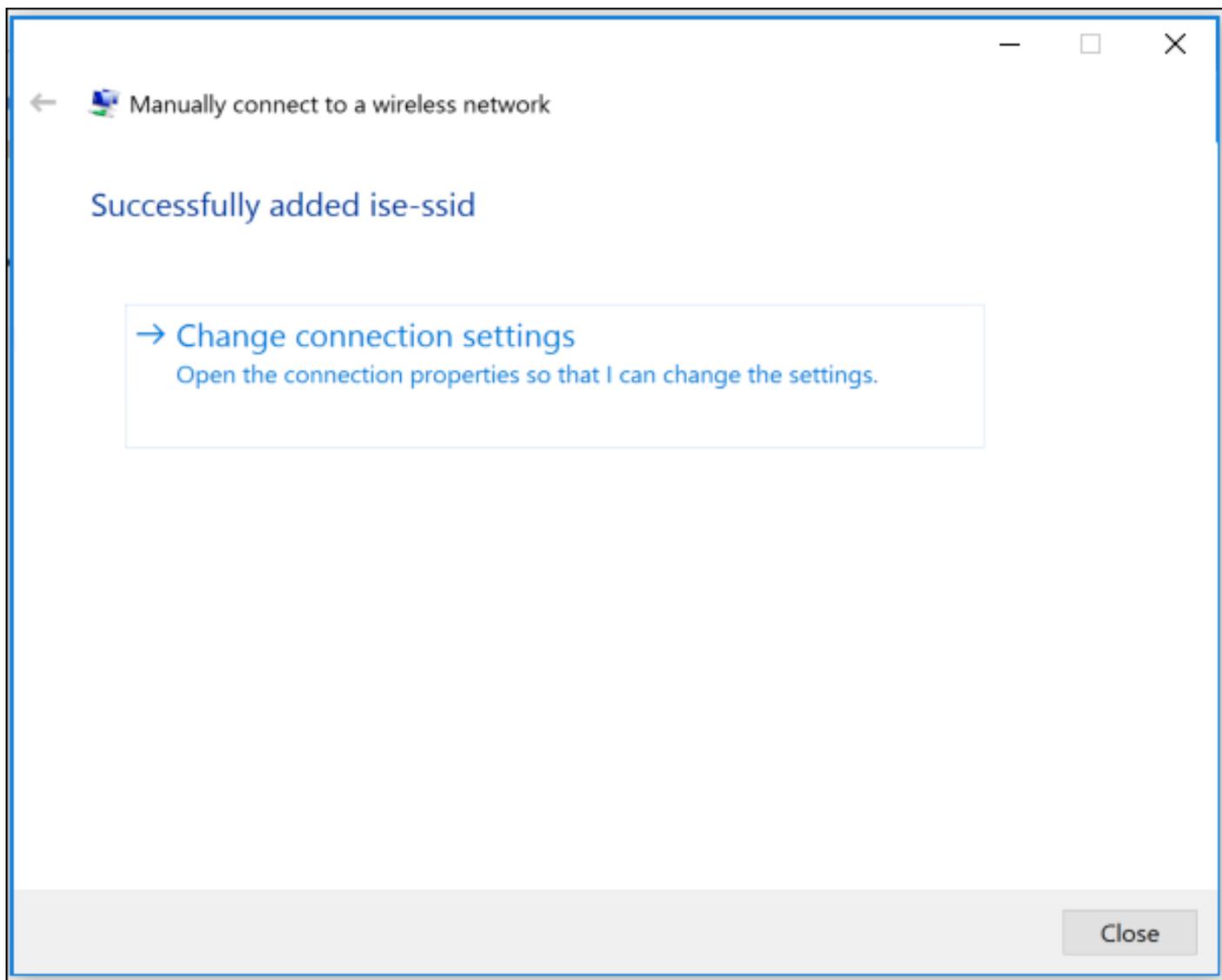
Start this connection automatically

Connect even if the network is not broadcasting

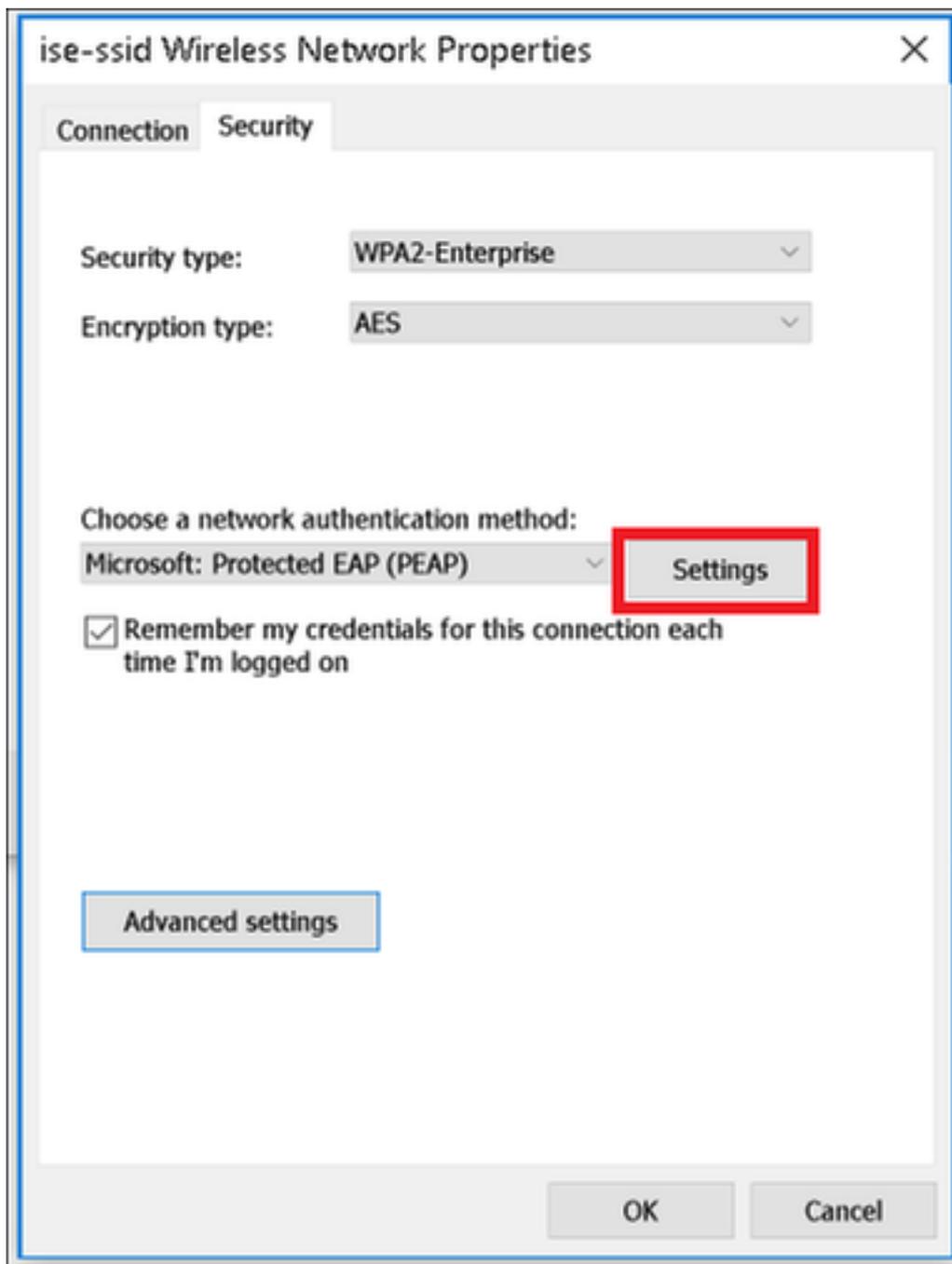
Warning: If you select this option, your computer's privacy might be at risk.

Next Cancel

ステップ 5 : WLAN プロファイルの設定をカスタマイズするには、[Change connection settings] を選択します。



ステップ 6 : [Security] タブに移動して [Settings] をクリックします。



ステップ 7 : RADIUS サーバが有効になっているかいないか選択します。

「はい」の場合は、「証明書を検証してサーバーのIDを確認する」を有効にし、「信頼できるルート証明機関」のリストからISEの自己署名証明書を選択します。

その後、[Configure] を選択して [Automatically use my Windows logon name and password...] を無効にし、[OK] をクリックします。



ステップ 8 : ユーザ クレデンシャルを設定します。

一度 [Security] タブに戻って [Advanced settings] を選択し、認証モードを [User authentication] として指定してユーザを認証するために ISE で設定されたクレデンシャルを保存します。

The screenshot shows a dialog box titled "ise-ssid Wireless Network Properties" with a close button (X) in the top right corner. The "Security" tab is selected. The "Security type" is set to "WPA2-Enterprise" and the "Encryption type" is set to "AES". Under "Choose a network authentication method:", "Microsoft: Protected EAP (PEAP)" is selected, and a "Settings" button is visible to its right. A checkbox labeled "Remember my credentials for this connection each time I'm logged on" is checked. At the bottom left, the "Advanced settings" button is highlighted with a red rectangular box. At the bottom right, there are "OK" and "Cancel" buttons.

## Advanced settings



802.1X settings

802.11 settings

Specify authentication mode:

User authentication

Save credentials

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):

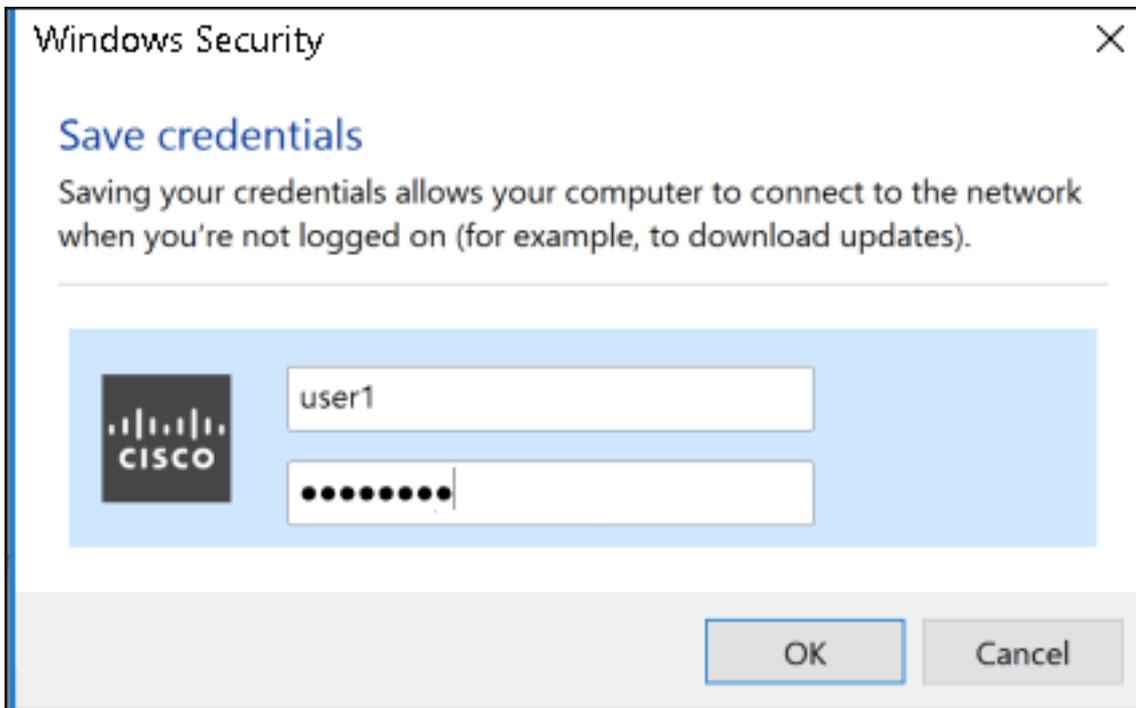
10

Allow additional dialogs to be displayed during single sign on

This network uses separate virtual LANs for machine and user authentication

OK

Cancel



## 確認

認証フローは WLC または ISE の観点から確認できます。

### ME の認証プロセス

特定のユーザの認証プロセスをモニタするには、次のコマンドを実行します。

```
> debug client <mac-add-client>
```

認証の成功例 ( 出力を一部省略しています ) :

```
*apfMsConnTask_0: Nov 25 16:36:24.333: 08:74:02:77:13:45 Processing assoc-req
station:08:74:02:77:13:45 AP:38:ed:18:c6:7b:40-01 thread:669ba80
*apfMsConnTask_0: Nov 25 16:36:24.333: 08:74:02:77:13:45 Association received from mobile on
BSSID 38:ed:18:c6:7b:4d AP 1852-4
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Applying site-specific Local Bridging
override for station 08:74:02:77:13:45 - vapId 3, site 'FlexGroup', interface 'management'
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Applying Local Bridging Interface
Policy for station 08:74:02:77:13:45 - vlan 0, interface id 0, interface 'management'
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Set Clinet Non AP specific
apfMsAccessVlan = 2400
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 This apfMsAccessVlan may be changed
later from AAA after L2 Auth
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Received 802.11i 802.1X key management
suite, enabling dot1x Authentication
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 0.0.0.0 START (0) Change state to
AUTHCHECK (2) last state START (0)
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 0.0.0.0 AUTHCHECK (2) Change state to
8021X_REQD (3) last state AUTHCHECK (2)
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 0.0.0.0 8021X_REQD (3) DHCP required on
```

**AP 38:ed:18:c6:7b:40 vapId 3 apVapId 3for this client**

\*apfMsConnTask\_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 apfPemAddUser2:session timeout forstation 08:74:02:77:13:45 - Session Tout 0, apfMsTimeOut '0' and sessionTimerRunning flag is 0

\*apfMsConnTask\_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 Stopping deletion of Mobile Station: (callerId: 48)

\*apfMsConnTask\_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 Func: apfPemAddUser2, Ms Timeout = 0, Session Timeout = 0

\*apfMsConnTask\_0: Nov 25 16:36:24.335: **08:74:02:77:13:45 Sending assoc-resp with status 0 station:08:74:02:77:13:45 AP:38:ed:18:c6:7b:40-01 on apVapId 3**

\*apfMsConnTask\_0: Nov 25 16:36:24.335: **08:74:02:77:13:45 Sending Assoc Response to station on BSSID 38:ed:18:c6:7b:4d (status 0) ApVapId 3 Slot 1**

\*spamApTask0: Nov 25 16:36:24.341: 08:74:02:77:13:45 Sent dot1x auth initiate message for mobile 08:74:02:77:13:45

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 reauth\_sm state transition 0 ---> 1 for mobile 08:74:02:77:13:45 at 1x\_reauth\_sm.c:47

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 EAP-PARAM Debug - eap-params for Wlan-Id :3 is disabled - applying Global eap timers and retries

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 Disable re-auth, use PMK lifetime.

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 Station 08:74:02:77:13:45 setting dot1x reauth timeout = 1800

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 dot1x - moving mobile 08:74:02:77:13:45 into Connecting state

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:24.342: **08:74:02:77:13:45 Sending EAP-Request/Identity to mobile 08:74:02:77:13:45 (EAP Id 1)**

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:24.401: **08:74:02:77:13:45 Received EAPOL EAPPKT from mobile 08:74:02:77:13:45**

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:24.401: **08:74:02:77:13:45 Received Identity Response (count=1) from mobile 08:74:02:77:13:45**

.

.

.

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.978: **08:74:02:77:13:45 Processing Access-Accept for mobile 08:74:02:77:13:45**

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.978: **08:74:02:77:13:45 Username entry (user1) created in mscb for mobile, length = 253**

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.978: 08:74:02:77:13:45 Station 08:74:02:77:13:45 setting dot1x reauth timeout = 1800

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.978: 08:74:02:77:13:45 Creating a PKC PMKID Cache entry for station 08:74:02:77:13:45 (RSN 2)

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Adding BSSID 38:ed:18:c6:7b:4d to PMKID cache at index 0 for station 08:74:02:77:13:45

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: New PMKID: (16)

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: [0000] 80 3a 20 8c 8f c2 4c 18 7d 4c 28 e7 7f 10 11 03

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Adding Audit session ID payload in Mobility handoff

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 0 PMK-update groupcast messages sent

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 PMK sent to mobility group

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Disabling re-auth since PMK lifetime can take care of same.

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Sending EAP-Success to mobile 08:74:02:77:13:45 (EAP Id 70)

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Freeing AAACB from Dot1xCB as AAA auth is done for mobile 08:74:02:77:13:45

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Found an cache entry for BSSID 38:ed:18:c6:7b:4d in PMKID cache at index 0 of station 08:74:02:77:13:45

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Found an cache entry for BSSID 38:ed:18:c6:7b:4d in PMKID cache at index 0 of station 08:74:02:77:13:45

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: Including PMKID in M1 (16)

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: [0000] 80 3a 20 8c 8f c2 4c 18 7d 4c 28 e7 7f 10 11 03

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: M1 - Key Data: (22)

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: [0000] dd 14 00 0f ac 04 80 3a 20 8c 8f c2 4c 18 7d 4c

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: [0016] 28 e7 7f 10 11 03

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: **08:74:02:77:13:45 Starting key exchange to mobile**

08:74:02:77:13:45, data packets will be dropped

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Sending EAPOL-Key Message to mobile

08:74:02:77:13:45

state INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Reusing allocated memory for EAP Pkt for retransmission to mobile 08:74:02:77:13:45

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Entering Backend Auth Success state (id=70) for mobile 08:74:02:77:13:45

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Received Auth Success while in Authenticating state for mobile 08:74:02:77:13:45

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 dot1x - moving mobile 08:74:02:77:13:45 into Authenticated state

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Received EAPOL-Key from mobile 08:74:02:77:13:45

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Received EAPOL-key in PTK\_START state (message 2) from mobile 08:74:02:77:13:45

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Successfully computed PTK from PMK!!!

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Received valid MIC in EAPOL Key Message M2!!!!!!

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.984: 00000000: 30 14 01 00 00 0f ac 04 01 00 00 0f ac 04 01 00 0.....

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.984: 00000010: 00 0f ac 01 0c 00 .....

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.984: 00000000: 01 00 00 0f ac 04 01 00 00 0f ac 04 01 00 00 0f .....

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.984: 00000010: ac 01 0c 00 ....

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 PMK: Sending cache add

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 Stopping retransmission timer for mobile 08:74:02:77:13:45

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 Sending EAPOL-Key Message to mobile 08:74:02:77:13:45

state PTKINITNEGOTIATING (message 3), replay counter 00.00.00.00.00.00.00.01

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 Reusing allocated memory for EAP Pkt for retransmission to mobile 08:74:02:77:13:45

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Received EAPOL-key in PTKINITNEGOTIATING state (message 4) from mobile 08:74:02:77:13:45

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Stopping retransmission timer for mobile 08:74:02:77:13:45

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 8021X\_REQD (3) Change state to L2AUTHCOMPLETE (4) last state 8021X\_REQD (3)

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Mobility query, PEM State: L2AUTHCOMPLETE

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Building Mobile Announce :

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Building Client Payload:

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Client Ip: 0.0.0.0

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Client Vlan Ip: 172.16.0.136, Vlan mask : 255.255.255.224

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Client Vap Security: 16384

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Virtual Ip: 192.0.2.1

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 ssid: ise-ssid

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Building VlanIpPayload.

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 L2AUTHCOMPLETE (4) DHCP required on AP 38:ed:18:c6:7b:40 vapId 3 apVapId 3for this client

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Not Using WMM Compliance code qosCap 00

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 L2AUTHCOMPLETE (4) Plumbed mobile LWAPP rule on AP 38:ed:18:c6:7b:40 vapId 3 apVapId 3 flex-acl-name:

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP\_REQD (7) last state L2AUTHCOMPLETE (4)

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 DHCP\_REQD (7)

pemAdvanceState2 6623, Adding TMP rule

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 DHCP\_REQD (7) Adding Fast Path rule

type = Airespace AP - Learn IP address

```

on AP 38:ed:18:c6:7b:40, slot 1, interface = 1, QOS = 0
IPv4 ACL ID = 255, IPv
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) mobility role
update request from Unassociated to Local
Peer = 0.0.0.0, Old Anchor = 0.0.0.0, New Anchor = 172.16.0.136
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) State Update from
Mobility-Incomplete to Mobility-Complete, mobility role=Local, client
state=APF_MS_STATE_ASSOCIATED
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) pemAdvanceState2
6261, Adding TMP rule
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) Replacing Fast
Path rule
type = Airespace AP - Learn IP address
on AP 38:ed:18:c6:7b:40, slot 1, interface = 1, QOS = 0
IPv4 ACL ID = 255,
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) Successfully
plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
*pemReceiveTask: Nov 25 16:36:25.990: 08:74:02:77:13:45 0.0.0.0 Added NPU entry of type 9,
dtlFlags 0x0
*pemReceiveTask: Nov 25 16:36:25.990: 08:74:02:77:13:45 0.0.0.0 Added NPU entry of type 9,
dtlFlags 0x0
*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 WcdbClientUpdate: IP Binding from WCDB
ip_learn_type 1, add_or_delete 1
*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 IPv4 Addr: 0:0:0:0
*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 In apfRegisterIpAddrOnMscb_debug:
regType=1 Invalid src IP address, 0.0.0.0 is part of reserved ip address range (caller
apf_ms.c:3593)
*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 IPv4 Addr: 0:0:0:0
*apfReceiveTask: Nov 25 16:36:27.840: 08:74:02:77:13:45 WcdbClientUpdate: IP Binding from WCDB
ip_learn_type 1, add_or_delete 1
*apfReceiveTask: Nov 25 16:36:27.841: 08:74:02:77:13:45 172.16.0.16 DHCP_REQD (7) Change state
to RUN (20) last state DHCP_REQD (7)

```

デバッグクライアントの出力を簡単に読むための手段として、ワイヤレスデバッグアナライザツールを使用します。

## [ワイヤレスデバッグアナライザ](#)

### ISE の認証プロセス

[Operations] > [RADIUS] > [Live Logs] に移動してどの認証ポリシーと認可ポリシー、認証プロファイルがユーザに割り当てられているか確認できます。

Time	Sta...	Details	Ide...	Endpoint ID	Endpoint ...	Authentication Policy	Authorization Policy	Authorization Profiles
No...	1		user1	08:74:02:77:13:45	Apple-Device	Default >> Rule name >> Default	Default >> NameAuthZrule	PermitAccess

もっと詳細の認証プロセスを見るには、[Details] をクリックします。