802.1x WLAN + VLAN override with Mobility Express (ME) 8.2 and ISE 2.1

Contents

Introduction
Prerequisites
Requirements
Components Used
Configure
Network Diagram
Configurations
Configuration on ME
Declare ME on ISE
Create a new user on ISE
Create the Authentication rule
Create the Authorization rule
Configuration of end device
Verify
Authentication process on ME
Authentication process on ISE

Introduction

This documents describes how to set up a WLAN (Wireless Local Area Network) with Wi-Fi Protected Access 2 (WPA2) Enterprise security with a Mobility Express controller and an external Remote Authentication Dial-In User Service (RADIUS) server. Identity Service Engine (ISE) is used as example of external RADIUS servers.

The Extensible Authentication Protocol (EAP) used in this guide is Protected Extensible Authentication Protocol (PEAP). Besides that the client is assigned to an specific VLAN (other than the one assigned to the WLAN ny default).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- 802.1x
- PEAP
- Certification Authority (CA)
- Certificates

Components Used

The information in this document is based on these software and hardware versions:

ME v8.2

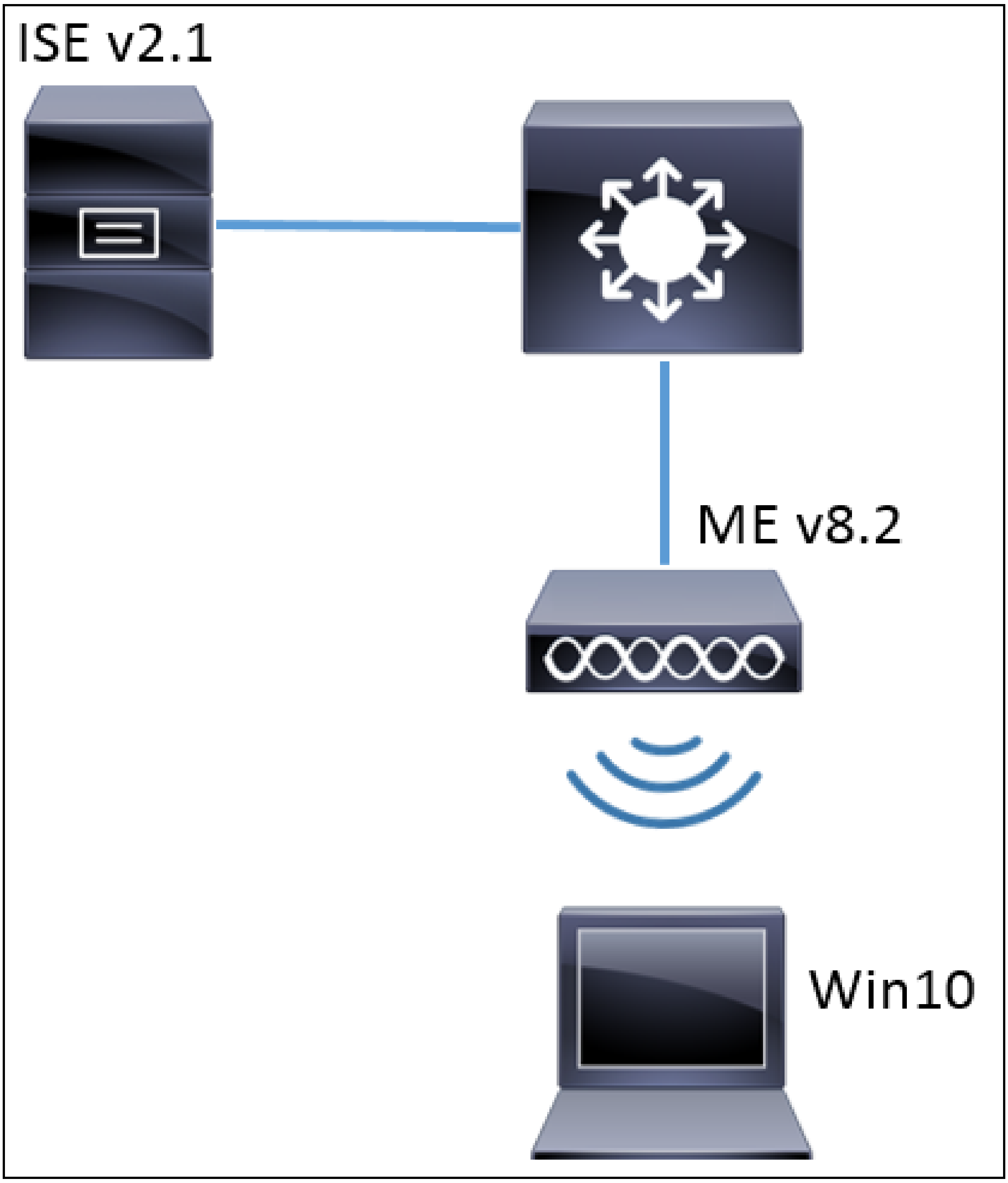
ISE v2.1

Windows 10 Laptop

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configure

Network Diagram



Configurations

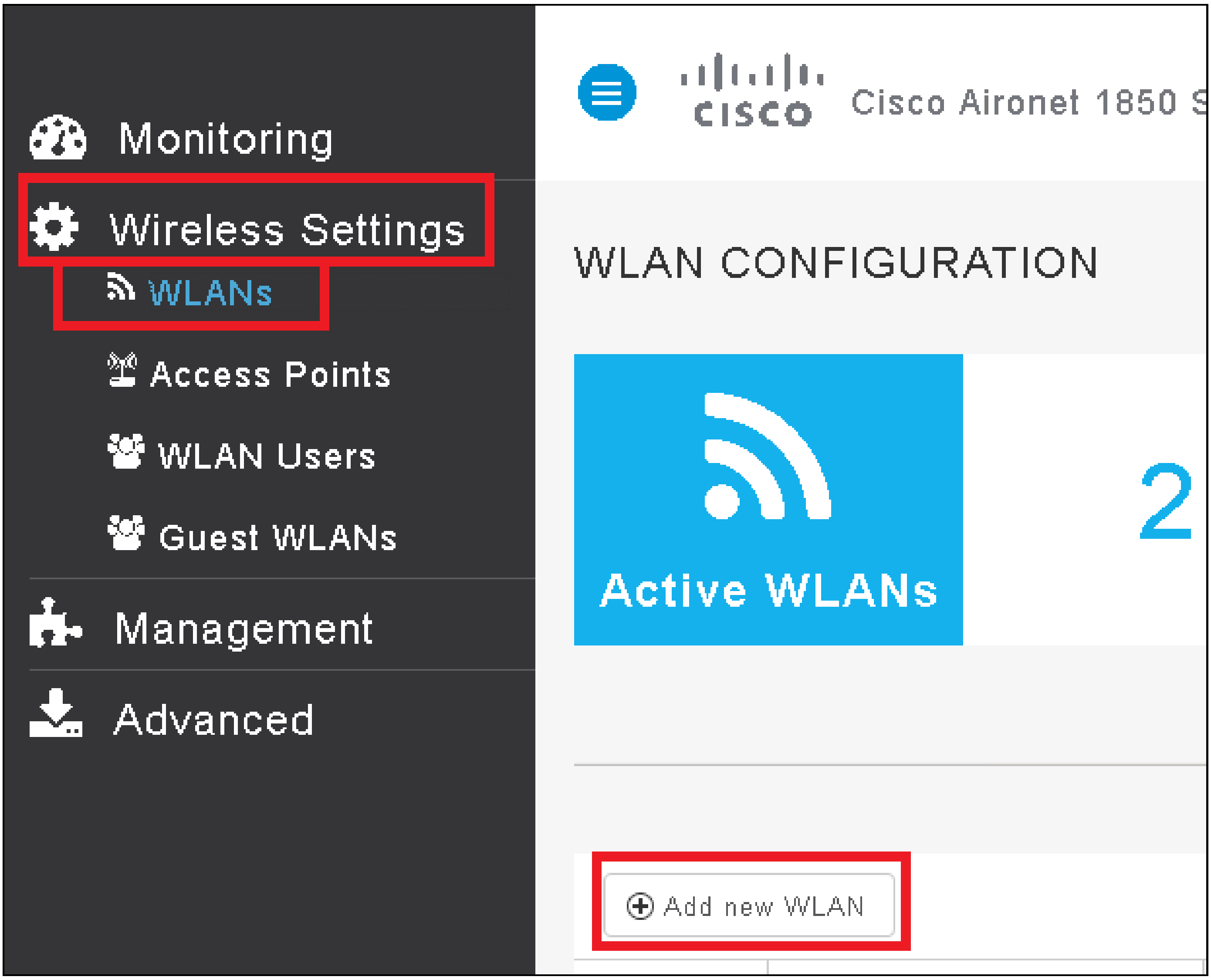
The general steps are:

1. Create the Service Set Identifier (SSID) in the ME and declare RADIUS server (ISE in this example) on ME
2. Declare ME on RADIUS server (ISE)
3. Create the authentication rule on ISE
4. Create the authorization rule on ISE
5. Configure the endpoint

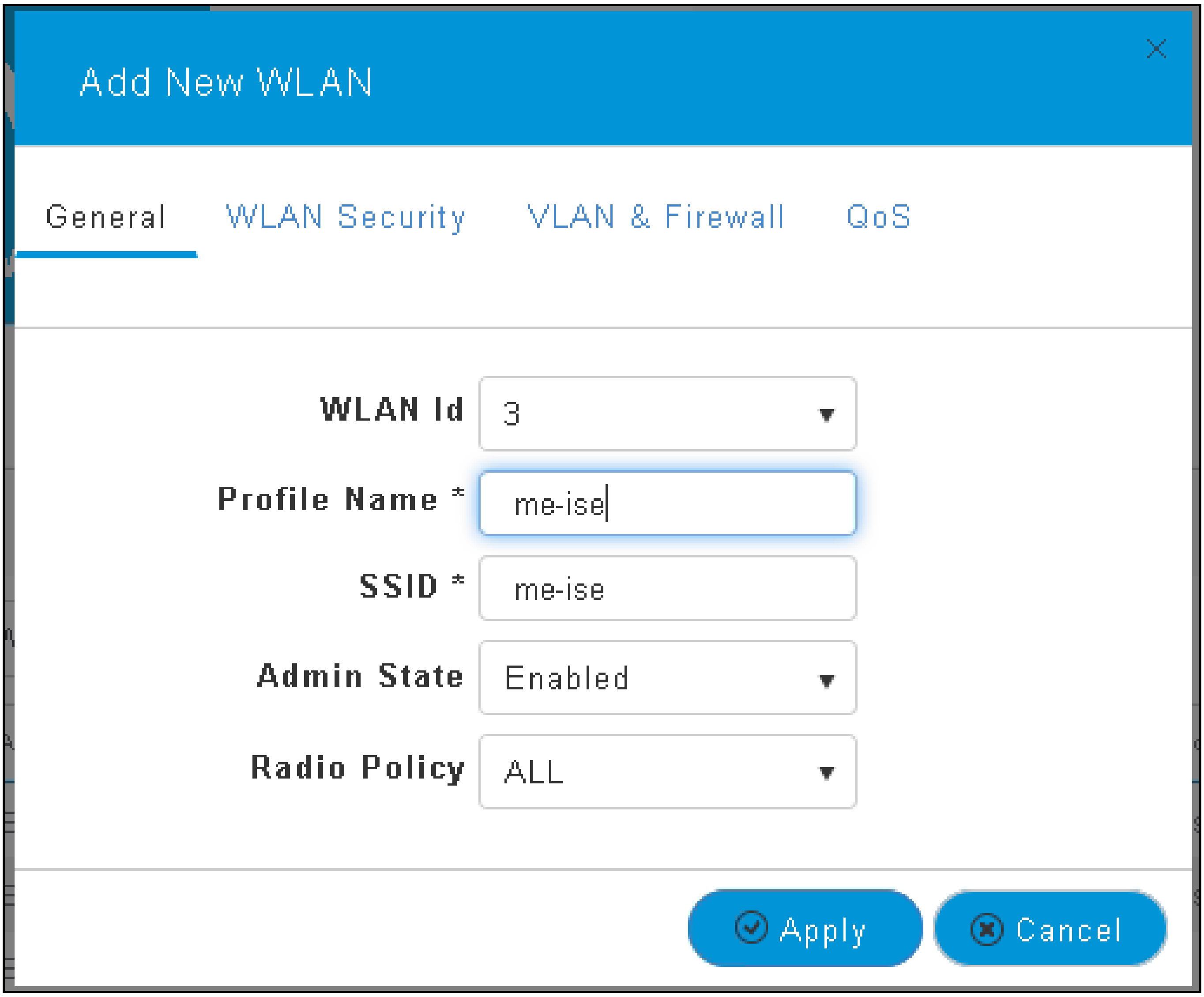
Configuration on ME

In order to allow communication between RADIUS server and ME it is needed to register RADIUS server on ME and vice versa. This step shows how to register RADIUS server on ME.

Step 1. Open the GUI of the ME and navigate to **Wireless Settings > WLANs > Add new WLAN.**



Step 2. Select a name for the WLAN.



Add New WLAN

General | WLAN Security | VLAN & Firewall | QoS

WLAN Id: 3

Profile Name *: me-ise

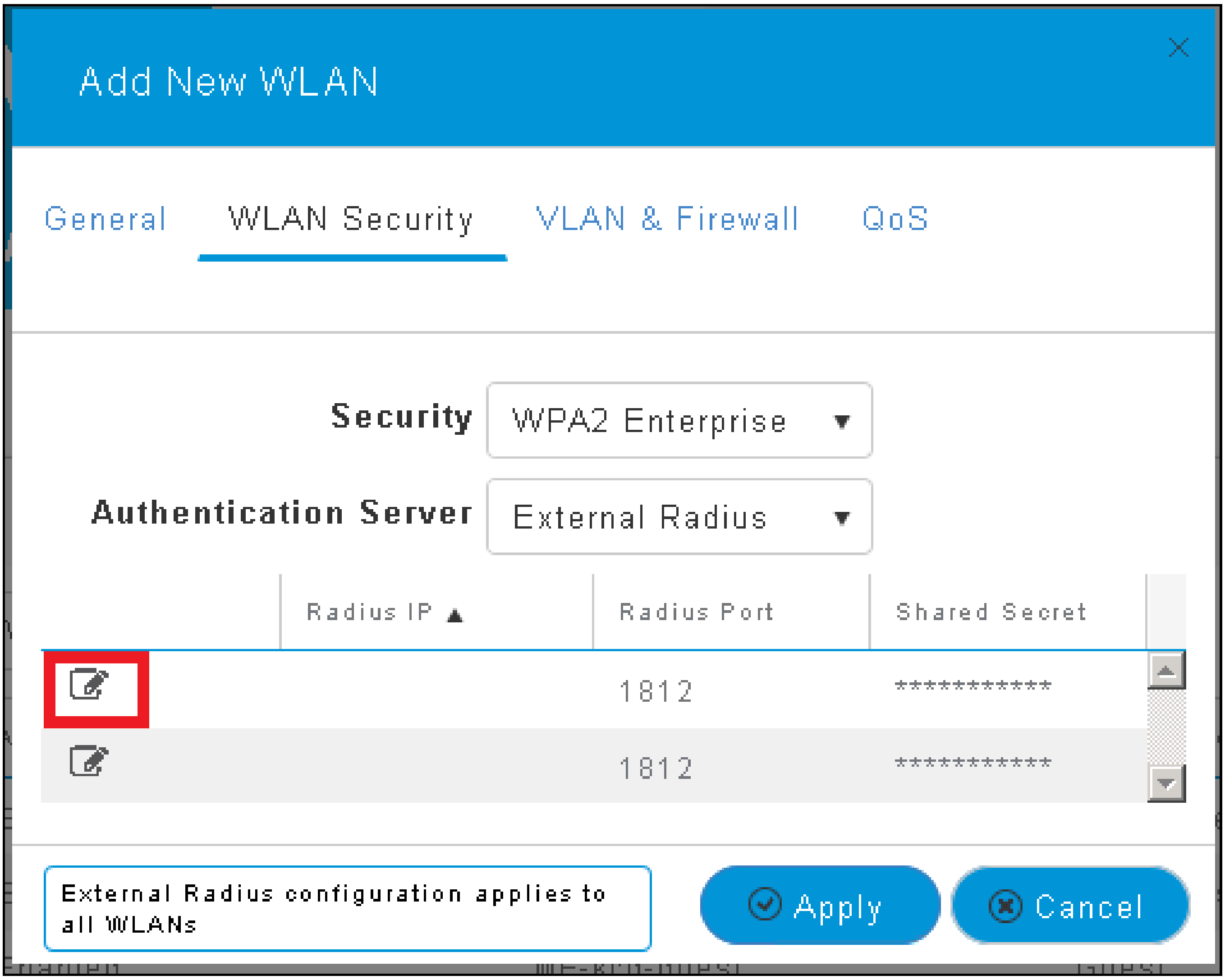
SSID *: me-ise

Admin State: Enabled

Radio Policy: ALL

Step 3. Specify Security configuration under **WLAN Security** tab.

Choose **WPA2 Enterprise**, for Authentication server choose **External RADIUS**. Click the edit option to add the RADIUS's ip address and pick a **Shared Secret** key.

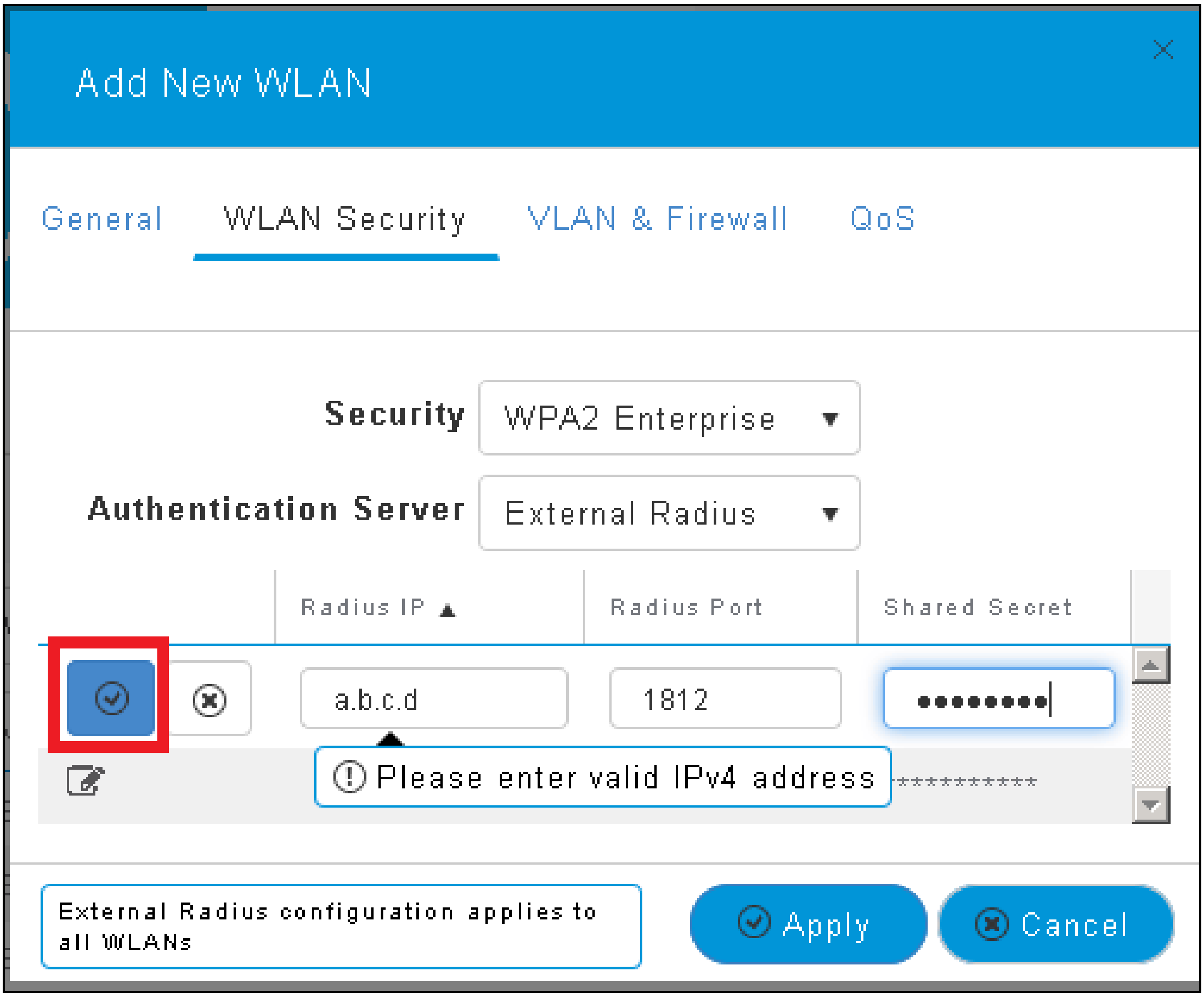


Security: WPA2 Enterprise ▾

Authentication Server: External Radius ▾

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

External Radius configuration applies to all WLANs



Security: WPA2 Enterprise

Authentication Server: External Radius

Radius IP	Radius Port	Shared Secret
a.b.c.d	1812	•••••••••
		***********

Please enter valid IPv4 address

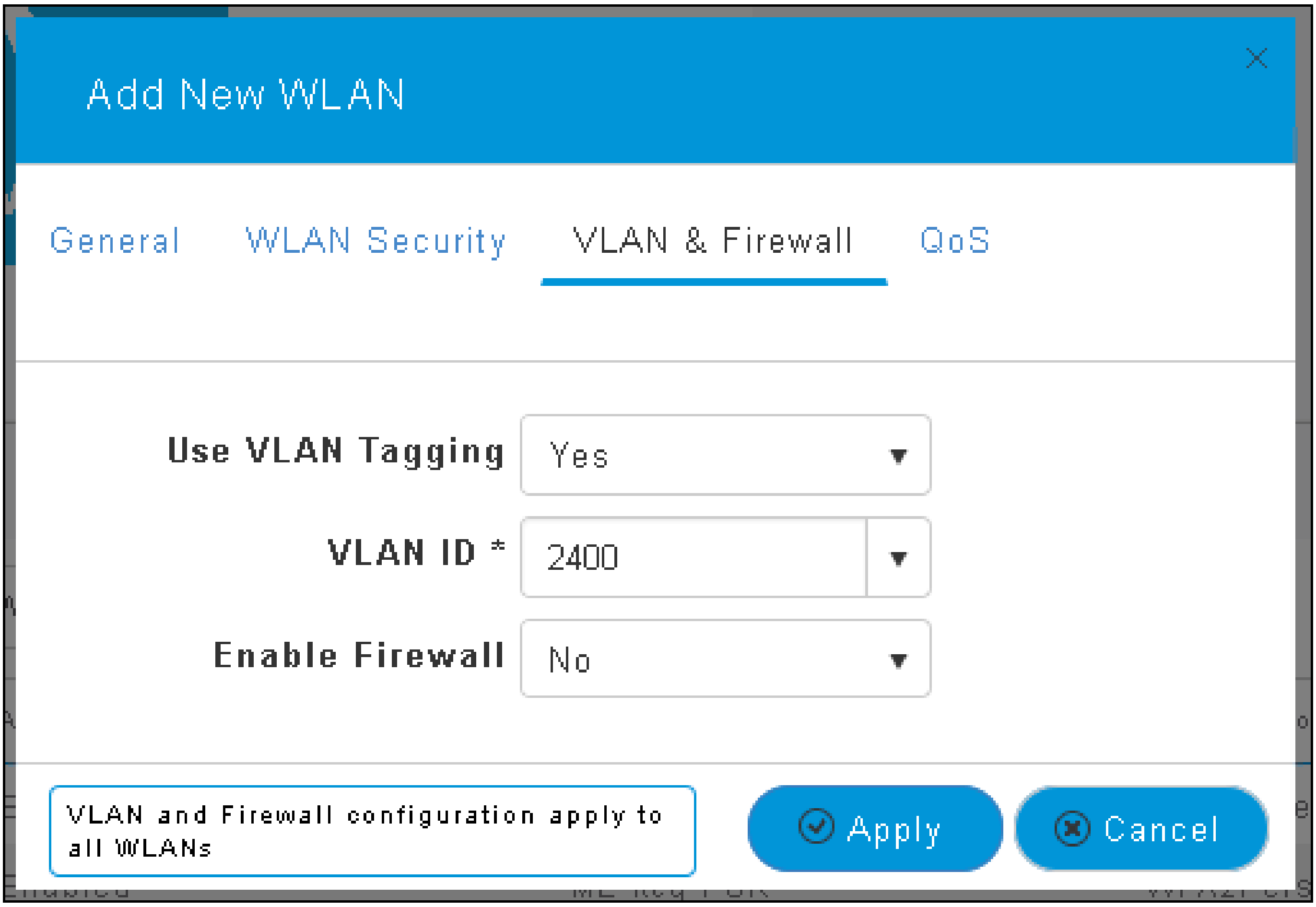
External Radius configuration applies to all WLANs

<a.b.c.d> corresponds to the RADIUS server.

Step 4. Assign a VLAN to the SSID.

If the SSID needs to be assigned to the AP's VLAN this step can be skipped.

In order to assign the users for this SSID to a specific VLAN (other than AP's VLAN), enable **Use VLAN Tagging** and assign the desired **VLAN ID**.



Use VLAN Tagging: Yes

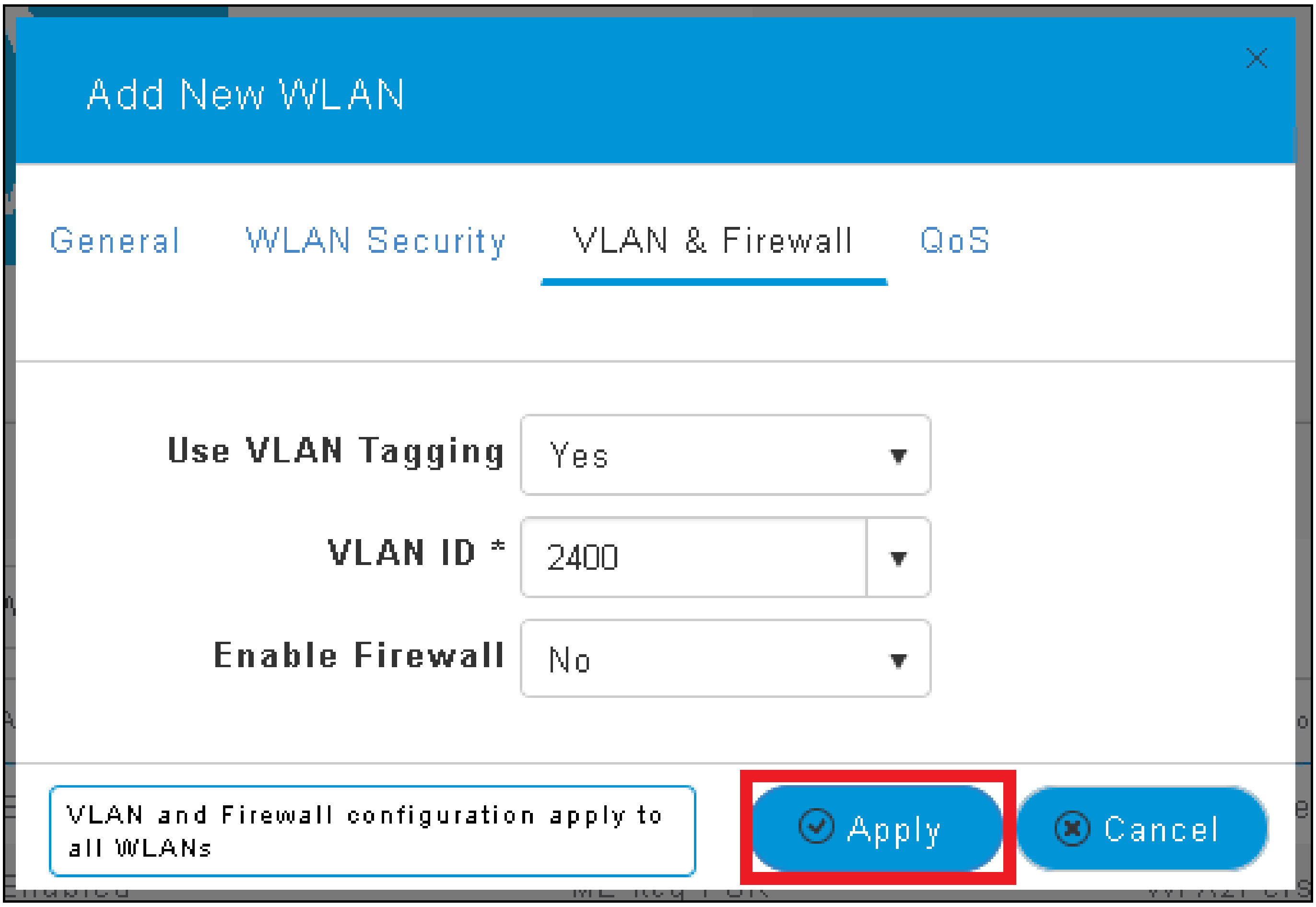
VLAN ID *: 2400

Enable Firewall: No

VLAN and Firewall configuration apply to all WLANs

Note: If VLAN Tagging is used, be sure that the switchport where the Access Point is connected to, is configured as trunk port and the AP VLAN is configured as native.

Step 5. Click **Apply** to finish the configuration.



Use VLAN Tagging: Yes

VLAN ID *: 2400

Enable Firewall: No

VLAN and Firewall configuration apply to all WLANs

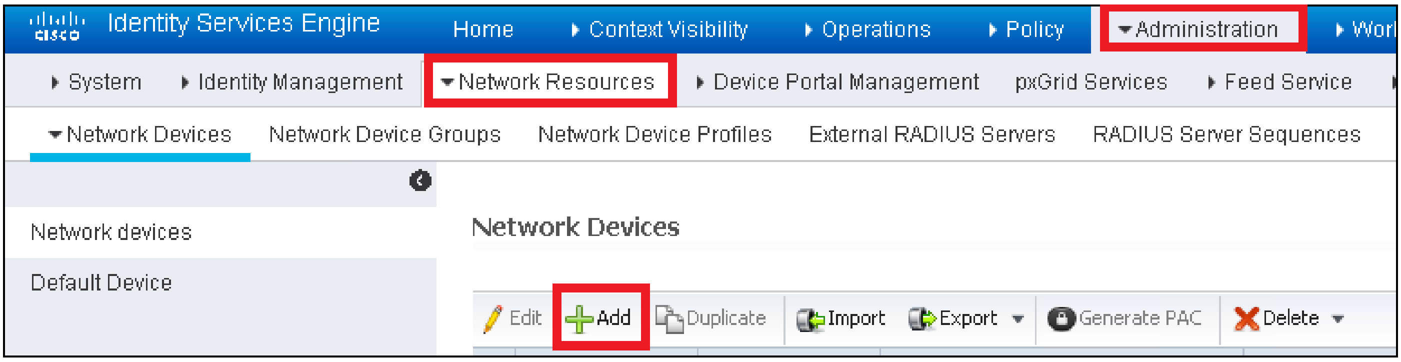
Step 6. Optional, configure the WLAN to accept the VLAN override.

Enable AAA override on the WLAN and add the needed VLANs. To do so you will nee to open a CLI session to the ME management interface and issue these commands:

```
>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>
```

Declare ME on ISE

Step 1. Open ISE console and navigate to **Administration > Network Resources > Network Devices > Add.**

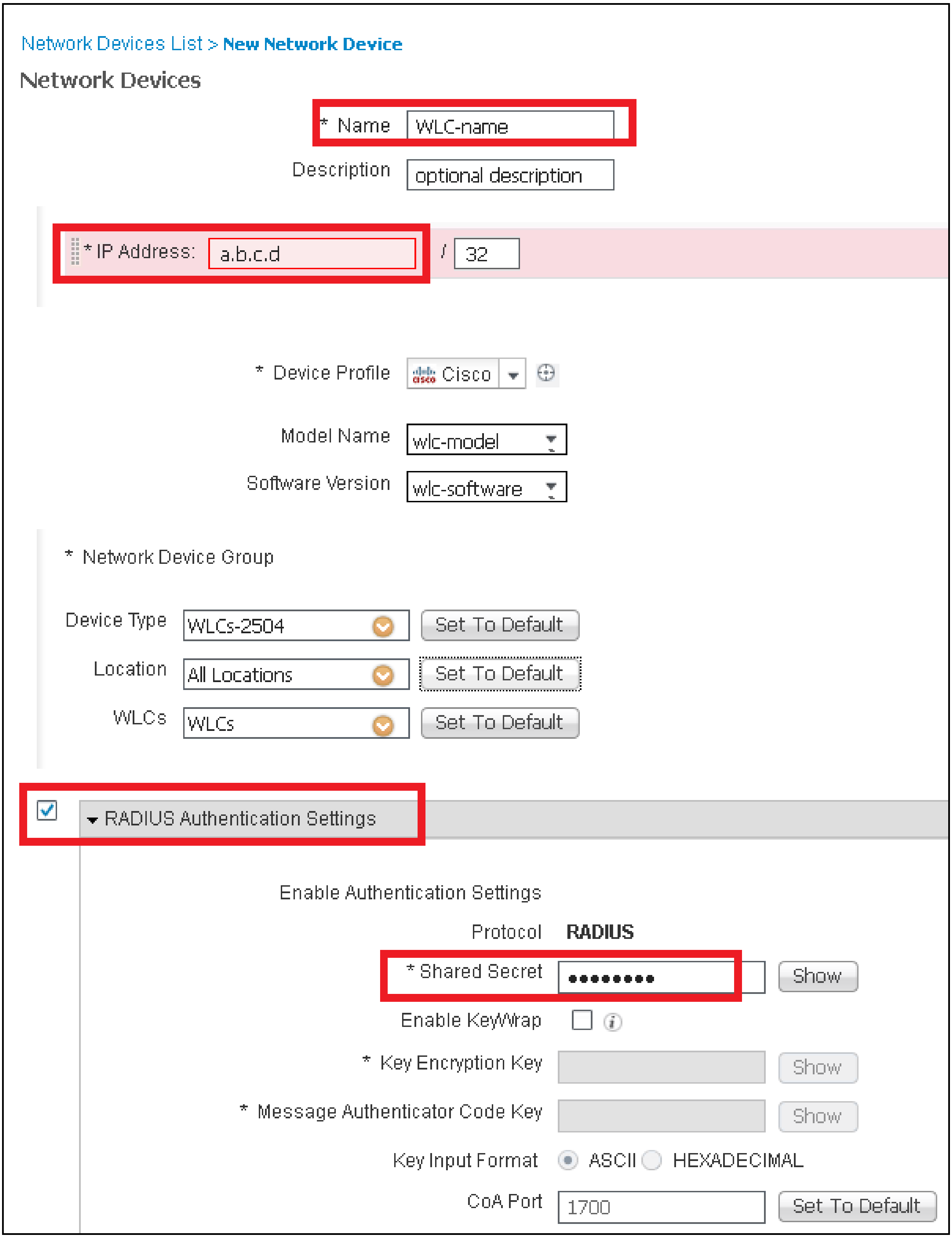


Step 2. Enter the information.

Optionally it can be specified a Model name, software version, description and assign Network

Device groups based on device types, location or WLCs.

a.b.c.d correspond to the ME's IP address.



Network Devices List > **New Network Device**

Network Devices

* Name: WLC-name

Description: optional description

* IP Address: a.b.c.d / 32

* Device Profile: Cisco

Model Name: wlc-model

Software Version: wlc-software

* Network Device Group

Device Type: WLCs-2504 — Set To Default

Location: All Locations — Set To Default

WLCs: WLCs — 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

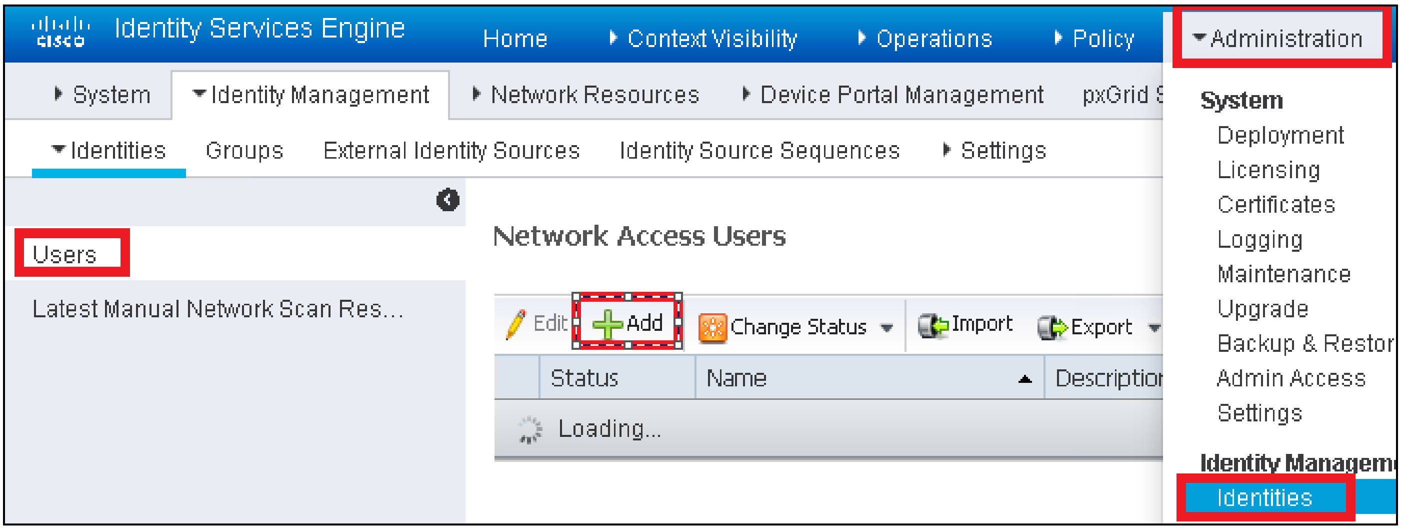
CoA Port: 1700 — Set To Default

For more information about Network Device Groups review this link:

[ISE - Network Device Groups](#)

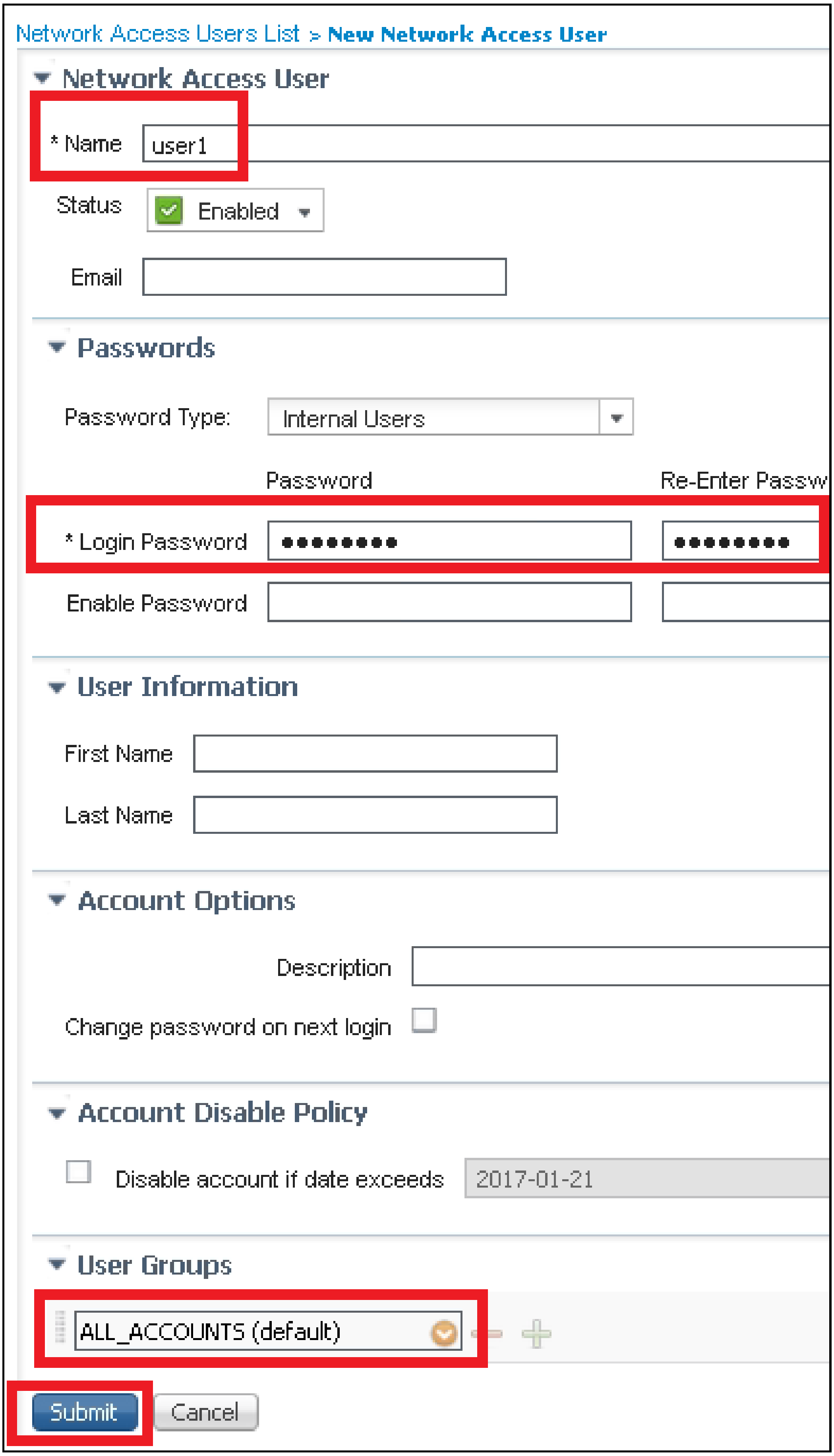
Create a new user on ISE

Step 1. Navigate to **Administration > Identity Management > Identities > Users > Add.**



Step 2. Enter the information.

In this example this user belongs to a group called ALL_ACCOUNTS but it can be adjusted as needed.



Network Access Users List > New Network Access User

Network Access User

* Name user1

Status ✓ Enabled

Email

Passwords

Password Type: Internal Users

	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 2017-01-21

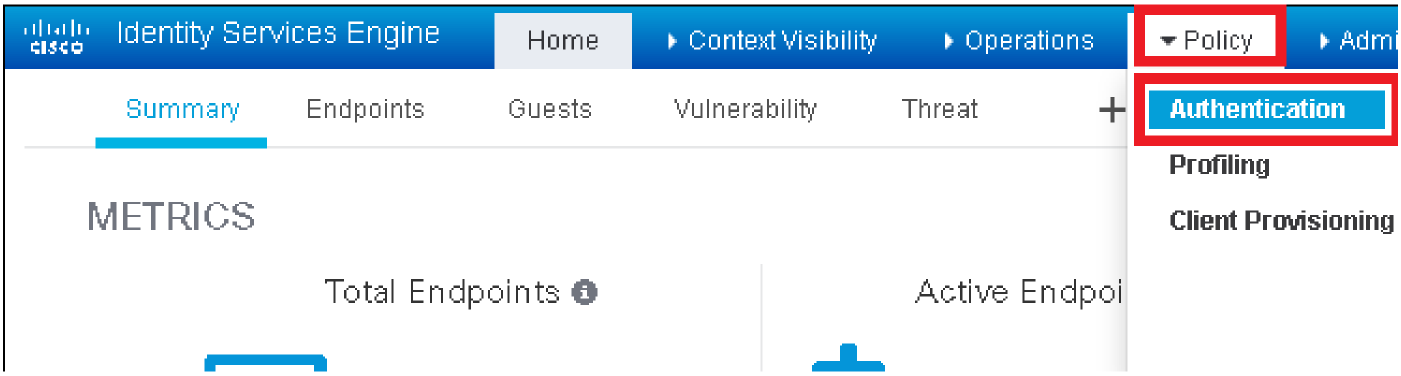
User Groups

ALL_ACCOUNTS (default)

Create the Authentication rule

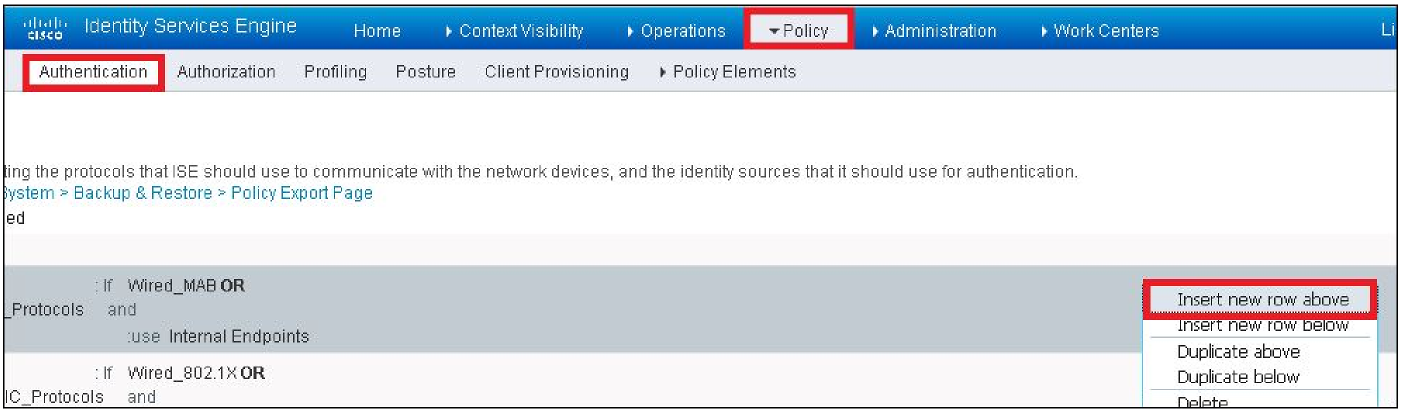
Authentication rules are used to verify if the credentials of the users are right (Verify if the user really is who it says it is) and limit the authentication methods that are allowed to be used by it.

Step 1. Navigate to **Policy > Authentication**.



Step 2. Insert a new authentication rule.

To do so navigate to **Policy > Authentication > Insert new row above/below.**



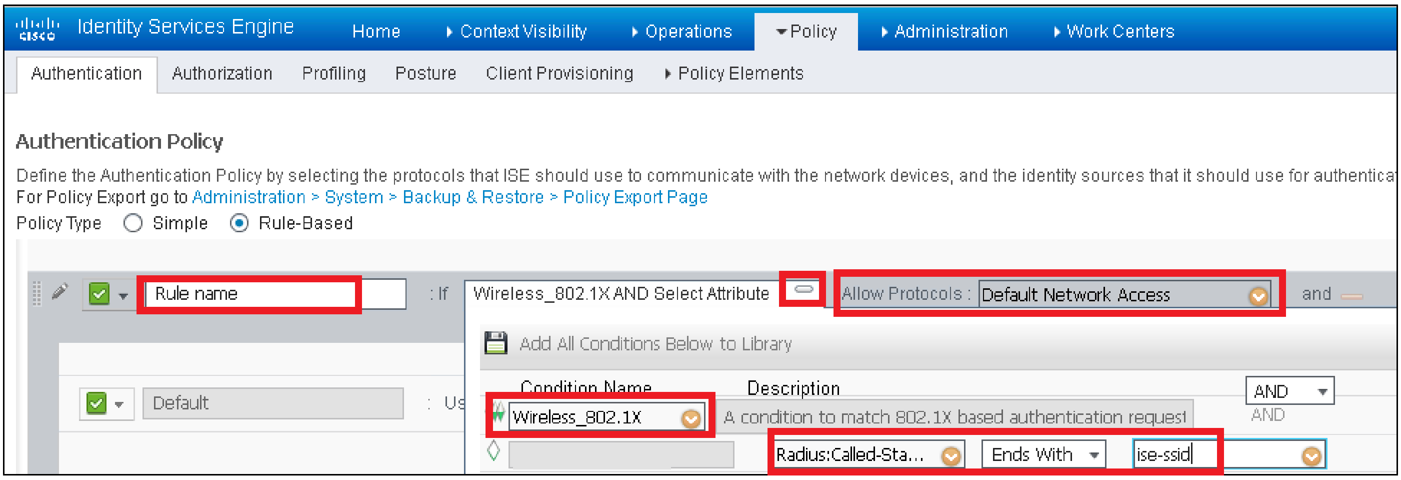
ing the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.
ystem > Backup & Restore > Policy Export Page
ed

: If Wired_MAB **OR**
_Protocols and
:use Internal Endpoints

: If Wired_802.1X **OR**
IC_Protocols and

Step 3. Enter the needed information

This authentication rule example allows all the protocols listed under the **Default Network Access** list, this applies to the authentication request for Wireless 802.1x clients and with Called-Station-ID and ends with *ise-ssid*.



Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentica
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Policy Type ○ Simple ● Rule-Based

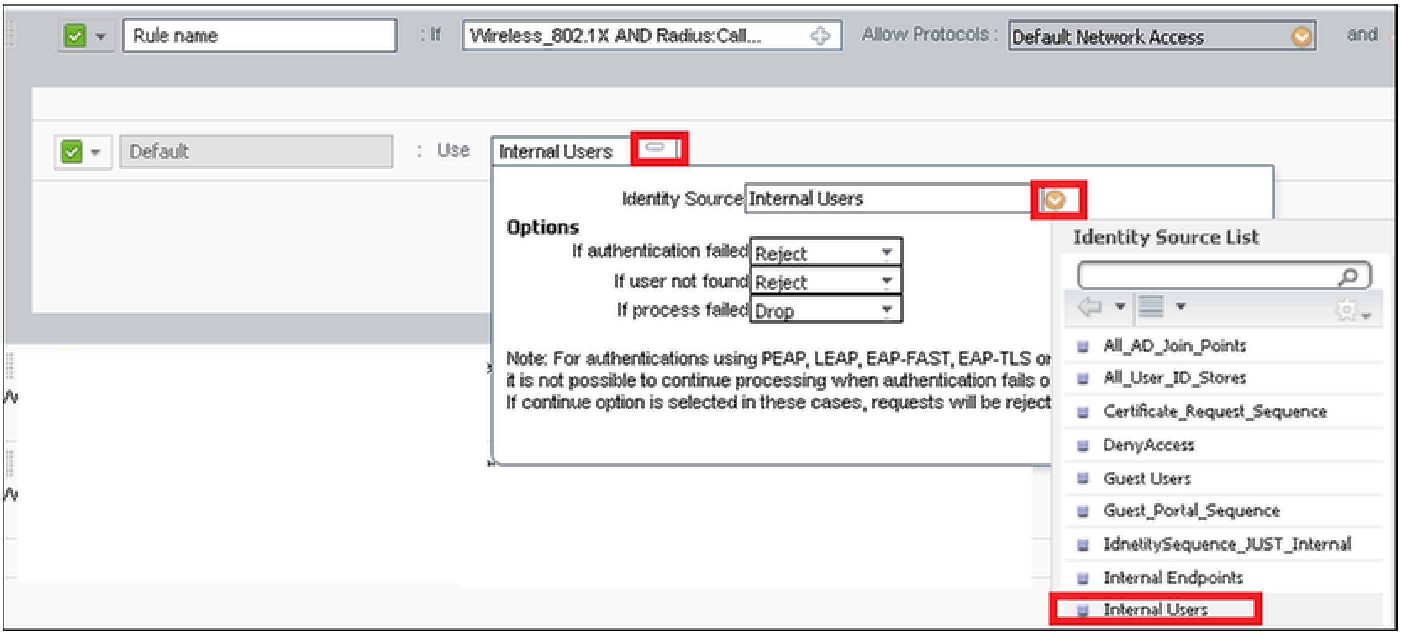
☑ Rule name : If Wireless_802.1X AND Select Attribute Allow Protocols : Default Network Access and

☑ Default : Us

Wireless_802.1X A condition to match 802.1X based authentication request

Radius:Called-Sta... Ends With ise-ssid

Also, choose the Identity source for the clients that matches this authentication rule, in this example it is used *Internal users*



Rule name : If Wireless_802.1X AND Radius:Call... Allow Protocols : Default Network Access and

Default : Use Internal Users

Identity Source Internal Users

Options

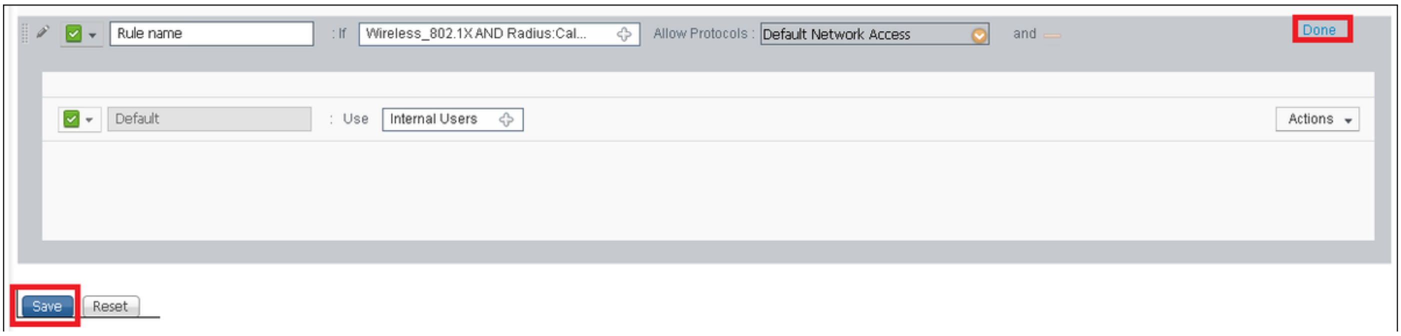
If authentication failed Reject

If user not found Reject

If process failed Drop

Note: For authentications using PEAP, LEAP, EAP-FAST, EAP-TLS or
it is not possible to continue processing when authentication fails o
If continue option is selected in these cases, requests will be reject

Once It is finished click **Done** and **Save**



Rule name : If Wireless_802.1X AND Radius:Cal... Allow Protocols : Default Network Access and

Default : Use Internal Users

For more information about Allow Protocols Policies consult this link:

Allowed Protocols Service

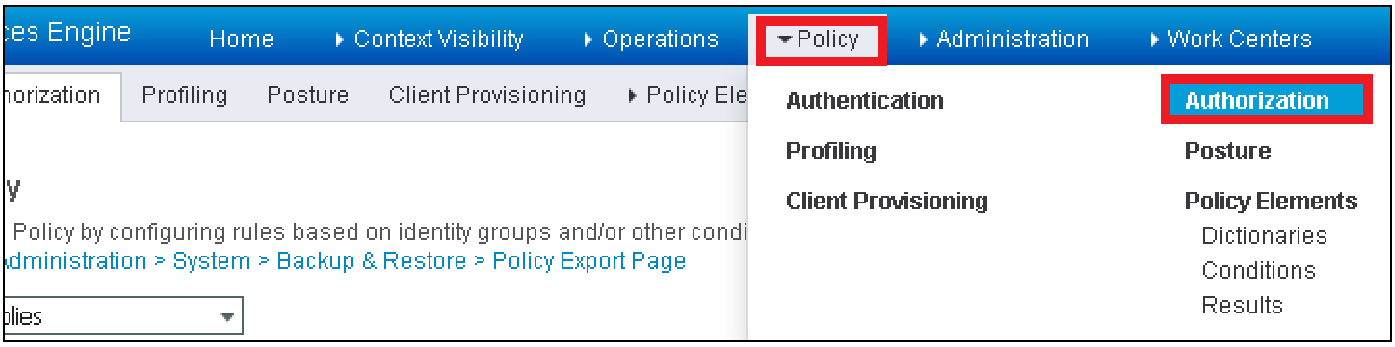
For more information about Identity sources consult this link:

Create a User Identity Group

Create the Authorization rule

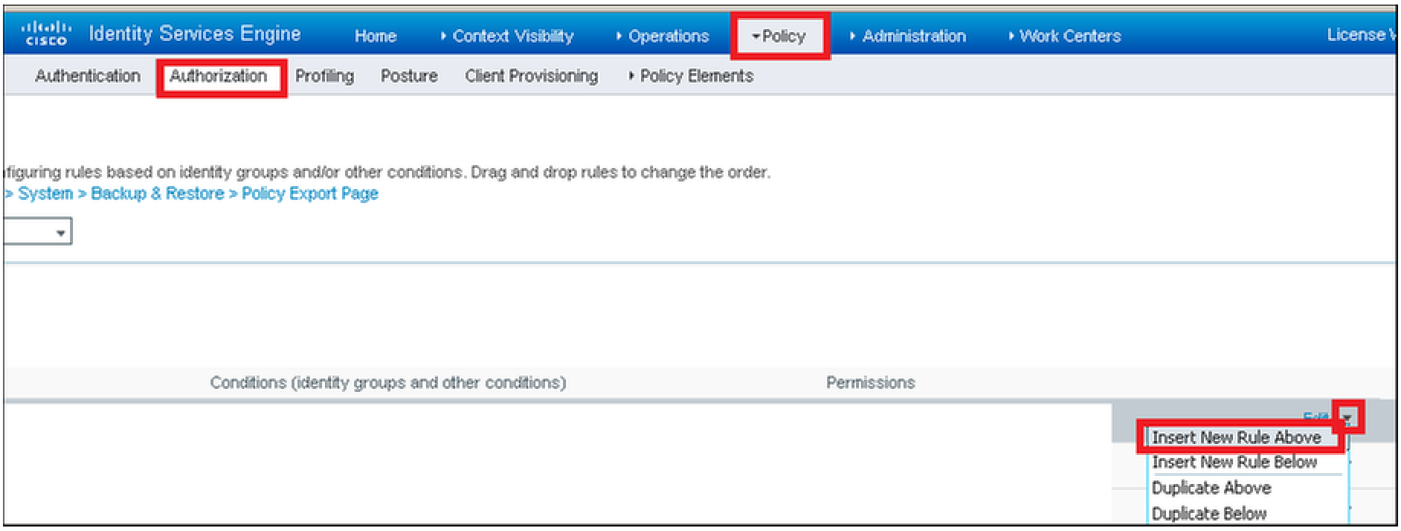
The authorization rule is the one in charge to determine if the client is allowed to join the network or not

Step 1. Navigate to **Policy > Authorization.**



Policy by configuring rules based on identity groups and/or other condi
Administration > System > Backup & Restore > Policy Export Page

Step 2. Insert a new rule. Navigate to **Policy > Authorization > Insert New Rule Above/Below.**

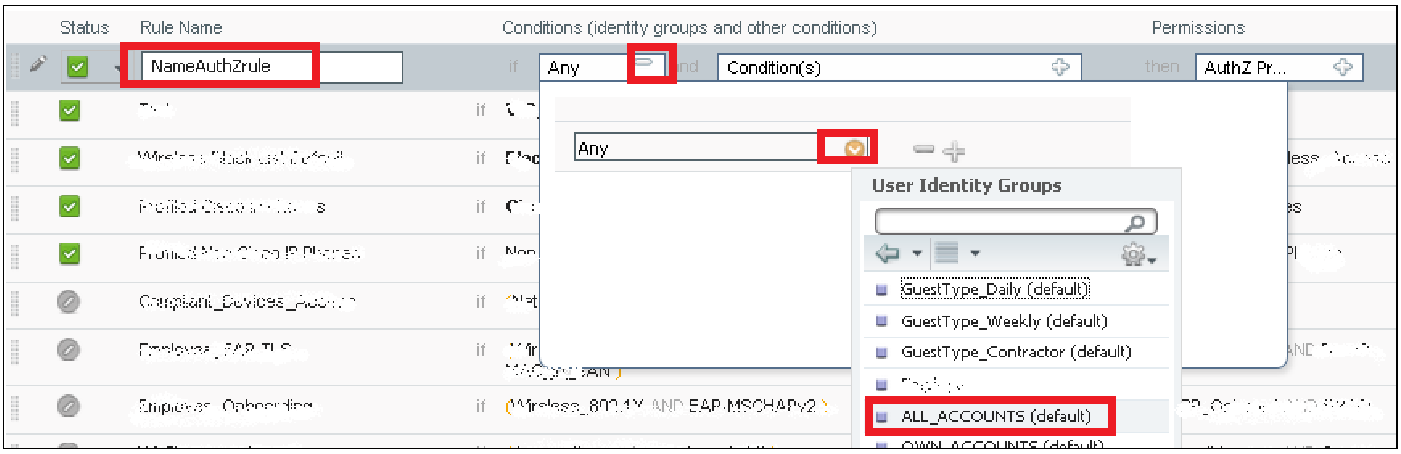


figuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

> System > Backup & Restore > Policy Export Page

Step 3. Enter the information.

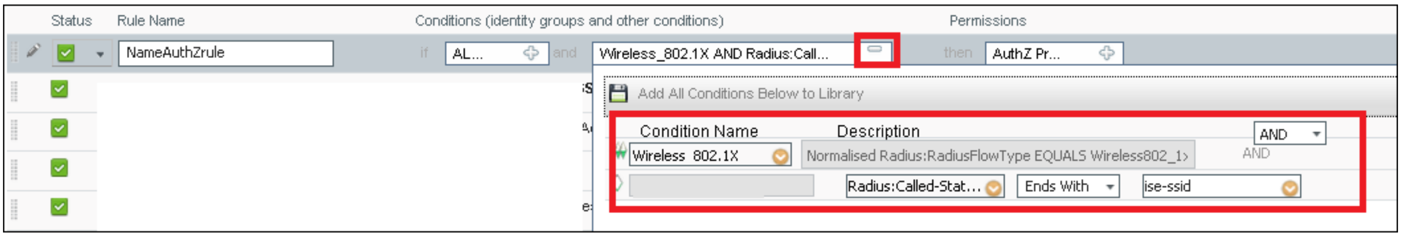
First choose a name for the rule and the Identity groups where the user is stored. In this example the user is stored in group *ALL_ACCOUNTS.*


Status
Rule Name
Conditions (identity groups and other conditions)
Permissions
User Identity Groups
GuestType_Daily (default)
GuestType_Weekly (default)
GuestType_Contractor (default)
ALL_ACCOUNTS (default)
OWN_ACCOUNTS (default)

Rule Name: NameAuthZrule if Any and Condition(s) then AuthZ Pr...

Any

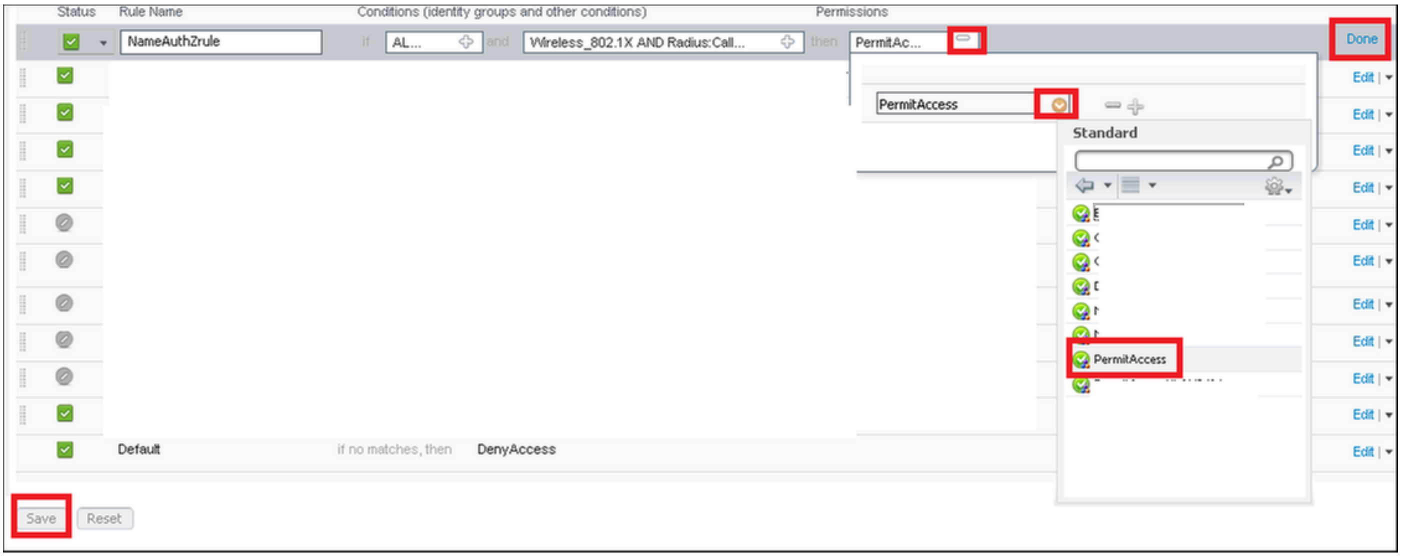
After that choose other conditions that make the authorization process to fall into this rule. In this example the authorization process hits this rule if it uses 802.1x Wireless and it is called station ID ends with *ise-ssid.*


Status
Rule Name
Conditions (identity groups and other conditions)
Permissions
Add All Conditions Below to Library
Condition Name
Description
AND

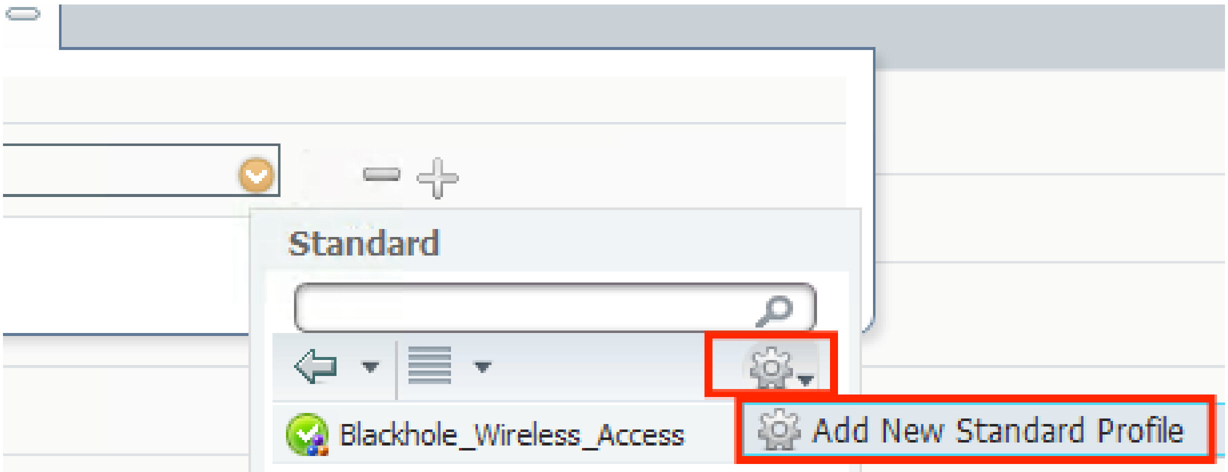
NameAuthZrule if AL... and Wireless_802.1X AND Radius:Call... then AuthZ Pr...

Condition Name	Description	AND
Wireless_802.1X	Normalised Radius:RadiusFlowType EQUALS Wireless802_1x	AND
	Radius:Called-Stat... Ends With ise-ssid	

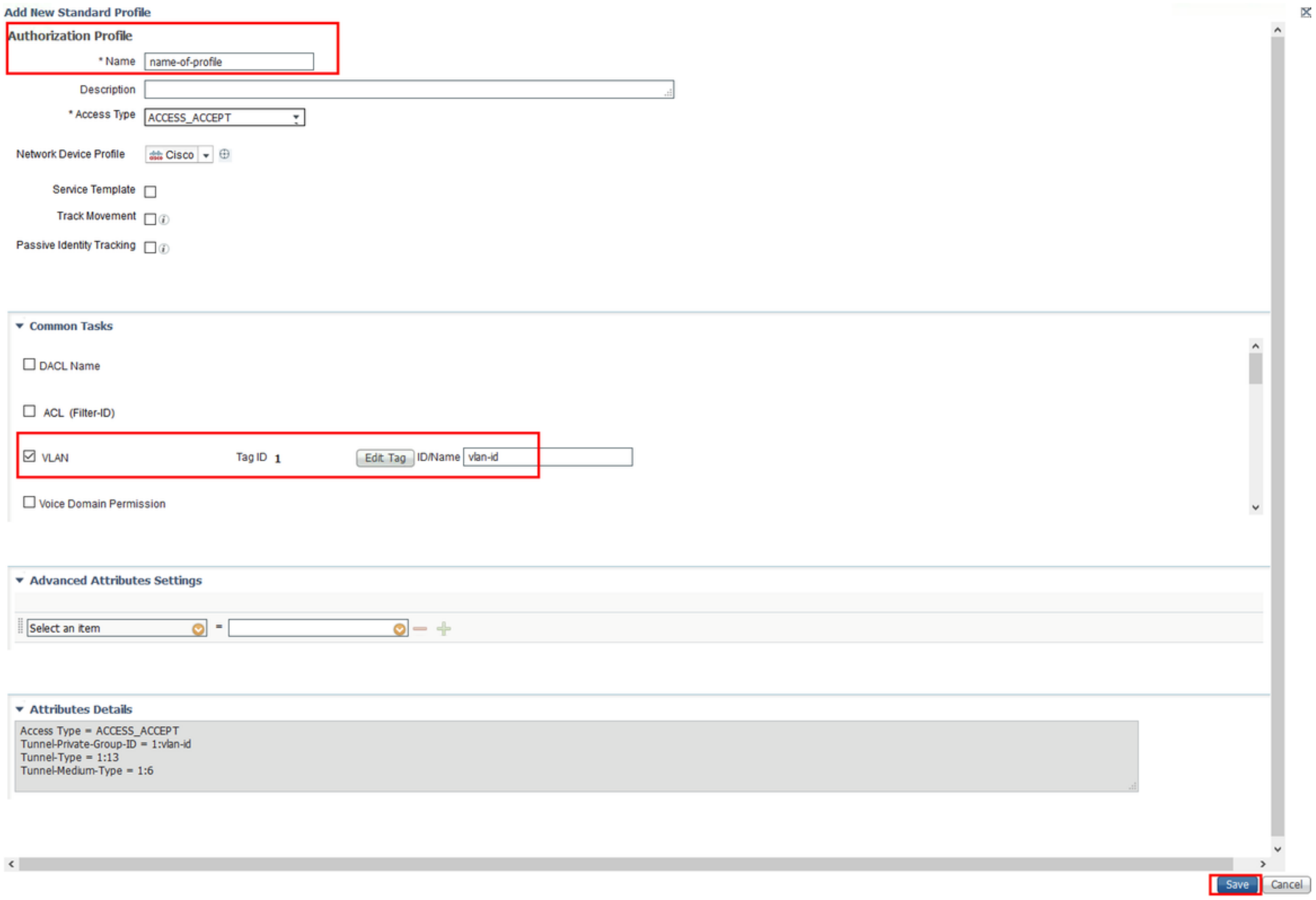
Finally choose the Authorization profile that allows the clients to join the network, click **Done** and **Save.**



Optionally, create a new authorization profile that will assign the wireless client to a different VLAN:



Enter the information:



Add New Standard Profile

Authorization Profile

* Name: name-of-profile

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template □

Track Movement □

Passive Identity Tracking □

Common Tasks

□ DACL Name

□ ACL (Filter-ID)

☑ VLAN Tag ID 1 Edit Tag ID/Name vlan-id

□ 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
```

Configuration of end device

Configure a Windows 10 laptop to connect to an SSID with 802.1x Authentication using PEAP/MS-CHAPv2 (Microsoft version of the Challenge-Handshake Authentication Protocol version 2).

In this configuration example ISE uses its self-signed certificate to perform the authentication.

To create the WLAN profile on the windows machine there are two options:

1. Install the self-signed certificate on the machine to validate and trust ISE server to complete the authentication
2. Bypass the validation of the RADIUS server and trust any RADIUS server used to perform the authentication (not recommended, as it can become a security issue)

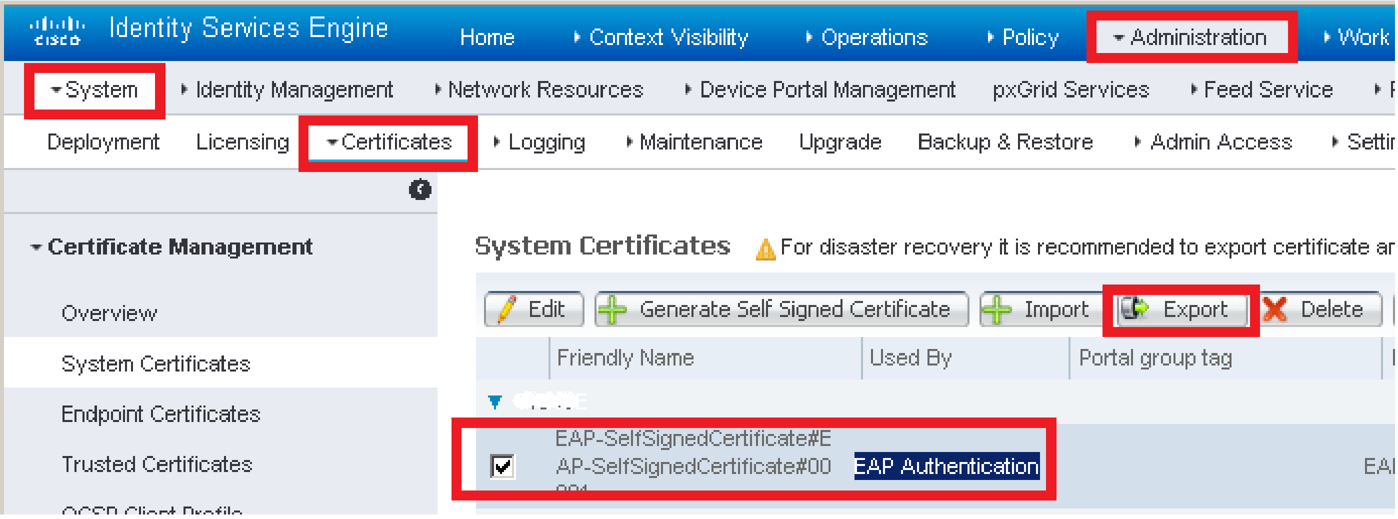
The configuration for these options are explained on End device configuration - Create the WLAN Profile - Step 7.

End device configuration - Install ISE self-signed certificate

Step 1. Export self-signed certificate from ISE.

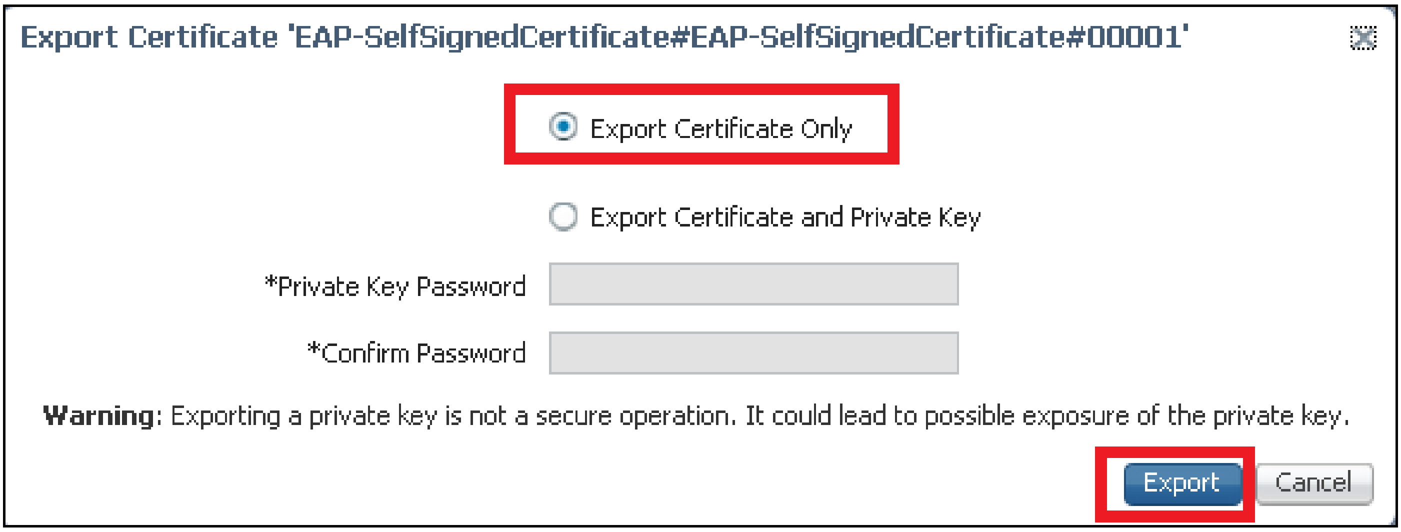
Log in to ISE and navigate to **Administration > System > Certificates > System Certificates**.

Then select the certificate used for **EAP Authentication** and click **Export.**



	Friendly Name	Used By	Portal group tag	
▼ [redacted]				
☑	EAP-SelfSignedCertificate#EAP-SelfSignedCertificate#00001	EAP Authentication		EAI

Save the certificate in the needed location. This certificate is installed on the Windows machine.


Export Certificate 'EAP-SelfSignedCertificate#EAP-SelfSignedCertificate#00001'

● Export Certificate Only

○ Export Certificate and Private Key

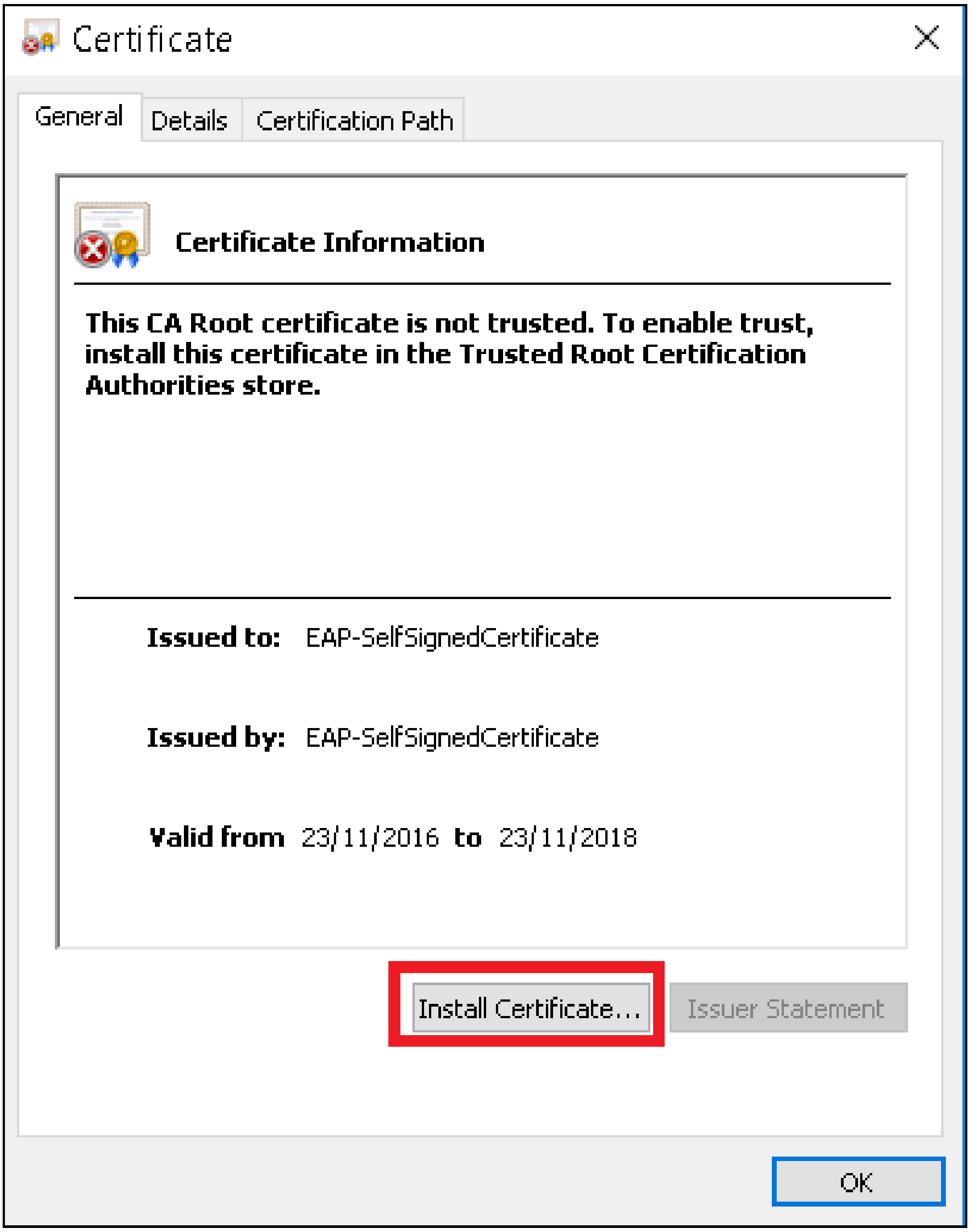
*Private Key Password

*Confirm Password

Warning: Exporting a private key is not a secure operation. It could lead to possible exposure of the private key.

Step 2. Install the certificate in the Windows machine.

Copy the certificate exported before into the Windows machine, change the extension of the file from .pem to .crt, after that double click on it and select **Install Certificate...**.



Certificate Information

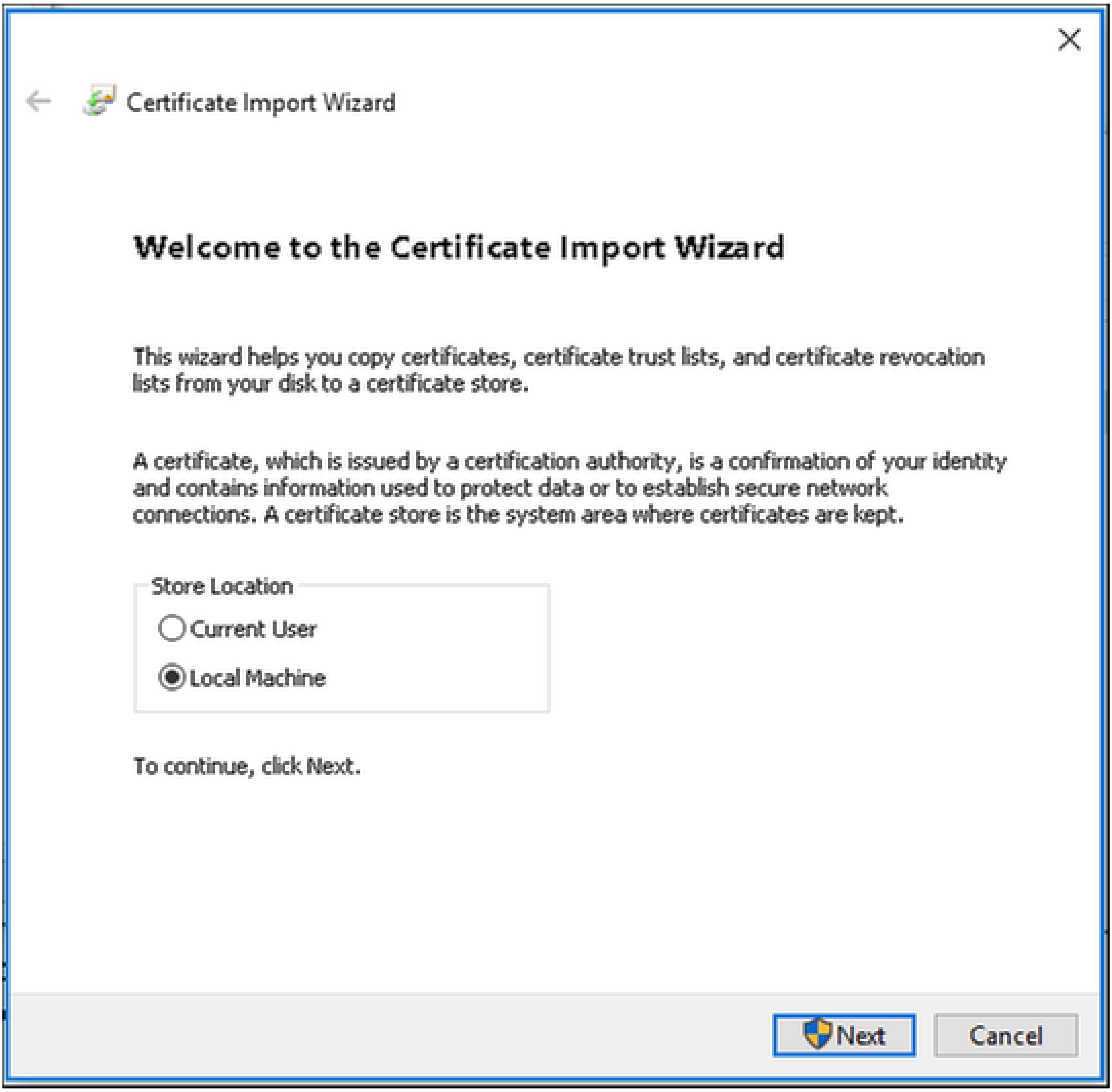
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: EAP-SelfSignedCertificate

Issued by: EAP-SelfSignedCertificate

Valid from 23/11/2016 to 23/11/2018

Choose to install it in **Local Machine,** then click **Next.**



Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

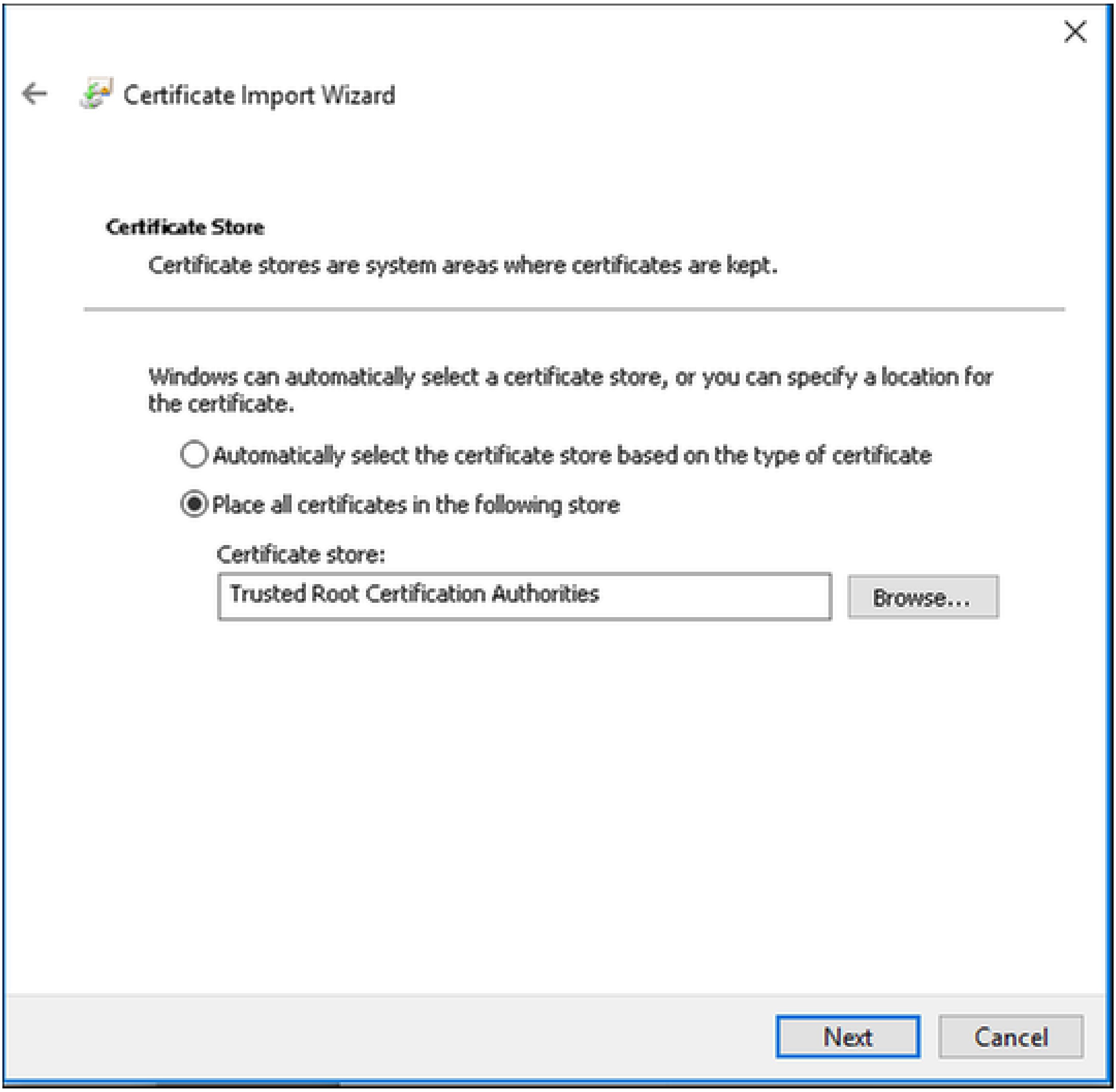
Store Location

○ Current User

● Local Machine

To continue, click Next.

Select **Place all certificates in the following store**, then browse and choose **Trusted Root Certification Authorities**. After that click **Next**.



Certificate Store

Certificate stores are system areas where certificates are kept.

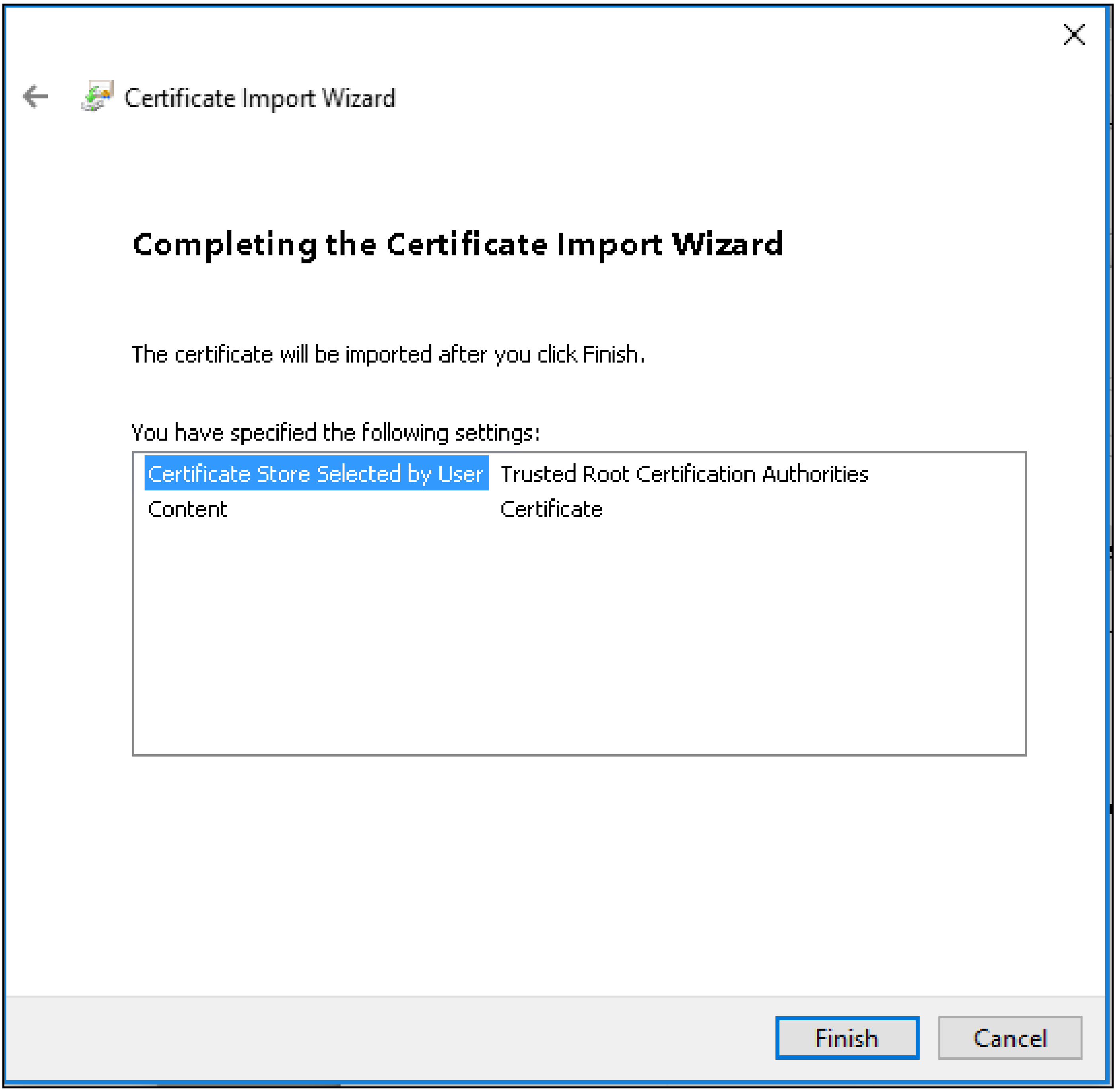
Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

Then click **Finish.**



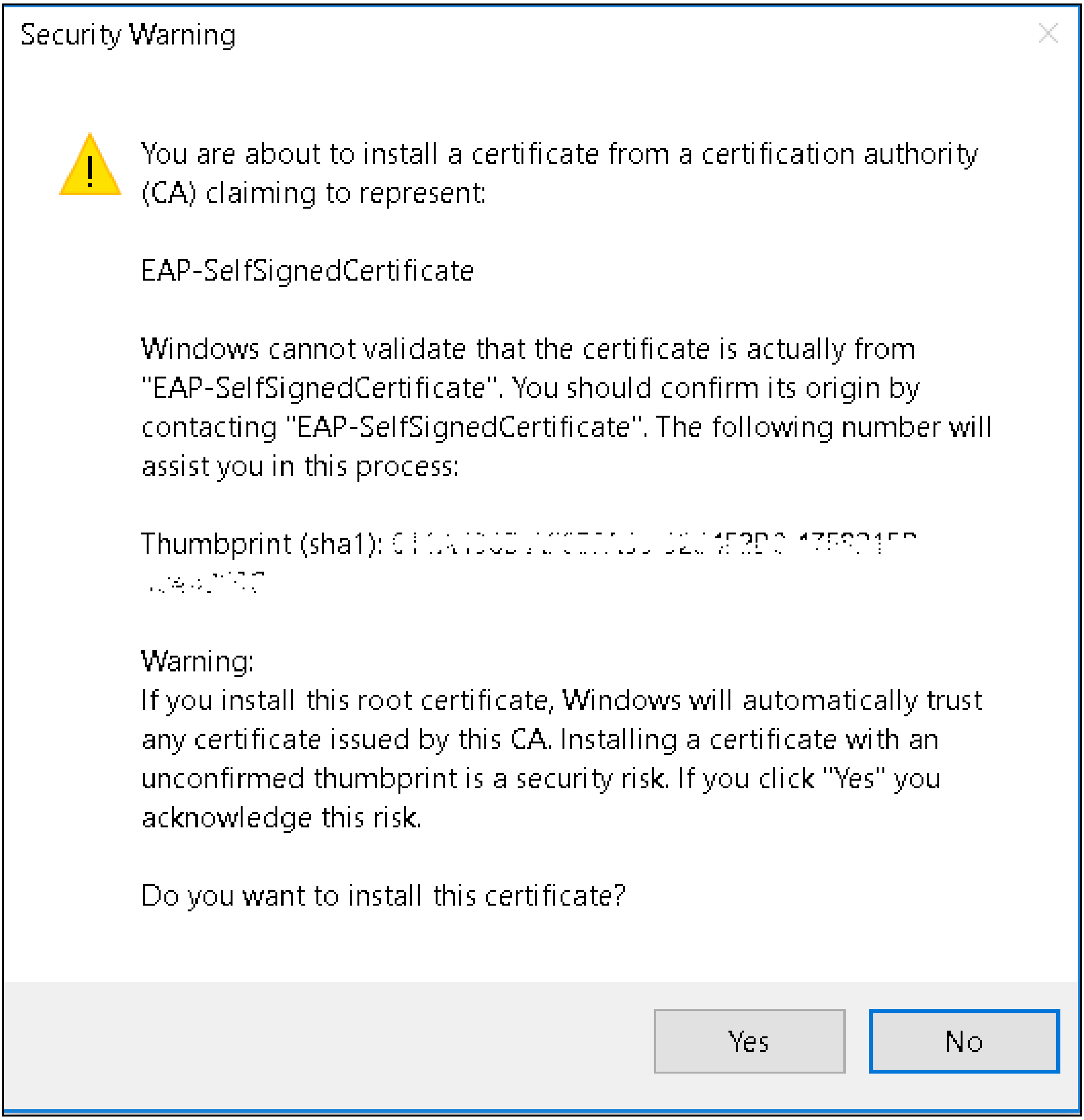
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate

At the end click **Yes** to confirm the installation of the certificate.



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

EAP-SelfSignedCertificate

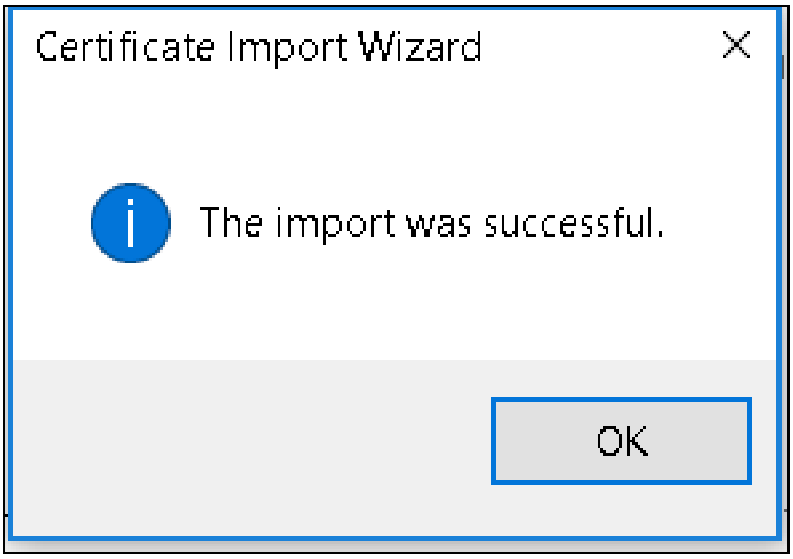
Windows cannot validate that the certificate is actually from "EAP-SelfSignedCertificate". You should confirm its origin by contacting "EAP-SelfSignedCertificate". The following number will assist you in this process:

Thumbprint (sha1): [redacted]

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?

Finally click **OK.**

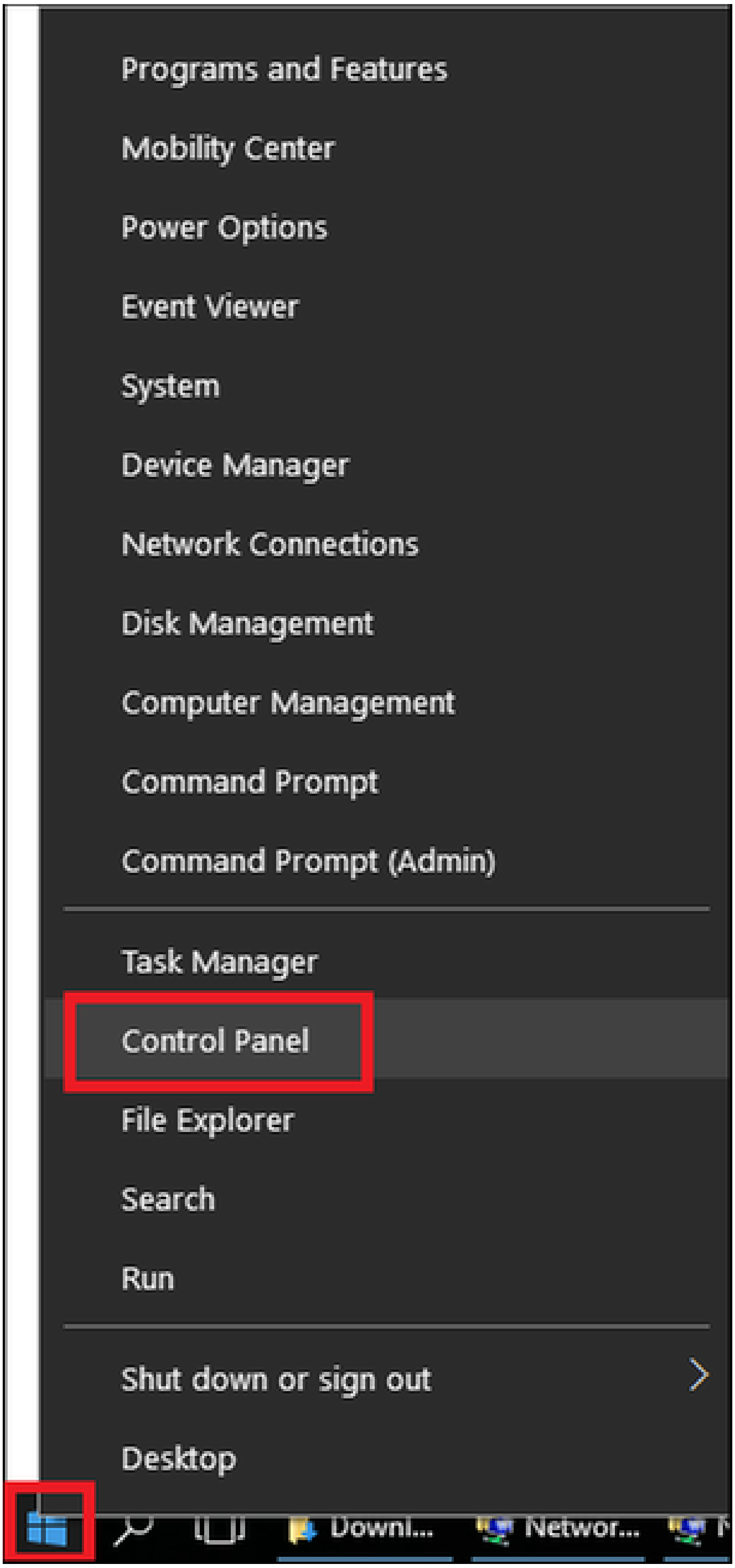


Certificate Import Wizard

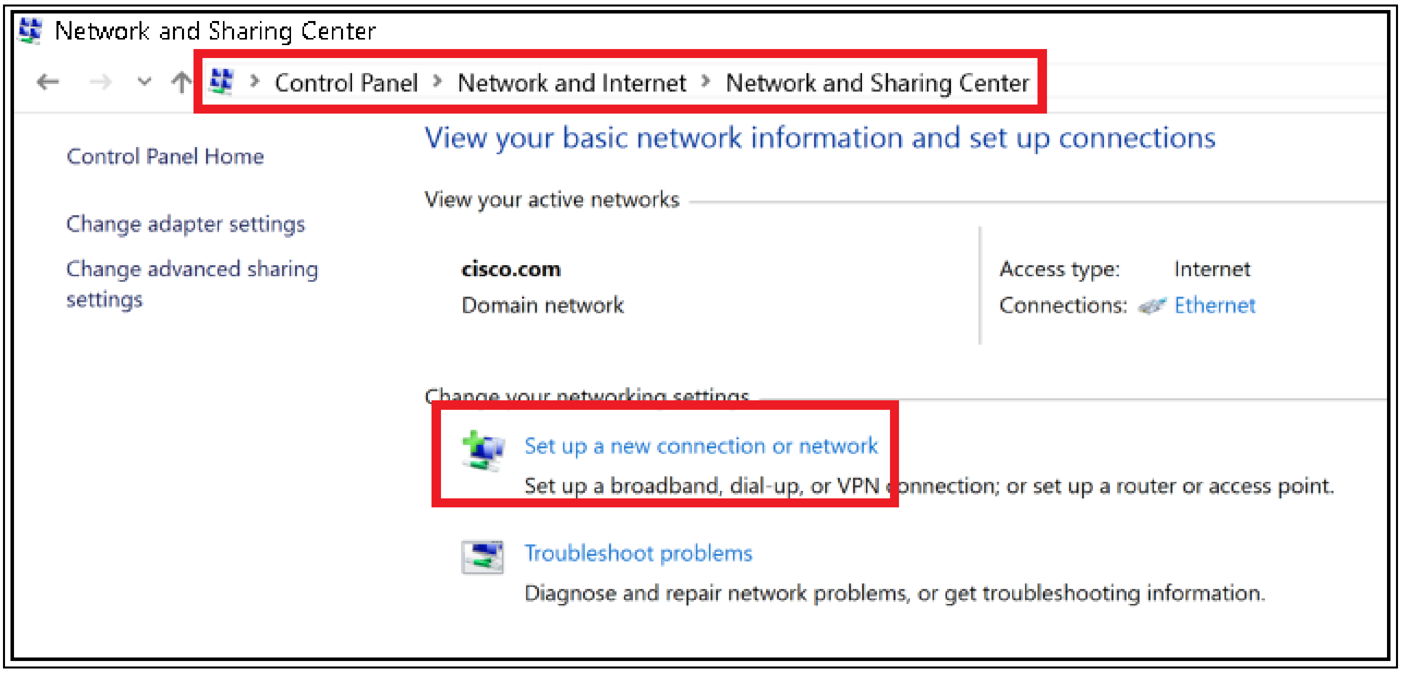
The import was successful.

End device configuration - Create the WLAN Profile

Step 1. Right click on **Start** icon and select **Control panel.**



Step 2. Navigate to **Network and Internet** and then to **Network and Sharing Center** and click on **Set up a new connection or network.**



Network and Sharing Center

Control Panel > Network and Internet > Network and Sharing Center

Control Panel Home

Change adapter settings

Change advanced sharing settings

View your basic network information and set up connections

View your active networks

cisco.com
Domain network

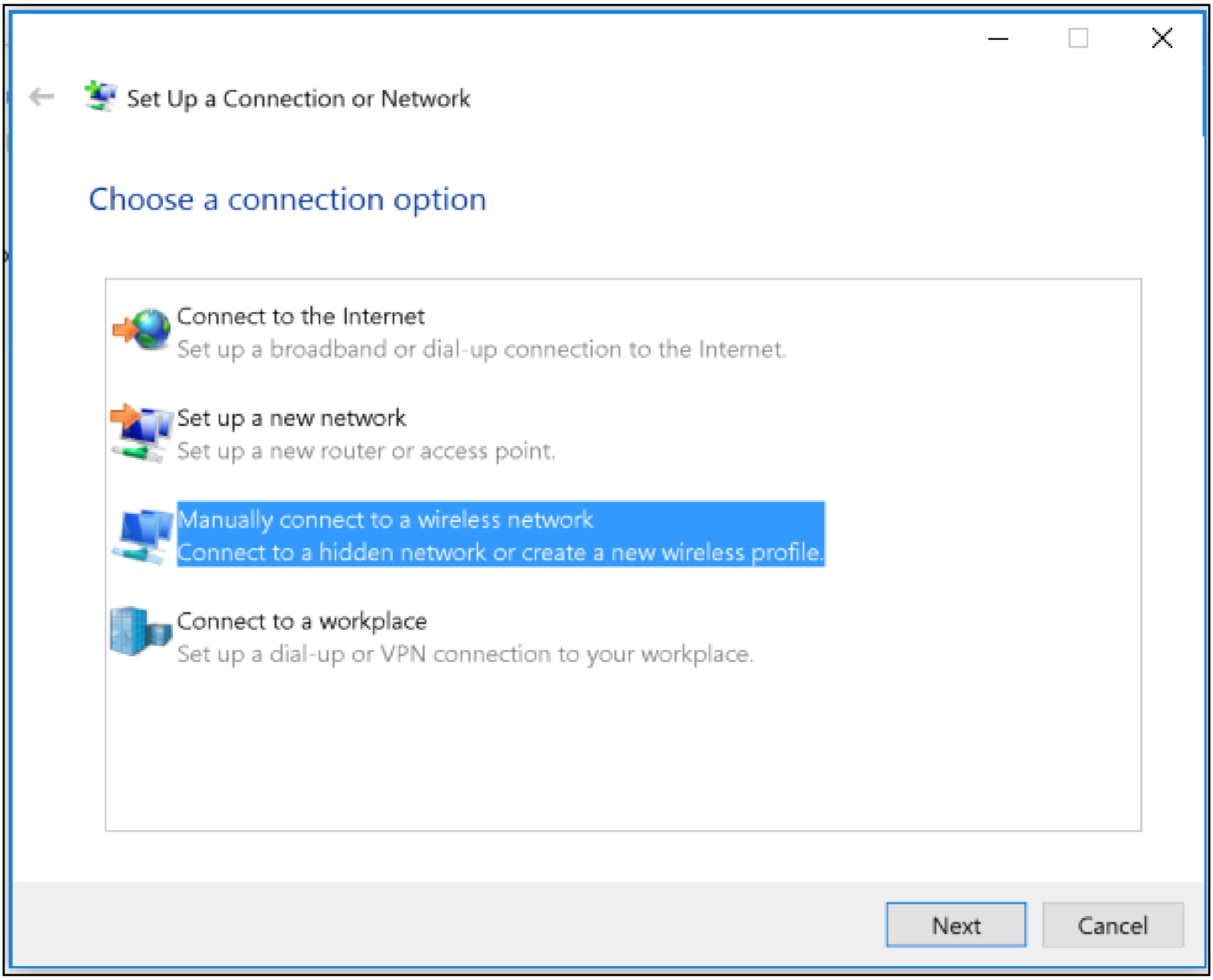
Access type: Internet
Connections: Ethernet

Change your networking settings

Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

Step 3. Select **Manually connect to a wireless network** and click **Next**.



Set Up a Connection or Network

Choose a connection option

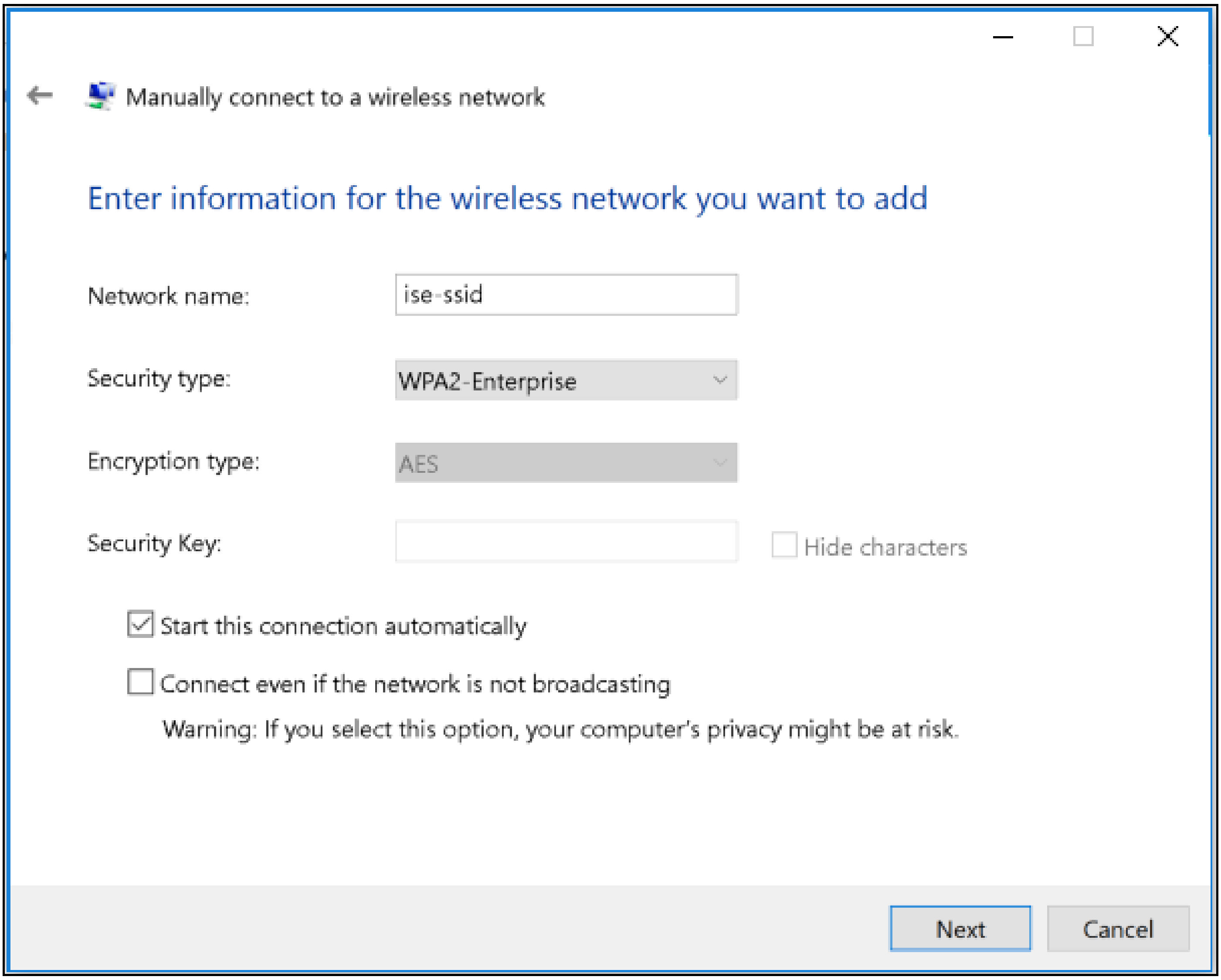
Connect to the Internet
Set up a broadband or dial-up connection to the Internet.

Set up a new network
Set up a new router or access point.

Manually connect to a wireless network
Connect to a hidden network or create a new wireless profile.

Connect to a workplace
Set up a dial-up or VPN connection to your workplace.

Step 4. Enter the information with the name of the SSID and security type WPA2-Enterprise and click **Next**.



Manually connect to a wireless network

Enter information for the wireless network you want to add

Network name: ise-ssid

Security type: WPA2-Enterprise

Encryption type: AES

Security Key:

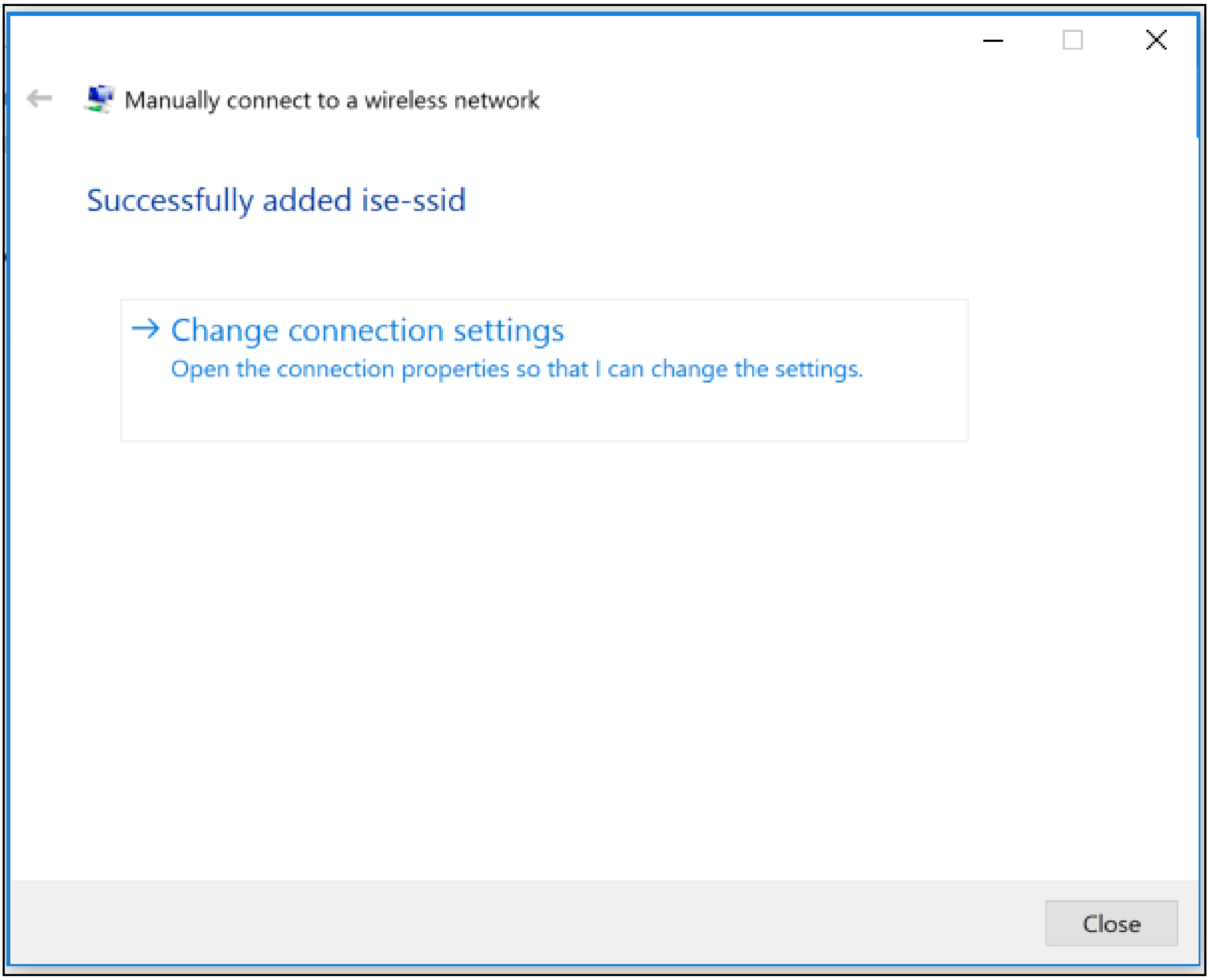
□ Hide characters

☑ 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.

Step 5. Select **Change connection settings** to customize the configuration of the WLAN profile.



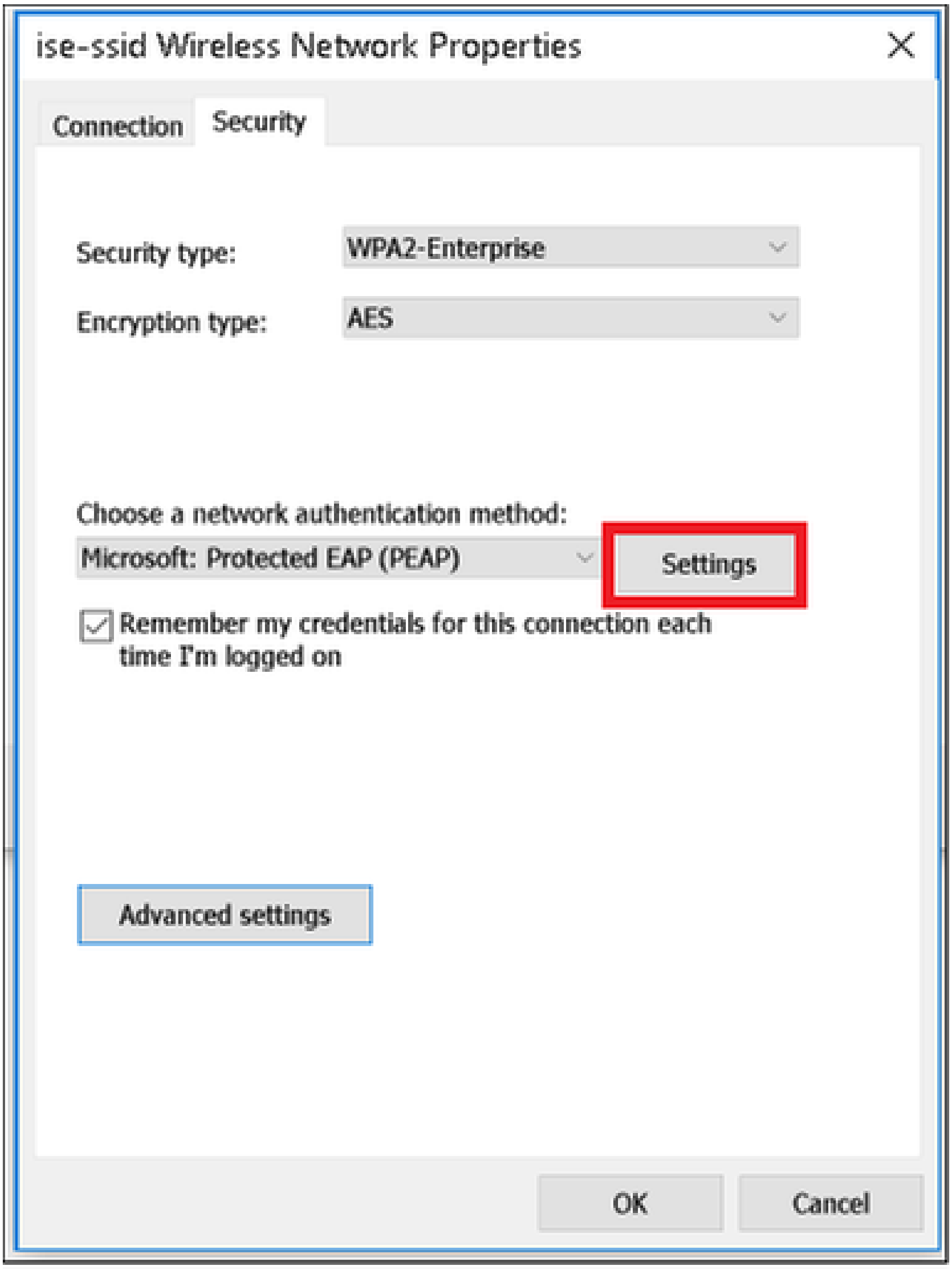
Manually connect to a wireless network

Successfully added ise-ssid

→ Change connection settings

Open the connection properties so that I can change the settings.

Step 6. Navigate to **Security** tab and click **Settings.**



ise-ssid Wireless Network Properties

Security type: WPA2-Enterprise

Encryption type: AES

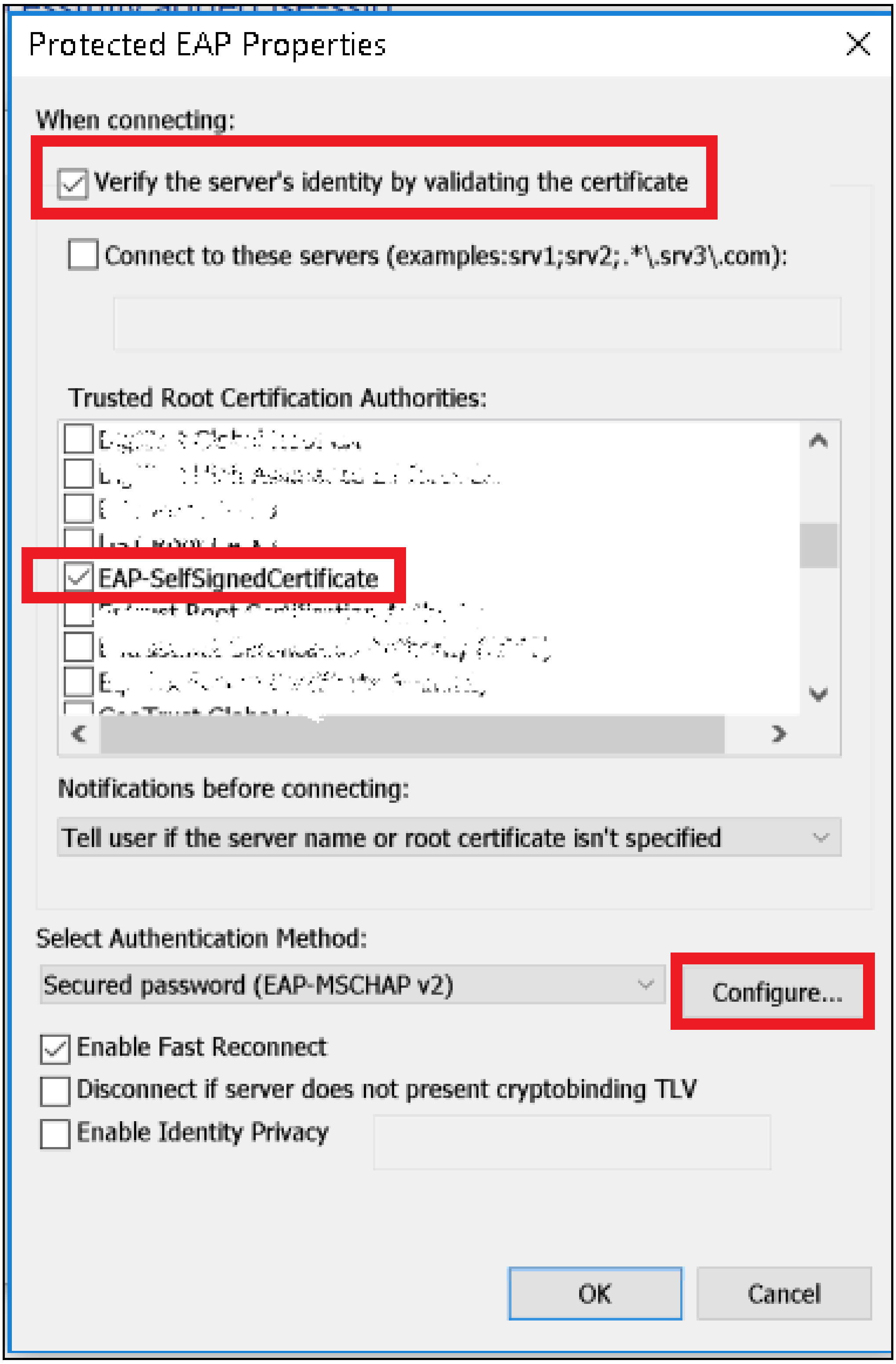
Choose a network authentication method: Microsoft: Protected EAP (PEAP)

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

Step 7. Choose if RADIUS server is validated or not.

If yes, enable **Verify the server's identity by validating the certificate** and from **Trusted Root Certification Authorities:** list select the self-signed certificate of ISE.

After that select **Configure** and disable **Automatically use my Windows logon name and password...**, then click **OK**



Protected EAP Properties

When connecting:

☑ Verify the server's identity by validating the certificate

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

Trusted Root Certification Authorities:

□ [redacted]
□ [redacted]
□ [redacted]
□ [redacted]
☑ EAP-SelfSignedCertificate
□ [redacted]
□ [redacted]
□ [redacted]
□ [redacted]

Notifications before connecting:

Tell user if the server name or root certificate isn't specified

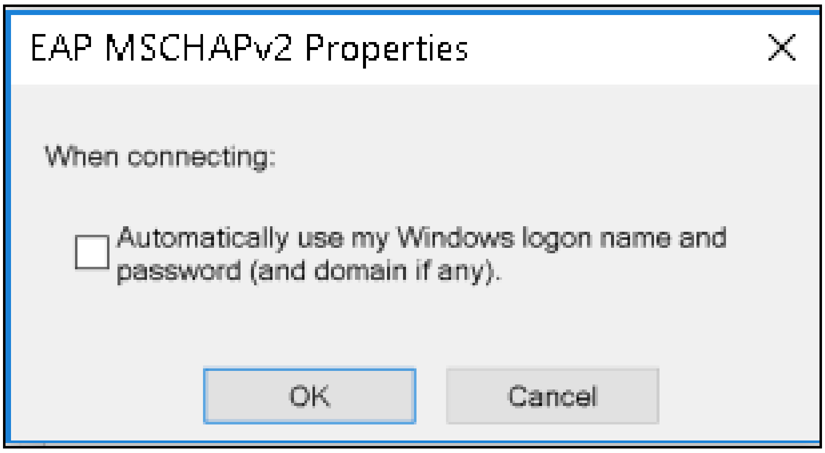
Select Authentication Method:

Secured password (EAP-MSCHAP v2)

☑ Enable Fast Reconnect

□ Disconnect if server does not present cryptobinding TLV

□ Enable Identity Privacy



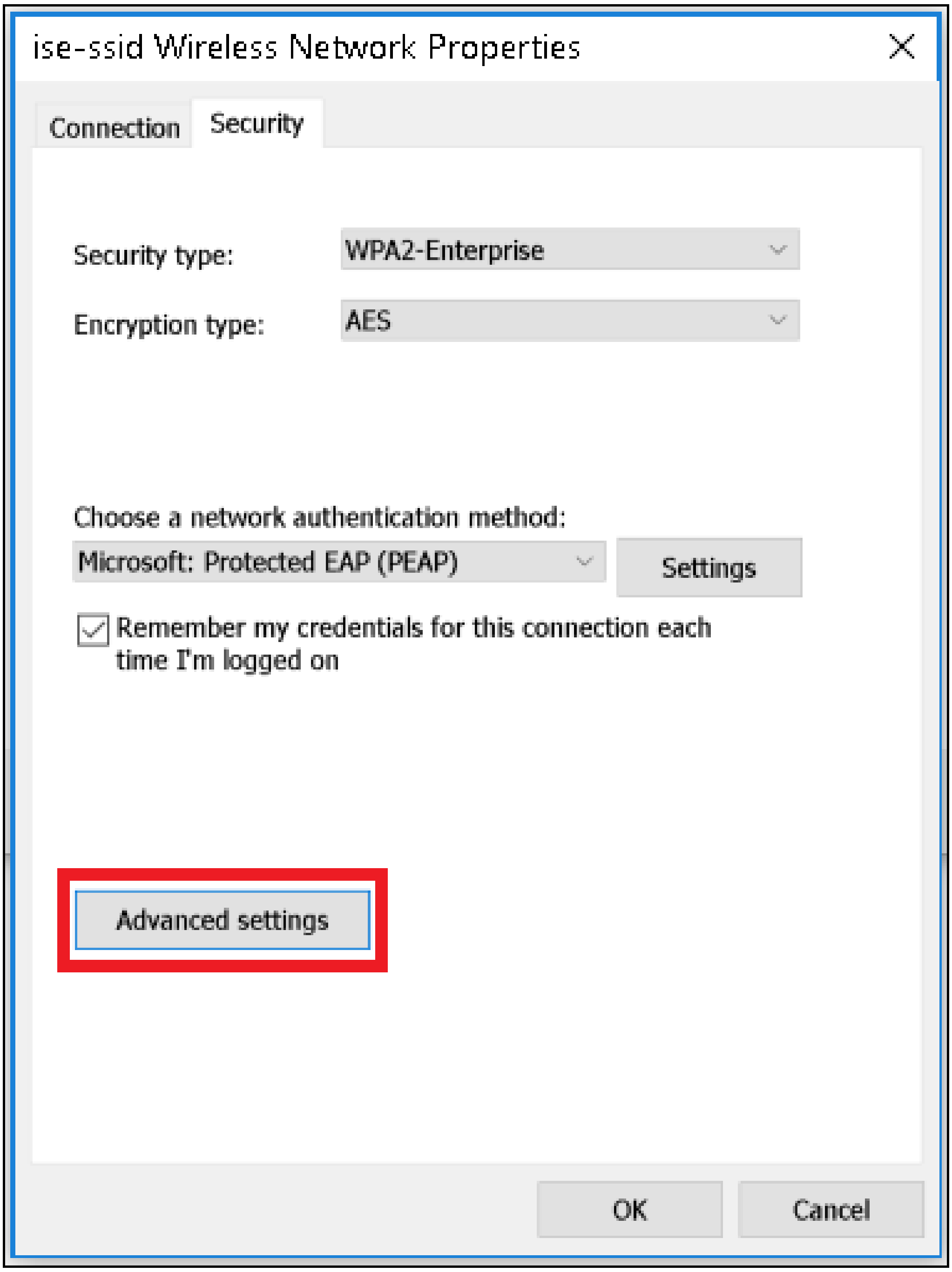
EAP MSCHAPv2 Properties

When connecting:

□ Automatically use my Windows logon name and password (and domain if any).

Step 8. Configure the user credentials

Once back to **Security** tab, select **Advanced settings**, specify authentication mode as **User authentication** and save the credentials that were configured on ISE to authenticate the user.



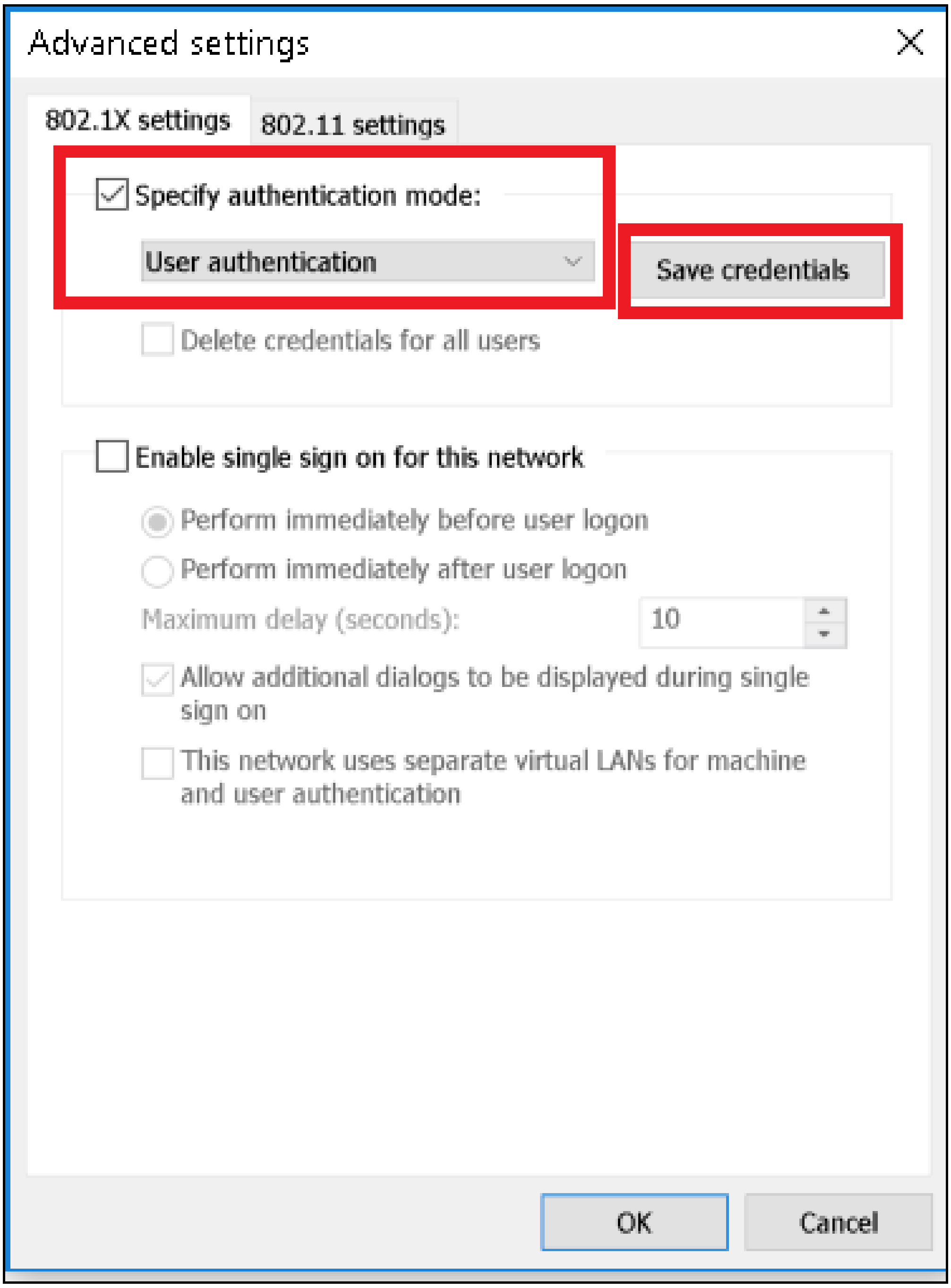
ise-ssid Wireless Network Properties

Security type: WPA2-Enterprise

Encryption type: AES

Choose a network authentication method: Microsoft: Protected EAP (PEAP)

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



Advanced settings

☑ Specify authentication mode:

User authentication

□ Delete credentials for all users

□ Enable single sign on for this network

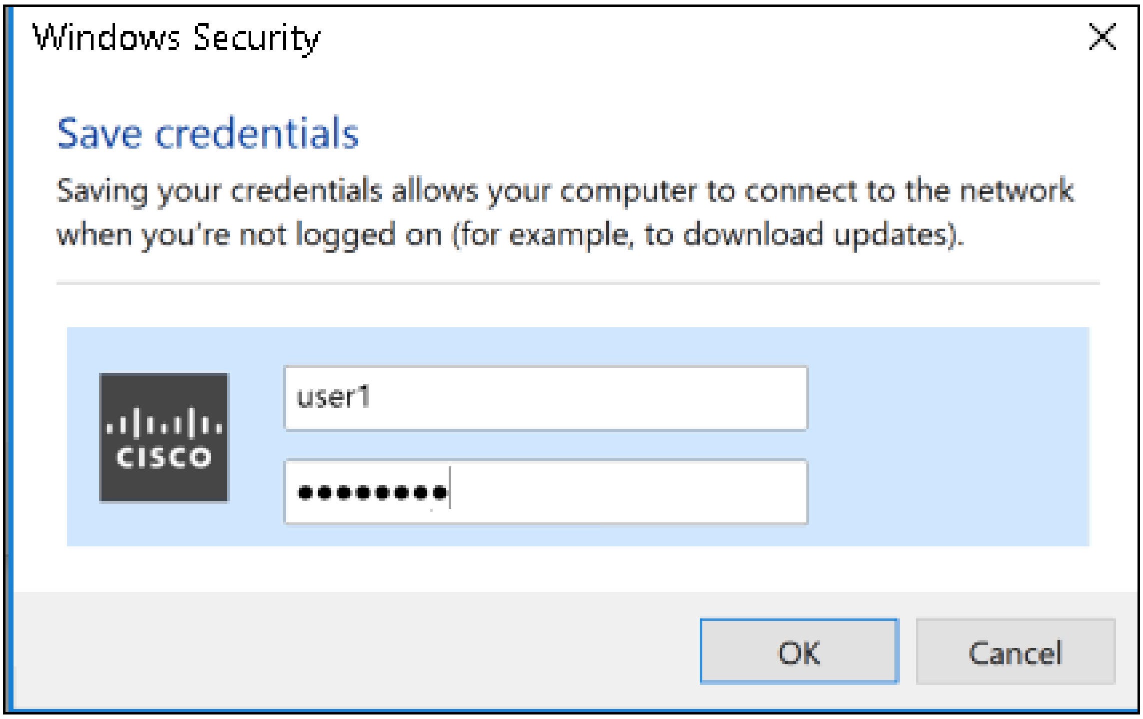
● Perform immediately before user logon

○ 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



Windows Security

Save credentials

Saving your credentials allows your computer to connect to the network when you're not logged on (for example, to download updates).

user1

●●●●●●●●

Verify

The authentication flow can be verified from WLC or from ISE perspective.

Authentication process on ME

Run this command to monitor the authentication process for a specific user:

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

Example of a successful authentication (some output has been omitted):

```
*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
```

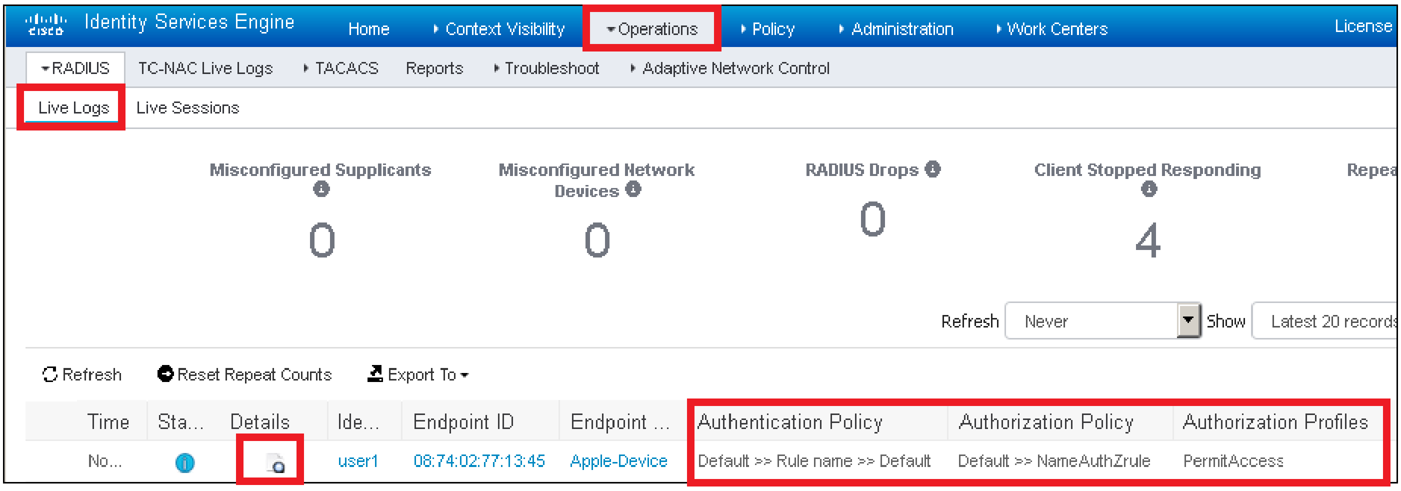
```
on AP 38:ed:18:c6:7b:40, slot 1, interface = 1, QOS = 0
IPv4 ACL ID = 255, IPv
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) mobility role
update request from Unassociated to Local
Peer = 0.0.0.0, Old Anchor = 0.0.0.0, New Anchor = 172.16.0.136
*apfReceiveTask: Nov 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)
```

For an easy way to read debug client outputs, use the *Wireless debug analyzer* tool:

Wireless Debug Analyzer

Authentication process on ISE

Navigate to **Operations > RADIUS > Live Logs** in order to see which authentication policy, authorization policy and authorization profile assigned to the user.



Misconfigured Supplicants 0

Misconfigured Network Devices 0

RADIUS Drops 0

Client Stopped Responding 4

Repea

Refresh Never

Show Latest 20 records

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

For more information click on **Details** to see a more detailed authentication process.