Configure EAP-TLS on 9800 WLC with ISE Internal CA

Contents

Introduction

This document describes EAP-TLS authentication using the Certificate Authority of Identity Services Engine to authenticate users.

Prerequisites

Components Used

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

- Wireless controller: C9800-40-K9 running 17.09.04a
- Cisco ISE: Running Version 3 Patch 4
- AP Model: C9130AXI-D
- Switch: 9200-L-24P

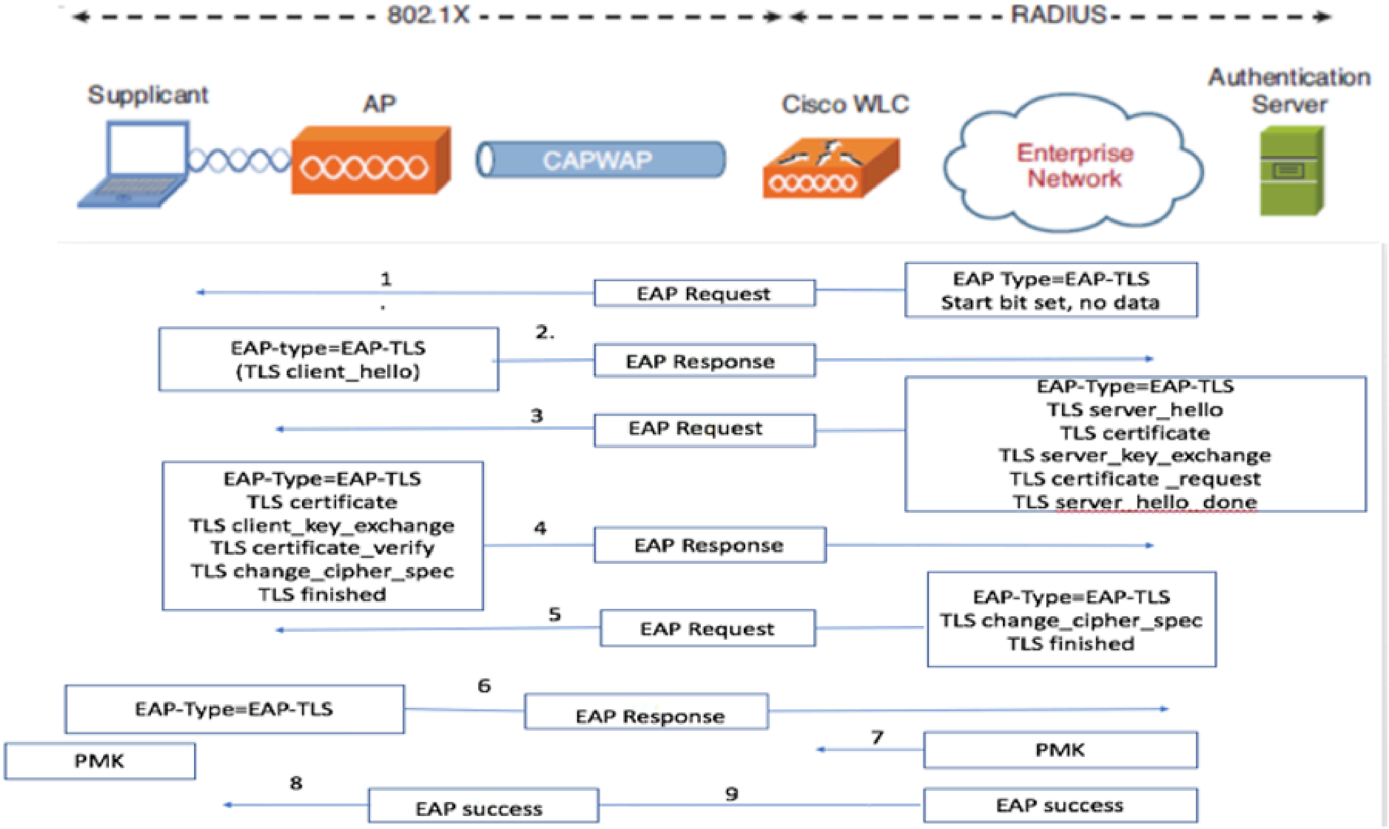
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Most organizations have their own CA that issues certificates to end users for EAP-TLS authentication. ISE includes an inbuilt certificate authority that can be used to generate certificates for users to be used in EAP-TLS authentication. In scenarios where using a full-fledged CA is not feasible, utilizing the ISE CA for user authentication becomes advantageous.

This document outlines the configuration steps required to effectively use the ISE CA to authenticate wireless users. EAP-TLS Authentication flow

EAP-TLS Authentication Flow



EAP-TLS Authentication Flow

Steps in the EAP-TLS Flow

1. The wireless client associates with the Access Point (AP).
2. At this stage, the AP does not permit data transmission and sends an authentication request.
3. The client, acting as the supplicant, responds with an EAP-Response Identity.
4. The Wireless LAN Controller (WLC) forwards the user ID information to the Authentication Server.
5. The RADIUS server replies to the client with an EAP-TLS Start Packet.
6. The EAP-TLS conversation begins from this point.
7. The client sends an EAP-Response back to the authentication server, including a **client_hello** handshake message with a cipher set to NULL.
8. The authentication server responds with an Access-Challenge packet containing:

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

9. The client replies with an EAP-Response message that includes:

```
Certificate (for server validation)
Client_key_exchange
Certificate_verify (to verify server trust)
Change_cipher_spec
TLS finished
```

10. Upon successful client authentication, the RADIUS server sends an Access-Challenge containing:

```
Change_cipher_spec
Handshake finished message
```

11. The client verifies the hash to authenticate the RADIUS server.

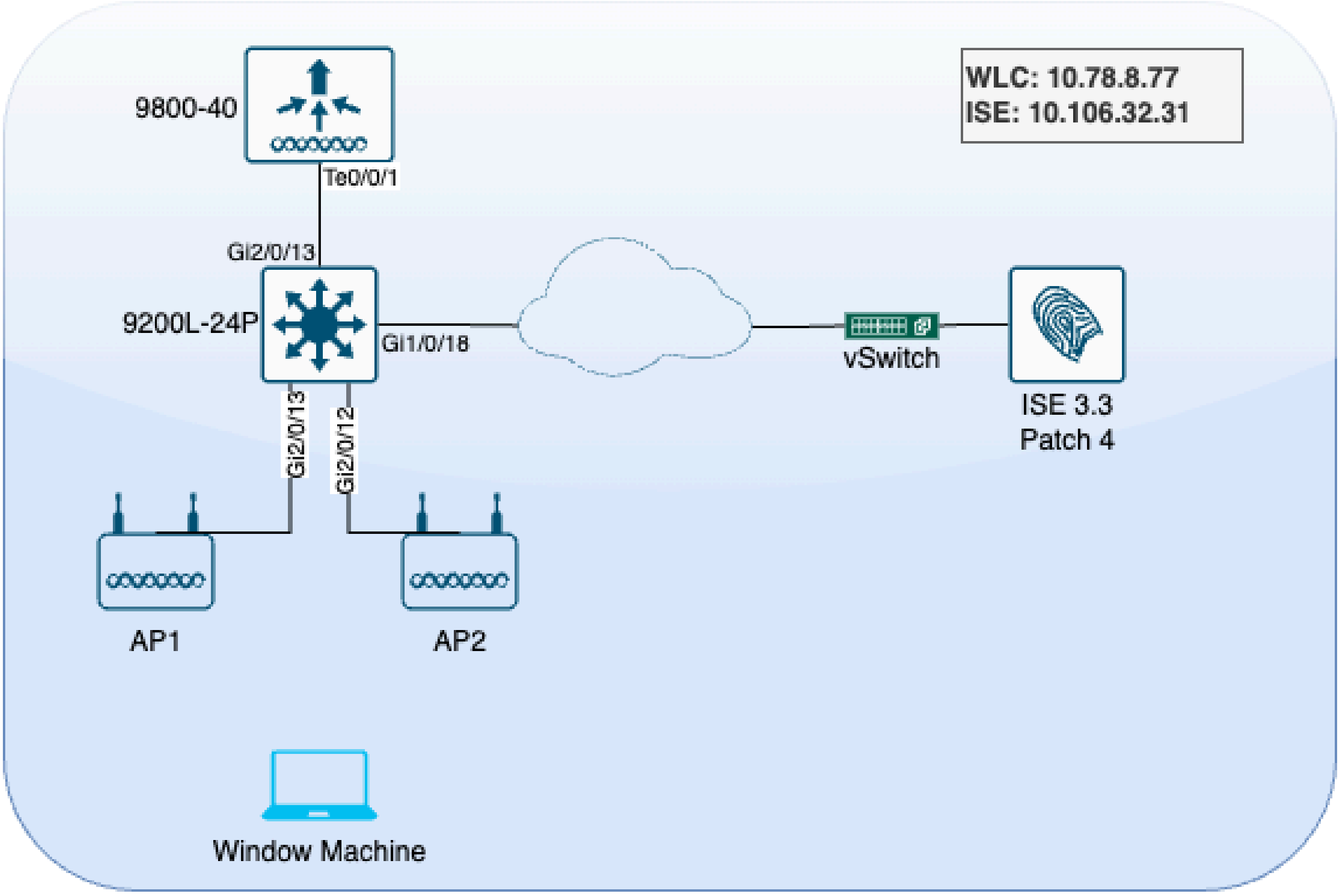
12. A new encryption key is dynamically derived from the secret during the TLS handshake.

13. An EAP-Success message is sent from the server to the authenticator and then to the supplicant.

14. The EAP-TLS enabled wireless client can now access the wireless network.

Configure

Network Diagram



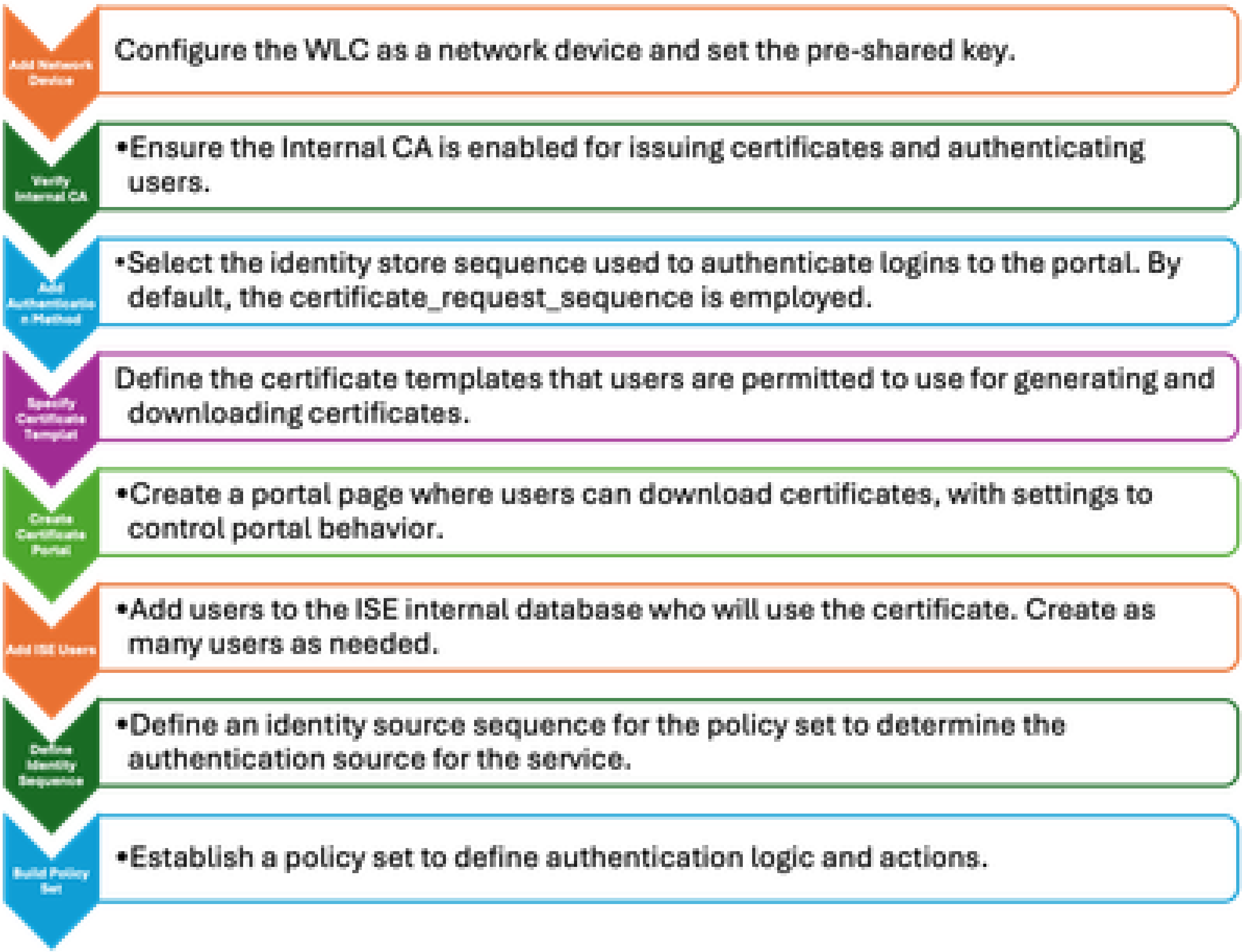
LAB Topology

Configurations

In this section, we configure two components: ISE and 9800 WLC.

ISE Configuration

Here are the configuration steps for the ISE server. Each step is accompanied by screenshots in this section to provide visual guidance.



Configure the WLC as a network device and set the pre-shared key.

•Ensure the Internal CA is enabled for issuing certificates and authenticating users.

•Select the identity store sequence used to authenticate logins to the portal. By default, the certificate_request_sequence is employed.

Define the certificate templates that users are permitted to use for generating and downloading certificates.

•Create a portal page where users can download certificates, with settings to control portal behavior.

•Add users to the ISE internal database who will use the certificate. Create as many users as needed.

•Define an identity source sequence for the policy set to determine the authentication source for the service.

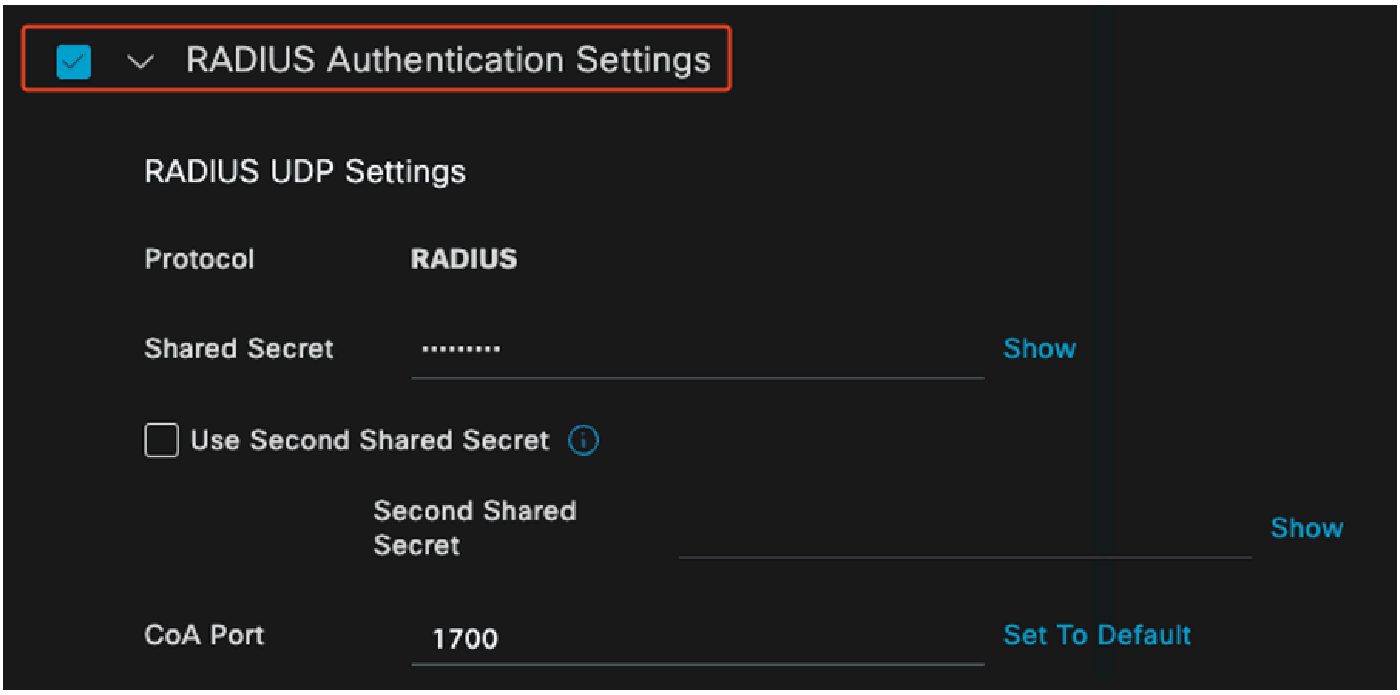
•Establish a policy set to define authentication logic and actions.

ISE Server Configuration Steps

Adding a Network Device

To add the Wireless LAN Controller (WLC) as a network device, use these instructions:

1. Navigate to **Administration** > **Network Resources** > **Network Devices**.
2. Click the **+Add** icon to initiate the process of adding the WLC.
3. Ensure that the pre-shared key matches both the WLC and the ISE server to enable proper communication.
4. Once all details are correctly entered, click **Submit** at the bottom left corner to save the configuration



☑ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

Shared Secret ••••••••• Show

□ Use Second Shared Secret

Second Shared Secret Show

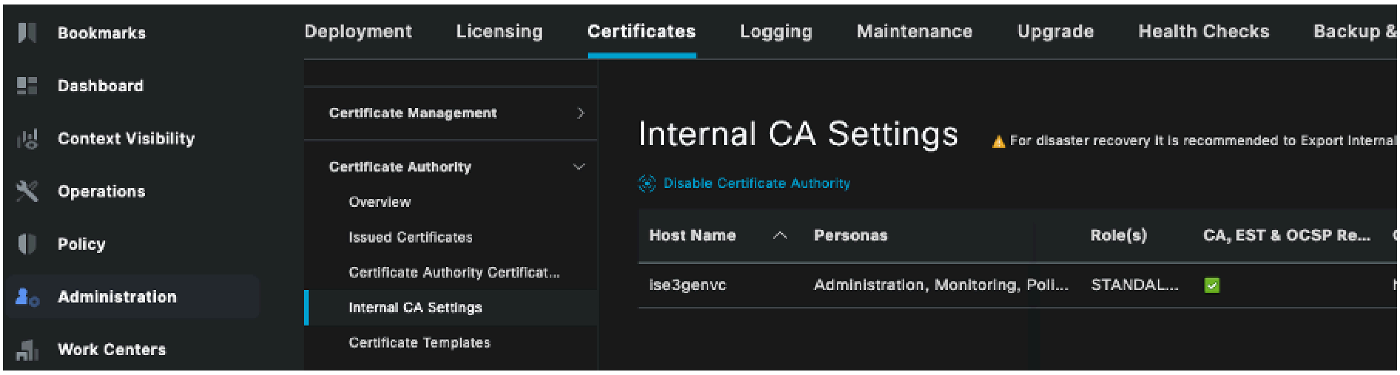
CoA Port 1700 Set To Default

Adding a Network Device

Verify Internal CA

To verify the Internal Certificate Authority (CA) settings, use these steps:

1. Go to **Administration** > **System** > **Certificates** > **Certificate Authority** > **Internal CA Settings**.
2. Ensure that the CA column is enabled to confirm that the internal CA is active.



Internal CA Settings

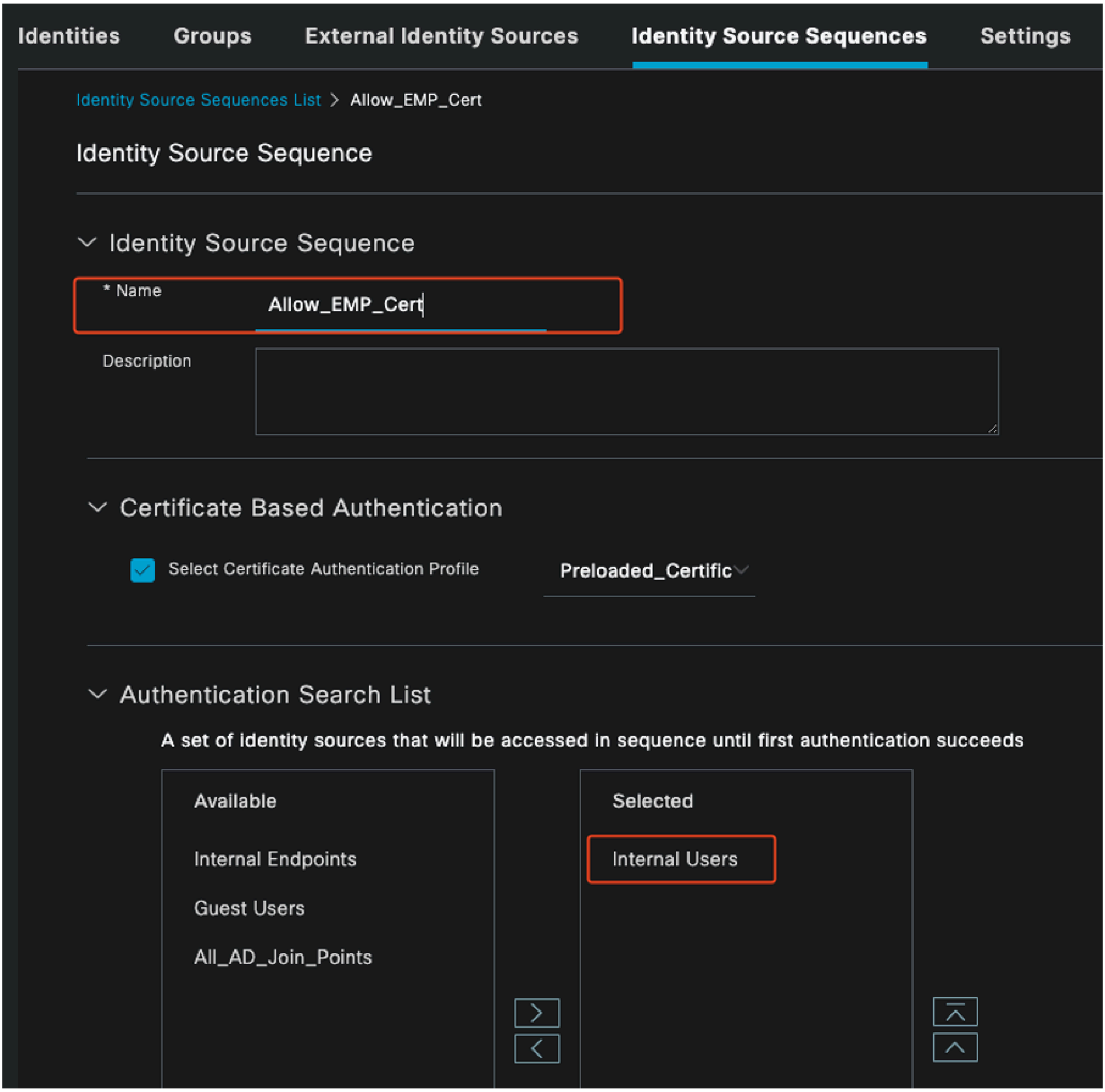
For disaster recovery it is recommended to Export Internal

Host Name	Personas	Role(s)	CA, EST & OCSP Re...
ise3genvc	Administration, Monitoring, Poli...	STANDAL...	✓

Verify Internal CA

Add Authentication Method

Navigate to **Administration** > **Identity Management** > **Identity Source Sequences**. Add a custom identity sequence to control the portal login source.


Identities
Groups
External Identity Sources
Identity Source Sequences
Settings
Identity Source Sequences List > Allow_EMP_Cert

Identity Source Sequence

Identity Source Sequence

* Name: Allow_EMP_Cert

Description:

Certificate Based Authentication

☑ Select Certificate Authentication Profile: Preloaded_Certific

Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available	Selected
Internal Endpoints	Internal Users
Guest Users	
All_AD_Join_Points	

Authentication Method

Specify Certificate Template

To specify a certificate template, use these steps:

Step 1. Navigate to **Administration** > **System** > **Certificates** > **Certificate Authority** > **Certificate Templates**.

Step 2. Click the **+Add** icon to create a new certificate template:

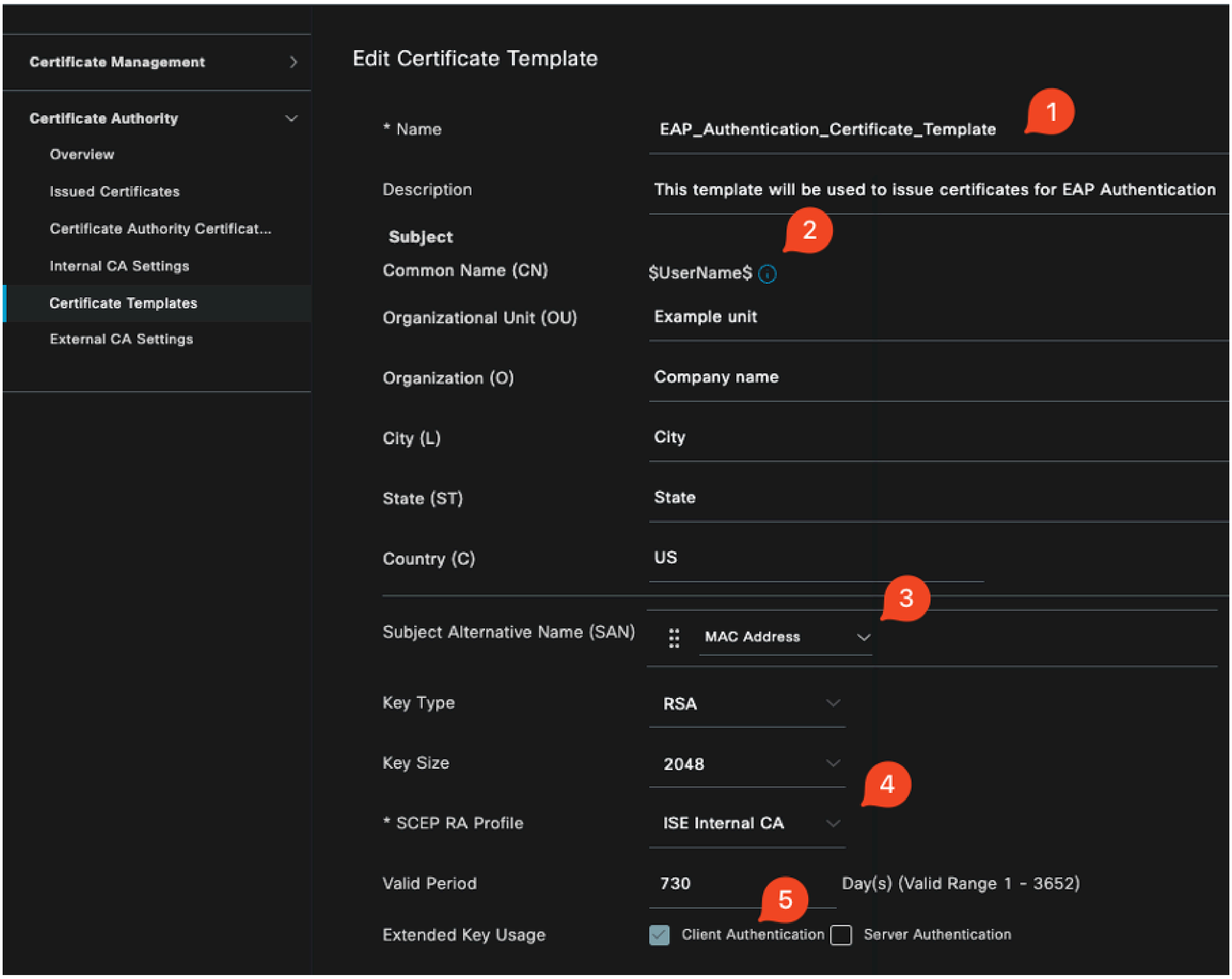
2.1 Provide a **unique name** that is local to the ISE server for the template.

2.2 Ensure the Common Name (CN) is set to $UserName$.

2.3 Verify that the Subject Alternative Name (SAN) is mapped to the MAC address.

2.4 **Set** the SCEP RA profile to ISE Internal CA.

2.5 In the extended key usage section, **enable** client authentication.



Edit Certificate Template

* Name	EAP_Authentication_Certificate_Template
Description	This template will be used to issue certificates for EAP Authentication
Subject	
Common Name (CN)	$UserName$
Organizational Unit (OU)	Example unit
Organization (O)	Company name
City (L)	City
State (ST)	State
Country (C)	US
Subject Alternative Name (SAN)	MAC Address
Key Type	RSA
Key Size	2048
* SCEP RA Profile	ISE Internal CA
Valid Period	730 Day(s) (Valid Range 1 - 3652)
Extended Key Usage	☑ Client Authentication ☐ Server Authentication

Certificate Template

Create Certificate Portal

To create a certificate portal for client certificate generation, use these steps:

Step 1. Navigate to **Administration** > **Device Portal Management** > **Certificate Provisioning**.

Step 2. Click **Create** to set up a new portal page.

Step 3. Provide a **unique name** for the portal to easily identify it.

3.1. Choose the **port number** for the portal to operate on; set this to 8443.

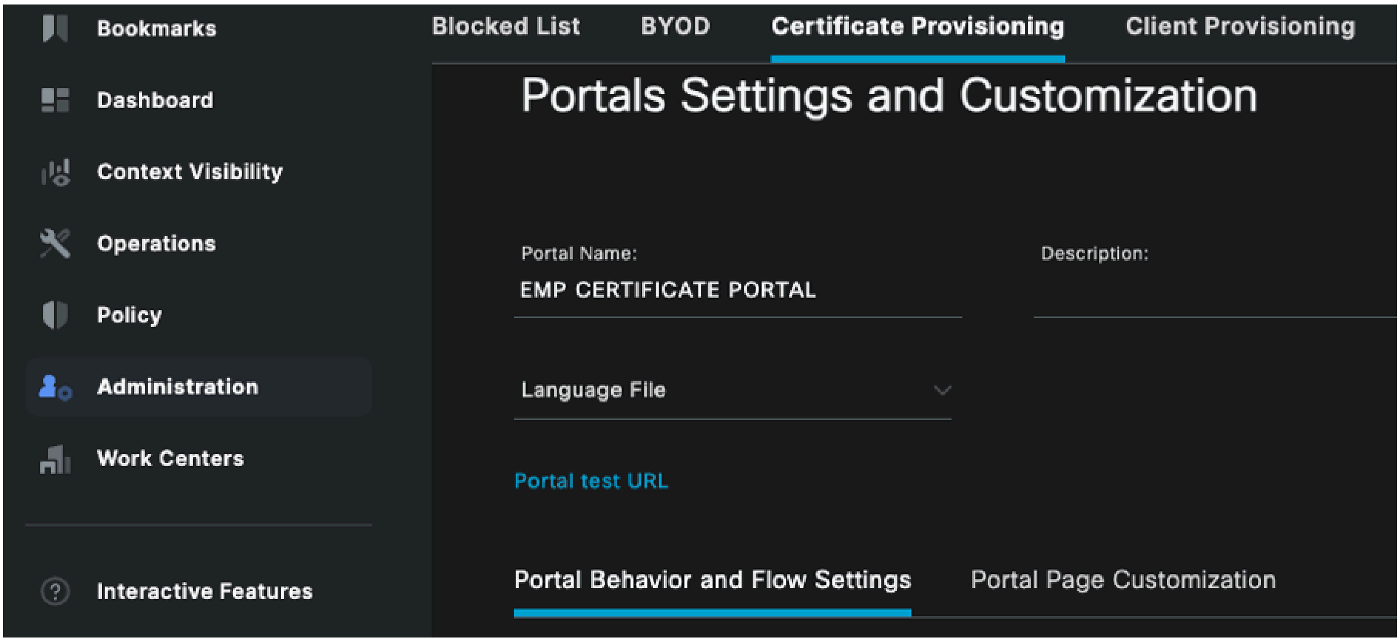
3.2. Specify the **interfaces** on which ISE listens for this portal.

3.3. Select the **Certificate Group Tag** as the Default Portal Certificate Group.

3.4. Select the **authentication method**, which indicates the identity store sequence used to authenticate login to this portal.

3.5. Include the **authorized groups** whose members can access the portal. For instance, select the **Employee** user group if your users belong to this group.

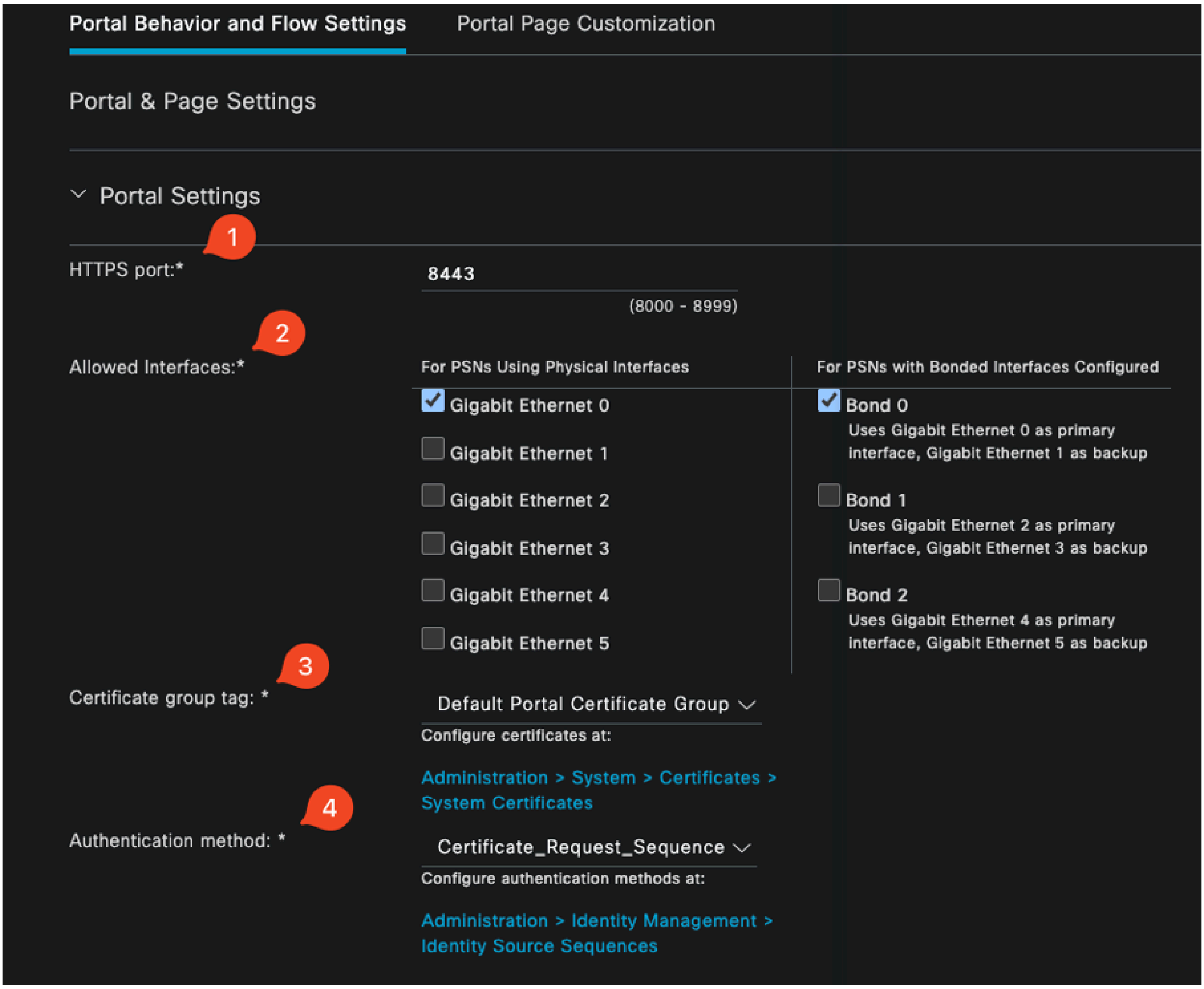
3.6. Define the **certificate templates** that are permitted under the Certificate Provisioning settings.



Portals Settings and Customization

Portal Name: EMP CERTIFICATE PORTAL

Description:



Portal & Page Settings

Portal Settings

HTTPS port:* 8443 (8000 - 8999)

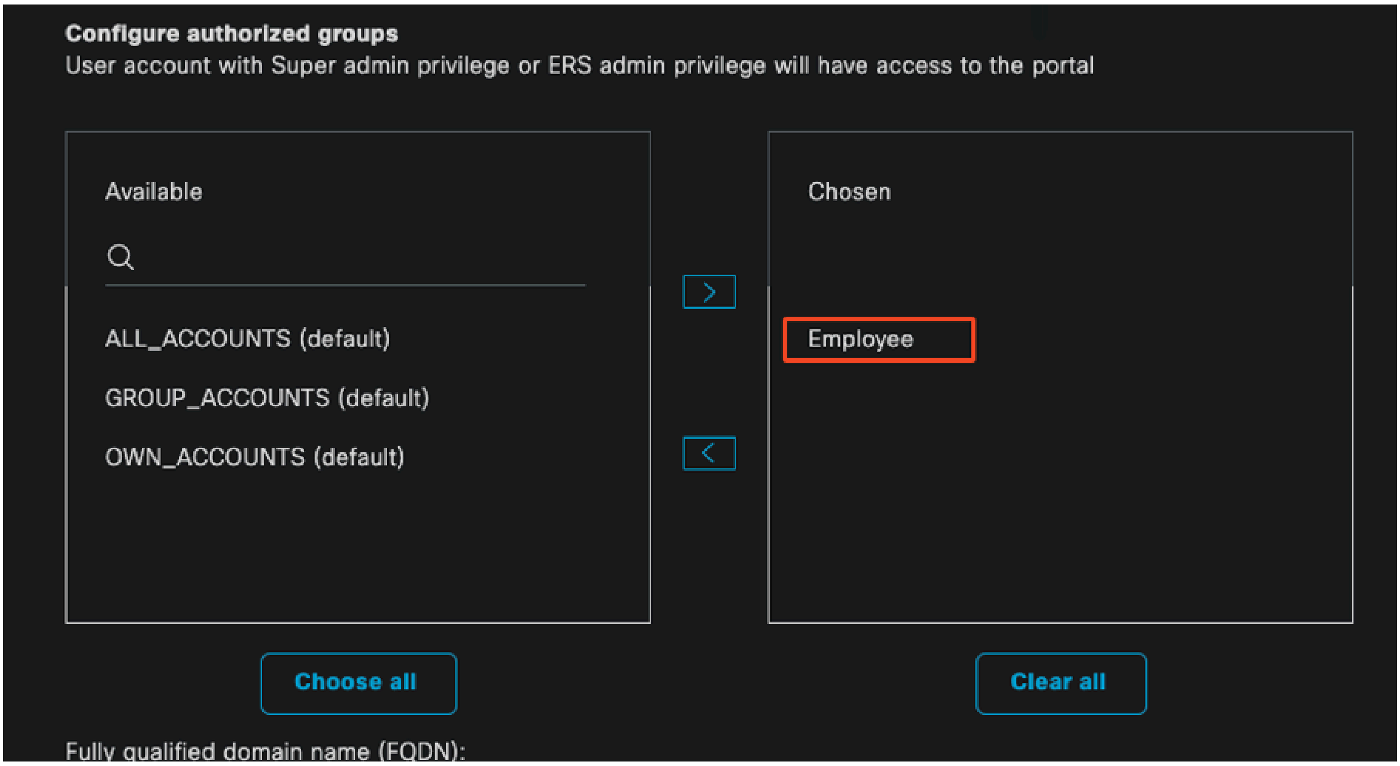
Allowed Interfaces:*

For PSNs Using Physical Interfaces
☑ Gigabit Ethernet 0
□ Gigabit Ethernet 1
□ Gigabit Ethernet 2
□ Gigabit Ethernet 3
□ Gigabit Ethernet 4
□ Gigabit Ethernet 5

For PSNs with Bonded Interfaces Configured
☑ Bond 0
Uses Gigabit Ethernet 0 as primary interface, Gigabit Ethernet 1 as backup
□ Bond 1
Uses Gigabit Ethernet 2 as primary interface, Gigabit Ethernet 3 as backup
□ Bond 2
Uses Gigabit Ethernet 4 as primary interface, Gigabit Ethernet 5 as backup

Certificate group tag: * Default Portal Certificate Group
Configure certificates at:
Administration > System > Certificates > System Certificates

Authentication method: * Certificate_Request_Sequence
Configure authentication methods at:
Administration > Identity Management > Identity Source Sequences

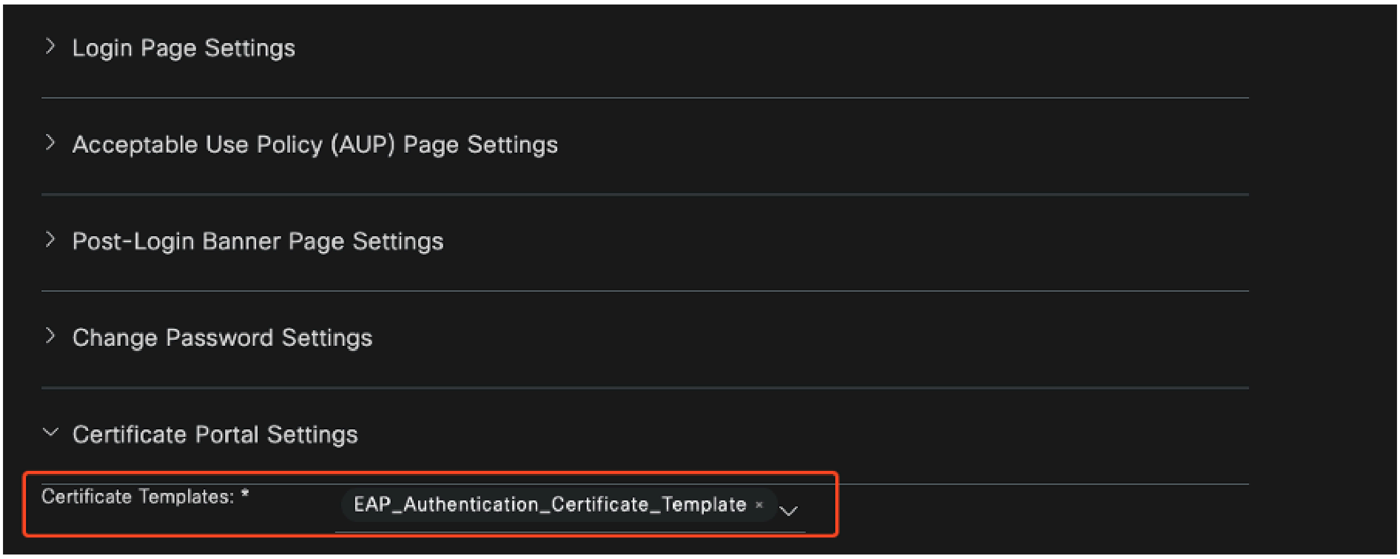


Configure authorized groups
User account with Super admin privilege or ERS admin privilege will have access to the portal

Available
ALL_ACCOUNTS (default)
GROUP_ACCOUNTS (default)
OWN_ACCOUNTS (default)

Chosen
Employee

Fully qualified domain name (FQDN):

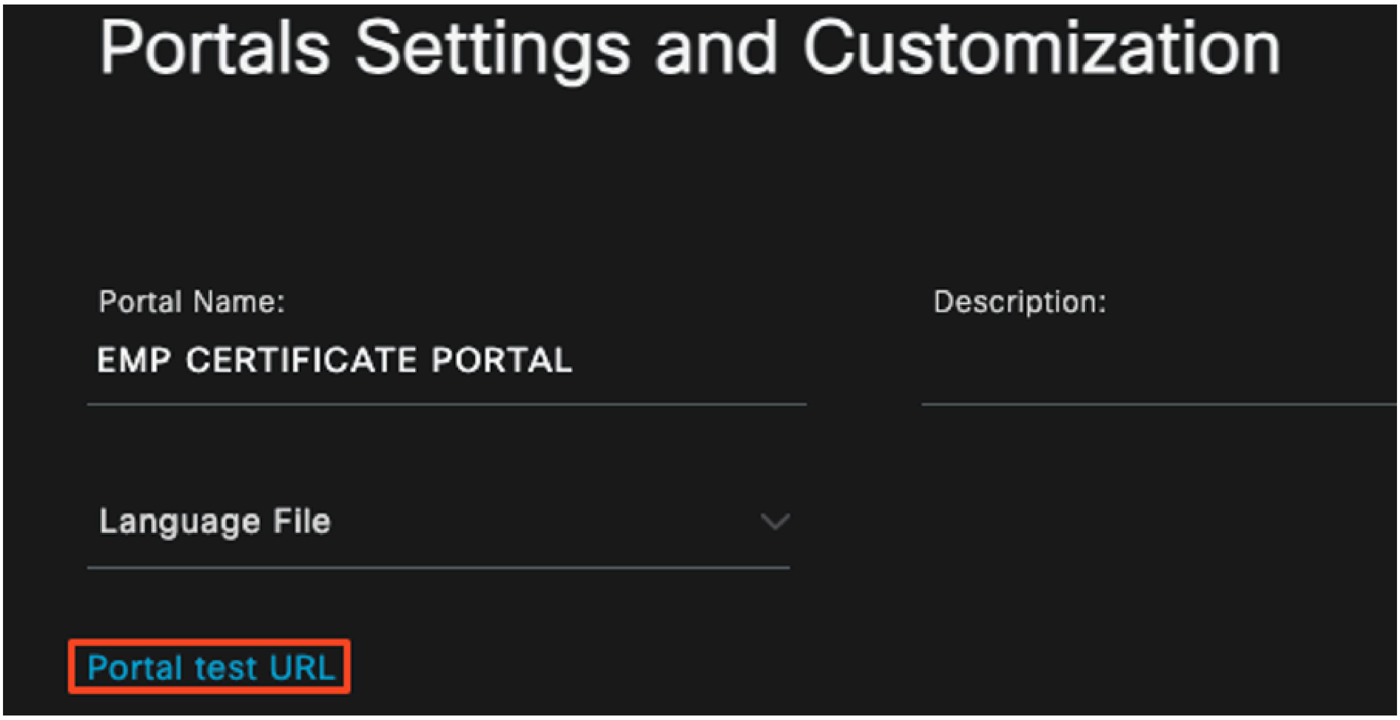


Login Page Settings
Acceptable Use Policy (AUP) Page Settings
Post-Login Banner Page Settings
Change Password Settings
Certificate Portal Settings

Certificate Templates: * EAP_Authentication_Certificate_Template

Certificate Portal Configuration

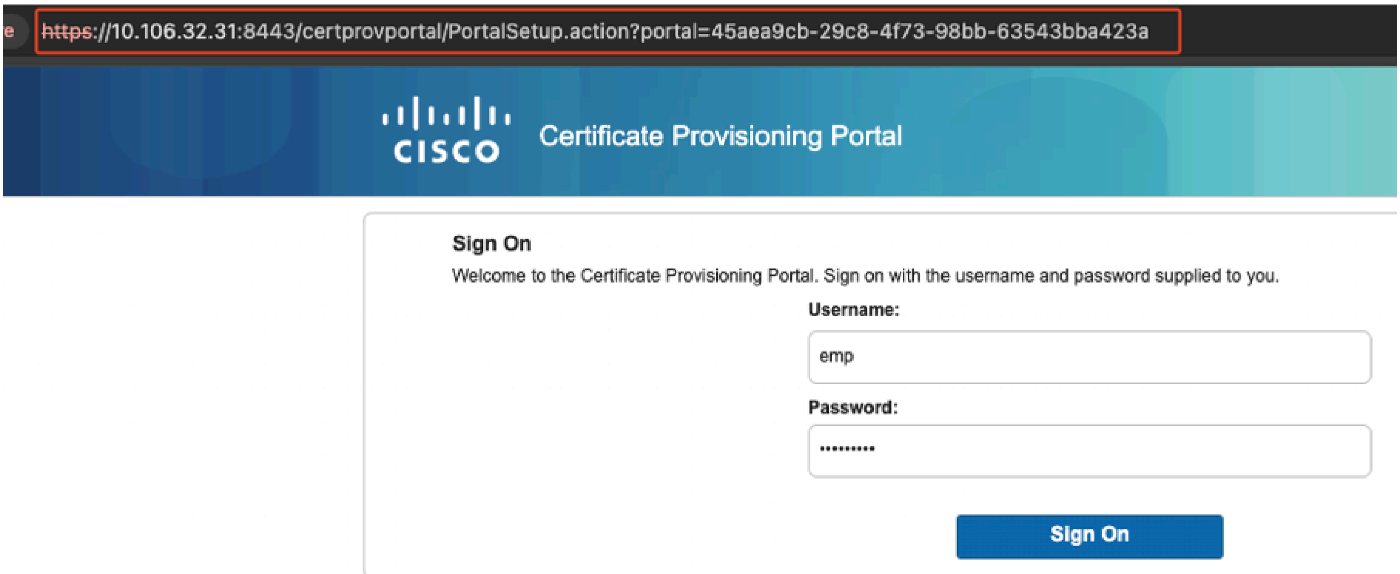
Once this setup is completed, you can test the portal by clicking on the **Portal Test URL**. This action opens the portal page.



Portal Name: EMP CERTIFICATE PORTAL

Description:

Test Portal Page URL


https://10.106.32.31:8443/certprovportal/PortalSetup.action?portal=45aea9cb-29c8-4f73-98bb-63543bba423a

Certificate Provisioning Portal

Sign On

Welcome to the Certificate Provisioning Portal. Sign on with the username and password supplied to you.

Username: emp

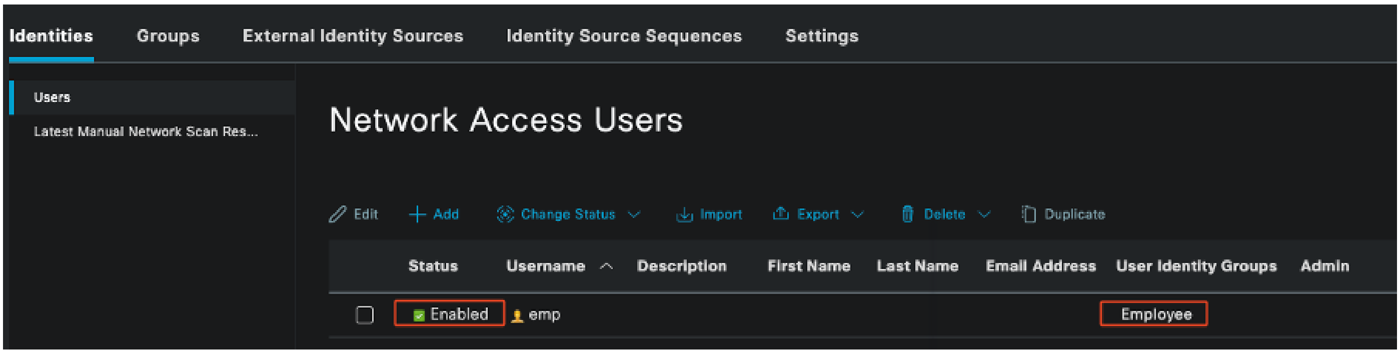
Password: •••••••••

Portal Page

Add Internal User

To create a user for authenticating via the certificate portal, use these steps:

1. Go to **Administration** > **Identity Management** > **Identities** > **Users**.
2. Click the option to add a user to the system.
3. Select the **User Identity Groups** that the user belongs to. For this example, assign the user to the **Employee** group.


Identities
Groups
External Identity Sources
Identity Source Sequences
Settings
Users
Latest Manual Network Scan Res...
Edit
Add
Change Status
Import
Export
Delete
Duplicate

Network Access Users

	Status	Username	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
□	Enabled	emp					Employee	

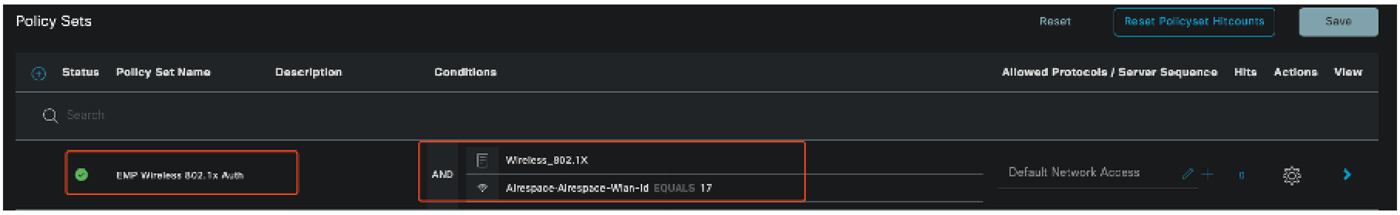
Adding Internal User

ISE Certificate Provisioning Portal and RADIUS Policy Configuration

The previous section covered the setup of the ISE certificate provisioning portal. Now, we configure the ISE RADIUS policy sets to allow user authentication.

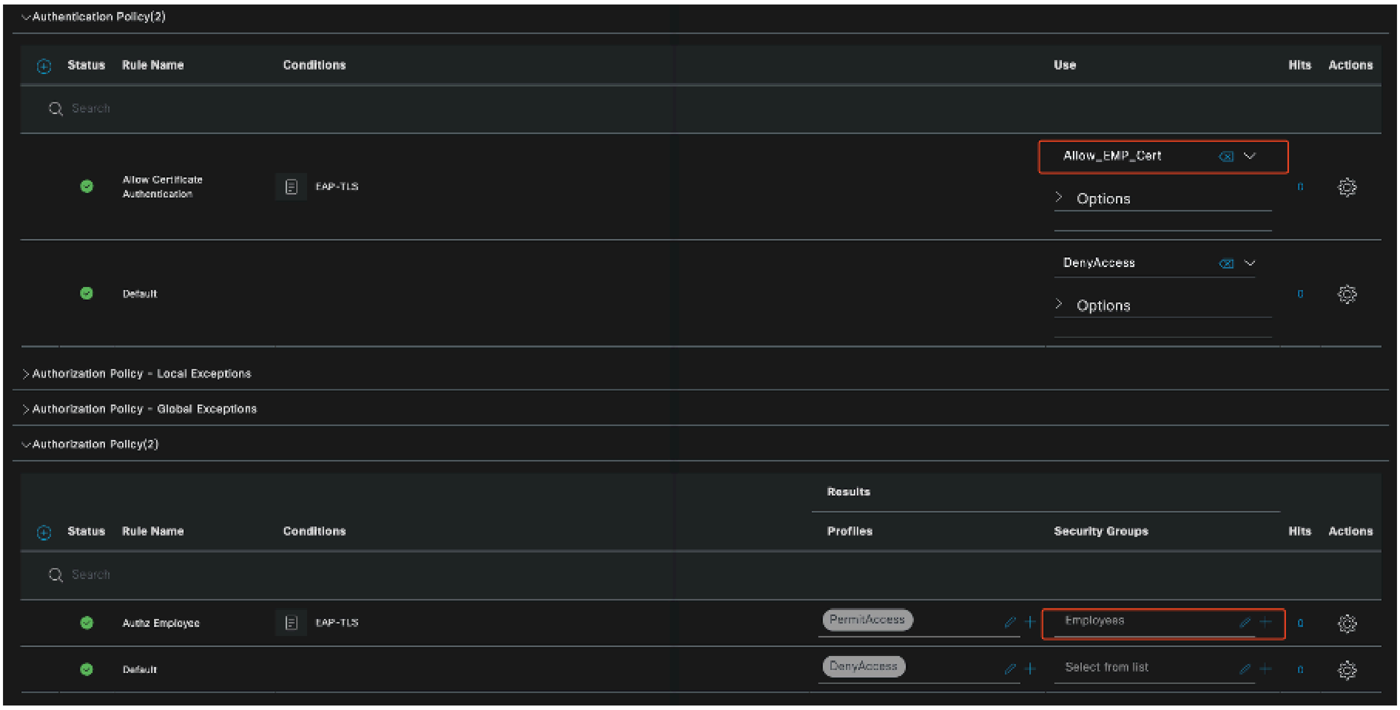
1. **Configure** ISE RADIUS Policy Sets
2. Navigate to **Policy** > **Policy Sets**.
3. Click the **plus sign (+)** to create a new policy set.

In this example, set up a simple policy set designed to authenticate users using their certificates.



Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
●	EMP Wireless 802.1x Auth		AND Wireless_802.1X Airespace-Airespace-Wlan-Id EQUALS 17	Default Network Access	0	⚙	>

Policy Set



Authentication Policy(2)

Status	Rule Name	Conditions	Use	Hits	Actions
●	Allow Certificate Authentication	EAP-TLS	Allow_EMP_Cert Options	0	⚙
●	Default		DenyAccess Options	0	⚙

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

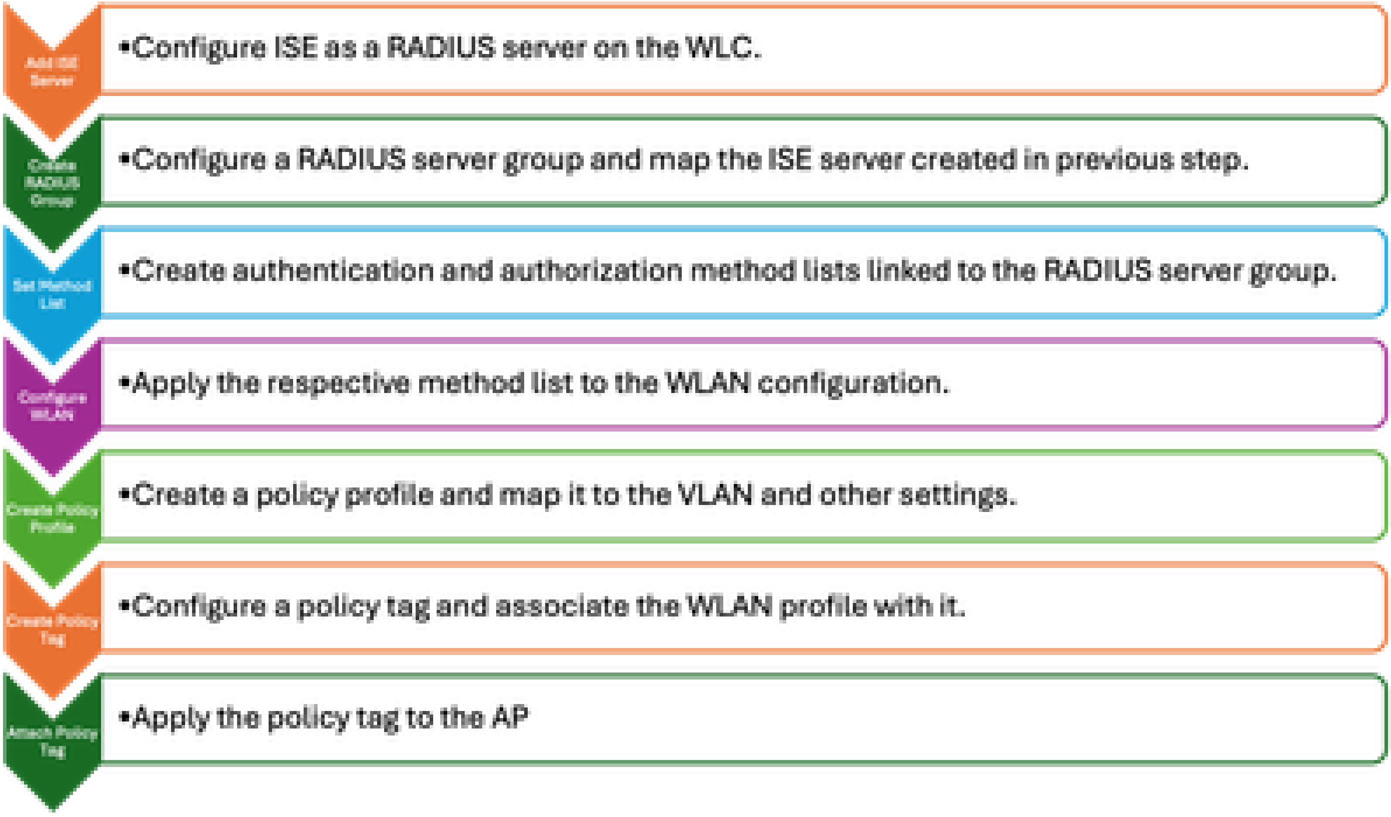
Authorization Policy(2)

			Results			
Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
●	Authz Employee	EAP-TLS	PermitAccess	Employees	0	⚙
●	Default		DenyAccess	Select from list	0	⚙

Policy Set Showing Authentication and Authorization Policies

9800 WLC configuration

Here are the configuration steps for the 9800 WLC. Each step is accompanied by screenshots in this section to provide visual guidance.

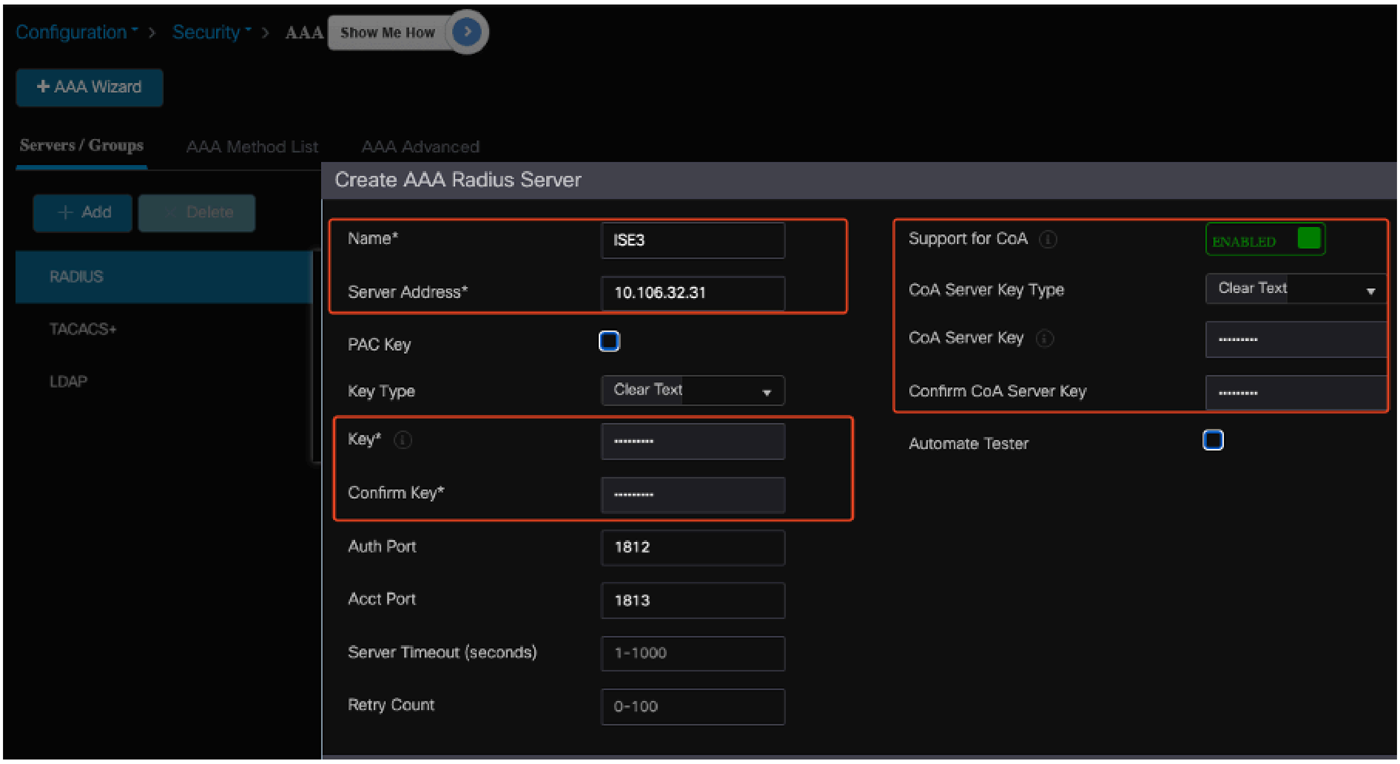


- Configure ISE as a RADIUS server on the WLC.
- Configure a RADIUS server group and map the ISE server created in previous step.
- Create authentication and authorization method lists linked to the RADIUS server group.
- Apply the respective method list to the WLAN configuration.
- Create a policy profile and map it to the VLAN and other settings.
- Configure a policy tag and associate the WLAN profile with it.
- Apply the policy tag to the AP

WLC Configuration Steps

Add ISE Server to 9800 WLC

1. To integrate the ISE server with the 9800 Wireless LAN Controller (WLC), use these steps:
2. Go to **Configuration** > **Security** > **AAA**.
3. Click the **Add** button to include the ISE server in the WLC configuration.

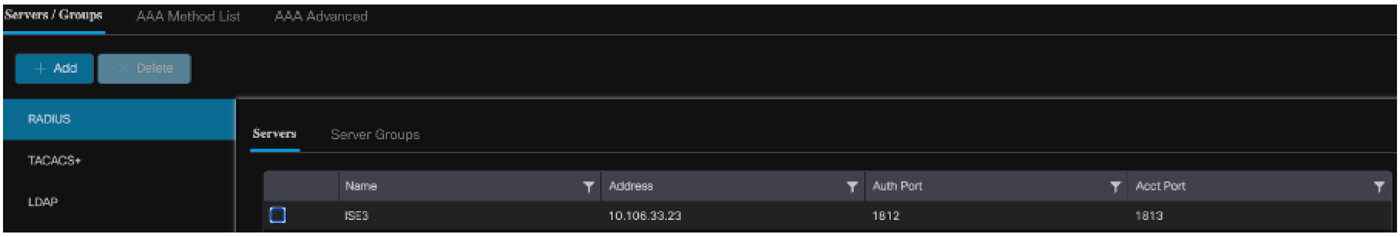


Create AAA Radius Server

Name*	ISE3
Server Address*	10.106.32.31
PAC Key	□
Key Type	Clear Text
Key*	·········
Confirm Key*	·········
Auth Port	1812
Acct Port	1813
Server Timeout (seconds)	1-1000
Retry Count	0-100
Support for CoA	ENABLED
CoA Server Key Type	Clear Text
CoA Server Key	·········
Confirm CoA Server Key	·········
Automate Tester	□

Adding ISE Server In the WLC

Once the server is added, it appears in the list of servers.



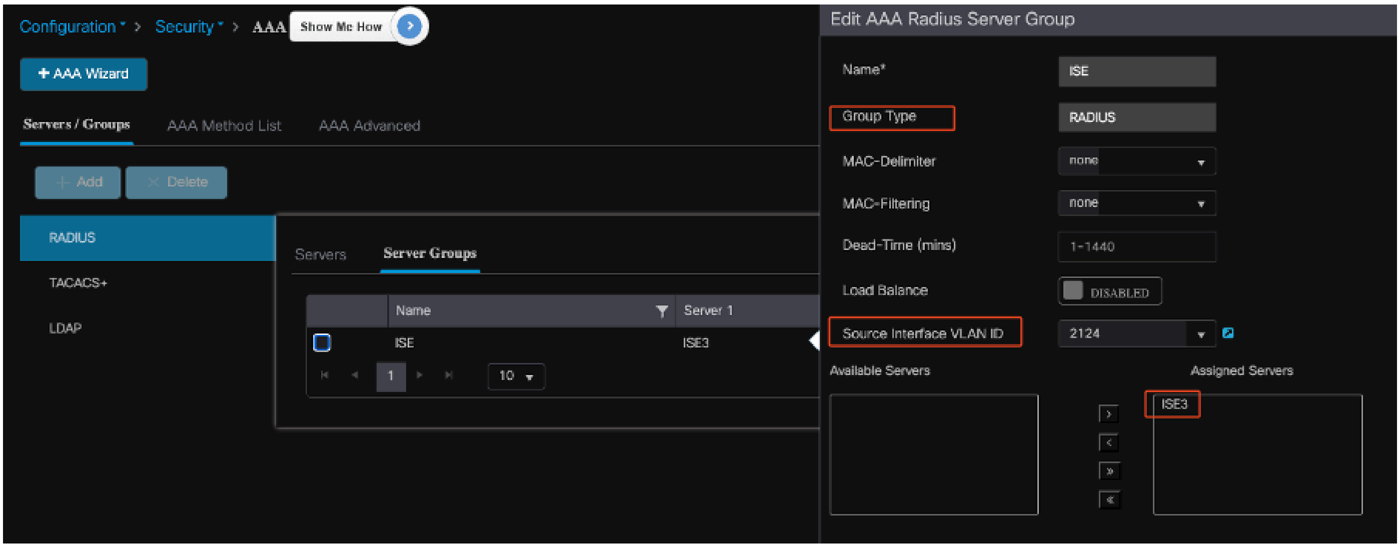
	Name	Address	Auth Port	Acct Port
□	ISE3	10.106.33.23	1812	1813

Showing Radius Servers

Add Server Group on 9800 WLC

To add a server group on the 9800 Wireless LAN Controller, complete these steps:

1. Navigate to **Configuration** > **Security** > **AAA**.
2. Click on the **Server Group** tab, then click **Add** to create a new server group.



	Name	Server 1
□	ISE	ISE3

Name*: ISE

Group Type: RADIUS

MAC-Delimiter: none

MAC-Filtering: none

Dead-Time (mins): 1-1440

Load Balance: DISABLED

Source Interface VLAN ID: 2124

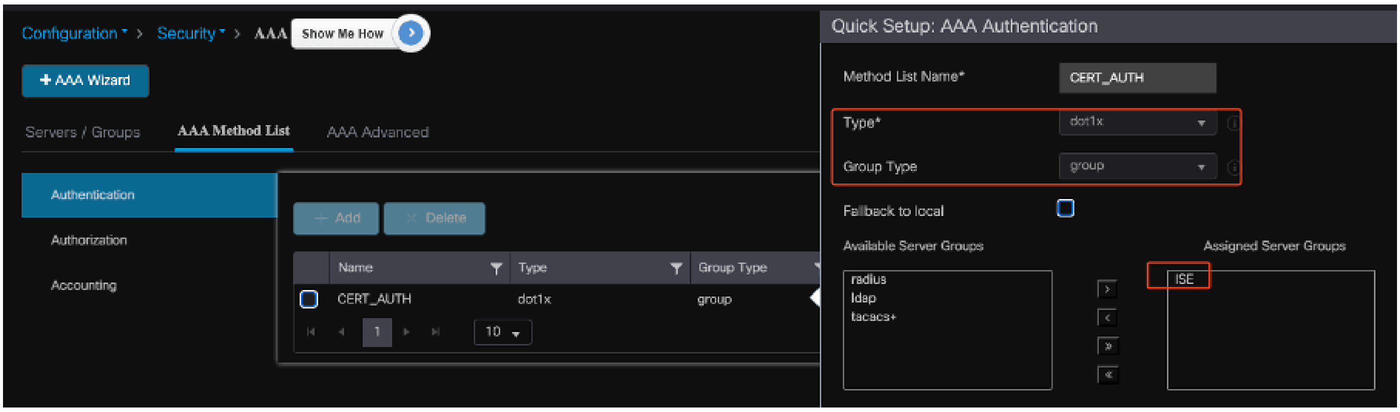
Assigned Servers: ISE3

Mapping ISE Servers to a Radius Server Group

Configure AAA Method List on 9800 WLC

After creating the server group, configure the authentication method list using these steps:

1. Navigate to **Configuration** > **Security** > **AAA** > **AAA Method List**.
2. In the Authentication tab, add a new authentication method list.
3. Set the type to **dot1x**.
4. Select **group** as the group type.
5. Include the **ISE server groups** that you created earlier as the server groups.



Name	Type	Group Type
CERT_AUTH	dot1x	group

Quick Setup: AAA Authentication

Method List Name* CERT_AUTH

Type* dot1x

Group Type group

Fallback to local □

Available Server Groups: radius, ldap, tacacs+

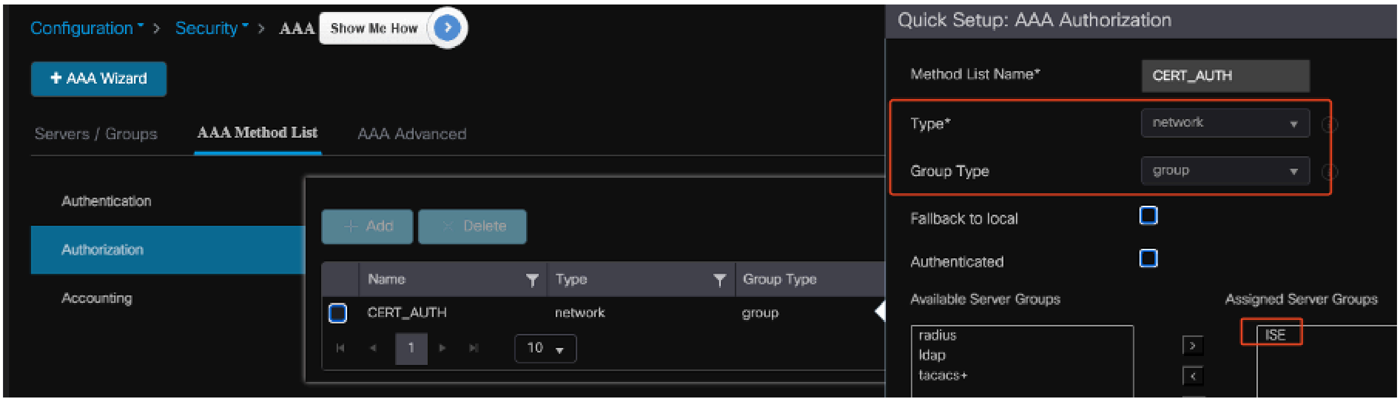
Assigned Server Groups: ISE

Creating Authentication Method Lists

Configure Authorization Method List on 9800 WLC

To set up the authorization method list, use these steps:

1. Navigate to the **Authorization tab** within the AAA Method List section.
2. Click **Add** to create a new authorization method list.
3. Choose **network** as the type.
4. Select **group** as the group type.
5. Include the **ISE server group** as the server group.



Name	Type	Group Type
CERT_AUTH	network	group

Quick Setup: AAA Authorization

Method List Name* CERT_AUTH

Type* network

Group Type group

Fallback to local □

Authenticated □

Available Server Groups: radius, ldap, tacacs+

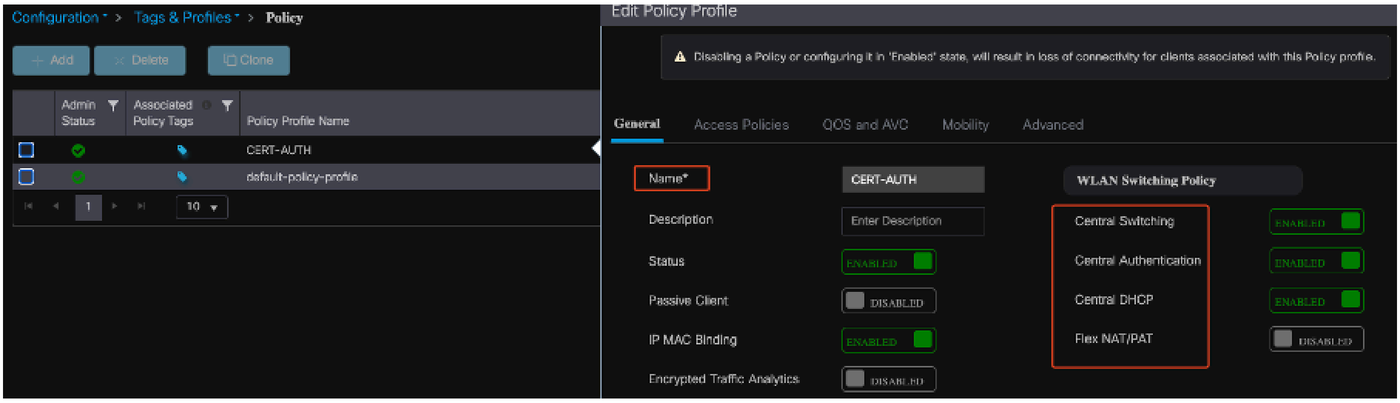
Assigned Server Groups: ISE

Adding Authorization Method List

Create a Policy Profile on 9800 WLC

With the RADIUS group configuration complete, proceed to create a policy profile:

1. Navigate to **Configuration** > **Tags & Profiles** > **Policy.**
2. Click **Add** to create a new policy profile.
3. Choose the appropriate parameters for your policy profile. In this example, everything is central and LAB VLAN is used as the client VLAN.



Admin Status	Associated Policy Tags	Policy Profile Name
✓	●	CERT-AUTH
✓	●	default-policy-profile

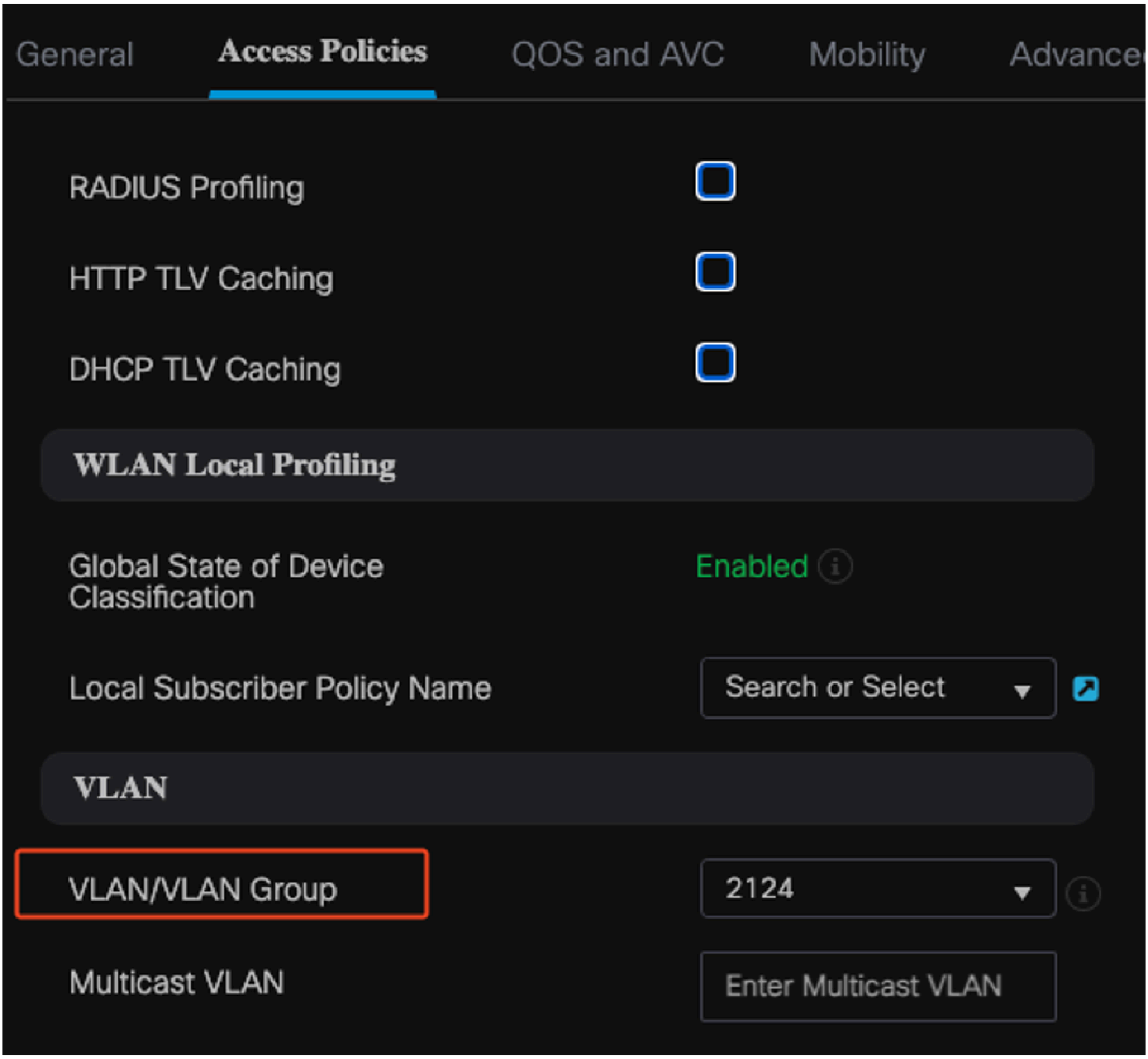
Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

Name*	CERT-AUTH
Description	Enter Description
Status	ENABLED
Passive Client	DISABLED
IP MAC Binding	ENABLED
Encrypted Traffic Analytics	DISABLED

WLAN Switching Policy

Central Switching	ENABLED
Central Authentication	ENABLED
Central DHCP	ENABLED
Flex NAT/PAT	DISABLED

Configuring Policy Profile



RADIUS Profiling	□
HTTP TLV Caching	□
DHCP TLV Caching	□

WLAN Local Profiling

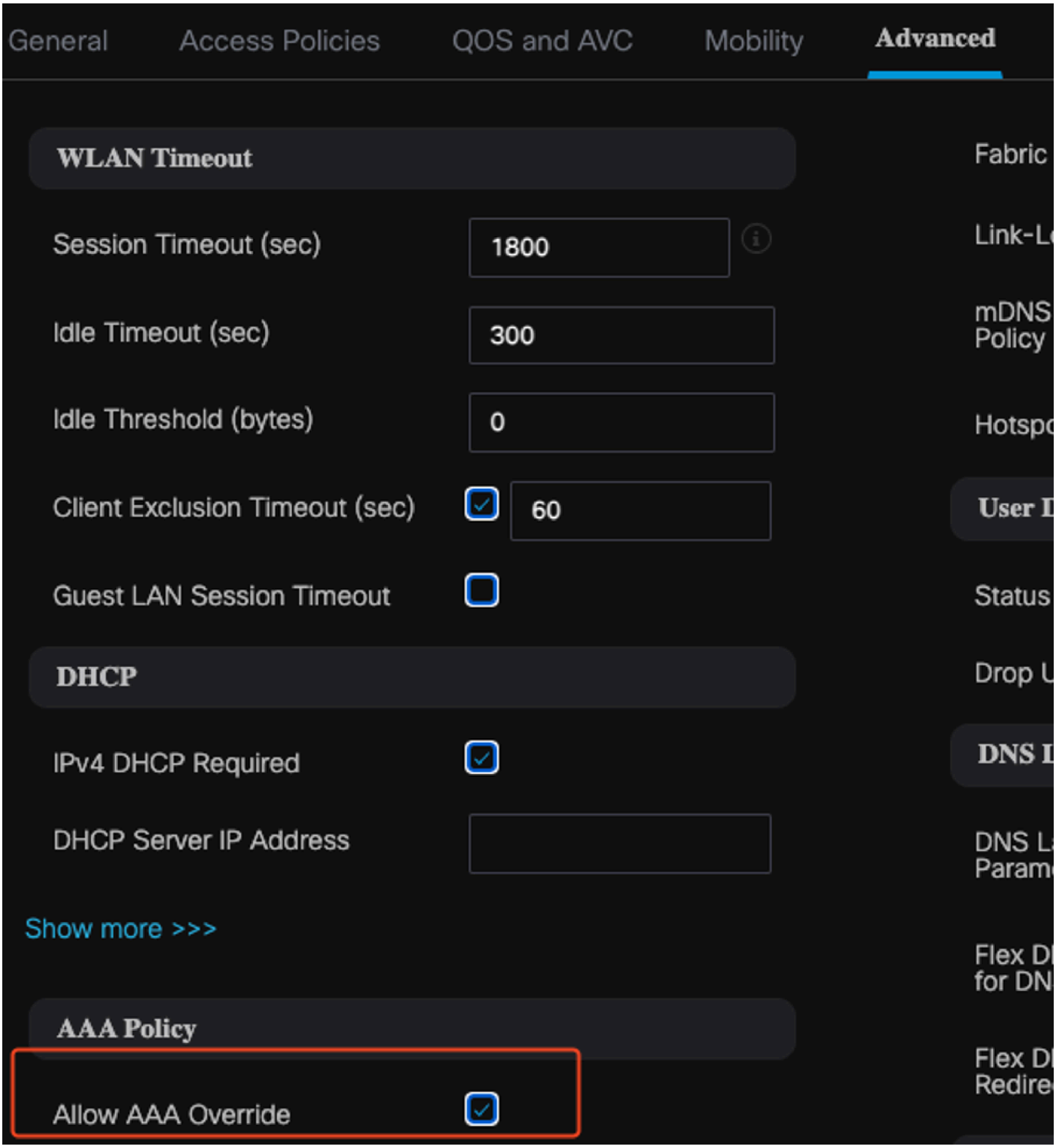
Global State of Device Classification	Enabled
Local Subscriber Policy Name	Search or Select

VLAN

VLAN/VLAN Group	2124
Multicast VLAN	Enter Multicast VLAN

VLAN to Policy Mapping

When configuring RADIUS authorization, ensure that the **AAA Override** option is enabled in the advanced tab of the policy profile settings. This setting allows the Wireless LAN Controller to apply RADIUS-based authorization policies to users and devices.



WLAN Timeout

Session Timeout (sec): 1800

Idle Timeout (sec): 300

Idle Threshold (bytes): 0

Client Exclusion Timeout (sec): ☑ 60

Guest LAN Session Timeout: □

DHCP

IPv4 DHCP Required: ☑

DHCP Server IP Address:

AAA Policy

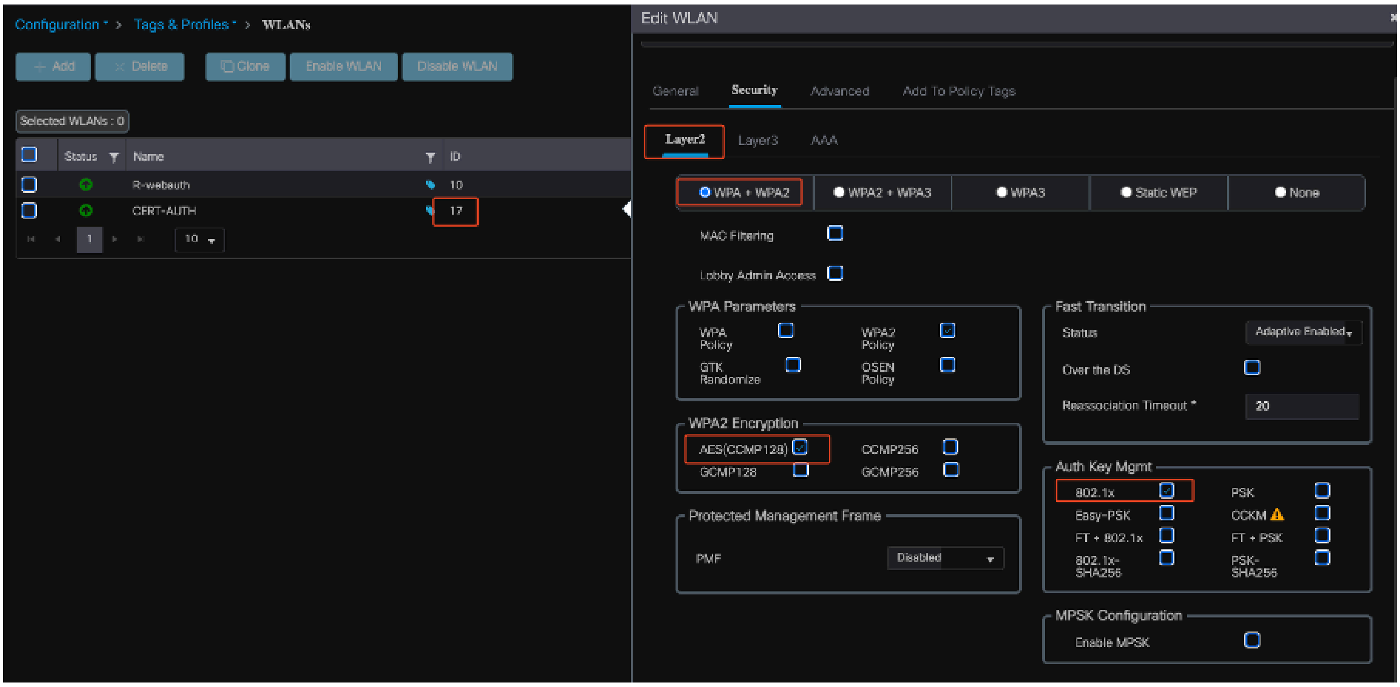
Allow AAA Override: ☑

AAA Override

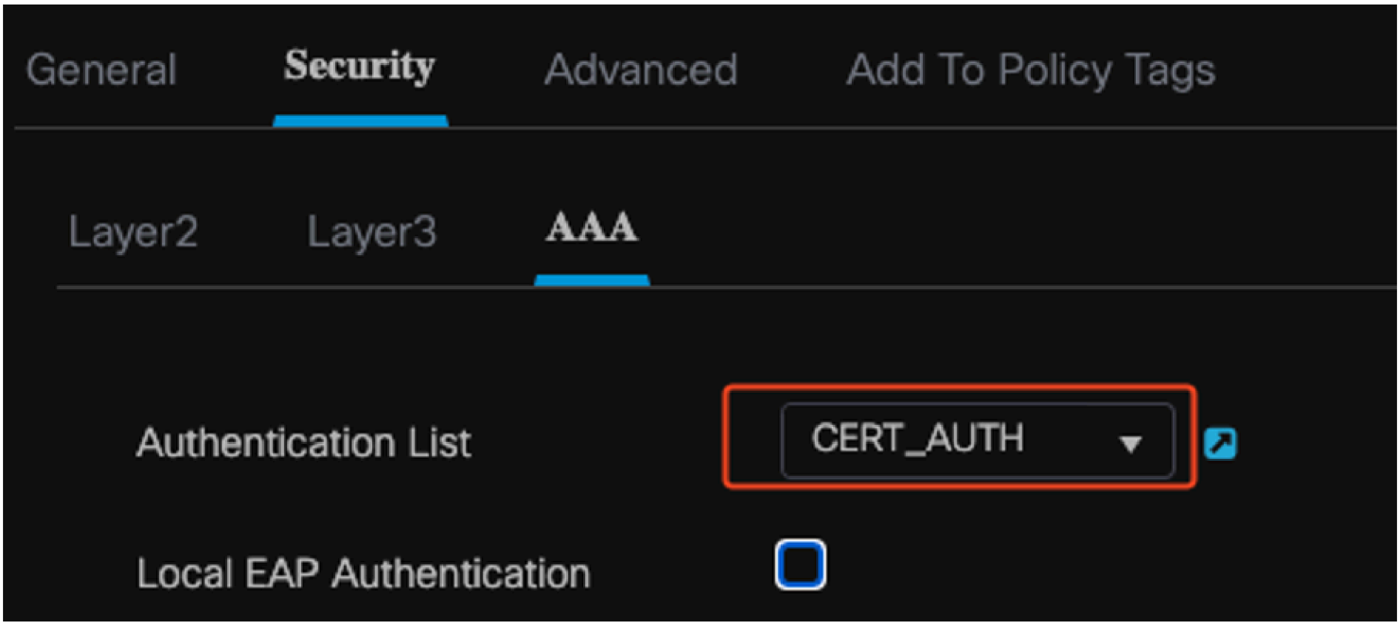
Create a WLAN on 9800 WLC

To set up a new WLAN with 802.1x authentication, use these steps:

1. Navigate to **Configuration** > **Tags & Profiles** > **WLANs**.
2. Click **Add** to create a new WLAN.
3. **Select** the Layer 2 authentication settings and enable 802.1x authentication.



WLAN Profile configuration

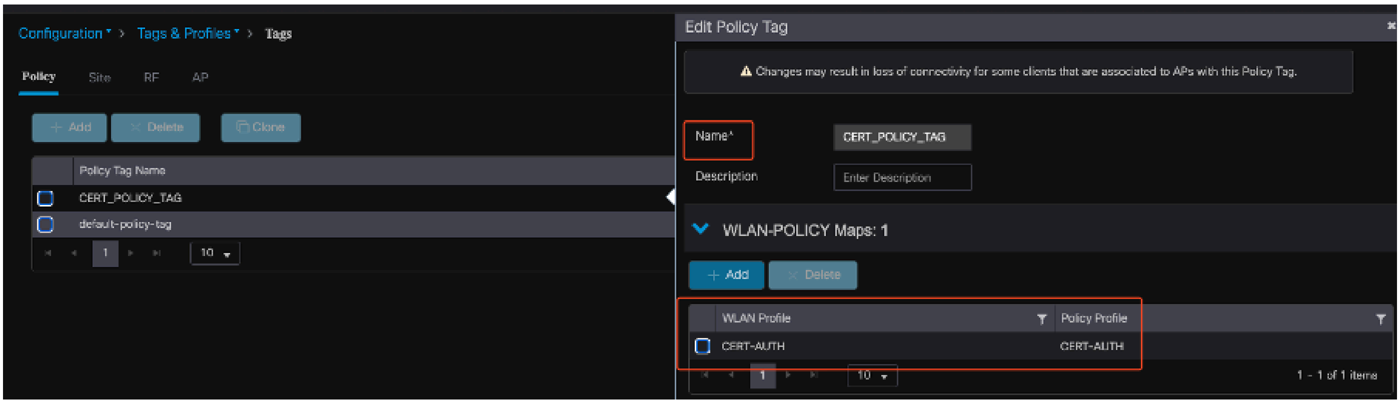


WLAN Profile to Method List Map

Map WLAN with Policy Profile on 9800 WLC

To associate your WLAN with a policy profile, use these steps:

1. Navigate to **Configuration** > **Tags & Profiles** > **Tags**.
2. Click **Add** to add a new tag.
3. In the WLAN-POLICY section, **map** the newly created WLAN to the appropriate policy profile.



⚠ Changes may result in loss of connectivity for some clients that are associated to APs with this Policy Tag.

Name* CERT_POLICY_TAG

Description Enter Description

WLAN-POLICY Maps: 1

	Policy Tag Name
□	CERT_POLICY_TAG
□	default-policy-tag

	WLAN Profile	Policy Profile
□	CERT-AUTH	CERT-AUTH

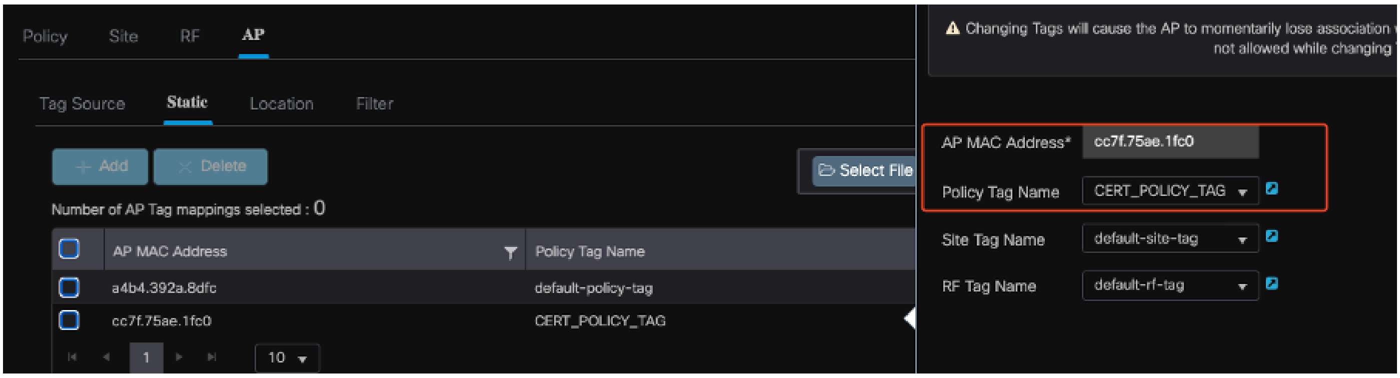
1 - 1 of 1 items

Policy TAG Configuration

Map Policy Tag to Access Point on 9800 WLC

To assign the policy tag to an Access Point (AP), complete these steps:

1. Navigate to **Configuration** > **Tags & Profiles** > **Tags** > **AP**.
2. Go to the Static section within the AP configuration.
3. Click the specific AP you want to configure.
4. **Assign** the policy tag you created to the selected AP.



⚠ Changing Tags will cause the AP to momentarily lose association not allowed while changing

Number of AP Tag mappings selected : 0

□	AP MAC Address	Policy Tag Name
□	a4b4.392a.8dfc	default-policy-tag
□	cc7f.75ae.1fc0	CERT_POLICY_TAG

AP MAC Address* cc7f.75ae.1fc0

Policy Tag Name CERT_POLICY_TAG

Site Tag Name default-site-tag

RF Tag Name default-rf-tag

AP TAG Assignment

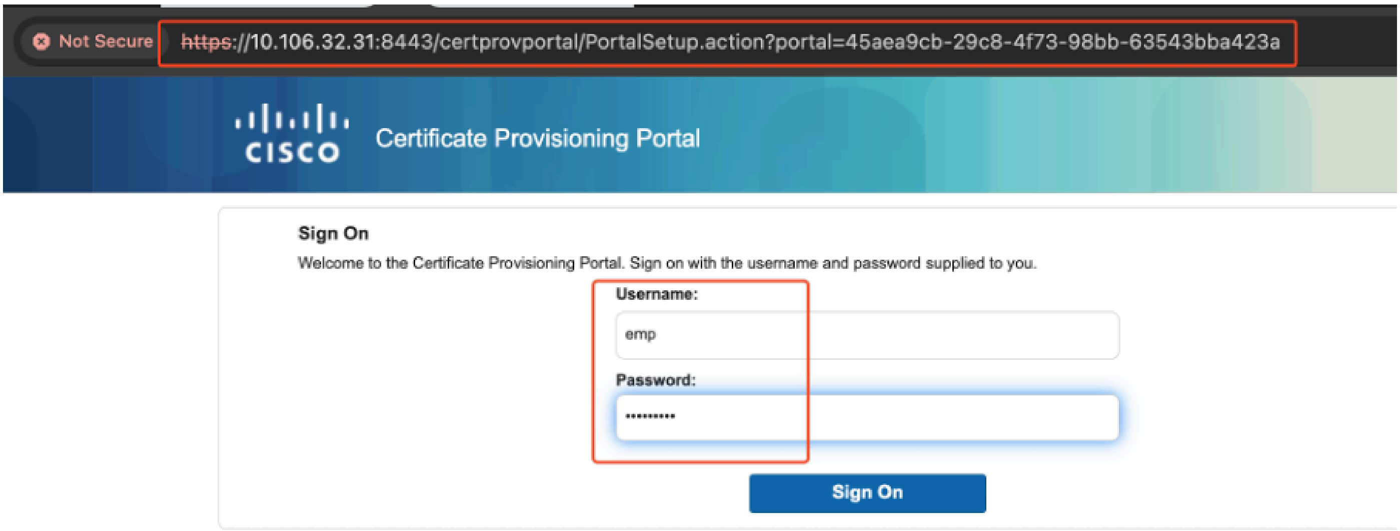
Running Configuration of the WLC After Setup Completion

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

wireless profile policy CERT-AUTH
 aaa-override
 ipv4 dhcp required
 vlan 2124
 no shutdown
 wlan CERT-AUTH policy CERT-AUTH
wlan CERT-AUTH 17 CERT-AUTH
 security dot1x authentication-list CERT_AUTH
 no shutdown
!
wireless tag policy CERT_POLICY_TAG
 wlan CERT-AUTH policy CERT-AUTH
```

Create and Download Certificate for the user

To create and download a certificate for a user, go through these steps:

1. Have the user log into the certificate portal that was set up earlier.



Not Secure ~~https~~://10.106.32.31:8443/certprovportal/PortalSetup.action?portal=45aea9cb-29c8-4f73-98bb-63543bba423a

Certificate Provisioning Portal

Sign On

Welcome to the Certificate Provisioning Portal. Sign on with the username and password supplied to you.

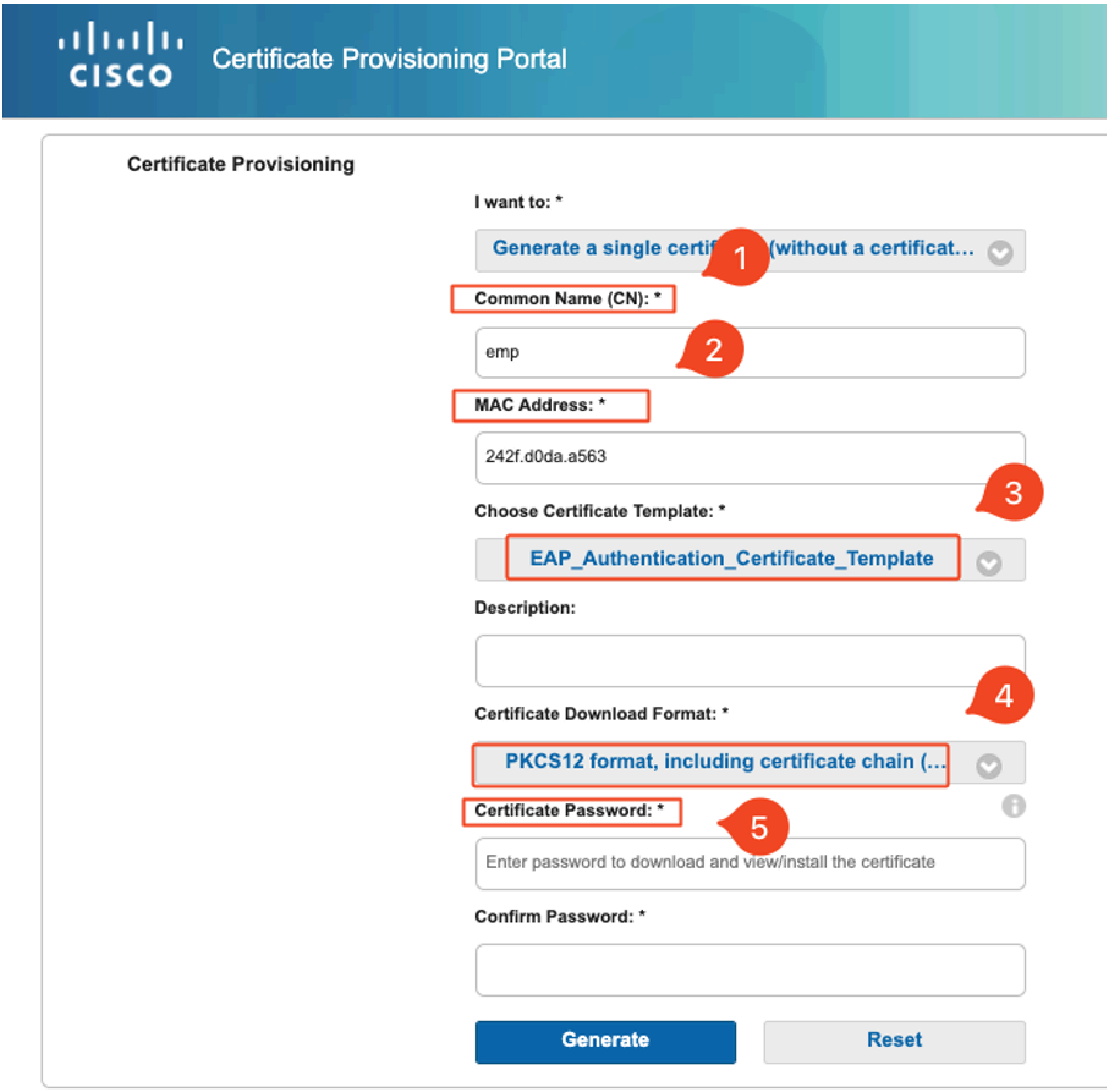
Username: emp

Password: ••••••••••

Accessing Certificate Portal

2. Accept the Acceptable Use Policy (AUP). The ISE then presents a page for certificate generation.

3. Select **Generate a single certificate (without a certificate signing request)**.



Certificate Provisioning Portal

Certificate Provisioning

I want to: *

Generate a single certi… (without a certificat…

Common Name (CN): *

emp

MAC Address: *

242f.d0da.a563

Choose Certificate Template: *

EAP_Authentication_Certificate_Template

Description:

Certificate Download Format: *

PKCS12 format, including certificate chain (…

Certificate Password: *

Enter password to download and view/install the certificate

Confirm Password: *

Generating Certificate

To generate a certificate via the Certificate Provisioning Portal, ensure that these mandatory fields are completed:

- CN: The authentication server uses the value that is presented in the Common Name field in the client certificate to authenticate a user. In the Common Name field, enter the username (that you used to log in to the Certificate Provisioning Portal).
- MAC Address: Subject Alternative Names (SAN) is an X.509 extension that allows various values to be associated with a security certificate. Cisco ISE, Release 2.0 supports MAC address only. Hence, in the SAN/MAC address field.
    - Certificate Template: The certificate template defies a set of fields that the CA uses when validating a request and issuing a certificate. Fields such as the Common Name (CN) are used to validate the request (CN must match the username)). Other fields are used by the CA while issuing the certificate.
- Certificate Password: You need a certificate password to secure your certificate. You must supply the

certificate password to view the contents of the certificate and to import the certificate on a device.
- Your password must conform to these rules:
- Password must contain at least 1 uppercase letter, 1 lowercase letter, and 1 digit
    - Password must be between 8 and 15 characters long
    - Allowed characters include A-Z, a-z, 0-9, _, #

Once all fields are filled out, select **Generate** to create and download the certificate.

Certificate Installation on a Windows 10 Machine

To install a certificate on a Windows 10 machine, open the Microsoft Management Console (MMC) using these steps:

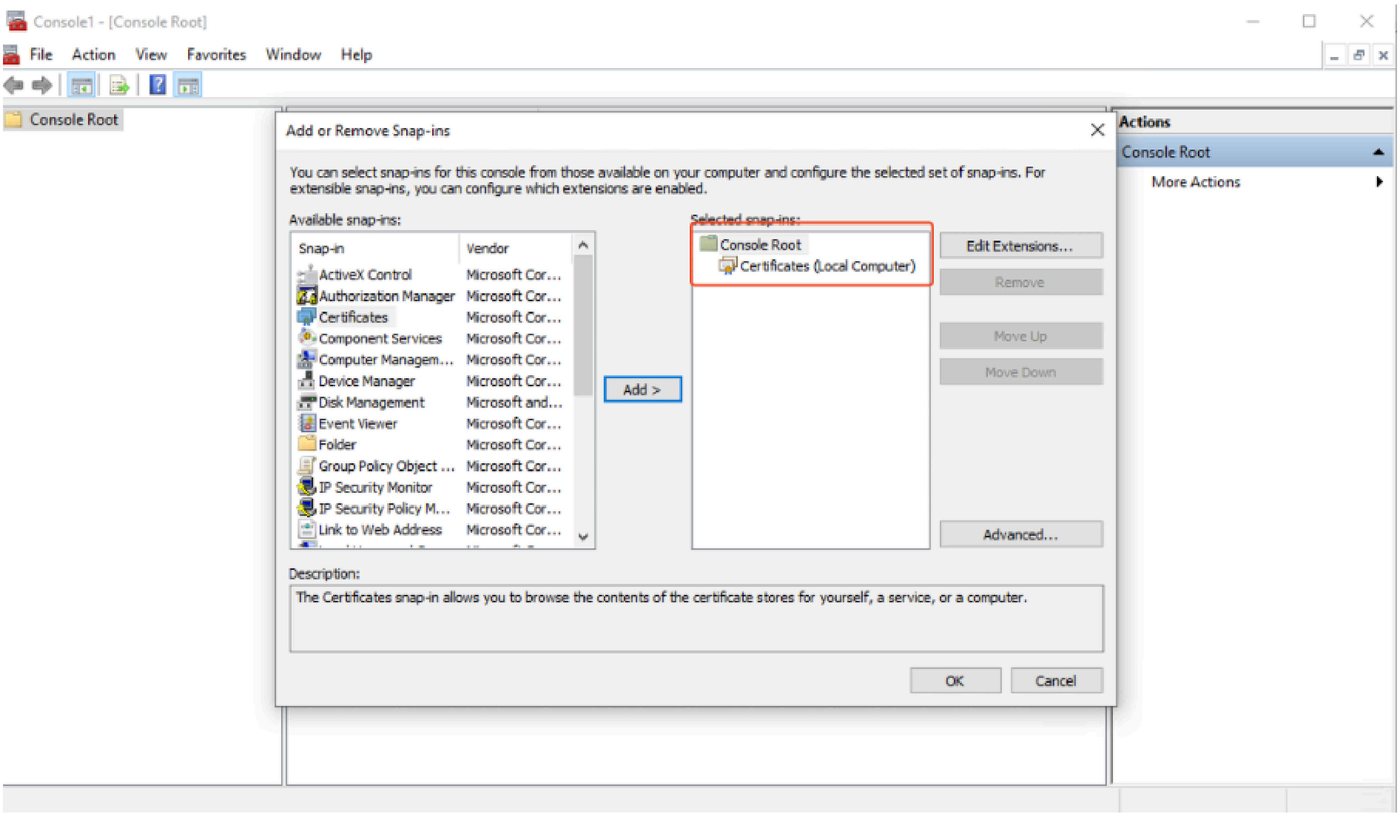
> **Note**: These instructions can vary based on your Windows setup, so consulting the Microsoft documentation for specific details is recommended.

---

1. Click **Start** and then **Run**.
2. Type **mmc** in the Run box and press Enter. The Microsoft Management Console opens.
3. Add **Certificate** Snap-In:

4. Go to **File > Add/Remove Snap-In.**
5. Select **Add**, then choose **Certificates** and click **Add**.
6. Select **Computer Account**, then **Local Compute**r, and click **Finish**.

These steps allow you to manage certificates on your local computer.



Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...
Link to Web Address	Microsoft Cor...

Selected snap-ins:

Console Root
Certificates (Local Computer)

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

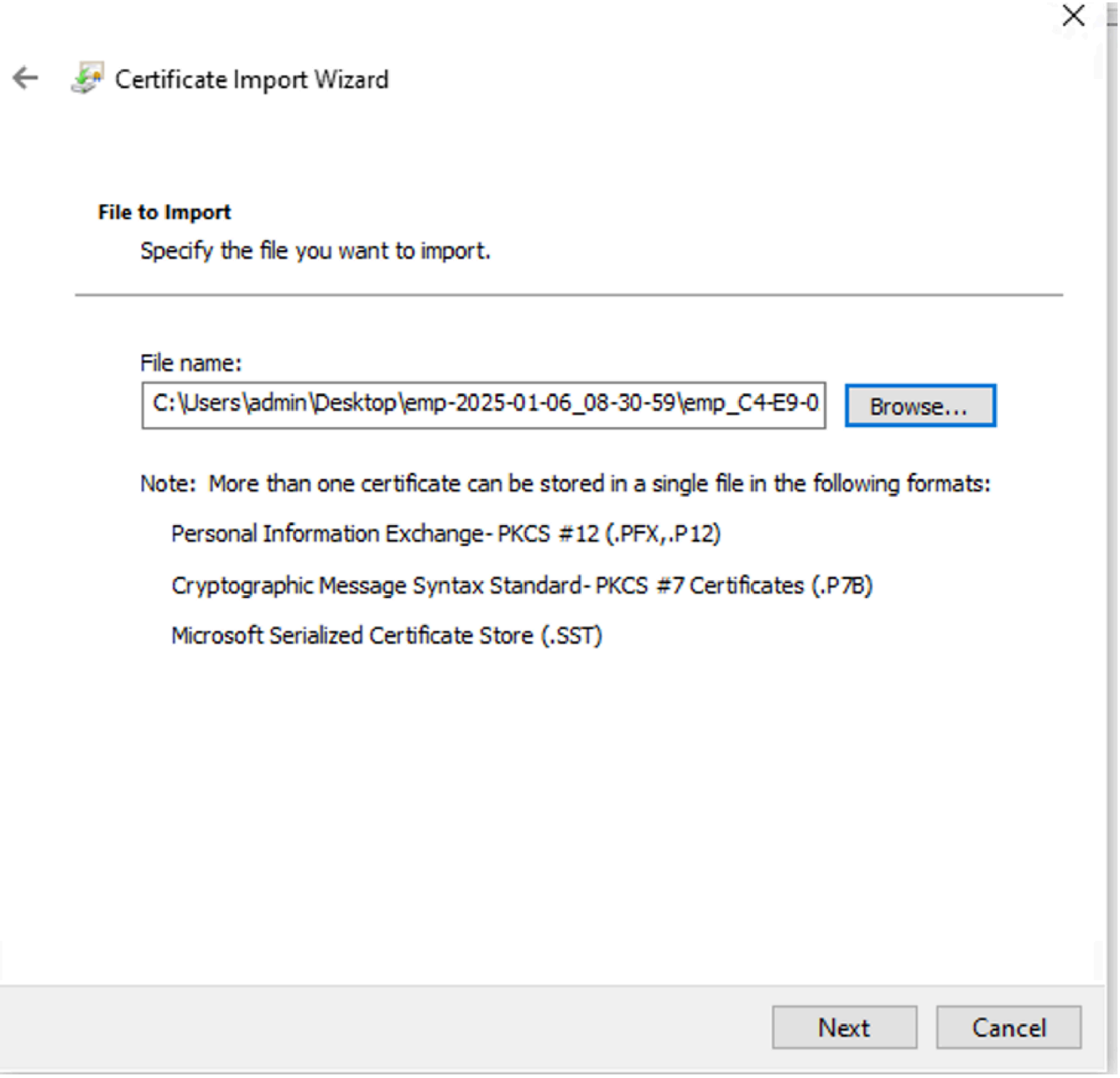
Windows MMC Console

Step 1. Import the Certificate:

1.1. Click on **Action** in the menu.

1.2. Go to **All Tasks**, then select **Import**.

1.3. Proceed through the prompts to locate and select the certificate file stored on your machine.



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

C:\Users\admin\Desktop\emp-2025-01-06_08-30-59\emp_C4-E9-0

Note: More than one certificate can be stored in a single file in the following formats:

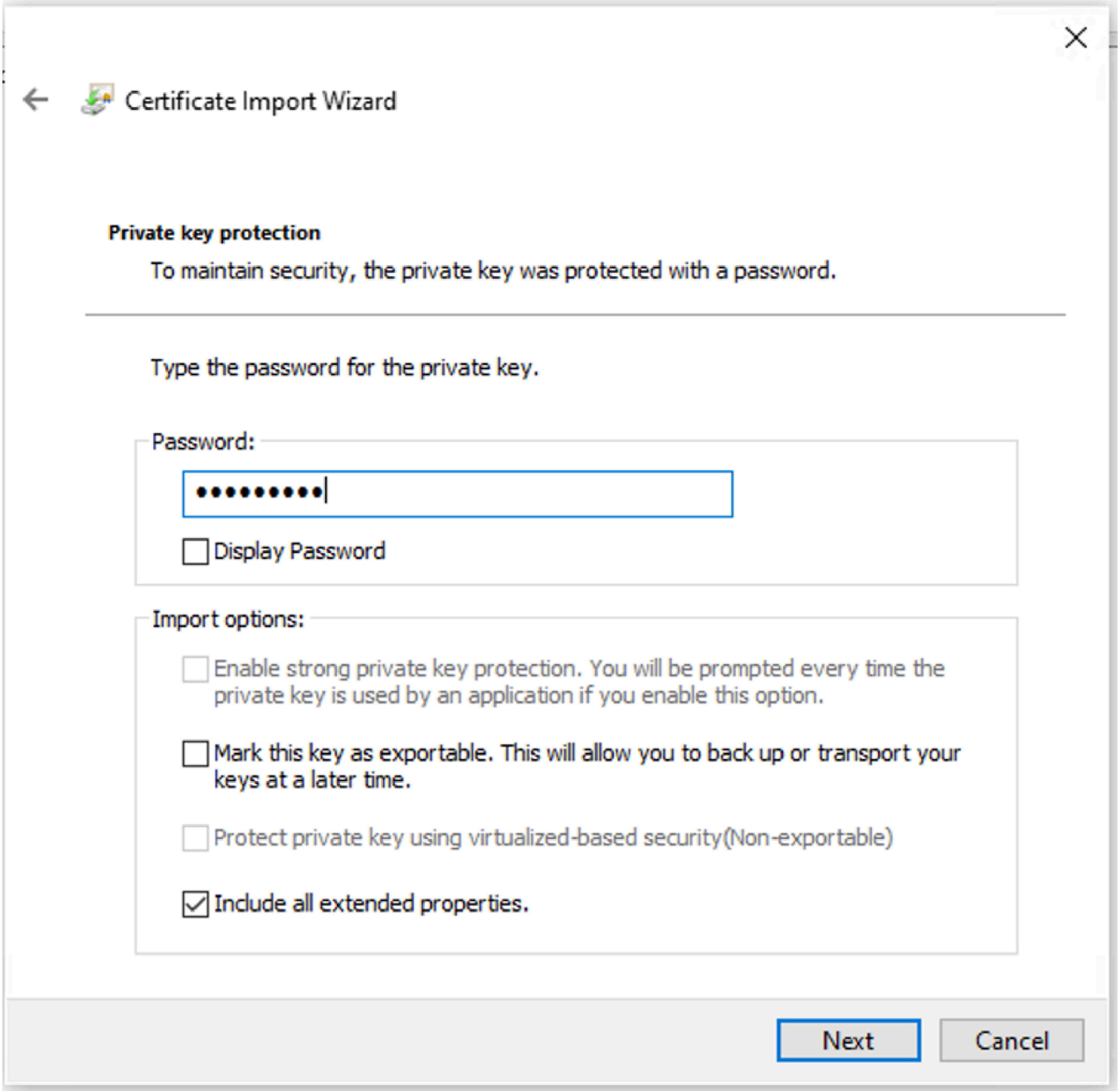
Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Importing Certificate

During the certificate import process, you are prompted to enter the password you created when generating the certificate on the portal. Ensure you enter this password accurately to successfully import and install the certificate on your machine.


Certificate Import Wizard

Private key protection

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

●●●●●●●●●●

□ Display Password

Import options:

□ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

□ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

□ Protect private key using virtualized-based security(Non-exportable)

☑ Include all extended properties.

Entering Certificate Password

Step 2. Move Certificates to Appropriate Folders:

2.1. Open the **Microsoft Management Console (MMC)** and navigate to the **Certificates (Local Computer) > Personal folder.**

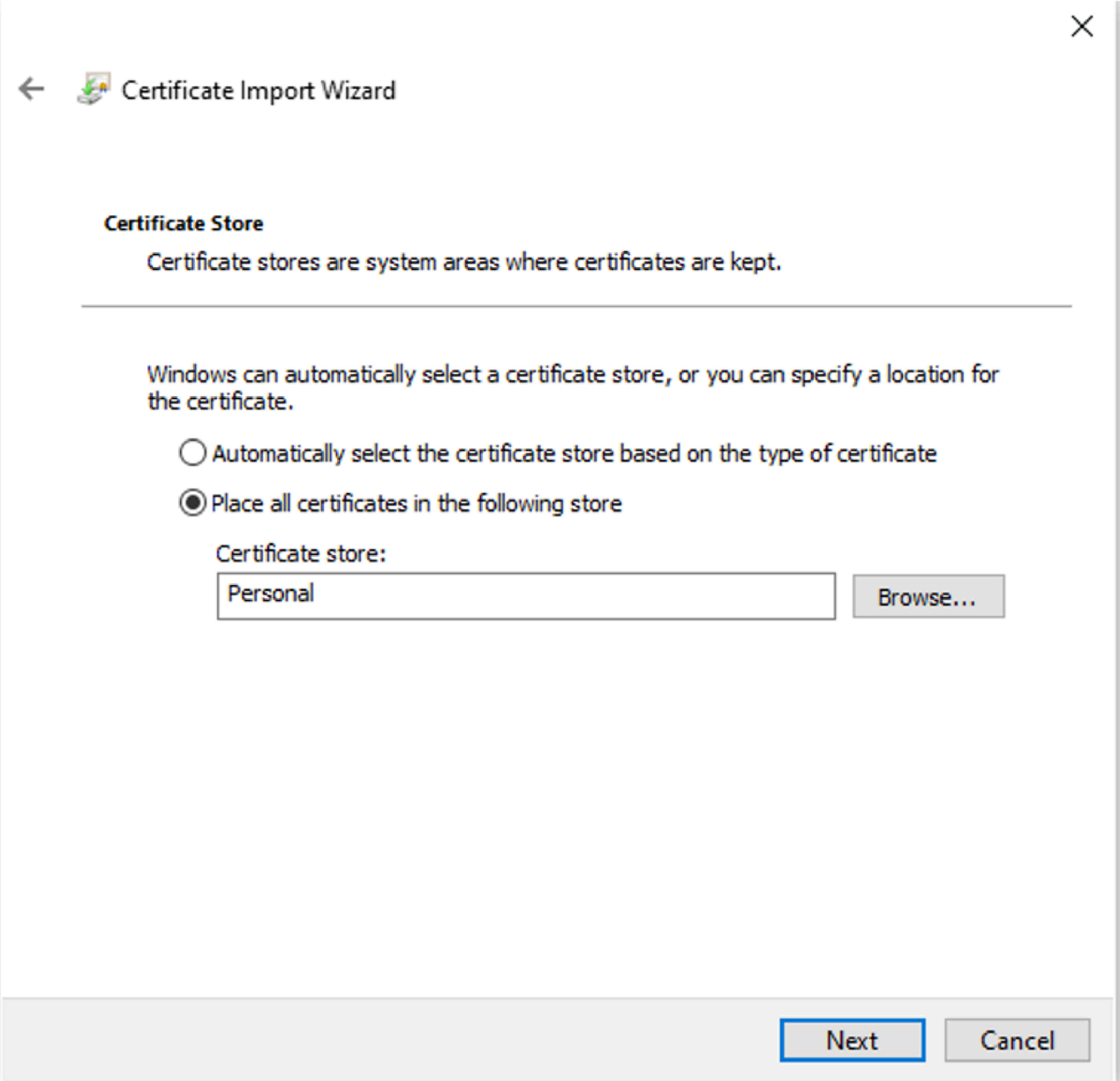
2.2. Review the certificates and determine their types (for example, Root CA, Intermediate CA, or Personal).

2.3. **Move** each certificate to the appropriate store:

2.4. Root CA Certificates: **Move** to Trusted Root Certification Authorities.

2.5. Intermediate CA Certificates: **Move** to Intermediate Certification Authorities.

2.6. Personal Certificates: **Leave** in the Personal folder.



Certificate Store

Certificate stores are system areas where certificates are kept.

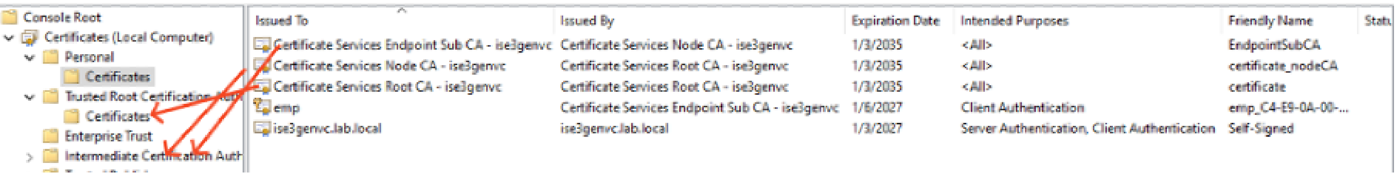
Windows can automatically select a certificate store, or you can specify a location for the certificate.

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

● Place all certificates in the following store

Certificate store: Personal

Storing Certificates in the Personal Folder


Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Auth
Certificates
Enterprise Trust
Intermediate Certification Auth

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Statu
Certificate Services Endpoint Sub CA - ise3genvc	Certificate Services Node CA - ise3genvc	1/3/2035	<All>	EndpointSubCA	
Certificate Services Node CA - ise3genvc	Certificate Services Root CA - ise3genvc	1/3/2035	<All>	certificate_nodeCA	
Certificate Services Root CA - ise3genvc	Certificate Services Root CA - ise3genvc	1/3/2035	<All>	certificate	
emp	Certificate Services Endpoint Sub CA - ise3genvc	1/6/2027	Client Authentication	emp_C4-E9-0A-00-...	
ise3genvc.lab.local	ise3genvc.lab.local	1/3/2027	Server Authentication, Client Authentication	Self-Signed	

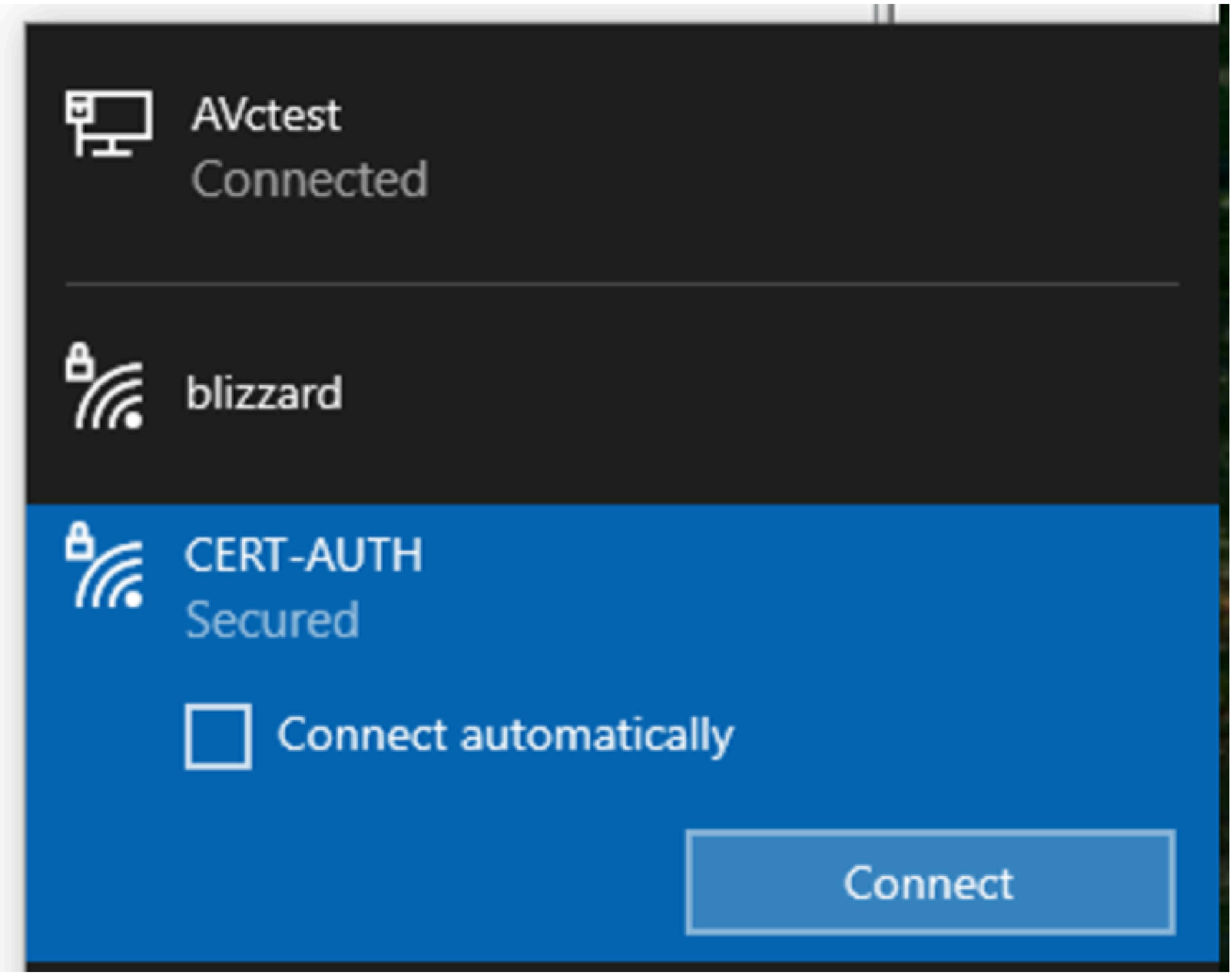
Moving Certificates in their Stores

Connecting the Windows Machine

Once the certificates are moved to the correct stores, use these steps to connect to the WLAN:

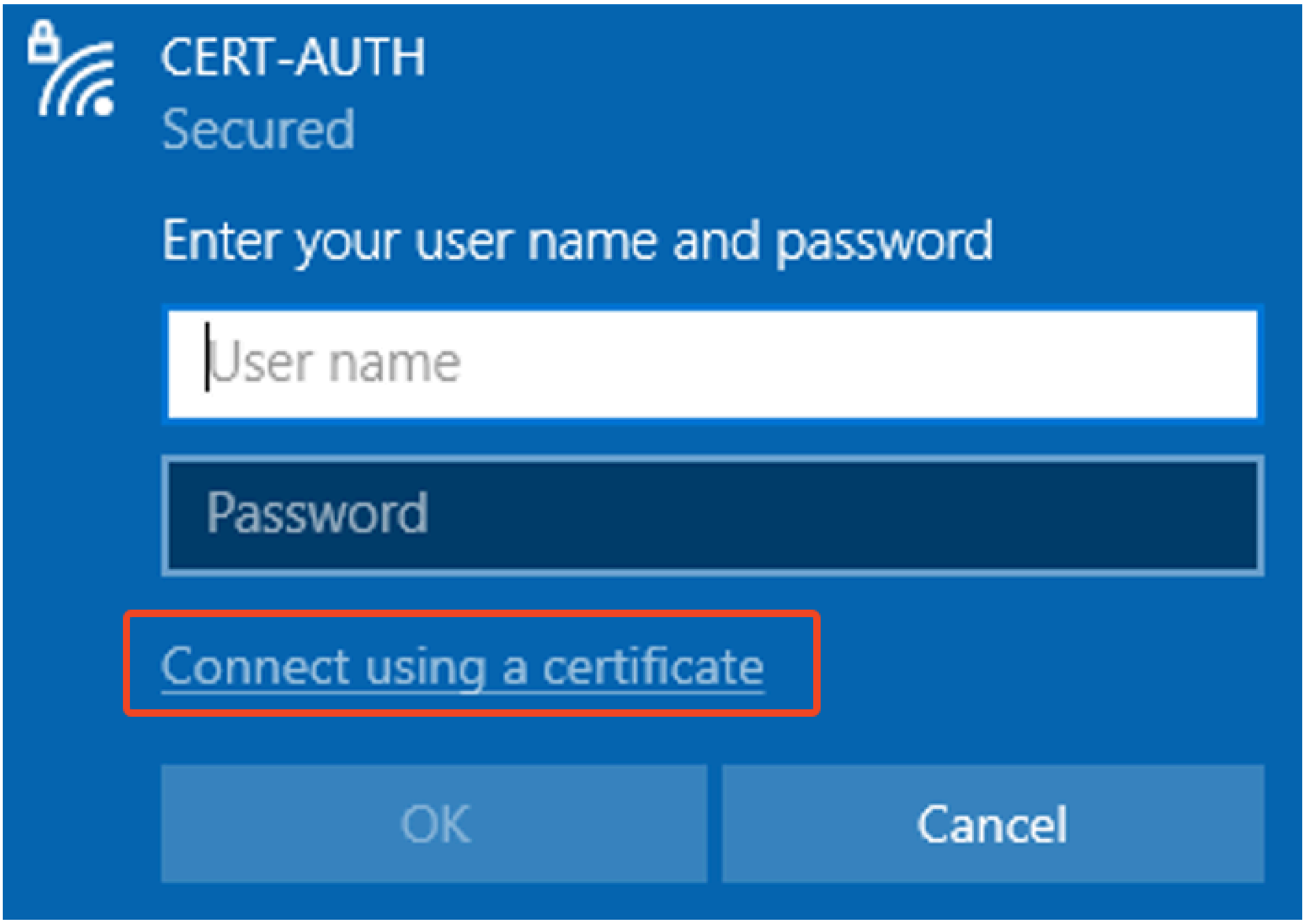
1. Click on the **network** icon in the system tray to view available wireless networks.
2. Find and **click** on the name of the WLAN you wish to connect to.
3. Click **Connect** and proceed with any additional prompts to complete the connection process using

your certificate for authentication.



Connecting to the Wireless Network

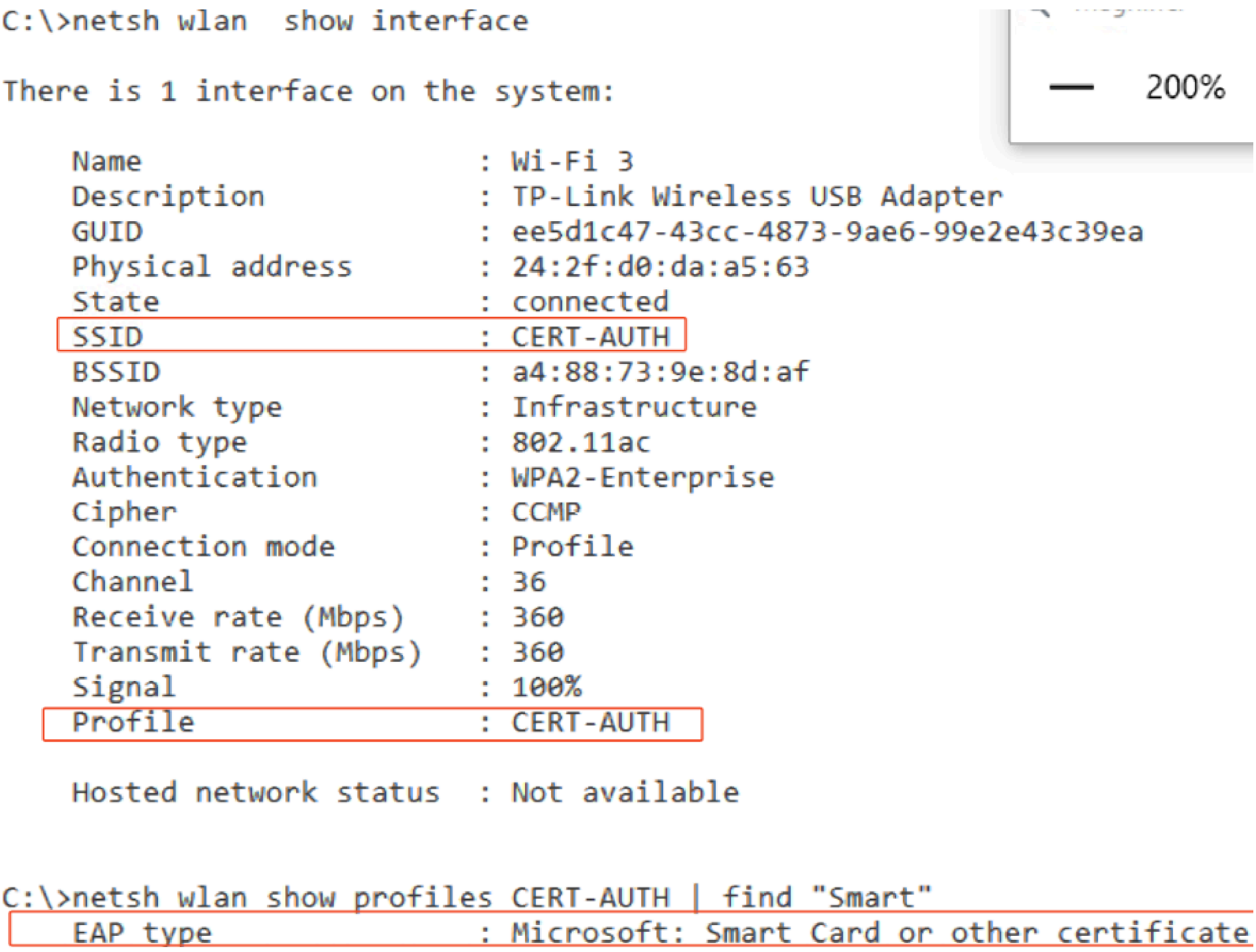
When prompted during the connection process to the WLAN, select the option to **Connect using a certificate.**


CERT-AUTH
Secured

Enter your user name and password

Using Certificate as Credential

This enables you to successfully connect to the wireless network using the certificate.



```
C:\>netsh wlan  show interface

There is 1 interface on the system:

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

    Hosted network status  : Not available


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

Verify Wireless Profile

Verify

Verify that the WLAN is being broadcast by the WLC:

<#root>

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

17

 CERT-AUTH

CERT-AUTH

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

Verify that the AP is up on the WLC:

```
POD6_9800#show ap summ
```

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

Ensure that the AP is broadcasting the WLAN:

<#root>

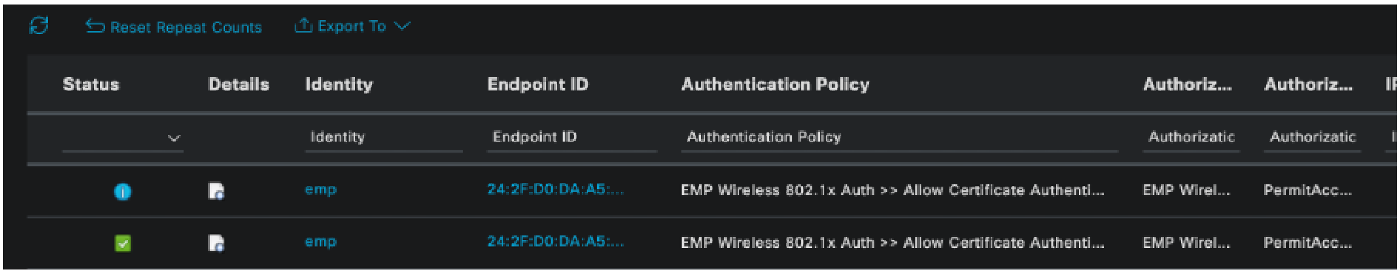
```
POD6_9800#show ap name AP1 wlan dot11 24ghz
Slot id : 0
WLAN ID BSSID
-------------------------
17 a488.739e.8da0

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

17

 a488.739e.8daf
```

Client connected using EAP-TLS:

<#root>

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

17

 IP Learn 11ac

Dot1x

 Local

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

Wireless LAN Network Name (SSID): CERT-AUTH


BSSID : a488.739e.8daf

EAP Type : EAP-TLS


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

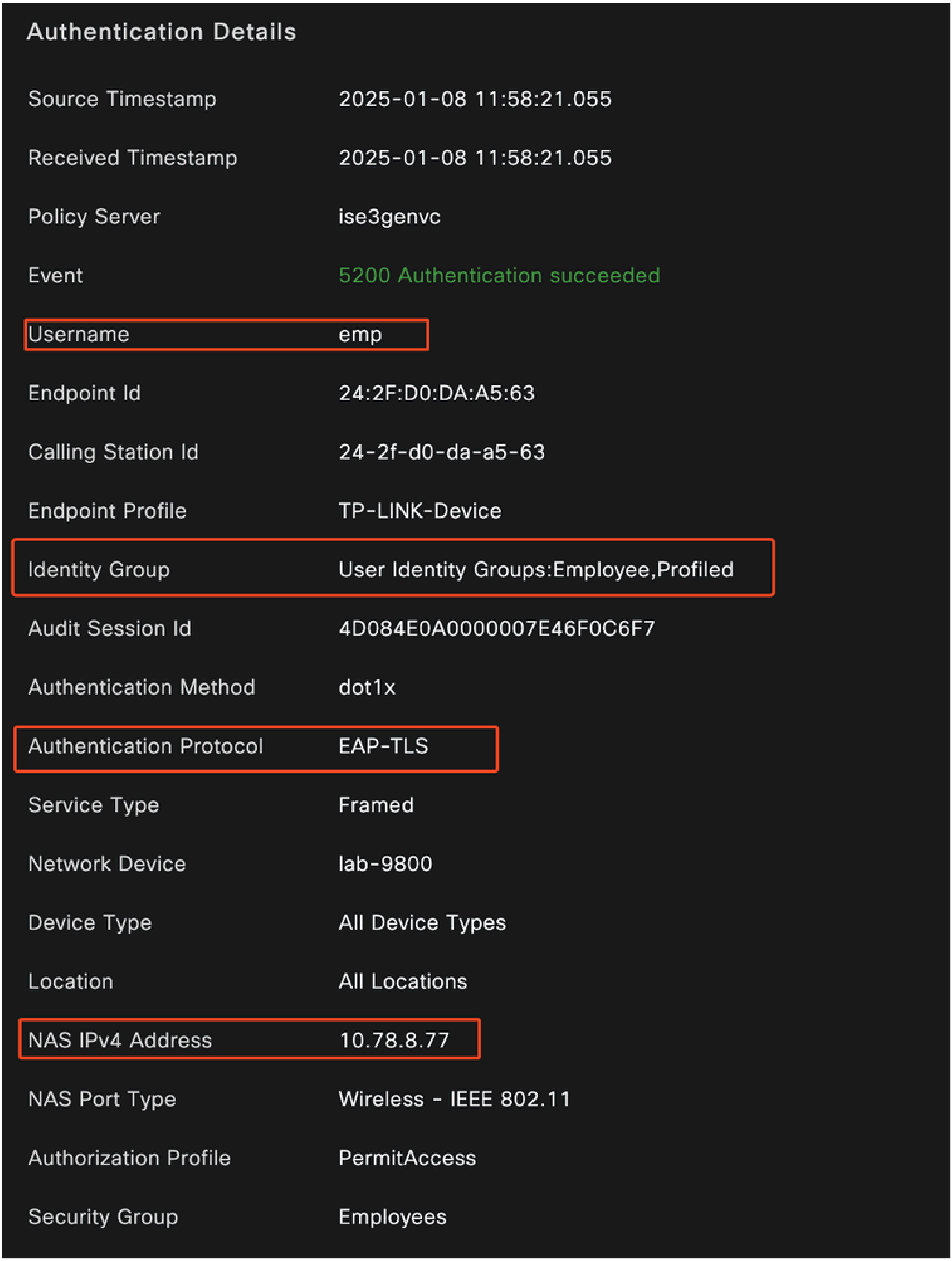
Cisco Radius ISE live logs:



Status	Details	Identity	Endpoint ID	Authentication Policy	Authoriz...	Authoriz...	I
		Identity	Endpoint ID	Authentication Policy	Authorizatic	Authorizatic	I
●		emp	24:2F:D0:DA:A5:...	EMP Wireless 802.1x Auth >> Allow Certificate Authenti...	EMP Wirel...	PermitAcc...	
✓		emp	24:2F:D0:DA:A5:...	EMP Wireless 802.1x Auth >> Allow Certificate Authenti...	EMP Wirel...	PermitAcc...	

ISE Radius Live Logs

Detailed authentication type:

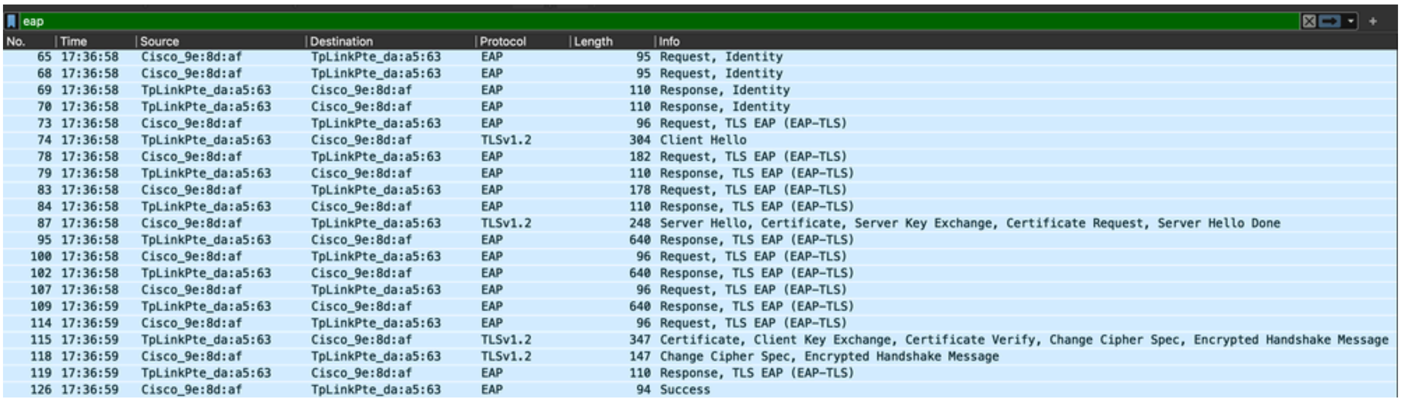


Authentication Details

Source Timestamp	2025-01-08 11:58:21.055
Received Timestamp	2025-01-08 11:58:21.055
Policy Server	ise3genvc
Event	5200 Authentication succeeded
Username	emp
Endpoint Id	24:2F:D0:DA:A5:63
Calling Station Id	24-2f-d0-da-a5-63
Endpoint Profile	TP-LINK-Device
Identity Group	User Identity Groups:Employee,Profiled
Audit Session Id	4D084E0A0000007E46F0C6F7
Authentication Method	dot1x
Authentication Protocol	EAP-TLS
Service Type	Framed
Network Device	lab-9800
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	10.78.8.77
NAS Port Type	Wireless - IEEE 802.11
Authorization Profile	PermitAccess
Security Group	Employees

ISE Detailed Logs

WLC EPC Capture showing the EAP-TLS packets:



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

WLC Capture Showing the EAP Transaction

- Packet number 87 corresponds to step 8 in the EAP-TLS Flow described at the beginning of the document.
- Packet number 115 corresponds to step 9 in the EAP-TLS Flow described at the beginning of the document.
- Packet number 118 corresponds to step 10 in the EAP-TLS Flow described at the beginning of the document.

Radio Active (RA) Trace Showing Client Connection: This RA trace is filtered to display a few of the relevant lines of the authentication transaction.

```
2025/01/08 11 58 20.816875191 {wncd_x_R0-2}{1} [ewlc-capwapmsg-sess] [15655] (debug) Encrypted DTLS message send. Dest IP 10.78.8.78[5256], length 499
2025/01/08 11 58 20.851392112 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Send Access-Request to 10.106.33.23 1812 id 0/25, len 390
2025/01/08 11 58 20.871842938 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Received from id 1812/25 10.106.33.23 0, Access-Challenge, len 123
2025/01/08 11 58 20.872246323 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Sent EAPOL packet - Version 3,EAPOL Type EAP, Payload Length 6, EAP-Type = EAP-TLS
2025/01/08 11 58 20.881960763 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Received EAPOL packet - Version 1,EAPOL Type EAP, Payload Length 204, EAP-Type = EAP-TLS
2025/01/08 11 58 20.882292551 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Send Access-Request to 10.106.33.23 1812 id 0/26, len 663
2025/01/08 11 58 20.926204990 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Received from id 1812/26 10.106.33.23 0, Access-Challenge, len 1135
2025/01/08 11 58 20.927390754 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Sent EAPOL packet - Version 3,EAPOL Type EAP, Payload Length 1012, EAP-Type = EAP-TLS
2025/01/08 11 58 20.935081108 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Received EAPOL packet - Version 1,EAPOL Type EAP, Payload Length 6, EAP-Type = EAP-TLS
2025/01/08 11 58 20.935405770 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Send Access-Request to 10.106.33.23 1812 id 0/27, len 465
2025/01/08 11 58 20.938485635 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Received from id 1812/27 10.106.33.23 0, Access-Challenge, len 1131
2025/01/08 11 58 20.939630108 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Sent EAPOL packet - Version 3,EAPOL Type EAP, Payload Length 1008, EAP-Type = EAP-TLS
2025/01/08 11 58 20.947417061 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Received EAPOL packet - Version 1,EAPOL Type EAP, Payload Length 6, EAP-Type
```

```
= EAP-TLS
2025/01/08 11 58 20.947722851 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Send Access-Request
to 10.106.33.23 1812 id 0/28, len 465
2025/01/08 11 58 20.949913199 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Received from id
1812/28 10.106.33.23 0, Access-Challenge, len 275
2025/01/08 11 58 20.950432303 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563
capwap_90800005] Sent EAPOL packet - Version 3,EAPOL Type EAP, Payload Length 158, EAP-Type =
EAP-TLS
2025/01/08 11 58 20.966862562 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563
capwap_90800005] Received EAPOL packet - Version 1,EAPOL Type EAP, Payload Length 1492, EAP-
Type = EAP-TLS
2025/01/08 11 58 20.967209224 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Send Access-Request
to 10.106.33.23 1812 id 0/29, len 1961
2025/01/08 11 58 20.971337739 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Received from id
1812/29 10.106.33.23 0, Access-Challenge, len 123
2025/01/08 11 58 20.971708100 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563
capwap_90800005] Sent EAPOL packet - Version 3,EAPOL Type EAP, Payload Length 6, EAP-Type =
EAP-TLS
2025/01/08 11 58 20.978742828 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563
capwap_90800005] Received EAPOL packet - Version 1,EAPOL Type EAP, Payload Length 1492, EAP-
Type = EAP-TLS
2025/01/08 11 58 20.979081544 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Send Access-Request
to 10.106.33.23 1812 id 0/30, len 1961
2025/01/08 11 58 20.982535977 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Received from id
1812/30 10.106.33.23 0, Access-Challenge, len 123
2025/01/08 11 58 20.982907200 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563
capwap_90800005] Sent EAPOL packet - Version 3,EAPOL Type EAP, Payload Length 6, EAP-Type =
EAP-TLS
2025/01/08 11 58 20.990141062 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563
capwap_90800005] Received EAPOL packet - Version 1,EAPOL Type EAP, Payload Length 1492, EAP-
Type = EAP-TLS
2025/01/08 11 58 20.990472026 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Send Access-Request
to 10.106.33.23 1812 id 0/31, len 1961
2025/01/08 11 58 20.994358525 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Received from id
1812/31 10.106.33.23 0, Access-Challenge, len 123
2025/01/08 11 58 20.994722151 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563
capwap_90800005] Sent EAPOL packet - Version 3,EAPOL Type EAP, Payload Length 6, EAP-Type =
EAP-TLS
2025/01/08 11 58 21.001735553 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563
capwap_90800005] Received EAPOL packet - Version 1,EAPOL Type EAP, Payload Length 247, EAP-
Type = EAP-TLS
2025/01/08 11 58 21.002076369 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Send Access-Request
to 10.106.33.23 1812 id 0/32, len 706
2025/01/08 11 58 21.013571608 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Received from id
1812/32 10.106.33.23 0, Access-Challenge, len 174
2025/01/08 11 58 21.013987785 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563
capwap_90800005] Sent EAPOL packet - Version 3,EAPOL Type EAP, Payload Length 57, EAP-Type =
EAP-TLS
2025/01/08 11 58 21.024429150 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563
capwap_90800005] Received EAPOL packet - Version 1,EAPOL Type EAP, Payload Length 6, EAP-Type
= EAP-TLS
2025/01/08 11 58 21.024737996 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Send Access-Request
to 10.106.33.23 1812 id 0/33, len 465
2025/01/08 11 58 21.057794929 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Received from id
```

```
1812/33 10.106.33.23 0, Access-Accept, len 324
2025/01/08 11 58 21.058149893 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563
capwap_90800005] Raised identity update event for eap method EAP-TLS
```

Troubleshoot

There are no specific troubleshooting steps for this issue beyond the typical Wireless 802.1x troubleshooting procedures:

1. Take Client RA trace debugs to check the authentication process.
2. Perform a WLC EPC capture to examine the packets between the client, WLC, and RADIUS server.
3. Check ISE live logs to verify that the request is matching the correct policy.
4. Verify on the Windows endpoint that the certificate is installed correctly and that the entire trust chain is present.

References

- Certificate Provisioning Portal FAQs, Release 3.2
- Understand ISE Internal Certificate Authority Services
- Understand and Configure EAP-TLS with a WLC and ISE