Configure 802.1X Supplicant for Access Points with 9800 Controller

Contents

Introduction

This document describes how to configure a Cisco Access Point (AP) as a 802.1x supplicant to be authorized on a switchport against a RADIUS server.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Wireless Lan Controller (WLC) and LAP (lightweight Access Point).
- 802.1x on Cisco switches and ISE
- Extensible Authentication Protocol (EAP)
- Remote Authentication Dial-In User Service (RADIUS)

Components Used

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

- WS-C3560CX, Cisco IOS® XE,15.2(3r)E2

- C9800-CL-K9, Cisco IOS® XE,17.6.5
- ISE 3.0
- AIR-CAP3702
- AIR-AP3802

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

In this setup, the access point (AP) acts as the 802.1x supplicant and is authenticated by the switch against the ISE with the EAP method EAP-FAST.

Once the port is configured for 802.1X authentication, the switch does not allow any traffic other than 802.1X traffic to pass through the port until the device connected to the port authenticates successfully.

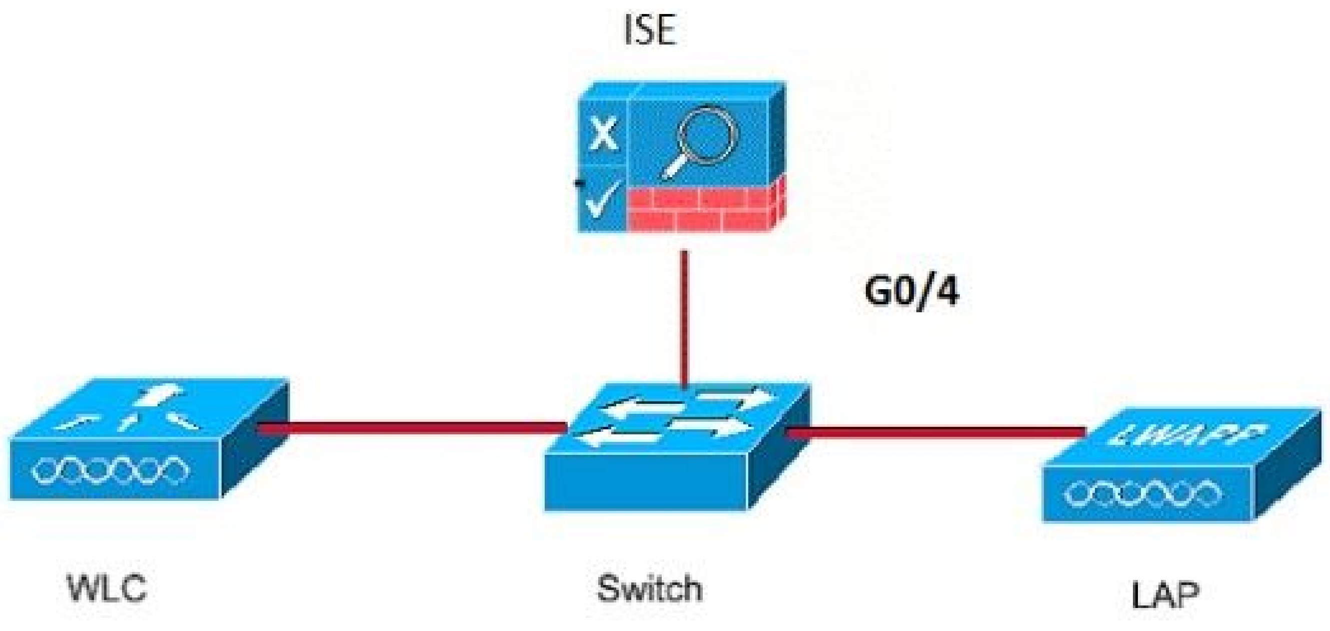
An AP can be authenticated either before it joins a WLC or after it has joined a WLC, in which case, configure 802.1X on the switch after the LAP joins the WLC.

Configure

In this section, you are presented with the information to configure the features described in this document.

Network Diagram

This document uses this network setup:

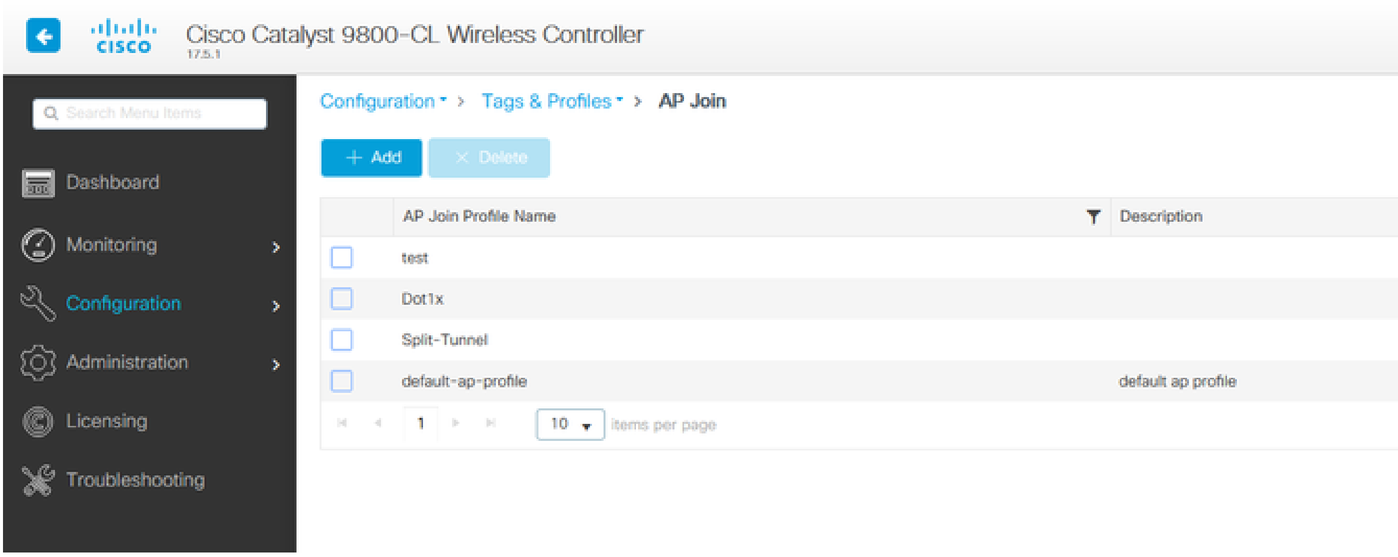


Configure the LAP As An 802.1x Supplicant

If The AP Is Already Joined To The WLC:

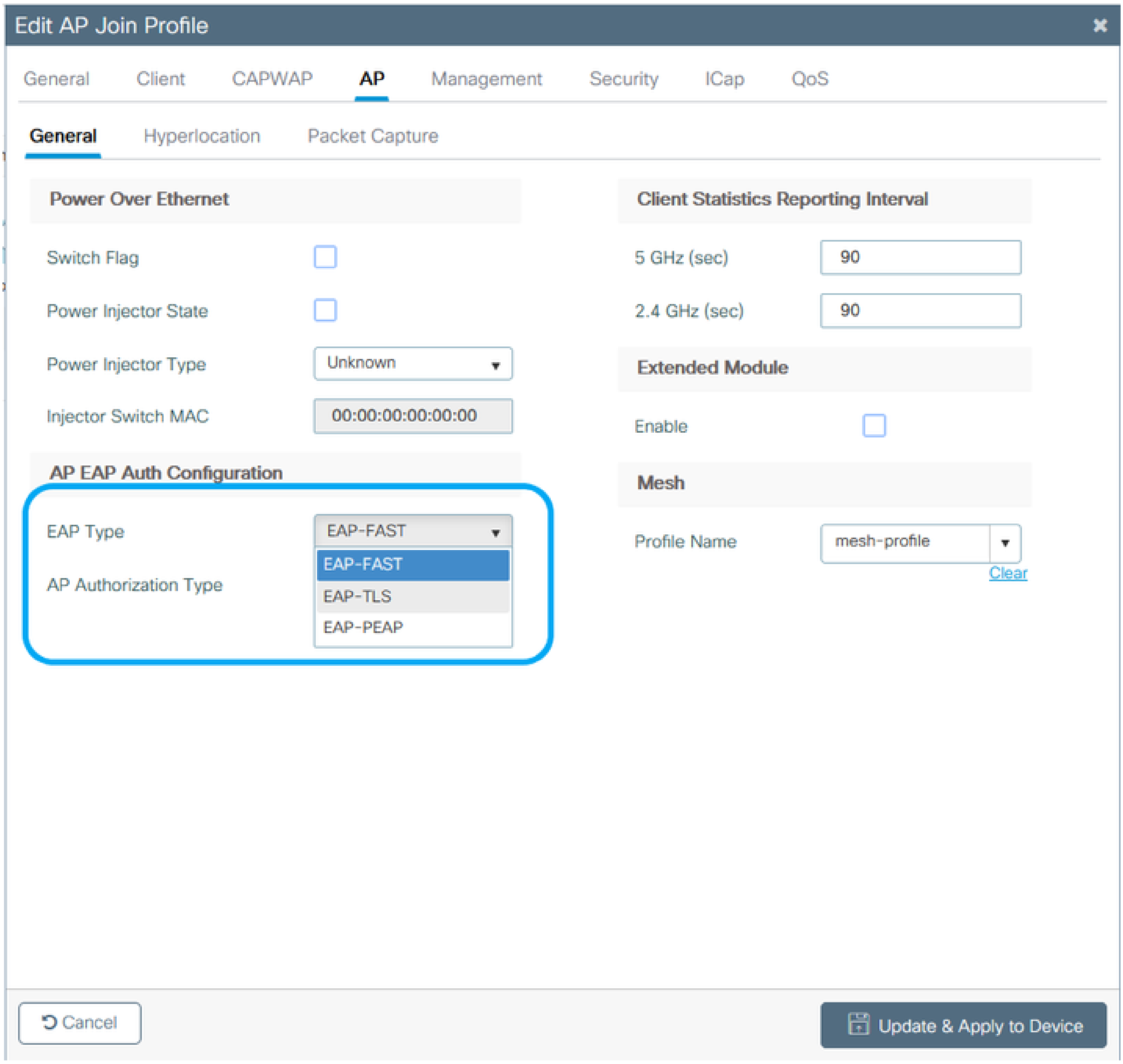
Configure 802.1x Authentication Type and Locally Significant Certificate (LSC) AP Authentication Type:

Step 1. Navigate to **Configuration** > **Tags & Profiles** > **AP Join** > On the **AP Join Profile** page, click **Add** to add a new join profile or edit an AP join profile when you click its name.



	AP Join Profile Name	Description
□	test	
□	Dot1x	
□	Split-Tunnel	
□	default-ap-profile	default ap profile

Step 2. In the AP Join Profile page, from **AP** > **General**, navigate to the **AP EAP Auth Configuration** section. From the **EAP Type** drop-down list, choose the EAP type as EAP-FAST, EAP-TLS, or EAP-PEAP to configure the dot1x authentication type. EAP-FAST is the only authentication type that uses username and passwords only and is the easiest to setup. PEAP and EAP-TLS require you to provision certificates on the access points through the LSC workflow (see the references section).



Edit AP Join Profile

Power Over Ethernet

Switch Flag □

Power Injector State □

Power Injector Type: Unknown

Injector Switch MAC: 00:00:00:00:00:00

AP EAP Auth Configuration

EAP Type: EAP-FAST

AP Authorization Type

Client Statistics Reporting Interval

5 GHz (sec): 90

2.4 GHz (sec): 90

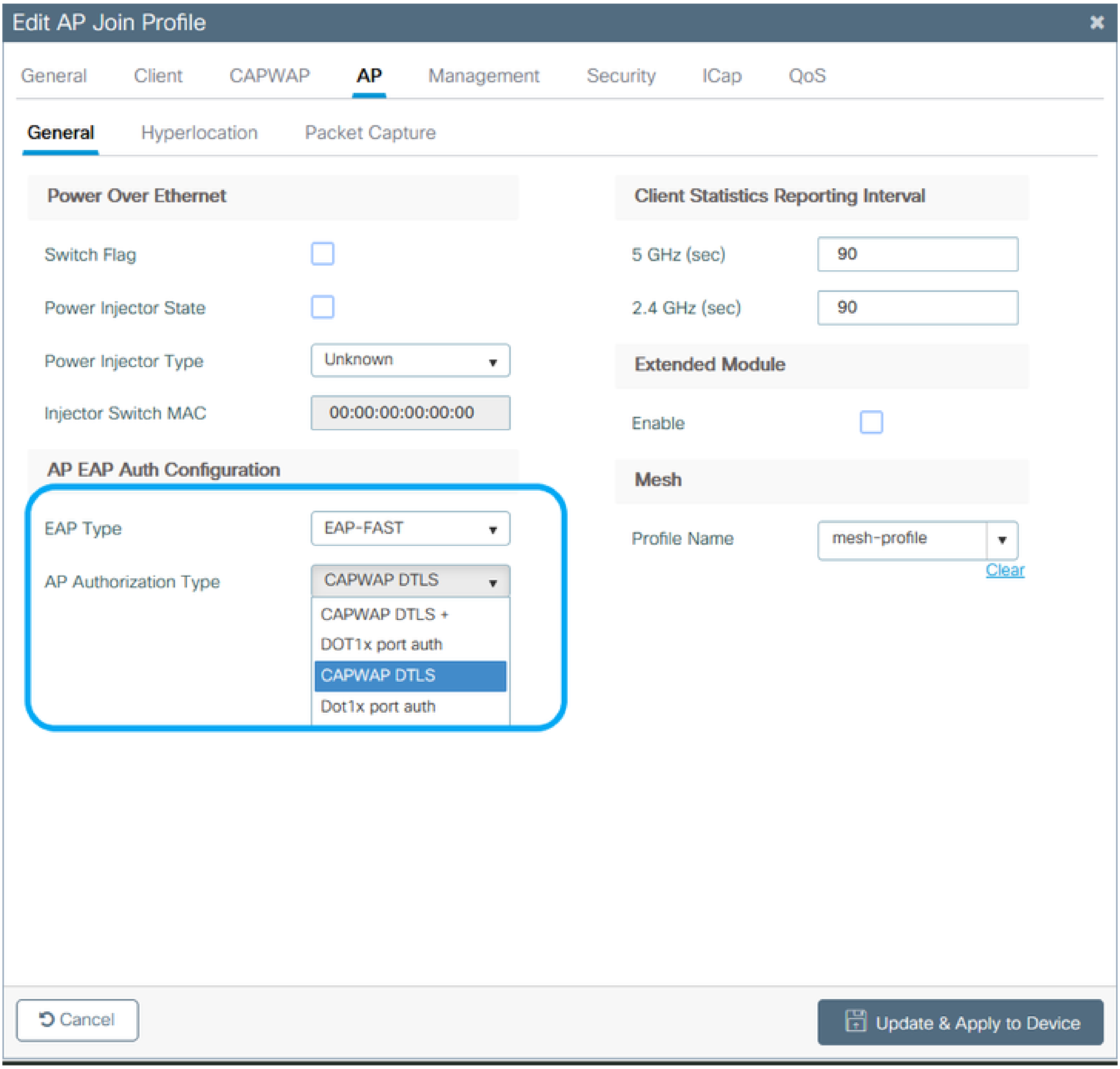
Extended Module

Enable □

Mesh

Profile Name: mesh-profile

Step 3. From the **AP Authorization Type** drop-down list, choose the type as either CAPWAP DTLS + or CAPWAP DTLS > Click **Update & Apply to Device**.



Edit AP Join Profile

Power Over Ethernet

Switch Flag □

Power Injector State □

Power Injector Type: Unknown

Injector Switch MAC: 00:00:00:00:00:00

AP EAP Auth Configuration

EAP Type: EAP-FAST

AP Authorization Type: CAPWAP DTLS

- CAPWAP DTLS +
- DOT1x port auth
- CAPWAP DTLS
- Dot1x port auth

Client Statistics Reporting Interval

5 GHz (sec): 90

2.4 GHz (sec): 90

Extended Module

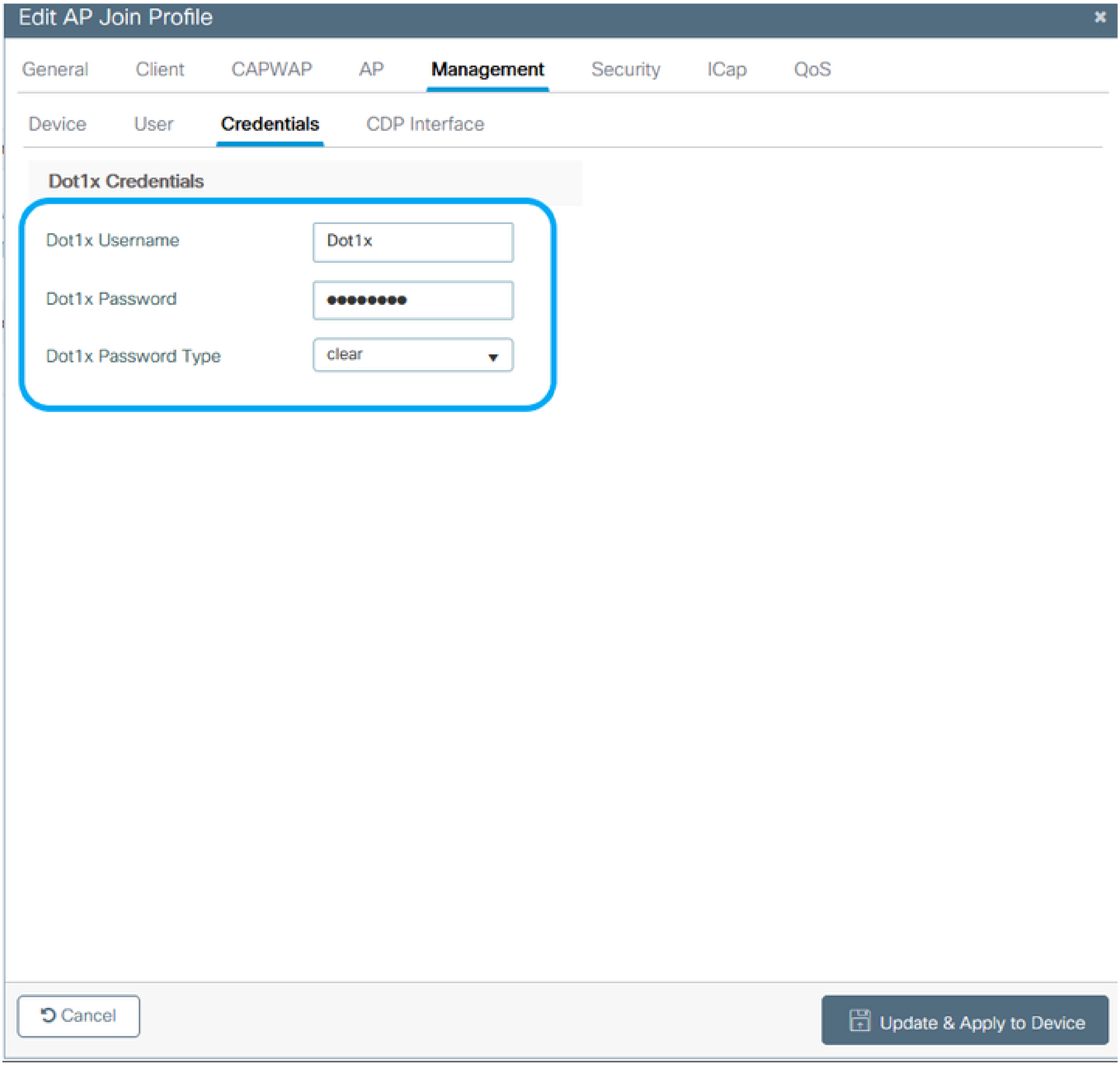
Enable □

Mesh

Profile Name: mesh-profile

Configure the 802.1x Username and Password:

Step 1. From **Management** > **Credentials** > **Enter Dot1x username and password details** > Choose the appropriate 802.1x password type > Click **Update & Apply to Device**



Dot1x Credentials

Dot1x Username: Dot1x

Dot1x Password: ●●●●●●●●●

Dot1x Password Type: clear

If The AP Has Not Joined To A WLC Yet:

Console into the LAP in order to set the credentials and use these CLI commands: (for Cheetah OS & Cisco IOS® APs)

CLI:

<#root>

```
LAP#

debug capwap console cli


LAP#

capwap ap dot1x username <username> password <password>
```

To Clear The Dot1x Credentials On The AP (If Needed)

For Cisco IOS® APs, after that reload the AP:

CLI:

<#root>

```
LAP#

clear capwap ap dot1x
```

For Cisco COS APs, after that reload the AP:

CLI:

<#root>

```
LAP#

capwap ap dot1x disable
```

Configure the Switch

Enable dot1x on the switch globally and add the ISE server to the switch.

CLI:

<#root>

```
Enable


Configure terminal


aaa new-model
aaa authentication dot1x default group radius


aaa authorization network default group radius


dot1x system-auth-control
Radius-server host <ISE IP address> auth-port <port> acct-port <port>
  key 7 <server key>
```

Configure the AP switch port.

CLI:

<#root>

```
configure terminal



interface GigabitEthernet</>
switchport access vlan <>
switchport mode access
authentication order dot1x
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast edge



end
```

If the AP is in **Flex Connect mode, local switching**, then an additional configuration has to be made on the switch interface to allow multiple MAC addresses on the port, since the client traffic is released at the AP level :

<#root>

```
authentication host-mode multi-host
```

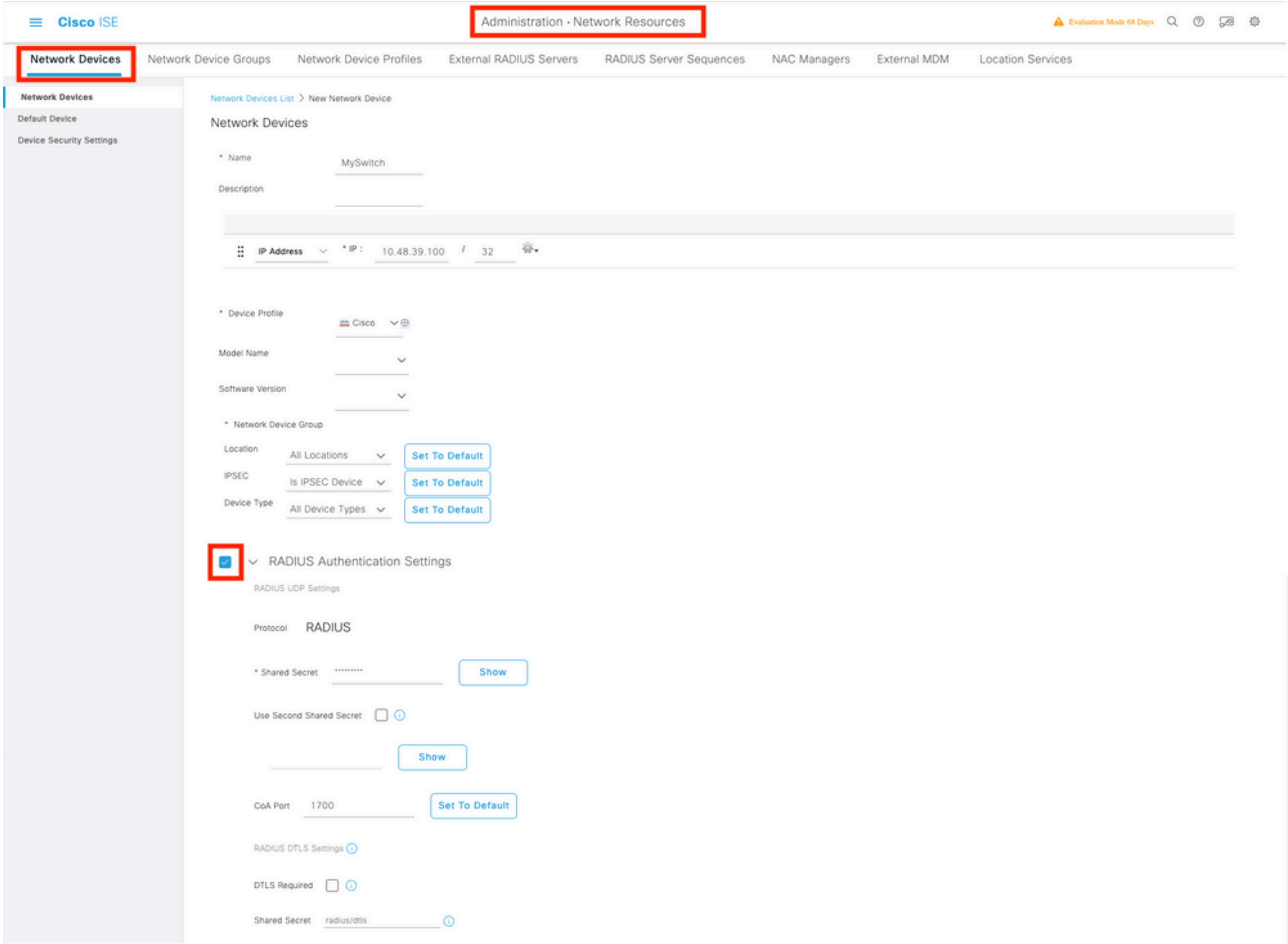
Note: Means reader take note. Notes contain helpful suggestions or references to material not covered in the document.

Note: Multi-host mode-authenticates the first MAC address and then allows an unlimited number of other MAC addresses. Enable the host mode on the switch ports if connected AP has been configured with local switching mode. It allows the client's traffic pass the switch port. If you want a secured traffic path, then enable dot1x on the WLAN to protect the client data

---

Configure the ISE Server

Step 1. **Add the switch as a network device on the ISE server.** Navigate to **Administration** > **Network Resources** > **Network Devices** > Click **Add** > Enter Device name, IP address, enable RADIUS Authentication Settings, Specify Shared Secret Value, COA port (or leave it as default) > **Submit**.



Network Devices

* Name: MySwitch

Description:

IP Address * IP : 10.48.39.100 / 32

* Device Profile: Cisco

Model Name:

Software Version:

* Network Device Group

Location: All Locations

IPSEC: Is IPSEC Device

Device Type: All Device Types

☑ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol: RADIUS

* Shared Secret: ·········

Use Second Shared Secret ☐

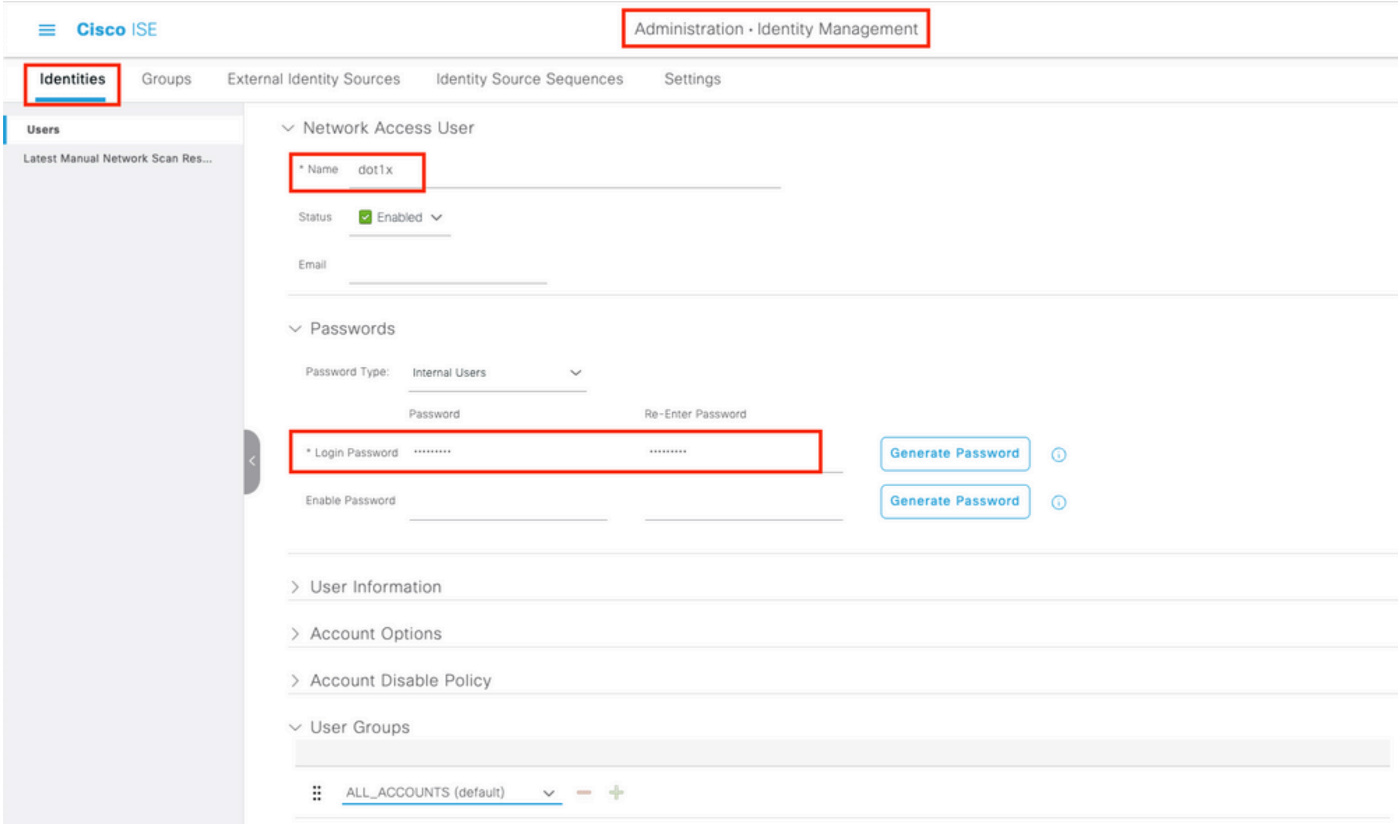
CoA Port: 1700

RADIUS DTLS Settings

DTLS Required ☐

Shared Secret: radius/dtls

Step 2**. Add the AP credentials to ISE**. Navigate to **Administration > Identity Management > Identities > Users** and click the **Add** button to add an user. Enter the credentials you configured on your AP Join Profile on your WLC. Note that the user is put in the default group here, but this can be adjusted as per your requirements.


Cisco ISE
Administration · Identity Management
Identities
Groups
External Identity Sources
Identity Source Sequences
Settings
Users
Latest Manual Network Scan Res...

Network Access User

* Name dot1x

Status ☑ Enabled

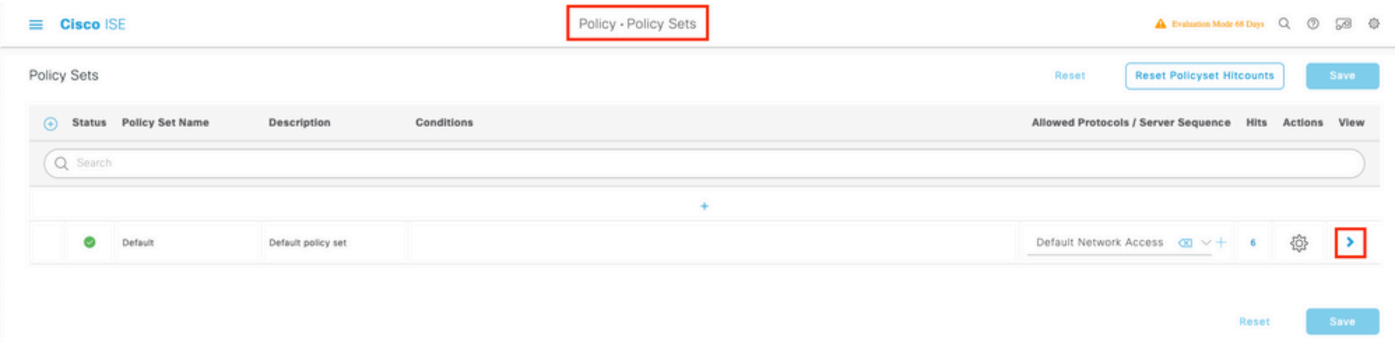
Email

Passwords

Password Type: Internal Users

	Password	Re-Enter Password
* Login Password	·········	·········
Enable Password		

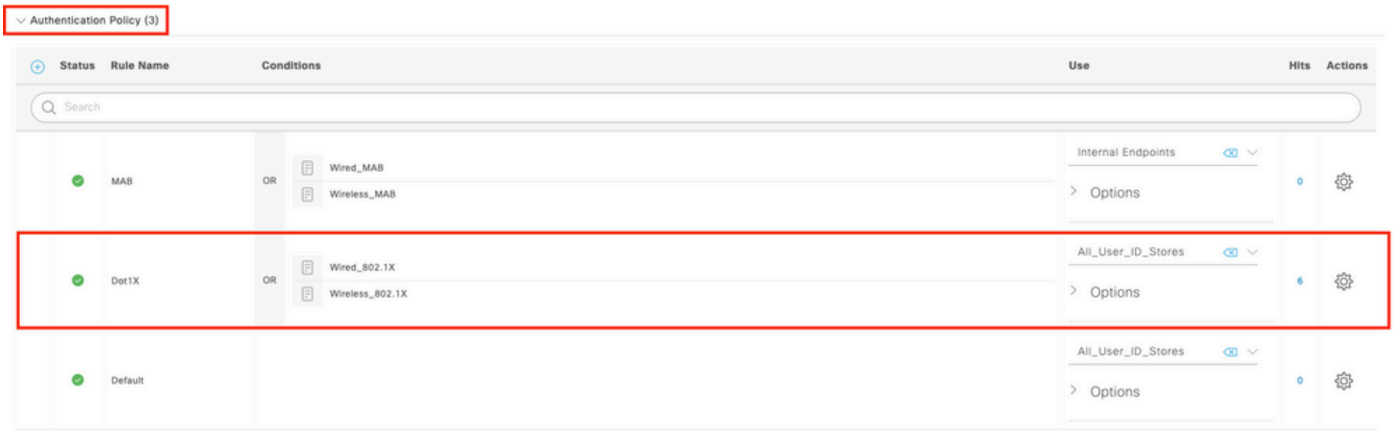
Step 3. On ISE, configure the **Authentication policy** and **Authorization policy**. Go to **Policy > Policy Sets** and select the policy set to configure and the blue arrow on the right. In this case, the default policy set is used but one can customize it as per the requirement.



Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
●	Default	Default policy set		Default Network Access	6	⚙	>

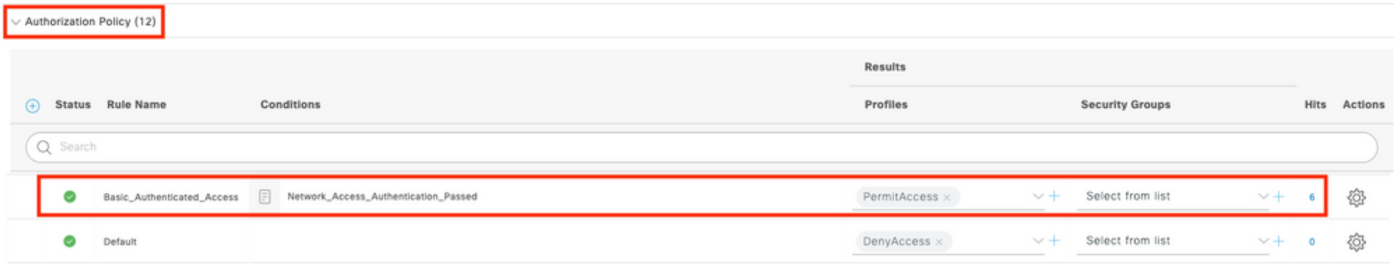
Then configure the **Authentication Policy and the Authorization Policy**. The policies shown here are the default policies created on the ISE server but can be adapted and customized as per your requirement.

In this example, the configuration can be translated into : "If wired 802.1X is used and the user is known on the ISE server, then we permit access to the users for which the authentication was successfull". The AP is then be authorized against the ISE server.



Authentication Policy (3)

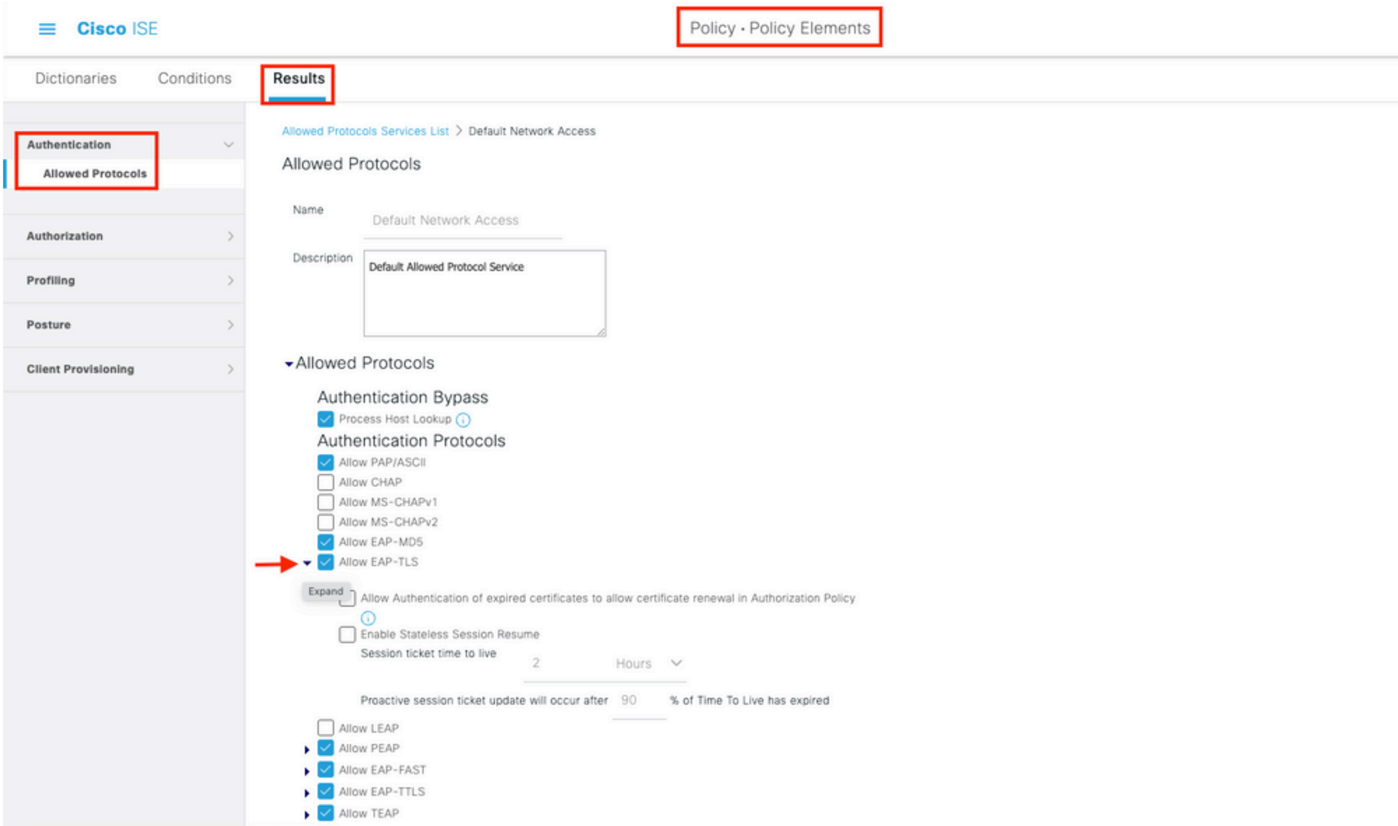
Status	Rule Name	Conditions	Use	Hits	Actions
●	MAB	OR Wired_MAB Wireless_MAB	Internal Endpoints Options	0	⚙
●	Dot1X	OR Wired_802.1X Wireless_802.1X	All_User_ID_Stores Options	6	⚙
●	Default		All_User_ID_Stores Options	0	⚙



Authorization Policy (12)

Status	Rule Name	Conditions	Results: Profiles	Results: Security Groups	Hits	Actions
●	Basic_Authenticated_Access	Network_Access_Authentication_Passed	PermitAccess	Select from list	6	⚙
●	Default		DenyAccess	Select from list	0	⚙

Step 4. Ensure that in the allowed protocols that Default Network Access, EAP-FAST is allowed. Navigate to **Policy** > **Policy Elements** > **Authentication** > **Results** > **Allowed Protocols** > **Default Network Access** > Enable **Allow EAP-TLS** > **Save**.



Allowed Protocols

Name: Default Network Access

Description: Default Allowed Protocol Service

Allowed Protocols

Authentication Bypass

☑ Process Host Lookup

Authentication Protocols

☑ Allow PAP/ASCII
□ Allow CHAP
□ Allow MS-CHAPv1
□ Allow MS-CHAPv2
☑ Allow EAP-MD5
☑ Allow EAP-TLS
□ Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy
□ Enable Stateless Session Resume
Session ticket time to live 2 Hours
Proactive session ticket update will occur after 90 % of Time To Live has expired
□ Allow LEAP
☑ Allow PEAP
☑ Allow EAP-FAST
☑ Allow EAP-TTLS
☑ Allow TEAP

Verify

Use this section to confirm that your configuration works properly.

Verify the Authentication Type

The show command displays the authentication information of an AP profile:

CLI:

```
9800WLC#show ap profile name <profile-name> detailed
```

Example:

```
9800WLC#show ap profile name default-ap-profile detailed
  AP Profile Name        : Dot1x
  …
  Dot1x EAP Method       : [EAP-FAST/EAP-TLS/EAP-PEAP/Not-Configured]
  LSC AP AUTH STATE      : [CAPWAP DTLS / DOT1x port auth / CAPWAP DTLS + DOT1x port auth]
```

Verify 802.1x on the Switch Port

The show command displays the authentication state of 802.1x on the switch port:

CLI:

```
Switch# show dot1x all
```

Output example:

```
Sysauthcontrol              Enabled
Dot1x Protocol Version            3

Dot1x Info for GigabitEthernet0/8
-----------------------------------
PAE                       = AUTHENTICATOR
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
```

Verify if the port has been authenticated or not

CLI:

```
Switch#show dot1x interface <AP switch port number> details
```

Output example:

```
Dot1x Info for GigabitEthernet0/8
-----------------------------------
PAE                       = AUTHENTICATOR
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30

Dot1x Authenticator Client List
-------------------------------
EAP Method                = FAST
Supplicant                = f4db.e67e.dd16
Session ID                = 0A30279E00000BB7411A6BC4
    Auth SM State         = AUTHENTICATED
    Auth BEND SM State    = IDLE
ED
Auth BEND SM State = IDLE
```

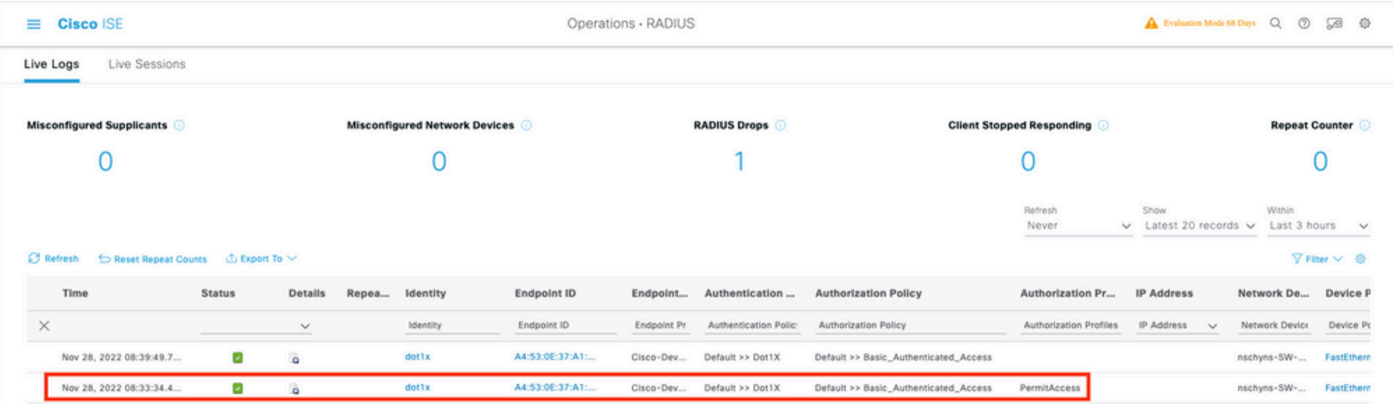
From CLI:

```
Switch#show authentication sessions
```

Output example:

```
Interface    MAC Address    Method  Domain  Status Fg Session ID
Gi0/8        f4db.e67e.dd16 dot1x   DATA    Auth      0A30279E00000BB7411A6BC4
```

In ISE, choose **Operations** > **Radius Livelogs** and confirm that the authentication is successful and the correct Authorization profile is pushed.



Misconfigured Supplicants: 0

Misconfigured Network Devices: 0

RADIUS Drops: 1

Client Stopped Responding: 0

Repeat Counter: 0

Refresh: Never

Show: Latest 20 records

Within: Last 3 hours

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authentication ...	Authorization Policy	Authorization Pr...	IP Address	Network De...	Device P
				Identity	Endpoint ID	Endpoint Pr	Authentication Polic	Authorization Policy	Authorization Profiles	IP Address	Network Devic	Device Pc
Nov 28, 2022 08:39:49.7...	✓			dot1x	A4:53:0E:37:A1:...	Cisco-Dev...	Default >> Dot1X	Default >> Basic_Authenticated_Access			nschyns-SW-...	FastEthern
Nov 28, 2022 08:33:34.4...	✓			dot1x	A4:53:0E:37:A1:...	Cisco-Dev...	Default >> Dot1X	Default >> Basic_Authenticated_Access	PermitAccess		nschyns-SW-...	FastEthern

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

1. Enter the **ping** command in order to check if the ISE server is reachable from the switch.
2. Make sure that the switch is configured as an AAA client on the ISE server.
3. Ensure that the shared secret is the same between the switch and the ISE server.
4. Check if EAP-FAST is enabled on the ISE server.
5. Check if the 802.1x credentials are configured for the LAP and are the same on the ISE server.
   Note: The username and password are case sensitive.
6. If authentication fails, enter these commands on the switch: **debug dot1x** and **debug authentication**.

Note that Cisco IOS based access points (802.11ac wave 1) do not support TLS version 1.1 and 1.2. This can cause an issue if your ISE or RADIUS server is configured to only allow TLS 1.2 inside 802.1X authentication.

References

Configuring 802.1X on APs with PEAP and EAP-TLS