Configure ISE BYOD with Single and Dual SSID in ISE 3.3

Contents

Introduction

The document describes how to configure and troubleshoot BYOD issues on ISE.

Background

BYOD is a feature which enables user to onboard their personal devices on ISE so that the user could use the network resource on the environment. It also helps the Network Administrator to restrict the user from accessing the critical resource from the personal devices.

Unlike guest flow where the device is authenticated with the Guest page using the internal store or Active directory on ISE. The BYOD allows the network administrator to install an endpoint profile on the endpoint to choose the type of EAP method. In scenarios like EAP-TLS, the client certificate is signed by the ISE itself to create a trust between the endpoint and ISE.

Prerequisites

Cisco recommends that you have knowledge of these topics:

- WLC controller
- Basic Knowledge on ISE

Component Used

These devices used are not restricted to one particular version for the BYOD flow:

- Catalyst 9800-CL Wireless Controller (17.12.3)
- ISE Virtual Machine (3.3)

What is Single SSID and Dual SSID BYOD on ISE?

Single SSID BYOD

In a Single SSID BYOD setup, users connect their personal devices directly to the corporate wireless network. The onboarding process occurs on the same SSID, where ISE facilitates device registration, provisioning, and policy enforcement. This approach simplifies user experience but requires secure onboarding and proper authentication methods to ensure network security.

Dual SSID BYOD

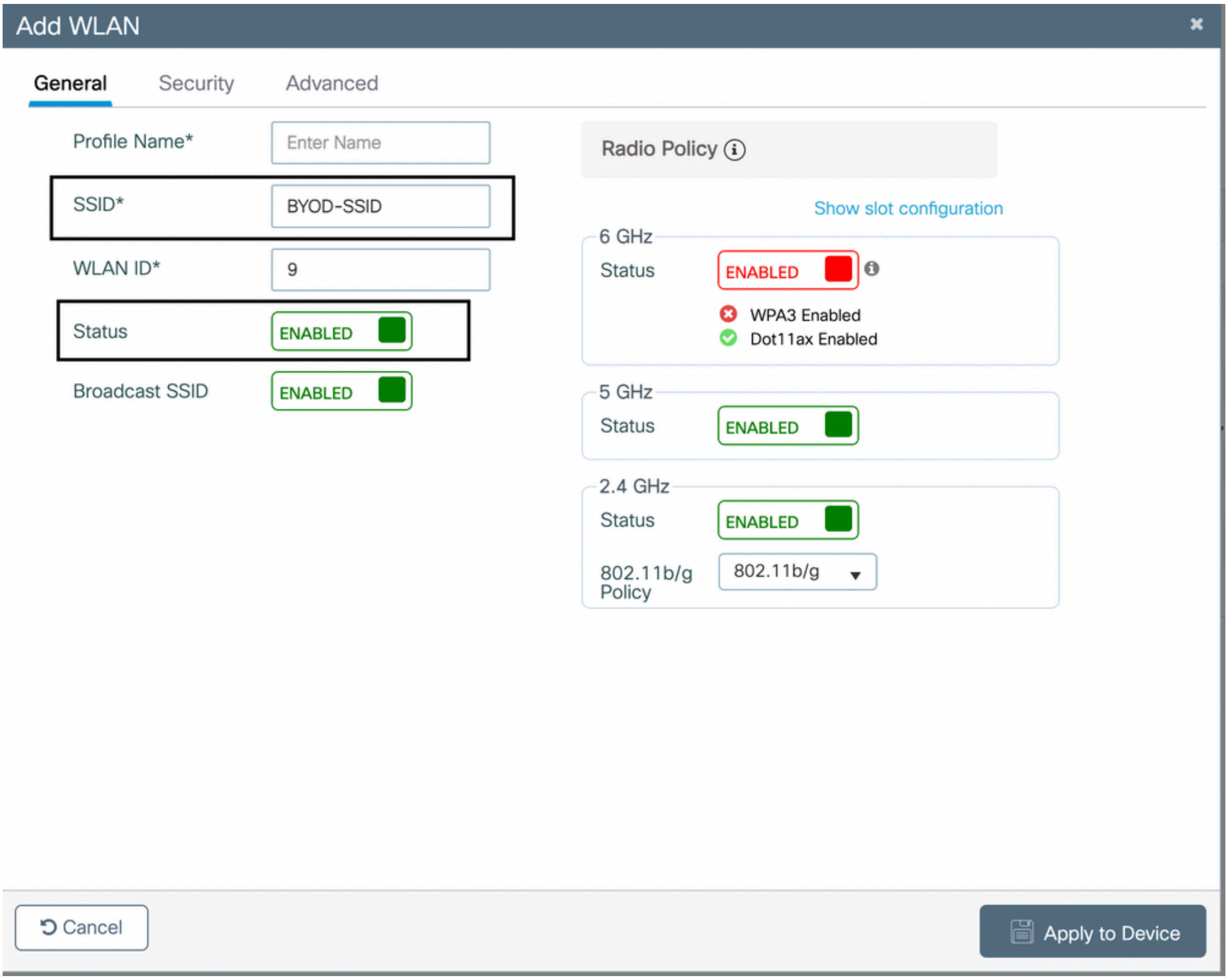
In a Dual SSID BYOD setup, two separate SSIDs are used: one for onboarding (unsecured or restricted access) and another for accessing the corporate network. Users initially connect to the onboarding SSID, complete device registration and provisioning via ISE, and then switch to the secure corporate SSID for network access. This provides an additional layer of security by segregating onboarding traffic from production traffic.

WLC Configuration

Create a WLAN for CWA

1. Go to **Configuration > Tags & Profiles > WLANs**.
2. Click **Add** to create a new WLAN.

- Set a WLAN Name and SSID (for example., BYOD-WiFi).
- Enable the WLAN.



Profile Name* Enter Name

SSID* BYOD-SSID

WLAN ID* 9

Status ENABLED

Broadcast SSID ENABLED

6 GHz

Status ENABLED

☒ WPA3 Enabled

✓ Dot11ax Enabled

5 GHz

Status ENABLED

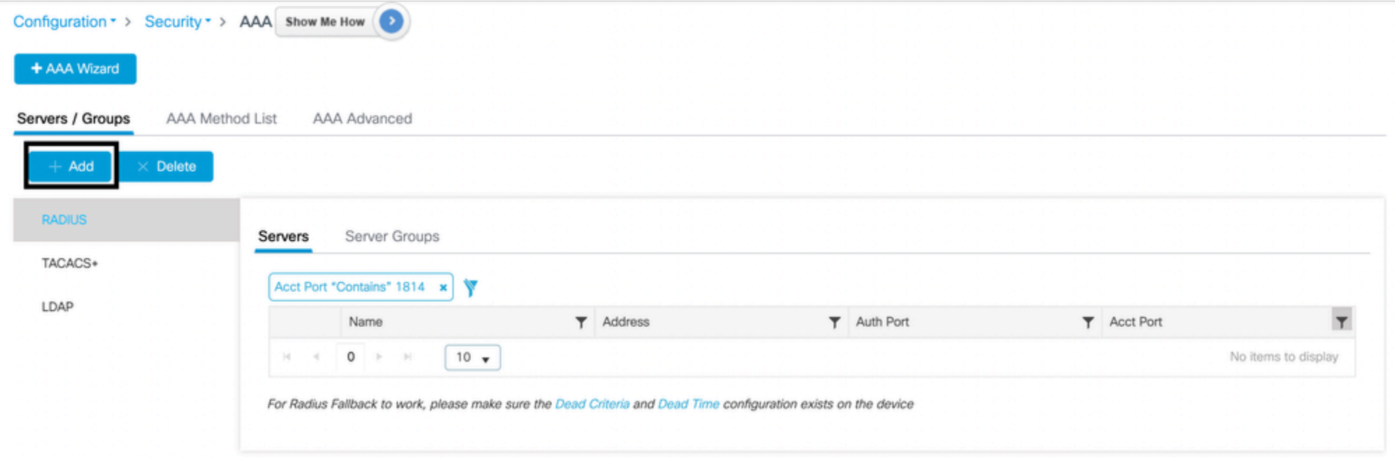
2.4 GHz

Status ENABLED

802.11b/g Policy 802.11b/g

Configure RADIUS Servers

1. Navigate to **Configuration** > **Security** > **AAA** > **RADIUS** > **Servers**.



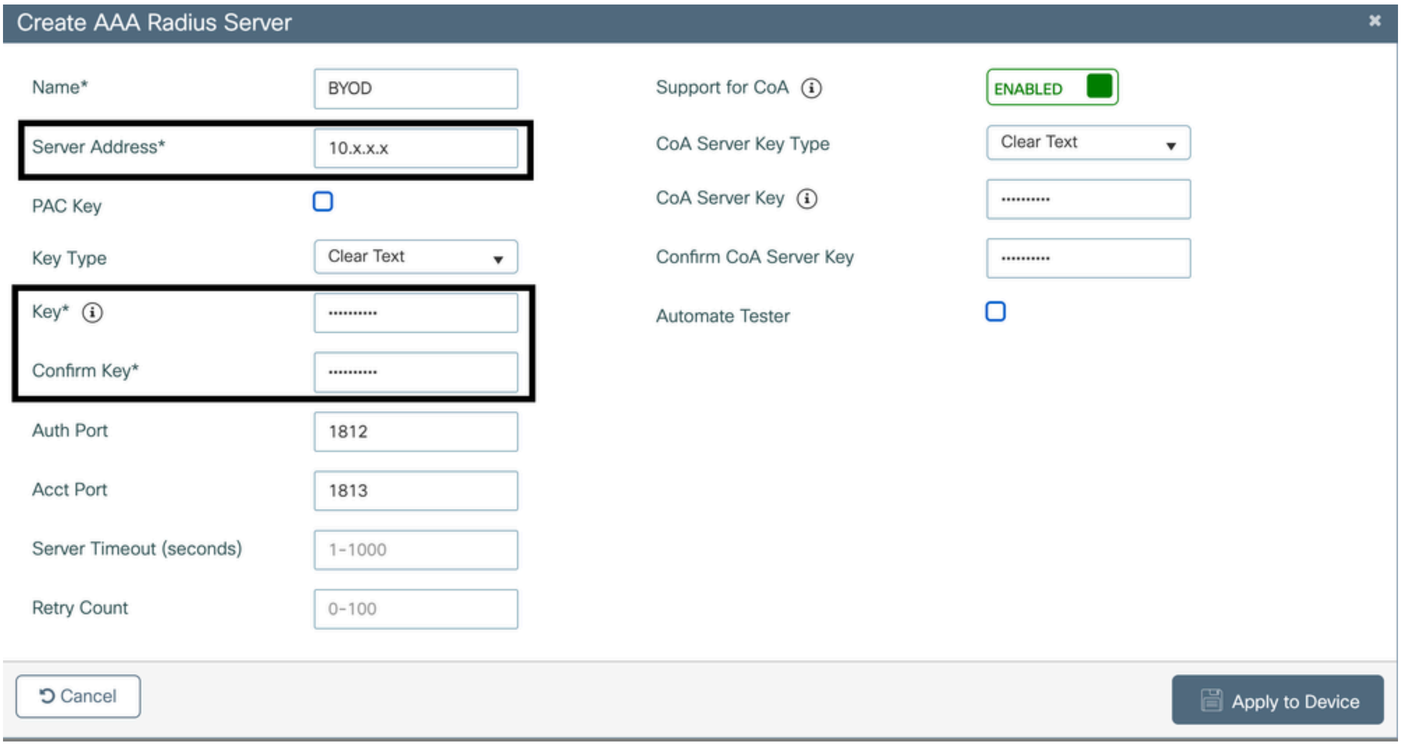
Acct Port "Contains" 1814 ×

Name	Address	Auth Port	Acct Port

0 10 ▾ No items to display

For Radius Fallback to work, please make sure the Dead Criteria and Dead Time configuration exists on the device

2. Click **Add** to configure ISE as a RADIUS server:
    - Server IP: IP address of ISE.
    - Shared Secret: Match the shared secret configured on ISE.

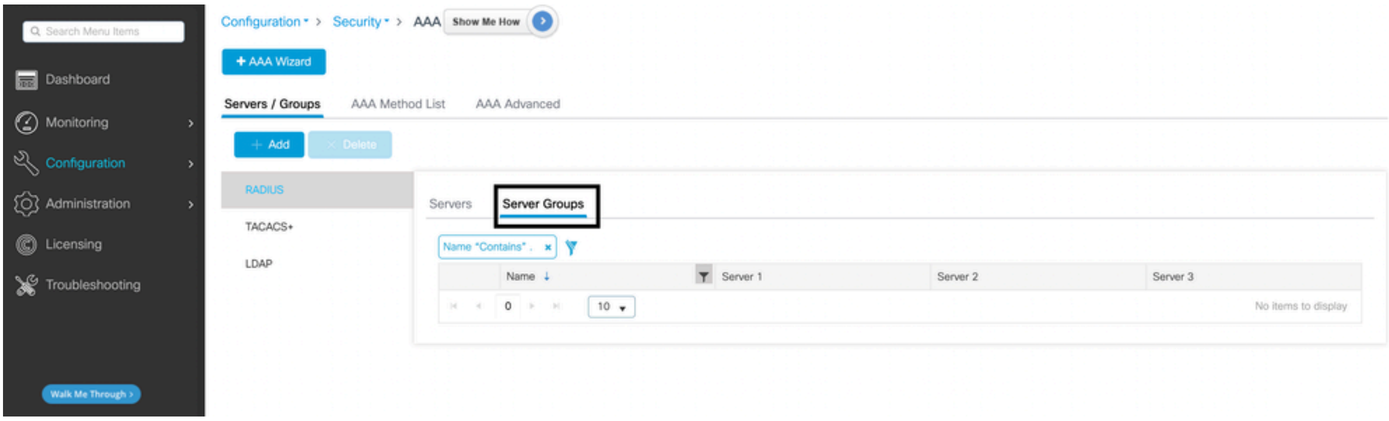


Create AAA Radius Server

Name*	BYOD	Support for CoA	ENABLED
Server Address*	10.x.x.x	CoA Server Key Type	Clear Text
PAC Key	□	CoA Server Key	••••••••••
Key Type	Clear Text	Confirm CoA Server Key	••••••••••
Key*	••••••••••	Automate Tester	□
Confirm Key*	••••••••••		
Auth Port	1812		
Acct Port	1813		
Server Timeout (seconds)	1-1000		
Retry Count	0-100		

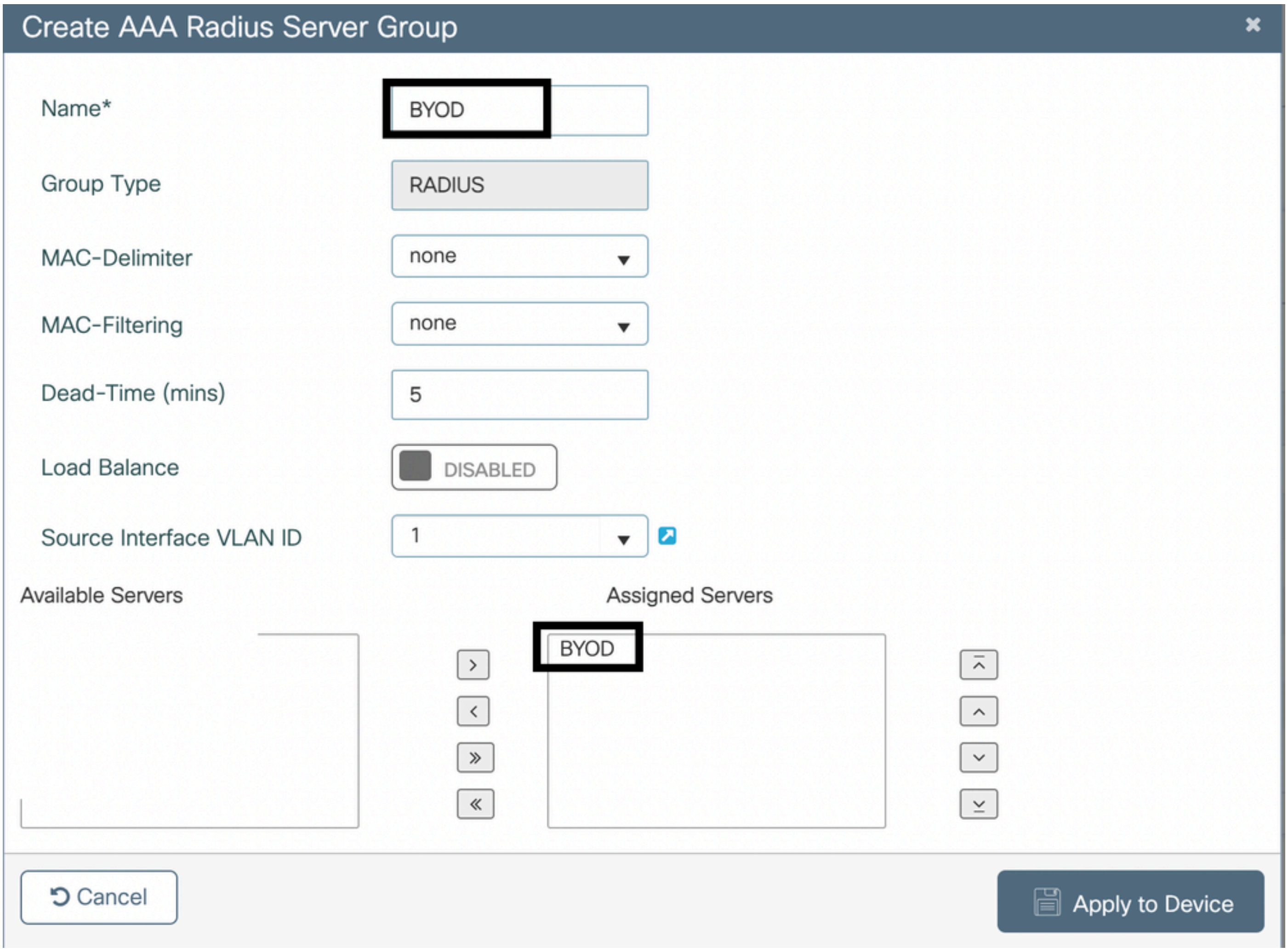
Configure AAA Servers

1. Navigate to **Configuration** > **Security** > **AAA** > **Servers/Groups**.



Name	Server 1	Server 2	Server 3
0 10			No items to display

2. Assign the RADIUS server to a new or existing Server Group.



Create AAA Radius Server Group

Name*: BYOD

Group Type: RADIUS

MAC-Delimiter: none

MAC-Filtering: none

Dead-Time (mins): 5

Load Balance: DISABLED

Source Interface VLAN ID: 1

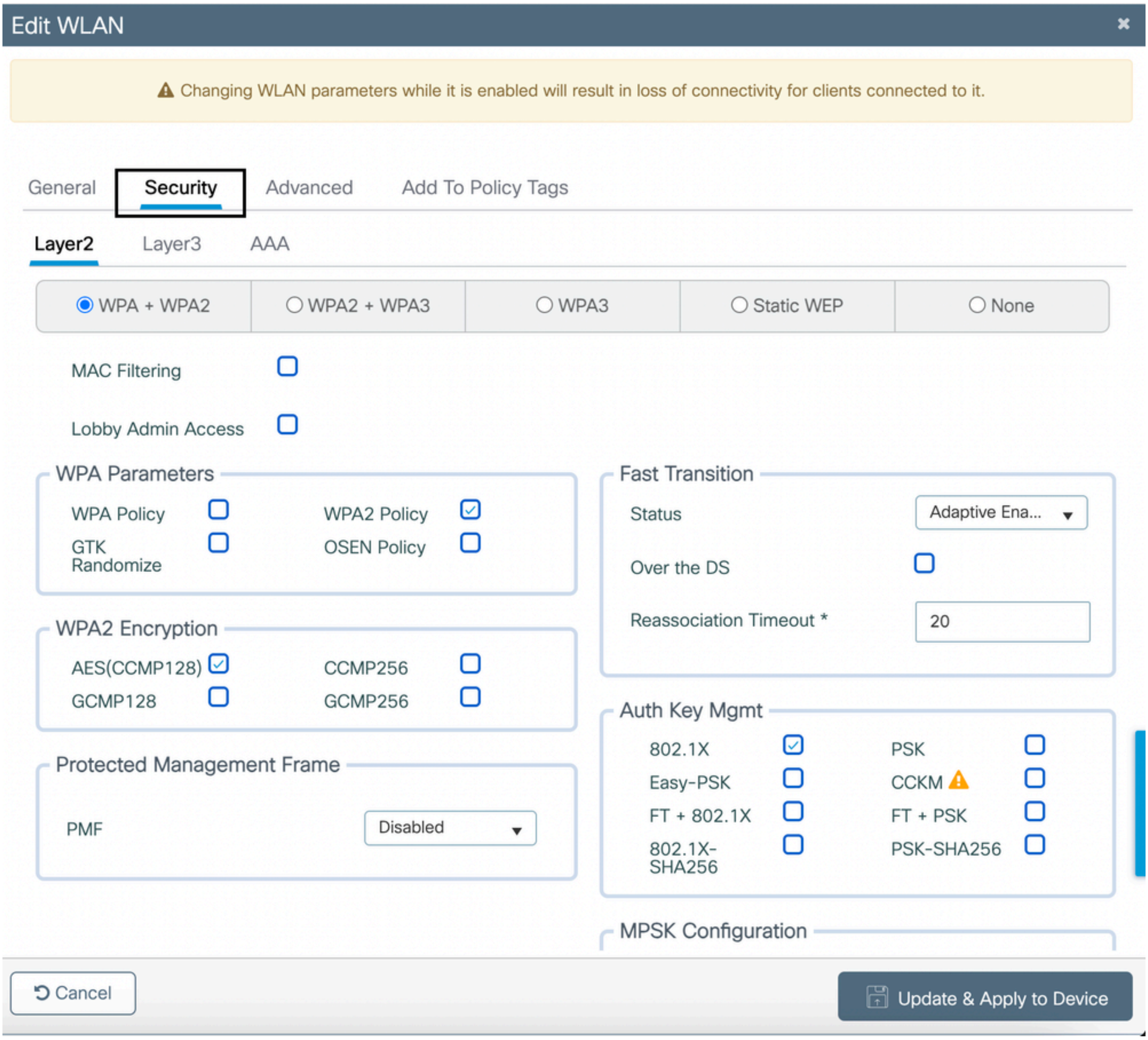
Available Servers

Assigned Servers: BYOD

Configure Security Policies for the WLAN

1. Navigate to **Configuration** > **Tags & Profiles** > **WLANs**. Edit the WLAN created earlier.

2. Under the **Security** > **Layer 2** tab:
   - Enable WPA+WPA2
   - Set AES(CCMP128) under WPA2 Encryption
   - Auth Key Mgmt as 802.1X



Edit WLAN ✖

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General | **Security** | Advanced | Add To Policy Tags

Layer2 | Layer3 | AAA

● WPA + WPA2 | ○ WPA2 + WPA3 | ○ WPA3 | ○ Static WEP | ○ None

MAC Filtering □

Lobby Admin Access □

WPA Parameters

WPA Policy	□	WPA2 Policy	☑
GTK Randomize	□	OSEN Policy	□

WPA2 Encryption

AES(CCMP128)	☑	CCMP256	□
GCMP128	□	GCMP256	□

Protected Management Frame

PMF: Disabled ▾

Fast Transition

Status: Adaptive Ena... ▾

Over the DS □

Reassociation Timeout *: 20

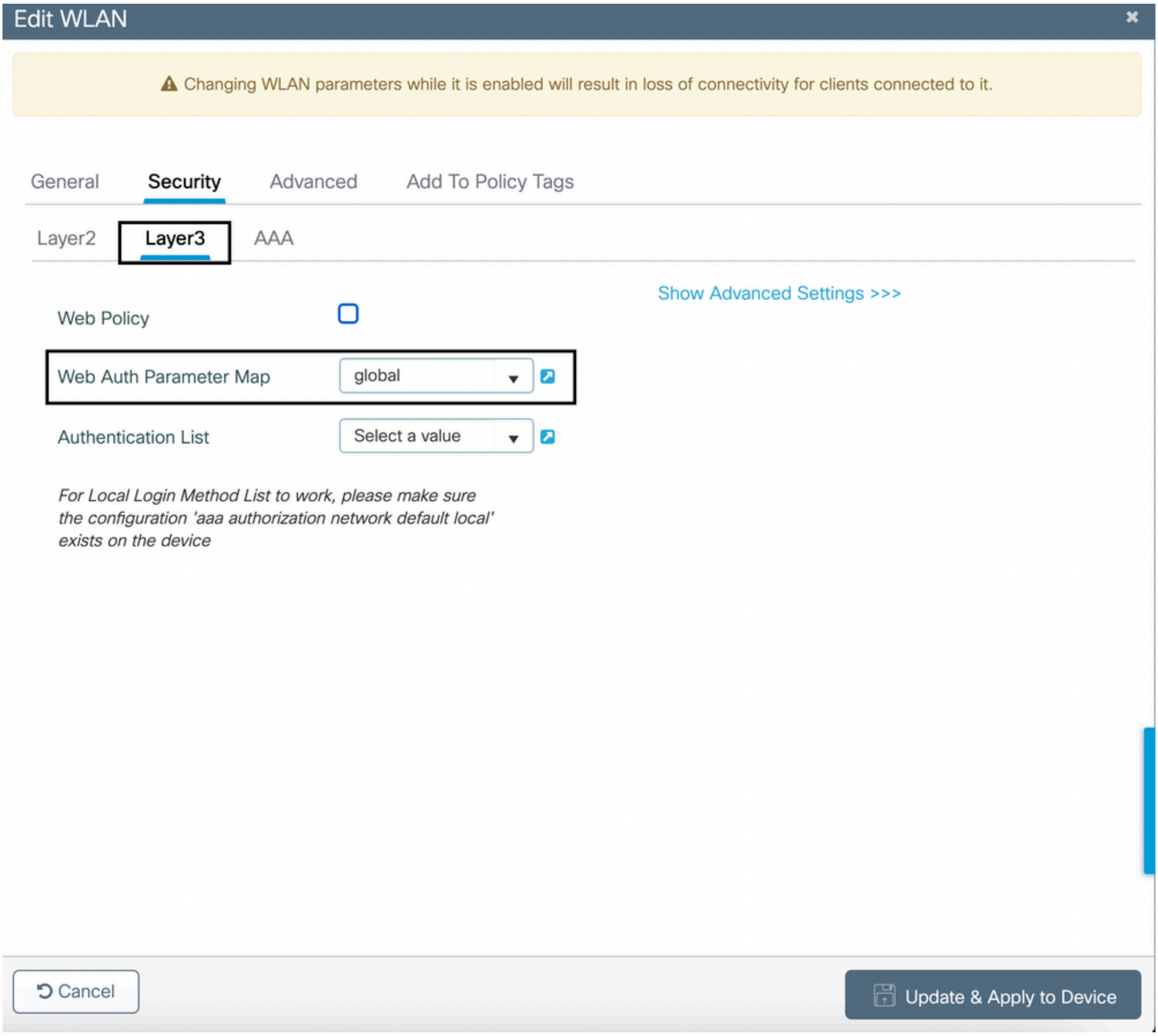
Auth Key Mgmt

802.1X	☑	PSK	□
Easy-PSK	□	CCKM ⚠	□
FT + 802.1X	□	FT + PSK	□
802.1X-SHA256	□	PSK-SHA256	□

MPSK Configuration

↺ Cancel | Update & Apply to Device

3. Under the **Security** > **Layer 3** tab, select global from the drop down for Web Auth Parameter Map.



Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General | Security | Advanced | Add To Policy Tags

Layer2 | Layer3 | AAA

Show Advanced Settings >>>

Web Policy □

Web Auth Parameter Map: global

Authentication List: Select a value

For Local Login Method List to work, please make sure the configuration 'aaa authorization network default local' exists on the device

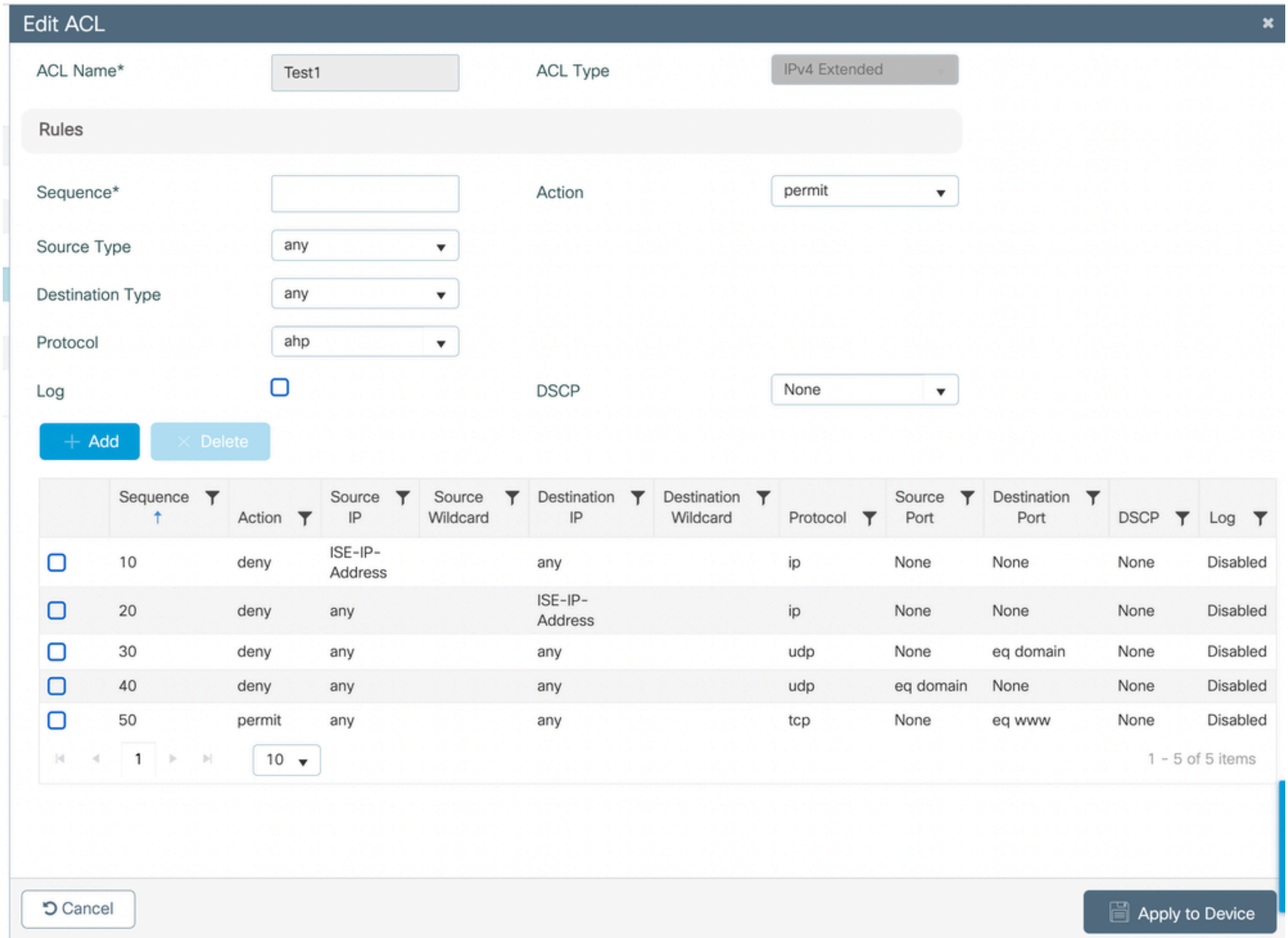
Configure Pre-Authentication ACL

Create an ACL to allow these actions for redirection:

- DNS traffic.
- HTTP/HTTPS to the ISE portal.
- Any required backend services.

To do so:

1. Navigate to **Configuration** > **Security** > **ACLs** > **Access Control Lists**.
2. Create a new ACL with rules to allow necessary traffic.



Edit ACL

ACL Name*	Test1	ACL Type	IPv4 Extended

Rules

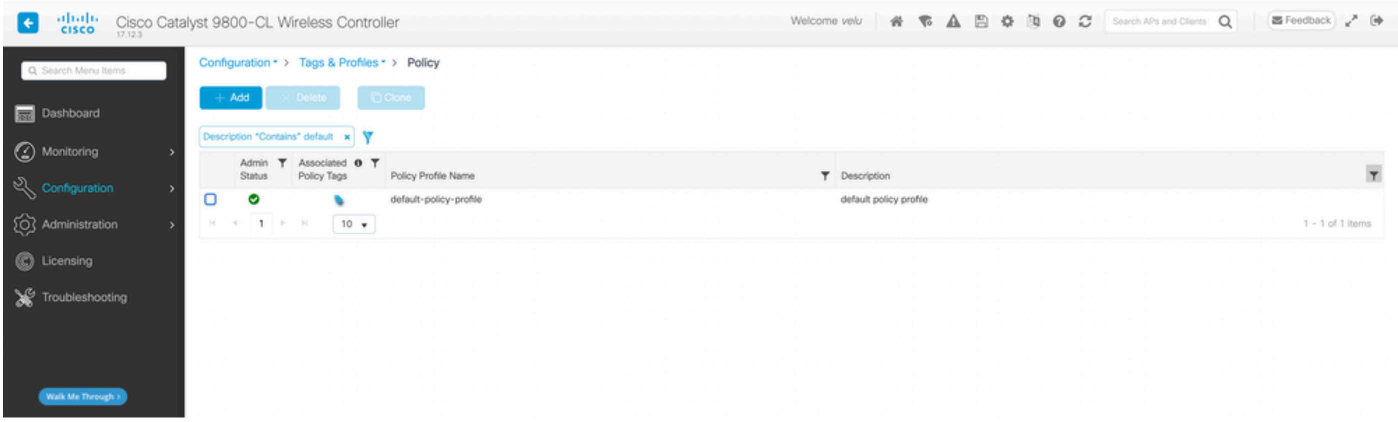
Sequence*		Action	permit
Source Type	any		
Destination Type	any		
Protocol	ahp		
Log	□	DSCP	None

	Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
□	10	deny	ISE-IP-Address		any		ip	None	None	None	Disabled
□	20	deny	any		ISE-IP-Address		ip	None	None	None	Disabled
□	30	deny	any		any		udp	None	eq domain	None	Disabled
□	40	deny	any		any		udp	eq domain	None	None	Disabled
□	50	permit	any		any		tcp	None	eq www	None	Disabled

1 - 5 of 5 items

Configure Policy Profile

1. Navigate to **Configuration > Tags & Profiles > Policy**. You can create or use the default policy



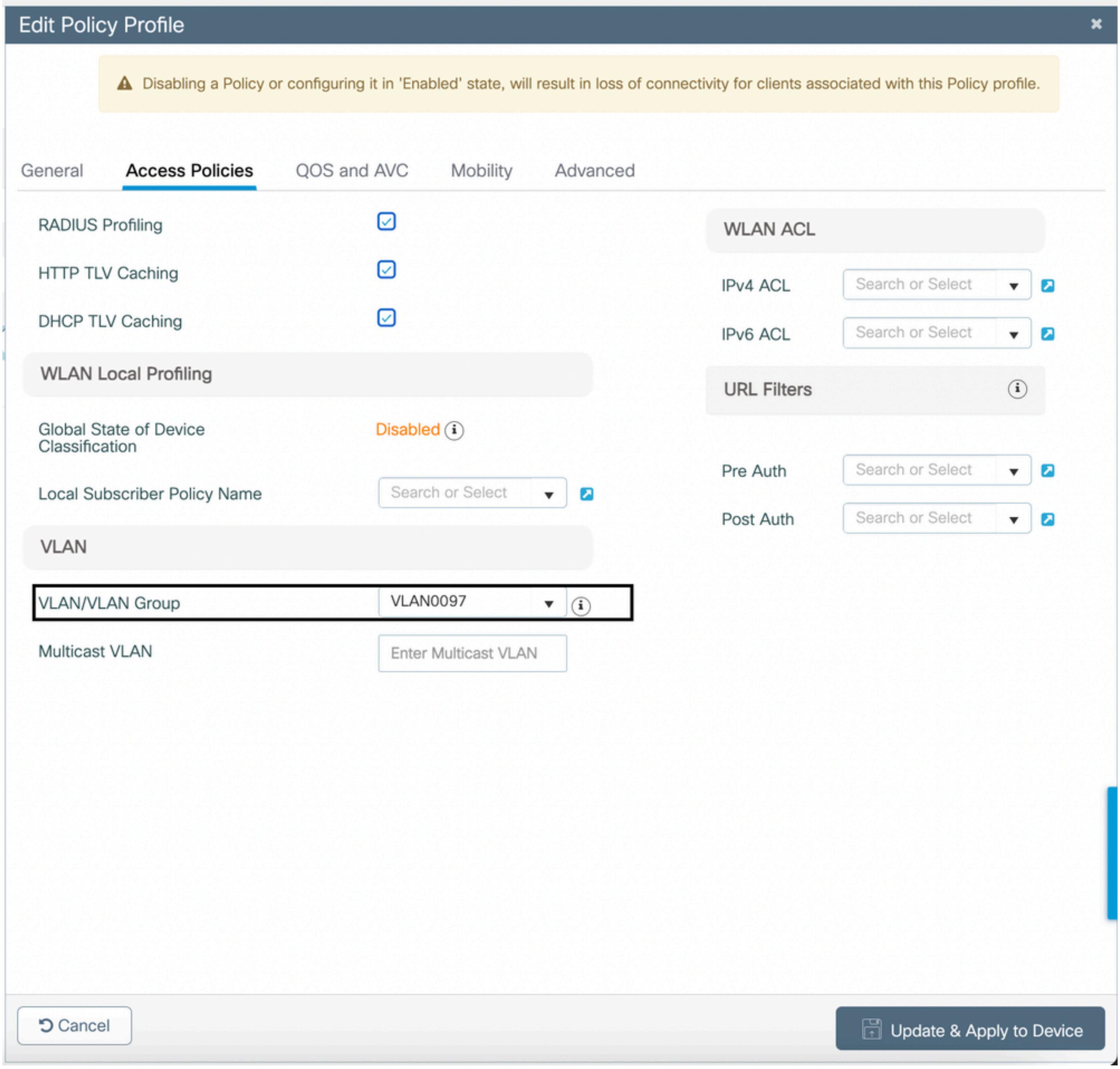
Configuration > Tags & Profiles > Policy

Description "Contains" default

	Admin Status	Associated Policy Tags	Policy Profile Name	Description
□	✓		default-policy-profile	default policy profile

1 - 1 of 1 items

2. Assign the appropriate VLAN under Access Policies



Edit Policy Profile

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

RADIUS Profiling ☑

HTTP TLV Caching ☑

DHCP TLV Caching ☑

WLAN Local Profiling

Global State of Device Classification: Disabled

Local Subscriber Policy Name: Search or Select

VLAN

VLAN/VLAN Group: VLAN0097

Multicast VLAN: Enter Multicast VLAN

WLAN ACL

IPv4 ACL: Search or Select

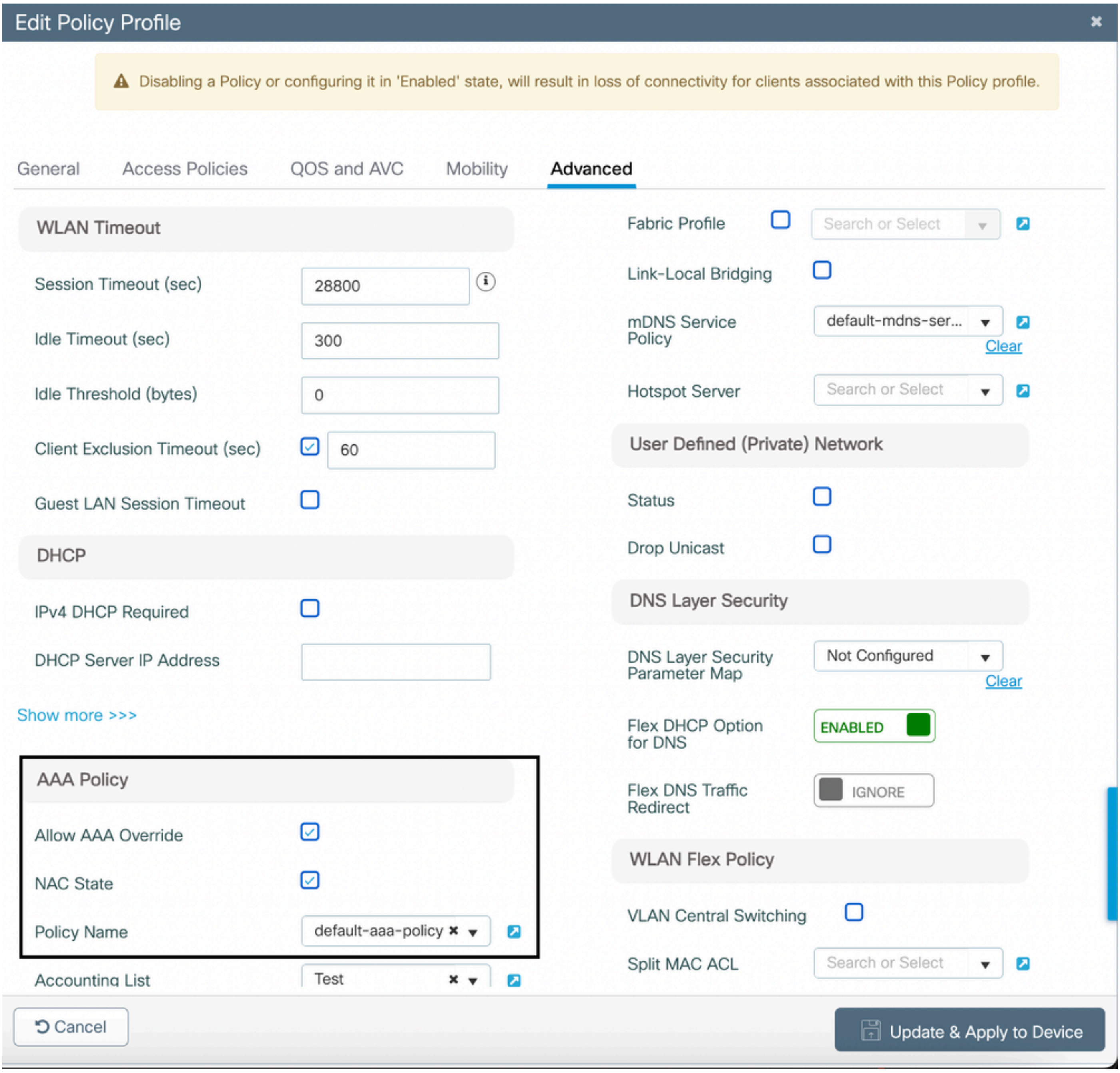
IPv6 ACL: Search or Select

URL Filters

Pre Auth: Search or Select

Post Auth: Search or Select

3. Also enable **Allow AAA Override** and **NAC state** under **Advanced of the policy**.



Edit Policy Profile

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

WLAN Timeout

Session Timeout (sec): 28800

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:

Show more >>>

AAA Policy

Allow AAA Override: ☑

NAC State: ☑

Policy Name: default-aaa-policy

Accounting List: Test

Fabric Profile: □ Search or Select

Link-Local Bridging: □

mDNS Service Policy: default-mdns-ser... Clear

Hotspot Server: Search or Select

User Defined (Private) Network

Status: □

Drop Unicast: □

DNS Layer Security

DNS Layer Security Parameter Map: Not Configured Clear

Flex DHCP Option for DNS: ENABLED

Flex DNS Traffic Redirect: IGNORE

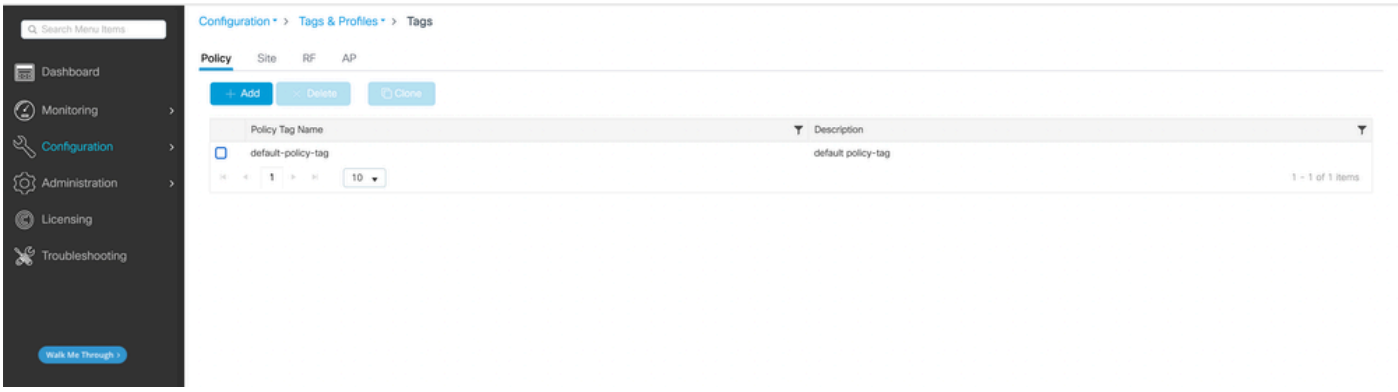
WLAN Flex Policy

VLAN Central Switching: □

Split MAC ACL: Search or Select

Apply Tags and Deploy

- Navigate to **Configuration** > **Tags & Profiles** > **Tags**.
- Create or edit a tag to include the WLAN and Policy Profile.
- Assign the tag to the Access Points.



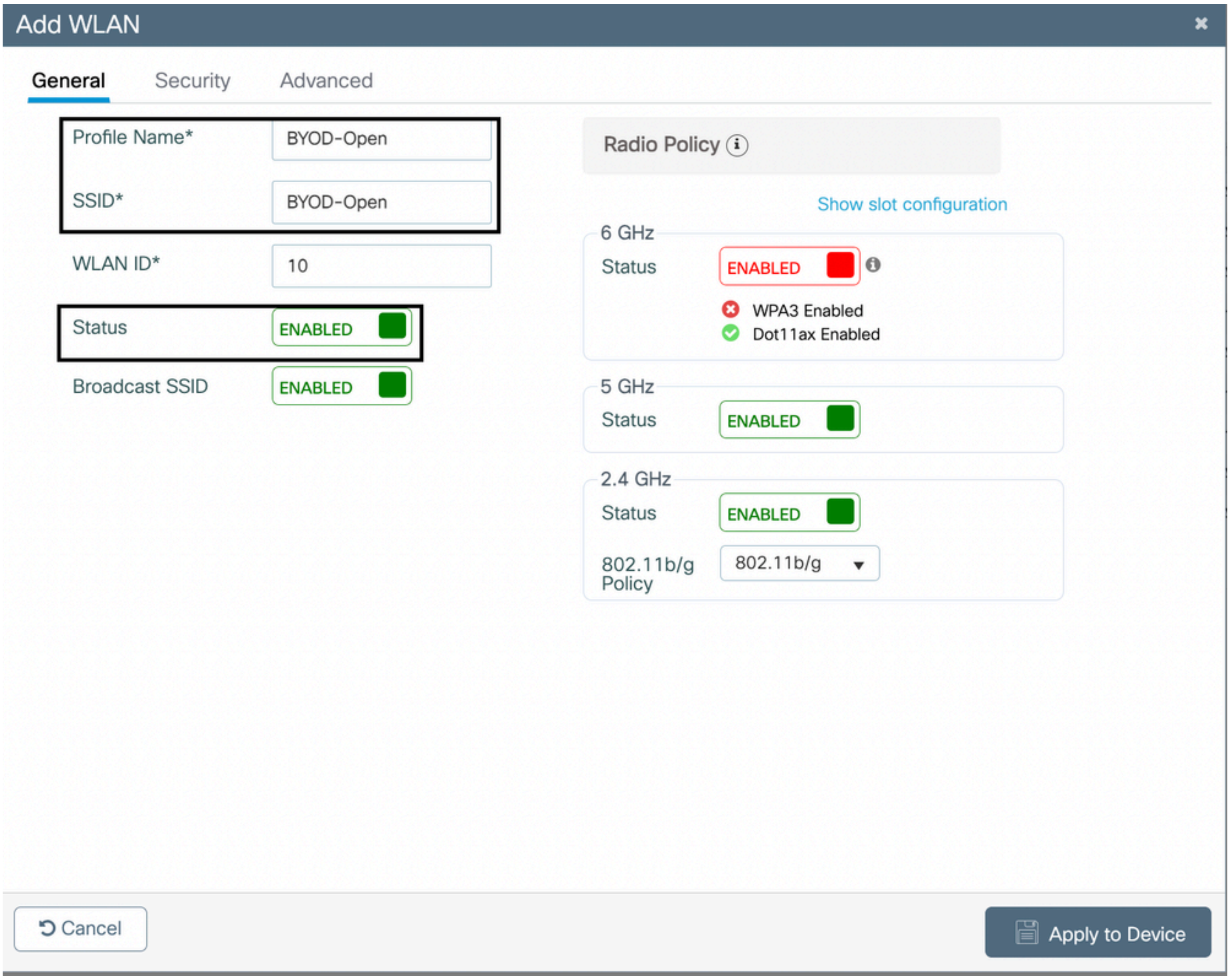
	Policy Tag Name	Description
□	default-policy-tag	default policy-tag

1 - 1 of 1 items

Configure an Open/ Unsecured SSID

The Open SSID is only created when you decide to have a Dual SSID BYOD Configuration on your environment.

1. Navigate to **Configuration** > **Tags & Profiles** > **WLANs**. Click the **Add** button.
2. Provide a SSID name under the General Tab and enable the WLAN button.



Add WLAN

General | Security | Advanced

Profile Name*: BYOD-Open

SSID*: BYOD-Open

WLAN ID*: 10

Status: ENABLED

Broadcast SSID: ENABLED

Radio Policy

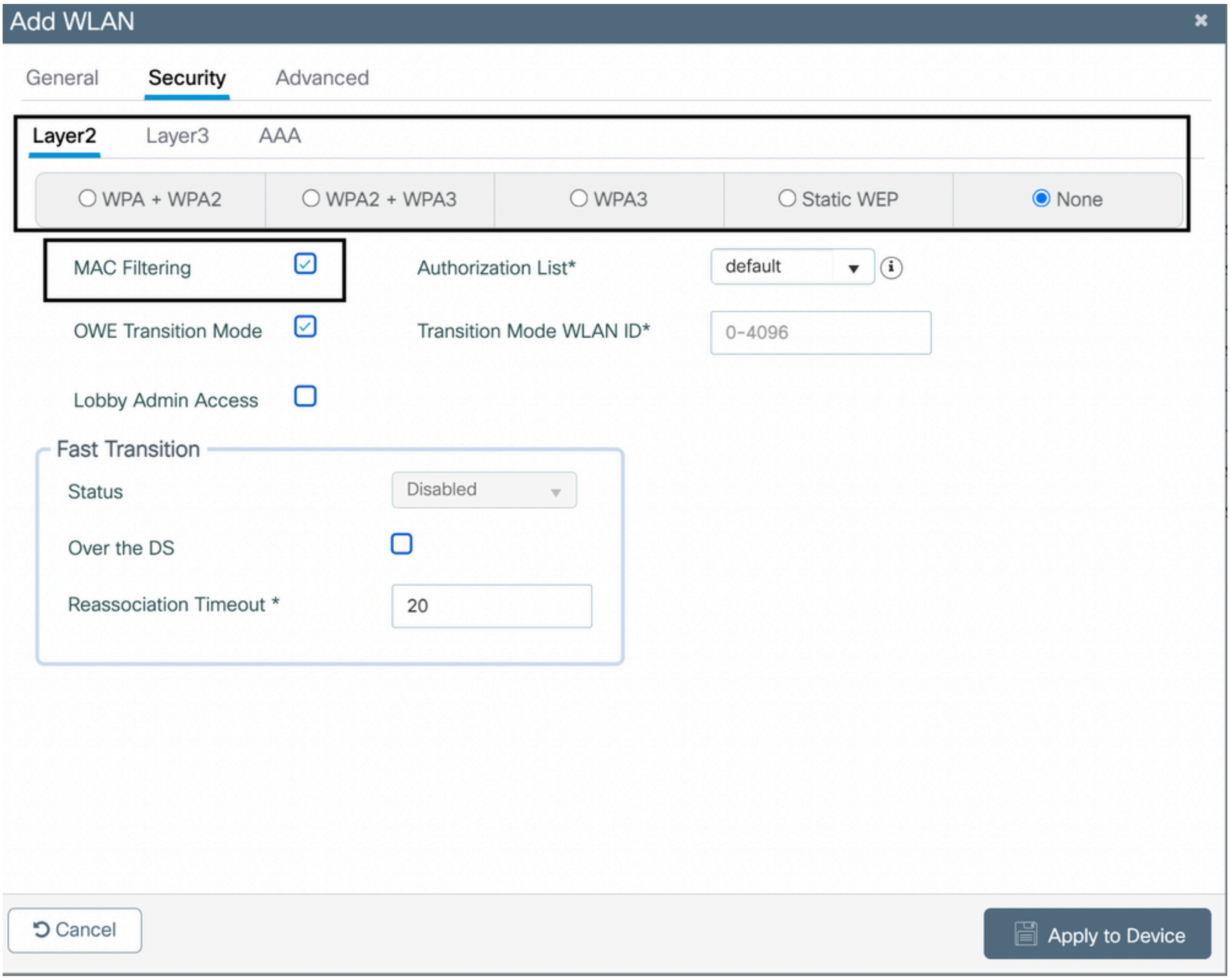
Show slot configuration

6 GHz
Status: ENABLED
WPA3 Enabled
Dot11ax Enabled

5 GHz
Status: ENABLED

2.4 GHz
Status: ENABLED
802.11b/g Policy: 802.11b/g

3. Click the **Security** tab from the same window. Select the **None** radio button and enable Mac Filtering.



Add WLAN

General | **Security** | Advanced

Layer2 | Layer3 | AAA

○ WPA + WPA2 ○ WPA2 + WPA3 ○ WPA3 ○ Static WEP ● None

MAC Filtering ☑

Authorization List* default

OWE Transition Mode ☑

Transition Mode WLAN ID* 0-4096

Lobby Admin Access □

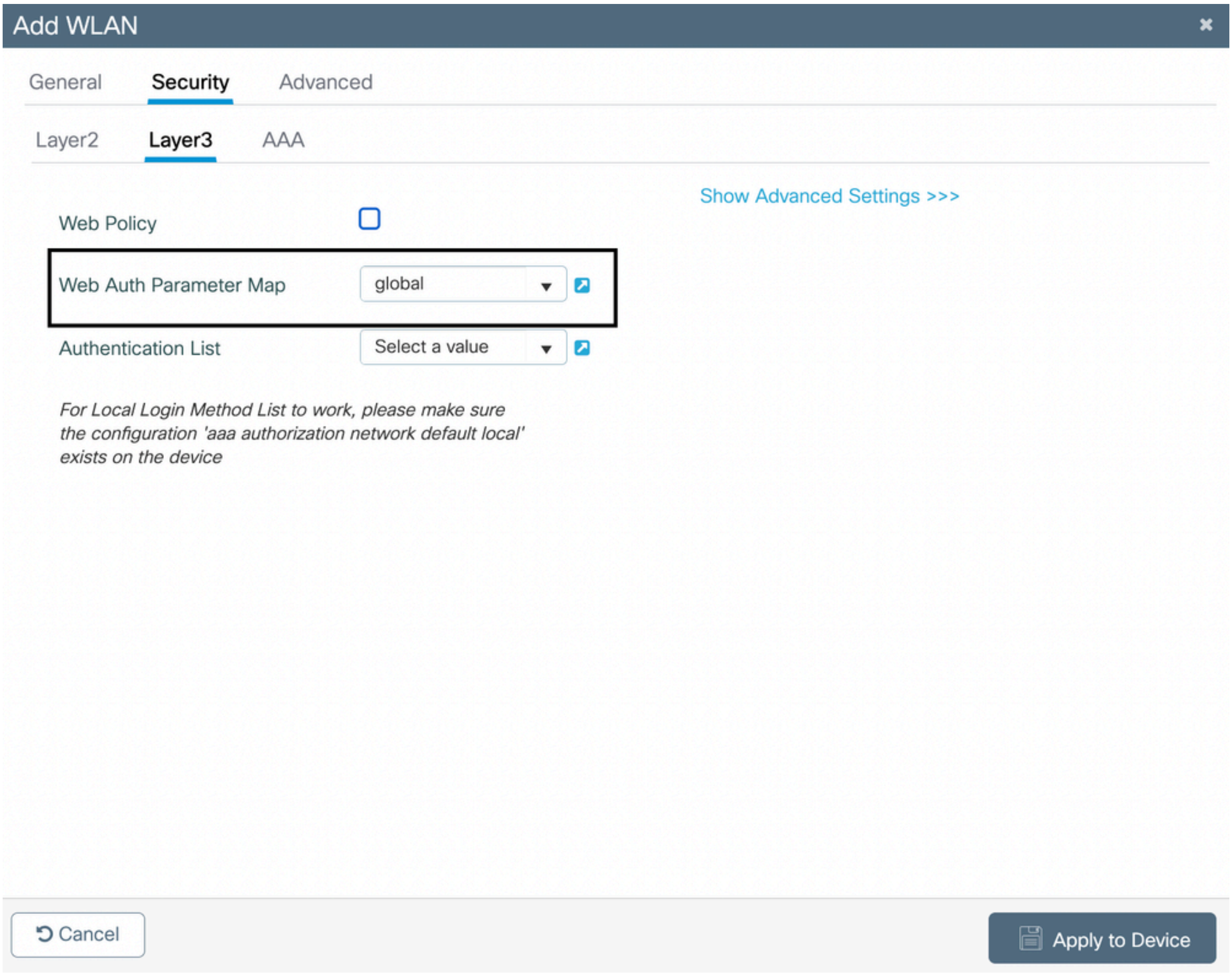
Fast Transition

Status Disabled

Over the DS □

Reassociation Timeout * 20

4. In **Layer 3** under **Security**, select the global setting for Web Auth Parameter Map. If you have any other web auth profile configured on the WLC, you can also map it here:



Web Policy □

Web Auth Parameter Map: global

Authentication List: Select a value

For Local Login Method List to work, please make sure the configuration 'aaa authorization network default local' exists on the device

ISE Configuration

Pre-requisites

- Ensure Cisco ISE is installed and licensed for BYOD functionality.
- Add your WLC to ISE as a network device with the RADIUS shared secret.

Certificates

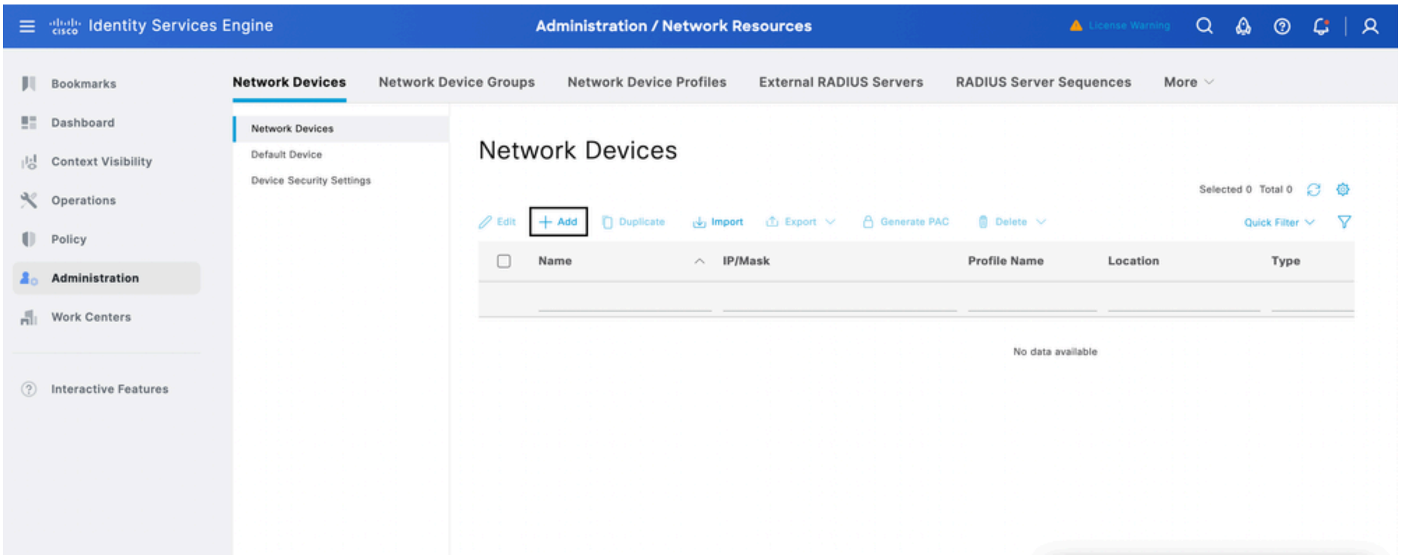
- Install a valid server certificate on ISE to avoid browser security warnings.
- Ensure the certificate is trusted by endpoints (signed by a well-known CA or an internal CA with trusted root).

DNS Configuration

- Ensure DNS resolves the ISE hostname for the BYOD portal.

Configure ISE Network Device

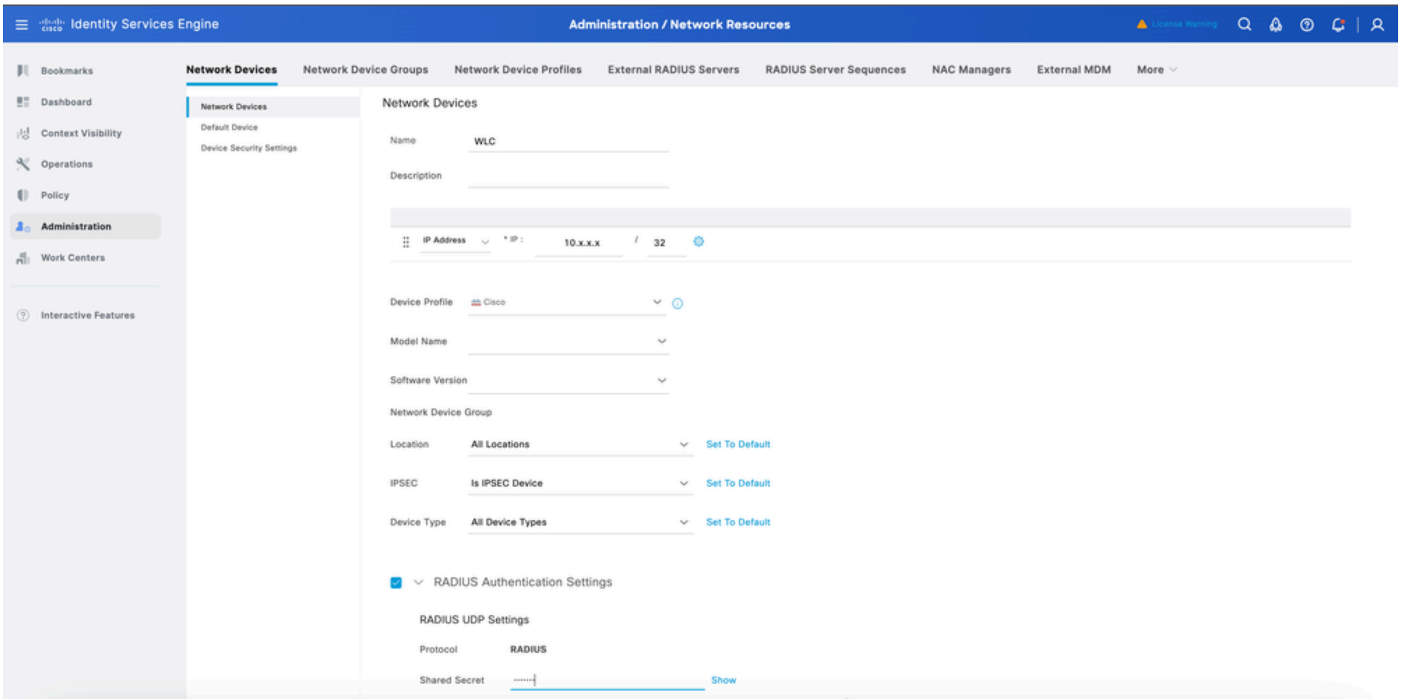
1. Log in to the ISE web UI.
2. Navigate to **Administration** > **Network Resources** > **Network Devices**.



No data available

3.Add your WLC as a network device:

- **Name**: Enter a name for the WLC.
- **IP Address**: Enter the WLC management IP.
- **RADIUS Shared Secret**: Enter the same shared secret as configured on the WLC.
- Click **Submit**.



Name: WLC

Description:

IP Address * IP : 10.x.x.x / 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

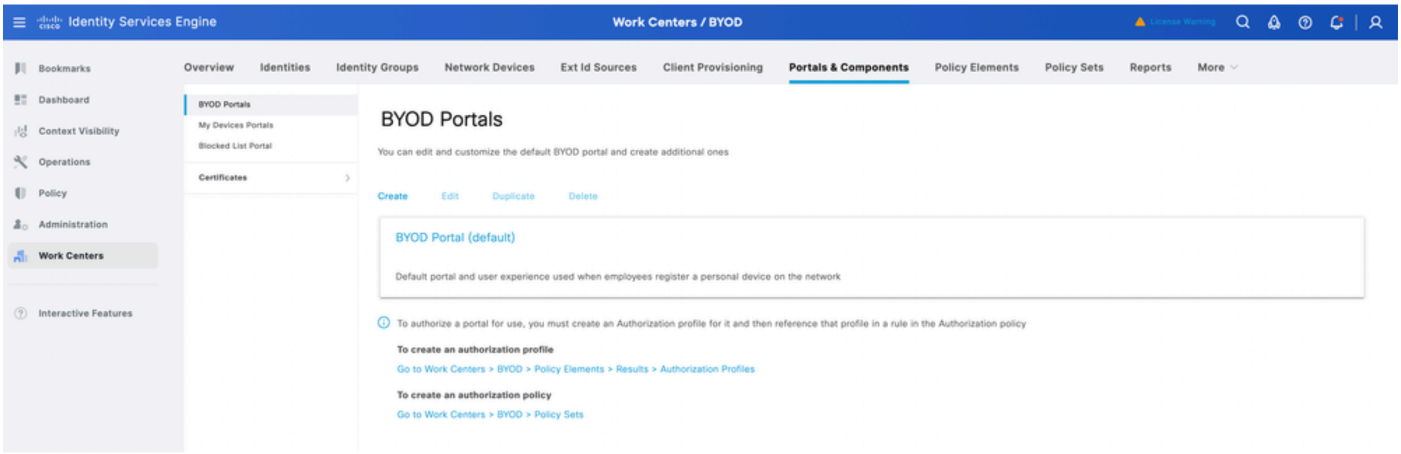
RADIUS UDP Settings

Protocol: RADIUS

Shared Secret: ------

Create a BYOD Portal

1. Navigate to **Work Centers** > **BYOD** > **Settings** > **Portals & Components** > **BYOD Portals**.
2. Click **Add** to create a BYOD portal or you could use the existing default portal on ISE.



BYOD Portals

You can edit and customize the default BYOD portal and create additional ones

BYOD Portal (default)

Default portal and user experience used when employees register a personal device on the network

To authorize a portal for use, you must create an Authorization profile for it and then reference that profile in a rule in the Authorization policy

To create an authorization profile

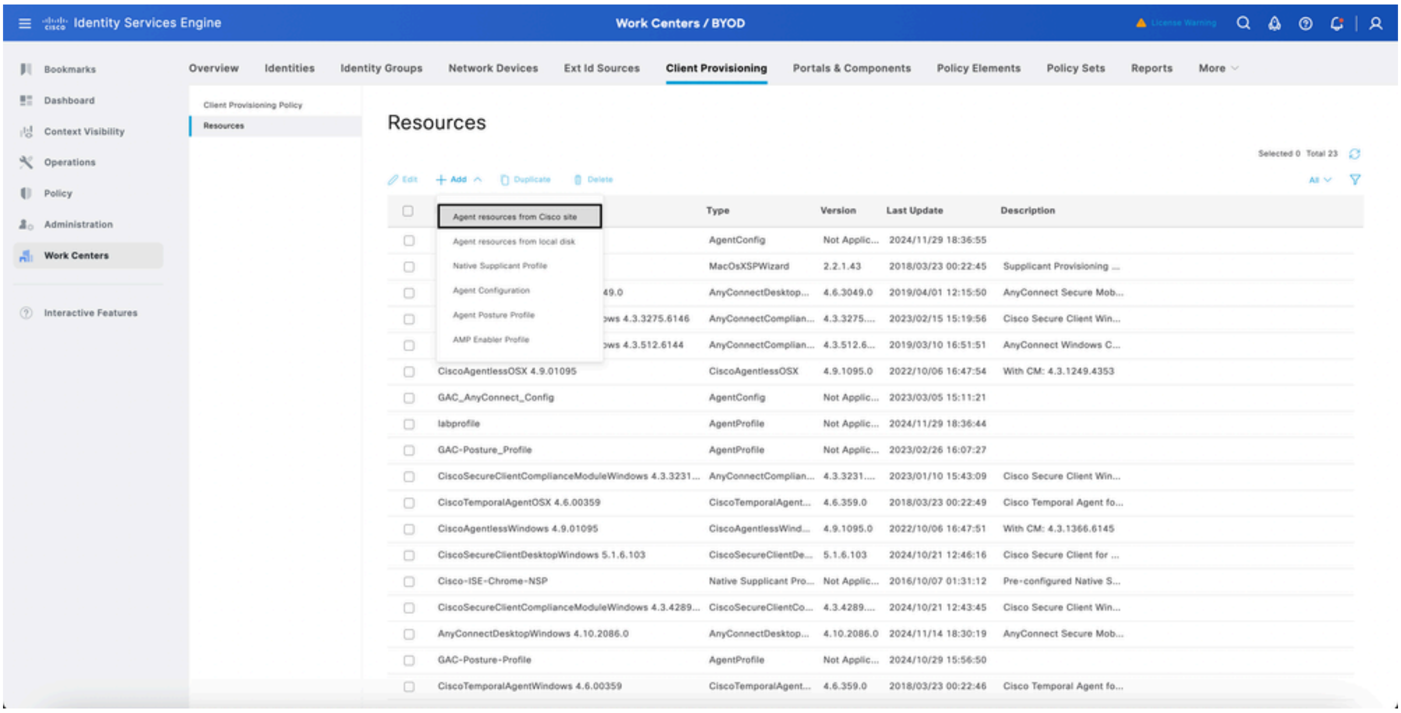
Go to Work Centers > BYOD > Policy Elements > Results > Authorization Profiles

To create an authorization policy

Go to Work Centers > BYOD > Policy Sets

Download Cisco IOS® Latest Version

1. Navigate to **Work Centers > BYOD > Client provisioning > Resources**.
2. Click the **Add** button and select agent resources from the Cisco site.

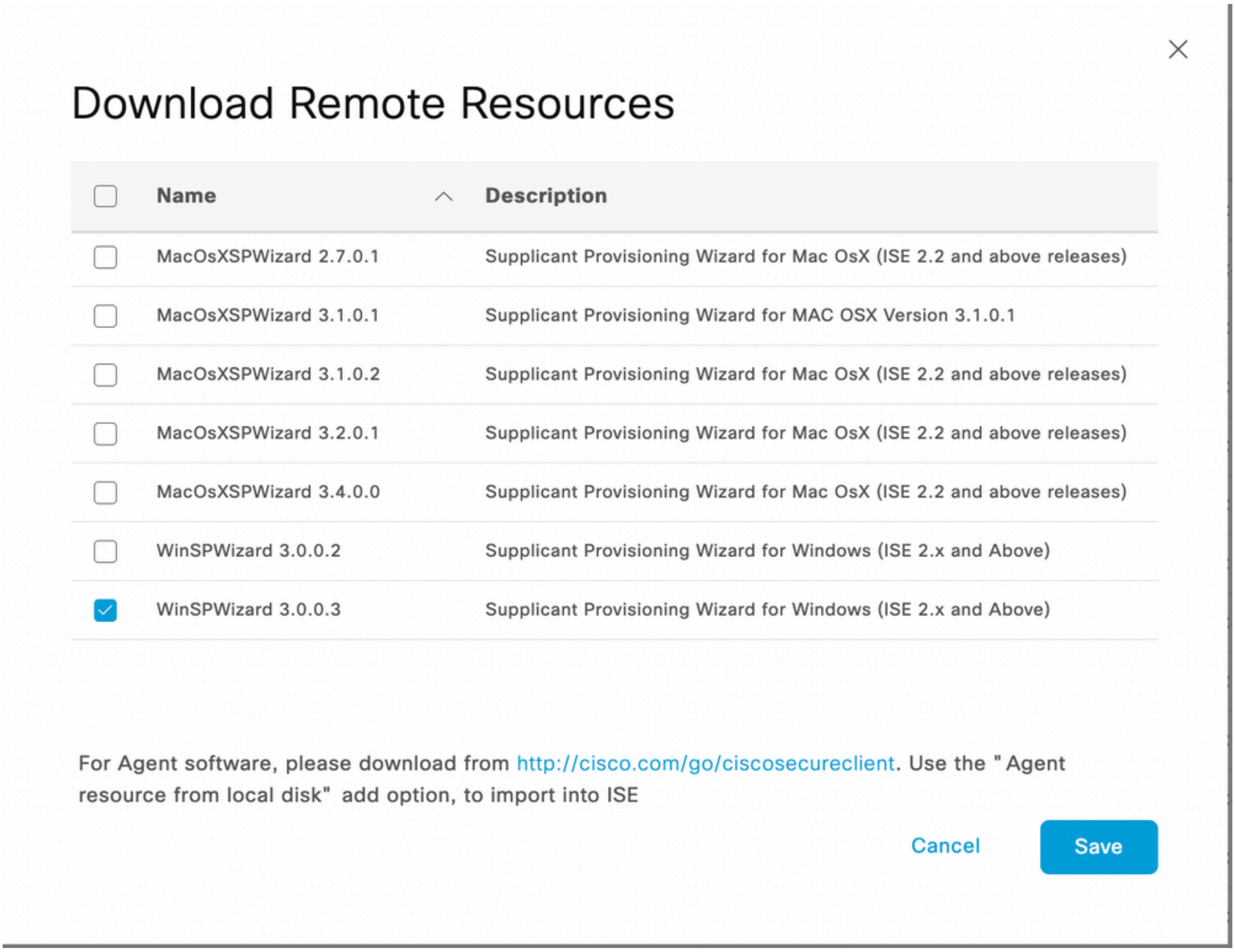


Resources

Selected 0 Total 23

□		Type	Version	Last Update	Description
□		AgentConfig	Not Applic...	2024/11/29 18:36:55	
□		MacOsXSPWizard	2.2.1.43	2018/03/23 00:22:45	Supplicant Provisioning ...
□	49.0	AnyConnectDesktop...	4.6.3049.0	2019/04/01 12:15:50	AnyConnect Secure Mob...
□	ows 4.3.3275.6146	AnyConnectComplian...	4.3.3275....	2023/02/15 15:19:56	Cisco Secure Client Win...
□	ows 4.3.512.6144	AnyConnectComplian...	4.3.512.6...	2019/03/10 16:51:51	AnyConnect Windows C...
□	CiscoAgentlessOSX 4.9.01095	CiscoAgentlessOSX	4.9.1095.0	2022/10/06 16:47:54	With CM: 4.3.1249.4353
□	GAC_AnyConnect_Config	AgentConfig	Not Applic...	2023/03/05 15:11:21	
□	labprofile	AgentProfile	Not Applic...	2024/11/29 18:36:44	
□	GAC-Posture_Profile	AgentProfile	Not Applic...	2023/02/26 16:07:27	
□	CiscoSecureClientComplianceModuleWindows 4.3.3231...	AnyConnectComplian...	4.3.3231....	2023/01/10 15:43:09	Cisco Secure Client Win...
□	CiscoTemporalAgentOSX 4.6.00359	CiscoTemporalAgent...	4.6.359.0	2018/03/23 00:22:49	Cisco Temporal Agent fo...
□	CiscoAgentlessWindows 4.9.01095	CiscoAgentlessWind...	4.9.1095.0	2022/10/06 16:47:51	With CM: 4.3.1366.6145
□	CiscoSecureClientDesktopWindows 5.1.6.103	CiscoSecureClientDe...	5.1.6.103	2024/10/21 12:46:16	Cisco Secure Client for ...
□	Cisco-ISE-Chrome-NSP	Native Supplicant Pro...	Not Applic...	2016/10/07 01:31:12	Pre-configured Native S...
□	CiscoSecureClientComplianceModuleWindows 4.3.4289...	CiscoSecureClientCo...	4.3.4289....	2024/10/21 12:43:45	Cisco Secure Client Win...
□	AnyConnectDesktopWindows 4.10.2086.0	AnyConnectDesktop...	4.10.2086.0	2024/11/14 18:30:19	AnyConnect Secure Mob...
□	GAC-Posture-Profile	AgentProfile	Not Applic...	2024/10/29 15:56:50	
□	CiscoTemporalAgentWindows 4.6.00359	CiscoTemporalAgent...	4.6.359.0	2018/03/23 00:22:46	Cisco Temporal Agent fo...

3. In the software list, select the latest Cisco IOS version to be downloaded.



Download Remote Resources

☐	Name	Description
☐	MacOsXSPWizard 2.7.0.1	Supplicant Provisioning Wizard for Mac OsX (ISE 2.2 and above releases)
☐	MacOsXSPWizard 3.1.0.1	Supplicant Provisioning Wizard for MAC OSX Version 3.1.0.1
☐	MacOsXSPWizard 3.1.0.2	Supplicant Provisioning Wizard for Mac OsX (ISE 2.2 and above releases)
☐	MacOsXSPWizard 3.2.0.1	Supplicant Provisioning Wizard for Mac OsX (ISE 2.2 and above releases)
☐	MacOsXSPWizard 3.4.0.0	Supplicant Provisioning Wizard for Mac OsX (ISE 2.2 and above releases)
☐	WinSPWizard 3.0.0.2	Supplicant Provisioning Wizard for Windows (ISE 2.x and Above)
☑	WinSPWizard 3.0.0.3	Supplicant Provisioning Wizard for Windows (ISE 2.x and Above)

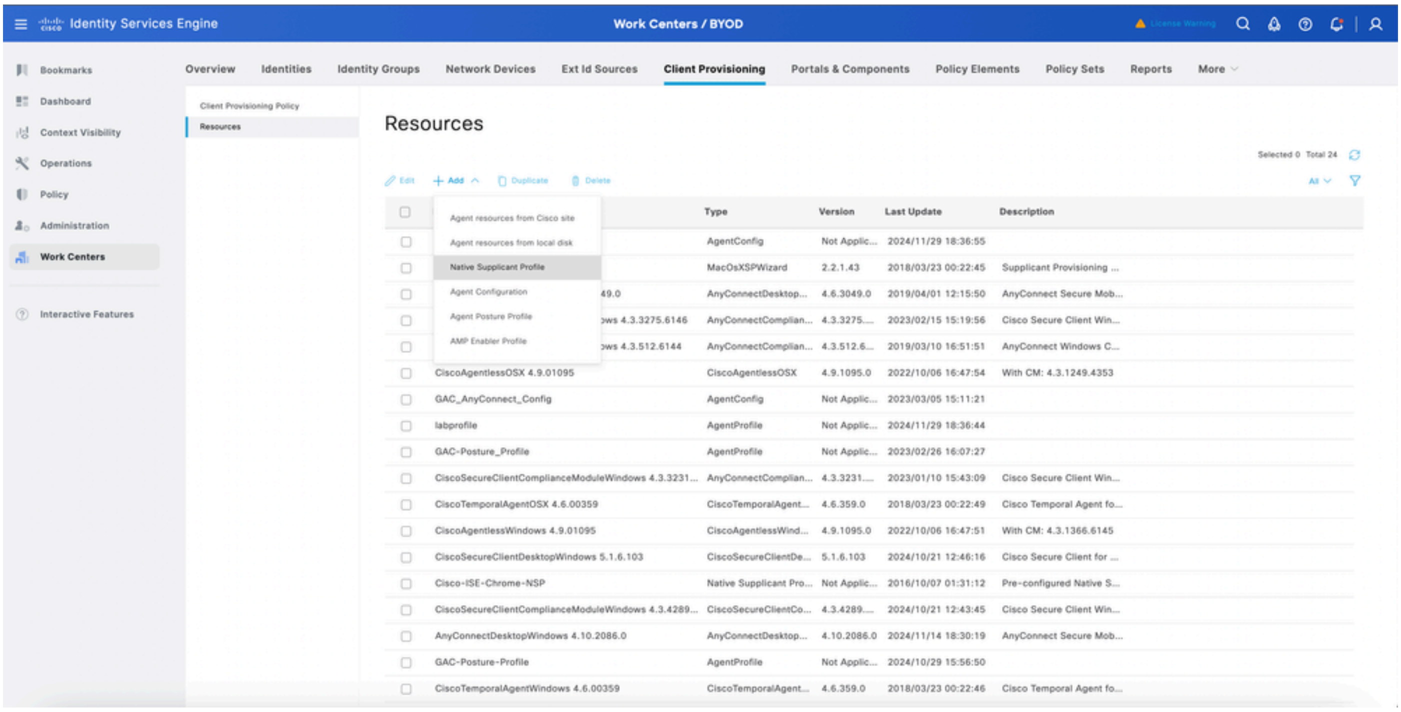
For Agent software, please download from http://cisco.com/go/ciscosecureclient. Use the " Agent resource from local disk" add option, to import into ISE

Note: Cisco IOS software is download on the ISE for Windows and MacOS endpoints. For Apple iPhone IOS, it uses a native supplicant to provision the device and For android device, you have Network setup assistant which needs to be downloaded from Play Store.

Create an Endpoint Profile

1. Navigate to **Work Centers > BYOD > Client provisioning > Resources**.

2. Click **Add**, select **Native supplicant profile** from the drop down menu.

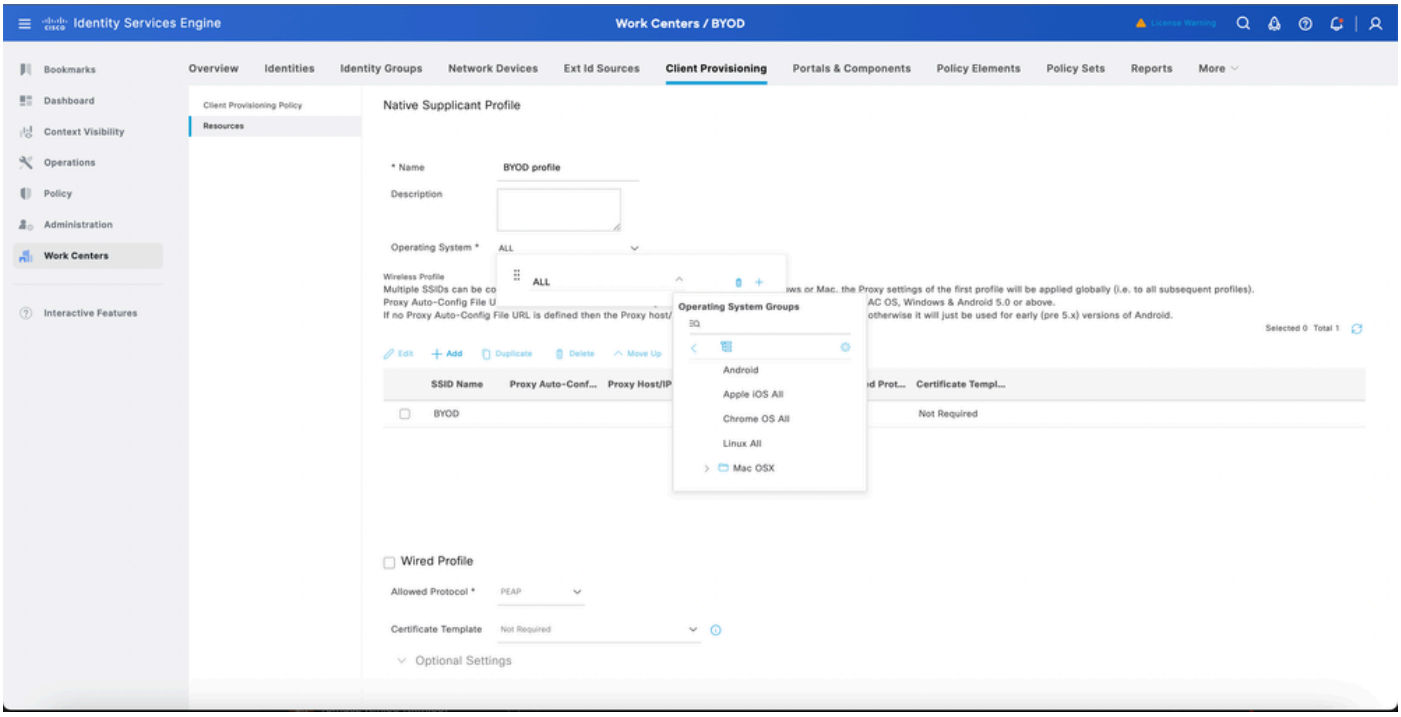


Resources

Selected 0 Total 24

	Type	Version	Last Update	Description
	AgentConfig	Not Applic...	2024/11/29 18:36:55	
	MacOsXSPWizard	2.2.1.43	2018/03/23 00:22:45	Supplicant Provisioning ...
49.0	AnyConnectDesktop...	4.6.3049.0	2019/04/01 12:15:50	AnyConnect Secure Mob...
ows 4.3.3275.6146	AnyConnectComplian...	4.3.3275....	2023/02/15 15:19:56	Cisco Secure Client Win...
ows 4.3.512.6144	AnyConnectComplian...	4.3.512.6...	2019/03/10 16:51:51	AnyConnect Windows C...
CiscoAgentlessOSX 4.9.01095	CiscoAgentlessOSX	4.9.1095.0	2022/10/06 16:47:54	With CM: 4.3.1249.4353
GAC_AnyConnect_Config	AgentConfig	Not Applic...	2023/03/05 15:11:21	
labprofile	AgentProfile	Not Applic...	2024/11/29 18:36:44	
GAC-Posture_Profile	AgentProfile	Not Applic...	2023/02/26 16:07:27	
CiscoSecureClientComplianceModuleWindows 4.3.3231...	AnyConnectComplian...	4.3.3231....	2023/01/10 15:43:09	Cisco Secure Client Win...
CiscoTemporalAgentOSX 4.6.00359	CiscoTemporalAgent...	4.6.359.0	2018/03/23 00:22:49	Cisco Temporal Agent fo...
CiscoAgentlessWindows 4.9.01095	CiscoAgentlessWind...	4.9.1095.0	2022/10/06 16:47:51	With CM: 4.3.1366.6145
CiscoSecureClientDesktopWindows 5.1.6.103	CiscoSecureClientDe...	5.1.6.103	2024/10/21 12:46:16	Cisco Secure Client for ...
Cisco-ISE-Chrome-NSP	Native Supplicant Pro...	Not Applic...	2016/10/07 01:31:12	Pre-configured Native S...
CiscoSecureClientComplianceModuleWindows 4.3.4289...	CiscoSecureClientCo...	4.3.4289....	2024/10/21 12:43:45	Cisco Secure Client Win...
AnyConnectDesktopWindows 4.10.2086.0	AnyConnectDesktop...	4.10.2086.0	2024/11/14 18:30:19	AnyConnect Secure Mob...
GAC-Posture-Profile	AgentProfile	Not Applic...	2024/10/29 15:56:50	
CiscoTemporalAgentWindows 4.6.00359	CiscoTemporalAgent...	4.6.359.0	2018/03/23 00:22:46	Cisco Temporal Agent fo...

3. Under the **Operating system** drop down, please select the required Operating system you would like to onboard the device or you could set it as ALL for onboard all the endpoints in your environment:



Native Supplicant Profile

* Name BYOD profile

Description

Operating System * ALL

ALL

Wireless Profile

Multiple SSIDs can be co ... ows or Mac. the Proxy settings of the first profile will be applied globally (i.e. to all subsequent profiles).

Proxy Auto-Config File U ... AC OS, Windows & Android 5.0 or above.

If no Proxy Auto-Config File URL is defined then the Proxy host/ ... otherwise it will just be used for early (pre 5.x) versions of Android.

Selected 0 Total 1

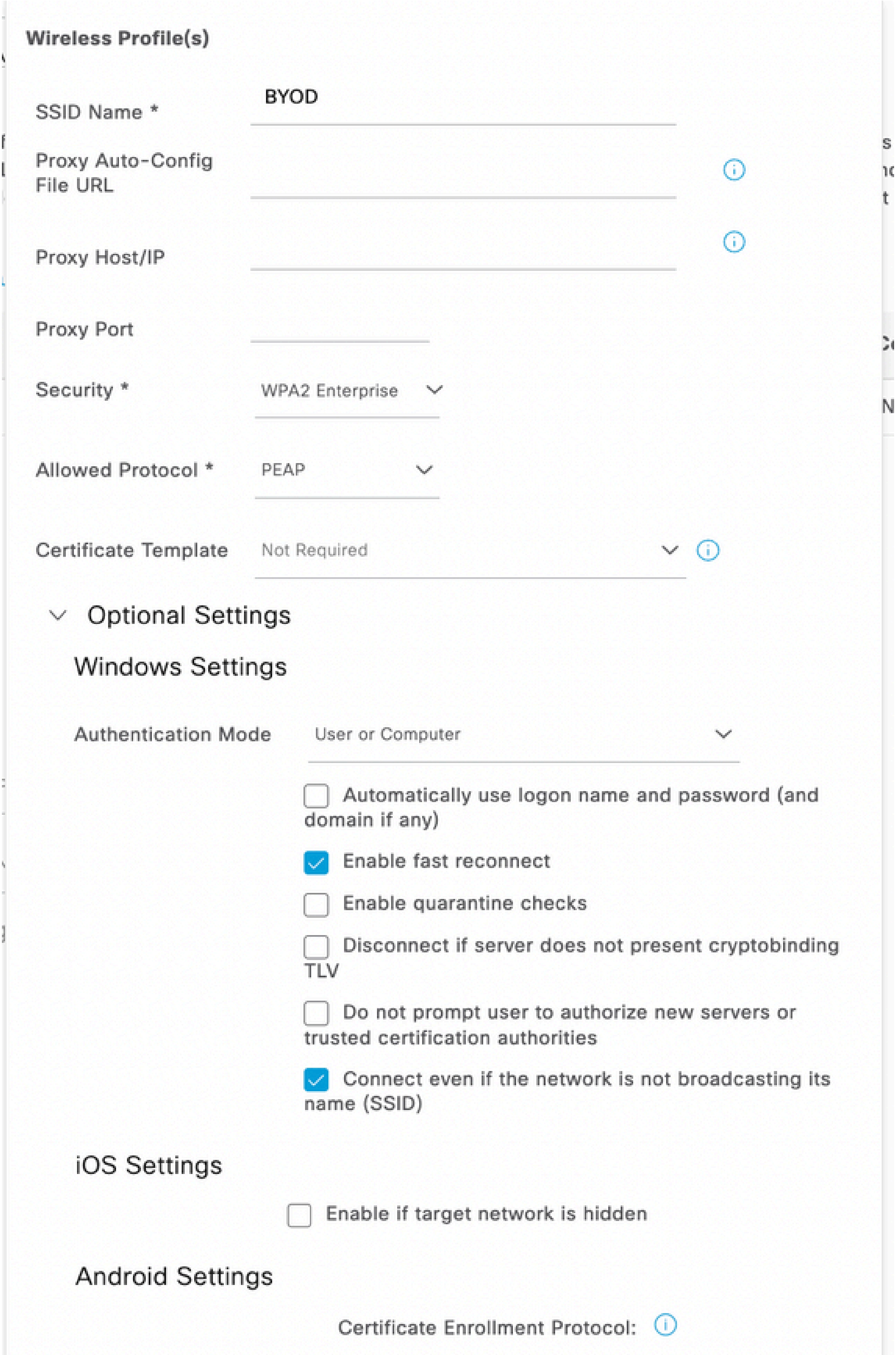
	SSID Name	Proxy Auto-Conf...	Proxy Host/IP	d Prot...	Certificate Templ...
□	BYOD				Not Required

□ Wired Profile

Allowed Protocol * PEAP

Certificate Template Not Required

4. Click **Add** from the page to create the endpoint profile to configure the 802.1X for the endpoint:



Wireless Profile(s)

SSID Name * BYOD

Proxy Auto-Config File URL

Proxy Host/IP

Proxy Port

Security * WPA2 Enterprise

Allowed Protocol * PEAP

Certificate Template Not Required

Optional Settings

Windows Settings

Authentication Mode User or Computer

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

☑ Enable fast reconnect

□ Enable quarantine checks

□ Disconnect if server does not present cryptobinding TLV

□ Do not prompt user to authorize new servers or trusted certification authorities

☑ Connect even if the network is not broadcasting its name (SSID)

iOS Settings

□ Enable if target network is hidden

Android Settings

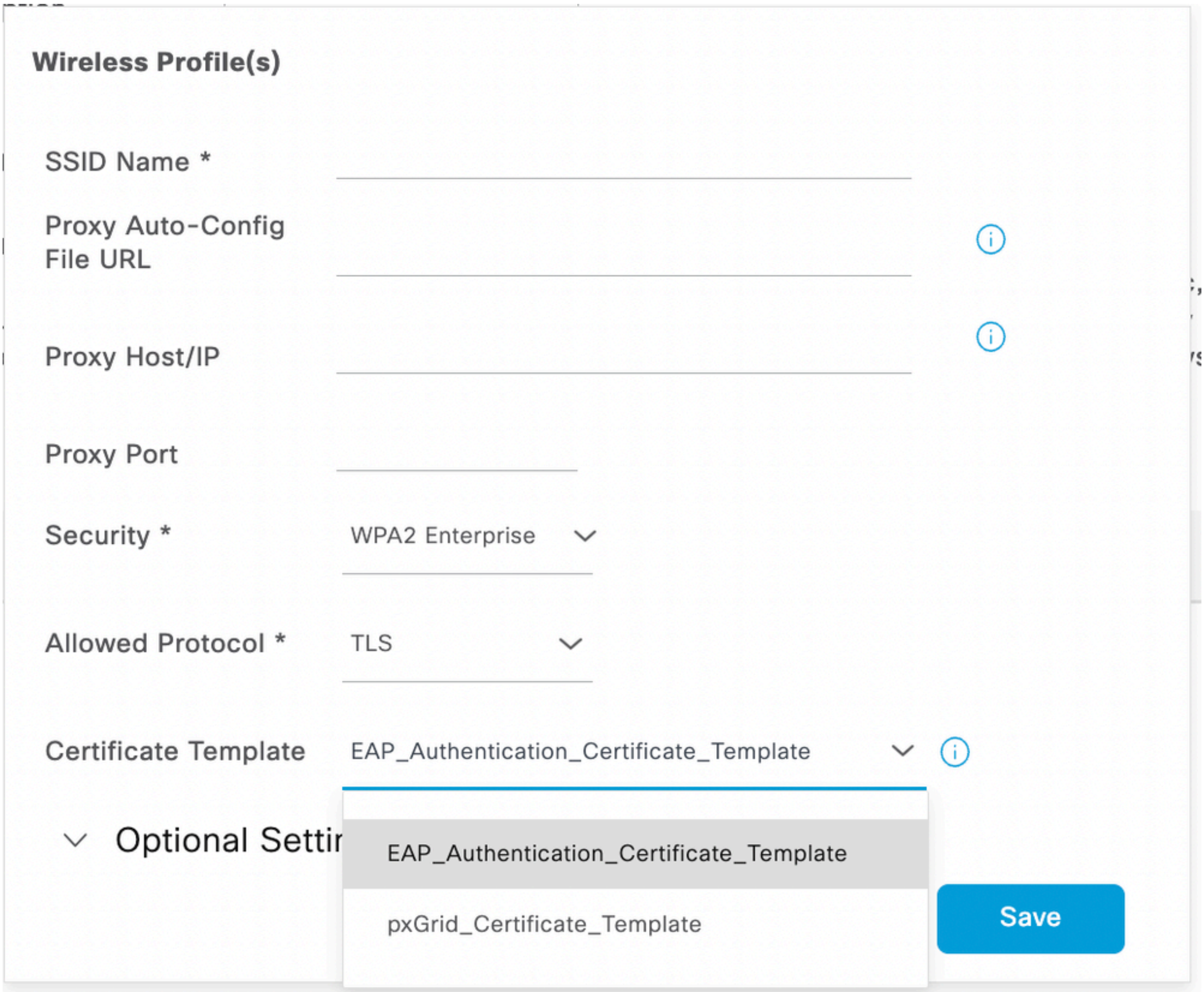
Certificate Enrollment Protocol:

: Depending on your requirement please configure the endpoint profile for the endpoint on your environment. The endpoints profile allows us to configure EAP-PEAP, EAP-TLS.

5. Click **Save**, then **Submit** on the endpoint profile.

Certificate Template

The Endpoint profile is preconfigured to perform EAP-TLS. A certificate Template must be added to the profile. By default, ISE has two templates pre-defined which can be chosen from the dropdown.



Wireless Profile(s)

SSID Name *

Proxy Auto-Config File URL

Proxy Host/IP

Proxy Port

Security * WPA2 Enterprise

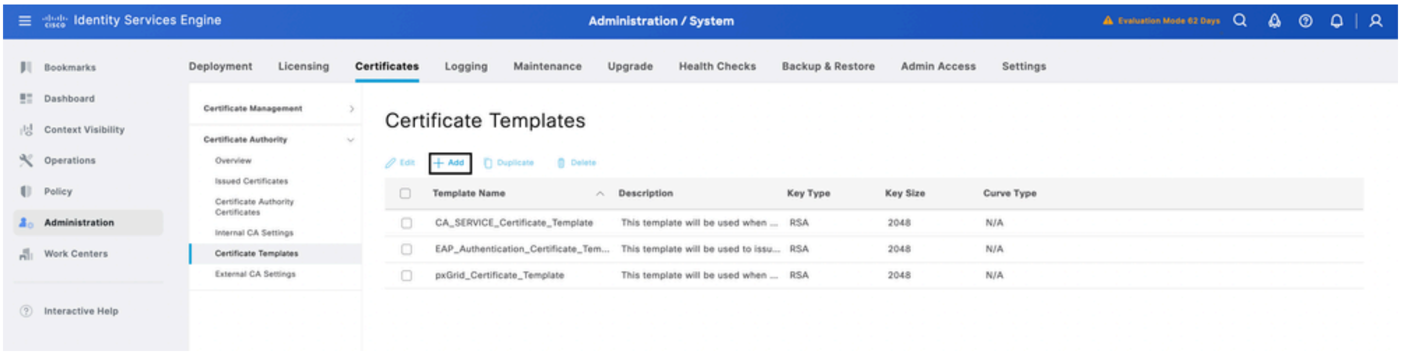
Allowed Protocol * TLS

Certificate Template EAP_Authentication_Certificate_Template

Optional Settir
EAP_Authentication_Certificate_Template
pxGrid_Certificate_Template
Save

To create a new Certificate template, follow these steps:

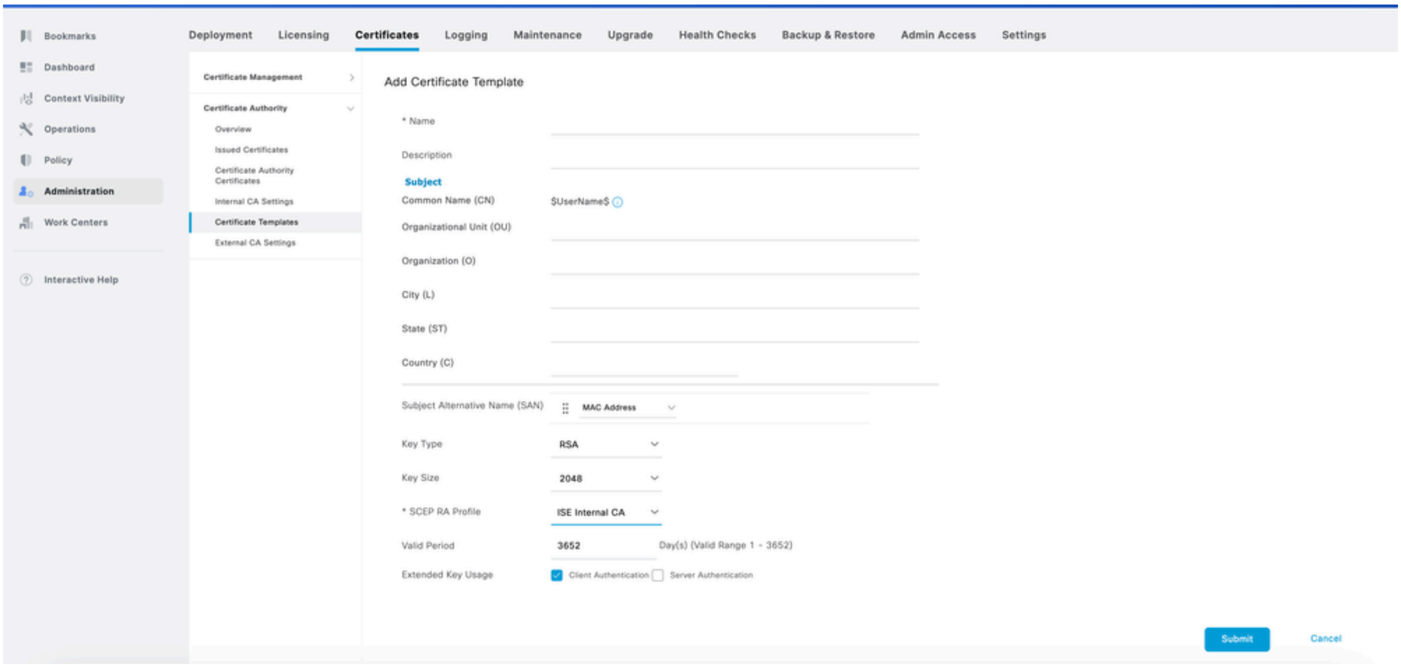
1. Navigate to **Administration** > **System** > **Certificates** > **Certificate Authority** > **Certificate Templates**.
2. Click the **Add** button from the page.



Certificate Templates

Template Name	Description	Key Type	Key Size	Curve Type
CA_SERVICE_Certificate_Template	This template will be used when ...	RSA	2048	N/A
EAP_Authentication_Certificate_Tem...	This template will be used to issu...	RSA	2048	N/A
pxGrid_Certificate_Template	This template will be used when ...	RSA	2048	N/A

3. Fill in the details tailored to meet the specific requirements of your organization.



Add Certificate Template

* Name

Description

Subject

Common Name (CN) $UserName$

Organizational Unit (OU)

Organization (O)

City (L)

State (ST)

Country (C)

Subject Alternative Name (SAN) MAC Address

Key Type RSA

Key Size 2048

* SCEP RA Profile ISE Internal CA

Valid Period 3652 Day(s) (Valid Range 1 - 3652)

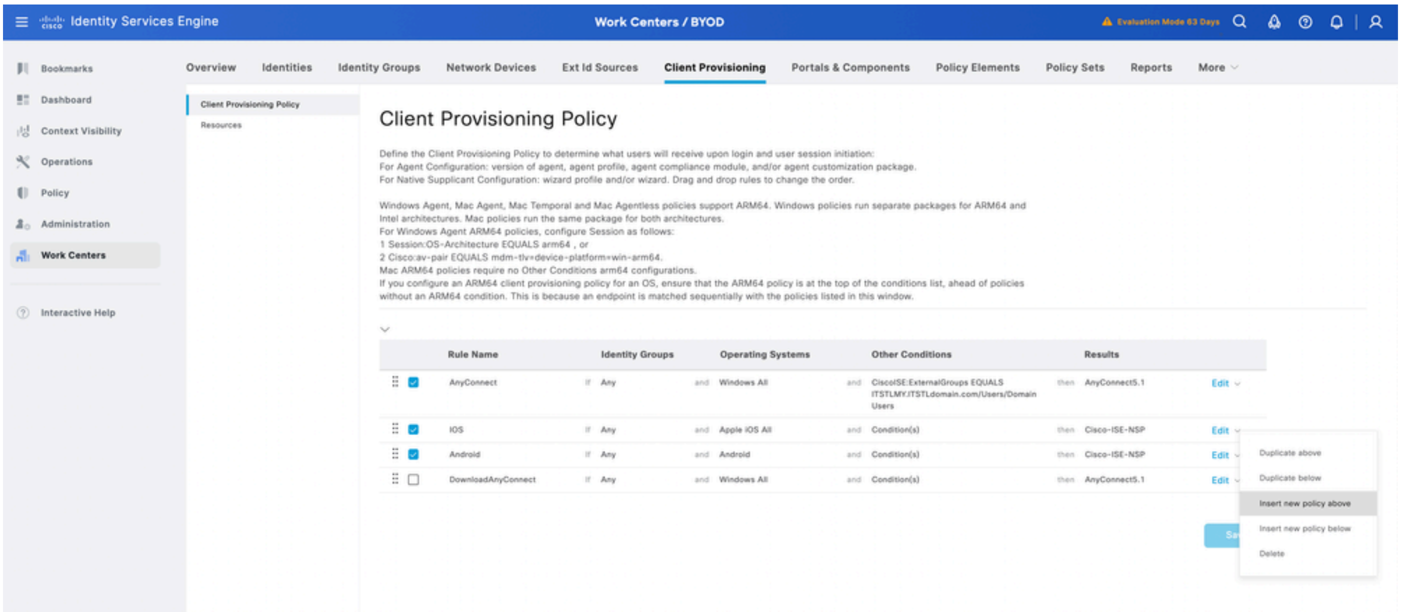
Extended Key Usage ☑ Client Authentication □ Server Authentication

4. Click **Submit** to save the changes.

Note: The certificate template could be useful in scenario when you have different domains and segment the user by adding a different value in the OU of the certificate.

Map an Endpoint Profile to the Client-provisioning Portal

1. Navigate to **Work Centers > BYOD > Client provisioning > Client provisioning Policy**.
2. Click **v** on of the rules to create a new client provisioning rule.



Client Provisioning Policy

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

Windows Agent, Mac Agent, Mac Temporal and Mac Agentless policies support ARM64. Windows policies run separate packages for ARM64 and Intel architectures. Mac policies run the same package for both architectures.
For Windows Agent ARM64 policies, configure Session as follows:
1 Session:OS-Architecture EQUALS arm64 , or
2 Cisco:av-pair EQUALS mdm-tlv=device-platform=win-arm64.
Mac ARM64 policies require no Other Conditions arm64 configurations.
If you configure an ARM64 client provisioning policy for an OS, ensure that the ARM64 policy is at the top of the conditions list, ahead of policies without an ARM64 condition. This is because an endpoint is matched sequentially with the policies listed in this window.

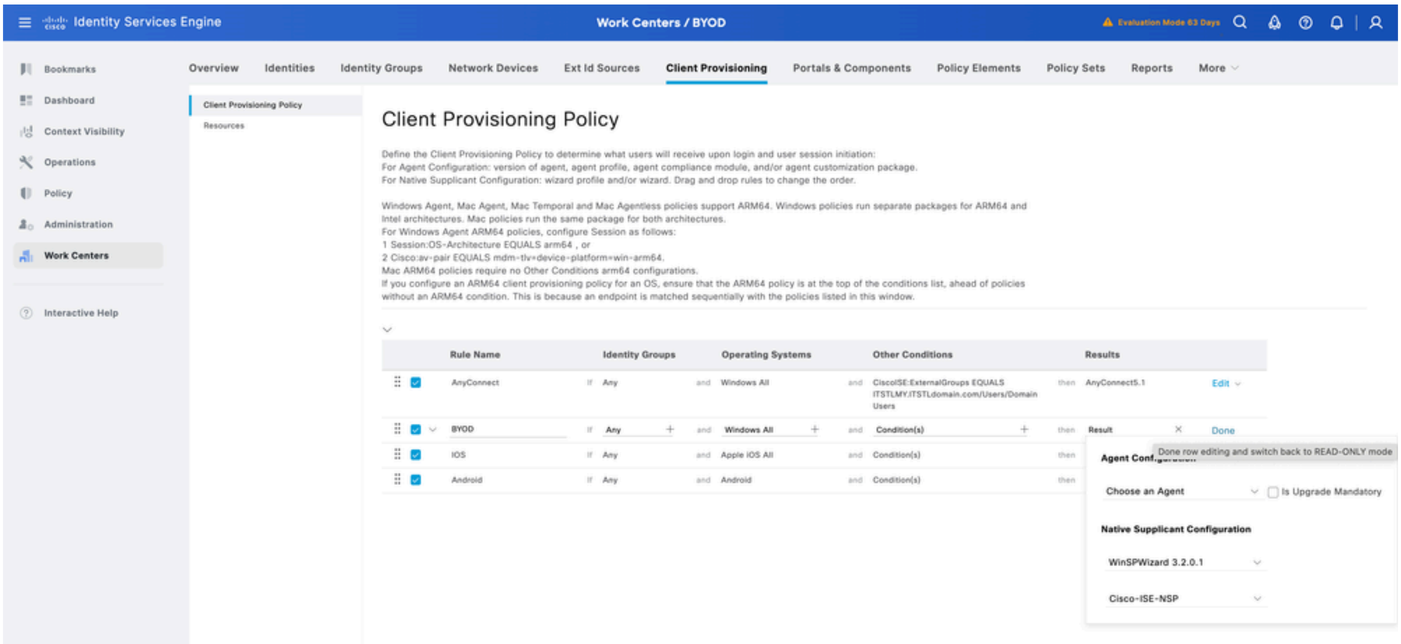
	Rule Name		Identity Groups		Operating Systems		Other Conditions		Results	
☑	AnyConnect	If	Any	and	Windows All	and	CiscoISE:ExternalGroups EQUALS ITSTLMY.ITSTLdomain.com/Users/Domain Users	then	AnyConnect5.1	Edit
☑	IOS	If	Any	and	Apple iOS All	and	Condition(s)	then	Cisco-ISE-NSP	Edit
☑	Android	If	Any	and	Android	and	Condition(s)	then	Cisco-ISE-NSP	Edit
□	DownloadAnyConnect	If	Any	and	Windows All	and	Condition(s)	then	AnyConnect5.1	Edit

3. Post creating the new rule on the page

4. Add the identity group if you would like restrict certain users to use the BYOD portal

5. Add the operating system which you would like to have access to the BYOD portal

6. Map the Cisco IOS version from the drop down and also select the endpoint profile which you have created from the result



Client Provisioning Policy

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

Windows Agent, Mac Agent, Mac Temporal and Mac Agentless policies support ARM64. Windows policies run separate packages for ARM64 and Intel architectures. Mac policies run the same package for both architectures.
For Windows Agent ARM64 policies, configure Session as follows:
1 Session:OS-Architecture EQUALS arm64 , or
2 Cisco:av-pair EQUALS mdm-tlv=device-platform=win-arm64.
Mac ARM64 policies require no Other Conditions arm64 configurations.
If you configure an ARM64 client provisioning policy for an OS, ensure that the ARM64 policy is at the top of the conditions list, ahead of policies without an ARM64 condition. This is because an endpoint is matched sequentially with the policies listed in this window.

	Rule Name		Identity Groups		Operating Systems		Other Conditions		Results	
☑	AnyConnect	If	Any	and	Windows All	and	CiscoISE:ExternalGroups EQUALS ITSTLMY.ITSTLdomain.com/Users/Domain Users	then	AnyConnect5.1	Edit
☑	BYOD	If	Any	and	Windows All	and	Condition(s)	then	Result	Done
☑	IOS	If	Any	and	Apple iOS All	and	Condition(s)	then		
☑	Android	If	Any	and	Android	and	Condition(s)	then		

Agent Configuration

Choose an Agent □ Is Upgrade Mandatory

Native Supplicant Configuration

WinSPWizard 3.2.0.1

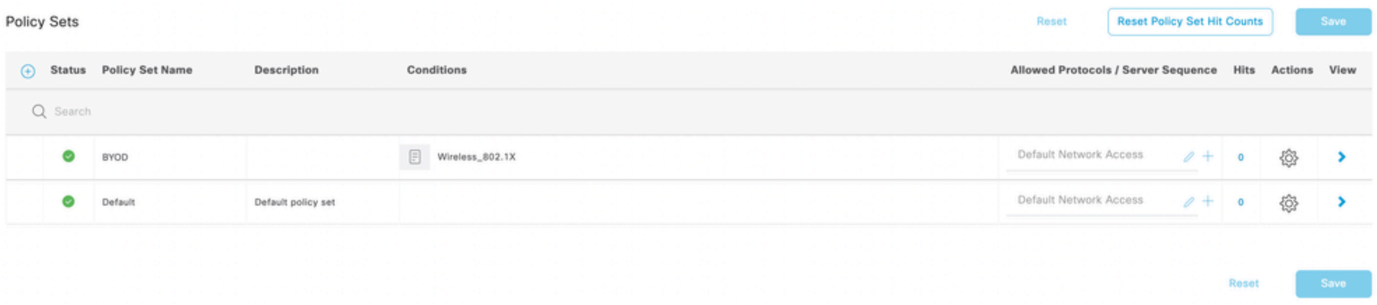
Cisco-ISE-NSP

7. Click **Done,** then the **Save** button.

Note: This policy impacts both posture client provisioning and BYOD provisioning, where the Agent Configuration section determines the posture agent and compliance module enforced for posture checks, while the Native Supplicant Configuration section manages settings for BYOD provisioning flows

Configure ISE Policy Sets for Single SSID BYOD

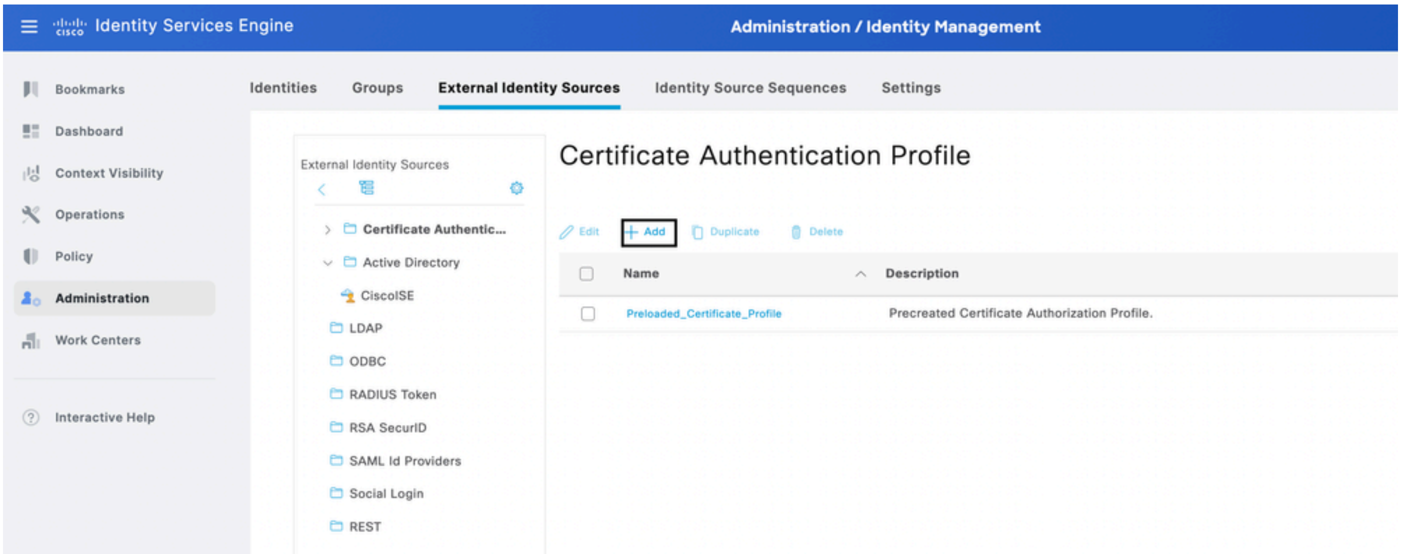
1. Navigate to **Policy > Policy Set** and create a policy for BYOD flow on ISE:



Policy Sets

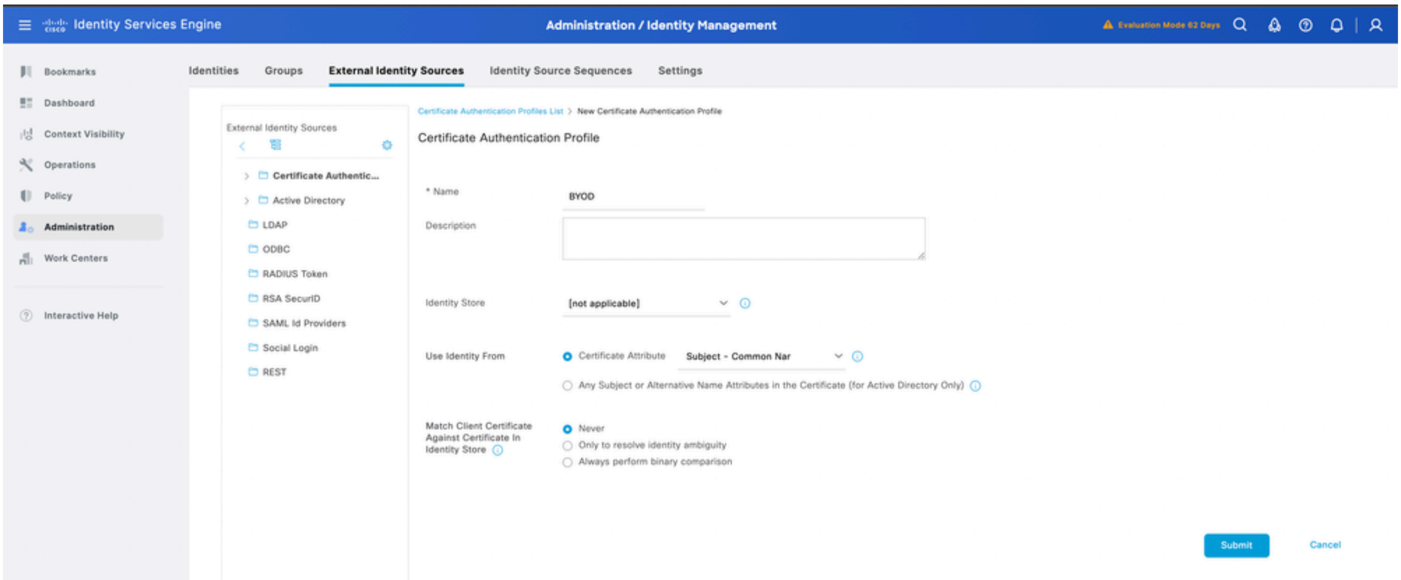
	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
	●	BYOD		Wireless_802.1X	Default Network Access	0	⚙	›
	●	Default	Default policy set		Default Network Access	0	⚙	›

2. Then, navigate to **Administration > Identity Management > External Identity Sources > Certificate Authentication Profile**. Click the **Add** button to create the Certificate profile:



Certificate Authentication Profile

	Name	Description
□	Preloaded_Certificate_Profile	Precreated Certificate Authorization Profile.



Certificate Authentication Profile

* Name: BYOD

Description:

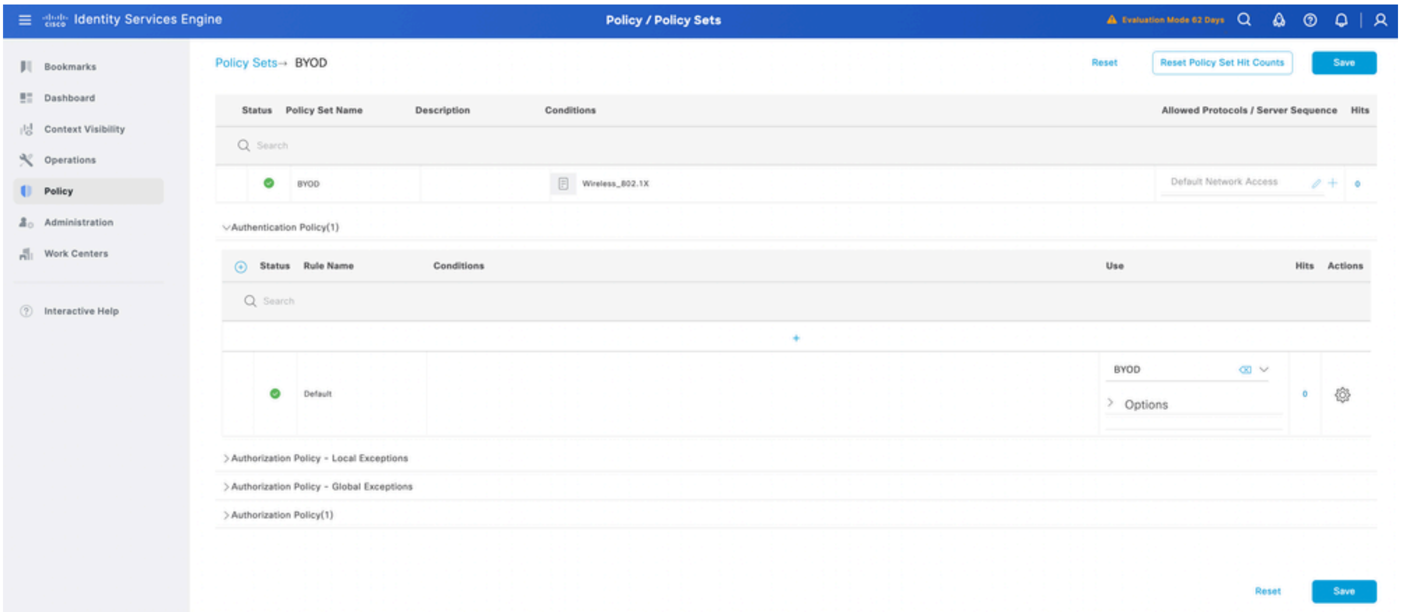
Identity Store: [not applicable]

Use Identity From: ● Certificate Attribute: Subject - Common Nar
○ Any Subject or Alternative Name Attributes in the Certificate (for Active Directory Only)

Match Client Certificate Against Certificate In Identity Store:
● Never
○ Only to resolve identity ambiguity
○ Always perform binary comparison

Note: In the Identity Store, you can always select your Active Directory which has been integrated to ISE to perform a user lookup from the certificate for addition security.

3. Click **Submit** to save the configuration. Then, map the certificate profile to the policy set for BYOD:



Policy Sets→ BYOD

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
●	BYOD		Wireless_802.1X	Default Network Access	0

Authentication Policy(1)

Status	Rule Name	Conditions	Use	Hits	Actions
●	Default		BYOD	0	

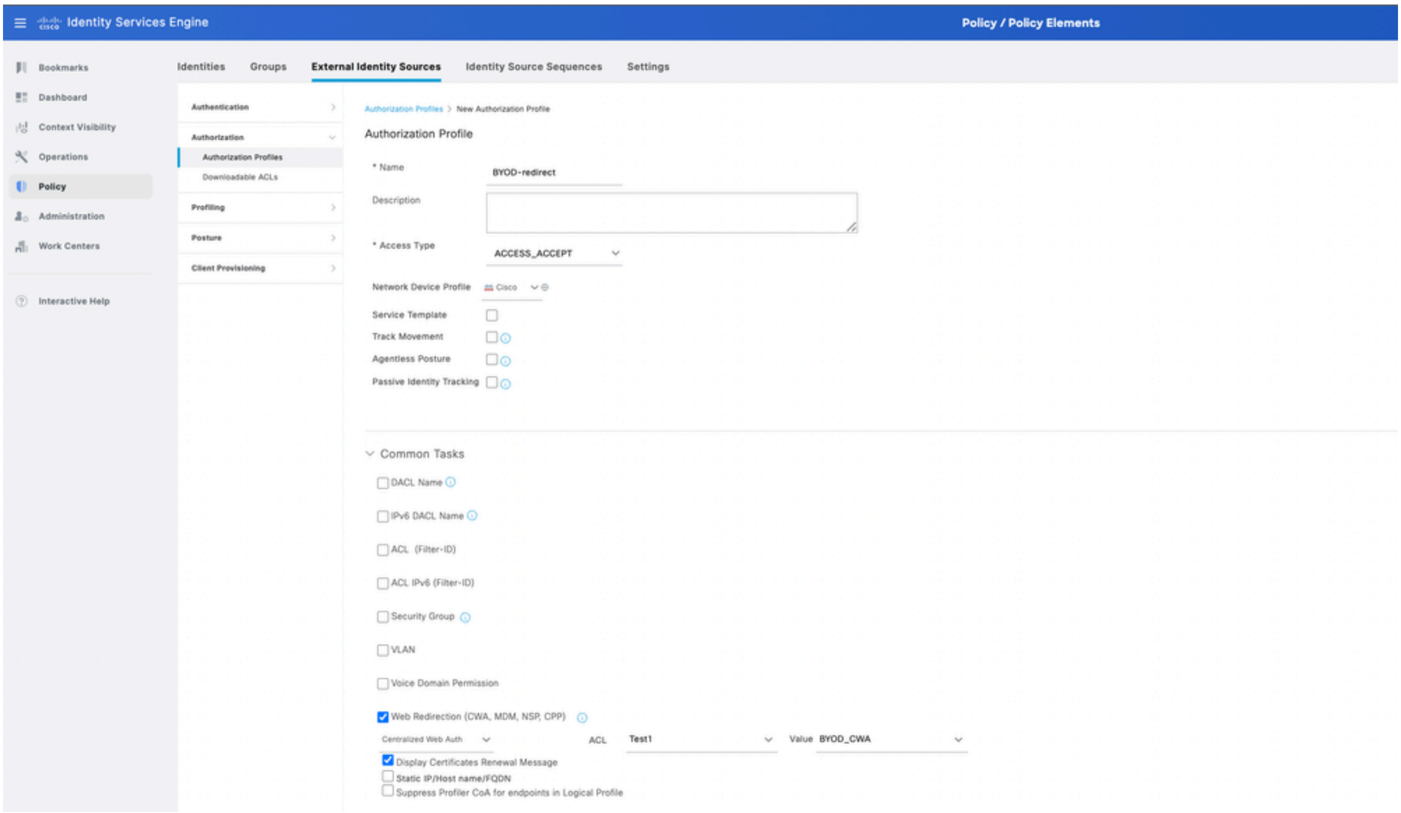
Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy(1)

4. Configure the Authorization profile for BYOD redirect and full access post the BYOD flow. Navigate to **Policy > Policy Elements > Results > Authorization > Authorization Profiles**.

5. Click **Add** and create a authorization profile. Check the Web Redirection (CWA,MDM,NSP,CPP) and map the BYOD portal page. Also, add the Redirection ACL name from WLC to the profile. For the Full access profile, configure a permit access with the respective corporate VLAN in the profile.



Authorization Profiles > New Authorization Profile

Authorization Profile

* Name: BYOD-redirect

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template □

Track Movement □

Agentless Posture □

Passive Identity Tracking □

Common Tasks

□ DACL Name

□ IPv6 DACL Name

□ ACL (Filter-ID)

□ ACL IPv6 (Filter-ID)

□ Security Group

□ VLAN

□ Voice Domain Permission

☑ Web Redirection (CWA, MDM, NSP, CPP)

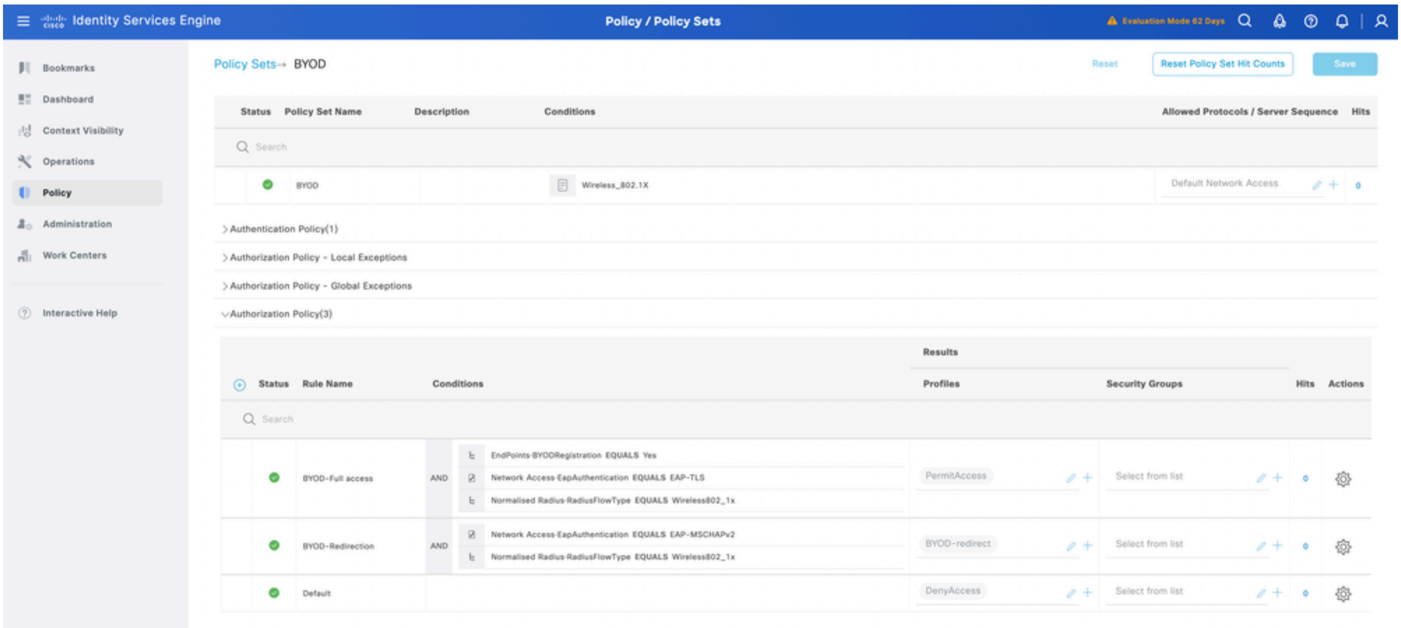
Centralized Web Auth ACL Test1 Value BYOD_CWA

☑ Display Certificates Renewal Message

□ Static IP/Host name/FQDN

□ Suppress Profiler CoA for endpoints in Logical Profile

6. Map the authorization profile to the Authorization rule. The BYOD full access must have the rule EndPoints·BYODRegistration equal yes so that the user gets full access to the network post the BYOD flow.



Policy Sets→ BYOD

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
●	BYOD		Wireless_802.1X	Default Network Access	0

> Authentication Policy(1)

> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions

∨ Authorization Policy(3)

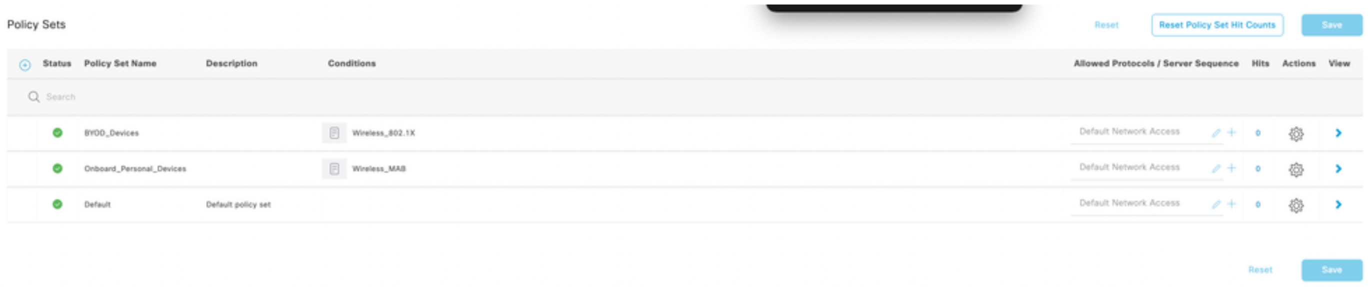
Status	Rule Name		Conditions	Results		Hits	Actions
				Profiles	Security Groups		
●	BYOD-Full access	AND	EndPoints·BYODRegistration EQUALS Yes Network Access·EapAuthentication EQUALS EAP-TLS Normalised Radius·RadiusFlowType EQUALS Wireless802_1x	PermitAccess	Select from list	0	⚙
●	BYOD-Redirection	AND	Network Access·EapAuthentication EQUALS EAP-MSCHAPv2 Normalised Radius·RadiusFlowType EQUALS Wireless802_1x	BYOD-redirect	Select from list	0	⚙
●	Default			DenyAccess	Select from list	0	⚙

Configure ISE Policy Sets for Dual SSID BYOD

In Dual SSID BYOD configuration, the two-policy set is configured on ISE. The First policy set is for the open/ unsecured SSID, where Policy Set configuration redirects the user to the BYOD page upon connecting to the open/ unsecured SSID

1. Navigate to **Policy** > **Policy Set** and create a Policy for BYOD flow on ISE.

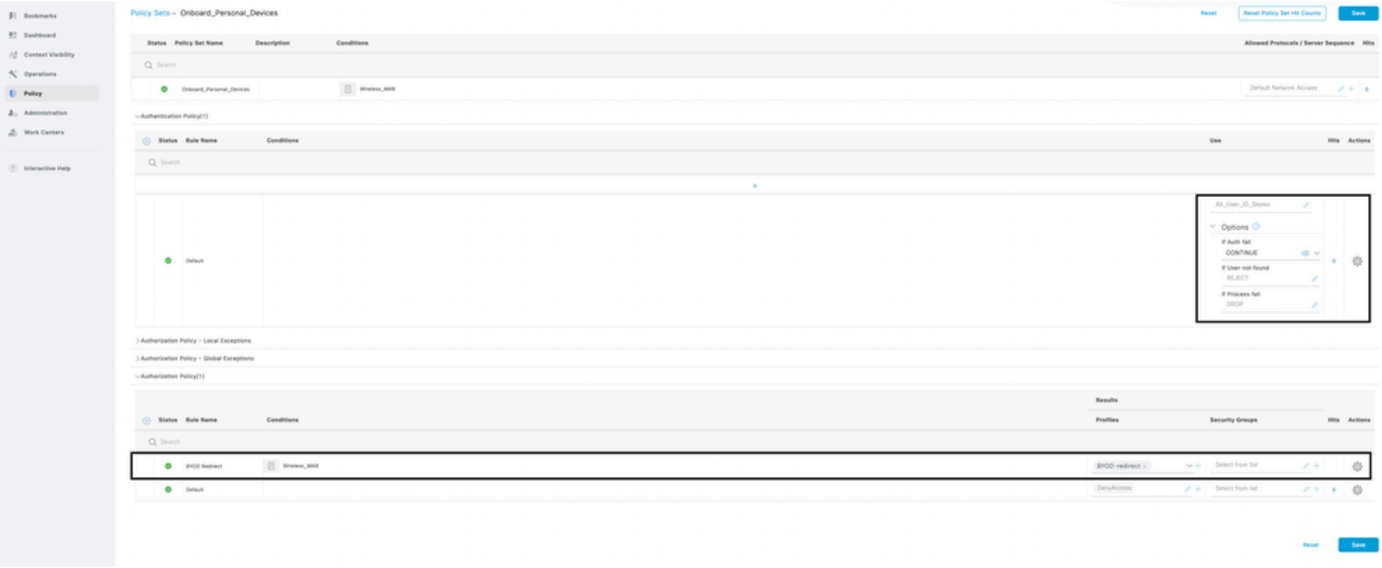
2. Create a Policy set for the Open/Unsecured SSID and Corporate SSID which authenticates the registered BYOD user on ISE.



Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
●	BYOD_Devices		Wireless_802.1X	Default Network Access	0	⚙	>
●	Onboard_Personal_Devices		Wireless_MAB	Default Network Access	0	⚙	>
●	Default	Default policy set		Default Network Access	0	⚙	>

3. In the Onboarding Policy set, find **Continue selected** under the options. For the authorization policy, create a condition and map the redirection authorization profile. The same steps are involved in creating the authorization profile, which could be found under in point 4.



Policy Sets → Onboard_Personal_Devices

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
●	Onboard_Personal_Devices		Wireless_MAB	Default Network Access	0

Authentication Policy(1)

Status	Rule Name	Conditions	Use	Hits	Actions
●	Default		All_User_ID_Stores Options If Auth fail: CONTINUE If User not found: REJECT If Process fail: DROP	0	

Authorization Policy - Local Exceptions

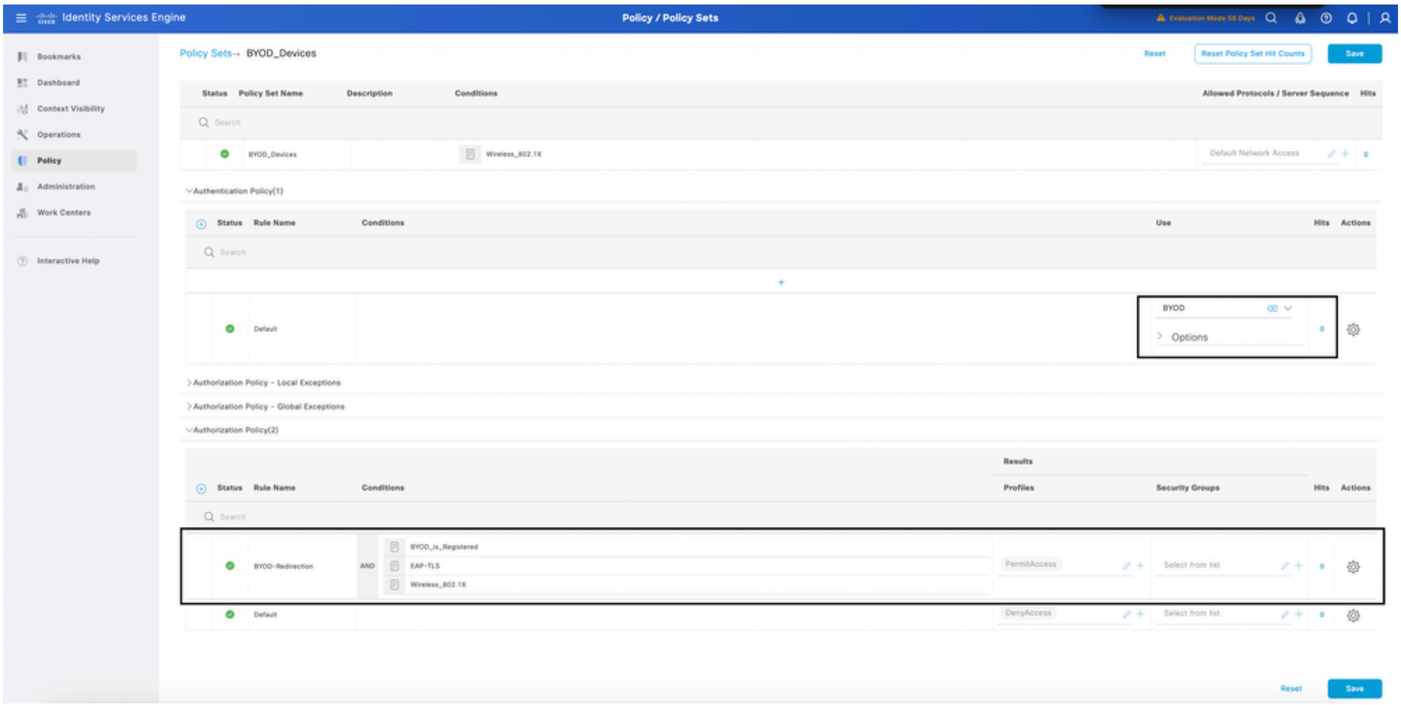
Authorization Policy - Global Exceptions

Authorization Policy(1)

Status	Rule Name	Conditions	Results: Profiles	Results: Security Groups	Hits	Actions
●	BYOD Redirect	Wireless_MAB	BYOD-redirect	Select from list		
●	Default		DenyAccess	Select from list	0	

4. In the BYOD Registered Policy Set, configure the authentication policy with the certificate profile same as found.

in *Configure ISE Policy Sets for Single SSID BYOD* in point 2. Also create a condition for authorization policy and map the full access profile to the policy.



Policy Sets → BYOD_Devices

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
●	BYOD_Devices		Wireless_802.1X	Default Network Access	0

Authentication Policy(1)

Status	Rule Name	Conditions	Use	Hits	Actions
●	Default		BYOD Options	0	

Authorization Policy - Local Exceptions

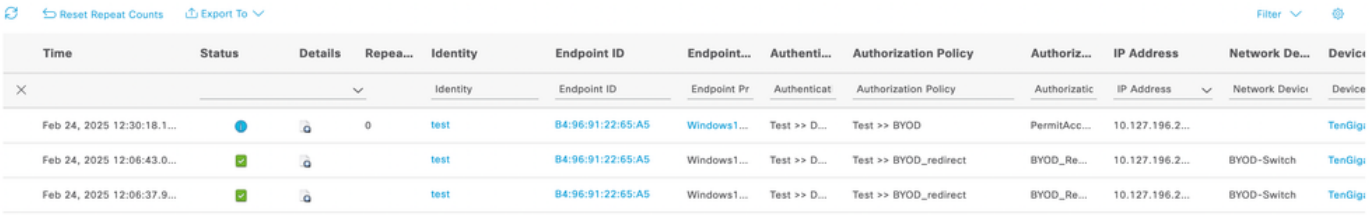
Authorization Policy - Global Exceptions

Authorization Policy(2)

Status	Rule Name	Conditions	Results: Profiles	Results: Security Groups	Hits	Actions
●	BYOD-Redirection	AND BYOD_is_Registered EAP-TLS Wireless_802.1X	PermitAccess	Select from list	0	
●	Default		DenyAccess	Select from list	0	

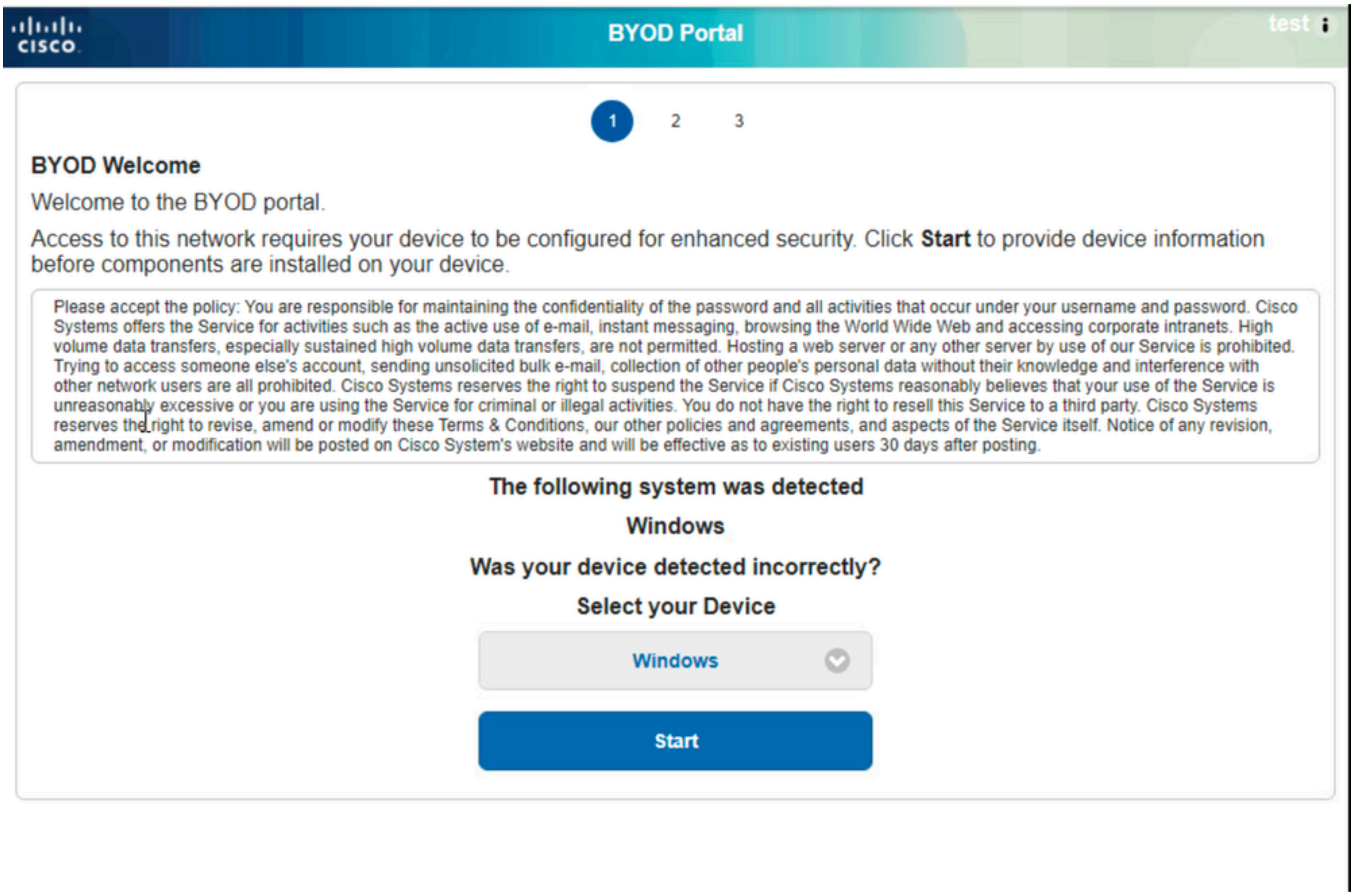
Logging

From the live log from ISE, the User authentication would be successful and will redirect to the BYOD Portal page. After completing the BYOD flow, the user would be grant access to the network



Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authenti...	Authorization Policy	Authoriz...	IP Address	Network De...	Devic
×				Identity	Endpoint ID	Endpoint Pr	Authenticat	Authorization Policy	Authorizatic	IP Address	Network Devic	Device
Feb 24, 2025 12:30:18.1...	●		0	test	B4:96:91:22:65:A5	Windows1...	Test >> D...	Test >> BYOD	PermitAcc...	10.127.196.2...		TenGig
Feb 24, 2025 12:06:43.0...	✓			test	B4:96:91:22:65:A5	Windows1...	Test >> D...	Test >> BYOD_redirect	BYOD_Re...	10.127.196.2...	BYOD-Switch	TenGig
Feb 24, 2025 12:06:37.9...	✓			test	B4:96:91:22:65:A5	Windows1...	Test >> D...	Test >> BYOD_redirect	BYOD_Re...	10.127.196.2...	BYOD-Switch	TenGig

From the user perspective, they would first be redirected to the BYOD Page and the appropriate device needs to selected from the Web page. For testing a Windows 10 device was used



BYOD Welcome

Welcome to the BYOD portal.

Access to this network requires your device to be configured for enhanced security. Click **Start** to provide device information before components are installed on your device.

Please accept the policy: You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited. Cisco Systems reserves the right to suspend the Service if Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or modification will be posted on Cisco System's website and will be effective as to existing users 30 days after posting.

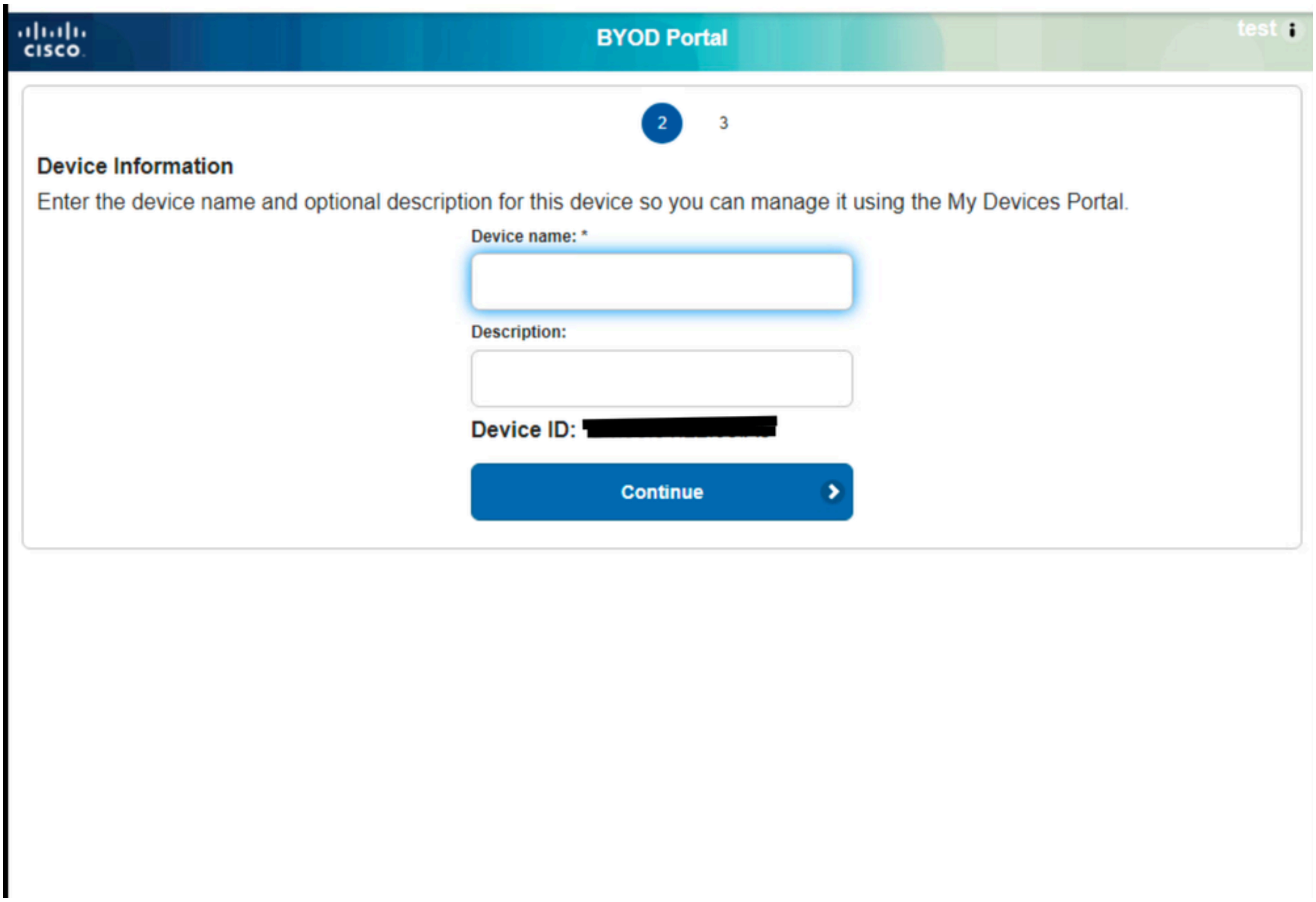
The following system was detected

Windows

Was your device detected incorrectly?

Select your Device

After clicking on the Next button, you would be directed to a page were the user would be requested to enter the name of the device and description



Device Information

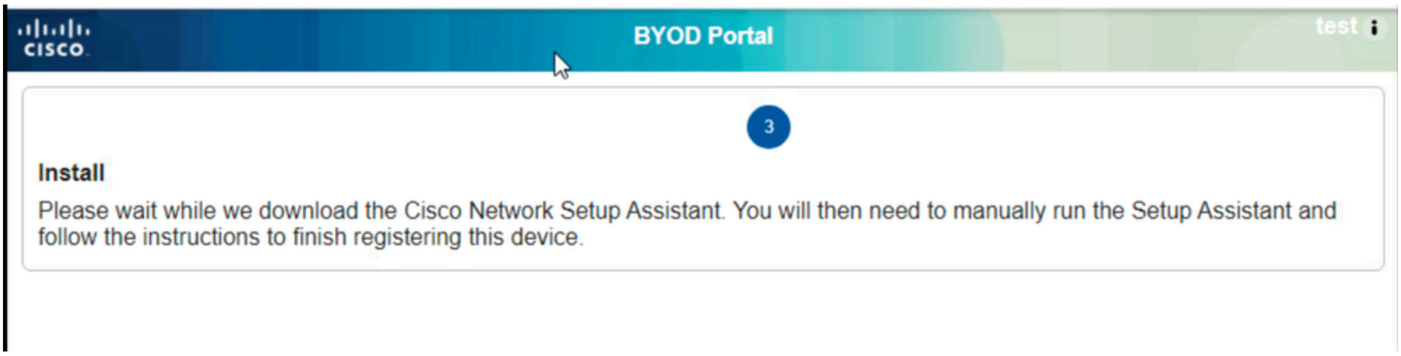
Enter the device name and optional description for this device so you can manage it using the My Devices Portal.

Device name: *

Description:

Device ID: [redacted]

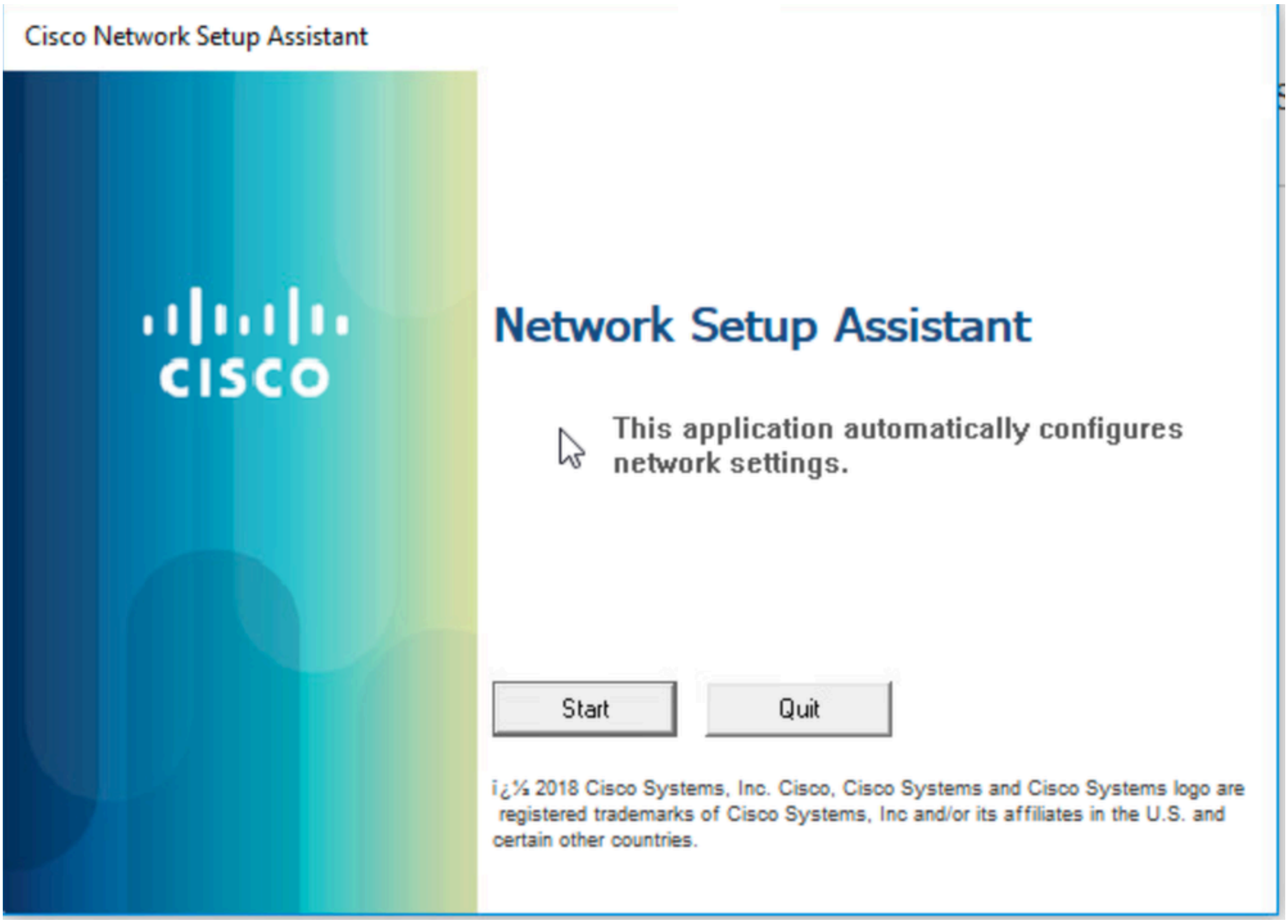
Post that the user would be requested to download the Network Assistant tool for downloading the Endpoint profile and EAP TLS certificate for authentication if the profile is configured to perform EAP-TLS authentication



Install

Please wait while we download the Cisco Network Setup Assistant. You will then need to manually run the Setup Assistant and follow the instructions to finish registering this device.

Run the Network Assistant Application in admin privileges and click on the start button to start the onboarding flow:

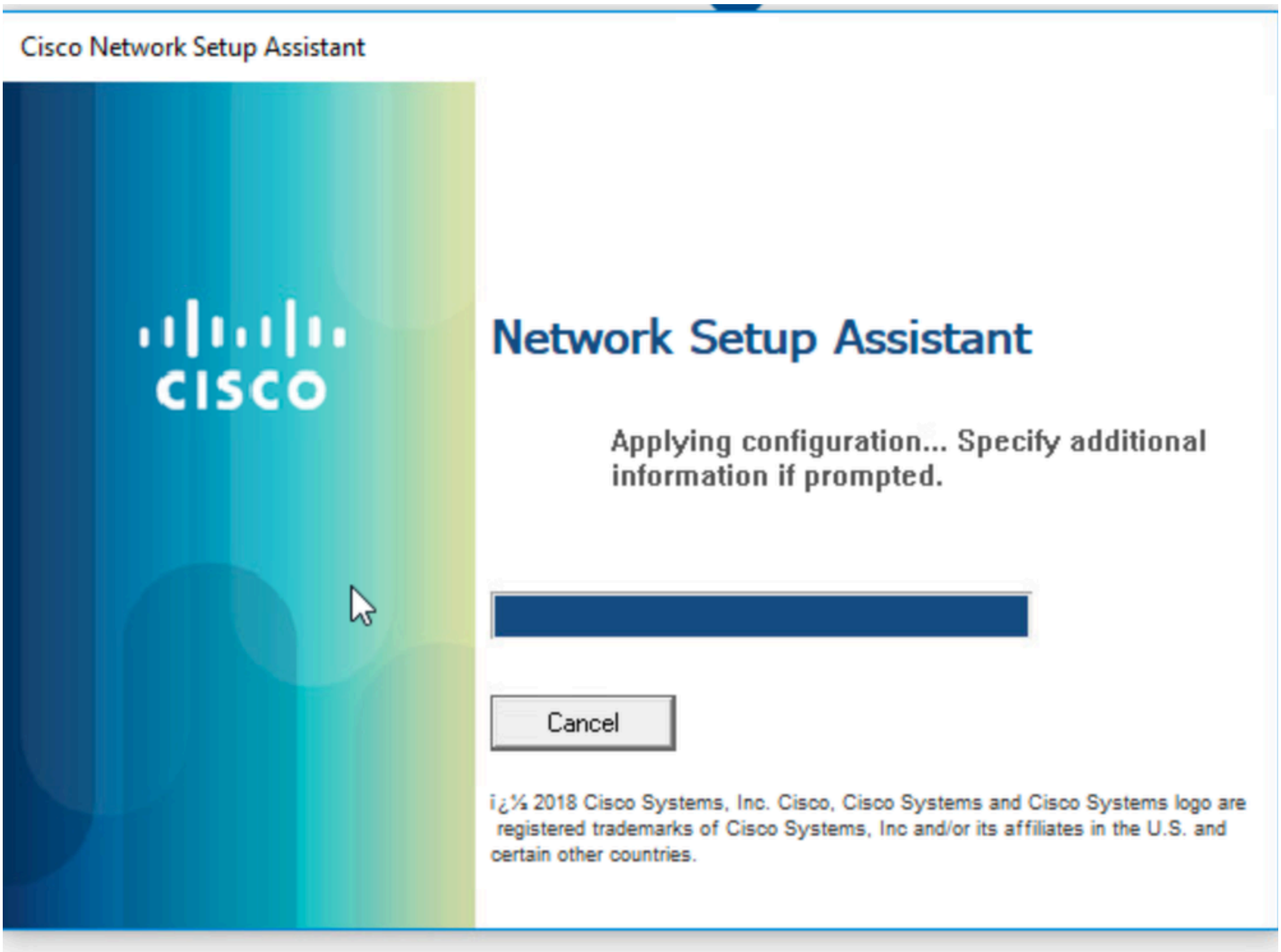


Cisco Network Setup Assistant

Network Setup Assistant

This application automatically configures network settings.

ï¿½ 2018 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc and/or its affiliates in the U.S. and certain other countries.



Cisco Network Setup Assistant

Network Setup Assistant

Applying configuration... Specify additional information if prompted.

ï¿½ 2018 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc and/or its affiliates in the U.S. and certain other countries.

The user has been successfully onboarded on the network with their personal device to access the resources.

Troubleshooting

To troubleshoot the issue with BYOD, please enable this debug on ISE

Attributes to be set to debug level:

- client (guest.log)
- client-webapp (guest.log)
- scep (ise-psc.log)
- ca-service (ise-psc.log)
- admin-ca (ise-psc.log)
- runtime-AAA (prrt-server.log)
- nsf (ise-psc.log)
- nsf-session (ise-psc.log)
- profiler (profiler.log)

Log Snippet

Guest Logs

These logs indicate that the user has successfully has redirected to the page and has downloaded the Network Assistant Application:

```
2025-02-24 12:06:08,053 INFO [https-jsse-nio-10.127.196.172-8443-exec-4][[]]
portalwebaction.utils.portal.spring.ISEPortalControllerUtils -:000000000000000B30D59CC5::::- mapping
path found in action-forwards, forwarding to: pages/byodWelcome.jsp  // The BYOD Welcome page
2025-02-24 12:06:09,968 INFO [https-jsse-nio-10.127.196.172-8443-exec-8][[]]
cpm.guestaccess.flowmanager.step.StepExecutor -:000000000000000B30D59CC5:::test:- Size of
pTranSteps:1
2025-02-24 12:06:09,968 INFO [https-jsse-nio-10.127.196.172-8443-exec-8][[]]
cpm.guestaccess.flowmanager.step.StepExecutor -:000000000000000B30D59CC5:::test:- getNextFlowStep,
pTranSteps:[id: d2513b7b-7249-4bc3-a423-0e7d9a0b2500]
2025-02-24 12:06:09,968 INFO [https-jsse-nio-10.127.196.172-8443-exec-8][[]]
cpm.guestaccess.flowmanager.step.StepExecutor -:000000000000000B30D59CC5:::test:- getNextFlowStep,
stepTran:d2513b7b-7249-4bc3-a423-0e7d9a0b2500
2025-02-24 12:06:09,979 INFO [https-jsse-nio-10.127.196.172-8443-exec-8][[]]
portalwebaction.utils.portal.spring.ISEPortalControllerUtils -:000000000000000B30D59CC5::::- mapping
path found in action-forwards, forwarding to: pages/byodRegistration.jsp
2025-02-24 12:06:14,643 INFO [https-jsse-nio-10.127.196.172-8443-exec-2][[]]
cpm.guestaccess.flowmanager.step.StepExecutor -:000000000000000B30D59CC5:::test:- Size of
pTranSteps:1
2025-02-24 12:06:14,643 INFO [https-jsse-nio-10.127.196.172-8443-exec-2][[]]
cpm.guestaccess.flowmanager.step.StepExecutor -:000000000000000B30D59CC5:::test:- getNextFlowStep,
pTranSteps:[id: f203b757-9e8a-473e-abdc-879d0cd37491]
2025-02-24 12:06:14,643 INFO [https-jsse-nio-10.127.196.172-8443-exec-2][[]]
cpm.guestaccess.flowmanager.step.StepExecutor -:000000000000000B30D59CC5:::test:- getNextFlowStep,
stepTran:f203b757-9e8a-473e-abdc-879d0cd37491
2025-02-24 12:06:14,647 INFO [https-jsse-nio-10.127.196.172-8443-exec-2][[]]
portalwebaction.utils.portal.spring.ISEPortalControllerUtils -:000000000000000B30D59CC5::::- mapping
path found in action-forwards, forwarding to: pages/byodInstall.jsp
2025-02-24 12:06:14,713 DEBUG [https-jsse-nio-10.127.196.172-8443-exec-10][[]]
cisco.cpm.client.provisioning.StreamingServlet -:000000000000000B30D59CC5::::- Session = null
2025-02-24 12:06:14,713 DEBUG [https-jsse-nio-10.127.196.172-8443-exec-10][[]]
cisco.cpm.client.provisioning.StreamingServlet -:000000000000000B30D59CC5::::- portalSessionId = null
2025-02-24 12:06:14,713 DEBUG [https-jsse-nio-10.127.196.172-8443-exec-10][[]]
cisco.cpm.client.provisioning.StreamingServlet -:000000000000000B30D59CC5::::- StreamingServlet
URI:/auth/provisioning/download/f6b73ef8-4502-4d50-81aa-
bbb91e8828da/NetworkSetupAssistant.exe    // The network Assistance application has been send to
the endpoint
```

Ise-Psc Logs

As the application is downloaded to the endpoint, the application initiates a SCEP flow to get the client certificate from ISE.

```
2025-02-24 12:04:39,807 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -:::::- CertStore contains 4 certificate(s):
2025-02-24 12:04:39,807 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -:::::- 1. '[issuer=CN=Certificate Services Root CA - iseguest;
serial=32281512738768960628252532784663302089]'
2025-02-24 12:04:39,808 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -:::::- 2. '[issuer=CN=Certificate Services Endpoint Sub CA - iseguest;
serial=131900858749761727853768227590303808637]'
2025-02-24 12:04:39,810 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -:::::- 3. '[issuer=CN=Certificate Services Root CA - iseguest;
serial=68627620160586308685849818775100698224]'
2025-02-24 12:04:39,810 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -:::::- 4. '[issuer=CN=Certificate Services Node CA - iseguest;
serial=72934767698603097153932482227548874953]'
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -:::::- Selecting encryption certificate
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -:::::- Selecting certificate with keyEncipherment keyUsage
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -:::::- Found 1 certificate(s) with keyEncipherment keyUsage
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -:::::- Using [issuer=CN=Certificate Services Endpoint Sub CA -
iseguest; serial=131900858749761727853768227590303808637] for message encryption
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -:::::- Selecting verifier certificate
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -:::::- Selecting certificate with digitalSignature keyUsage
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -:::::- Found 1 certificate(s) with digitalSignature keyUsage
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -:::::- Using [issuer=CN=Certificate Services Endpoint Sub CA -
iseguest; serial=131900858749761727853768227590303808637] for message verification
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -:::::- Selecting issuer certificate
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -:::::- Selecting certificate with basicConstraints
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -:::::- Found 3 certificate(s) with basicConstraints
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -:::::- Using [issuer=CN=Certificate Services Endpoint Sub CA -
iseguest; serial=131900858749761727853768227590303808637] for issuer
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
com.cisco.cpm.scep.PKIServerLoadBalancer -:::::- SCEP servers performance metrics : name[live/dead,
total reqs, total failures, inflight reqs, Average RTT]
http://127.0.0.1:9444/caservice/scep[live,96444,1,0,120]
```

Endpoint Profile Download

After the SCEP process is completed and the endpoint installs the certificate, the application downloads the endpoint profile for future authentication which would be performed by the device:

```
2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]]
cisco.cpm.client.provisioning.EvaluationServlet -:::::- Refferer = Windows    // The Windows device has
been detected based on the webpage
2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]]
cisco.cpm.client.provisioning.EvaluationServlet -:::::- Session = 000000000000000B30D59CC5
2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]]
```

```
cisco.cpm.client.provisioning.EvaluationServlet -:::::- Session = 000000000000000B30D59CC5
2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]]
cisco.cpm.client.provisioning.EvaluationServlet -:::::- provision nsp profile
2025-02-24 12:06:26,546 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -:::::- Session = 000000000000000B30D59CC5
2025-02-24 12:06:26,546 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -:::::- portalSessionId = null
2025-02-24 12:06:26,546 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -:::::- StreamingServlet
URI:/auth/provisioning/download/b8ce01e6-b150-4d4e-9698-40e48d5e0197/Cisco-ISE-NSP.xml//The
NSP profile is downloaded to the endpoint
2025-02-24 12:06:26,547 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -:::::- Streaming to ip: file type: NativeSPProfile file
name:Cisco-ISE-NSP.xml     //The Network Assistant Application
2025-02-24 12:06:26,547 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -:::::- BYODStatus:INIT_PROFILE
2025-02-24 12:06:26,547 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -:::::- userId has been set to test
2025-02-24 12:06:26,558 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -:::::- redirect type is: SUCCESS_PAGE, redirect url is: for
mac:
```