Configure ISE BYOD with Single and Dual SSID in ISE 3.3

Contents

Introduction

Background

- Access Key Authentication Mechanism

Prerequisites

- Requirements
- Components Used

What is Single SSID and Dual SSID BYOD on ISE?

- Single SSID BYOD
- Dual SSID BYOD

WLC Configuration

- Create a WLAN for CWA
- Configure RADIUS Servers
- Configure AAA Servers
- Configure Security Policies for the WLAN
- Configure Pre-Authentication ACL
- Configure Policy Profile
- Apply Tags and Deploy
- Configure an Open/ Unsecured SSID

ISE Configuration

- Pre-requisites
- Certificates
- DNS Configuration

Configure ISE Network Device

Create a BYOD Portal

Download Cisco IOS® Latest Version

Create an Endpoint Profile

- Certificate Template

Map an Endpoint Profile to the Client-provisioning Portal

Configure ISE Policy Sets for Single SSID BYOD

Configure ISE Policy Sets for Dual SSID BYOD

Logging

Troubleshoot

Log Snippet

- Guest Logs
- Ise-Psc Logs
- Endpoint Profile Download

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 Cisco Identity Services Engine (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.

Access Key Authentication Mechanism

A new access key authentication mechanism has been introduced on the BYOD portal installation page to enhance security and prevent session hijacking between the browser and the Network Setup Assistant.

When a user accesses the BYOD installation page, an access key is dynamically generated and displayed in the BYOD portal. This key is unique per session and serves as a token to validate the onboarding process. The user must note this access key and enter it in the Network Setup Assistant during the device onboarding process.

Upon launching, the Network Setup Assistant prompts the user to enter the access key. The Network Setup Assistant validates the entered access key against the key generated by the BYOD portal before proceeding with onboarding. If the access key matches, the onboarding process continues. If the key does not match, the user is prompted to enter the correct key.

If your Cisco ISE version does not support access key authentication, the Network Setup Assistant presents the No Token Authentication option. This option allows users to bypass the access key entry and continue onboarding without the access key.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- WLC controller
- Basic Knowledge on ISE

Components 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)

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.

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

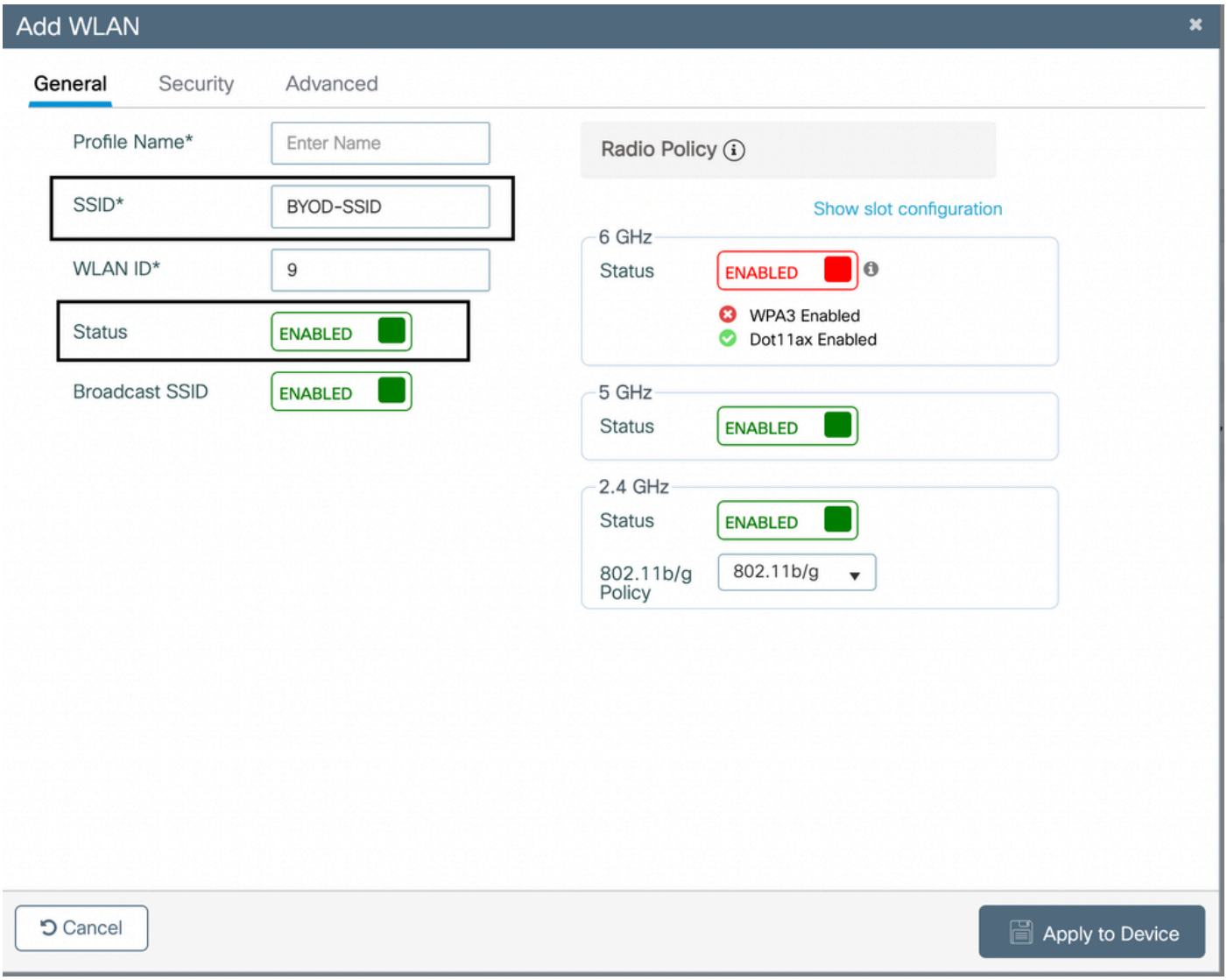
In a Dual SSID BYOD setup, two separate SSIDs are used: one for onboarding (unsecured or restricted access) and another for accessing the corporate network. Users initially connect to the onboarding SSID, complete device registration and provisioning via ISE, and then switch to the secure corporate SSID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

WLC Configuration

Create a WLAN for CWA

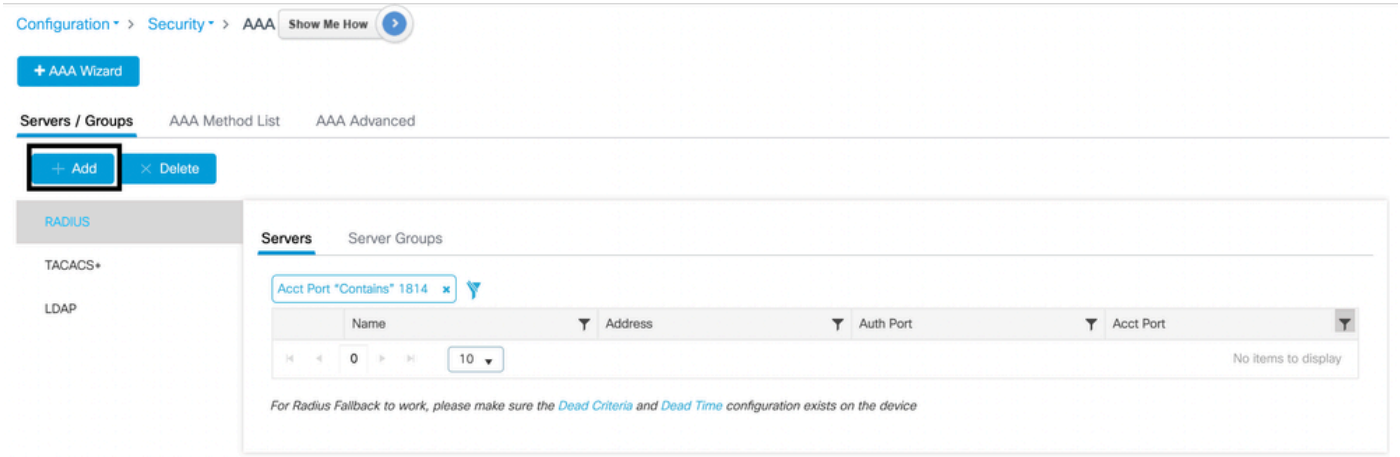
1. Navigate to **Configuration > Tags & Profiles > WLANs**.
2. Click **Add** to create a new WLAN.

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

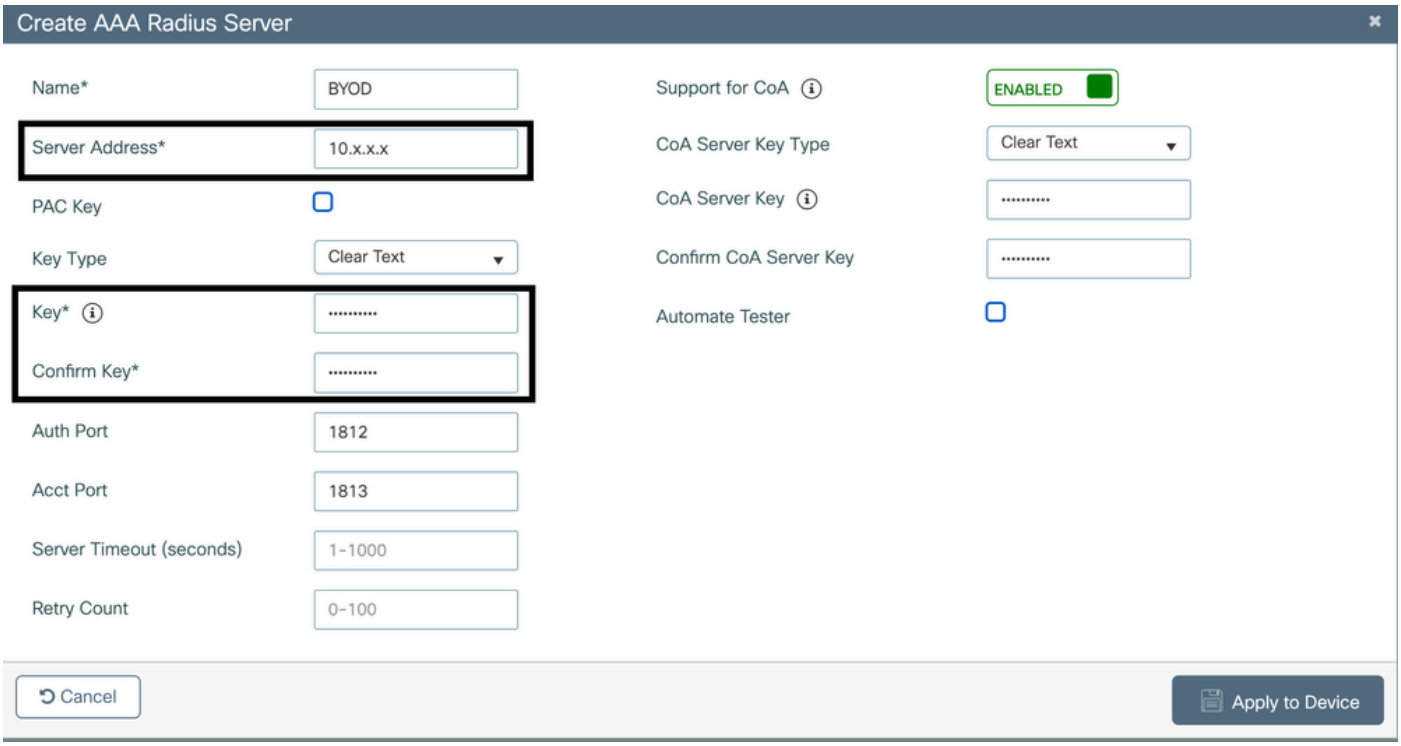


Configure RADIUS Servers

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

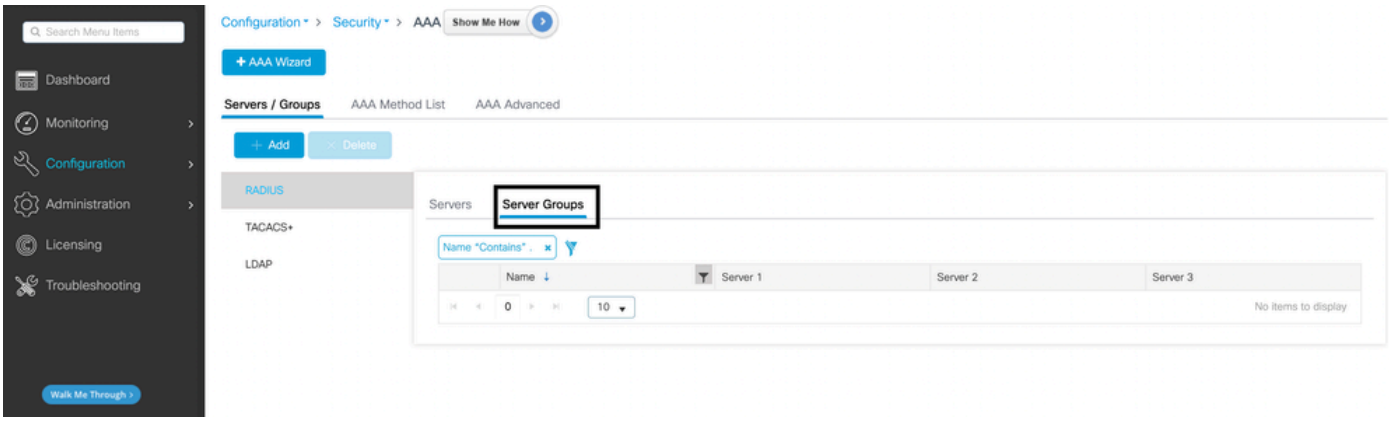


2. Click **Add** to configure ISE as a RADIUS server:
    - **Server IP**: IP address of ISE.
    - **Shared secret**: Match the shared secret configured on ISE.

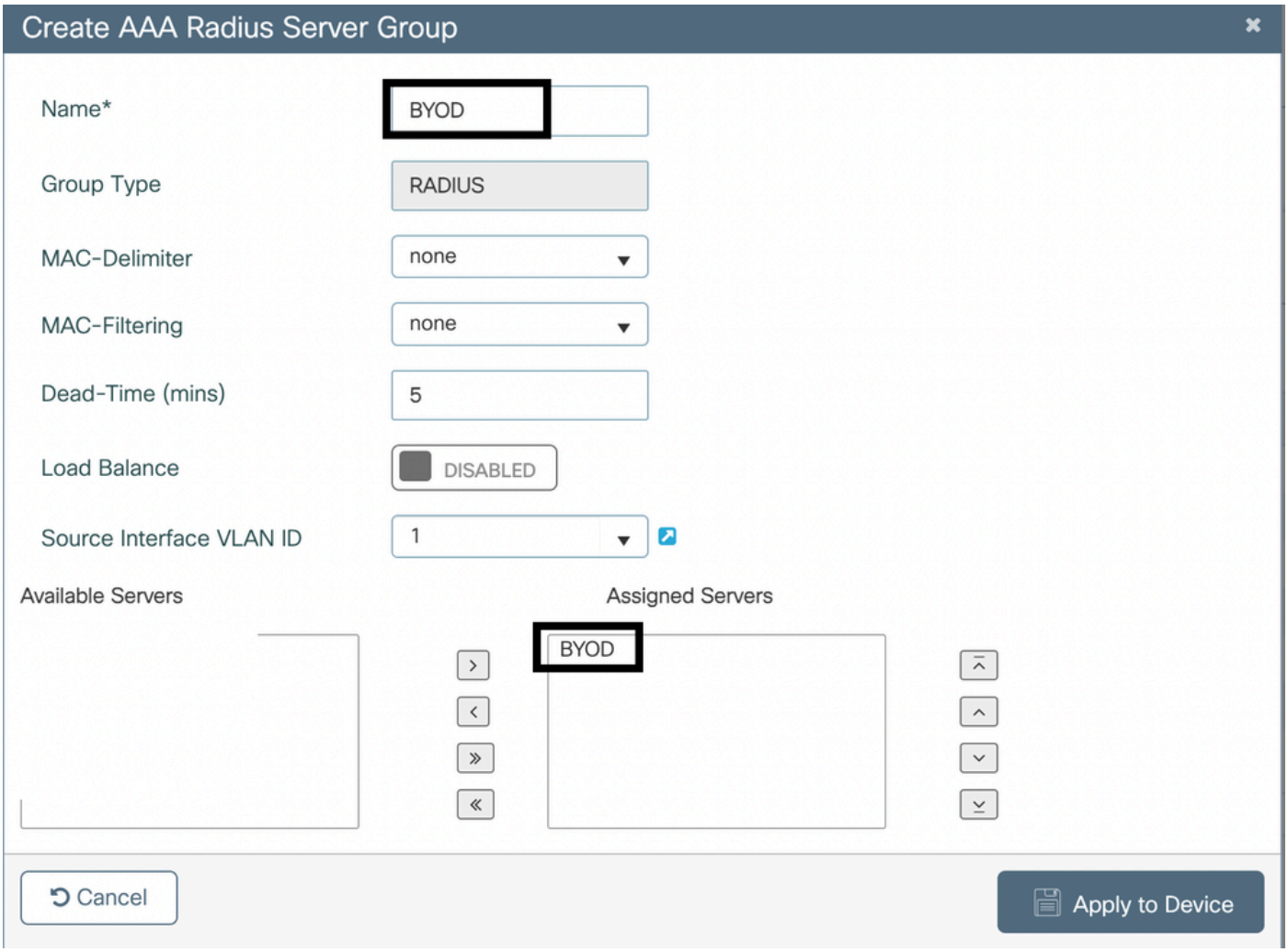


Configure AAA Servers

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



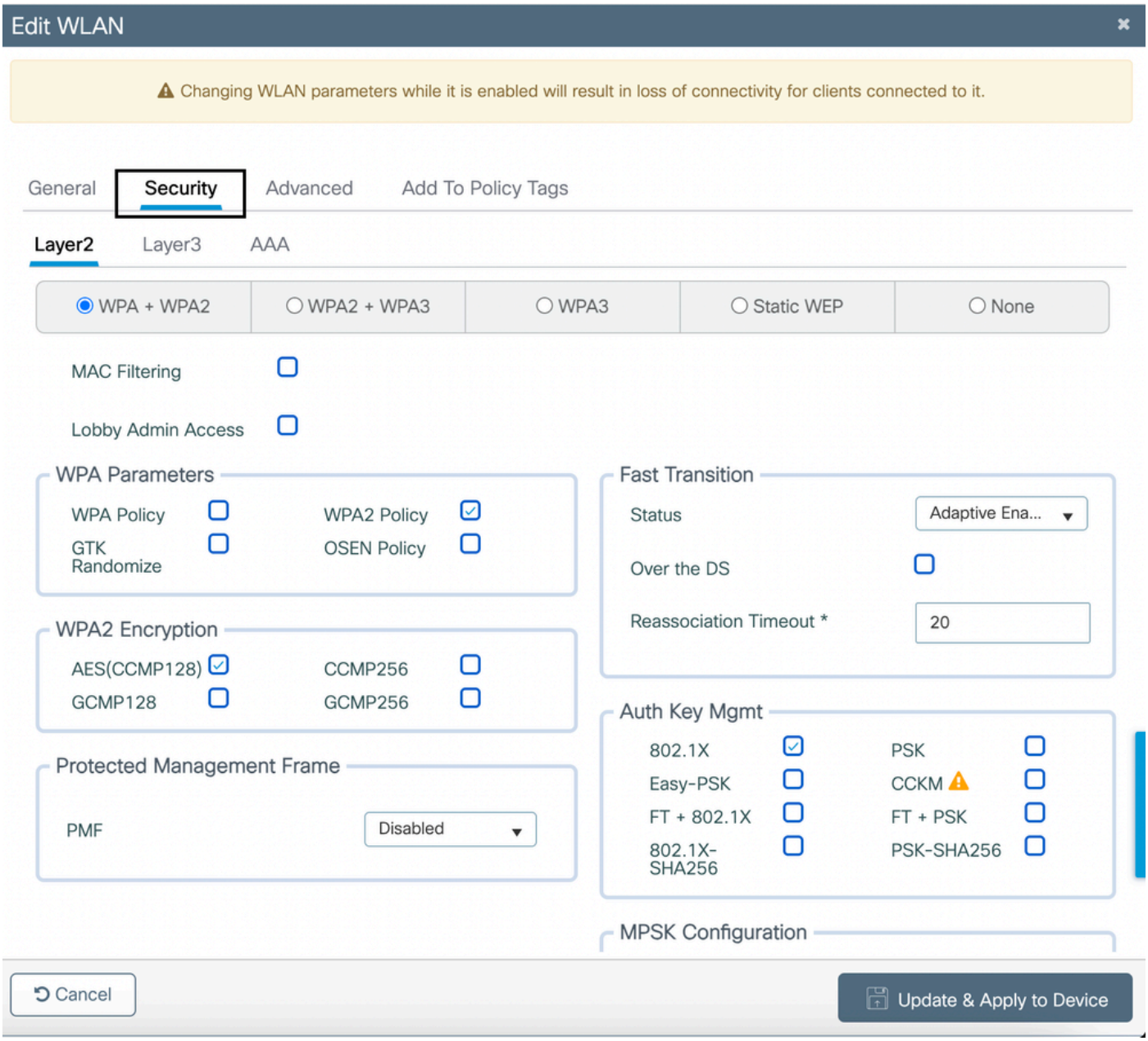
2. Assign the RADIUS server to a new or existing Server Group.



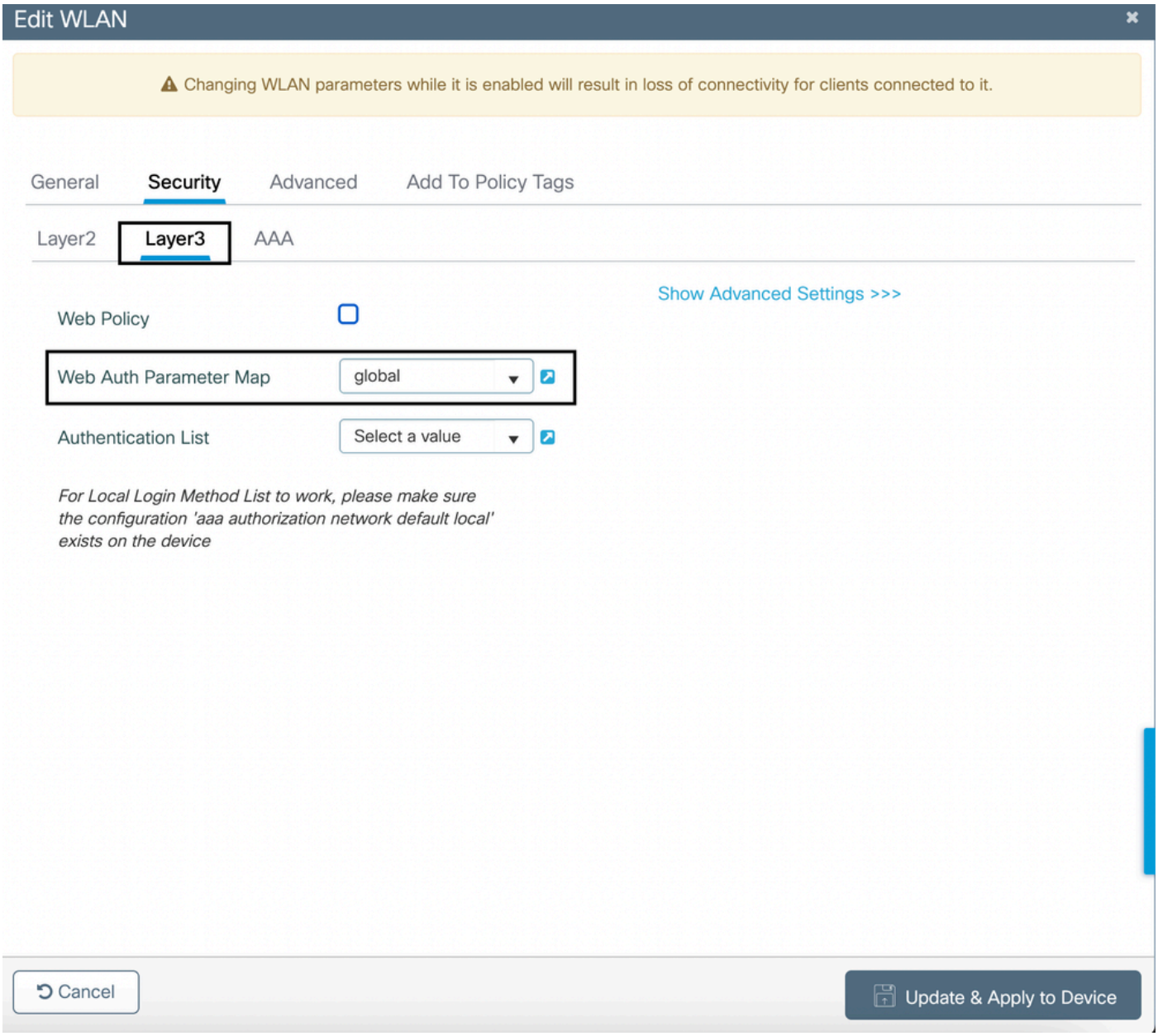
Configure Security Policies for the WLAN

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**.
- Set **Auth Key Mgmt** as **802.1X**.



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



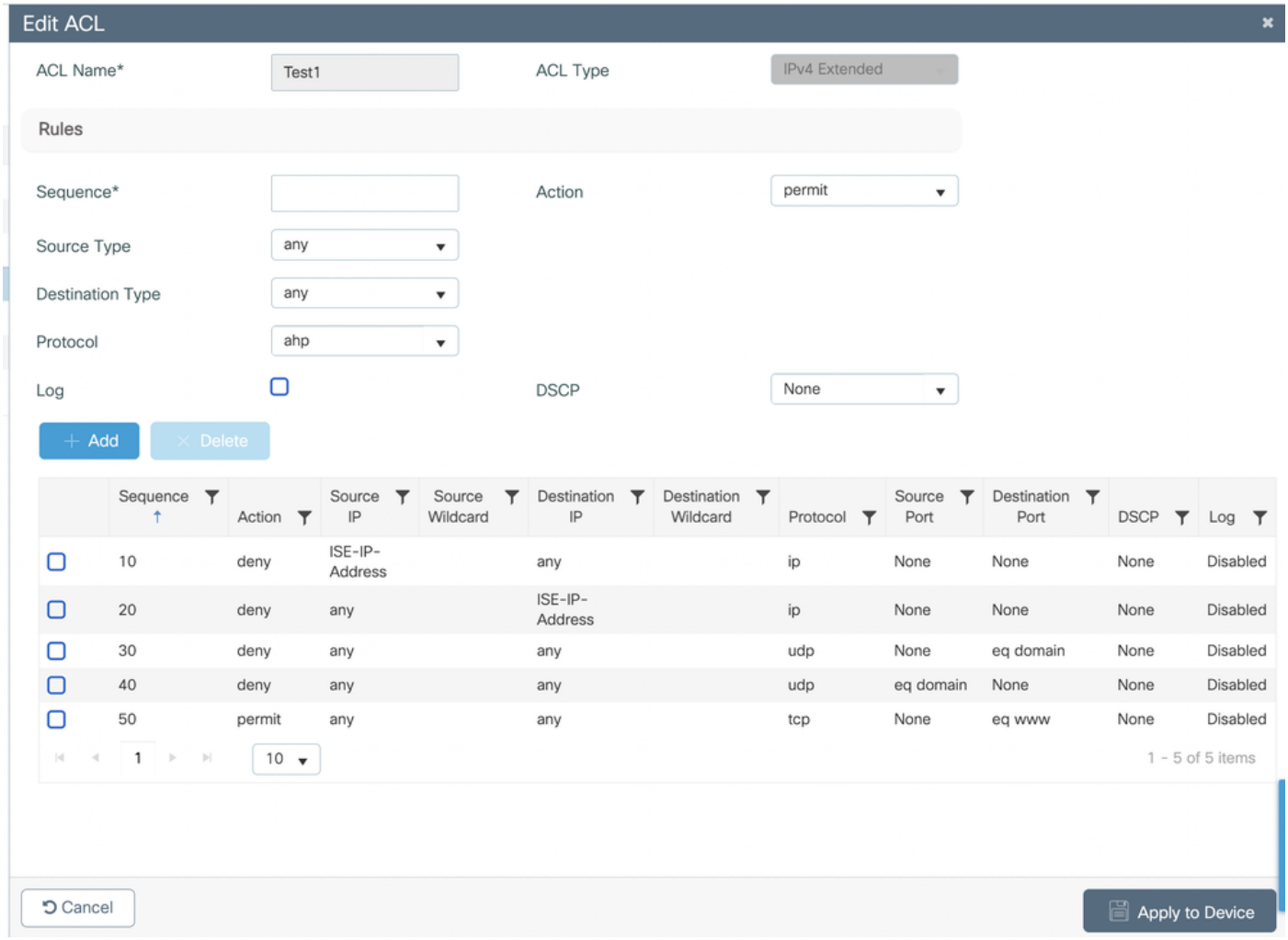
Configure Pre-Authentication ACL

Create an ACL to allow these actions for redirection:

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

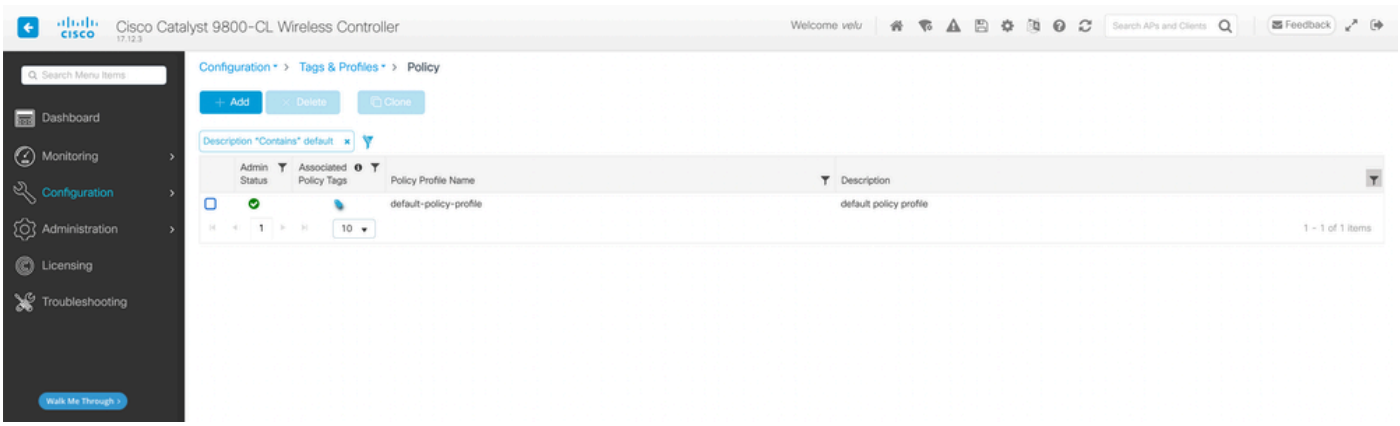
To do so:

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

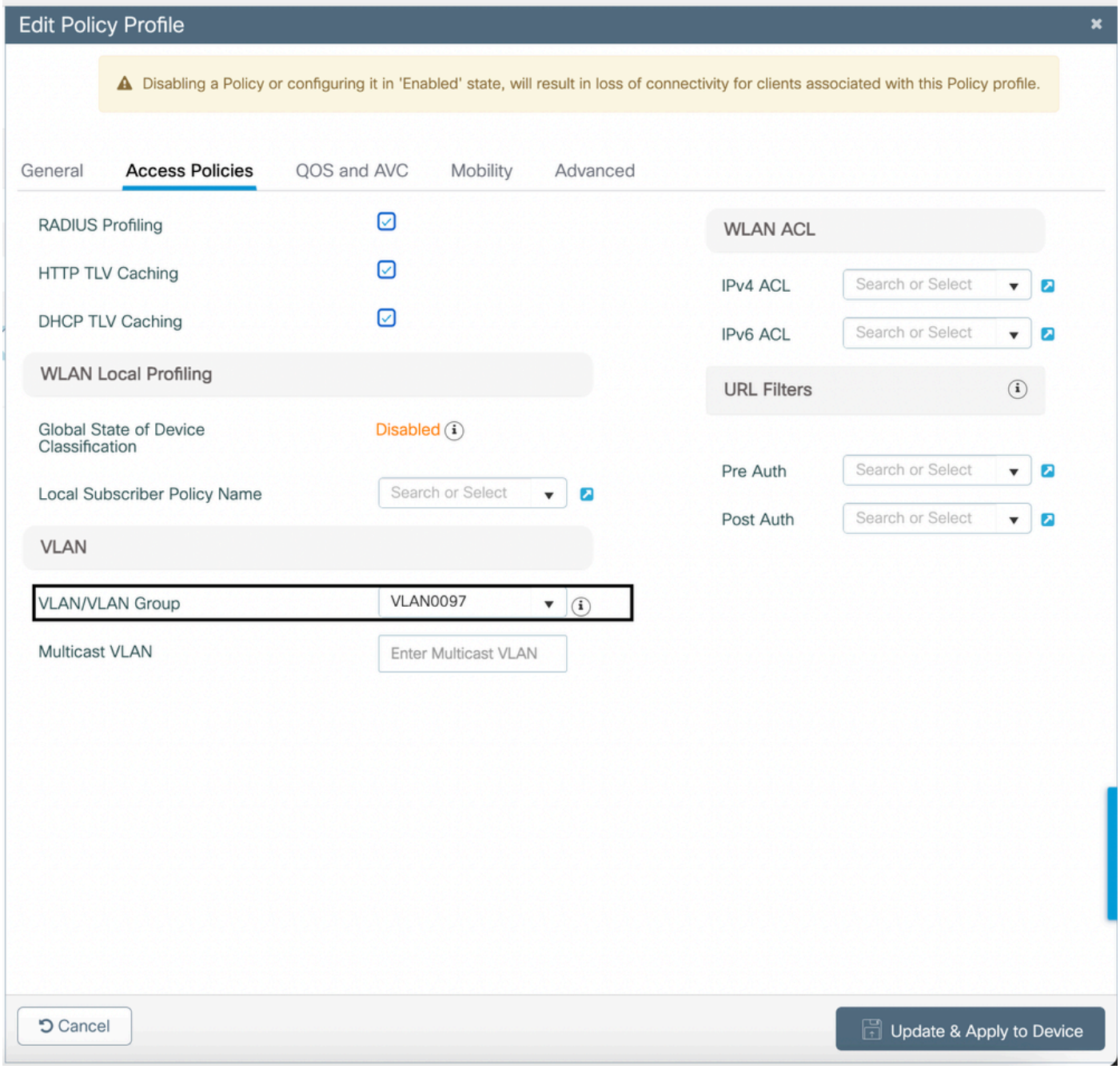


Configure Policy Profile

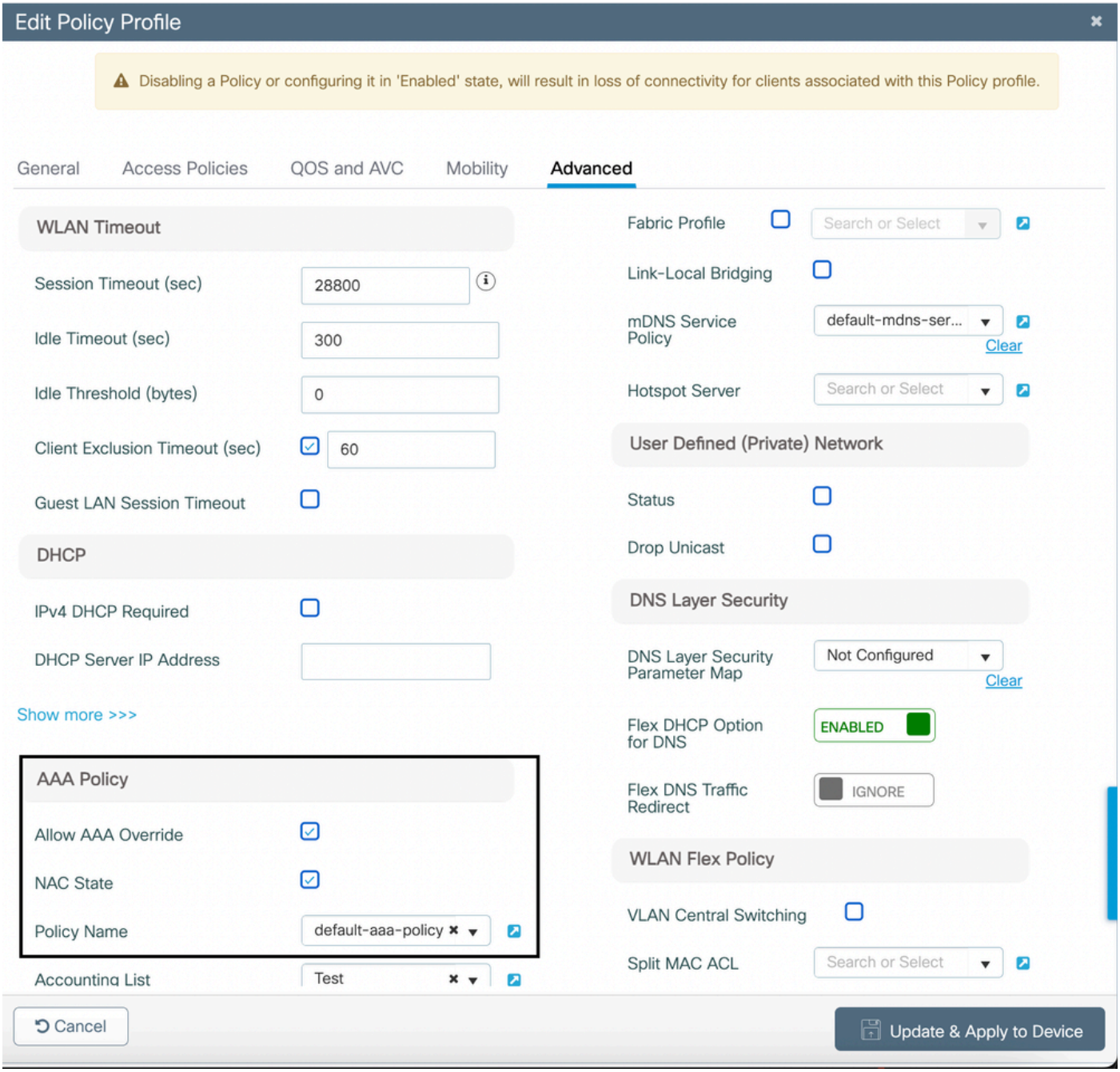
1. Navigate to **Configuration > Tags & Profiles > Policy**. You can create or use the default policy:



2. Assign the appropriate VLAN under Access Policies:

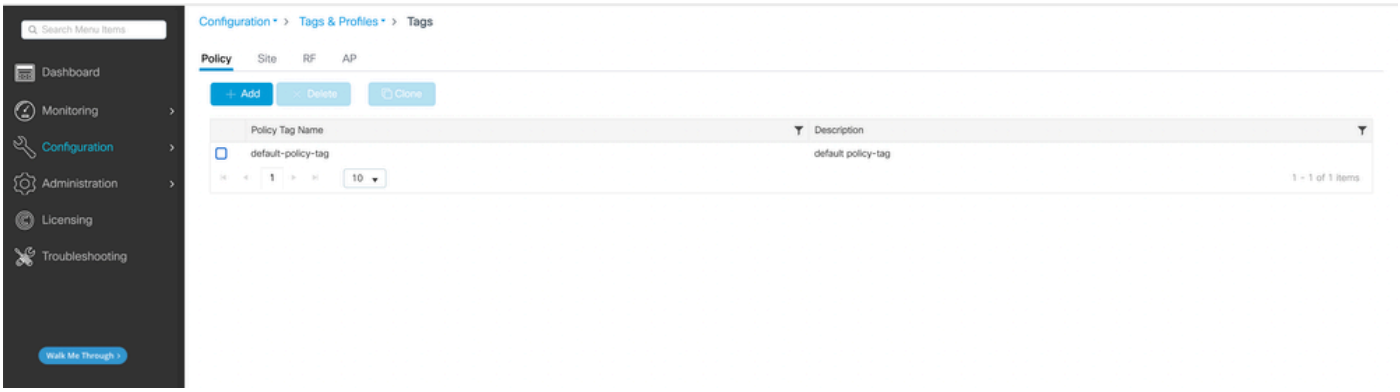


3. Also enable **Allow AAA Override** and **NAC state** under **Advanced of the policy**.



Apply Tags and Deploy

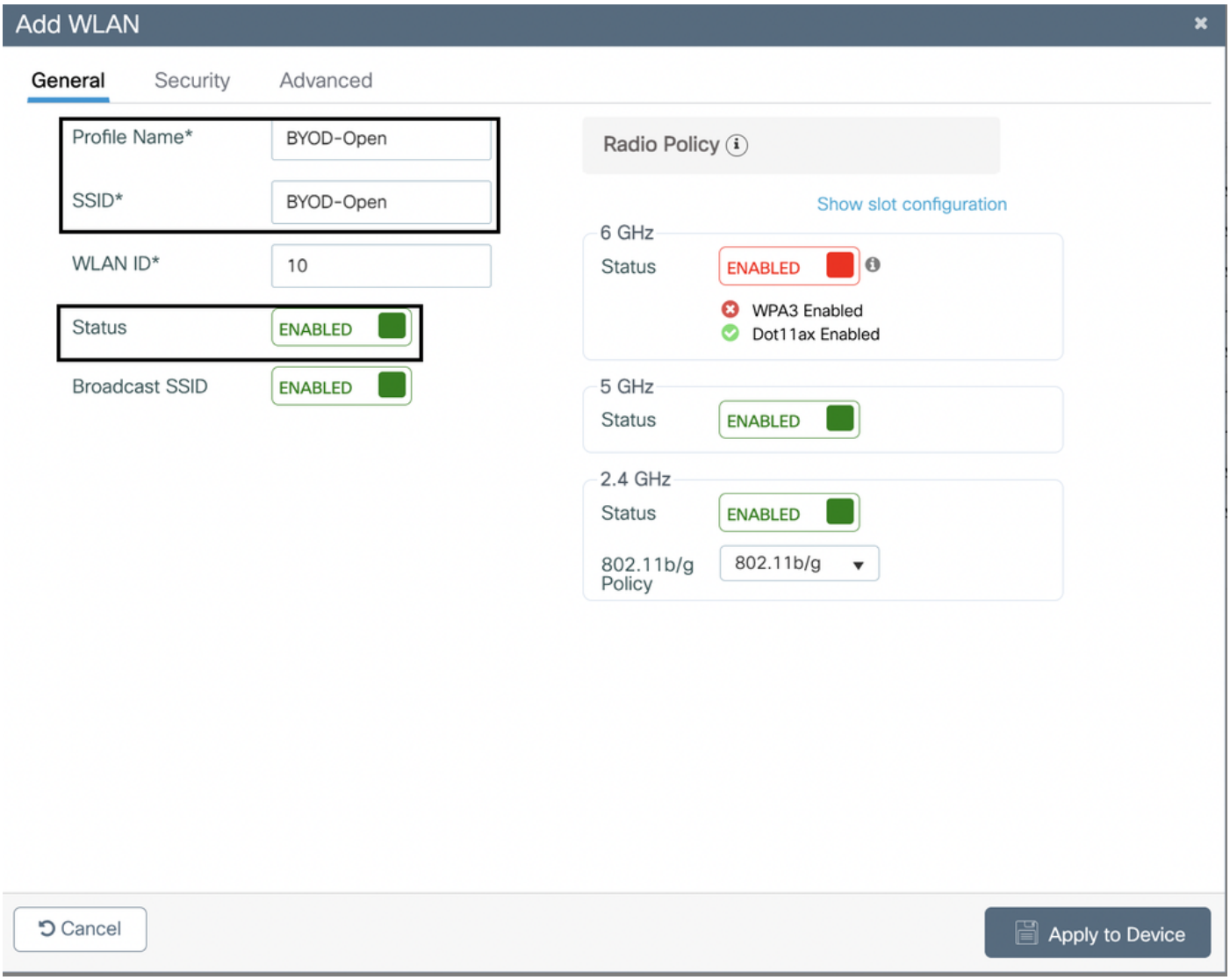
- Navigate to **Configuration > Tags & Profiles > Tags**.
- Create or edit a tag to include the WLAN and Policy Profile.
- Assign the tag to the Access Points.



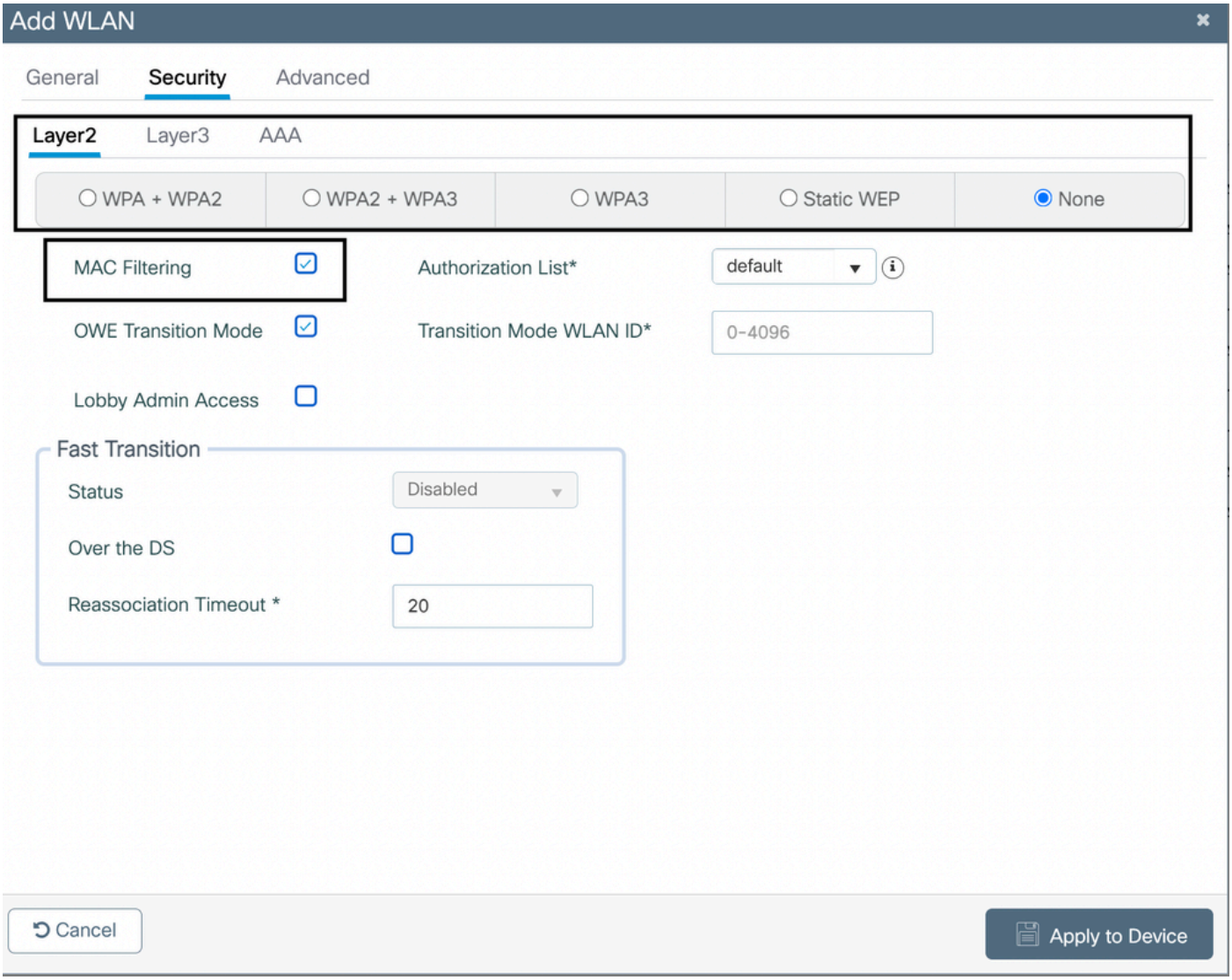
Configure an Open/ Unsecured SSID

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

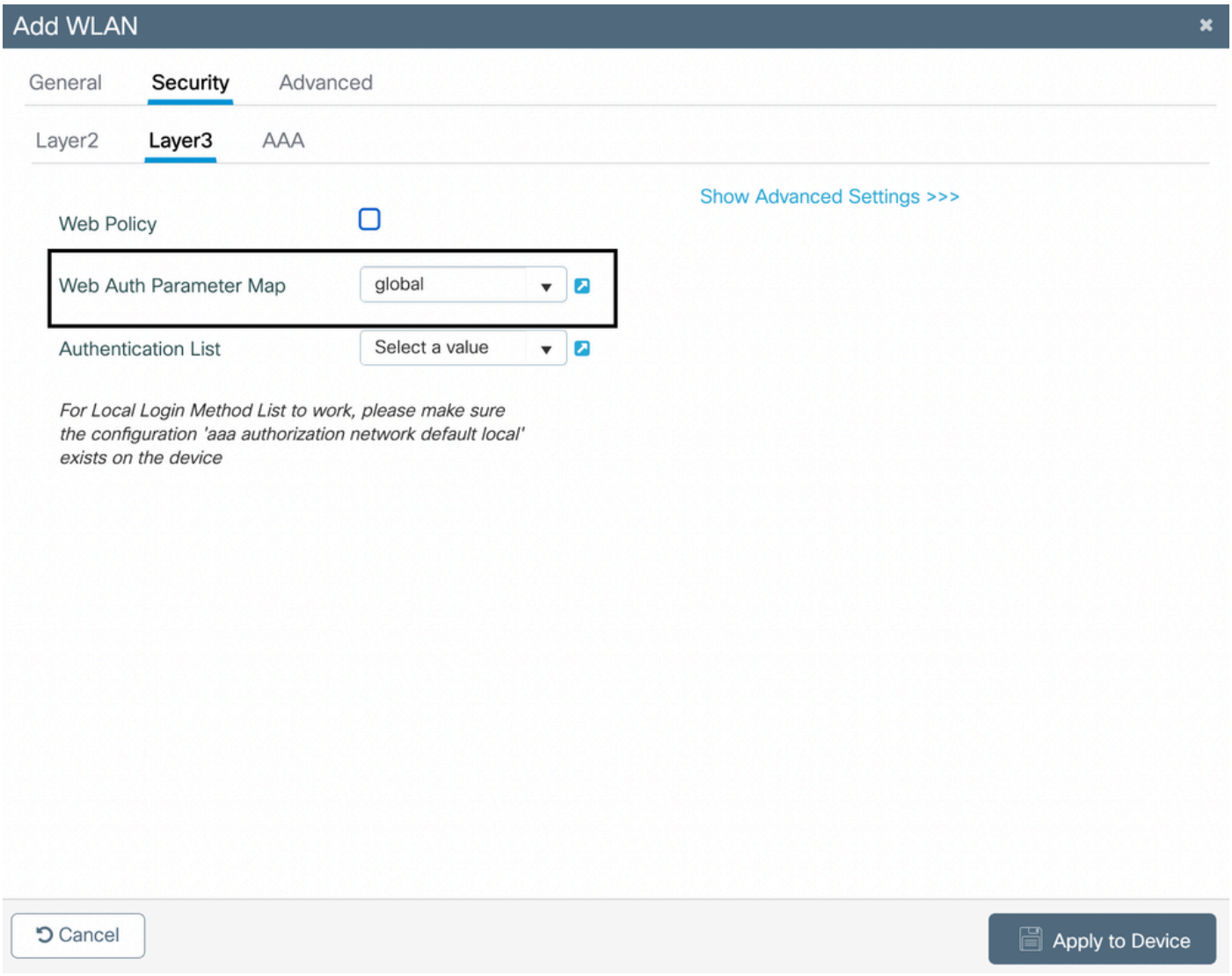
1. Navigate to **Configuration > Tags & Profiles > WLANs**. Click the **Add** button.
2. Provide a SSID name under the **General** tab and enable the **WLAN** button.



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



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:



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

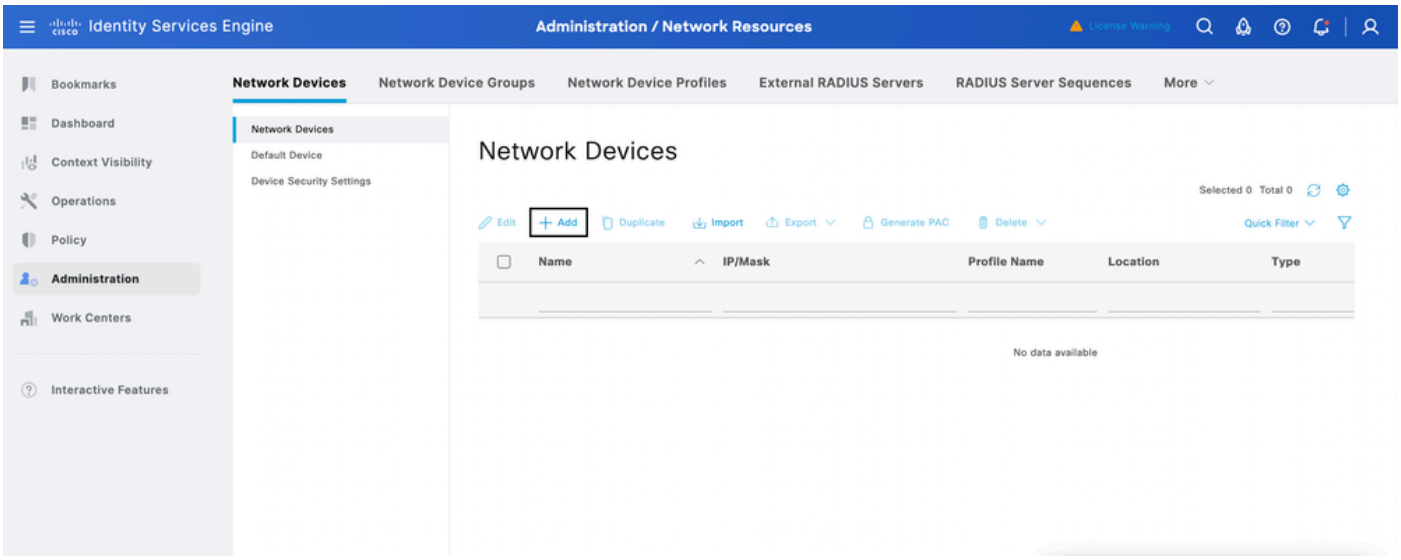
- Install a valid server certificate on ISE to avoid browser security warnings.
- Ensure the certificate is trusted by endpoints (signed by a well-known CA or an internal CA with trusted root).

DNS Configuration

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

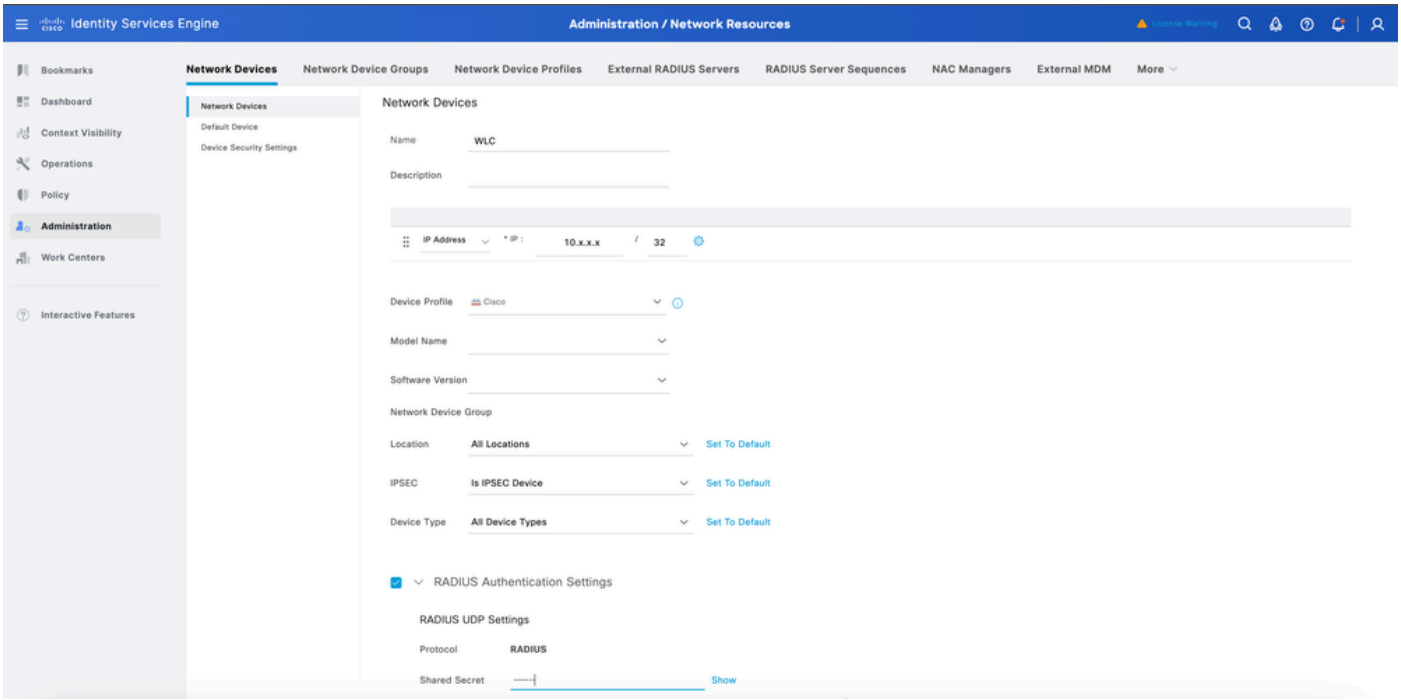
Configure ISE Network Device

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



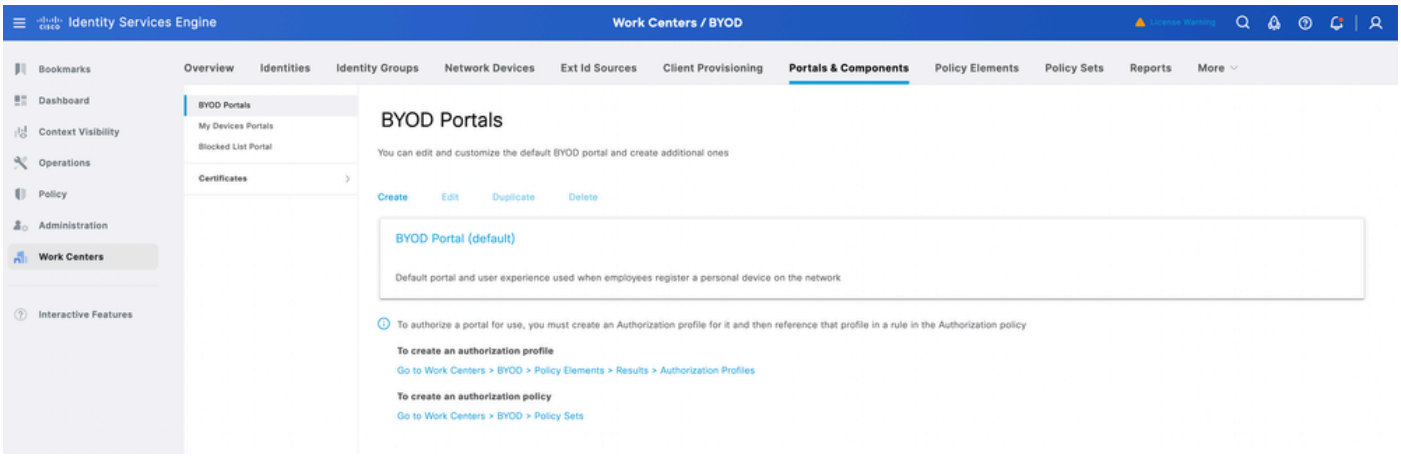
3.Add your WLC as a network device:

- **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**.



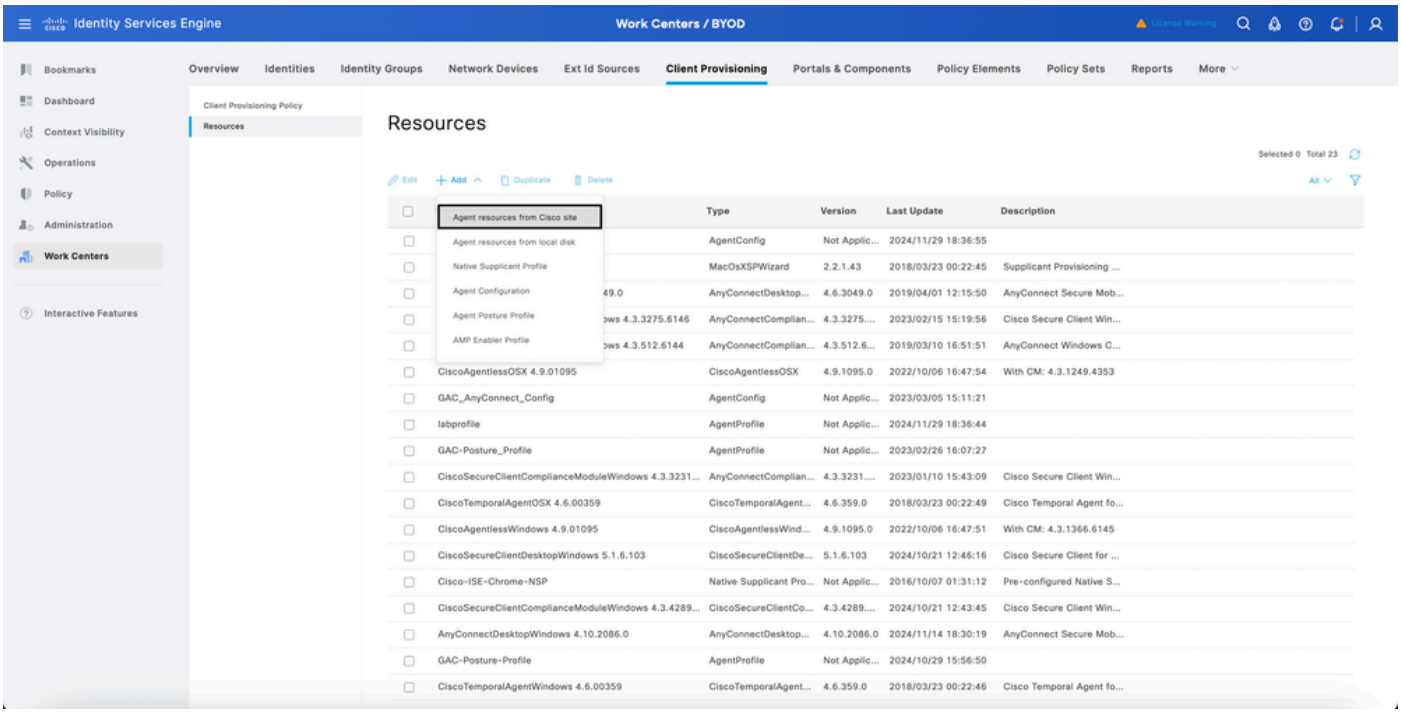
Create a BYOD Portal

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.

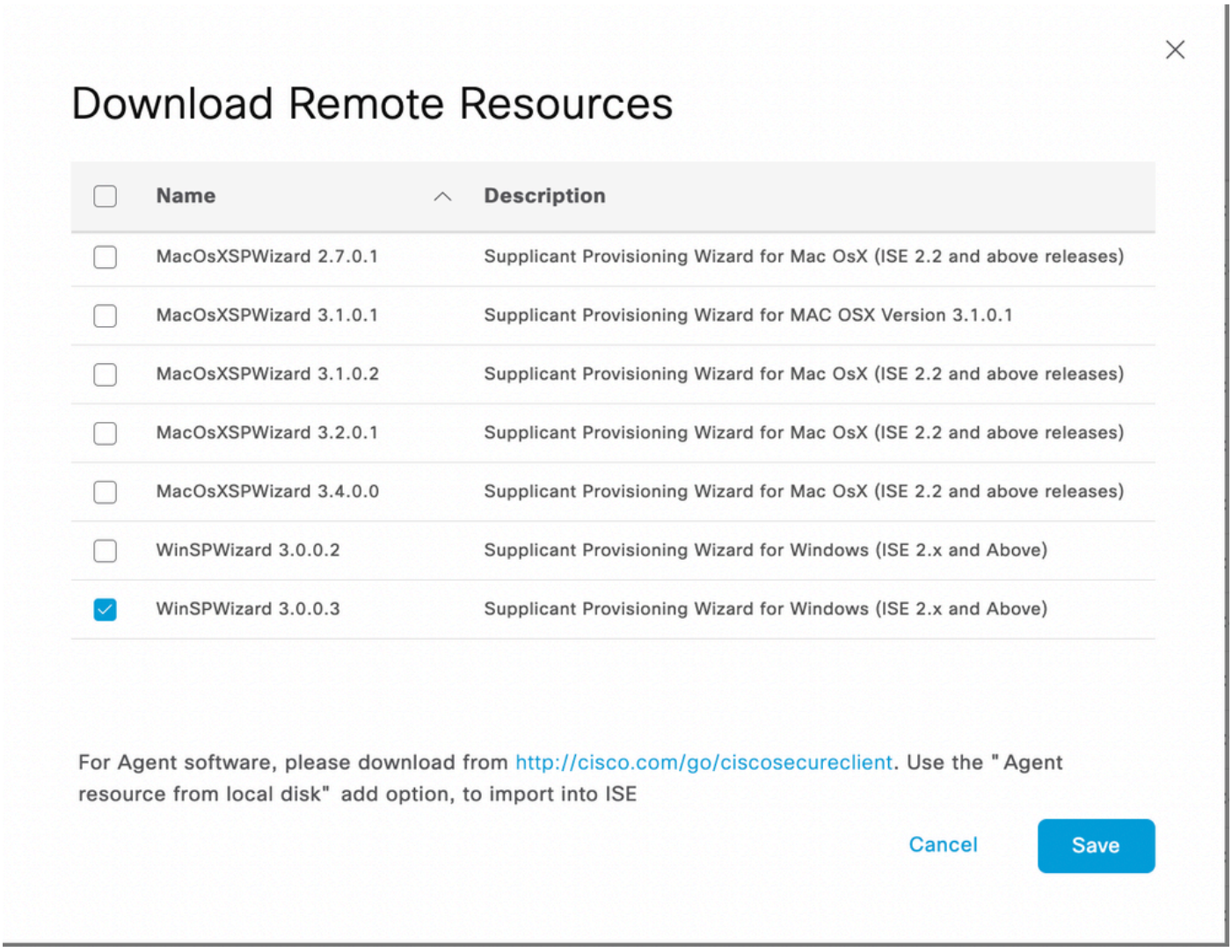


Download Cisco IOS® Latest Version

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



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

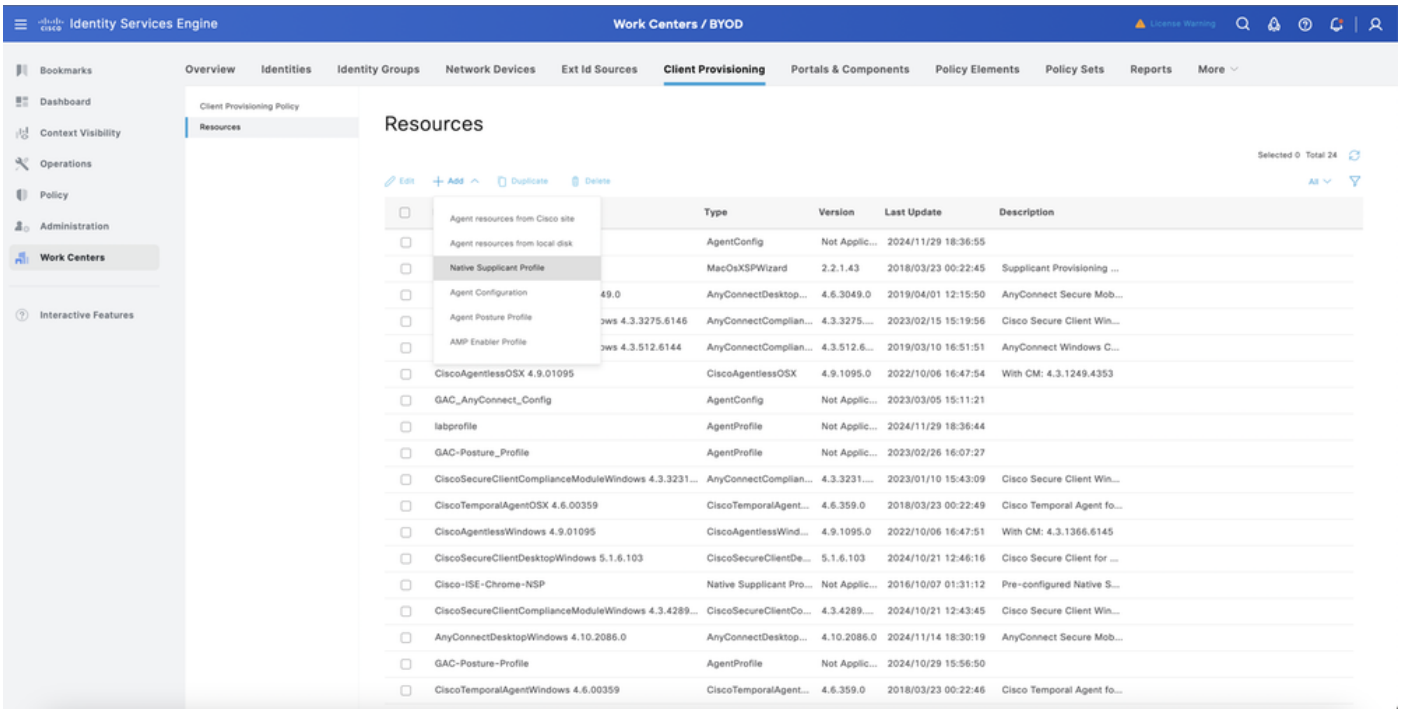


Note: Cisco IOS software is download on the ISE for Windows and MacOS endpoints. For Apple iPhone IOS, it uses a native supplicant to provision the device and For android device, you have Network setup assistant which needs to be downloaded from Play Store.

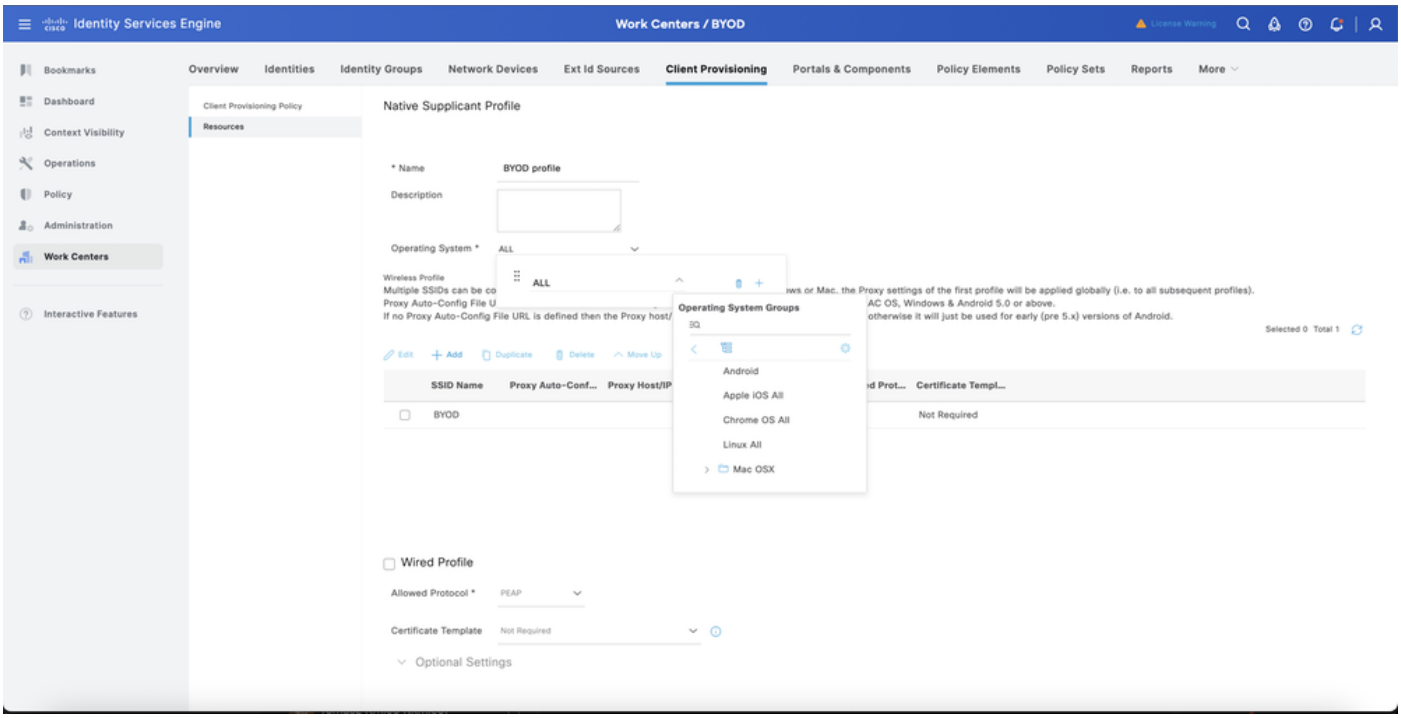
Create an Endpoint Profile

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

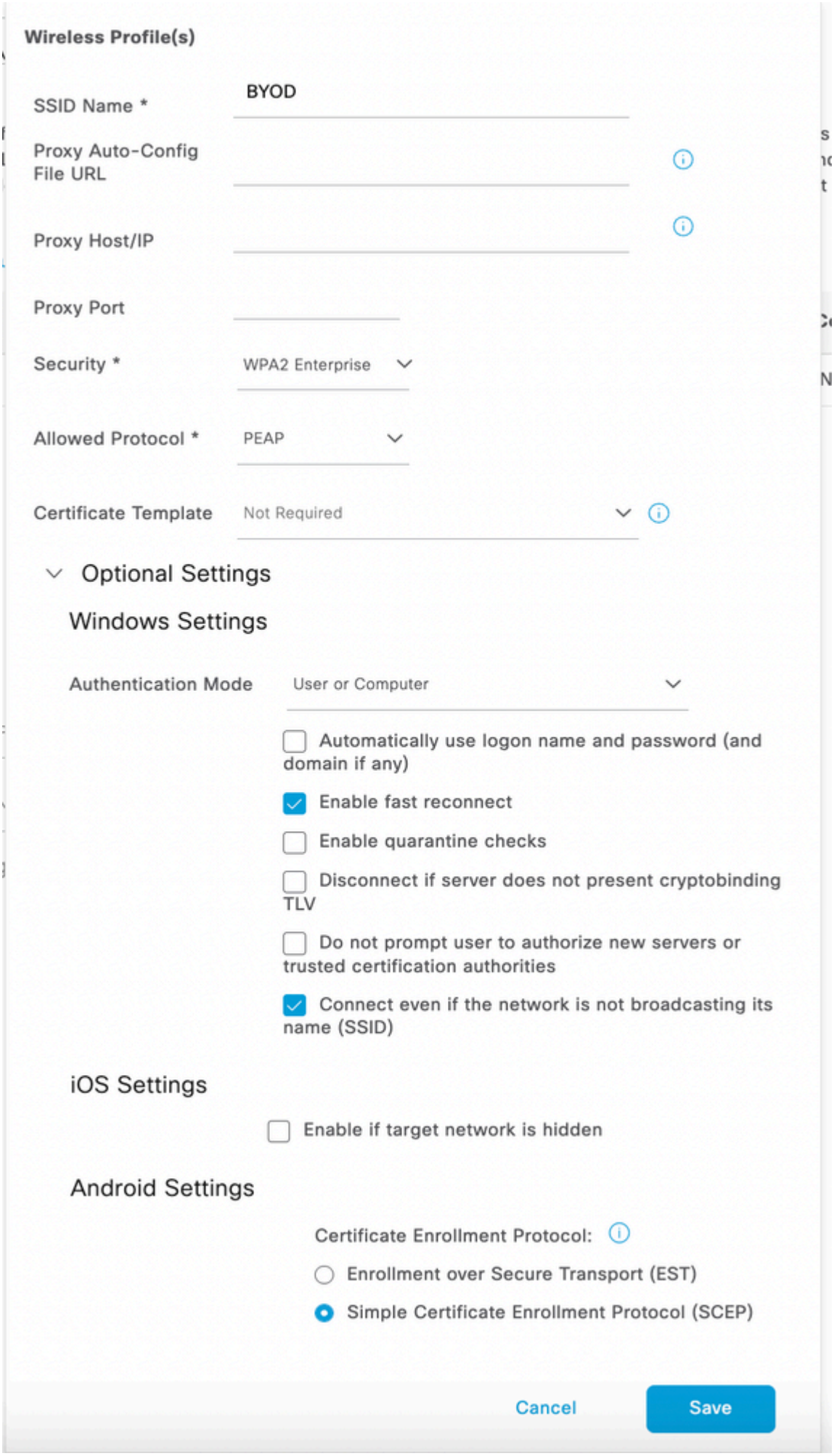
2. Click **Add**, select **Native supplicant profile** from the drop down menu.



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:



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

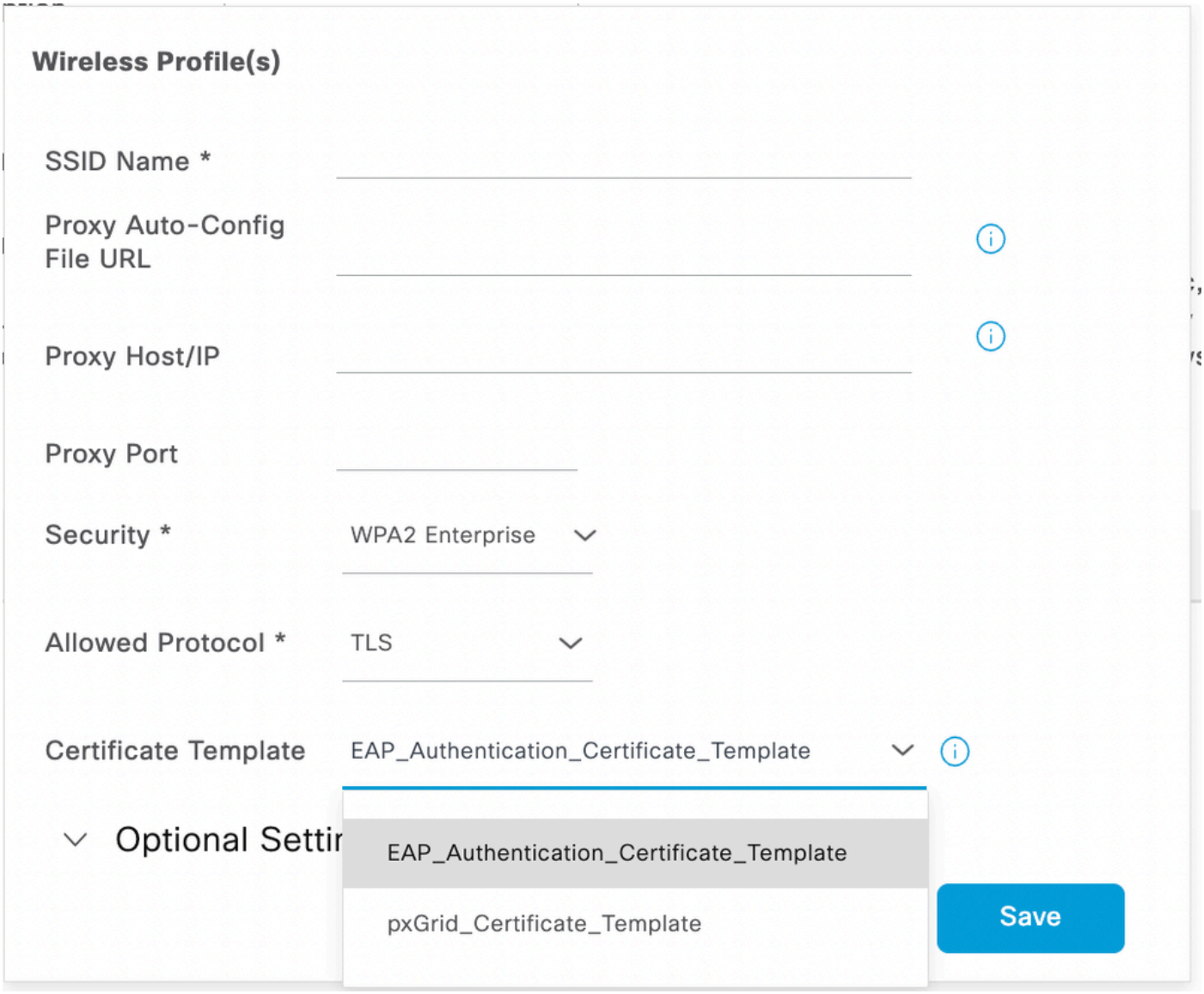

Wireless Profile(s)
SSID Name *
BYOD
Proxy Auto-Config File URL
Proxy Host/IP
Proxy Port
Security *
WPA2 Enterprise
Allowed Protocol *
PEAP
Certificate Template
Not Required
Optional Settings
Windows Settings
Authentication Mode
User or Computer
Automatically use logon name and password (and domain if 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:
Enrollment over Secure Transport (EST)
Simple Certificate Enrollment Protocol (SCEP)
Cancel
Save

Note: 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.

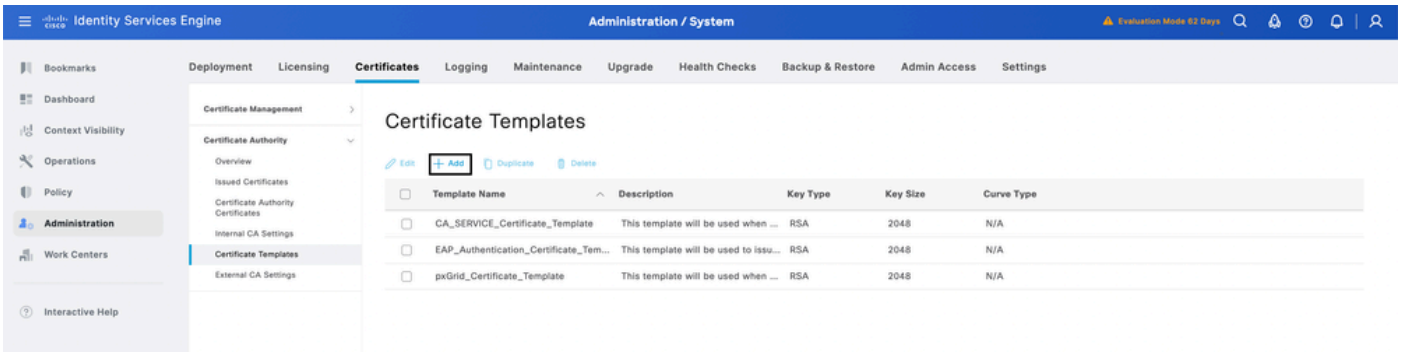
Certificate Template

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.

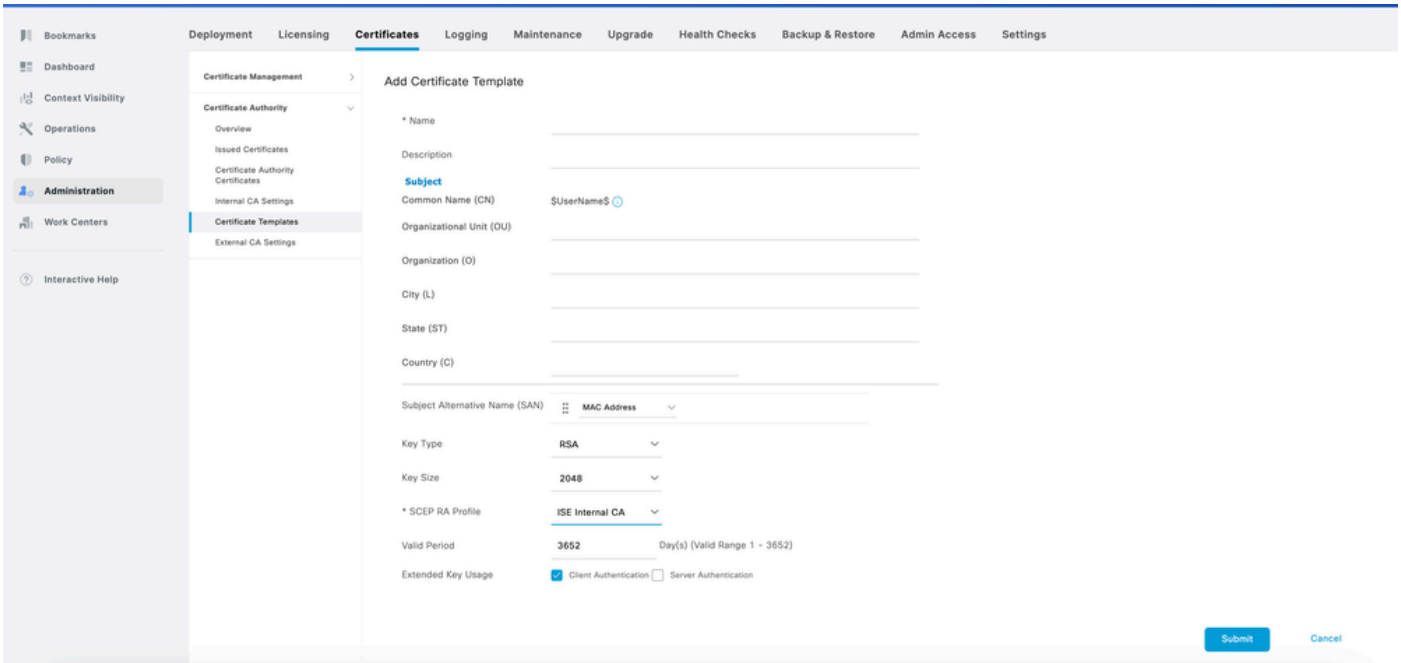


To create a new certificate template, follow these steps:

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



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

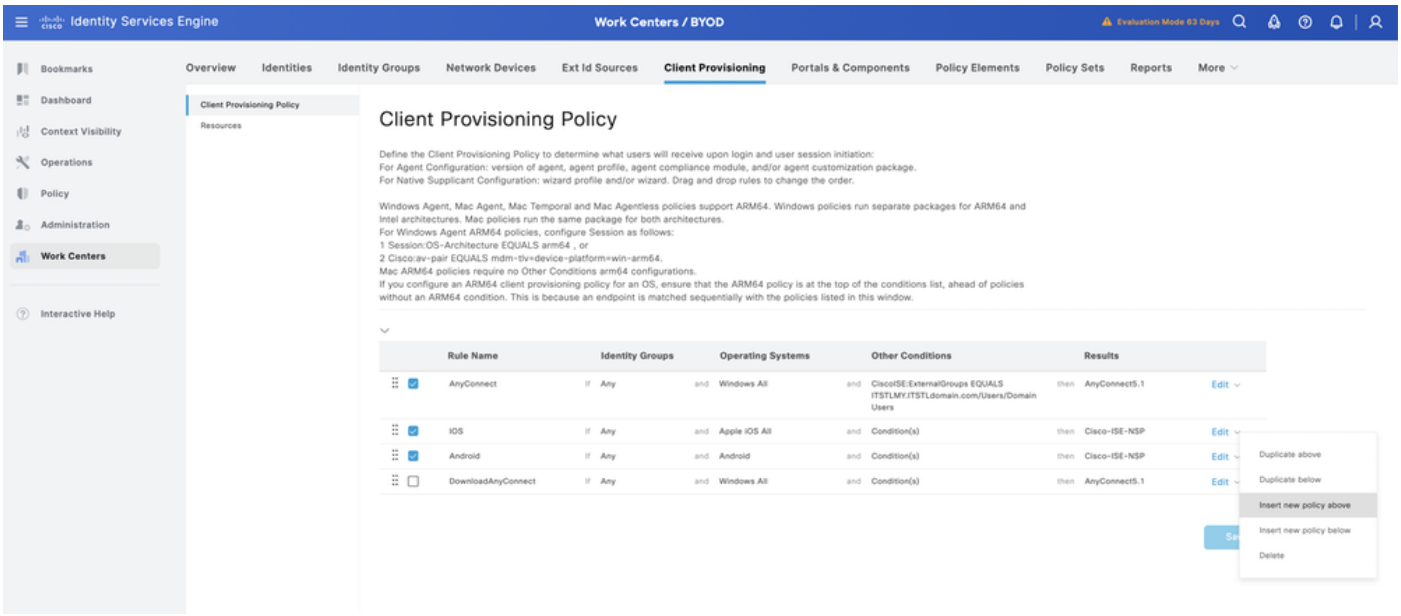


4. Click **Submit** to save the changes.

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.

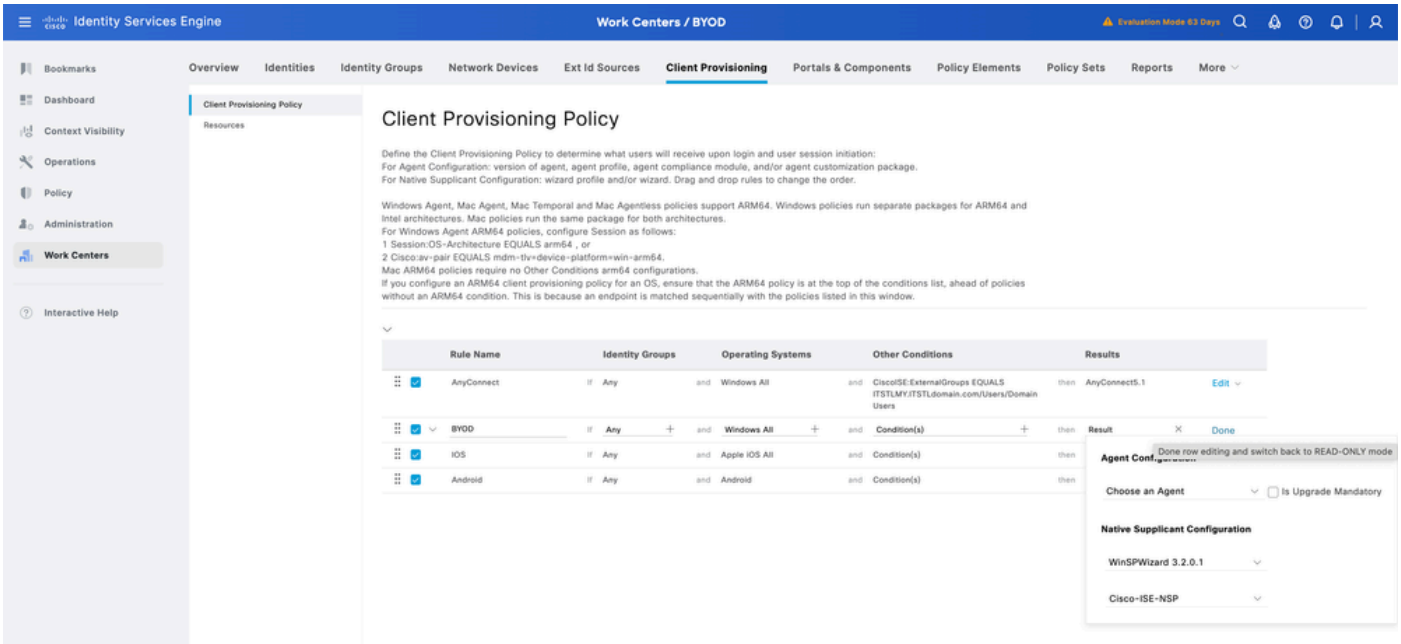


3. Post creating the new rule on the page

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.



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

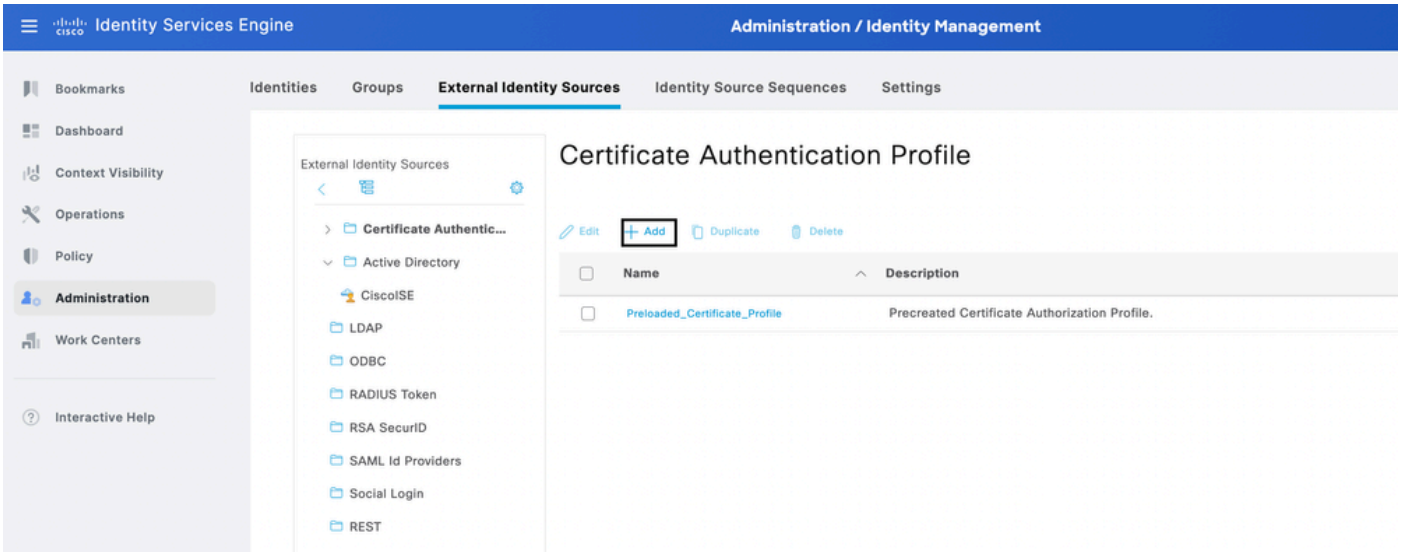
---

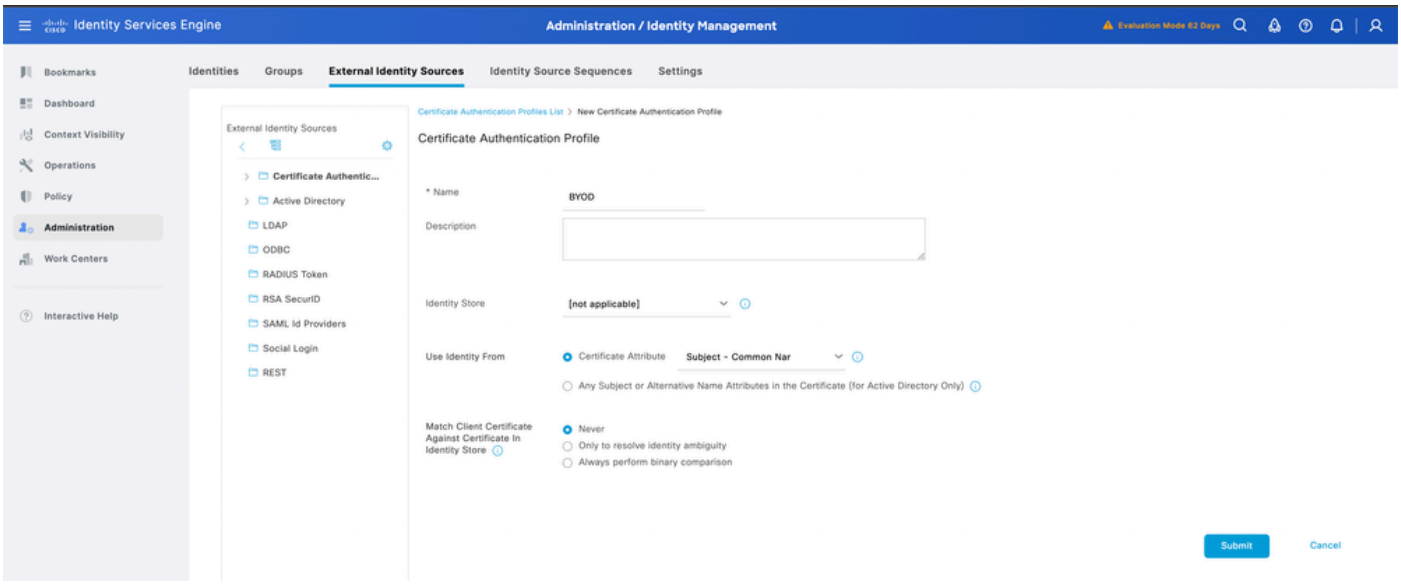
Configure ISE Policy Sets for Single SSID BYOD

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



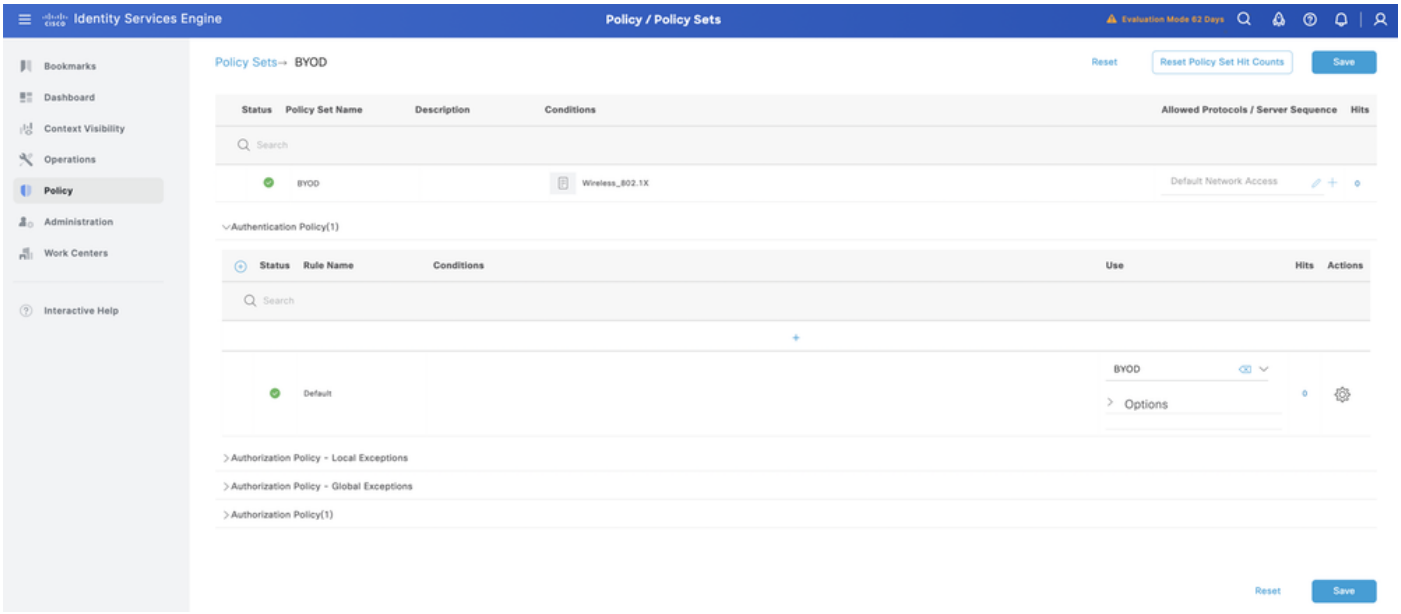
2. Then, navigate to **Administration > Identity Management > External Identity Sources > Certificate Authentication Profile**. Click the **Add** button to create the certificate profile:





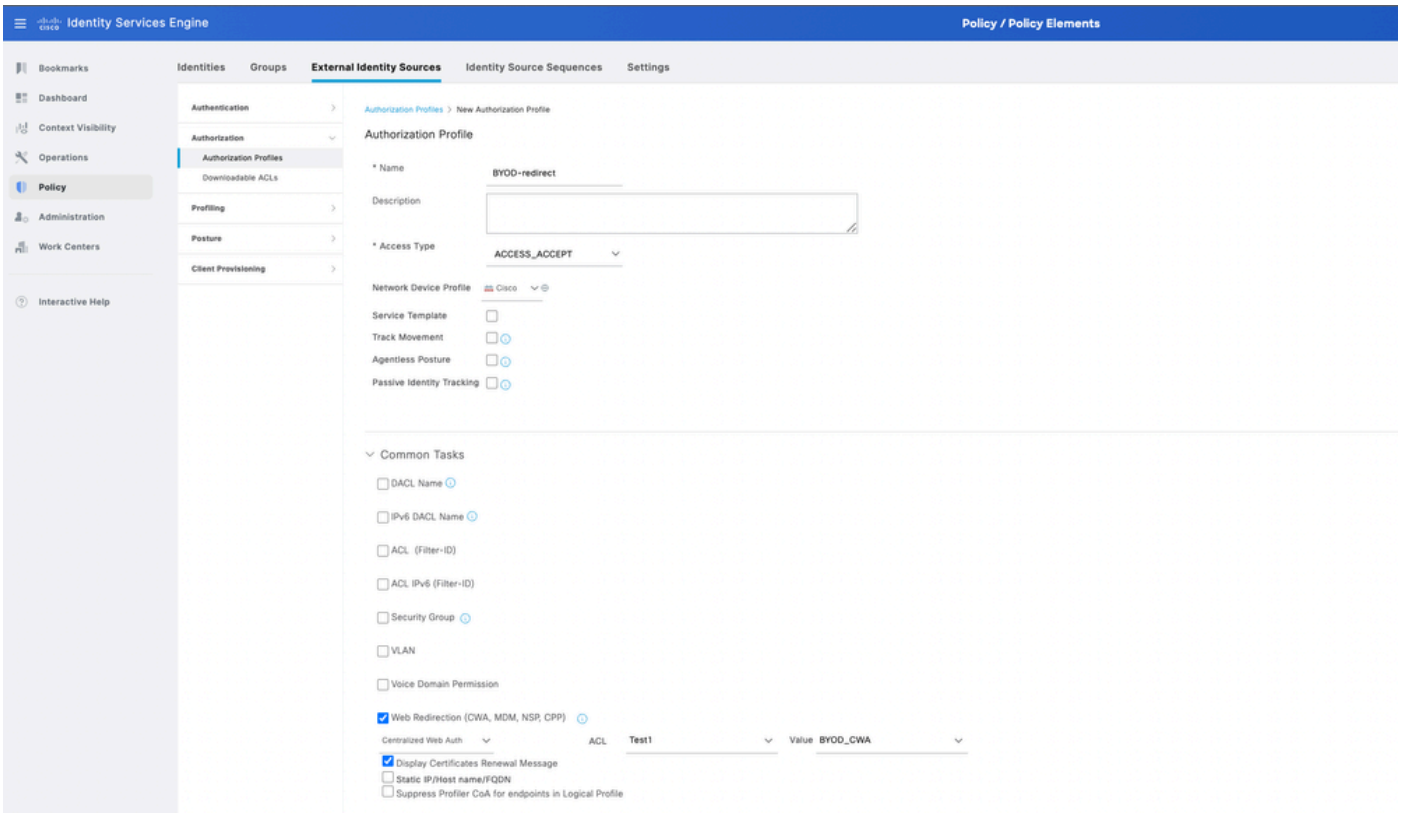
Note: In the Identity Store, you can always select your Active Directory which has been integrated to ISE to perform a user lookup from the certificate for addition security.

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

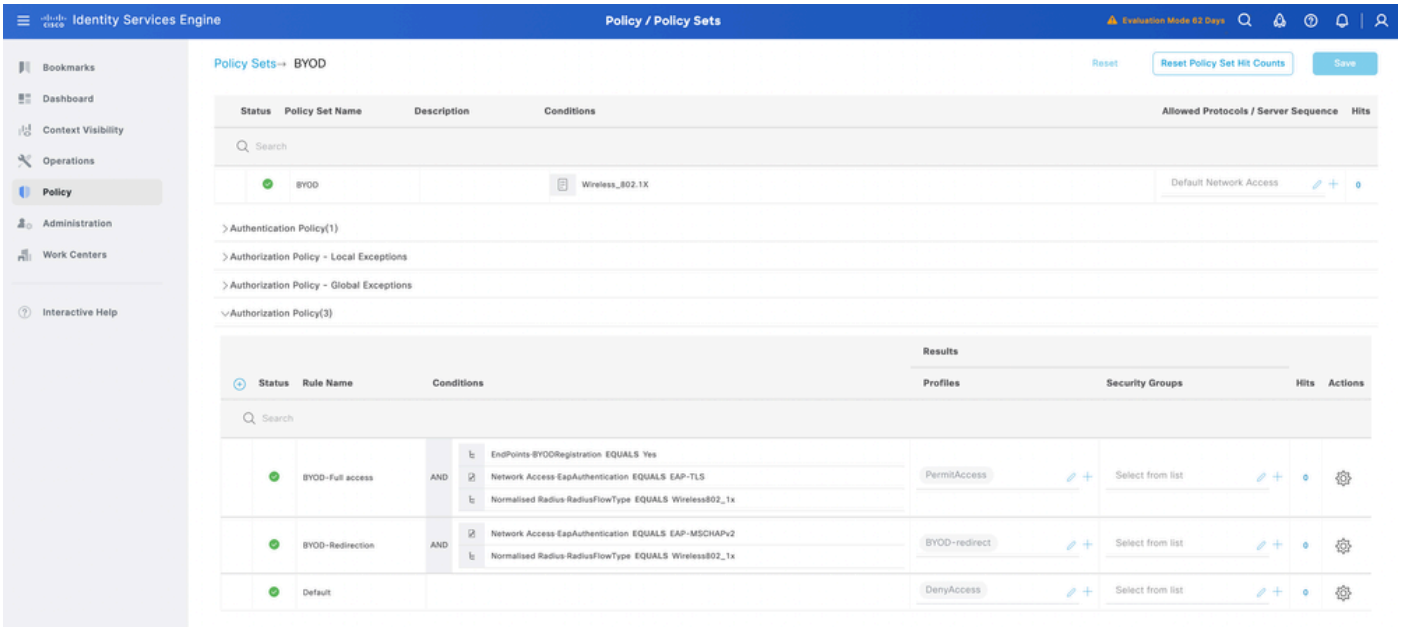


4. Configure the Authorization profile for BYOD redirect and full access post the BYOD flow. Navigate to **Policy > Policy Elements > Results > Authorization > Authorization Profiles**.

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.



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.



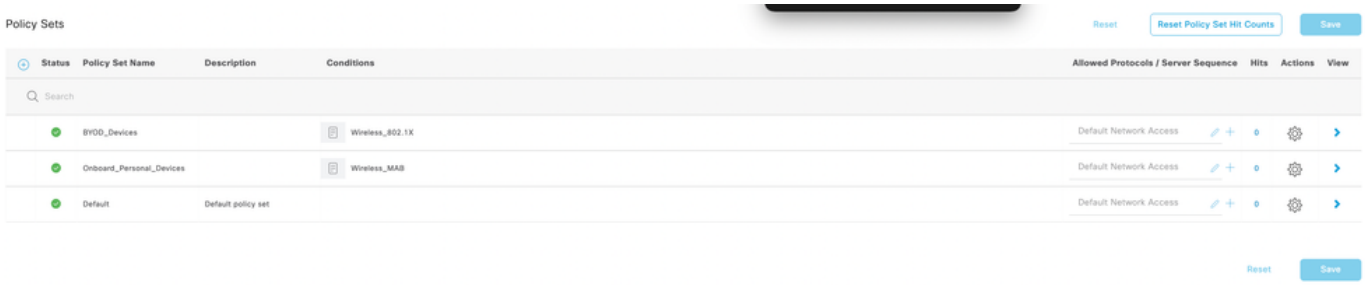
Configure ISE Policy Sets for Dual SSID BYOD

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 Portal** page upon

connecting to the open/ unsecured SSID:

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

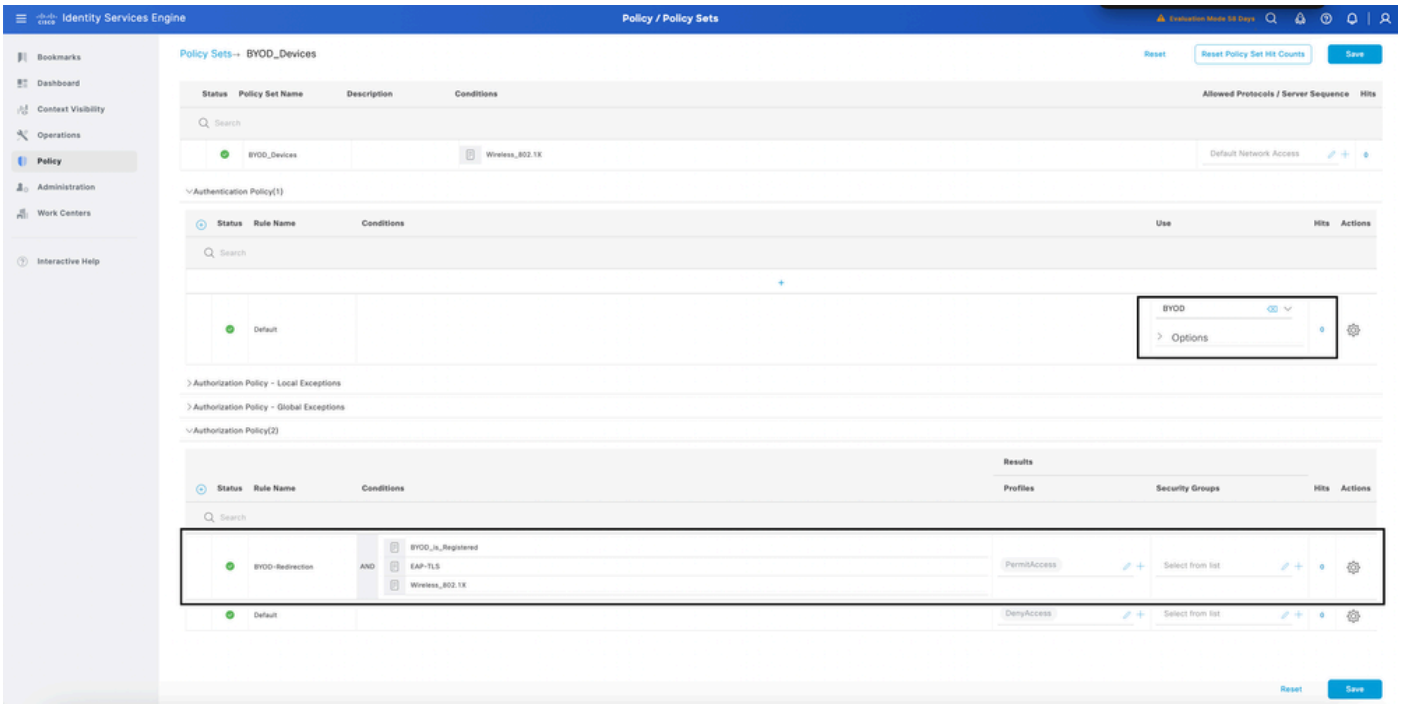
2. Create a policy set for the Open/Unsecured SSID and Corporate SSID which authenticates the registered BYOD user on ISE.



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.

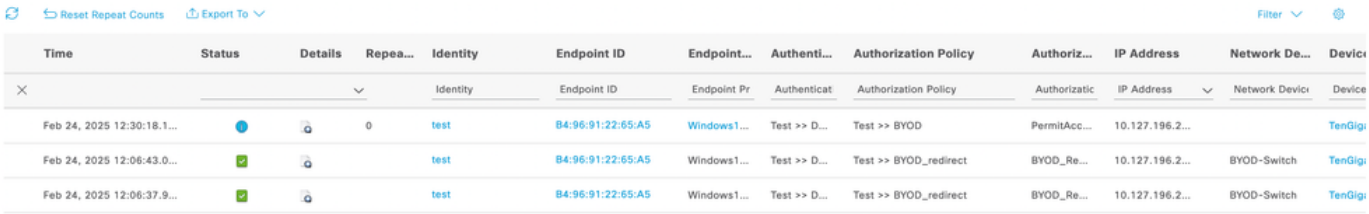


4. In the **BYOD Registered Policy Set**, configure the authentication policy with the certificate profile same as found in *Configure ISE Policy Sets for Single SSID BYOD* in point 2. Also create a condition for authorization policy and map the full access profile to the policy.

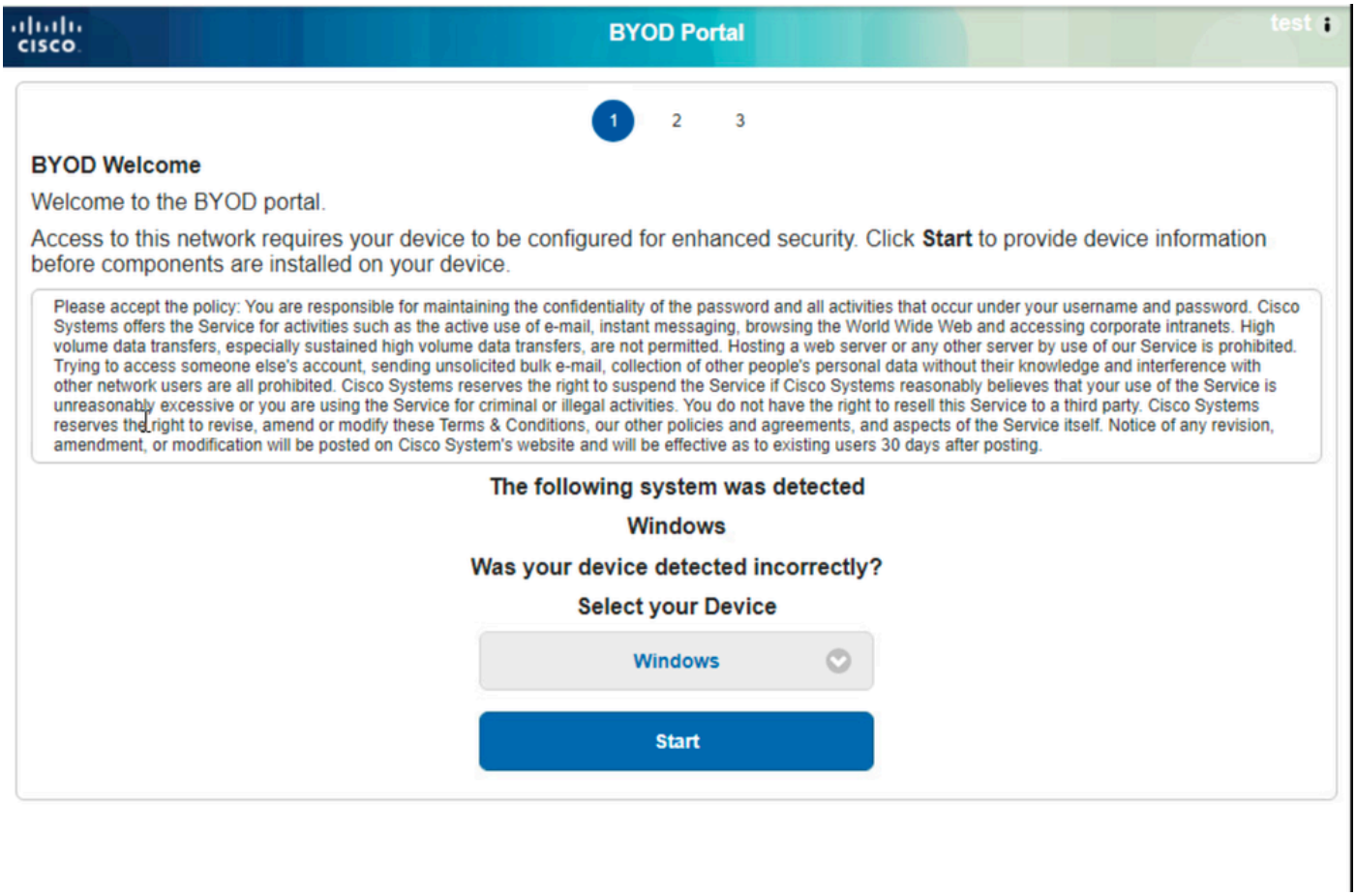


Logging

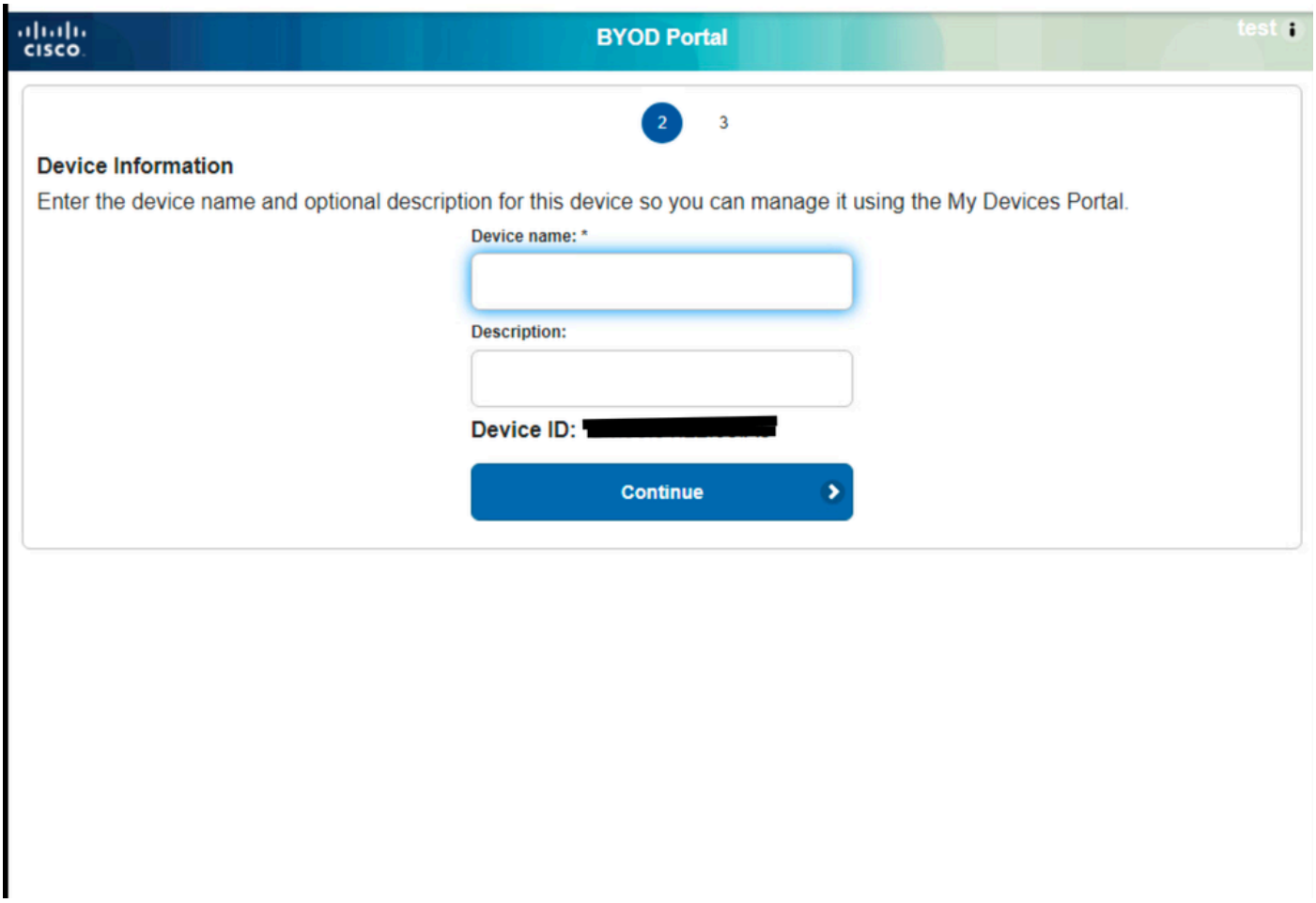
From the live log from ISE, the user authentication is successful and redirects to the **BYOD Portal** page. After completing the BYOD flow, the user would be grant access to the network:



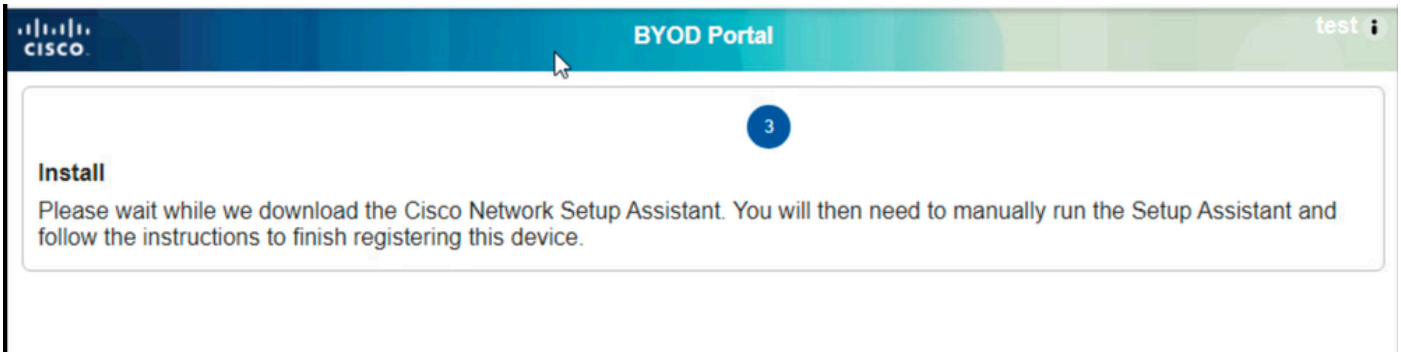
From the user perspective, they would first be redirected to the **BYOD Portal** page and the appropriate device needs to selected from the web page. For testing, a Windows 10 device was used:



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:

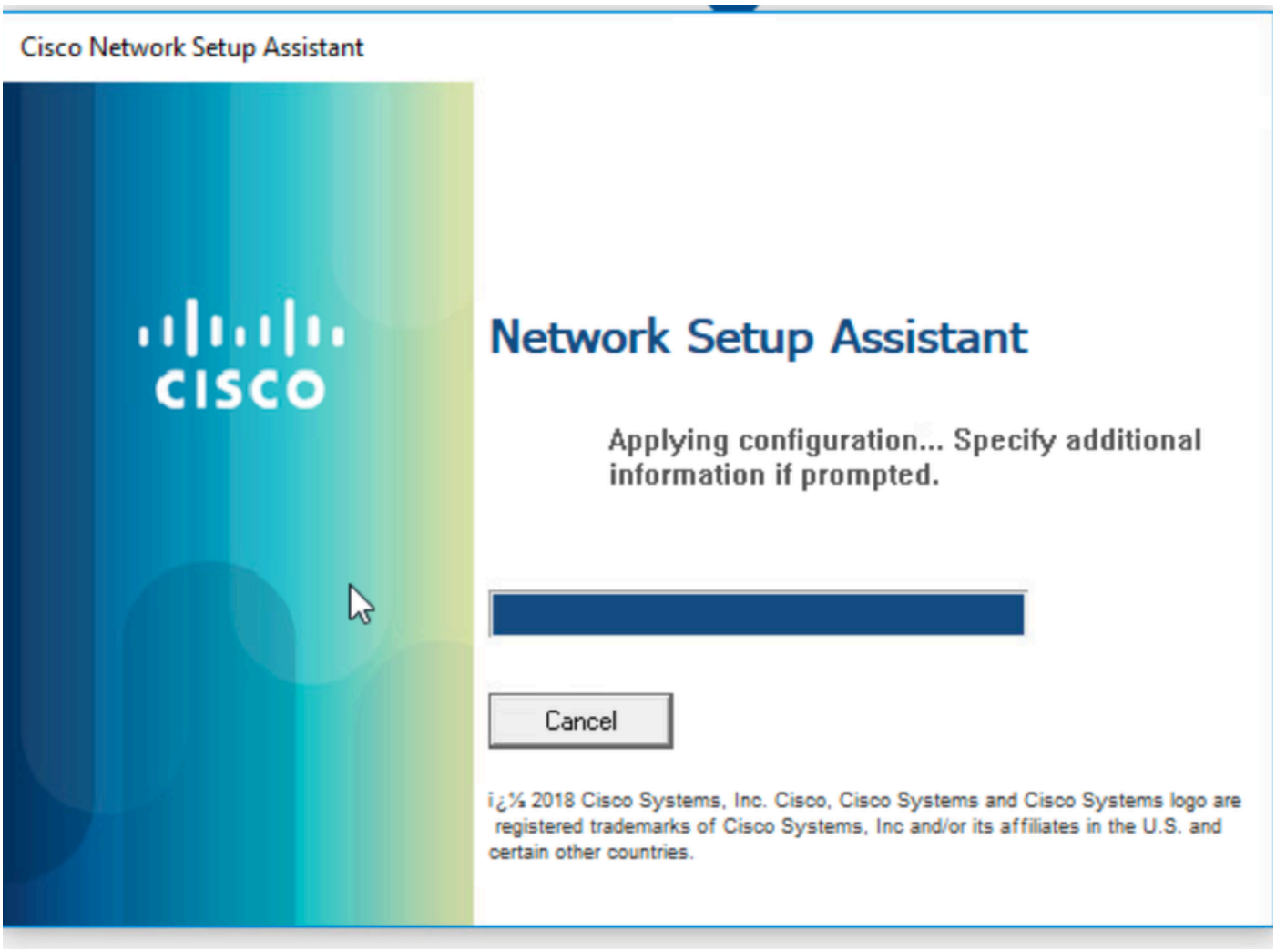


Post that the user would be requested to download the Network Assistant tool for downloading the Endpoint profile and EAP TLS certificate for authentication if the profile is configured to perform EAP-TLS authentication:



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.
Start
Quit
i¿¼ 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.

Troubleshoot

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=322815127387689606282525327846633020 89]'
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=729347676986030971539324822275488749 53]'
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: