Configuración de ISE BYOD con SSID único y dual en ISE 3.3

Contenido

Introducción

El documento describe cómo configurar y solucionar problemas de BYOD en ISE.

Background

BYOD es una función que permite al usuario incorporar sus dispositivos personales en ISE para que el usuario pueda utilizar los recursos de red del entorno. También ayuda al administrador de red a restringir el acceso del usuario al recurso crítico desde los dispositivos personales.

A diferencia del flujo de invitados, en el que el dispositivo se autentica con la página Invitado mediante el almacén interno o Active Directory en ISE. BYOD permite al administrador de red instalar un perfil de terminal en el terminal para elegir el tipo de método EAP. En escenarios como EAP-TLS, el certificado de cliente está firmado por el propio ISE para crear una relación de confianza entre el terminal e ISE.

Prerequisites

Cisco recomienda que tenga conocimiento sobre estos temas:

- controlador WLC
- Conocimientos básicos sobre ISE

Componente utilizado

Estos dispositivos no se limitan a una versión concreta para el flujo de BYOD:

- Controlador inalámbrico Catalyst 9800-CL (17.12.3)
- Máquina virtual ISE (3.3)

¿Qué es BYOD con SSID único y SSID dual en ISE?

BYOD con SSID único

En una configuración BYOD con un solo SSID, los usuarios conectan sus dispositivos personales directamente a la red inalámbrica corporativa. El proceso de incorporación se produce en el mismo SSID, donde ISE facilita el registro de dispositivos, el aprovisionamiento y la aplicación de políticas. Este enfoque simplifica la experiencia del usuario, pero requiere una incorporación segura y métodos de autenticación adecuados para garantizar la seguridad de la red.

BYOD SSID dual

En una configuración BYOD con SSID dual, se utilizan dos SSID independientes: una para la incorporación (acceso no seguro o restringido) y otra para el acceso a la red corporativa. Los usuarios se conectan inicialmente al SSID incorporado, finalizan el registro y el aprovisionamiento de dispositivos mediante ISE y, a continuación, cambian al SSID corporativo seguro para acceder

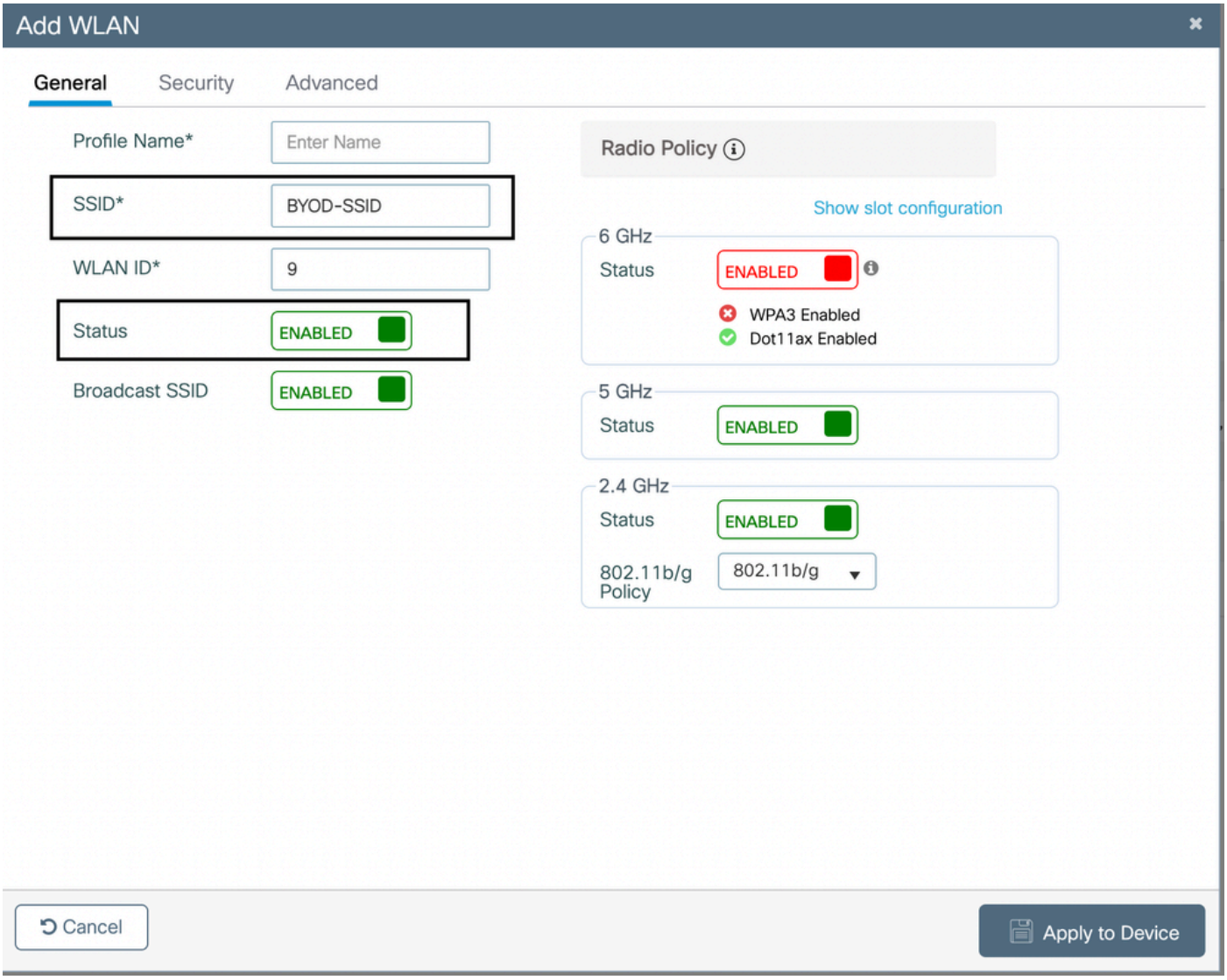
a la red. Esto proporciona una capa adicional de seguridad al segregar el tráfico de incorporación del tráfico de producción.

Configuración de WLC

Creación de una WLAN para CWA

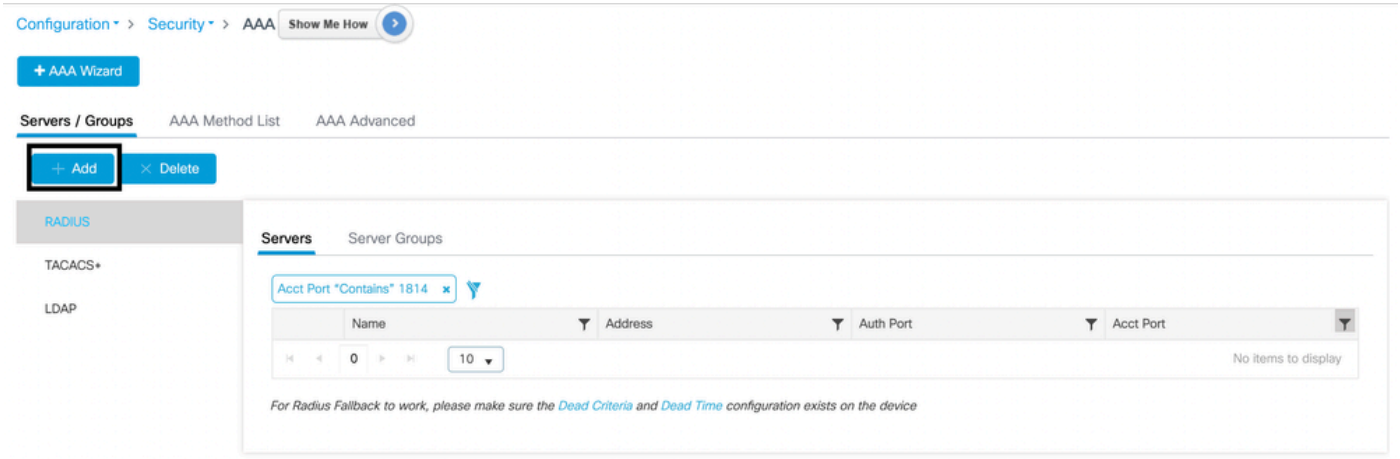
1. Vaya a Configuration > Tags & Profiles > WLANs.
2. Haga clic en Add para crear una nueva WLAN.

    - Establezca un nombre de WLAN y un SSID (por ejemplo, BYOD-WiFi).
    - Active la WLAN.

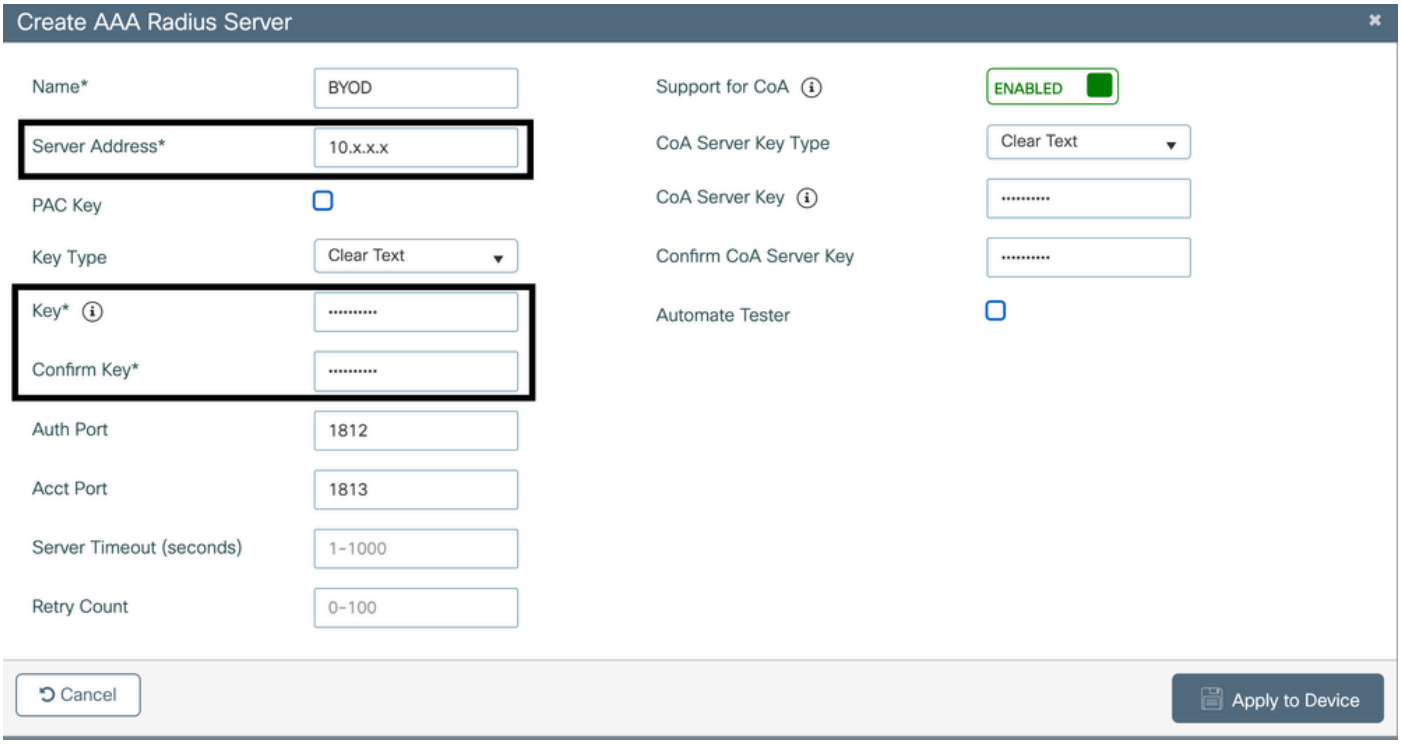


Configure los servidores RADIUS

1. Vaya a Configuration > Security > AAA > RADIUS > Servers.

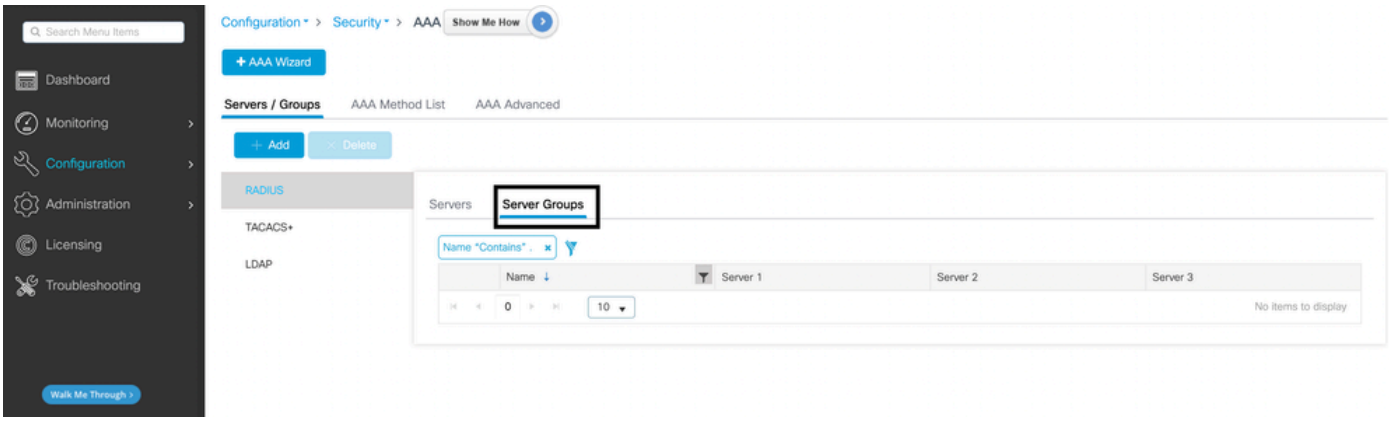


2. Haga clic en Agregar para configurar ISE como servidor RADIUS:
    - IP del servidor: Dirección IP de ISE.
    - secreto compartido: Coincida con el secreto compartido configurado en ISE.

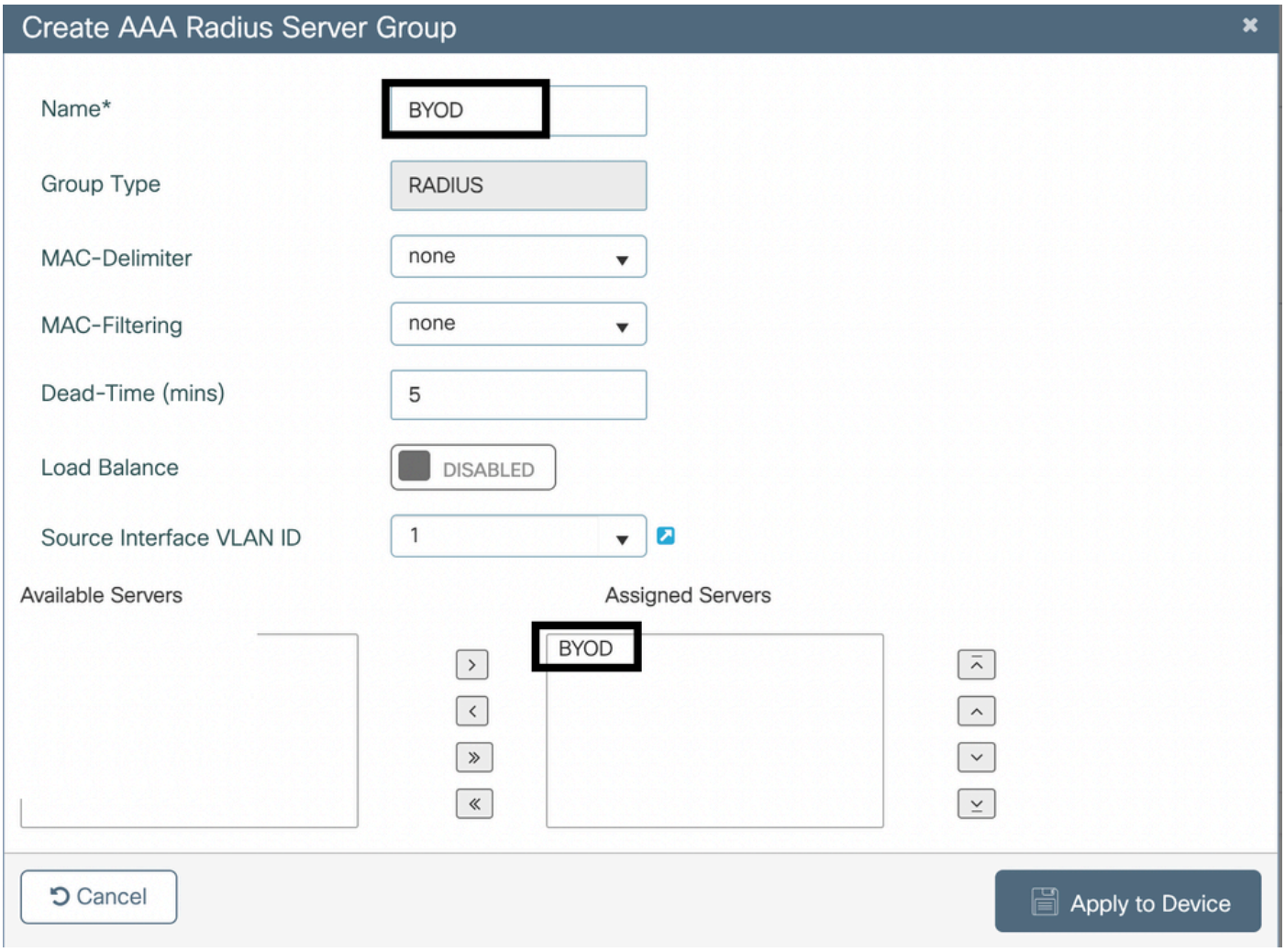


Configuración de servidores AAA

1. Vaya a Configuration > Security > AAA > Servers/Groups.



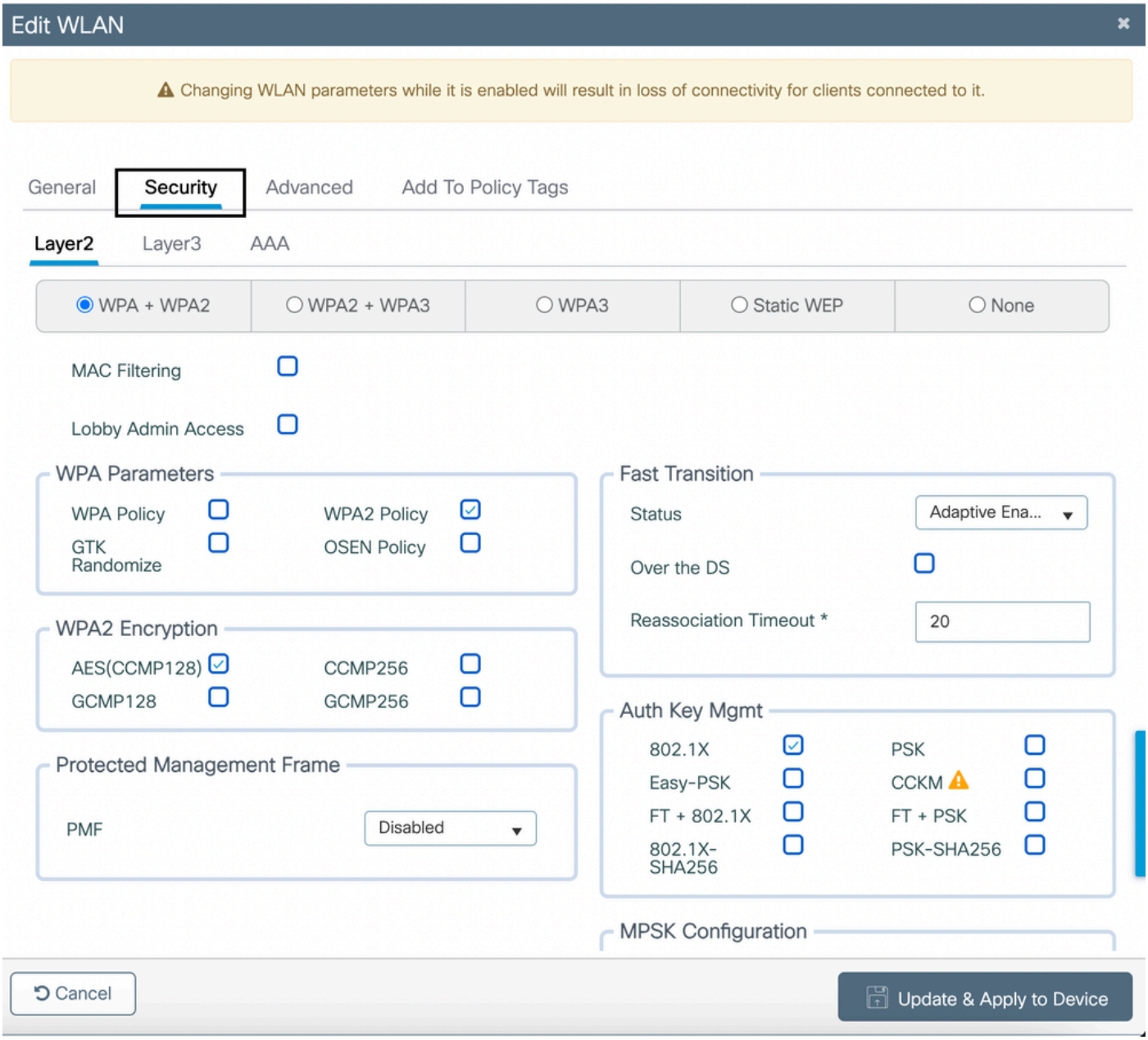
2. Asigne el servidor RADIUS a un grupo de servidores nuevo o existente.



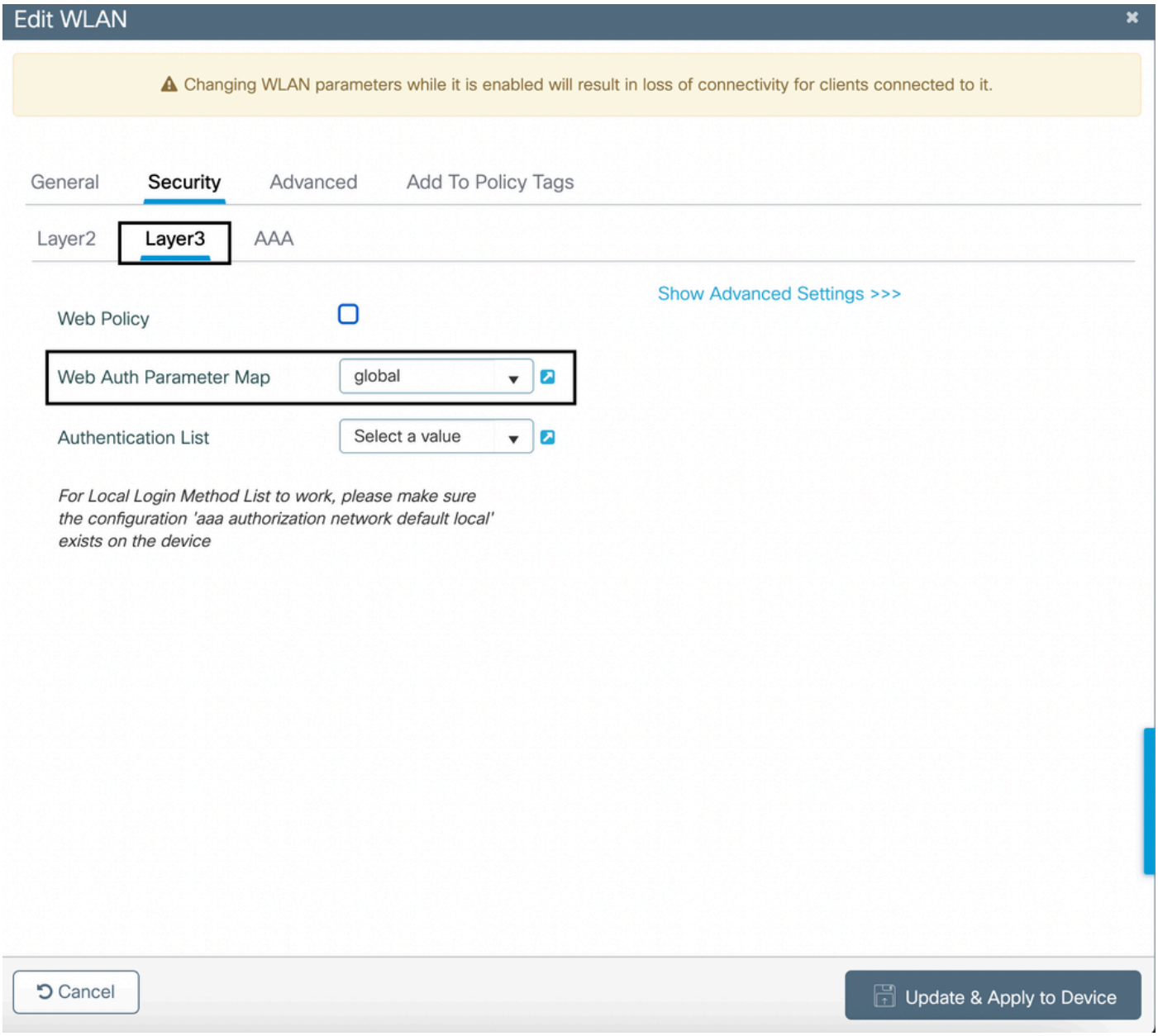
Configuración de las políticas de seguridad para la WLAN

1. Vaya a Configuration > Tags & Profiles > WLANs. Edite la WLAN creada anteriormente.

2. En la pestaña Security > Layer 2:
   - Activar WPA+WPA2
   - Establecer AES (CCMP128) con encriptación WPA2
   - Gestión de claves de autenticación como 802.1X



3. En la pestaña Security > Layer 3, seleccione global en el menú desplegable para Web Auth Parameter Map.



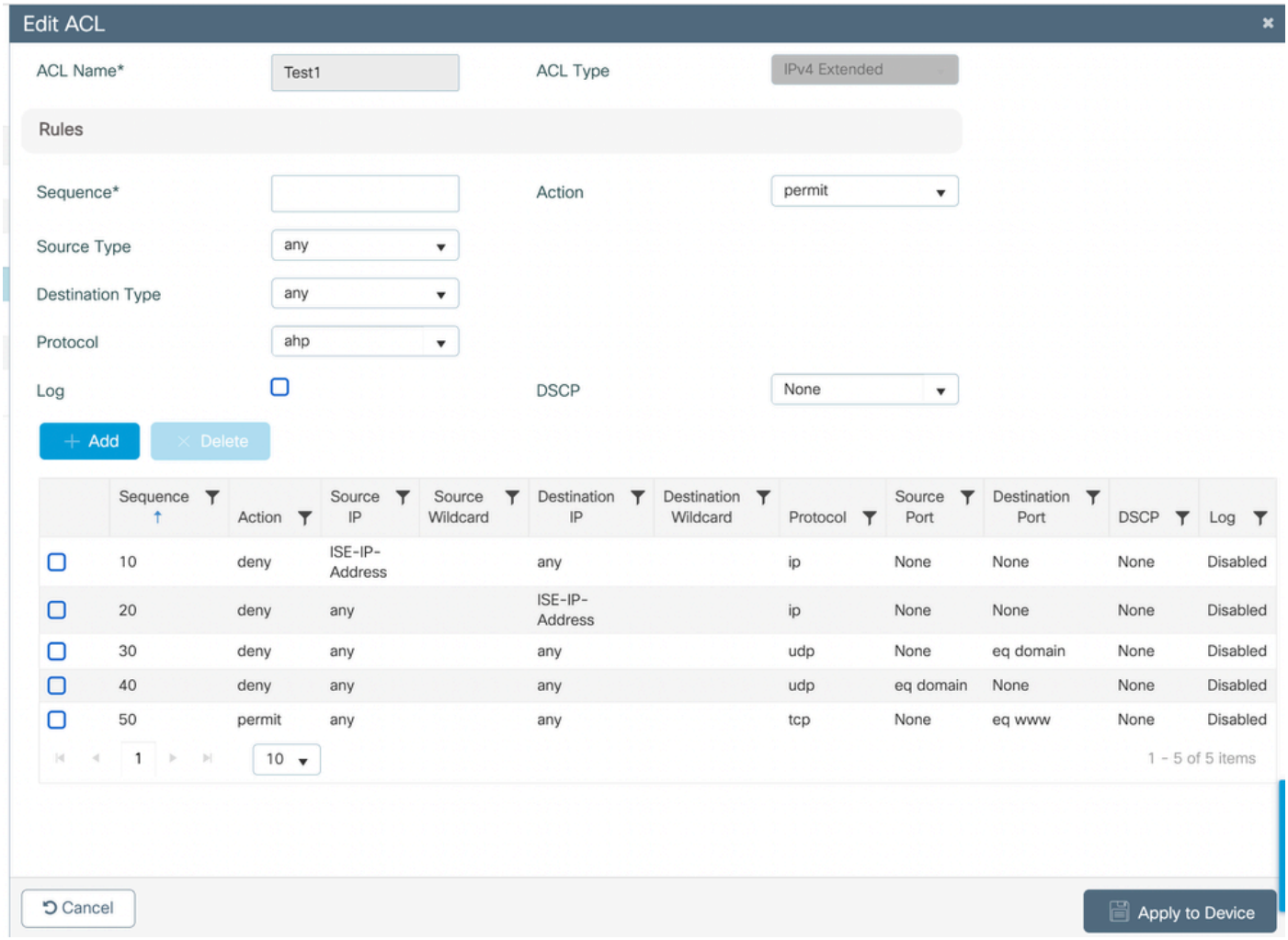
Configurar ACL de autenticación previa

Cree una lista de control de acceso para permitirUtilice acciones para la redirección:

- Tráfico DNS.
- HTTP/HTTPS al portal de ISE.
- Cualquier servicio backend necesario.

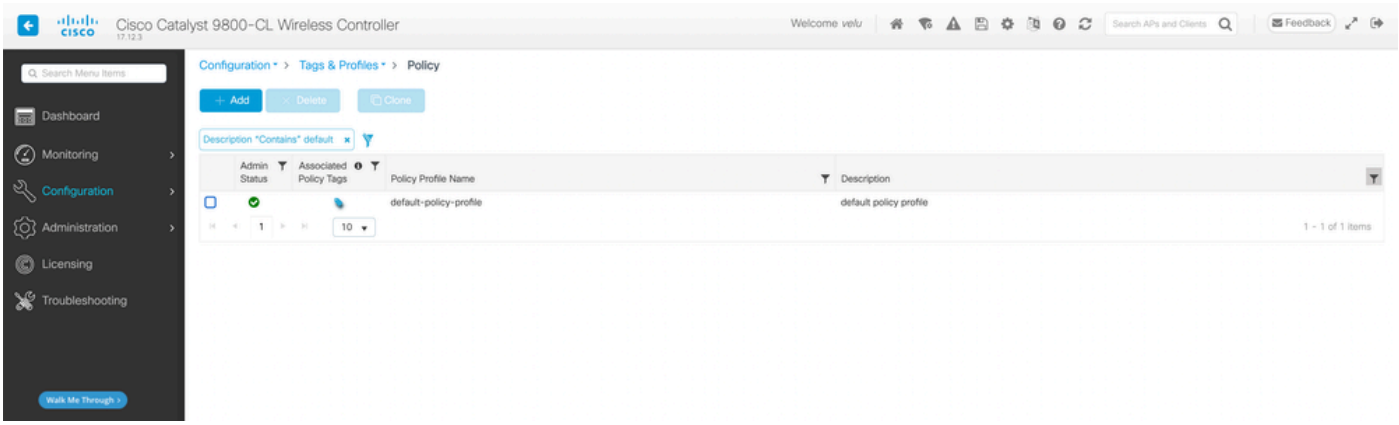
Para ello:

1. Vaya a Configuration > Security > ACL > Access Control Lists.
2. Cree una nueva ACL con reglas para permitir el tráfico necesario.

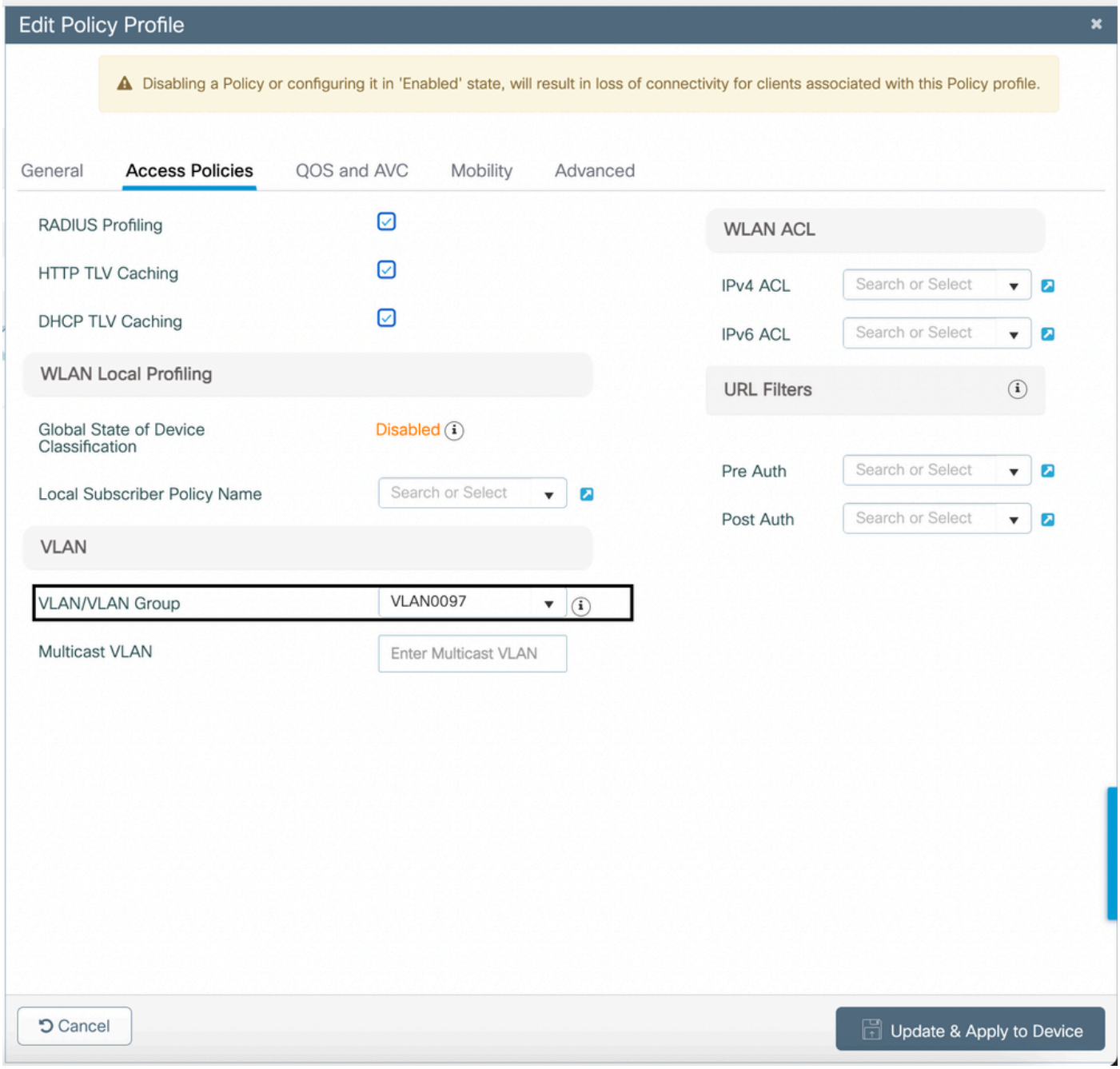


Configurar perfil de directiva

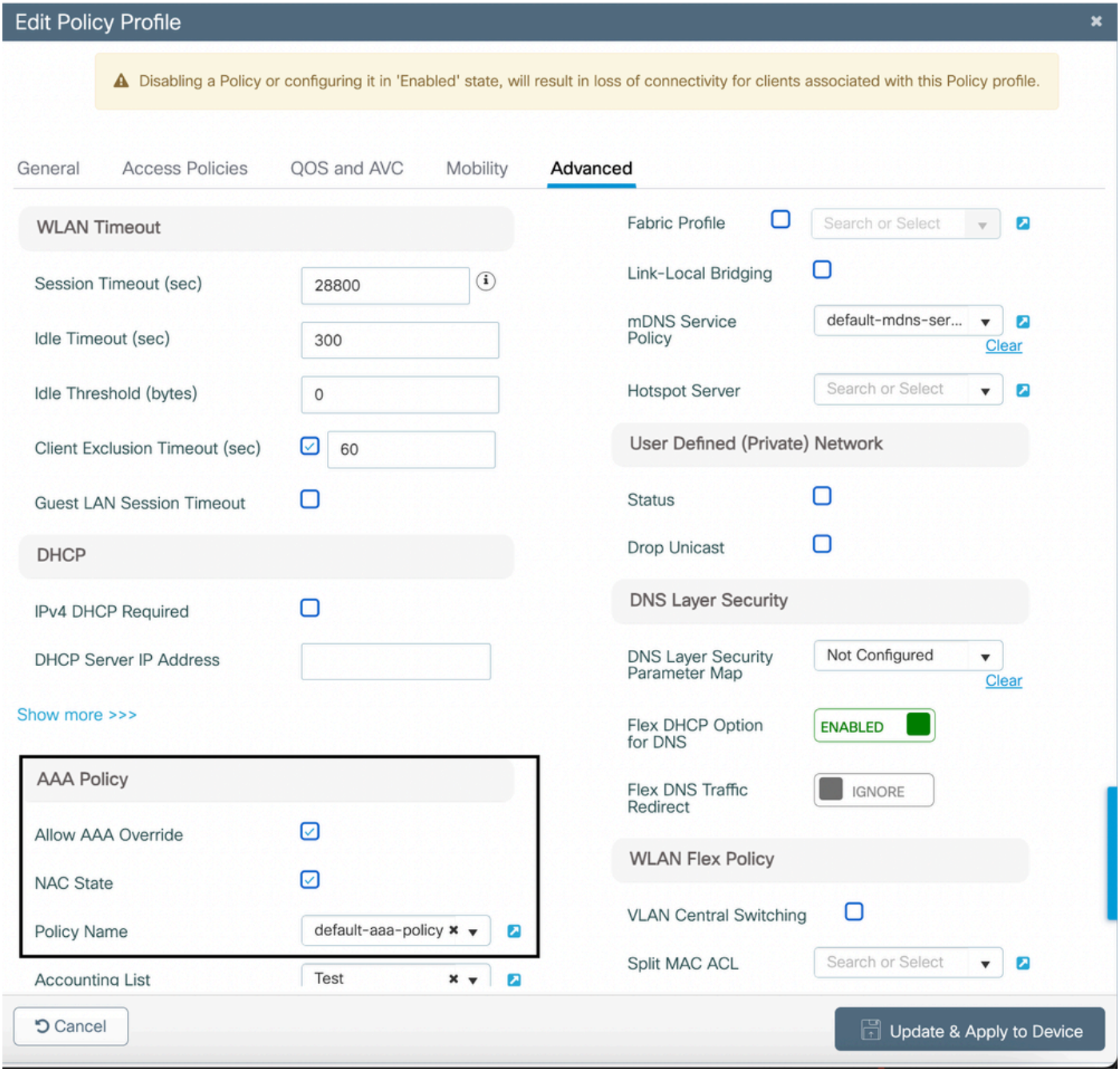
1. Vaya a Configuration > Tags & Profiles > Policy. Puede crear o utilizar la directiva predeterminada



2. Asigne la VLAN adecuada en Políticas de acceso

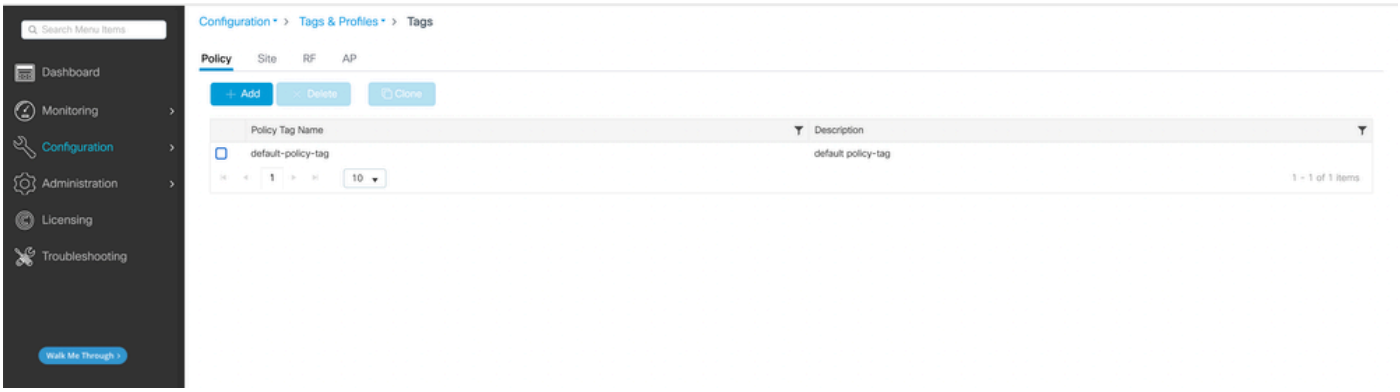


3. Habilite también Allow AAA Override y NAC state bajo Advanced de la política.



Aplicación de etiquetas e implementación

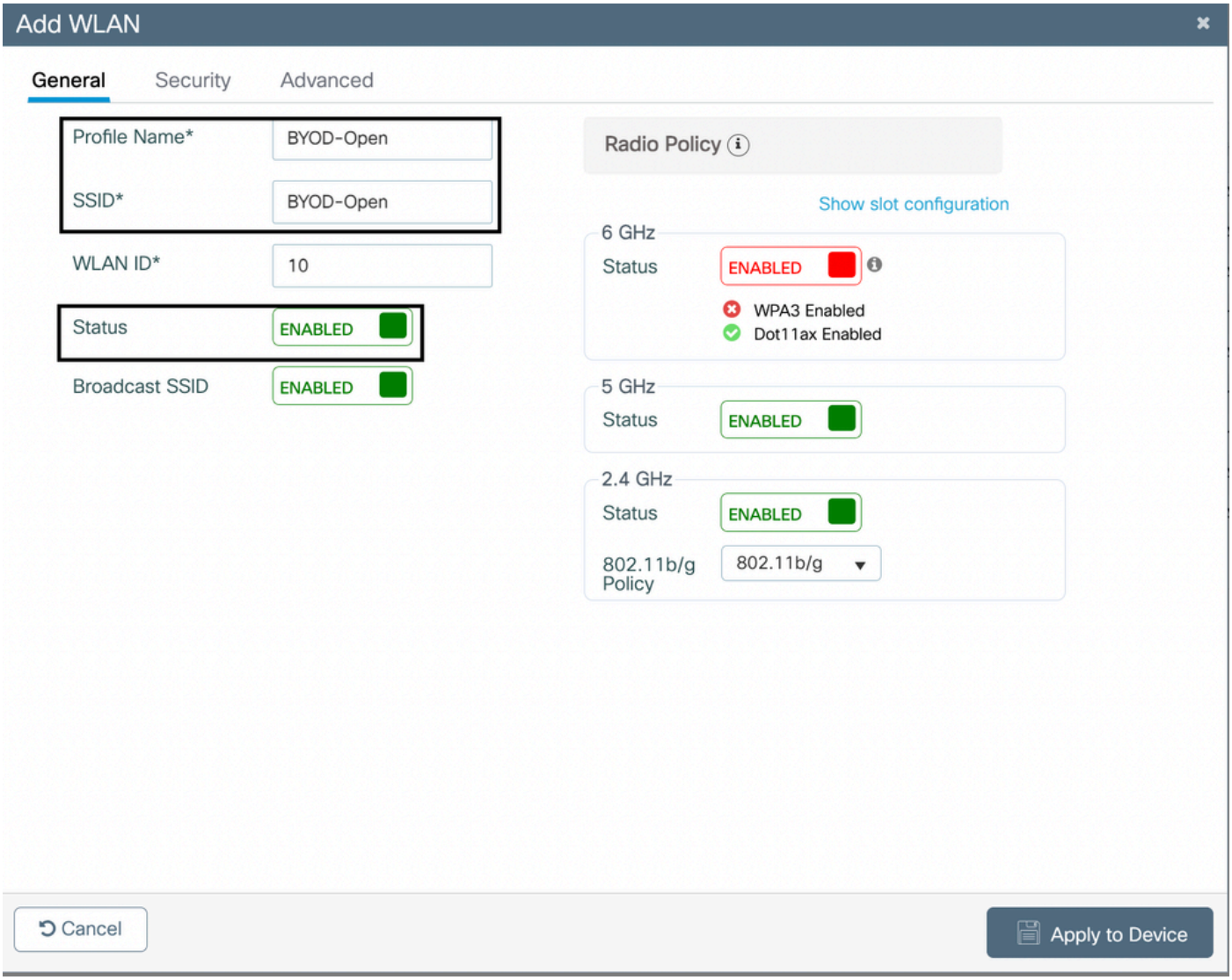
- Vaya a Configuración > Etiquetas y perfiles > Etiquetas.
- Cree o edite una etiqueta para incluir el perfil de política y WLAN.
- Asigne la etiqueta a los puntos de acceso.



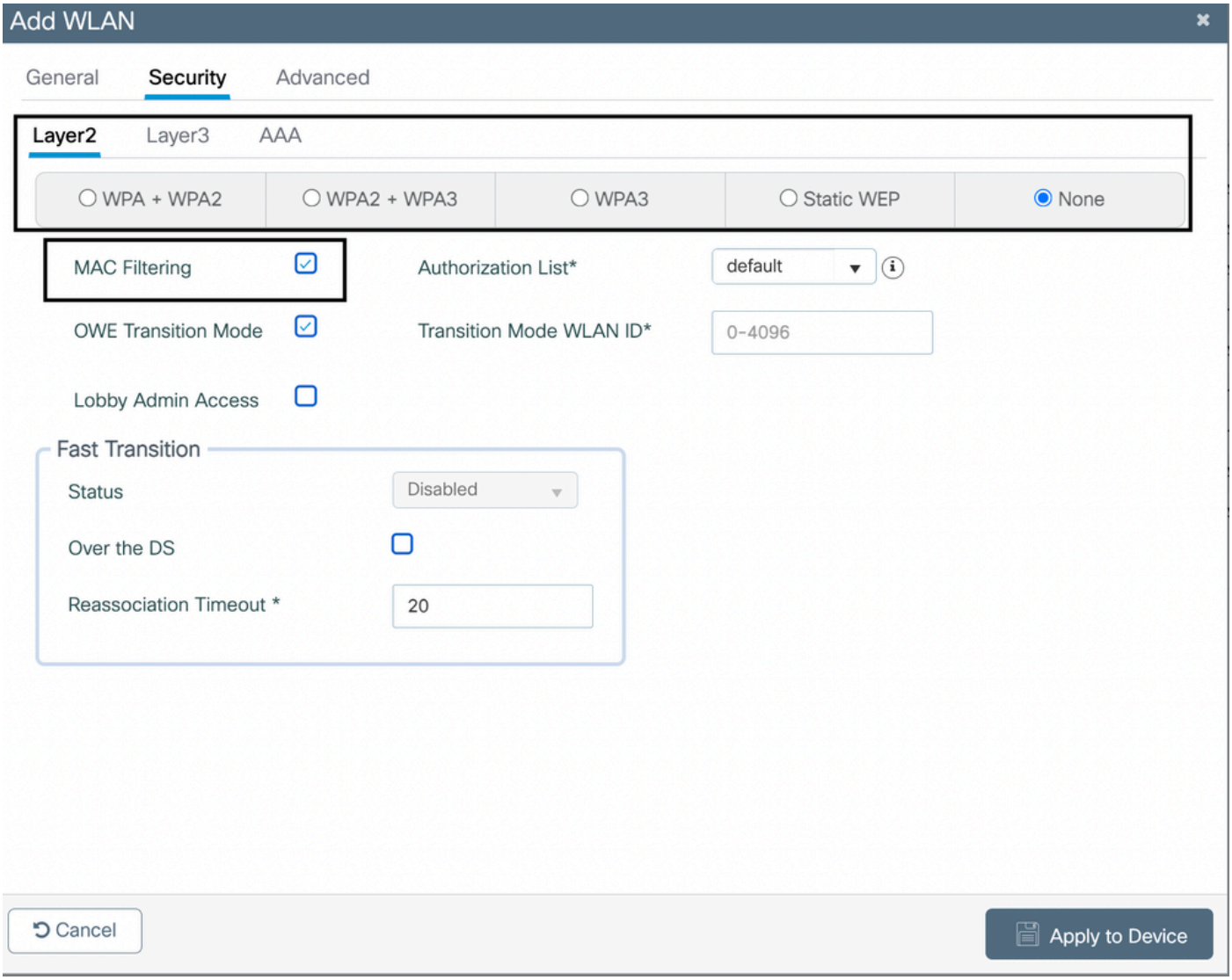
Configuración de un SSID abierto/no seguro

El SSID abierto solo se crea cuando decide tener una configuración BYOD SSID dual en su entorno.

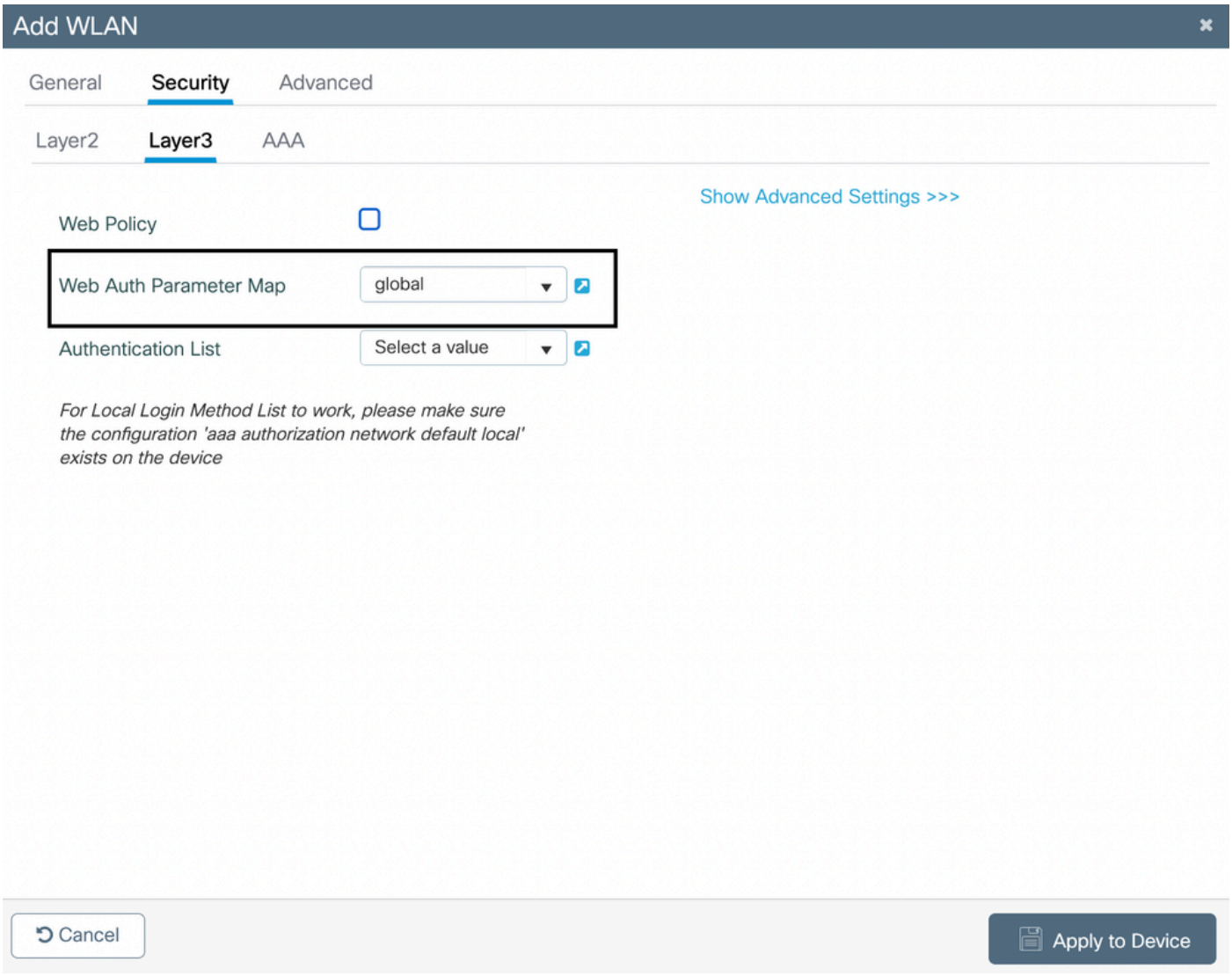
1. Vaya a Configuration > Tags & Profiles > WLANs. 'Haga clic en el botón Add (Agregar).'
2. Proporcione un nombre SSID en la ficha General (General) y active el botón WLAN.



3. Haga clic en la pestaña Seguridad desde la misma ventana. Seleccione el botón de opción None y active el filtrado de Mac.



4. En Capa 3 bajo Seguridad, seleccione la configuración global para Web Auth Parameter Map. Si tiene cualquier otro perfil de autenticación web configurado en el WLC, también puede asignarlo aquí:



Configuración de ISE

Requisitos previos

- Asegúrese de que Cisco ISE está instalado y cuenta con licencia para la funcionalidad BYOD.
- Agregue su WLC a ISE como un dispositivo de red con el secreto compartido RADIUS.

Certificados

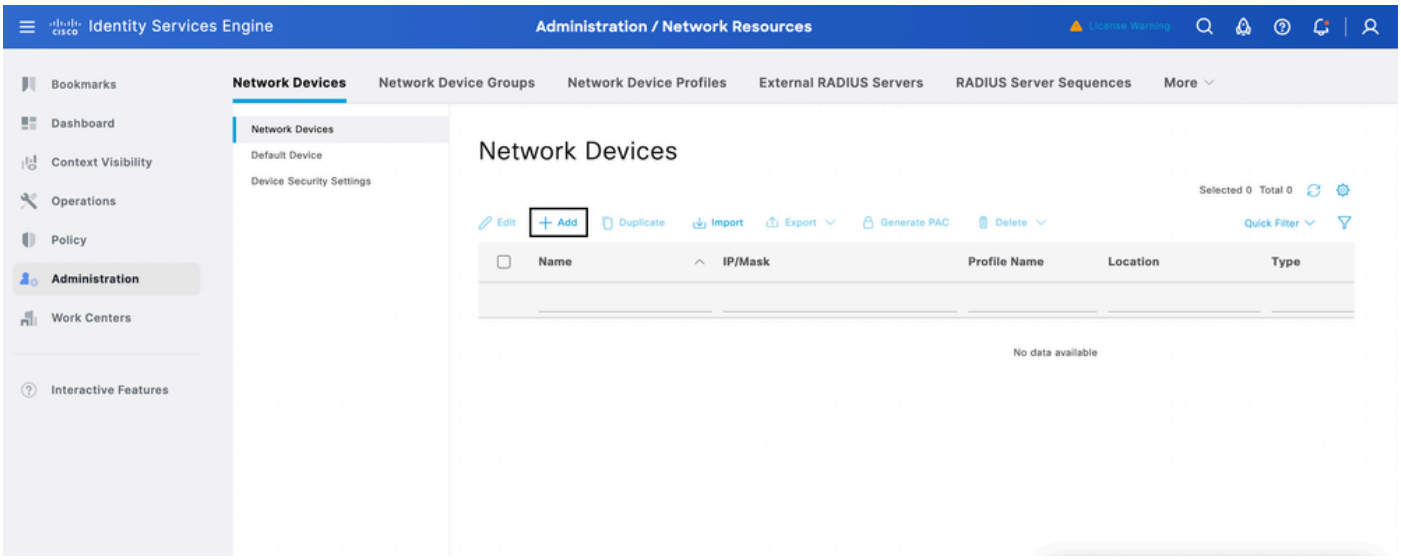
- Instale un certificado de servidor válido en ISE para evitar las advertencias de seguridad del navegador.
- Asegúrese de que los extremos confían en el certificado (firmado por una CA conocida o una CA interna con raíz de confianza).

Configuración de DNS

- Asegúrese de que DNS resuelva el nombre de host de ISE para el portal BYOD.

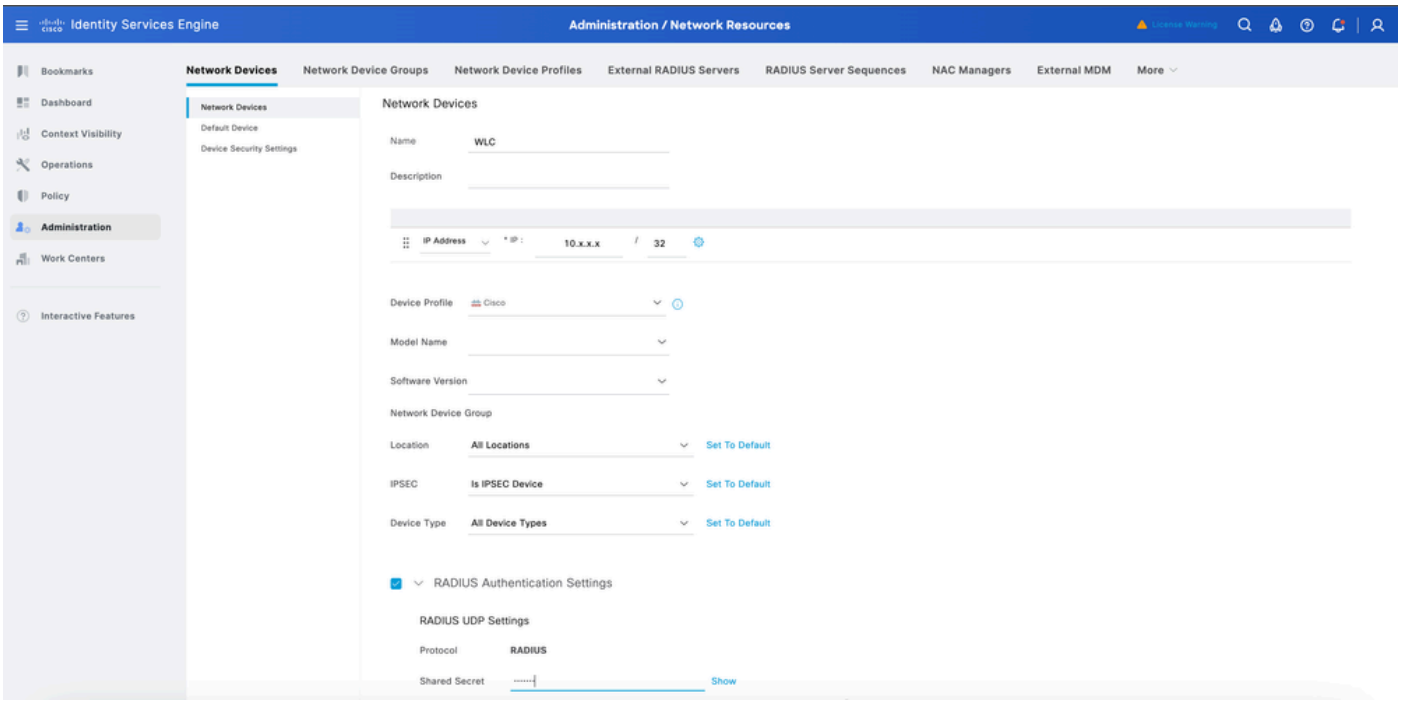
Configuración del dispositivo de red ISE

1. Inicie sesión en la interfaz de usuario web de ISE.
2. Vaya a Administration > Network Resources > Network Devices.



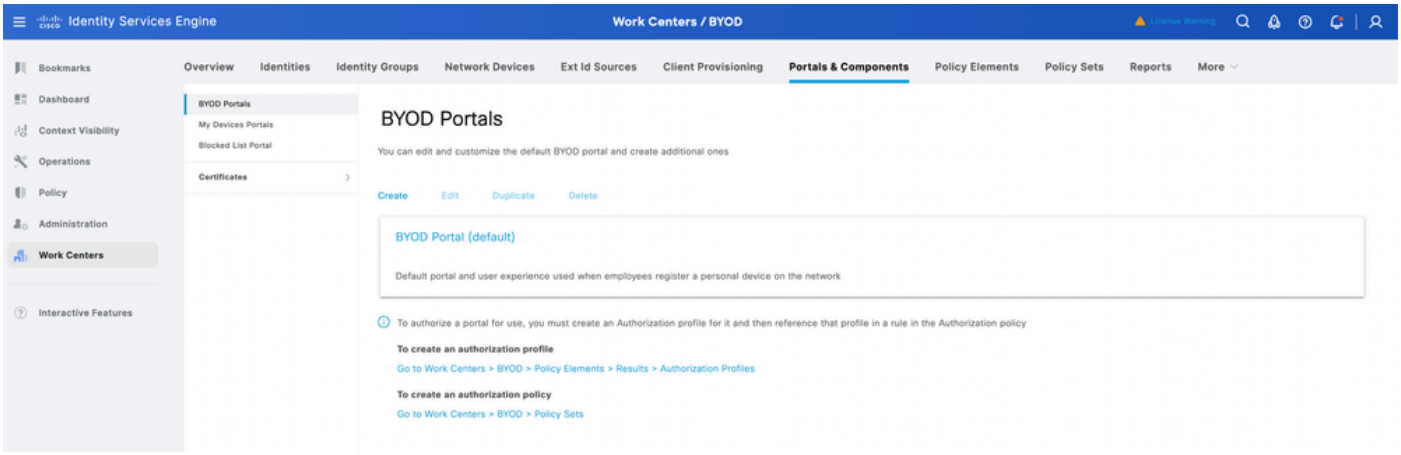
3.Add su WLC como dispositivo de red:

- Nombre: Introduzca un nombre para el WLC.
- IP Address: Introduzca la IP de administración del WLC.
- Secreto compartido RADIUS: Ingrese el mismo secreto compartido que se configuró en el WLC.
- Haga clic en Submit (Enviar).



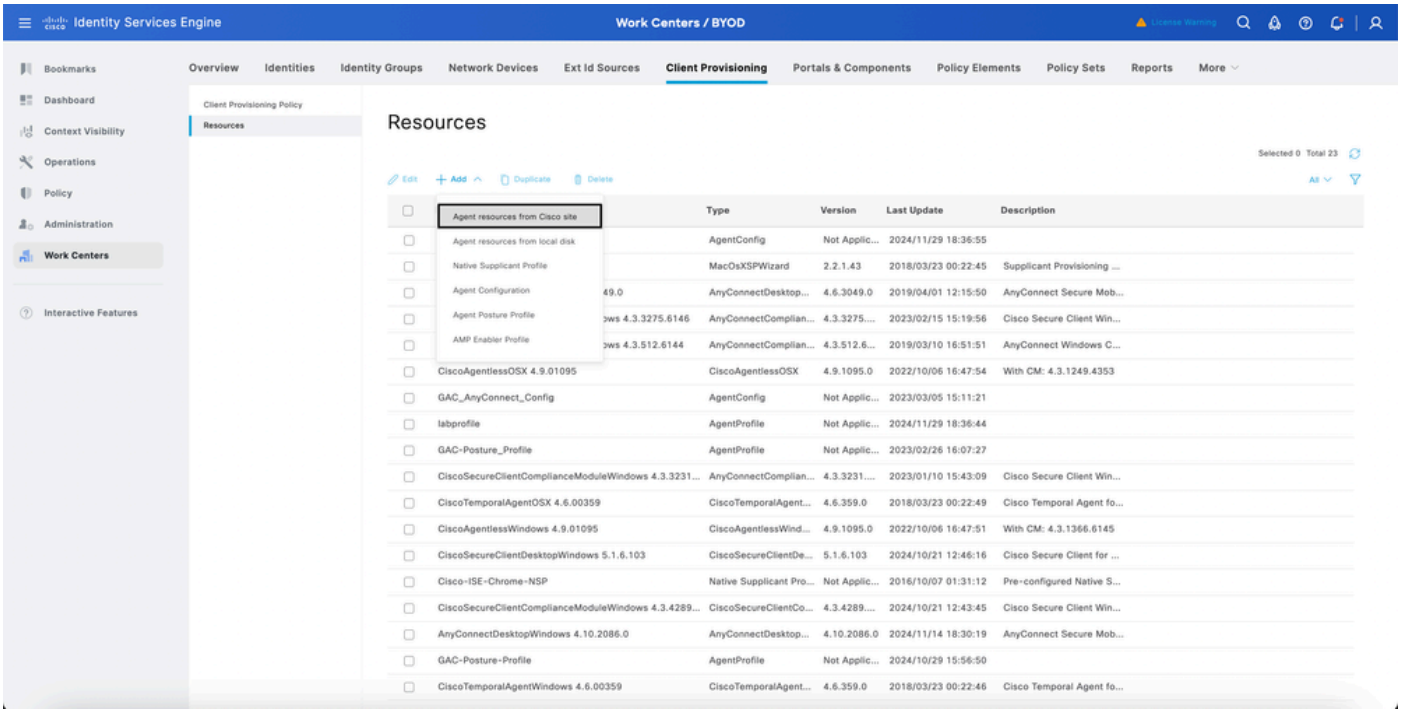
Creación de un portal BYOD

1. Vaya a Centros de trabajo > BYOD > Configuración > Portales y componentes > Portales BYOD.
2. Haga clic en Agregar para crear un portal BYOD o puede utilizar el portal predeterminado existente en ISE.



Descargar la última versión de Cisco IOS®

1. Vaya a Centros de trabajo > BYOD > Aprovisionamiento de clientes > Recursos.
2. Haga clic en el botón Add y seleccione los recursos de agente del sitio de Cisco.



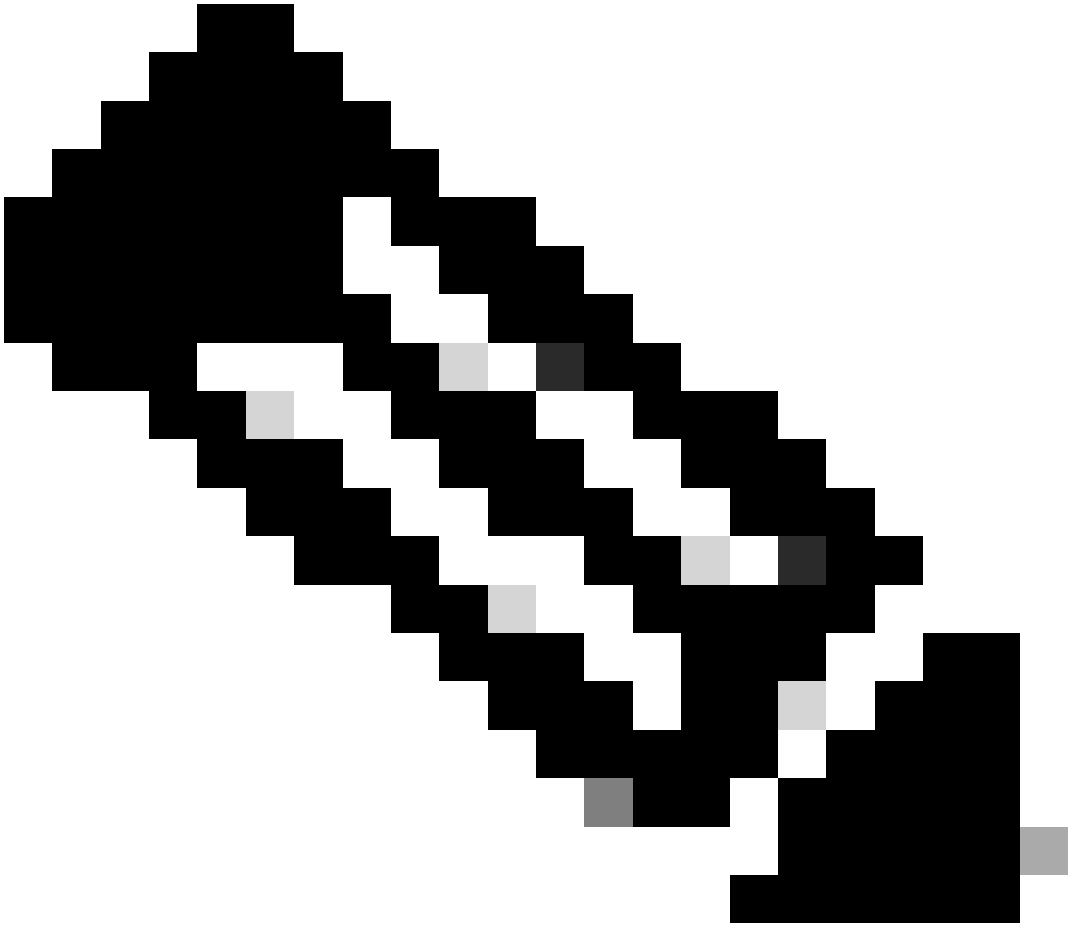
3. En la lista de software, seleccione la última versión de Cisco IOS que se descargará.

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

Cancel Save

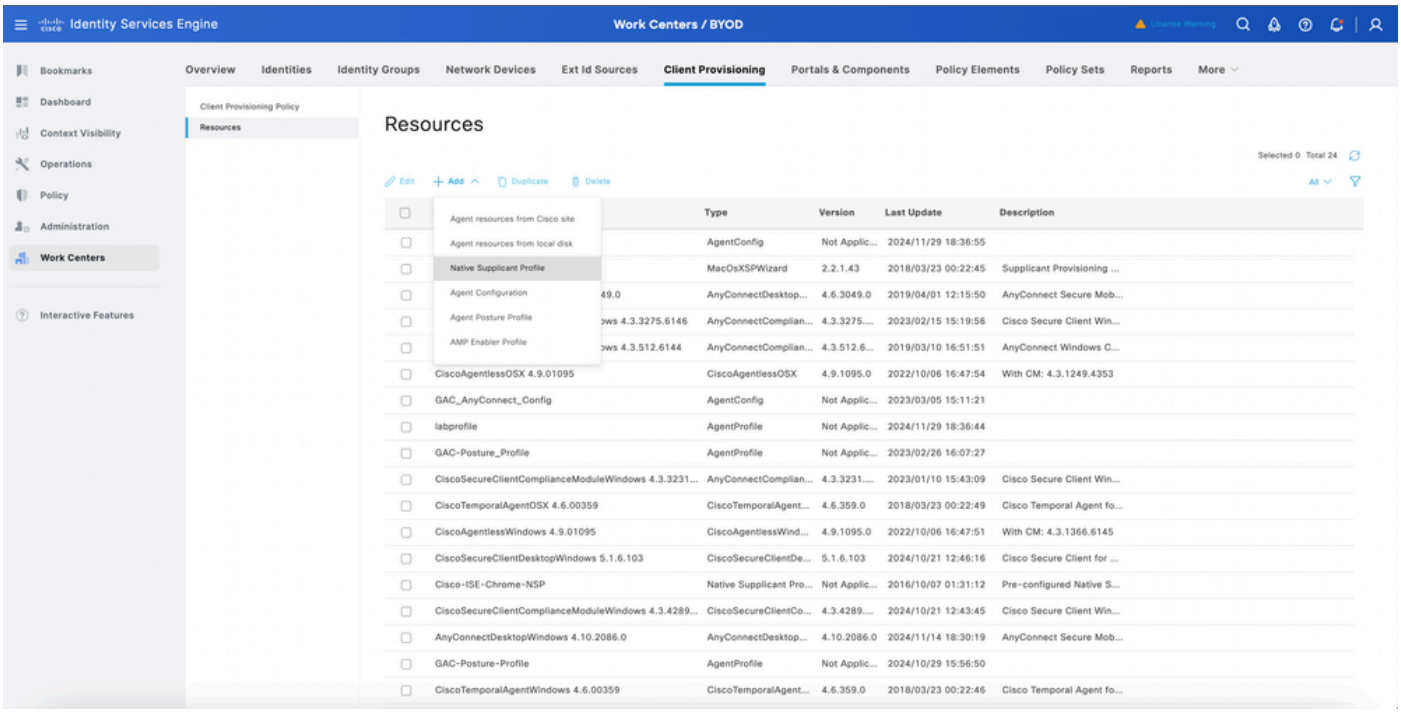


Nota: El software Cisco IOS se descarga en ISE para terminales Windows y MacOS. Para Apple iPhone IOS, utiliza un suplicante nativo para aprovisionar el dispositivo y para el dispositivo Android, tiene un asistente de configuración de red que debe descargarse de Play Store.

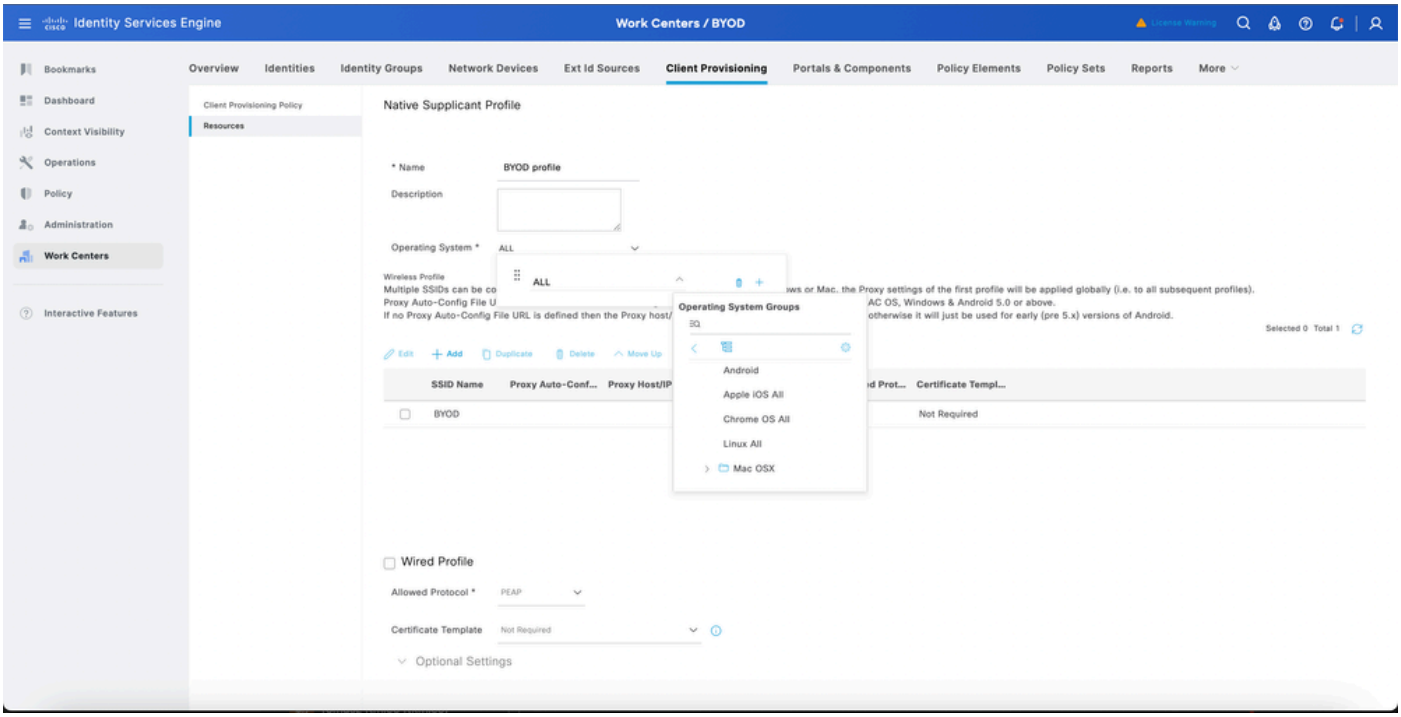
Crear un perfil de terminal

1. Vaya a Centros de trabajo > BYOD > Aprovisionamiento de clientes > Recursos.

2. Haga clic en Agregar, seleccione Perfil de solicitante nativo en el menú desplegable.



3. En el menú desplegable Sistema operativo, seleccione el sistema operativo requerido que desea incorporar al dispositivo o puede configurarlo como ALL (TODOS) para incorporar todos los terminales de su entorno:



4. Haga clic en Agregar en la página para crear el perfil de terminal para configurar 802.1X para el terminal:

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)
- [x] 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
- [x] Connect even if the network is not broadcasting its name (SSID)

iOS Settings

- [ ] Enable if target network is hidden

Android Settings

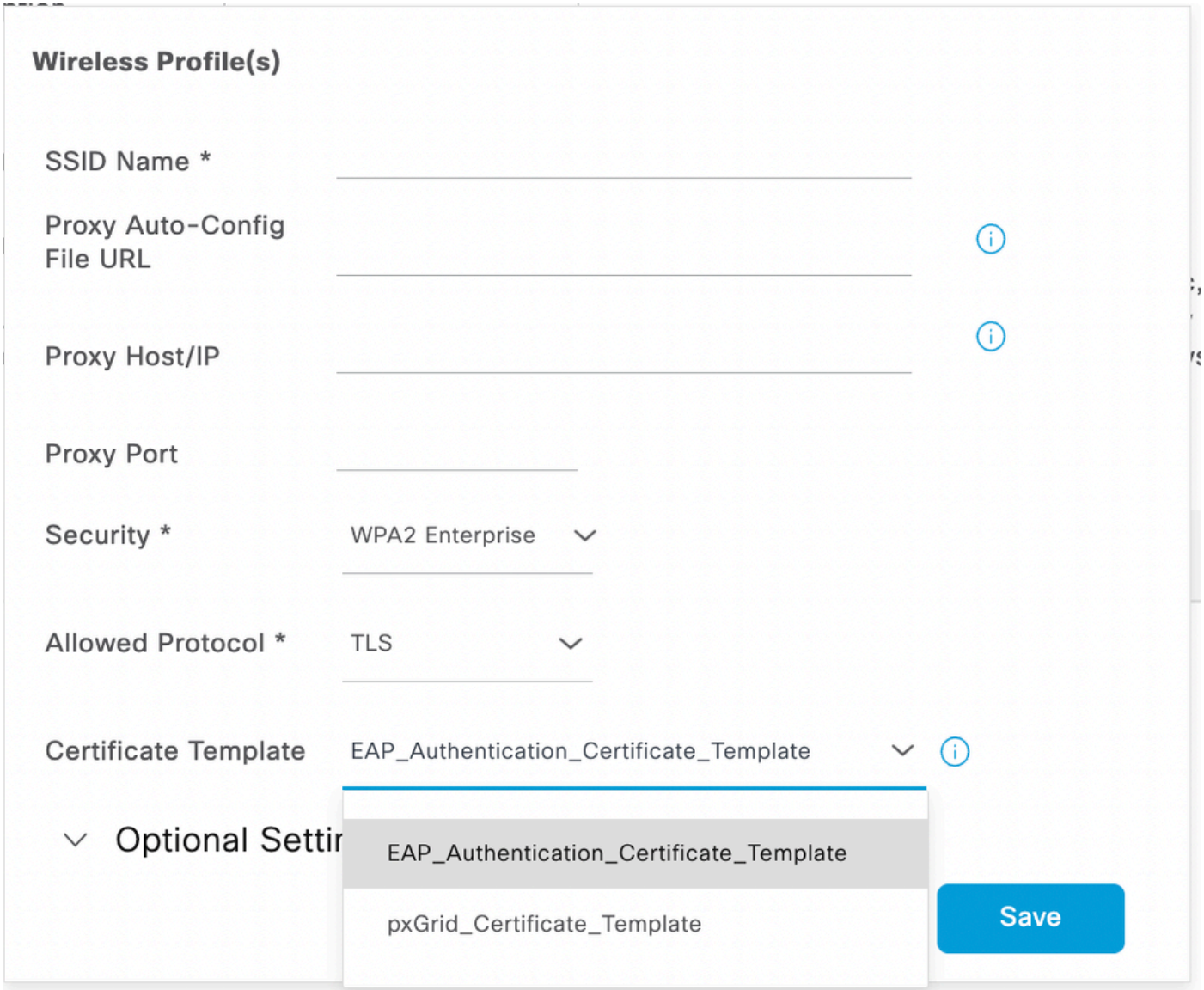
Certificate Enrollment Protocol:

En función de sus necesidades, configure el perfil de terminal para el terminal de su entorno. El perfil de terminales nos permite configurar EAP-PEAP, EAP-TLS.

5. Haga clic en Guardar y, a continuación, en Enviar en el perfil de terminal.

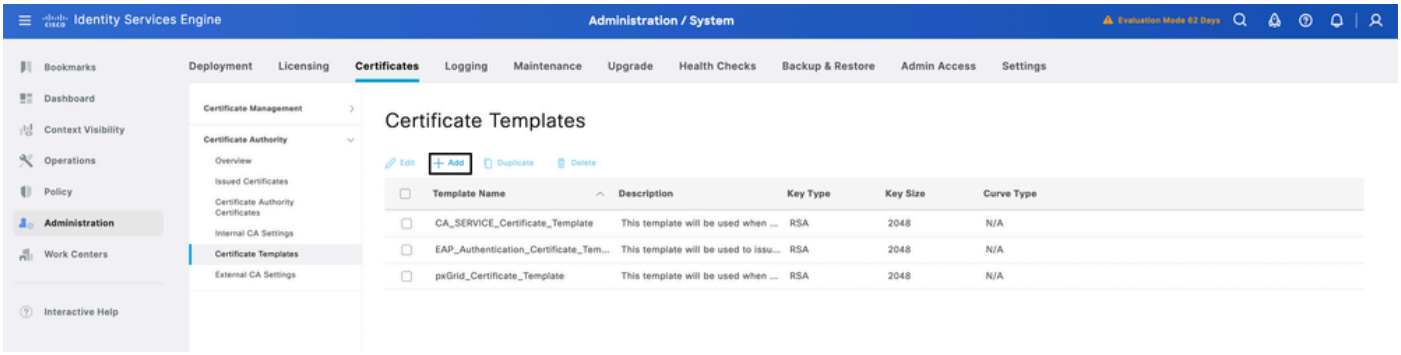
Plantilla de certificado

El perfil de terminal está preconfigurado para realizar EAP-TLS. Se debe agregar una plantilla de certificado al perfil. De forma predeterminada, ISE tiene dos plantillas predefinidas que se pueden seleccionar en el menú desplegable.

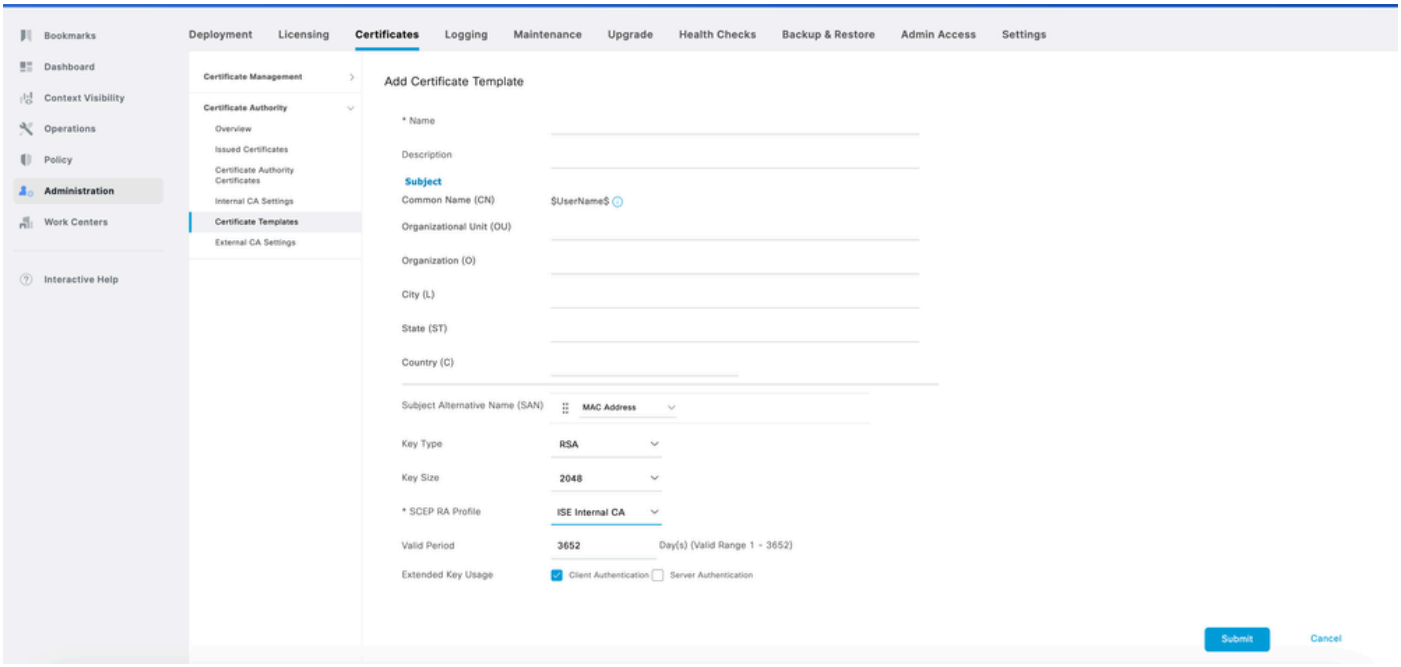


Para crear una nueva plantilla de certificado, siga estos pasos:

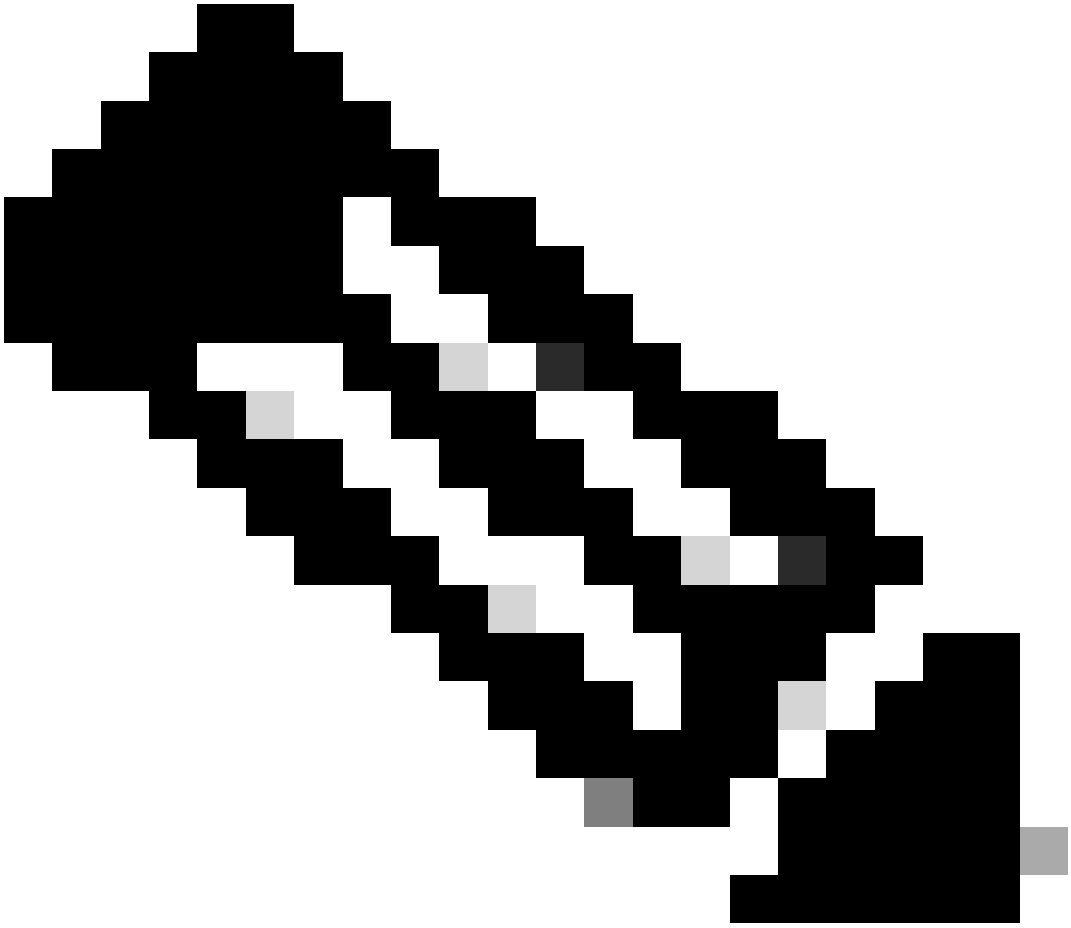
1. Vaya a Administration > System > Certificates > Certificate Authority > Certificate Templates.
2. Haga clic en el botón Agregar de la página.



3. Rellene los datos personalizados para satisfacer los requisitos específicos de su organización.



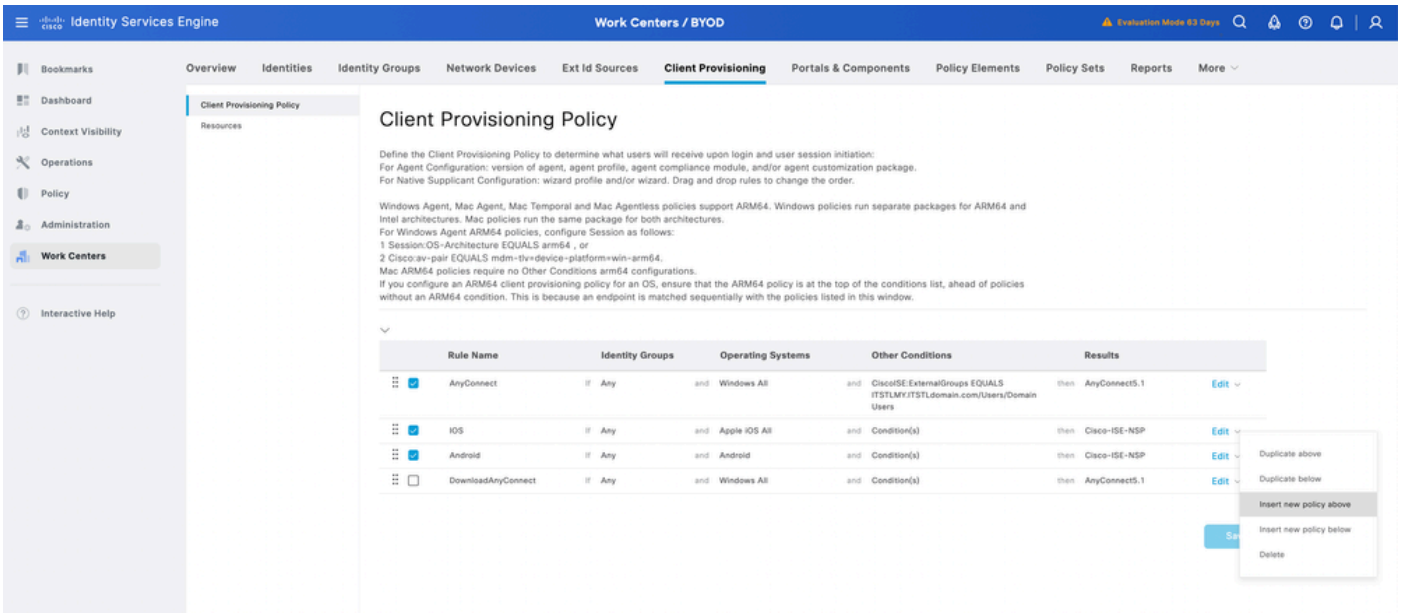
4. Haga clic en Enviar para guardar los cambios.



Nota: La plantilla de certificado podría ser útil en situaciones en las que tiene diferentes dominios y segmenta al usuario agregando un valor diferente en la unidad organizativa del certificado.

Asignar un perfil de terminal al portal de aprovisionamiento de clientes

1. Vaya a Centros de trabajo > BYOD > Aprovisionamiento de clientes > Política de aprovisionamiento de clientes.
2. Haga clic en v en de las reglas para crear una nueva regla de aprovisionamiento de cliente.

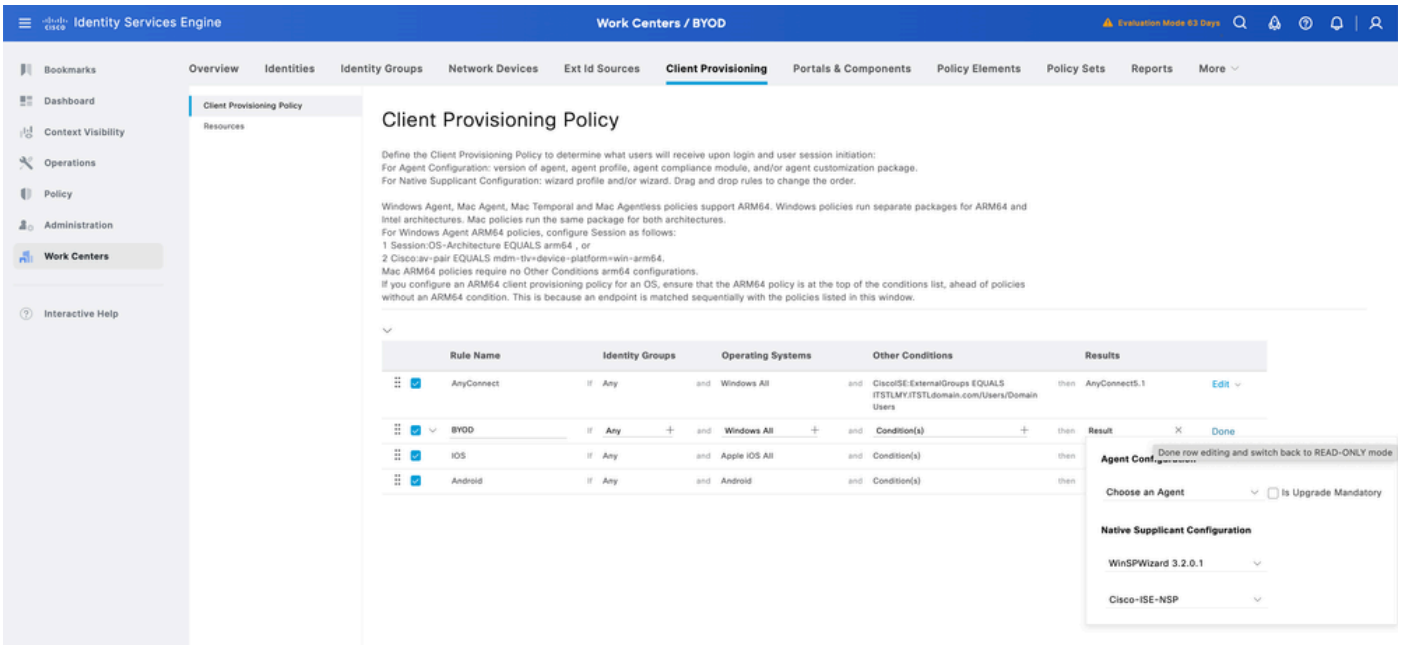


3. Contabilizar la creación de la nueva regla en la página

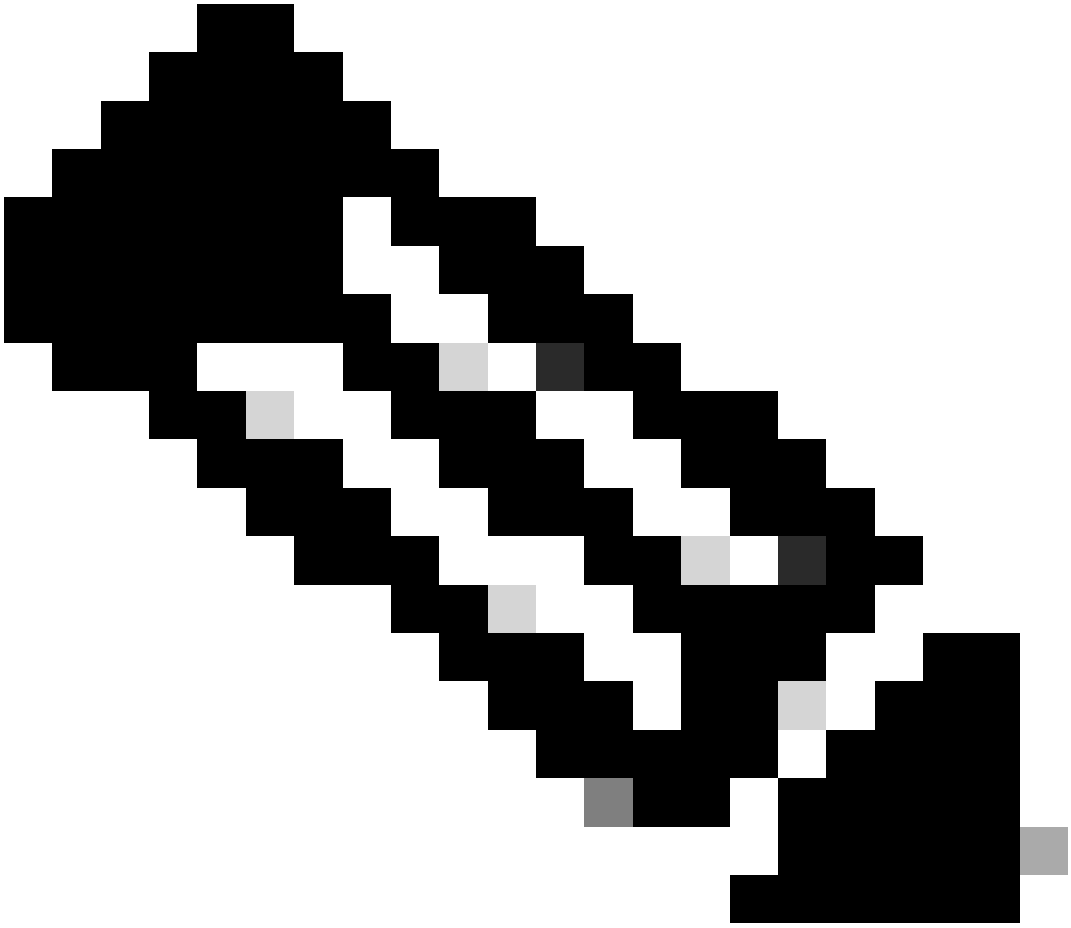
4. Agregue el grupo de identidad si desea restringir el uso del portal BYOD por parte de determinados usuarios

5. Agregue el sistema operativo al que desea tener acceso en el portal BYOD

6. Asigne la versión de Cisco IOS de la lista desplegable y también seleccione el perfil de terminal que ha creado a partir del resultado



7. Haga clic en Finalizado, a continuación, en el botón Guardar.

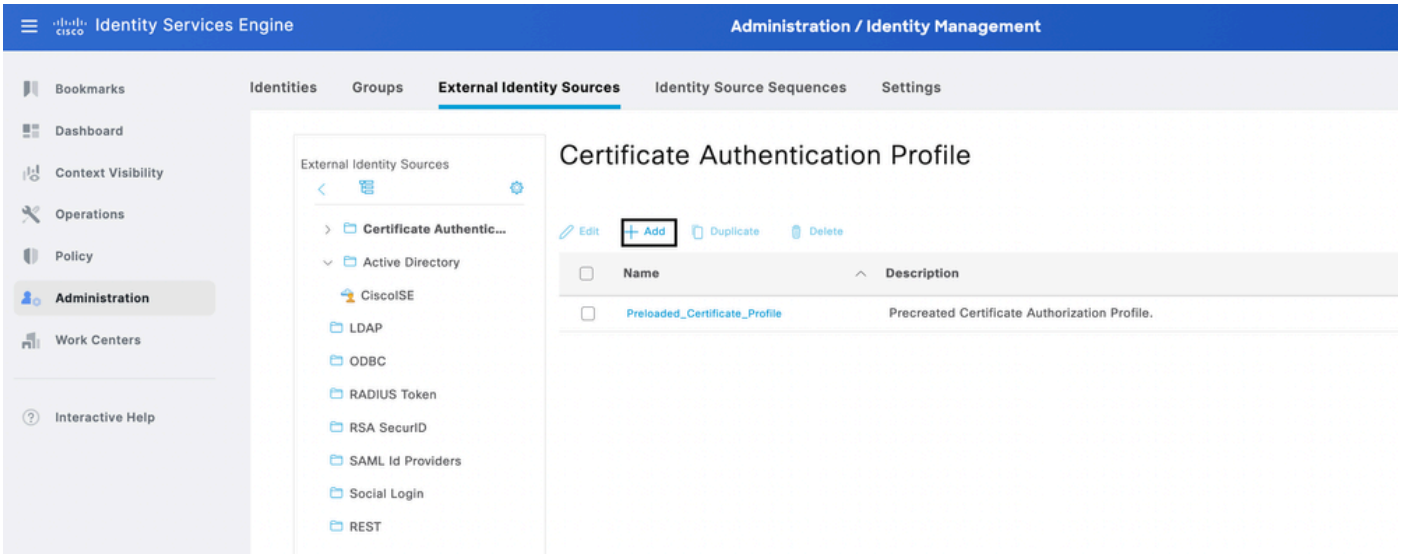


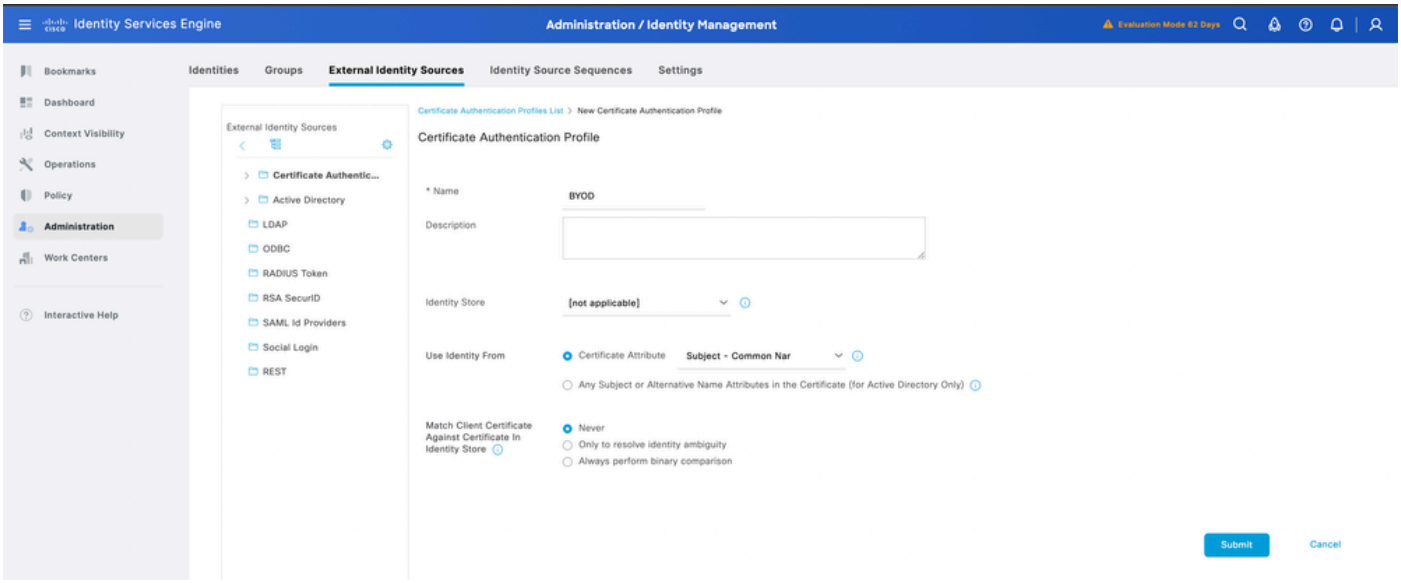
Nota: Esta política afecta tanto al aprovisionamiento de clientes de estado como al aprovisionamiento de BYOD, donde la sección Configuración del agente determina el agente de estado y el módulo de cumplimiento de normativas aplicados para las comprobaciones de estado, mientras que la sección Configuración del suplicante nativo gestiona la configuración de los flujos de aprovisionamiento de BYOD

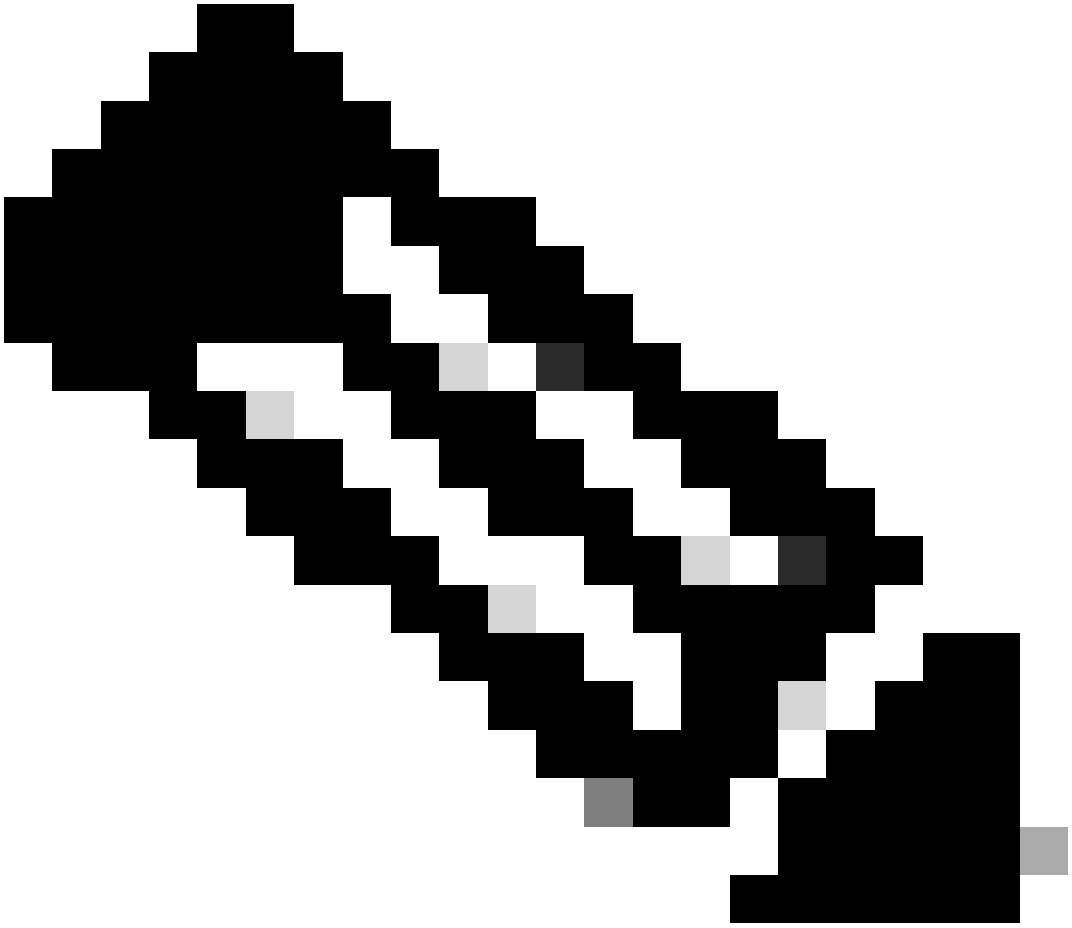
Configuración de conjuntos de políticas de ISE para BYOD con SSID único

1. Vaya a Policy > Policy Set y cree una política para el flujo de BYOD en ISE:

2. Luego, navegue hasta Administración > Administración de identidad > Orígenes de identidad externos > Perfil de autenticación de certificado. Haga clic en el botón Add para crear el perfil de certificado:

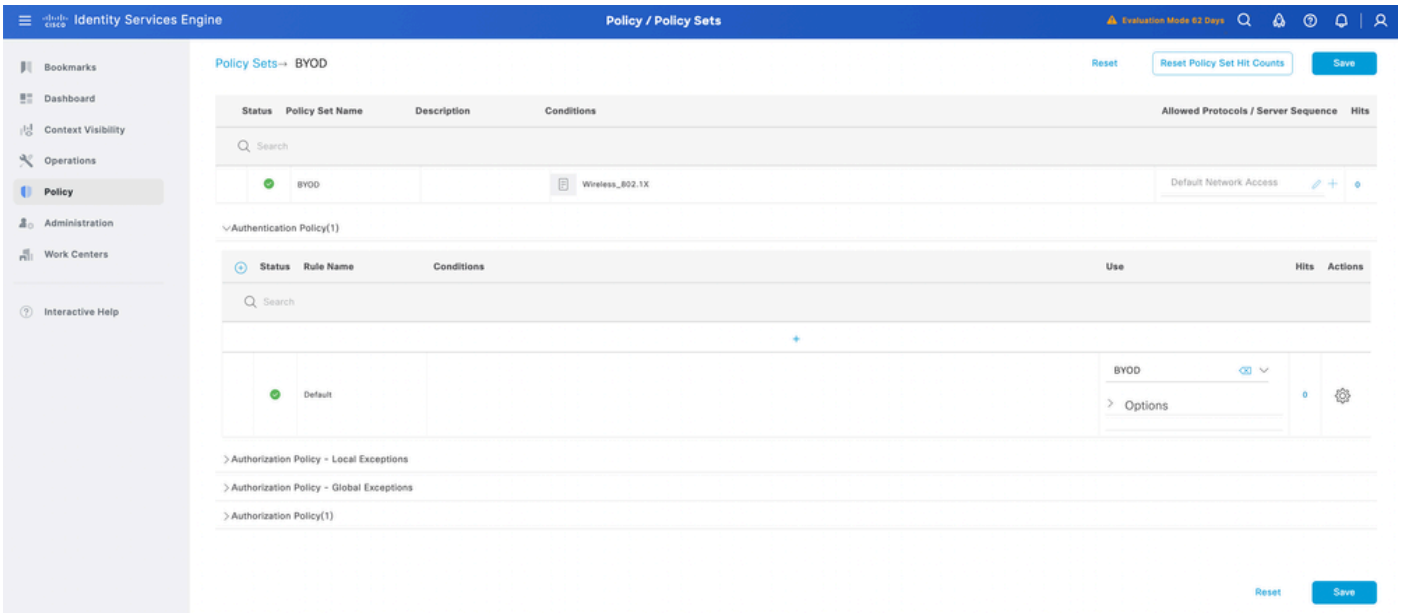






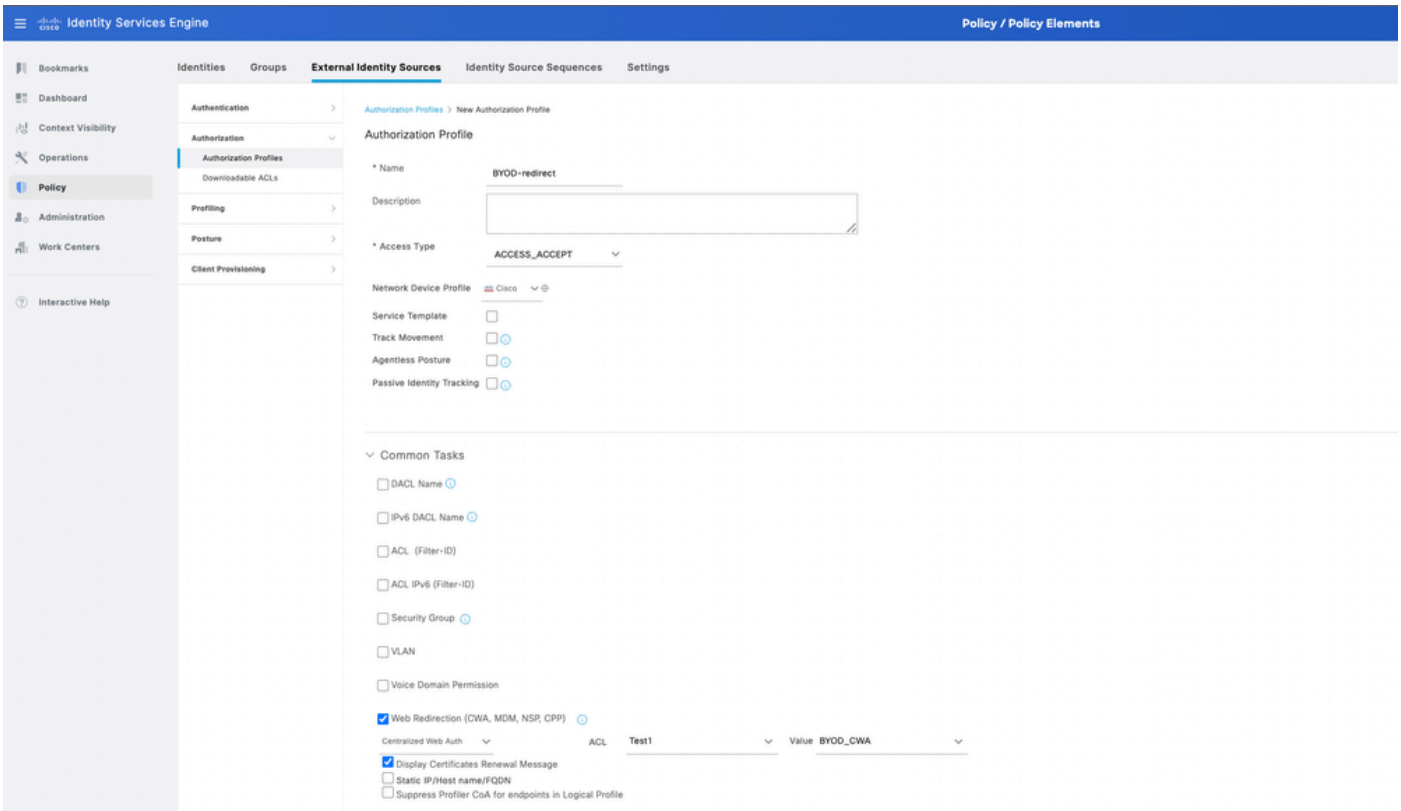
Nota: En el almacén de identidades, siempre puede seleccionar su Active Directory que se ha integrado en ISE para realizar una búsqueda de usuario desde el certificado para obtener seguridad adicional.

3. Haga clic en Enviar para guardar la configuración. A continuación, asigne el perfil del certificado al conjunto de políticas para BYOD:

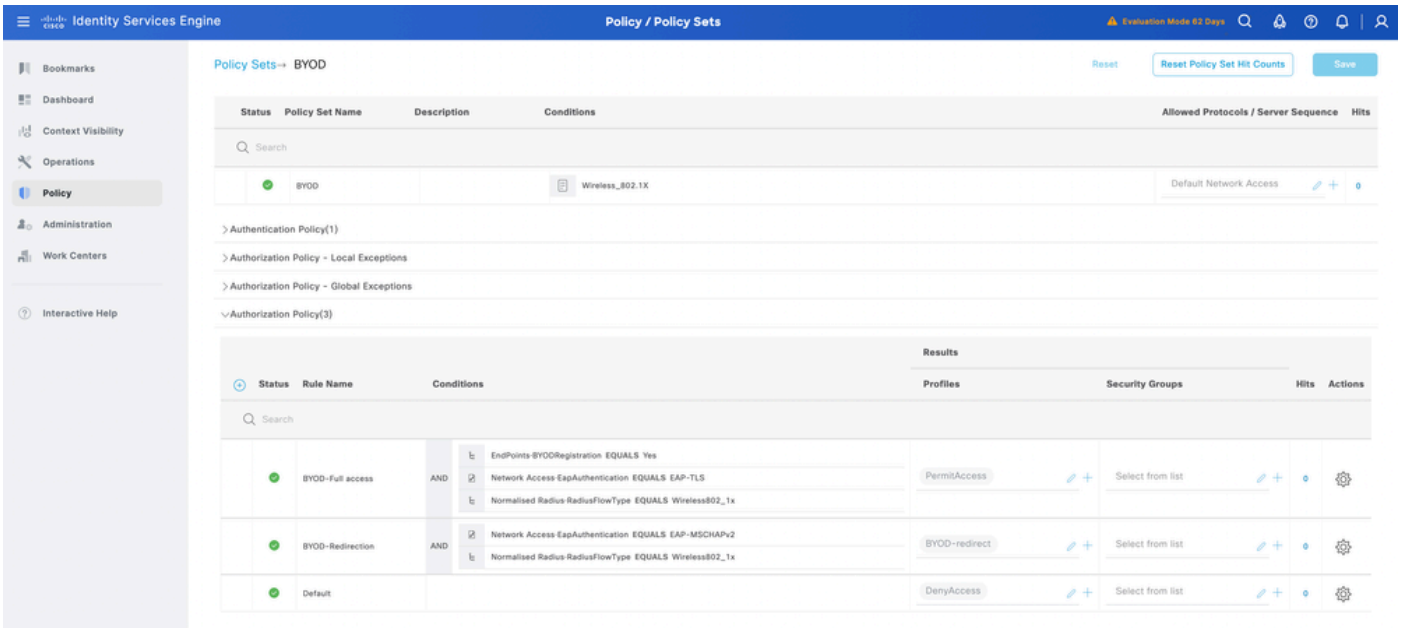


4. Configure el perfil de autorización para la redirección de BYOD y el acceso completo después del flujo de BYOD. Vaya a Política > Elementos de política > Resultados > Autorización > Perfiles de autorización.

5. Haga clic en Agregar y cree un perfil de autorización. Consulte Web Redirection (CWA, MDM, NSP, CPP) y asigne la página del portal BYOD. Además, agregue el nombre de la ACL de redirección del WLC al perfil. Para el perfil de acceso completo, configure un permiso de acceso con la VLAN corporativa respectiva en el perfil.



6. Asigne el perfil de autorización a la regla de autorización. El acceso completo a BYOD debe tener la regla EndPoints·BYODRegistration igual que yes para que el usuario tenga acceso completo a la red después del flujo de BYOD.

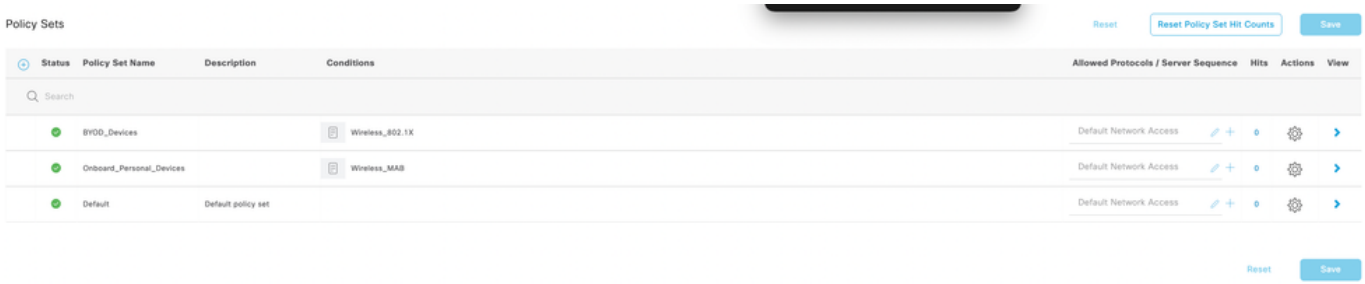


Configuración de conjuntos de políticas de ISE para BYOD SSID dual

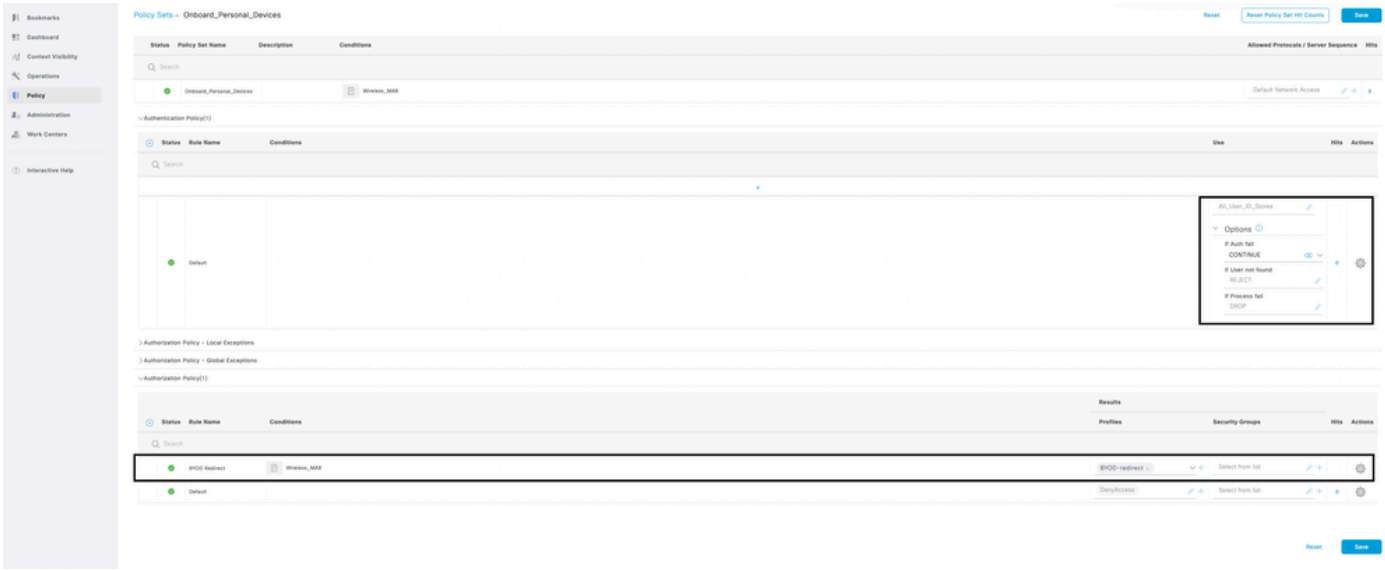
En la configuración de BYOD con SSID dual, el conjunto de dos políticas se configura en ISE. El primer conjunto de políticas es para el SSID abierto/no seguro, donde la configuración del conjunto de políticas redirige al usuario a la página BYOD al conectarse al SSID abierto/no seguro

1. Vaya a Policy > Policy Set y cree una política para el flujo de BYOD en ISE.

2. Cree un conjunto de políticas para el SSID abierto/no seguro y el SSID corporativo que autentique al usuario BYOD registrado en ISE.

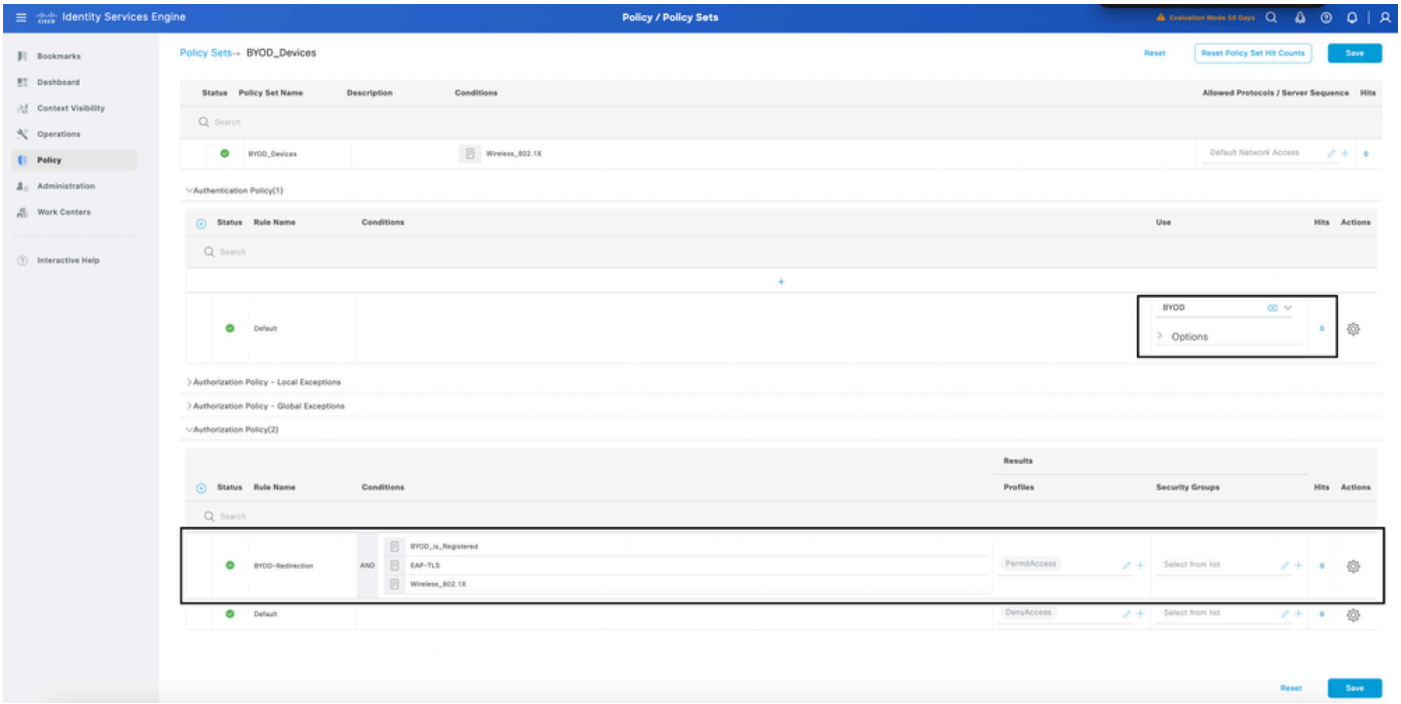


3. En el conjunto de políticas de Onboarding, busque Continue selected en las opciones. Para la directiva de autorización, cree una condición y asigne el perfil de autorización de redirección. Los mismos pasos se aplican en la creación del perfil de autorización, que se puede encontrar en el punto 4.



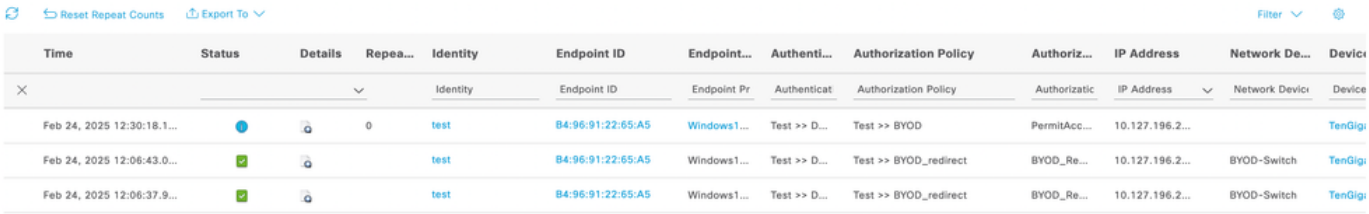
4. En el conjunto de políticas registradas de BYOD, configure la política de autenticación con el mismo perfil de certificado que encontró.

en Configure ISE Policy Sets for Single SSID BYOD en el punto 2. Cree también una condición para la política de autorización y asigne el perfil de acceso completo a la política.

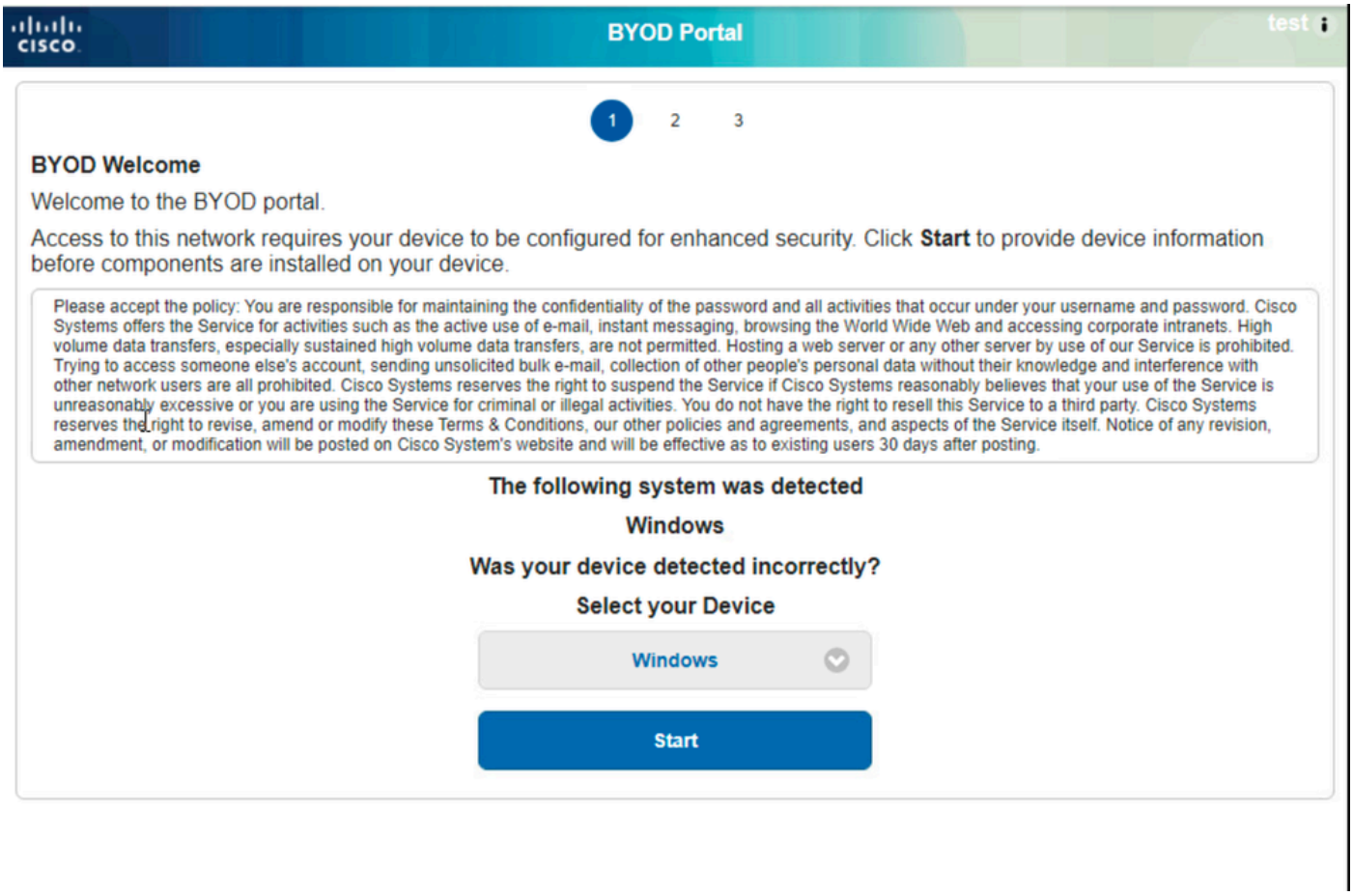


Registro

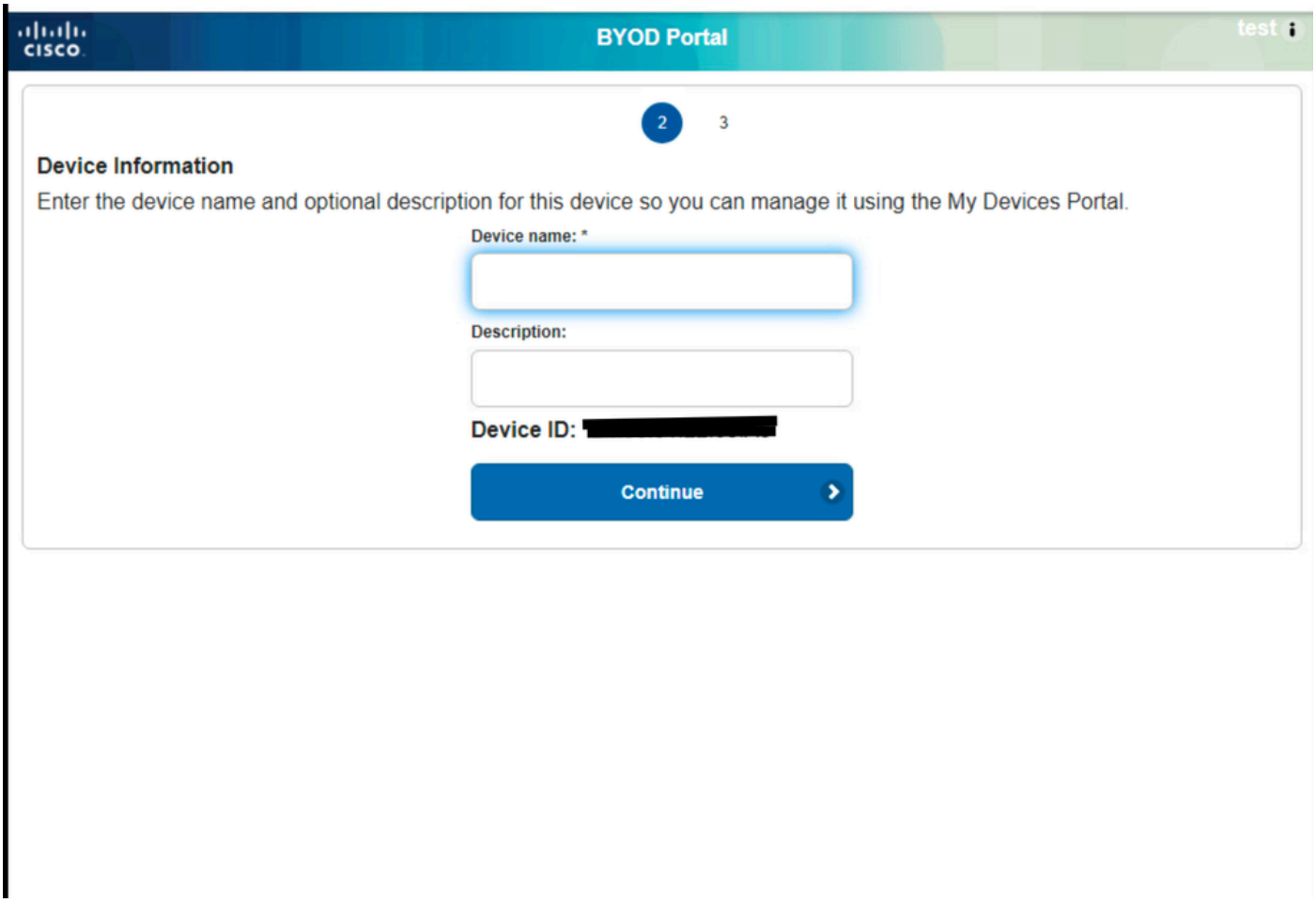
A partir del registro en directo de ISE, la autenticación de usuario se realizará correctamente y se redirigirá a la página del portal BYOD. Una vez finalizado el flujo de BYOD, el usuario tendría acceso a la red



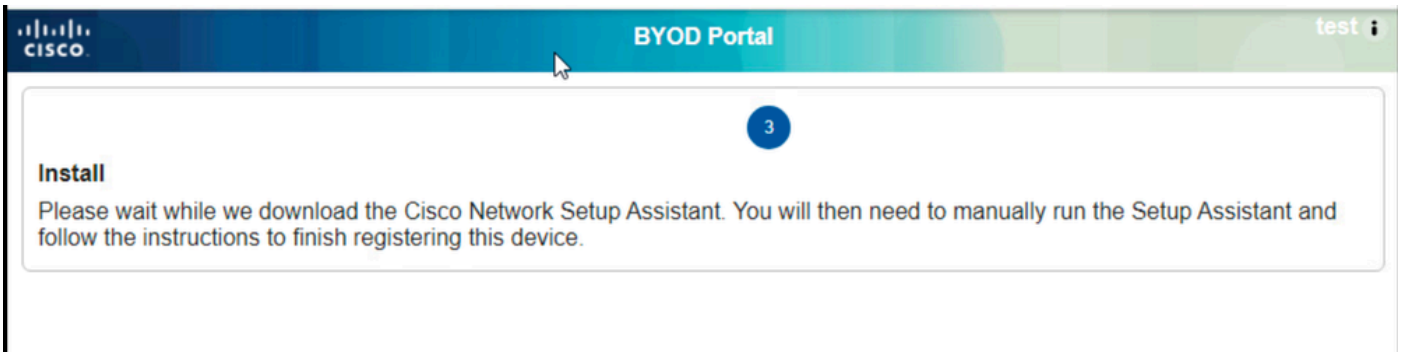
Desde la perspectiva del usuario, en primer lugar se redirigirían a la página de BYOD y el dispositivo adecuado tendría que seleccionarse en la página web. Para la prueba se utilizó un dispositivo Windows 10



Después de hacer clic en el botón Next (Siguiente), se le dirigirá a una página en la que se le solicitará al usuario que introduzca el nombre del dispositivo y la descripción

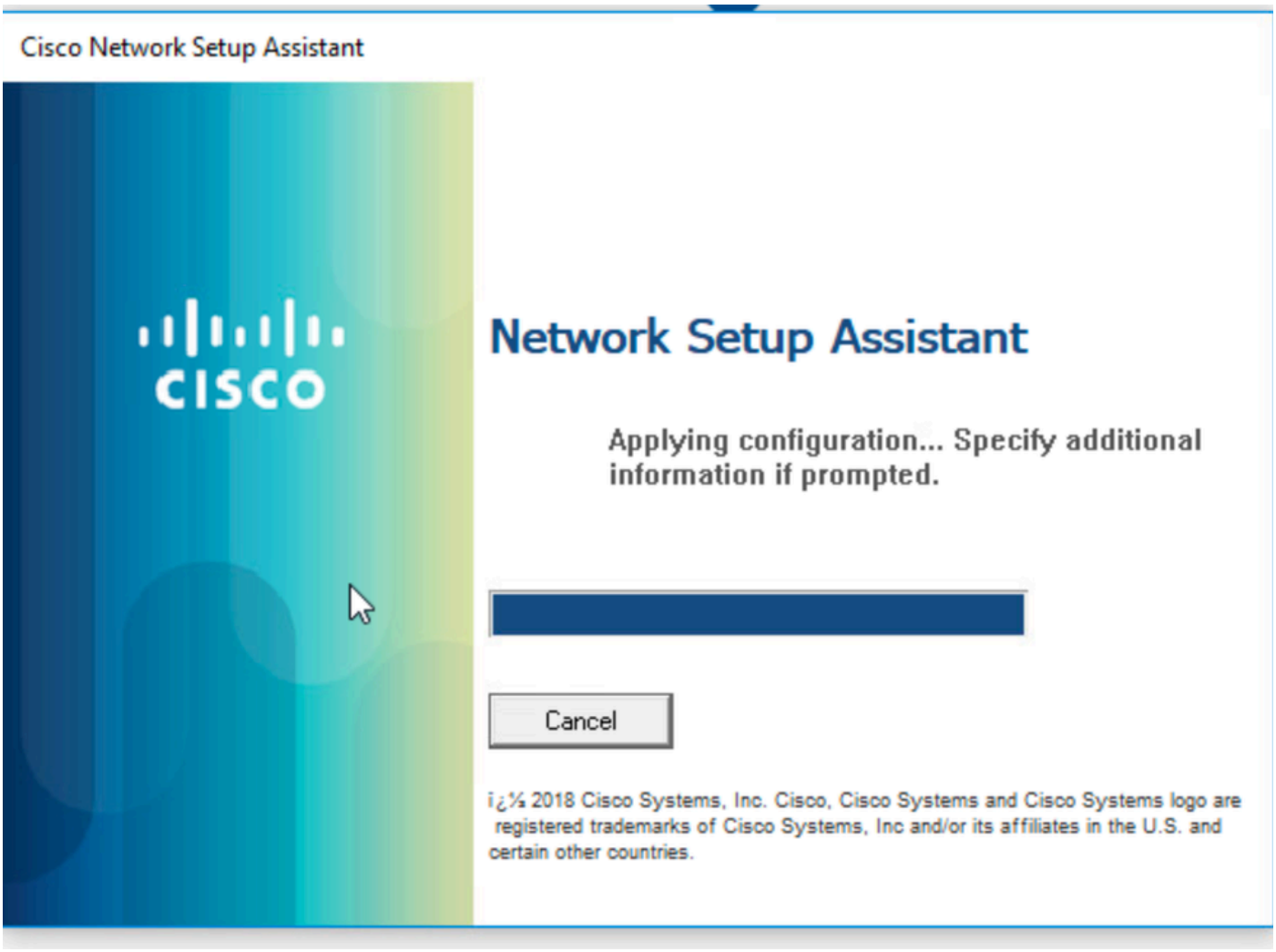


Indicación de que se solicitaría al usuario que descargara la herramienta Network Assistant para descargar el perfil de terminal y el certificado EAP-TLS para la autenticación si el perfil está configurado para realizar la autenticación EAP-TLS



Ejecute la aplicación Network Assistant con privilegios de administrador y haga clic en el botón Start (Iniciar) para iniciar el flujo de incorporación:


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.



El usuario se ha incorporado correctamente a la red con su dispositivo personal para acceder a los recursos.

Resolución de problemas

Para solucionar el problema de BYOD, habilite esta depuración en ISE

Atributos que se deben establecer en el nivel de depuración:

- cliente (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)

Fragmento de registro

Registros de invitados

Estos registros indican que el usuario se ha redirigido correctamente a la página y ha descargado la aplicación Network Assistant:

2025-02-24 12:06:08,053 INFO [https-jsse-nio-10.127.196.172-8443-exec-4][[]] portalwebaction.utils.portal.spring.ISEPortalControllerUtils -:000000000000000B30D59CC5:::- ruta de mapeo encontrada en action-for pupilos, reenviar a: pages/byodWelcome.jsp // Página de bienvenida de BYOD
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:- Tamaño de pTranPasos: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, pTransPasos: [id: d2513b7b-7249-4bc3-a423-0e7d9a0b250]
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, stepTrans:d2 5513b7b-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:::- ruta de asignación encontrada en acción-hacia adelante, reenvío : 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:- Tamaño de pTranPasos: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, pTransPasos: [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, stepTrans:f2 03b757-9e8a-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:::- ruta de mapeo encontrada en action-forward, reenviar a : 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 // La red La aplicación de asistencia se ha enviado al terminal

Registros De Ise-Psc

A medida que la aplicación se descarga en el terminal, la aplicación inicia un flujo SCEP para obtener el certificado de cliente de ISE.

2025-02-24 12:04:39,807 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -::::- CertStore contiene 4 certificado(s):
2025-02-24 12:04:39,807 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -::::- 1. '[issuer=CN=CA raíz de Servicios de Certificate Server - 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=CA raíz de Servicios de Certificate Server - iseguest; serial=686276201605863086858498187751006982 24]'
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 -::::- Selección del certificado de cifrado
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -::::- Selección de certificado con keyEncipherment keyUsage
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -::::- Se han encontrado 1 certificado(s) con keyEncipherment keyUsage
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -::::- Usando [issuer=CN=Certificate Services Endpoint Sub CA - iseguest; serial=131900858749761727853768227590303808637] para el cifrado de mensajes
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -:::::- Seleccionar certificado de verificador
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -:::::- Selección de certificado con digitalSignature keyUsage
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -::::- Encontrado 1 certificado(s) con digitalSignature keyUsage
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -::::- Usando [issuer=CN=Certificate Services Endpoint Sub CA - iseguest; serial=131900858749761727853768227590303808637] para verificación de mensajes
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -:::::- Selección de certificado de emisor
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -:::::- Selección de certificado con restricciones básicas
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -::::- Se han encontrado 3 certificado(s) con restricciones basicConstraints

2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -::::- Usando [issuer=CN=Certificate Services Endpoint Sub CA - iseguest; serial=131900858749761727853768227590303808637] para emisor
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] com.cisco.cpm.scep.PKIServerLoadBalancer -::::- Mediciones de rendimiento de los servidores SCEP : name[activo/muerto, total de solicitudes, total de errores, solicitudes en curso, promedio de RTT]
http://127.0.0.1:9444/caservice/scep[activo,96444,1,0,120]

Descarga de perfiles de terminales

Una vez finalizado el proceso SCEP y cuando el terminal instala el certificado, la aplicación descarga el perfil del terminal para la futura autenticación que realizará el dispositivo:

2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]] cisco.cpm.client.provisioning.EvaluationServlet -::::- Referer = Windows // El dispositivo Windows se ha detectado en función de la página web
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 -::::- perfil de aprovisionamiento de nsp
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//El perfil NSP se descarga en el terminal
2025-02-24 12:06:26,547 DEBUG [https-jsse-nio-8905-exec-2][[]] cisco.cpm.client.provisioning.StreamingServlet -::::- Streaming a ip: tipo de archivo: NativeSPProfile: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 se ha configurado para probar
2025-02-24 12:06:26,558 DEBUG [https-jsse-nio-8905-exec-2][[]] cisco.cpm.client.provisioning.StreamingServlet -::::- el tipo de redirección es: SUCCESS_PAGE, la URL de redirección es: para mac:

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).