Configuración de la posición en Catalyst 9800 WLC e ISE

Contenido

Introducción

Este documento describe cómo configurar una WLAN de estado en un WLC Catalyst 9800 e ISE a través de la interfaz gráfica de usuario (GUI).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración general del 9800 WLC
- Configuración de perfiles y políticas de ISE

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- 9800 WLC Cisco IOS® XE Cupertino v17.9.5
- Identity Service Engine (ISE) v3.2
- Portátil Windows 10 Enterprise

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Flujo de funciones de RADIUS NAC y CoA del controlador de LAN inalámbrica

1. El cliente autentica usando la autenticación dot1x.

2. La aceptación de acceso de RADIUS transporta la URL redirigida para el puerto 80 y las ACL previas a la autenticación que incluyen permitir direcciones IP y puertos, o poner en cuarentena VLAN.

3. El cliente se redirige a la URL proporcionada en access accept, y se pone en un nuevo estado hasta que se realice la validación de estado. El cliente en este estado se comunica con el servidor ISE y se valida con las políticas configuradas en el servidor ISE NAC.

4. El agente NAC del cliente inicia la validación de estado (tráfico al puerto 80): El agente envía la solicitud de detección HTTP al puerto 80, que el controlador redirige a la URL proporcionada en la aceptación de acceso. El ISE sabe que el cliente está intentando ponerse en contacto con él y responde directamente. De esta manera, el cliente aprende acerca de la IP del servidor ISE y, a partir de ahora, el cliente habla directamente con el servidor ISE.

5. El WLC permite este tráfico porque la ACL está configurada para permitir este tráfico. En caso de anulación de VLAN, el tráfico se puentea de modo que llegue al servidor ISE.

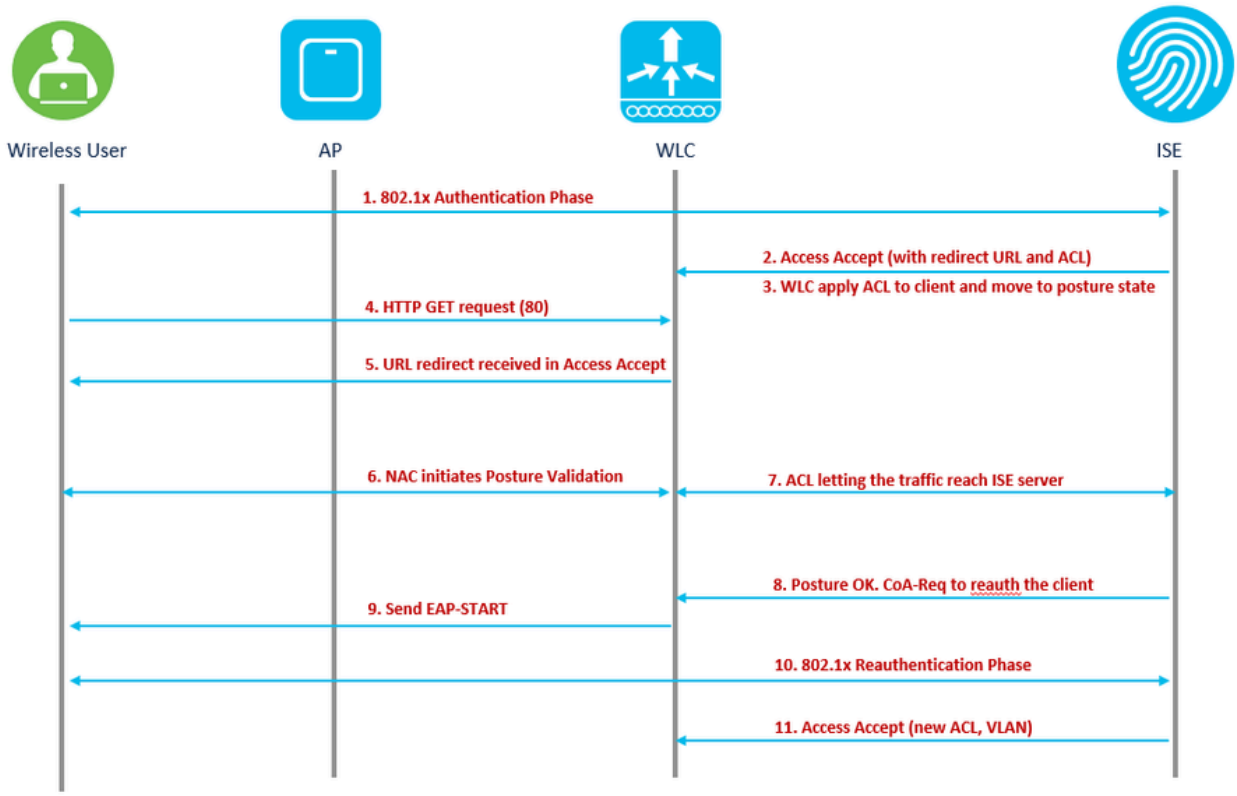
6. Una vez que el cliente de ISE completa la evaluación, se envía una petición de CoA de RADIUS con el servicio de reautenticación al WLC. Esto inicia la reautenticación del cliente (mediante el envío de EAP-START). Una vez que la reautenticación se realiza correctamente, ISE envía la aceptación de acceso con una nueva ACL (si la hay) y sin redirección de URL ni acceso a VLAN.

7. El WLC tiene soporte para CoA-Req y Disconnect-Req según RFC 3576. El WLC necesita soportar CoA-Req para el servicio de reautenticación, según RFC 5176.

8. En lugar de ACL descargables, las ACL preconfiguradas se utilizan en el WLC. El servidor ISE envía simplemente el nombre de ACL, que ya está configurado en el controlador.

9. Este diseño funciona para ambos casos de VLAN y ACL. En caso de anulación de VLAN, simplemente redirigimos el puerto 80 y permite el resto (bridge) del tráfico en la VLAN de cuarentena. Para la ACL, se aplica la ACL previa a la autenticación recibida en la aceptación de acceso.

Esta figura proporciona una representación visual de este flujo de funciones:



flujo de trabajo de funciones

Para este caso práctico, un SSID que solo se utiliza para usuarios corporativos está habilitado para el estado. No existen otros casos prácticos, como BYOD, Invitado o cualquier otro en este SSID.

Cuando un cliente inalámbrico se conecta al SSID de postura por primera vez, debe descargar e instalar el módulo de postura en el portal redirigido de ISE y, por último, debe aplicarse con las ACL relevantes en función del resultado de la comprobación de postura (Conforme/No conforme).

Configurar

Diagrama de la red

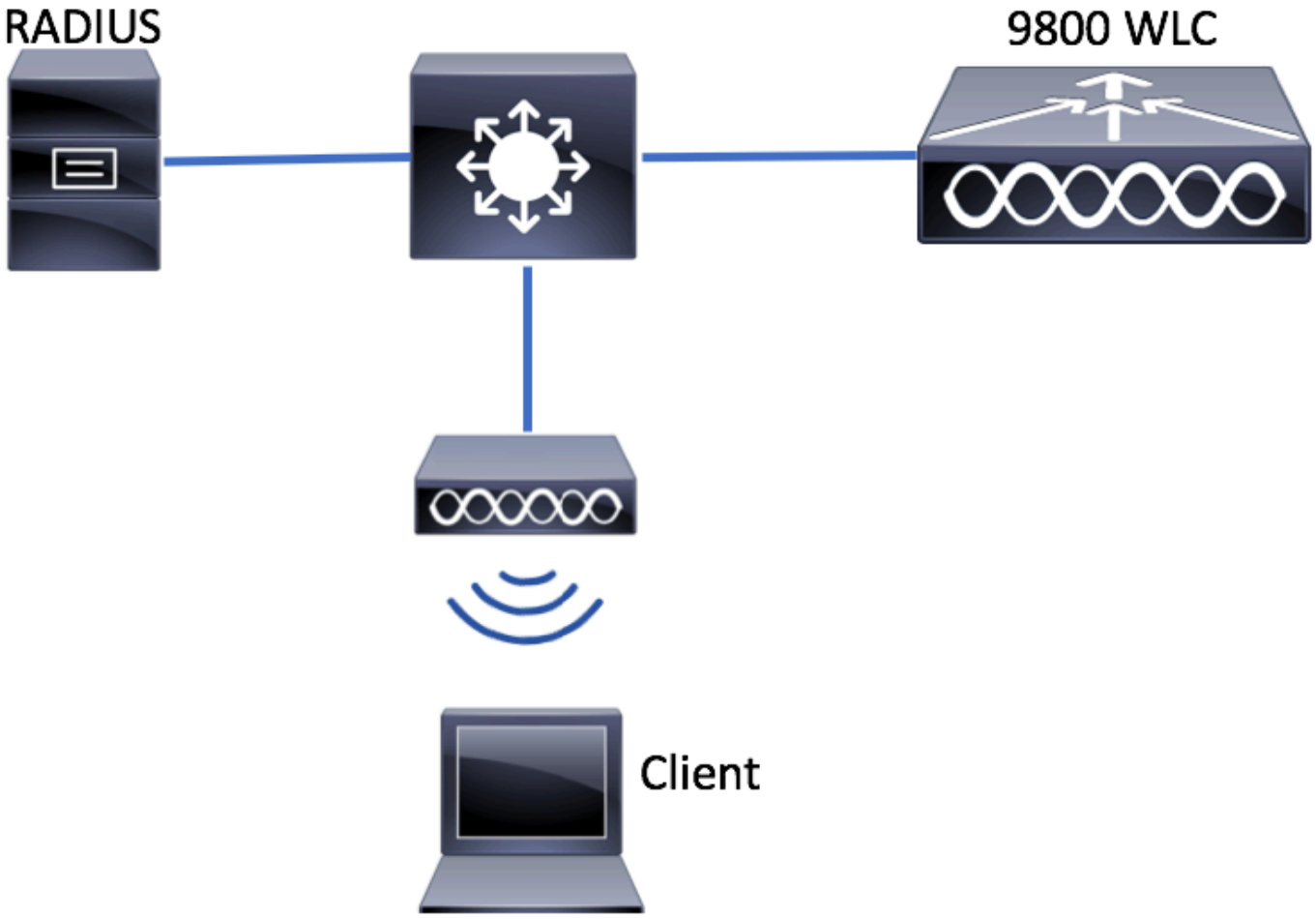
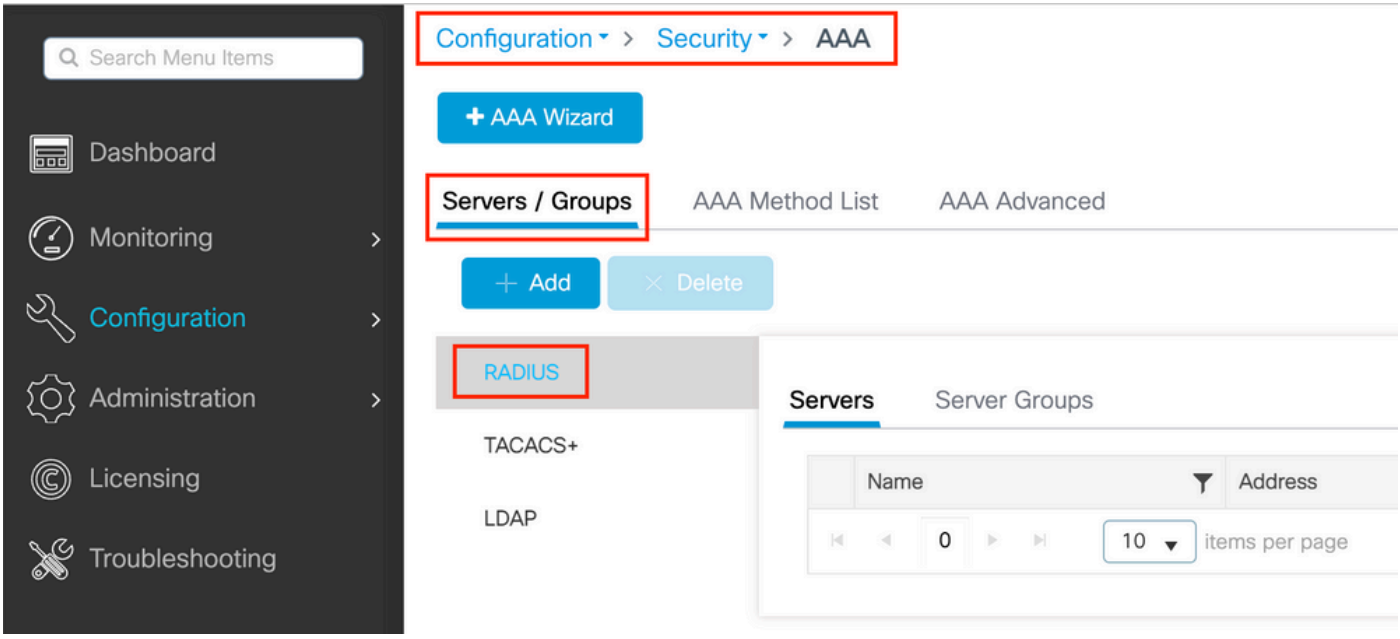


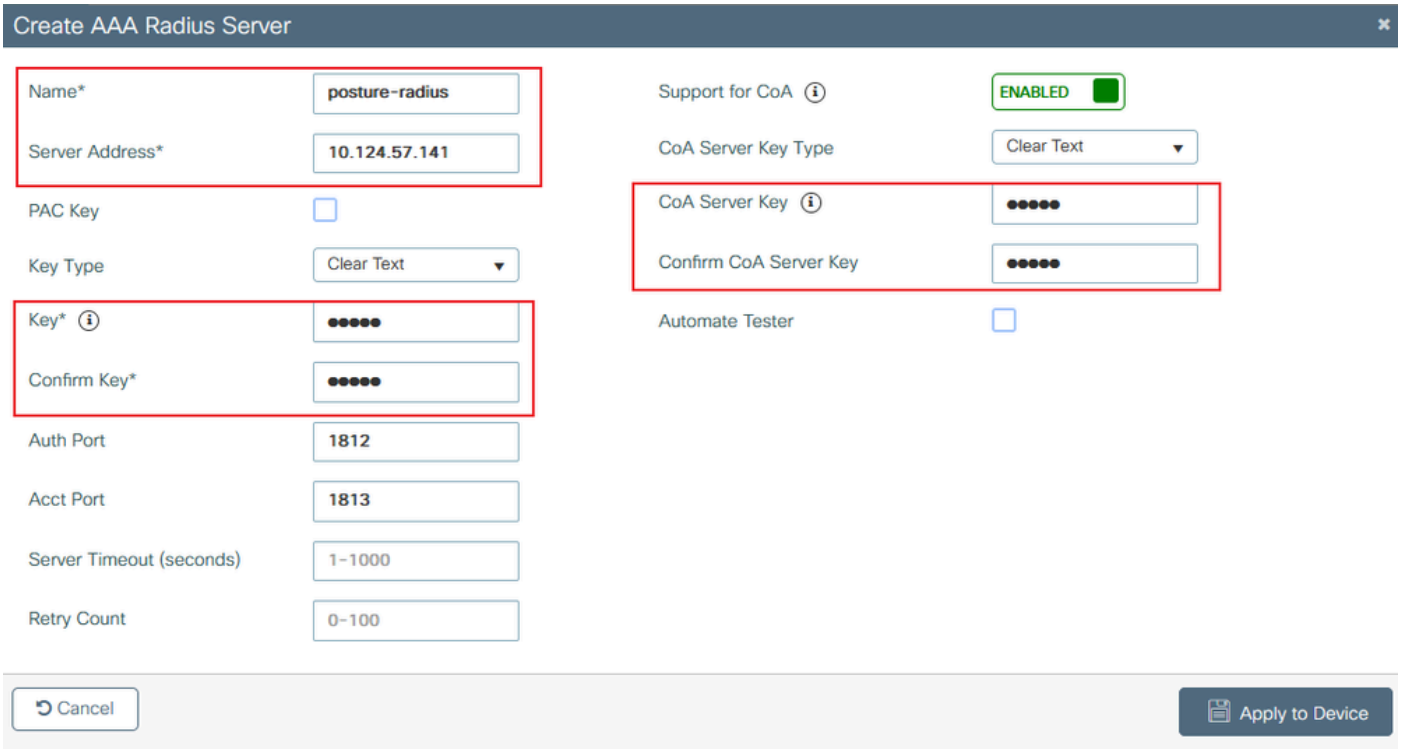
Diagrama de la red

Configuración de AAA en WLC 9800

Paso 1. Agregue el servidor ISE a la configuración del WLC 9800. Navegue hasta Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > + Add e ingrese la información del servidor RADIUS como se muestra en las imágenes. Asegúrese de que la compatibilidad con CoA está habilitada para NAC de estado.

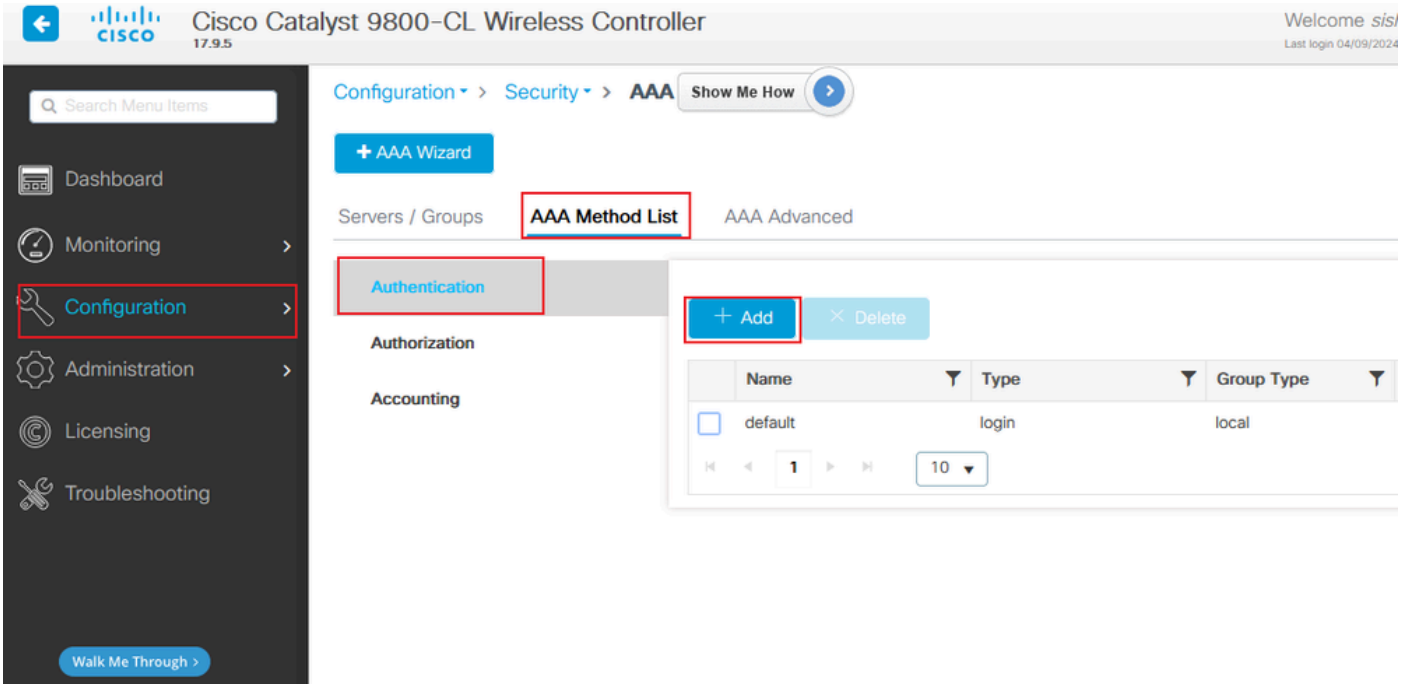


9800 crear servidor RADIUS

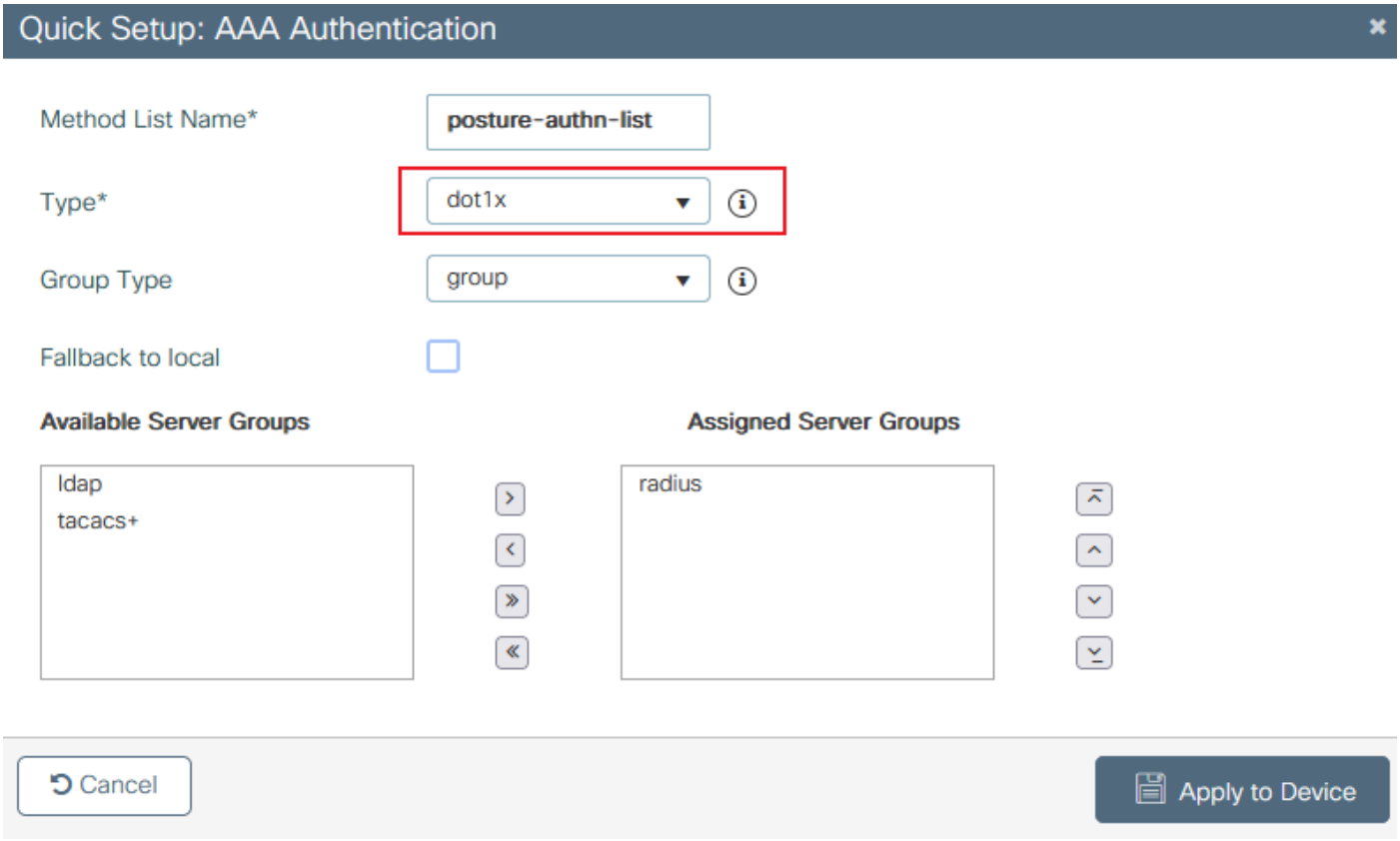


9800 crear detalles de RADIUS

Paso 2. Cree una lista de métodos de autenticación. Vaya a Configuration > Security > AAA > AAA Method List > Authentication > + Add como se muestra en la imagen:

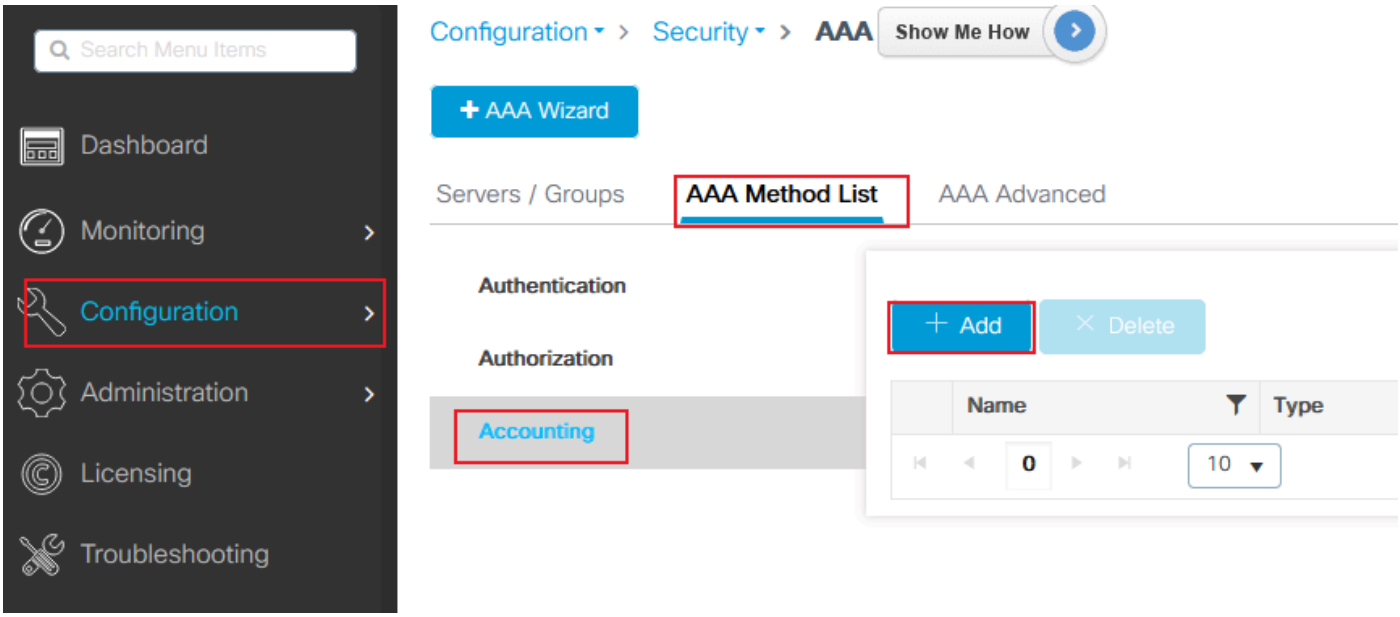


9800 agregar lista de autenticación

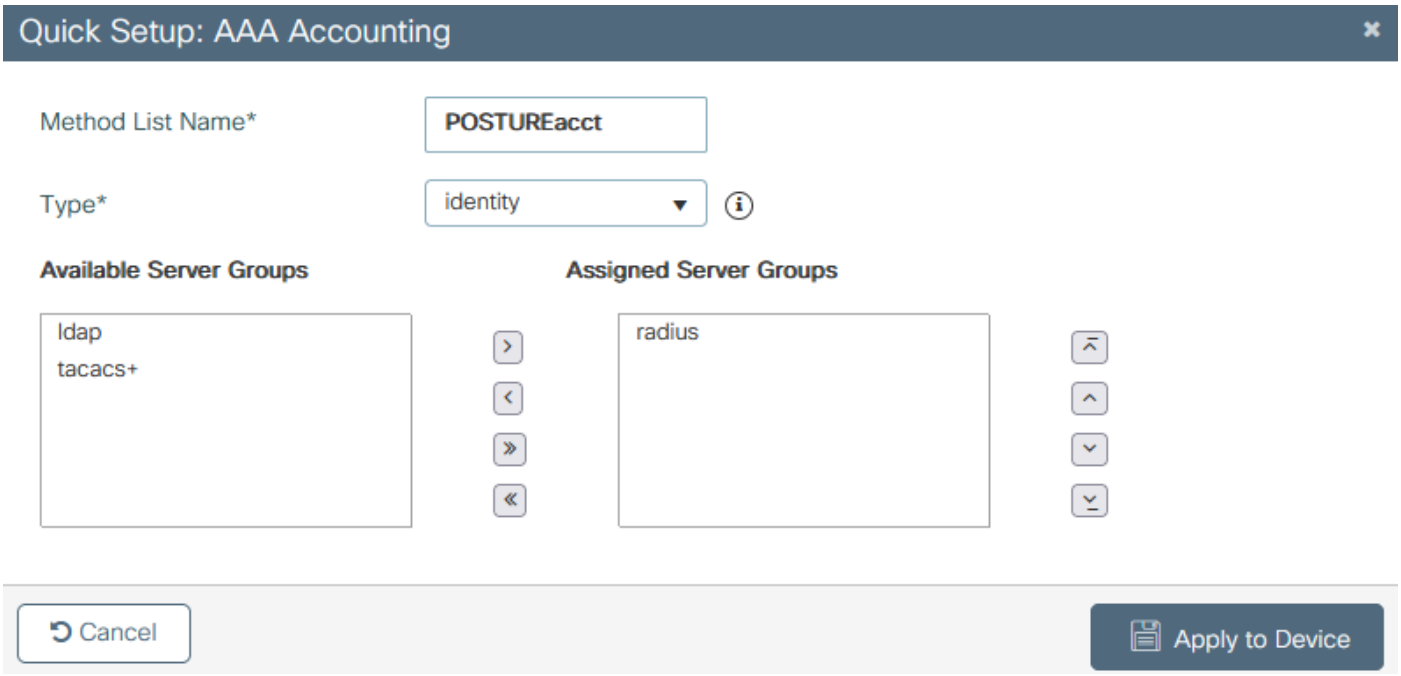


9800 crear detalles de lista de autenticación

Paso 3. (Opcional) Cree una lista de métodos de contabilidad como se muestra en la imagen:



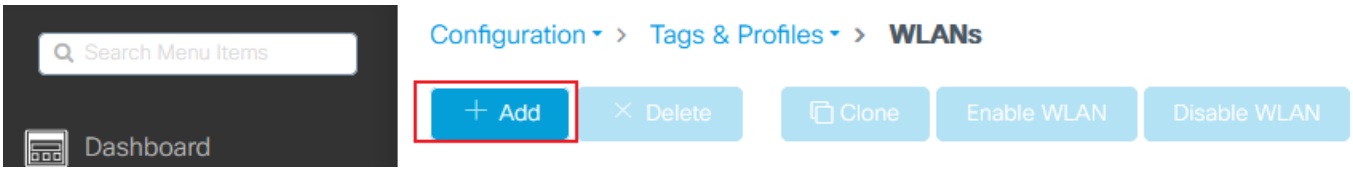
9800 agregar lista de cuentas



9800 crear detalles de la lista de cuentas

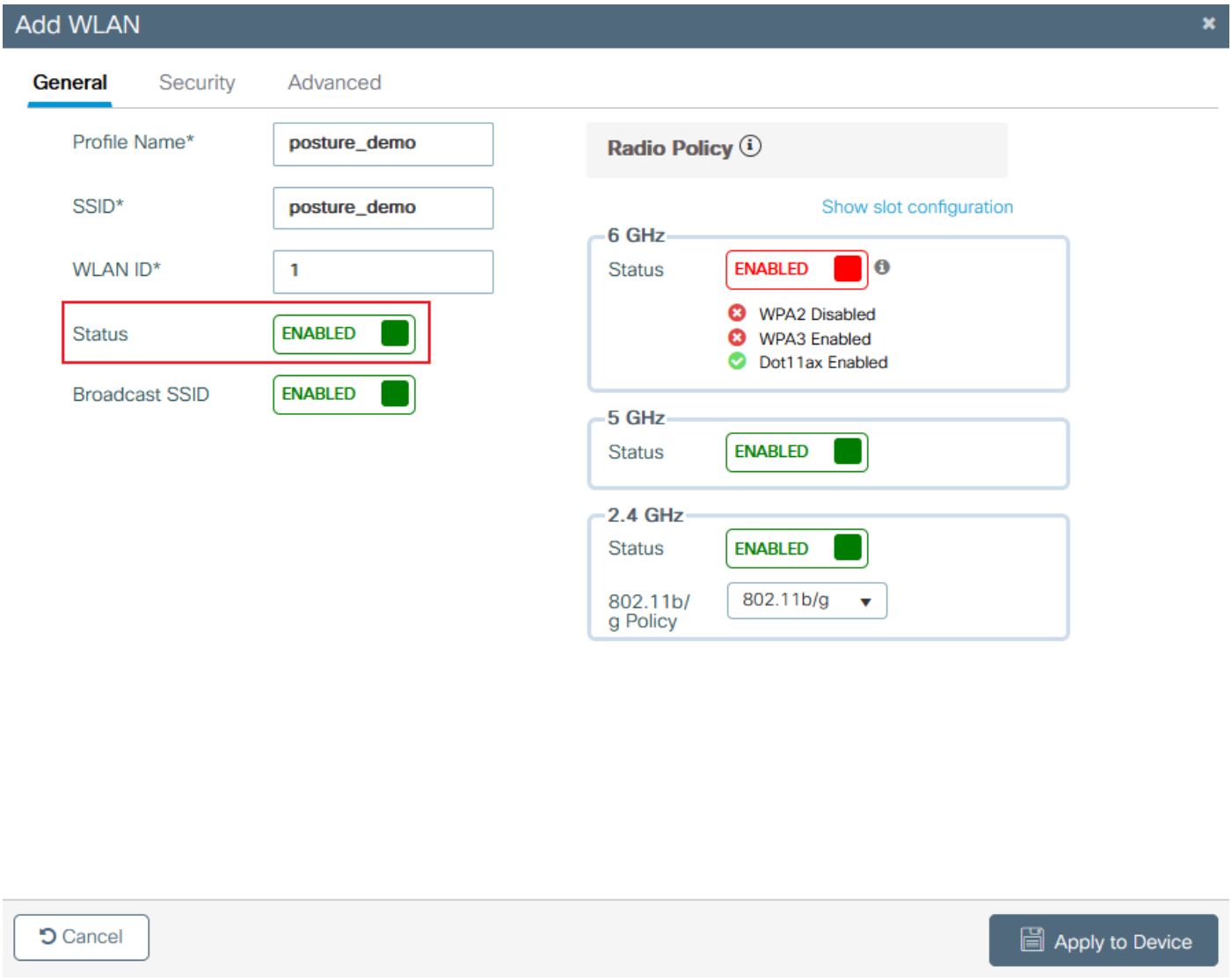
Configuración de WLAN

Paso 1. Cree la WLAN. Vaya a Configuration > Tags & Profiles > WLANs > + Add y configure la red según sea necesario:



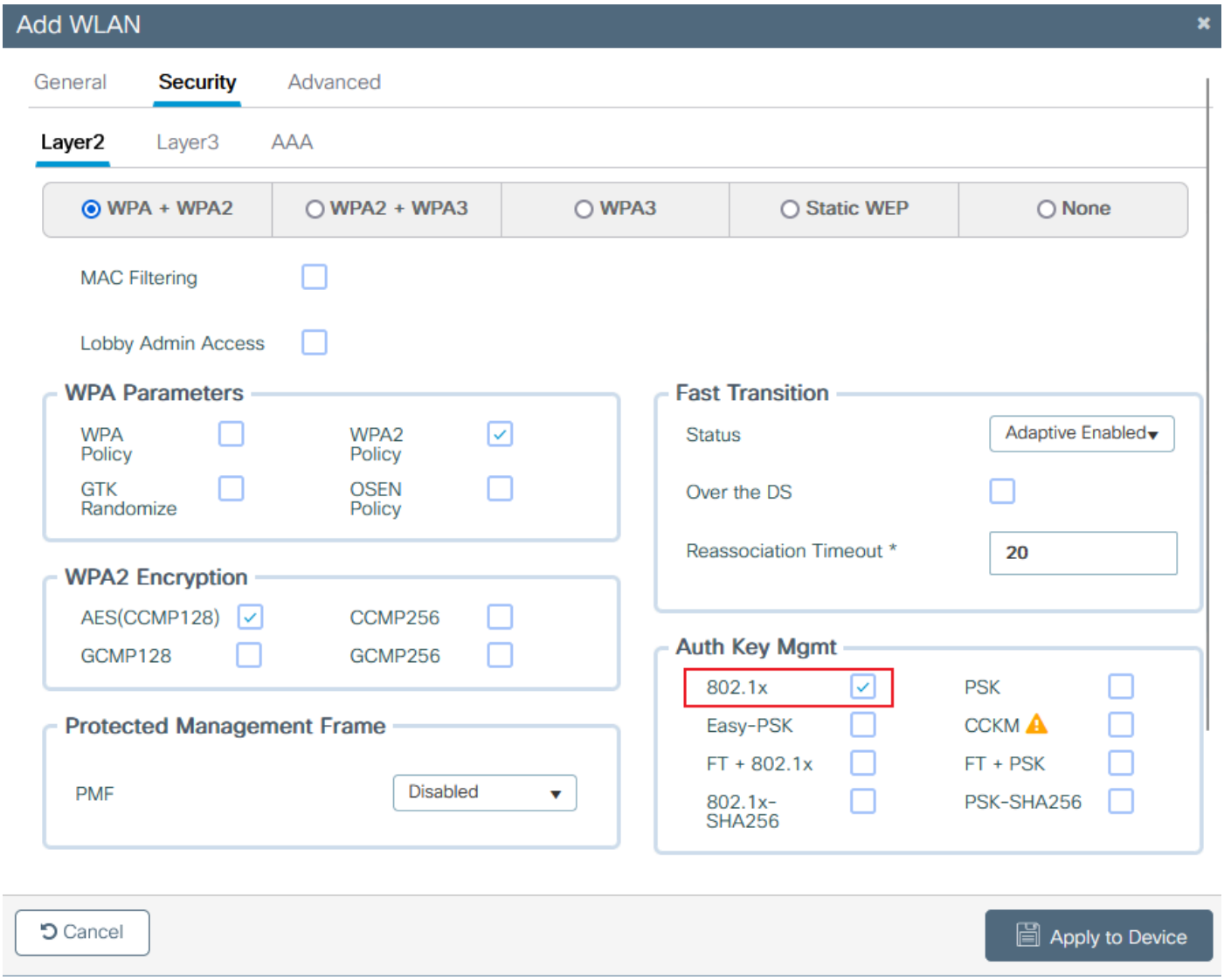
9800 WLAN add

Paso 2. Introduzca la información general de WLAN.

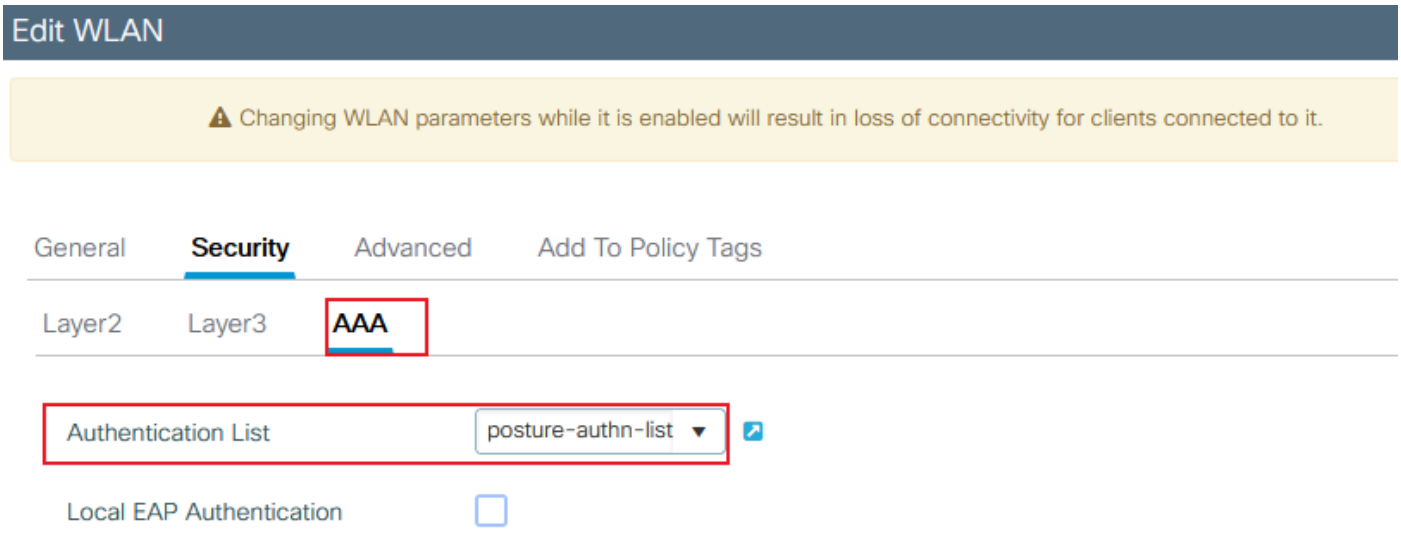


9800 crear WLAN general

Paso 3. Navegue hasta la pestaña Seguridad y elija el método de seguridad necesario. En este caso, elija '802.1x' y la lista de autenticación AAA (que creó en el Paso 2. en la sección Configuración AAA) son necesarias:



9800 crear seguridad WLAN L2

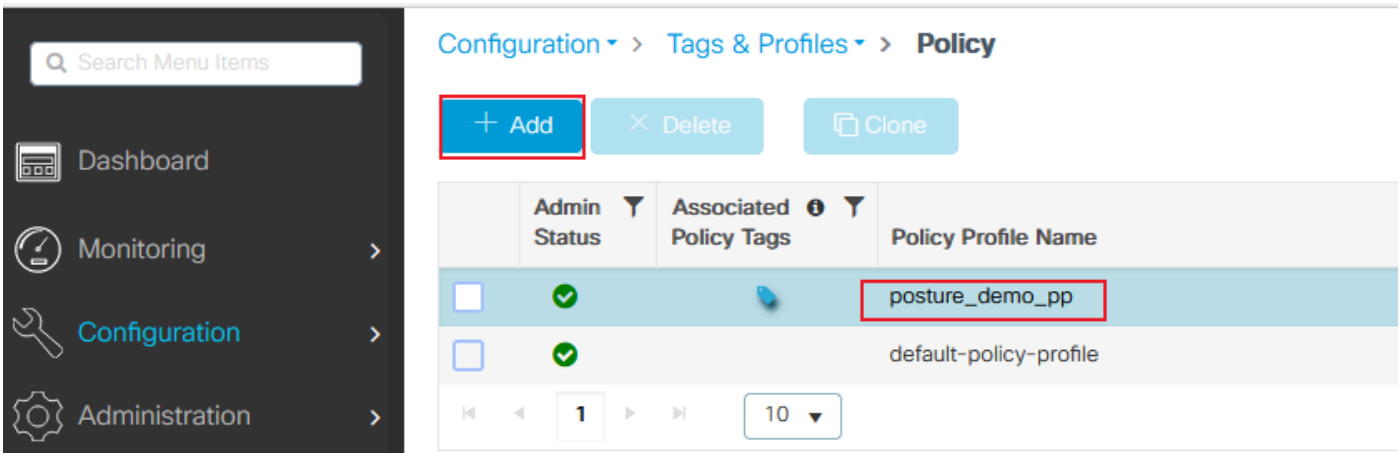


9800 crear seguridad WLAN AAA

Configuración del perfil de la política

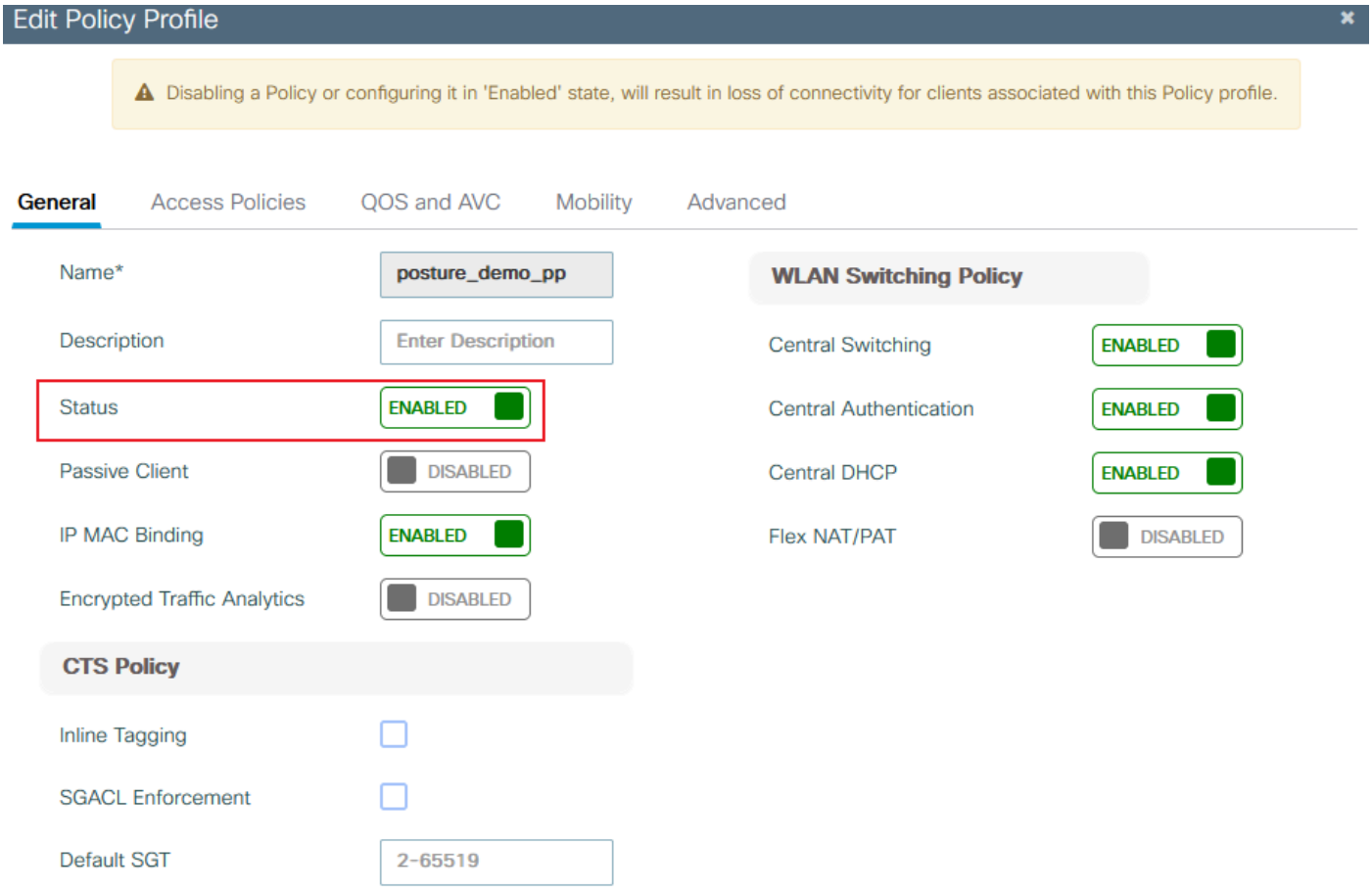
Dentro de un perfil de política, puede decidir asignar los clientes a los que se aplicará la VLAN, entre otras configuraciones (como la lista de controles de acceso (ACL), la calidad de servicio (QoS), el ancla de movilidad, los temporizadores, etc.). Puede utilizar su perfil de política predeterminado o puede crear uno nuevo.

Paso 1. Crear un nuevo perfil de política. Navegue hasta Configuration > Tags & Profiles > Policy y cree uno nuevo:



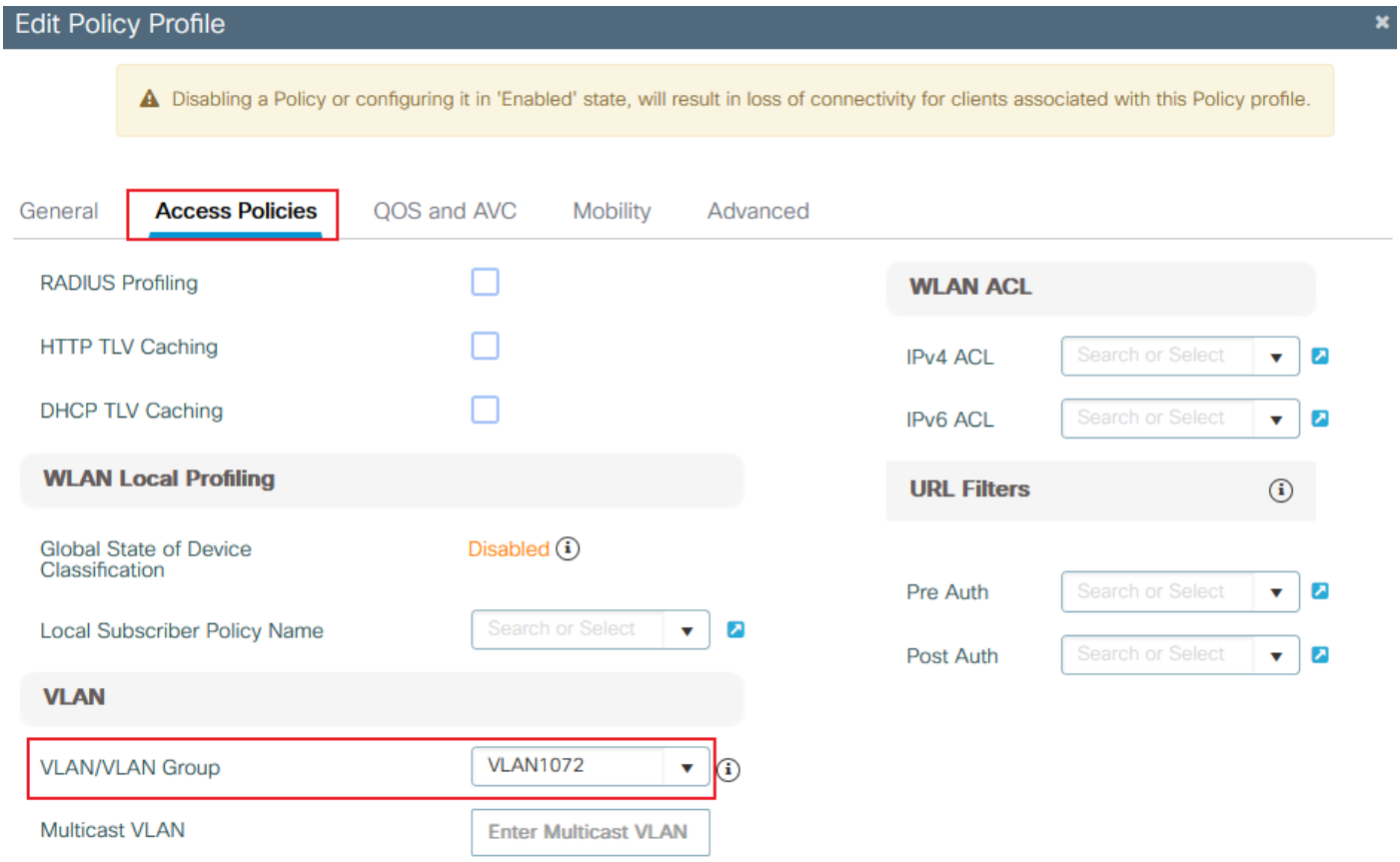
9800 agregar perfil de directiva

Asegúrese de que el perfil esté habilitado.



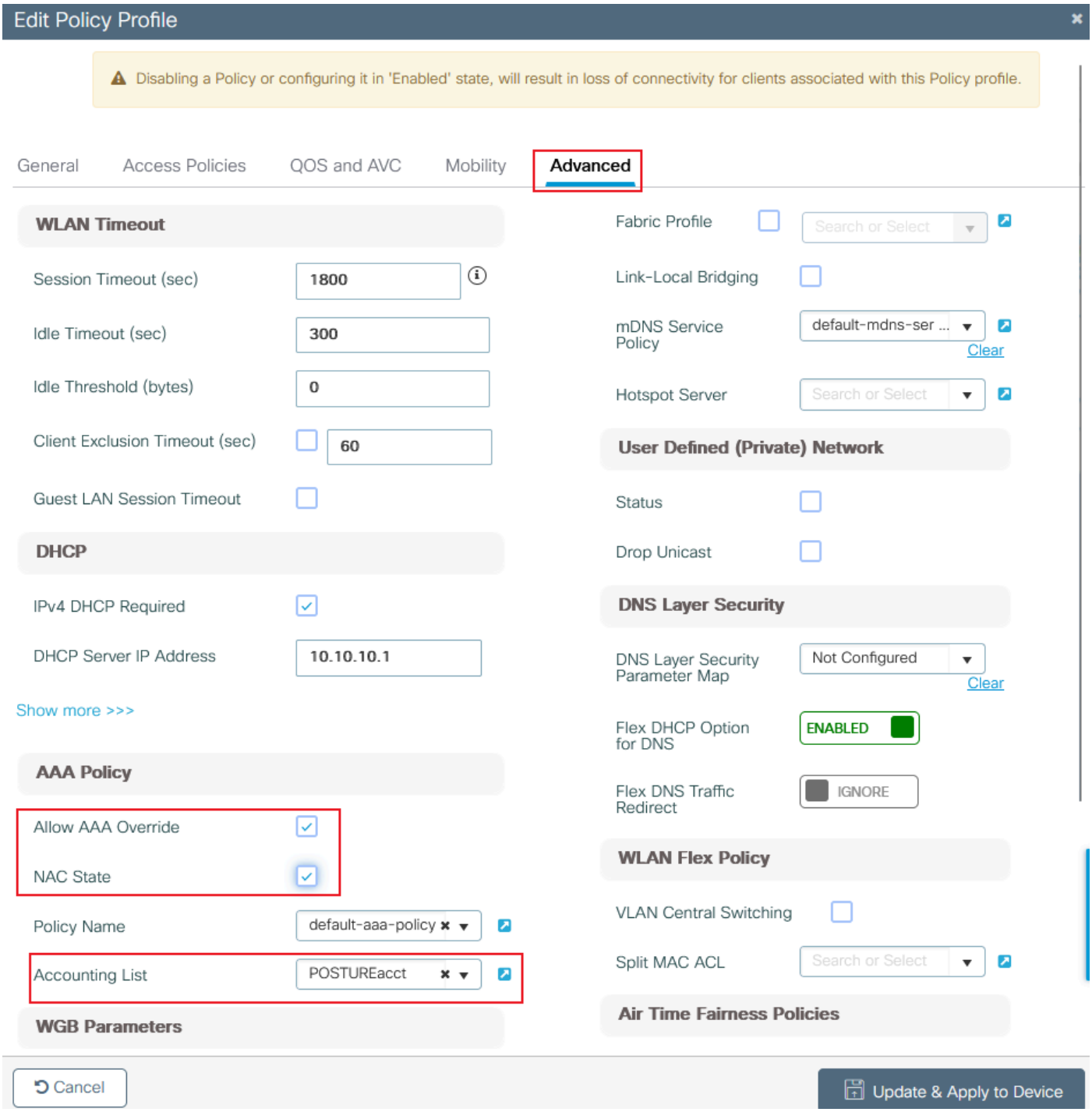
9800 crear perfil de políticas general

Paso 2. Elija la VLAN. Navegue hasta la pestaña Access Policies y elija el nombre de la VLAN en la lista desplegable o escriba manualmente el VLAN-ID. No configure una ACL en el perfil de política:



9800 crear perfil de política VLAN

Paso 3. Configure el perfil de políticas para aceptar anulaciones de ISE (permitir la sustitución de AAA) y el cambio de autorización (CoA) (estado de NAC). Opcionalmente, también puede especificar un método de contabilidad:

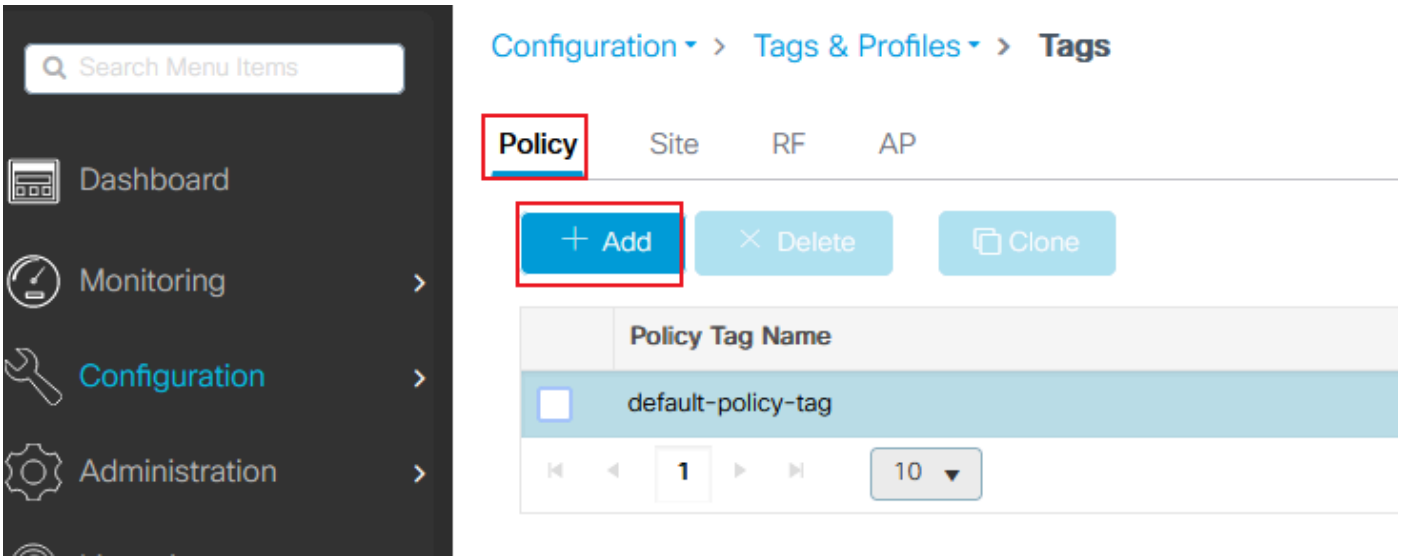


9800 crear perfil de políticas Avance

Configuración de etiquetas de políticas

Dentro de la etiqueta de política se encuentra el enlace del SSID con el perfil de política. Puede crear una nueva etiqueta de política o utilizar la etiqueta de política predeterminada.

Navegue hasta Configuration > Tags & Profiles > Tags > Policy y agregue uno nuevo si es necesario, como se muestra en la imagen:



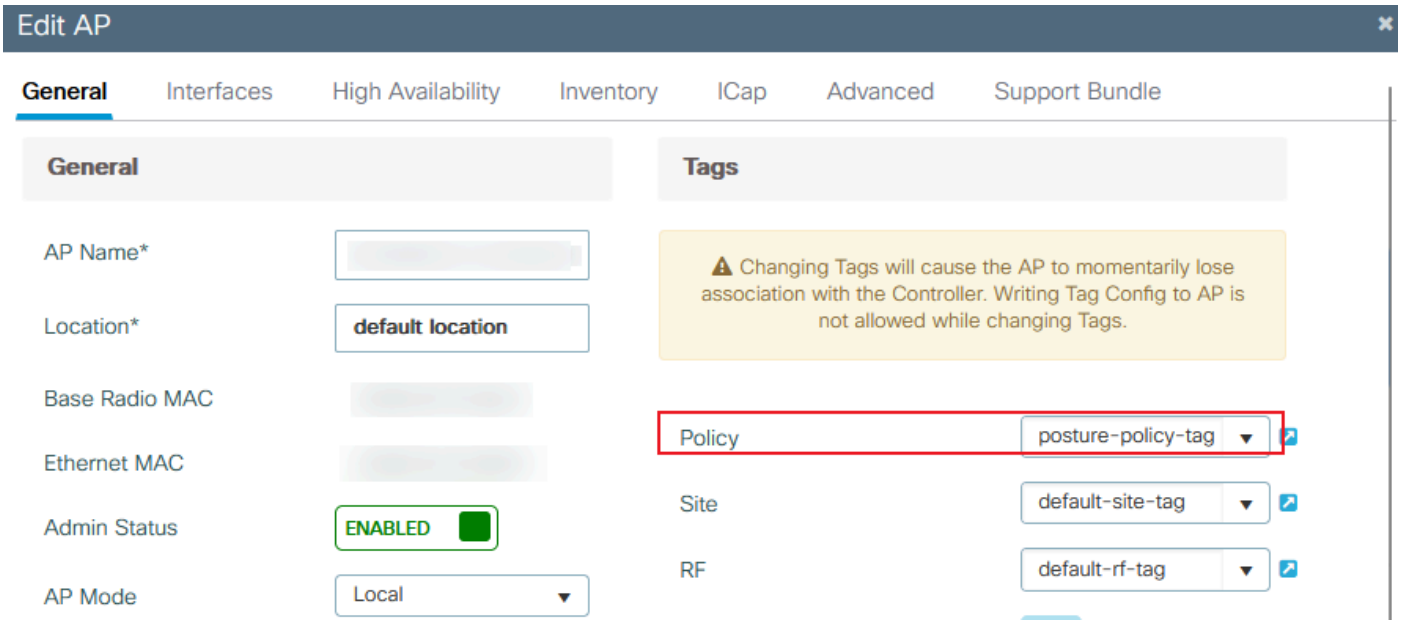
9800 etiqueta de política add

Vincule su perfil de WLAN con el perfil de política deseado:

Detalles de la etiqueta de política 9800

Asignación de etiquetas de políticas

Asigne la etiqueta de política a los AP necesarios. Navegue hasta Configuration > Wireless > Access Points > AP Name > General Tags , realice la asignación necesaria y luego haga clic en Update & Apply to Device .



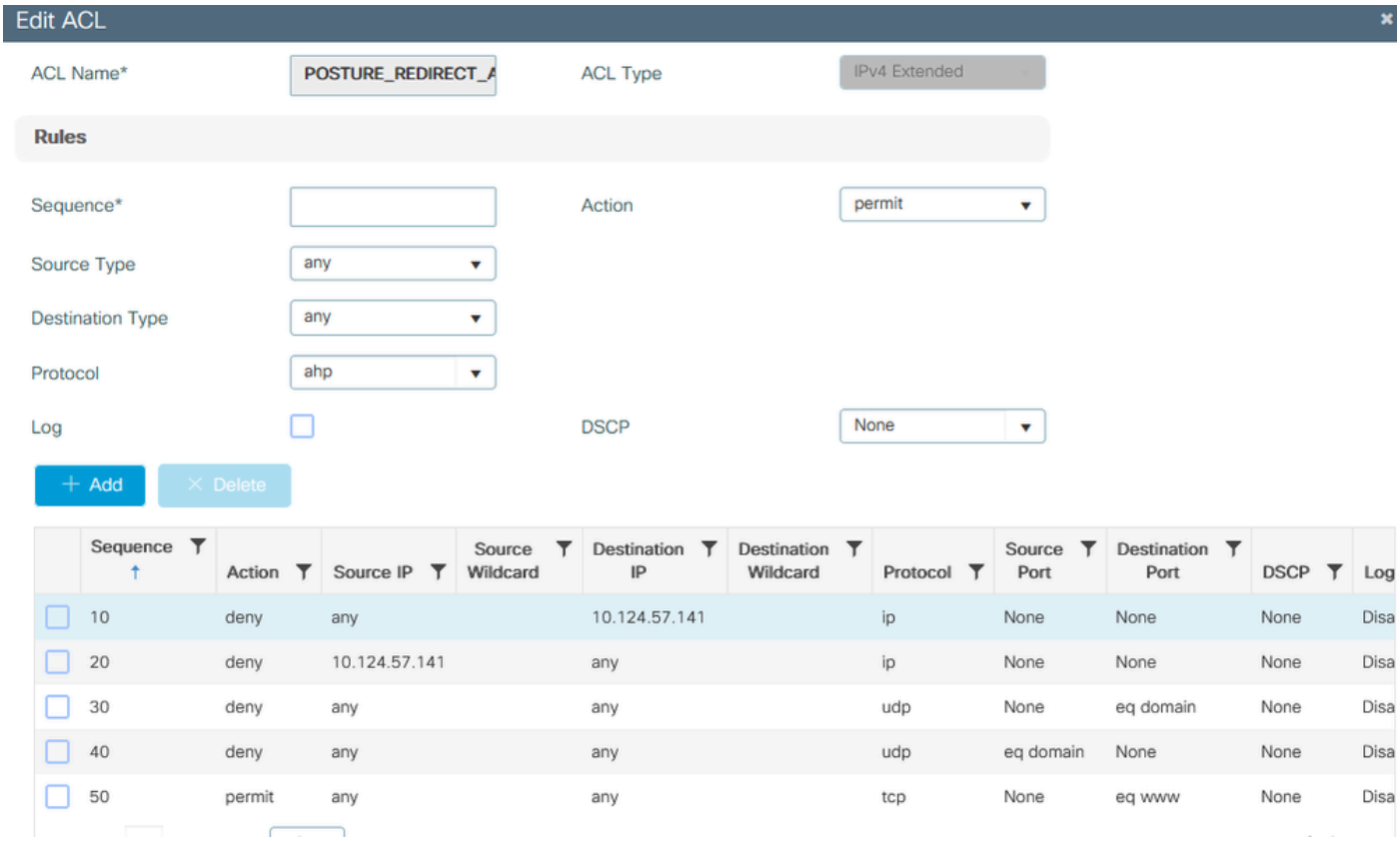
Asignación de etiqueta de directiva 9800

Configuración de ACL de redireccionamiento

Vaya a Configuración > Seguridad > ACL > + Agregar para crear una nueva ACL.

La ACL utilizada para la redirección del portal de postura tiene los mismos requisitos que la CWA (autenticación web central).

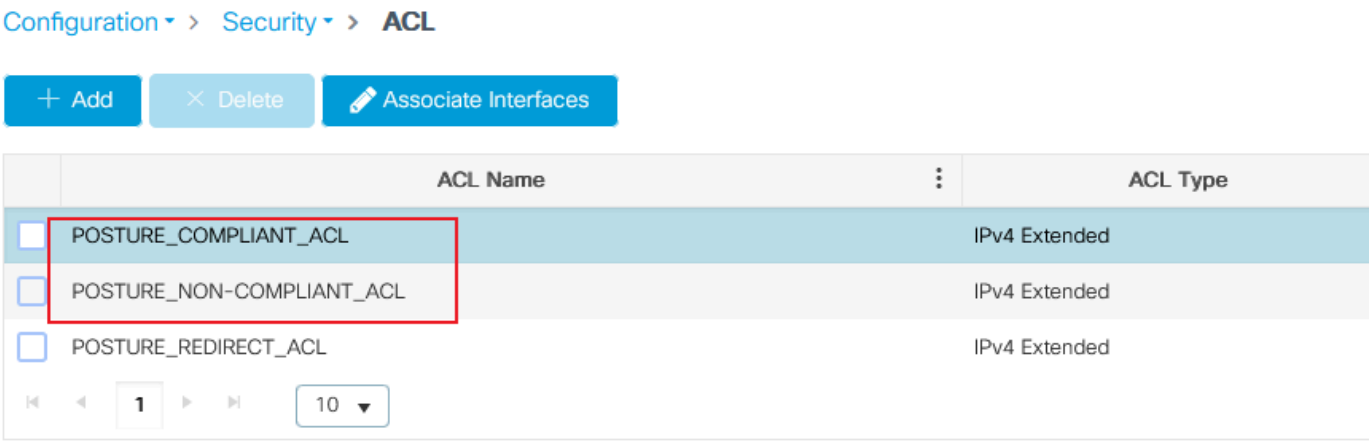
Debe denegar el tráfico a los nodos de PSN de ISE, así como también debe denegar el DNS y permitir el resto. Esta ACL de redirección no es una ACL de seguridad, sino una ACL de punt que define qué tráfico va a la CPU (en permisos) para un tratamiento adicional (como la redirección) y qué tráfico permanece en el plano de datos (en negación) y evita la redirección. La ACL debe verse de la siguiente manera (reemplace 10.124.57.141 con su dirección IP de ISE en este ejemplo):



Detalles de ACL de redirección 9800

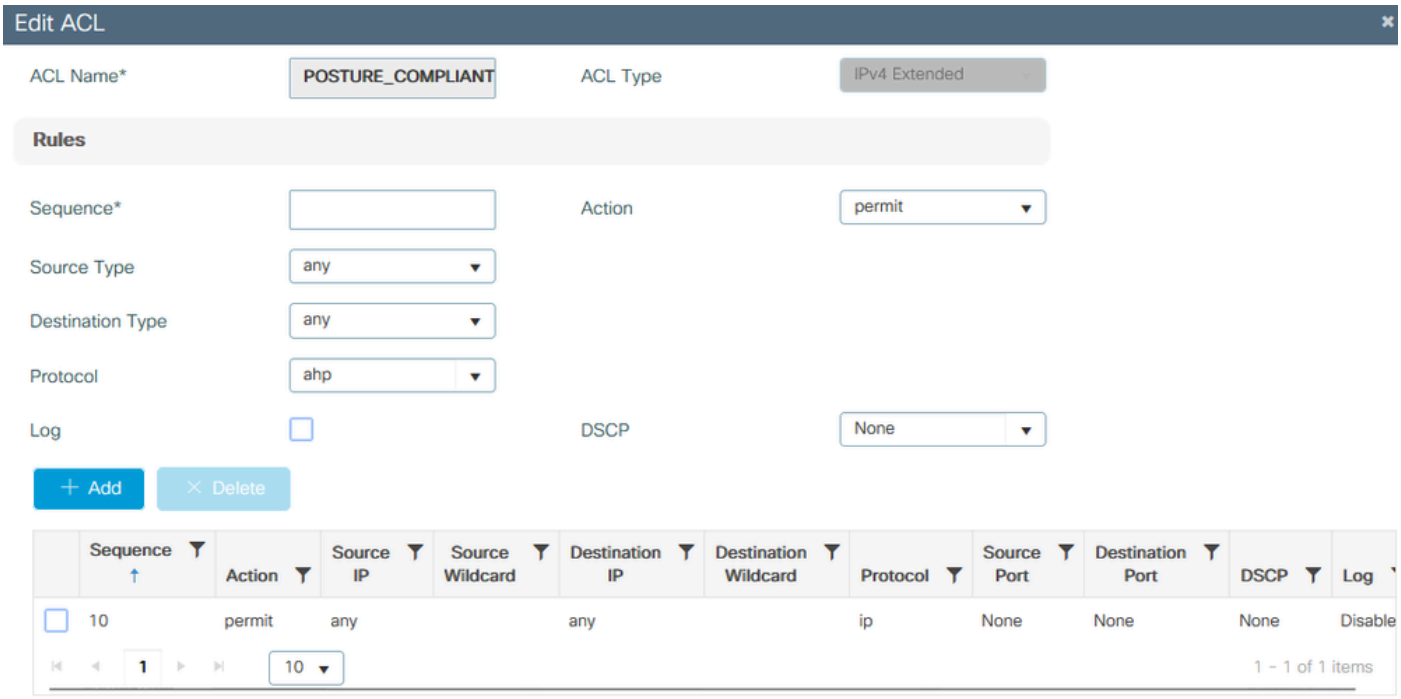
Configuración de ACL de políticas

En este caso, debe definir ACL separadas en el WLC 9800 para ISE para autorizar los escenarios de cumplimiento y no cumplimiento según el resultado de la verificación de estado.



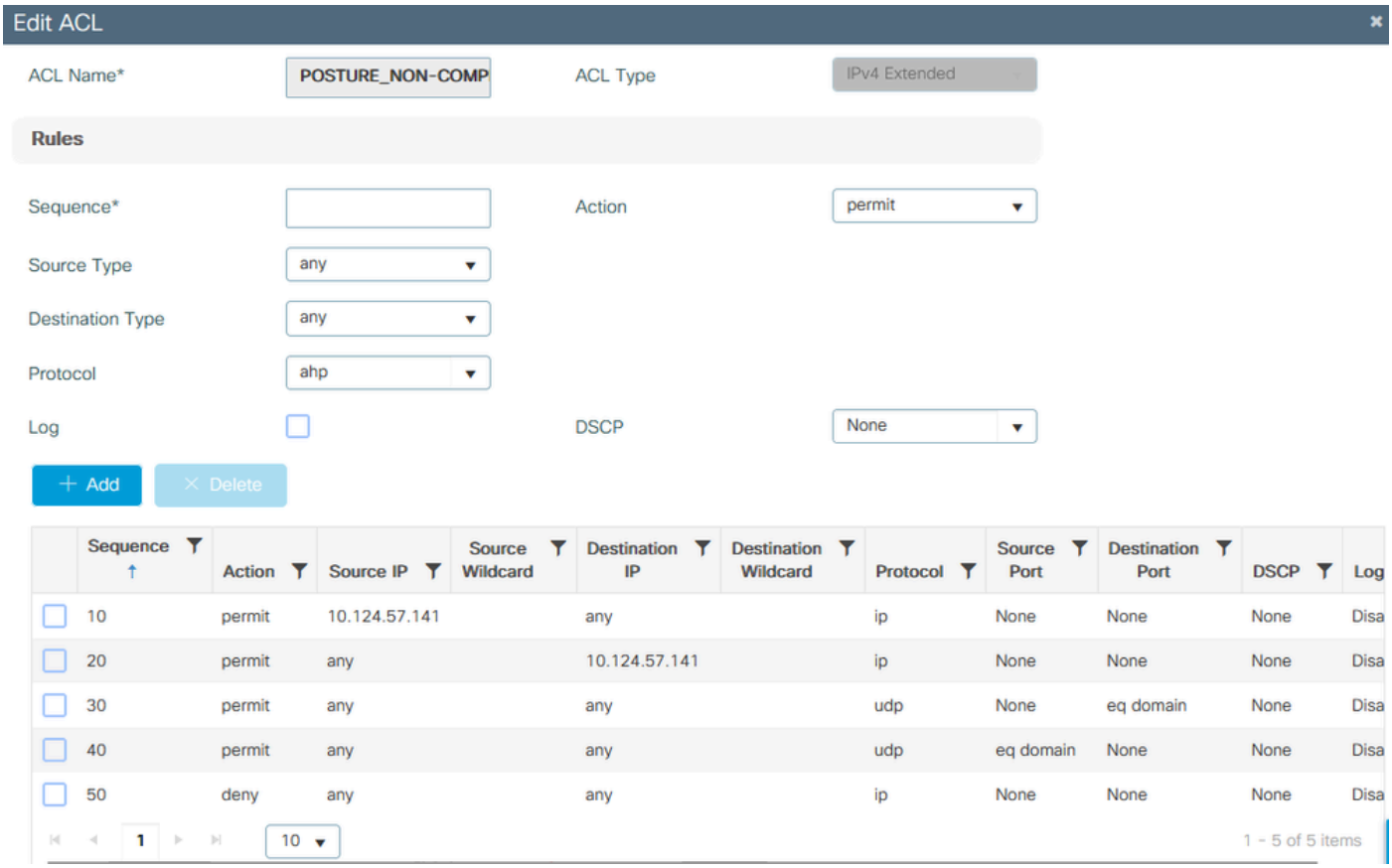
9800 ACL general

Para el escenario de conformidad, simplemente utilice permit all en este caso. Como otra configuración común, también puede hacer que ISE no autorice ninguna ACL en el resultado conforme, lo que equivale a permitir todo en el lado 9800:



Compatible con 9800 ACL

En el caso de no conformidad, el cliente solo permite el acceso a determinadas redes, normalmente el servidor de corrección (ISE en este caso):

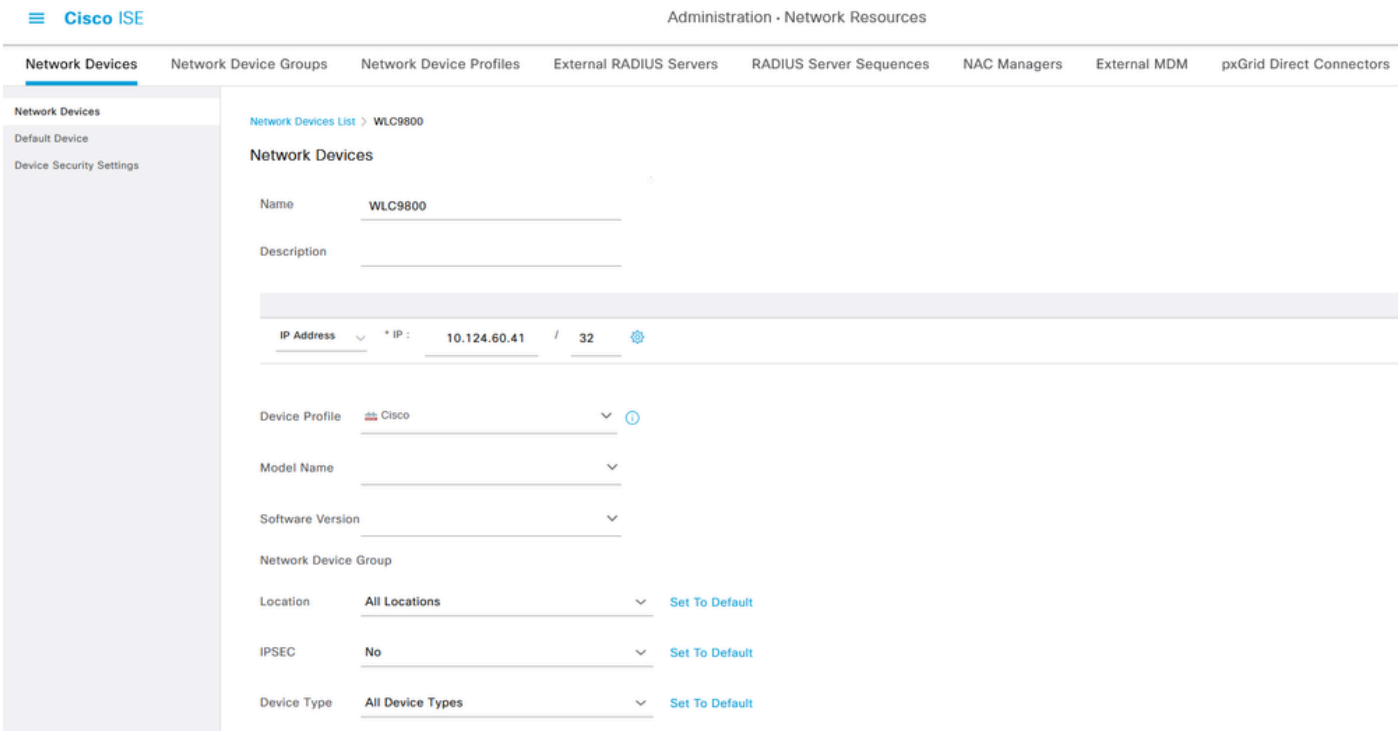


9800 ACL: no conforme

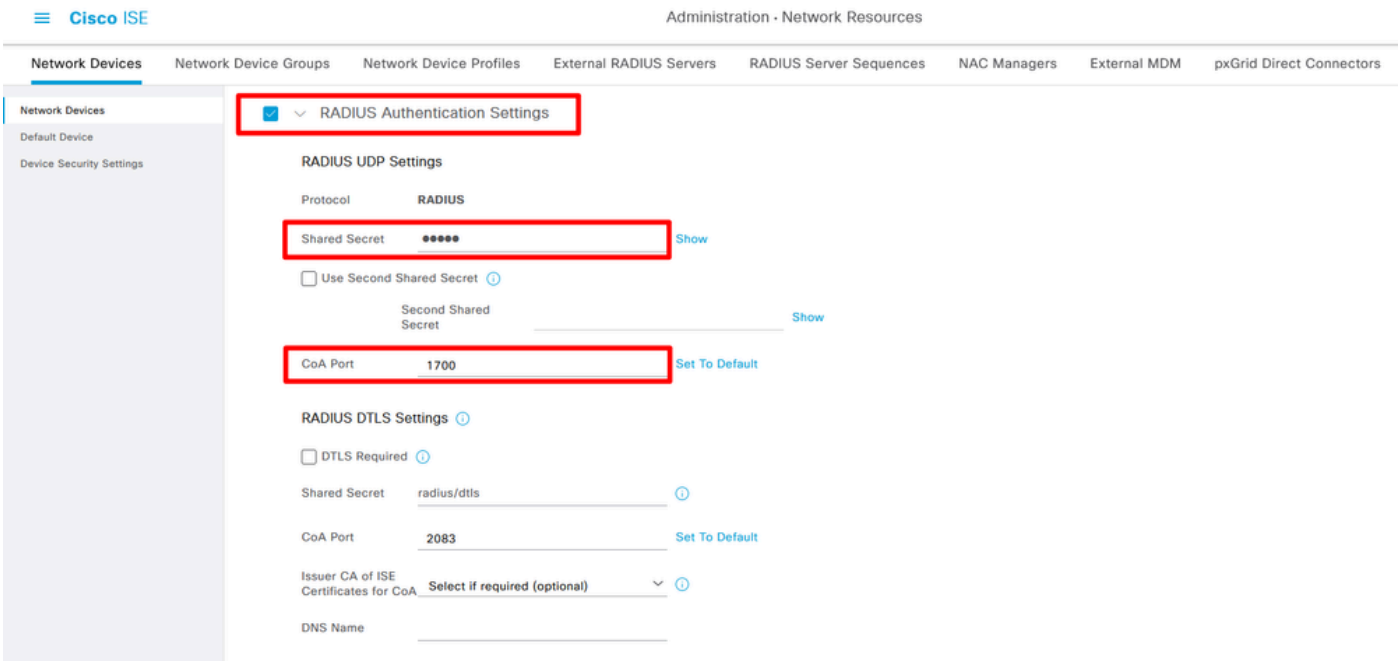
Configuración AAA y parámetro de estado en ISE

Requisito de condición: En este ejemplo, el requisito para determinar la conformidad es detectar si existe un archivo de prueba específico en el escritorio utilizado para probar Windows PC.

Paso 1. Agregue el WLC 9800 como NAD en el ISE. Vaya a Administración> Recursos de red> Dispositivos de red> Agregar:



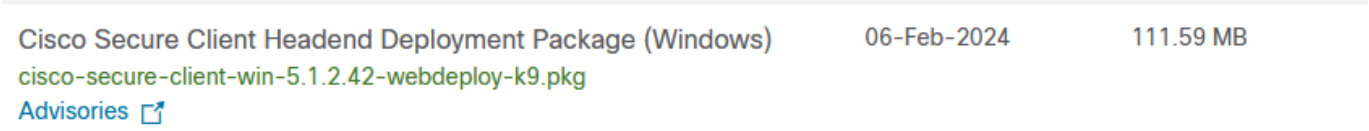
Agregar dispositivo de red 01



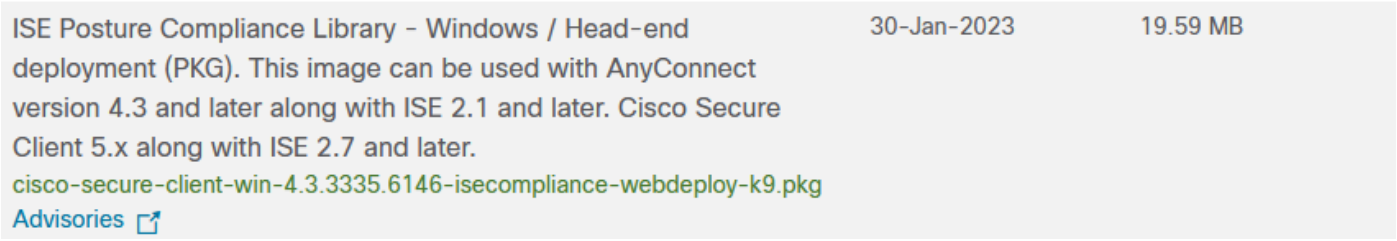
Agregar dispositivo de red 02

Paso 2. Descargue el paquete de implementación de cabecera y el módulo de cumplimiento de Cisco Secure Client en el sitio web de Cisco Software CCO.

Acceda y busque en Cisco Secure Client:

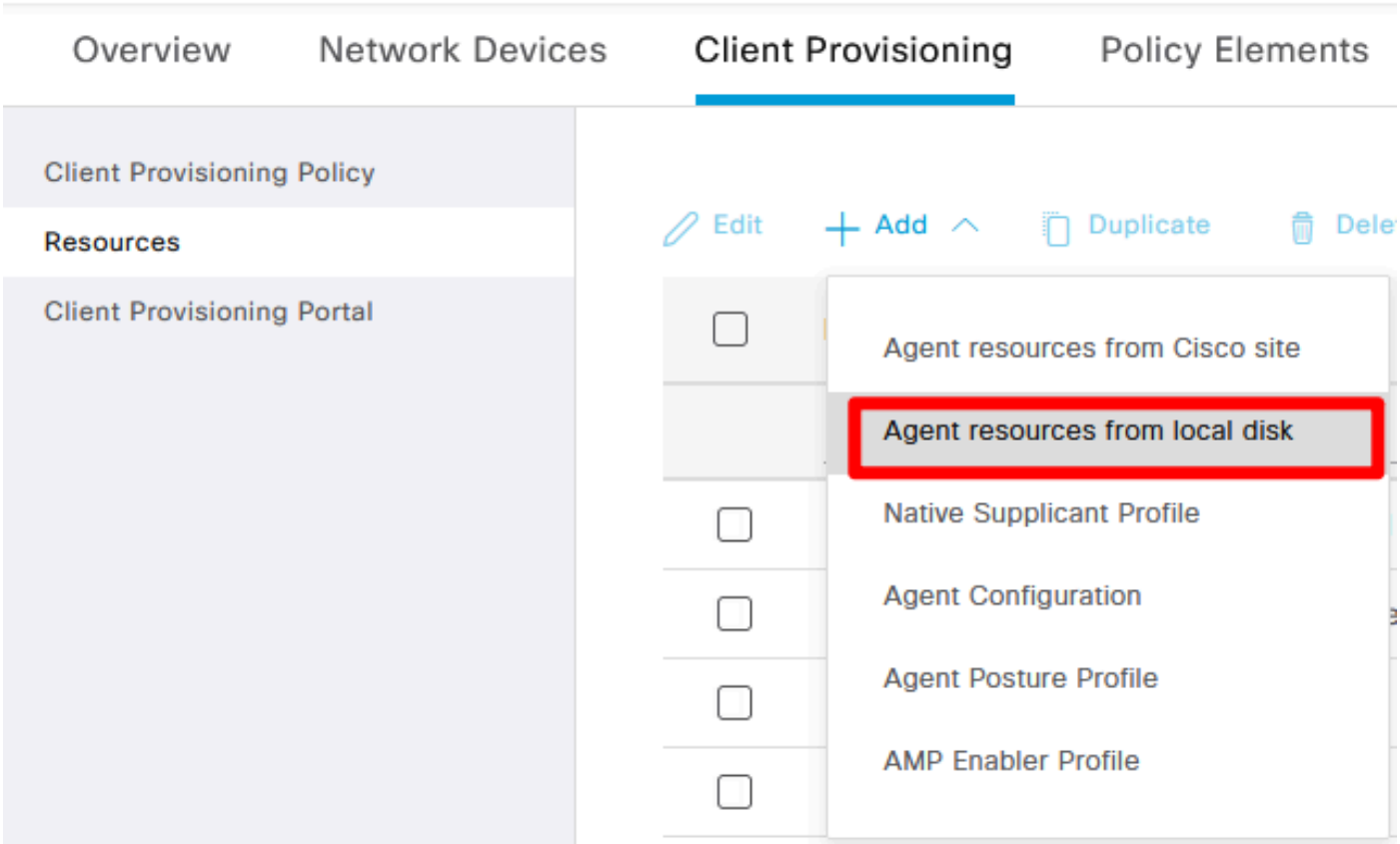


Secure Client 5.1.2.42

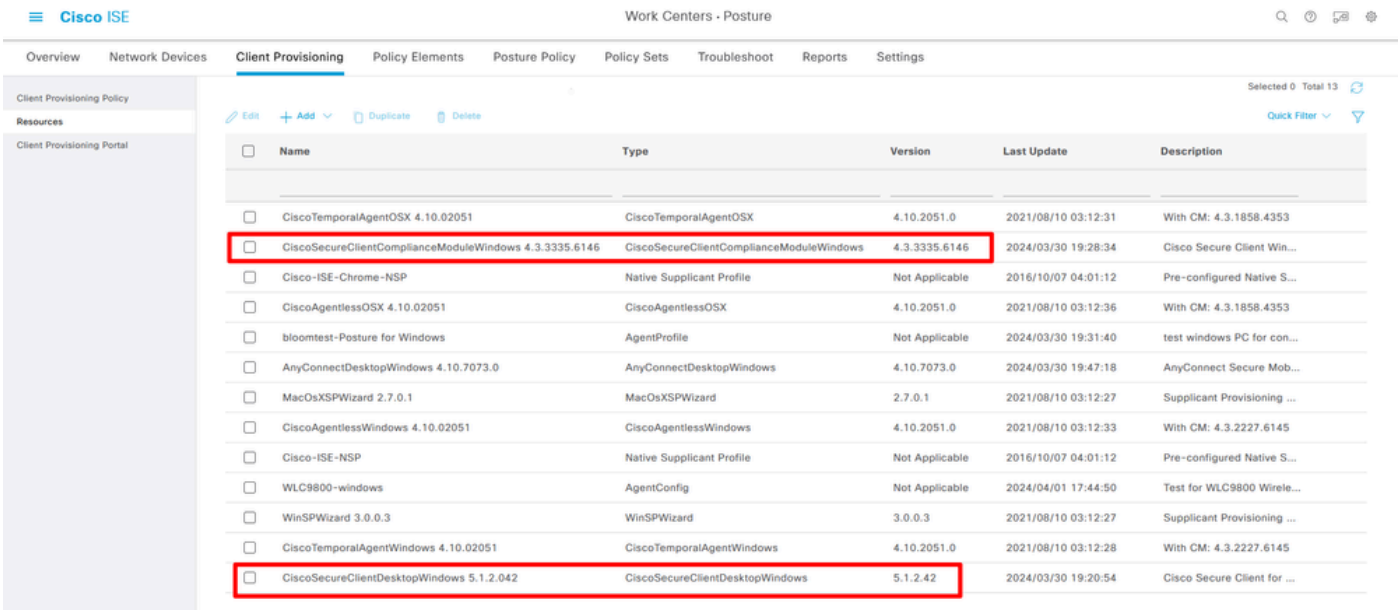


Módulo de cumplimiento de ISE 4.3

Paso 3. Cargue el paquete de implementación de cabecera de Cisco Secure Client y el paquete del módulo de cumplimiento en ISE Client Provisioning. Navegue hasta Centros de trabajo> Postura> Aprovisionamiento del cliente> Recursos . Haga clic en Agregar, Elija Recursos de agente del disco local en el cuadro desplegable:

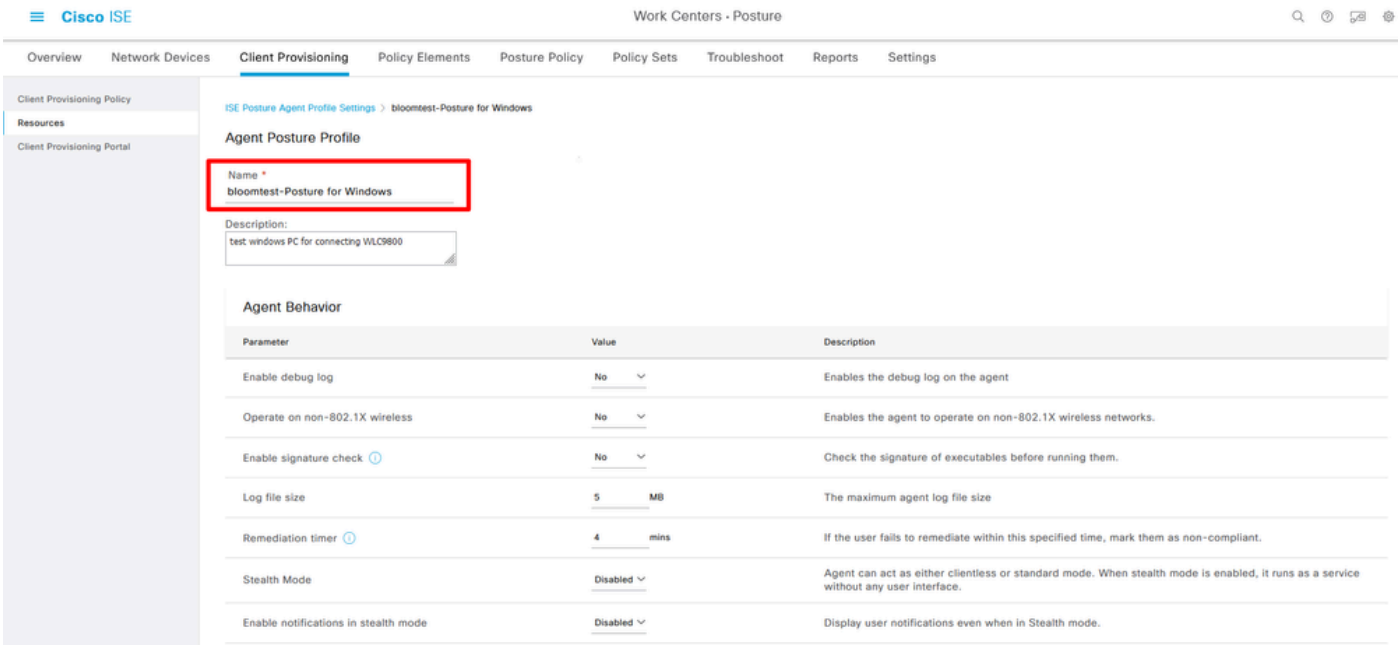


Cargar cliente seguro



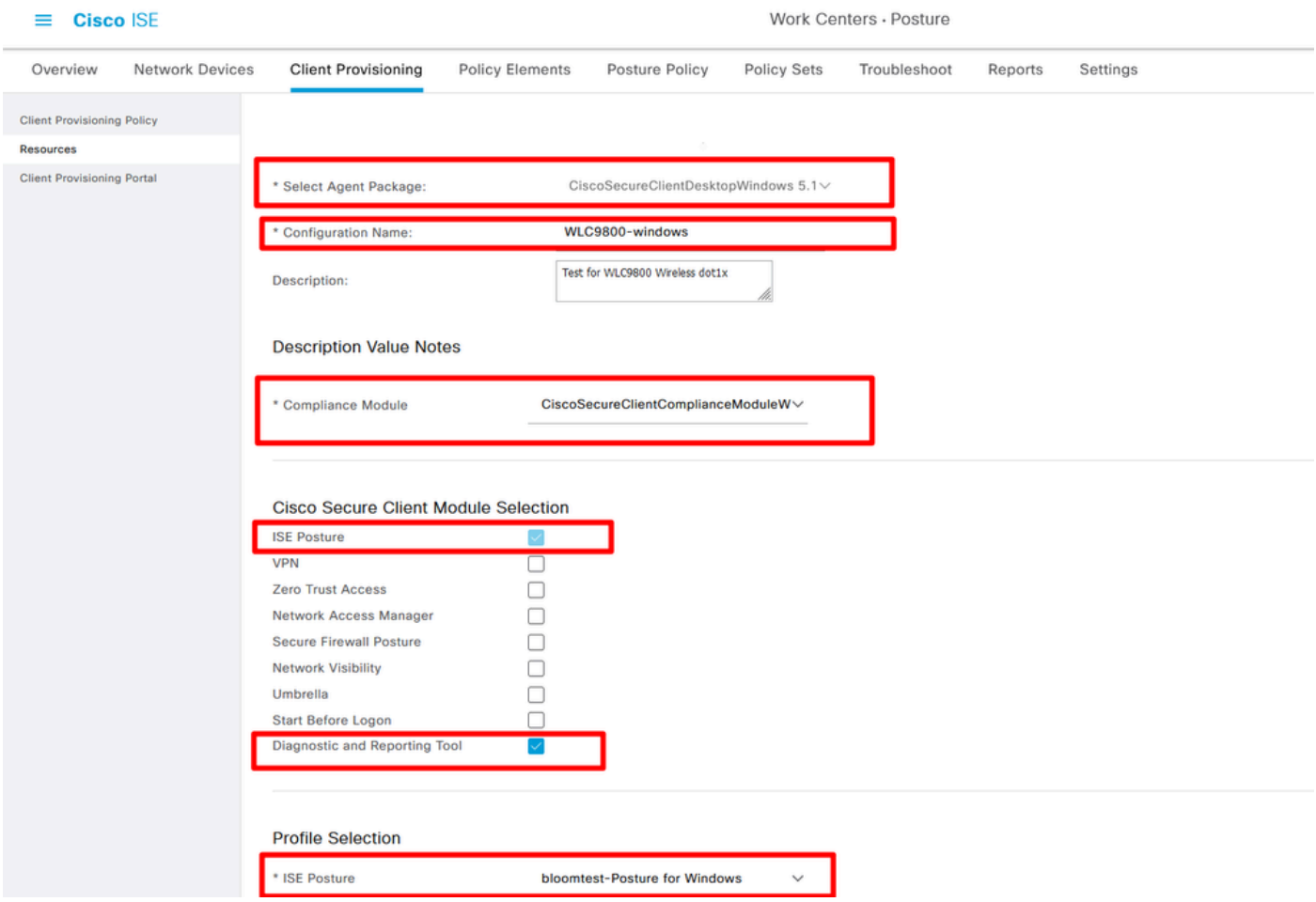
Carga de Secure Client y Compliance Module correctamente

Paso 4. Crear perfil de postura del agente Navegue hasta Centros de trabajo> Postura> Aprovisionamiento del cliente> Recursos> Agregar> Perfil de postura del agente:



Perfil de postura del agente

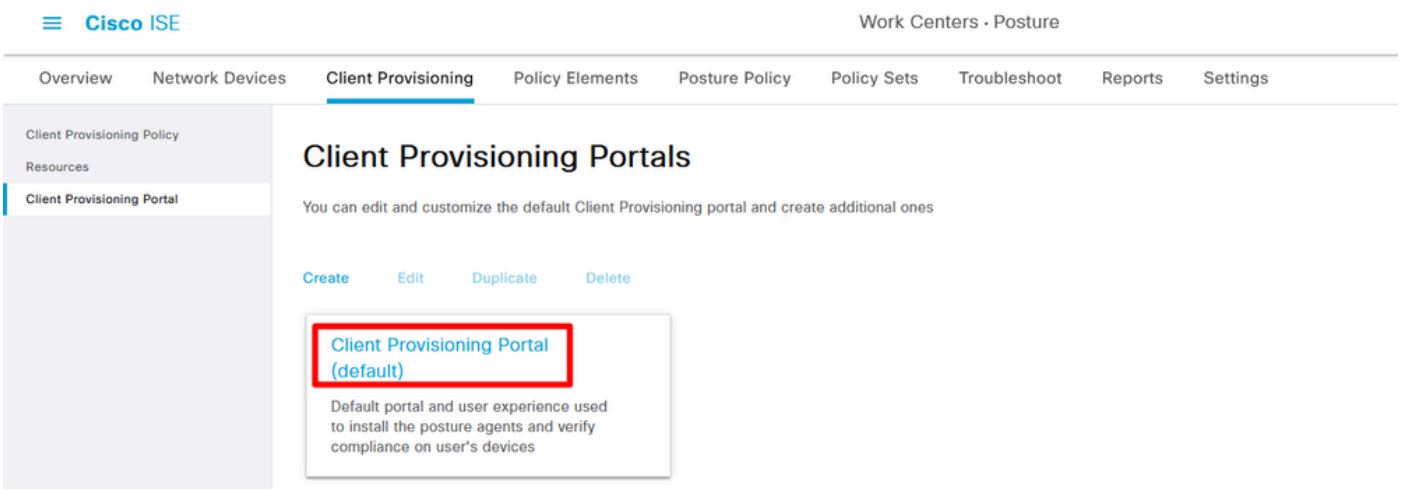
Paso 5. Crear configuración de agente Navegue hasta Centros de trabajo> Estado> Aprovisionamiento de cliente> Recursos> Agregar> Configuración de agente:



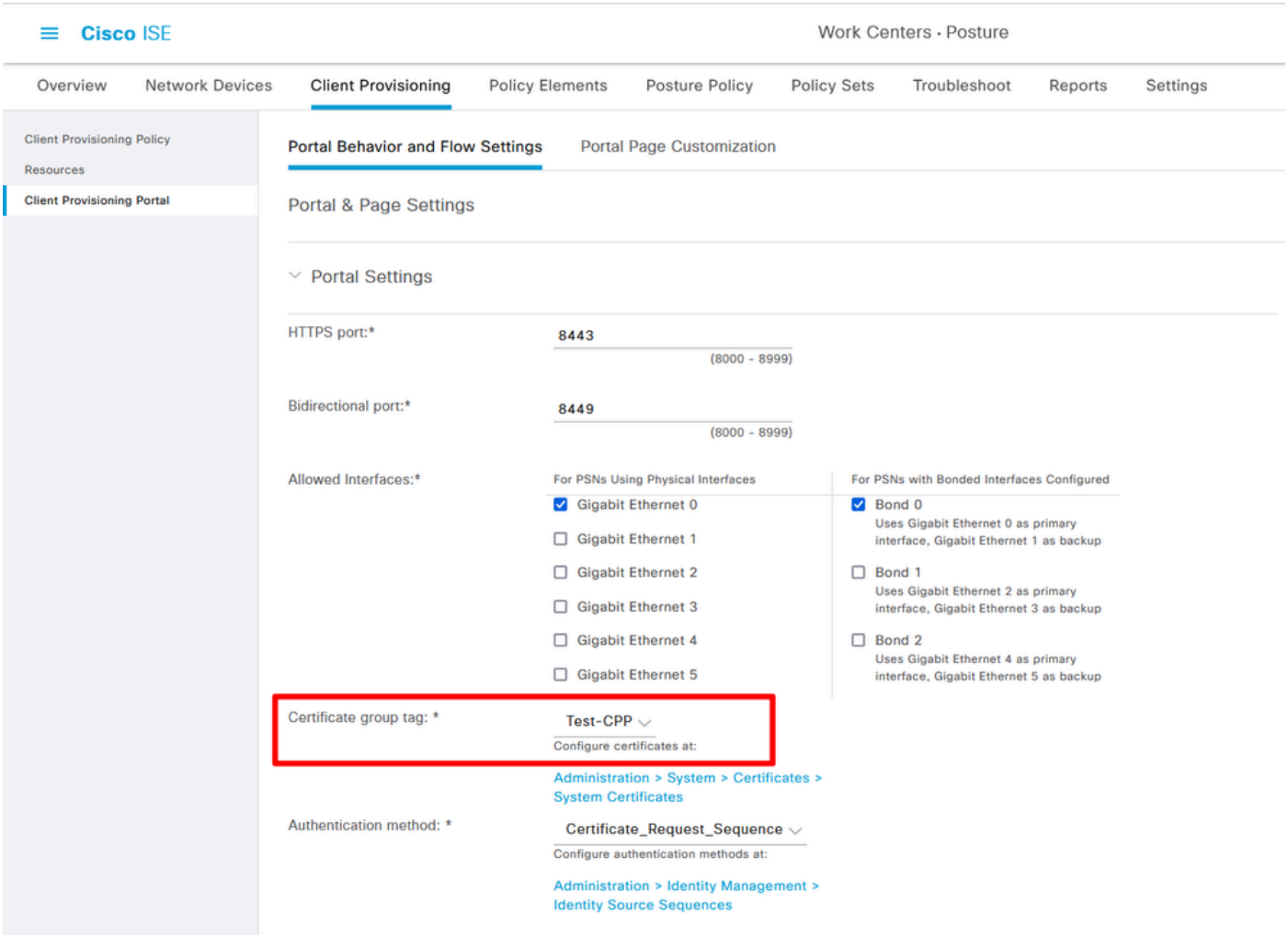
Agregar configuración de agente

Paso 6. Confirme el portal de aprovisionamiento de clientes; utilice el portal predeterminado para probar que es correcto. (Genere CSR y solicite un certificado SSL del servidor de la CA y sustituya la etiqueta Grupo de certificados en esta configuración del portal. De lo contrario, se producirá una advertencia de certificado no fiable durante el proceso de prueba.)

Vaya a Centros de trabajo> Estado> Aprovisionamiento de clientes> Portales de aprovisionamiento de clientes:

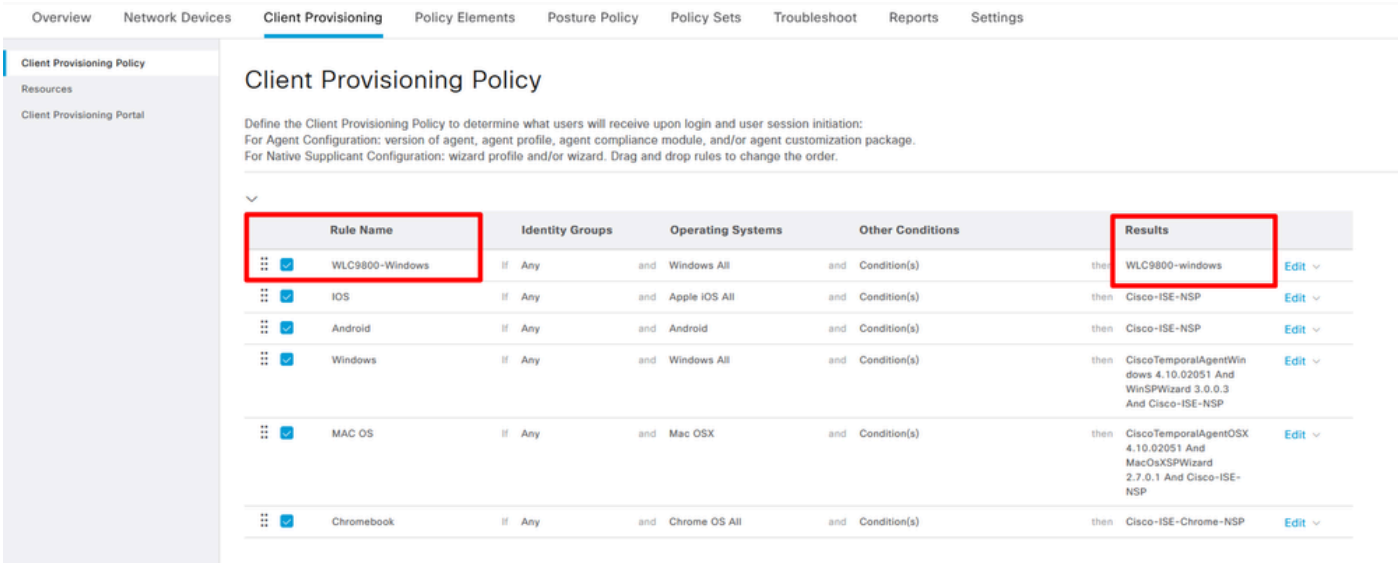


Seleccione Client Provisioning Portal 01



Seleccione Client Provisioning Portal 02

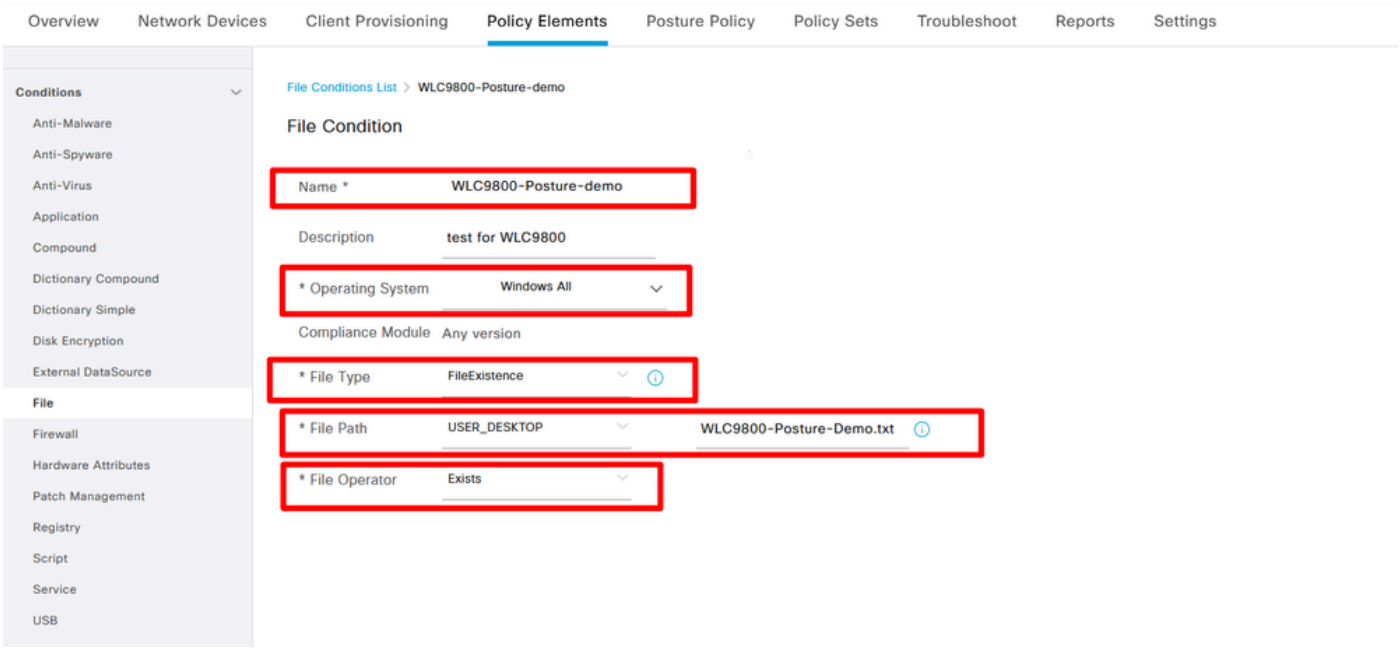
Paso 7. Crear política de aprovisionamiento de clientes. Vaya a Centros de trabajo > Estado > Aprovisionamiento de cliente > Directiva de aprovisionamiento de cliente > Editar > insertar nueva directiva arriba.



Crear directiva de aprovisionamiento de clientes

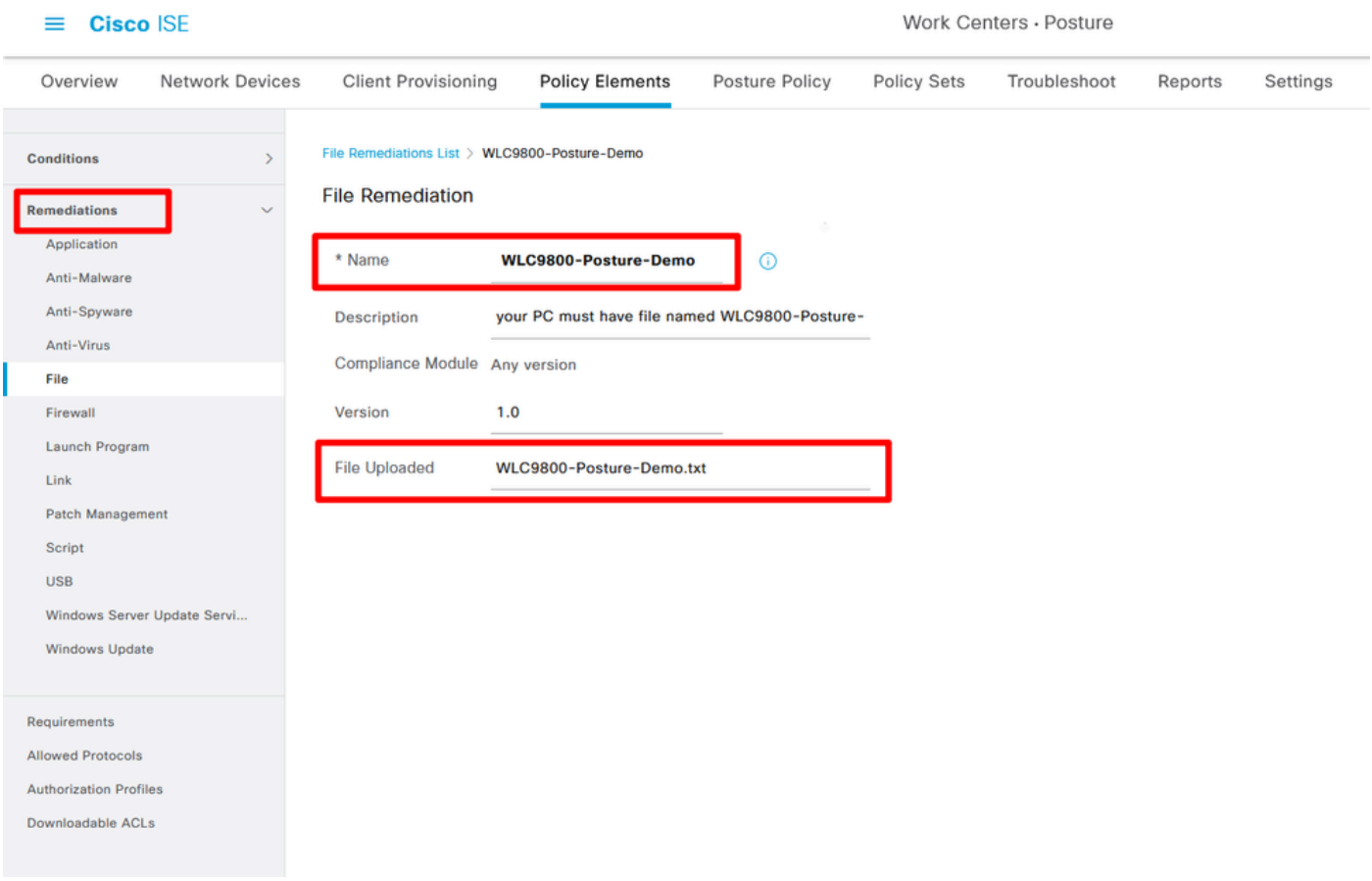
Paso 8. Crear condiciones de archivo. Vaya a Centros de trabajo> Condición> Elementos de

directiva> Condiciones> Archivo> Condiciones de archivo> Agregar:



Crear condición de archivo

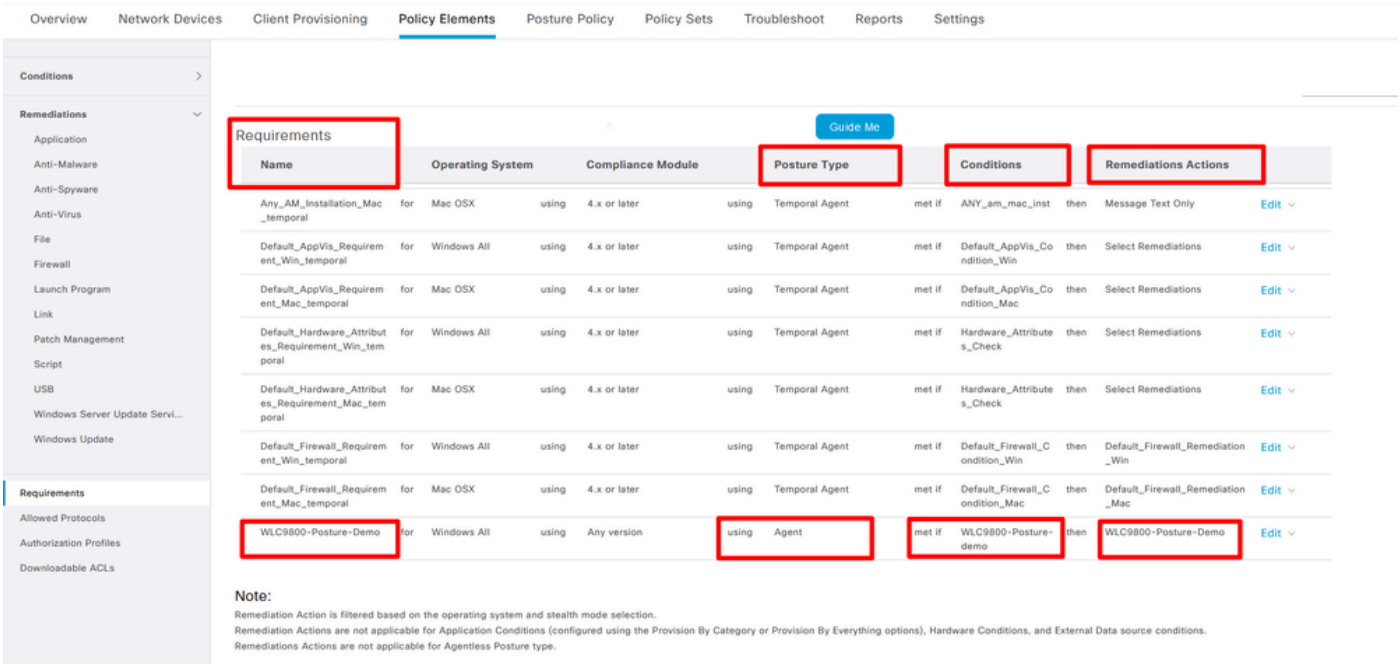
Paso 9. Crear Remediaciones Vaya a Centros de Trabajo> Postura> Elementos de Política> Remediaciones > Archivo> Agregar:



Crear remediación de archivo

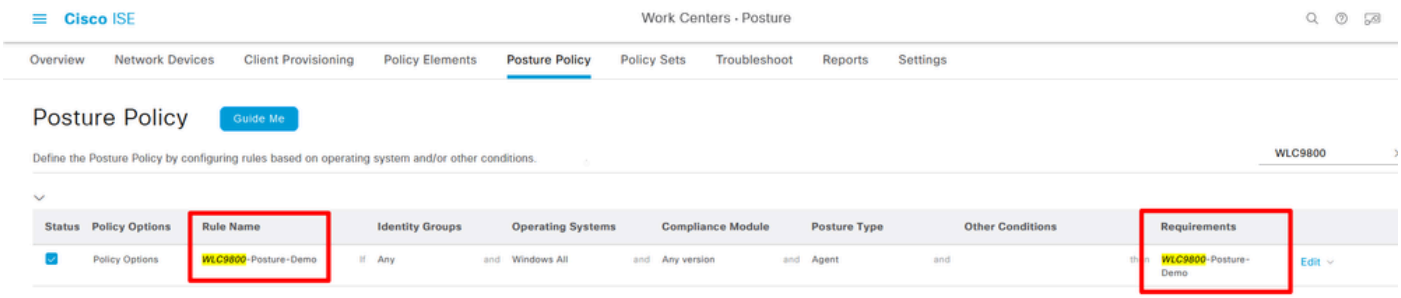
Paso 10. Crear Requisito. Vaya a Centros de trabajo> Condición> Elementos de directiva>

Requisitos> Insertar nuevo requisito:



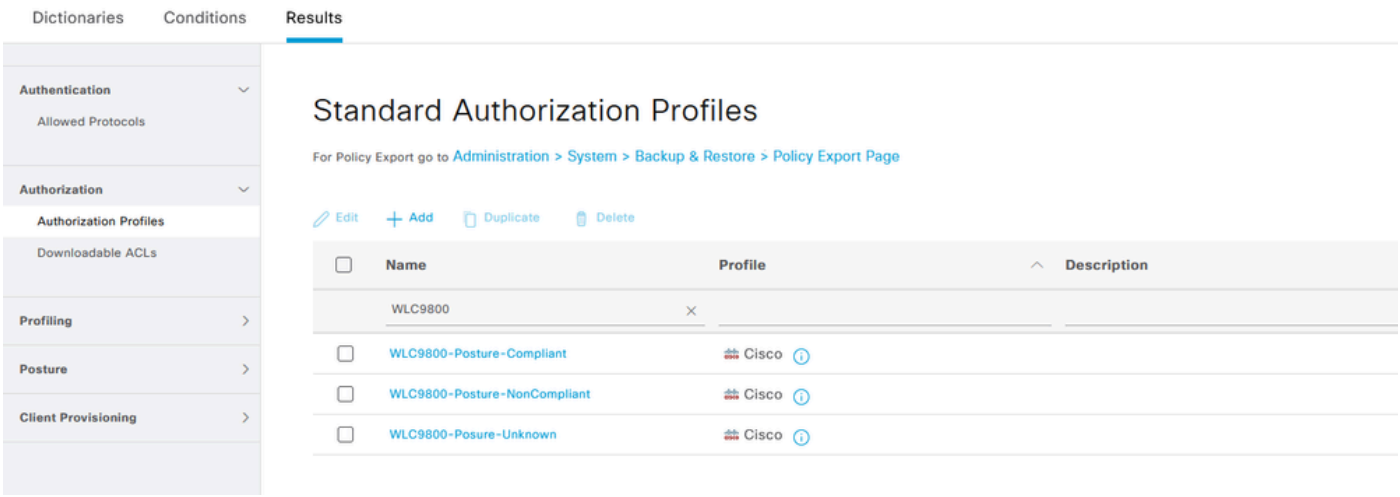
Crear requisito de estado

Paso 11. Crear política de estado. Vaya a Centros de trabajo> Estado> Insertar nueva directiva:

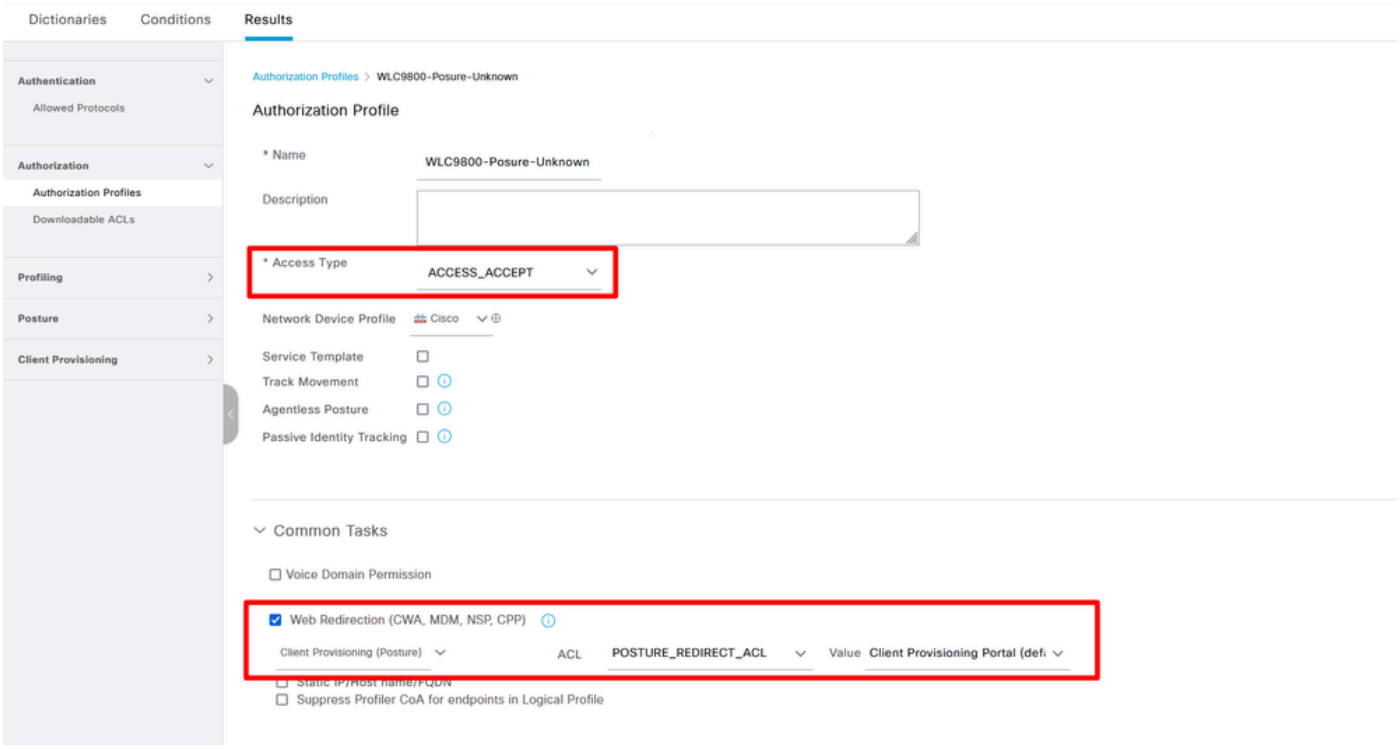


Crear política de estado

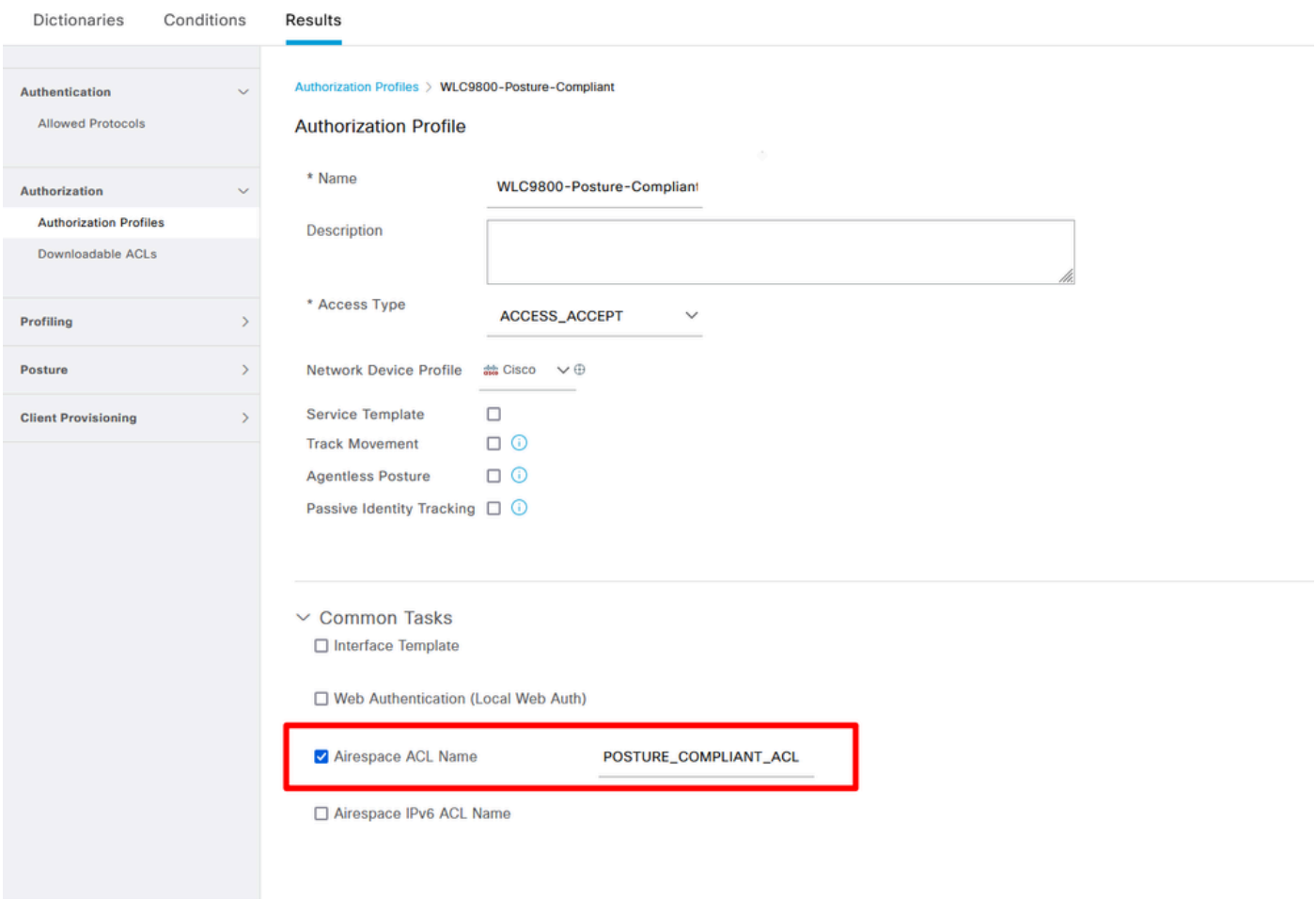
Paso 12. Crear tres perfiles de autorización: El estado es Desconocido; El estado es No conforme; El estado de condición es compatible. Vaya a Directiva> Elementos de directiva> Resultados> Autorización> Perfiles de autorización> Agregar:



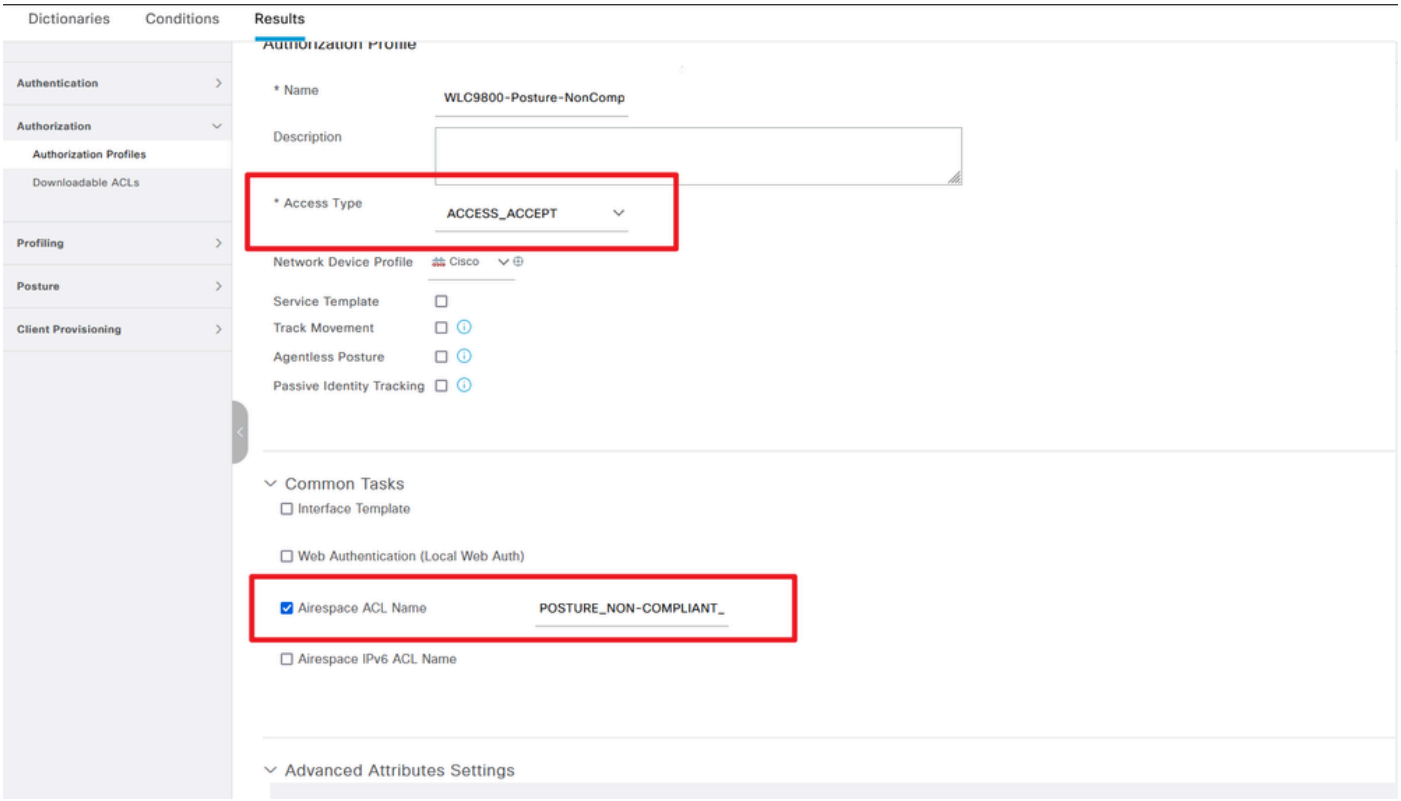
Crear perfiles de autorización 01



Crear perfiles de autorización 02



Crear perfiles de autorización 03

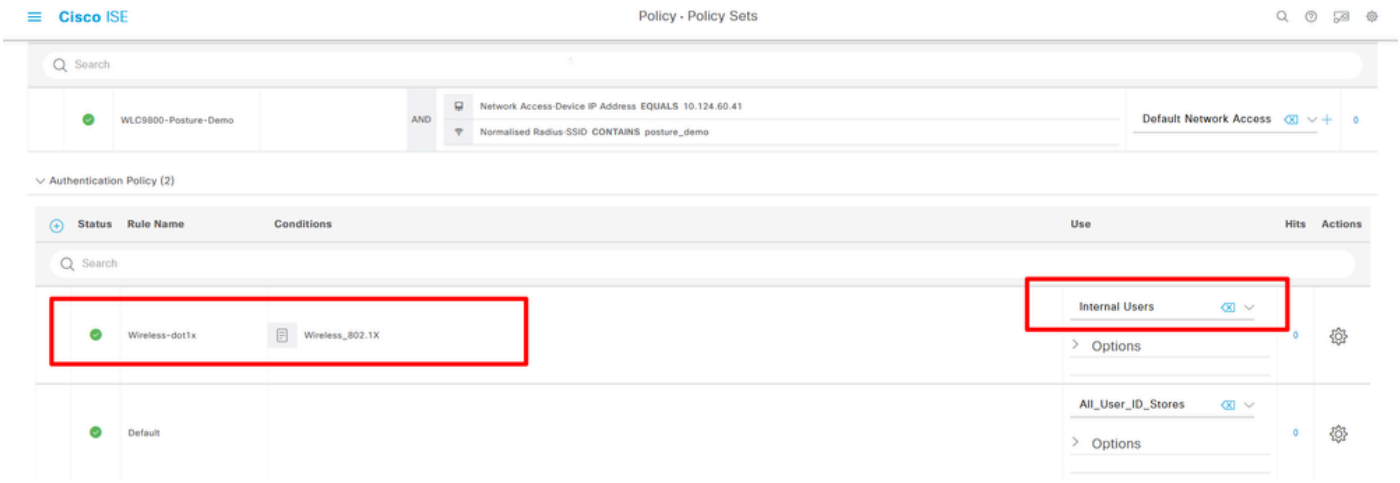


Paso 13. Creación de Juegos de Políticas. Vaya a Directiva> Directiva

Crear conjuntos de políticas

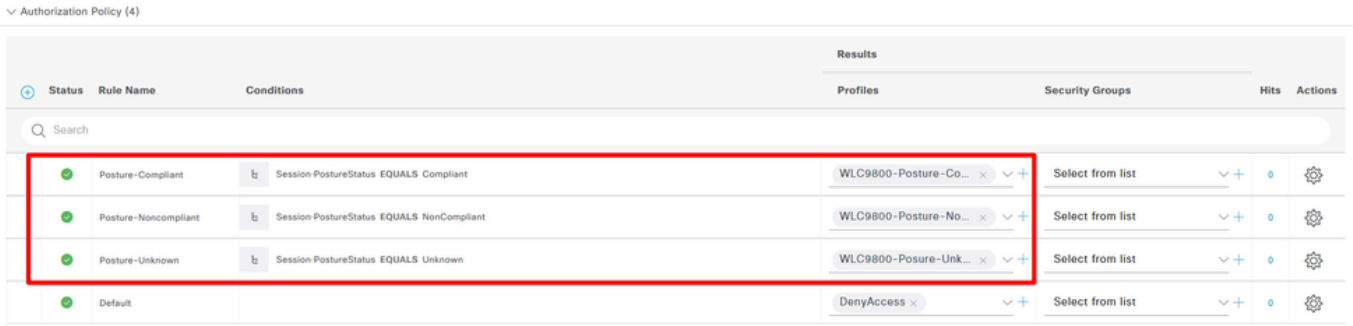
Conjuntos> Agregar icono:

Paso 14. Crear política de autenticación Navegue hasta Política> Conjuntos de políticas> Expanda "WLC9800-Posture-Demo"> Política de autenticación> Agregar:



Crear política de autenticación

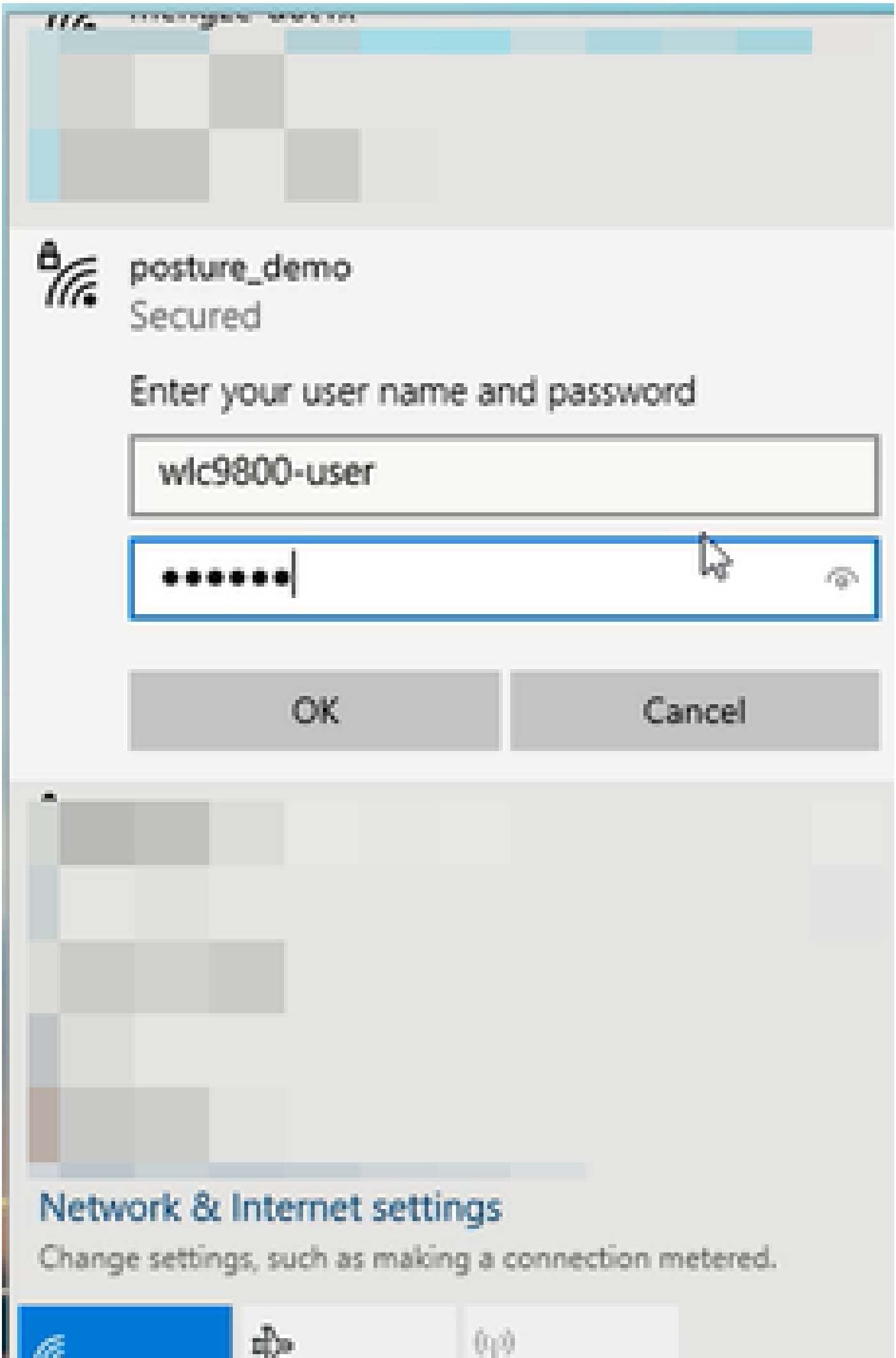
Paso 15. Crear política de autorización Vaya a Política> Conjuntos de políticas> Expandir "WLC9800-Posture-Demo"> Política de autorización> Agregar:



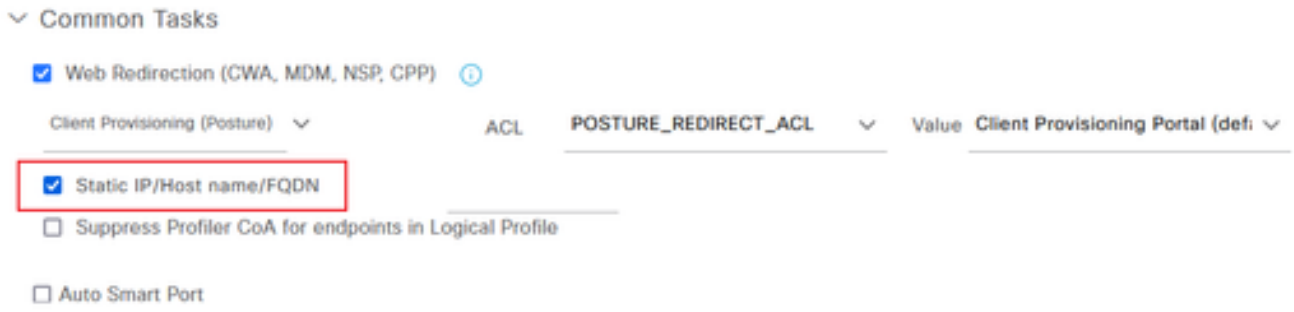
Crear directiva de autorización

Examples

1. Demostración de estado de SSID de prueba conectada con credenciales 802.1X correctas.


posture_demo
Secured
Enter your user name and password
wlc9800-user
OK
Cancel
Network & Internet settings
Change settings, such as making a connection metered.

- Si el navegador se ha redirigido a la URL del portal de ISE pero no se puede cargar la página, compruebe si el nombre de dominio de ISE no se agrega al servidor DNS, por lo que el cliente no puede resolver la URL del portal. Para resolver rápidamente este problema, verifique Static IP/Host name/FQDN bajo el Perfil de autorización para proporcionar la dirección IP en la URL de redirección. Sin embargo, esto puede suponer un problema de seguridad, ya que expone la dirección IP de ISE.



Recopilar depuraciones

Habilitar depuraciones en C9800

Habilitar depuraciones en ISE

Referencias

- Configuración de CWA en Catalyst 9800 WLC e ISE - Cisco
- BYOD inalámbrico con Identity Services Engine
- Implementar el estado de ISE
- Solución de problemas de administración y estado de sesiones de ISE
- Comparación del flujo de redirección de postura de ISE con el flujo sin redirección de postura de ISE

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).