Configuración de la Autenticación Web Local con Autenticación Externa

Contenido

Información Relacionada

Introducción

Este documento describe cómo configurar la autenticación Web local con autenticación externa en un WLC 9800 e ISE.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración de controladores LAN inalámbricos (WLC) 9800
- Puntos de acceso ligeros (LAP)
- Cómo configurar un servidor web externo Identity Services Engine (ISE).
- Cómo configurar y configurar servidores DHCP y DNS.

Componentes Utilizados

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

- 9800-40 WLC Cisco IOS® XE, versión 17.18.4a con APSP1 y APSP2
- Identity Services Engine (ISE), versión 3.2.0.542
- Punto de acceso Wi-Fi 7 de la serie Cisco® Wireless 9172I, versión 17.18.4.2012

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.

Autenticación Web

La autenticación Web es una función de seguridad de capa 3 que permite a los usuarios invitados tener acceso a la red.

Esta función está diseñada para proporcionar acceso de invitado fácil y seguro a SSID abiertos, sin necesidad de configurar un perfil de usuario, y también puede funcionar con métodos de seguridad de capa 2.

El propósito de la autenticación web es permitir que los dispositivos no fiables (invitados) accedan a la red con privilegios de acceso a la red limitados, a través de una WLAN de invitado que se puede configurar con mecanismos de seguridad y que la seguridad de la red no se vea comprometida. Para que los usuarios invitados tengan acceso a la red, deben autenticarse correctamente, es decir, deben proporcionar las credenciales correctas o aceptar la política de uso aceptable (AUP) para obtener acceso a la red.

La autenticación web es una ventaja para las empresas porque fomenta la fidelidad de los usuarios, hace que la empresa sea compatible con el uso de una renuncia de responsabilidad que el usuario invitado debe aceptar y permite a la empresa interactuar con los visitantes.

Para implementar la autenticación web, se debe tener en cuenta cómo se gestionan el portal de invitados y la autenticación. Existen dos métodos comunes:

- Autenticación web local (LWA): Método de redirección de usuarios invitados a un portal directamente desde el WLC. La redirección y la ACL pre-WebAuth se configuran localmente en el WLC.
- Autenticación web central (CWA): Método de redirección de usuarios invitados en el que la URL de redirección y la ACL de redirección se configuran de forma centralizada en un servidor externo (por ejemplo, ISE) y se comunican al WLC mediante RADIUS. En la autenticación web central, la URL de redirección y la ACL de redirección se encuentran centralizadas en un servidor externo (como RADIUS). El servidor RADIUS es el que maneja la autenticación, envía las instrucciones al WLC. En CWA, el WLC no requiere un certificado de web-auth local, solo se necesita un certificado en el portal web central y requiere un servidor de autenticación central, como ISE. Para leer CWA con más detalle, navegue hasta Configure Central Web Authentication (CWA) en Catalyst 9800 WLC e ISE.

En la autenticación Web local, el portal Web puede estar presente en el WLC o en un servidor externo. En LWA con la autenticación externa, el portal web está presente en el WLC. En LWA con servidor web externo, el portal web está presente en un servidor externo (como Cisco DNA Spaces). Un ejemplo de LWA con servidor Web externo se describe detalladamente en: Configure el portal cautivo de los espacios DNA con el WLC de Catalyst 9800.

Diagrama de los diferentes métodos de autenticación web:

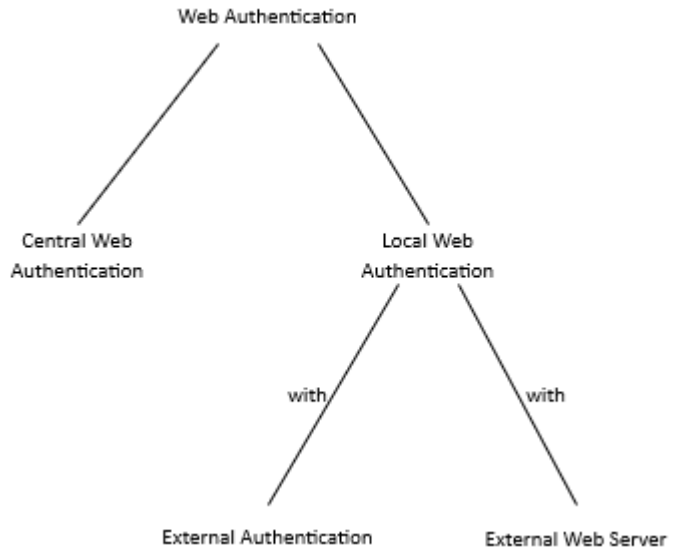


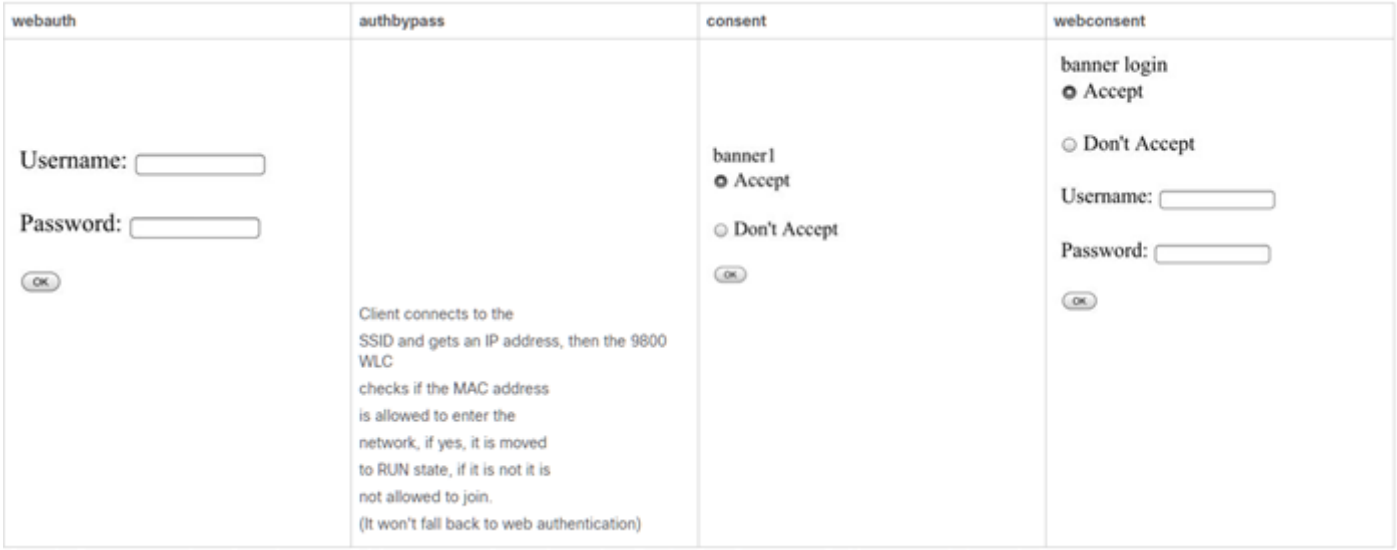
Diagrama de los diferentes métodos de autenticación Web

Nota: Si está implementando Wi-Fi 7 AP con autenticación web en un WLC 9800, asegúrese de ejecutar una versión recomendada de Cisco IOS XE como 17.18.4a o posterior.

Tipos de autenticación

Existen cuatro tipos de autenticación para autenticar al usuario invitado:

- Webauth: Introduzca el nombre de usuario y la contraseña.
- Consentimiento (web-passthrough): Aceptar AUP.
- Authbypass: Autenticación basada en la dirección MAC del dispositivo del usuario invitado.
- Consentimiento web: Una mezcla entre nombre de usuario/contraseña y aceptar AUP.



Cuatro tipos de autenticación para autenticar al usuario invitado

Base de datos para autenticación

Las credenciales para la autenticación se pueden almacenar en un servidor LDAP, localmente en el WLC o en el servidor RADIUS.

- Base de datos local: Las credenciales (nombre de usuario y contraseña) se almacenan localmente en el WLC.
- Base de datos LDAP: Las credenciales se almacenan en la base de datos back-end LDAP. El WLC consulta al servidor LDAP para las credenciales de un usuario determinado en la base de datos.
- Base de datos RADIUS: Las credenciales se almacenan en la base de datos back-end RADIUS. El WLC consulta al servidor RADIUS para las credenciales de un usuario determinado en la base de datos.

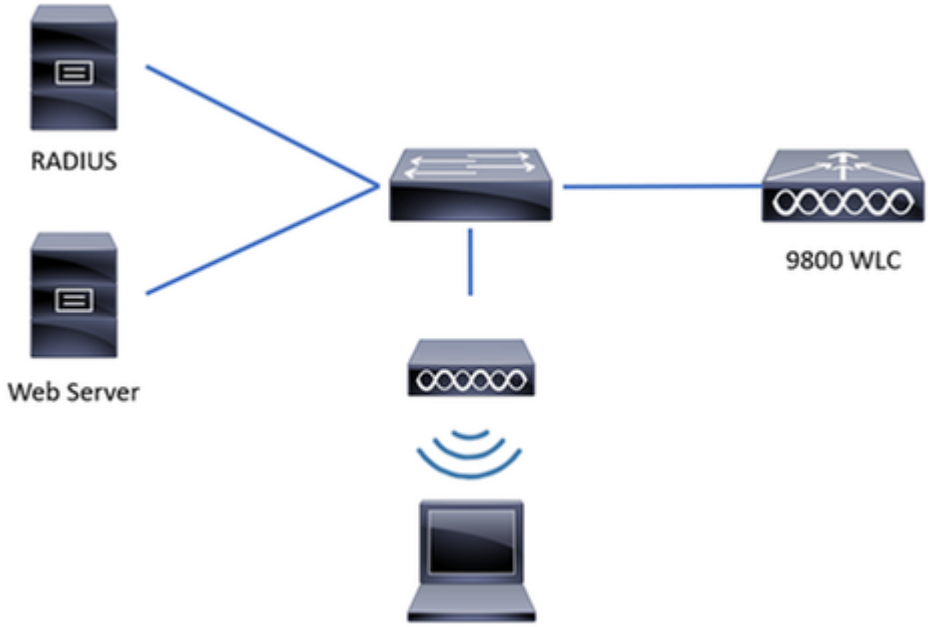
Autenticación web local

En la autenticación Web local, el usuario invitado es redirigido a un portal Web directamente desde el WLC.

El portal web puede estar en el WLC o en otro servidor. Lo que hace local es el hecho de que la URL de redirección y la ACL que coincide con el tráfico deben estar en el WLC (no en la ubicación del portal web). En LWA, cuando un usuario invitado se conecta con el WLAN invitado, el WLC intercepta la conexión del usuario invitado y los redirige a la URL del portal web, donde se

le pide al usuario invitado que autentique. Cuando el usuario invitado ingresa credenciales (nombre de usuario y contraseña), el WLC captura las credenciales. El WLC autentica al usuario invitado con un servidor LDAP, servidor RADIUS o base de datos local (base de datos presente localmente en el WLC). En el caso del servidor RADIUS (un servidor externo como ISE), se puede utilizar no solo para almacenar credenciales, sino también para proporcionar opciones de registro de dispositivos y autoaprovisionamiento. En el caso de un servidor web externo, como Cisco DNA Spaces, el portal web está presente allí. En LWA hay un certificado en el WLC y otro en el portal web.

La imagen representa la topología genérica de LWA:



Topología genérica de LWA

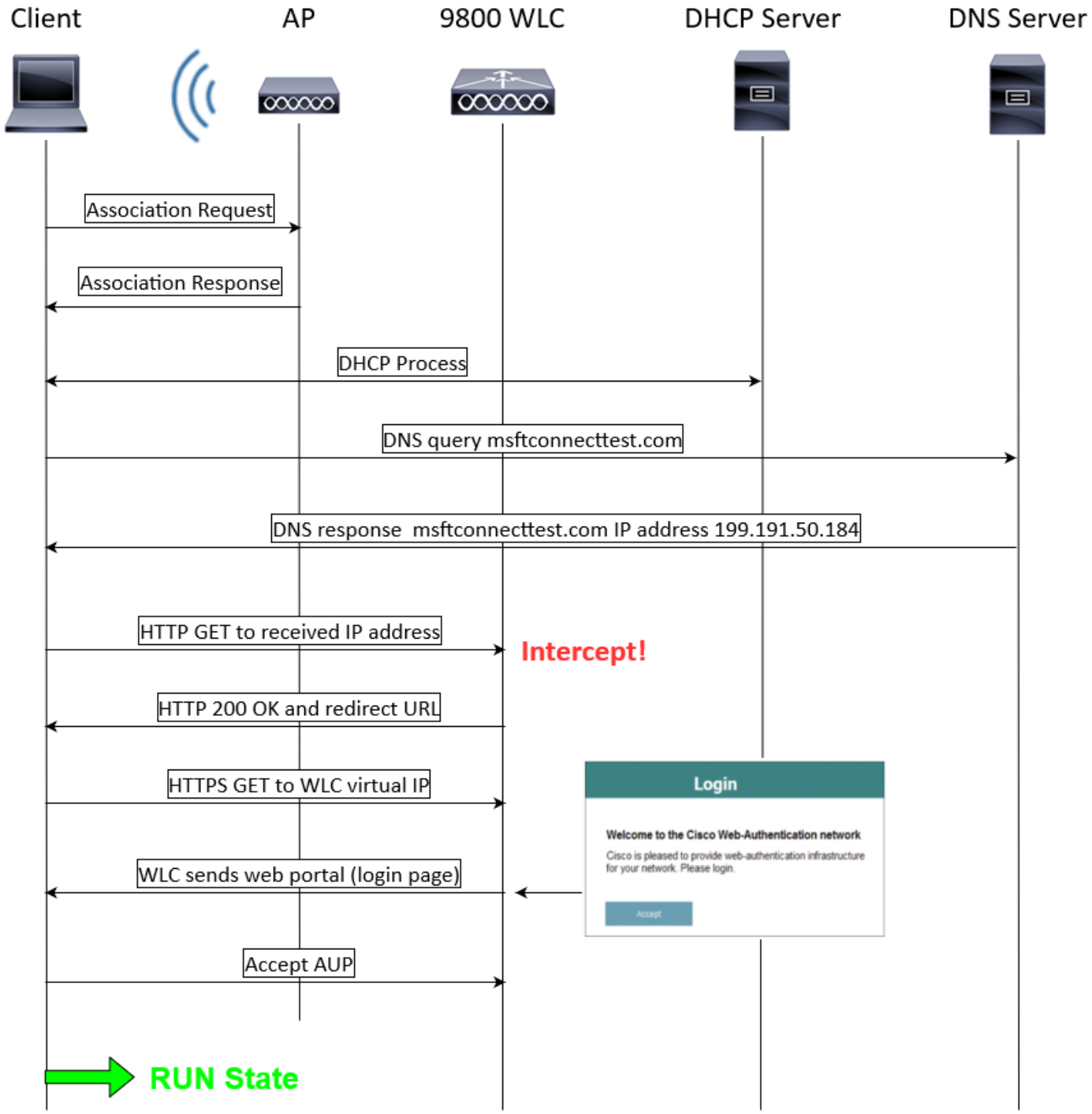
Dispositivos en la topología de red de LWA:

- Cliente: Envía solicitudes al servidor DHCP y DNS, solicita acceso al WLAN invitado y responde a las solicitudes del WLC.
- Punto de Acceso: Conectado a un switch, transmite la WLAN de invitado y proporciona conexión inalámbrica a los dispositivos de los usuarios invitados. También permite paquetes DHCP y DNS antes de que se autentique al usuario invitado (antes de introducir credenciales válidas).
- WLC: Administra los AP y los clientes. El WLC hospeda la URL de redirección y la ACL que coincide con el tráfico. Intercepta solicitudes HTTP de los usuarios invitados y los redirige a un portal web (página de inicio de sesión) donde los usuarios invitados deben autenticarse. Captura las credenciales y autentica a los usuarios invitados, y envía solicitudes de acceso a un servidor externo, servidor LDAP o base de datos local para confirmar si las credenciales son válidas.
- Servidor de autenticación: Responde a las solicitudes de acceso del WLC con

aceptación/rechazo de acceso. El servidor de autenticación valida las credenciales del usuario invitado y notifica al WLC si las credenciales son válidas o no válidas. Si las credenciales son válidas, el usuario invitado está autorizado a acceder a la red (el servidor de autenticación proporciona opciones para el registro del dispositivo y el autoaprovisionamiento). Si las credenciales no son válidas, se deniega al usuario invitado el acceso a la red.

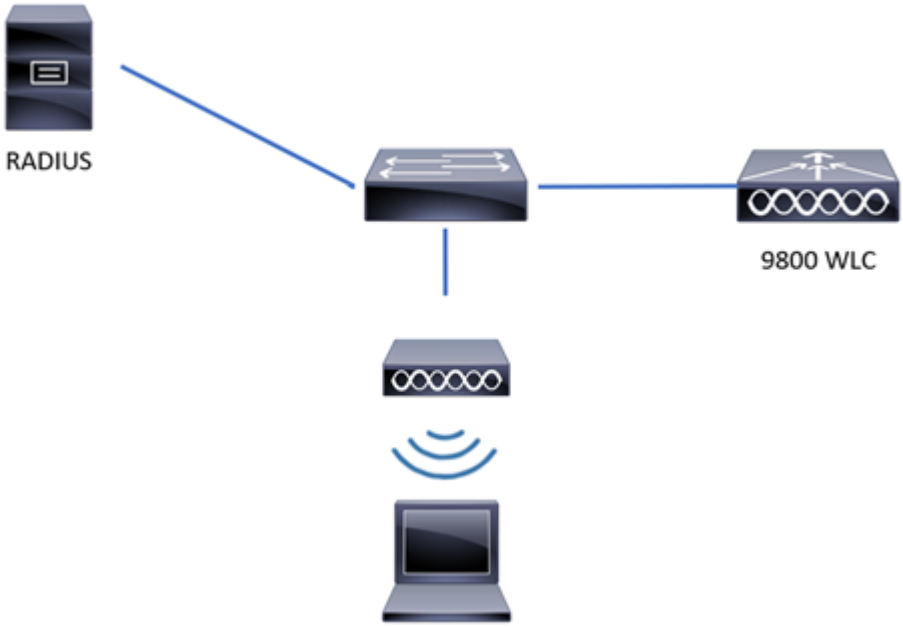
Flujo LWA:

- El usuario invitado se asocia con un AP que transmite la WLAN del invitado.
- El usuario invitado pasa a través del proceso DHCP para obtener una dirección IP.
- El usuario invitado desea realizar una comprobación de conectividad a Internet en el portal cautivo. Si se trata de un dispositivo de Apple, intenta el portal cautivo de Apple; si se trata de un dispositivo Android que intenta el portal cautivo de Android; si se trata de un dispositivo Windows, prueba el portal de pruebas de Windows connect.
- El usuario invitado envía una consulta DNS para solicitar la dirección IP del portal cautivo. El servidor DNS responde a la consulta con la dirección IP correspondiente.
- El usuario invitado envía un mensaje HTTP GET a la dirección IP del portal cautivo.
- El WLC intercepta ese mensaje y responde al usuario invitado con HTTP 200 OK y la URL de redireccionamiento.
- El usuario invitado envía un mensaje HTTPS GET a la IP virtual del WLC y el WLC responde con el portal web.
- Se le solicita al usuario invitado que introduzca las credenciales de autenticación en el portal web.
- El portal web redirige al usuario al WLC con las credenciales proporcionadas (si se utiliza un portal web externo).
- El WLC autentica al usuario invitado a través de una base de datos local, o envía una consulta al servidor RADIUS o LDAP, para confirmar si las credenciales son correctas (si el tipo de autenticación es webaccept o webauth).
- Si las credenciales son correctas, el WLC autentica al usuario invitado y pasa al estado RUN. Si las credenciales son incorrectas, el WLC elimina el usuario invitado.
- El WLC redirige al cliente de nuevo a la URL original que fue introducida en el explorador Web.



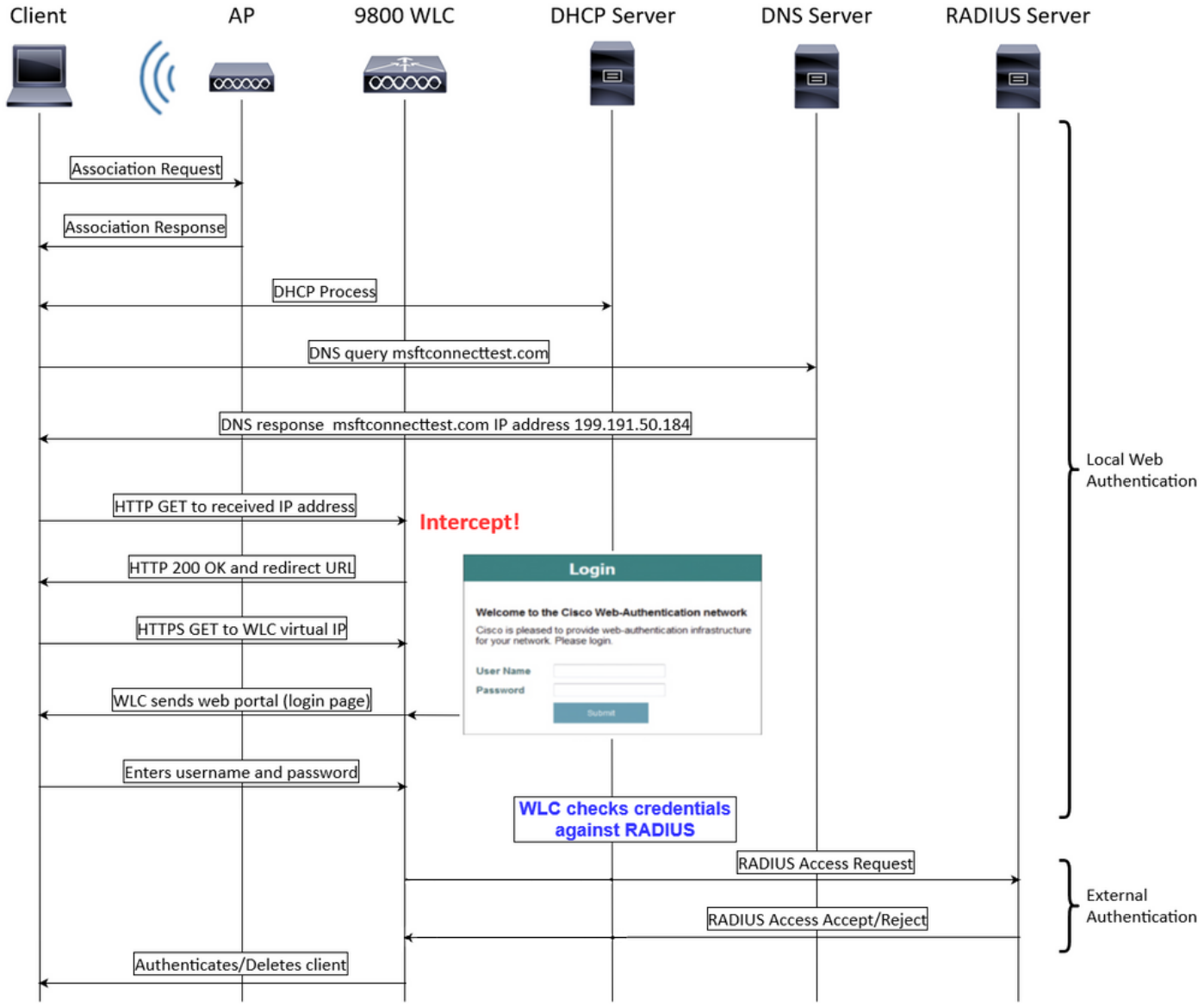
Flujo de LWA

Autenticación Web Local con Autenticación Externa



Topología genérica de LWA-EA

LWA-EA es un método de LWA donde el portal web y la URL de redirección se encuentran en el WLC y las credenciales se almacenan en un servidor externo, como ISE. El WLC captura las credenciales y autentica al cliente a través de un servidor RADIUS externo. Cuando el usuario invitado ingresa las credenciales, el WLC verifica las credenciales contra RADIUS, envía una solicitud de acceso RADIUS y recibe una aceptación/rechazo de acceso RADIUS del servidor RADIUS. A continuación, si las credenciales son correctas, el usuario invitado pasa al estado RUN. Si las credenciales son incorrectas, el usuario invitado es eliminado por el WLC.



Flujo LWA-EA

Configurar

Diagrama de la red

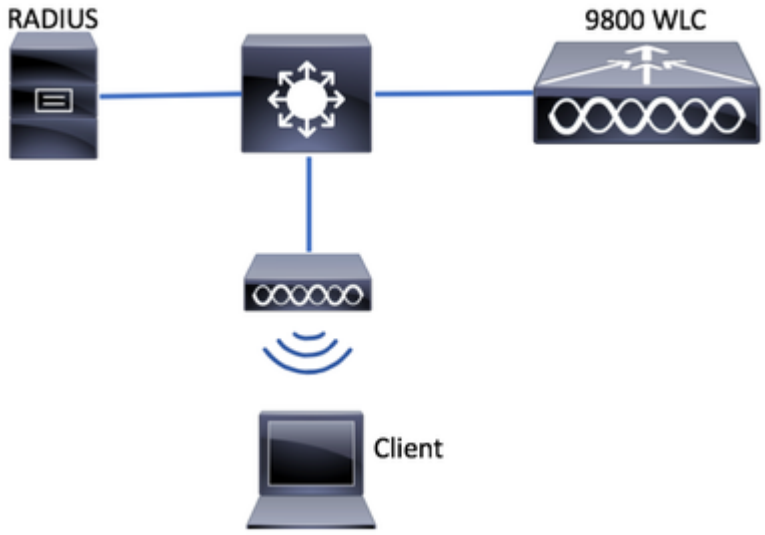


Diagrama de la red

Nota: Este ejemplo de configuración sólo cubre la conmutación/autenticación central. La configuración de conmutación local flexible tiene requisitos ligeramente diferentes para configurar la autenticación web.

Configuración de la Autenticación Web Local con Autenticación Externa en la CLI

Configuración del Servidor AAA y el Grupo de Servidores

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#radius server RADIUS
9800WLC(config-radius-server)#address ipv4 <ip address> auth-port 1812 acct-port 1813
9800WLC(config-radius-server)#key cisco
9800WLC(config-radius-server)#exit
9800WLC(config)#aaa group server radius RADIUSGROUP
9800WLC(config-sg-radius)#server name RADIUS
9800WLC(config-sg-radius)#end
```

Configuración de la autenticación y autorización locales

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#aaa new-model
```

```
9800WLC(config)#aaa authentication login LWA_AUTHENTICATION group RADIUSGROUP
9800WLC(config)#aaa authorization network LWA_AUTHORIZATION group RADIUSGROUP
9800WLC(config)#end
```

Configure Parameter Maps

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)# parameter-map type webauth global
9800WLC(config-params-parameter-map)#virtual-ip ipv4 192.0.2.1
9800WLC(config-params-parameter-map)#trustpoint <trustpoint name>
9800WLC(config-params-parameter-map)#end
```

Configurar parámetros de seguridad de WLAN

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#wlan LWA_EA 1 LWA_EA
9800WLC(config-wlan)#no security wpa
9800WLC(config-wlan)#no security wpa wpa2
9800WLC(config-wlan)#no security wpa wpa2 ciphers aes
9800WLC(config-wlan)#no security wpa akm dot1x
9800WLC(config-wlan)#security web-auth
9800WLC(config-wlan)#security web-auth authentication-list LWA_AUTHENTICATION
9800WLC(config-wlan)#security web-auth parameter-map global
9800WLC(config-wlan)#no shutdown
9800WLC(config-wlan)#end
```

Crear perfil de política inalámbrica

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#wireless profile policy POLICY_PROFILE
9800WLC(config-wireless-policy)#vlan <vlan name>
9800WLC(config-wireless-policy)#no shutdown
9800WLC(config-wireless-policy)#end
```

Crear una etiqueta de directiva

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#wireless tag policy POLICY_TAG
```

```
9800WLC(config-policy-tag)#wlan LWA_EA policy POLICY_PROFILE
9800WLC(config-policy-tag)# end
```

Asignar una etiqueta de política a un AP

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#ap <MAC address>
9800WLC(config-ap-tag)#policy-tag POLICY_TAG
9800WLC(config-ap-tag)#end
```

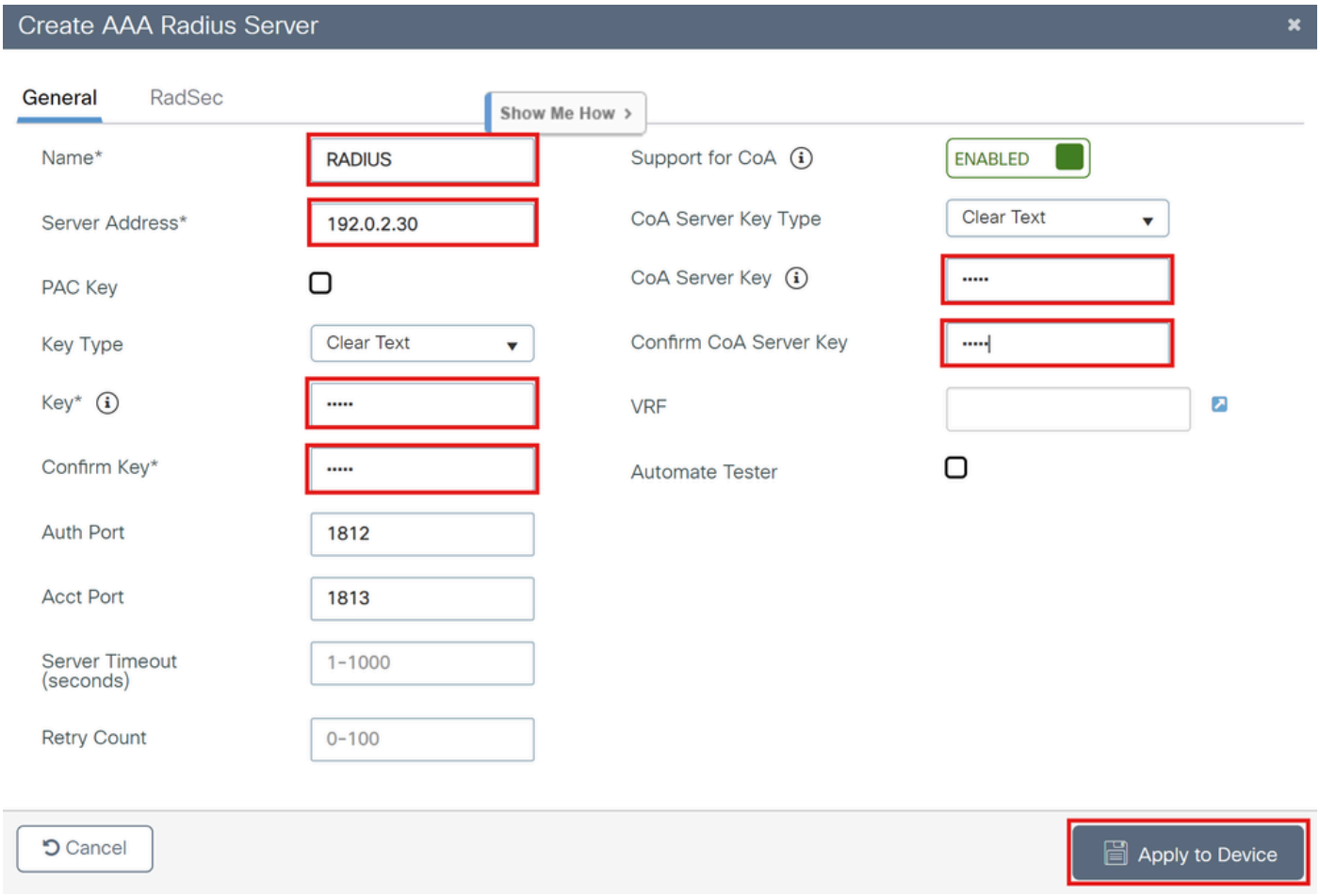
Para finalizar la configuración del lado de ISE, diríjase a la sección Configuración de ISE.

Configuración de la Autenticación Web Local con Autenticación Externa en la WebUI

Configuración de AAA en WLC 9800

Paso 1. Agregue el servidor ISE a la configuración del WLC 9800.

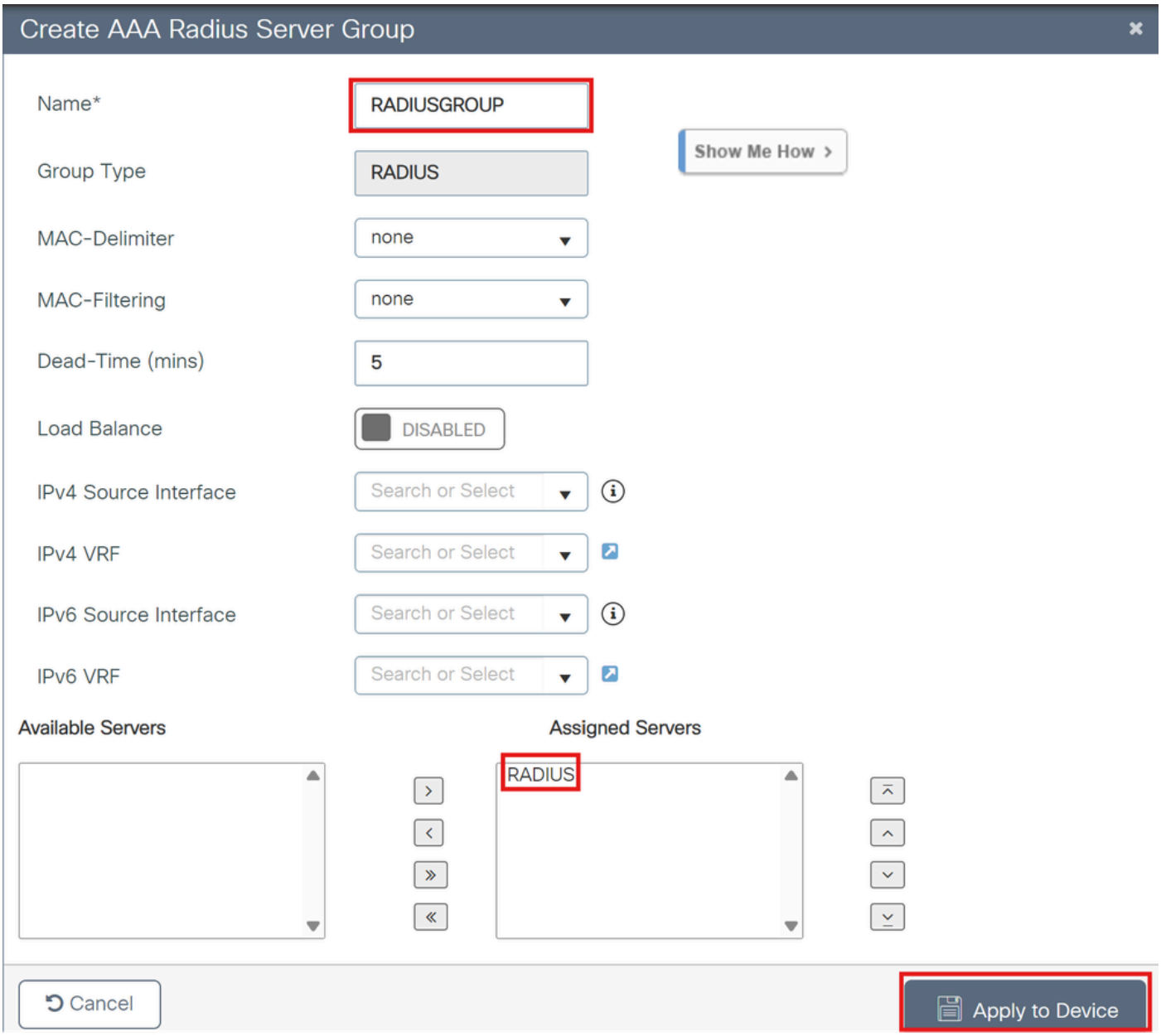
Navegue hasta Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > + Add e ingrese la información del servidor RADIUS como se muestra en la imagen:



Configuración de AAA en WLC 9800

Paso 2. Agregue el grupo de servidores RADIUS.

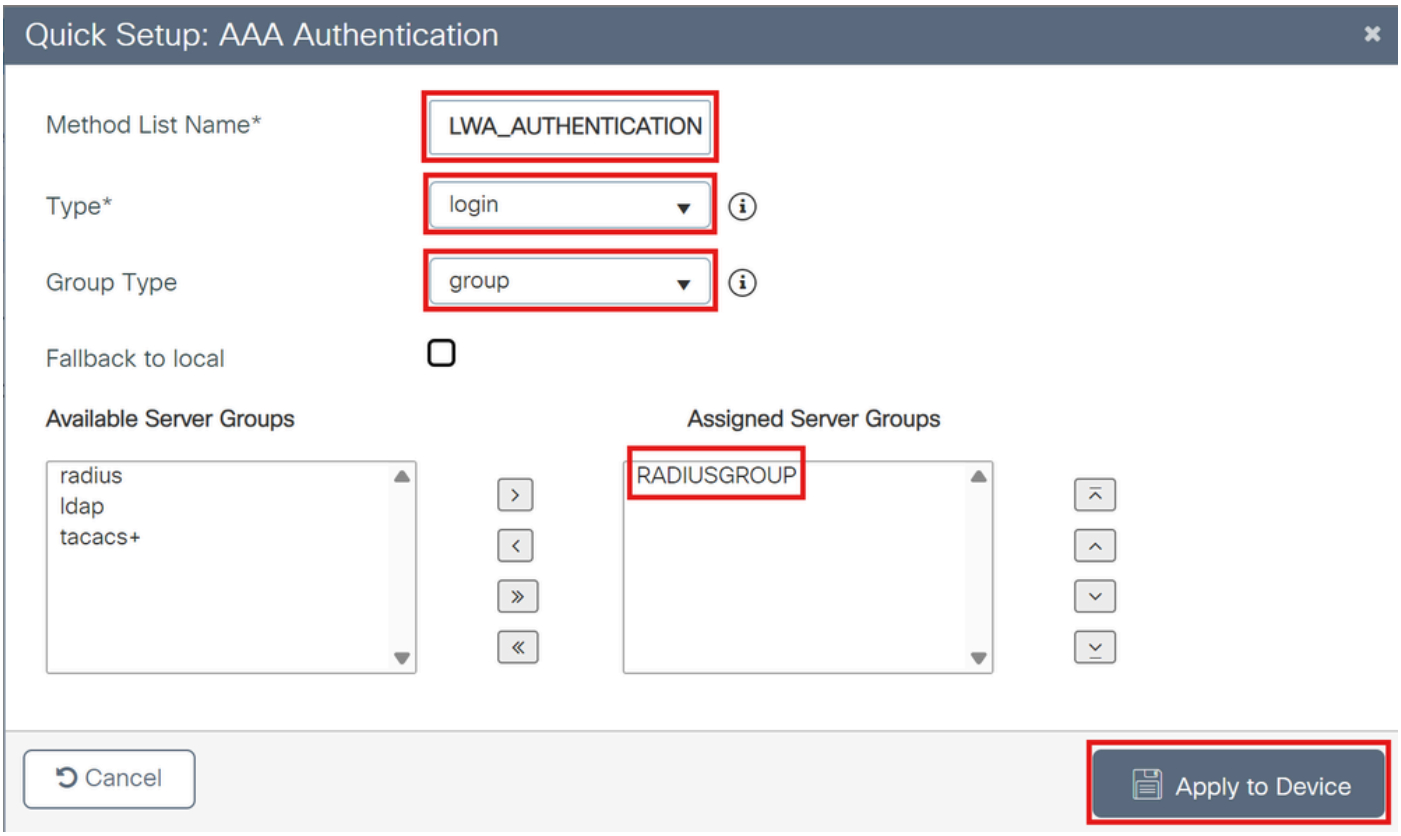
Navegue hasta Configuration > Security > AAA > Servers/Groups > RADIUS > Servers Group > + Add e ingrese la información del grupo de servidores RADIUS:



Agregar el grupo de servidores RADIUS

Paso 3. Cree una lista de métodos de autenticación.

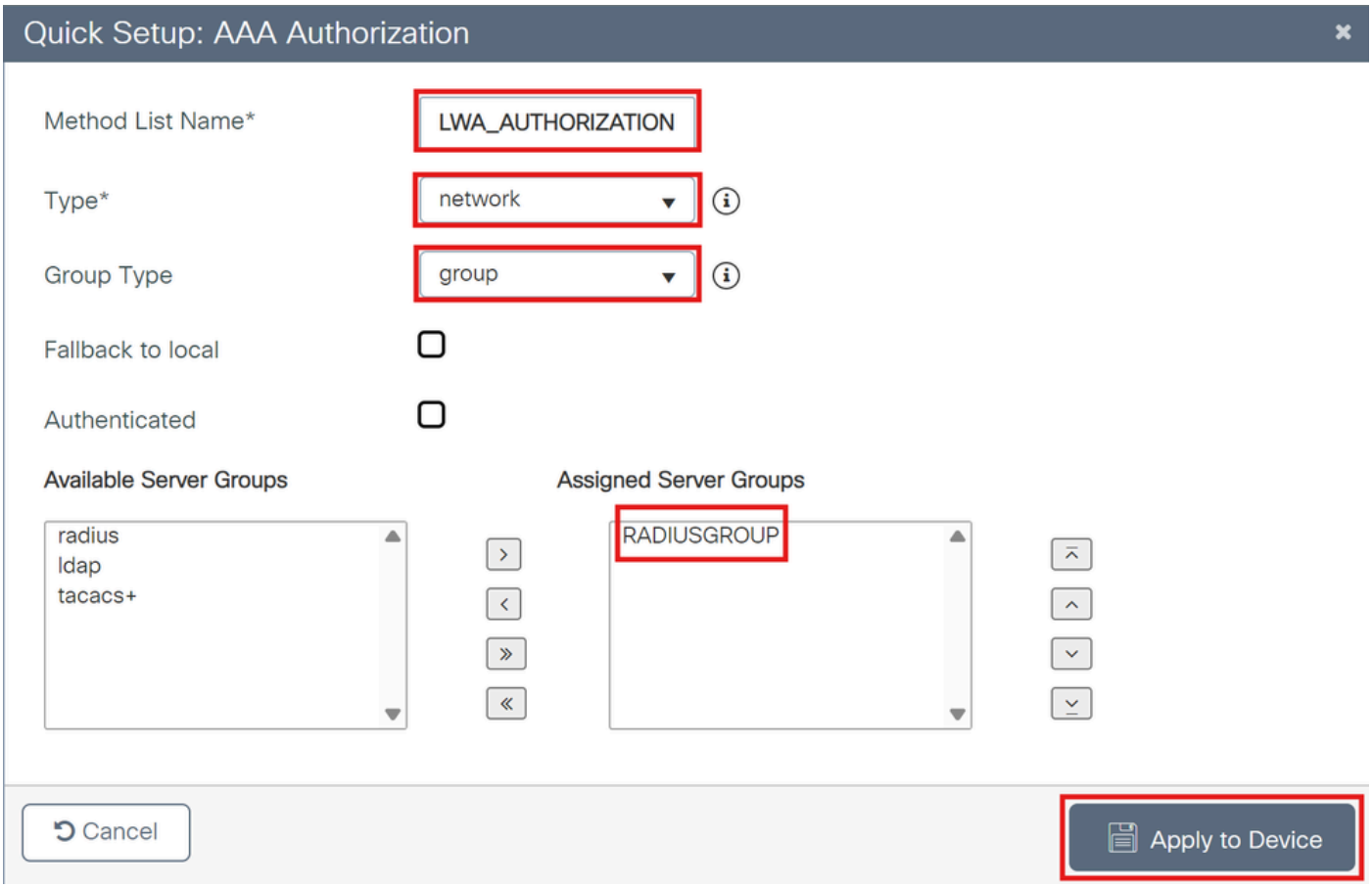
Vaya a Configuration > Security > AAA > AAA Method List > Authentication > + Add:



Crear una lista de métodos de autenticación

Paso 4. Crear una lista de métodos de autorización.

Vaya a Configuration > Security > AAA > AAA Method List > Authorization > + Add:

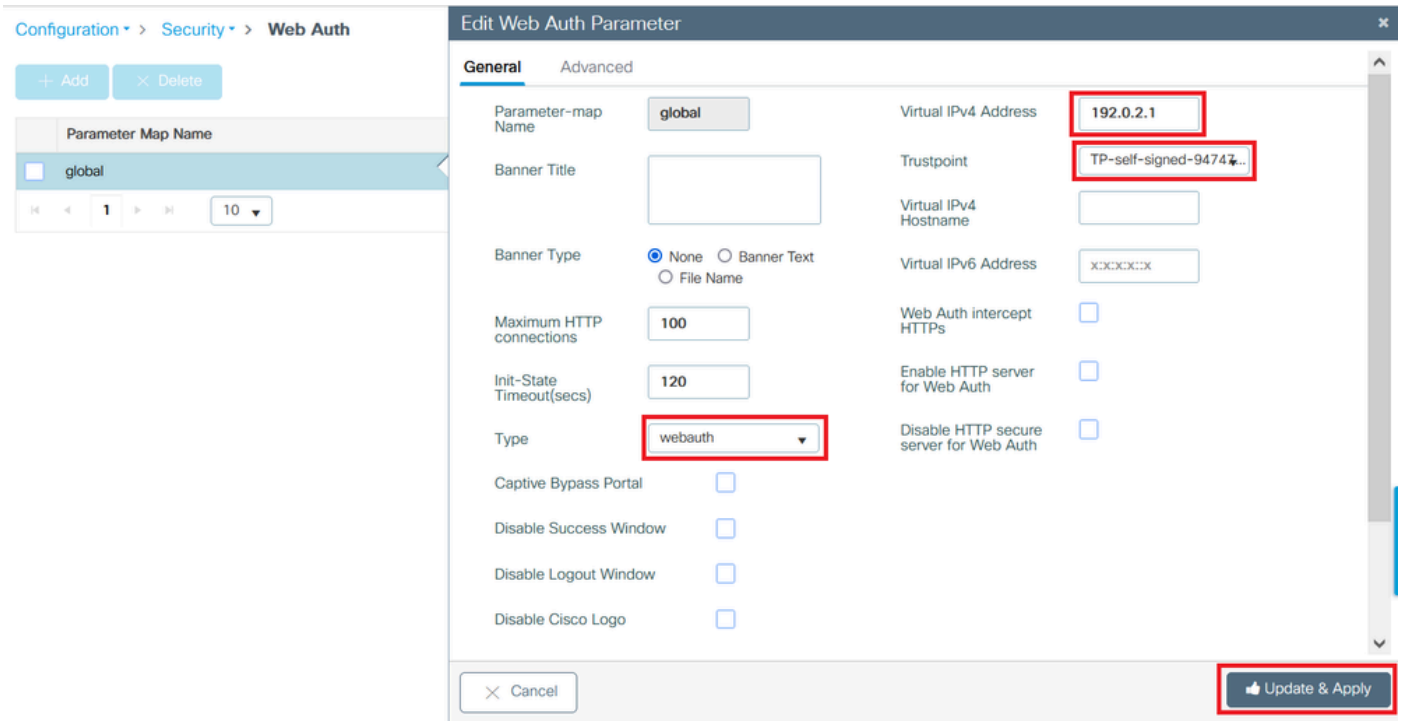


Cree una lista de métodos de autorización

Configuración de WebAuth

Cree o edite un mapa de parámetro. Seleccione el tipo como webauth, la dirección IPv4 virtual debe ser una dirección no utilizada en la red para evitar conflictos de direcciones IP y agregue un punto de confianza.

Navegue hasta Configuration > Security > Web Auth > + Add o seleccione un mapa de parámetro:

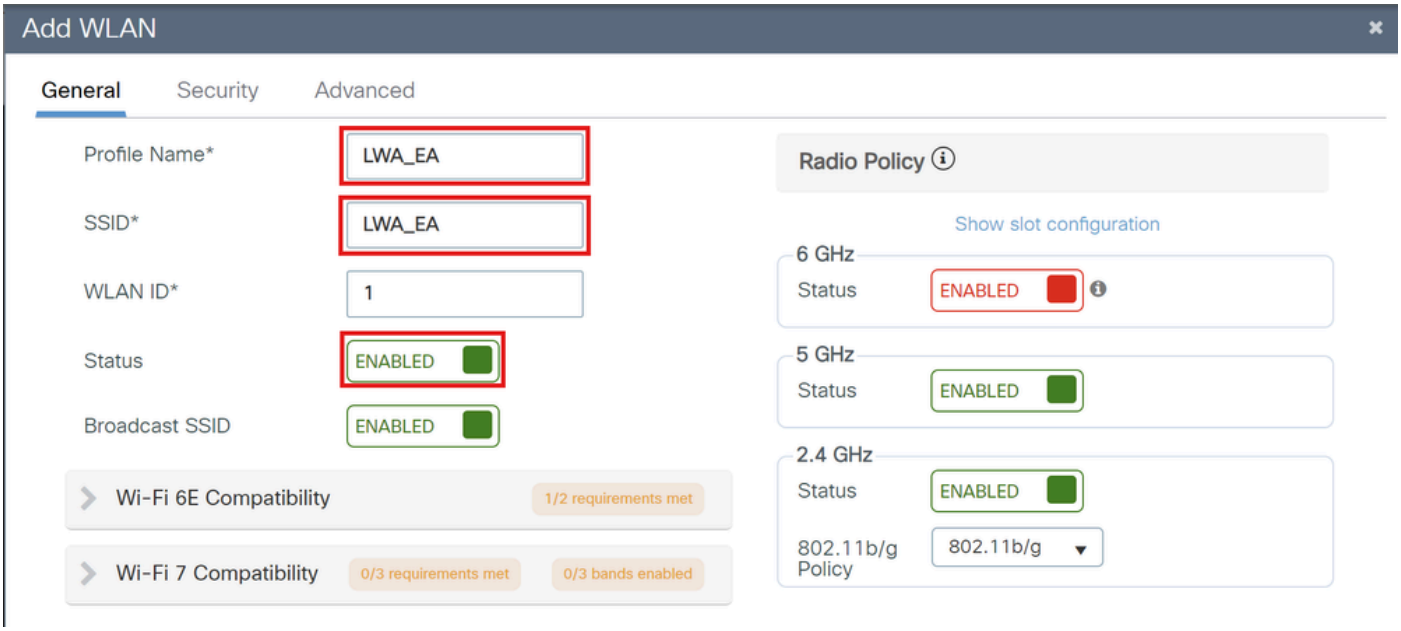


Configuración de WebAuth

Configuración de WLAN

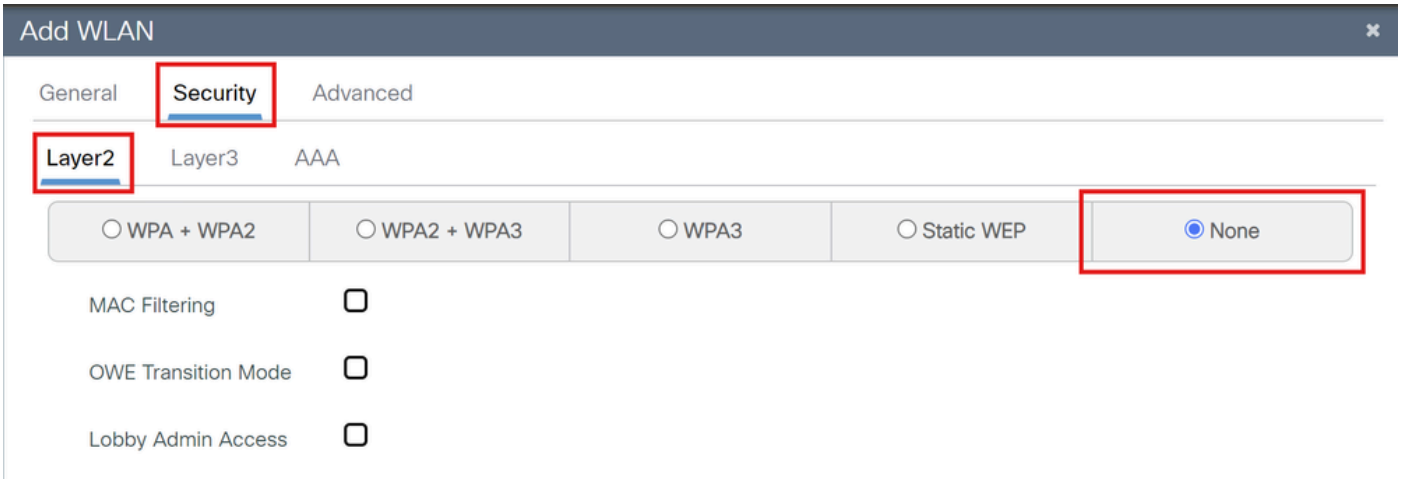
Paso 1. Cree la WLAN.

Vaya a Configuración > Etiquetas y perfiles > WLAN > + Agregar y configure la red según sea necesario.



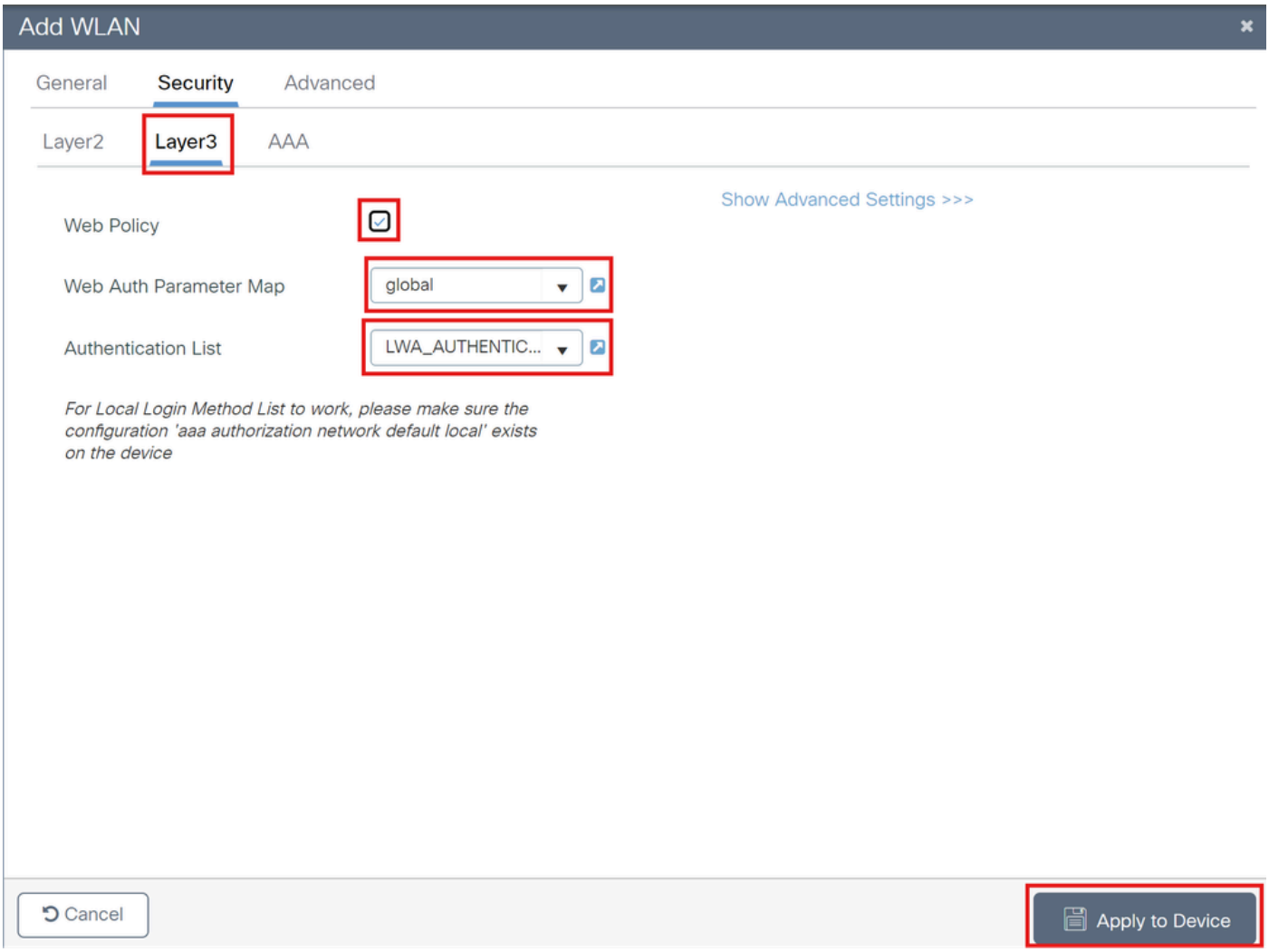
Cree una WLAN.

Paso 2. Navegue hasta Seguridad > Capa 2 y en Modo de Seguridad de Capa 2 seleccione Ninguno.



Creación de la seguridad WLAN

Paso 3. Navegue hasta Seguridad > Capa 3 y en Política Web marque la casilla, en Mapa de Parámetro de Autenticación Web seleccione el nombre del parámetro y en Lista de Autenticación seleccione la lista de autenticación creada anteriormente.



Creación de la lista de autenticación WLAN

La WLAN se muestra en la lista WLAN:

WLAN creada

Configuración del perfil de la política

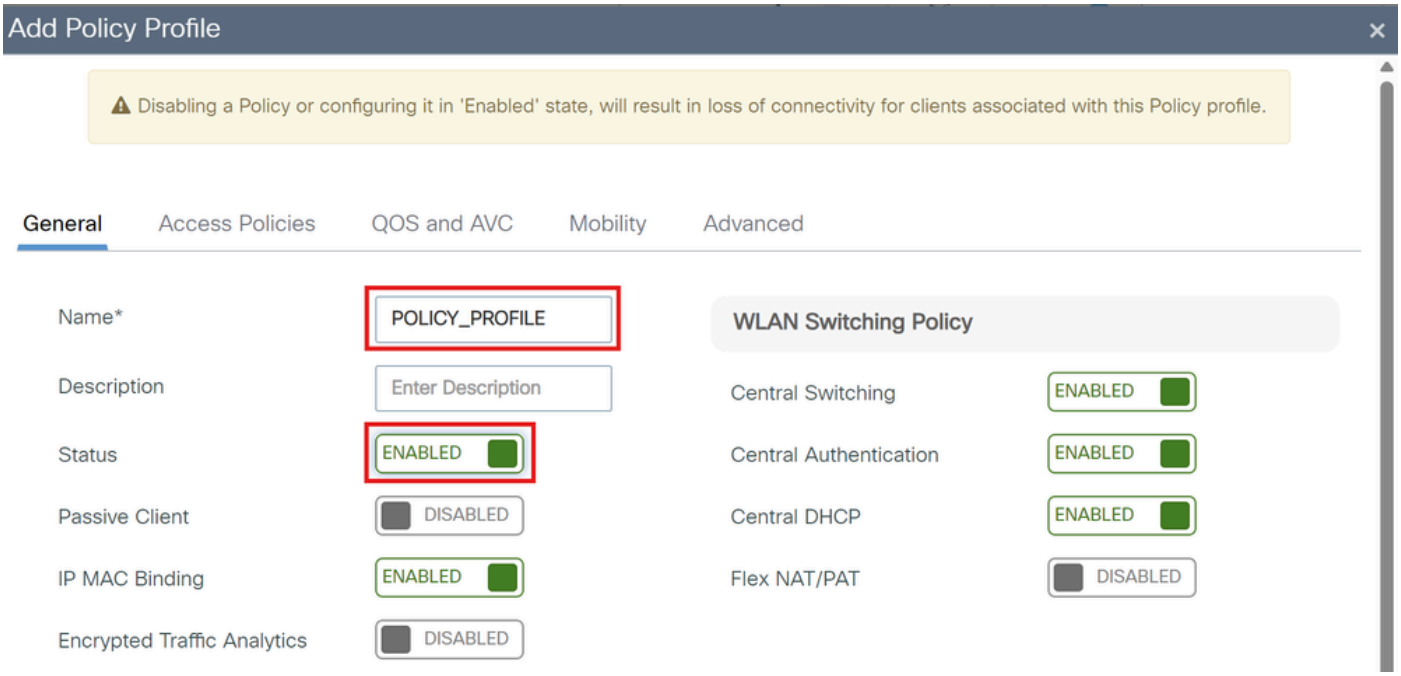
Dentro de un perfil de política, puede seleccionar la VLAN que asigna los clientes, entre otras configuraciones.

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 configure su perfil de política predeterminado o cree uno nuevo.

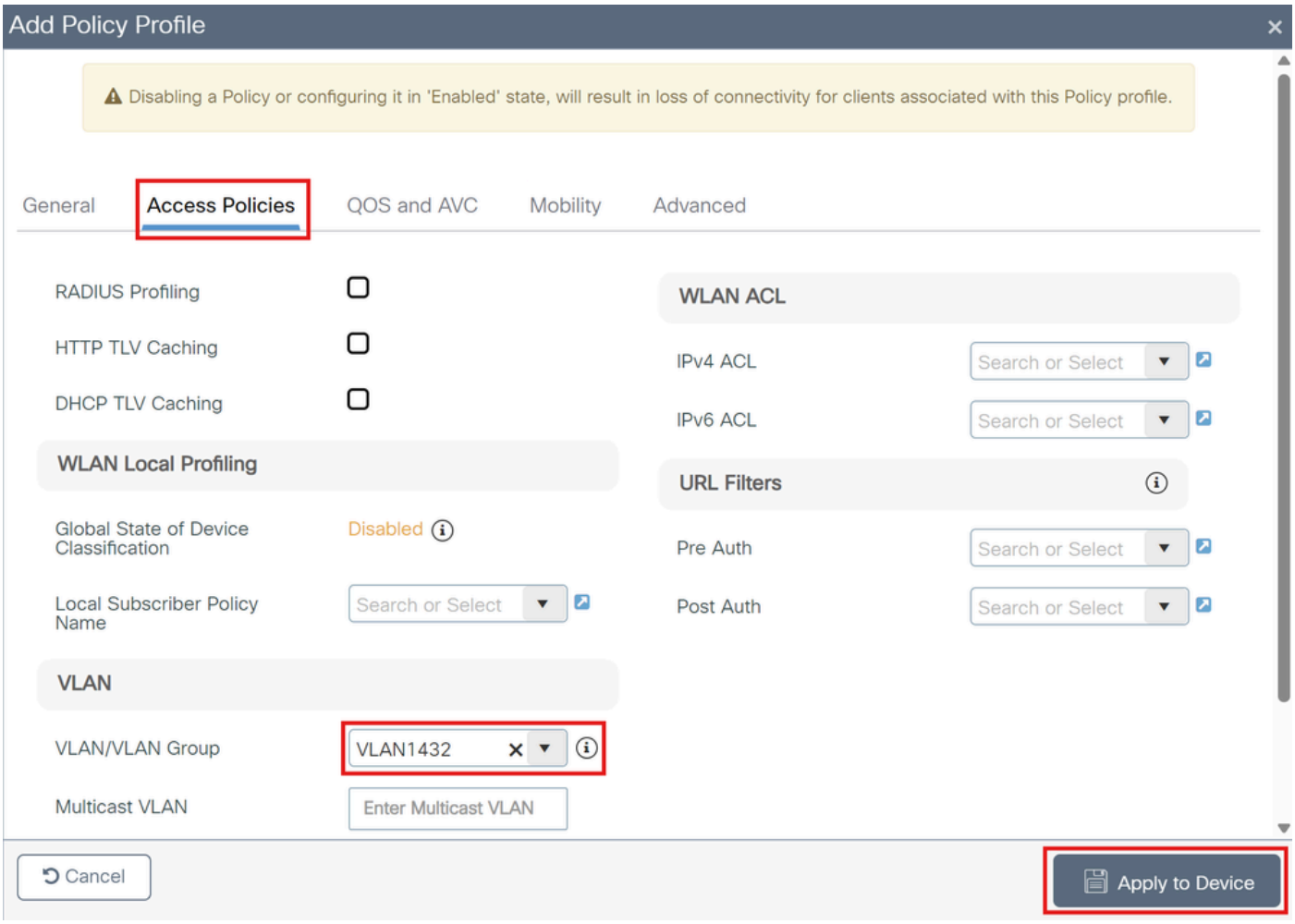
Asegúrese de que el perfil esté habilitado.



Crear un nuevo perfil de política

Paso 2. Seleccione la VLAN.

Vaya a la ficha Políticas de acceso y seleccione el nombre de la VLAN en el menú desplegable o escriba manualmente la ID de VLAN.



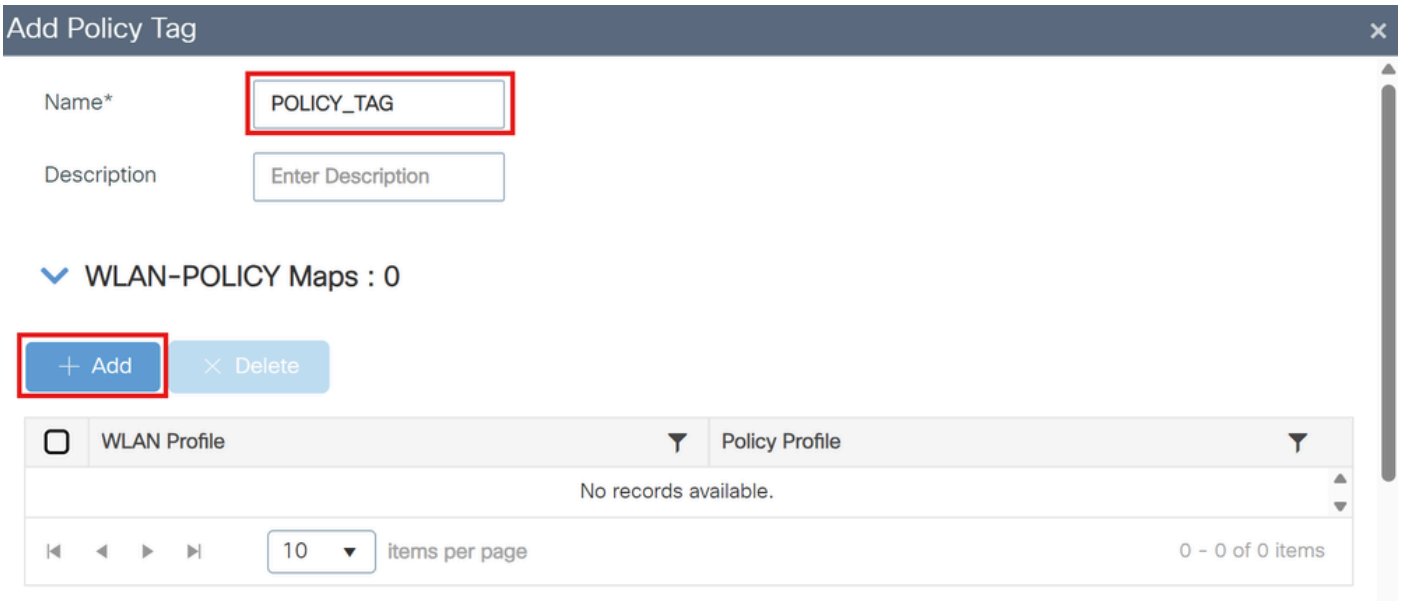
Seleccione la VLAN

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.

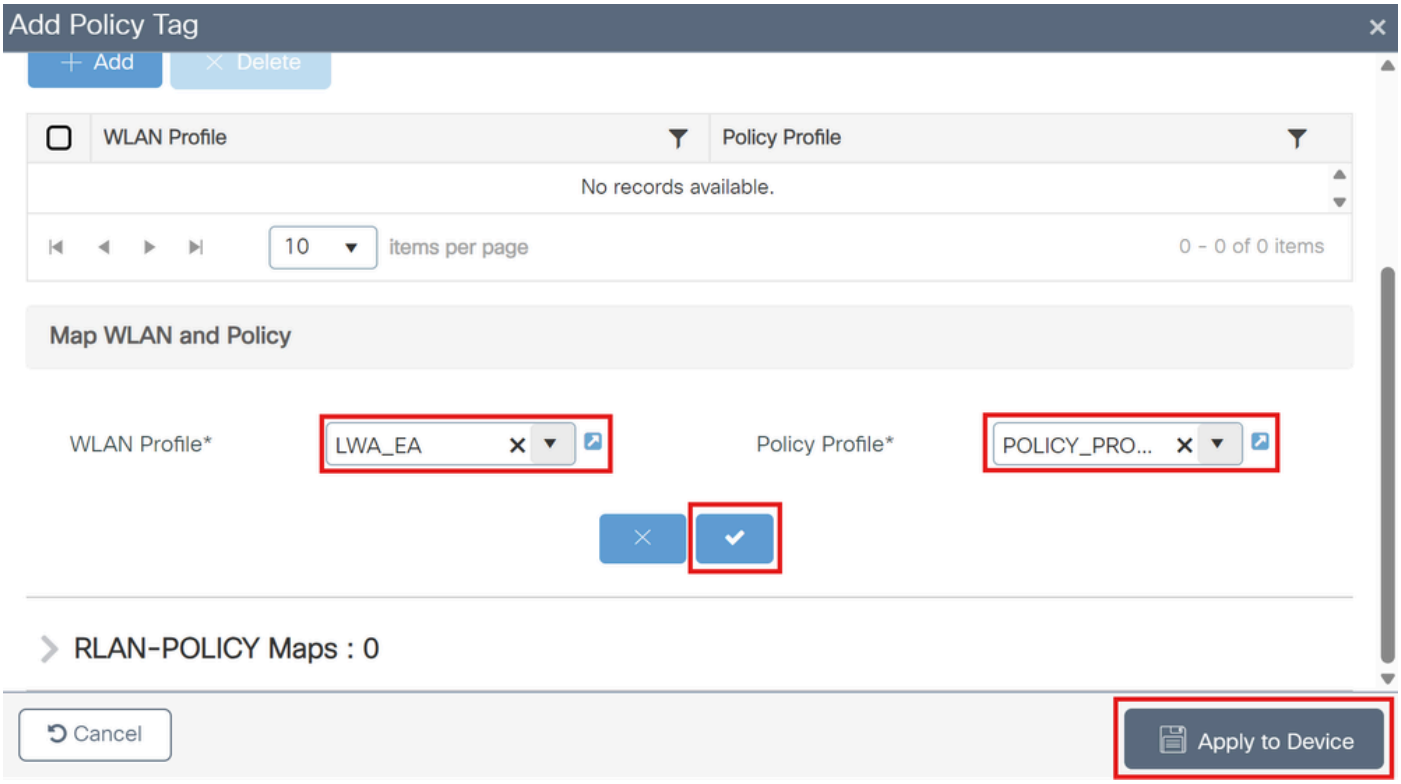
Vaya a Configuración > Etiquetas y perfiles > Etiquetas > Política y agregue una nueva si es necesario, como se muestra en la imagen.

Seleccione + Agregar:



Configuración de etiquetas de políticas

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

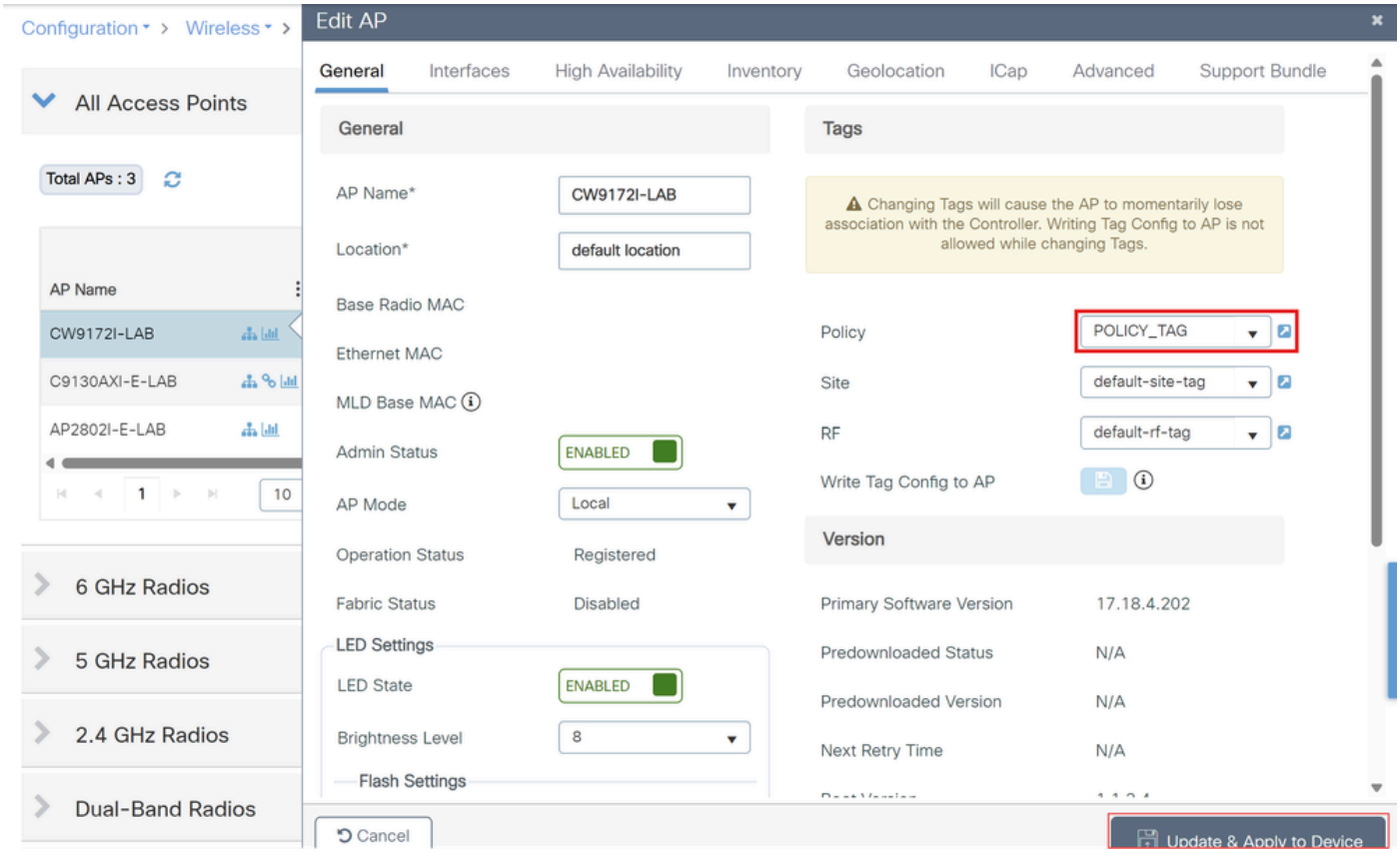


Configuración de etiquetas de políticas

Asignación de etiquetas de políticas

Asigne la etiqueta de política a los AP necesarios.

Para asignar la etiqueta a un AP, vaya a Configuración > Inalámbrica > Puntos de acceso > Nombre del AP > Etiquetas generales, realice la asignación necesaria y, luego, haga clic en Actualizar y aplicar al dispositivo.

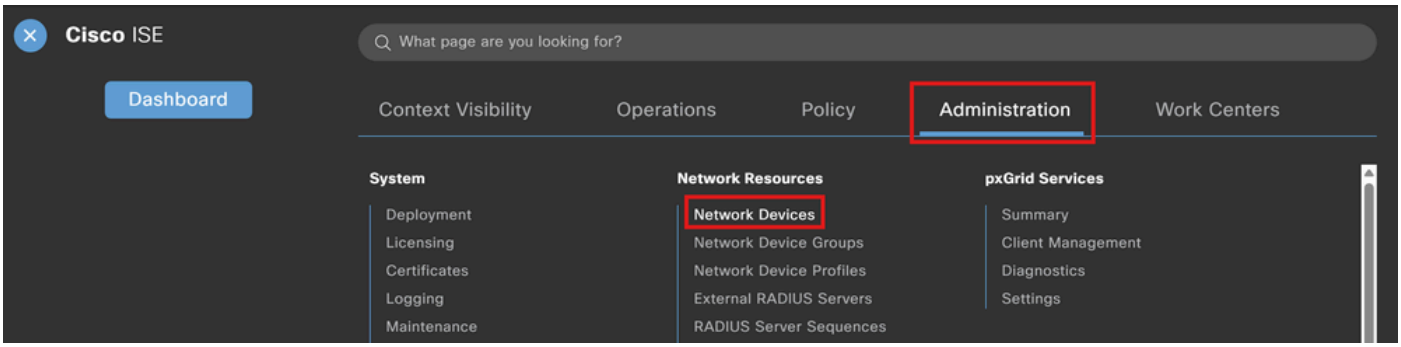


Asignación de etiquetas de políticas

Configuración de ISE

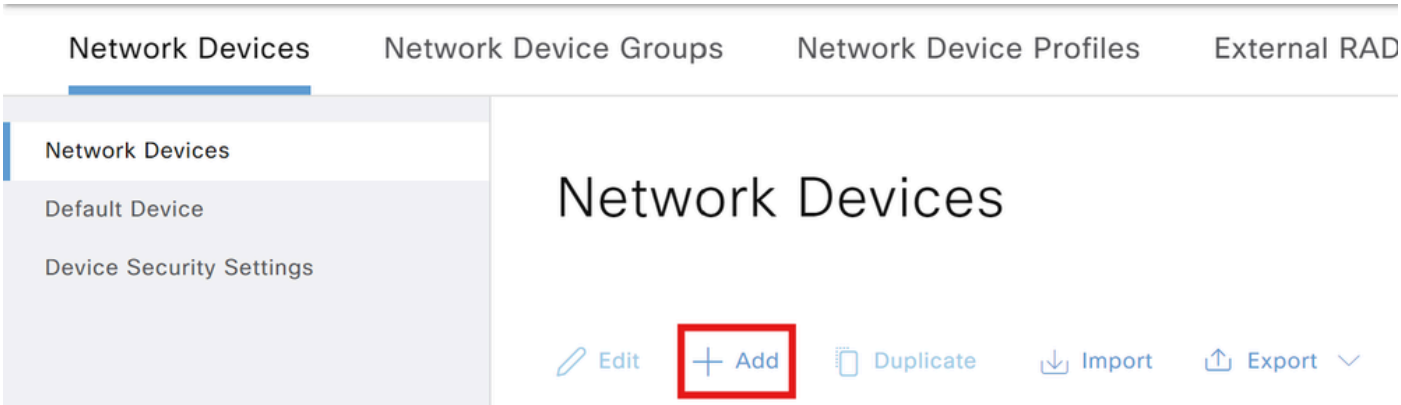
Adición del WLC 9800 a ISE

Paso 1. Vaya a Administration > Network Resources > Network Devices como se muestra en la imagen.



Adición del WLC 9800 a ISE

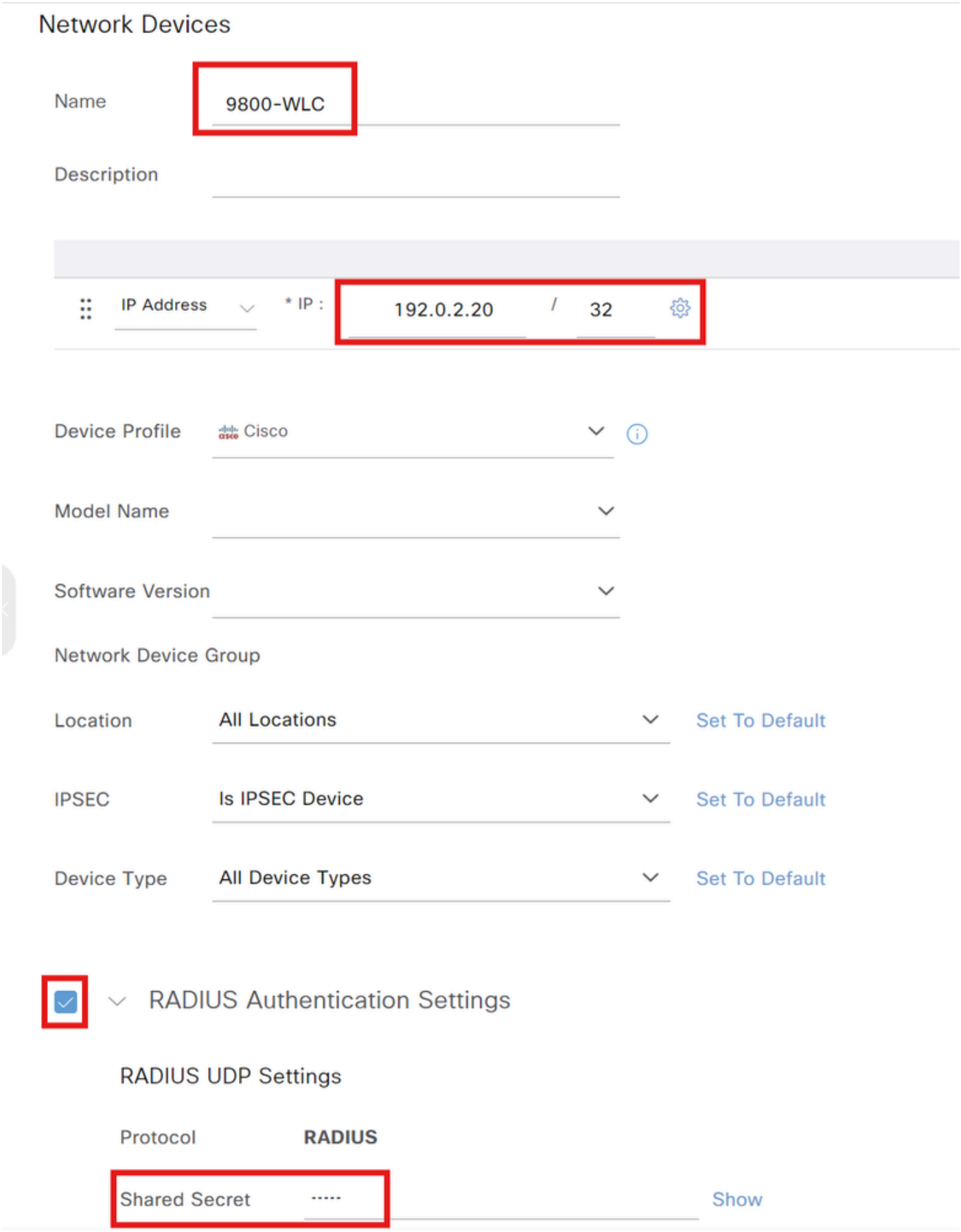
Paso 2. Haga clic en +Agregar.



Agregar dispositivos de red

Opcionalmente, puede ser un nombre de modelo especificado, una versión de software, una descripción o una asignación de grupos de dispositivos de red según los tipos de dispositivos, la ubicación o los WLC.

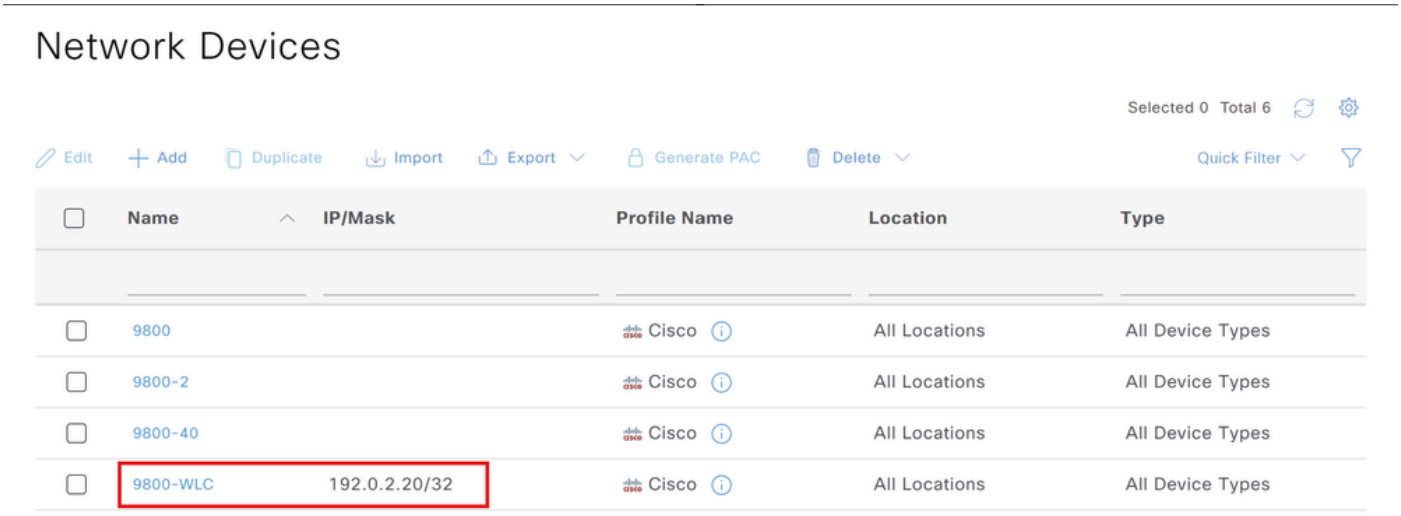
Paso 3. Ingrese los ajustes del WLC 9800 como se muestra en la imagen. Ingrese la misma clave RADIUS definida al crear el servidor en el lado del WLC. A continuación, haga clic en Enviar.



Configuración de WLC 9800

Paso 4. Navegue hasta Administración > Recursos de red > Dispositivos de red, puede ver la lista

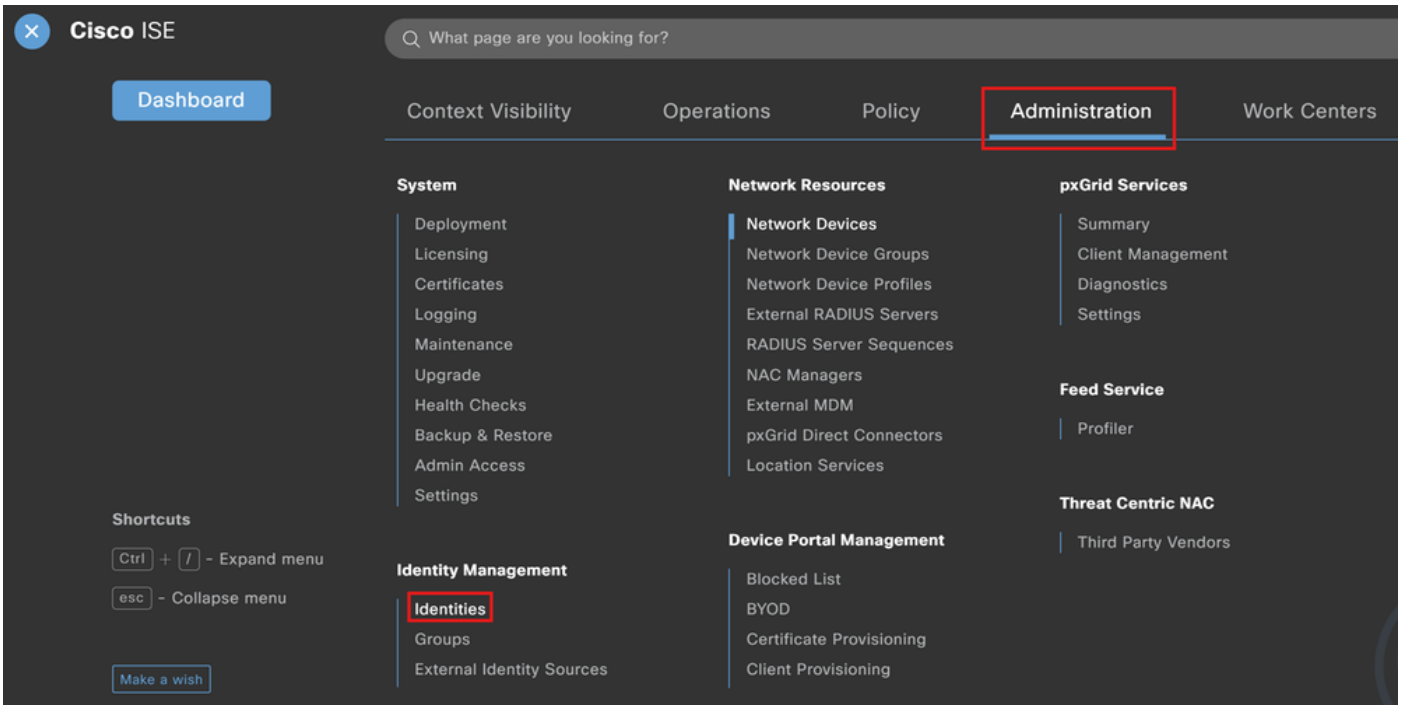
de dispositivos de red.



Lista de dispositivos de red

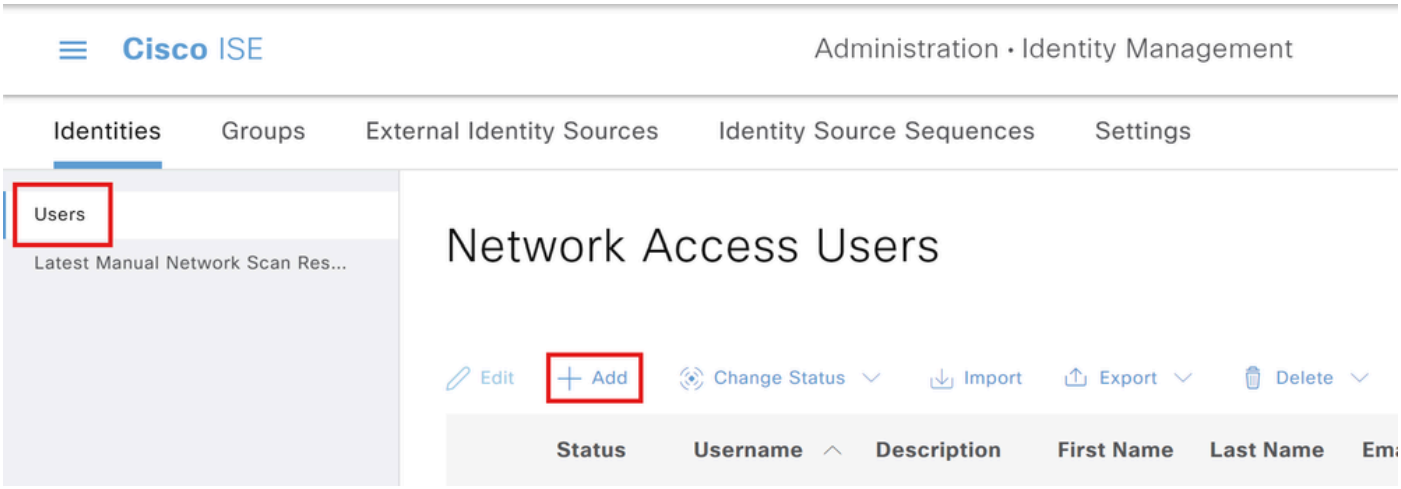
Creación de un usuario nuevo en ISE

Paso 1. Navegue hasta Administración > Gestión de Identidad > Identidades:



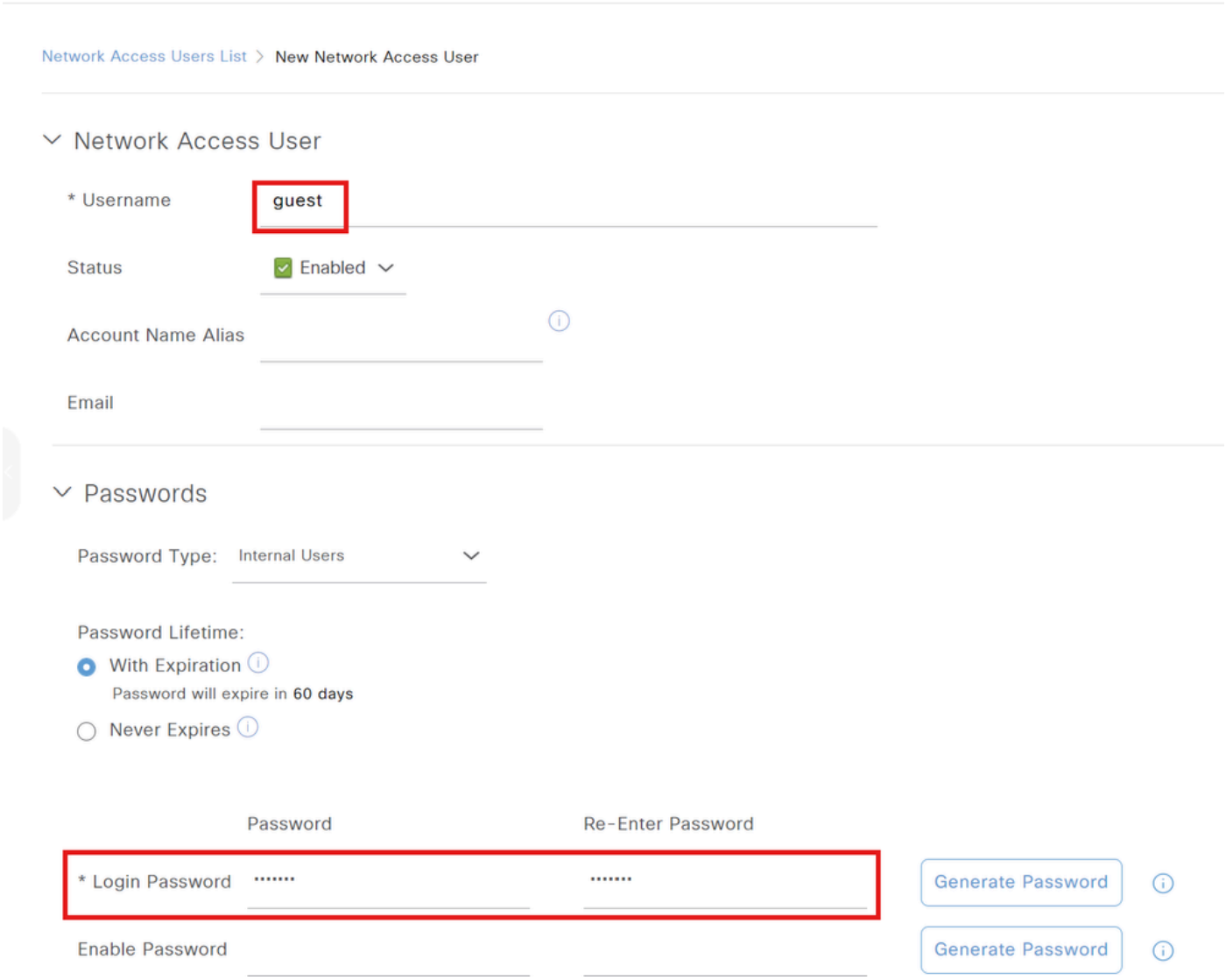
Administración de ISE: identidades

Paso 2. Navegue hasta Usuarios, haga clic en +Agregar.



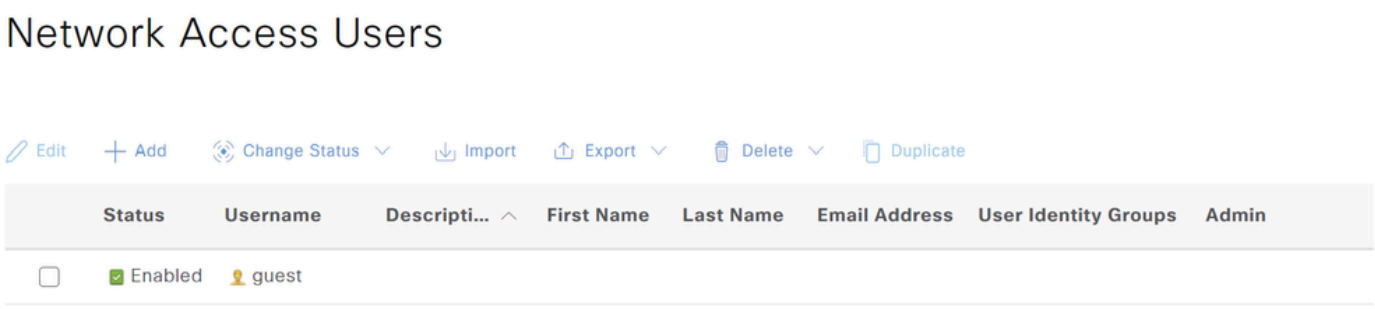
Agregar usuario

Paso 3. Introduzca el nombre de usuario y la contraseña del usuario invitado y haga clic en Enviar.



Creación de un usuario nuevo en ISE

Paso 4. Navegue hasta Administration > Identity Management > Identities > Users, puede ver la lista de usuarios.



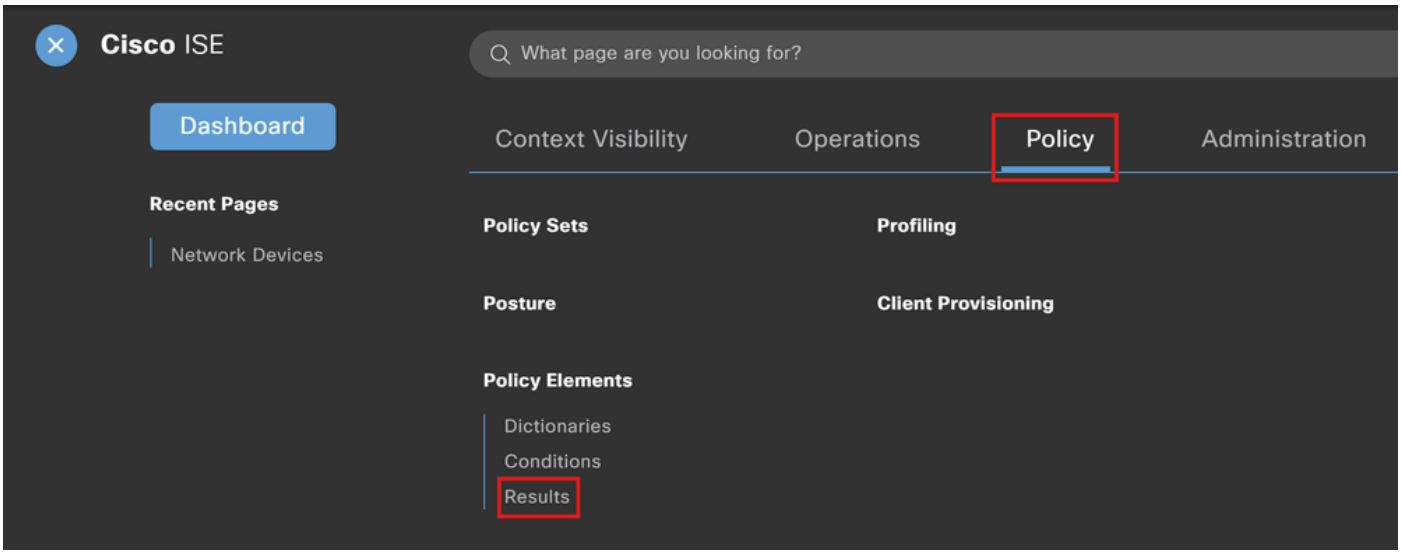
Lista de usuarios de acceso a red

Creación del perfil de autorización

El perfil de política es el resultado asignado a un cliente según sus parámetros (dirección MAC, credenciales, WLAN utilizada, etc.). Puede asignar configuraciones específicas, como redes de área local virtuales (VLAN), listas de control de acceso (ACL), redireccionamientos del localizador uniforme de recursos (URL), etc.

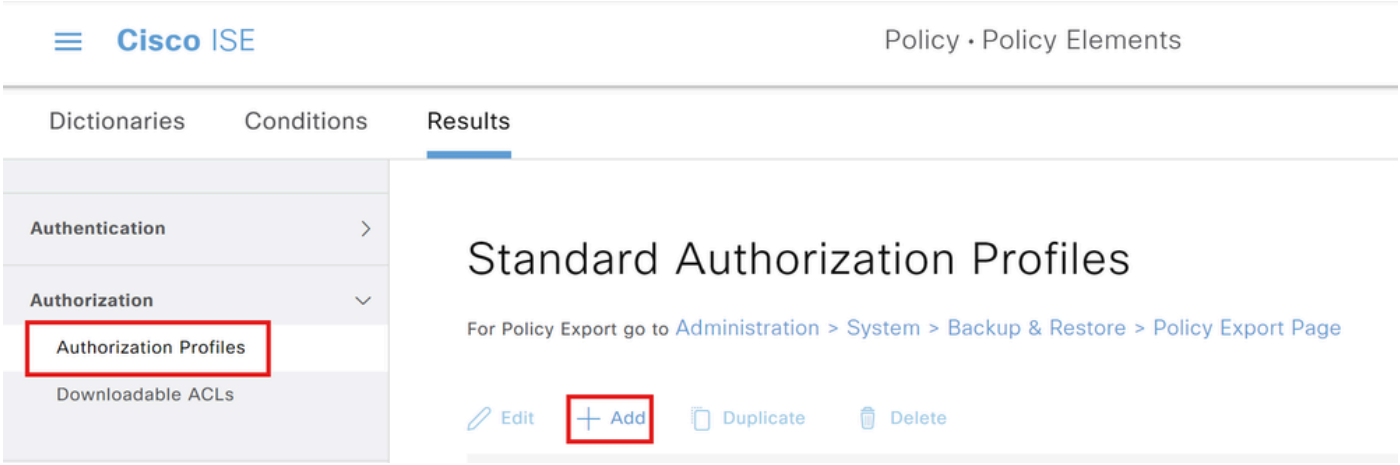
Estos pasos muestran cómo crear el perfil de autorización necesario para redirigir al cliente al portal de autenticación. Tenga en cuenta que en versiones recientes de ISE ya existe un resultado de autorización Cisco_Webauth. Aquí puede editarlo para modificar el nombre de la ACL de redireccionamiento para que coincida con lo que configuró en el WLC.

Paso 1. Navegue hasta Política > Elementos de Política > Resultados.



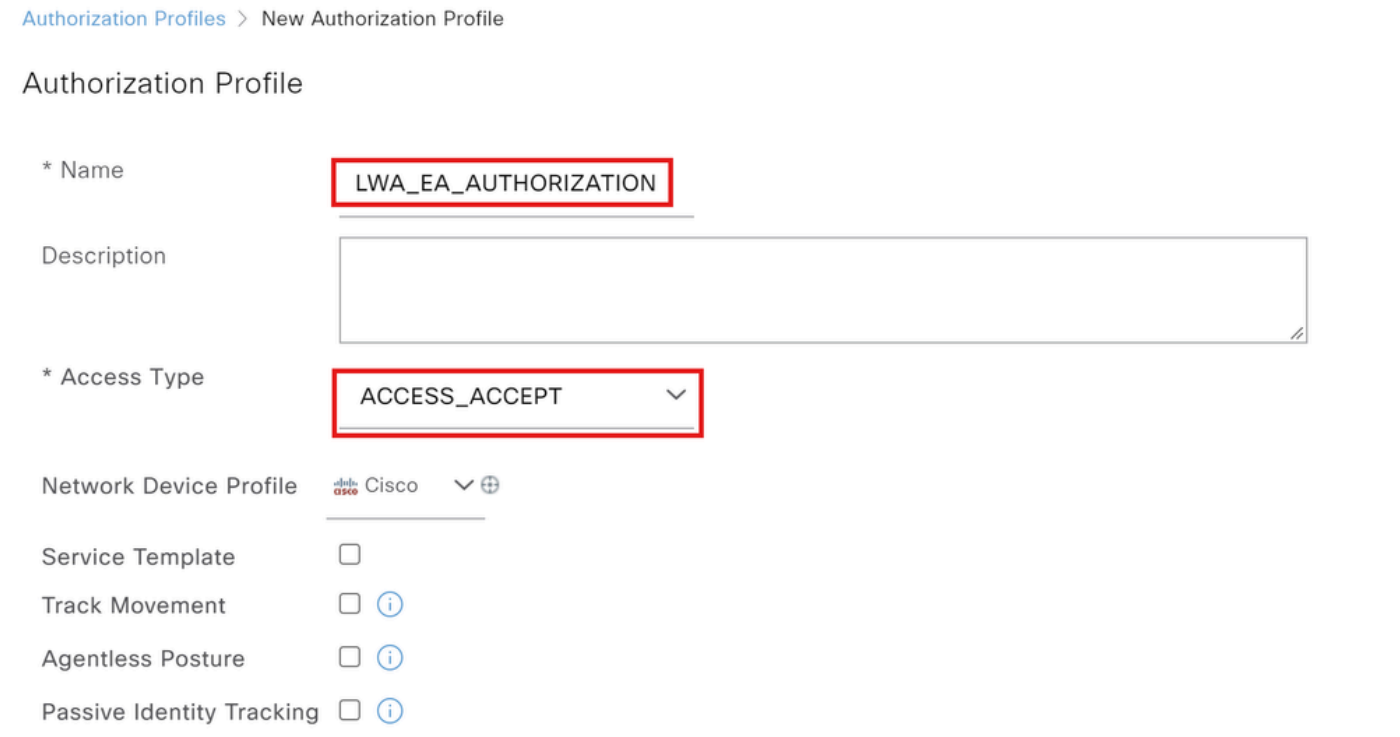
Política de ISE - Resultados

Paso 2. Vaya a Autorización > Perfiles de autorización. Haga clic en +Agregar para crear el perfil de autorización.



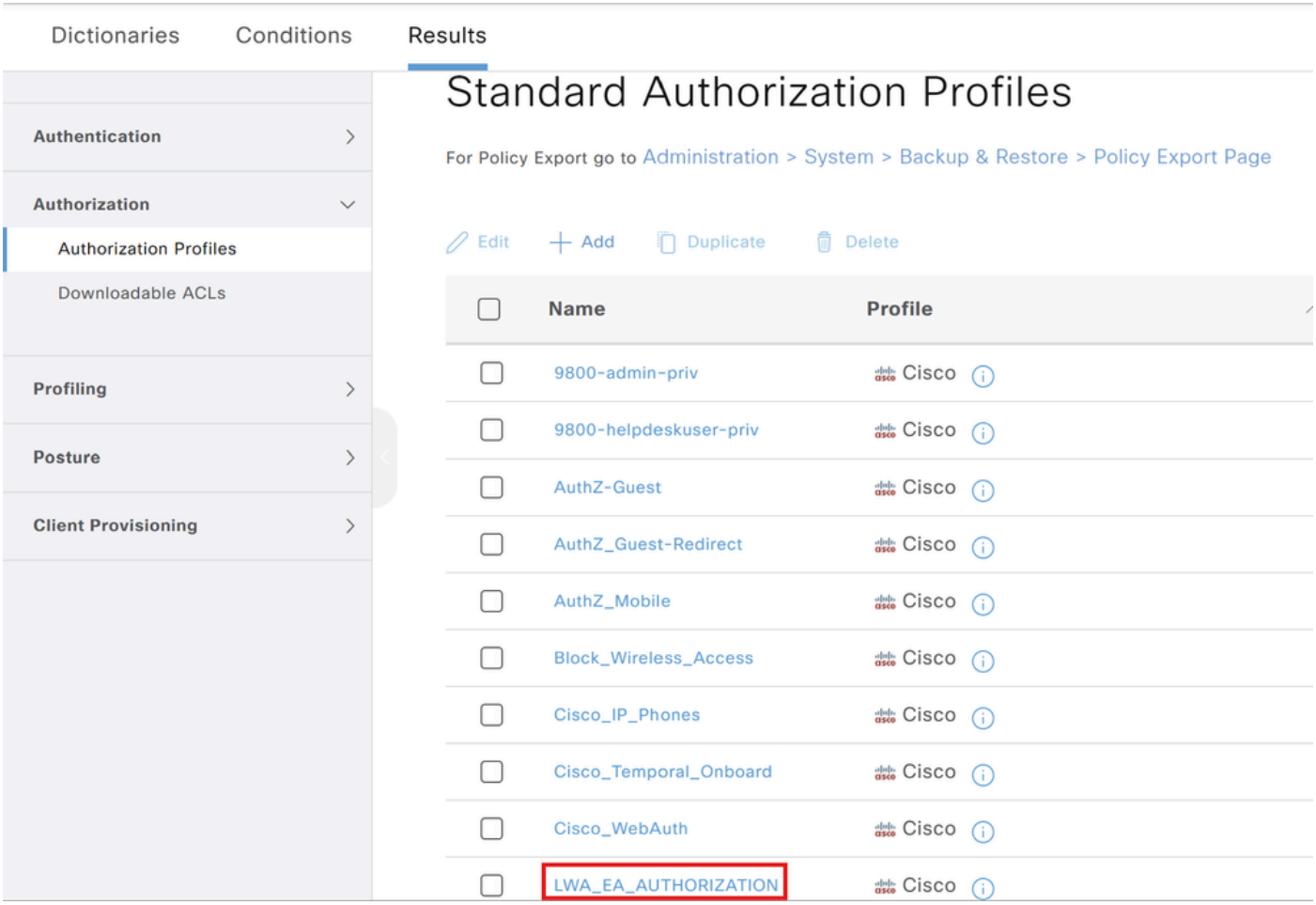
Agregar perfil de autorización

Paso 3. Cree el perfil de autorización LWA_EA_AUTHORIZATION. Los detalles de los atributos deben ser Access Type=ACCESS_ACCEPT. Haga clic en Submit (Enviar).



Creación del perfil de autorización

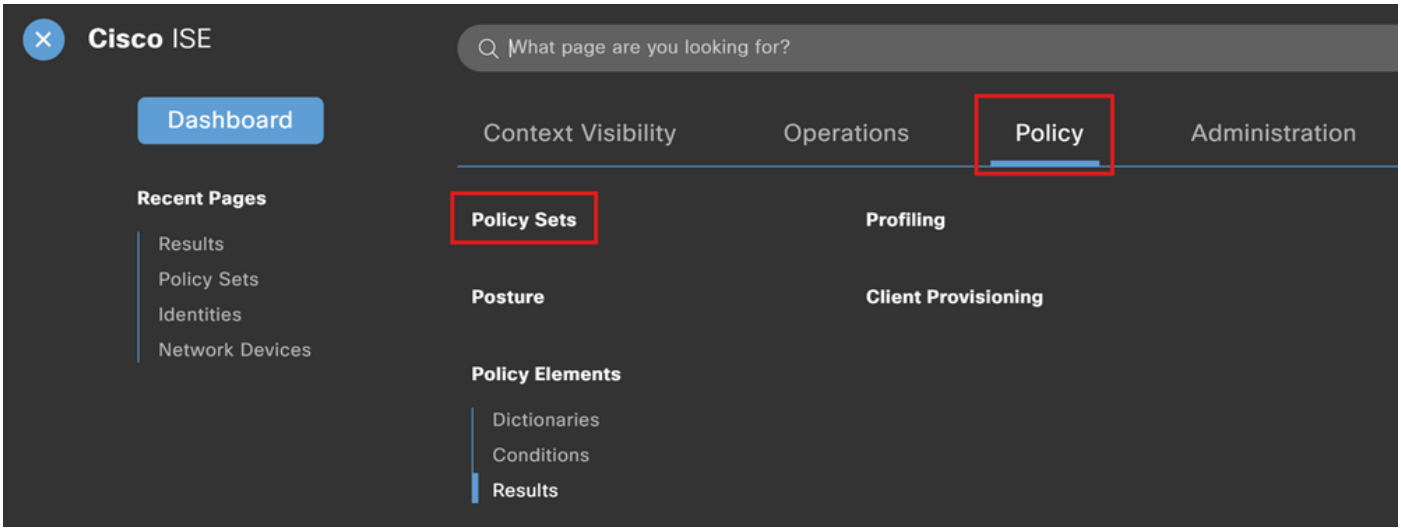
Paso 4. Navegue hasta Política > Elementos de Política > Resultados > Autorización > Perfiles de Autorización, puede ver los perfiles de autorización.



Lista de perfiles de autorización

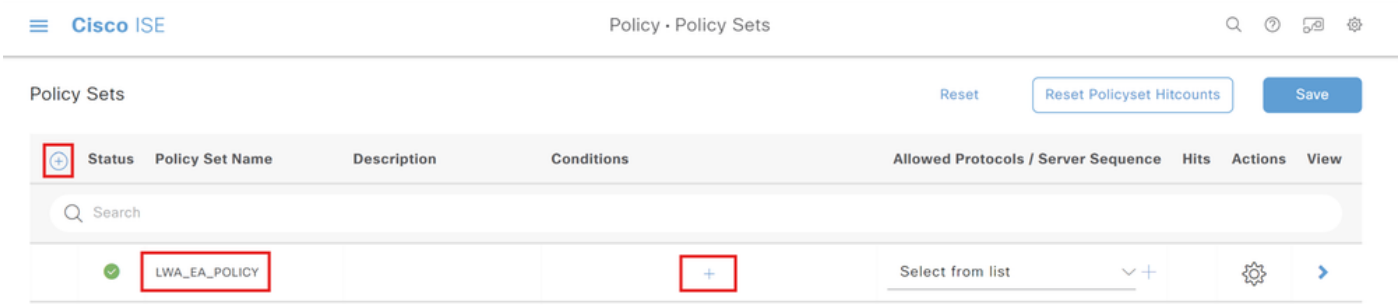
Configuración de la regla de autenticación

Paso 1. Vaya a Política > Juegos de Políticas.



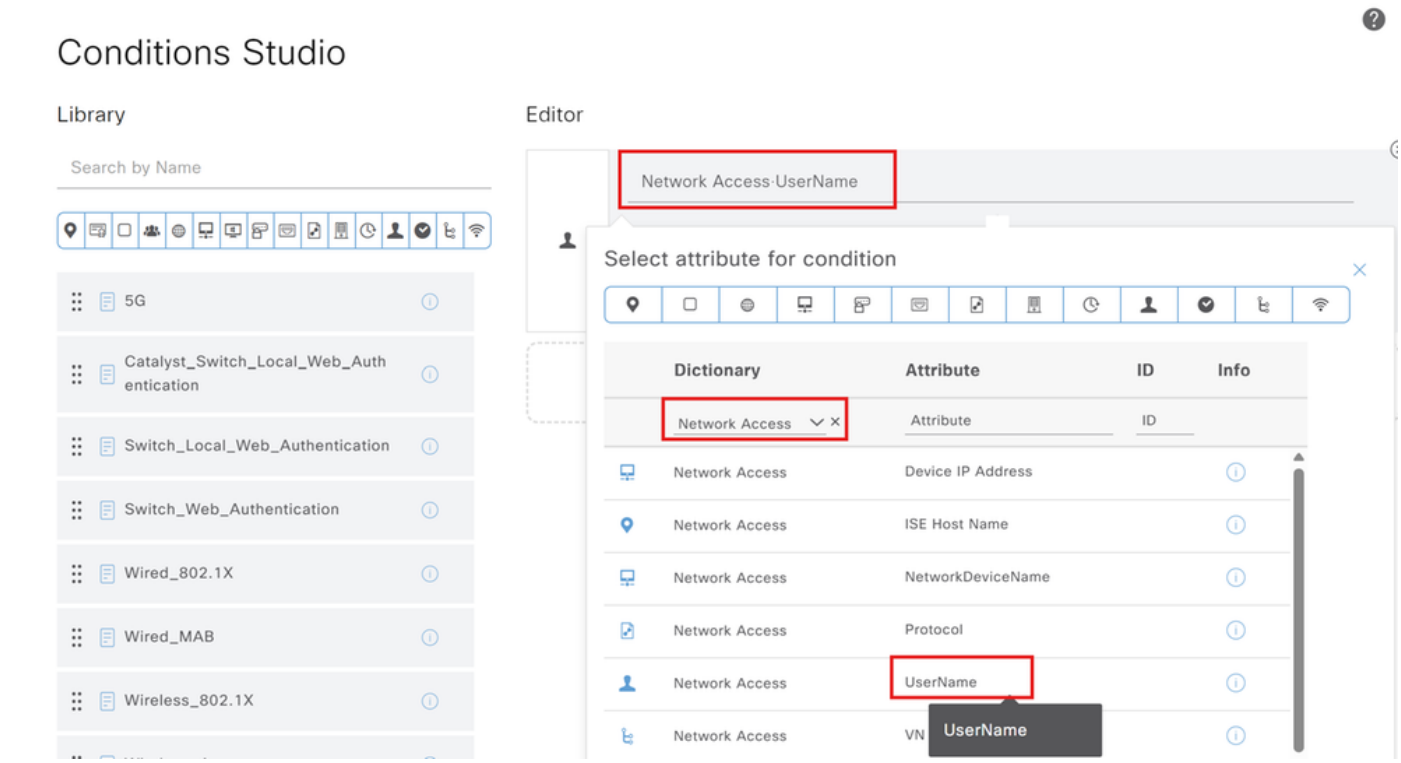
Política de ISE: conjuntos de políticas

Paso 2. Seleccione el signo + y escriba el nombre del juego de políticas LWA_EA_POLICY. Haga clic en la columna Condiciones.



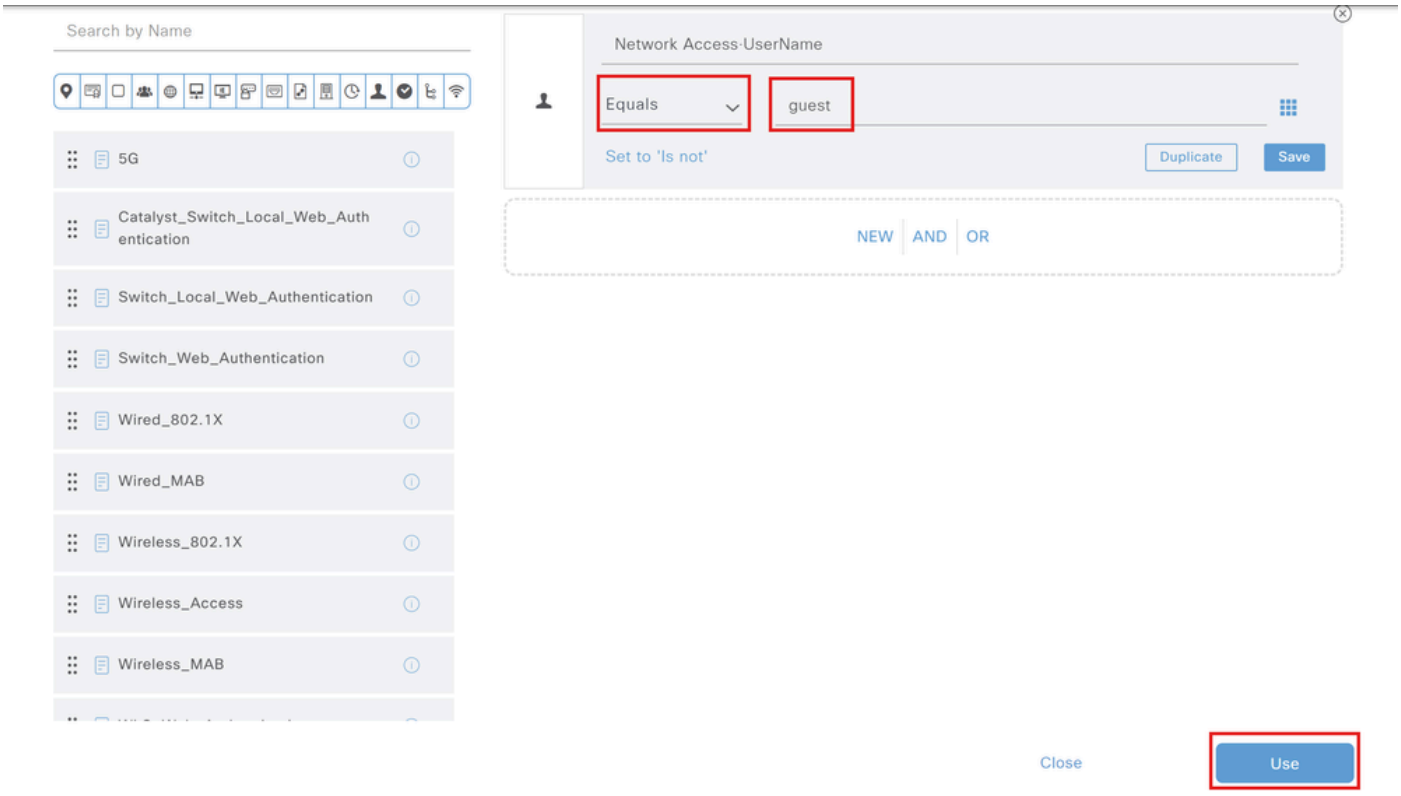
Configuración de la regla de autenticación

Paso 3. En Diccionario, seleccione Acceso a la red. En Atributo, seleccione Nombre de usuario.



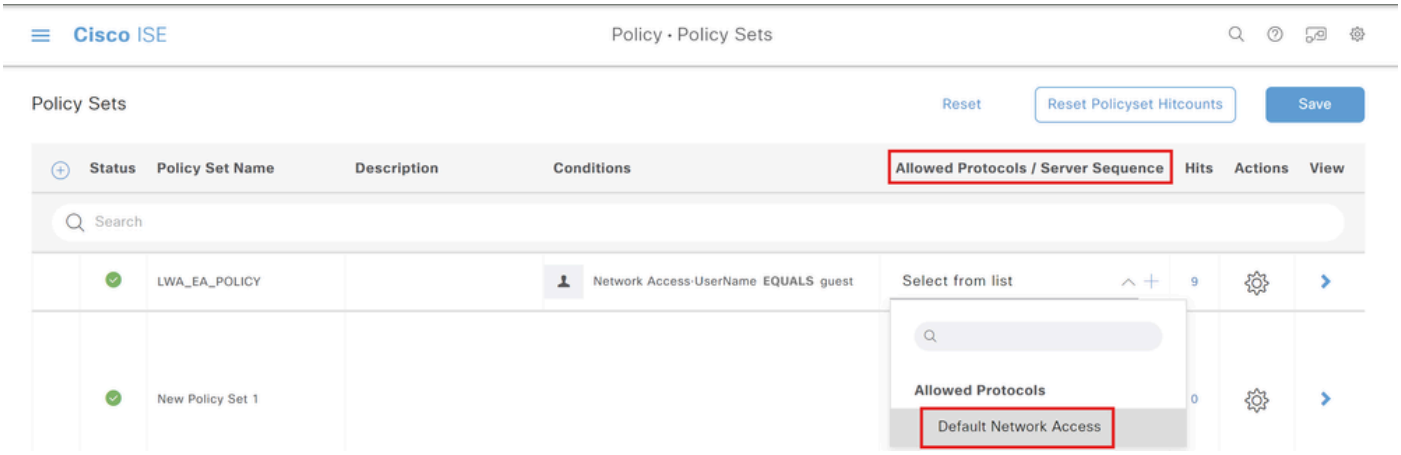
Acceso a red Diccionario

Paso 4. Establezca Equals y escriba guest en el cuadro de texto (el nombre de usuario definido en Administration > Identity Management > Identities > Users). Haga clic en Save para guardar los cambios.



Nombre de usuario invitado

Paso 5. Navegue hasta Política > Juegos de Políticas. En el conjunto de directivas que ha creado, en la columna Protocolos permitidos/Secuencia de servidor, seleccione Acceso de red predeterminado.



Conjuntos de políticas

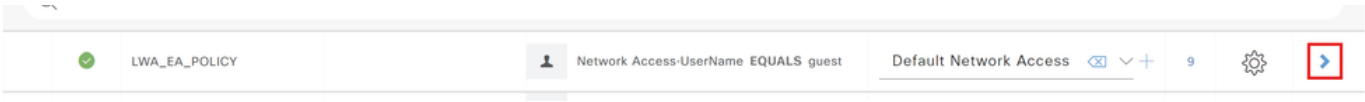
Paso 6. Haga clic en Guardar para guardar los cambios.

Configuración de las reglas de autorización

La regla de autorización es la encargada de determinar qué resultado de permiso (perfil de

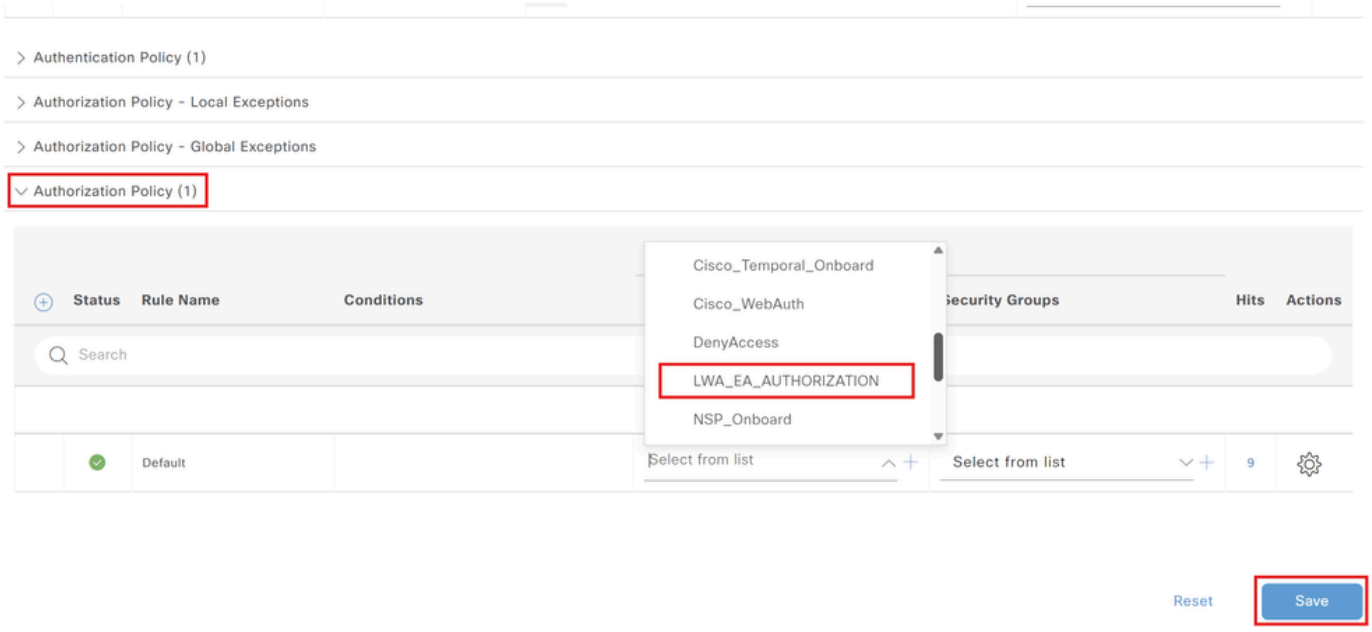
autorización) se aplica al cliente.

Paso 1. Vaya a Política > Juegos de Políticas. Haga clic en el icono de flecha del conjunto de directivas que ha creado.



Flecha del conjunto de políticas

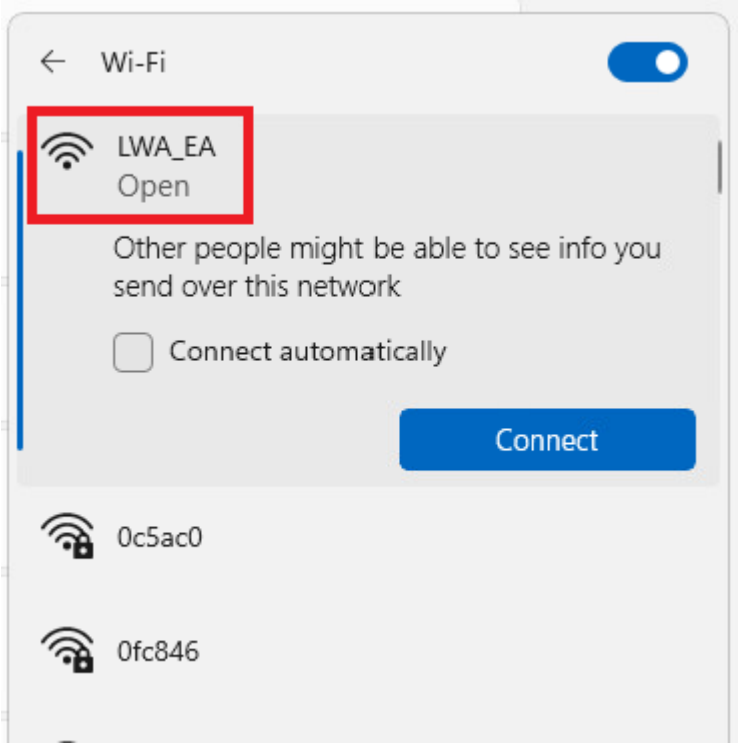
Paso 2. En la misma página Conjunto de políticas, expanda Política de autorización como se muestra en la imagen. En la columna Profiles, elimine DenyAccess y agregue LWA_EA_AUTHORIZATION. Haga clic en Save para guardar los cambios.



Política de autorización

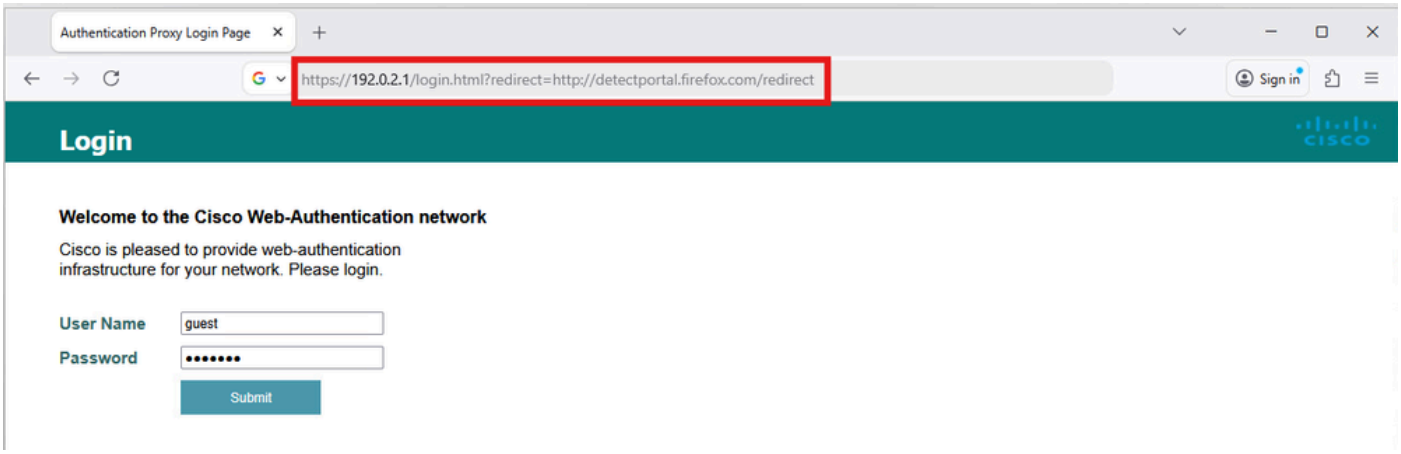
Conectar cliente invitado

Paso 1. En el ordenador/teléfono, navegue hasta las redes Wi-Fi, busque el SSID LWA_EA y seleccione Connect.



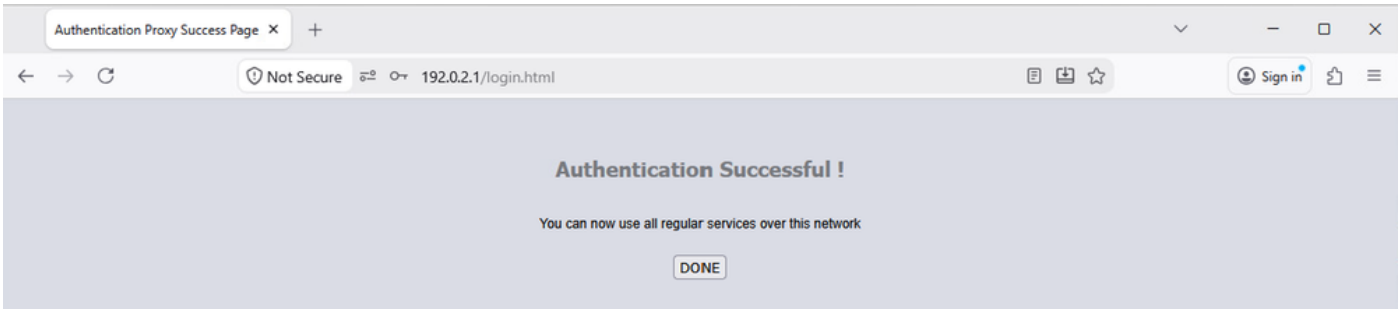
Conectar cliente invitado

Paso 2. Aparece una ventana del navegador, con la página de inicio de sesión. La URL de redirección se encuentra en el cuadro URL, y debe escribir el Nombre de usuario y la Contraseña para obtener acceso a la red. A continuación, seleccione Enviar.



Página de inicio de sesión con URL de redirección

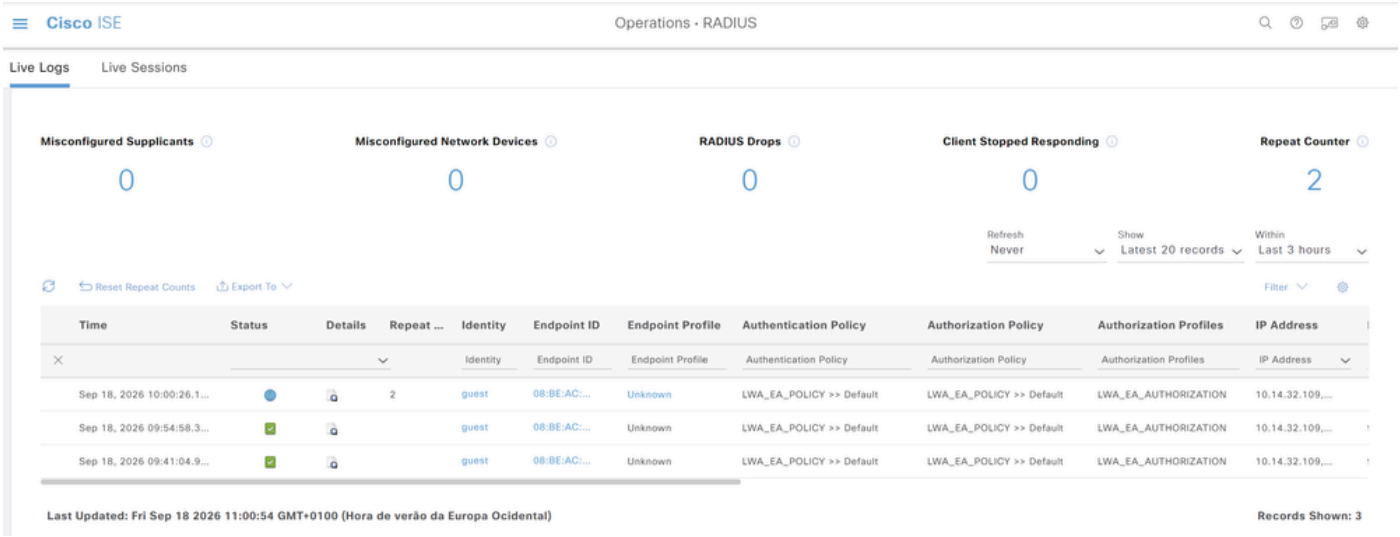
Si las credenciales son correctas, aparece una página de autenticación correcta:



Página Autenticación: Conexión Satisfactoria

Nota: La URL presentada fue proporcionada por el WLC. Contiene la IP virtual del WLC y el redireccionamiento para la URL de la prueba de la conexión de Windows.

Paso 3. Navegue hasta Operaciones > RADIUS > Registros en vivo. Puede ver el dispositivo cliente autenticado, junto con sus directivas de autenticación y autorización.



Registros activos de Radius

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Show WLAN Summary

```
<#root>

9800WLC#show wlan summary

Number of WLANs: 1
```

```
ID Profile Name SSID Status 2.4GHz/5GHz Security
-----------------------------------------------
```

1 LWA_EA LWA_EA UP [open],[Web Auth]

```
9800WLC#
```

show wlan name LWA_EA

```
WLAN Profile Name : LWA_EA
==========================================
Identifier : 1
Description :
Network Name (SSID) : LWA_EA
Status : Enabled
Broadcast SSID : Enabled
Advertise-Apname : Disabled
Universal AP Admin : Disabled
(...)
Accounting list name :
802.1x authentication list name : Disabled
802.1x authorization list name : Disabled
Security
```

Web Based Authentication : Enabled

```
OWE Transition Mode : Disabled
Conditional Web Redirect : Disabled
Splash-Page Web Redirect : Disabled
Webauth On-mac-filter Failure : Disabled
```

Webauth Authentication List Name : LWA_AUTHENTICATION

Webauth Authorization List Name : Disabled

Webauth Parameter Map : global

```
(...)
Security-2.4GHz/5GHz
```

802.11 Authentication : Open System

```
Static WEP Keys : Disabled
```

Wi-Fi Protected Access (WPA/WPA2/WPA3) : Disabled

```
OSEN : Disabled
PMF Support : Disabled
(...)
Band Select : Disabled
Load Balancing : Disabled
(...)
```

Show Parameter Map Configuration

9800WLC#show running-config | section parameter-map type webauth global

```
parameter-map type webauth global
type webauth
virtual-ip ipv4 192.0.2.1
trustpoint TP-self-signed-123456
```

Show AAA Information

<#root>

9800WLC#show aaa method-lists authentication

```
authen queue=AAA_ML_AUTHEN_LOGIN
```

name=LWA_AUTHENTICATION valid=TRUE id=BD000005 :state=ALIVE : SERVER_GROUP RADIUSGROUP

```
authen queue=AAA_ML_AUTHEN_ENABLE
authen queue=AAA_ML_AUTHEN_PPP
authen queue=AAA_ML_AUTHEN_SGBP
(...)
```

9800WLC#show aaa method-lists authorization

```
author queue=AAA_ML_AUTHOR_SHELL
author queue=AAA_ML_AUTHOR_NET
```

name=LWA_AUTHORIZATION valid=TRUE id=90000006 :state=ALIVE : SERVER_GROUP RADIUSGROUP

```
author queue=AAA_ML_AUTHOR_CONN
author queue=AAA_ML_AUTHOR_IPMOBILE
author queue=AAA_ML_AUTHOR_RM
(...)
```

9800WLC#show aaa servers

```
RADIUS: id 2, priority 1, host 192.0.2.30, auth-port 1812, acct-port 1813, hostname RADIUS


State: current UP, duration 8421s, previous duration 0s
Dead: total time 0s, count 0
Platform State from SMD: current UP, duration 8421s, previous duration 0s
SMD Platform Dead: total time 0s, count 0
Platform State from WNCD (0) : current UP
(...)
```

Troubleshoot

Problemas comunes

Éstas son varias guías sobre cómo resolver problemas de autenticación Web, tales como:

- Los usuarios no pueden autenticarse.
- Problemas de certificado.
- La URL de redirección no funciona.
- Los usuarios invitados no pueden conectarse a la WLAN de invitado.
- Los usuarios no obtienen una dirección IP.
- Error al redirigir a la página de inicio de sesión de autenticación Web.
- Después de la autenticación correcta, los usuarios invitados no pueden obtener acceso a Internet.

Estas guías describen detalladamente los pasos para solucionar problemas:

- Solucionar problemas comunes de autenticación Web
- Otras situaciones a resolver

Depuración condicional y seguimiento activo de radio y captura de paquetes incrustada

Puede habilitar el seguimiento de depuración condicional y captura de Radio Active (RA), que proporciona seguimientos de nivel de depuración para todos los procesos que interactúan con la condición especificada (dirección MAC del cliente en este caso). Para habilitar la depuración condicional, utilice los pasos de la guía, Depuración condicional y seguimiento de RadioActive.

También puede recopilar la captura de paquetes integrados (EPC). EPC es una función de captura de paquetes que permite una vista de los paquetes destinados a, originados y que pasan

a través de los WLC Catalyst 9800, concretamente los paquetes GET DHCP, DNS y HTTP en LWA. Estas capturas se pueden exportar para analizarlas sin conexión con Wireshark. Para ver los pasos detallados sobre cómo hacerlo, consulte Captura de Paquetes Integrada.

Ejemplo de un intento exitoso

Este es el resultado de RA_traces para un intento exitoso de identificar cada una de las fases en el proceso de asociación/autenticación, mientras está en conexión con un SSID de invitado con el servidor RADIUS.

Asociación/autenticación 802.11:

[client-orch-sm] [17062]: (nota): MAC: 08be.ac3f Asociación recibida. BSSID cc70.edcf.552f, WLAN LWA_EA, Slot 1 AP 2ce3.8eb4, CW9172I-LAB
[client-orch-sm] [17062]: (depuración): MAC: 08be.ac3f Se recibió una solicitud de asociación Dot11. Procesamiento iniciado, SSID: LWA_EA, Perfil de política: POLICY_PROFILE, Nombre de AP: CW9172I-LAB, Ap Dirección Mac: 2ce3.8eb4BSSID ID MAC0000.0000.0000wlan: 1RSSI: -49, SNR: 46
[client-orch-state] [17062]: (nota): MAC: 08be.ac3f Transición de estado de cliente: S_CO_INIT -> S_CO_ASSOCIATING
[dot11-validate] [17062]: (información): MAC: 08be.ac3f Dot11 es decir validar las velocidades ext/supp. Validación aprobada para tasas admitidas radio_type 2
[dot11-validate] [17062]: (información): MAC: 08be.ac3f WiFi directo: Dot11 valida el IE P2P. El IE P2P no está presente.
[dot11] [17062]: (depuración): MAC: 08be.ac3f dot11 envía respuesta de asociación. Respuesta de asociación de tramas con resp_status_code: 0
[dot11] [17062]: (depuración): MAC: 08be.ac3f Dot11 Información de capacidad byte1 1, byte2: 11
[dot11-frame] [17062]: (información): MAC: 08be.ac3f WiFi directo: omitir compilación Assoc Resp con P2P IE: Política de Wifi Direct desactivada
[dot11] [17062]: (información): MAC: 08be.ac3f dot11 envía respuesta de asociación. Enviando respuesta assoc de longitud: 130 con resp_status_code: 0, DOT11_STATUS: DOT1_STATUS_SUCCESS
[dot11] [17062]: (nota): MAC: 08be.ac3f Éxito de asociación. AID 1, Itinerancia = Falso, WGB = Falso, 11r = Falso, 11w = Itinerancia rápida falsa = Falso
[dot11] [17062]: (información): MAC: 08be.ac3f Transición de estado DOT11: S_DOT11_INIT -> S_DOT11_ASSOCIATED
[client-orch-sm] [17062]: (depuración): MAC: La asociación Dot11 de la estación 08be.ac3f se ha realizado correctamente.

Proceso de aprendizaje de IP:

[client-orch-state] [17062]: (nota): MAC: 08be.ac3f Transición de estado de cliente: S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LEARN_IN_PROGRESS
[client-iplearn] [17062]: (información): MAC: 08be.ac3f Transición de estado de aprendizaje de IP: S_IPLEARN_INIT -> S_IPLEARN_IN_PROGRESS
[client-auth] [17062]: (información): MAC: 08be.ac3f Transición de estado de interfaz de autenticación de cliente: S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_L2_WEBAUTH_DONE
[client-iplearn] [17062]: (nota): MAC: 08be.ac3f La IP del cliente se ha aprendido correctamente. Método: IP de DHCP: 10.14.32.109
[client-iplearn] [17062]: (información): MAC: 08be.ac3f Transición de estado de aprendizaje de IP: S_IPLEARN_IN_PROGRESS -> S_IPLEARN_COMPLETE
[client-orch-sm] [17062]: (depuración): MAC: 08be.ac3f Respuesta de aprendizaje de ip recibida. método: IPLEARN_METHOD_DHCP

Autenticación de capa 3:

[client-orch-sm] [17062]: (depuración): MAC: 08be.ac3f Autenticación L3 activada. estado = 0x0, correcto
[client-orch-state] [17062]: (nota): MAC: 08be.ac3f Transición de estado de cliente: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_L3_AUTH_IN_PROGRESS
[client-auth] [17062]: (nota): MAC: Autenticación L3 08be.ac3f iniciada. LWA
[client-auth] [17062]: (información): MAC: 08be.ac3f Transición de estado de interfaz de autenticación de cliente: S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_WEBAUTH_PENDING

[webauth-httpd] [17062]: (información): capwap_90000004[08be.ac3f][10.14.32.109]GET rcvd cuando está en estado LOGIN
[webauth-httpd] [17062]: (información): capwap_90000004[08be.ac3f][10.14.32.109]HTTP GET request
[webauth-httpd] [17062]: (información): capwap_90000004[08be.ac3f][10.14.32.109]Parse GET, src [10.14.32.109] dst [10.107.221.82] url [http://firefox detect portal/]
[webauth-httpd] [17062]: (información): capwap_90000004[08be.ac3f][10.14.32.109]Leer completo: parse_request return 8
[webauth-io] [17062]: (información): capwap_90000004[08be.ac3f][10.14.32.109]56538/219 estado de E/S READING -> WRITING
[webauth-io] [17062]: (información): capwap_90000004[08be.ac3f][10.14.32.109]56538/219 ESTADO DE E/S ESCRITURA -> LECTURA
[webauth-io] [17062]: (información): capwap_90000004[08be.ac3f][10.14.32.109]56539/218 estado de E/S NEW -> READING
[webauth-io] [17062]: (información): capwap_90000004[08be.ac3f][10.14.32.109]56539/218 Read event, Message ready
[webauth-httpd] [17062]: (información): capwap_90000004[08be.ac3f][10.14.32.109]POST rcvd cuando está en estado LOGIN

Autenticación de capa 3 exitosa, mueva el cliente al estado RUN:

[auth-mgr] [17062]: (información): [08be.ac3f:capwap_90000004] Se recibió el nombre de usuario invitado para el cliente 08be.ac3f
[auth-mgr] [17062]: (información): Se recibe la notificación [08be.ac3f:capwap_90000004] auth mgr attr add/change para attr auth-domain(954)
[auth-mgr] [17062]: (información): [08be.ac3f:capwap_90000004] Método webauth que cambia el estado de 'En ejecución' a 'Correcto de autenticación'
[auth-mgr] [17062]: (información): [08be.ac3f:capwap_90000004] Estado de cambio de contexto de 'En ejecución' a 'Correcto de autenticación'
[auth-mgr] [17062]: (información): [08be.ac3f:capwap_90000004] auth mgr attr: se recibe una notificación de adición/cambio para el método attr(757)
[auth-mgr] [17062]: (información): [08be.ac3f:capwap_90000004] Evento desencadenado AUTHZ_SUCCESS (11)
[auth-mgr] [17062]: (información): [08be.ac3f:capwap_90000004] Estado de cambio de contexto de 'Éxito Authc' a 'Éxito Authz'
[webauth-acl] [17062]: (información): capwap_90000004[08be.ac3f][10.14.32.109]Aplicación de ACL de desconexión IPv4 a través de SVM, name: IP-Adm-V4-LOGOUT-ACL, prioridad: 51, IIF-ID: 0
[webauth-sess] [17062]: (información): capwap_90000004[08be.ac3f][10.14.32.109]Param-map used: global
[webauth-state] [17062]: (información): capwap_90000004[08be.ac3f][10.14.32.109]Param-map used: global
[webauth-state] [17062]: (información): capwap_90000004[08be.ac3f][10.14.32.109]State AUTHC_SUCCESS -> AUTHZ
[webauth-page] [17062]: (información): capwap_90000004[08be.ac3f][10.14.32.109]Página de envío de Webauth correcta
[webauth-io] [17062]: (información): capwap_90000004[08be.ac3f][10.14.32.109]56539/218 AUTENTICACIÓN del estado de E/S -> ESCRITURA
[webauth-io] [17062]: (información): capwap_90000004[08be.ac3f][10.14.32.109]56539/218 ESTADO

DE E/S ESCRITURA -> FIN
[webauth-httpd] [17062]: (información): capwap_90000004[08be.ac3f][10.14.32.109]56539/218 Elimine E/S ctx y cierre el socket, id [99000029]
[client-auth] [17062]: (nota): MAC: Autenticación L3 08be.ac3f correcta. ACL:[]
[client-auth] [17062]: (información): MAC: 08be.ac3f Transición de estado de interfaz de autenticación de cliente: S_AUTHIF_WEBAUTH_PENDING -> S_AUTHIF_WEBAUTH_DONE
[webauth-httpd] [17062]: (información): capwap_90000004[08be.ac3f][10.48.39.243]56538/219 Retire IO ctx y cierre el socket, id [D7000028]
[errmsg] [17062]: (información): %CLIENT_ORCH_LOG-6-CLIENT_ADDED_TO_RUN_STATE: R0/0: wncd: Entrada de nombre de usuario (invitado) unida con ssid (LWA_EA) para dispositivo con MAC: 08be.ac3f
[aaa-attr-inf] [17062]: (información): [Applied attribute :bsn-vlan-interface-name 0 "VLAN0039"]
[aaa-attr-inf] [17062]: (información): [Atributo aplicado : timeout 0 1800 (0x708)]
[aaa-attr-inf] [17062]: (información): [Atributo aplicado : url-redirect-acl 0 "IP-Adm-V4-LOGOUT-ACL"]
[ewlc-qos-client] [17062]: (información): MAC: Controlador de estado de ejecución 08be.ac3f Client QoS
[rog-proxy-capwap] [17062]: (depuración): Notificación de estado de EJECUCIÓN del cliente administrado: 08be.ac3f
[client-orch-state] [17062]: (nota): MAC: 08be.ac3f Transición de estado de cliente: S_CO_L3_AUTH_IN_PROGRESS -> S_CO_RUN

Información Relacionada

- Soporte técnico y descargas de Cisco

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).