Configuración de la autenticación local en el modo FlexConnect

Contenido

- Introducción
  - Antecedentes
    - Descripción general y requisitos de FlexConnect
    - Modos de Funcionamiento
    - Itinerancia segura rápida
    - Modo de gran escala FlexConnect
    - Compatibilidad con Wi-Fi 7 FlexConnect
    - Escenarios de resistencia de FlexConnect
  - Prerequisites
    - Requirements
    - Componentes Utilizados
  - Configurar
    - Diagrama de la red
    - Configuración de servidores AAA
    - Configuración del modo FlexConnect en el sitio remoto
    - Configuración de WLAN 802.1x con autenticación local mediante un servidor RADIUS externo
    - Configuración de ISE
    - Configuración de PSK WLAN con autenticación local
  - Verificación
  - Troubleshoot
    - Escenario independiente
  - Información Relacionada

Introducción

Este documento describe cómo funciona la autenticación local de FlexConnect y cómo configurarla mediante el controlador inalámbrico Cisco Catalyst serie 9800 (WLC)

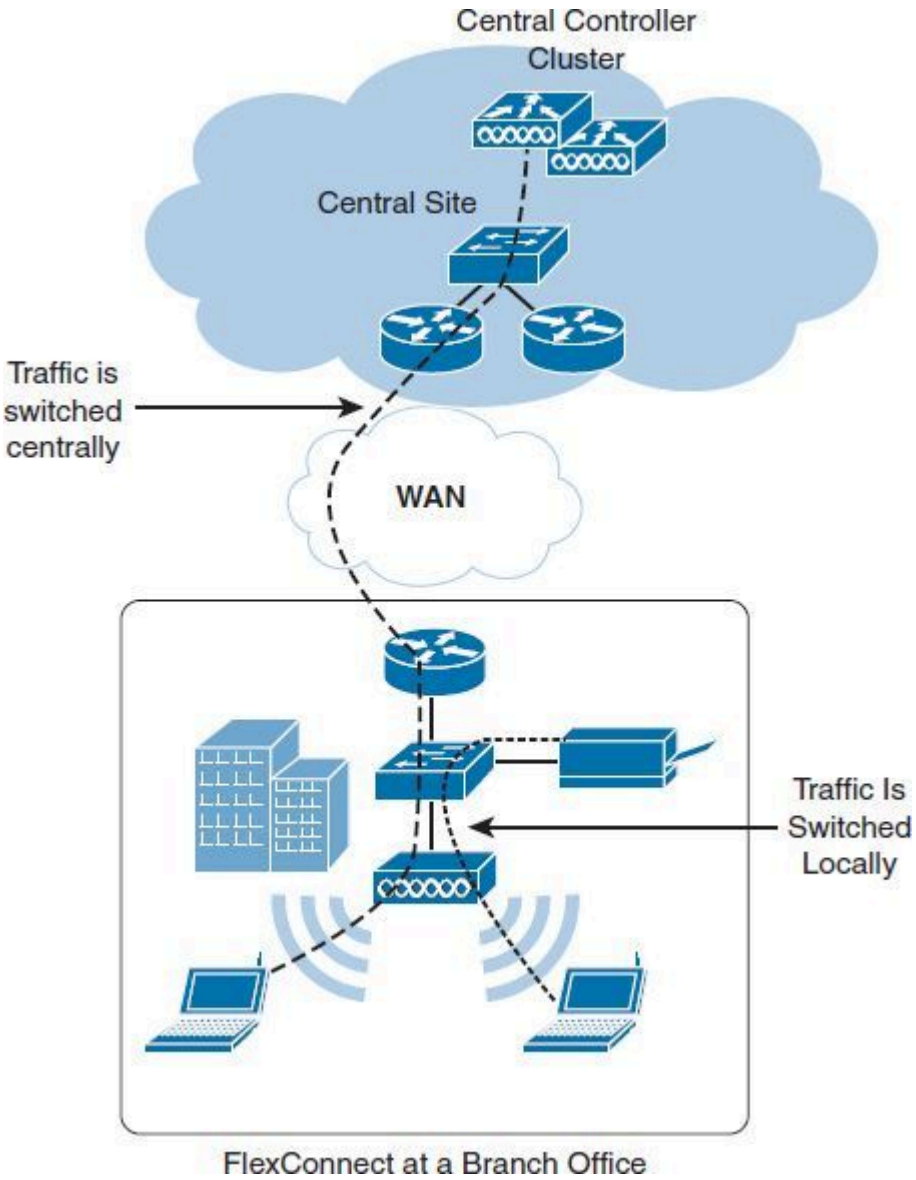
Antecedentes

Descripción general y requisitos de FlexConnect

FlexConnect permite que el punto de acceso (AP) de las sucursales u oficinas remotas se

conecte a un controlador centralizado y, al mismo tiempo, permita el procesamiento local del tráfico inalámbrico. A diferencia de las implementaciones inalámbricas centralizadas tradicionales, en las que todo el tráfico inalámbrico se canaliza al controlador mediante CAPWAP (control y aprovisionamiento de puntos de acceso inalámbricos), FlexConnect permite que el tráfico se conmute localmente y que el punto de acceso de la sucursal lo gestione directamente. Este switching local proporciona al AP cierto grado de autonomía, permitiendo que servicios clave como seguridad, roaming y calidad de servicio (QoS) funcionen independientemente del controlador.

Aunque FlexConnect está diseñado principalmente para el switching del tráfico local, también ofrece la flexibilidad de conmutar de forma centralizada SSID específicos (identificador del conjunto de servicios) cuando sea necesario. Por ejemplo, si cierto tráfico debe pasar a través de un firewall central, esos SSID se pueden enviar de vuelta al controlador a través de CAPWAP para el switching centralizado. Esta doble capacidad permite que un solo punto de acceso FlexConnect admita simultáneamente WLAN conmutadas tanto local como centralmente (red de área local inalámbrica).



FlexConnect at a Branch Office

Un punto de acceso FlexConnect implementado en una sucursal conmuta localmente un SSID mientras que otro se conmuta de forma centralizada

Modos de Funcionamiento

Los puntos de acceso FlexConnect funcionan de dos modos: modo conectado y modo independiente.

- Modo conectado, el AP mantiene una conexión activa al controlador a través del canal de control CAPWAP.
- El modo autónomo es un estado de reserva que ocurre cuando el AP pierde la conectividad con el controlador.

En condiciones normales, los puntos de acceso FlexConnect funcionan en modo conectado, donde el controlador administra servicios críticos como la autenticación centralizada, la creación de perfiles de clientes y la gestión de recursos de radio (RRM). Mientras que se espera que el AP permanezca en este modo la mayor parte del tiempo, cambia automáticamente al modo autónomo si se pierde la comunicación con el controlador. En el modo autónomo, el AP continúa funcionando, conmutando localmente el tráfico y permitiendo que los clientes permanezcan conectados. Los AP autentican independientemente a los clientes sin reenviar las solicitudes de autenticación a un controlador central. Sin embargo, ciertos servicios dependientes del controlador (como RRM y autenticación de cliente centralizada) dejan de estar disponibles temporalmente.

Por ejemplo, si una interrupción de la WAN (red de área extensa) interrumpe la conexión entre el AP y el controlador pero el acceso a Internet permanece activo, el AP pasa al modo autónomo y continúa procesando el tráfico conmutado localmente sin interrupción. Los clientes existentes permanecen conectados, pero los nuevos clientes que requieren autenticación central no pueden unirse a la red, a menos que se configure la autenticación local. Los puntos de acceso FlexConnect se pueden configurar para que realicen la autenticación local durante los fallos de la WAN, lo que garantiza un servicio continuo incluso cuando el controlador no esté disponible.

Mientras está en modo autónomo, estas funciones no están disponibles para el AP:

- Autenticación web del cliente
- Autenticación de invitados (redirección del portal)
- Cualquier SSID conmutado centralmente
- RRM

- Movilidad IPv6 de capa 3
- Perfiles nativos
- Clasificación de políticas
- Gateway de detección de servicios
- Actualizaciones de configuración

Para obtener una lista completa de las funciones y las configuraciones de WLAN admitidas en el modo independiente (autenticación local), consulte la matriz de funciones: Matriz de funciones de los puntos de acceso inalámbricos de Cisco

Un escenario de fallo común de FlexConnect implica una pérdida completa o una degradación significativa de la WAN, lo que interrumpe el canal de control CAPWAP. Cuando el AP pierde la conectividad con el controlador debido a los problemas de WAN, cambia inmediatamente al modo autónomo.

El objetivo principal durante un fallo de WAN es restaurar la comunicación con el controlador lo antes posible para reanudar la funcionalidad completa.

Cuando un punto de acceso de FlexConnect entra en modo independiente debido a un fallo de la WAN, los clientes activos permanecen conectados y pueden desplazarse sin problemas entre los puntos de acceso dentro del dominio o la etiqueta del sitio de FlexConnect, pero el roaming entre las diferentes etiquetas del sitio de FlexConnect puede requerir una reautenticación completa. Sin embargo, los nuevos clientes que intentan unirse a la WLAN conmutada localmente no pueden autenticarse porque el servidor AAA (servidor de autenticación, autorización y administración de cuentas) en la ubicación central es inalcanzable.

Itinerancia segura rápida

La autenticación EAP (protocolo de autenticación extensible) introduce una latencia más alta en comparación con la autenticación PSK (clave precompartida) debido al intercambio de tramas EAP con el servidor AAA. Sin embargo, con la itinerancia segura rápida, un cliente experimenta una autenticación 802.1X/EAP completa solamente durante su asociación inicial con la red. En las itinerancias subsiguientes a los AP vecinos, se omite el intercambio EAP, dejando solamente el intercambio de señales de cuatro vías, que es significativamente más rápido ya que no involucra al servidor AAA. Esta tabla describe los diversos métodos de roaming seguro rápido soportados por el WLC 9800 tanto en el modo local como en las implementaciones de FlexConnect.

Función	Modo local	FlexConnect	FlexConnect	FlexConnect

		(modo conectado; Autenticación central)	(modo conectado: autenticación local)	(individual)
Almacenamiento en caché de teclas persistente (SKC)	Not Supported	Not Supported	Not Supported	Not Supported
Almacenamiento en caché de claves oportunista (OKC)	Supported	Supported	Supported	Compatible (hasta que caduque la sesión del cliente)
Gestión centralizada de claves de Cisco (CCKM)	Supported	Supported	Supported	Not Supported
FT-802.11r/Adaptive 11r (transición rápida) (en directo)	Supported	Supported	Supported	Compatible (hasta que caduque la sesión del cliente)
FT-802.11r/Adaptive 11r (transición rápida) (en DS)	Supported	Supported	Not Supported	Not Supported

En el modo independiente, la itinerancia rápida depende de que el material de claves almacenado en caché siga siendo válido. Cuando caduca la sesión/PMK (clave maestra en pares) en caché, el AP no puede obtener nueva información de clave derivada del controlador hasta que se restaure la conectividad del controlador.

Modo de gran escala FlexConnect

A partir de Cisco IOS XE 17.8.1 en adelante, la capacidad del sitio flexible se ha ampliado para admitir 300 puntos de acceso y 3000 clientes 802.1x.

La propagación de PMK permite que los AP dentro del mismo sitio de FlexConnect compartan información de PMK, lo que reduce la necesidad de un intercambio de EAP completo durante el

roaming. La propagación de PMK no está habilitada de forma predeterminada.

Utilice estos comandos para verificar la propagación de PMK y para habilitar PMK:

- show wireless stats pmk-propagation
- propagar pmk

Compatibilidad con Wi-Fi 7 FlexConnect

En esta tabla se resumen las funciones de FlexConnect compatibles con la familia de puntos de acceso Wi-Fi 7 CW917x.

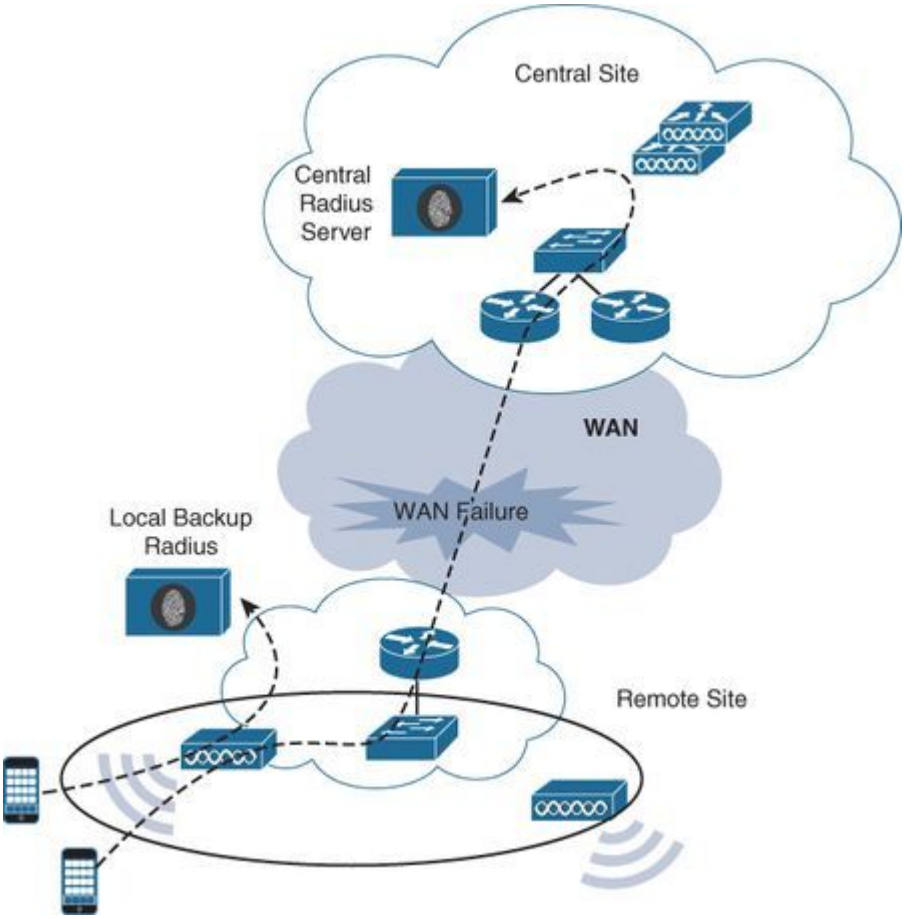
Función	Soporte
Conmutación local	Supported
Switching central	Supported
Asignación WLAN-VLAN	Supported
Autenticación local con RADIUS externo	Supported
WPA3 Enterprise	Supported
Fast Roaming FT-802.11r	Supported
Funcionamiento de enlaces múltiples (MLO)	Supported
Autenticación local con RADIUS interno	Not Supported
WPA3-Enterprise-192	Not Supported

Escenarios de resistencia de FlexConnect

1. En una configuración de resistencia N+1, varios controladores activos comparten un controlador de copia de seguridad común que asume el control si falla cualquier controlador activo. Cuando un controlador principal se desconecta, los AP FlexConnect cambian inmediatamente al modo independiente y comienzan a buscar el controlador de respaldo. Durante este período de desconexión, los clientes conmutados centralmente se desconectan de los AP. Una vez que los AP localizan y sincronizan con el controlador de respaldo, los clientes que requieren acceso a los SSID conmutados centralmente se vuelven a conectar. Mientras tanto, los clientes conmutados localmente no se ven afectados y continúan operando sin notar la interrupción del servicio.
2. Proporcione un servidor AAA de copia de seguridad en la ubicación remota, al que pueda acceder el grupo FlexConnect. Con la autenticación local habilitada, este servidor RADIUS de respaldo sólo se utiliza cuando los AP ingresan en el modo autónomo—permanece

inactivo mientras los AP están en el modo conectado. Cuando los AP de FlexConnect utilizan el servidor AAA de respaldo local para la autenticación, las claves de autenticación se distribuyen a través de todos los AP en el grupo de FlexConnect, tal como lo harían con un servidor AAA centralizado. Esto garantiza que los nuevos clientes todavía puedan vagar sin problemas entre los APs sin necesidad de reautenticarse, incluso cuando el servidor RADIUS de respaldo está en uso.

3. Cualquier método presente en la Matriz de funciones para los puntos de acceso inalámbricos de Cisco que permita la autenticación local.



Los clientes se autentican contra un servidor AAA de respaldo local cuando el servidor AAA central deja de estar disponible debido a una falla de WAN

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

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

- Controlador inalámbrico Catalyst C9800-CL para la nube con Cisco IOS® XE Dublin 17.18.3
- Punto de acceso Catalyst CW9164I-ROW v17.18.3.18
- Punto de acceso Aironet® AIR-AP2802I-E-K9 v17.18.3.18
- 2 Identity Services Engine v3.2.0.542

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.

Configurar

Diagrama de la red

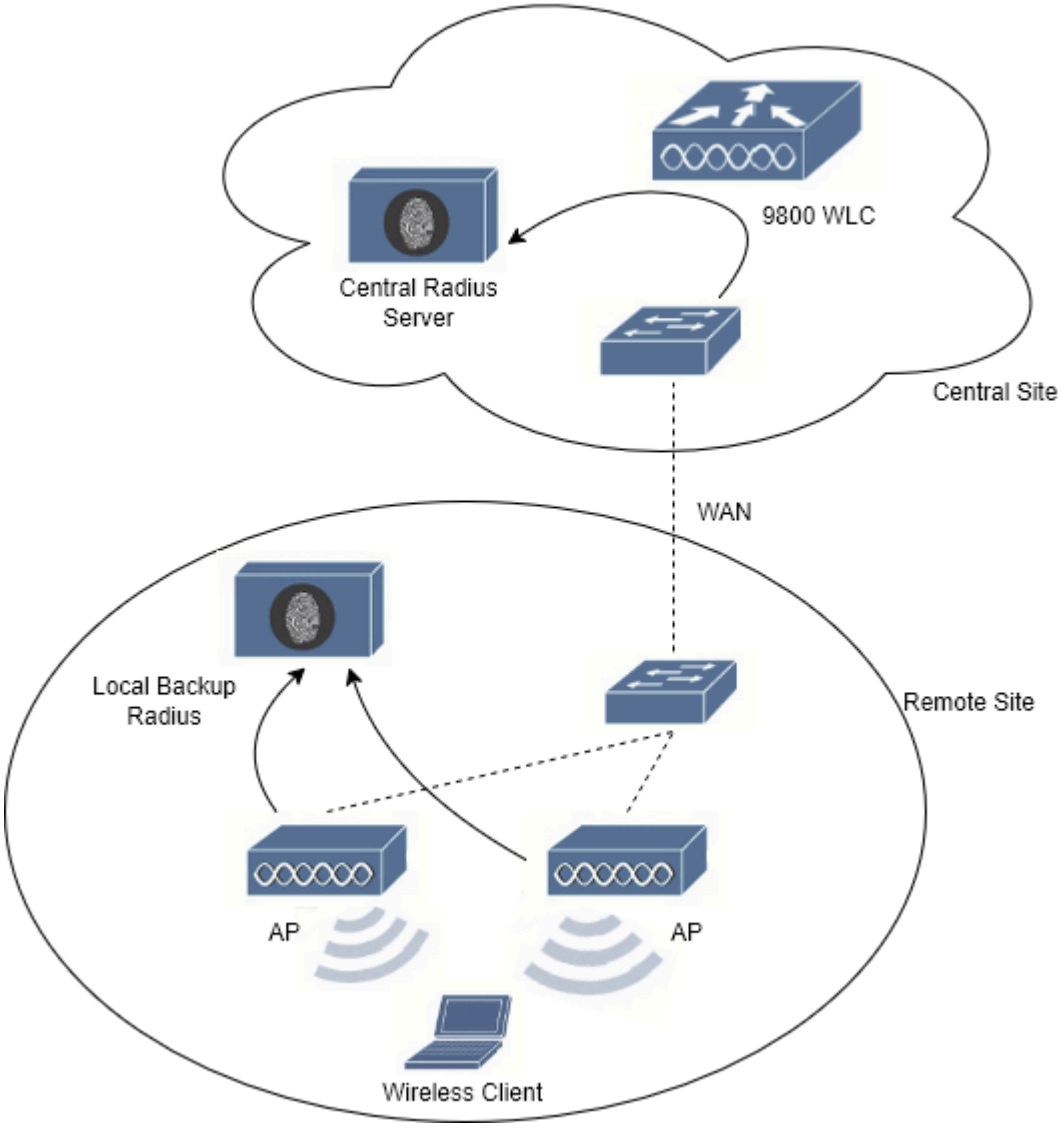


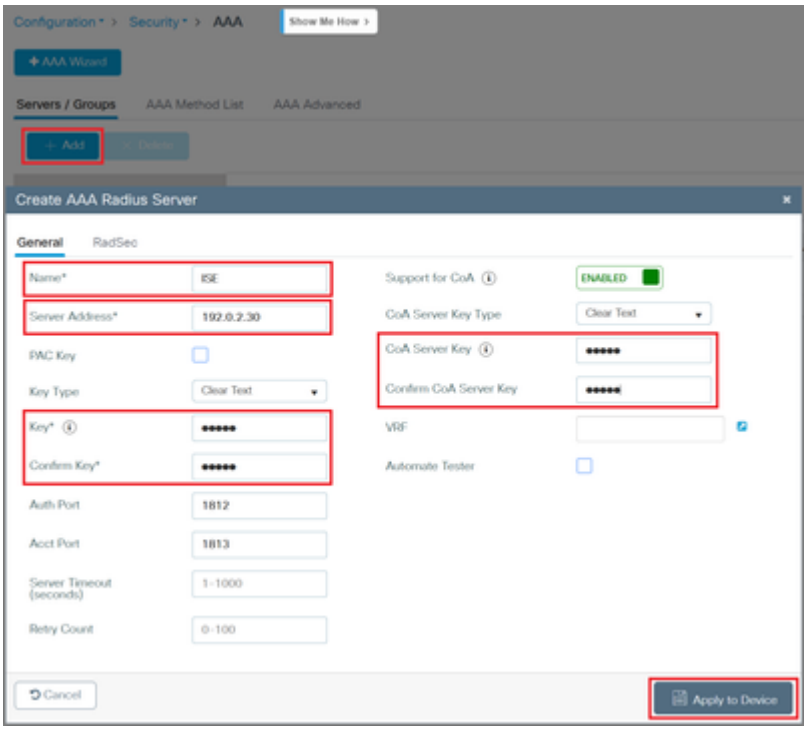
Diagrama de la red

Configuración de servidores AAA

Paso 1. Para configurar una WLAN 802.1x necesita crear el grupo de servidores AAA en el WLC 9800.

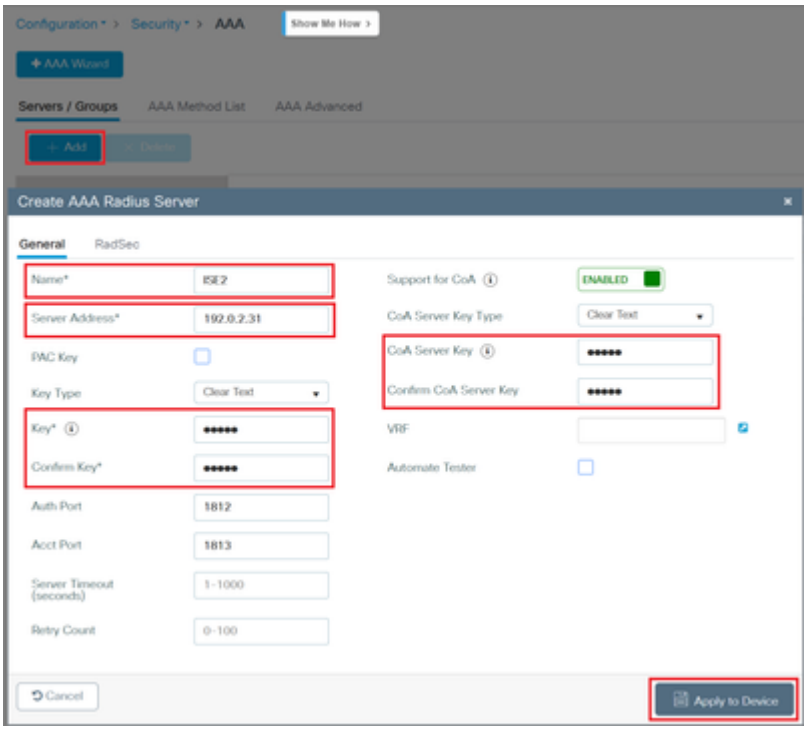
Cree un servidor AAA para cada sitio: el del sitio central y el otro del sitio remoto.

Vaya a Configuration > Security > AAA > Server/Groups > Servers y seleccione +Add. Dé un nombre al servidor, su dirección IP, la clave (y la clave de confirmación), habilite el soporte CoA (Cambio de autorización) e ingrese la clave del servidor CoA (y confirme la clave del servidor CoA). Las claves deben ser las mismas.



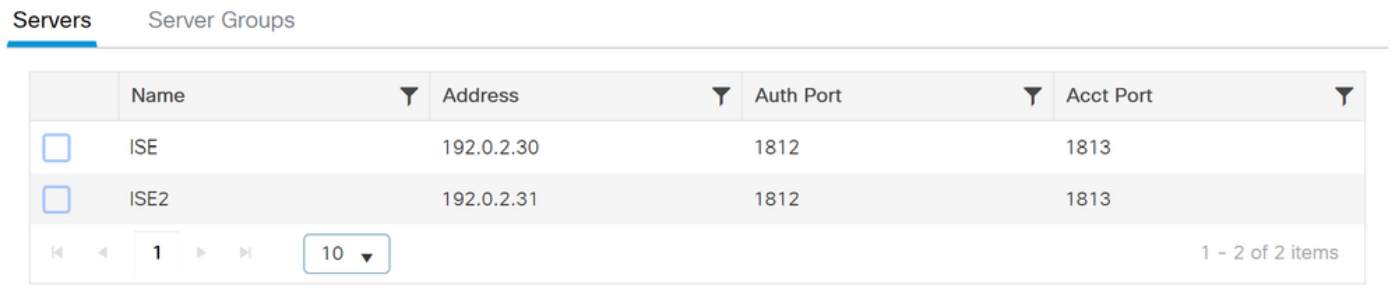
Haga clic en Aplicar al dispositivo.

Paso 2. Crear el otro servidor AAA:

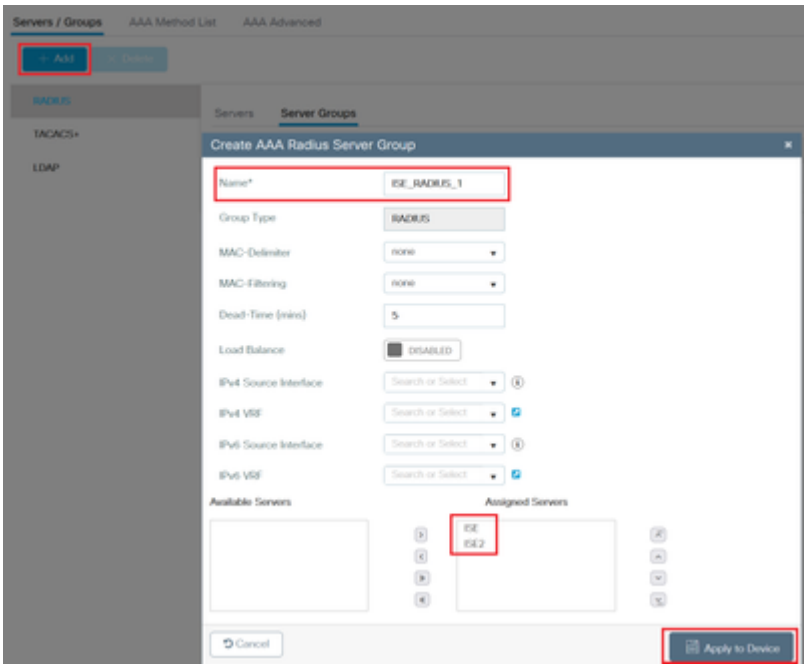


Haga clic en Aplicar al dispositivo.

Ahora verá los servidores AAA configurados:

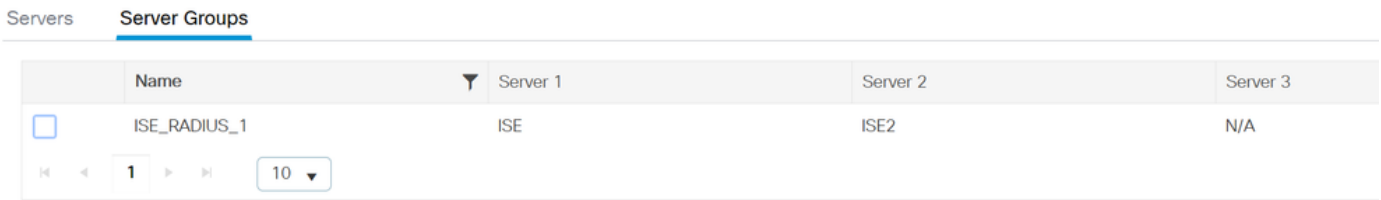


Paso 3. Navegue hasta Configuration > Security > AAA > Server/Groups > Server Groups y seleccione +Add. Dé un nombre al servidor de grupo y seleccione los servidores AAA creados anteriormente en la columna Assigned Servers:



Haga clic en Aplicar al dispositivo.

A continuación, verá el grupo de servidores AAA configurado:



CLI:

```
aaa new-model
```

```
!
radius server ISE
address ipv4 192.0.2.30 auth-port 1812 acct-port 1813
key keystring
!
radius server ISE2
address ipv4 192.0.2.31 auth-port 1812 acct-port 1813
key keystring
!
aaa server radius dynamic-author
client 192.0.2.30 server-key keystring
client 192.0.2.31 server-key keystring
!
aaa group server radius ISE_RADIUS_1
server name ISE
server name ISE2
deadtime 5
```

Configuración del modo FlexConnect en el sitio remoto

Paso 1. El primer paso es configurar FlexConnect en el sitio remoto.

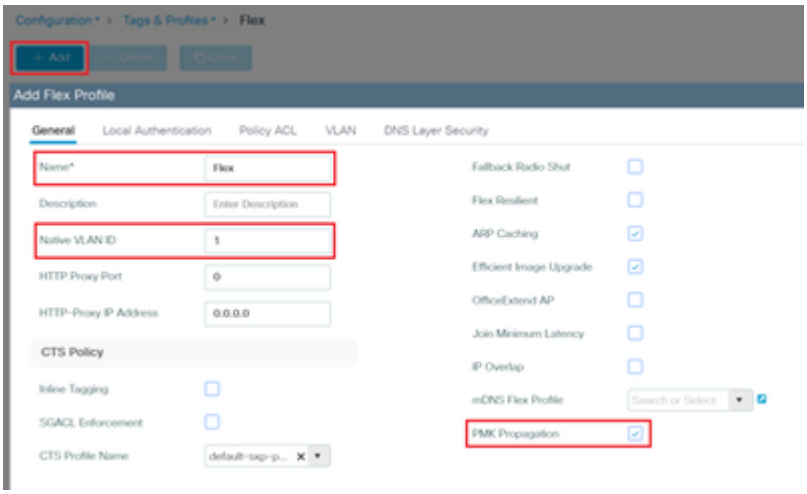
Utilice esta guía para cambiar el modo de los puntos de acceso a Flex: Comprender FlexConnect en el controlador inalámbrico Catalyst 9800.

Los AP de esta guía/laboratorio utilizan el mismo Flex Profile.

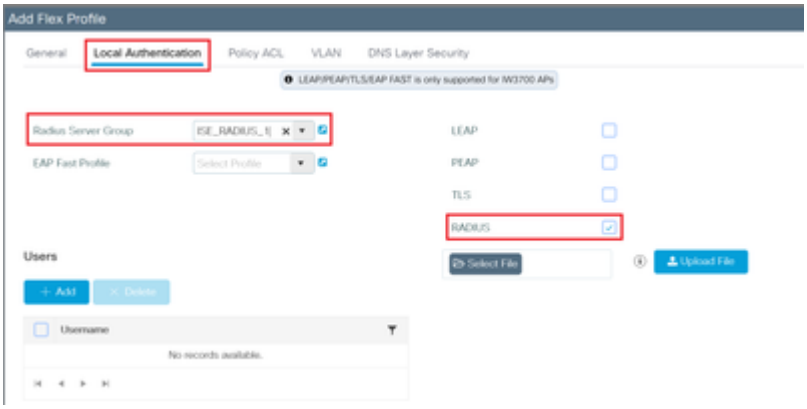
Paso 2. Vaya a Configuración > Etiquetas y perfiles > Flex.

Cree un nuevo nombre de perfil de Flex con +Agregar. En la ficha General, asigne un nombre al perfil, introduzca la ID de la VLAN nativa (red de área local virtual) y active la propagación PMK.

Habilite la propagación de PMK para facilitar el roaming de clientes inalámbricos sin problemas compartiendo la información de PMK entre los AP dentro de un solo sitio.

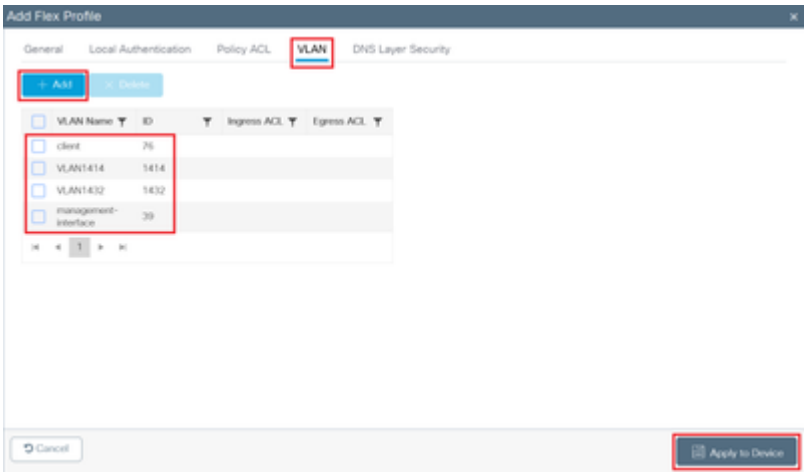


Paso 3. Para 802.1x WLAN, en la pestaña Autenticación Local seleccione el Grupo de Servidores Radius y habilite RADIUS:



Consejo: En el caso de una WLAN PSK, no es necesario agregar nada en esta ficha.

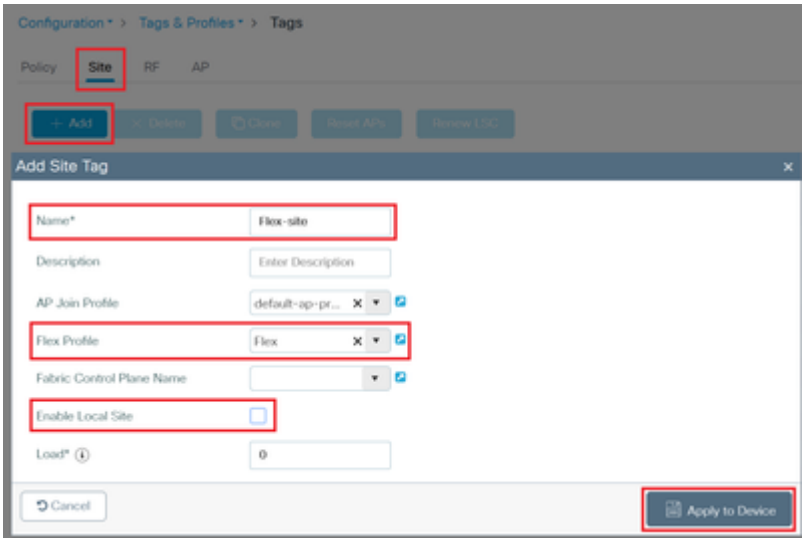
Paso 4. En la pestaña VLAN agregue todas las VLAN que utilizan los clientes, los AP y el servidor RADIUS. Asegúrese de establecer la correspondencia correcta de cada nombre de VLAN con el ID de VLAN correcto:



Al final, haga clic en Update & Apply to Device.

Paso 5. Navegue hasta Configuración > Etiquetas y perfiles > Etiquetas > Sitio y seleccione +Agregar.

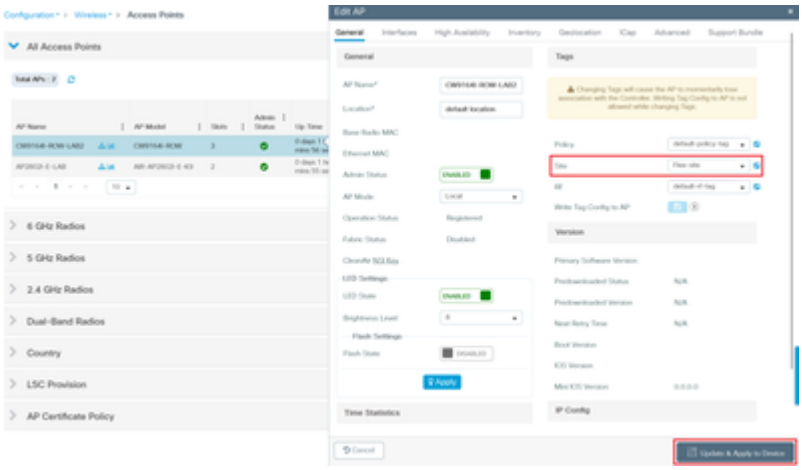
Cree la etiqueta del sitio con el perfil flexible creado anteriormente. Asigne un nombre, seleccione el Flex Profile correcto y desactive Enable Local Site. Asegúrese de que el perfil de unión al AP sea el correcto.



Haga clic en Aplicar al dispositivo.

Paso 6. Navegue hasta Configuración > Inalámbrico > Puntos de acceso.

Seleccione su AP, en General > Tags cambie la etiqueta del sitio a la etiqueta previamente configurada:

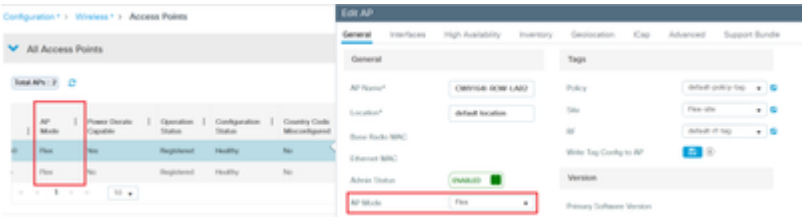


Haga clic en Update & Apply to Device.

El AP se desconecta del WLC y se vuelve a unir con el modo Flex AP.

En la misma página, cuando el AP se vuelve a unir, puede verificar el modo AP en la columna AP Mode.

Si selecciona el AP, se muestra la nueva etiqueta Sitio:



CLI:

```
wireless profile flex Flex
ip http client proxy 0.0.0.0 0
local-auth radius-server-group ISE_RADIUS_1
vlan-name client
vlan-id 76
vlan-name VLAN1414
vlan-id 1414
vlan-name VLAN1432
vlan-id 1432
vlan-name management-interface
vlan-id 39
pmk propagate
!
wireless tag site Flex-site
ap-profile default-ap-profile
no local-site
flex-profile Flex
```

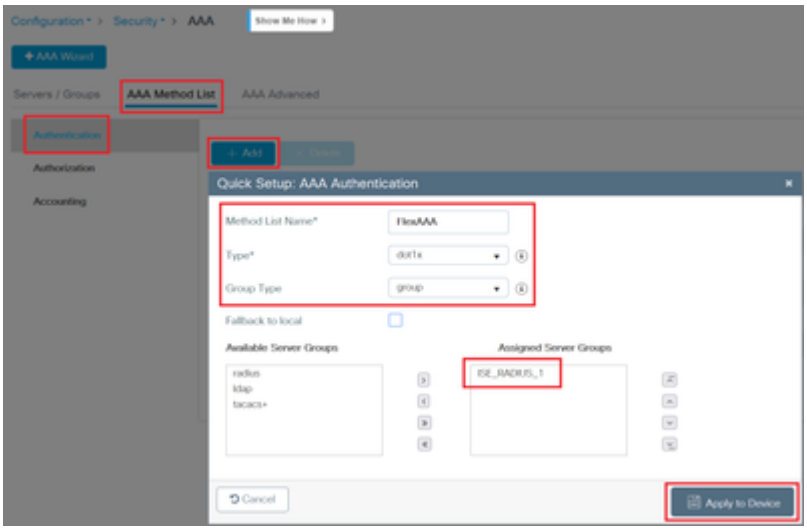
```
!
ap h.h.h (AP Radio MAC address)
policy-tag default-policy-tag
site-tag Flex-site
rf-tag default-rf-tag
```

Configuración de WLAN 802.1x con autenticación local mediante un servidor RADIUS externo

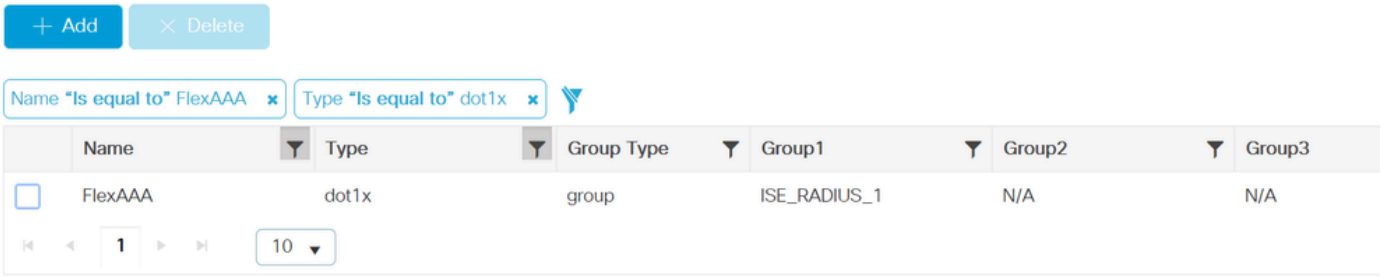
Paso 1. Cree la lista de métodos de autenticación.

Navegue hasta Configuration > Security > AAA, en la pestaña Lista de métodos AAA > Authentication.

Seleccione +Add, asigne un nombre al nombre de la lista de métodos, seleccione dot1x como tipo, seleccione group como tipo de grupo y asigne el grupo de servidores AAA en la columna Assigned Server Groups:



Ahora verá la lista de métodos AAA creada:



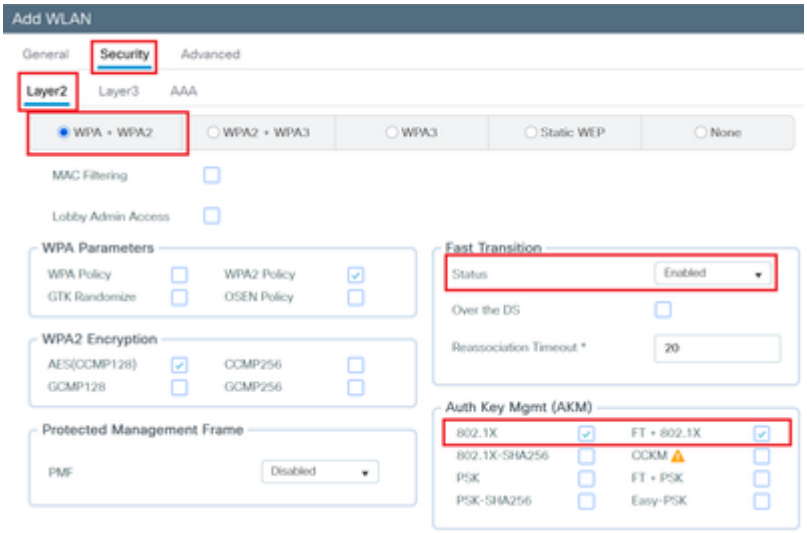
Paso 2. Cree la WLAN.

Vaya a Configuration > Tags & Profiles > WLANs, seleccione +Add.

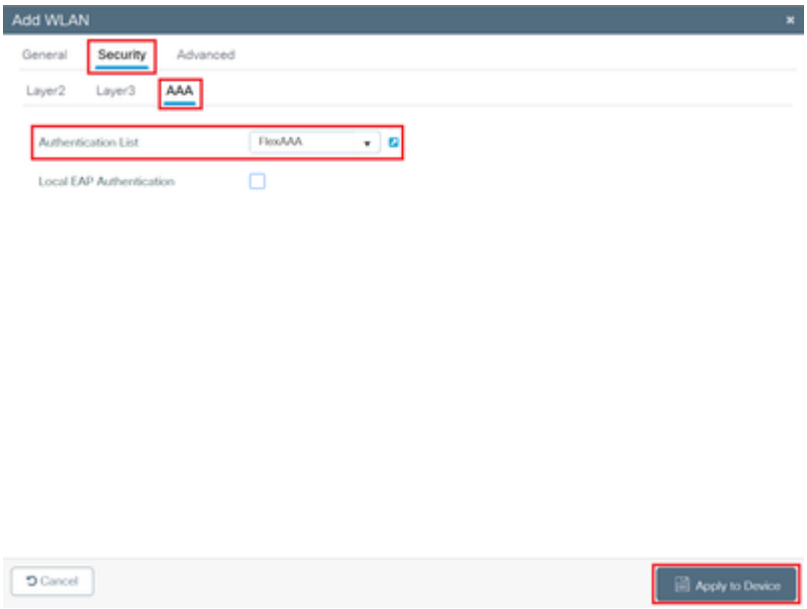
En la etiqueta General, cree un nombre para Profile Name (Nombre del perfil), SSID y enable Status (Activar estado):



Paso 3. Navegue hasta Seguridad > Capa 2 pestaña, seleccione WPA+WPA2 (acceso Wi-Fi protegido), Transición rápida como habilitada, Gestión de clave de autenticación 802.1X y FT+802.1X:



Paso 4. Navegue hasta Seguridad > AAA pestaña, en el menú desplegable Lista de Autenticación seleccione la lista creada anteriormente:



Haga clic en Update & Apply to Device.

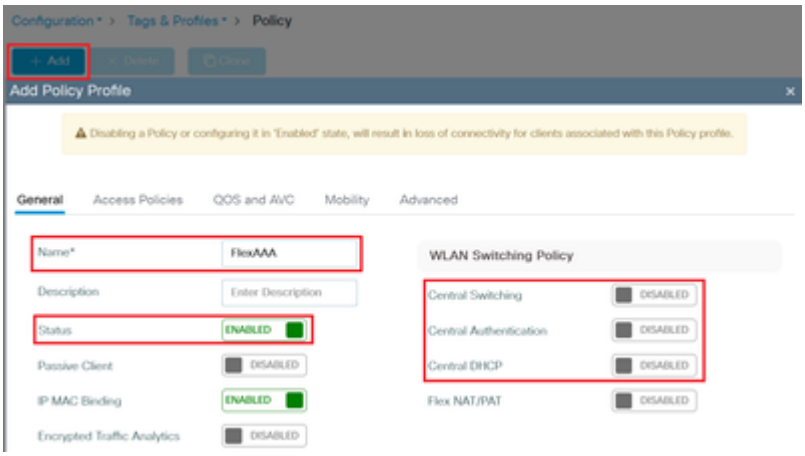
A continuación, verá la WLAN creada:



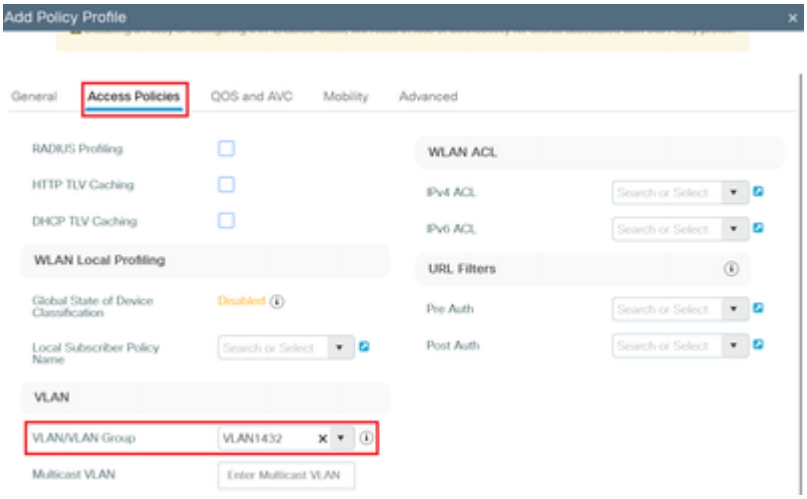
Paso 5. Creación del Perfil de Política.

Vaya a Configuration > Tags & Profiles > Policy.

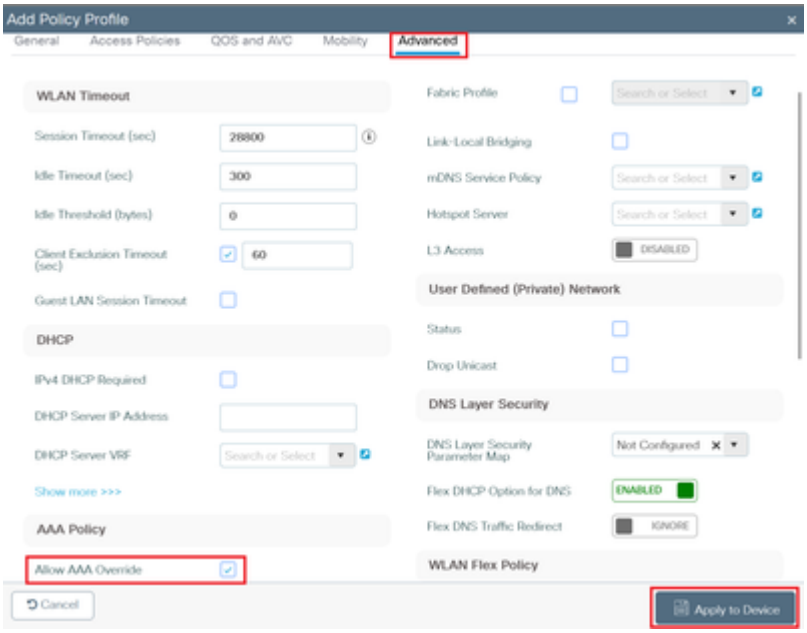
Seleccione +Add y en la ficha General asigne un nombre al perfil de política, habilite el estado y deshabilite el switching central, la autenticación central y el DHCP central (protocolo de configuración dinámica de host):



Paso 6. Vaya a la pestaña Políticas de acceso, seleccione la VLAN:

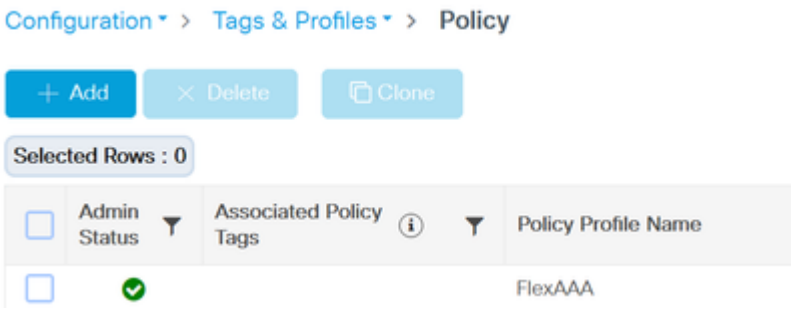


Paso 7. Acceda a la pestaña Avanzado, active Permitir Sustitución AAA.:



Haga clic en Update & Apply to Device.

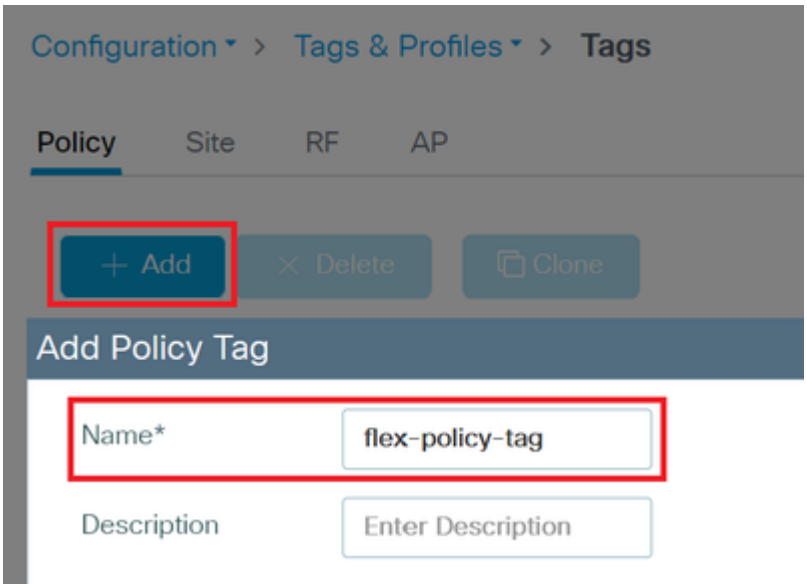
Puede ver el perfil de directiva en la lista:



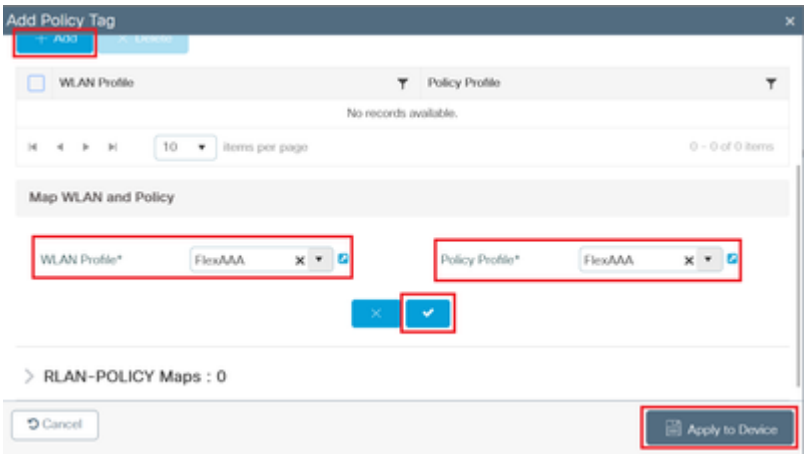
Paso 8. Crear etiqueta de directiva.

Vaya a Configuración > Etiquetas y perfiles > Etiquetas

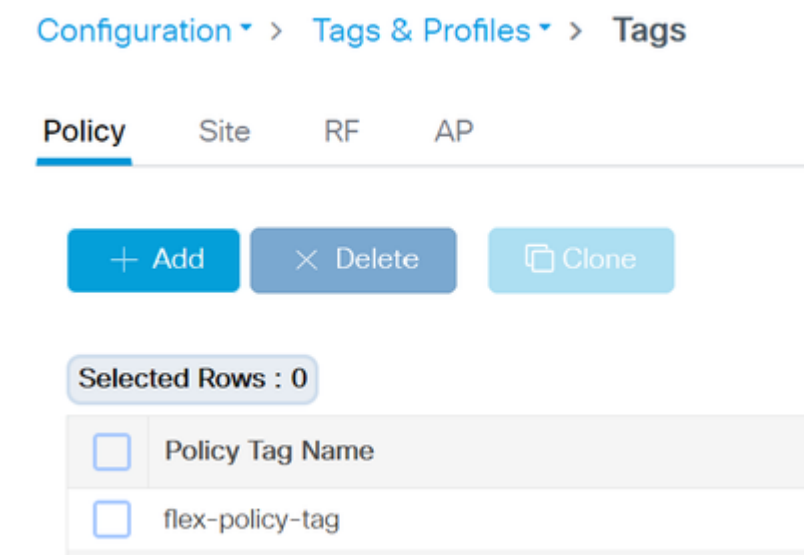
En la ficha Directiva, seleccione +Agregar. Dé un nombre a la etiqueta de directiva:



Desplácese hacia abajo y seleccione +Add bajo WLAN-POLICY Maps. En Perfil WLAN (Perfil WLAN), seleccione la WLAN creada anteriormente en el menú desplegable. En Perfil de directiva, seleccione el Perfil de directiva creado anteriormente en el menú desplegable. Haga clic en el botón de verificación y, a continuación, en Aplicar al dispositivo:

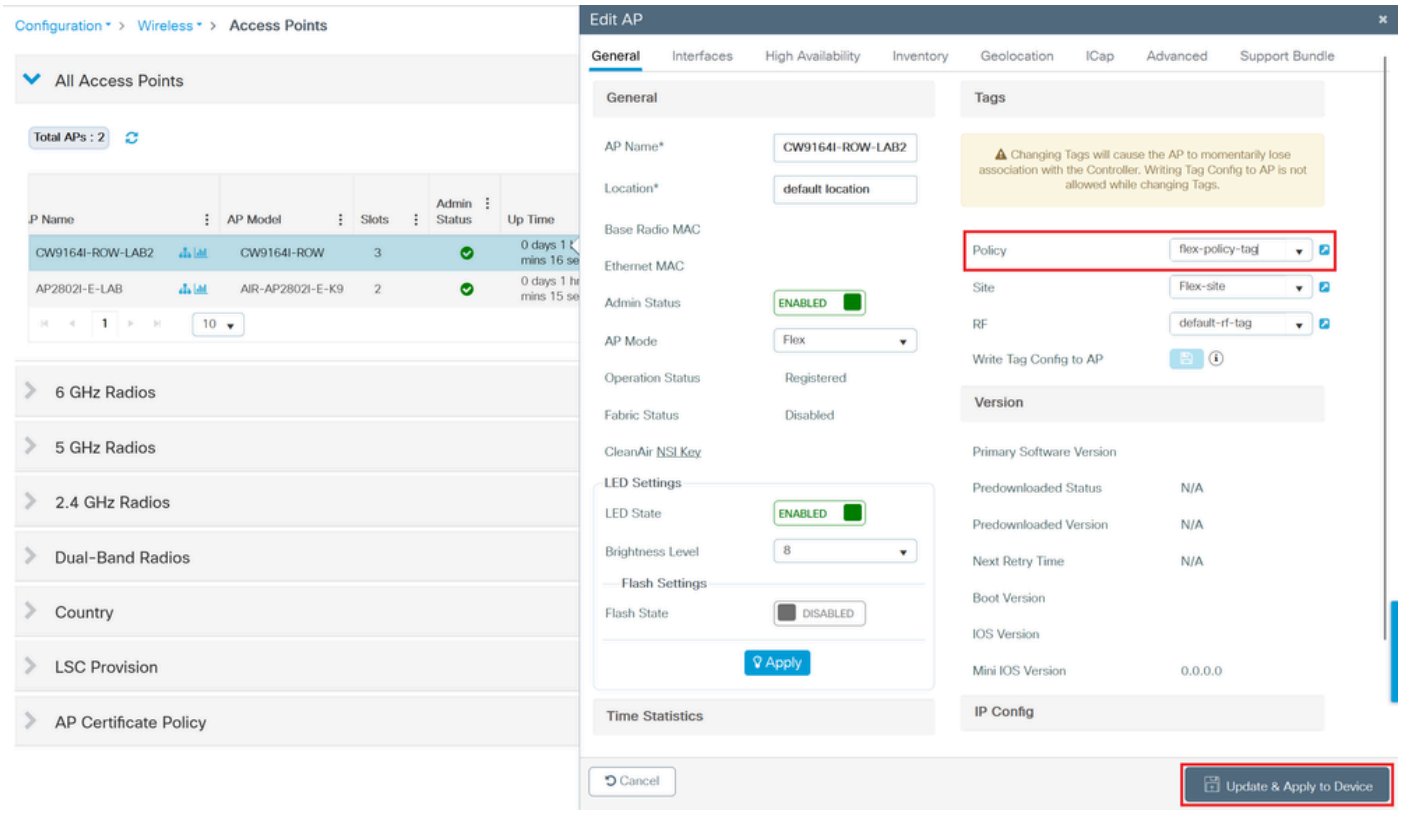


Puede ver la etiqueta de directiva en la lista:



Paso 9. Asigne la etiqueta de política en la etiqueta APs.

Vaya a Configuration > Wireless > Access Points. Seleccione el AP para cambiar la etiqueta.



Haga clic en Update & Apply to Device.

El AP se desune y vuelve a unirse con la nueva etiqueta de política.

Cuando el AP se une de nuevo, puede verificar la lista de puntos de acceso, confirmar que el AP está en el modo Flex, y las etiquetas asignadas:



CLI:

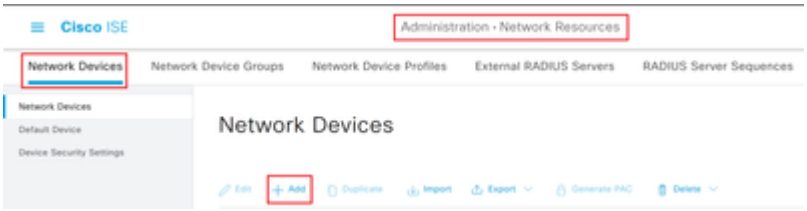
```
aaa authentication dot1x FlexAAA group ISE_RADIUS_1
!
wlan FlexAAA 4 FlexAAA
radio policy dot11 24ghz
radio policy dot11 5ghz
security ft
security wpa akm ft dot1x
security dot1x authentication-list FlexAAA
no shutdown
```

```
!
wireless profile policy FlexAAA
aaa-override
no central authentication
no central dhcp
no central switching
vlan VLAN1432
no shutdown
!
wireless tag policy flex-policy-tag
wlan FlexAAA policy FlexAAA
!
ap h.h.h (AP Radio MAC address)
policy-tag flex-policy-tag
site-tag Flex-site
rf-tag default-rf-tag
```

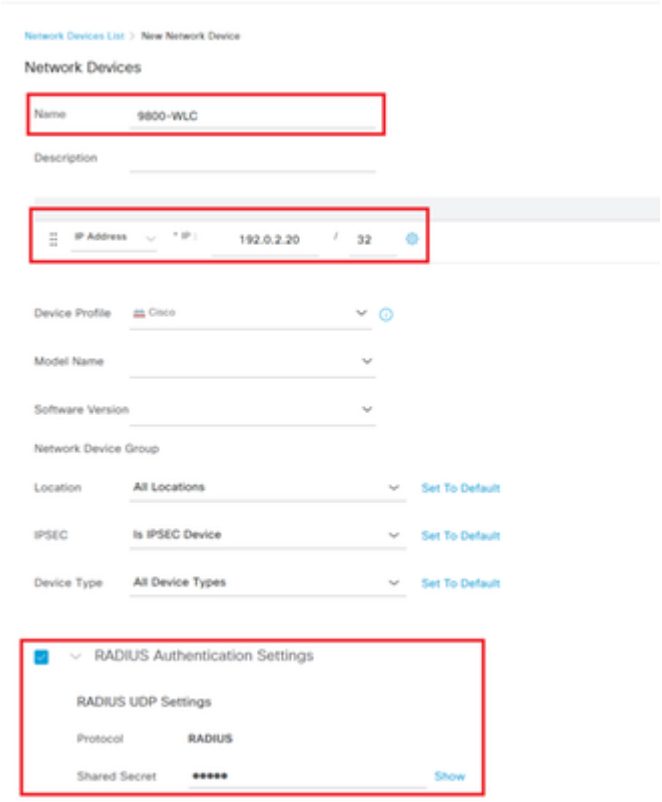
Configuración de ISE

Ahora necesita configurar ISE para poder autenticar a los clientes cuando estén en la autenticación local.

Paso 1.Vaya a Administración > Recursos de red > Dispositivos de red. Seleccione +Agregar.



Paso 2. Agregue el 9800 WLC. Asigne un nombre, agregue su dirección IP, habilite RADIUS Authentication Settings (Parámetros de autenticación RADIUS) y agregue la clave secreta compartida. Esta clave debe ser la misma clave que configuró anteriormente cuando creó los servidores AAA en el WLC 9800.



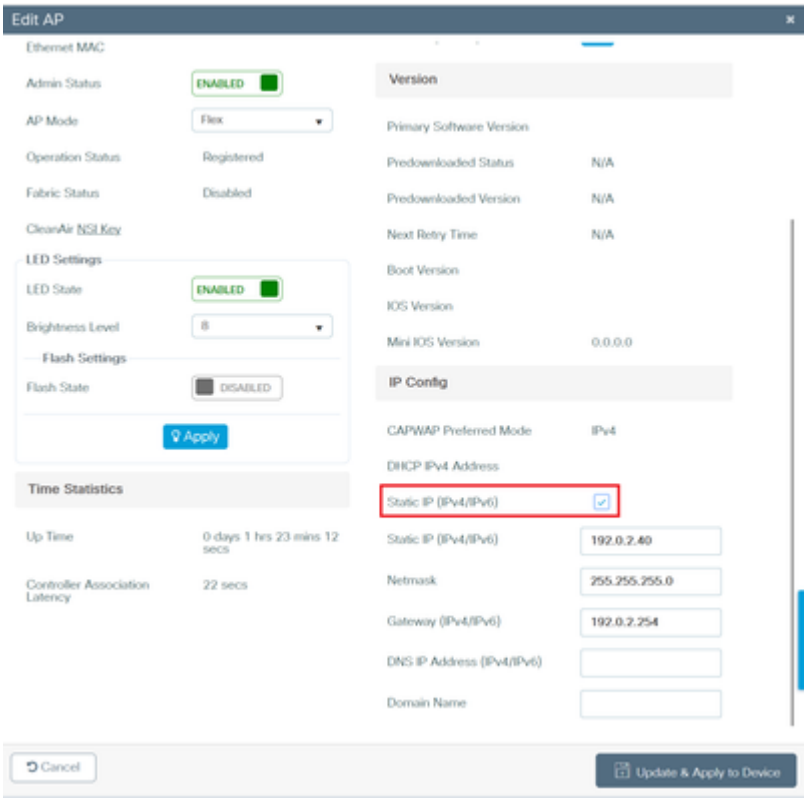
En la esquina inferior derecha, haga clic en Guardar.

Paso 3. Necesitamos agregar los APs en la lista de dispositivos de red, para que puedan actuar como autenticadores/reenviadores AAA cuando el sitio remoto pierde el link WAN (y cuando los APs pasan al modo autónomo).

Navegue hasta Configuration > Wireless > Access Points en la GUI del 9800 WLC y tome nota de cada dirección IP del AP.

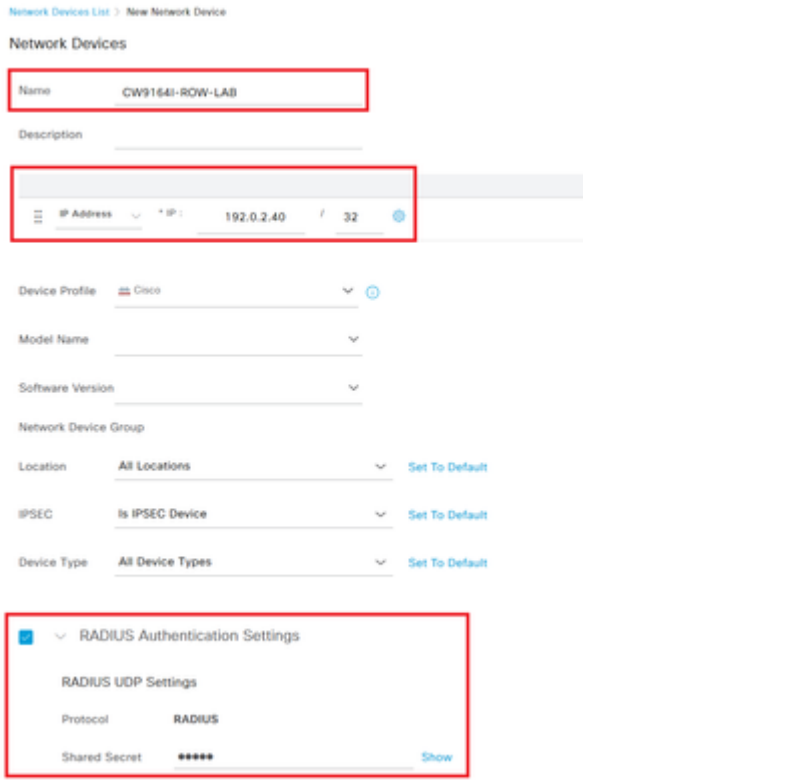
Nota: Configure la dirección IP de cada punto de acceso flexible en Estático. Cuando los AP pierden y recuperan la conexión con el WLC 9800, pueden volver con una dirección IP diferente de DHCP, y por lo tanto perder la comunicación con ISE.

Active IP estática (IPv4/IPv6). Haga clic en Update & Apply to Device:



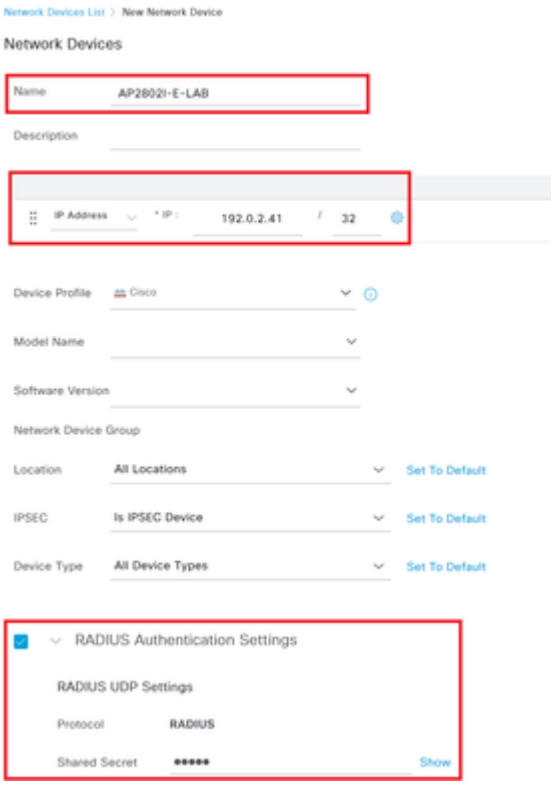
Paso 4. De nuevo en ISE, navegue hasta Administration > Network Resources > Network Devices. Seleccione +Agregar.

Agregue sus AP como dispositivos de red, la misma configuración que el WLC 9800:



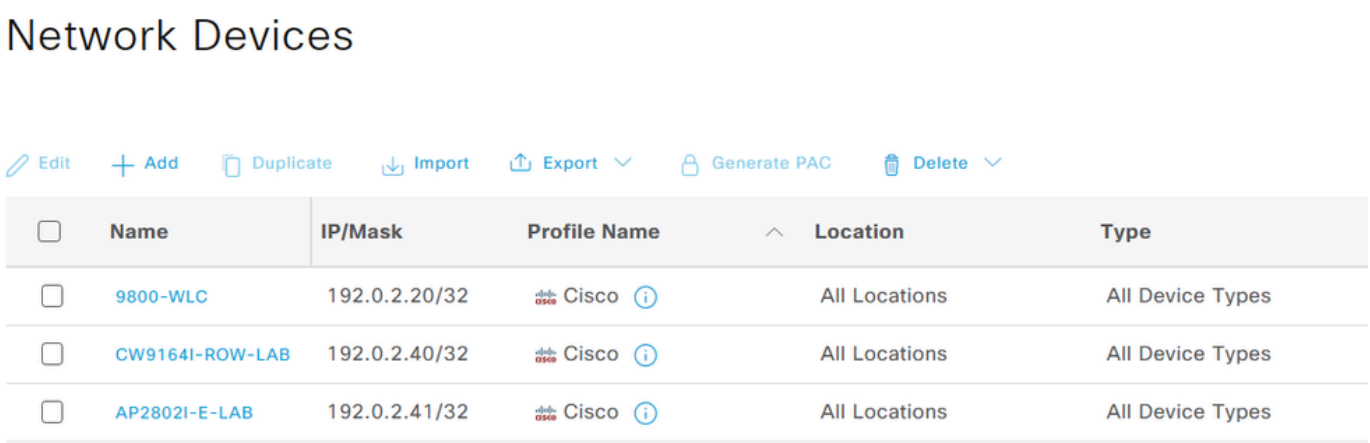
En la esquina inferior derecha, haga clic en Guardar.

Para el segundo AP:



En la esquina inferior derecha, haga clic en Guardar.

Puede ver esta lista de dispositivos de red:



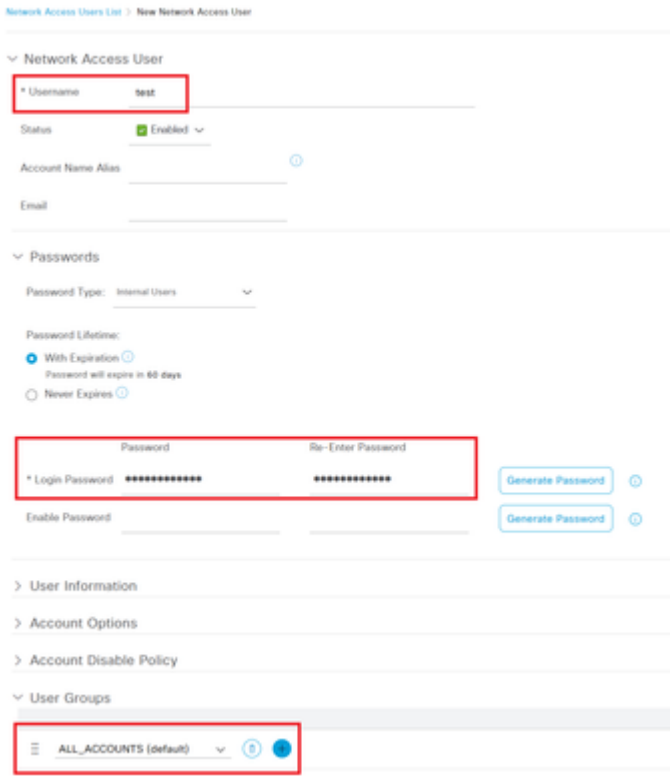
Si sus AP están en rangos de IP contiguos, puede utilizar la función de máscara para configurar una sola entrada que defina el secreto compartido para un grupo entero (si no todos) de AP. En

realidad, no es necesario configurar un dispositivo de red por AP en ISE. Sin embargo, tenga en cuenta que, al utilizar comodines y máscaras, deja cierto margen para que un dispositivo no autorizado intente actuar como reenviador a ISE.

Paso 5. Navegue hasta Administration > Identity Management > Identities, en la pestaña Users, y cree un usuario para la autenticación 802.1x. Seleccione +Agregar:

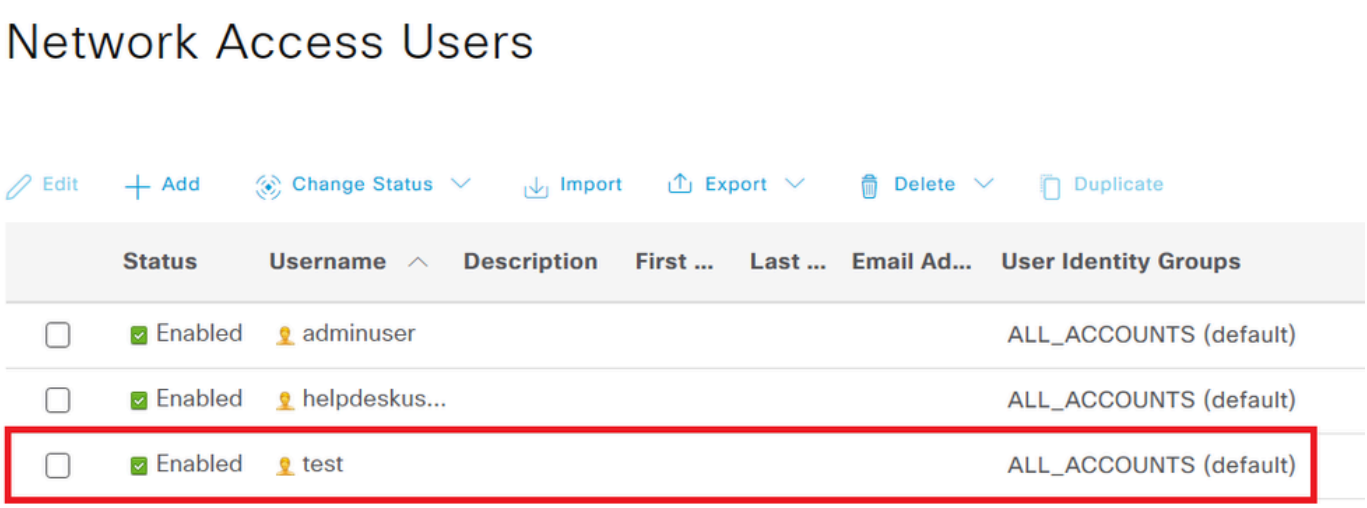


Cree un nombre de usuario, la contraseña (y escriba la misma contraseña en Volver a introducir contraseña) y seleccione ALL_ACCOUNTS (predeterminado) en el menú desplegable Grupos de usuarios:

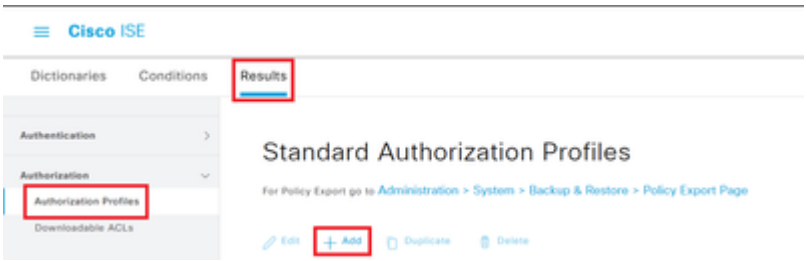


En la esquina inferior derecha, haga clic en Submit.

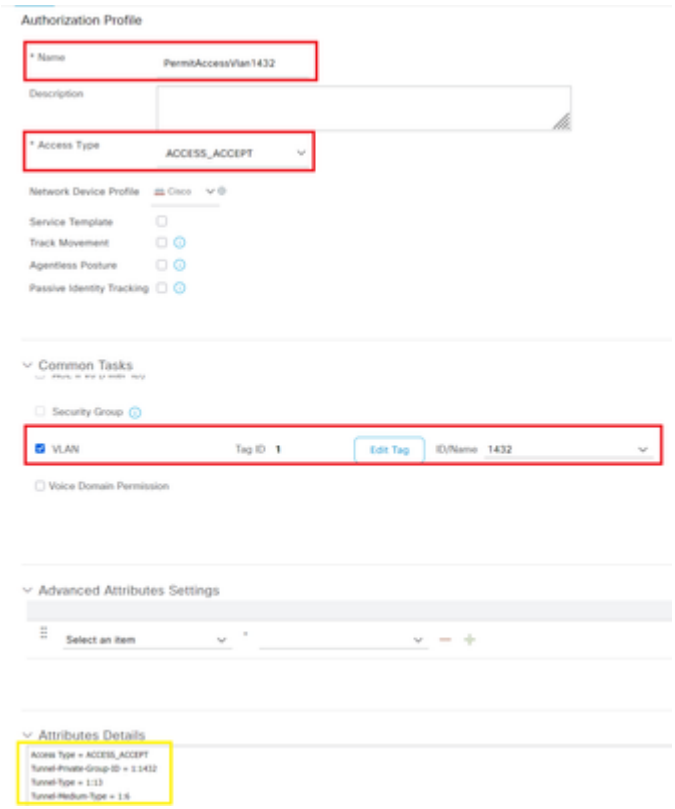
Puede ver el usuario en la lista Network Access Users (Usuarios de acceso a red):



Paso 6. Navegue hasta Política > Elementos de Política > Resultados. En la pestaña Authorization > Authorization Profiles, seleccione +Add.



Cree el perfil de autorización para la VLAN a la que están asignados los clientes de autenticación local:

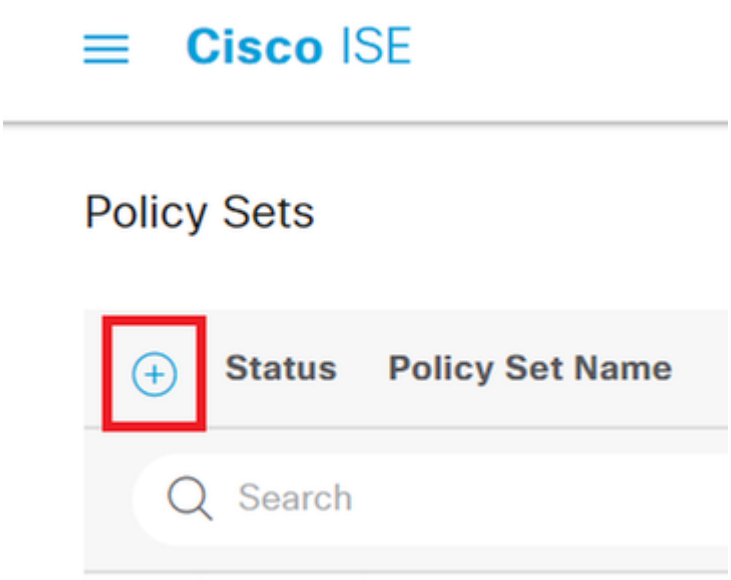


En la esquina inferior derecha, haga clic en Submit.

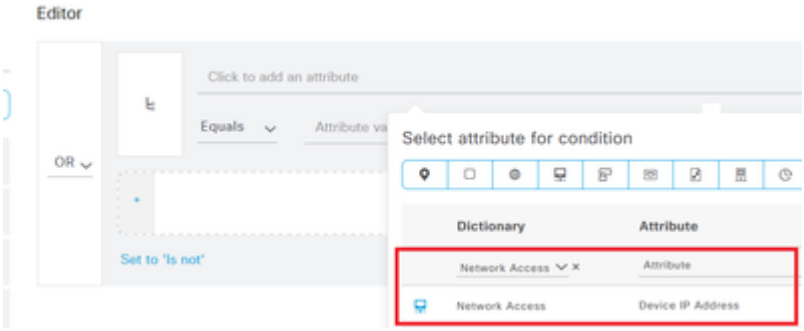
Verá los detalles de los atributos que ISE envía al WLC/AP en un escenario exitoso.

Paso 7. Vaya a Política > Juegos de Políticas. Cree un nuevo conjunto de directivas.

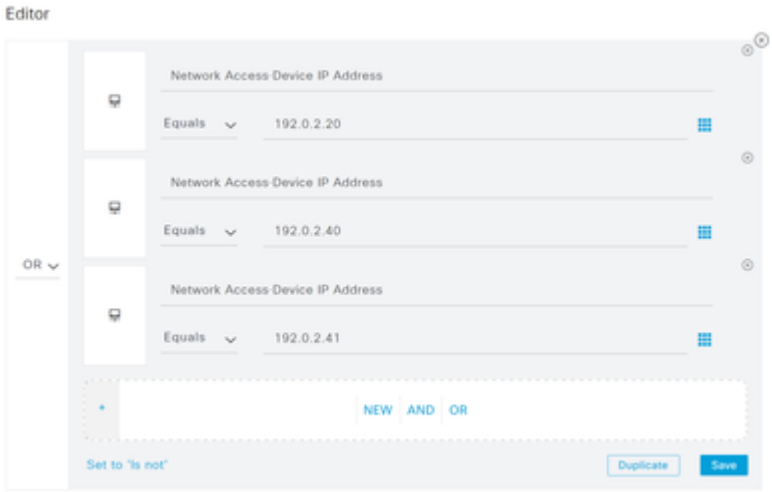
Haga clic en el signo +:



Dé un nombre al conjunto de directivas. En la columna Conditions, agregue la regla OR y el diccionario Network Access, con el atributo Device IP Address, seleccione Equals:

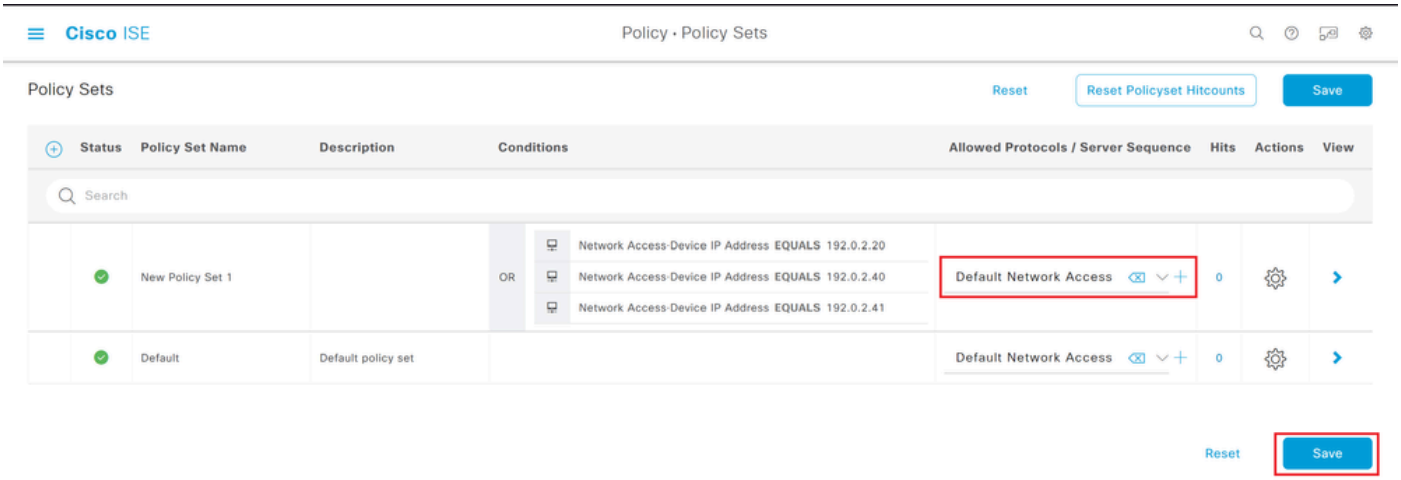


Agregue el WLC 9800 y las direcciones IP de los AP:

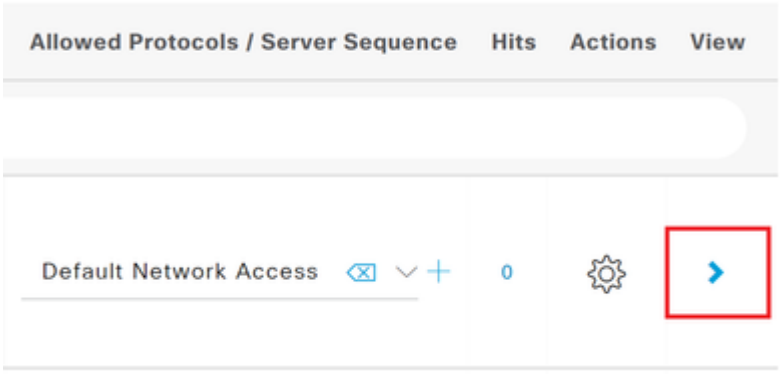


En la esquina inferior derecha, haga clic en Usar.

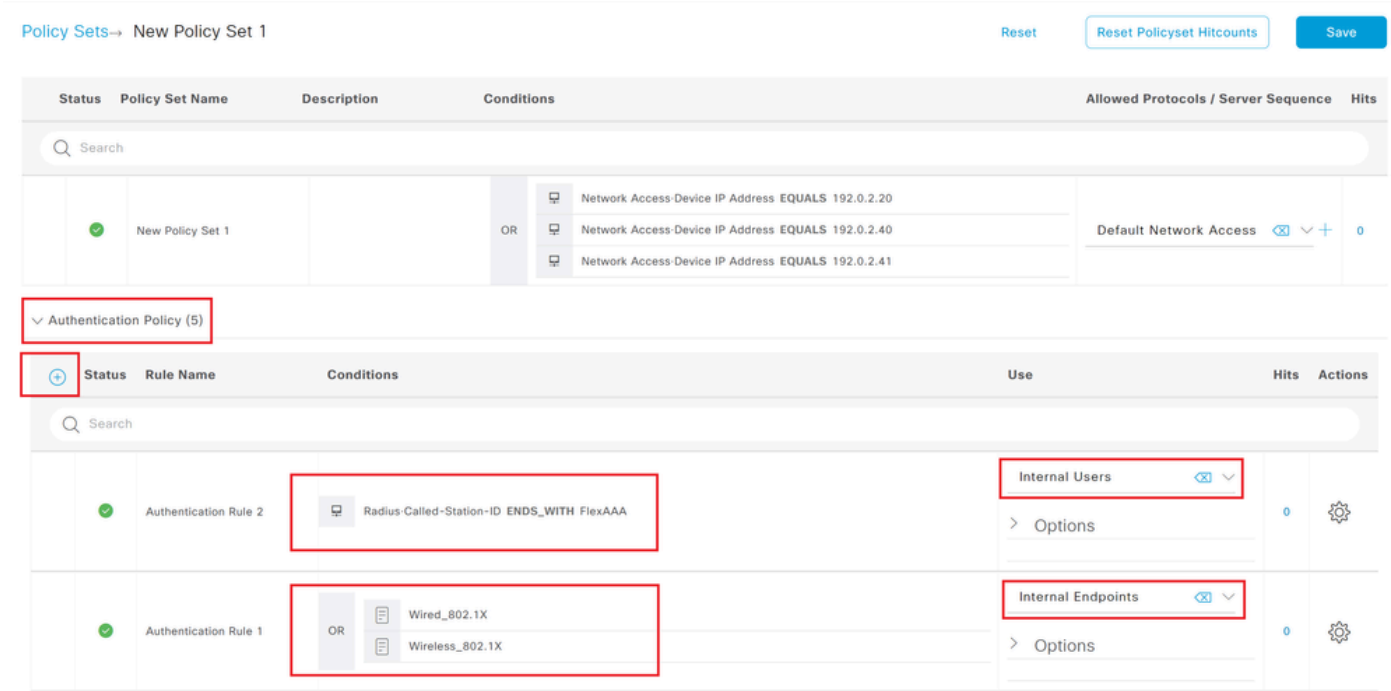
Paso 8. En la columna Allowed Protocols seleccione Default Network Access. Al final, haga clic en Save:



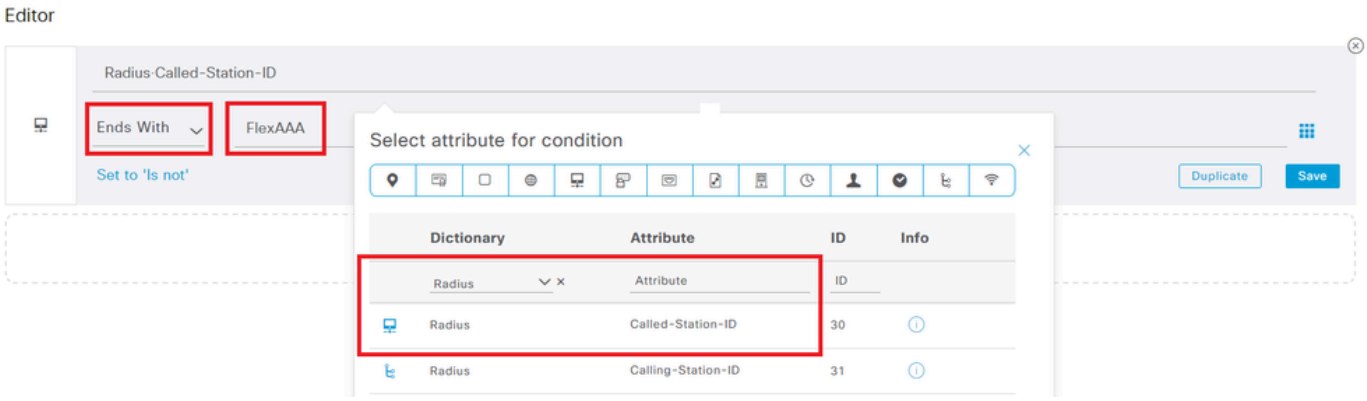
Paso 9. En la columna Ver, haga clic en el signo de flecha:



Paso 10. Expanda Authentication Policy, cree dos nuevas políticas: uno para el nombre WLAN y otro para la configuración 802.1X:

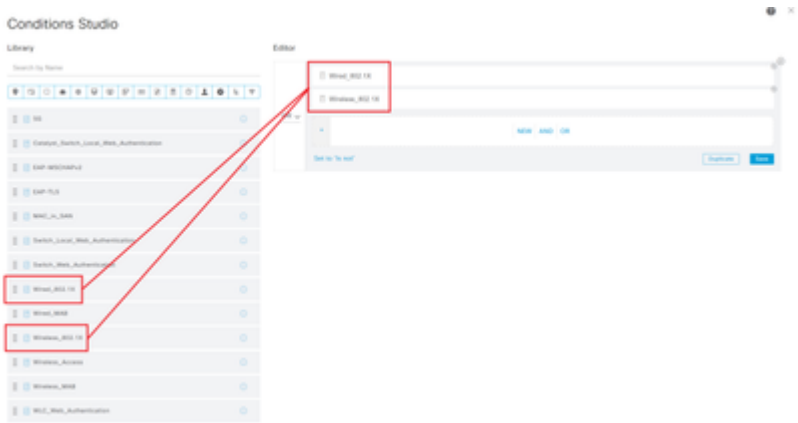


Para el nombre WLAN, cree la Condición con el diccionario Radius y el atributo Called-Station-ID. Seleccione Ends With (Termina con) y escriba el nombre de WLAN:



En la esquina inferior derecha, haga clic en Usar. Para esta política, en la columna Use, seleccione Internal Users.

Paso 11. Para la política 802.1X, cree la Condición con la biblioteca Wired_802.1X y Wireless_802.1X disponible en ISE. Puede arrastrar y soltar estos elementos y seleccionar la condición O:



En la esquina inferior derecha, haga clic en Usar. Para esta política, en la columna Use, seleccione Internal Endpoints.

Paso 12. Desplácese hasta Directiva de autorización y cree una nueva directiva. Dé un nombre y cree la misma Condición que la creada para el nombre WLAN en la Política de autenticación.

En la columna Profiles, seleccione en el menú desplegable el perfil PermitAccessVlan1432:



En la esquina inferior derecha, haga clic en Guardar.

Configuración de PSK WLAN con autenticación local

Paso 1. Configure primero los AP en el modo Flex como se describe en la sección Configuración del modo FlexConnect en el sitio remoto.

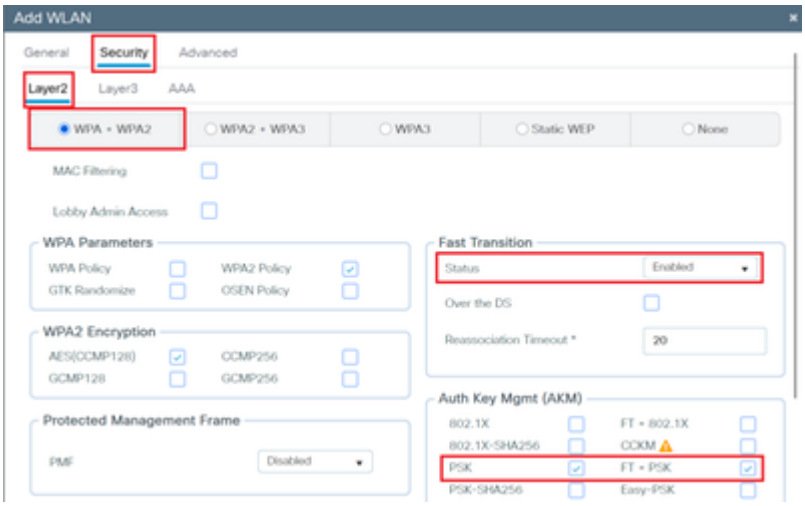
Paso 2. Cree la WLAN.

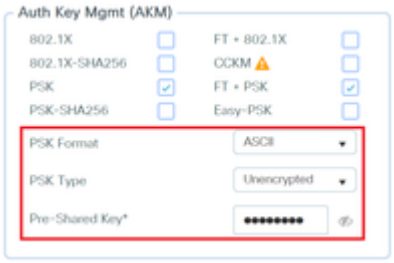
Vaya a Configuration > Tags & Profiles > WLANs, seleccione +Add.

En la etiqueta General, cree un nombre para Profile Name (Nombre del perfil), SSID y enable Status (Activar estado):



Paso 3. Navegue hasta Seguridad > Capa 2 pestaña seleccione WPA+WPA2, Transición rápida como habilitada, Auth Key Mgmt PSK y FT+PSK, elija el formato PSK y el tipo PSK que desee, y escriba la clave precompartida que desea que utilicen sus clientes:





Haga clic en Update & Apply to Device.

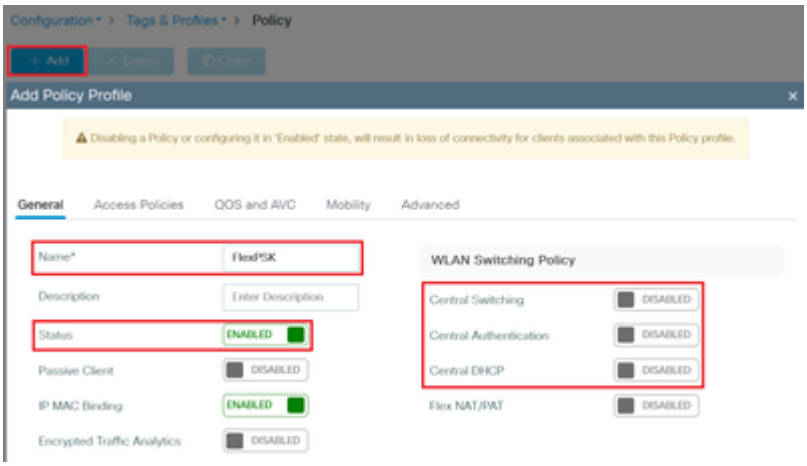
Puede ver la WLAN creada:



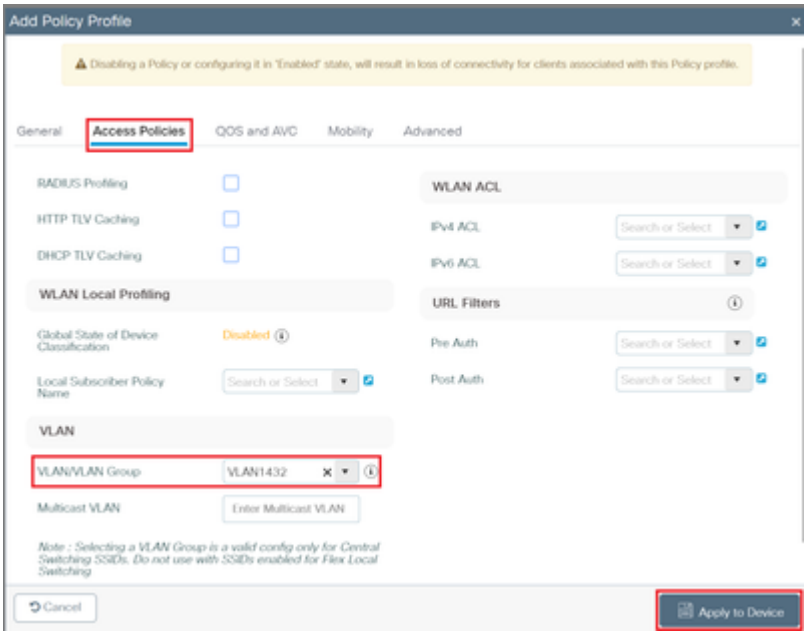
Paso 4. Crear el Perfil de Política.

Vaya a Configuration > Tags & Profiles > Policy .

Seleccione +Add y en la ficha General asigne un nombre al perfil de política, habilite el estado y deshabilite el switching central, la autenticación central y el DHCP central:

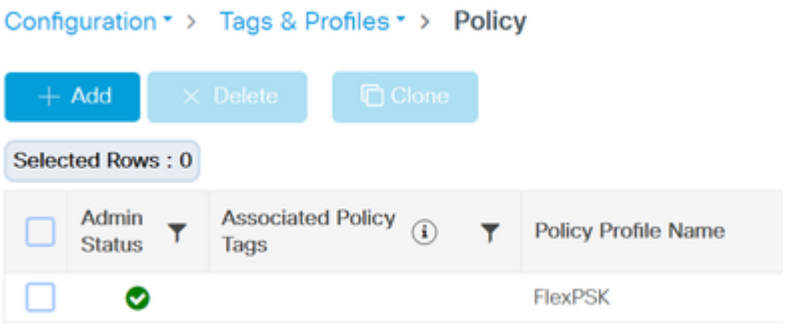


Paso 5. Navegue a la pestaña Políticas de acceso, seleccione la VLAN:



Haga clic en Update & Apply to Device.

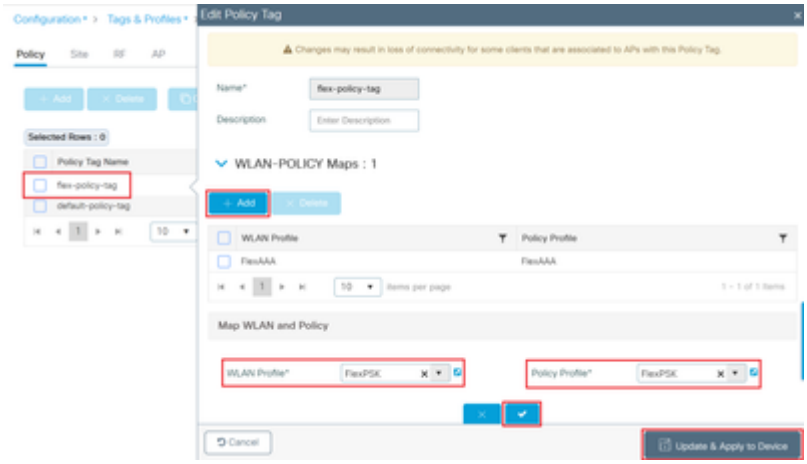
Puede ver el perfil de directiva en la lista:



Paso 6. Puede crear una nueva etiqueta de política o editar la existente.

Vaya a Configuration > Tags & Profiles > Tags para editar la etiqueta de política existente. Seleccione la etiqueta que desea editar.

Seleccione +Add en WLAN-POLICY Maps. En Perfil WLAN (Perfil WLAN), seleccione la WLAN creada anteriormente en el menú desplegable. En Perfil de directiva, seleccione el Perfil de directiva creado anteriormente en el menú desplegable. Haga clic en el botón de verificación y, a continuación, en Aplicar al dispositivo:



Si la etiqueta de política ya está asignada en el AP, no necesita hacer nada más.

Si no es así, asigne la etiqueta de política en la etiqueta APs. Navegue hasta Configuración > Inalámbrico > Puntos de acceso. Seleccione el AP para cambiar la etiqueta de política y haga clic en "Update & Apply to Device" (Actualizar y aplicar al dispositivo).

El AP se desune y vuelve a unirse con la nueva etiqueta de política.

Cuando el AP se une de nuevo, puede verificar la lista de puntos de acceso, confirmar que el AP está en el modo Flex, y tiene las etiquetas asignadas correctas.

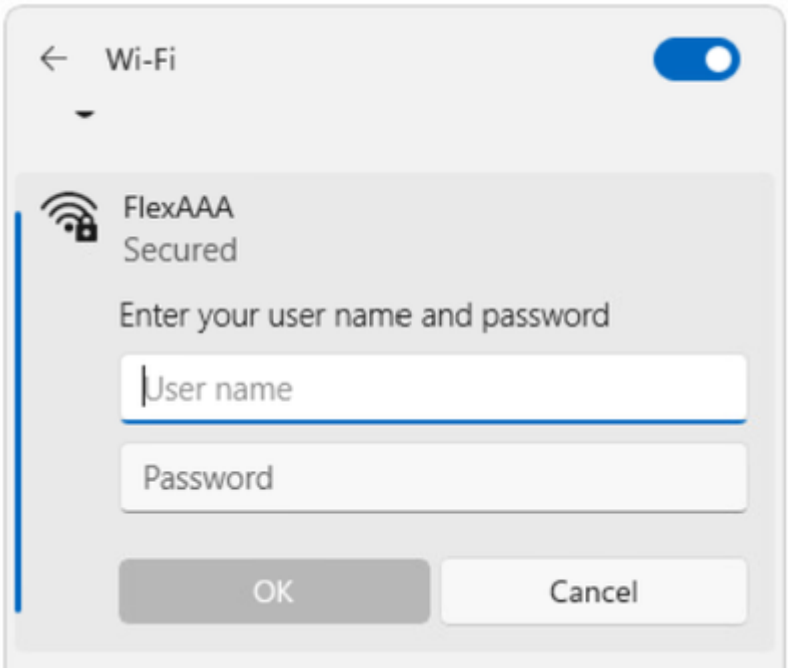
CLI:

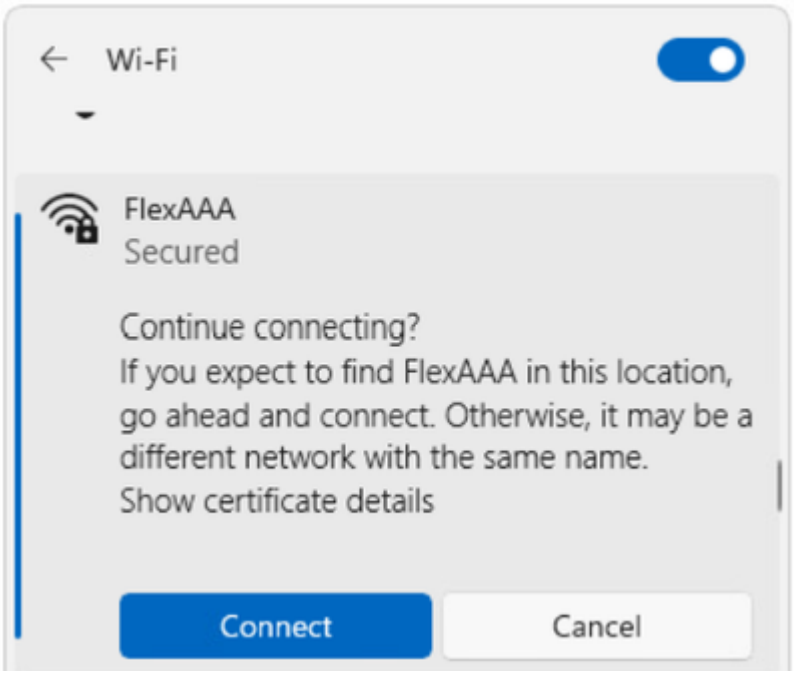
```
wlan FlexPSK 5 FlexPSK
radio policy dot11 24ghz
radio policy dot11 5ghz
security ft
security wpa psk set-key ascii 0 Password123
no security wpa akm dot1x
security wpa akm ft psk
security wpa akm psk
```

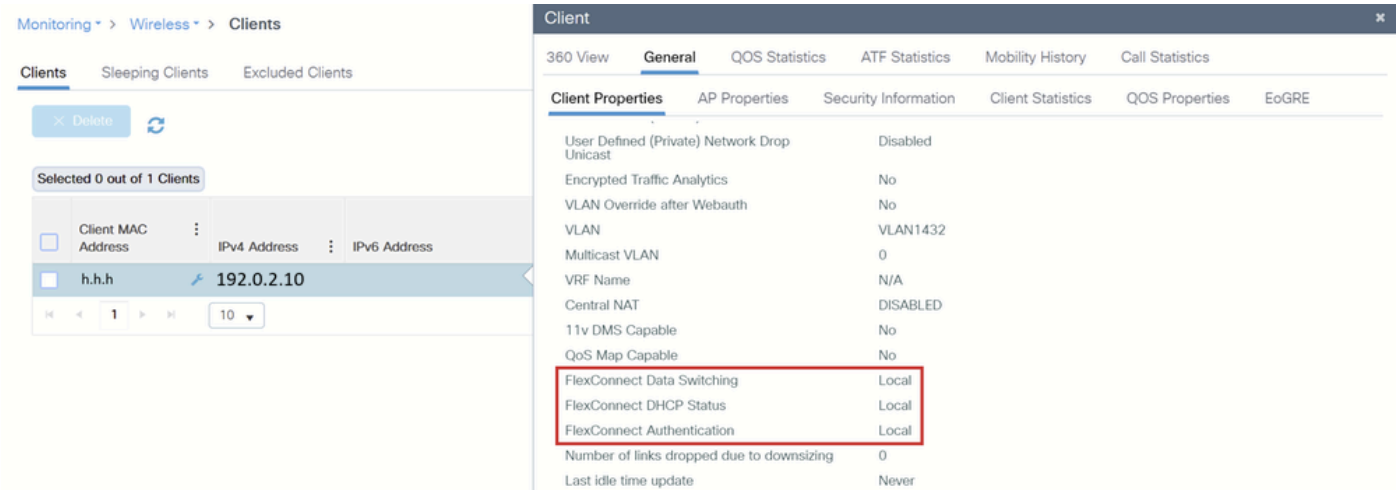
```
no shutdown
!
wireless profile policy FlexPSK
no central authentication
no central dhcp
no central switching
vlan VLAN1432
no shutdown
!
wireless tag policy flex-policy-tag
wlan FlexAAA policy FlexAAA
wlan FlexPSK policy FlexPSK
!
ap h.h.h (AP Radio MAC address)
policy-tag flex-policy-tag
site-tag Flex-site
rf-tag default-rf-tag
```

Verificación

Para WLAN 802.1x:







CLI:

```
C9800-1#show wireless client mac-address      h.h.h        detail

Client MAC Address : h.h.h
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address :192.0.2.10
Client IPv6 Addresses :
Client Username : test
AP MAC Address :
AP Name: CW9164I-ROW-LAB2
AP slot : 1
Client State : Associated
Policy Profile : FlexAAA
Flex Profile : Flex
Wireless LAN Id: 4
WLAN Profile Name: FlexAAA
Wireless LAN Network Name (SSID): FlexAAA
BSSID :
Connected For : 134 seconds
Protocol : 802.11ac
Channel : 48
Client IIF-ID : 0xa0000001
Association Id : 33
```

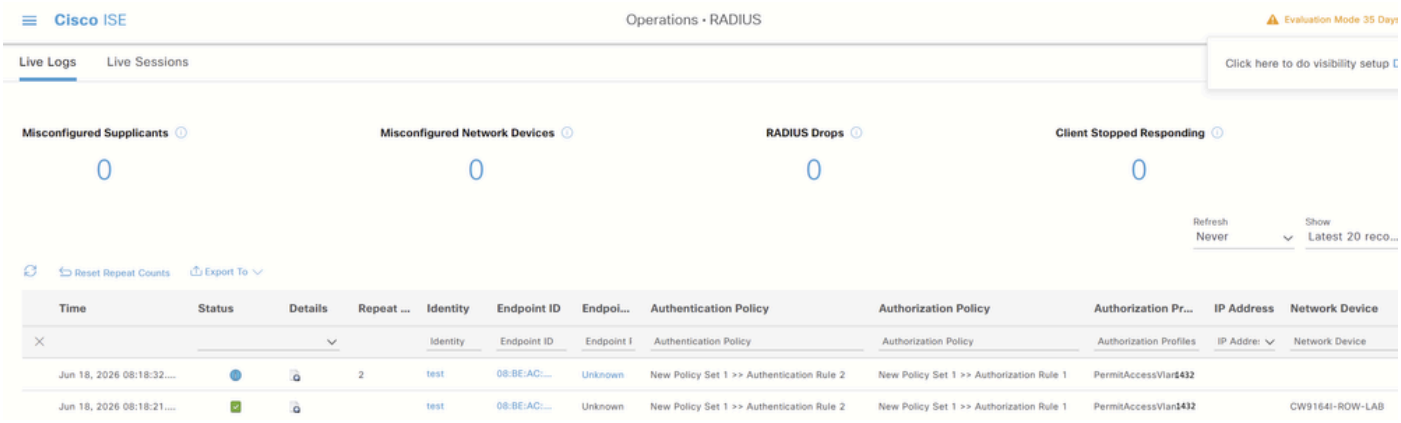
```
QoS Map Capable : No
FlexConnect Data Switching : Local
FlexConnect Dhcp Status : Local
FlexConnect Authentication : Local
Client Statistics:
```

En la CLI del AP:

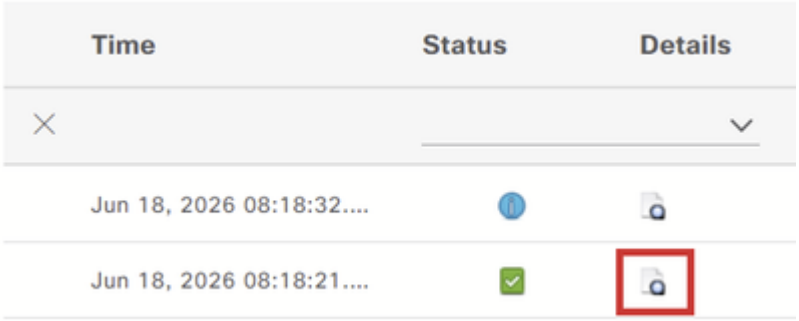
```
CW9164I-ROW-LAB#show dot11 clients

Total dot11 clients: 1
      Client MAC   Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
MM:MM:MM:MM:MM:MM          1       1  33   FlexAAA  -45 MCS9ISS          No         No
```

En ISE



IP Address	Network Device	Device Port	Identity Group	Posture ...	Server
IP Addre:	Network Device	Device Port	Identity Group	Posture Sta	Server
		Radio:1Wlan:1			ISE1
	CW9164I-ROW-LAB	Radio:1Wlan:1	User Identity Groups:ALL_ACCOUNTS (default),Unknown		ISE1



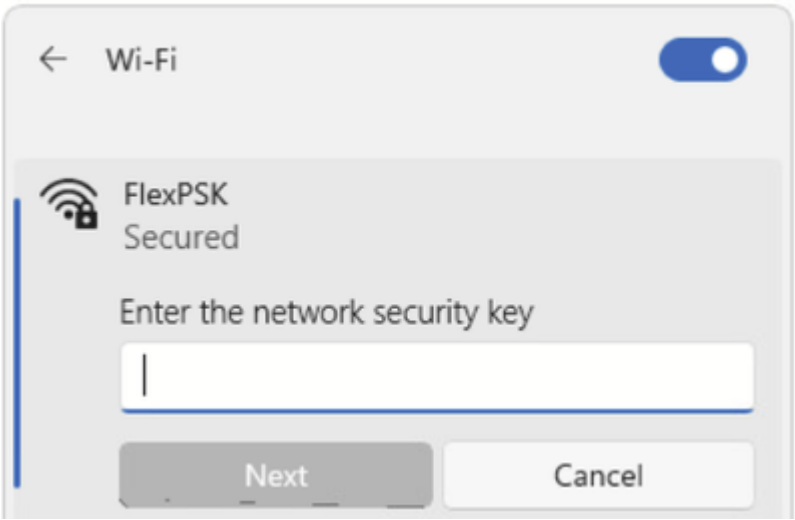
Cisco ISE

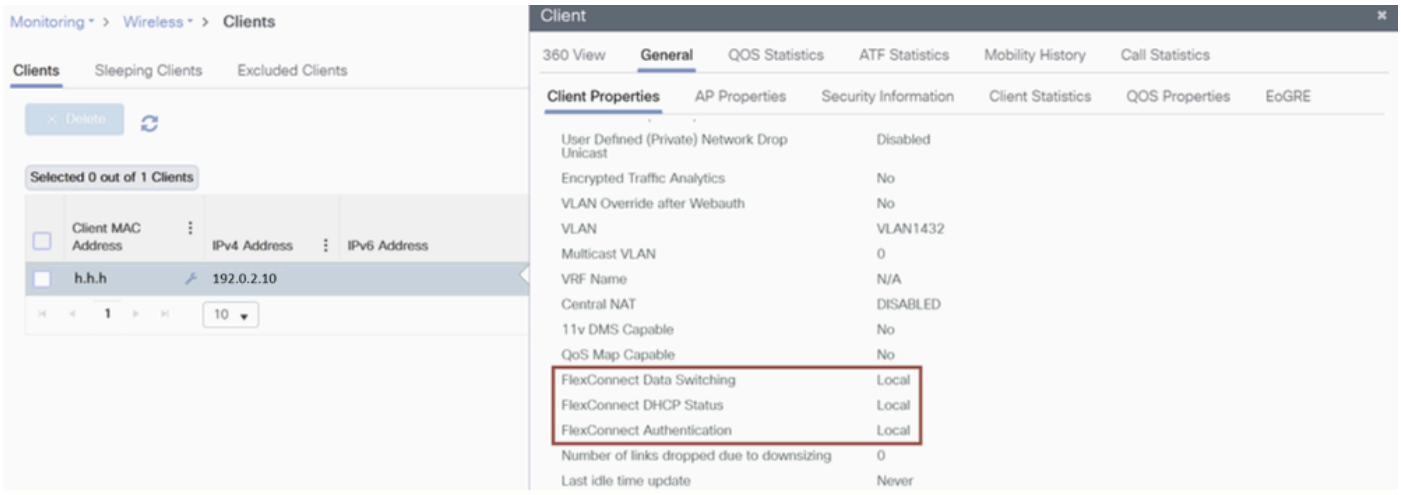
Overview

Event	5200 Authentication succeeded
Username	test
Endpoint Id	HH:HH:HH:HH:HH:HH
Endpoint Profile	Unknown
Authentication Policy	New Policy Set 1 >> Authentication Rule 2
Authorization Policy	New Policy Set 1 >> Authorization Rule 1
Authorization Result	PermitAccessVlan1432

Authentication Identity Store	Internal Users
Identity Group	User Identity Groups:ALL_ACCOUNTS (default),Unknown
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-MSCHAPv2)
Service Type	Framed
Network Device	CW9164I-ROW-LAB
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	192.0.2.40
NAS Port Id	Radio:1Wlan:1
NAS Port Type	Wireless - IEEE 802.11
Authorization Profile	PermitAccessVlan1432
Response Time	64 milliseconds

Para WLAN PSK:





CLI:

```
C9800-1#show wireless client mac-address h.h.h detail

Client MAC Address : h.h.h
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address : 192.0.2.10
Client IPv6 Addresses :
Client Username: N/A
AP MAC Address :
AP Name: CW9164I-ROW-LAB2
AP slot : 1
Client State : Associated
Policy Profile : FlexPSK
Flex Profile : Flex
Wireless LAN Id: 5
WLAN Profile Name: FlexPSK
Wireless LAN Network Name (SSID): FlexPSK
BSSID :
Connected For : 116 seconds
Protocol : 802.11ac
Channel : 48
Client IIF-ID : 0xa0000001
Association Id : 33
```

```
QoS Map Capable : No
FlexConnect Data Switching : Local
FlexConnect Dhcp Status : Local
FlexConnect Authentication : Local
Client Statistics:
```

En la CLI del AP:

```
CW9164I-ROW-LAB#show dot11 clients

Total dot11 clients: 1
      Client MAC   Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
                        1       2  33   FlexPSK  -45 MCS9ISS           No          No
```

Troubleshoot

Habilite las depuraciones de AP y el seguimiento de RA con la dirección MAC del cliente, en sincronización.

En el AP habilite estas depuraciones:

debug flexconnect event
debug flexconnect pmk
debug flexconnect dot11r
debug dot11 client management information
debug dot11 client management critical
debug dot11 client management errors
debug dot11 client management events

Para WLAN 802.1x:

Los logs de debugs AP con autenticación exitosa:

El AP maneja la máquina de estado 802.11 y la administración de claves locales.
El AP procesa la asociación y prepara al cliente para la autenticación.

```
[*06/19/2026 06:49:00.1836] CLSM[HH:HH:HH:HH:HH:HH]: client moved from UNASSOC to AUTH
[*06/19/2026 06:49:00.1890] wcp/flex_roam_st :: Flexconnect 11r enabled for client HH:HH:HH:HH:HH:HH
[*06/19/2026 06:49:00.1908] CLSM[HH:HH:HH:HH:HH:HH]: client moved from AUTH to ASSOC
[*06/19/2026 06:49:00.1909] Sending ADD MOBILE to client SM for local auth client mac HH:HH:HH:HH:HH:HH
[*06/19/2026 06:49:00.1931] CLSM[HH:HH:HH:HH:HH:HH]: client moved from ASSOC to 8021X
```

El AP procesa la autorización, aplica el reemplazo de VLAN y mueve al cliente al estado FWD (Reenvío).

```
[*06/19/2026 06:49:20.3601] received WCP_EVENT_CLIENT_AUTHORIZE (non) roaming case clearing roam flags
[*06/19/2026 06:49:20.3601] CLSM[HH:HH:HH:HH:HH:HH]: WCP_EVENT_CLIENT_AUTHORIZE : Plumbing key info to
[*06/19/2026 06:49:20.3612] wcp/flex_roam_st :: Flexconnect AAA Override Vlan with WLAN mapping: 1432 f
[*06/19/2026 06:49:20.3625] CLSM[HH:HH:HH:HH:HH:HH]: client moved from 8021X to IPLEARN_PENDING
[*06/19/2026 06:49:20.3627] wcp/flex_roam_st :: Flexconnect Sending HREAP_APAUTH_CLIENT_ADD
[*06/19/2026 06:49:20.3627] CLSM[HH:HH:HH:HH:HH:HH]: Retrieved key for FT+FT_DOT1X algono: 8, vlanId: 1
[*06/19/2026 06:49:20.3627] CLSM[HH:HH:HH:HH:HH:HH]: Local auth (Add) on radio 1 Vap 0 reported to WLC
[*06/19/2026 06:49:20.3701] chatter: pmk_tracker :: PMKTracker: add dot11r entry for client HH:HH:HH:HH
[*06/19/2026 06:49:20.4313] CLSM[HH:HH:HH:HH:HH:HH]: Authorize succeeded to radio intf apr1v0
[*06/19/2026 06:49:20.4317] CLSM[HH:HH:HH:HH:HH:HH]: Local auth on radio 1 Vap 0 IP 192.0.2.10 updatere
[*06/19/2026 06:49:20.4318] CLSM[HH:HH:HH:HH:HH:HH]: client moved from IPLEARN_PENDING to FWD
```

Registros de seguimiento de RA para la misma autenticación satisfactoria:

El seguimiento de RA registra la orquestación de la sesión del WLC. El WLC valida la identidad y la política del cliente.
El WLC reconoce la asociación de FlexConnect.

```
2026/06/19 06:49:20.934325580 {wncd_x_R0-1}{1}: [client-orch-sm] [18318]: (note): MAC: hhhh.hhhh.hhhh H
2026/06/19 06:49:20.936543415 {wncd_x_R0-1}{1}: [dot1x] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040000
2026/06/19 06:49:20.936579730 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
2026/06/19 06:49:20.936600851 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
2026/06/19 06:49:20.936654791 {wncd_x_R0-1}{1}: [ewlc-infra-evq] [18318]: (note): Authentication Succes
2026/06/19 06:49:20.936769433 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
```

El WLC empuja la política al AP.

```
2026/06/19 06:49:20.937447786 {wncd_x_R0-1}{1}: [svm] [18318]: (info): [hhhh.hhhh.hhhh] Applied User Pr
2026/06/19 06:49:20.937451734 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: c
2026/06/19 06:49:20.937452534 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: t
2026/06/19 06:49:20.937455590 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: v
2026/06/19 06:49:20.937456177 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: m
2026/06/19 06:49:20.937458436 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: u
2026/06/19 06:49:20.937462127 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile:tu
2026/06/19 06:49:20.937462755 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: t
2026/06/19 06:49:20.937463426 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: t
2026/06/19 06:49:20.937464035 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: t
```

Autorización correcta.

```
2026/06/19 06:49:20.937594042 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
2026/06/19 06:49:20.937597878 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
```

Parámetros del cliente.
19/06/2026 06:49:20.939394217 {wncd_x_R0-1}{1}: [dot11] [18318]: (nota): MAC: hhhh.hhhh.hhhh Parámetros de entrada de ruta de datos del cliente - ssid:FlexAAA,slot_id:1 bssid ifid: 0x0, id_radio: 0x90400008, wlan_ifid: 0xf0400004

El WLC aprende la IP vía DHCP/ARP local.
19/06/2026 06:49:21.001000218 {wncd_x_R0-1}{1}: [client-iplearn] [18318]: (nota): MAC: hhhhh.hhhh.hhhh La IP del cliente se ha aprendido correctamente. Método: IP de indagación de IP: 192.0.2.10

El cliente está completamente conectado.
19/06/2026 06:49:21.002363496 {wncd_x_R0-1}{1}: [errmsg] [18318]: (información): %CLIENT_ORCH_LOG-6-CLIENT_ADDED_TO_RUN_STATE: R0/1: wncd: Entrada de nombre

de usuario (prueba) junto con ssid (FlexAAA) para el dispositivo con MAC: hhhh.hhhh.hhhh en el canal (48)
19/06/2026 06:49:21.002795009 {wncd_x_R0-1}{1}: [client-orch-state] [18318]: (nota): MAC: hhhh.hhhh.hhhh Transición de estado de cliente: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_RUN

Escenario independiente

Comportamiento durante la pérdida de conectividad AP-WLC y la recuperación subsiguiente.

El AP se une al WLC. El cliente realiza una autenticación 802.1X exitosa y el AP pasa al cliente al estado FWD (Forwarding).

En ISE RADIUS Live Logs vemos la sesión del cliente.

```
[*07/06/2026 20:26:05.8590] chatter: pmk_tracker :: PMKTracker: add dot11r entry for client HH:HH:HH:HH
[*07/06/2026 20:26:05.9330] CLSM[HH:HH:HH:HH:HH:HH]: Authorize succeeded to radio intf apr0v0
[*07/06/2026 20:26:05.9330] CLSM[HH:HH:HH:HH:HH:HH]: Local auth on radio 0 Vap 0 IP 192.0.2.10 updatere
[*07/06/2026 20:26:05.9330] CLSM[HH:HH:HH:HH:HH:HH]: client moved from IPLEARN_PENDING to FWD
```

```
CW9164I-ROW-LAB2#show dot11 clients

Total dot11 clients: 1
Client MAC Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH 0 1 1 FlexAAA -40 M7 No No
```

El AP no alcanza el WLC, agota su conteo de retransmisión, y cambia al modo autónomo. Los clientes existentes permanecen conectados localmente.

```
[*07/06/2026 20:28:47.0840] Re-Tx Count=1, Max Re-Tx Value=5, SendSeqNum=33, NumofPendingMsgs=4
[*07/06/2026 20:28:50.0860] Re-Tx Count=2, Max Re-Tx Value=5, SendSeqNum=34, NumofPendingMsgs=5
[*07/06/2026 20:28:53.0870] Re-Tx Count=3, Max Re-Tx Value=5, SendSeqNum=35, NumofPendingMsgs=6
[*07/06/2026 20:28:56.0990] Re-Tx Count=4, Max Re-Tx Value=5, SendSeqNum=35, NumofPendingMsgs=6
[*07/06/2026 20:28:59.1000] Re-Tx Count=5, Max Re-Tx Value=5, SendSeqNum=35, NumofPendingMsgs=6
[*07/06/2026 20:29:02.1010] Max retransmission count exceeded, going back to DISCOVER mode.
[*07/06/2026 20:29:02.1020] Flexconnect Switching to Standalone Mode!
[*07/06/2026 20:29:02.2170] CAPWAP State: DTLS Teardown
```

Pero el cliente sigue conectado:

CW9164I-ROW-LAB2#show dot11 clients

Total de clientes dot11: 1
ID de ranura MAC de cliente ID de WLAN ID Nombre de WLAN RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH 0 1 FlexAAA -40 M7 No No

Cuando el cliente se traslada a otro AP en modo autónomo, el intercambio de señales EAP falla debido a la incapacidad de alcanzar el servidor RADIUS. El cliente es desautorizado y eliminado del AP.

```
[*07/06/2026 20:34:44.7240] CLSM[HH:HH:HH:HH:HH:HH]: Session timeout
[*07/06/2026 20:36:15.2670] hostapd:apr0v0: CTRL-EVENT-EAP-RETRANSMIT hh:hh:hh:hh:hh:hh
[*07/06/2026 20:36:15.2670] hostapd:apr0v0: CTRL-EVENT-EAP-TIMEOUT-FAILURE hh:hh:hh:hh:hh:hh
[*07/06/2026 20:36:15.2680] wcp/flex_roam_st :: Flexconnect hapdev: Received UNAUTHORIZE for hh:hh:hh:h
[*07/06/2026 20:36:15.2680] wcp/flex_roam_st :: Flexconnect hapdev: recv'd UNAUTH with DISCONNECT REQUE
[*07/06/2026 20:36:15.2680] CLSM[HH:HH:HH:HH:HH:HH]: Client delete initiated with timeout of 10 seconds
[*07/06/2026 20:36:15.2770] CLSM[HH:HH:HH:HH:HH:HH]: Remove success from ClientIPTable on apr0v0
[*07/06/2026 20:36:15.2780] CLSM[HH:HH:HH:HH:HH:HH]: Not sending DELETE to cont, reason CLIENT_DEL_EAP_
[*07/06/2026 20:36:15.2780] CLSM[HH:HH:HH:HH:HH:HH]: Deauthorize succeeded to radio intf apr0v0
[*07/06/2026 20:36:15.2780] CLSM[HH:HH:HH:HH:HH:HH]: client moved from FWD to DELETE_PENDING
[*07/06/2026 20:36:15.2880] CLSM[HH:HH:HH:HH:HH:HH]: Send Deauth with reason 2 force 1 - Radio 0 Vap 0
[*07/06/2026 20:36:25.0830] CLSM[HH:HH:HH:HH:HH:HH]: Delete timeout
[*07/06/2026 20:36:25.0830] CLSM[HH:HH:HH:HH:HH:HH]: Delete client reassoc 0 succeeded to radio intf ap
```

El AP envía la sesión del cliente al servidor RADIUS de respaldo.

El AP recupera la conectividad al WLC. El AP vuelve al modo conectado y sincroniza la información de la sesión del cliente local con el WLC.

La sesión del cliente realiza transiciones entre los nodos ISE principal y de copia de seguridad en función del estado de la conectividad del punto de acceso.

El AP y el cliente se muestran como conectados en el WLC, y el cliente no notó ninguna desconexión o inestabilidad cuando la conectividad entre el AP y el WLC estaba inactiva.

```
CW9164I-ROW-LAB2#show dot11 clients

Total dot11 clients: 0


Upon roaming back, the client undergoes local authentication. The AP processes the association and move

[*07/06/2026 20:48:49.2830] CLSM[HH:HH:HH:HH:HH:HH]: US Auth(b0) seq 2653 IF 23 slot 0 vap 0 len 30 sta
[*07/06/2026 20:48:49.2840] CLSM[HH:HH:HH:HH:HH:HH]: DS Auth len 30 slot 0 vap 0
[*07/06/2026 20:48:49.2850] CLSM[HH:HH:HH:HH:HH:HH]: Driver send mgmt frame success Radio 0 Vap 0
[*07/06/2026 20:48:49.2850] CLSM[HH:HH:HH:HH:HH:HH]: client moved from UNASSOC to AUTH
[*07/06/2026 20:48:49.2920] CLSM[HH:HH:HH:HH:HH:HH]: US Reassoc Req(20) seq 2654 IF 23 slot 0 vap 0 len
```

```
[*07/06/2026 20:48:49.2930] CLSM[HH:HH:HH:HH:HH:HH]: AUTH TYPE RSNIE DOT1X
[*07/06/2026 20:48:49.2940] CLSM[HH:HH:HH:HH:HH:HH]: Populate client capability: cap_from_click=true, m
[*07/06/2026 20:48:49.2940] Flexconnect local_auth 1 local_assoc 1 frame subtype 32
[*07/06/2026 20:48:49.2940] CLSM[HH:HH:HH:HH:HH:HH]: radio id: 0, vap id: 0, max clients for this wlan:
[*07/06/2026 20:48:49.2940] CLSM[HH:HH:HH:HH:HH:HH]: radio state: 1, client state: 1, max_client_per_ra
[*07/06/2026 20:48:49.2940] Adding RM Capable IE - Len = 5, RRM[0] = 73, RRM[1] = c0
[*07/06/2026 20:48:49.2940] DS [re]Assoc 1 req_len=201 resp_len=146 11r_len=0 cckm 0 qos_flag 1 status
[*07/06/2026 20:48:49.2940] CLSM[HH:HH:HH:HH:HH:HH]: DS Reassoc Resp(30) IF 0 slot 0 vap 0 state AUTH,
[*07/06/2026 20:48:49.2950] CLSM[HH:HH:HH:HH:HH:HH]: Driver send mgmt frame success Radio 0 Vap 0
[*07/06/2026 20:48:49.2950] CLSM[HH:HH:HH:HH:HH:HH]: client moved from AUTH to ASSOC
[*07/06/2026 20:48:49.2950] Sending ADD MOBILE to client SM for local auth client mac HH:HH:HH:HH:HH:HH
[*07/06/2026 20:48:49.2960] wcp/flex_roam_st :: Flexconnect Sending ADD_MOBILE_PAYLOAD (v4-client-acl-n
[*07/06/2026 20:48:49.2960] wcp/flex_roam_st :: Flexconnect encode_and_send_add_mobile_to_dott11_client
[*07/06/2026 20:48:49.2960] CLSM[HH:HH:HH:HH:HH:HH]: ADD_MOBILE AID 1
[*07/06/2026 20:48:49.2960] CLSM[HH:HH:HH:HH:HH:HH]: Driver Add Client success AID 1 Radio 0 Vap 0 Enc
[*07/06/2026 20:48:49.2960] CLSM[HH:HH:HH:HH:HH:HH]: Added to ClientIPTable on apr0v0
[*07/06/2026 20:48:49.2970] CLSM[HH:HH:HH:HH:HH:HH]: client moved from ASSOC to 8021X
[*07/06/2026 20:48:49.2970] CLSM[HH:HH:HH:HH:HH:HH]: Added to WCP client table AID 1 Radio 0 Vap 0 Enc
[*07/06/2026 20:48:49.2980] wcp/flex_roam_st :: Flexconnect hapdev: client WCP_EVENT_CLIENT_ASSOC/REASS
[*07/06/2026 20:48:49.6360] received WCP_EVENT_CLIENT_AUTHORIZE (non) roaming case clearing roam flags
[*07/06/2026 20:48:49.6360] wcp/flex_roam_st :: Flexconnect (AUTHORIZE) received PTK thru wcp_event
[*07/06/2026 20:48:49.6370] wcp/flex_roam_st :: Flexconnect HH:HH:HH:HH:HH:HH client ACL , Qos Profile:
[*07/06/2026 20:48:49.6370] wcp/flex_roam_st :: Flexconnect AAA Override Vlan with WLAN mapping: 1432 f
[*07/06/2026 20:48:49.6370] wcp/flex_roam_st :: Flexconnect Sending ADD_MOBILE_PAYLOAD (v4-client-acl-n
[*07/06/2026 20:48:49.6370] wcp/flex_roam_st :: Flexconnect encode_and_send_add_mobile_to_dott11_client
[*07/06/2026 20:48:49.6370] CLSM[HH:HH:HH:HH:HH:HH]: ADD_MOBILE AID 1
[*07/06/2026 20:48:49.6380] CLSM[HH:HH:HH:HH:HH:HH]: check vlan override vlan 1432
[*07/06/2026 20:48:49.6380] CLSM[HH:HH:HH:HH:HH:HH]: Client ADD Encrypt Key success AID 1 Radio 0 Enc 4
[*07/06/2026 20:48:49.6380] CLSM[HH:HH:HH:HH:HH:HH]: client moved from 8021X to IPLEARN_PENDING
[*07/06/2026 20:48:49.6390] wcp/flex_roam_st :: Flexconnect Sending HREAP_APAUTH_CLIENT_ADD
[*07/06/2026 20:48:49.6900] CLSM[HH:HH:HH:HH:HH:HH]: Authorize succeeded to radio intf apr0v0
[*07/06/2026 20:48:49.6910] CLSM[HH:HH:HH:HH:HH:HH]: client moved from IPLEARN_PENDING to FWD


CW9164I-ROW-LAB2#show dot11 clients

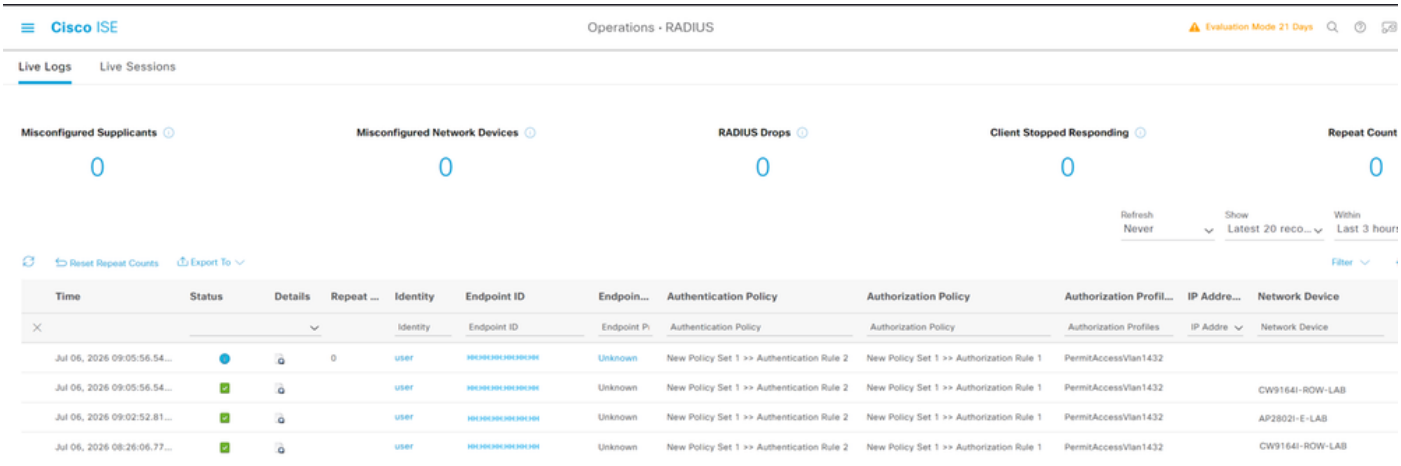
Total dot11 clients: 1
Client MAC Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH 0 1 1 FlexAAA -39 M7 No No



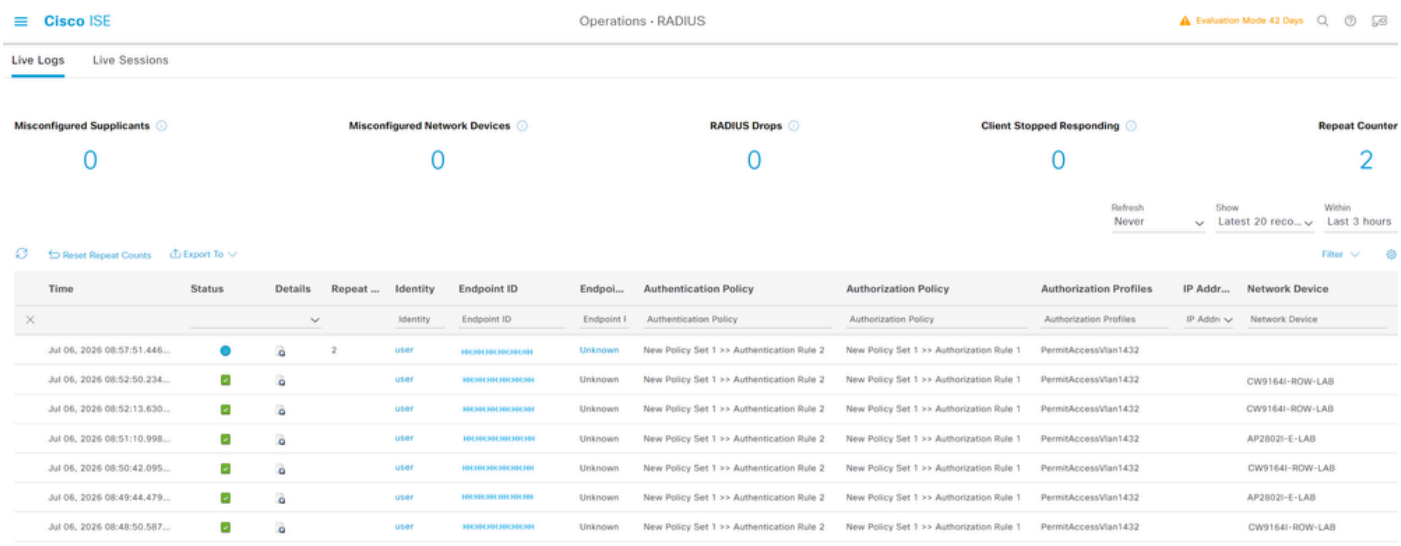

*07/06/2026 20:59:57.7690] Discovery Response from 192.0.2.20
[*07/06/2026 21:00:08.0080] CAPWAP State: DTLS Setup
[*07/06/2026 21:00:08.4820] CAPWAP State: Join
[*07/06/2026 21:00:09.3740] Sending Join request to 192.0.2.20 through port 5253, packet size 1376
[*07/06/2026 21:00:09.3780] Join Response from 192.0.2.20, packet size 1397
[*07/06/2026 21:00:09.4040] CAPWAP State: Image Data
[*07/06/2026 21:00:09.5020] CAPWAP State: Configure
[*07/06/2026 21:00:12.5510] CAPWAP State: Run
[*07/06/2026 21:00:12.6480] AP has joined controller C9800-1
[*07/06/2026 21:00:12.6490] Flexconnect Switching to Connected Mode!
[*07/06/2026 21:00:12.6520] CLSM[HH:HH:HH:HH:HH:HH]: AP_REAP_CLIENT_INFO_PAYLOAD Client MAC HH:HH:HH:HH
[*07/06/2026 21:00:12.6520] AssocTimeAtAP 1783371169 clientBitmap=0x13
[*07/06/2026 21:00:12.6520] CLSM[00:00:00:00:00:00]: Numbers of Local Switching clients to report : 1
[*07/06/2026 21:00:14.8270] chatter: pmk_tracker :: PMKTracker: add dot11r entry for client HH:HH:HH:HH
[*07/06/2026 21:00:14.8270] chatter: bssid BB:BB:BB:BB:BB:BB, life_time 1783371774, created_at 17833716
[*07/06/2026 21:00:14.8280] chatter: pmk_tracker :: PMKTracker: add dot11r entry for client HH:HH:HH:HH
[*07/06/2026 21:00:14.8280] chatter: bssid BB:BB:BB:BB:BB:BB, life_time 1783371774, created_at 17833716
```

```
CW9164I-ROW-LAB2# show dot11 clients

Total dot11 clients: 1
Client MAC Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH 0 1 1 FlexAAA -40 M7 No No
```



ISE principal: Registra la sesión inicial (08:26:06) y la sesión reanudada después de la restauración de la conectividad del WLC (09:02:52).



ISE de respaldo: Captura la actividad de la sesión (08:48:50 - 08:57:51) mientras el AP funcionaba en modo autónomo.

La primera sesión fue a las 08:26:06, después de que el AP perdió la conectividad al WLC y se movió al modo autónomo.

La sesión 09:02:52 es la primera sesión después de que el AP restableció la conectividad con el WLC.

Información Relacionada

- CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide, 2a edición
- Guía de Configuración del Software del Controlador Inalámbrico Cisco Catalyst Serie 9800, Cisco IOS XE 17.8.x - Capítulo: FlexConnect
- Notas de la versión del controlador inalámbrico Catalyst de Cisco serie 9800, versión 17.8.x de Cisco IOS XE Cupertino
- Matriz de funciones de los puntos de acceso inalámbricos de Cisco
- 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).