Configuración de asignación de VLAN dinámica con WLC basada en ISE para mapa de grupo de Active Directory

Contenido

Introducción

Este documento describe el concepto de asignación de VLAN dinámica.

Prerequisites

El documento describe cómo configurar el controlador de LAN inalámbrica (WLC) y el servidor de Identity Services Engine (ISE) para asignar clientes de LAN inalámbrica (WLAN) a una VLAN específica de forma dinámica.

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimientos básicos de controladores de LAN inalámbrica (WLC) y puntos de acceso ligeros (LAP)
- Conocimiento funcional de un servidor de autenticación, autorización y contabilidad (AAA) como ISE
- Conocimiento completo de las redes inalámbricas y de los problemas de seguridad

inalámbrica
- Conocimiento funcional y configurable de la asignación de VLAN dinámica
- Conocimientos básicos de los servicios de Microsoft Windows AD, así como de los conceptos de controlador de dominio y DNS
- Conocimiento básico del protocolo de control y aprovisionamiento de puntos de acceso (CAPWAP)

Componentes Utilizados

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

- WLC de Cisco serie 5520 que ejecuta la versión de firmware 8.8.111.0
- AP de Cisco serie 4800
- Suplicante nativo de Windows y NAM de Anyconnect
- Cisco Secure ISE versión 2.3.0.298
- Microsoft Windows 2016 Server configurado como controlador de dominio
- Switch Cisco serie 3560-CX que ejecuta la versión 15.2(4)E1

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.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Asignación de VLAN dinámica con servidor RADIUS

En la mayoría de los sistemas WLAN, cada WLAN tiene una política estática que se aplica a todos los clientes asociados a un identificador de conjunto de servicios (SSID) o WLAN en la terminología del controlador. Aunque es eficaz, este método tiene limitaciones porque requiere que los clientes se asocien con diferentes SSID para heredar diferentes QoS y directivas de seguridad.

La solución WLAN de Cisco aborda esta limitación gracias a la compatibilidad con las redes de identidad. Esto permite que la red anuncie un solo SSID, pero permite que usuarios específicos hereden diferentes QoS, atributos de VLAN y/o políticas de seguridad basadas en las credenciales del usuario.

La asignación de VLAN dinámica es una de estas funciones que colocan a un usuario inalámbrico en una VLAN específica en función de las credenciales suministradas por el usuario. Esta tarea de asignar usuarios a una VLAN específica es gestionada por un servidor de autenticación RADIUS, como Cisco ISE. Se puede utilizar, por ejemplo, para permitir que el host inalámbrico permanezca en la misma VLAN al desplazarlo dentro de una red del campus.

El servidor Cisco ISE autentica a los usuarios inalámbricos en una de las diversas bases de datos posibles, incluida su base de datos interna. Por ejemplo:

- BD interna
- Directorio activo
- Protocolo ligero de acceso a directorios (LDAP) genérico
- Bases de datos relacionales compatibles con ODBC (Open Database Connectivity)
- Servidores de token de SecurID de Rivest, Shamir y Adelman (RSA)
- Servidores de token compatibles con RADIUS

Los protocolos de autenticación de Cisco ISE y las fuentes de identidad externas admitidas enumeran los diversos protocolos de autenticación admitidos por las bases de datos internas y externas de ISE.

Este documento se centra en la autenticación de usuarios inalámbricos que utilizan la base de datos externa de Windows Active Directory.

Después de una autenticación correcta, ISE recupera la información de grupo de ese usuario de la base de datos de Windows y lo asocia al perfil de autorización correspondiente.

Cuando un cliente intenta asociarse con un LAP registrado con un controlador, el LAP pasa las credenciales del usuario al WLC con la ayuda del método EAP respectivo.

El WLC envía esas credenciales a ISE con el uso del protocolo RADIUS (encapsulando el EAP) e ISE pasa las credenciales de los usuarios a AD para su validación con la ayuda del protocolo KERBEROS.

AD valida las credenciales del usuario y, tras una autenticación correcta, informa al ISE.

Una vez que la autenticación es exitosa, el servidor ISE pasa ciertos atributos del Grupo de Trabajo de Ingeniería de Internet (IETF) al WLC. Estos atributos RADIUS deciden el ID de VLAN que se debe asignar al cliente inalámbrico. El SSID (WLAN, en términos de WLC) del cliente no importa porque el usuario siempre está asignado a este ID de VLAN predeterminado.

Los atributos del usuario de RADIUS que se utilizan para la asignación del ID de VLAN son:

- IETF 64 (tipo de túnel)—Establezca esto en VLAN
- IETF 65 (tipo de túnel medio)—Establezca esta opción en 802

- IETF 81 (ID de grupo privado de túnel)—Establezca esto en ID de VLAN

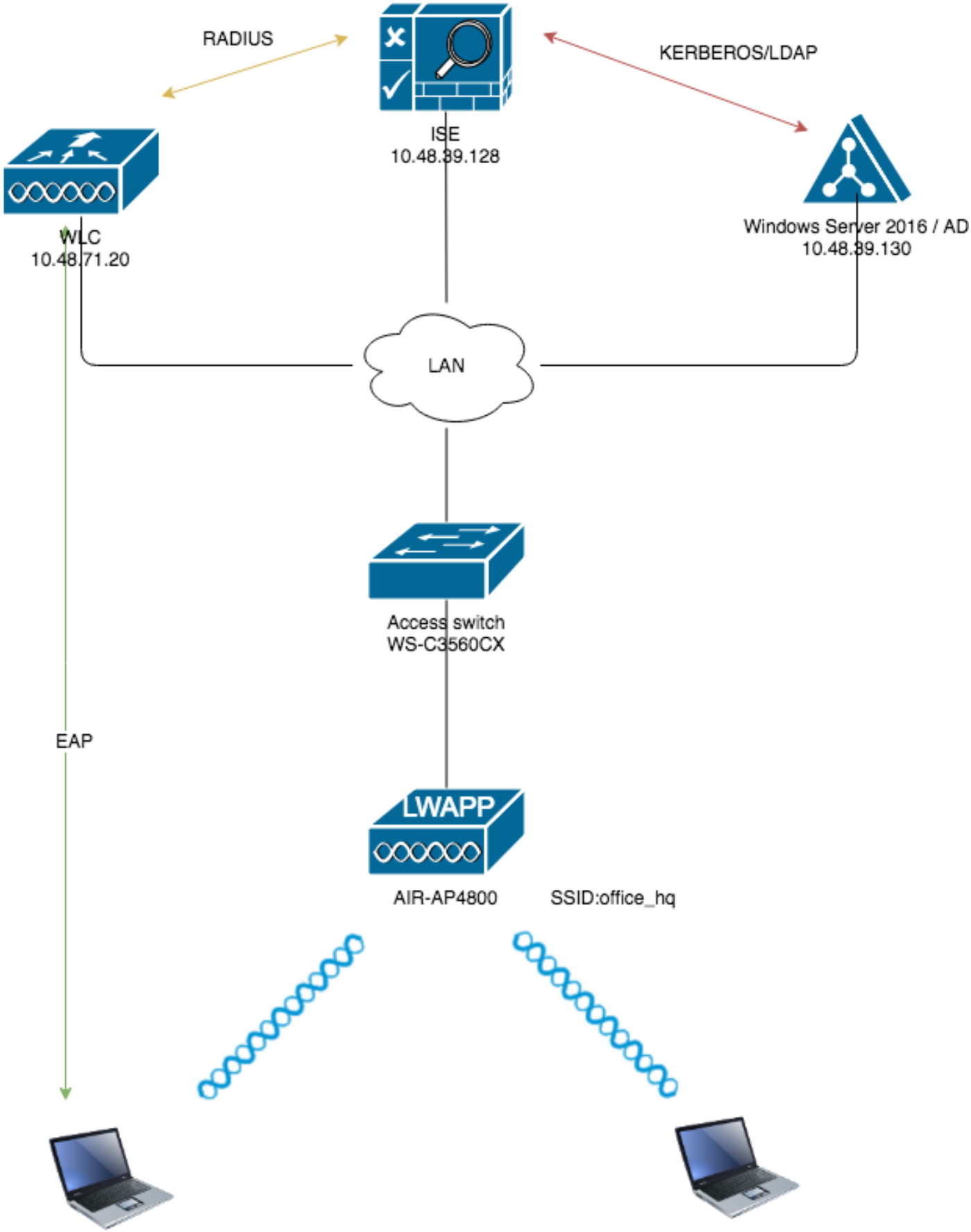
El ID de VLAN es de 12 bits y toma un valor entre 1 y 4094, ambos inclusive. Debido a que Tunnel-Private-Group-ID es de tipo cadena, como se define en RFC2868 para su uso con IEEE 802.1X, el valor entero de ID de VLAN se codifica como una cadena. Una vez que se envían estos atributos del túnel, es necesario rellenar el campo Tag (Etiqueta).

Como se indicó en RFC 2868, sección 3.1: el campo Tag tiene un octeto de longitud y está pensado para proporcionar un medio de agrupar atributos en el mismo paquete que hacen referencia al mismo túnel. Los valores válidos para este campo son de 0x01 a 0x1F, ambos incluidos. Si el campo Tag (Etiqueta) no se utiliza, debe tener el valor cero (0x00). Consulte RFC 2868 para obtener más información sobre todos los atributos de RADIUS.

Configurar

Esta sección proporciona la información necesaria para configurar las funciones descritas en el documento.

Diagrama de la red

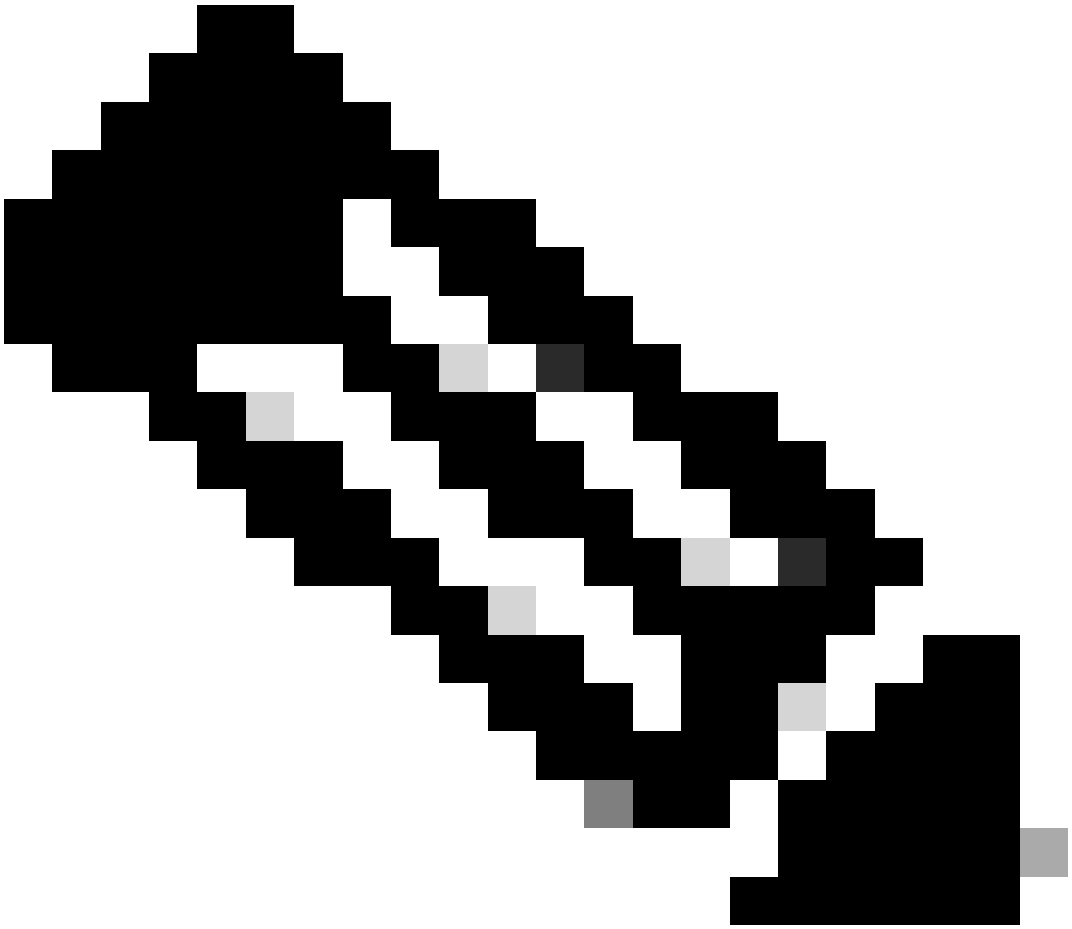


Configuraciones

Estos son los detalles de configuración de los componentes utilizados en este diagrama:

- La dirección IP del servidor ISE (RADIUS) es 10.48.39.128.
- La dirección de la interfaz de administración y del administrador AP del WLC es 10.48.71.20.
- El servidor DHCP reside en la red LAN y está configurado para los grupos de clientes respectivos; no se muestra en el diagrama.
- VLAN1477 y VLAN1478 se utilizan en esta configuración. Los usuarios del departamento de Marketing se configuran para ser colocados en la VLAN1477 y los usuarios del departamento de HR se configuran para ser colocados en la VLAN1478 por el servidor RADIUS cuando ambos usuarios se conectan al mismo SSID: office_hq.

  VLAN1477: 192.168.77.0/24. Gateway: 192.168.77.1 VLAN1478: 192.168.78.0/24. Gateway: 192.168.78.1
- Este documento utiliza 802.1x conPEAP-mschapv2como mecanismo de seguridad.



Nota: Cisco recomienda que utilice métodos de autenticación avanzados, como EAP-

---

FAST y EAP-TLS, para proteger la WLAN.

Estas suposiciones se realizan antes de realizar esta configuración:

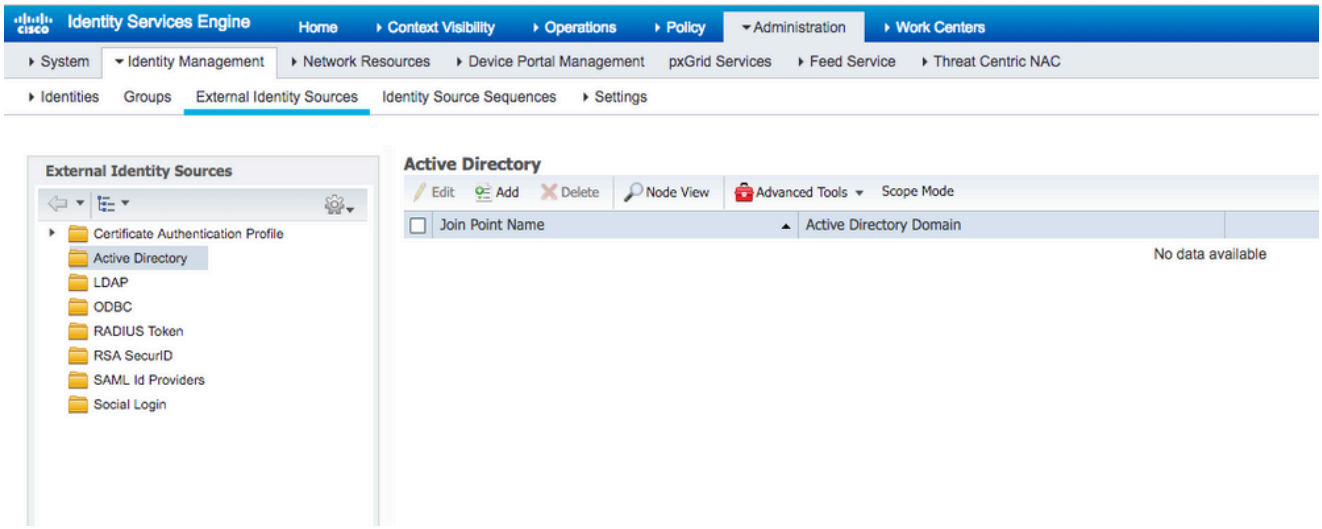
- El LAP ya está registrado con el WLC
- Al servidor DHCP se le asigna un ámbito DHCP
- Existe conectividad de capa 3 entre todos los dispositivos de la red
- El documento describe la configuración requerida en el lado inalámbrico y asume que la red con cables está en su lugar
- Los usuarios y grupos respectivos se configuran en AD

Para lograr la asignación de VLAN dinámica con WLC basados en la asignación de grupo de ISE a AD, se deben realizar estos pasos:

1. Integración de ISE a AD y configuración de políticas de autenticación y autorización para usuarios en ISE.
2. Configuración de WLC para soportar la autenticación dot1x y la invalidación AAA para el SSID 'office_hq'.
3. Configuración del solicitante del cliente final.

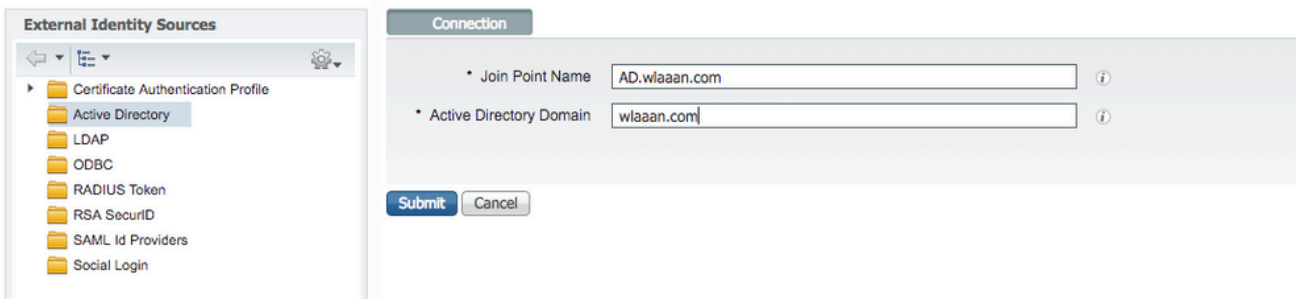
Integración de ISE a AD y configuración de políticas de autenticación y autorización para usuarios en ISE

1. Inicie sesión en la interfaz de usuario web de ISE con una cuenta de administrador.
2. Desplácese hastaAdministration > Identity management > External Identity Sources > Active directory.

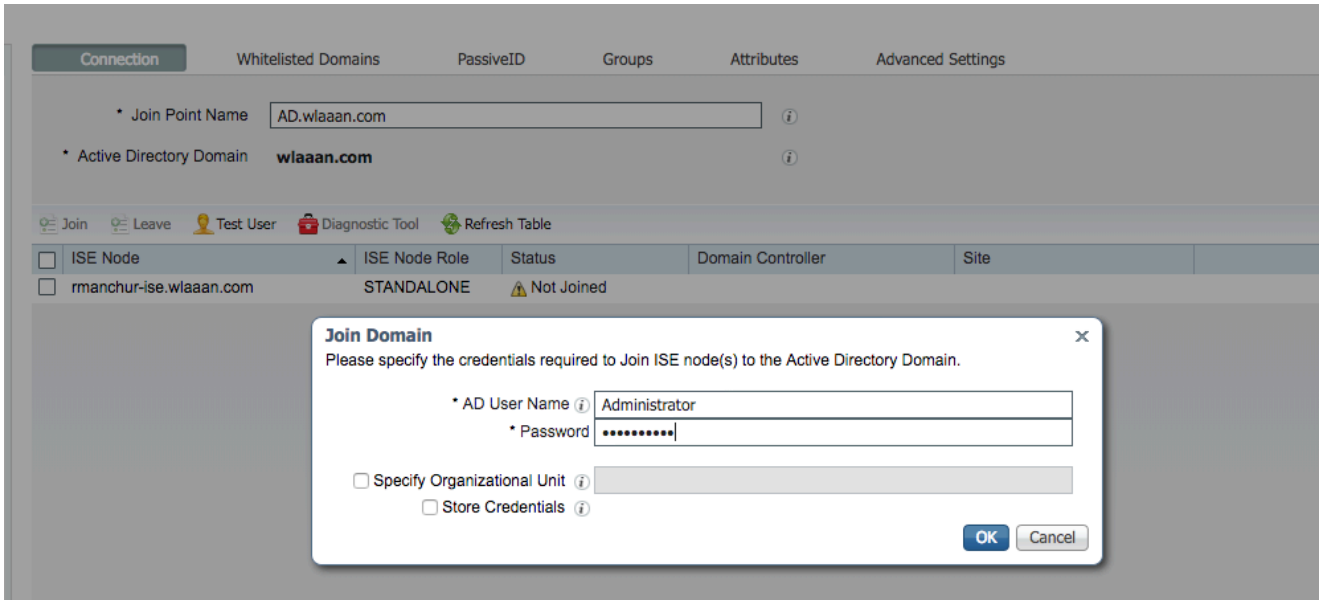


3. Haga clic en Agregar e ingrese el nombre de dominio y el nombre de almacén de identidad de la configuración de Nombre de punto de unión de Active Directory. En el ejemplo, ISE se registra en el dominiowlaaan.comy se especifica joinpoint comoAD.wlaaan.com: nombre localmente

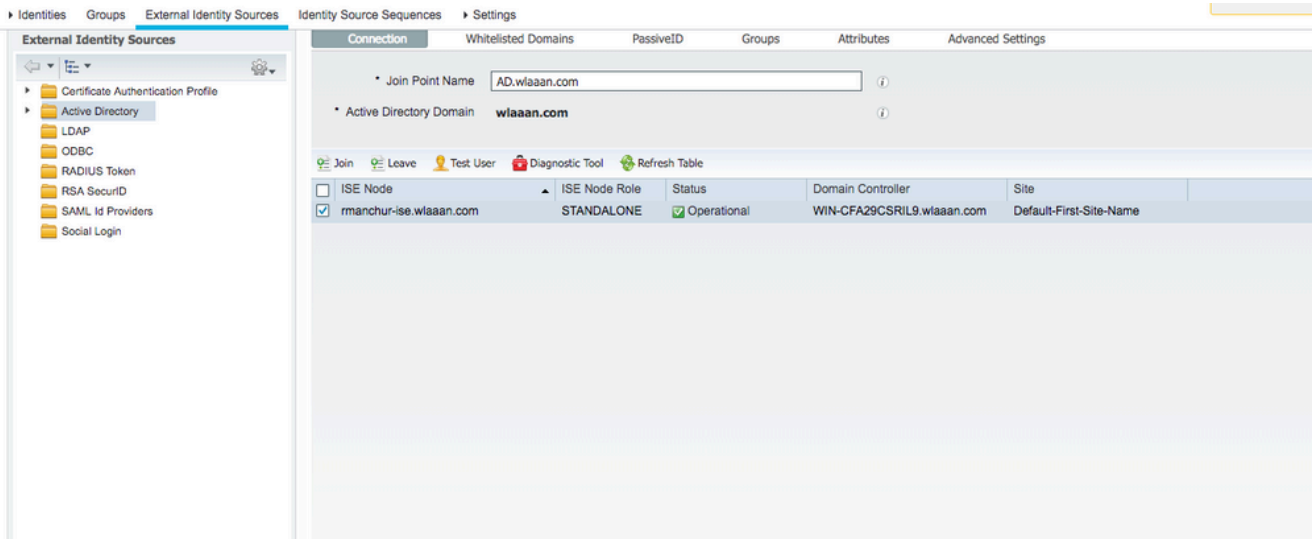
significativo para ISE.



4. Se abre una ventana emergente después de`Submit`pulsar un botón que le pregunta si desea unirse a ISE para AD inmediatamente. Pulse`Yes`y proporcione credenciales de usuario de Active Directory con derechos de administrador para agregar un nuevo host al dominio.



5. Después de este punto, debe haber registrado ISE correctamente en AD.

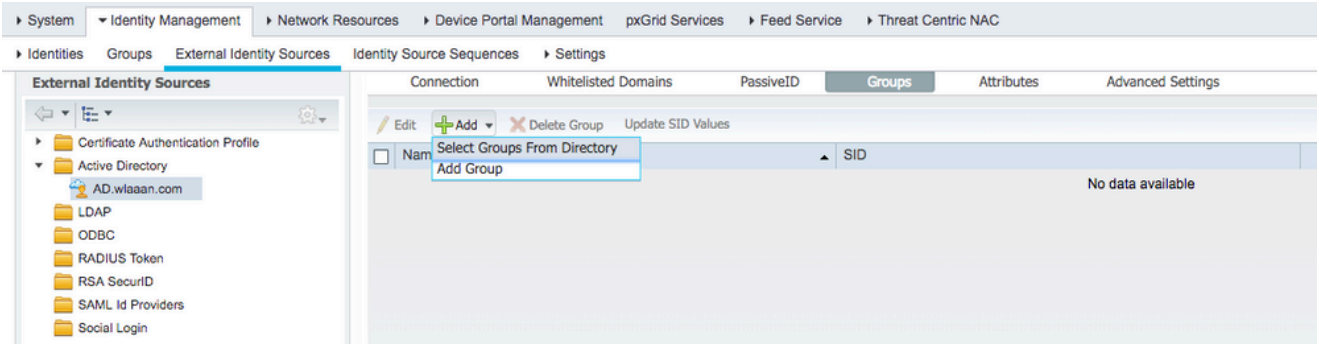


En caso de que tenga algún problema con el proceso de registro, puede utilizarDiagnostic Tool para ejecutar las pruebas necesarias para la conectividad de AD.

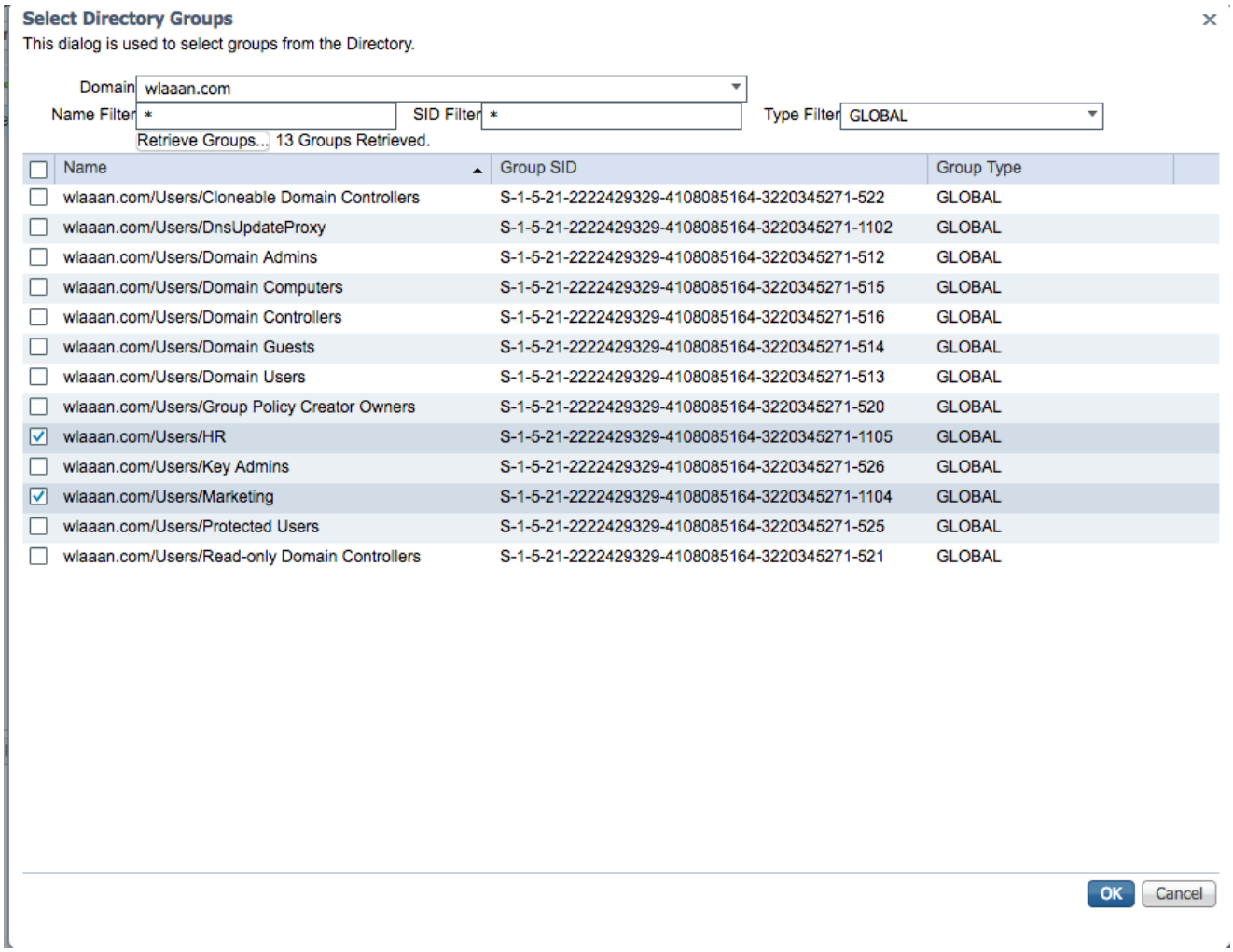
6. Debe recuperar los grupos de los directorios activos que se utilizan para asignar los perfiles de autorización respectivos. Desplácese hastaAdministration > Identity management > External Identity Sources > Active directory >

   > Groups

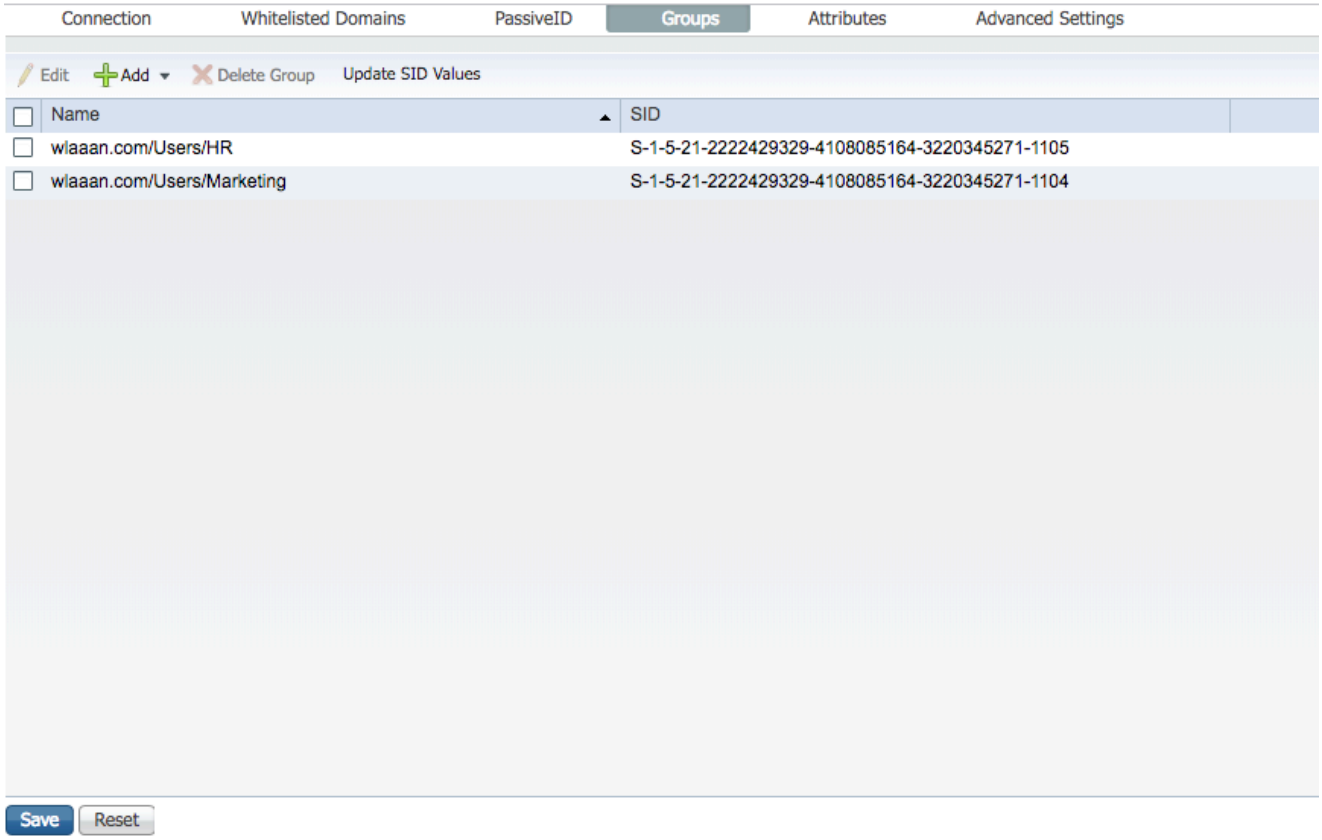
   , haga clic enAddy elijaSelect Groups from Active Directory.



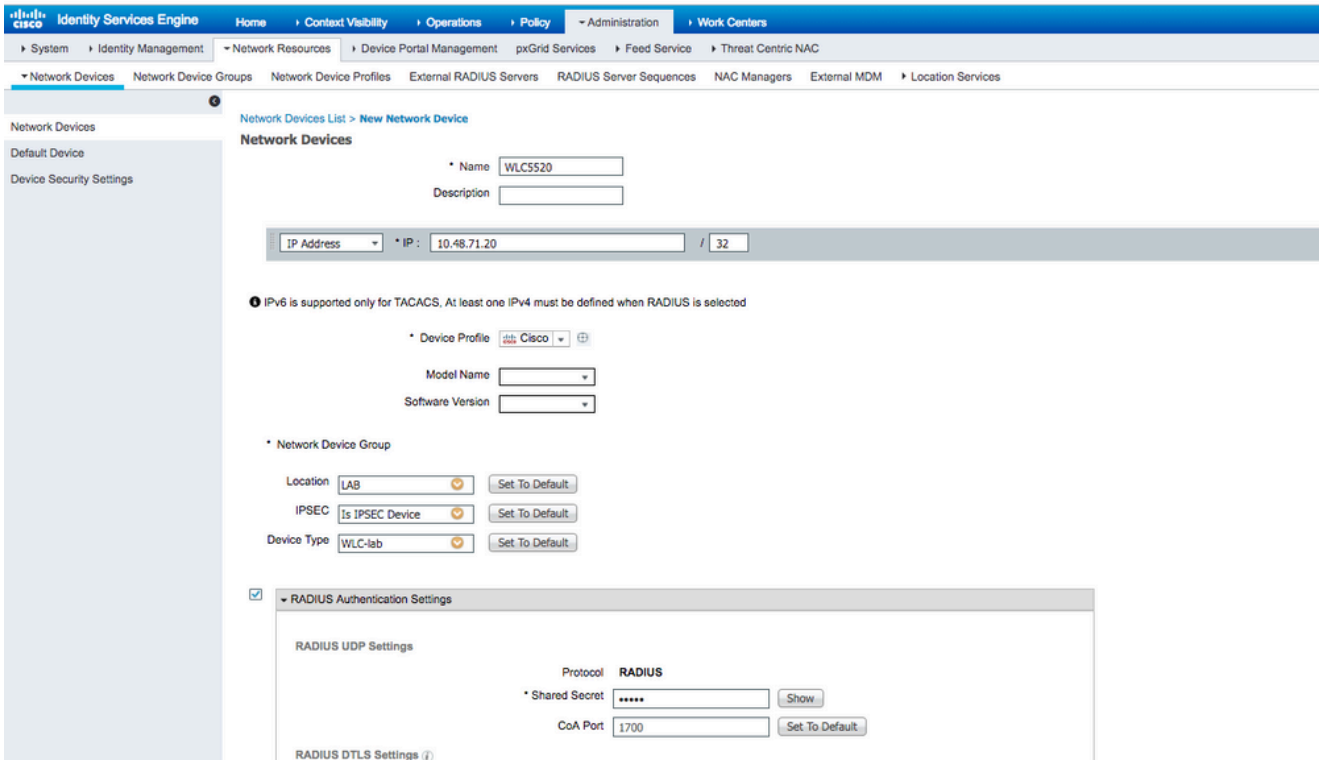
7. Se abre una nueva ventana emergente donde puede especificar un filtro para recuperar grupos específicos o recuperar todos los grupos de AD.
   Elija los grupos respectivos de la lista de grupos de AD y pulseOK.



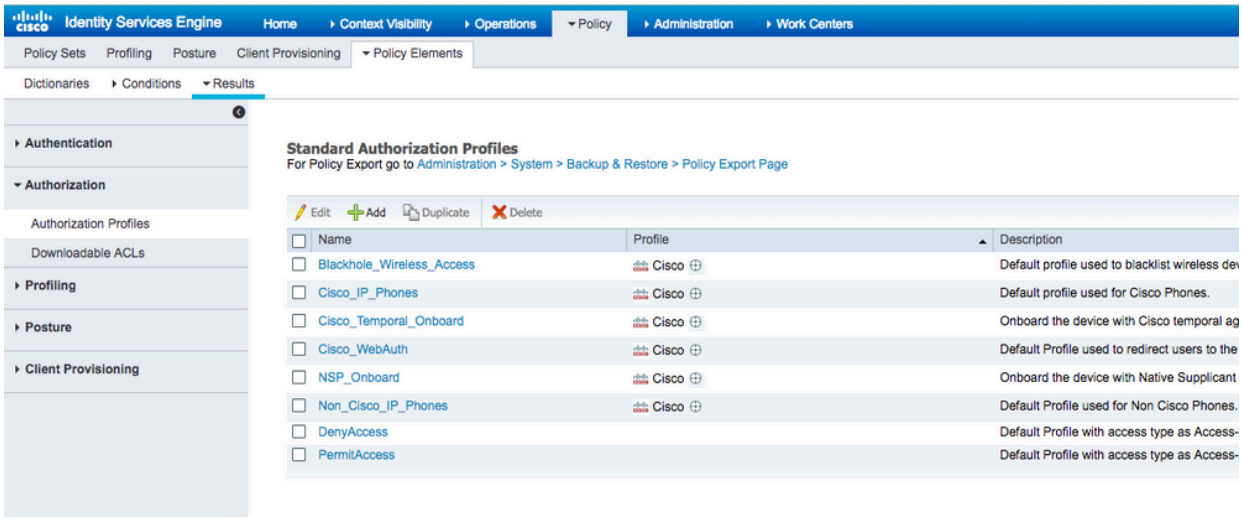
8. Los grupos respectivos se agregan a ISE y se pueden guardar. PulseSave.



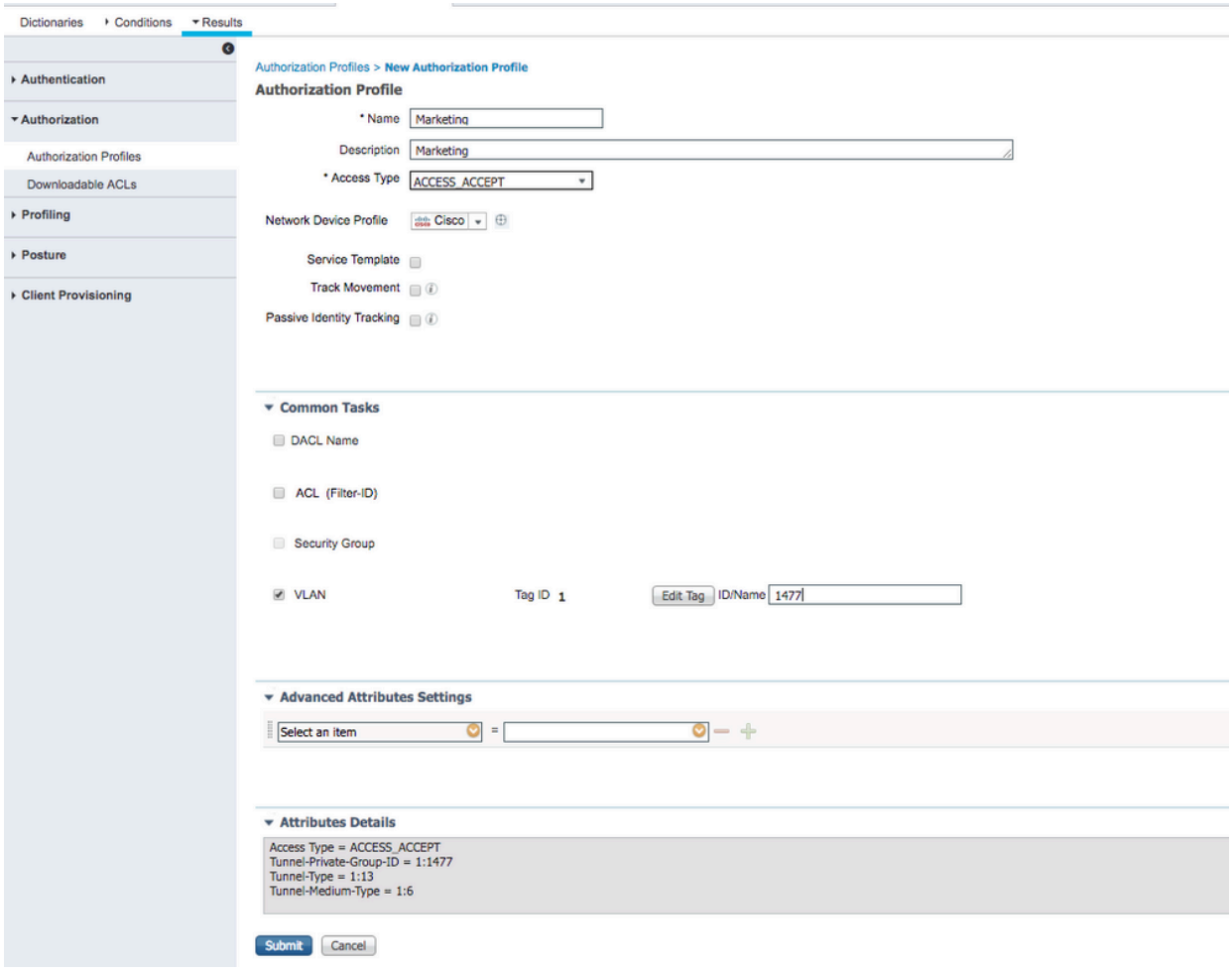
9. Agregue el WLC a la lista de dispositivos de red ISE: navegue hastaAdministration > Network Resources > Network Devicesy presioneAdd.
   Configuración completa, proporcionando la dirección IP de la administración del WLC y el secreto compartido del RADIUS entre el WLC e ISE.



10. Ahora, después de unirse a ISE en AD y agregar el WLC a la lista de dispositivos, puede iniciar la configuración de las políticas de autenticación y autorización para los usuarios.
    - Cree un perfil de autorización para asignar usuarios de Marketing a VLAN1477 y del grupo HR a VLAN1478.
      Navegue hasta Policy > Policy Elements > Results > Authorization > Authorization profiles y haga clic en el Add botón para crear un nuevo perfil.

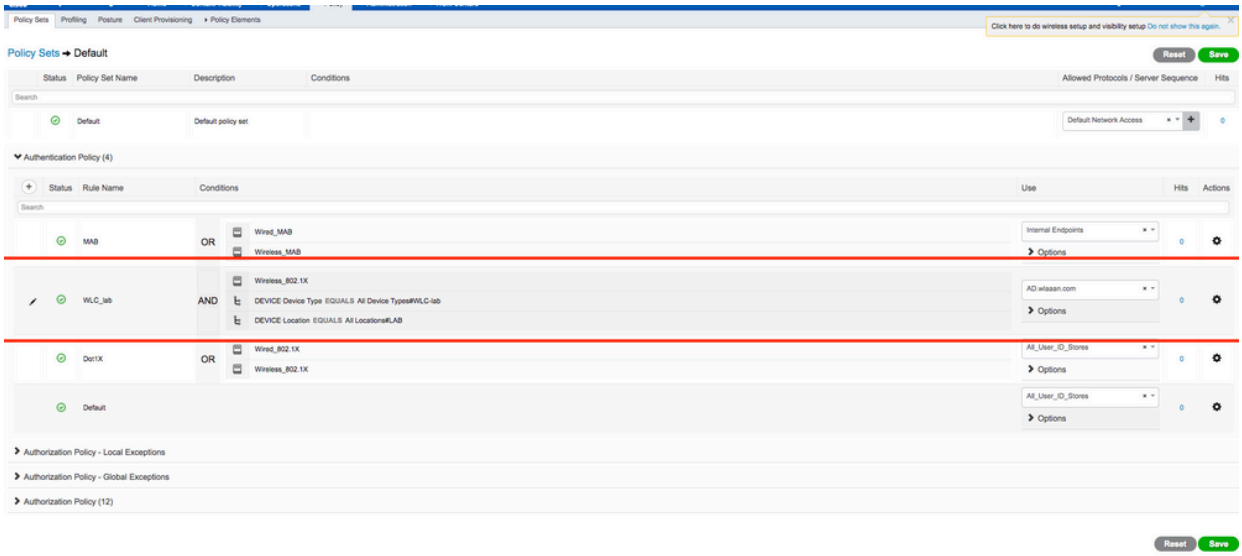


    - Complete la configuración del perfil de autorización con información de VLAN para el grupo respectivo; el ejemplo muestra las Marketing configuraciones de grupo.

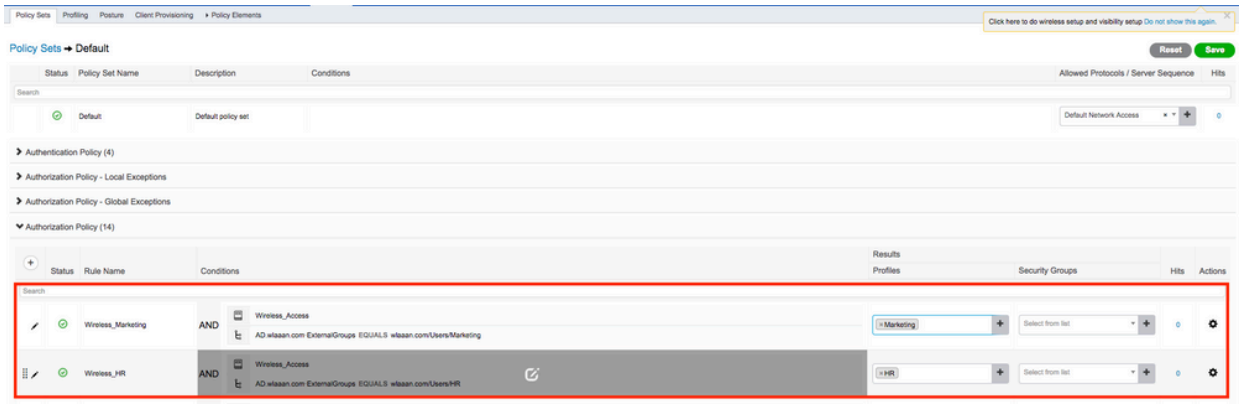


Se debe realizar una configuración similar para otros grupos y se deben configurar los atributos de etiqueta de VLAN respectivos.

- Una vez configurados los perfiles de autorización, puede definir directivas de autenticación para los usuarios inalámbricos. Esto se puede hacer configurando`Custom`o modificando el conjunto de`Default`directivas. En este ejemplo, se modifica el conjunto de directivas Predeterminado. Desplácese hasta`Policy > Policy Sets > Default`. De forma predeterminada para el`dot1x`tipo de autenticación, ISE va a utilizar`All_User_ID_Stores`, aunque funciona incluso con la configuración predeterminada actual, ya que AD forma parte de la lista de origen de identidad de`All_User_ID_Stores`, este ejemplo utiliza una regla más específica`WLC_lab`para ese controlador de LAB respectivo y utiliza AD como único origen para la autenticación.

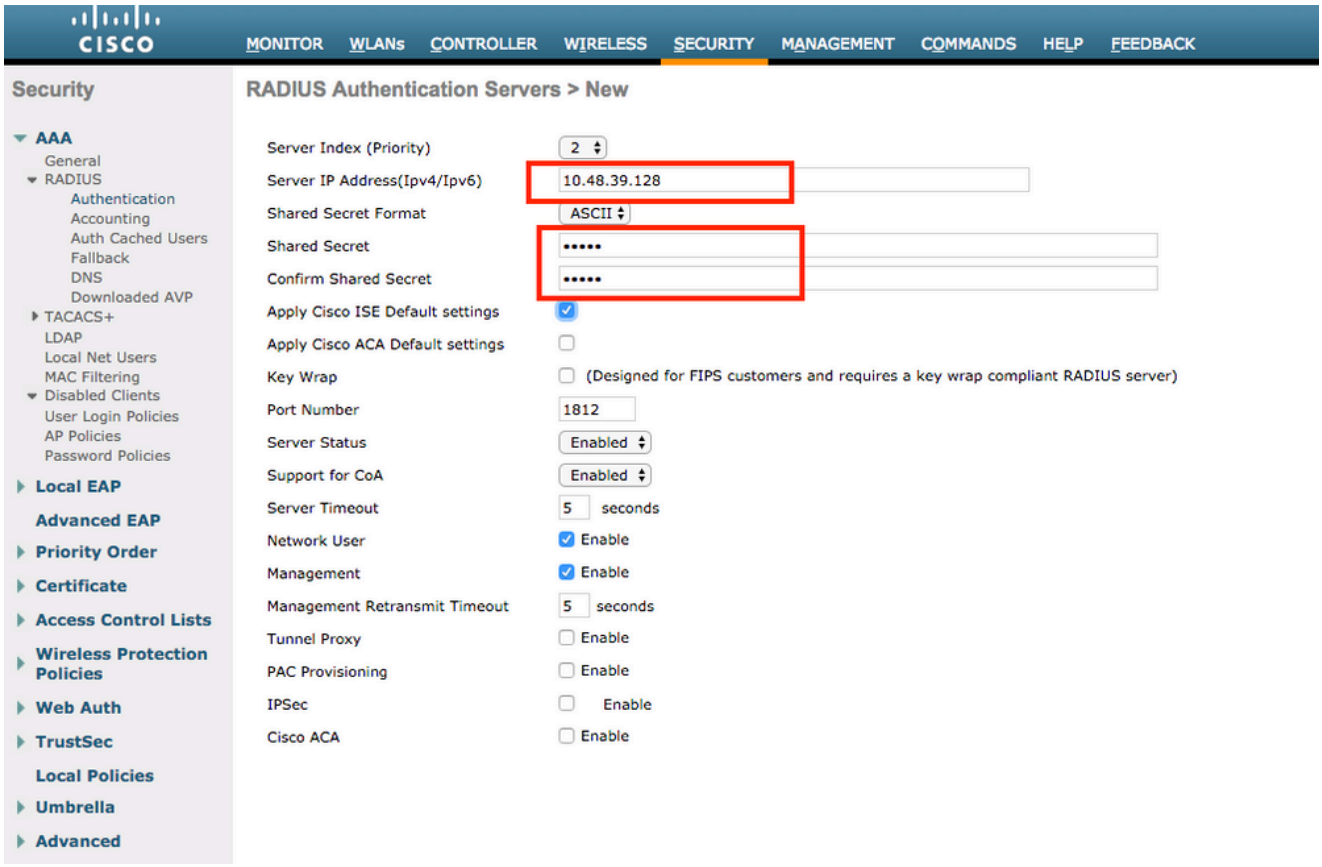


- Ahora debe crear directivas de autorización para los usuarios que asignen los perfiles de autorización respectivos en función de la pertenencia a grupos. Navegue hastaAuthorization policyla sección y cree políticas para cumplir ese requisito.

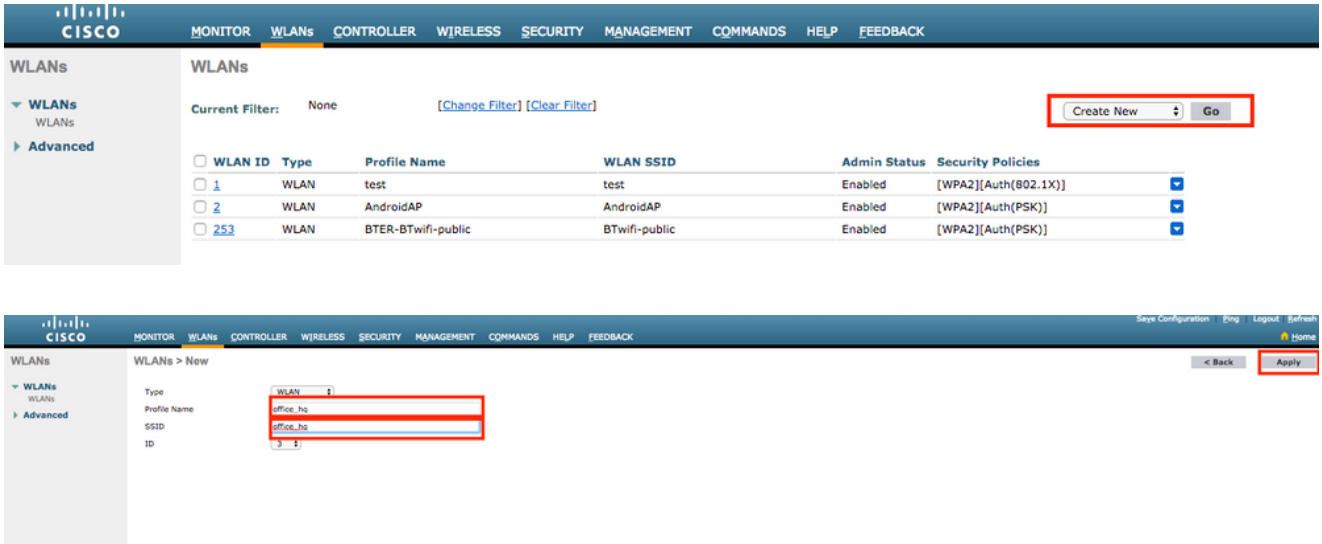


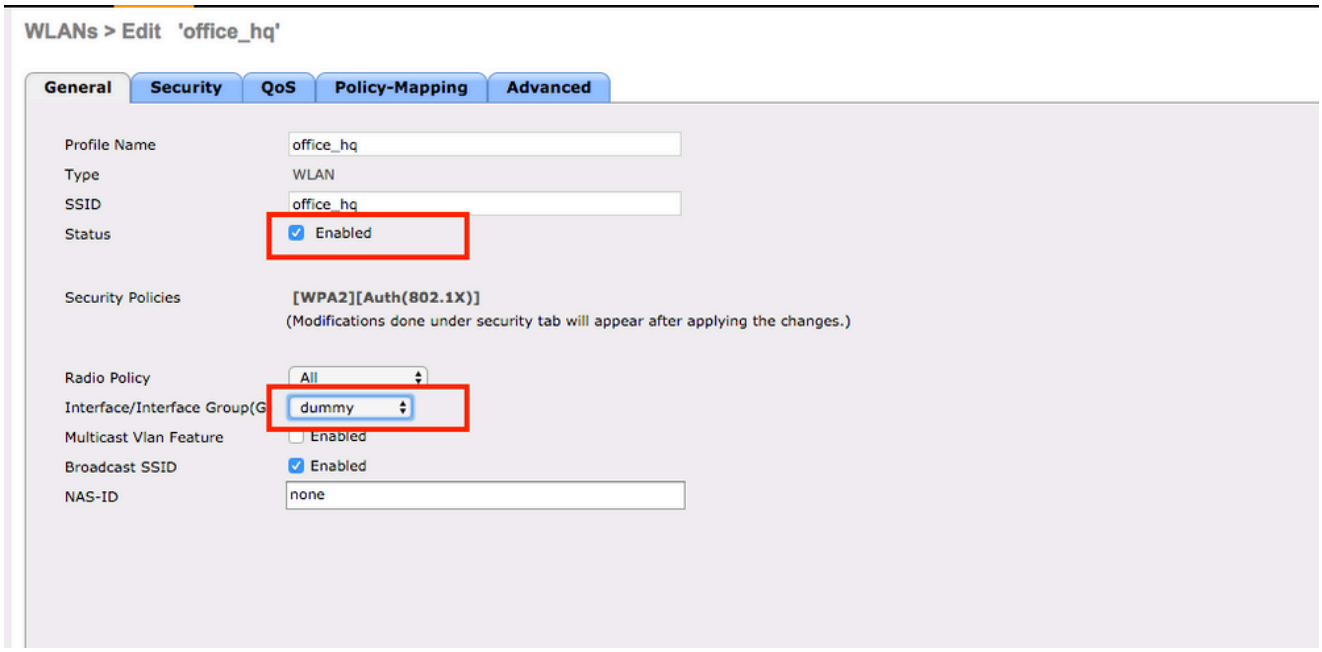
Configuración WLC para soportar la autenticación dot1x y la invalidación AAA para el SSID 'office_hq'

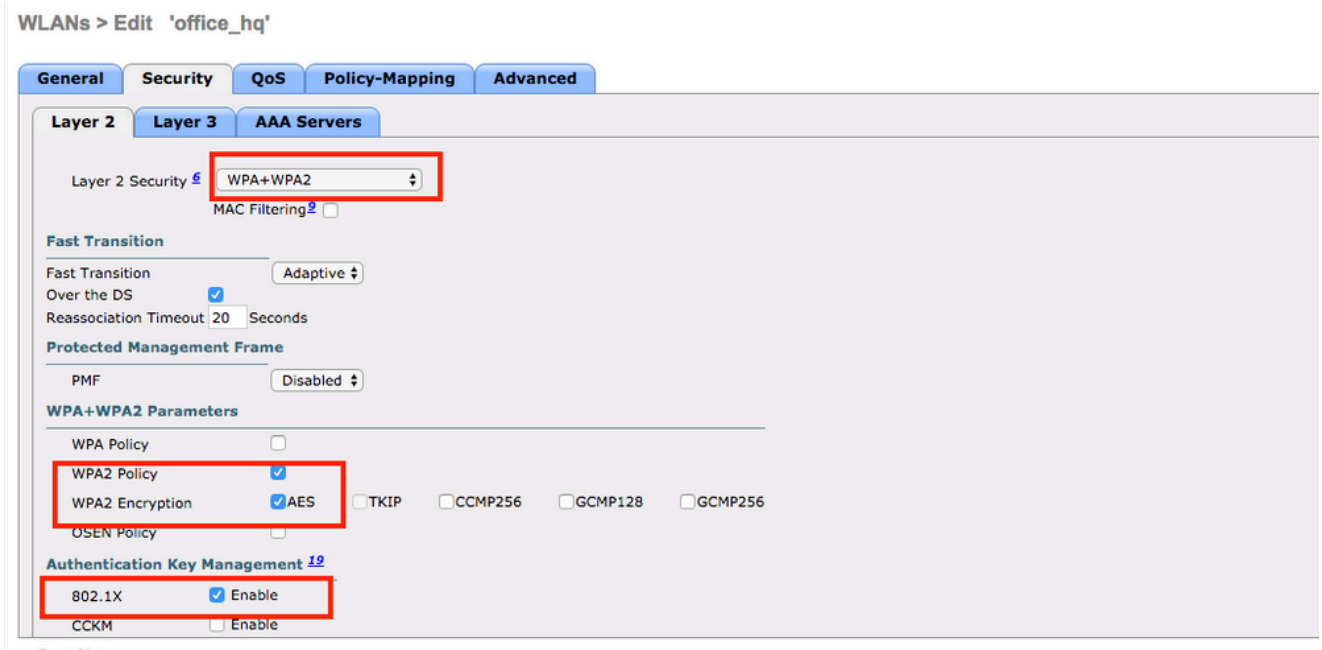
1. Configure ISE como servidor de autenticación RADIUS en WLC. Vaya a laSecurity > AAA > RADIUS > Authenticationsección de la interfaz de usuario web y proporcione la dirección IP de ISE y la información secreta compartida.

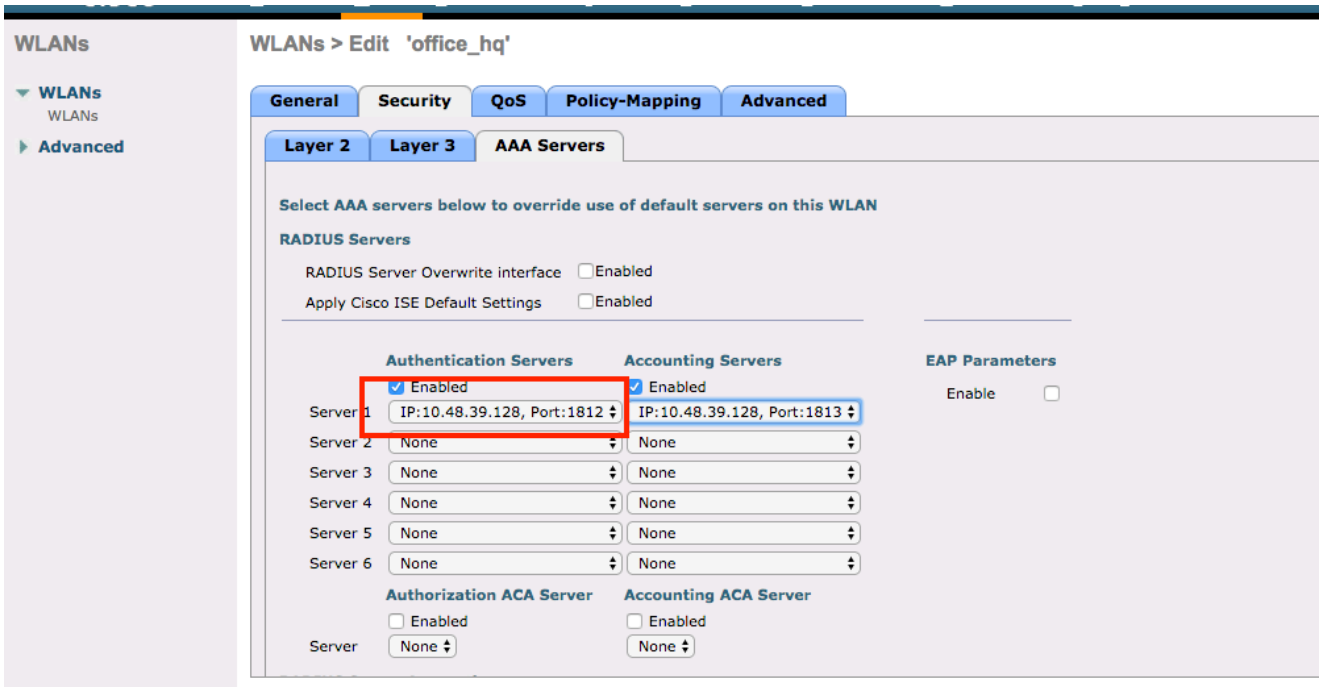


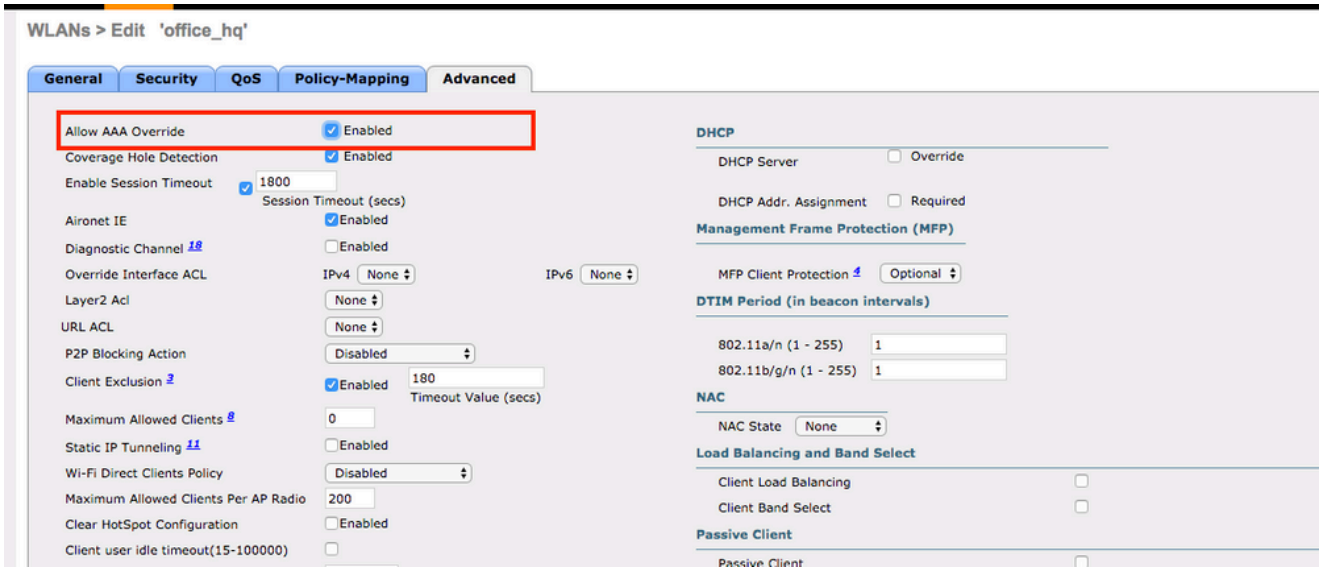
2. Configure el SSID`office_hq`bajo la sección`WLANs`en el WLC; este ejemplo configura el SSID con`WPA2/AES+dot1x`y la invalidación AAA. Se elige la interfaz`Dummy`para la WLAN ya que la VLAN adecuada se asigna a través de RADIUS de todos modos. Esta interfaz ficticia se debe crear en el WLC y se le debe dar una dirección IP, pero la dirección IP no tiene que ser válida y la VLAN en la que se coloca no se puede crear en el switch de link ascendente de modo que si no se está asignando ninguna VLAN, el cliente no puede ir a ninguna parte.



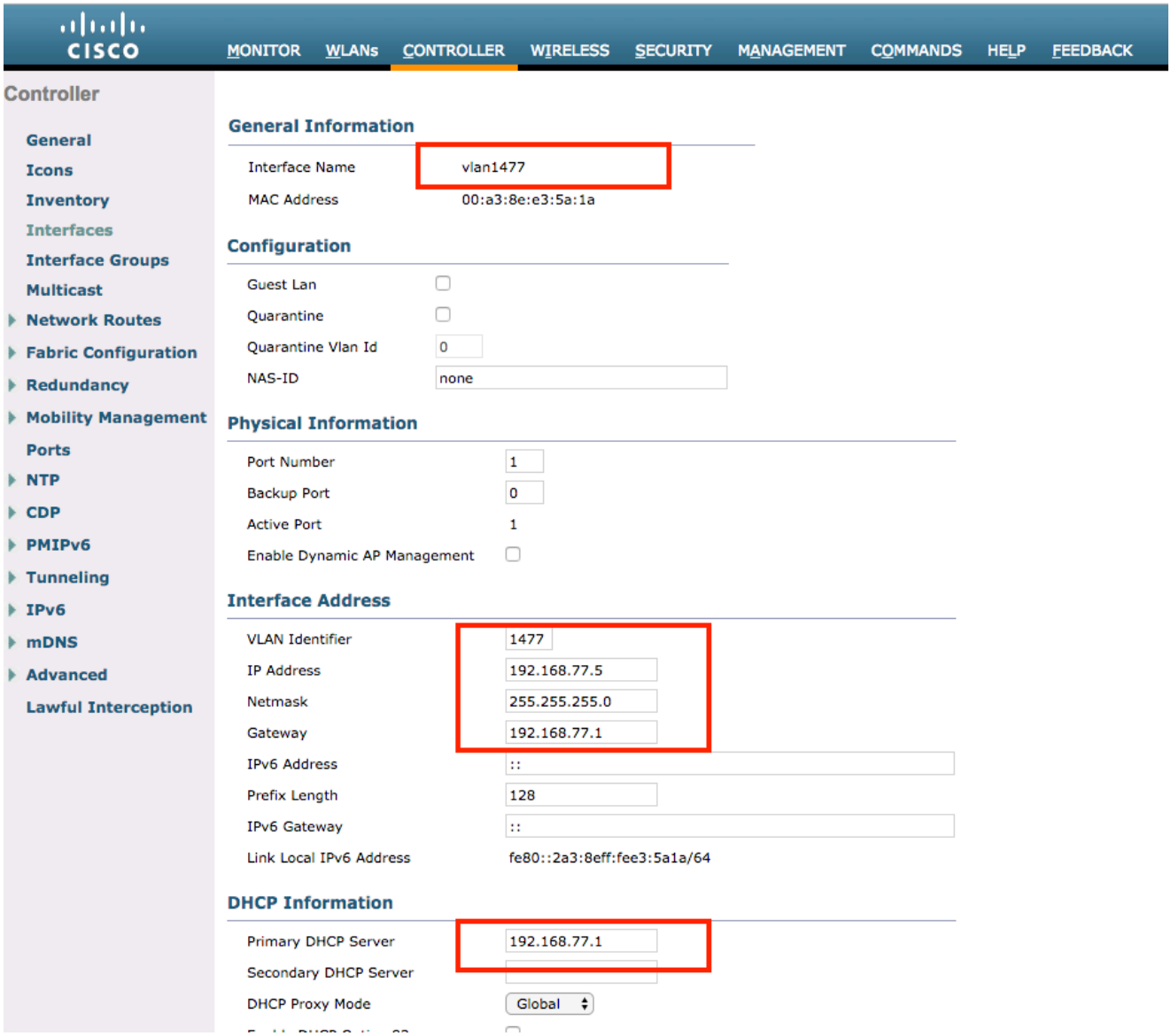

WLANs > Edit 'office_hq'
General
Security
QoS
Policy-Mapping
Advanced
Profile Name
office_hq
Type
WLAN
SSID
office_hq
Status
Enabled
Security Policies
[WPA2][Auth(802.1X)]
(Modifications done under security tab will appear after applying the changes.)
Radio Policy
All
Interface/Interface Group(G
dummy
Multicast Vlan Feature
Enabled
Broadcast SSID
Enabled
NAS-ID
none


WLANs > Edit 'office_hq'
General
Security
QoS
Policy-Mapping
Advanced
Layer 2
Layer 3
AAA Servers
Layer 2 Security
WPA+WPA2
MAC Filtering
Fast Transition
Fast Transition
Adaptive
Over the DS
Reassociation Timeout
20
Seconds
Protected Management Frame
PMF
Disabled
WPA+WPA2 Parameters
WPA Policy
WPA2 Policy
WPA2 Encryption
AES
TKIP
CCMP256
GCMP128
GCMP256
OSEN Policy
Authentication Key Management
802.1X
Enable
CCKM
Enable





3. También debe crear interfaces dinámicas en el WLC para las VLAN de usuario. Vaya al menú de la`Controller > Interfaces`interfaz de usuario. El WLC puede honrar solamente la asignación de VLAN recibida vía AAA si tiene una interfaz dinámica en esa VLAN.



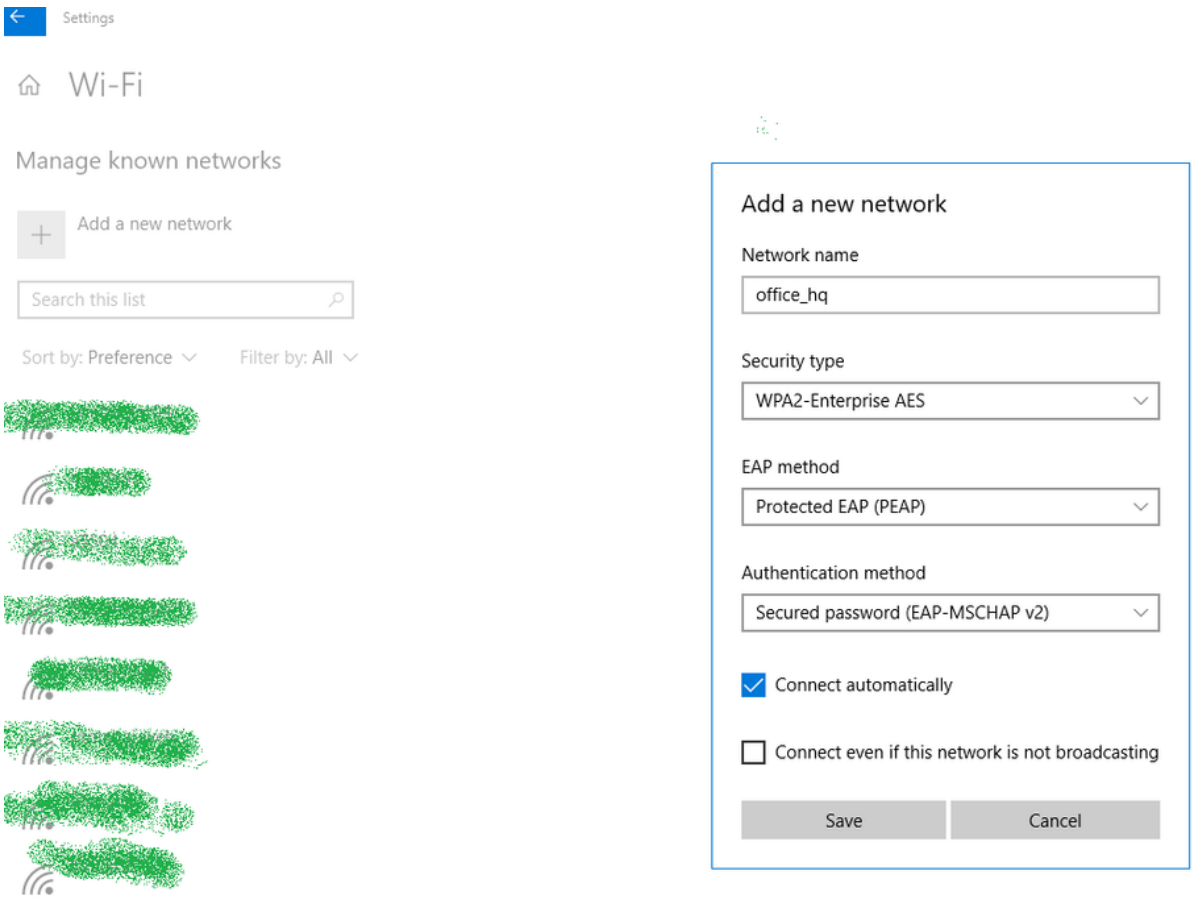
Verificación

Utilice el suplicante nativo de Windows 10 y el NAM de Anyconnect para probar las conexiones.

Dado que utiliza autenticación EAP-PEAP e ISE utiliza un certificado de firma automática (SSC), debe aceptar una advertencia de certificado o deshabilitar la validación de certificados. En un entorno corporativo, debe utilizar un certificado firmado y de confianza en ISE y asegurarse de que los dispositivos del usuario final tienen el certificado raíz adecuado instalado en la lista de CA de confianza.

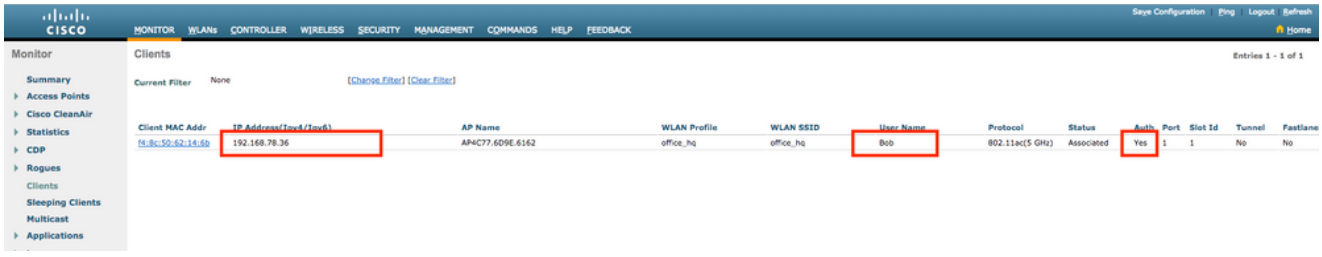
Probar conexión con Windows 10 y suplicante nativo:

1. AbraNetwork & Internet settings > Wi-Fi > Manage known networksy cree un nuevo perfil de red pulsando elAdd new networkbotón; rellene la información necesaria.



2. Compruebe el registro de autenticación en ISE y asegúrese de que se ha seleccionado el perfil adecuado para el usuario.

3. Verifique la entrada del cliente en el WLC y asegúrese de que esté asignado a la VLAN correcta y que esté en el estado RUN.



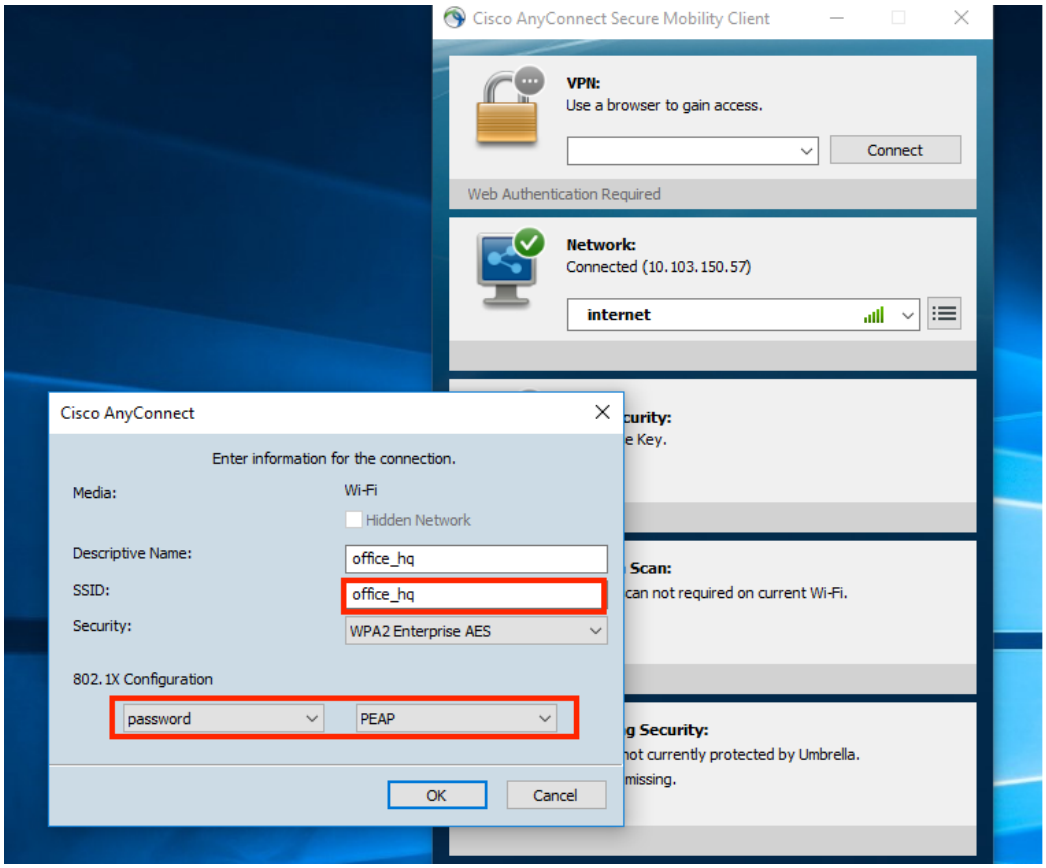
4. Desde la WLC CLI, el estado del cliente se puede verificar con elshow client dertails :

```
show client detail f4:8c:50:62:14:6b
Client MAC Address.............................. f4:8c:50:62:14:6b
Client Username ................................ Bob
```

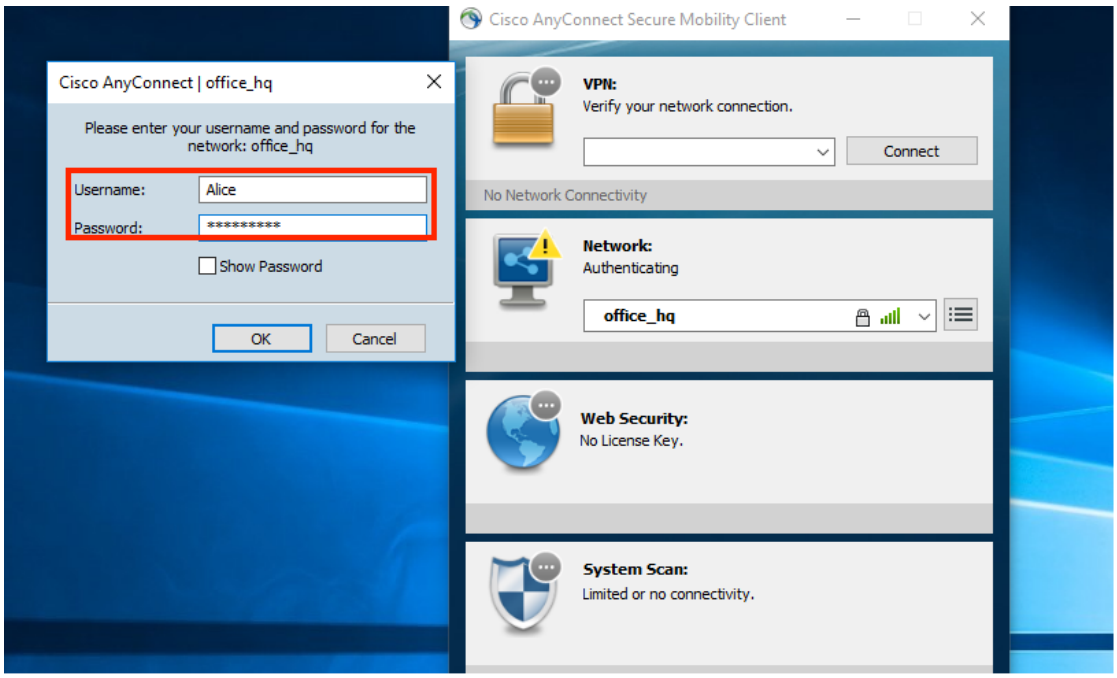
```
Client Webauth Username ..... N/A
Hostname: .....
Device Type: ..... Intel-Device
AP MAC Address..... 70:69:5a:51:4e:c0
AP Name..... AP4C77.6D9E.6162
AP radio slot Id..... 1
Client State..... Associated
User Authenticated by ..... RADIUS Server
Client User Group..... Bob
Client NAC OOB State..... Access
Wireless LAN Id..... 3
Wireless LAN Network Name (SSID)..... office_hq
Wireless LAN Profile Name..... office_hq
Hotspot (802.11u)..... Not Supported
Connected For ..... 242 secs
BSSID..... 70:69:5a:51:4e:cd
Channel..... 36
IP Address..... 192.168.78.36
Gateway Address..... 192.168.78.1
Netmask..... 255.255.255.0
...
Policy Manager State..... RUN
...
EAP Type..... PEAP
Interface..... vlan1478
VLAN..... 1478
Quarantine VLAN..... 0
Access VLAN..... 1478
```

Pruebe la conexión con Windows 10 y Anyconnect NAM:

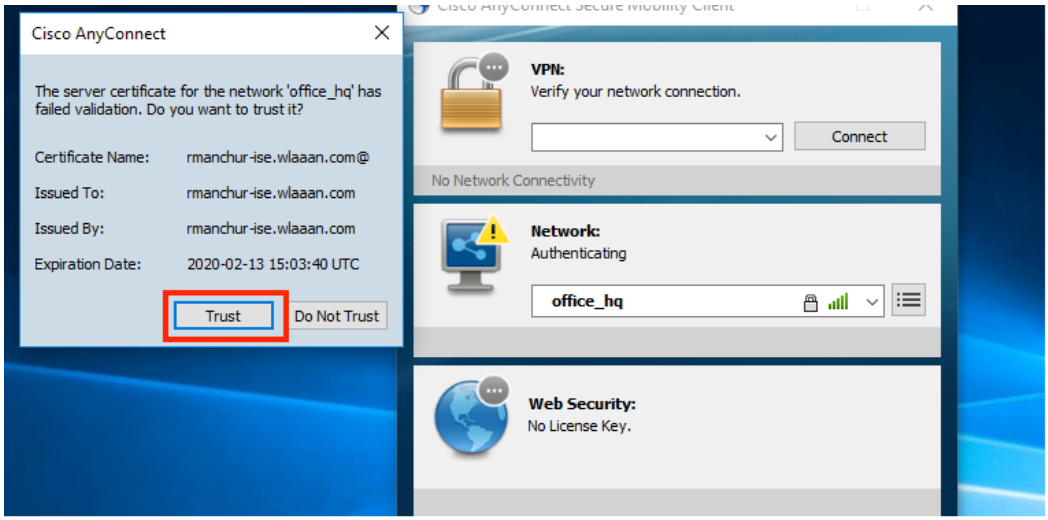
1. Elija el SSID de la lista de SSID disponibles y el tipo de autenticación EAP respectivo (en este ejemplo PEAP) y el formulario de autenticación interno.



2. Proporcione el nombre de usuario y la contraseña para la autenticación de usuarios.

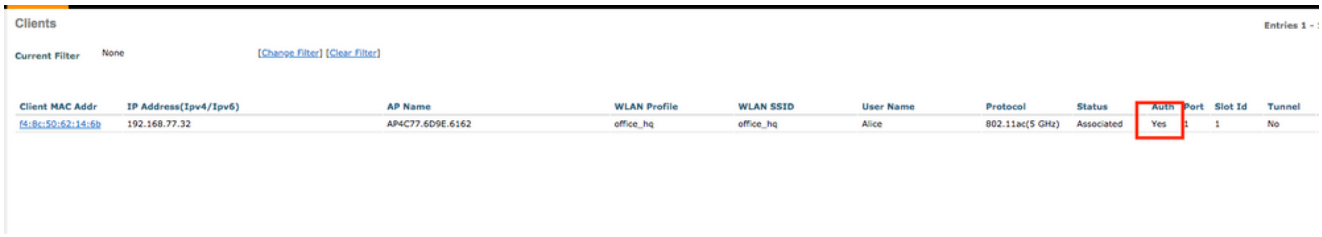


3. Dado que ISE envía un SSC al cliente, debe elegir manualmente confiar en el certificado (en el entorno de producción se recomienda instalar el certificado de confianza en ISE).



4. Compruebe los registros de autenticación en ISE y asegúrese de que se ha seleccionado el perfil de autorización correcto para el usuario.

5. Verifique la entrada del cliente en el WLC y asegúrese de que esté asignado a la VLAN correcta y que esté en el estado RUN.



6. Desde la WLC CLI, el estado del cliente se puede verificar con el`show client dertails` :

```
Client MAC Address.............................. f4:8c:50:62:14:6b
Client Username ................................ Alice
Client Webauth Username ........................ N/A
Hostname: ......................................
Device Type: ................................... Intel-Device
AP MAC Address.................................. 70:69:5a:51:4e:c0
AP Name......................................... AP4C77.6D9E.6162
AP radio slot Id................................ 1
```

```
Client State..................................... Associated
User Authenticated by ........................... RADIUS Server
Client User Group................................ Alice
Client NAC OOB State............................. Access
Wireless LAN Id.................................. 3
Wireless LAN Network Name (SSID)................. office_hq
Wireless LAN Profile Name........................ office_hq
Hotspot (802.11u)................................ Not Supported
Connected For ................................... 765 secs
BSSID............................................ 70:69:5a:51:4e:cd
Channel.......................................... 36
IP Address....................................... 192.168.77.32
Gateway Address.................................. 192.168.77.1
Netmask.......................................... 255.255.255.0
...
Policy Manager State............................. RUN
...
Policy Type...................................... WPA2
Authentication Key Management.................... 802.1x
Encryption Cipher................................ CCMP-128 (AES)
Protected Management Frame ...................... No
Management Frame Protection...................... No
EAP Type......................................... PEAP
Interface........................................ vlan1477
VLAN............................................. 1477
```

Troubleshoot

1. Utilice`test aaa radius username`

   `password`

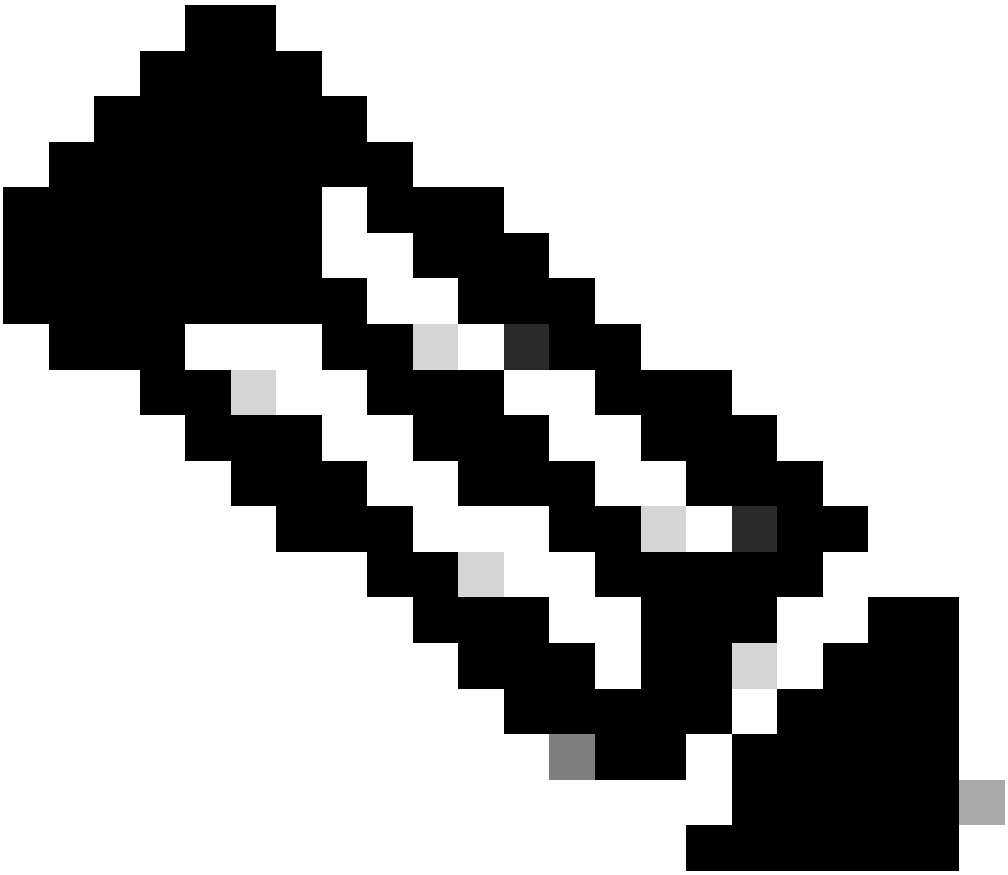
   `wlan-id`

   para probar la conexión RADIUS entre WLC e ISE y el`test aaa show radius`para mostrar los resultados.

```
test aaa radius username Alice password <removed> wlan-id 2

Radius Test Request
  Wlan-id.......................................... 2
  ApGroup Name..................................... none

  Attributes                    Values
  ----------                    ------
  User-Name                     Alice
  Called-Station-Id             00-00-00-00-00-00:AndroidAP
  Calling-Station-Id            00-11-22-33-44-55
  Nas-Port                      0x00000001 (1)
```

```
  Nas-Ip-Address                  10.48.71.20
  NAS-Identifier                  0x6e6f (28271)
  Airespace / WLAN-Identifier     0x00000002 (2)
  User-Password                   cisco!123
  Service-Type                    0x00000008 (8)
  Framed-MTU                      0x00000514 (1300)
  Nas-Port-Type                   0x00000013 (19)
  Cisco / Audit-Session-Id        1447300a0000003041d5665c
  Acct-Session-Id                 5c66d541/00:11:22:33:44:55/743


test radius auth request successfully sent. Execute 'test aaa show radius' for response

(Cisco Controller) >test aaa show radius

Radius Test Request
  Wlan-id..................................... 2
  ApGroup Name................................ none
Radius Test Response

Radius Server            Retry Status
-------------            ----- ------
10.48.39.128             1     Success

Authentication Response:
  Result Code: Success

  Attributes                      Values
  ----------                      ------
  User-Name                       Alice
  State                           ReauthSession:1447300a0000003041d5665c
  Class                           CACS:1447300a0000003041d5665c:rmanchur-ise/339603379/59
  Tunnel-Type                     0x0000000d (13)
  Tunnel-Medium-Type              0x00000006 (6)
  Tunnel-Group-Id                 0x000005c5 (1477)


(Cisco Controller) >
```

2. Utilice el debug client para resolver problemas de conectividad del cliente inalámbrico.
3. Utilicedebug aaa all enablepara resolver problemas de autenticación y autorización en el WLC.



Nota: Utilice este comando solamente con el`debug mac addr`para limitar la salida basada en la dirección MAC para la cual se realiza la depuración.

4. Consulte los registros en vivo y los registros de sesión de ISE para identificar problemas, fallas de autenticación y problemas de comunicación AD.

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).