Ejemplo de Configuración de Autenticación Web Central en WLCs de Acceso Convergente y Acceso Unificado

Contenido

Introducción

Este documento describe cómo configurar la autenticación web central en el controlador de LAN inalámbrica de acceso convergente (WLC) y también entre el WLC de acceso convergente y el WLC de acceso unificado (5760 y también entre 5760 y 5508).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimientos básicos de Cisco WLC 5508, 5760, 3850
- Conocimientos básicos de Identity Services Engine (ISE)
- Conocimientos básicos de Movilidad inalámbrica
- Conocimientos básicos sobre el anclaje de invitados

Componentes Utilizados

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

- WLC 5760 que ejecuta Cisco IOS® XE Release 3.3.3
- WLC 5508 que ejecuta Cisco Aironet OS Release 7.6
- Switch 3850 que ejecuta Cisco IOS XE Release 3.3.3
- Cisco ISE que ejecuta la versión 1.2

Configurar

> **Nota: Use el Command Lookup Tool (únicamente clientes registrados) para obtener más información sobre los comandos que se utilizan en esta sección.**

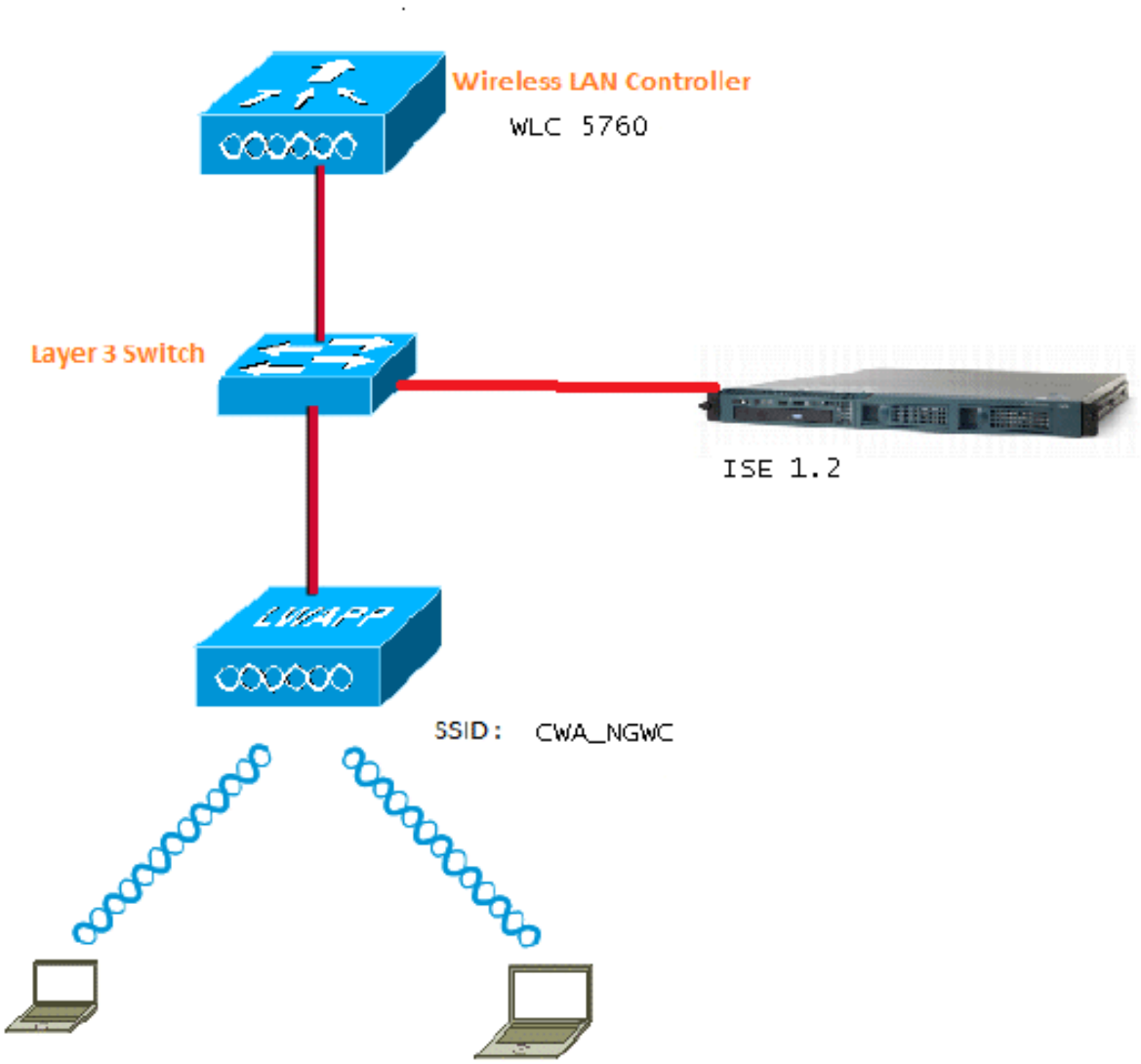
El flujo incluye estos pasos:

1. El usuario se asocia al identificador del conjunto de servicios (SSID) de autenticación web, que en realidad es open+macfilters y no ofrece seguridad de capa 3.
2. El usuario abre el explorador.
3. El WLC redirige al portal de invitados.
4. El usuario se autentica en el portal.
5. ISE envía un cambio de autorización RADIUS (CoA: puerto UDP 1700) para indicar al controlador que el usuario es válido y, finalmente, envía atributos RADIUS como la lista de control de acceso (ACL).
6. Se le solicita al usuario que vuelva a intentar la dirección URL original.

Cisco utiliza tres configuraciones de implementación diferentes que cubren todos los escenarios diferentes para lograr la autenticación web central (CWA).

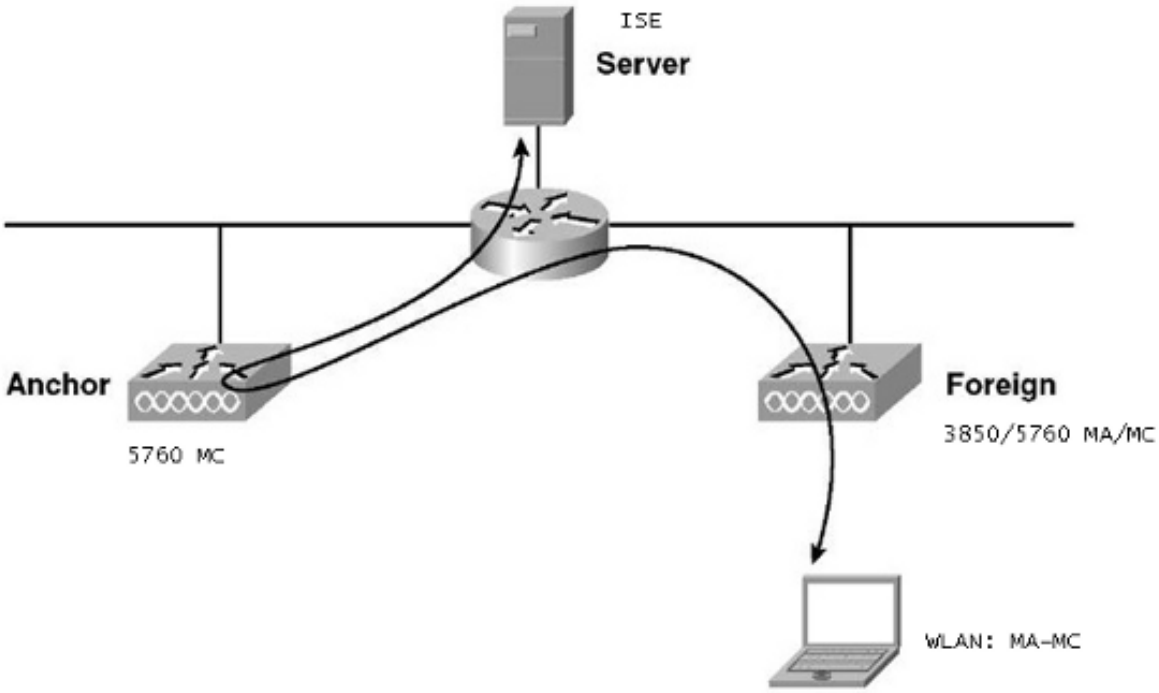
Topología 1

El WLC 5760 actúa como un WLC autónomo y los puntos de acceso terminan en el mismo WLC 5760. Los clientes se conectan a LAN inalámbrica (WLAN) y se autentican en ISE.



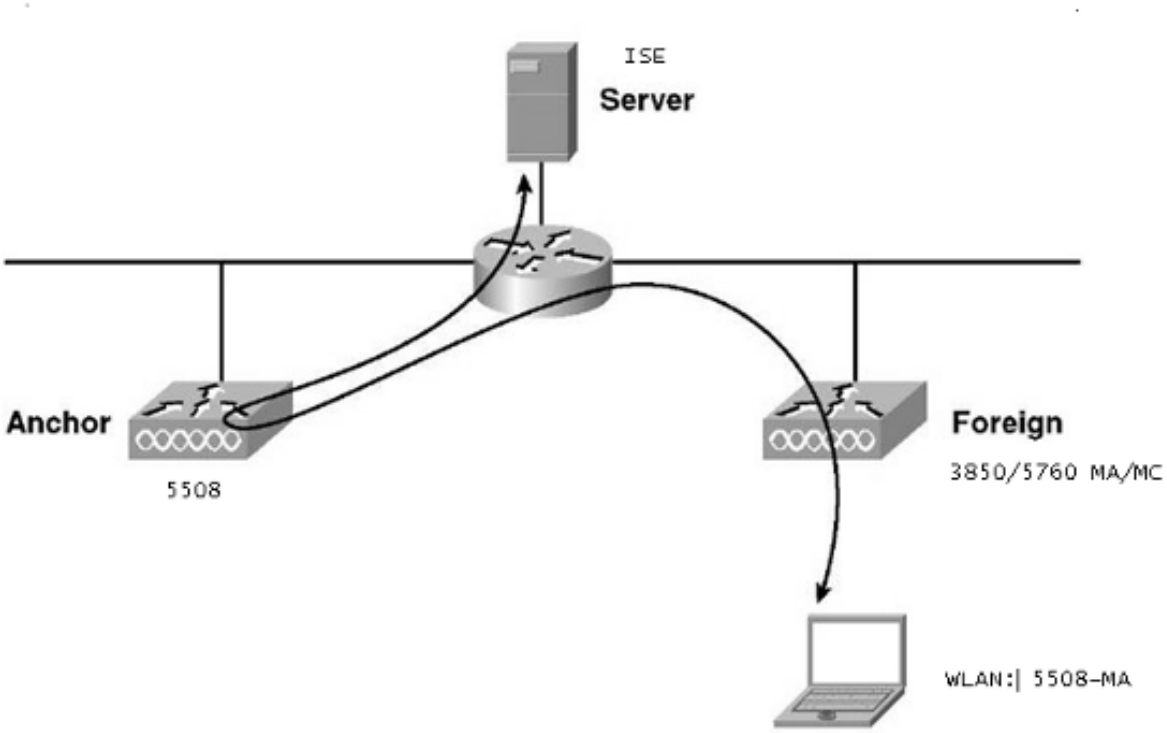
Topología 2

Anclaje de invitado entre el WLC de acceso convergente con uno que actúa como controlador de movilidad y el otro que actúa como agente de movilidad. El agente de movilidad es el WLC externo y el controlador de movilidad es el delimitador.



Topología 3

Anclaje de invitado entre el Cisco Unified WLC 5508 y el WLC 5760/3850 de acceso convergente con uno que actúa como controlador de movilidad y el otro que actúa como agente de movilidad. El agente de movilidad/controlador de movilidad es el WLC externo y el controlador de movilidad 5508 es el delimitador.



Nota: Hay muchas implementaciones en las que el delimitador es el controlador de movilidad y el WLC externo es el agente de movilidad que obtiene la licencia de otro controlador de movilidad. En este caso, el WLC extranjero tiene solamente un ancla y ese ancla es el que empuja las políticas. El anclaje doble no se admite y no funciona, ya que no se espera que funcione de esa manera.

Ejemplo:

El WLC 5508 actúa como el anclaje y el WLC 5760 actúa como el controlador de movilidad para un switch 3850 que actúa como un agente de movilidad. Para la WLAN externa de anclaje, el WLC 5508 será el anclaje para la WLAN externa 3850. No hay necesidad de configurar esa WLAN en el WLC 5760 en absoluto. Si apunta el switch 3850 al anclaje 5760, y luego de este WLC 5760 al WLC 5508 como un anclaje doble, no funcionará ya que esto se convierte en anclaje doble y las políticas están en el anclaje 5508.

Si usted tiene una configuración que incluye un WLC 5508 como el ancla, un WLC 5760 como el controlador de movilidad, y un switch 3850 como el agente de movilidad y el WLC extranjero, entonces en cualquier punto del tiempo el ancla para el switch 3850 será el WLC 5760 o el WLC 5508. No puede ser a la vez y el doble anclaje no funciona.

Ejemplo de Configuración de Topología 1

Consulte la Topología 1 para ver el diagrama y la explicación de la red.

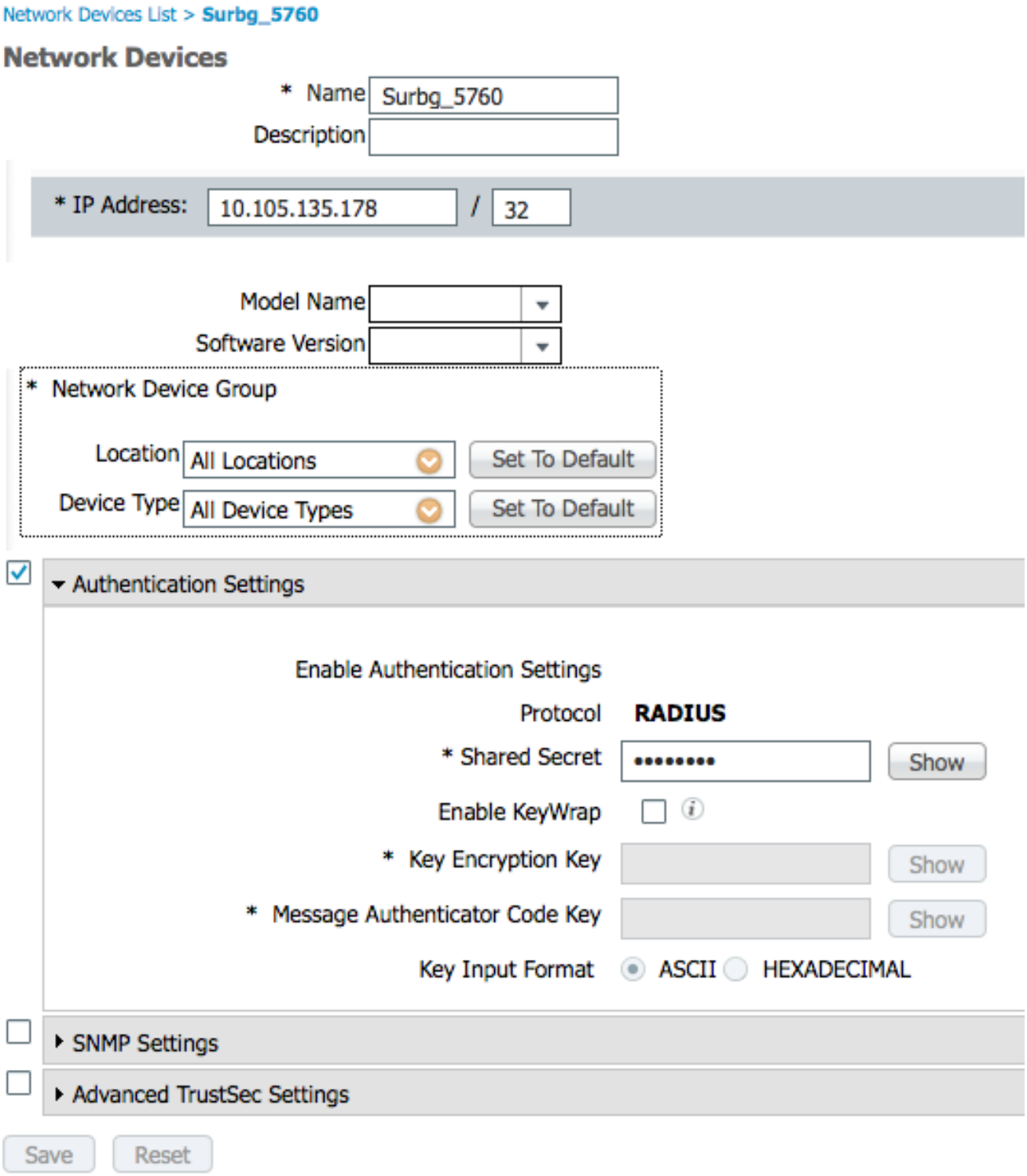
La configuración es un proceso de dos pasos:

1. Configuración en ISE.
2. Configuración en el WLC.

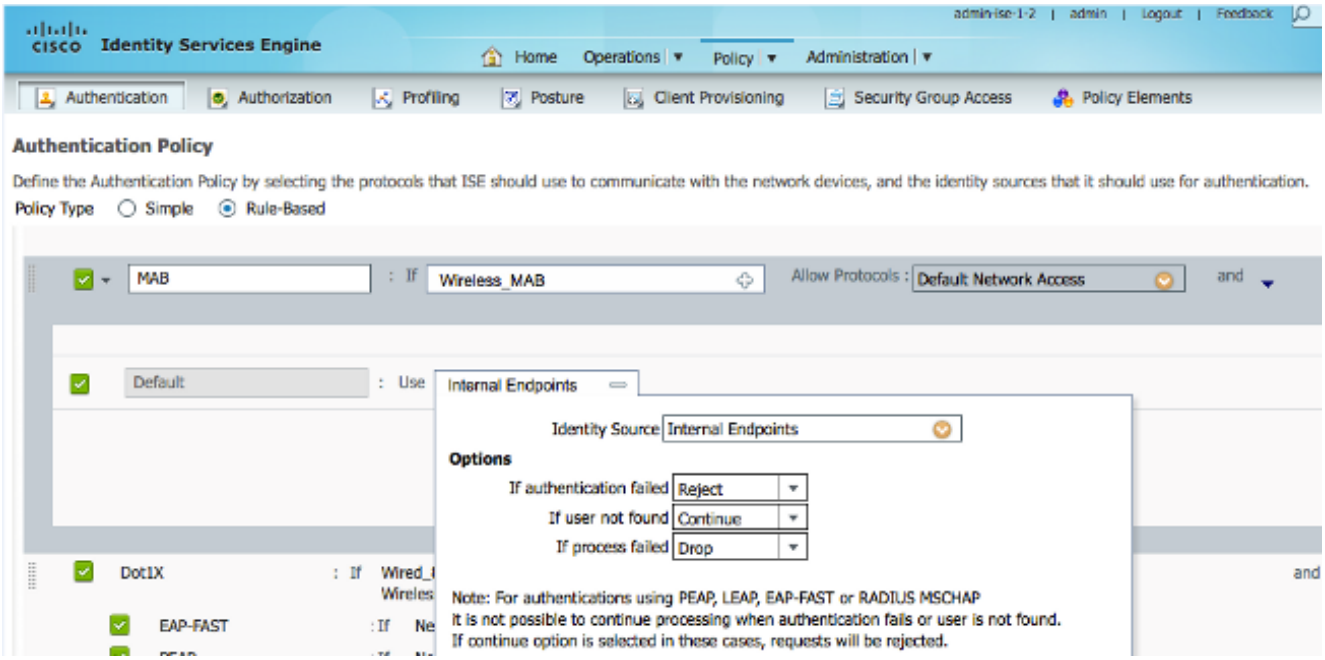
El WLC 5760 actúa como un WLC autónomo y los usuarios se autentican en el ISE.

Configuración en ISE

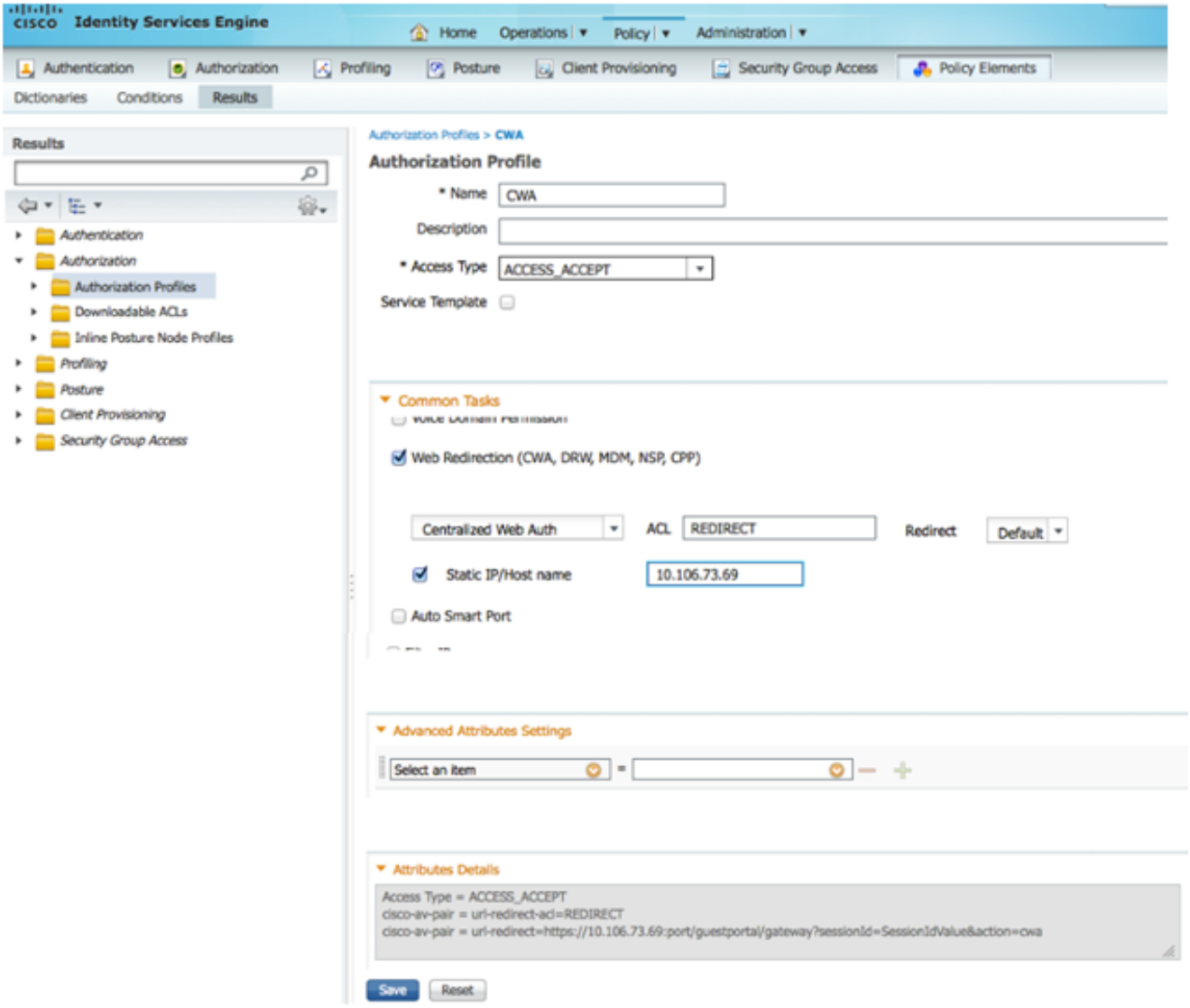
1. Elija **ISE GUI > Administration > Network Resource > Network Devices List > Add** para agregar el WLC en ISE como el cliente de Autenticación, Autorización y Contabilización (AAA). Asegúrese de ingresar el mismo secreto compartido en el WLC que se agrega en el servidor RADIUS. **Nota**: Mientras que usted despliega Anchor-Foreign, usted apenas necesita agregar el WLC extranjero. No es necesario agregar el WLC de anclaje en el ISE como cliente AAA. En este documento, se utiliza la misma configuración de ISE para todos los demás escenarios de implementación.



2. En la GUI de ISE, elija **Policy > Authentication > MAB > Edit** para crear la política de autenticación. La política de autenticación acepta la dirección MAC del cliente, que apunta a los puntos finales internos. Seleccione estas opciones en la lista Opciones:En la lista desplegable If authentication failed, elija **Reject**.En la lista desplegable Si no se encuentra el usuario, seleccione **Continuar**.En la lista desplegable Si el proceso ha fallado, elija **Abandonar**.Cuando configura con estas opciones, el cliente que falla la autorización MAC continúa con el portal de
invitados.

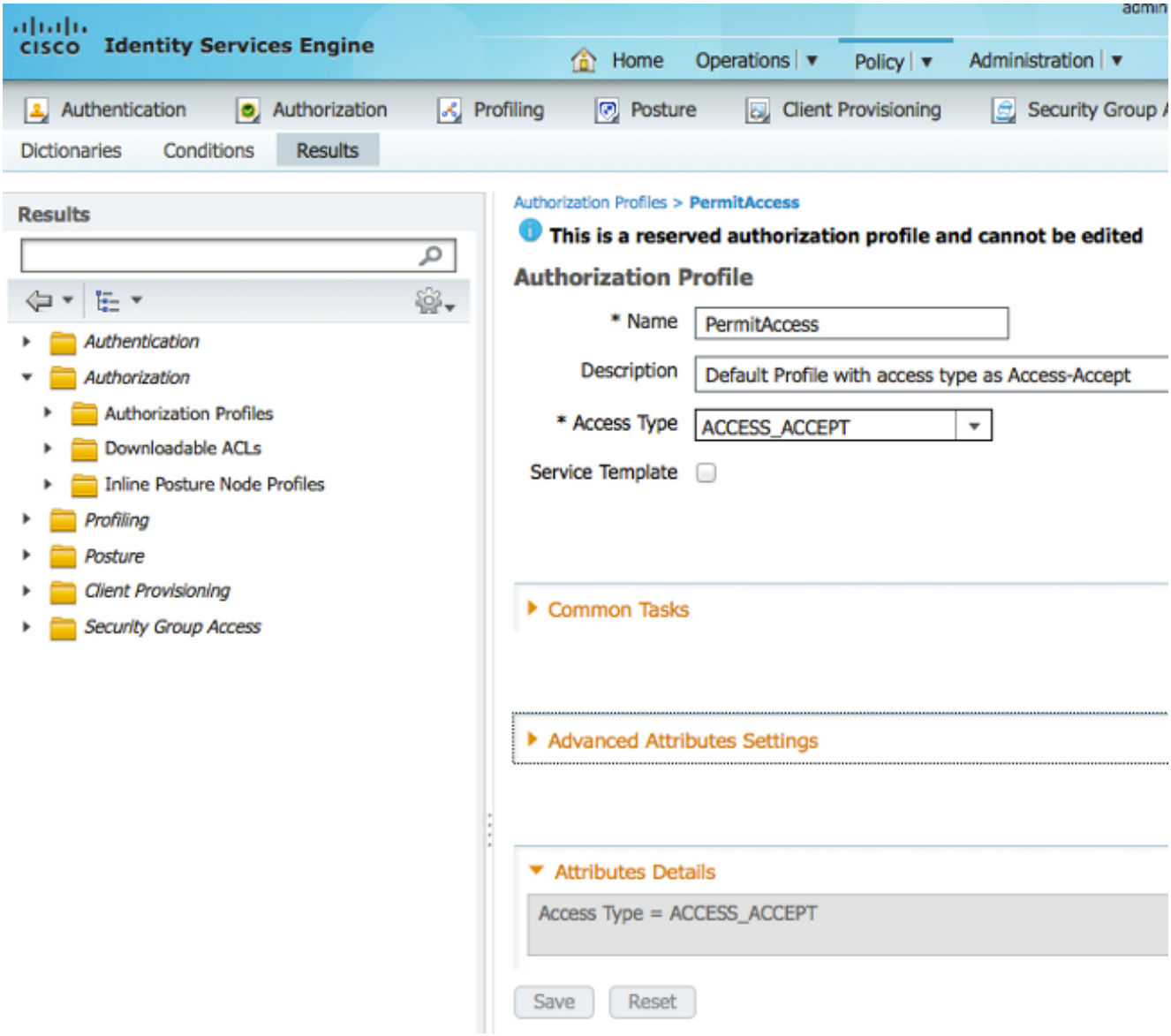


3. En la GUI de ISE, elija **Policy > Authorization > Results > Authorization Profiles > Add**. Complete los detalles y haga clic en **Guardar** para crear el perfil de autorización. Este perfil ayuda a los clientes a ser redirigidos a la URL de redireccionamiento después de la autenticación MAC, donde los clientes ingresan el nombre de usuario/contraseña de invitado.

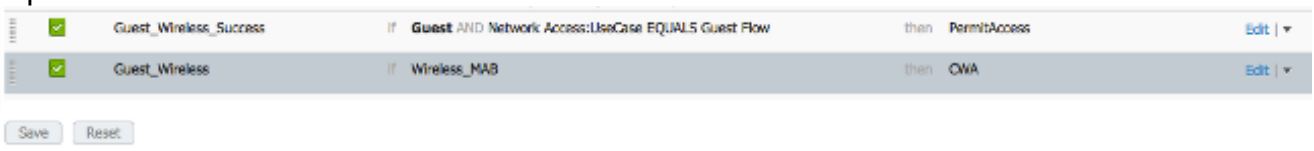


4. Desde la GUI de ISE, elija **Policy > Authorization > Results > Authorization Profiles > Add**

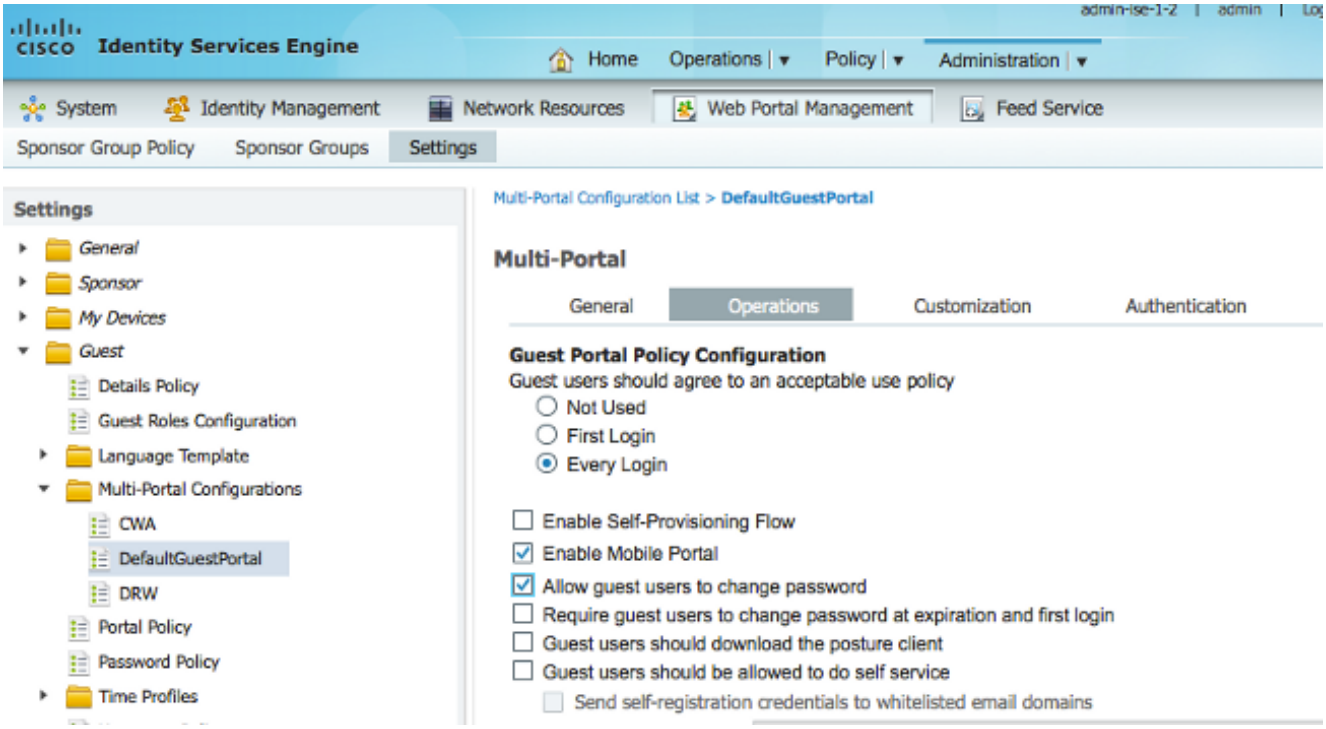
para crear otro perfil de autorización que permita el acceso a los usuarios con las credenciales correctas.



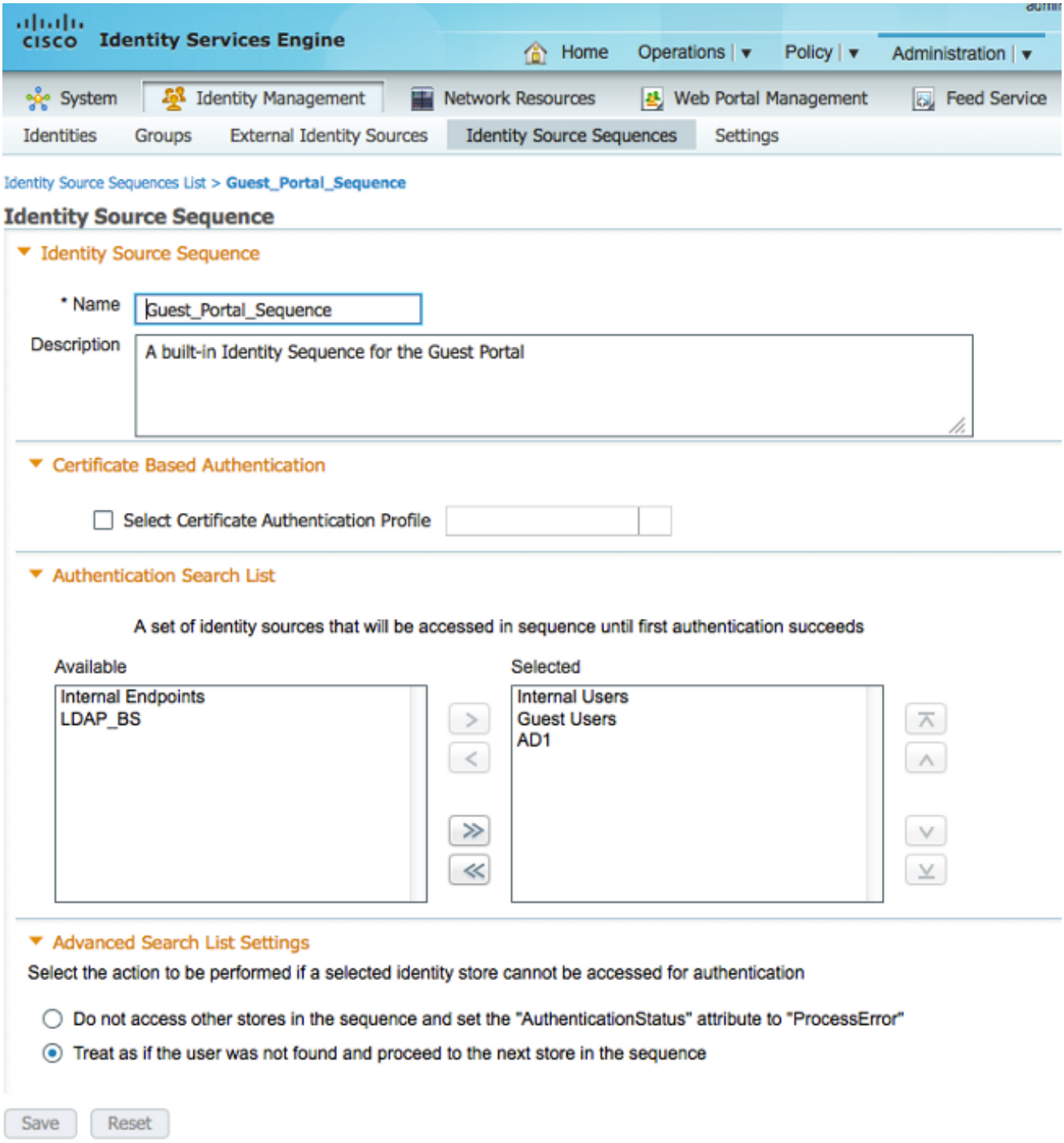
5. Cree las directivas de autorización. La política de autorización 'Guest_Wireless' envía la URL de redirección y la ACL de redirección a la sesión del cliente. El perfil que aparece aquí es el CWA, como se muestra anteriormente.La política de autorización 'Guest_Wireless-Scess' proporciona acceso completo a un usuario invitado que se ha autenticado correctamente a través del portal de invitados. Después de que el usuario se autentica con éxito en el portal de invitados, la autorización dinámica es enviada por el WLC. Esto reautentica la sesión del cliente con el atributo 'Network Access:Usecase EQUALS Guest Flow'.Las directivas de autorización finales tienen el siguiente aspecto:



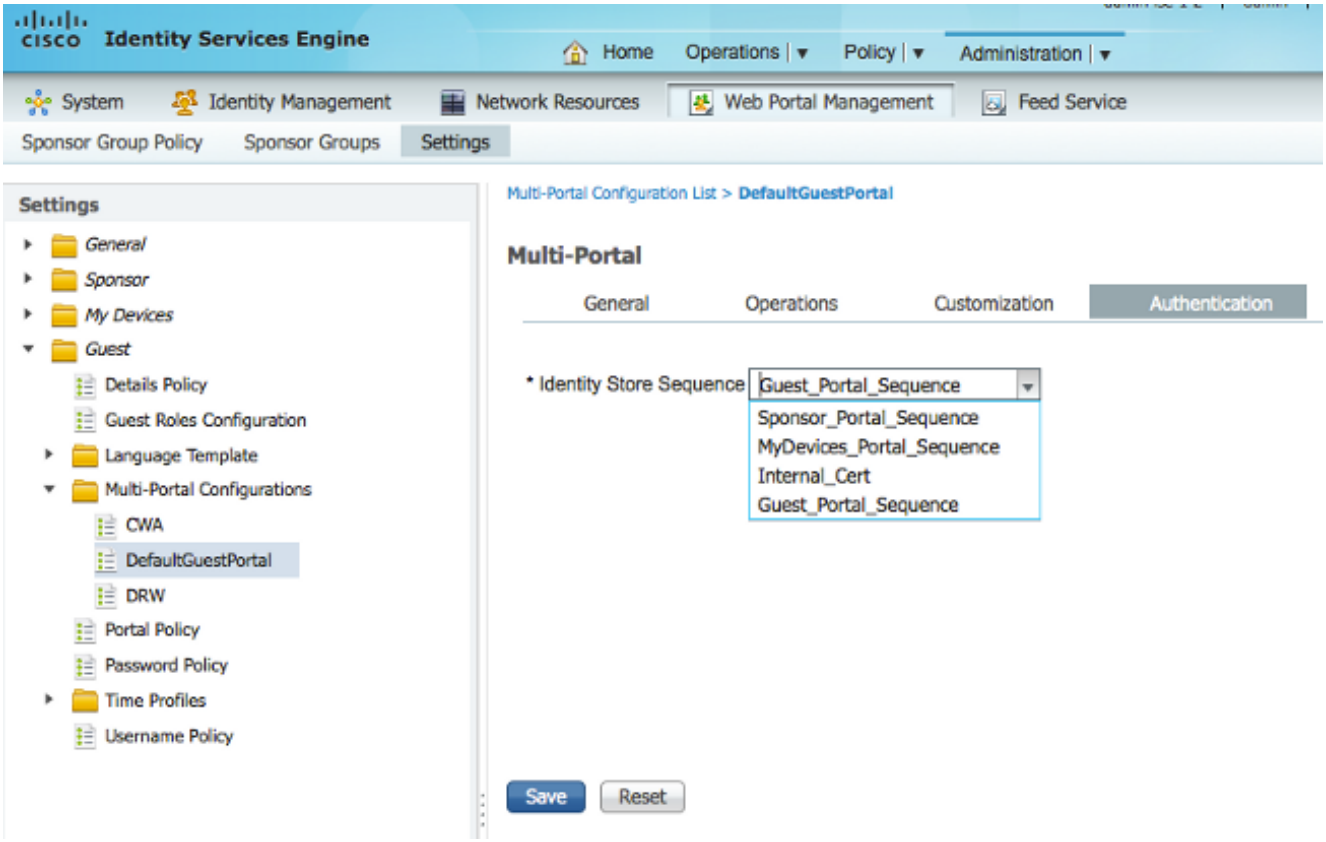
6. Opcional: en este caso, se utilizan las configuraciones predeterminadas de varios portales. En función de los requisitos, se puede cambiar en la GUI. En la GUI de ISE, elija **Administration > Web Portal management > Multi Portal Configurations > DefaultGuestPortal**.



Se crea Guest_Portal_sequence que permite a los usuarios Interno, Invitado y AD.



7. En la GUI de ISE, elija **Guest > Multi-Portal Configurations > DefaultGuestPortal**. En la lista desplegable Identificar secuencia de almacén, elija **Guest_Portal_Sequence**.



Configuración en el WLC

1. Defina el servidor ISE Radius en el WLC 5760.
2. Configure el servidor RADIUS, el grupo de servidores y la lista de métodos con la CLI.

```
dot1x system-auth-control

radius server ISE
address ipv4 10.106.73.69 auth-port 1645 acct-port 1646
 timeout 10
 retransmit 3
 key Cisco123


aaa group server radius ISE
server name ISE
deadtime 10

aaa authentication dot1x ISE group ISE
aaa authorization network ISE group ISE

aaa authorization network MACFILTER group ISE
aaa accounting identity ISE start-stop group ISE
!

aaa server radius dynamic-author
client 10.106.73.69 server-key Cisco123
auth-type any
```

3. Configure la WLAN con la CLI.

```
wlan CWA_NGWC 10 CWA_NGWC
 aaa-override
accounting-list ISE
client vlan VLAN0012
no exclusionlist
mac-filtering MACFILTER
nac
```

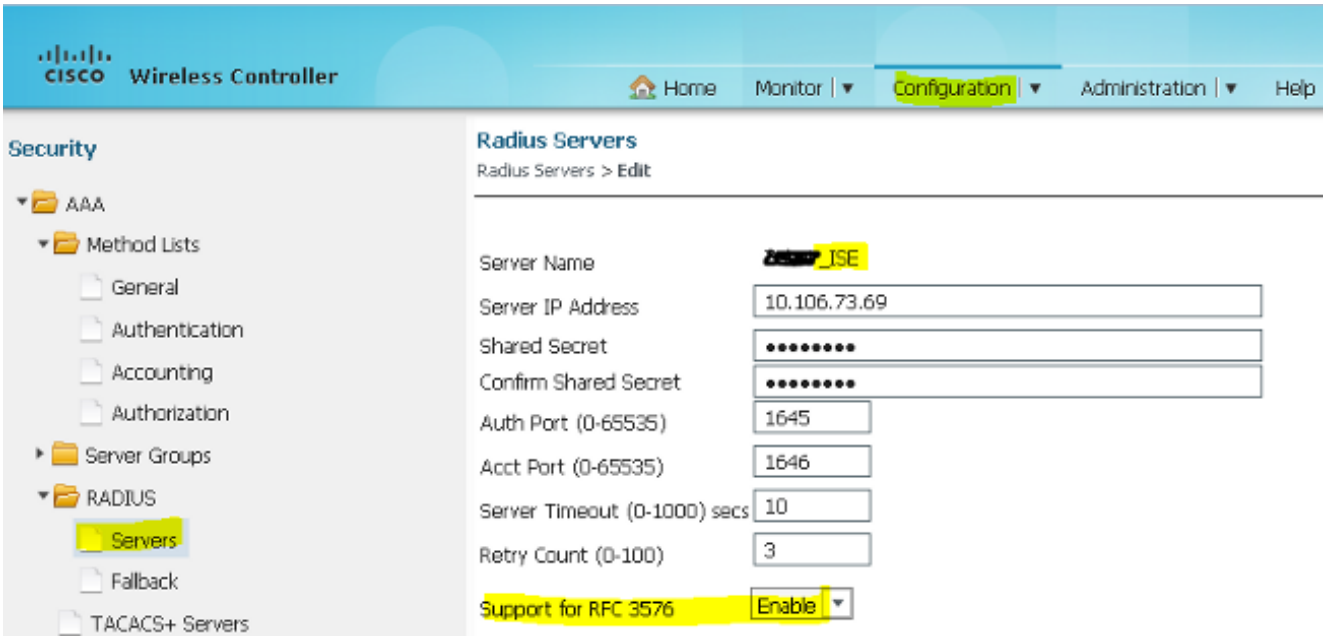
```
no security wpa
no security wpa akm dot1x
no security wpa wpa2
 no security wpa wpa2 ciphers aes
 security dot1x authentication-list ISE
 session-timeout 1800
 no shutdown
```

4. Configure las ACL de redirección con la CLI. Esta es la url-redirect-acl que ISE devuelve como anulación de AAA junto con la URL de redirección para la redirección del portal de invitados. Se trata de una ACL directa que se utiliza actualmente en la arquitectura unificada. Esta es una ACL 'punt' que es una especie de ACL inversa que normalmente utilizaría para la arquitectura Unified. Debe bloquear el acceso a DHCP, el servidor DHCP, DNS, el servidor DNS e ISE. Solo permita www, 443 y 8443 según sea necesario. Este portal de invitados de ISE utiliza el puerto 8443 y la redirección sigue funcionando con la ACL que se muestra aquí. Aquí ICMP está habilitado, pero en función de las reglas de seguridad puede denegar o permitir.

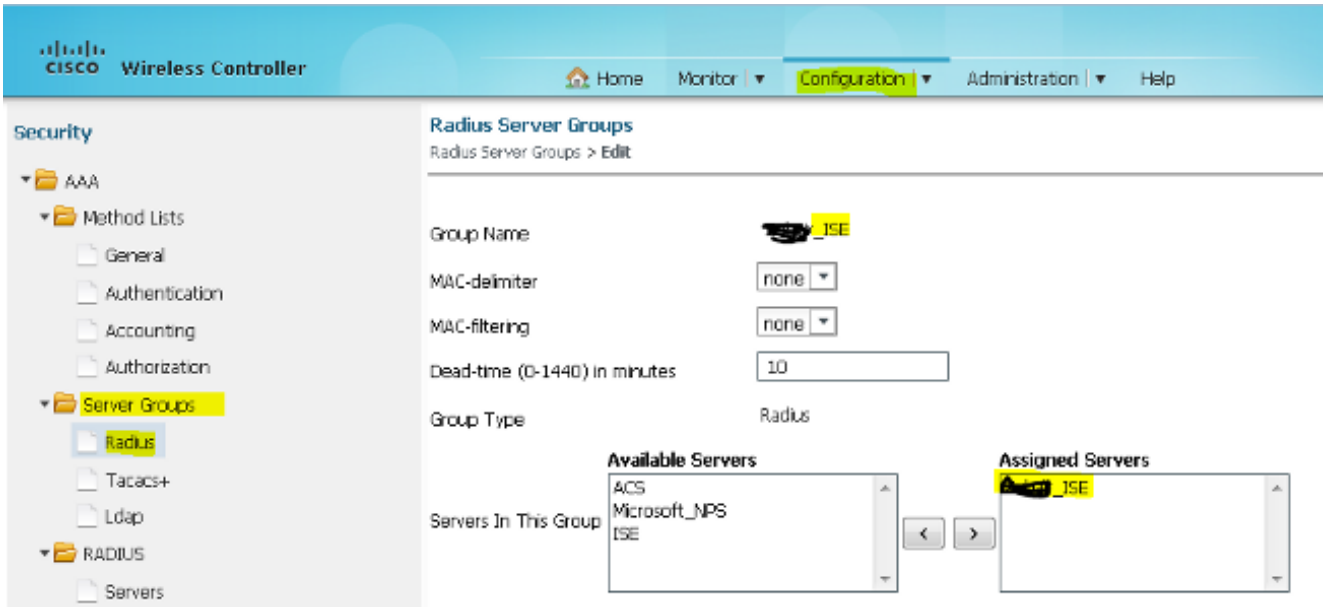
```
ip access-list extended REDIRECT
 deny icmp any any
 deny udp any any eq bootps
 deny udp any any eq bootpc
 deny udp any any eq domain
deny ip any host 10.106.73.69
 permit tcp any any eq www
 permit tcp any any eq 443
```

Precaución: Cuando habilita HTTPS, puede causar algunos problemas de CPU altos debido a la escalabilidad. No lo habilite a menos que lo recomiende el equipo de diseño de Cisco.

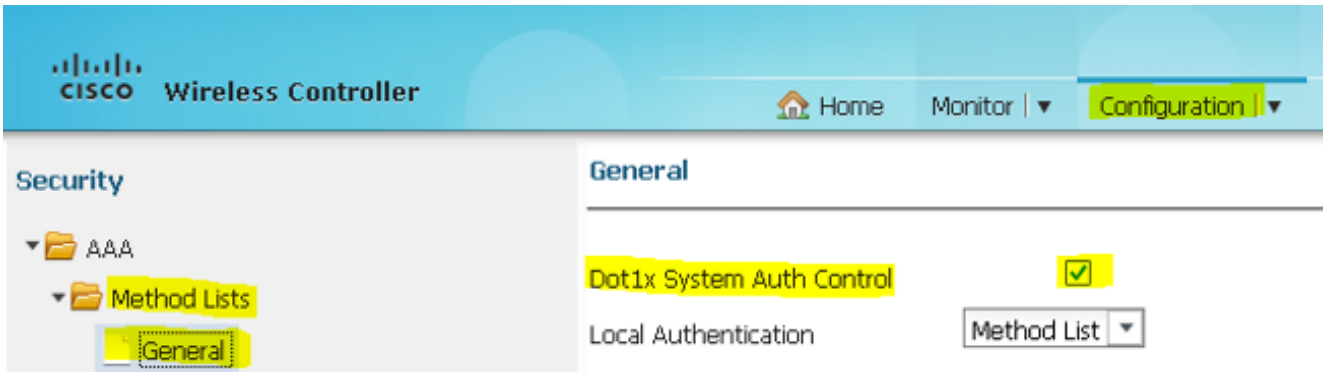
5. En la GUI del controlador inalámbrico, elija **AAA > RADIUS > Servers**. Configure el servidor RADIUS, el grupo de servidores y la Lista de métodos en la GUI. Complete todos los parámetros y asegúrese de que la clave secreta compartida configurada aquí coincida con la configurada en el ISE para este dispositivo. En la lista desplegable Support for RFC 3576 (Compatibilidad con RFC 3576), seleccione **Enable**.



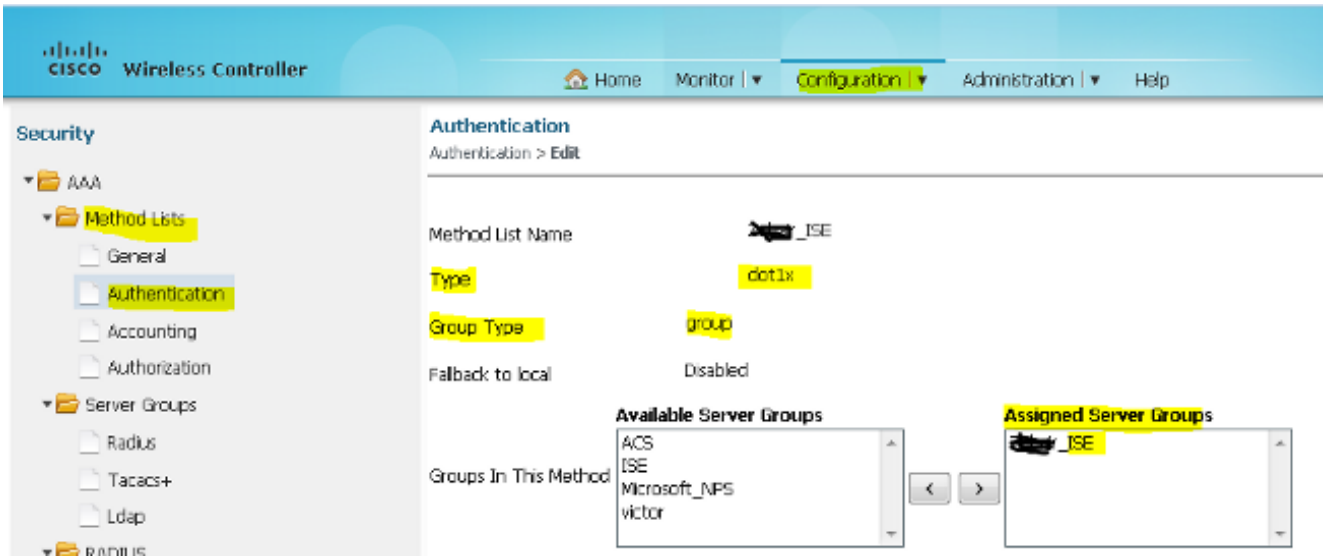
6. En la GUI del controlador inalámbrico, elija **AAA > Server Groups > Radius**. Agregue el servidor RADIUS creado anteriormente a los grupos de servidores.



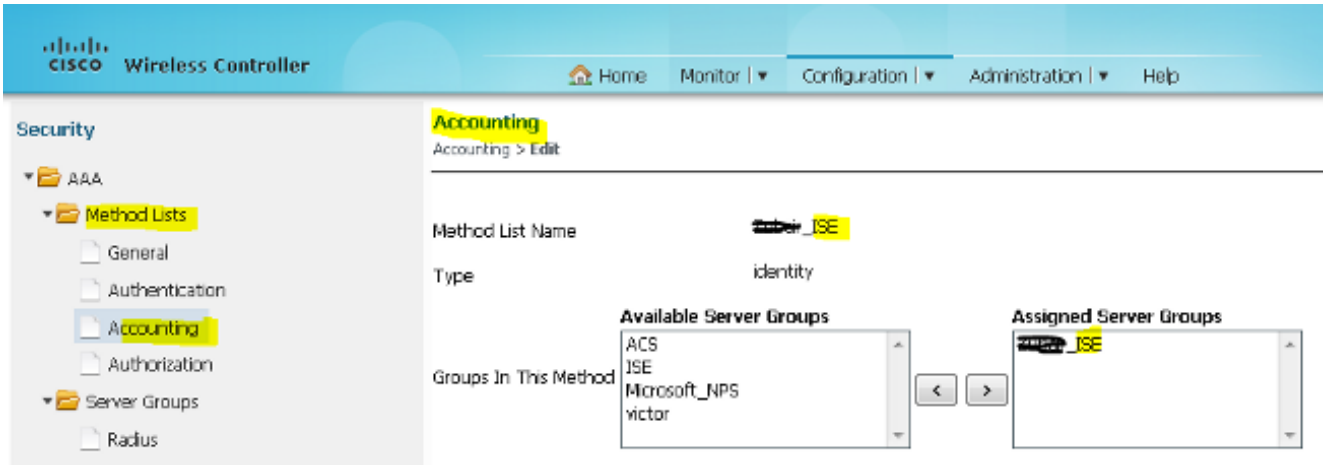
7. En la GUI del controlador inalámbrico, elija **AAA > Listas de métodos > General**. Marque la casilla de verificación **Dot1x System Auth Control**. Si desactiva esta opción, AAA no funcionará.



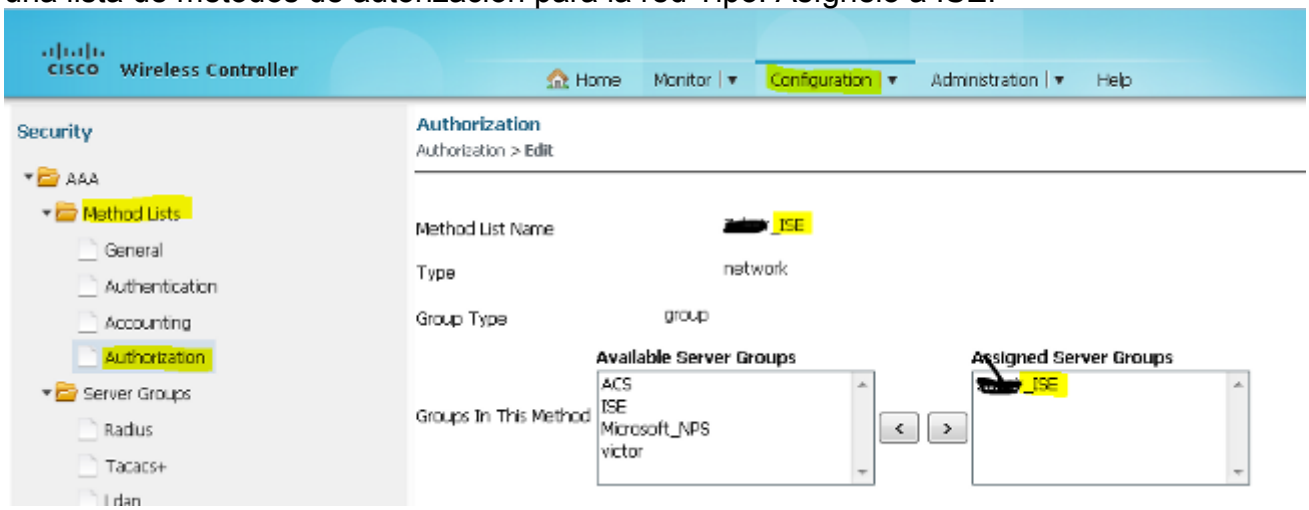
8. En la GUI del controlador inalámbrico, elija **AAA > Listas de métodos > Autenticación**. Cree una lista de métodos de autenticación para el tipo dot1X. El tipo de grupo es group. Asígnelo a ISE.



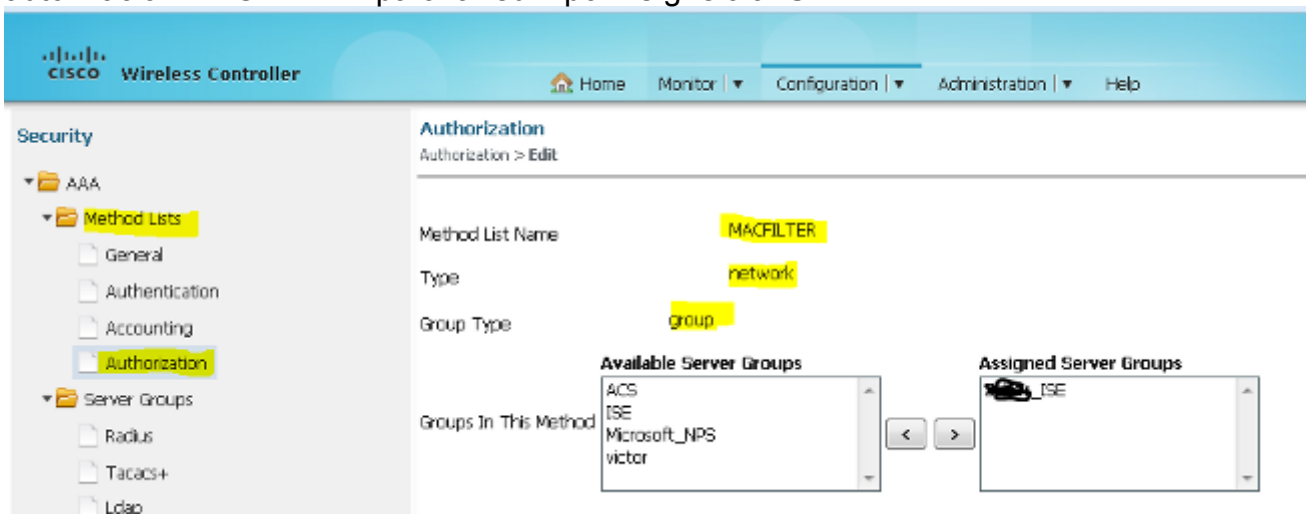
9. En la GUI del controlador inalámbrico, elija **AAA > Listas de métodos > Contabilización**. Cree una lista de métodos de contabilidad para la identidad de tipo. Asígnelo a ISE.



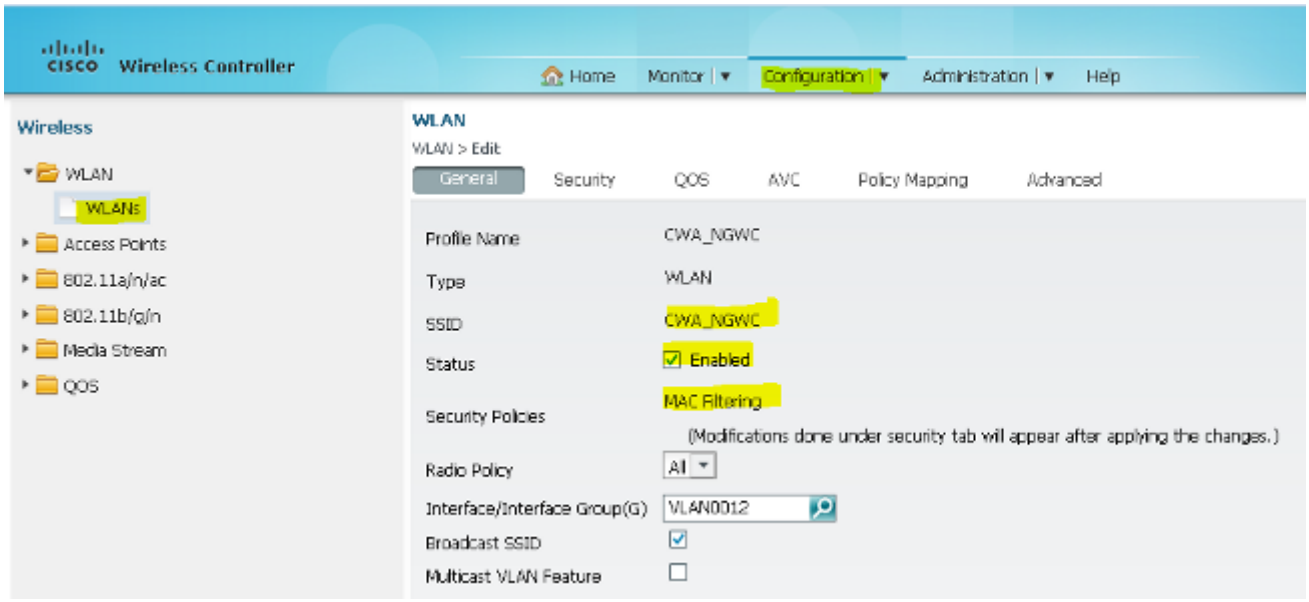
10. En la GUI del controlador inalámbrico, elija **AAA > Listas de métodos > Autorización**. Cree una lista de métodos de autorización para la red Tipo. Asígnelo a ISE.



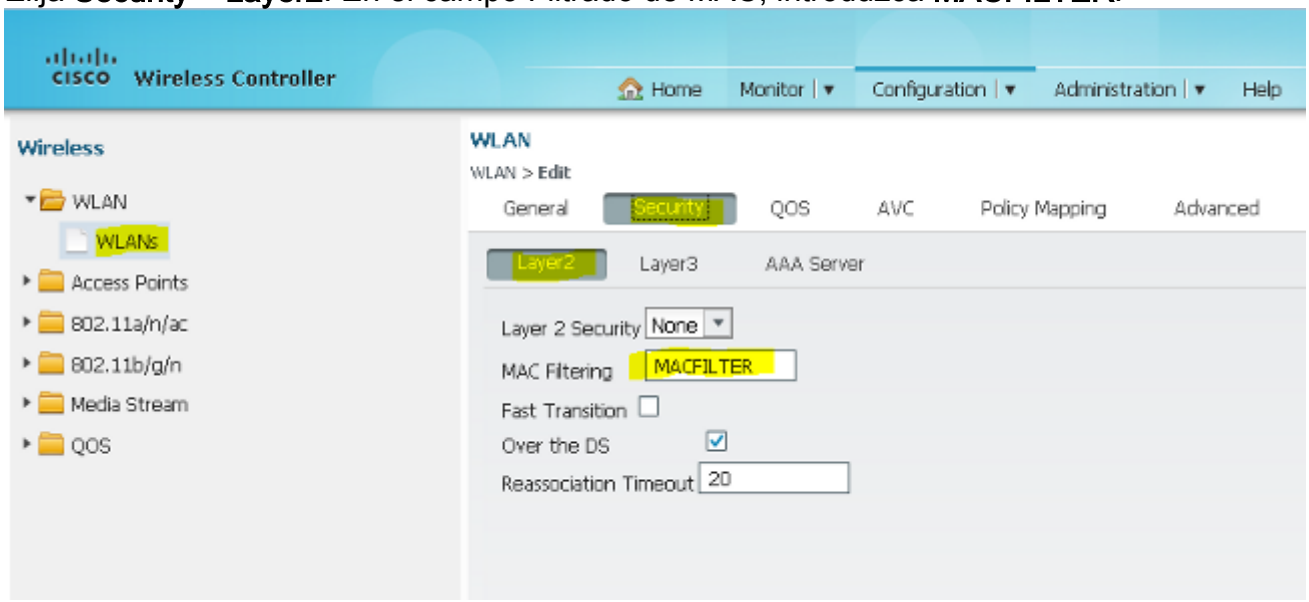
11. Opcional, ya que también hay MAC en caso de fallo. Cree una lista de métodos de autorización MACFILTER para la red Tipo. Asígnelo a ISE.



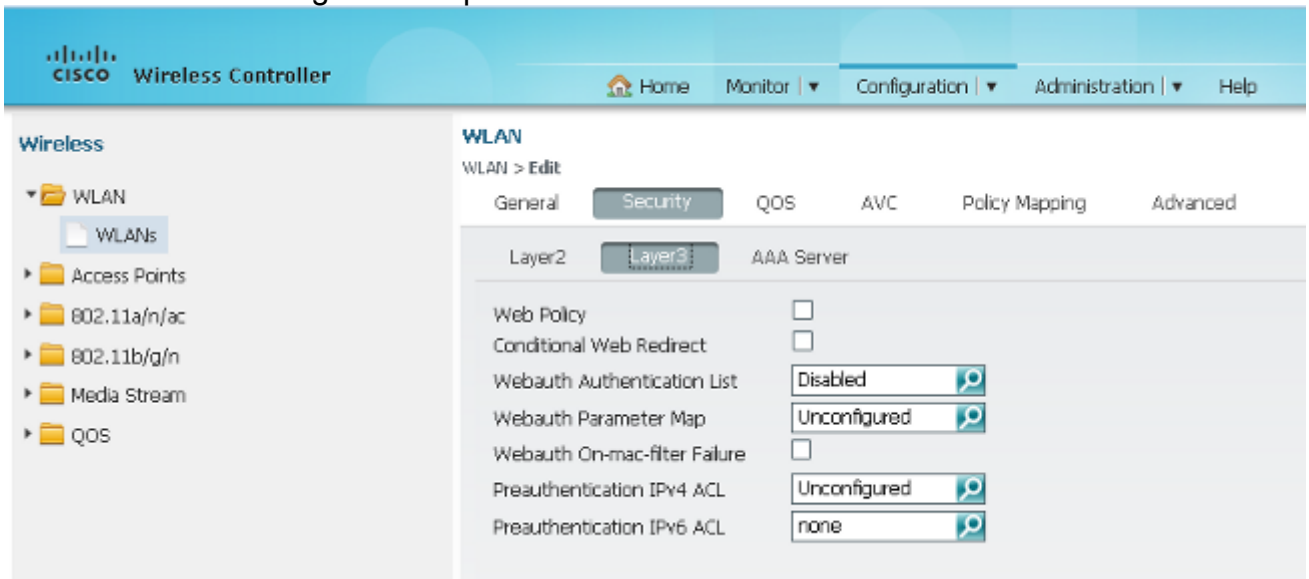
12. En la GUI del controlador inalámbrico, elija **WLAN > WLANs**. Cree una nueva configuración con los parámetros que se muestran aquí.



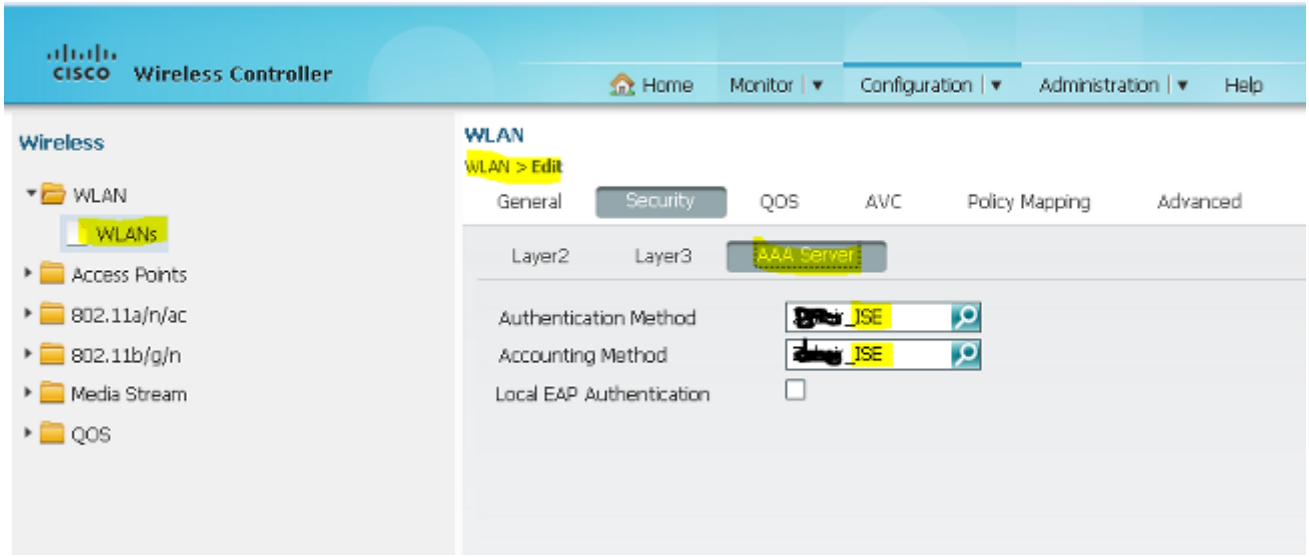
13. Elija **Security > Layer2**. En el campo Filtrado de MAC, introduzca **MACFILTER**.



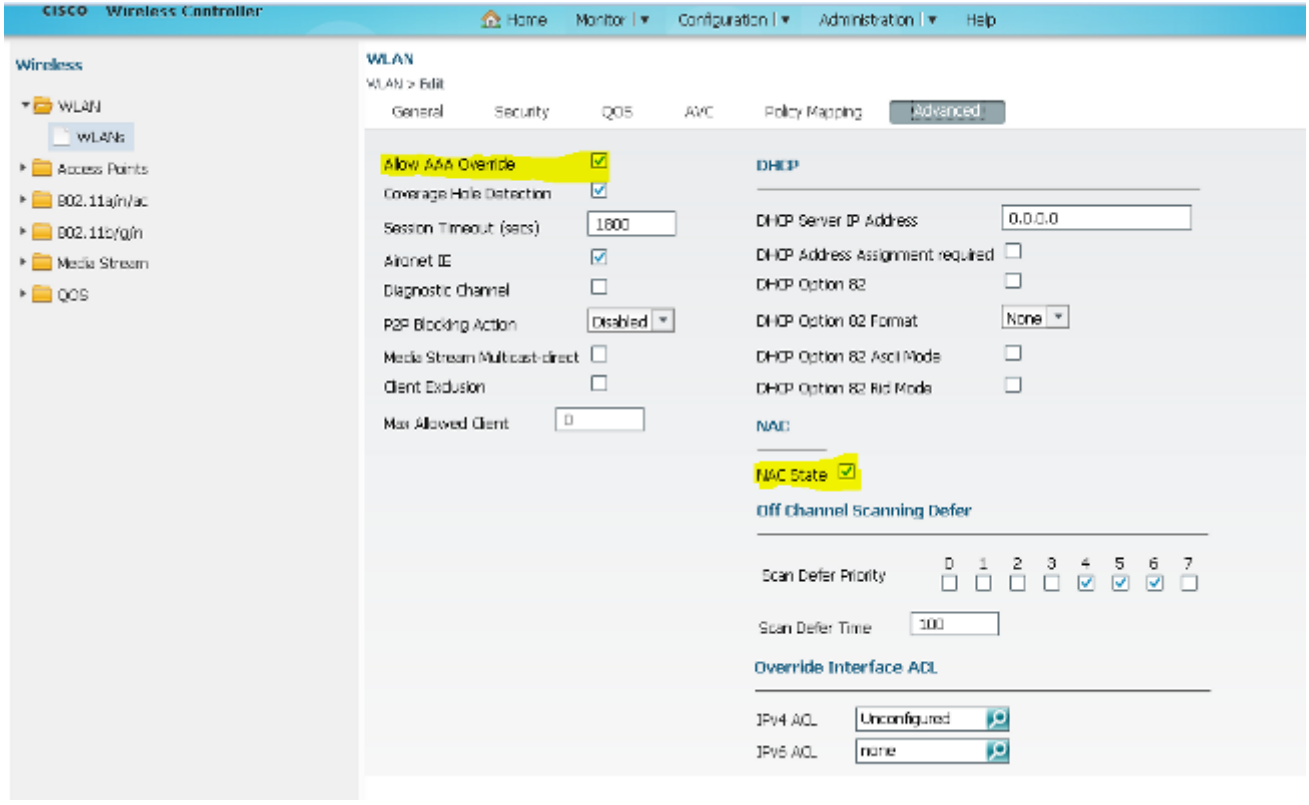
14. No es necesario configurar la capa 3.



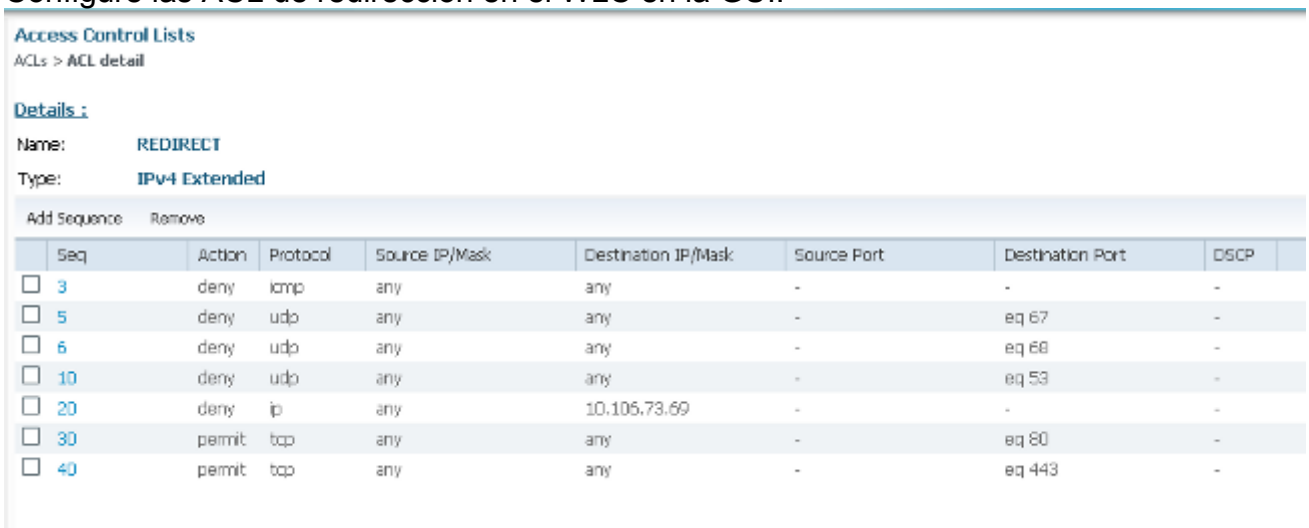
15. Elija **Security > AAA Server**. En la lista desplegable Método de autenticación, seleccione **ISE**. En la lista desplegable Método de contabilidad, seleccione **ISE**.



16. Elija **Advanced**. Marque la casilla de verificación **Allow AAA Override**. Marque la casilla de verificación **NAC State**.



17. Configure las ACL de redirección en el WLC en la GUI.



Seq	Action	Protocol	Source IP/Mask	Destination IP/Mask	Source Port	Destination Port	DSCP
3	deny	icmp	any	any	-	-	-
5	deny	udp	any	any	-	eq 67	-
6	deny	udp	any	any	-	eq 68	-
10	deny	udp	any	any	-	eq 53	-
20	deny	ip	any	10.105.73.69	-	-	-
30	permit	tcp	any	any	-	eq 80	-
40	permit	tcp	any	any	-	eq 443	-

Ejemplo de Configuración de Topología 2

Vea la Topología 2 para ver el diagrama y la explicación de la red.

Esta configuración también es un proceso de dos pasos.

Configuración en ISE

La configuración de ISE es la misma que la de Topology 1.

No es necesario agregar el controlador de anclaje en ISE. Solo tiene que agregar el WLC externo en el ISE, definir el servidor RADIUS en el WLC externo y asignar la política de autorización en la WLAN. En el Anchor solo necesita habilitar el filtrado de MAC.

En este ejemplo de configuración, hay dos WLC 5760 que actúan como un anclaje externo. En caso de que desee utilizar el WLC 5760 como un anclaje y el switch 3850 como el anclaje externo, que es el agente de movilidad, a otro controlador de movilidad, entonces la misma configuración es correcta. Sin embargo, no es necesario configurar la WLAN en el segundo controlador de movilidad del cual el switch 3850 obtiene las licencias. Solo necesita señalar el switch 3850 al WLC 5760 que actúa como anclaje.

Configuración en el WLC

1. En Foreign (Externo), configure el servidor ISE con la lista de métodos AAA para AAA y asigne la WLAN a una autorización de filtro MAC. **Nota**: Configure la ACL de redirección tanto en el Anchor como en el Foreign y también en el filtrado MAC.

```
dot1x system-auth-control

radius server ISE
 address ipv4 10.106.73.69 auth-port 1645 acct-port 1646
 timeout 10
 retransmit 3
 key Cisco123


aaa group server radius ISE
 server name ISE
 deadtime 10


aaa authentication dot1x ISE group ISE

aaa authorization network ISE group ISE

aaa authorization network MACFILTER group ISE
aaa accounting identity ISE start-stop group ISE
!

aaa server radius dynamic-author
 client 10.106.73.69 server-key Cisco123
 auth-type any

wlan MA-MC 11 MA-MC
 aaa-override
 accounting-list  ISE
 client vlan VLAN0012
```

```
 mac-filtering MACFILTER
 mobility anchor 10.105.135.244
nac
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
security dot1x authentication-list ISE
 session-timeout 1800
 no shutdown
```

2. Configure las ACL de redirección con la CLI. Esta es la url-redirect-acl que ISE devuelve como anulación de AAA junto con la URL de redirección para la redirección del portal de invitados. Se trata de una ACL directa que se utiliza actualmente en la arquitectura unificada. Esta es una ACL 'punt' que es una especie de ACL inversa que normalmente utilizaría para la arquitectura Unified. Debe bloquear el acceso a DHCP, el servidor DHCP, DNS, el servidor DNS e ISE. Solo permita www, 443 y 8443 según sea necesario. Este portal de invitados de ISE utiliza el puerto 8443 y la redirección sigue funcionando con la ACL que se muestra aquí. Aquí ICMP está habilitado, pero en función de las reglas de seguridad puede denegar o permitir.

```
ip access-list extended REDIRECT
 deny icmp any any
deny udp any any eq bootps
 deny udp any any eq bootpc
 deny udp any any eq domain
deny ip any host 10.106.73.69
 permit tcp any any eq www
 permit tcp any any eq 443
```

   Precaución: Cuando habilita HTTPS, puede causar algunos problemas de CPU altos debido a la escalabilidad. No lo habilite a menos que lo recomiende el equipo de diseño de Cisco.

3. Configure la movilidad en el ancla.

```
wireless mobility group member ip 10.105.135.244 public-ip 10.105.135.244 group surbg
```

   Nota: Si configura lo mismo con el switch 3850 que con el switch externo, asegúrese de definir el grupo de pares del switch en el controlador de movilidad y viceversa en el controlador de movilidad. Luego configure las configuraciones de CWA anteriores en el switch 3850.

4. Configuración en el anclaje. En el anclaje, no es necesario configurar ninguna configuración de ISE. Solo necesita la configuración de WLAN.

```
wlan MA-MC 6 MA-MC
 aaa-override
 client vlan VLAN0012
 mac-filtering MACFILTER
 mobility anchor
nac
 nbsp;no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 session-timeout 1800
 no shutdown
```

5. Configure la movilidad en el ancla. Defina el otro WLC como el miembro de la movilidad en este WLC.

```
wireless mobility group member ip 10.105.135.178 public-ip 10.105.135.178 group surbg
```

6. Configure las ACL de redirección con la CLI. Esta es la url-redirect-acl que ISE devuelve como anulación de AAA junto con la URL de redirección para la redirección del portal de invitados. Se trata de una ACL directa que se utiliza actualmente en la arquitectura unificada. Esta es una ACL 'punt' que es una especie de ACL inversa que normalmente utilizaría para

la arquitectura Unified. Debe bloquear el acceso a DHCP, el servidor DHCP, DNS, el servidor DNS e ISE. Solo permita www, 443 y 8443 según sea necesario. Este portal de invitados de ISE utiliza el puerto 8443 y la redirección sigue funcionando con la ACL que se muestra aquí. Aquí ICMP está habilitado, pero en función de las reglas de seguridad puede denegar o permitir.

```
ip access-list extended REDIRECT
 deny icmp any any
 deny udp any any eq bootps
 deny udp any any eq bootpc
 deny udp any any eq domain
 deny ip any host 10.106.73.69
 permit tcp any any eq www
 permit tcp any any eq 443
```

Precaución: Cuando habilita HTTPS, puede causar algunos problemas de CPU altos debido a la escalabilidad. No lo habilite a menos que lo recomiende el equipo de diseño de Cisco.

Ejemplo de Configuración de Topología 3

Consulte la Topología 3 para ver el diagrama y la explicación de la red.

Este es también un proceso de dos pasos.

Configuración en ISE

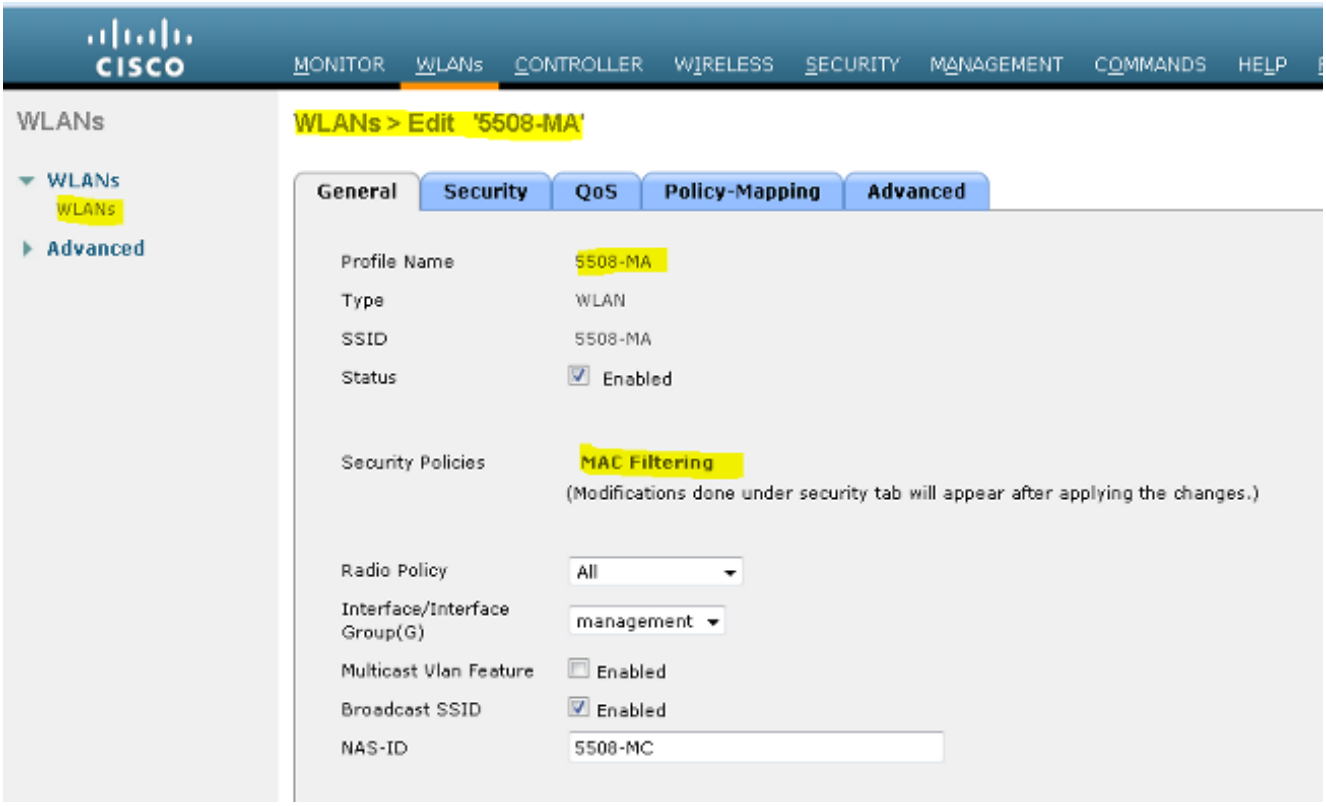
La configuración de ISE es la misma que la de Topology 1 Configuration.

No es necesario agregar el controlador de anclaje en ISE. Solo tiene que agregar el WLC externo en el ISE, definir el servidor RADIUS en el WLC externo y asignar la política de autorización en la WLAN. En el Anchor solo necesita habilitar el filtrado de MAC.

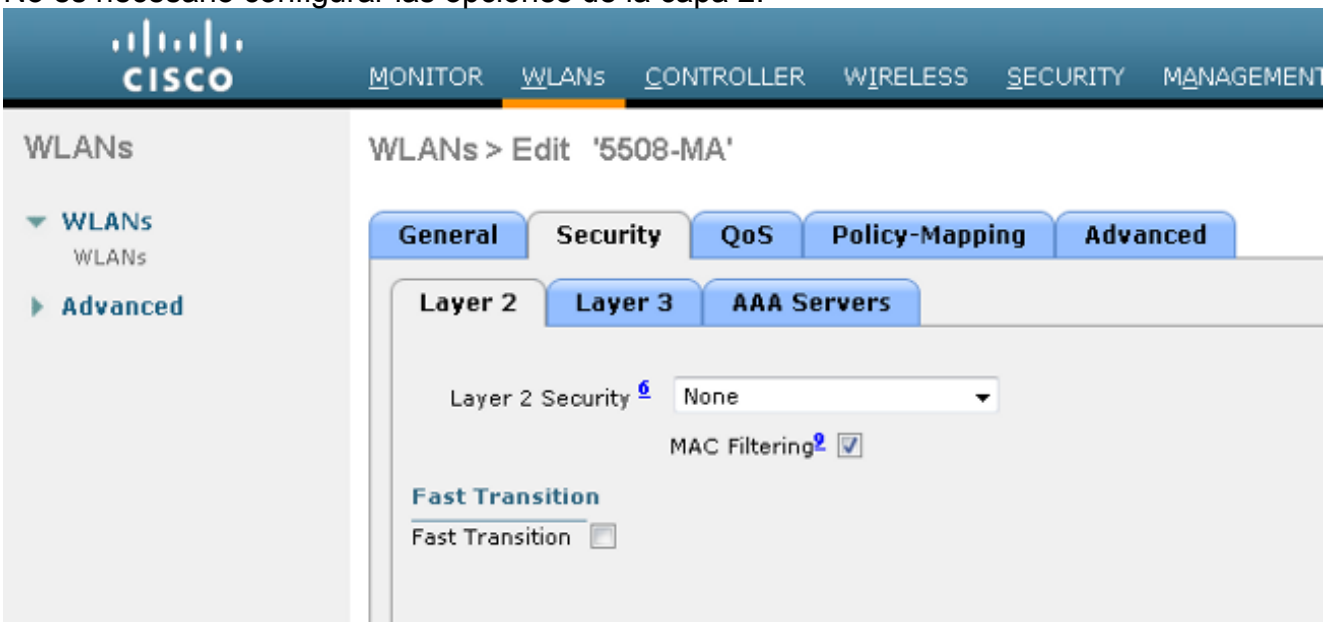
En este ejemplo, hay un WLC 5508 que actúa como un ancla y un WLC 5760 que actúa como un WLC extranjero. Si desea utilizar un WLC 5508 como un anclaje y un switch 3850 y un WLC externo, que es un agente de movilidad, a otro controlador de movilidad, entonces la misma configuración es correcta. Sin embargo, no es necesario configurar la WLAN en el segundo controlador de movilidad del cual el switch 3850 obtiene las licencias. Solo tiene que señalar el switch 3850 al WLC 5508 que actúa como anclaje.

Configuración en el WLC

1. En el WLC externo, configure el servidor ISE con la lista de métodos AAA para AAA y asigne la WLAN a una autorización de filtro MAC. Esto no es necesario en el anclaje. **Nota**: Configure la ACL de redirección en el WLC de anclaje y externo y también en el filtrado de MAC.
2. Desde el WLC 5508 GUI, elija **WLANs > New** para configurar el Anchor 5508. Complete los detalles para habilitar el filtrado de MAC.



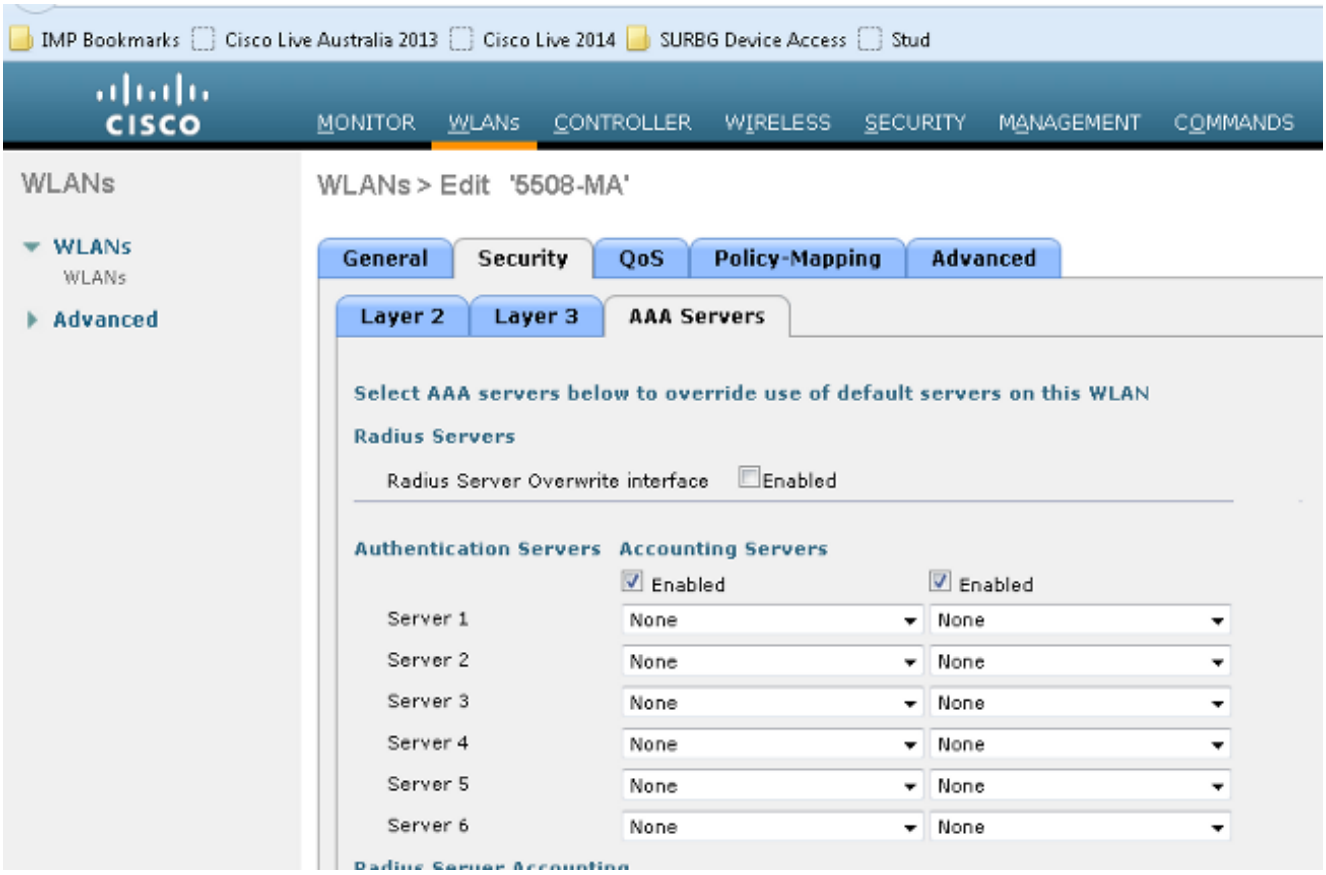
3. No es necesario configurar las opciones de la capa 2.



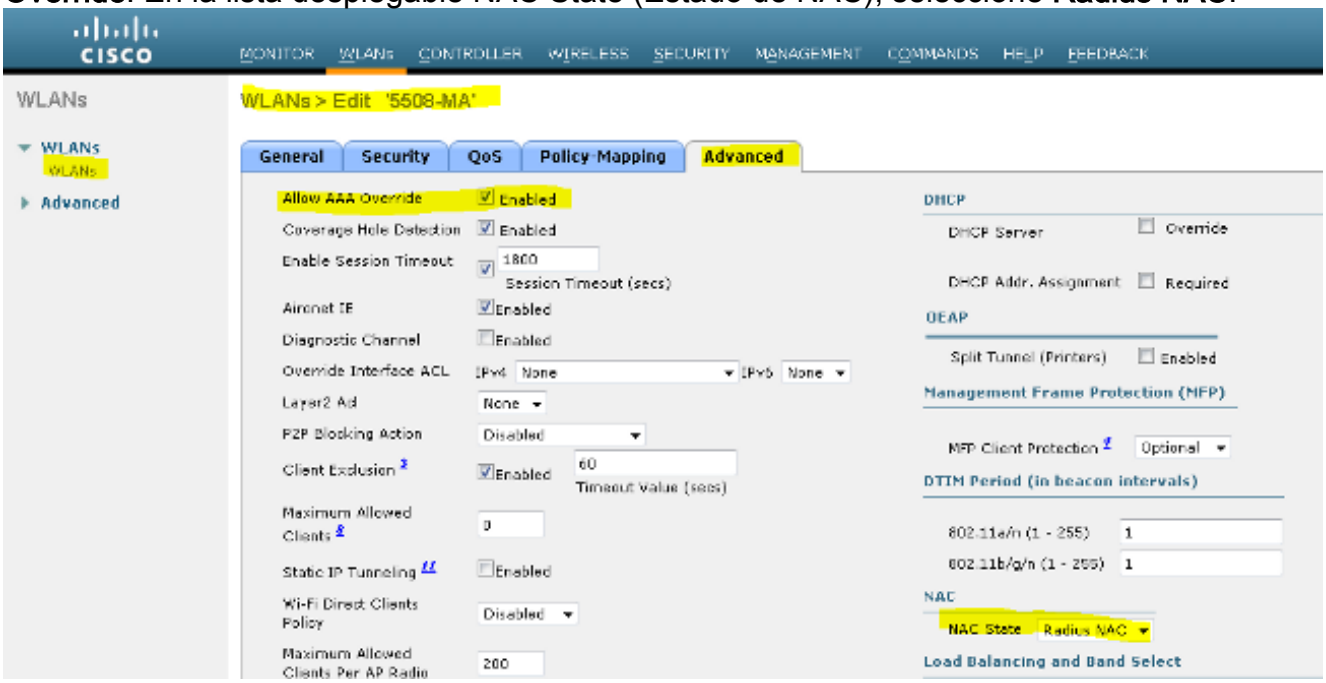
4. No es necesario configurar las opciones de la capa 3.

5. Los servidores AAA se deben inhabilitar en el WLC de Anchor AireOS para que la CoA sea

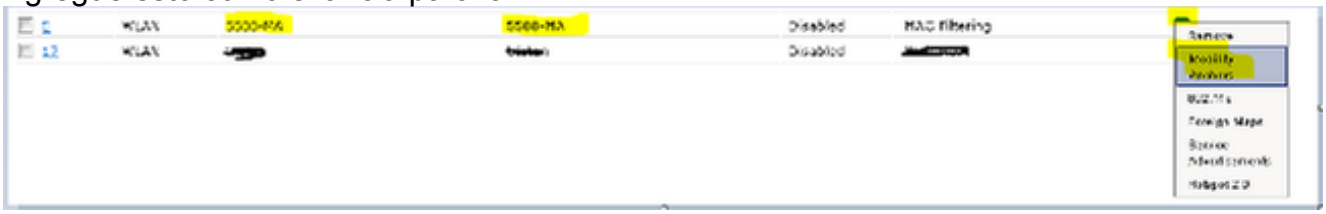
procesada por la NGWC extranjera. Los servidores AAA sólo se pueden habilitar en el WLC de anclaje si no hay servidores RADIUS configurados en: Seguridad > AAA > RADIUS > Autenticación



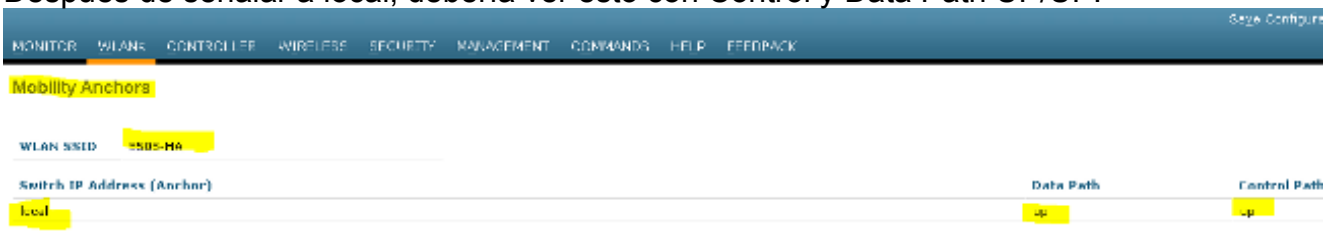
6. Elija **WLAN > WLAN > Edit > Advanced**. Marque la casilla de verificación **Allow AAA Override**. En la lista desplegable NAC State (Estado de NAC), seleccione **Radius NAC**.



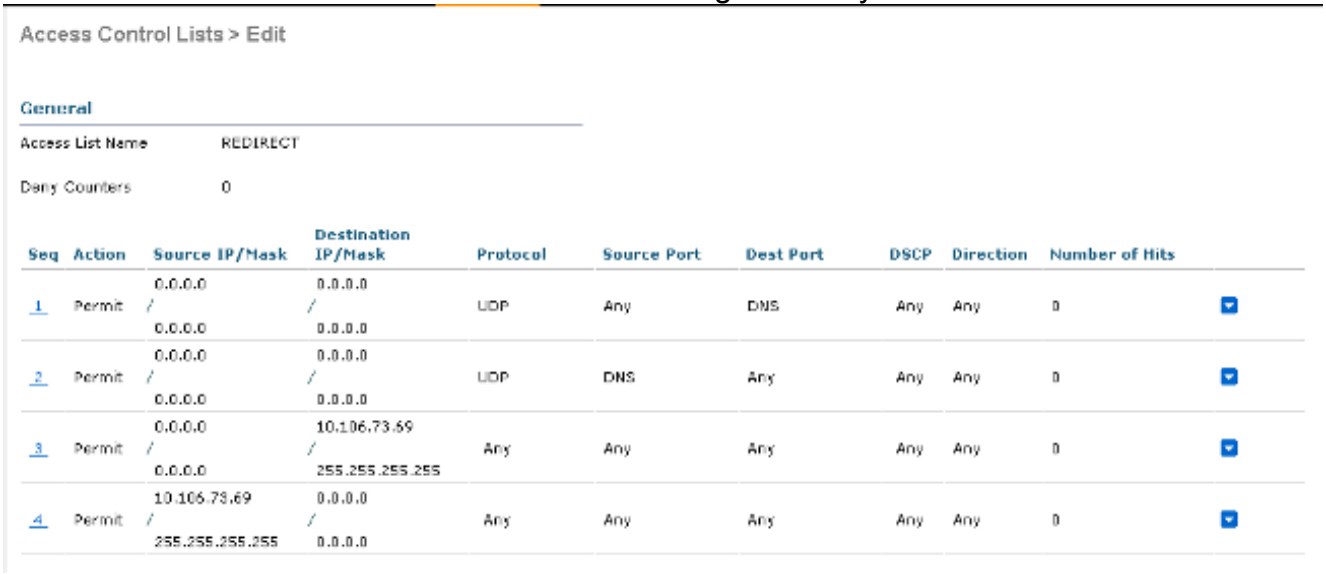
7. Agregue esto como el ancla para la WLAN.



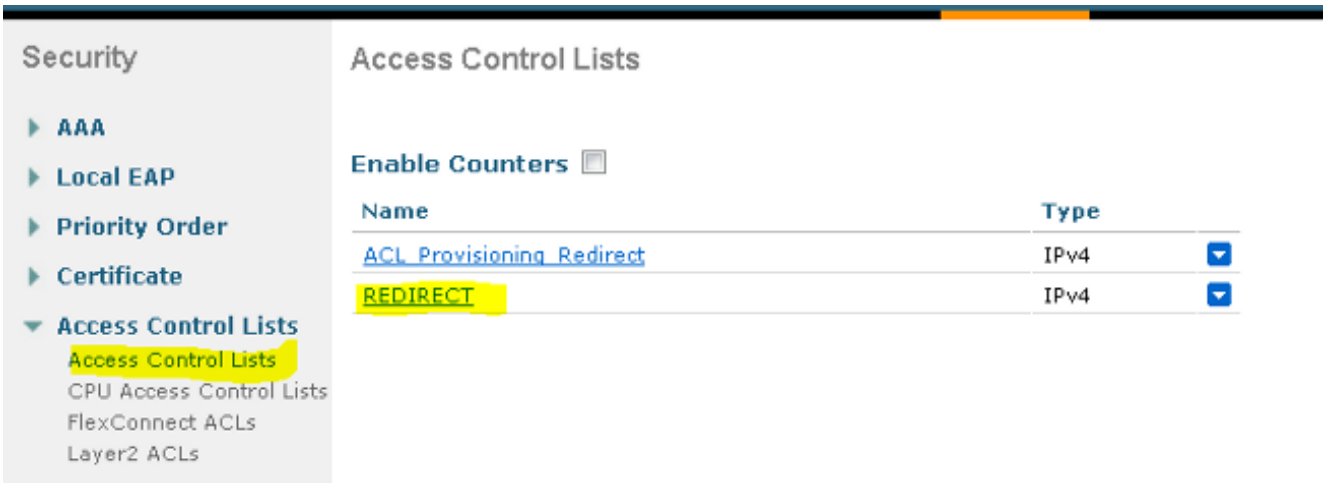
8. Después de señalar a local, debería ver esto con Control y Data Path UP/UP.



9. Cree la ACL de redirección en el WLC. Esto deniega DHCP y DNS. Permite HTTP/HTTP.



Así es como se ve después de que se crea la ACL.



10. Defina el servidor RADIUS de ISE en el WLC 5760.
11. Configure el servidor RADIUS, el grupo de servidores y la lista de métodos con la CLI.

```
dot1x system-auth-control

radius server ISE
 address ipv4 10.106.73.69 auth-port 1645 acct-port 1646
 timeout 10
 retransmit 3
 key Cisco123


aaa group server radius ISE
 server name ISE
 deadtime 10

aaa authentication dot1x ISE group ISE
```

```
aaa authorization network ISE group ISE

aaa authorization network MACFILTER group ISE

aaa accounting identity ISE start-stop group ISE

!

aaa server radius dynamic-author
 client 10.106.73.69 server-key Cisco123
 auth-type any
```

12. Configure la WLAN desde la CLI.

```
wlan 5508-MA 15 5508-MA
 aaa-override
 accounting-list ISE
 client vlan VLAN0012
 mac-filtering MACFILTER
 mobility anchor 10.105.135.151
 nac
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 security dot1x authentication-list ISE
 session-timeout 1800
 shutdown
```

13. Defina el otro WLC como el miembro de la movilidad en este WLC.

```
wireless mobility group member ip 10.105.135.151public-ip 10.105.135.151 group Mobile-1
```

Nota: Si configura lo mismo con el WLC 3850 como el Externo, asegúrese de definir el grupo de peers del Switch en el Controlador de Movilidad y viceversa en el Controlador de Movilidad. Luego configure las configuraciones de CWA anteriores en el WLC 3850.

14. Configure las ACL de redirección con la CLI. Esta es la url-redirect-acl que ISE devuelve como anulación de AAA junto con la URL de redirección para la redirección del portal de invitados. Se trata de una ACL directa que se utiliza actualmente en la arquitectura unificada. Esta es una ACL 'punt' que es una especie de ACL inversa que normalmente utilizaría para la arquitectura Unified. Debe bloquear el acceso a DHCP, el servidor DHCP, DNS, el servidor DNS e ISE. Solo permita www, 443 y 8443 según sea necesario. Este portal de invitados de ISE utiliza el puerto 8443 y la redirección sigue funcionando con la ACL que se muestra aquí. Aquí ICMP está habilitado, pero en función de las reglas de seguridad puede denegar o permitir.

```
ip access-list extended REDIRECT
 deny icmp any any
 deny udp any any eq bootps
 deny udp any any eq bootpc
 deny udp any any eq domain
 deny ip any host 10.106.73.69
 permit tcp any any eq www
 permit tcp any any eq 443
```

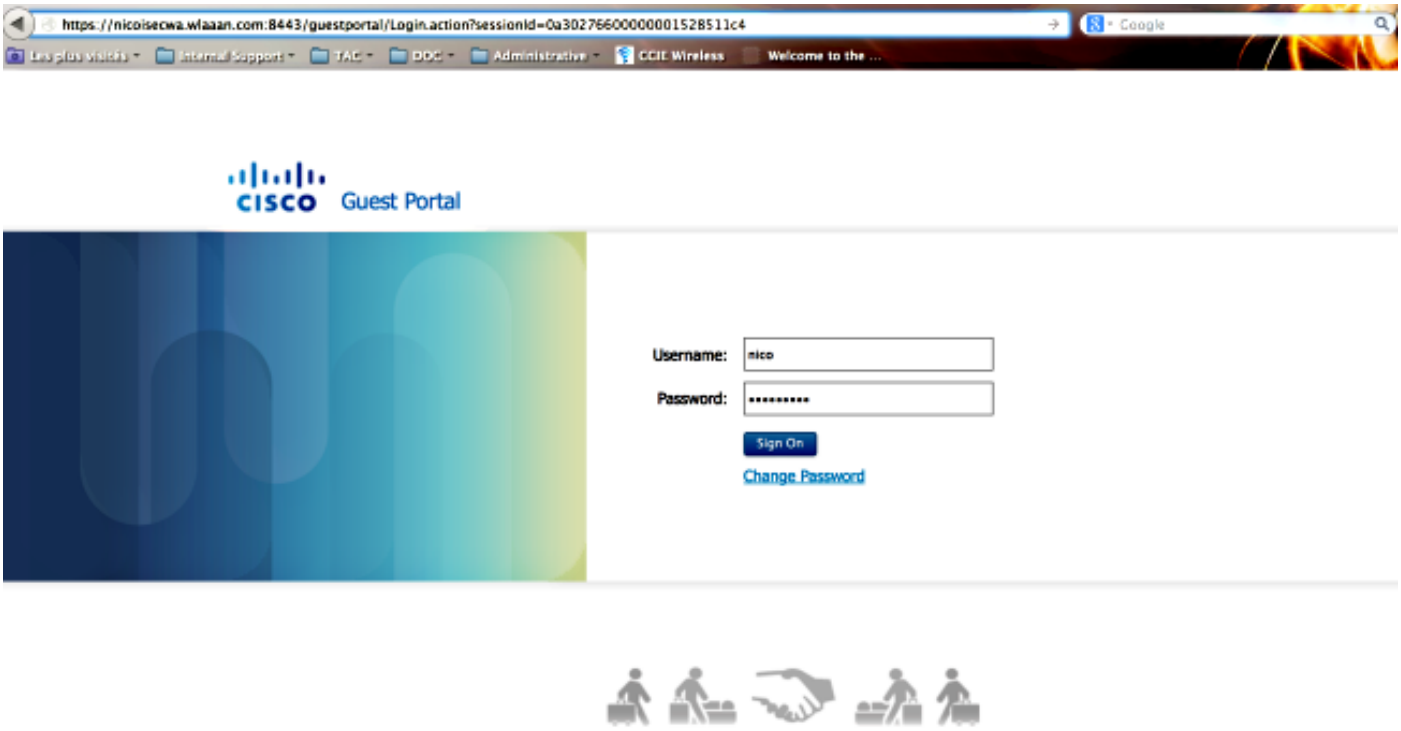
Precaución: Cuando habilita HTTPS, puede causar algunos problemas de CPU altos debido a la escalabilidad. No lo habilite a menos que lo recomiende el equipo de diseño de Cisco.

Verificación

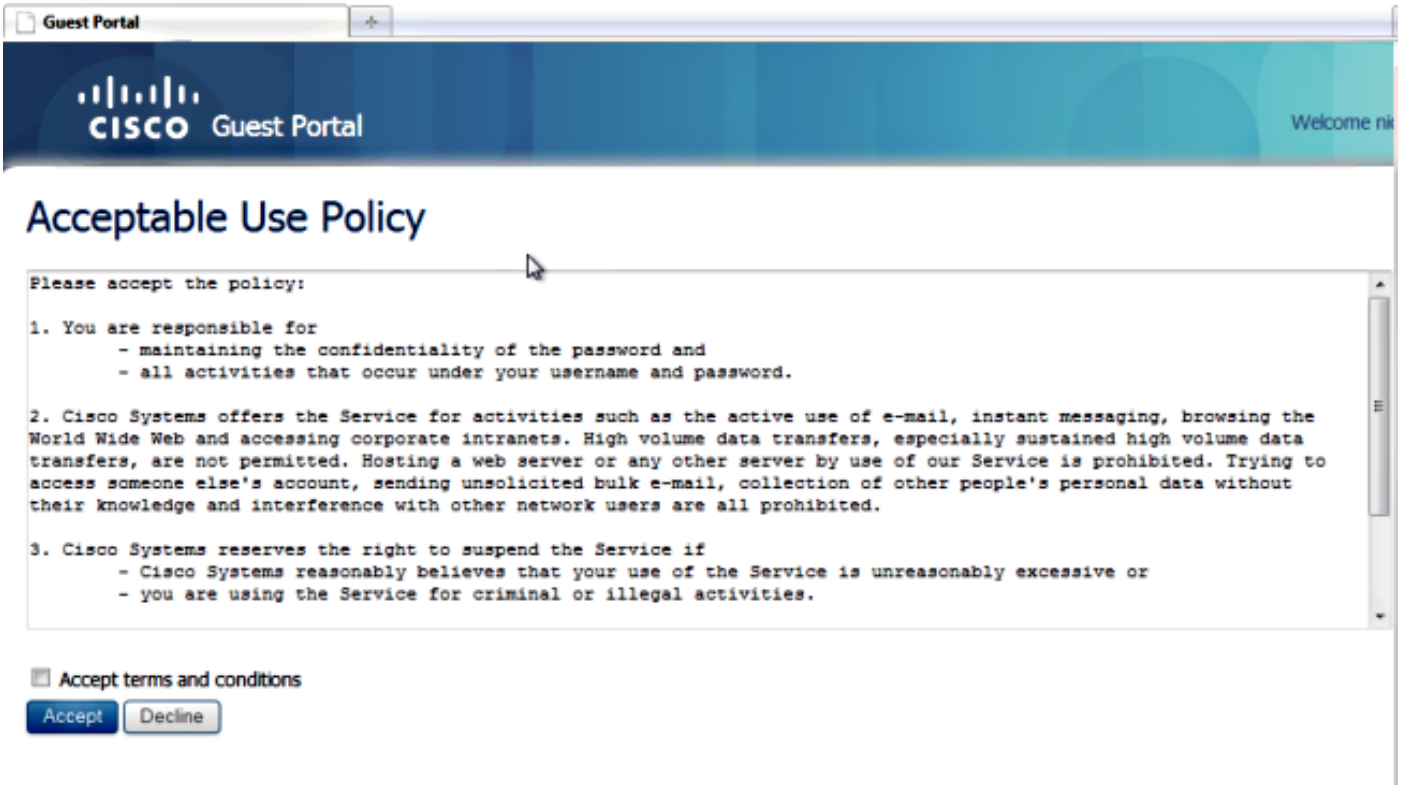
Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta de interpretación de información de salida (disponible para clientes registrados únicamente) admite ciertos comandos show. Utilice la herramienta para ver una análisis de información de salida del comando show.

Conecte el cliente al SSID configurado. Una vez que reciba la dirección IP y cuando el cliente vaya al estado de autenticación Web requerida, abra el explorador. Introduzca sus credenciales de cliente en el portal.

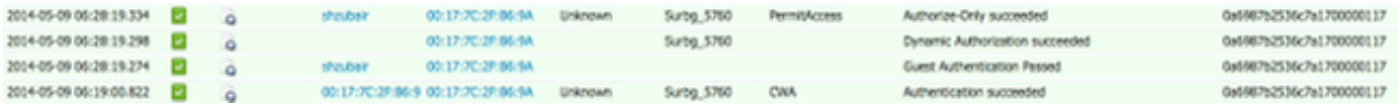


Después de una autenticación correcta, marque la casilla de verificación **Aceptar términos y condiciones**. Haga clic en **Aceptar**.



Recibirá un mensaje de confirmación y ahora podrá navegar a Internet.

En el ISE, el flujo de clientes es similar al siguiente:



Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

La herramienta de interpretación de información de salida (disponible para clientes registrados únicamente) admite ciertos comandos show. Utilice la herramienta para ver una análisis de información de salida del comando show.

> **Nota: Consulte Información Importante sobre Comandos Debug antes de utilizar los comandos debug.**

En el WLC de acceso convergente, se recomienda ejecutar seguimientos en lugar de depuraciones. En el WLC Aironet OS 5508, solo necesita ingresar **debug client <client mac>** y **debug web-auth redirect enable mac <client mac>**.

```
set trace group-wireless-client level debug
set trace group-wireless-secure level debug

set trace group-wireless-client filter mac 0017.7c2f.b69a
set trace group-wireless-secure filter mac 0017.7c2f.b69a
```

Algunos defectos conocidos en Cisco IOS-XE y Aironet OS se incluyen en el Id. de error de Cisco CSCun38344.

Así es como se ve el flujo exitoso de CWA en los seguimientos:

```
[05/09/14 13:13:15.951 IST 63d7 8151] 0017.7c2f.b69a Association received from mobile
```

on AP c8f9.f983.4260
[05/09/14 13:13:15.951 IST 63d8 8151] 0017.7c2f.b69a qos upstream policy is unknown
and downstream policy is unknown

**[05/09/14 13:13:15.951 IST 63e0 8151] 0017.7c2f.b69a Applying site-specific IPv6
override for station 0017.7c2f.b69a - vapId 15, site 'default-group', interface
'VLAN0012'**
[05/09/14 13:13:15.951 IST 63e1 8151] 0017.7c2f.b69a Applying local bridging Interface
Policy for station 0017.7c2f.b69a - vlan 12, interface 'VLAN0012'
[05/09/14 13:13:15.951 IST 63e2 8151] 0017.7c2f.b69a
 **** Inside applyLocalProfilingPolicyAction ****

[05/09/14 13:13:15.951 IST 63e3 8151] 0017.7c2f.b69a *** **Client State = START**
instance = 1 instance Name POLICY_PROFILING_80211_ASSOC, OverrideEnable = 1
deviceTypeLen=0, deviceType=(null), userRoleLen=0, userRole=(null

**[05/09/14 13:13:15.951 IST 63eb 8151] 0017.7c2f.b69a AAAS: Submitting mac filter
request for user 00177c2fb69a, uniqueId=280 mlist=MACFILTER**
[05/09/14 13:13:15.951 IST 63ec 8151] 0017.7c2f.b69a AAAS: auth request sent
**05/09/14 13:13:15.951 IST 63ed 8151] 0017.7c2f.b69a apfProcessAssocReq
(apf_80211.c:6149) Changing state for mobile 0017.7c2f.b69a on AP c8f9.f983.4260
 from Idle to AAA Pending**

[05/09/14 13:13:15.951 IST 63ee 8151] 0017.7c2f.b69a Reason code 0, Preset 4, AAA cause 1
[05/09/14 13:13:15.951 IST 63ef 8151] 0017.7c2f.b69a Scheduling deletion of Mobile
Station: (callerId: 20) in 10 seconds
[05/09/14 13:13:15.951 IST 63f0 211] **Parsed CLID MAC Address = 0:23:124:47:182:154**
[05/09/14 13:13:15.951 IST 63f1 211] AAA SRV(00000118): process author req
[05/09/14 13:13:15.951 IST 63f2 211] **AAA SRV(00000118): Author method=SERVER_GROUP Zubair_ISE**
[05/09/14 13:13:16.015 IST 63f3 220] AAA SRV(00000118): protocol reply PASS for Authorization
[05/09/14 13:13:16.015 IST 63f4 220] AAA SRV(00000118): Return Authorization status=PASS
[05/09/14 13:13:16.015 IST 63f5 8151] 0017.7c2f.b69a AAAS: received response, cid=266
[05/09/14 13:13:16.015 IST 63f6 8151] 0017.7c2f.b69a AAAS: deleting context, cid=266
[05/09/14 13:13:16.015 IST 63f7 8151] 0017.7c2f.b69a Not comparing because the ACLs have
not been sent yet.
[05/09/14 13:13:16.015 IST 63f8 8151] 0017.7c2f.b69a Final flag values are, epmSendAcl 1,
epmSendAclDone 0
[05/09/14 13:13:16.015 IST 63f9 8151] 0017.7c2f.b69a
client incoming attribute size are 193
**[05/09/14 13:13:16.015 IST 63fa 8151] 0017.7c2f.b69a AAAS: mac filter callback
status=0 uniqueId=280**
**[05/09/14 13:13:16.015 IST 63fb 8151] 0017.7c2f.b69a AAA Override Url-Redirect
'https://10.106.73.69:8443/guestportal/gateway?sessionId=0a6987b2536c871300000118&action=cwa'
set**
[05/09/14 13:13:16.015 IST 63fc 8151] **0017.7c2f.b69a Redirect URL received for
client from RADIUS. for redirection.**
[05/09/14 13:13:16.015 IST 63fd 8151] 0017.7c2f.b69a Setting AAA Override
Url-Redirect-Acl 'REDIRECT'
[05/09/14 13:13:16.015 IST 63fe 8151] 0017.7c2f.b69a AAA Override Url-Redirect-Acl
'REDIRECT'
[05/09/14 13:13:16.015 IST 63ff 8151] 0017.7c2f.b69a Local Policy: At the start of
apfApplyOverride2. Client State START

[05/09/14 13:13:16.015 IST 6400 8151] 0017.7c2f.b69a Applying new AAA override for
station 0017.7c2f.b69a
[05/09/14 13:13:16.015 IST 6401 8151] 0017.7c2f.b69a Local Policy: Applying new
AAA override for station
[05/09/14 13:13:16.015 IST 6402 8151] 0017.7c2f.b69a Override Values: source: 2,
valid_bits: 0x0000, qosLevel: -1 dscp: 0xffffffff, dot1pTag: 0xffffffff,
sessionTimeout: -1
[05/09/14 13:13:16.015 IST 6403 8151] 0017.7c2f.b69a dataAvgC: -1, rTAvgC: -1,
dataBurstC: -1 rTimeBurstC: -1, vlanIfName: , aclName:
[05/09/14 13:13:16.015 IST 6404 8151] 0017.7c2f.b69a Local Policy: Applying
override policy

[05/09/14 13:13:16.015 IST 6405 8151] 0017.7c2f.b69a Clearing Dhcp state for station ---
[05/09/14 13:13:16.015 IST 6406 8151] 0017.7c2f.b69a Local Policy: Before Applying WLAN policy AccessVLAN = 12 and SessionTimeout is 1800 and apfMsTimeout is 1800

[05/09/14 13:13:16.015 IST 6407 8151] 0017.7c2f.b69a Local Policy:Setting Interface name e VLAN0012

[05/09/14 13:13:16.015 IST 6408 8151] 0017.7c2f.b69a Local Policy:Setting local bridging VLAN name VLAN0012 and VLAN ID 12

[05/09/14 13:13:16.015 IST 6409 8151] 0017.7c2f.b69a Applying WLAN ACL policies to client
[05/09/14 13:13:16.015 IST 640a 8151] 0017.7c2f.b69a No Interface ACL used for Wireless client in WCM(NGWC)
[05/09/14 13:13:16.015 IST 640b 8151] 0017.7c2f.b69a apfApplyWlanPolicy: Retaining the ACL recieved in AAA attributes 255 on mobile
[05/09/14 13:13:16.015 IST 640c 8151] 0017.7c2f.b69a Local Policy: After Applying WLAN policy AccessVLAN = 12 and SessionTimeout is 1800 and apfMsTimeout is 1800

[05/09/14 13:13:16.015 IST 641a 8151] 0017.7c2f.b69a WCDB_ADD: Platform ID allocated successfully ID:259
[05/09/14 13:13:16.015 IST 641b 8151] 0017.7c2f.b69a WCDB_ADD: Adding opt82 len 0
[05/09/14 13:13:16.015 IST 641c 8151] 0017.7c2f.b69a WCDB_ADD: ssid 5508-MA bssid c8f9.f983.4260 vlan 12 auth=ASSOCIATION(0) wlan(ap-group/global) 15/15 client 0 assoc 1 mob=Unassoc(0) radio 0 m_vlan 12 ip 0.0.0.0 src 0x506c800000000f dst 0x0 cid 0x47ad4000000145 glob rsc id 259dhcpsrv 0.0.0
[05/09/14 13:13:16.015 IST 641d 8151] 0017.7c2f.b69a Change state to AUTHCHECK (2) last state START (0)

[05/09/14 13:13:16.015 IST 641e 8151] 0017.7c2f.b69a Change state to L2AUTHCOMPLETE (4) last state AUTHCHECK (2)

[05/09/14 13:13:16.015 IST 641f 8151] 0017.7c2f.b69a WCDB_AUTH: Adding opt82 len 0
[05/09/14 13:13:16.015 IST 6420 8151] 0017.7c2f.b69a WCDB_LLM: NoRun Prev Mob 0, Curr Mob 0 llmReq 1, return False
[05/09/14 13:13:16.015 IST 6421 207] [WCDB] ==Add event: type Regular Wireless client (0017.7c2f.b69a) client id (0x47ad4000000145) client index (259) vlan (12) auth_state (ASSOCIATION) mob_state (INIT)
[05/09/14 13:13:16.015 IST 6422 207] [WCDB] ===intf src/dst (0x506c800000000f)/(0x0) radio_id (0) p2p_state (P2P_BLOCKING_DISABLE) switch/asic (1/0)
[05/09/14 13:13:16.015 IST 6423 8151] 0017.7c2f.b69a WCDB_CHANGE: auth=L2_AUTH(1) vlan 12 radio 0 client_id 0x47ad4000000145 mobility=Unassoc(0) src_int 0x506c800000000f dst_int 0x0 ackflag 0 reassoc_client 0 llm_notif 0 ip 0.0.0.0 ip_learn_type 0
[05/09/14 13:13:16.015 IST 6424 8151] 0017.7c2f.b69a WCDB_CHANGE: In L2 auth but l2ack waiting lfag not set,so set
[05/09/14 13:13:16.015 IST 6425 8151] 0017.7c2f.b69a Not Using WMM Compliance code qosCap 00
[05/09/14 13:13:16.016 IST 6426 8151] 0017.7c2f.b69a **Change state to DHCP_REQD (7) last state L2AUTHCOMPLETE (4)**

[05/09/14 13:13:16.016 IST 6434 8151] 0017.7c2f.b69a Sending Assoc Response to station on BSSID c8f9.f983.4260 (status 0) ApVapId 15 Slot 0
[05/09/14 13:13:16.016 IST 6435 8151] 0017.7c2f.b69a apfProcessRadiusAssocResp (apf_80211.c:2316) Changing state for mobile 0017.7c2f.b69a on AP c8f9.f983.4260 from Associated to Associated

[05/09/14 13:13:16.016 IST 6436 8151] 0017.7c2f.b69a 1XA: Session Push for

```
Non-dot1x wireless client
[05/09/14 13:13:16.016 IST 6437 8151] 0017.7c2f.b69a 1XA: Calling Auth Mgr
to Push wireless session for client  47ad4000000145 uid 280
[05/09/14 13:13:16.016 IST 6438 8151] 0017.7c2f.b69a Session Push for
wireless client

[05/09/14 13:13:16.016 IST 6439 8151] 0017.7c2f.b69a Session Manager Call
Client 47ad4000000145, uid 280, capwap id 506c800000000f,Flag 1 Audit-Session
ID 0a6987b2536c871300000118 policy name (null)

[05/09/14 13:13:16.016 IST 643a 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF:
[0017.7c2f.b69a, Ca2] Session start request from Client[1] for
0017.7c2f.b69a (method: No method, method list: none, aaa id:
0x00000118) - session-push,  policy
[05/09/14 13:13:16.016 IST 643b 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF:
[0017.7c2f.b69a, Ca2]  - client iif_id: 47AD4000000145, session ID:
0a6987b2536c871300000118 for 0017.7c2f.b69a
[05/09/14 13:13:16.016 IST 643c 243] ACCESS-CORE-SM-SYNC-NOTF:
[0017.7c2f.b69a, Ca2] Delay add/update sync of auth-domain for
0017.7c2f.b69a / 0xFE000110
[05/09/14 13:13:16.017 IST 643d 243] ACCESS-CORE-SM-CLIENT-DOT11-ERR:
[0017.7c2f.b69a, Ca2] Invalid client authorization notification: NO method
[05/09/14 13:13:16.017 IST 643e 243] ACCESS-CORE-SM-SYNC-NOTF:
[0017.7c2f.b69a, Ca2] Delay add/update sync of dc-profile-name for
0017.7c2f.b69a / 0xFE000110
[05/09/14 13:13:16.017 IST 643f 243] ACCESS-CORE-SM-SYNC-NOTF:
[0017.7c2f.b69a, Ca2] Delay add/update sync of dc-device-name for
0017.7c2f.b69a / 0xFE000110
[05/09/14 13:13:16.017 IST 6440 243] ACCESS-CORE-SM-SYNC-NOTF:
[0017.7c2f.b69a, Ca2] Delay add/update sync of
dc-device-class-tag for 0017.7c2f.b69a / 0xFE000110
[05/09/14 13:13:16.017 IST 6441 243] ACCESS-CORE-SM-SYNC-NOTF:
[0017.7c2f.b69a, Ca2] Delay add/update sync of dc-certainty-metric for
0017.7c2f.b69a / 0xFE000110
[05/09/14 13:13:16.017 IST 6442 243] ACCESS-CORE-SM-SYNC-NOTF:
[0017.7c2f.b69a, Ca2] Delay add/update sync of dc-opaque for
0017.7c2f.b69a / 0xFE000110
[05/09/14 13:13:16.017 IST 6443 243] ACCESS-CORE-SM-SYNC-NOTF:
[0017.7c2f.b69a, Ca2] Delay add/update sync of dc-protocol-map for
0017.7c2f.b69a / 0xFE000110
[05/09/14 13:13:16.017 IST 6444 22] [WCDB] wcdb_ffcp_add_cb: client (0017.7c2f.b69a)
client (0x47ad4000000145): FFCP operation (CREATE) return code (0)
[05/09/14 13:13:16.017 IST 6445 22] [WCDB] wcdb_send_add_notify_callback_event:
Notifying other features about client add
[05/09/14 13:13:16.017 IST 6446 22] [WCDB] wcdb_sisf_client_add_notify:
Notifying SISF of DEASSOC to DOWN any old entry for 0017.7c2f.b69a
[05/09/14 13:13:16.017 IST 6447 22] [WCDB] wcdb_sisf_client_add_notify:
Notifying SISF of new Association for 0017.7c2f.b69a
[05/09/14 13:13:16.017 IST 6448 8151] 0017.7c2f.b69a WCDB SPI response msg handler
client code 0 mob state 0
[05/09/14 13:13:16.017 IST 6449 8151] 0017.7c2f.b69a WcdbClientUpdate: L2 Auth ACK
from WCDB
[05/09/14 13:13:16.017 IST 644a 8151] 0017.7c2f.b69a WCDB_L2ACK: wcdbAckRecvdFlag
updated
[05/09/14 13:13:16.017 IST 644b 8151] 0017.7c2f.b69a WCDB_AUTH: Adding opt82 len 0
[05/09/14 13:13:16.017 IST 644c 8151] 0017.7c2f.b69a WCDB_CHANGE: Suppressing SPI
(Mobility state not known) pemstate 7 state LEARN_IP(2) vlan 12 client_id
0x47ad4000000145 mob=Unassoc(0) ackflag 2 dropd 1
[05/09/14 13:13:18.796 IST 644d 8151] 0017.7c2f.b69a Local Policy:
apf_ms_radius_override.c apfMsSumOverride 447  Returning fail from apfMsSumOverride
[05/09/14 13:13:18.802 IST 644e 8151] 0017.7c2f.b69a Applying post-handoff policy
for station  0017.7c2f.b69a  - valid mask 0x0

[05/09/14 13:13:18.802 IST 644f 8151] 0017.7c2f.b69a     QOS Level: -1, DSCP: -1,
```

```
dot1p: -1, Data Avg: -1, realtime Avg: -1, Data Burst -1, Realtime Burst -1
 --More--

[05/09/14 13:13:18.802 IST 6450 8151] 0017.7c2f.b69a     Session: -1,
User session: -1, User elapsed -1
   Interface: N/A ACL: N/A Qos Pol Down   Qos Pol Up

[05/09/14 13:13:18.802 IST 6451 8151] 0017.7c2f.b69a Local Policy: At the start of
apfApplyOverride2. Client State DHCP_REQD

[05/09/14 13:13:18.802 IST 6452 8151] 0017.7c2f.b69a Applying new AAA override for
station  0017.7c2f.b69a
[05/09/14 13:13:18.802 IST 6453 8151] 0017.7c2f.b69a Local Policy: Applying new AAA
override for station
[05/09/14 13:13:18.802 IST 6454 8151] 0017.7c2f.b69a Override Values: source: 16,
valid_bits: 0x0000, qosLevel: -1 dscp: 0xffffffff, dot1pTag: 0xffffffff,
sessionTimeout: -1
[05/09/14 13:13:18.802 IST 6455 8151] 0017.7c2f.b69a dataAvgC: -1, rTAvgC: -1,
dataBurstC: -1 rTimeBurstC: -1, vlanIfName: , aclName:
[05/09/14 13:13:18.802 IST 6456 8151] 0017.7c2f.b69a Local Policy: Applying
override policy
[05/09/14 13:13:18.802 IST 6457 8151] 0017.7c2f.b69a Clearing Dhcp state for
station  ---
[05/09/14 13:13:18.802 IST 6458 8151] 0017.7c2f.b69a Local Policy: Before Applying
WLAN policy AccessVLAN = 12 and SessionTimeout  is 1800 and apfMsTimeout is 1800

[05/09/14 13:13:18.802 IST 6459 8151] 0017.7c2f.b69a Local Policy:Setting Interface
name e VLAN0012

[05/09/14 13:13:18.802 IST 645a 8151] 0017.7c2f.b69a Local Policy:Setting local
bridging VLAN  name VLAN0012 and VLAN ID  12

[05/09/14 13:13:18.802 IST 645b 8151] 0017.7c2f.b69a Applying WLAN ACL policies
to client
[05/09/14 13:13:18.802 IST 645c 8151] 0017.7c2f.b69a No Interface ACL used for
Wireless client in WCM(NGWC)
[05/09/14 13:13:18.802 IST 645d 8151] 0017.7c2f.b69a apfApplyWlanPolicy:
Retaining the ACL recieved in AAA attributes 255 on mobile
[05/09/14 13:13:18.802 IST 645e 8151] 0017.7c2f.b69a Local Policy: After
Applying WLAN policy AccessVLAN = 12 and SessionTimeout  is 1800 and
apfMsTimeout is 1800

[05/09/14 13:13:18.802 IST 645f 8151] 0017.7c2f.b69a Local Policy: After Applying
Site Override  policy AccessVLAN = 12 and SessionTimeout  is 1800 and
apfMsTimeout is 1800

[05/09/14 13:13:18.802 IST 6460 8151] 0017.7c2f.b69a Inserting AAA Override struct
for mobile MAC:  0017.7c2f.b69a , source 16

[05/09/14 13:13:18.802 IST 6461 8151] 0017.7c2f.b69a Inserting new RADIUS override
into chain for station  0017.7c2f.b69a
[05/09/14 13:13:18.802 IST 6462 8151] 0017.7c2f.b69a Override Values: source: 16,
valid_bits: 0x0000, qosLevel: -1 dscp: 0xffffffff, dot1pTag: 0xffffffff,
sessionTimeout: -1
[05/09/14 13:13:18.802 IST 6463 8151] 0017.7c2f.b69a dataAvgC: -1, rTAvgC: -1,
dataBurstC: -1 rTimeBurstC: -1, vlanIfName: , aclName:
[05/09/14 13:13:18.802 IST 6464 8151] 0017.7c2f.b69a Local Policy: After ovr
check continuation
[05/09/14 13:13:18.802 IST 6465 8151] 0017.7c2f.b69a Local Policy:
apf_ms_radius_override.c apfMsSumOverride 447  Returning fail from
apfMsSumOverride
[05/09/14 13:13:18.802 IST 6466 8151] 0017.7c2f.b69a Local Policy: Calling
applyLocalProfilingPolicyAction from Override2
```

```
[05/09/14 13:13:18.802 IST 6467 8151] 0017.7c2f.b69a
 **** Inside applyLocalProfilingPolicyAction ****

[05/09/14 13:13:18.802 IST 6468 8151] 0017.7c2f.b69a *** Client State =
DHCP_REQD instance = 2 instance Name POLICY_PROFILING_L2_AUTH,
OverrideEnable = 1 deviceTypeLen=0, deviceType=(null), userRoleLen=0,
userRole=(null)

[05/09/14 13:13:18.802 IST 6469 8151] 0017.7c2f.b69a     Local Profiling Values :
isValidVlan = 0, vlan = 0, isVlanRecdInDelete = 0, isValidSessionTimeout = 0,
 sessionTimeout=0, isSessionTORecdInDelete = 0  ProtocolMap = 0 ,applyPolicyAtRun= 0
[05/09/14 13:13:18.802 IST 646a 8151] 0017.7c2f.b69a          ipv4ACL = [],
ipv6ACL = [], inQoS = [unknown], outQoS = [unknown]
[05/09/14 13:13:18.802 IST 646b 8151] 0017.7c2f.b69a Local Policy: At the End
AccessVLAN = 12 and SessionTimeout  is 1800 and apfMsTimeout is 1800

[05/09/14 13:13:18.802 IST 646c 8151] 0017.7c2f.b69a apfMsRunStateInc
[05/09/14 13:13:18.802 IST 646d 8151] 0017.7c2f.b69a Session Update for Non-dot1x client

[05/09/14 13:13:18.802 IST 646e 8151] 0017.7c2f.b69a 1XA: Session Push for Non-dot1x
wireless client
[05/09/14 13:13:18.802 IST 646f 8151] 0017.7c2f.b69a 1XA: Calling Auth Mgr to Push
wireless session for client  47ad4000000145 uid 280
 --More--
[05/09/14 13:13:18.802 IST 6470 8151] 0017.7c2f.b69a Session Update for Pushed Sessions

[05/09/14 13:13:18.802 IST 6471 8151] 0017.7c2f.b69a Session Manager Call Client
47ad4000000145, uid 280, capwap id 506c800000000f,Flag 0 Audit-Session ID
0a6987b2536c871300000118 policy name (null)

[05/09/14 13:13:18.802 IST 6472 8151] 0017.7c2f.b69a Change state to RUN (20) last
state DHCP_REQD (7)

[05/09/14 13:13:18.802 IST 6473 8151] 0017.7c2f.b69a WCDB_AUTH: Adding opt82 len 0
[05/09/14 13:13:18.802 IST 6474 8151] 0017.7c2f.b69a WCDB_LLM: prev Mob state 0 curr
Mob State 3 llReq flag 1
[05/09/14 13:13:18.802 IST 6475 8151] 0017.7c2f.b69a WCDB_LLM: prev Mob state 0
currMob State 3 afd action 1
[05/09/14 13:13:18.802 IST 6476 8151] 0017.7c2f.b69a WCDB_LLM: pl handle 259 vlan_id
12 auth RUN(4) mobility 3 client_id 0x47ad4000000145 src_interface 0x506c800000000f
dst_interface 0x75e18000000143 client_type 0 p2p_type 1 bssid c8f9.f983.4260 radio_id
0 wgbid 0000.0000.0000
[05/09/14 13:13:18.802 IST 6477 8151] 0017.7c2f.b69a WCDB_CHANGE: auth=RUN(4) vlan
12 radio 0 client_id 0x47ad4000000145 mobility=ExpForeign(3) src_int 0x506c800000000f
dst_int 0x75e18000000143 ackflag 2 reassoc_client 0 llm_notif 1 ip  0.0.0.0
ip_learn_type 0
[05/09/14 13:13:18.802 IST 6478 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF:
[0017.7c2f.b69a, Ca2] Session update from Client[1] for 0017.7c2f.b69a,
ID list 0x00000000, policy
[05/09/14 13:13:18.802 IST 6479 8151] 0017.7c2f.b69a WCDB_AUTH: Adding opt82 len 0
[05/09/14 13:13:18.802 IST 647a 8151] 0017.7c2f.b69a WCDB_LLM: prev Mob state 3
curr Mob State 3 llReq flag 0
[05/09/14 13:13:18.802 IST 647b 8151] 0017.7c2f.b69a WCDB_CHANGE: auth=RUN(4)
vlan 12 radio 0 client_id 0x47ad4000000145 mobility=ExpForeign(3) src_int
0x506c800000000f dst_int 0x75e18000000143 ackflag 2 reassoc_client 0 llm_notif 0
ip  0.0.0.0 ip_learn_type 0
[05/09/14 13:13:18.802 IST 647c 8151] 0017.7c2f.b69a AAAS: creating accounting start
record using method list Zubair_ISE, passthroughMode 1
[05/09/14 13:13:18.802 IST 647d 8151] 0017.7c2f.b69a AAAS: initialised accounting
start request, uid=280 passthrough=1
[05/09/14 13:13:18.802 IST 647e 8151] 0017.7c2f.b69a AAAS: accounting request sent
[05/09/14 13:13:18.803 IST 647f 207] [WCDB] ==Update event: client (0017.7c2f.b69a)
client id:(0x47ad4000000145) vlan (12->12) global_wlan (15->15) auth_state
(L2_AUTH_DONE->RUN) mob_st<truncated>
```

[05/09/14 13:13:18.803 IST 6480 207] [WCDB] ===intf src/dst
(0x506c800000000f->0x506c800000000f)/(0x0->0x75e18000000143)
radio/bssid (0->0)/(c8f9.f983.4260->c8f9.f983.4260) llm_notify (true) addr v4/v6
(<truncated>
[05/09/14 13:13:18.803 IST 6481 207] [WCDB] Foreign client add. Final llm
notified = false
[05/09/14 13:13:18.803 IST 6482 207] [WCDB] wcdb_client_mcast_update_notify:
No mcast action reqd
[05/09/14 13:13:18.803 IST 6483 207] [WCDB] wcdb_ffcp_wcdb_client_update_notify
client (0017.7c2f.b69a) id 0x47ad4000000145 ffcp update with flags=0x0
[05/09/14 13:13:18.803 IST 6484 207] [WCDB] wcdb_client_state_change_notify:
update flags = 0x3
[05/09/14 13:13:18.803 IST 6485 8151] 0017.7c2f.b69a aaa attribute list length is 79
[05/09/14 13:13:18.803 IST 6486 207] ACCESS-CORE-SM-CLIENT-DOT11-NOTF: [0017.7c2f.b69a]
WCDB RUN notification for 0017.7c2f.b69a
[05/09/14 13:13:18.803 IST 6487 8151] 0017.7c2f.b69a Sending SPI
spi_epm_epm_session_create successfull
[05/09/14 13:13:18.803 IST 6488 8151] 0017.7c2f.b69a 0.0.0.0, auth_state 20
mmRole ExpForeign !!!
[05/09/14 13:13:18.803 IST 6489 8151] 0017.7c2f.b69a 0.0.0.0, auth_state 20 mmRole
ExpForeign, updating wcdb not needed
[05/09/14 13:13:18.803 IST 648a 8151] 0017.7c2f.b69a Tclas Plumb needed: 0
[05/09/14 13:13:18.803 IST 648b 207] [WCDB] wcdb_sisf_client_update_notify:
Notifying SISF to remove assoc in Foreign
[05/09/14 13:13:18.803 IST 648c 207] [WCDB] ==Update event: client (0017.7c2f.b69a)
client id:(0x47ad4000000145) vlan (12->12) global_wlan (15->15) auth_state (RUN->RUN)
mob_st<truncated>
[05/09/14 13:13:18.803 IST 648d 207] [WCDB] ===intf src/dst
(0x506c800000000f->0x506c800000000f)/(0x75e18000000143->0x75e18000000143)
radio/bssid (0->0)/(c8f9.f983.4260->c8f9.f983.4260) llm_notify (false)
addr v4/v6 (<truncated>
[05/09/14 13:13:18.803 IST 648e 207] [WCDB] wcdb_client_mcast_update_notify:
No mcast action reqd
[05/09/14 13:13:18.803 IST 648f 207] [WCDB] wcdb_ffcp_wcdb_client_update_notify
client (0017.7c2f.b69a) id 0x47ad4000000145 ffcp update with flags=0x0
[05/09/14 13:13:18.803 IST 6490 207] [WCDB] wcdb_client_state_change_notify:
update flags = 0x2
[05/09/14 13:13:18.803 IST 6491 207] ACCESS-CORE-SM-CLIENT-DOT11-NOTF:
[0017.7c2f.b69a] WCDB RUN notification for 0017.7c2f.b69a
[05/09/14 13:13:18.803 IST 6492 207] [WCDB] wcdb_sisf_client_update_notify:
Notifying SISF to remove assoc in Foreign
[05/09/14 13:13:18.803 IST 6493 386] [WCDB] wcdb_ffcp_cb: client (0017.7c2f.b69a)
client (0x47ad4000000145): FFCP operation (UPDATE) return code (0)
[05/09/14 13:13:18.803 IST 6494 386] [WCDB] wcdb_ffcp_cb: client (0017.7c2f.b69a)
client (0x47ad4000000145): FFCP operation (UPDATE) return code (0)
[05/09/14 13:13:18.803 IST 6495 243] ACCESS-CORE-SM-SYNC-NOTF: [0017.7c2f.b69a, Ca2]
Delay add/update sync of iif-id for 0017.7c2f.b69a / 0xFE000110
[05/09/14 13:13:18.803 IST 6496 243] ACCESS-CORE-SM-SYNC-NOTF: [0017.7c2f.b69a, Ca2]
Delay add/update sync of audit-session-id for 0017.7c2f.b69a / 0xFE000110
[05/09/14 13:13:18.803 IST 6497 8151] 0017.7c2f.b69a Received session_create_response
for client handle 20175213735969093
[05/09/14 13:13:18.803 IST 6498 8151] 0017.7c2f.b69a Received session_create_response
with EPM session handle 4261413136
[05/09/14 13:13:18.803 IST 6499 8151] 0017.7c2f.b69a Splash Page redirect client
or posture client
 --More--
[05/09/14 13:13:18.803 IST 649a 8151] 0017.7c2f.b69a REDIRECT ACL present in the
attribute list
[05/09/14 13:13:18.803 IST 649b 8151] 0017.7c2f.b69a Setting AAA Override
Url-Redirect-Acl 'REDIRECT'
**[05/09/14 13:13:18.803 IST 649c 8151] 0017.7c2f.b69a AAA Override Url-Redirect-Acl
'REDIRECT'**
**[05/09/14 13:13:18.803 IST 649d 8151] 0017.7c2f.b69a AAA Override Url-Redirect
'https://10.106.73.69:8443/guestportal/gateway?sessionId=0a6987b2536c871300000118&action=cwa'**

set
[05/09/14 13:13:18.803 IST 649e 8151] 0017.7c2f.b69a Wireless Client mobility role is not ExportAnchor/Local. Hence we are not sending request to EPM
[05/09/14 13:13:20.445 IST 649f 8151] 0017.7c2f.b69a WCDB_IP_UPDATE: new ipv4 0.0.0.0 ip_learn_type 0 deleted ipv4 0.0.0.0
[05/09/14 13:13:20.446 IST 64a0 207] [WCDB] wcdb_foreign_client_ip_addr_update: Foreign client (0017.7c2f.b69a) ip addr update received.
[05/09/14 13:13:20.446 IST 64a1 207] [WCDB] SISF Update: IPV6 Addr[0] : fe80::6c1a:b253:d711:c7f
[05/09/14 13:13:20.446 IST 64a2 207] [WCDB] SISF Update : Binding delete status for V6: = 0
[05/09/14 13:13:20.446 IST 64a3 207] [WCDB] wcdb_sisf_client_update_notify: Notifying SISF to remove assoc in Foreign
[05/09/14 13:13:20.448 IST 64a4 8151] 0017.7c2f.b69a MS got the IP, resetting the Reassociation Count 0 for client
[05/09/14 13:13:20.448 IST 64a5 8151] 0017.7c2f.b69a AAAS: creating accounting interim record using method list Zubair_ISE, passthroughMode 1
[05/09/14 13:13:20.449 IST 64a6 8151] 0017.7c2f.b69a AAAS: initialised accounting interim request, uid=280 passthrough=1
[05/09/14 13:13:20.449 IST 64a7 8151] 0017.7c2f.b69a AAAS: accounting request sent
[05/09/14 13:13:20.449 IST 64a8 8151] 0017.7c2f.b69a Guest User() assigned IP Address (10.105.135.190)
[05/09/14 13:13:20.449 IST 64a9 8151] 0017.7c2f.b69a Assigning Address 10.105.135.190 to mobile
[05/09/14 13:13:20.449 IST 64aa 8151] 0017.7c2f.b69a WCDB_IP_UPDATE: new ipv4 10.105.135.190 ip_learn_type DHCP deleted ipv4 0.0.0.0
[05/09/14 13:13:20.449 IST 64ab 8151] 0017.7c2f.b69a AAAS: creating accounting interim record using method list Zubair_ISE, passthroughMode 1
[05/09/14 13:13:20.449 IST 64ac 8151] 0017.7c2f.b69a AAAS: initialised accounting interim request, uid=280 **passthrough=1**
[05/09/14 13:13:20.449 IST 64ad 8151] 0017.7c2f.b69a AAAS: accounting request sent
[05/09/14 13:13:20.449 IST 64ae 8151] 0017.7c2f.b69a 10.105.135.190, auth_state 20 mmRole ExpForeign !!!
[05/09/14 13:13:20.449 IST 64af 207] [WCDB] wcdb_foreign_client_ip_addr_update: Foreign client (0017.7c2f.b69a) ip addr update received.
[05/09/14 13:13:20.449 IST 64b0 8151] 0017.7c2f.b69a 10.105.135.190, auth_state 20 mmRole ExpForeign, updating wcdb not needed
[05/09/14 13:13:20.449 IST 64b1 8151] 0017.7c2f.b69a Tclas Plumb needed: 0
[05/09/14 13:13:20.449 IST 64b2 207] [WCDB] SISF Update: IPV6 Addr[0] : fe80::6c1a:b253:d711:c7f
[05/09/14 13:13:20.449 IST 64b3 207] [WCDB] SISF Update : Binding delete status for V6: = 0
[05/09/14 13:13:20.449 IST 64b4 207] [WCDB] wcdb_sisf_client_update_notify: Notifying SISF to remove assoc in Foreign
[05/09/14 13:13:20.449 IST 64b5 243] ACCESS-CORE-SM-SYNC-NOTF: [0017.7c2f.b69a, Ca2] Delay add/update sync of addr for 0017.7c2f.b69a / 0xFE000110
[05/09/14 13:13:49.429 IST 64b6 253] ACCESS-CORE-SM-CLIENT-SPI-NOTF: [0017.7c2f.b69a, Ca2] Session authz update requested cmd 5, mac 0017.7c2f.b69a, attr-list 0x0 for Client[1]
[05/09/14 13:13:49.430 IST 64b7 253] ACCESS-CORE-SM-CLIENT-SPI-NOTF: [0017.7c2f.b69a, Ca2] Session authz update request sent to Client[1]
[05/09/14 13:13:49.430 IST 64b8 8151] 0017.7c2f.b69a 1XA: Processing update request from dot1x. COA type 5
[05/09/14 13:13:49.430 IST 64b9 8151] 0017.7c2f.b69a AAAS: authorization init, uid=280, context=268
[05/09/14 13:13:49.430 IST 64ba 8151] 0017.7c2f.b69a AAAS: initialised auth request, uinque id=280, context id = 268, context reqHandle 0xfefc172c
[05/09/14 13:13:49.430 IST 64bb 8151] 0017.7c2f.b69a AAAS: Submitting mac filter request for user 00177c2fb69a, uniqueId=280 mlist=MACFILTER
[05/09/14 13:13:49.430 IST 64bc 8151] 0017.7c2f.b69a AAAS: auth request sent
[05/09/14 13:13:49.430 IST 64bd 8151] 0017.7c2f.b69a processing COA type 5
 was successful
[05/09/14 13:13:49.430 IST 64be 8151] 0017.7c2f.b69a processing COA type 5
 was successful
[05/09/14 13:13:49.430 IST 64bf 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF: [0017.7c2f.b69a, Ca2] Session authz update response received for Client[1]

[05/09/14 13:13:49.430 IST 64c0 211] Parsed CLID MAC Address = 0:23:124:47:182:154
[05/09/14 13:13:49.430 IST 64c1 211] AAA SRV(00000118): process author req
[05/09/14 13:13:49.430 IST 64c2 211] AAA SRV(00000118): **Author method=SERVER_GROUP Zubair_ISE**
[05/09/14 13:13:49.430 IST 64c3 211] Parsed CLID MAC Address = 0:23:124:47:182:154
[05/09/14 13:13:49.430 IST 64c4 211] AAA SRV(00000000): process response req
[05/09/14 13:13:49.469 IST 64c5 220] **AAA SRV(00000118): protocol reply PASS for Authorization**
[05/09/14 13:13:49.469 IST 64c6 220] **AAA SRV(00000118): Return Authorization status=PASS**
[05/09/14 13:13:49.469 IST 64c7 8151] 0017.7c2f.b69a AAAS: received response, cid=268
[05/09/14 13:13:49.469 IST 64c8 8151] 0017.7c2f.b69a AAAS: deleting context, cid=268
[05/09/14 13:13:49.469 IST 64c9 8151] 0017.7c2f.b69a Not comparing because the ACLs have not been sent yet.
[05/09/14 13:13:49.469 IST 64ca 8151] 0017.7c2f.b69a Final flag values are, epmSendAcl 1, epmSendAclDone 0
[05/09/14 13:13:49.469 IST 64cb 8151] 0017.7c2f.b69a client incoming attribute size are 77
 --More--
[05/09/14 13:13:49.469 IST 64cc 8151] 0017.7c2f.b69a AAAS: mac filter callback status=0 uniqueId=280
[05/09/14 13:13:49.469 IST 64cd 8151] 0017.7c2f.b69a Local Policy: At the start of apfApplyOverride2. Client State RUN

[05/09/14 13:13:49.469 IST 64ce 8151] 0017.7c2f.b69a Applying new AAA override for station 0017.7c2f.b69a
[05/09/14 13:13:49.469 IST 64cf 8151] 0017.7c2f.b69a Local Policy: Applying new AAA override for station
[05/09/14 13:13:49.469 IST 64d0 8151] 0017.7c2f.b69a Override Values: source: 2, valid_bits: 0x0000, qosLevel: -1 dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1
[05/09/14 13:13:49.469 IST 64d1 8151] 0017.7c2f.b69a dataAvgC: -1, rTAvgC: -1, dataBurstC: -1 rTimeBurstC: -1, vlanIfName: , aclName:
[05/09/14 13:13:49.469 IST 64d2 8151] 0017.7c2f.b69a Local Policy: Applying override policy
[05/09/14 13:13:49.469 IST 64d3 8151] 0017.7c2f.b69a Clearing Dhcp state for station ---
[05/09/14 13:13:49.469 IST 64d4 8151] 0017.7c2f.b69a Local Policy: Before Applying WLAN policy AccessVLAN = 12 and SessionTimeout is 1800 and apfMsTimeout is 1800

[05/09/14 13:13:49.469 IST 64d5 8151] 0017.7c2f.b69a Local Policy:Setting Interface name e VLAN0012

[05/09/14 13:13:49.469 IST 64d6 8151] 0017.7c2f.b69a Local Policy:Setting local bridging VLAN name VLAN0012 and VLAN ID 12

[05/09/14 13:13:49.469 IST 64d7 8151] 0017.7c2f.b69a Applying WLAN ACL policies to client
[05/09/14 13:13:49.469 IST 64d8 8151] 0017.7c2f.b69a No Interface ACL used for Wireless client in WCM(NGWC)
[05/09/14 13:13:49.469 IST 64d9 8151] 0017.7c2f.b69a apfApplyWlanPolicy: Retaining the ACL recieved in AAA attributes 255 on mobile
[05/09/14 13:13:49.469 IST 64da 8151] 0017.7c2f.b69a Local Policy: After Applying WLAN policy AccessVLAN = 12 and SessionTimeout is 1800 and apfMsTimeout is 1800

[05/09/14 13:13:49.469 IST 64db 8151] 0017.7c2f.b69a Local Policy: After Applying Site Override policy AccessVLAN = 12 and SessionTimeout is 1800 and apfMsTimeout is 1800

[05/09/14 13:13:49.469 IST 64dc 8151] 0017.7c2f.b69a Inserting AAA Override struct for mobile
   MAC: 0017.7c2f.b69a , source 2

[05/09/14 13:13:49.469 IST 64dd 8151] 0017.7c2f.b69a Inserting new RADIUS override into chain for station 0017.7c2f.b69a
[05/09/14 13:13:49.469 IST 64de 8151] 0017.7c2f.b69a Override Values: source: 2, valid_bits: 0x0000, qosLevel: -1 dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1
[05/09/14 13:13:49.469 IST 64df 8151] 0017.7c2f.b69a dataAvgC: -1, rTAvgC: -1, dataBurstC: -1 rTimeBurstC: -1, vlanIfName: , aclName:
[05/09/14 13:13:49.469 IST 64e0 8151] 0017.7c2f.b69a Local Policy: After ovr check continuation

[05/09/14 13:13:49.469 IST 64e1 8151] 0017.7c2f.b69a Local Policy: apf_ms_radius_override.c apfMsSumOverride 447 Returning fail from apfMsSumOverride
[05/09/14 13:13:49.469 IST 64e2 8151] 0017.7c2f.b69a Local Policy: Calling applyLocalProfilingPolicyAction from Override2

[05/09/14 13:13:49.469 IST 64e3 8151] 0017.7c2f.b69a
**** Inside applyLocalProfilingPolicyAction ****

[05/09/14 13:13:49.469 IST 64e4 8151] 0017.7c2f.b69a *** Client State = RUN instance = 2 instance Name POLICY_PROFILING_L2_AUTH, OverrideEnable = 1 deviceTypeLen=0, deviceType=(null), userRoleLen=0, userRole=(null)

[05/09/14 13:13:49.469 IST 64e5 8151] 0017.7c2f.b69a   Local Profiling Values : isValidVlan = 0, vlan = 0, isVlanRecdInDelete = 0, isValidSessionTimeout = 0,
 sessionTimeout=0, isSessionTORecdInDelete = 0 ProtocolMap = 0 ,applyPolicyAtRun= 0
[05/09/14 13:13:49.469 IST 64e6 8151] 0017.7c2f.b69a   ipv4ACL = [], ipv6ACL = [], inQoS = [unknown], outQoS = [unknown]
[05/09/14 13:13:49.469 IST 64e7 8151] 0017.7c2f.b69a Local Policy: At the End AccessVLAN = 12 and SessionTimeout is 1800 and apfMsTimeout is 1800

[05/09/14 13:13:49.469 IST 64e8 8151] 0017.7c2f.b69a In >= L2AUTH_COMPLETE for station 0017.7c2f.b69a
[05/09/14 13:13:49.469 IST 64e9 8151] 0017.7c2f.b69a AAAS: creating accounting interim record using method list Zubair_ISE, passthroughMode 1
[05/09/14 13:13:49.469 IST 64ea 8151] 0017.7c2f.b69a AAAS: initialised accounting interim request, uid=280 passthrough=1
[05/09/14 13:13:49.469 IST 64eb 8151] 0017.7c2f.b69a AAAS: accounting request sent
[05/09/14 13:13:49.469 IST 64ec 8151] 0017.7c2f.b69a Not Using WMM Compliance code qosCap 00
[05/09/14 13:13:49.469 IST 64ed 8151] 0017.7c2f.b69a In SPI call for >= L2AUTH_COMPLETE for station 0017.7c2f.b69a
[05/09/14 13:13:49.469 IST 64ee 8151] 0017.7c2f.b69a WCDB_AUTH: Adding opt82 len 0
[05/09/14 13:13:49.469 IST 64ef 8151] 0017.7c2f.b69a WCDB_LLM: prev Mob state 3 curr Mob State 3 llReq flag 0
[05/09/14 13:13:49.469 IST 64f0 8151] 0017.7c2f.b69a WCDB_CHANGE: auth=RUN(4) vlan 12 radio 0 client_id 0x47ad4000000145 mobility=ExpForeign(3) src_int 0x506c800000000f dst_int 0x75e18000000143 ackflag 2 reassoc_client 0 llm_notif 0 ip 10.105.135.190 ip_learn_type DHCP
 --More--
[05/09/14 13:13:49.469 IST 64f1 8151] 0017.7c2f.b69a apfMsAssoStateInc
[05/09/14 13:13:49.469 IST 64f2 8151] 0017.7c2f.b69a apfPemAddUser2 (apf_policy.c:197) Changing state for mobile 0017.7c2f.b69a on AP c8f9.f983.4260 from AAA Pending to Associated

[05/09/14 13:13:49.469 IST 64f3 8151] 0017.7c2f.b69a Reason code 0, Preset 4, AAA cause 1
[05/09/14 13:13:49.469 IST 64f4 8151] 0017.7c2f.b69a Scheduling deletion of Mobile Station:
 (callerId: 49) in 1800 seconds
[05/09/14 13:13:49.469 IST 64f5 8151] 0017.7c2f.b69a Ms Timeout = 1800, Session Timeout = 1800

[05/09/14 13:13:49.469 IST 64f6 207] [WCDB] ==Update event: client (0017.7c2f.b69a) client id:(0x47ad4000000145) vlan (12->12) global_wlan (15->15) auth_state (RUN->RUN) mob_st<truncated>
[05/09/14 13:13:49.469 IST 64f7 207] [WCDB] ===intf src/dst (0x506c800000000f->0x506c800000000f)/(0x75e18000000143->0x75e18000000143) radio/bssid (0->0)/(c8f9.f983.4260->c8f9.f983.4260) llm_notify (false) addr v4/v6 (<truncated>
[05/09/14 13:13:49.469 IST 64f8 207] [WCDB] wcdb_client_mcast_update_notify: No mcast action reqd
[05/09/14 13:13:49.469 IST 64f9 207] [WCDB] wcdb_ffcp_wcdb_client_update_notify client (0017.7c2f.b69a) id 0x47ad4000000145 ffcp update with flags=0x0
[05/09/14 13:15:47.411 IST 650a 8151] 0017.7c2f.b69a Acct-interim update sent for station 0017.7c2f.b69a
[05/09/14 13:16:38.431 IST 650b 8151] 0017.7c2f.b69a
Client stats update: Time now in sec 1399621598, Last Acct Msg Sent at 1399621547 sec

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).