

Configuración de la Autenticación Web Central con Anclaje en Catalyst 9800

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configure un Catalyst 9800 anclado a otro Catalyst 9800](#)

[Diagrama de la red](#)

[Configuración de AAA en ambos 9800](#)

[Configure las WLAN en los WLC](#)

[Cree el perfil de política y la etiqueta de política en el WLC externo](#)

[Cree el perfil de política en el WLC de anclaje](#)

[Redirigir configuración de ACL en ambos 9800](#)

[Configuración de ISE](#)

[Configure un Catalyst 9800 anclado a un WLC AireOS](#)

[Configuración externa de Catalyst 9800](#)

[Configuraciones AAA en el WLC AireOS de anclaje](#)

[Configuración WLAN en el WLC AireOS](#)

[Redirigir ACL en el WLC AireOS](#)

[Configuración de ISE](#)

[Diferencias en la configuración cuando el WLC de AireOS es el externo y el Catalyst 9800 es el ancla](#)

[Verificación](#)

[Troubleshoot](#)

[Información de Troubleshooting de Catalyst 9800](#)

[Detalles del cliente](#)

[Captura de paquetes integrada](#)

[Rastreo de RadioActive](#)

[Información de resolución de problemas de AireOS](#)

[Detalles del cliente](#)

[Depuraciones desde la CLI](#)

[Referencias](#)

Introducción

Este documento describe cómo configurar y resolver problemas de autenticación web central (CWA) en el Catalyst 9800 que apunta a otro controlador de LAN inalámbrica (WLC) como ancla de movilidad, que abarca el destino con AireOS u otro WLC 9800.

Prerequisites

Requirements

Se recomienda que tenga una comprensión básica del WLC 9800, AireOS WLC y Cisco ISE. Se asume que antes de iniciar la configuración de anclaje de CWA ya ha activado el túnel de movilidad entre los dos WLC. Esto está fuera del alcance de este ejemplo de configuración. Si necesita ayuda con esto, consulte el documento titulado "[Creación de túneles de movilidad en los controladores Catalyst 9800](#)"

Componentes Utilizados

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

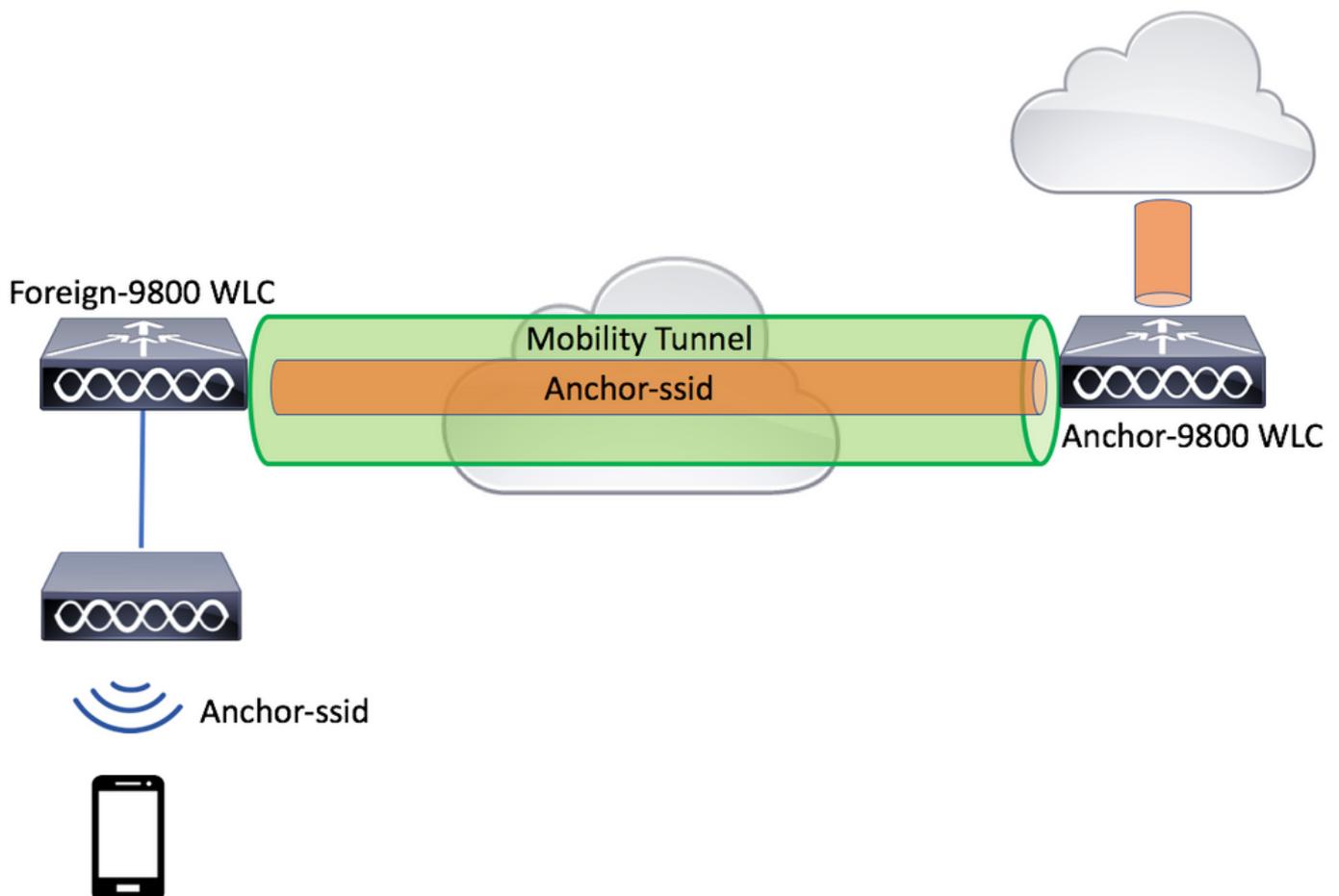
9800 17.2.1

5520 8.5.164 Imagen IRCM

ISE 2.4

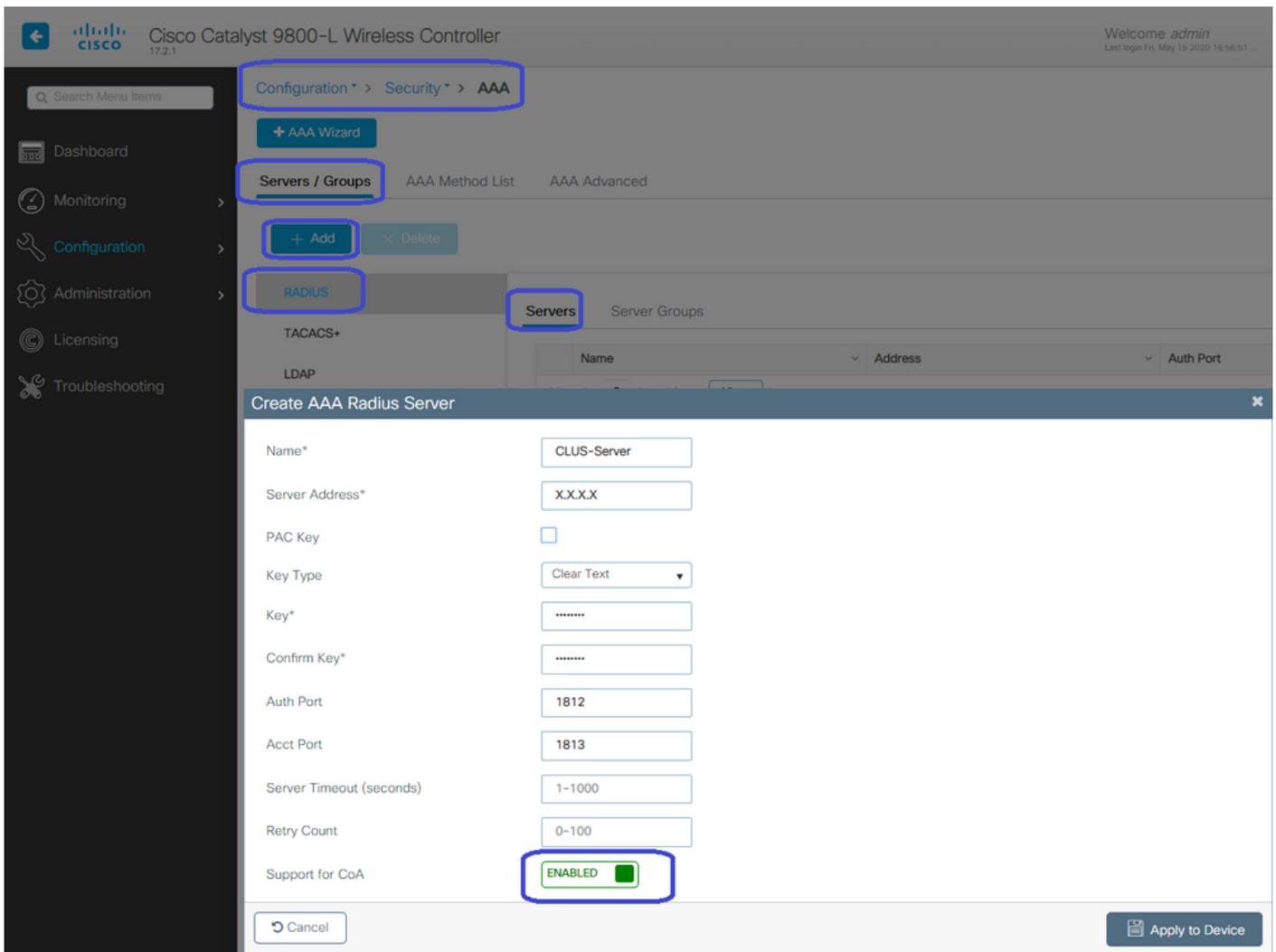
Configure un Catalyst 9800 anclado a otro Catalyst 9800

Diagrama de la red



Configuración de AAA en ambos 9800

Tanto en el anclaje como en el externo deberá agregar primero el servidor RADIUS y asegurarse de que la CoA esté habilitada. Esto se puede hacer en el menú **Configuration>Security>AAA>Servers/Groups>Server>** Haga clic en el botón **Add**



Ahora tendrá que crear un grupo de servidores y colocar el servidor que acaba de configurar en ese grupo. Esto se hace aquí **Configuration>Security>AAA>Servers/Groups>Server Groups>+Add**.

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller configuration page. The breadcrumb navigation is **Configuration > Security > AAA**. The **Servers / Groups** tab is selected, and the **Server Groups** sub-tab is active. A **Create AAA Radius Server Group** dialog box is open, showing the following configuration:

- Name*: CLUS-Server-Group
- Group Type: RADIUS
- MAC-Delimiter: none
- MAC-Filtering: none
- Dead-Time (mins): 1-1440

The **Assigned Servers** list contains **CLUS-Server**. The **Apply to Device** button is visible at the bottom right.

Ahora, cree una lista de métodos de **autorización** (no se requiere una lista de métodos de autenticación para CWA) donde el tipo es red y el tipo de grupo es group. Agregue el grupo de servidores de la acción anterior a esta lista de métodos.

Esta configuración se realiza aquí **Configuration>Security>AAA>Servers/AAA Method List>Authorization>+Add**

The screenshot displays the Cisco Catalyst 9800-L Wireless Controller configuration interface. The breadcrumb navigation at the top reads "Configuration > Security > AAA". The left sidebar contains navigation options: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area shows the "AAA Method List" configuration page. The "Authentication" tab is selected, and the "Authorization" sub-tab is active. A "+ Add" button is highlighted. Below this, a "Quick Setup: AAA Authorization" dialog box is open. The dialog contains the following fields and options:

- Method List Name*: CLUS-AuthZ-Meth-List
- Type*: network
- Group Type: group
- Fallback to local:
- Authenticated:
- Available Server Groups: radius, ldap, tacacs+, ISE1
- Assigned Server Groups: CLUS-Server-Group

At the bottom of the dialog, there are "Cancel" and "Apply to Device" buttons.

(Opcional) Cree una lista de métodos de contabilidad utilizando el mismo grupo de servidores que la lista de métodos de autorización. La lista de contabilidad se puede crear aquí **Configuration>Security>AAA>Servers/AAA Method List>Accounting>+Add**

The screenshot displays the Cisco Catalyst 9800-L Wireless Controller configuration interface. The breadcrumb navigation at the top reads "Configuration > Security > AAA". The left sidebar shows the navigation menu with "Configuration" selected. The main content area is titled "AAA Method List" and includes a "+ Add" button. A modal window titled "Quick Setup: AAA Accounting" is open, showing the following configuration details:

- Method List Name*: CLUS-Acct-Meth-List
- Type*: identity
- Available Server Groups: radius, ldap, tacacs+, ISE1
- Assigned Server Groups: CLUS-Server-Group

Buttons for "Cancel" and "Apply to Device" are visible at the bottom of the modal.

Configure las WLAN en los WLC

Cree y configure las WLAN en ambos WLC. Las WLAN deben coincidir en ambos. El tipo de seguridad debe ser el filtrado mac y se debe aplicar la lista de métodos de autorización del paso anterior. Esta configuración se realiza en **Configuración>Etiquetas y perfiles>WLANs>+Agregar**

Cisco Catalyst 9800-L Wireless Controller 17.2.1

Configuration > Tags & Profiles > WLANs

+ Add Delete Enable WLAN Disable WLAN

Number of WLANs selected : 0

Status	Name	ID
--------	------	----

Add WLAN

General Security Advanced

Profile Name* Radio Policy

SSID* Broadcast SSID

WLAN ID*

Status

Cancel Apply to Device

Cisco Catalyst 9800-L Wireless Controller 17.2.1

Configuration > Tags & Profiles > WLANs

+ Add Delete Enable WLAN Disable WLAN

Number of WLANs selected : 0

Status	Name	ID
--------	------	----

Add WLAN

General Security Advanced

Layer2 Layer3 AAA

Layer 2 Security Mode Lobby Admin Access

MAC Filtering Fast Transition

OWE Transition Mode Over the DS

Authorization List* Reassociation Timeout

Cancel Apply to Device

Cree el perfil de política y la etiqueta de política en el WLC externo

Vaya a la interfaz de usuario web del WLC externo.

Para crear el perfil de política, vaya a **Configuration>Tags & Profiles>Policy>+Add**

Al anclar, debe utilizar el switching central.

The screenshot displays the Cisco Catalyst 9800-L Wireless Controller web interface. The breadcrumb navigation path is **Configuration > Tags & Profiles > Policy**. The **+ Add** button is highlighted. The **Add Policy Profile** dialog is open, showing the **General** tab. A warning message states: "Configuring in enabled state will result in loss of connectivity for clients associated with this profile." The **Name*** is **CLUS-Policy-Profile**, **Description** is **Policy Profile for CLUS**, and **Status** is **ENABLED**. The **WLAN Switching Policy** section is highlighted, showing **Central Switching**, **Central Authentication**, **Central DHCP**, and **Central Association** all set to **ENABLED**, and **Flex NAT/PAT** set to **DISABLED**. The **CTS Policy** section includes **Inline Tagging**, **SGACL Enforcement**, and **Default SGT** (set to **2-65519**). The **Apply to Device** button is visible at the bottom right.

En la ficha "Avanzado", la anulación de AAA y RADIUS NAC son obligatorias para CWA. Aquí también puede aplicar la lista de métodos de contabilidad si decide hacerlo.

Configuration > Tags & Profiles > Policy

+ Add × Delete

Status Policy Profile Name Description

Add Policy Profile

General Access Policies QOS and AVC Mobility **Advanced**

WLAN Timeout

Session Timeout (sec) 1800

Idle Timeout (sec) 300

Idle Threshold (bytes) 0

Client Exclusion Timeout (sec) 60

Guest LAN Session Timeout

DHCP

IPv4 DHCP Required

DHCP Server IP Address

Show more >>>

AAA Policy

Allow AAA Override

NAC State

NAC Type RADIUS

Policy Name default-aaa-policy x

Accounting List CLUS-Acct-Meth-x

Fabric Profile Search or Select

mDNS Service Policy Search or Select

Hotspot Server Search or Select

User Private Network

Status

Drop Unicast

Umbrella

Umbrella Parameter Map Not Configured Clear

Flex DHCP Option for DNS **ENABLED**

DNS Traffic Redirect **IGNORE**

WLAN Flex Policy

VLAN Central Switching

Split MAC ACL Search or Select

Air Time Fairness Policies

2.4 GHz Policy Search or Select

En la pestaña "Movilidad" **NO** marque la casilla de verificación "exportar anclaje" sino más bien agregue el WLC de anclaje a la lista de anclaje. Asegúrese de pulsar "Aplicar al dispositivo". Como recordatorio, esto supone que ya tiene una configuración de túnel de movilidad entre los dos controladores

Cisco Catalyst 9800-L Wireless Controller

Configuration > Tags & Profiles > Policy

+ Add × Delete

Status Policy Profile Name Description

Add Policy Profile

General Access Policies QOS and AVC **Mobility** Advanced

Mobility Anchors

Export Anchor

Static IP Mobility **DISABLED**

Adding Mobility Anchors will cause the enabled VLANs to momentarily disable and may result in loss of connectivity for some clients.

Drag and Drop/double click/click on the arrow to add/remove Anchors

Available (0)

Anchor IP

No anchors available

Selected (1)

Anchor IP	Anchor Priority
192.168.160.18	Primary (1)

Cancel Apply to Device

Para que los APs usen este perfil de política, necesitará crear una etiqueta de política y aplicarla a

los APs que desea utilizar.

Para crear la etiqueta de política, vaya a **Configuration>Tags & Profiles>Tags?Policy>+Add**

The screenshot displays the Cisco Catalyst 9800-L Wireless Controller configuration page. The breadcrumb navigation at the top reads "Configuration > Tags & Profiles > Tags". The "Policy" tab is selected, and the "+ Add" button is highlighted. A modal dialog titled "Add Policy Tag" is open, showing the following fields: "Name*" with the value "CLUS-Policy-Tag" and "Description" with the value "Policy Tag for CLUS". Below these fields, it indicates "WLAN-POLICY Maps: 0" and shows another "+ Add" button. A table with columns "WLAN Profile" and "Policy Profile" is shown, with "0" items per page and "No items to display". The "Map WLAN and Policy" section contains two dropdown menus: "WLAN Profile*" set to "CLUS-WLAN-Name" and "Policy Profile*" set to "CLUS-Policy-Profile". A checkmark button is highlighted. At the bottom of the dialog, there are "Cancel" and "Apply to Device" buttons, with the latter being highlighted.

Para agregar esto a varios AP al mismo tiempo, vaya a **Configuration>Wireless Setup>Advanced>Start Now**. Haga clic en las barras de viñetas junto a "Tag APs" y agregue la etiqueta a los AP que elija.

Configuration > Wireless Setup > Advanced

+ Tag APs

Number of APs: 3
Selected Number of APs: 3

AP Name	AP Model	AP MAC	AP Mode
<input checked="" type="checkbox"/> Jays2800	AIR-AP2802I-B-K9	002a.10f3.6b60	Local
<input checked="" type="checkbox"/> Jays3800	AIR-AP3802I-B-K9	70b3.1755.0520	Local
<input checked="" type="checkbox"/> AP0062.ec20.122c	AIR-CAP2702I-B-K9	cc16.7e6c.3cf0	Local

1 10 items per page

Tag APs

Tags

Policy: CLUS-Policy-Tag

Site: Search or Select

RF: Search or Select

Changing AP Tag(s) will cause associated AP(s) to reconnect

Cancel Apply to Device

Cree el perfil de política en el WLC de anclaje

Vaya a la interfaz de usuario web del WLC de anclaje. Agregue el perfil de política en el anclaje 9800 bajo **Configuración>Etiquetas y perfiles>Etiquetas>Política>+Agregar**. Asegúrese de que coincide con el perfil de política hecho en el externo excepto para la pestaña de movilidad y la lista de contabilidad.

Aquí no agrega un anclaje, pero sí marca la casilla de verificación "Exportar anclaje". No agregue la lista de cuentas aquí. Como recordatorio, esto supone que ya tiene una configuración de túnel de movilidad entre los dos controladores

Nota: No hay razón para asociar este perfil a una WLAN en una etiqueta de política. Esto creará problemas si lo hace. Si desea utilizar la misma WLAN para AP en este WLC, cree otro perfil de política para él.

← Cisco 17.2.1 Cisco Catalyst 9800-L Wireless Controller

Configuration > Tags & Profiles > Policy

+ Add × Delete

Add Policy Profile

General Access Policies QOS and AVC **Mobility** Advanced

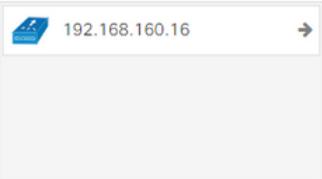
Mobility Anchors

Export Anchor

Static IP Mobility DISABLED

Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients.

Drag and Drop/double click/click on the arrow to add/remove Anchors

Available (1)	Selected (0)	
Anchor IP	Anchor IP	Anchor Priority
 192.168.160.16 →	Anchors not assigned	

Cancel Apply to Device

Redirigir configuración de ACL en ambos 9800

A continuación, debe crear la configuración de ACL de redirección en ambos 9800. Las entradas en el Foreign no importan ya que será el WLC de anclaje que aplica la ACL al tráfico. El único requisito es que esté allí y tenga alguna entrada. Las entradas en el ancla tienen que "denegar" el acceso a ISE en el puerto 8443 y "permitir" todo lo demás. Esta ACL sólo se aplica al tráfico que llega "dentro" del cliente, por lo que no se necesitan reglas para el tráfico de retorno. DHCP y DNS pasarán sin entradas en la ACL.

Cisco Catalyst 9800-L Wireless Controller 17.2.1 Welcome admin
Last login None

Configuration > Security > ACL

+ Add - Delete Associate Interfaces

Add ACL Setup

ACL Name* ACL Type

Rules

Sequence* Action

Source Type

Destination Type

Protocol

Log DSCP

Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
<input type="checkbox"/> 10	deny	any		192.168.160.99		tcp	None	eq 8443	None	Disabled
<input type="checkbox"/> 100	permit	any		any		ip	None	None	None	Disabled

10 items per page 1 - 2 of 2 items

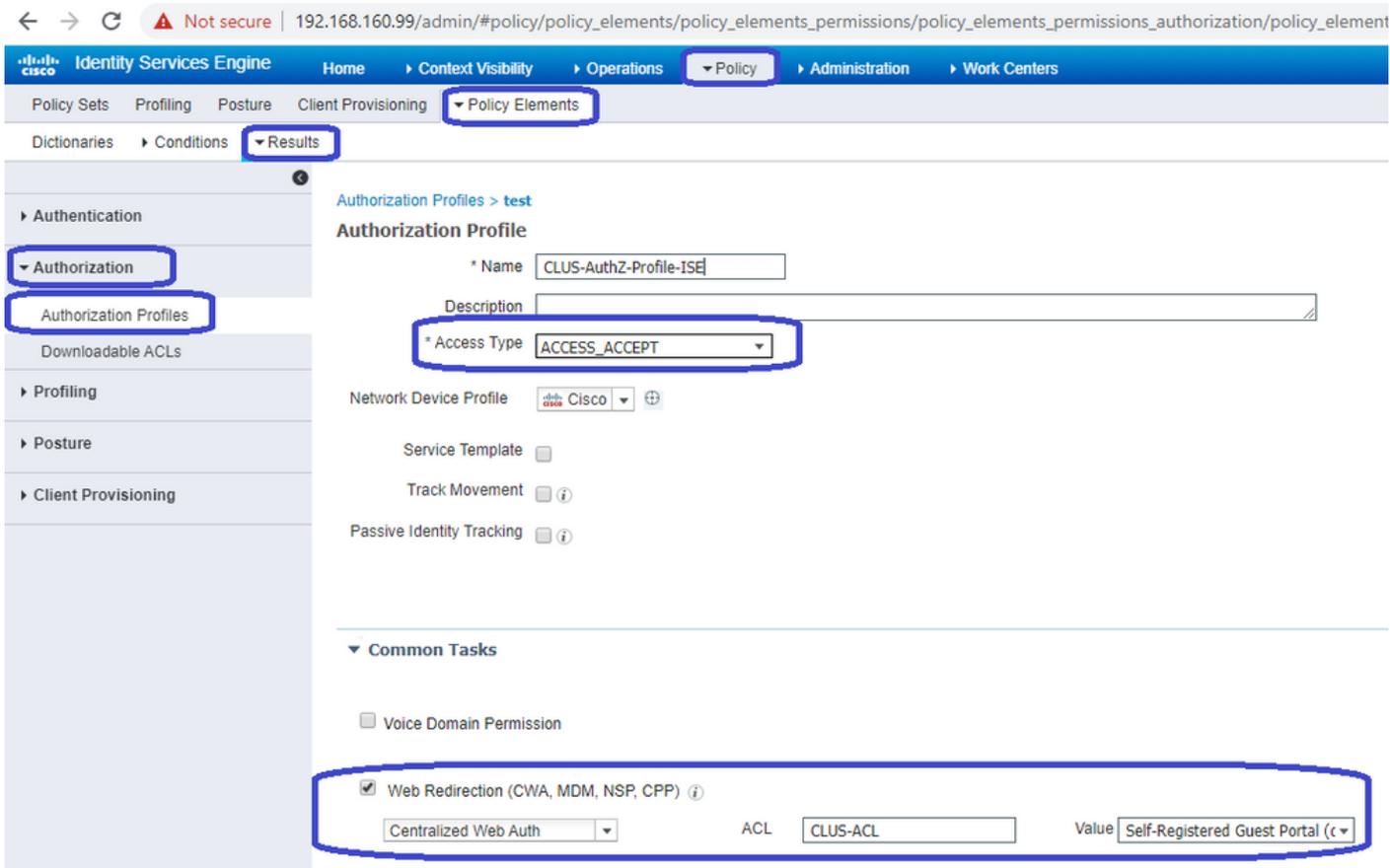
Cancel Apply to Device

Configuración de ISE

El último paso es configurar ISE para CWA. Hay muchas opciones para esto, pero este ejemplo se ceñirá a lo básico y usará el portal de invitados autoregistrado predeterminado.

En ISE, debe crear un perfil de autorización, un conjunto de políticas con una política de autenticación y una política de autorización que utilice el perfil de autorización, agregar el 9800(external) a ISE como dispositivo de red y crear un nombre de usuario y una contraseña para iniciar sesión en la red.

Para crear el perfil de autorización, vaya a **Policy>Policy Elements>Authorization>Results>Authorization Profiles**, a continuación, haga clic en **Add**. Asegúrese de que el tipo de acceso devuelto es "access_accept" y, a continuación, establezca los AVP(pares valor-atributo) que desea devolver. Para CWA, la ACL de redirección y la URL de redirección son obligatorias, pero también puede enviar cosas como el ID de VLAN y el tiempo de espera de sesión. Es importante que el nombre de la ACL coincida con el nombre de la ACL de redirección en el externo y el 9800 de anclaje.

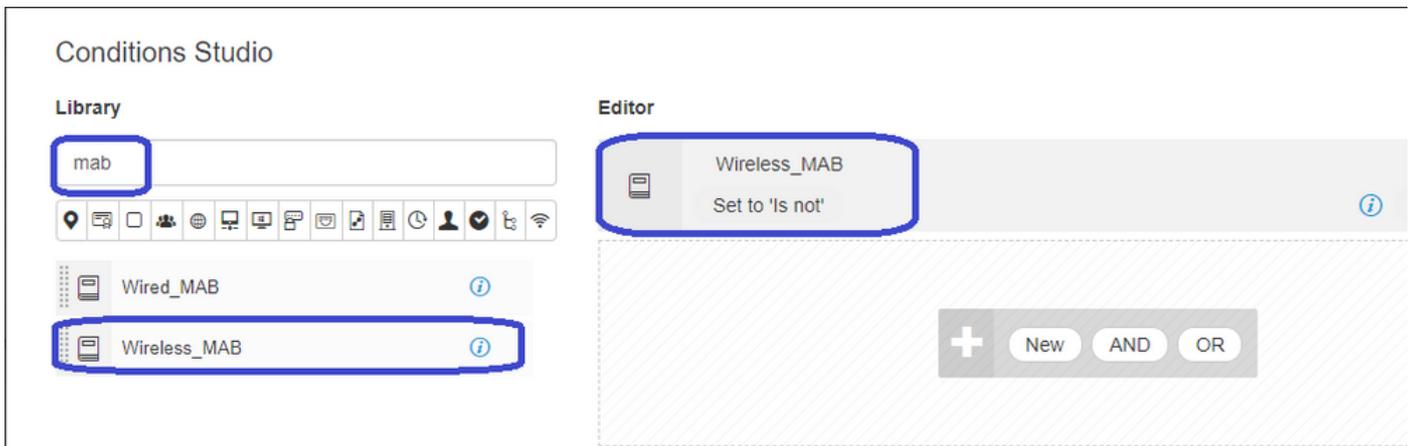


A continuación, debe configurar una forma de aplicar el perfil de autorización que acaba de crear a los clientes que pasan por CWA. Para lograrlo, una manera es crear un conjunto de políticas que omita la autenticación cuando se usa MAB y aplicar el perfil de autorización cuando se usa el SSID enviado en el ID de estación llamada. De nuevo, hay muchas maneras de lograrlo, así que si necesita algo más específico o más seguro, esta es la forma más simple de hacerlo.

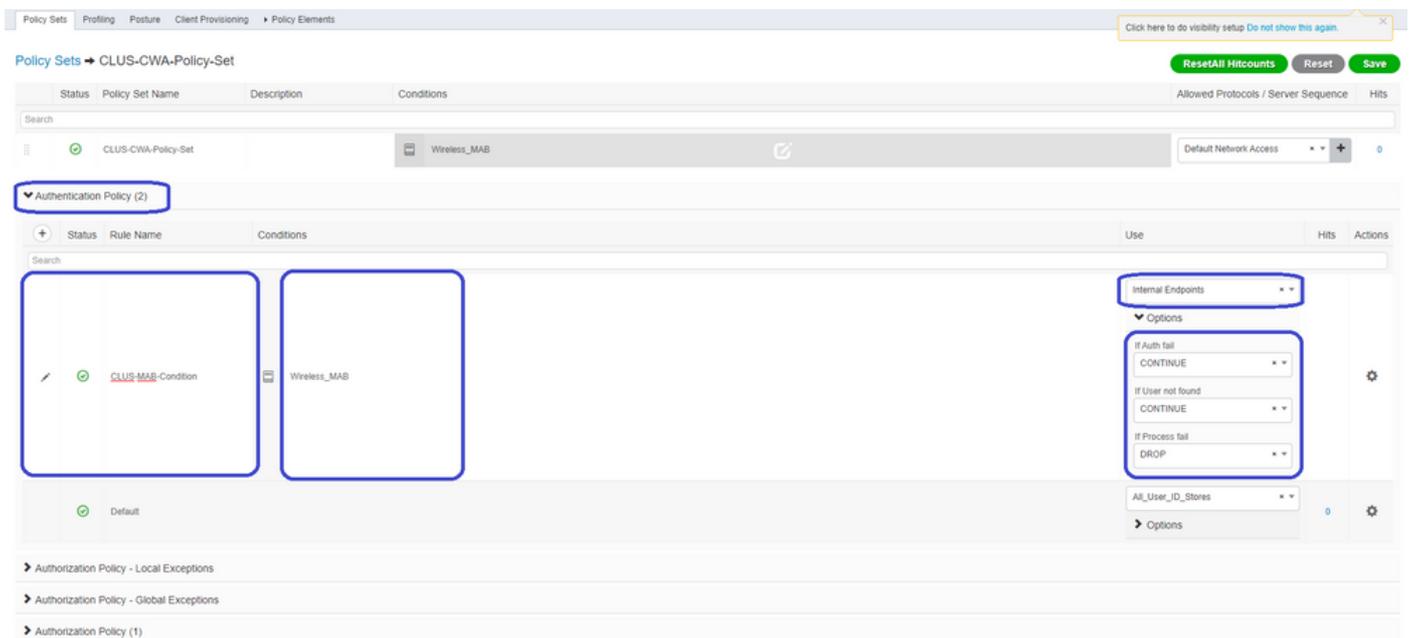
Para crear el conjunto de políticas, vaya a **Policy>Policy Set** y pulse el botón + en el lado izquierdo de la pantalla. Asigne el nombre al nuevo conjunto de políticas y asegúrese de que esté configurado como "acceso a la red predeterminado" o cualquier lista de protocolos permitidos que permita "Búsqueda de host de procesos" para MAB(para verificar la lista de protocolos permitidos vaya a Política>Elementos de políticas>Resultados>Autenticación>Protocolos permitidos). Ahora, presione el signo + en medio del nuevo conjunto de políticas que creó.



Para este conjunto de políticas cada vez que MAB se utiliza en ISE, pasará a través de este conjunto de políticas. Posteriormente, puede hacer políticas de autorización que coincidan con el ID de la estación llamada para que se puedan aplicar resultados diferentes dependiendo de la WLAN que se esté utilizando. Este proceso es muy personalizable con muchas cosas en las que puede coincidir.



Dentro del conjunto de políticas , cree las políticas. La política de autenticación puede coincidir de nuevo en MAB, pero necesita cambiar el almacén de ID para utilizar "terminales internos" y debe cambiar las opciones para continuar con la autenticación de error y el usuario no encontrado.



Una vez establecida la política de autenticación, debe crear dos reglas en la política de autorización. Esta política se lee como una ACL, por lo que el orden necesita tener la regla post-auth arriba y la regla pre-auth abajo. La regla posterior a la autenticación coincidirá con los usuarios que ya han pasado por guest-flow. Esto es para decir que si ya firmaron, golpearán esa regla y pararán ahí. Si no han iniciado sesión, continuarán por la lista y aplicarán la regla anterior a la autenticación obteniendo la redirección. Es una buena idea hacer coincidir las reglas de la política de autorización con el ID de la estación llamada que termina con el SSID para que sólo llegue a las WLAN configuradas para hacerlo.

Policy Sets → CLUS-CWA-Policy-Set Reset All Hitcounts

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server S
✓	CLUS-CWA-Policy-Set		Wireless_MAB	Default Network Access

Authentication Policy (2)
 Authorization Policy - Local Exceptions
 Authorization Policy - Global Exceptions
 Authorization Policy (4)

Status	Rule Name	Conditions	Results	Profiles	Security Groups
✓	Post-CWA	AND Network Access UseCase EQUALS Guest Flow Radius Called-Station-ID ENDS_WITH CLUS-SSID	CLUS-Post-Auth		Select from list
✓	MAB on WLAN	AND Radius Called-Station-ID ENDS_WITH CLUS-SSID Wireless_MAB	CLUS-AuthZ-Profile-ISE		Select from list
✓	Flex AuthZ	Radius Called-Station-ID ENDS_WITH FLEX-CWA	CLUS-Flex_CWA		Select from list
✓	Default		DenyAccess		Select from list

Ahora que el conjunto de políticas está configurado, debe informar a ISE acerca del 9800 (Foreign) para que ISE confíe en él como un autenticador. Esto se puede hacer en **Admin>Network Resources>Network Device>+**. Debe asignarle un nombre, establecer la dirección IP (o, en este caso, toda la subred de administración), activar RADIUS y establecer el secreto compartido. El secreto compartido en ISE debe coincidir con el secreto compartido en el 9800 o este proceso fallará. Después de agregar la configuración, pulse el botón enviar para guardarla.

Identity Services Engine Administration

System Identity Management **Network Resources** Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services

Network Devices List > JaysNet

Network Devices

Default Device
Device Security Settings

* Name **CLUS_Net-Device**
Description

IP Address * IP: **192.168.160.0** / **24**

* Device Profile Cisco
Model Name
Software Version

* Network Device Group
Location All Locations Set To Default
IPSEC No Set To Default
Device Type All Device Types Set To Default

RADIUS Authentication Settings

RADIUS UDP Settings
Protocol RADIUS
Shared Secret ********* Show
Use Second Shared Secret Show
CoA Port 1700 Set To Default

RADIUS DTLS Settings

Finalmente, deberá agregar el nombre de usuario y la contraseña que el cliente ingresará en la

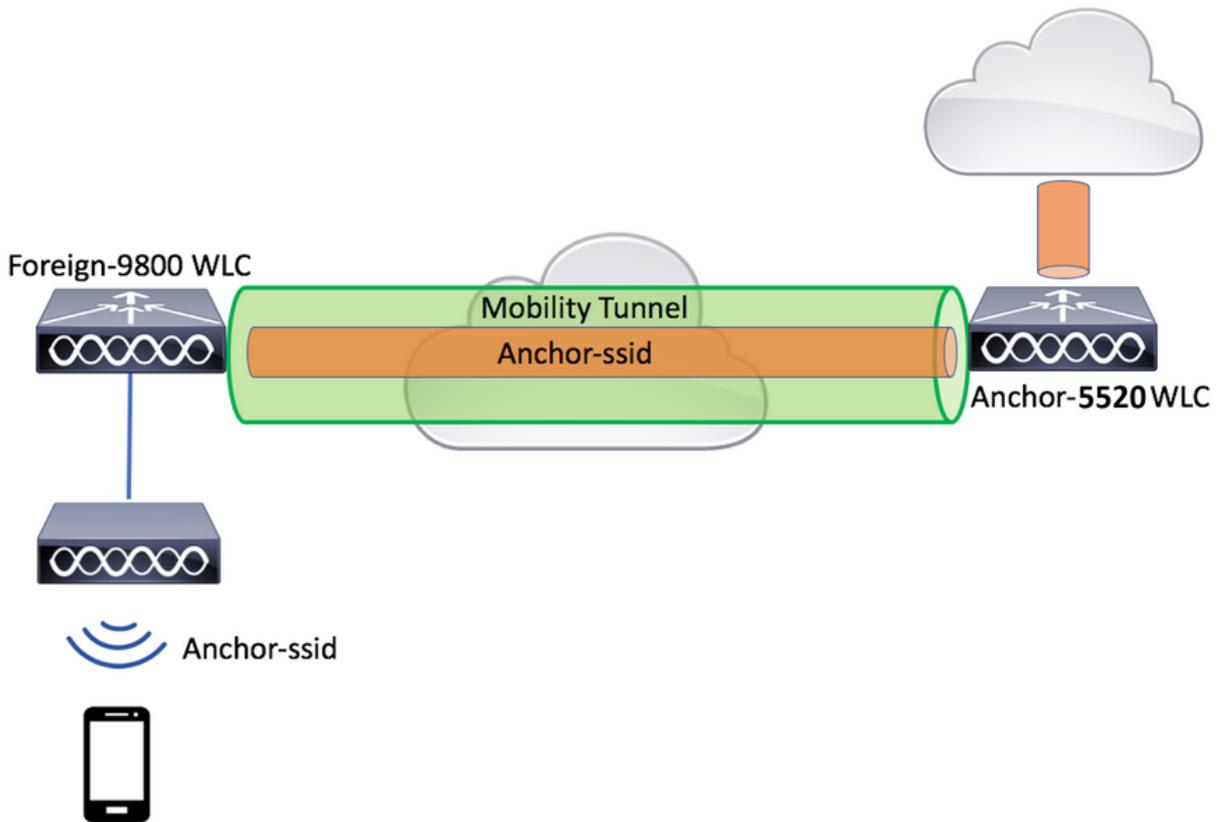
página de inicio de sesión para validar que deben tener acceso a la red. Esto se realiza bajo **Admin>Identity Management>Identity>Users>+Add** y asegúrese de enviar después de agregarlo. Al igual que todo lo demás con ISE, esto es personalizable y no tiene que ser un usuario almacenado localmente, pero, de nuevo, es la configuración más sencilla.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation path is: Administration > Identity Management > Identities > Users > New Network Access User. The form fields are as follows:

- Network Access User:**
 - * Name: CLUS-User
 - Status: Enabled
 - Email: [Empty]
- Passwords:**
 - Password Type: Internal Users
 - * Login Password: [Masked]
 - Re-Enter Password: [Masked]
 - Enable Password: [Empty]
- User Information:**
 - First Name: [Empty]
 - Last Name: [Empty]
- Account Options:**
 - Description: [Empty]
 - Change password on next login:
- Account Disable Policy:**
 - Disable account if date exceeds: 2020-07-17 (yyyy-mm-dd)
- User Groups:**
 - Select an item: [Dropdown menu]

Buttons: **Submit** (highlighted), Cancel

Configure un Catalyst 9800 anclado a un WLC AireOS



Configuración externa de Catalyst 9800

Siga los mismos pasos descritos anteriormente, saltando la sección "Crear el perfil de política en el WLC de anclaje".

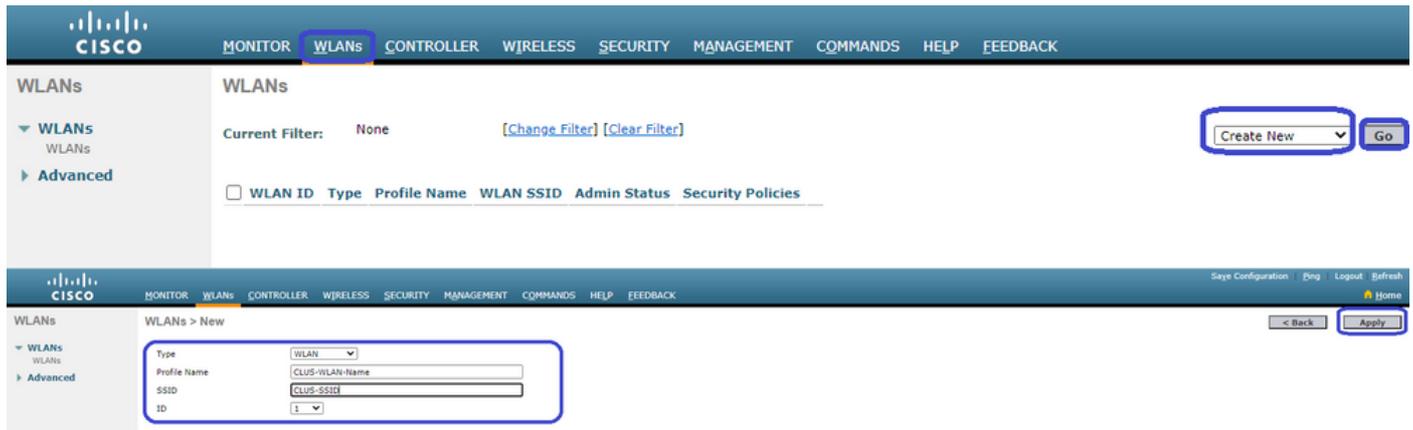
Configuraciones AAA en el WLC AireOS de anclaje

Agregue el servidor al WLC yendo a **Security>AAA>RADIUS>Authentication>New**. Agregue la dirección IP del servidor, el secreto compartido y la compatibilidad con CoA.

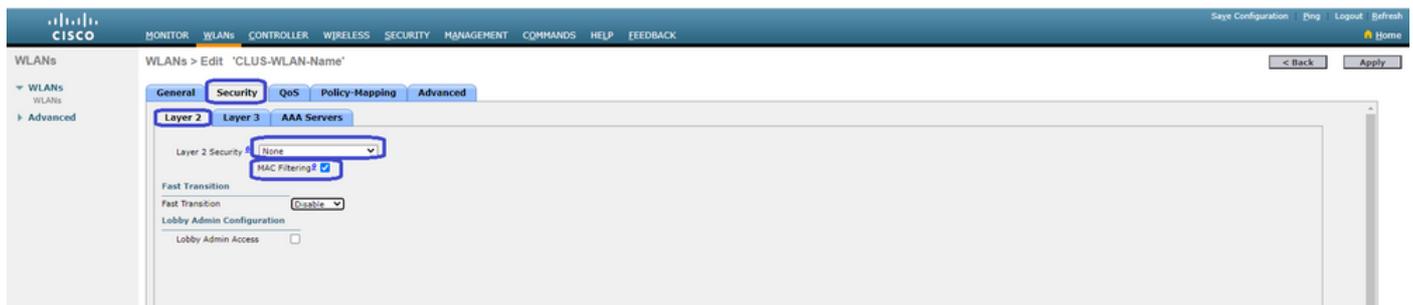
Configuración WLAN en el WLC AireOS

Para crear la WLAN, vaya a **WLANs>Create New>Go**.

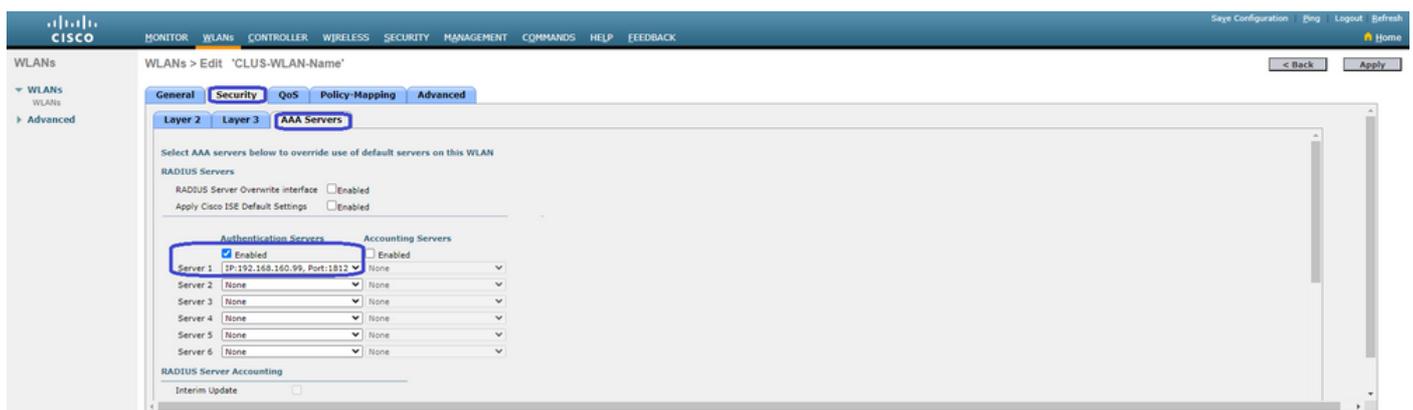
Configure el nombre del perfil, el ID de WLAN y el SSID, luego presione "Aplicar".



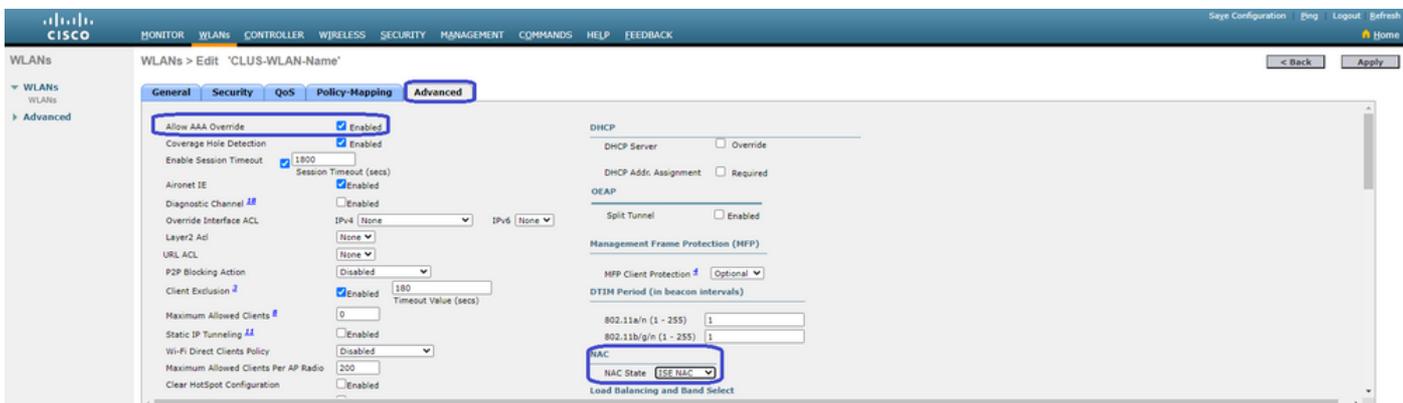
Esto le llevará a la configuración de WLAN. En la ficha "General" puede agregar la interfaz que desea que utilicen los clientes si no va a configurar ISE para enviarla en los AVP. A continuación, vaya a la ficha **Security>Layer2** y haga coincidir la configuración de "Layer 2 Security" que utilizó en el 9800 y active "MAC Filtering".



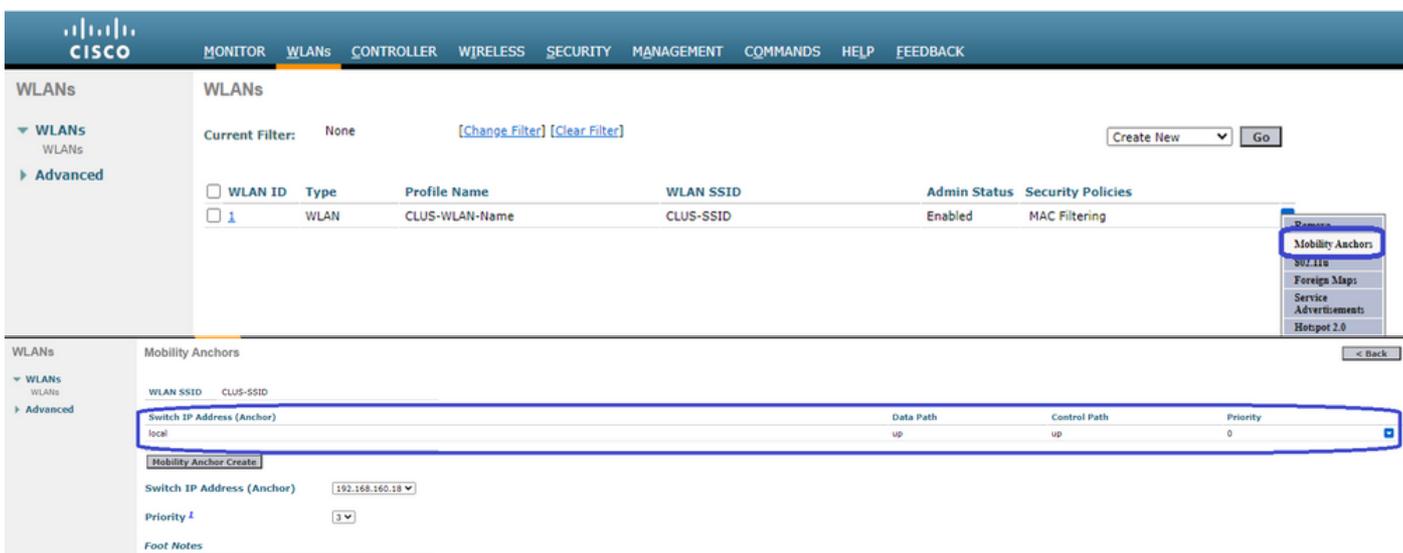
Ahora pase a la ficha **Security>AAA Servers** y establezca el servidor ISE como "Authentication Servers" (Servidores de autenticación). **No** establezca nada para los "servidores de contabilidad". Desmarque la casilla "Habilitar" para la contabilización.



Mientras aún se encuentra en las configuraciones de WLAN, pase a la pestaña "Avanzado" y habilite "Permitir Anulación AAA", así como cambie el "Estado NAC" a "NAC ISE"



Lo último es anclarlo a sí mismo. Para ello, vuelva a la página **WLANs** y pase el cursor sobre el cuadro azul de la derecha de **WLAN>Mobility Anchors**. Establezca "Cambiar dirección IP (delimitador)" en local y pulse el botón "Crear anclaje de movilidad". Luego debe aparecer con prioridad 0 anclada local.



Redirigir ACL en el WLC AireOS

Esta es la configuración final necesaria en el WLC AireOS. Para crear la ACL de redirección, vaya a **Security>Access Control Lists>Access Control Lists>New**. Introduzca el nombre de la ACL (debe coincidir con lo que se envía en los AVP) y pulse "Aplicar".



Ahora haga clic en el nombre de la ACL que acaba de crear. Haga clic en el botón "Agregar nueva regla". A diferencia del controlador 9800, en el WLC AireOS, usted configura una sentencia permit para el tráfico que se permite alcanzar ISE sin ser redirigido. DHCP y DNS se permiten de forma predeterminada.

The screenshot shows the Cisco ISE Security configuration page for Access Control Lists (ACL). The left sidebar shows the navigation menu with 'Access Control Lists' highlighted. The main content area shows the 'General' tab for an ACL named 'CLUS-ACL'. The 'Deny Counters' are set to 5. A table lists the ACL rules:

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	192.168.160.99 / 255.255.255.255	TCP	Any	8443	Any	Any	273
2	Permit	192.168.160.99 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	8443	Any	Any	Any	566

Configuración de ISE

El último paso es configurar ISE para CWA. Hay muchas opciones para esto, pero este ejemplo se ceñirá a lo básico y usará el portal de invitados autoregistrado predeterminado.

En ISE, debe crear un perfil de autorización, un conjunto de políticas con una política de autenticación y una política de autorización que utilice el perfil de autorización, agregar el 9800(external) a ISE como dispositivo de red y crear un nombre de usuario y una contraseña para iniciar sesión en la red.

Para crear el perfil de autorización, vaya **aPolicy>Policy Elements>Authorization>Results>Authorization Profiles>+Add**.

Asegúrese de que el tipo de acceso devuelto es "access_accept" y, a continuación, establezca los AVP(pares valor-atributo) que desea devolver. Para CWA, la ACL de redirección y la URL de redirección son obligatorias, pero también puede enviar cosas como el ID de VLAN y el tiempo de espera de sesión. Es importante que el nombre de la ACL coincida con el nombre de la ACL de redirección en el WLC externo y el WLC de anclaje.

The screenshot shows the Cisco ISE Identity Services Engine configuration page for an Authorization Profile. The left sidebar shows the navigation menu with 'Authorization Profiles' highlighted. The main content area shows the 'Authorization Profile' configuration for 'test'. The 'Name' is 'CLUS-AuthZ-Profile-ISE'. The 'Access Type' is set to 'ACCESS_ACCEPT'. The 'Network Device Profile' is 'Cisco'. The 'Web Redirection (CWA, MDM, NSP, CPP)' checkbox is checked, and the 'Value' is set to 'Self-Registered Guest Portal'.

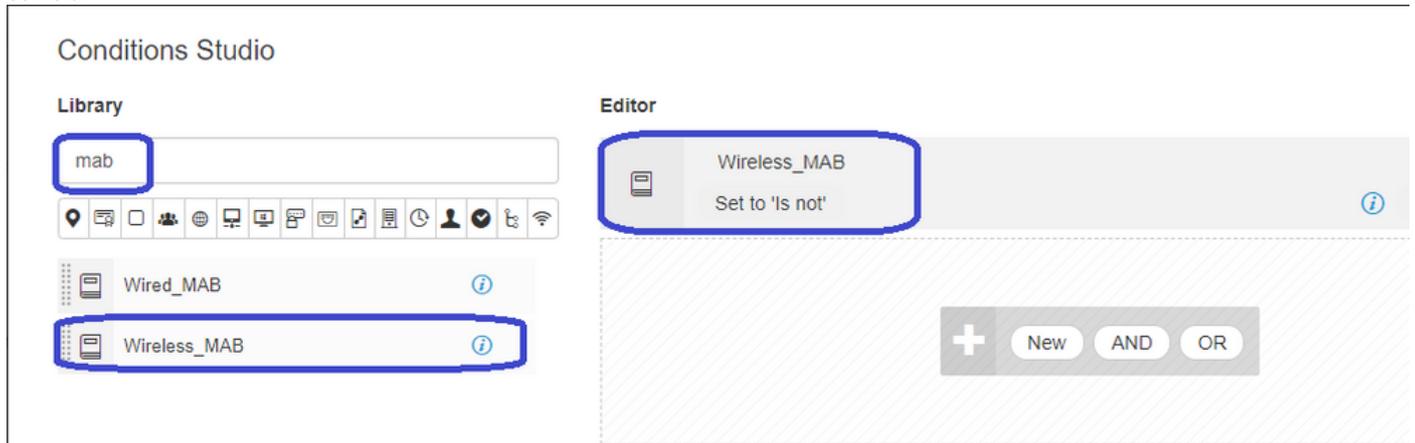
A continuación, debe configurar una forma de aplicar el perfil de autorización que acaba de crear a los clientes que pasan por

CWA. Para lograrlo, una manera es crear un conjunto de políticas que omita la autenticación cuando se usa MAB y aplicar el perfil de autorización cuando se usa el SSID enviado en el ID de estación llamada. De nuevo, hay muchas maneras de lograrlo, así que si necesita algo más específico o más seguro, esta es la forma más simple de hacerlo.

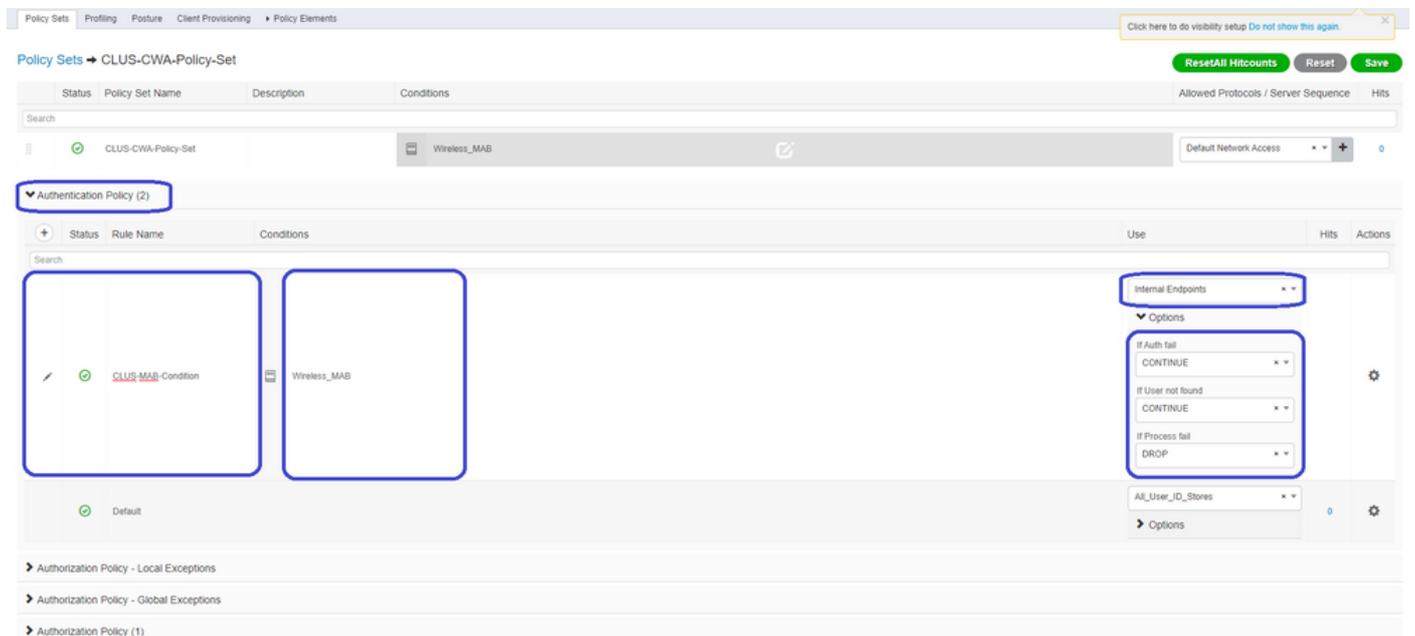
Para crear el conjunto de políticas, vaya a **Policy>Policy Settings** y presione el botón + en el lado izquierdo de la pantalla. Asigne el nombre al nuevo conjunto de políticas y asegúrese de que esté configurado como "acceso a la red predeterminado" o cualquier lista de protocolos permitidos que permita "Búsqueda de host de procesos" para MAB(para verificar la lista de protocolos permitidos vaya a Política>Elementos de políticas>Resultados>Autenticación>Protocolos permitidos). Ahora, presione el signo + en medio del nuevo conjunto de políticas que creó.



Para este conjunto de políticas cada vez que MAB se utiliza en ISE, pasará a través de este conjunto de políticas. Posteriormente, puede hacer políticas de autorización que coincidan con el ID de la estación llamada para que se puedan aplicar resultados diferentes dependiendo de la WLAN que se esté utilizando. Este proceso es muy personalizable con muchas cosas en las que puede coincidir



Dentro del conjunto de políticas , cree las políticas. La política de autenticación puede coincidir de nuevo en MAB, pero necesita cambiar el almacén de ID para utilizar "terminales internos" y debe cambiar las opciones para continuar con la autenticación de error y el usuario no encontrado.



Una vez establecida la política de autenticación, debe crear dos reglas en la política de autorización. Esta política se lee como una ACL, por lo que el orden necesita tener la regla post-auth arriba y la regla pre-auth abajo. La regla posterior a la autenticación coincidirá con los usuarios que ya han pasado por guest-flow. Esto es para decir que si ya firmaron, golpearán esa regla y pararán ahí. Si no han iniciado sesión, continuarán por la lista y aplicarán la regla anterior a la autenticación obteniendo la redirección. Es una buena idea hacer coincidir las reglas de la política de autorización con el ID de la estación llamada que termina con el SSID para que sólo llegue a las WLAN configuradas para hacerlo.

Policy Sets → CLUS-CWA-Policy-Set Reset All Hitcounts

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server S		
⊕	CLUS-CWA-Policy-Set		Wireless_MAB	Default Network Access		
Authentication Policy (2)						
Authorization Policy - Local Exceptions						
Authorization Policy - Global Exceptions						
Authorization Policy (4)						
+	Status	Rule Name	Conditions	Results	Profiles	Security Groups
⊕	⊕	Post-CWA	AND Network Access UseCase EQUALS Guest Flow Radius Called-Station-ID ENDS_WITH CLUS-SSID	CLUS-Post-Auth	+	Select from list
⊕	⊕	MAB on WLAN	AND Radius Called-Station-ID ENDS_WITH CLUS-SSID Wireless_MAB	CLUS-AuthZ-Profile-ISE	+	Select from list
⊕	⊕	Flex AuthZ	Radius Called-Station-ID ENDS_WITH FLEX-CWA	CLUS-Flex_CWA	+	Select from list
⊕	⊕	Default		DenyAccess	+	Select from list

Ahora que el conjunto de políticas está configurado, debe informar a ISE acerca del 9800 (Foreign) para que ISE confíe en él como un autenticador. Esto se puede hacer en **Admin > Recursos de red > Dispositivo de red > +**. Debe asignarle un nombre, establecer la dirección IP (o, en este caso, toda la subred de administración), activar RADIUS y establecer el secreto compartido. El secreto compartido en ISE debe coincidir con el secreto compartido en el 9800 o este proceso fallará. Después de agregar la configuración, pulse el botón enviar para guardarla.

The screenshot displays the Cisco Identity Services Engine (ISE) Administration console. The navigation menu at the top includes: Home, Context Visibility, Operations, Policy, Administration, and Work Centers. Under Administration, the path is: System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Service > Threat Centric NAC. The left sidebar shows: Network Devices, Network Device Groups, Network Device Profiles, External RADIUS Servers, RADIUS Server Sequences, NAC Managers, External MDM, and Location Services. The main configuration area is titled 'Network Devices List > JaysNet' and 'Network Devices'. The configuration fields are: * Name: CLUS_Net-Device; Description: (empty); IP Address: 192.168.160.0; Subnet: 24; * Device Profile: Cisco; Model Name: (empty); Software Version: (empty); * Network Device Group: Location: All Locations; IPSEC: No; Device Type: All Device Types. The 'RADIUS Authentication Settings' section is expanded, showing: RADIUS UDP Settings; Protocol: RADIUS; Shared Secret: (masked); Use Second Shared Secret: (unchecked); CoA Port: 1700. The 'RADIUS DTLS Settings' section is collapsed.

Finalmente, deberá agregar el nombre de usuario y la contraseña que el cliente ingresará en la página de inicio de sesión para validar que deben tener acceso a la red. Esto se hace en **Admin>Identity Management>Identity>Users>+Addy** asegúrese de enviar después de agregarlo. Al igual que todo lo demás con ISE, esto es personalizable y no tiene que ser un usuario almacenado localmente, pero, de nuevo, es la configuración más sencilla.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation menu includes System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, Threat Centric NAC, Identities, Groups, External Identity Sources, Identity Source Sequences, and Settings. The main content area is titled 'Network Access Users List > New Network Access User'. The form contains the following sections:

- Network Access User:** * Name (CLUS-User), Status (Enabled), Email.
- Passwords:** Password Type (Internal Users), * Login Password, Re-Enter Password, Enable Password, and Generate Password buttons.
- User Information:** First Name, Last Name.
- Account Options:** Description, Change password on next login checkbox.
- Account Disable Policy:** Disable account if date exceeds (2020-07-17).
- User Groups:** Select an item dropdown.

The 'Submit' button is highlighted with a red box.

Diferencias en la configuración cuando el WLC de AireOS es el externo y el Catalyst 9800 es el ancla

Si desea que el WLC de AireOS sea el controlador externo, la configuración es la misma que antes con sólo dos diferencias.

1. La contabilidad AAA nunca se realiza en el anclaje, por lo que el 9800 no tendría una lista de métodos contables y el WLC AireOS tendría la contabilización habilitada y apuntando a ISE.
2. El AireOS tendría que anclar al 9800 en lugar de a sí mismo. En el perfil de política, el 9800 no tendría un anclaje seleccionado pero tendría la casilla "Exportar anclaje" activada.
3. Es importante tener en cuenta que cuando los WLC de AireOS exportan el cliente al 9800, no hay concepto de perfiles de política, envía solamente el Nombre del Perfil de WLAN. Por lo tanto, el 9800 aplicará el Nombre del Perfil WLAN enviado desde AireOS tanto al Nombre del Perfil WLAN como al Nombre del Perfil de Política. Eso dijo que cuando se anclan de un WLC AireOS a un WLC 9800, el Nombre del Perfil WLAN en ambos WLC y el Nombre del Perfil de Política en el 9800, todos deben coincidir.

Verificación

Para verificar las configuraciones en el **9800 WLC** ejecute los comandos

- AAA

Show Run | section aaa|radius

- WLAN

Show wlan id <wlan id>

- Perfil de política

Show wireless profile policy detailed <profile name>

- Etiqueta de política

Show wireless tag policy detailed <policy tag name>

- ACL

Show IP access-list <ACL name>

- Verificar que la movilidad esté a la altura del ancla

Show wireless mobility summary

Para verificar las configuraciones en el WLC AireOS ejecute los comandos

- AAA

Show radius summary

Nota: RFC3576 es la configuración de CoA

- WLAN

Show WLAN <wlan id>

- ACL

Show acl detailed <acl name>

- Verificar que la movilidad esté a la altura de lo que ocurre en el extranjero

Show mobility summary

Troubleshoot

La resolución de problemas tiene un aspecto diferente en función del punto del proceso que detenga el cliente. Por ejemplo, si el WLC nunca obtiene una respuesta de ISE en MAB, el cliente se quedaría atascado en el "Estado del Administrador de Políticas: Asociando" y no se exportaría al ancla. En esta situación, usted sólo resolvería problemas en el Foreign y podría recolectar un seguimiento de RA y una captura de paquetes para el tráfico entre el WLC y el ISE. Otro ejemplo sería que MAB ha pasado correctamente pero el cliente no recibe la redirección. En este caso,

debe asegurarse de que el extranjero recibió la redirección en los AVPs y la aplicó al cliente. También debe verificar el anclaje para asegurarse de que el cliente esté allí con la ACL correcta. Este alcance de la solución de problemas está fuera del diseño de este documento técnico (verifique las referencias de las pautas genéricas de troubleshooting del cliente).

Para obtener más ayuda con la solución de problemas de CWA en el WLC 9800, consulte Cisco Live. presentación DGTL-TSCENT-404

Información de Troubleshooting de Catalyst 9800

Detalles del cliente

```
show wireless client mac-address
```

Aquí debe ver el "Estado del administrador de políticas", "Administrador de sesiones>Método de autenticación", "Función de movilidad".

También puede encontrar esta información en la GUI en Monitoring>Clientes

Captura de paquetes integrada

Desde la CLI, el comando inicia *#monitor capture <nombre de captura>* luego las opciones vienen después de eso.

Desde la GUI, vaya a Solucionar problemas>Captura de paquetes>+Agregar

Rastreo de RadioActive

Desde la CLI

```
debug wireless mac/ip
```

Utilice la forma no del comando para detenerlo. Esto se registrará en un archivo en la memoria flash de inicialización denominado "ra_trace", luego en la dirección MAC o IP del cliente y la fecha y hora.

Desde la GUI, vaya a Solucionar problemas>Seguimiento radiactivo>+Agregar. Agregue la dirección mac o ip del cliente, haga clic en apply y luego presione start. Después de haber pasado por el proceso varias veces, detenga el seguimiento, genere el registro y descárguelo en su dispositivo.

Información de resolución de problemas de AireOS

Detalles del cliente

Desde la CLI *show client details <client mac>*

Desde el monitor GUI>Clientes

Depuraciones desde la CLI

Debug client

Debug mobility handoff

Debug mobility config

Referencias

[Creación de túneles de movilidad con 9800 controladores](#)

[Depuración inalámbrica y recopilación de registros en 9800](#)