

Configuración de CWA con AP FlexConnect en un WLC con ISE

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuración de WLC](#)

[Configuración de ISE](#)

[Crear el perfil de autorización](#)

[Crear una regla de autenticación](#)

[Crear una regla de autorización](#)

[Activar la renovación de IP \(opcional\)](#)

[Flujo de tráfico](#)

[Verificación](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar la autenticación web central con los AP FlexConnect en un WLC ISE en el modo de conmutación local.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

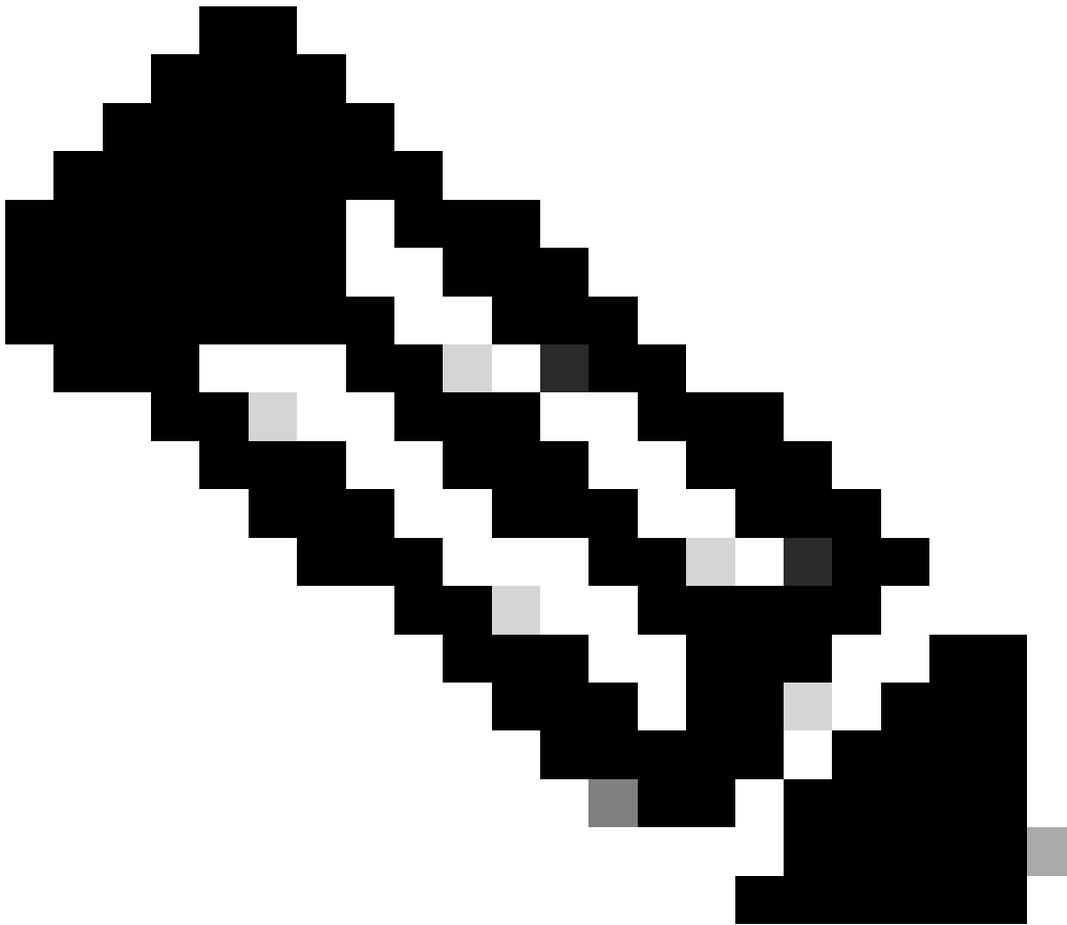
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Identity Services Engine (ISE), versión 1.2.1
- Software Wireless LAN Controller (WLC), versión 7.4.100.0

- Puntos de acceso (AP)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes



Nota: En este momento, la autenticación local en los FlexAP no se admite para este escenario.

Otros documentos de esta serie

- [Ejemplo de Configuración de Autenticación Web Central con un Switch y Identity Services Engine](#)
- [Ejemplo de configuración de autenticación web central en WLC e ISE](#)

Configurar

Existen varios métodos para configurar la autenticación web central en el controlador de LAN inalámbrica (WLC). El primer método es la autenticación Web local en la que el WLC redirige el tráfico HTTP a un servidor interno o externo donde se le pide al usuario que autentique. Luego, el WLC obtiene las credenciales (enviadas de vuelta a través de una solicitud GET HTTP en el caso de un servidor externo) y realiza una autenticación RADIUS. En el caso de un usuario invitado, se requiere un servidor externo (como Identity Service Engine (ISE) o NAC Guest Server (NGS)), ya que el portal proporciona funciones como el registro de dispositivos y el autoaprovisionamiento. Este proceso incluye los siguientes pasos:

1. El usuario se asocia al SSID de autenticación Web.
2. El usuario abre el explorador.
3. El WLC redirige al portal de invitados (como ISE o NGS) tan pronto como se ingresa una URL.
4. El usuario se autentica en el portal.
5. El portal de invitados redirige de nuevo al WLC con las credenciales ingresadas.
6. El WLC autentica al usuario invitado a través de RADIUS.
7. El WLC redirige de nuevo a la URL original.

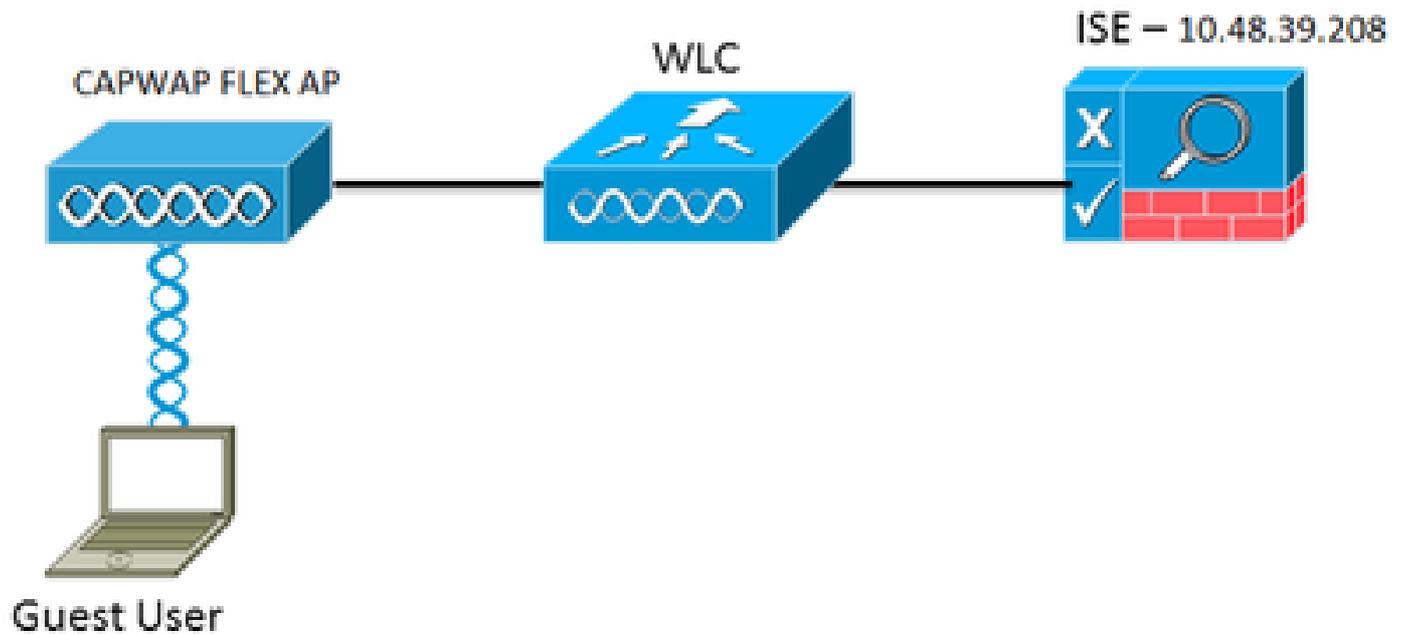
Este proceso incluye una gran cantidad de redirección. El nuevo enfoque consiste en utilizar la autenticación web central que funciona con ISE (versiones posteriores a la 1.1) y WLC (versiones posteriores a la 7.2). Este proceso incluye los siguientes pasos:

1. El usuario se asocia al SSID de autenticación Web.
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.

Esta sección describe los pasos necesarios para configurar la autenticación web central en WLC e ISE.

Diagrama de la red

Esta configuración utiliza esta configuración de red:



Configuración de la red

Configuración de WLC

La configuración del WLC es bastante directa. Se utiliza un truco (igual que en los switches) para obtener la URL de autenticación dinámica de ISE. (Dado que utiliza CoA, es necesario crear una sesión, ya que el ID de sesión forma parte de la URL). El SSID se configura para utilizar el filtrado de MAC e ISE se configura para devolver un mensaje de aceptación de acceso incluso si no se encuentra la dirección MAC, de modo que envía la URL de redirección para todos los usuarios.

Además, RADIUS Network Admission Control (Control de admisión a la red o NAC) y AAA Override deben estar habilitados. RADIUS NAC permite que ISE envíe una solicitud CoA que indica que el usuario está ahora autenticado y puede acceder a la red. También se utiliza para la evaluación del estado en la que el ISE cambia el perfil del usuario en función del resultado del estado.

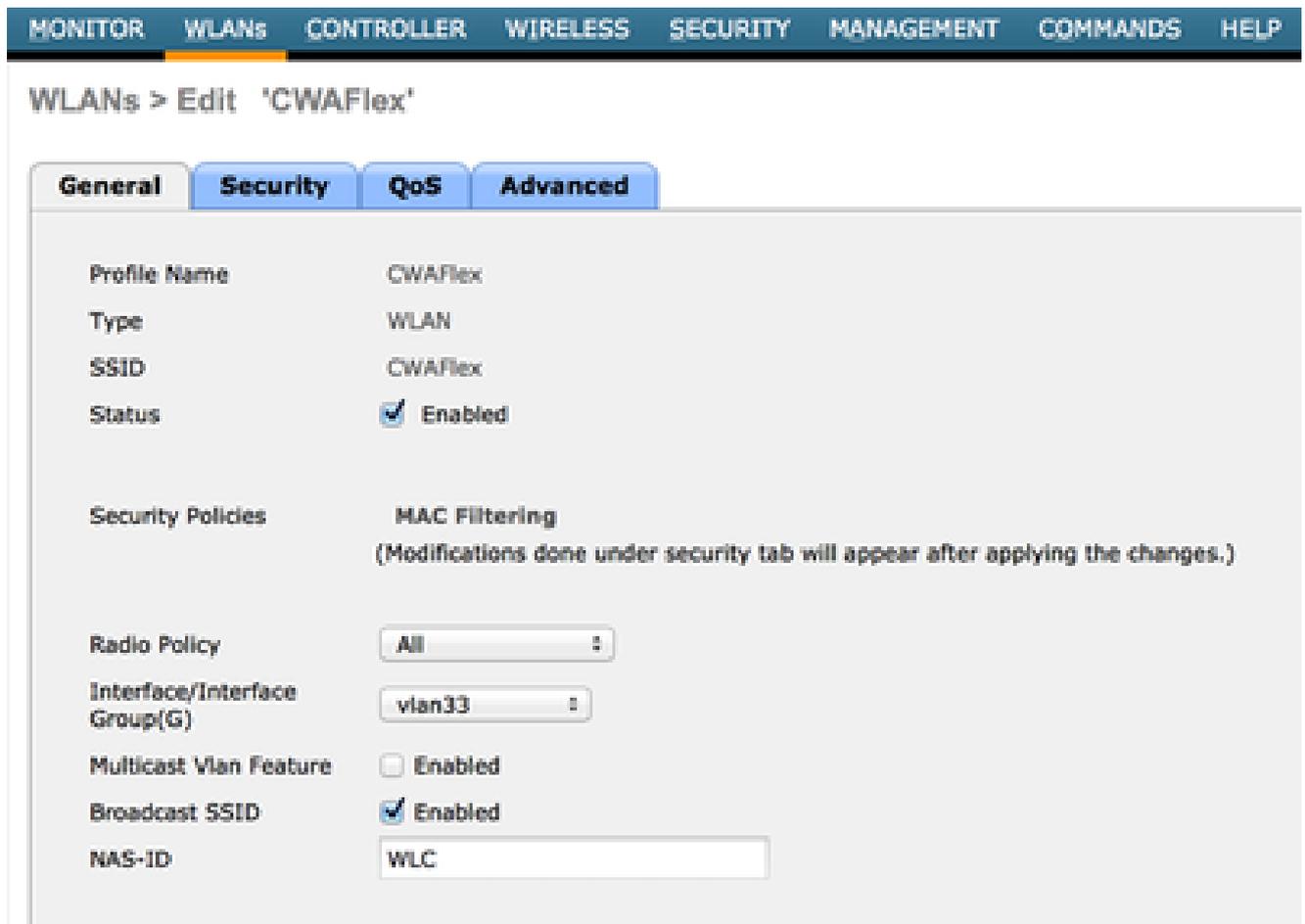
1. Asegúrese de que el servidor RADIUS tenga RFC3576 (CoA) habilitado, que es el valor predeterminado.

The screenshot shows the Cisco configuration interface for RADIUS Authentication Servers. The left sidebar contains a navigation menu with the following items: AAA, General, RADIUS, Authentication (highlighted with a red box), Accounting, Fallback, TACACS+, LDAP, Local Net Users, MAC Filtering, Disabled Clients, User Login Policies, AP Policies, Password Policies, Local EAP, Priority Order, Certificate, Access Control Lists, Wireless Protection Policies, Web Auth, TrustSec SXP, and Advanced. The main content area is titled 'RADIUS Authentication Servers > Edit' and displays the following configuration details:

Server Index	1
Server Address	10.48.39.208
Shared Secret Format	ASCII
Shared Secret	***
Confirm Shared Secret	***
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	Enabled
Support for RFC 3576	Enabled (highlighted with a red box)
Server Timeout	2 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable

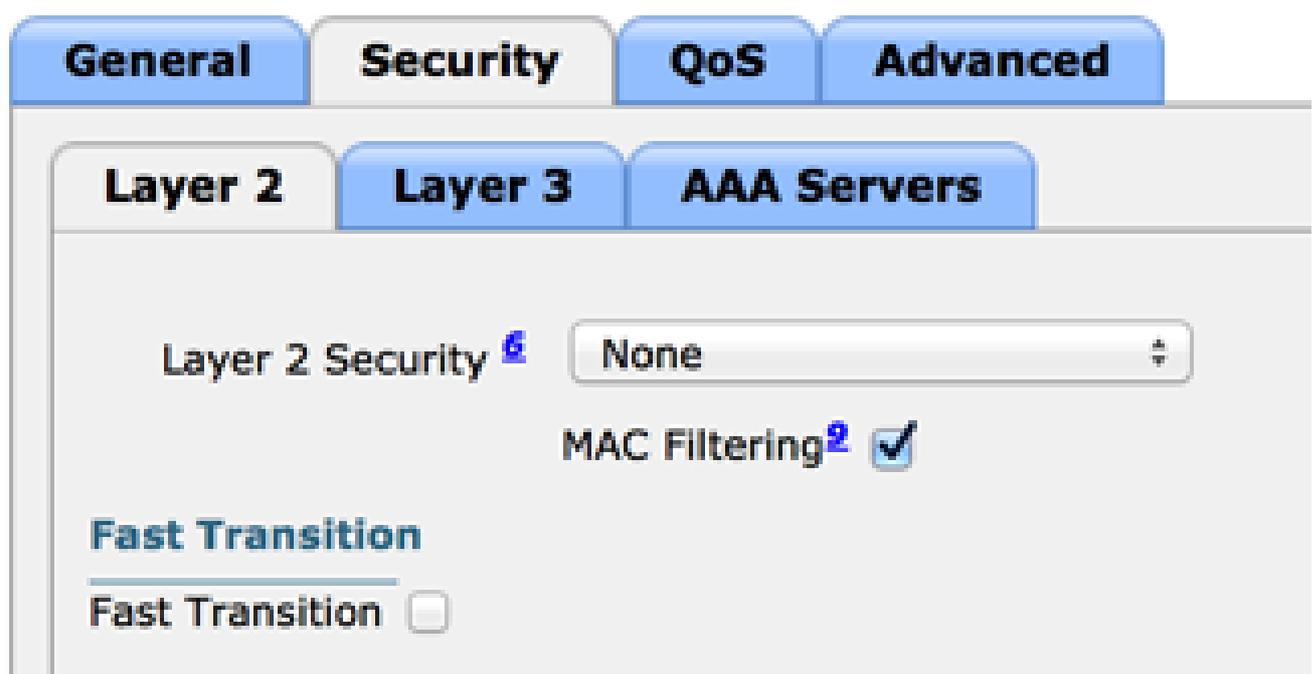
El servidor RADIUS tiene RFC3576

2. Cree una nueva WLAN. Este ejemplo crea una nueva WLAN llamada CWAFlex y la asigna a vlan33. (Tenga en cuenta que no tendrá mucho efecto ya que el punto de acceso está en modo de conmutación local.)



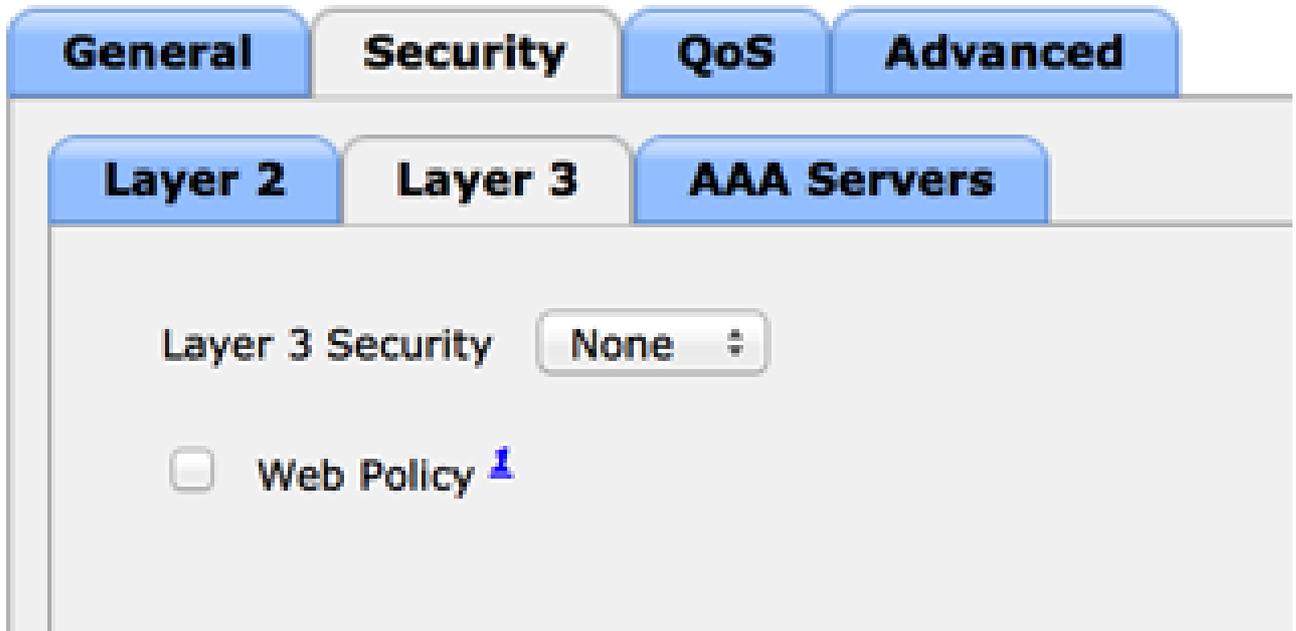
Creación de una WLAN nueva

3. En la ficha Seguridad, active el filtrado de direcciones MAC como seguridad de capa 2.



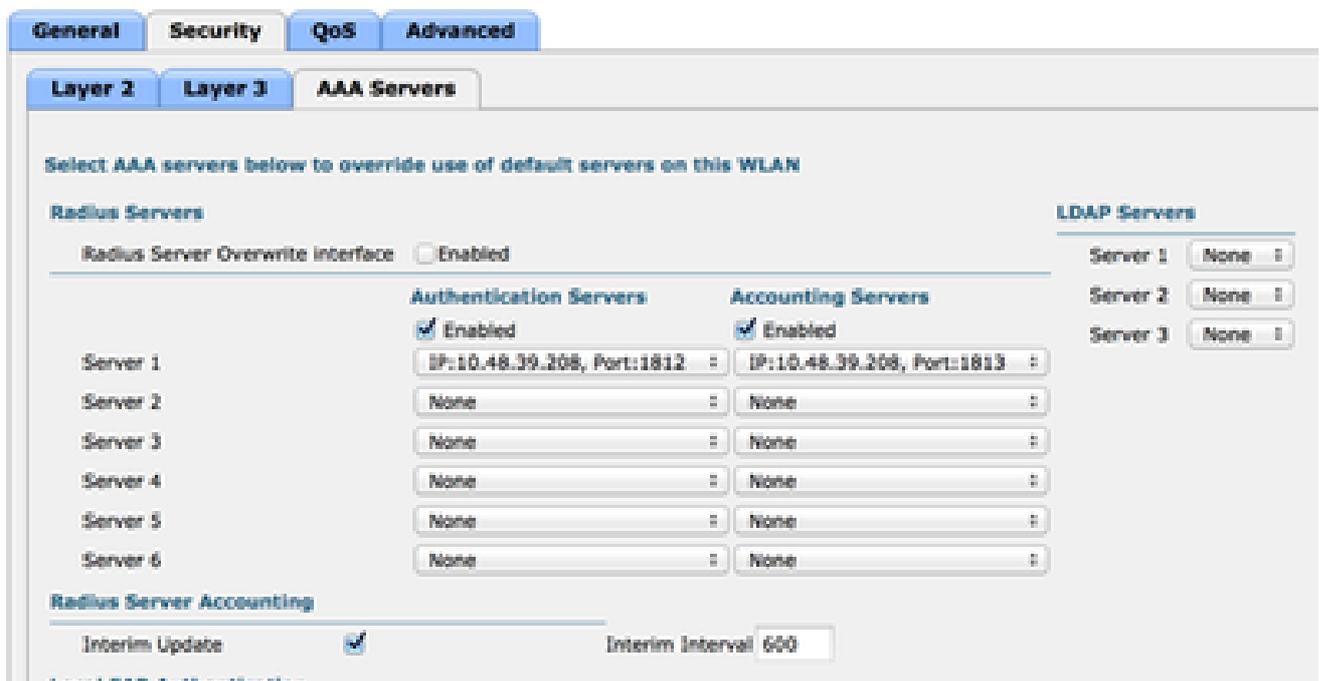
Activar filtrado de MAC

4. En la ficha Layer 3 (Capa 3), asegúrese de que la seguridad esté desactivada. (Si la autenticación Web está activada en la capa 3, la autenticación Web local está activada, no la autenticación Web central.)

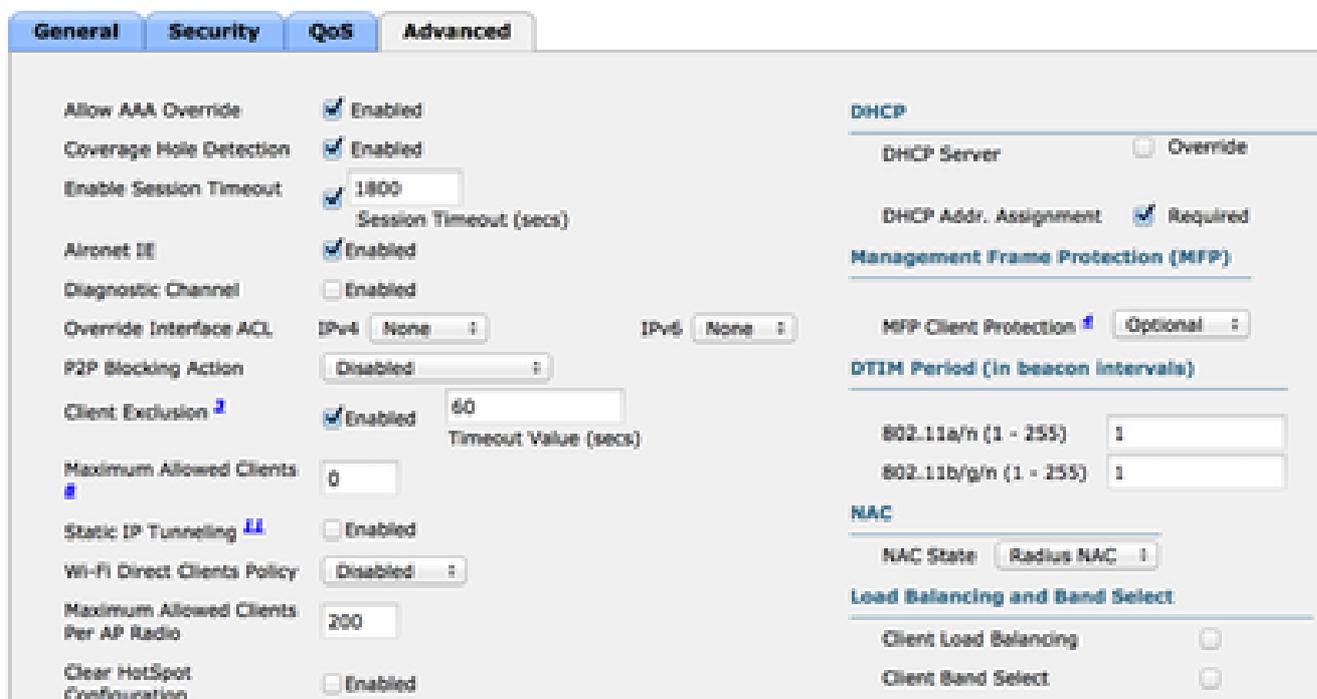


Asegúrese de que la seguridad está desactivada

5. En la pestaña AAA Servers (Servidores AAA), seleccione el servidor ISE como servidor RADIUS para la WLAN. De manera opcional, puede seleccionarla para la contabilidad con el fin de disponer de información más detallada sobre ISE.



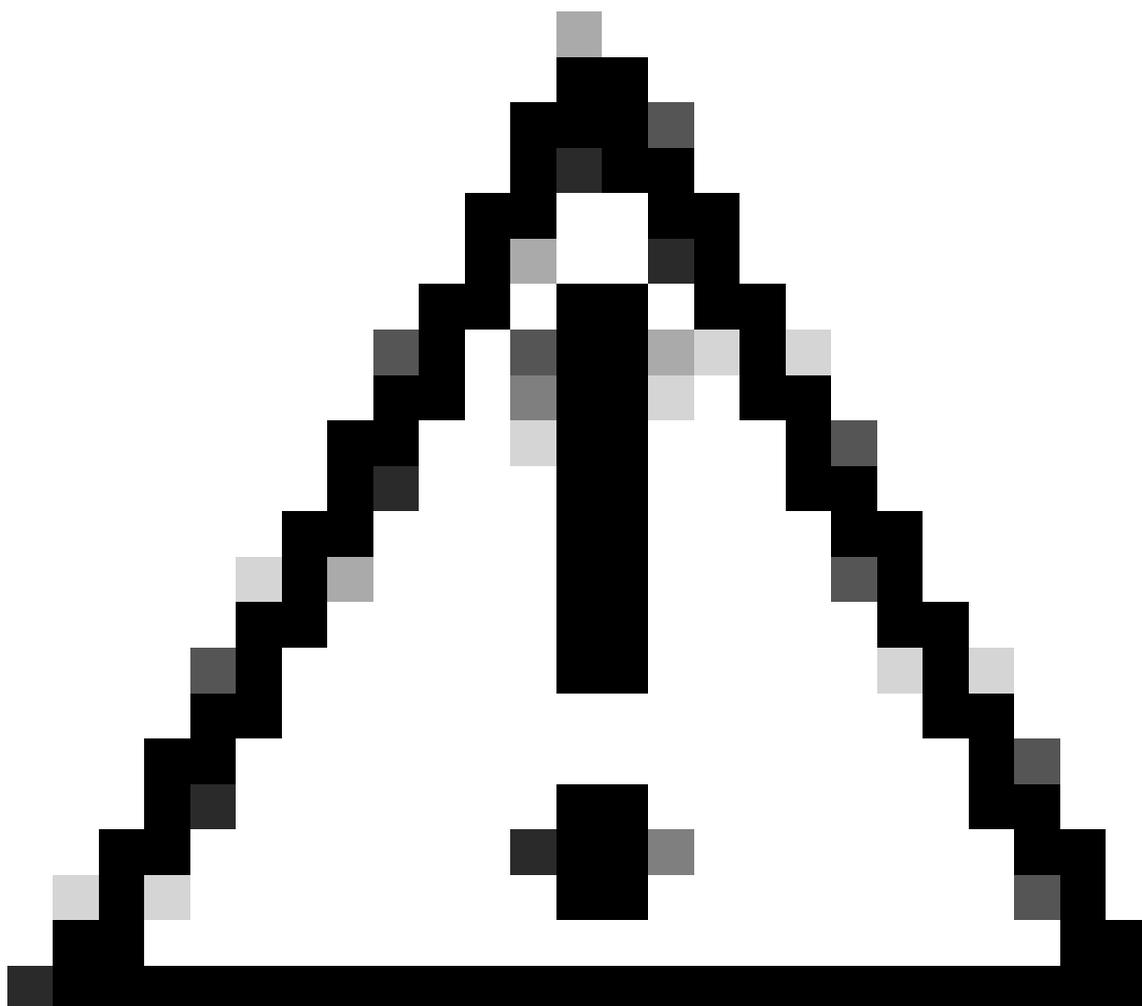
- 6. En la ficha Opciones avanzadas, asegúrese de que la opción Permitir anulación de AAA está activada y de que Radius NAC está seleccionado para el estado de NAC.



Asegúrese de que Permitir Anulación de AAA esté marcado

- 7. Cree una ACL de redirección.

Se hace referencia a esta ACL en el mensaje Access-Accept de ISE y se define qué tráfico debe redirigirse (denegarse por la ACL) y qué tráfico no debe redirigirse (permitido por la ACL). Básicamente, se deben permitir DNS y el tráfico hacia/desde ISE



Precaución: un problema con los puntos de acceso de FlexConnect es que debe crear una ACL de FlexConnect independiente de la ACL normal. Este problema se documenta en el ID de bug de Cisco [CSCue68065](#) y se corrige en la versión 7.5. En el WLC 7.5 y posterior, solamente se requiere una FlexACL, y no se necesita ninguna ACL estándar. El WLC espera que la ACL de redirección devuelta por ISE sea una ACL normal. Sin embargo, para garantizar su funcionamiento, necesita aplicar la misma ACL que FlexConnect ACL. (Solo los usuarios registrados de Cisco pueden acceder a la información y las herramientas internas de Cisco).

Este ejemplo muestra cómo crear una ACL FlexConnect denominada flexred:

CISCO MONITOR WLANs CONTROLLER **WIRELESS** SECURITY

Wireless

- Access Points
 - All APs
 - Radios
 - 802.11a/n
 - 802.11b/g/n
 - Dual-Band Radios
 - Global Configuration
- Advanced
 - Mesh
 - RF Profiles
 - FlexConnect Groups
 - FlexConnect ACLs

FlexConnect Access Control Lists

Acl Name

[flexred](#)

Cree una ACL de FlexConnect denominada FlexRed

- a. Cree reglas para permitir el tráfico DNS, así como el tráfico hacia ISE y rechace el resto.

CISCO MONITOR WLANs CONTROLLER **WIRELESS** SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Wireless

- Access Points
 - All APs
 - Radios
 - 802.11a/n
 - 802.11b/g/n
 - Dual-Band Radios
 - Global Configuration
- Advanced
 - Mesh
 - RF Profiles
 - FlexConnect Groups
 - FlexConnect ACLs
- 802.11a/n
- 802.11b/g/n
- Media Stream

Access Control Lists > Edit

General

Access List Name: flexred

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP
1	Permit	0.0.0.0 / 0.0.0.0	10.48.39.208 / 255.255.255.255	Any	Any	Any	Any <input type="button" value="v"/>
2	Permit	10.48.39.208 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any <input type="button" value="v"/>
3	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any <input type="button" value="v"/>
4	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any <input type="button" value="v"/>
5	Deny	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any <input type="button" value="v"/>

Permitir tráfico DNS

Si desea obtener la máxima seguridad, sólo puede permitir el puerto 8443 hacia ISE. (Si realiza un seguimiento, debe agregar puertos de estado típicos, como 8905, 8906, 8909, 8910.)

- b. (Sólo en el código anterior a la versión 7.5 debido al error de Cisco [IDCSCue68065](#)) Elija Seguridad > Listas de control de acceso para crear una ACL idéntica con el

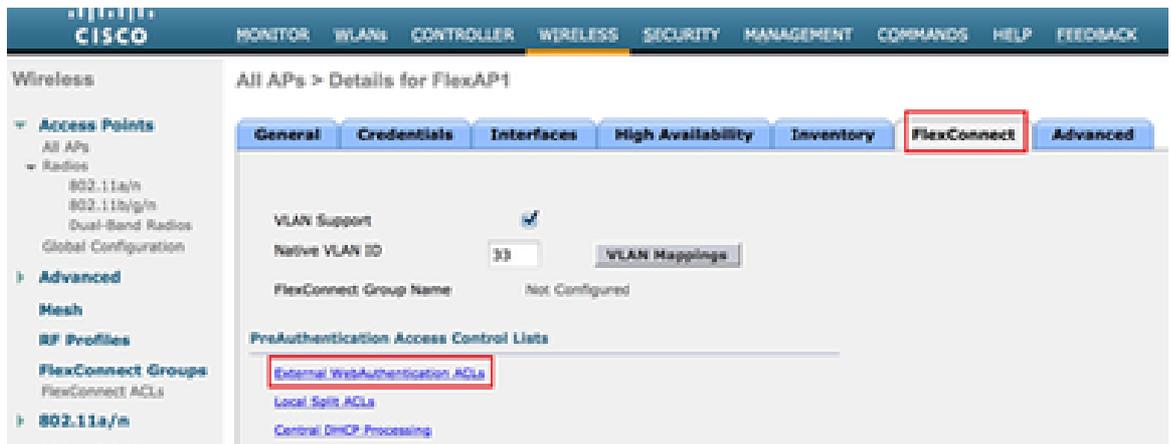
mismo nombre.

The screenshot shows the Cisco configuration interface for Security > Access Control Lists. The left sidebar contains a navigation tree with 'Access Control Lists' selected. The main content area shows 'Enable Counters' with an unchecked checkbox and a table with one entry: 'flexred' of type 'IPv4'.

Name	Type
flexred	IPv4

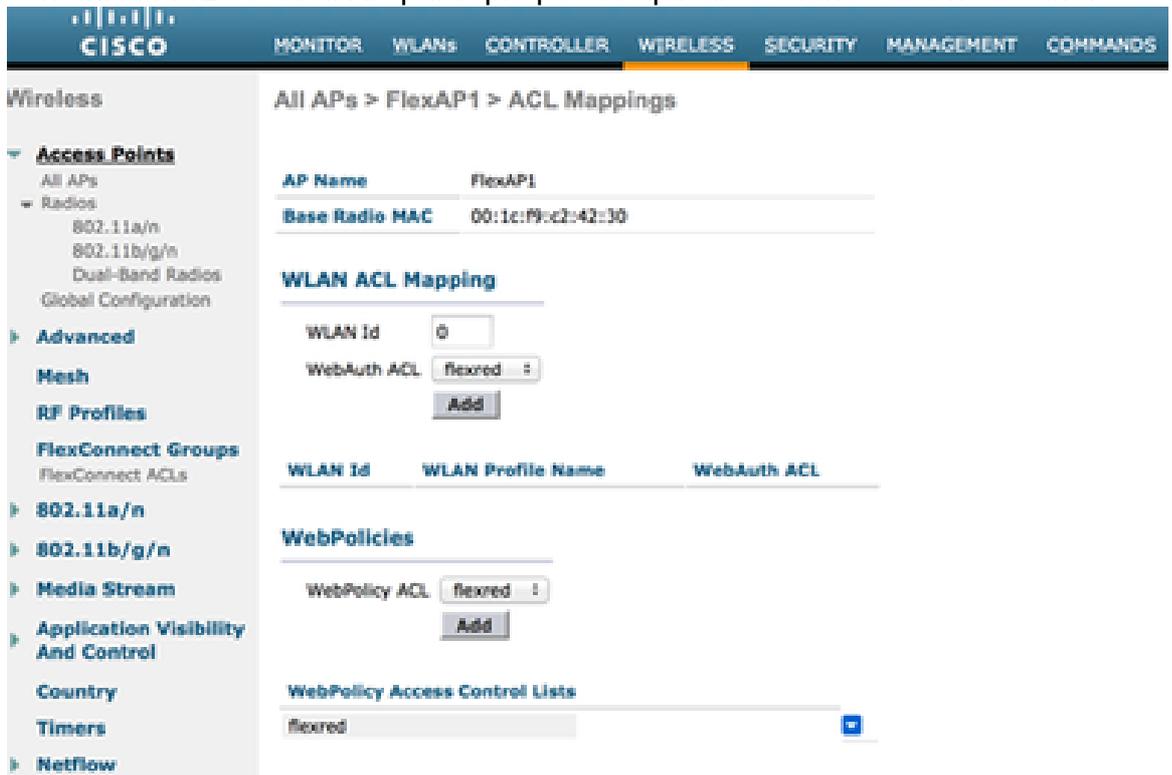
Crear ACL idéntica

- c. Prepare el punto de acceso de FlexConnect específico. Tenga en cuenta que para una implementación más grande, normalmente utilizaría grupos de FlexConnect y no realizaría estos elementos por AP por motivos de escalabilidad.
1. Haga clic en Wireless y seleccione el punto de acceso específico.
 2. Haga clic en la pestaña FlexConnect y haga clic en ACL de autenticación web externas. (Antes de la versión 7.4, esta opción se denominaba políticas web.)



Haga clic en la ficha FlexConnect

3. Agregue la ACL (denominada flexred en este ejemplo) al área de políticas web. Esto envía previamente la ACL al punto de acceso. Todavía no se aplica, pero el contenido ACL se da al AP para que pueda aplicarse cuando sea necesario.



Agregar ACL al área de políticas web

La configuración del WLC está ahora completa.

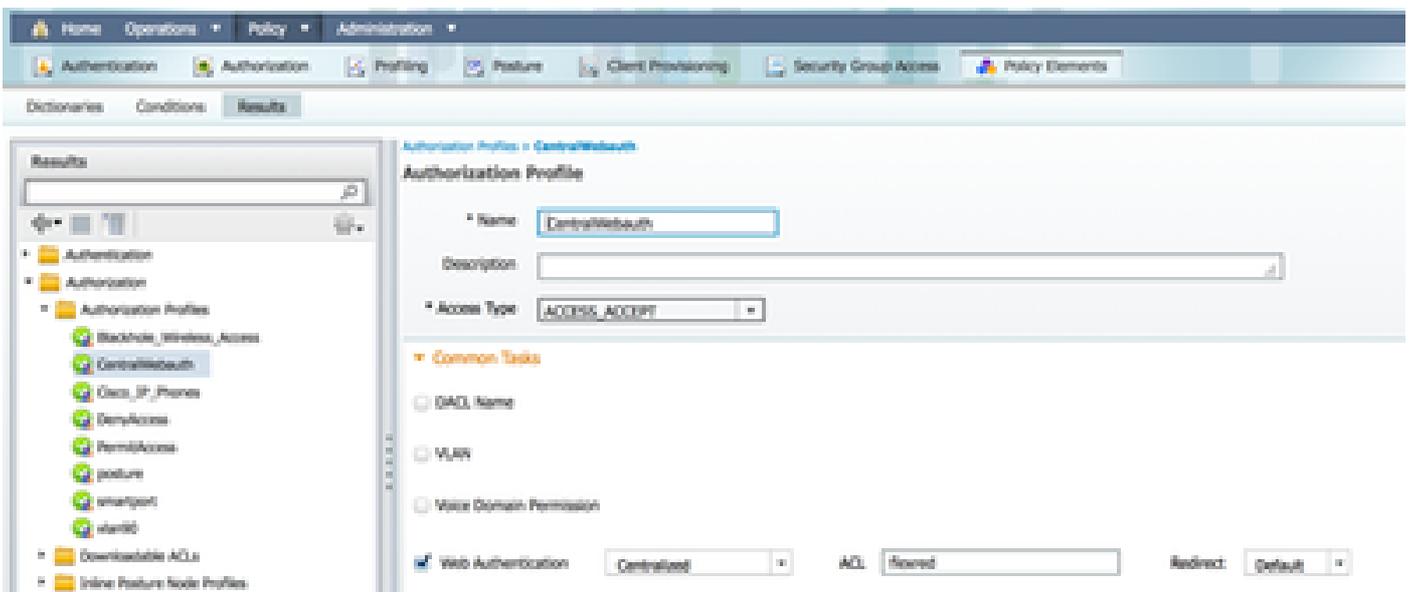
Configuración de ISE

Crear el perfil de autorización

Complete estos pasos para crear el perfil de autorización:

1. Haga clic en Directiva y, a continuación, haga clic en Elementos de directiva.
2. Haga clic en Resultados.
3. Expanda Autorización y, a continuación, haga clic en Perfil de autorización.
4. Haga clic en el botón Add para crear un nuevo perfil de autorización para webauth central.
5. En el campo Nombre, introduzca un nombre para el perfil. Este ejemplo utiliza CentralWebauth.
6. Elija ACCESS_ACCEPT en la lista desplegable Tipo de acceso.
7. Marque la casilla de verificación Web Authentication y elija Centralized Web Auth en la lista desplegable.
8. En el campo ACL, ingrese el nombre de la ACL en el WLC que define el tráfico que será redirigido. En este ejemplo se utiliza flexred.
9. Elija Default en la lista desplegable Redirect.

El atributo Redirect define si ISE ve el portal web predeterminado o un portal web personalizado creado por el administrador de ISE. Por ejemplo, la ACL flexionada en este ejemplo desencadena una redirección en el tráfico HTTP desde el cliente a cualquier lugar.



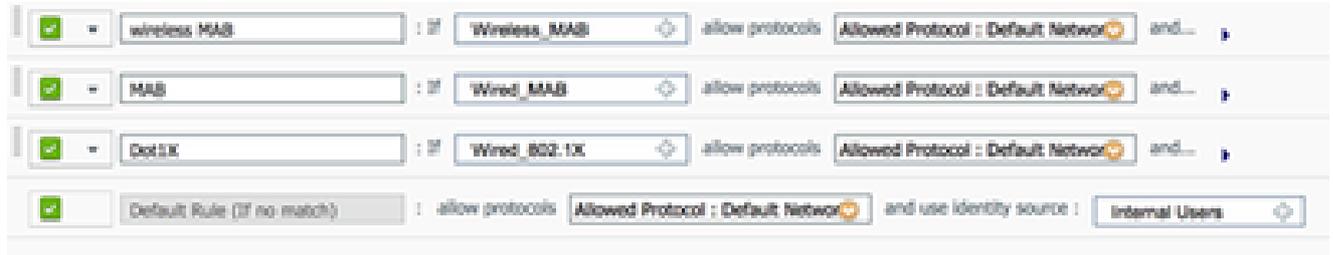
ACL Activa una Redirección en el Tráfico HTTP del Cliente a Cualquier Lugar

Crear una regla de autenticación

Complete estos pasos para utilizar el perfil de autenticación para crear la regla de autenticación:

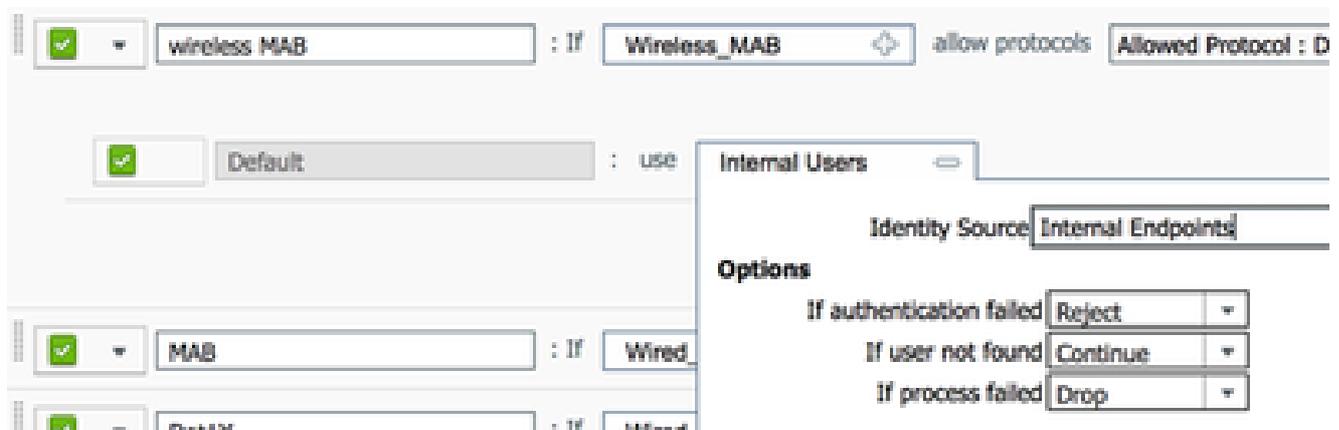
1. En el menú Directiva, haga clic en Autenticación.

Esta imagen muestra un ejemplo de cómo configurar la regla de política de autenticación. En este ejemplo, se configura una regla que se activará cuando se detecte el filtrado de MAC.



Cómo Configurar la Regla de Política

2. Introduzca un nombre para la regla de autenticación. En este ejemplo se utiliza Wireless mab.
3. Seleccione el icono más (+) en el campo Condición If.
4. Elija Condición compuesta y, a continuación, elija Wireless_MAB .
5. Elija Default network access as allowed protocol.
6. Haga clic en la flecha situada junto a y ... para expandir aún más la regla.
7. Haga clic en el icono + del campo Origen de identidad y seleccione Terminales internos.
8. Elija Continuar en la lista desplegable Si no se encuentra el usuario.



Haga clic en Continue

Esta opción permite autenticar un dispositivo (a través de webauth) incluso si se desconoce su dirección MAC. Los clientes Dot1x todavía pueden autenticarse con sus credenciales y no deben preocuparse por esta configuración.

Crear una regla de autorización

Ahora hay varias reglas que configurar en la directiva de autorización. Cuando la PC está asociada, pasará por el filtrado de MAC; se supone que la dirección MAC no se conoce, por lo que se devuelven la autenticación web y la ACL. Esta regla de MAC no conocido se muestra en la siguiente imagen y se configura en esta sección.

	2nd AUTH	if	Network: Access:UseCase EQUALS Guest Flow	then	vlan34
	IS-a-GUEST	if	IdentityGroup:Name EQUALS Guest	then	PermitAccess
	MAC not known	if	Network: Access:AuthenticationStatus EQUALS UnknownUser	then	CentralWebauth

MAC no conocido

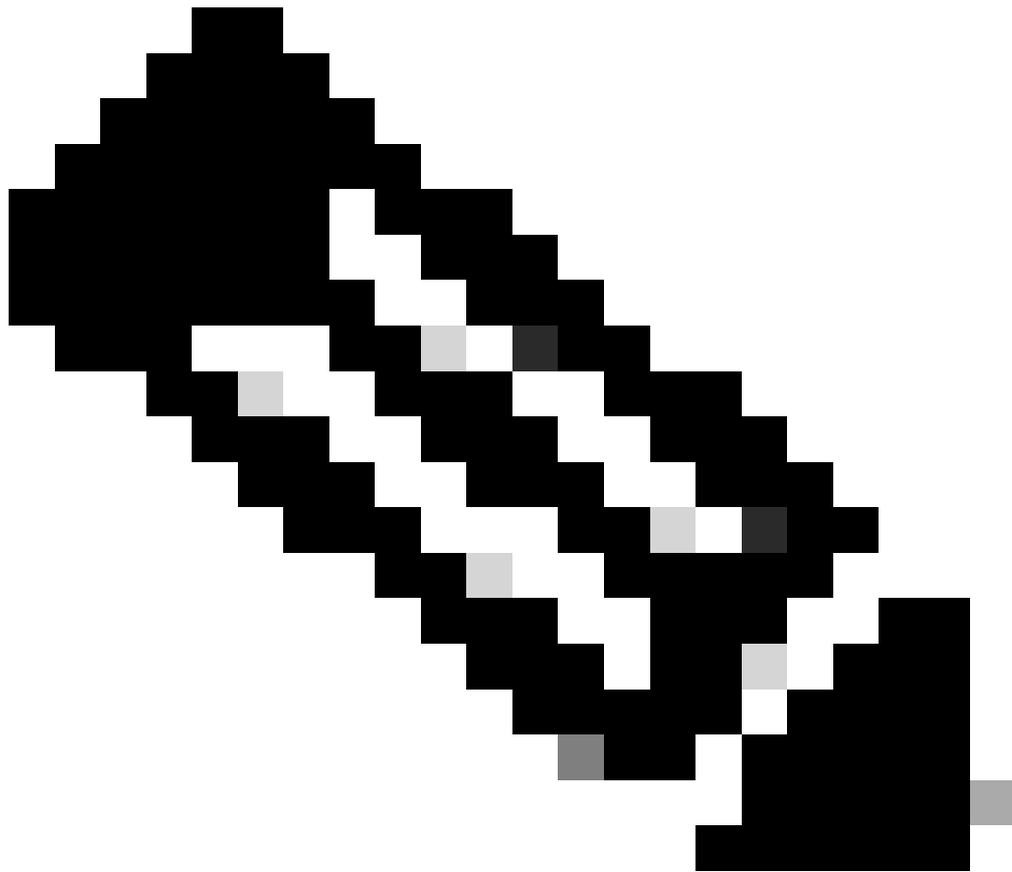
Complete estos pasos para crear la regla de autorización:

1. Cree una nueva regla e introduzca un nombre. Este ejemplo utiliza MAC no conocido.
2. Haga clic en el icono más (+) del campo de condición y elija crear una nueva condición.
3. Expanda la lista desplegable de expresiones.
4. Elija Network access y amplíelo.
5. Haga clic en AuthenticationStatus y elija el operador Equals.
6. Elija UnknownUser en el campo de la derecha.
7. En la página Autorización general, elija CentralWebauth ([Perfil de autorización](#)) en el campo situado a la derecha de la palabra then .

Este paso permite que ISE continúe aunque no se conozca al usuario (o MAC).

Los usuarios desconocidos ahora se muestran con la página de inicio de sesión. Sin embargo, una vez que introducen sus credenciales, se les vuelve a presentar una solicitud de autenticación en ISE; por lo tanto, se debe configurar otra regla con una condición que se cumpla si el usuario es un usuario invitado. En este ejemplo, Si UseridentityGroup es igual a Guestis se utiliza, y se supone que todos los invitados pertenecen a este grupo.

8. Haga clic en el botón de acciones ubicado al final de la regla MAC not known y elija insertar una nueva regla arriba.



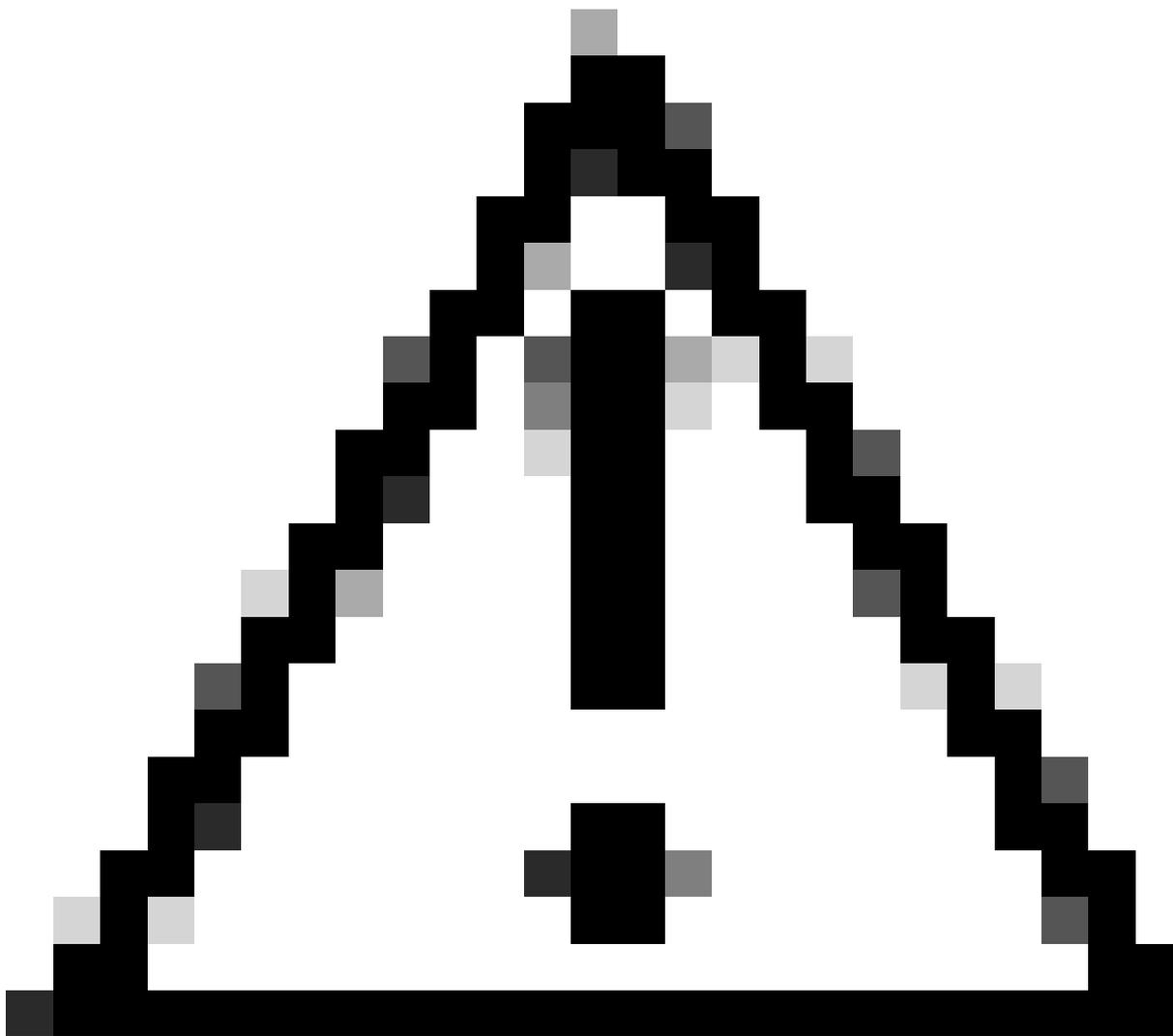
Nota: Es muy importante que esta nueva regla venga antes de la regla MAC no conocida.

9. Ingrese 2nd AUTH en el campo de nombre.
10. Seleccione un grupo de identidades como condición. En este ejemplo se elige Guest.
11. En el campo condición, haga clic en el icono más (+) y elija crear una nueva condición.
12. Elija Network Access , y haga clic en UseCase .
13. Elija Equals como operador.
14. Elija GuestFlow como el operando correcto. Esto significa que atrapará a los usuarios que acaban de iniciar sesión en la página web y volverán después de un cambio de autorización (la parte de flujo de invitados de la regla) y solo si pertenecen al grupo de identidad de invitados.
15. En la página de autorización, haga clic en el icono más (+) (situado junto a continuación)

para elegir un resultado para la regla.

En este ejemplo, se asigna un perfil preconfigurado (vlan34); esta configuración no se muestra en este documento.

Puede elegir una opción Permitir Acceso o crear un perfil personalizado para devolver la VLAN o los atributos que desee.



Precaución: en ISE versión 1.3, en función del tipo de autenticación web, ya no se puede encontrar el caso práctico de flujo de invitados. La regla de autorización tendría que contener el grupo de usuarios invitados como única condición posible.

Activar la renovación de IP (opcional)

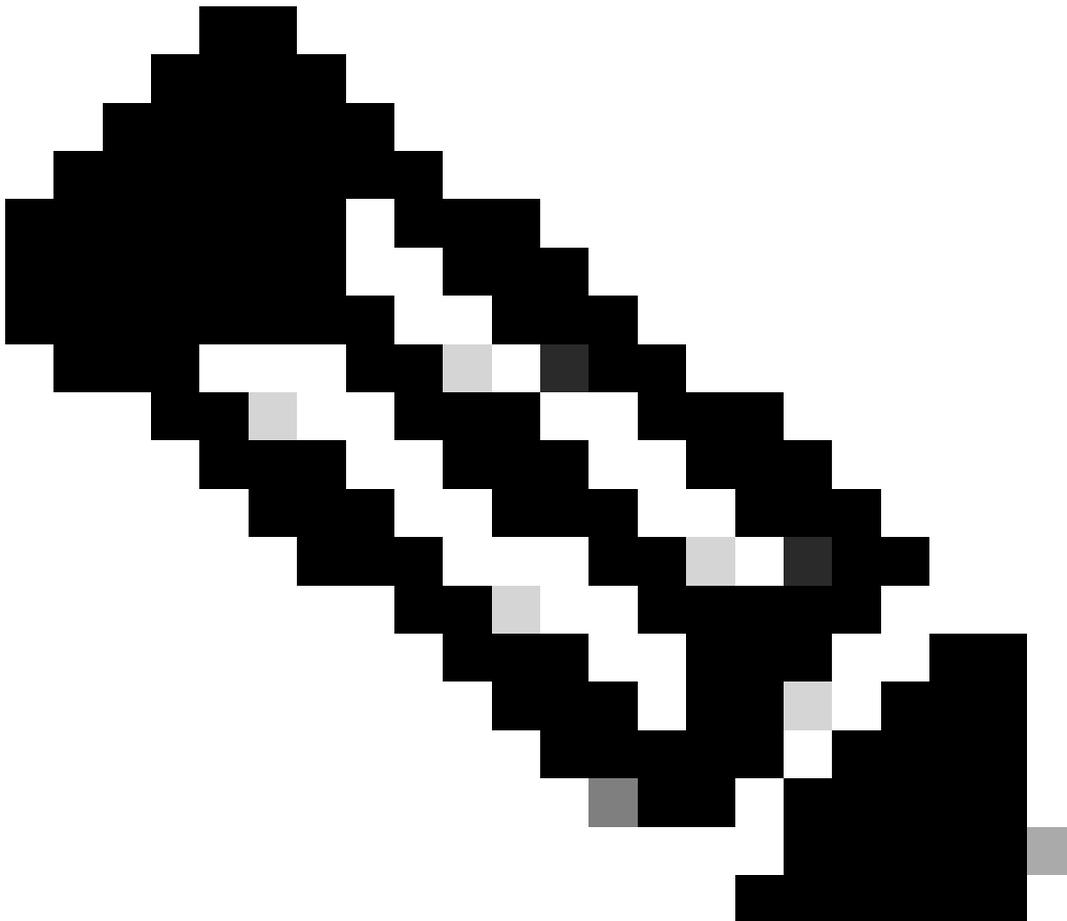
Si asigna una VLAN, el paso final es que el PC cliente renueve su dirección IP. Este paso lo consigue el portal de invitados para clientes de Windows. Si no configuró una VLAN para la regla

de 2nd AUTH anteriormente, puede omitir este paso.

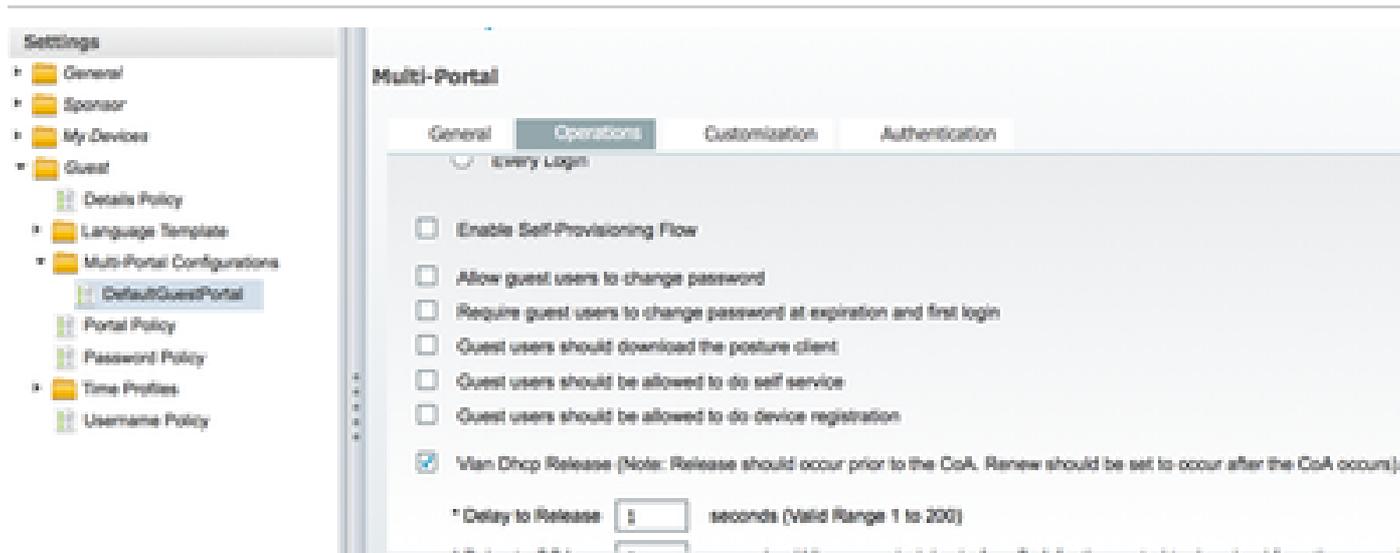
Tenga en cuenta que en los puntos de acceso FlexConnect, la VLAN debe preexistir en el propio punto de acceso. Por lo tanto, si no lo hace, puede crear una asignación VLAN-ACL en el propio AP o en el grupo flexible donde no aplique ninguna ACL para la nueva VLAN que desea crear. Esto crea una VLAN (sin ninguna ACL).

Si asignó una VLAN, complete estos pasos para habilitar la renovación de IP:

1. Haga clic en Administración y, a continuación, en Administración de invitados.
 2. Haga clic en Configuración.
 3. Expanda Invitado y, a continuación, Configuración multiportal.
 4. Haga clic en DefaultGuestPortal o en el nombre de un portal personalizado que haya creado.
 5. Haga clic en la casilla de verificación Vlan DHCP Release.
-



Nota: Esta opción sólo funciona para clientes de Windows.



Haga clic en la casilla de verificación Liberación de DHCP de VLAN

Flujo de tráfico

Puede parecer difícil entender qué tráfico se envía en qué lugar de este escenario. Aquí tiene una breve reseña:

- El cliente envía una solicitud de asociación por el aire para el SSID.
- El WLC maneja la autenticación de filtrado MAC con ISE (donde recibe los atributos de redirección).
- El cliente solo recibe una respuesta assoc después de que se haya completado el filtrado de MAC.
- El cliente envía una solicitud DHCP y el punto de acceso la conmuta LOCALMENTE para obtener una dirección IP del sitio remoto.
- En el estado Central_webauth, el tráfico marcado para negar en la ACL de redirección (por lo que HTTP normalmente) se conmuta CENTRALMENTE. Por lo tanto, no es el AP el que hace la redirección sino el WLC; por ejemplo, cuando el cliente solicita cualquier sitio web, el AP envía esto al WLC encapsulado en CAPWAP y el WLC falsifica esa dirección IP del sitio web y redirige hacia ISE.
- El cliente se redirige a la URL de redirección de ISE. Esto se conmuta de nuevo LOCALMENTE (porque alcanza el permiso en la ACL de redirección flexible).
- Una vez en el estado RUN, el tráfico se conmuta localmente.

Verificación

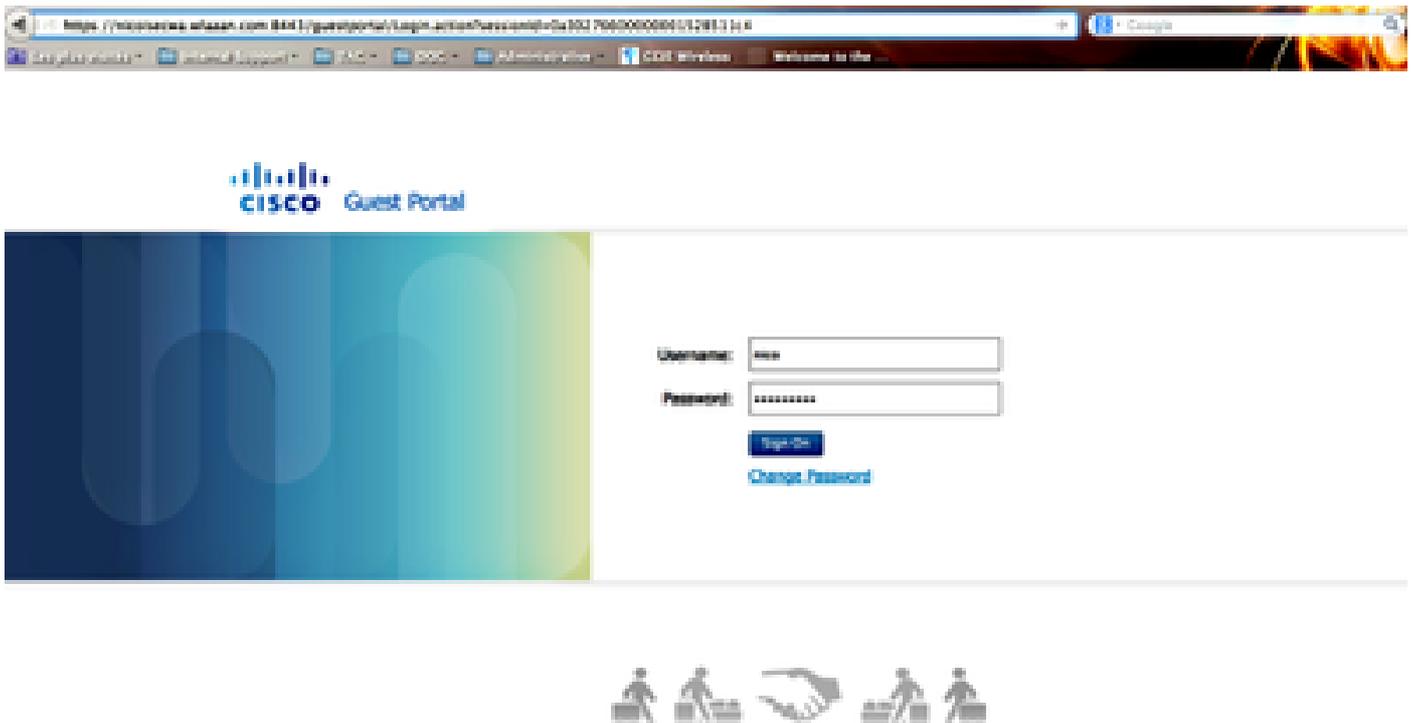
Una vez que el usuario está asociado al SSID, la autorización se muestra en la página de ISE.

Apr 09, 2013 11:48:27.179 AM	✔	🔒	Nico	08:13:06:21:76:13	nico@ic	Vlan34	Guest	NotApplicable
Apr 09, 2013 11:48:27.174 AM	✔	🔒			nico@ic			Dynamic Author...
Apr 09, 2013 11:48:58.073 AM	✔	🔒	Nico	08:13:06:21:76:13			Guest	Guest Authentic...
Apr 09, 2013 11:47:18.476 AM	✔	🔒		08:13:06:21:76:13	08:13:06:21:76:13	nico@ic	CentralWebauth	Pending Authentication ...

Se muestra la autorización

De abajo hacia arriba, puede ver la autenticación de filtrado de direcciones MAC que devuelve los atributos CWA. A continuación se muestra el inicio de sesión en el portal con el nombre de usuario. A continuación, ISE envía una CoA al WLC y la última autenticación es una autenticación de filtrado mac de capa 2 en el lado del WLC, pero ISE recuerda al cliente y al nombre de usuario y aplica la VLAN necesaria que configuramos en este ejemplo.

Cuando se abre cualquier dirección en el cliente, el navegador se redirige a ISE. Asegúrese de que el sistema de nombres de dominio (DNS) está configurado correctamente.



Redirigido a ISE

El acceso a la red se concede después de que el usuario acepte las directivas.



Signed on successfully
You can now type in the original URL in the browser's address bar.

You can now type in the original URL in the browser's address bar.



En el controlador, el estado del administrador de políticas y el estado RADIUS NAC cambian de POSTURE_REQD a RUN.

Información Relacionada

- [Soporte técnico y descargas de Cisco](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).