

Configuración de CWA inalámbrico y flujos de zonas Wi-Fi de ISE con AireOS y WLC de última generación

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuración del WLC de Unified 5508](#)

[Configuración global](#)

[Configuración del identificador del conjunto de servicios \(SSID\) del invitado:](#)

[Configuración de la ACL de redirección](#)

[Redirección de HTTPS](#)

[Conmutación por fallo agresiva](#)

[Bypass cautivo](#)

[Configuración de NGWC 3850 convergente](#)

[Configuración global](#)

[configuración SSID](#)

[Configuración de ACL de redireccionamiento](#)

[Configuración de la interfaz de línea de comandos \(CLI\)](#)

[Configuración de ISE](#)

[Tareas comunes de configuración de ISE](#)

[Caso práctico 1: CWA con autenticación de invitado en cada conexión de usuario](#)

[Caso práctico 2: CWA con Device Registration que aplica la autenticación de invitado una vez al día.](#)

[Caso práctico 3: portal HostSpot](#)

[Verificación](#)

[Caso práctico 1](#)

[Caso práctico 2](#)

[Caso práctico 3](#)

[Switching local FlexConnect en AireOS](#)

[Escenario de anclaje externo](#)

[Troubleshoot](#)

[Estados rotos comunes en AireOS y WLC de acceso convergente](#)

[WLC de AireOS](#)

[NGWC](#)

[ISE](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar tres casos de invitados en Identity Services Engine con Cisco AireOS y Next Generation Wireless LAN Controllers.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Controladores de LAN inalámbrica de Cisco (Unified and Converged Access)
- Identity Services Engine (ISE)

Componentes Utilizados

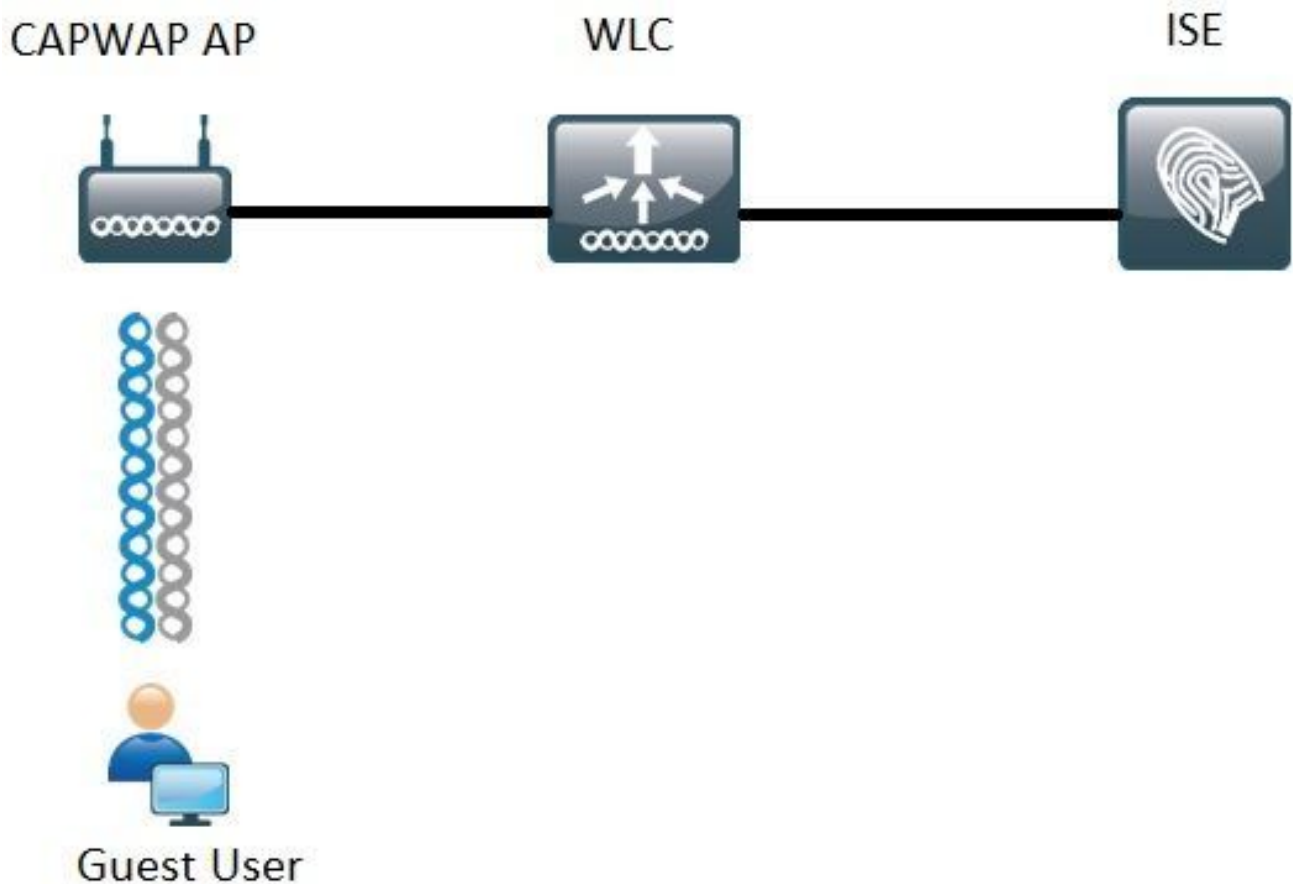
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Identity Services Engine versión 2.1
- Controlador Cisco Wireless LAN Controller 5508 con 8.0.121.0
- Controlador inalámbrico de última generación (NGWC) catalyst 3850 (WS-C3850-24P) con 3 de junio de 2004

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

Configurar

Diagrama de la red



Los pasos que se describen en este documento describen la configuración típica en los WLC de acceso unificado y convergente para admitir cualquier flujo de invitado con ISE.

Configuración del WLC de Unified 5508

Independientemente del caso práctico configurado en ISE, desde la perspectiva del WLC, todo comienza con un terminal inalámbrico que se conecta a un SSID abierto con el filtrado de MAC habilitado (más anulación de AAA y RADIUS NAC) que apunta a ISE como el servidor de autenticación y contabilidad. Esto garantiza que ISE pueda enviar dinámicamente los atributos necesarios al WLC para la aplicación correcta de una redirección al portal de invitados de ISE.

Configuración global

1. Agregue ISE globalmente como servidor de autenticación y cuentas.
 - Navegue hasta **Seguridad > AAA > Autenticación** y haga clic en **Nuevo**



- Introducir la IP del servidor ISE y el secreto compartido
- Asegúrese de que el Estado del servidor y **Soporte para RFC 3676** (Cambio de autorización o soporte de CoA) estén configurados en **Habilitado**.
- En el tiempo de espera del servidor de forma predeterminada, los WLC de AireOS tienen 2 segundos. Dependiendo de las características de la red (latencia, ISE y WLC en diferentes ubicaciones), puede ser beneficioso aumentar el tiempo de espera del servidor a al menos 5 segundos para evitar eventos de failover innecesarios.
- Haga clic en Apply (Aplicar).
- Si hay varios nodos de servicios de políticas (PSN) para configurar, continúe para crear entradas de servidor adicionales.

Nota: Este ejemplo de configuración en particular incluye 2 instancias de ISE

- Navegue hasta **Seguridad > AAA > RADIUS > Contabilización** y haga clic en **Nuevo**
- Introducir la IP del servidor ISE y el secreto compartido
- Asegúrese de que el Estado del servidor está establecido en **Activado**
- Aumente el tiempo de espera del servidor si es necesario (el valor predeterminado es 2 segundos).

2. Configuración de reserva.

En el entorno unificado una vez que se activa el tiempo de espera del servidor, el WLC se mueve al siguiente servidor configurado. Siguiendo en la línea desde WLAN. Si no hay otro disponible, el WLC selecciona el siguiente en la lista de servidores globales. Cuando se configuran varios servidores en el SSID (Primario, Secundario) una vez que ocurre el failover el WLC por defecto continúa enviando la autenticación y (o) el tráfico de la contabilidad permanentemente a la instancia secundaria incluso si el servidor primario está otra vez en línea.

Para mitigar este comportamiento, habilite la reserva. Vaya a **Security > AAA > RADIUS > Fallback**. El comportamiento predeterminado es desactivado. La única forma de recuperarse de un evento de caída del servidor requiere la intervención del administrador (rebotar globalmente el estado de administrador del servidor).

Para activar la reserva, dispone de dos opciones:

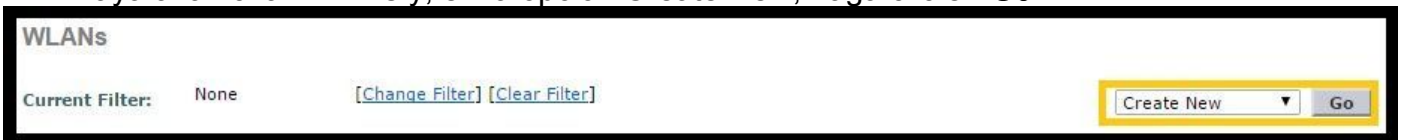
- **Pasivo** - En el modo pasivo, si un servidor no responde a la solicitud de la autenticación del WLC, el WLC mueve el servidor a la cola inactiva y fija un temporizador (opción del intervalo en el seg.). Cuando el temporizador expira, el WLC mueve el servidor a la cola activa independientemente del estado real de los servidores. Si la solicitud de autenticación da lugar a un evento de tiempo de espera (lo que significa que el servidor aún está inactivo), la entrada del servidor se mueve de nuevo a la cola Inactiva y el temporizador vuelve a funcionar. Si el servidor responde correctamente, permanece en la cola activa. Los valores configurables aquí van de 180 a 3600 segundos.
- **Activo** - En el modo activo, cuando un servidor no responde a la solicitud de autenticación del WLC, el WLC marca el servidor como muerto, luego mueve el servidor al pool de servidores no activo y comienza a enviar mensajes de sondeo periódicamente hasta que ese servidor responde. Si el servidor responde, entonces el WLC mueve el servidor muerto al pool activo y deja de enviar los mensajes de la sonda.

En este modo, el WLC requiere que ingrese un nombre de usuario y un intervalo de sondeo en segundos (180 a 3600).

Nota: La sonda WLC no requiere una autenticación exitosa. En cualquier caso, una autenticación exitosa o fallida se considera una respuesta del servidor que es suficiente para promover el servidor a la cola activa.

Configuración del identificador del conjunto de servicios (SSID) del invitado:

- Vaya a la ficha WLANs y, en la opción Create New, haga clic en Go:



- Introduzca el nombre del perfil y el nombre SSID. Haga clic en Apply (Aplicar).
- En la ficha General (General), seleccione la interfaz o el grupo de interfaces que se utilizará (VLAN de invitado).



- En **Seguridad** > Capa 2 > Seguridad de Capa 2, seleccione **Ninguno** y active la casilla de verificación **Filtrado Mac**.



- En la pestaña **Servidores AAA**, establezca Servidores de autenticación y contabilidad en **habilitados** y seleccione sus servidores primarios y secundarios.



- **Actualización Interina:** Esta es una configuración opcional que no agrega ningún beneficio a este flujo. Si prefiere habilitarlo, el WLC i debe ejecutar el código 8.x o superior:

Desactivado: la función está completamente desactivada.

Habilitado con Intervalo 0: El WLC envía actualizaciones de contabilidad a ISE cada vez que hay un cambio en la entrada Mobile Station Control Block (MSCB) del cliente (ie. asignación o cambio de dirección IPv4 o IPv6, evento de itinerancia de cliente.) No se envían actualizaciones periódicas adicionales.

Habilitado con un intervalo interino configurado: en este modo, el WLC envía notificaciones a ISE sobre los cambios de entrada de MSCB del cliente y también envía notificaciones de contabilidad periódicas adicionales en el intervalo configurado (independientemente de cualquier cambio).

- En Advanced Tab Enable **Allow AAA Override** y en **NAC state** seleccione **RADIUS NAC**. Esto garantiza que el WLC aplique cualquier par de valores de atributo (AVP) que provenga de ISE.
- Vaya a la ficha general SSID y establezca el estado de SSID en **Activado**

WLANs > Edit 'Guest'

General	Security	QoS	Policy-Mapping	Advanced
Profile Name	Guest			
Type	WLAN			
SSID	Guest			
Status	<input checked="" type="checkbox"/> Enabled			

- Aplique los cambios.

Configuración de la ACL de redirección

ISE hace referencia a esta ACL y determina qué tráfico se redirige y a qué tráfico se permite acceder.

- Vaya a **Security Tab > Access Control Lists** y haga clic en **New**
- Este es un ejemplo de ACL

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	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Any	0
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Any	0
3	Permit	0.0.0.0 / 0.0.0.0	157.210 / 255.255.255.255	TCP	Any	8443	Any	Any	0
4	Permit	157.210 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	8443	Any	Any	Any	0
5	Permit	0.0.0.0 / 0.0.0.0	157.21 / 255.255.255.255	TCP	Any	8443	Any	Any	0
6	Permit	157.21 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	8443	Any	Any	Any	0

Esta ACL debe permitir el acceso desde y hacia los servicios DNS y los nodos ISE a través del puerto TCP 8443. Hay una denegación implícita en la parte inferior que significa que el resto del tráfico se redirige a la URL del portal de invitados de ISE.

Redirección de HTTPS

Esta función es compatible con las versiones 8.0.x y posteriores de AireOS, pero está desactivada de forma predeterminada. Para habilitar el soporte HTTPS vaya a **WLC Management > HTTP-HTTPS > HTTPS Redirection** y configúrelo en **Enabled** o aplique este comando en CLI:

```
(Cisco Controller) >config network web-auth https-redirect enable
```

Advertencias de certificado después de habilitar el redireccionamiento HTTPS

Después de habilitar https-redirect, el usuario puede experimentar problemas de confianza de certificados durante el redireccionamiento. Esto se observa incluso si hay un certificado en cadena válido en el controlador e incluso si este certificado está firmado por una autoridad de certificación de confianza de terceros. La razón es que el certificado instalado en el WLC se emite a su nombre de host de interfaz virtual o dirección IP. Cuando el cliente intenta <https://cisco.com>, el navegador espera que el certificado se emita a cisco.com. Sin embargo, para que el WLC pueda interceptar el GET emitido por el cliente, primero necesita establecer la sesión HTTPS para la cual el WLC presenta su certificado de interfaz virtual durante la fase de intercambio de señales SSL. Esto hace que el navegador muestre una advertencia ya que el certificado presentado durante el intercambio de señales SSL no se ha emitido al sitio web original al que el cliente está intentando acceder (por ejemplo, cisco.com opuesto al nombre de host de la interfaz virtual del WLC). Puede ver diferentes mensajes de error de certificado en diferentes navegadores, pero todos están relacionados con el mismo problema.

Conmutación por fallo agresiva

Esta función está habilitada de forma predeterminada en los WLC de AireOS. Cuando se habilita la conmutación por fallas agresiva, el WLC marca el servidor AAA como no responsivo y se mueve al siguiente servidor AAA configurado después de que un evento de tiempo de espera RADIUS afecte a un cliente.

Cuando la función está inhabilitada el WLC conmuta por error al servidor siguiente solamente si el evento de tiempo de espera de RADIUS ocurre con por lo menos 3 sesiones del cliente. Esta función se puede inhabilitar mediante este comando (no es necesario reiniciar para este comando):

```
(Cisco Controller) >config radius aggressive-failover disable
```

Para verificar el estado actual de la función:

```
(Cisco Controller) >show radius summary
```

```
Vendor Id Backward Compatibility..... Disabled
Call Station Id Case..... lower
Acct Call Station Id Type..... Mac Address
Auth Call Station Id Type..... AP's Radio MAC Address:SSID
Extended Source Ports Support..... Enabled
Aggressive Failover..... Disabled
```

Bypass cautivo

Los terminales que admiten un mecanismo de Asistente de red cautiva (CNA) para detectar un portal cautivo e iniciar automáticamente una página de inicio de sesión suelen hacerlo a través de un pseudoexplorador en una ventana controlada, mientras que otros terminales inician un explorador totalmente compatible para activarlo. En el caso de los terminales en los que el CNA inicia un pseudonavegador, esto puede interrumpir el flujo cuando se redirige a un portal cautivo de ISE. Esto suele afectar a los dispositivos Apple IOS y tiene efectos especialmente negativos

en los flujos que requieren el registro del dispositivo, VLAN DHCP-Release, verificación de cumplimiento.

Depender de la complejidad del flujo en uso, se puede recomendar para habilitar el desvío cautivo. En tal escenario, el WLC ignora el mecanismo de detección del portal CNA y el cliente necesita abrir un navegador para iniciar el proceso de redirección.

Verifique el estado de la función:

```
(Cisco Controller) >show network summary

Web Auth CMCC Support ..... Disabled
Web Auth Redirect Ports ..... 80,3128
Web Auth Proxy Redirect ..... Disable
Web Auth Captive-Bypass ..... Disabled
Web Auth Secure Web ..... Enable
Web Auth Secure Redirection ..... Enable
```

Para habilitar esta característica, escriba este comando:

```
(Cisco Controller) >config network web-auth captive-bypass enable
Web-auth support for Captive-Bypass will be enabled.
```

You must reset system for this setting to take effect.

El WLC avisa al usuario que para que los cambios tengan efecto se necesita un sistema de reinicio (reinicio).

En este punto, un **show network summary** muestra la función como habilitada, pero para que los cambios tengan efecto, el WLC debe reiniciarse.

Configuración de NGWC 3850 convergente

Configuración global

1. Agregar ISE globalmente como servidor de autenticación y contabilidad

- Navegue hasta **Configuration > Security > RADIUS > Servers** y haga clic en **New**
- Introduzca la **dirección IP del servidor ISE**, el **secreto compartido**, el **tiempo de espera del servidor** y el **recuento de reintentos** que refleje sus condiciones ambientales.
- Asegúrese de que **Support for RFC 3570 (CoA support)** esté habilitado.
- Repita el proceso para agregar una entrada del servidor secundario.

RADIUS Servers

Radius Servers > **New**

Server Name

Server IP Address

Shared Secret

Confirm Shared Secret

Auth Port (0-65535)

Acct Port (0-65535)

Server Timeout (1-1000)secs

Retry Count (0-100)

Support for RFC 3576 ▾

2. Crear el grupo de servidores de ISE

- Navegue hasta **Configuration > Security > Server Groups** y haga clic en **New**
- Asigne un nombre al grupo e introduzca un valor **de tiempo muerto** en minutos. Este es el tiempo que el controlador mantiene al servidor en la cola Inactiva antes de que se promueva nuevamente a la lista de servidores activos.
- En la lista Servidores disponibles, agréguelos a la columna Servidores asignados.

Radius Server Group

Radius Server Group > **New**

Name

MAC-delimiter ▾

MAC-filtering ▾

Dead-time (0-1440) in minutes

Group Type

Servers In This Group

Available Servers

< >

Assigned Servers

ISE2

ISE1

3. Habilitación global de Dot1x

- Vaya a **Configuration > AAA > Method Lists > General** y habilite **Dot1x system Auth Control**

General

Dot1x System Auth Control

Local Authentication

Local Authorization

4. Configurar listas de métodos

- Navegue hasta **Configuration > AAA > Method Lists > Authentication** y cree una nueva lista de métodos. En este caso, es Type Dot1x y Group ISE_Group (grupo creado en el paso anterior). A continuación, pulse **Aplicar**

Authentication
Authentication > New

Method List Name

Type: dot1x login

Group Type: group local

Fallback to local

Groups In This Method

Available Server Groups

Assigned Server Groups

ISE_Group

- Haga lo mismo para la contabilización (**Configuración > AAA > Listas de métodos > contabilidad**) y la autorización (**Configuración > AAA > Listas de métodos > Autorización**). Deben tener este aspecto

Accounting
Accounting > New

Method List Name

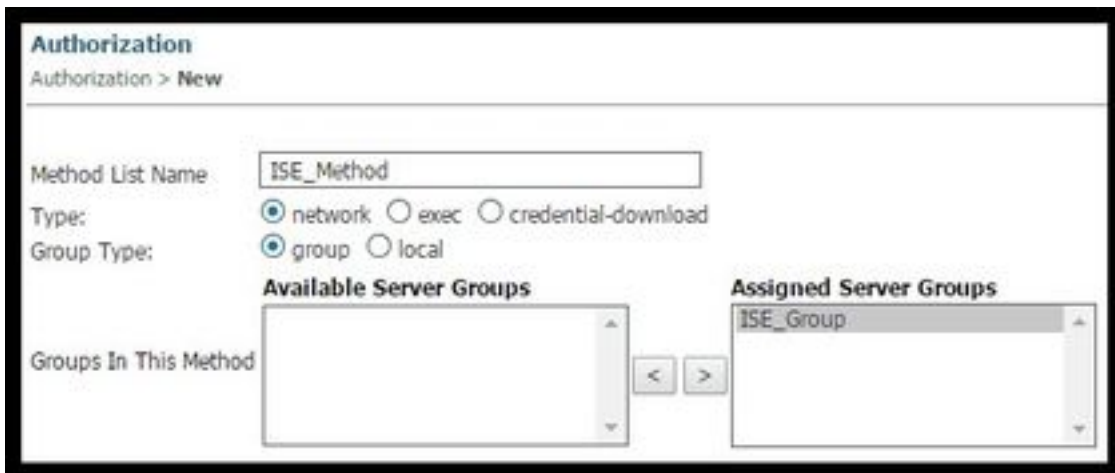
Type: dot1x exec identity network commands

Groups In This Method

Available Server Groups

Assigned Server Groups

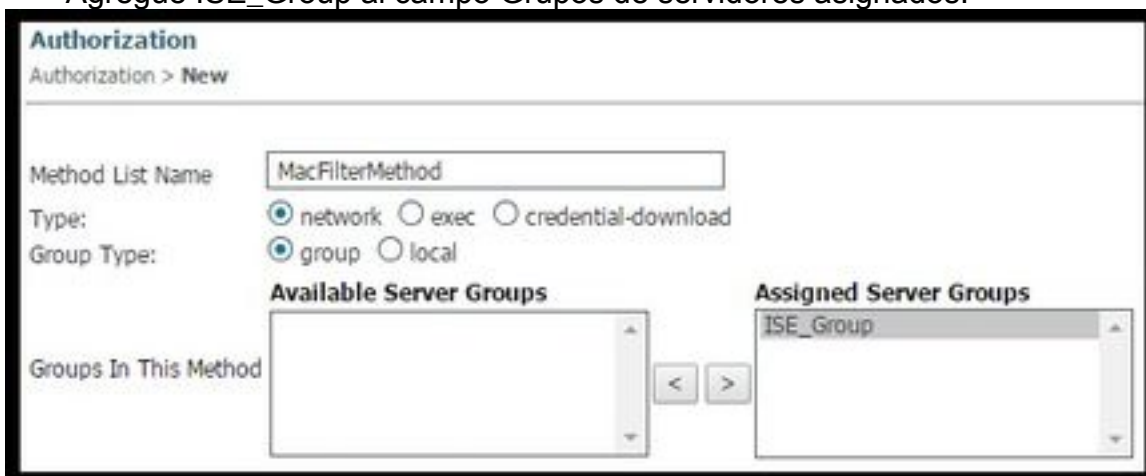
ISE_Group



5. Cree el método de filtro MAC de autorización.

Posteriormente, se realiza una llamada desde la configuración de SSID.

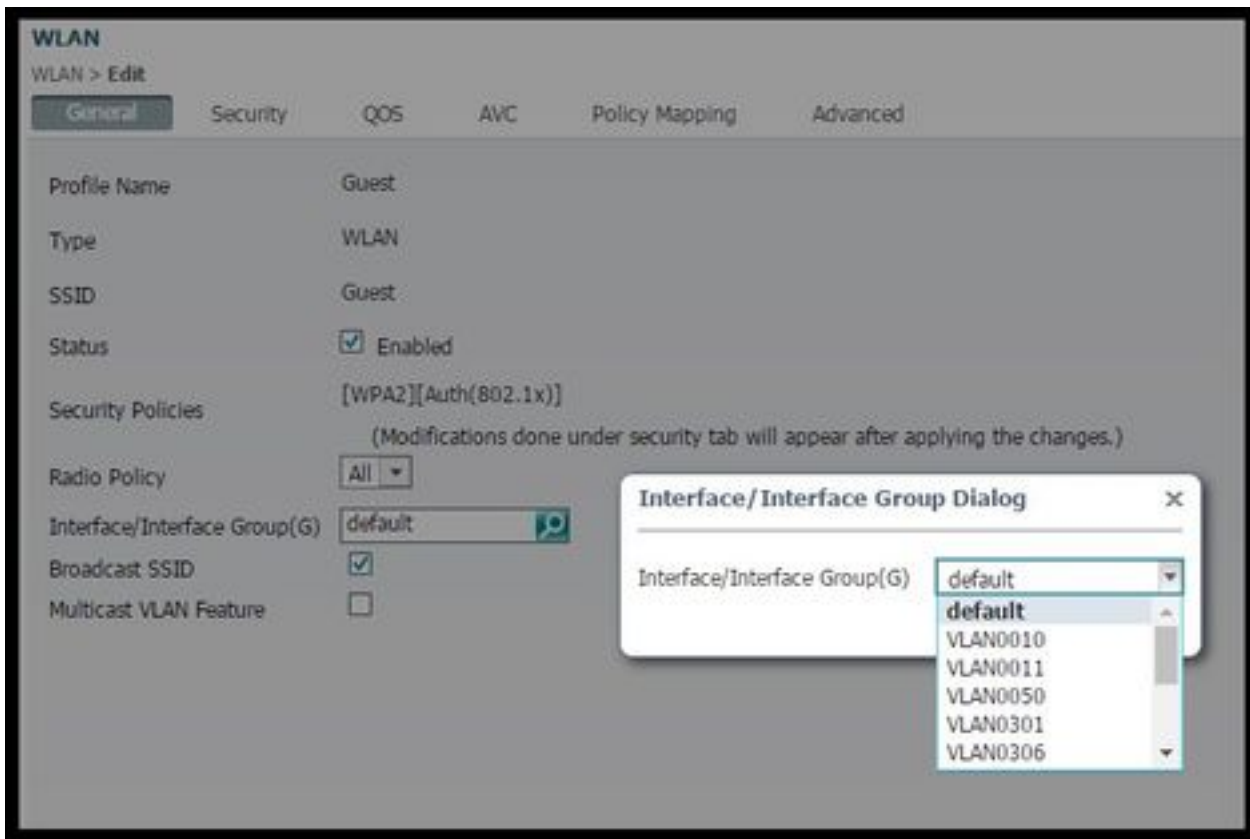
- Navegue hasta **Configuration > AAA > Method Lists > Authorization** y haga clic en **New**.
- Introduzca el **nombre de la lista de métodos**. Elija **Tipo = Red** y **Grupo Tipo**.
- Agregue ISE_Group al campo Grupos de servidores asignados.



configuración SSID

1. Cree el SSID de invitado

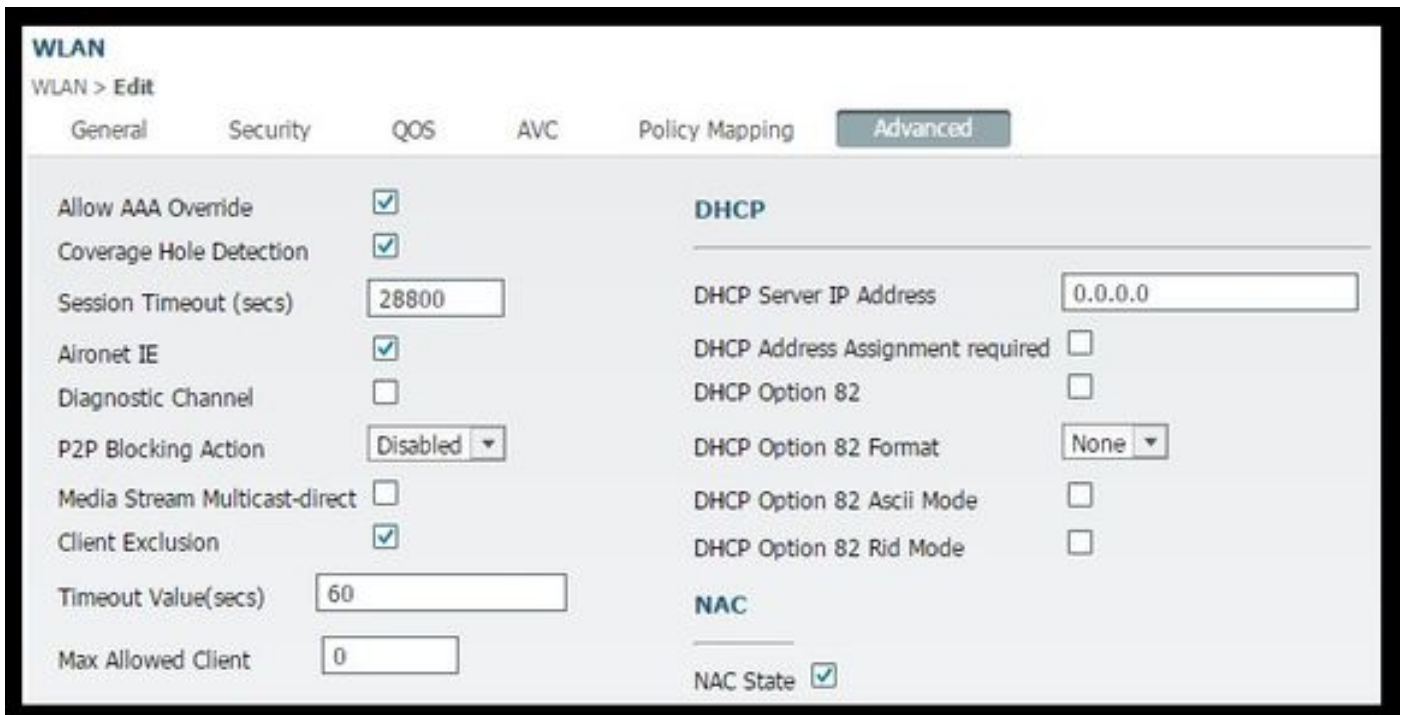
- Navegue hasta **Configuration > Wireless > WLANs** y haga clic en **New**
- Introduzca el ID de WLAN, SSID y nombre de perfil y haga clic en **Apply** (Aplicar).
- Una vez en la configuración de SSID en **Interface / Interface Group** (Interfaz / Grupo de interfaz) seleccione la interfaz de capa 3 de VLAN de invitado.



- En **Security > Layer 2**, seleccione **None** y, junto a **Mac Filtering**, introduzca el nombre de la lista de métodos de filtrado de Mac que configuró anteriormente (MacFilterMethod).
- En la pestaña **Seguridad > Servidor AAA**, seleccione las listas de métodos de autenticación y contabilidad (ISE_Method) adecuadas.



- En la pestaña **Advanced**, habilite **Allow AAA Override** y **NAC state**. El resto de la configuración debe ajustarse según los requisitos de cada implementación (tiempo de espera de sesión, exclusión de clientes, compatibilidad con extensiones Aironet).



- Vaya a la ficha General y establezca el valor de Status (Estado) en Enabled (Activado). A continuación, pulse **Aplicar**.

Configuración de ACL de redireccionamiento

ISE hace referencia a esta ACL más adelante en access-accept en respuesta a la solicitud MAB inicial. La NGWC lo utiliza para determinar el tráfico que se debe redirigir y el que se debe permitir que pase.

- Navegue hasta **configuration > security > ACL > Access Control Lists** y haga clic en **Add New**.
- Seleccione Extended e introduzca el nombre de ACL.
- Esta imagen muestra un ejemplo de una lista de control de acceso redirigida típica:



Nota: la línea 10 es opcional. Esto se suele agregar para las propuestas de solución de

problemas. Esta ACL debe permitir el acceso a los servicios DHCP y DNS, así como al puerto TCP 8443 (denegar ACE) de los servidores ISE. El tráfico HTTP y HTTPS se redirige (permitir ACE).

Configuración de la interfaz de línea de comandos (CLI)

Toda la configuración descrita en los pasos anteriores también se puede aplicar a través de la CLI.

802.1x habilitado globalmente

```
dot1x system-auth-control
```

Configuración AAA global

```
aaa new-model
!
aaa authentication dot1x ISE_Method group ISE_Group
aaa authorization network ISE_Method group ISE_Group
aaa authorization network MacFilterMethod group ISE_Group
aaa accounting Identity ISE_Method start-stop group ISE_Group
!
aaa server radius dynamic-author
  client 172.16.157.210 server-key *****
  client 172.16.157.21 server-key *****
  auth-type any
!
radius server ISE1
  address ipv4 172.16.157.210 auth-port 1812 acct-port 1813
  timeout 5
  retransmit 2
  key *****
!
radius server ISE2
  address ipv4 172.16.157.21 auth-port 1812 acct-port 1813
  timeout 5
  retransmit 2
  key *****
!
!
aaa group server radius ISE_Group
  server name ISE2
  server name ISE1
  deadtime 10
  mac-delimiter colon
!
```

Configuración de WLAN

```
wlan Guest 1 Guest
aaa-override
accounting-list ISE_Method
client vlan VLAN0301
mac-filtering MacFilterMethod
nac
```

```
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security dot1x authentication-list ISE_Method
no security ft over-the-ds
session-timeout 28800
no shutdown
```

Ejemplo de ACL de Redireccionamiento

```
3850#show ip access-lists Guest_Redirect
Extended IP access list Guest_Redirect
 10 deny icmp any any
 20 deny udp any any eq bootps
 30 deny udp any any eq bootpc
 40 deny udp any any eq domain
 50 deny tcp any host 172.16.157.210 eq 8443
 60 deny tcp any host 172.16.157.21 eq 8443
 70 permit tcp any any eq www
 80 permit tcp any any eq 443
```

Compatibilidad con HTTP y HTTPS

```
3850#show run | inc http
ip http server
ip http secure-server
```

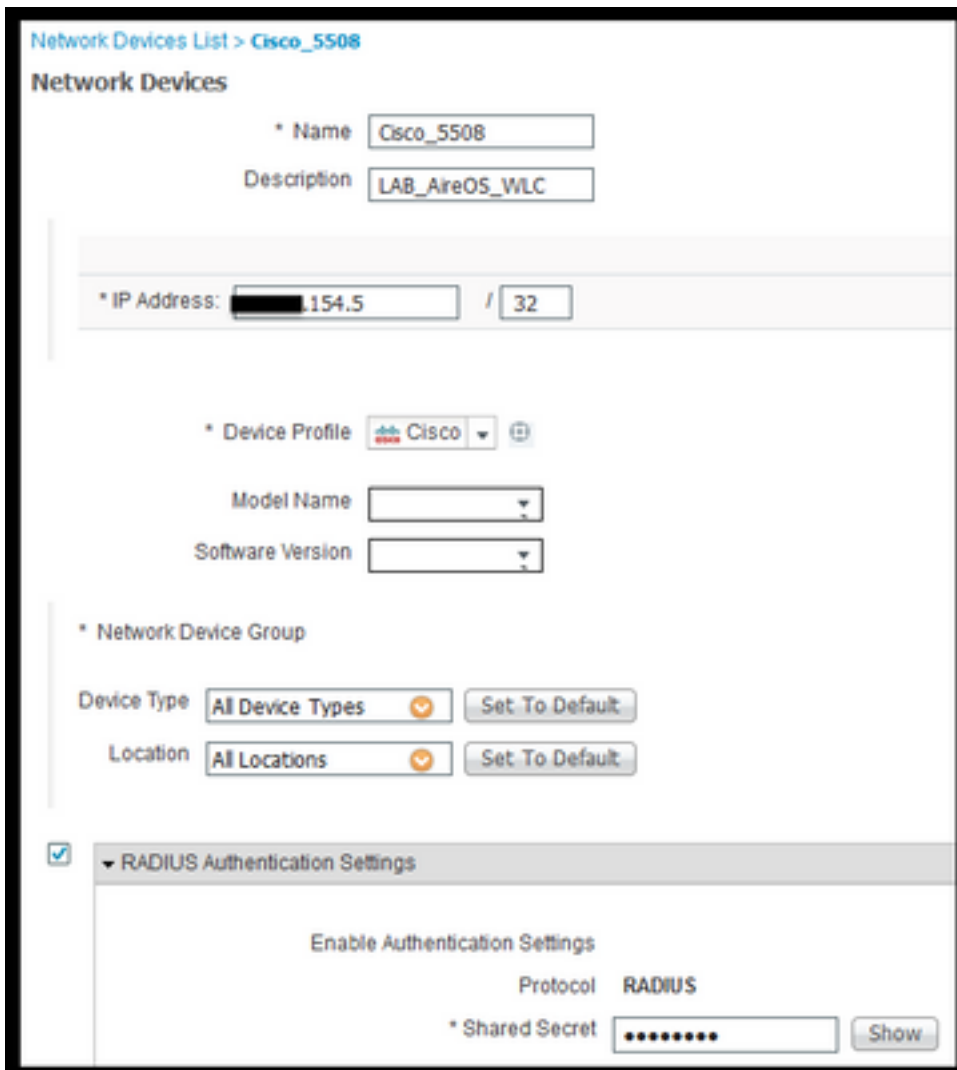
Nota: Si aplica una ACL para restringir el acceso al WLC sobre HTTP, afecta la redirección.

Configuración de ISE

En esta sección se describe la configuración necesaria en ISE para admitir todos los casos prácticos que se describen en este documento.

Tareas comunes de configuración de ISE

1. Inicie sesión en ISE y navegue hasta **Administration > Network Resources > Network Devices** y haga clic en **Add** .
2. Ingrese el **nombre** asociado al WLC y la **dirección IP** del dispositivo.
3. Marque la casilla **RADIUS authentication settings** y escriba el **Shared Secret** configurado en el lado del WLC. A continuación, haga clic en **Enviar**.

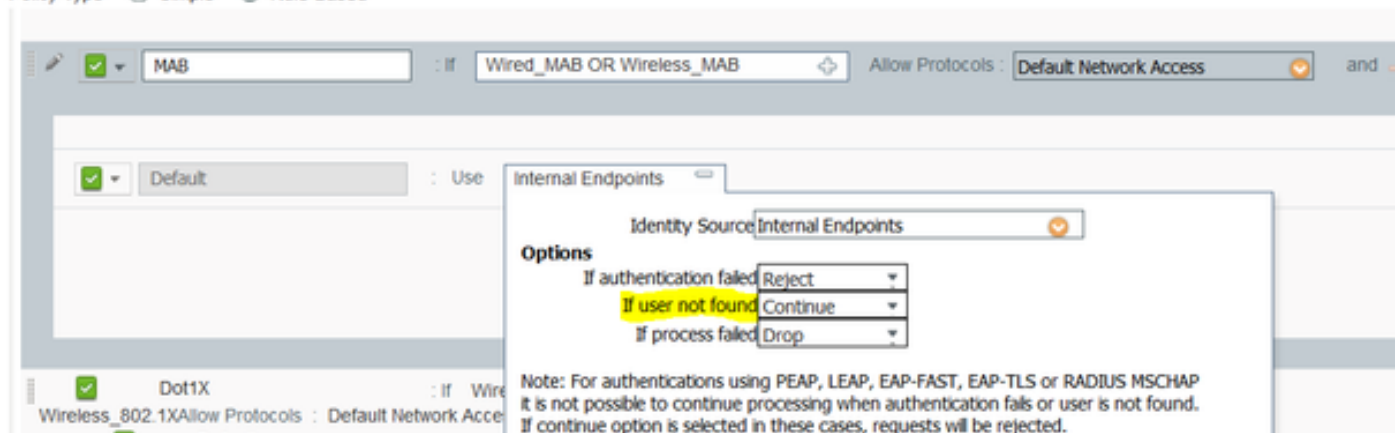


4. Navegue hasta Directiva > Autenticación y en MAB haga clic en Editar y asegúrese de que en **Uso: Terminales Internos** la opción **Si no se encuentra el usuario** esté establecida en Continuar (debe estar allí de forma predeterminada).

Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication. For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Policy Type Simple Rule-Based



Caso práctico 1: CWA con autenticación de invitado en cada conexión de usuario

Visión general de flujo

1. El usuario inalámbrico se conecta al SSID de invitado.

2. El WLC autentica el terminal en función de su dirección MAC en ISE como servidor AAA.
3. ISE devuelve y acepta el acceso con dos pares de valores de atributo (AVP): url-redirect y url-redirect-acl. Una vez que el WLC aplica estos AVPs a la sesión del terminal, la estación pasa a DHCP-Required y una vez que toma una dirección IP permanece en CENTRAL_WEB_AUTH. En este paso el WLC está listo para comenzar a redirigir el tráfico http / https del cliente.
4. El usuario final abre el navegador web y una vez que se genera el tráfico HTTP o HTTPS, el WLC redirige al usuario al portal de invitados de ISE.
5. Una vez que el usuario llega al portal de invitados, se le solicita que introduzca las credenciales de invitado (creadas por el patrocinador en este caso).
6. Tras la validación de credenciales, ISE muestra la página AUP y, una vez que el cliente acepta, se envía al WLC un tipo de CoA dinámico Volver a autenticar.
7. El WLC vuelve a procesar la autenticación de filtrado de MAC sin emitir una desautenticación a la estación móvil. Esto debe realizarse sin problemas hasta el terminal.
8. Una vez que se produce el evento de reautenticación, ISE vuelve a evaluar las políticas de autorización y, en esta ocasión, el terminal recibe un acceso de permiso, ya que anteriormente se producía un evento de autenticación de invitado correcto.

Este proceso se repite cada vez que el usuario se conecta al SSID.

Configuración

1. Navegue hasta ISE y navegue hasta **Centros de trabajo > Acceso de invitado > Configurar > Portales de invitado > Seleccionar Portal de invitado patrocinado** (o cree un nuevo tipo de portal Patrocinado-Invitado).
2. En **Guest Device Registration settings** uncheck all options and click **Save**.



3. Acceda a **Política > Elementos de Política > Resultados > Autorización > Perfiles de Autorización**. Haga clic en Add (Agregar).

4. Este perfil se empuja hacia abajo al WLC el **Redirect-URL** y el **Redirect-URL-ACL** en respuesta a la solicitud de derivación de autenticación Mac (MAB) inicial.

- Una vez que la redirección web (CWA, MDM, NSP, CPP) marca, seleccione Centralized Web Auth, luego ingrese el nombre de ACL de redirección en el campo ACL y en **Value**, seleccione **Sponsored Guest Portal**(default) o cualquier otro portal específico creado en pasos anteriores.

El perfil debe tener un aspecto similar al de esta imagen. A continuación, haga clic en **Guardar**.

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

Common Tasks

Web Redirection (CWA, MDM, NSP, CPP) (i)

Centralized Web Auth ACL Value

Display Certificates Renewal Message

Static IP/Host name/FQDN

Los detalles de atributo en la parte inferior de la página incluyen los pares de valores de atributo (AVP) a medida que se envían al WLC

Attributes Details

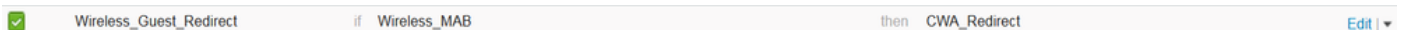
```
Access Type = ACCESS_ACCEPT
cisco-av-pair = url-redirect-acl=Guest_Redirect
cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=a65b8890-2230-11e6-99ab-005056bf55e0&daysToExpiry=value&action=cwa
```

5. Navegue hasta **Política > Autorización** e inserte una nueva regla. Esta regla es la que dispara el proceso de redirección en respuesta a la solicitud de autenticación MAC inicial del WLC. (En este caso llamada **Wireless_Guest_Redirect**).

6. En **Condiciones**, seleccione **Seleccionar Condición Existente de Biblioteca** y, a continuación, en **nombre de condición**, seleccione **Condición Compuesta**. Seleccione una condición compuesta predefinida denominada **Wireless_MAB**.

Nota: Esta condición consta de 2 atributos Radius esperados en la solicitud de acceso originada desde el WLC (NAS-Port-Type= IEEE 802.11 <presente en todas las solicitudes inalámbricas> y Service-Type = Call Check< que se refiere a una solicitud específica para una derivación de autenticación MAC>)

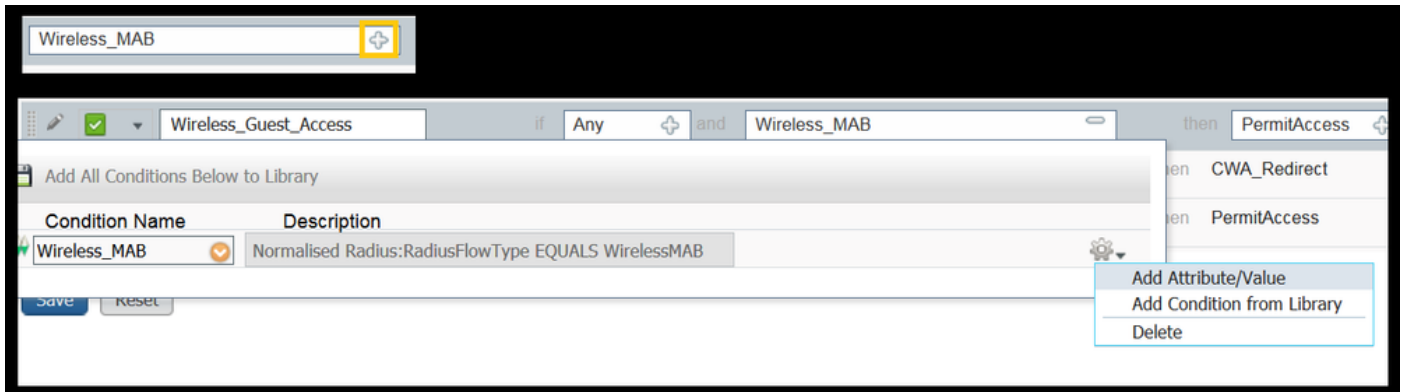
7. En resultados, seleccione **Estándar > CWA_Redirect** (Perfil de autorización creado en el paso anterior). A continuación, haga clic en **Finalizado** y **Guardar**



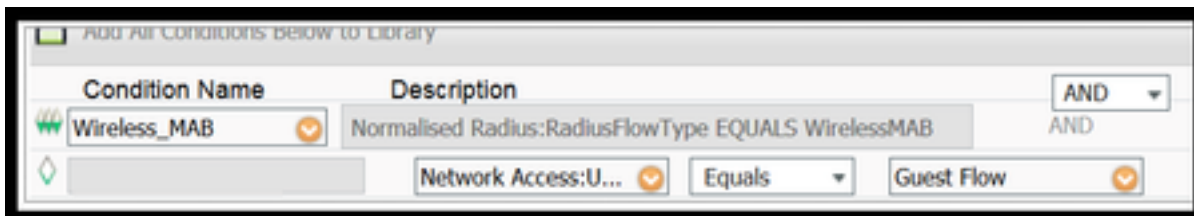
8. Desplácese hasta el final de la regla **CWA_Redirect** y haga clic en la flecha situada junto a **Editar**. A continuación, seleccione **duplicar arriba**.

9. Modifique el nombre, ya que se trata de la política con la que coincide el terminal una vez que la sesión se ha vuelto a autenticar en la CoA de ISE (en este caso, Wireless_Guest_Access).

10. Junto a la condición compuesta **Wireless_MAB**, haga clic en el símbolo + para expandir las condiciones y, al final de la condición **Wireless_MAB**, haga clic en **Agregar atributo/valor**.



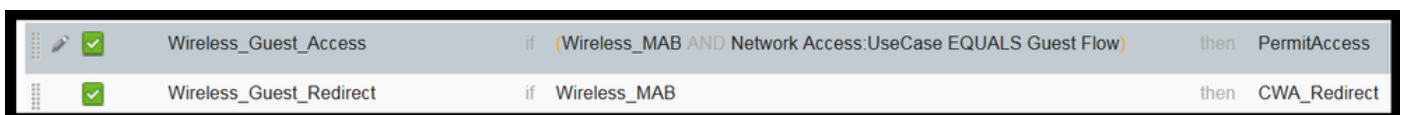
11. En "Seleccionar atributo", seleccione **Network Access > UseCase Equals Guest flow**



12. En **Permisos**, seleccione **PermisoAcceso**. A continuación, haga clic en **Finalizado** y **Guardar**



Las dos políticas deben tener un aspecto similar al siguiente:



Caso práctico 2: CWA con Device Registration que aplica la autenticación de invitado una vez al día.

Visión general de flujo

1. El usuario inalámbrico se conecta al SSID de invitado.
2. El WLC autentica el terminal en función de su dirección MAC en ISE como servidor AAA.
3. ISE devuelve y acepta el acceso con dos pares de valores de atributo (AVP) (url-redirect y url-redirect-acl).
4. Una vez que el WLC aplica este AVPs a la sesión del terminal, la estación pasa a DHCP-Required y una vez que toma una dirección IP permanece en CENTRAL_WEB_AUTH. En este paso el WLC está listo para comenzar a redirigir el tráfico http / https del cliente.
5. El usuario final abre el navegador web y una vez que se genera el tráfico HTTP o HTTPS, el WLC redirige al usuario al portal de invitados de ISE.
6. Una vez que el usuario llega al portal de invitados, se le solicita que introduzca las

credenciales creadas por el patrocinador.

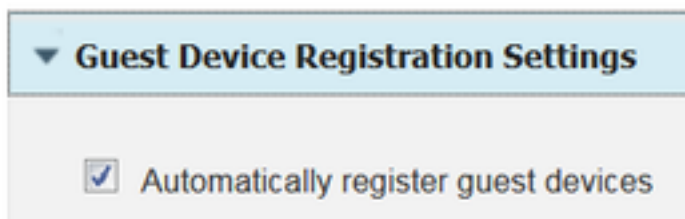
7. Tras la validación de credenciales, ISE agrega este terminal a un grupo de identidad de terminal (registro de dispositivo) específico (preconfigurado).
8. Se muestra la página AUP y, una vez que el cliente acepta, se vuelve a autenticar un tipo de CoA dinámico. Se envía al WLC.
9. El WLC para volver a procesar la autenticación de filtrado de MAC sin emitir una desautenticación a la estación móvil. Esto debe realizarse sin problemas hasta el terminal.
10. Una vez que se produce el evento de reautenticación, ISE vuelve a evaluar las políticas de autorización. Esta vez, dado que el terminal es miembro del grupo de identidad de terminal correcto, ISE devuelve un access accept sin restricciones.
11. Dado que el terminal se ha registrado en el paso 6, cada vez que el usuario vuelve, se le permite trabajar en la red hasta que se elimine manualmente de ISE, o bien se ejecute una política de depuración de terminales vaciando los terminales que cumplan los criterios.

En esta situación de laboratorio, la autenticación se aplica una vez al día. El desencadenador de reautenticación es Endpoint Purge Policy, que quita todos los extremos del grupo de identidad de terminales usado todos los días.

Nota: es posible aplicar el evento de autenticación de invitado en función del tiempo transcurrido desde la última aceptación de la PUA. Puede ser una opción si necesita aplicar el inicio de sesión de invitado más a menudo que una vez al día (por ejemplo, cada 4 horas).

Configuración

1. En ISE, vaya a **Centros de trabajo > Acceso de invitado > Configurar > Portales de invitado > Seleccionar Portal de invitado patrocinado** (o cree un nuevo tipo de portal Patrocinado-Invitado).
2. En **Guest Device Registration** , verifique que la opción **Automatically register guest devices** esté marcada. Click **Save**.



3. Vaya a **Centro de trabajo > Acceso de invitado > Configurar > Tipos de invitado** o simplemente haga clic en el acceso directo especificado en Configuración de registro de dispositivo de invitado en el portal.

▼ Guest Device Registration Settings

Automatically register guest devices

A message displays to guests when they reach the maximum number of supported devices.

Allow guests to register devices

You can set the maximum number of supported devices in the guest type settings.

Device information will be stored in the endpoint identity group specified in the guest type of the user logging in to this portal.

Configure guest types at:

[Work Centers > Guest Access > Configure > Guest Types](#)

4. Cuando el usuario patrocinador crea una cuenta de invitado, le asigna un tipo de invitado. Cada tipo de invitado individual puede tener un terminal registrado que pertenece a un grupo de identidad de terminal diferente. Para asignar el grupo de identidad de terminal al que se debe agregar el dispositivo, seleccione el tipo de invitado que utiliza el patrocinador para estos usuarios invitados (este caso práctico se basa en Semanalmente (valor predeterminado)).

5. Una vez en el tipo de invitado, en **Opciones de inicio de sesión** seleccione el Grupo de terminales del menú desplegable **Grupo de identidad de terminales para el registro de dispositivos de invitado**

Maximum devices guests can register: (1-999)

Endpoint identity group for guest device registration: ⓘ

6. Acceda a **Política > Elementos de Política > Resultados > Autorización > Perfiles de Autorización**. Haga clic en Add (Agregar).

7. Este perfil se envía al WLC, la **Redirect-URL** y la **Redirect-URL-ACL** en respuesta a la solicitud de omisión de autenticación Mac (MAB) inicial.

- Una vez que la redirección web (CWA, MDM, NSP, CPP) marca, seleccione **Centralized Web Auth**, luego Escriba el nombre de la ACL de redirección en el campo **ACL** y en **Value**, seleccione el portal creado para este flujo (CWA_DeviceRegistration).

Authorization Profiles > New Authorization Profile

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

▼ Common Tasks

VLAN

Voice Domain Permission

Web Redirection (CWA, MDM, NSP, CPP) (i)

Centralized Web Auth ACL Value

8. Acceda a **Política > Autorización** e inserte una nueva regla. Esta regla es la que dispara el proceso de redirección en respuesta a la solicitud de autenticación MAC inicial del WLC. (En este caso llamada **Wireless_Guest_Redirect**).

9. En **Condiciones**, seleccione **Seleccionar Condición Existente de Biblioteca** y, a continuación, en **nombre de condición**, seleccione **Condición Compuesta**. Seleccione una condición compuesta predefinida denominada **Wireless_MAB**.

10. En results (resultados), seleccione **Standard > CWA_DeviceRegistration** (Perfil de autorización creado en el paso anterior). A continuación, haga clic en **Finalizado y Guardar**

<input checked="" type="checkbox"/>	Wireless_Guest_Redirect	if	Wireless_MAB	then	CWA_DeviceRegistration
-------------------------------------	-------------------------	----	--------------	------	------------------------

11. Duplique la política anterior y modifique su nombre, ya que se trata de la política a la que llega el terminal después de volver del evento de reautenticación (denominado **Wireless_Guest_Access**).

12. En el cuadro **Detalles del grupo de identidad**, seleccione **Grupo de identidad de terminales** y seleccione el grupo al que hizo referencia en Tipo de invitado (GuestEndpoints).

13. En Resultados, seleccione **PermisoAcceso**. Haga clic en **Finalizado y Guardar** los cambios.

<input checked="" type="checkbox"/>	Wireless_Guest_Access	if	GuestEndpoints AND Wireless_MAB	then	PermitAccess
<input checked="" type="checkbox"/>	Wireless_Guest_Redirect	if	Wireless_MAB	then	CWA_DeviceRegistration

14. Cree una política de depuración de terminales que borre el grupo de terminales invitados diariamente.

- Vaya a **Administración > Administración de identidades > Configuración > Depuración de terminales**
- En las reglas de **depuración** debe haber una de forma predeterminada que desencadene la eliminación de los puntos finales de invitado si el tiempo transcurrido es superior a 30 días.
- Modifique la directiva existente para GuestEndpoints o cree una nueva (en caso de que se haya eliminado la directiva predeterminada). Tenga en cuenta que las políticas de depuración se ejecutan cada día a una hora definida.


En este caso, la condición es Miembros de GuestEndpoints con Días transcurridos inferiores a 1 día

Caso práctico 3: portal HostSpot

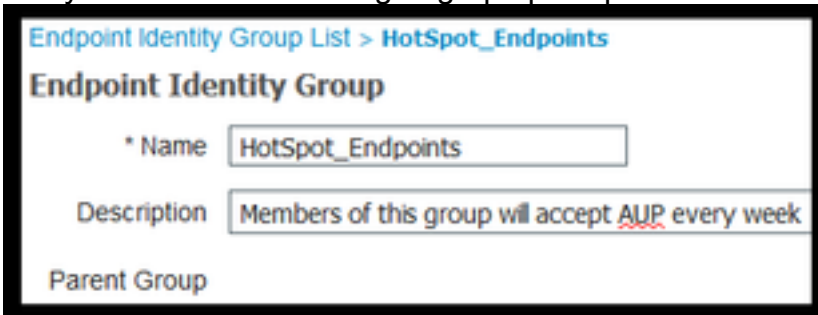
Visión general de flujo

1. El usuario inalámbrico se conecta al SSID de invitado.
2. El WLC autentica el punto final basándose en su dirección MAC usando ISE como servidor AAA.
3. ISE devuelve una aceptación de acceso con dos pares de valores de atributo (AVP): url-redirect y url-redirect-acl.
4. Una vez que el WLC aplica estos AVPs a la sesión del terminal, la estación pasa a DHCP-Required y una vez que toma una dirección IP permanece en CENTRAL_WEB_AUTH. En este paso el WLC está listo para redirigir el tráfico http / https del cliente.
5. El usuario final abre el navegador web y una vez que se genera el tráfico HTTP o HTTPS, el WLC redirige al usuario al portal ISE HotSpot.
6. Una vez en el portal, se le pide al usuario que acepte una política de uso aceptable.
7. ISE agrega la dirección MAC del terminal (ID del terminal) al grupo de identidad del terminal configurado.
8. El nodo de servicios de políticas (PSN) que procesa la solicitud emite un tipo de CoA dinámico **Admin-Reset** al WLC.
9. Una vez que el WLC termina de procesar el CoA entrante, emite un des-authenticate al cliente (la conexión es pérdida para el tiempo que toma para que el cliente vuelva).
10. Una vez que el cliente se vuelve a conectar, se crea una nueva sesión para que no haya continuidad de la sesión en ISE. Significa que la autenticación se procesa como un nuevo subproceso.
11. Dado que el extremo se agrega al grupo de identidad de extremo configurado y existe una directiva de autorización que comprueba si el extremo forma parte de ese grupo, la nueva autenticación coincide con esta directiva. El resultado es un acceso completo a la red de invitado.
12. El usuario no debe tener que aceptar la AUP de nuevo a menos que el objeto de identidad de terminal se purgue de la base de datos de ISE como resultado de una política de depuración de terminales.

Configuración

1. Cree un nuevo grupo de identidad de terminales al que mover estos dispositivos tras el registro. Navegue hasta **Centros de trabajo > Acceso de invitado > Grupos de identidad > Grupos de identidad de terminales** y haga clic en  .
- Introduzca un nombre de grupo (en este caso, HotSpot_Endpoints). Agregue una descripción

y no se necesitará ningún grupo principal.



Endpoint Identity Group List > HotSpot_Endpoints

Endpoint Identity Group

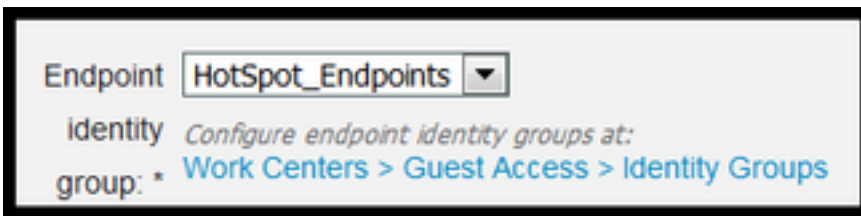
* Name

Description

Parent Group

2. Vaya a **Centros de trabajo > Acceso de invitado > Configurar > Portales de invitado > seleccione Portal de zona Wi-Fi (predeterminado)**.

3. Expanda Configuración del portal y, en Grupo de identidad de terminales, seleccione el grupo **HotSpot_Endpoints** en **Grupo de identidad de terminales**. Esto envía los dispositivos registrados al grupo especificado.



Endpoint

identity *Configure endpoint identity groups at:*
group: * [Work Centers > Guest Access > Identity Groups](#)

4. **Guarde** los cambios.

5. Cree el perfil de autorización que llama al portal HotSpot cuando la autenticación MAB es originada por el WLC.

- Vaya a **Policy > Policy elements > Results > authorization > Authorization Profiles** y cree uno (HotSpotRedirect).
- Una vez que se verifica la **redirección web (CWA, MDM, NSP, CPP)**, seleccione **Hot Spot**, luego escriba el nombre de ACL de redirección en el campo ACL (Guest_Redirect) y como un portal de selección de valor correcto (**Hotspot Portal (default)**).

Add New Standard Profile

Authorization Profile

* Name:

Description:

* Access Type:

Network Device Profile:

Common Tasks

Voice Domain Permission

Web Redirection (CWA, MDM, NSP, CPP) ⓘ

Hot Spot: ACL: Value:

Static IP/Host name/FQDN

Attributes Details

Access Type = ACCESS_ACCEPT
 cisco-av-pair = url-redirect-ad=Guest_Redirect
 cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=a60e04d0-2230-11e6-99ab-005056bf55e0&action=cwa&type=drw

6. Cree la política de autorización que desencadena el resultado de HotSpotRedirect tras la solicitud MAB inicial del WLC.

- Navegue hasta **Política > Autorización** e inserte una nueva regla. Esta regla es la que dispara el proceso de redirección en respuesta a la solicitud de autenticación MAC inicial del WLC. (En este caso llamada **Wireless_HotSpot_Redirect**).
- En **Condiciones**, seleccione **Seleccionar condición existente de la biblioteca** y, a continuación, en **nombre de condición**, seleccione **Condición compuesta**
- En **results (resultados)**, seleccione **Standard > HotSpotRedirect** (Perfil de autorización creado en el paso anterior). A continuación, haga clic en **Finalizado** y **Guardar**

7. Cree la segunda política de autorización.

- Duplique la política anterior y modifique su nombre, ya que se trata de la política a la que llega el terminal cuando vuelve del evento de reautenticación (denominado **Wireless_HotSpot_Access**).
- En el cuadro **Detalles del grupo de identidad**, seleccione **Grupo de identidad de terminales** y, a continuación, seleccione el grupo que creó anteriormente (**HotSpot_Endpoints**).
- En **Resultados**, seleccione **PermitAccess**. Haga clic en **Finalizado** y **Guardar** los cambios.

✔	Wireless_HotSpot_Access	if HotSpot_Endpoints AND Wireless_MAB	then PermitAccess
✔	Wireless_HotSpot_Redirect	if Wireless_MAB	then HotSpotRedirect

8. Configure la política de depuración que borra los terminales con un tiempo transcurrido superior a 5 días.

- Vaya a **Administration > Identity Management > Settings > Endpoint Purge** y en **Purge rules** cree uno nuevo.
- En el cuadro **Detalles del grupo de identidad**, seleccione **Grupo de identidad de terminales > HotSpot_Endpoints**
- En **conditions**, haga clic en **Create New Condition (Advanced Option)** .

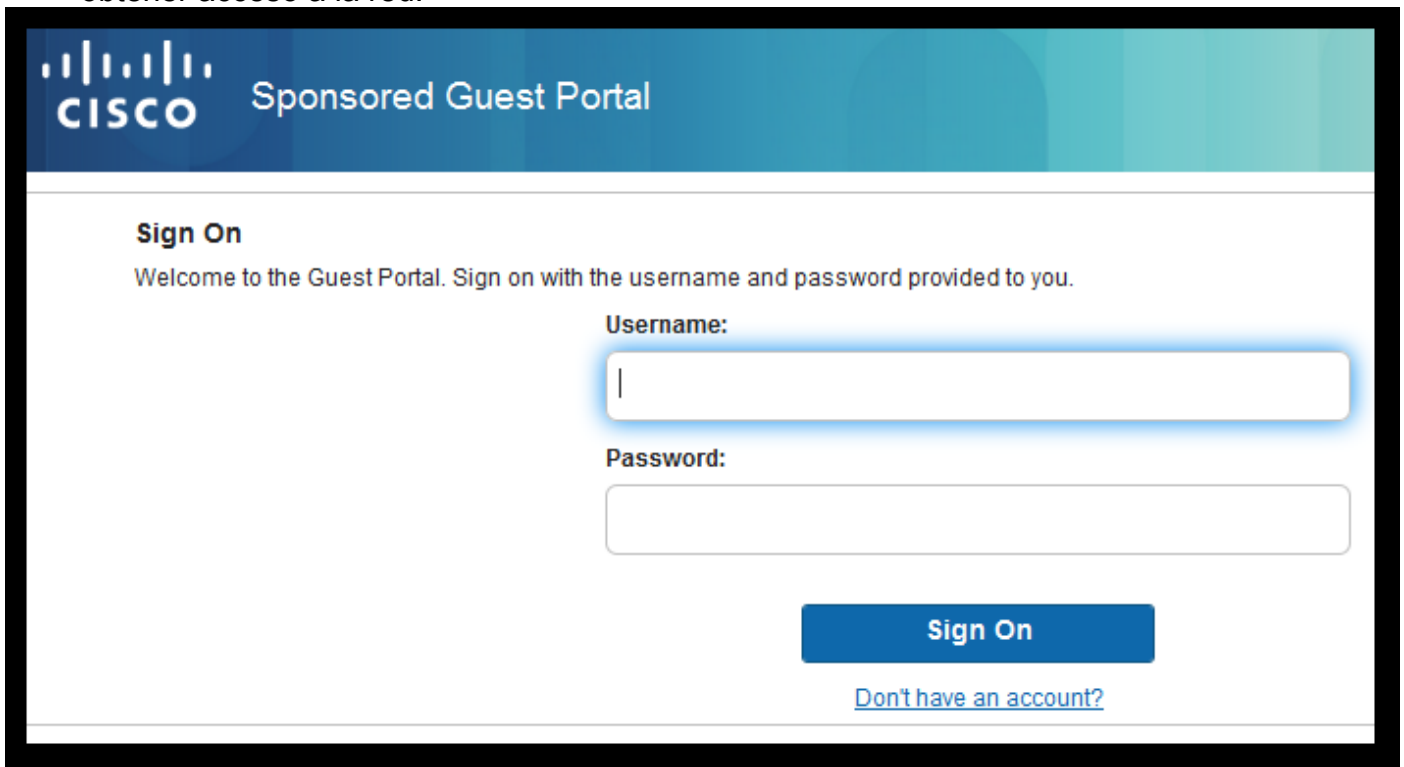
- En Seleccionar atributo, elija *ENDPOINTPURGE: Días transcurridos SUPERIORES A 5 días*

HotSpot_Endpoints_PurgeRule if **HotSpot_Endpoints** AND ENDPOINTPURGE:ElapsedDays GREATERTHAN 5

Verificación

Caso práctico 1

1. El usuario se conecta al SSID de invitado.
2. Abre el explorador y, en cuanto se genera tráfico HTTP, se muestra el portal de invitados.
3. Una vez que el usuario invitado autentica y acepta la PUA, se muestra una página de éxito.
4. Se envía una CoA de reautenticación (transparente para el cliente).
5. La sesión del terminal se vuelve a autenticar con acceso completo a la red.
6. Cualquier conexión de invitado posterior debe pasar la autenticación de invitado antes de obtener acceso a la red.



The screenshot shows a web portal with a blue header containing the Cisco logo and the text "Sponsored Guest Portal". Below the header, the page is titled "Sign On" and includes a welcome message: "Welcome to the Guest Portal. Sign on with the username and password provided to you." There are two input fields: "Username:" and "Password:". Below the fields is a blue "Sign On" button and a link that says "Don't have an account?".



Sponsored Guest Portal

Acceptable Use Policy

Please read the Acceptable Use Policy

Please accept the policy: You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited. Cisco Systems reserves the right to suspend the Service if Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or

Accept

Decline



Sponsored Guest Portal

Success

You now have Internet access through this network.

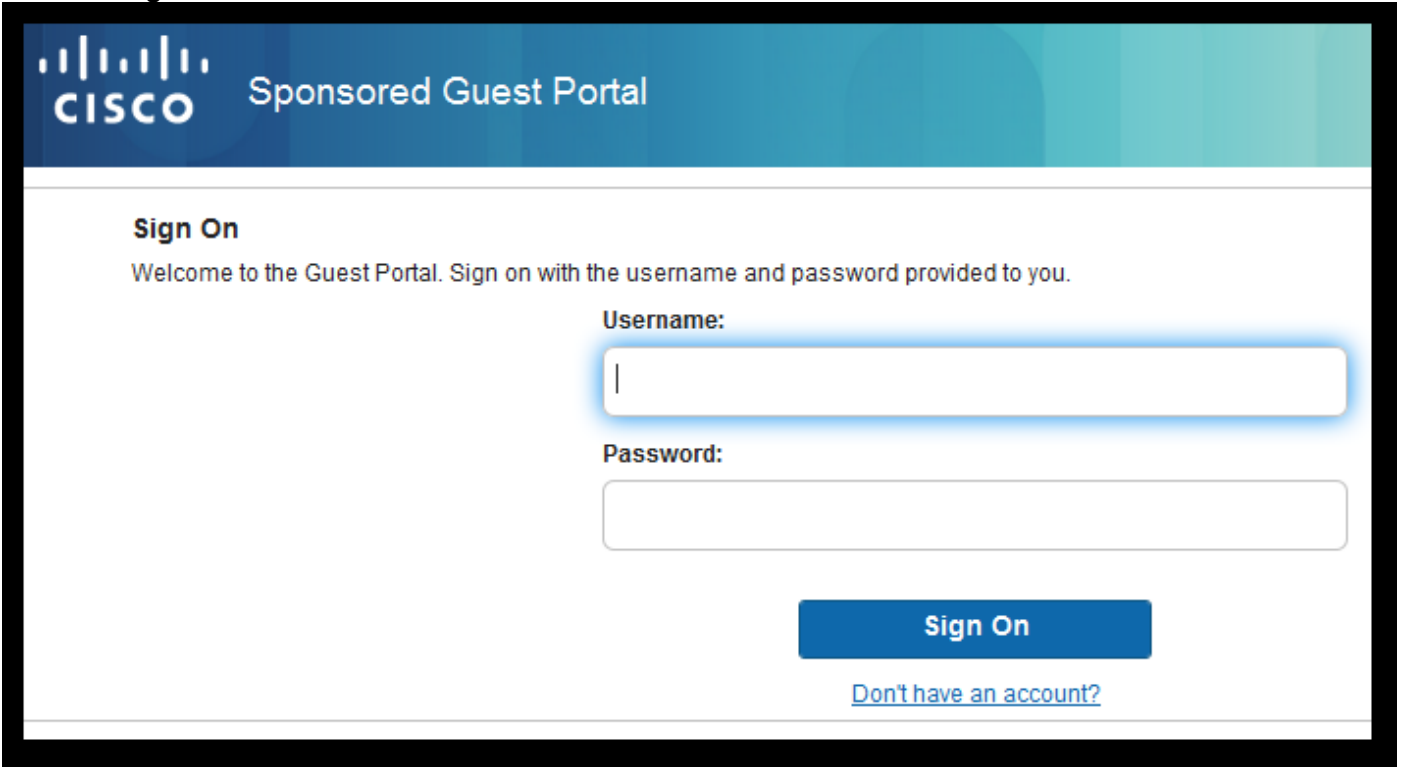
Flujo de registros en directo de RADIUS de ISE:

🔔	🔒	1001	68:7F:74:72:18:2E	Windows7-Wo...	Default >> MAB	Default >> Wir...	PermitAccess	← Accounting Start
✅	🔒	1001	68:7F:74:72:18:2E	Windows7-Wo...	Default >> MAB	Default >> Wir...	PermitAccess	← Re-Authentication Event
✅	🔒		68:7F:74:72:18:2E					← CoA Event
✅	🔒	1001	68:7F:74:72:18:2E					← Guest Authentication Event
✅	🔒	68:7F:74:72:18:2E	68:7F:74:72:18:2E	Windows7-Wo...	Default >> MA...	Default >> Wir...	CWA_Redirect	← Initial MAB request

Caso práctico 2

1. El usuario se conecta al SSID de invitado.
2. Abre el explorador y, en cuanto se genera tráfico HTTP, se muestra el portal de invitados.
3. Una vez que el usuario invitado autentica y acepta la PUA, el dispositivo se registra.

4. Se muestra una página de confirmación y se envía una CoA de reautenticación (transparente para el cliente).
5. La sesión del terminal se vuelve a autenticar con acceso completo a la red.
6. Cualquier conexión de invitado posterior 9 permitida sin aplicar la autenticación de invitado, siempre y cuando el extremo se encuentre todavía en el grupo de identidad de punto final configurado.



The image shows a screenshot of the Cisco Sponsored Guest Portal. At the top left, there is the Cisco logo and the text "Sponsored Guest Portal". Below this, the page is titled "Sign On" and includes a welcome message: "Welcome to the Guest Portal. Sign on with the username and password provided to you." There are two input fields: "Username:" and "Password:". Below the input fields is a blue "Sign On" button and a link that says "Don't have an account?".

CISCO Sponsored Guest Portal

Sign On

Welcome to the Guest Portal. Sign on with the username and password provided to you.

Username:

Password:

Sign On

[Don't have an account?](#)



Acceptable Use Policy

Please read the Acceptable Use Policy

Please accept the policy: You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited. Cisco Systems reserves the right to suspend the Service if Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or

Accept

Decline

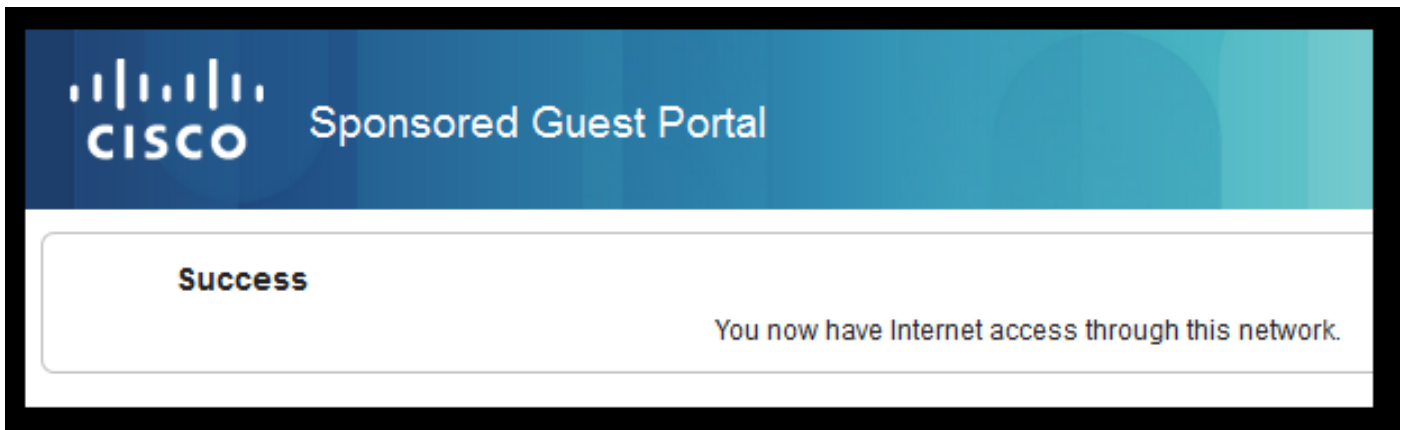


Welcome Message

Click **Continue** to connect to the network.

You're very close to gaining network access.

Continue



Flujo de registros en directo de RADIUS de ISE:

Status	Details	Identity	Endpoint ID	Authorization Profiles	Identity Group
●		68:7F:74:72:1...	68:7F:74:72:...	PermitAccess	
✓		68:7F:74:72:1...	68:7F:74:72:...	PermitAccess	GuestEndpoints
✓		hfr592	68:7F:74:72:...	PermitAccess	User Identity Groups:GuestType_Contractor (default)...
✓			68:7F:74:72:...		
✓		hfr592	68:7F:74:72:...		GuestType_Contractor (default)
✓		68:7F:74:72:1...	68:7F:74:72:...	CWA_DeviceRegistration	Profiled

Annotations on the right side of the table:

- Accounting Start
- Subsequent MAB request(no redirect to guest portal)
- Re-Authentication Event
- CoA Reauth Event
- Guest Authentication and Device Registration
- Initial MAB request

Caso práctico 3

1. El usuario se conecta al SSID de invitado.
2. Abre el explorador y, en cuanto se genera tráfico HTTP, se muestra una página AUP.
3. Una vez que el usuario invitado acepta la PUA, el dispositivo se registra.
4. Se muestra una página de confirmación y se envía una CoA de restablecimiento de administrador (transparente para el cliente).
5. El terminal se vuelve a conectar con acceso completo a la red.
6. Se permite cualquier conexión de invitado posterior sin exigir la aceptación de AUP (a menos que se configure lo contrario) mientras el terminal permanezca en el grupo de identidad de terminal configurado.



Acceptable Use Policy

Please read the Acceptable Use Policy.

Please accept the policy: You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited. Cisco Systems reserves the right to suspend the Service if Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or modification will be posted on Cisco System's website and will be effective as to existing users 30 days after posting.

Accept

Decline



Connection Successful

You have successfully connected to the network.

Switching local FlexConnect en AireOS

Cuando se configura el switching local de FlexConnect, el administrador de red debe asegurarse de que:

- La ACL de redirección se configura como una ACL de FlexConnect.
- La ACL de redireccionamiento se ha aplicado como política a través del AP en sí en la pestaña **FlexConnect > ACL de autenticación web externa > Políticas > Seleccione ACL de redireccionamiento** y haga clic en **Aplicar**

All APs > Details for aaa-ap-3

General Credentials Interfaces High Availability Inventory **FlexConnect** Advanced

VLAN Support

Native VLAN ID 301 **VLAN Mappings**

FlexConnect Group Name Not Configured

PreAuthentication Access Control Lists

External WebAuthentication ACLs

[Local Split ACLs](#)

[Central DHCP Processing](#)

[Layer2 ACLs](#)

Policies

Policy ACL CWA_Redirect

Policy Access Control Lists

CWA_Redirect

También puede agregar la política ACL al grupo de FlexConnect al que pertenece (Inalámbrico > Grupos de FlexConnect > Seleccione el grupo correcto > Asignación de ACL > Políticas Seleccione la ACL de redirección y haga clic en Agregar)

FlexConnect Groups > Edit 'test'

General Local Authentication Image Upgrade **ACL Mapping** Central DHCP WLAN VLAN mapping

AAA VLAN-ACL mapping WLAN-ACL mapping **Policies**

Policies

Policy ACL CWA_Redirect

Policy Access Control Lists

CWA_Redirect

TOR_Redirect

La adición de la ACL de la política acciona el WLC para empujar la ACL configurada hacia abajo a los miembros AP del grupo de FlexConnect. Si no lo hace, se producirá un problema de redirección web.

Escenario de anclaje externo

En los escenarios de anclaje automático (Foreign-Anchor) es importante destacar estos hechos:

- La ACL de redirección debe definirse en el WLC externo y de anclaje. Incluso cuando solo se aplica en el ancla.
- La autenticación de la capa 2 es siempre manejada por el WLC extranjero. Esto es crítico durante las fases de diseño (también para la resolución de problemas) ya que todo el tráfico de autenticación y contabilización de RADIUS ocurre entre ISE y el WLC externo.
- Una vez que los AVPs de redireccionamiento se aplican a la sesión del cliente, el WLC externo actualiza la sesión del cliente en el anclaje a través de un mensaje de transferencia de movilidad.
- En este punto, el WLC de anclaje comienza a aplicar el Redireccionamiento usando el Redirect-ACL que se ha preconfigurado.
- La contabilidad debe estar completamente desactivada en el SSID del WLC de anclaje para evitar que las actualizaciones de cuentas hacia ISE (que hacen referencia al mismo evento de autenticación) provengan tanto del anclaje como del extranjero.
- Las ACL basadas en URL no se soportan en escenarios de anclaje externo.

Troubleshoot

Estados rotos comunes en AireOS y WLC de acceso convergente

1. El cliente no puede unirse al SSID de invitado

"**show client detailed xx:xx:xx:xx:xx:xx:xx**" revela que el cliente está atascado en **START**. Generalmente éste es un indicador del WLC incapaz de aplicar un atributo que el servidor AAA devuelve.

Verifique que el nombre de la ACL de redirección que envía ISE coincida exactamente con el nombre de la ACL predefinida en el WLC.

El mismo principio se aplica a cualquier otro atributo que haya configurado ISE para que se aplique al WLC (ID de VLAN, nombres de interfaz, ACL de Airespace). El cliente debe realizar la transición a DHCP y, a continuación, a **CENTRAL_WEB_AUTH**.

2. Los AVP de redirección se aplican a la sesión del cliente, pero la redirección no funciona

Verifique que el estado del administrador de políticas del cliente sea **CENTRAL_WEB_AUTH** con una dirección IP válida alineada con la interfaz dinámica configurada para el SSID y también que los atributos Redirigir ACL y URL-Redirigir se apliquen a la sesión del cliente.

Redirigir ACL

En los WLCs de AireOS, la ACL de redirección debe permitir explícitamente el tráfico que no se debe redirigir, como DNS e ISE en el puerto TCP 8443 en ambas direcciones y la negación implícita `ip any` desencadena el resto del tráfico que se redirigirá.

En el acceso convergente, la lógica es la opuesta. Denegar ACE omite la redirección mientras permitir ACE activa la redirección. Es por esto que se recomienda permitir explícitamente los

puertos TCP 80 y 443.

Verifique el acceso a ISE a través del puerto 8443 desde la VLAN de invitado. Si todo se ve bien desde la perspectiva de la configuración, la manera más fácil de avanzar es capturar detrás del adaptador inalámbrico del cliente y verificar dónde se interrumpe el redireccionamiento.

- ¿Se produce la resolución DNS?
- ¿Ha finalizado el protocolo de enlace de 3 vías TCP con la página solicitada?
- ¿El WLC devuelve una acción de redirección después de que el cliente inicie el GET?
- ¿Se completó el protocolo de enlace de 3 vías TCP contra ISE en 8443?

3. El cliente no puede acceder a la red después de que ISE introdujera un cambio en la VLAN al final del flujo de invitados

Una vez que el cliente ha tomado una dirección IP al principio del flujo (estado de preredirección), si se pulsa un cambio de VLAN después de que se produzca la autenticación de invitado (tras la reautenticación de CoA), la única forma de forzar una liberación o renovación de DHCP en el flujo de invitado (sin agente de estado) es a través de un applet de Java que en los dispositivos móviles no funcionan.

Esto deja al cliente agujeros negros en VLAN X con una dirección IP de VLAN Y. Esto debe tenerse en cuenta al planificar la solución.

4. ISE muestra el mensaje "Error interno de HTTP 500, no se ha encontrado la sesión Radius" en el navegador del cliente invitado durante la redirección

Suele ser un indicador de la pérdida de sesiones en ISE (la sesión ha finalizado). La razón más común para esto es la contabilización configurada en el WLC de anclaje cuando se ha desplegado Foreign-Anchor. Para corregir esta deshabilitación de cuentas en el delimitador y dejar el identificador externo Autenticación y cuentas.

5. El cliente se desconecta y permanece desconectado o se conecta a un SSID diferente después de aceptar la AUP en el portal HotSpot de ISE.

Esto se puede esperar en HotSpot debido al cambio dinámico de la autorización (CoA) implicado en este flujo (CoA Admin Reset) que hace que el WLC emita una autenticación a la estación inalámbrica. La mayoría de los terminales inalámbricos no tienen ningún problema para volver al SSID después de que se produzca la desautenticación, pero en algunos casos el cliente se conecta a otro SSID preferido en respuesta al evento de desautenticación. No se puede hacer nada desde ISE o WLC para evitarlo, ya que depende del cliente inalámbrico adherirse al SSID original o conectarse a otro SSID disponible (preferido).

En este caso, el usuario inalámbrico debe volver a conectarse manualmente al SSID de HotSpot.

WLC de AireOS

```
(Cisco Controller) >debug client
```

Depurar conjuntos de clientes para DEPURAR un conjunto de componentes implicados en los

cambios del equipo de estado de cliente.

```
(Cisco Controller) >show debug
```

```
MAC Addr 1..... AA:AA:AA:AA:AA:AA
```

Debug Flags Enabled:

```
  dhcp packet enabled.
  dot11 mobile enabled.
  dot11 state enabled
  dot1x events enabled.
  dot1x states enabled.
  mobility client handoff enabled.
  pem events enabled.
  pem state enabled.
  802.11r event debug enabled.
  802.11w event debug enabled.
  CCKM client debug enabled.
```

Depurar componentes AAA

```
(Cisco Controller) >debug aaa {events, detail and packets} enable
```

Esto puede afectar a los recursos en función de la cantidad de usuarios que se conectan a través de MAB o Dot1X SSID. Estos componentes en el nivel DEBUG registran las transacciones AAA entre WLC e ISE e imprimen los paquetes RADIUS en la pantalla.

Esto es crítico si usted sabe que ISE no puede entregar los atributos esperados, o si el WLC no los procesa correctamente.

Redirección de Web-Auth

```
(Cisco Controller) >debug web-auth redirect enable mac aa:aa:aa:aa:aa:aa
```

Esto se puede utilizar para verificar que el WLC está disparando con éxito el redireccionamiento. Este es un ejemplo de cómo debe verse la redirección desde los debugs:

```
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- parser host is 10.10.10.10
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- parser path is /
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- added redirect=, URL is now
https://TORISE21A.RTPAAA.NET:8443/portal/gateway?sessionId=0e249a0500000682577ee2a2&portal=9fc44
212-2da2-11e6-a5e2-005056a15f11&action=cwa&to
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- str1 is now
https://TORISE21A.RTPAAA.NET:8443/portal/gateway?sessionId=0e249a0500000682577ee2a2&portal=9fc44
212-2da2-11e6-a5e2-005056a15f11&action=cwa&token=c455b075d20c
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- clen string is Content-Length: 430

*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- Message to be sent is
  HTTP/1.1 200 OK
Location:
https://TORISE21A.RTPAAA.NET:8443/portal/gateway?sessionId=0e249a0500000682577ee2a2&portal=9fc44
212-2da2-11e6-a5e2-0050
```

NGWC

Depurar conjuntos de clientes para DEPURAR un conjunto de componentes implicados en los cambios del equipo de estado de cliente.

```
3850#debug client mac-address <client MAC>
```

Este componente imprime los paquetes RADIUS (autenticación y cuentas) en la pantalla. Esto es útil cuando necesita verificar que ISE ofrece los AVP adecuados y también para verificar que CoA se envía y procesa correctamente.

```
3850#debug radius
```

Esto hará que todas las transiciones AAA (autenticación, autorización y contabilidad) donde los clientes inalámbricos estén involucrados. Esto es crítico para verificar que el WLC analiza correctamente los AVP y los aplica a la sesión del cliente.

```
3850#debug aaa wireless all
```

Esto puede activarse cuando sospecha un problema de redirección en la NGWC.

```
3850#debug epm plugin redirect all
```

```
3850#debug ip http transactions
```

```
3850#debug ip http url
```

ISE

Registros de RADIUS Live

Verifique que la solicitud MAB inicial se haya procesado correctamente en ISE y que ISE devuelva los atributos esperados. Navegue hasta **Operaciones > RADIUS > Registros en vivo** y filtre la salida usando el cliente MAC bajo **ID de terminal**. Una vez encontrado el evento de autenticación, haga clic en los detalles y verifique los resultados enviados como parte de la aceptación.



Result

UserName	68:7F:74:72:18:2E
User-Name	68-7F-74-72-18-2E
State	ReauthSession:0e249a0500000682577ee2a2
Class	CACS:0e249a0500000682577ee2a2:TORISE21A/254695377/6120
cisco-av-pair	url-redirect-acl=TOR_Redirect
cisco-av-pair	url-redirect=https://TORISE21A.RTPAAA.NET:8443/portal/gateway?sessionId=0e249a0500000682577ee2a2&portal=9fc44212-2da2-11e6-a5e2-005056a15f11&action=cwa&token=c455b075d20cf2b4e969abb648533fea

TCPDump

Esta función se puede utilizar cuando se necesita una mirada más profunda en el intercambio de paquetes RADIUS entre ISE y el WLC. De esta manera, puede probar que ISE envía los atributos correctos en access-accept sin la necesidad de habilitar debugs en el lado del WLC. Para iniciar una captura mediante TCDDump, vaya a **Operaciones > Solucionar problemas > Herramientas de diagnóstico > Herramientas generales > TCPDump**.

Este es un ejemplo de un flujo correcto capturado a través de TCPDump

Source	Destination	Protocol	Length	Info
154.5	157.13	RADIUS	299	Access-Request(1) (id=0, l=257)
157.13	154.5	RADIUS	443	Access-Accept(2) (id=0, l=401)
154.5	157.13	RADIUS	340	Accounting-Request(4) (id=8, l=298)
157.13	154.5	RADIUS	62	Accounting-Response(5) (id=8, l=20)
157.13	154.5	RADIUS	244	CoA-Request(43) (id=1, l=202)
154.5	157.13	RADIUS	80	CoA-ACK(44) (id=1, l=38)
154.5	157.13	RADIUS	299	Access-Request(1) (id=1, l=257)
157.13	154.5	RADIUS	239	Access-Accept(2) (id=1, l=197)

Estos son los AVP enviados en respuesta a la solicitud MAB inicial (segundo paquete en la captura de pantalla anterior).

RADIUS Protocol

```
Code: Access-Accept (2)
Packet identifier: 0x0 (0)
Length: 401
Authenticator: f1eaaffcfaa240270b885a9ba8ccd06d
[This is a response to a request in frame 1]
[Time from request: 0.214509000 seconds]
Attribute Value Pairs
  AVP: l=19 t=User-Name(1): 00-05-4E-41-19-FC
  AVP: l=40 t=State(24): 52656175746853657373696f6e3a30653234396130353030...
  AVP: l=55 t=Class(25): 434143533a30653234396130353030303030616130353536...
  AVP: l=37 t=Vendor-Specific(26) v=ciscoSystems(9)
    VSA: l=31 t=Cisco-AVPair(1): url-redirect-acl=Gues_Redirect
  AVP: l=195 t=Vendor-Specific(26) v=ciscoSystems(9)
    VSA: l=189 t=Cisco-AVPair(1): url-
```

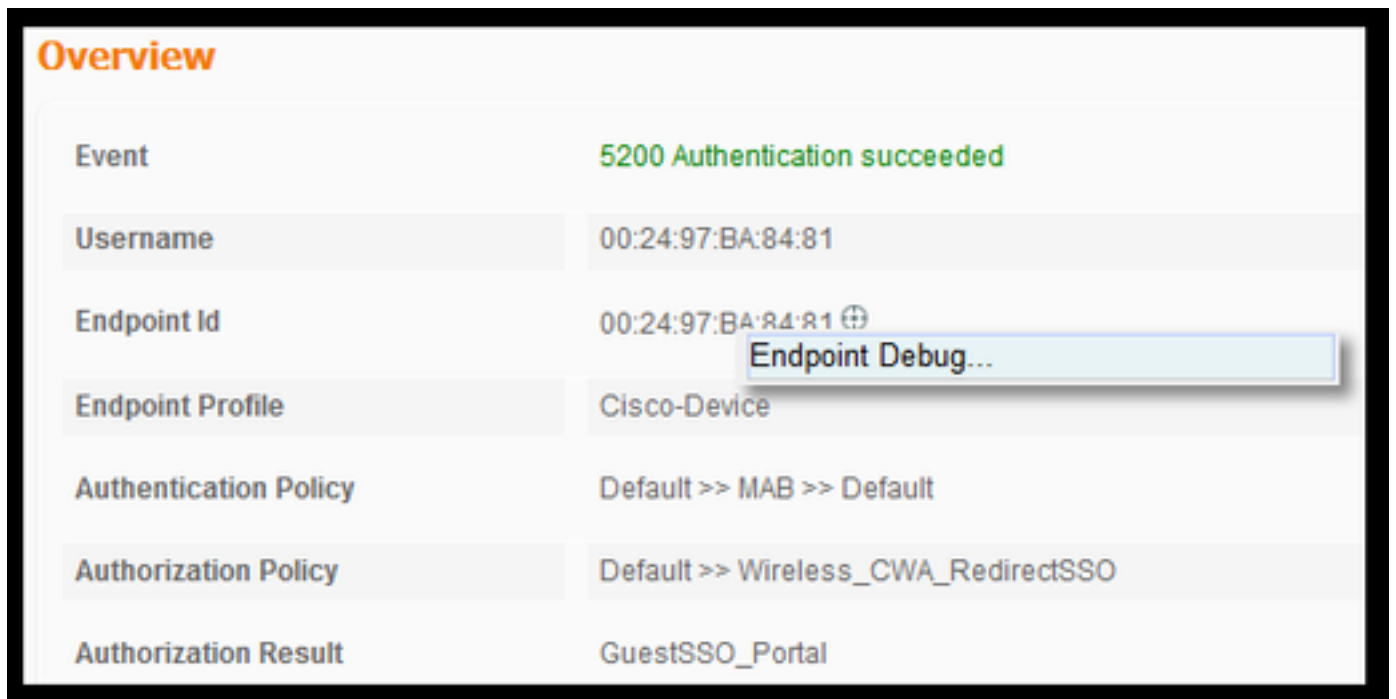
redirect=https://ise21a.rtpaaa.net:8443/portal/gateway?sessionId=0e249a050000aa05565e1c9&portal=194a5780-5e4e-11e4-b905-005056bf2f0a&action=cwa&token=c6c8a6b0d683ea0c650282b4372a7622

AVP: l=35 t=Vendor-Specific(26) v=ciscoSystems(9)

Depuraciones de terminales:

Si necesita profundizar en los procesos de ISE que implican decisiones de políticas, selección de portal, autenticación de invitados, CoA con la forma más sencilla de abordarlo es habilitar **depuraciones de terminales** en lugar de tener que establecer componentes completos en el nivel de depuración.

Para habilitar esto, navegue hasta **Operaciones > Troubleshooting > DiagnosticTools > General Tools > EndPoint Debug**.

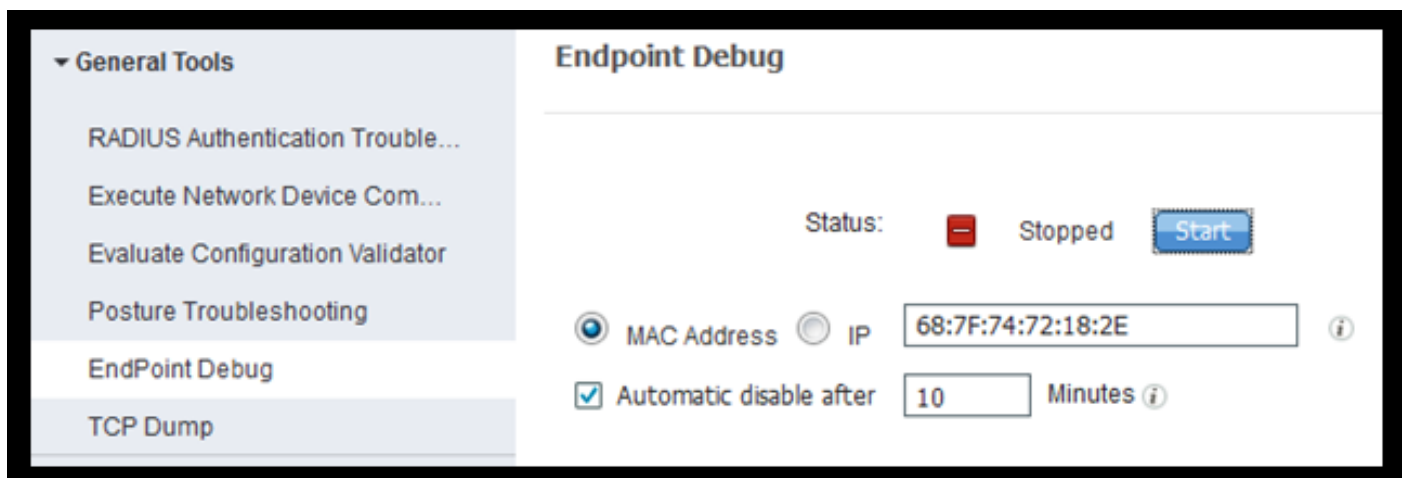


The screenshot shows the 'Overview' page in the ISE GUI. It displays the following information:

Event	5200 Authentication succeeded
Username	00:24:97:BA:84:81
Endpoint Id	00:24:97:BA:84:81 ⓘ
Endpoint Profile	Cisco-Device
Authentication Policy	Default >> MAB >> Default
Authorization Policy	Default >> Wireless_CWA_RedirectSSO
Authorization Result	GuestSSO_Portal

A tooltip labeled 'Endpoint Debug...' is visible over the Endpoint Id field.

Una vez en la página Endpoint debug, ingrese la dirección MAC del punto final y haga clic en start when ready para recrear el problema.



The screenshot shows the 'Endpoint Debug' configuration page in the ISE GUI. The left sidebar shows 'General Tools' with 'EndPoint Debug' selected. The main area shows the following configuration:


Status: ■ Stopped Start


MAC Address IP ⓘ


Automatic disable after Minutes ⓘ

Una vez que se haya detenido la depuración, haga clic en el enlace que identifica el ID del terminal para descargar el resultado de la depuración.

Endpoint Debug

Status:  Processing ...

MAC Address IP 

Automatic disable after Minutes 

Selected 0 | Total 1

<input type="checkbox"/>	File Name	Host Name	Modified Date	Size (Bytes)
<input type="checkbox"/>	68-7f-74-72-18-2e	TORISE21A	Jul 8 12:06	1021448

Información Relacionada

[Compilaciones de AireOS recomendadas por TAC](#)

[Guía de Configuración del Controlador Inalámbrico de Cisco, Versión 8.0.](#)

[Guía del administrador de Cisco Identity Services Engine, versión 2.1](#)

[Configuración inalámbrica NGWC universal con Identity Services Engine](#)

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).