Ejemplo de Configuración de Autenticación Web Local del Portal de Invitado de Identity Services Engine

Contenido

Introducción

Este documento describe cómo configurar la autenticación Web local (LWA) con el portal de invitados Cisco Identity Services Engine (ISE).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- ISE
- Controlador de LAN inalámbrica de Cisco (WLC)

Componentes Utilizados

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

- ISE versión 1.4
- WLC versión 7.4

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

Este documento describe la configuración de LWA. Sin embargo, Cisco recomienda utilizar la autenticación web centralizada (CWA) con ISE siempre que sea posible. Hay algunos escenarios donde se prefiere LWA o la única opción, por lo que este es un ejemplo de configuración para esos escenarios.

Configurar

LWA requiere ciertos requisitos previos y una configuración importante en el WLC, así como algunos cambios necesarios en el ISE.

Antes de que se traten, aquí se presenta un esbozo del proceso LWA con ISE.

Proceso LWA con el portal de invitados ISE

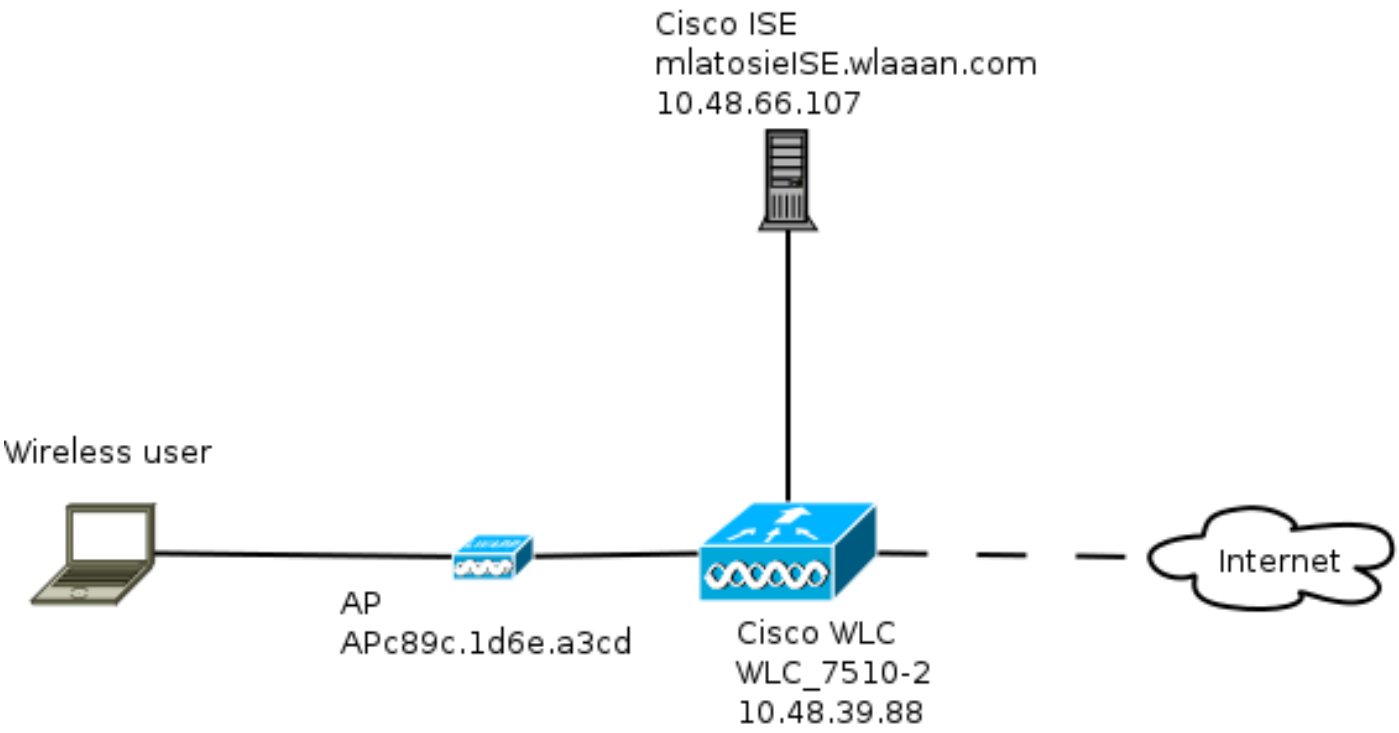
1. El explorador intenta buscar una página web.
2. El WLC intercepta la solicitud HTTP(S) y la redirige al ISE.
   En ese encabezado de redirección HTTP se almacenan varias partes clave de la información. A continuación se muestra un ejemplo de la URL de redirección:
   https://mlatosieise.wlaaan.com:8443/portal/PortalSetup.action?portal=27963fb0-e96e-11e4-a30a-005056bf01c9#&ui-state=dialog?switch_url=https://1.1.1.1/login.html&ap_mac=b8:be:bf:14:41:90&client_mac=28:cf:e9:13:47:cb&wlan=mlatosie_LWA&redirect=yahoo.com/
   Desde la URL de ejemplo, puede ver que el usuario intentó comunicarse con "yahoo.com". La URL también contiene información sobre el nombre de la red de área local inalámbrica (WLAN) (mlatosie_LWA) y las direcciones MAC del punto de acceso y cliente (AP). En el ejemplo de URL, **1.1.1.1** es el WLC, y **mlatosieise.wlaaan.com** es el servidor ISE.
3. El usuario se presenta con la página de inicio de sesión de invitado de ISE e ingresa el nombre de usuario y la contraseña.
4. El ISE realiza la autenticación con respecto a su secuencia de identidad configurada.
5. El navegador vuelve a redirigir. Esta vez, envía credenciales al WLC. El explorador proporciona el nombre de usuario y la contraseña que el usuario introdujo en el ISE sin ninguna interacción adicional del usuario. Este es un ejemplo de solicitud GET al WLC.
   GET /login.html?redirect_url=http://yahoo.com/&username=mlatosie%40cisco.com&password=ityh&buttonClicked=4&err_flag=0
   Una vez más, se incluyen la URL original (**yahoo.com**), el nombre de usuario

(**mlatosie@cisco.com**) y la contraseña (**ityh**).
Nota: Aunque la URL está visible aquí, la solicitud real se envía a través de Secure Sockets Layer (SSL), que se indica mediante HTTPS y es difícil de interceptar.

6. El WLC utiliza RADIUS para autenticar ese nombre de usuario y contraseña contra el ISE y permite el acceso.
7. El usuario se redirige al portal especificado. Consulte la sección **"Configurar ISE externo como URL de webauth"** de este documento para obtener más información.

Diagrama de la red

Esta figura describe la topología lógica de los dispositivos utilizados en este ejemplo.



Requisitos previos de configuración

Para que el proceso LWA funcione correctamente, un cliente debe poder obtener:

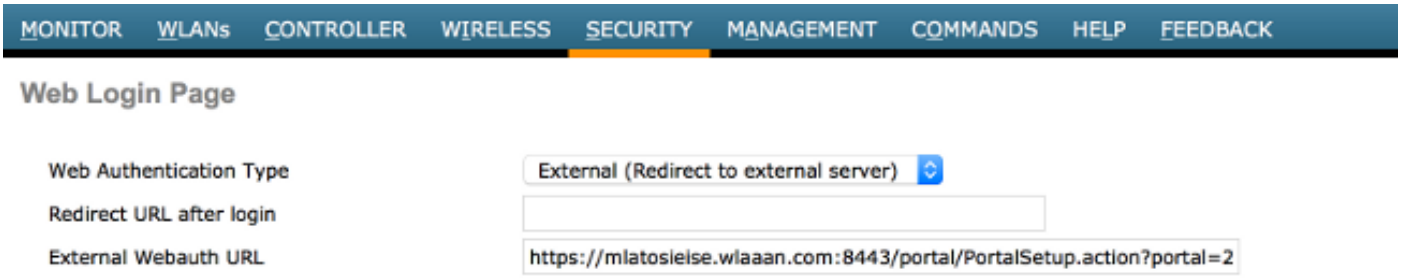
- Configuración de dirección IP y máscara de red
- Ruta predeterminada
- Servidor DNS

Todo esto se puede proporcionar con DHCP o la configuración local. La resolución DNS debe funcionar correctamente para que el LWA funcione.

Configurar la WLC

Configure el ISE externo como URL de Webauth globalmente

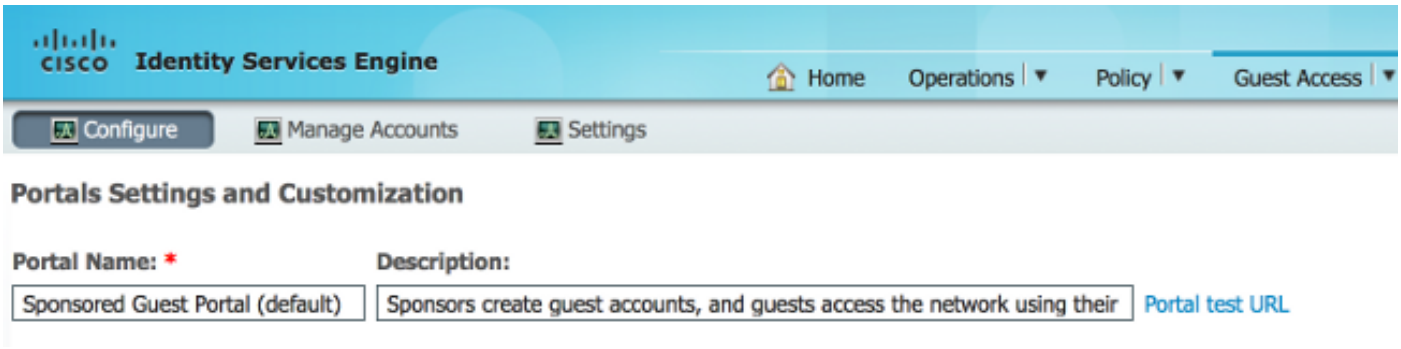
En **Seguridad > Autenticación web > Página de inicio de sesión web**, puede acceder a esta información.



Nota: Este ejemplo utiliza una URL de Webauth externa y se tomó de la versión 1.4 de ISE. Si tiene una versión diferente, consulte la guía de configuración para entender qué se debe configurar.

También es posible configurar esta configuración por WLAN. A continuación, se encuentra en los parámetros de seguridad WLAN específicos. Éstos invalidan la configuración global.

Para encontrar la URL correcta para su portal específico, elija **ISE > Guest Policy > Configure > su portal específico**. Haga clic con el botón derecho del ratón en el enlace de "URL de prueba del portal" y elija **copiar ubicación del enlace**.



En este ejemplo, la URL completa es: https://mlatosieise.wlaaan.com:8443/portal/PortalSetup.action?portal=27963fb0-e96e-11e4-a30a-005056bf01c9

Configuración de las listas de control de acceso (ACL)

Para que la autenticación web funcione, se debe definir el tráfico permitido. Determine si se deben utilizar ACL de FlexConnect o ACL normales. Los AP de FlexConnect utilizan ACL de FlexConnect, mientras que los AP que utilizan switching centralizado utilizan ACL normales.

Para entender en qué modo funciona un AP particular, elija **Wireless > Access points** y elija el cuadro desplegable **AP name > AP Mode**. Una implementación típica es **local** o **FlexConnect**.

En **Seguridad > Listas de Control de Acceso,** elija **ACL de FlexConnect** o **ACL**. En este ejemplo, se permitió todo el tráfico UDP para permitir específicamente el intercambio DNS y el tráfico al ISE (10.48.66.107).

General

Access List Name FLEX_GUEST

Deny Counters 634752

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	Any	Any	Any	208398
2	Permit	10.48.66.107 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	Any	Any	Any	Any	32155
3	Permit	0.0.0.0 / 0.0.0.0	10.48.66.107 / 255.255.255.255	TCP	Any	Any	Any	Any	24532

Este ejemplo utiliza FlexConnect, por lo que se definen **tanto** FlexConnect como las ACL estándar.

Este comportamiento se documenta en el ID de bug de Cisco CSCue68065 con respecto a los controladores WLC 7.4. Ya no es necesario en el WLC 7.5 donde sólo necesita una FlexACL y ya no hay una ACL estándar

Configuración del identificador del conjunto de servicios (SSID) para LWA

En **WLANs,** elija el **ID de WLAN** para editar.

Configuración de autenticación web

Aplique las mismas ACL que se definieron en el paso anterior y habilite la autenticación web.

WLANs > Edit 'mlatosie_LWA'

General | Security | QoS | Advanced

Layer 2 | Layer 3 | AAA Servers

Layer 3 Security None

Web Policy

Authentication

Passthrough

Conditional Web Redirect

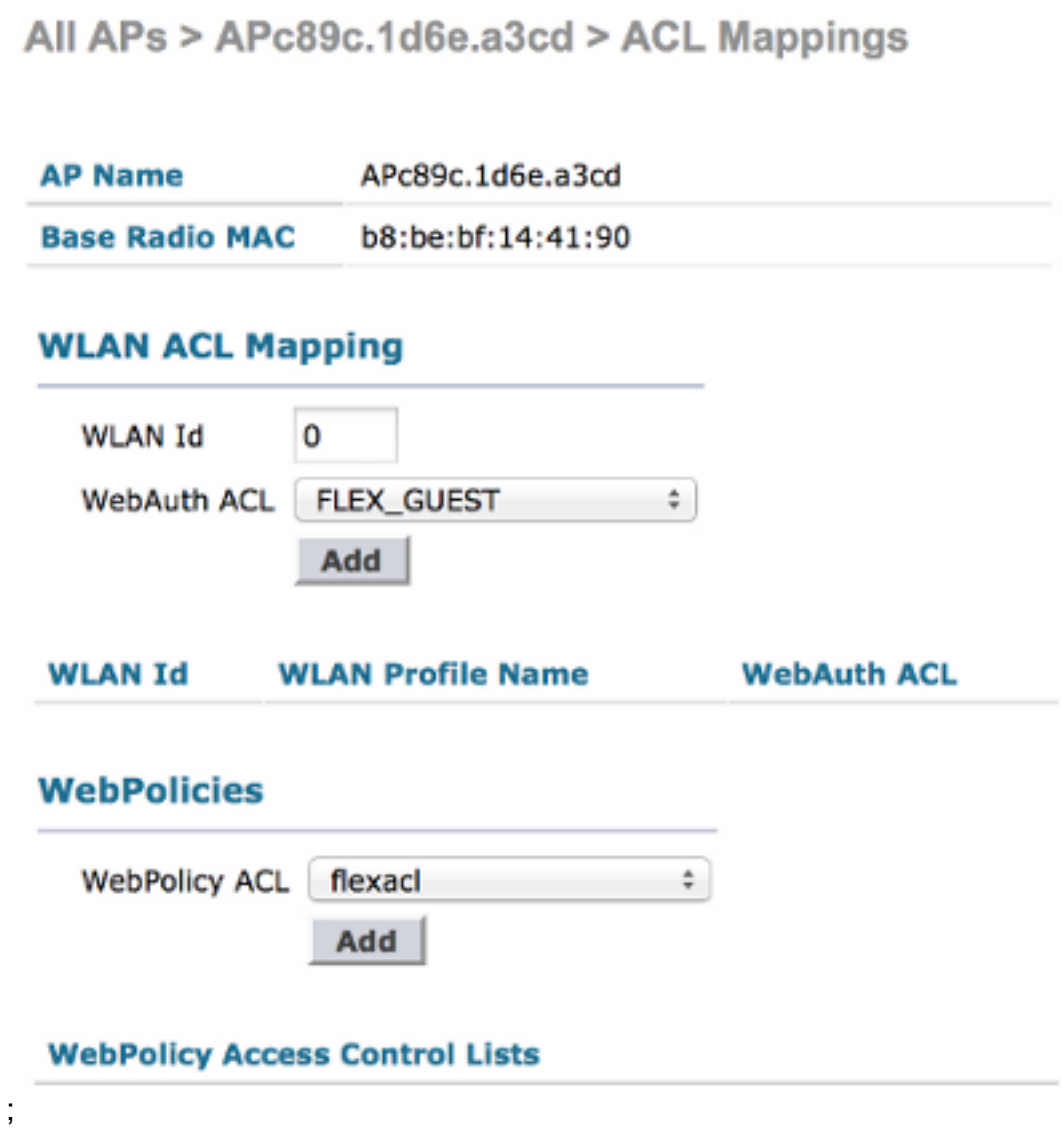
Splash Page Web Redirect

On MAC Filter failure[10]

Preauthentication ACL IPv4 FLEX_GUEST IPv6 None WebAuth FlexAcl FLEX_GUEST

Over-ride Global Config Enable

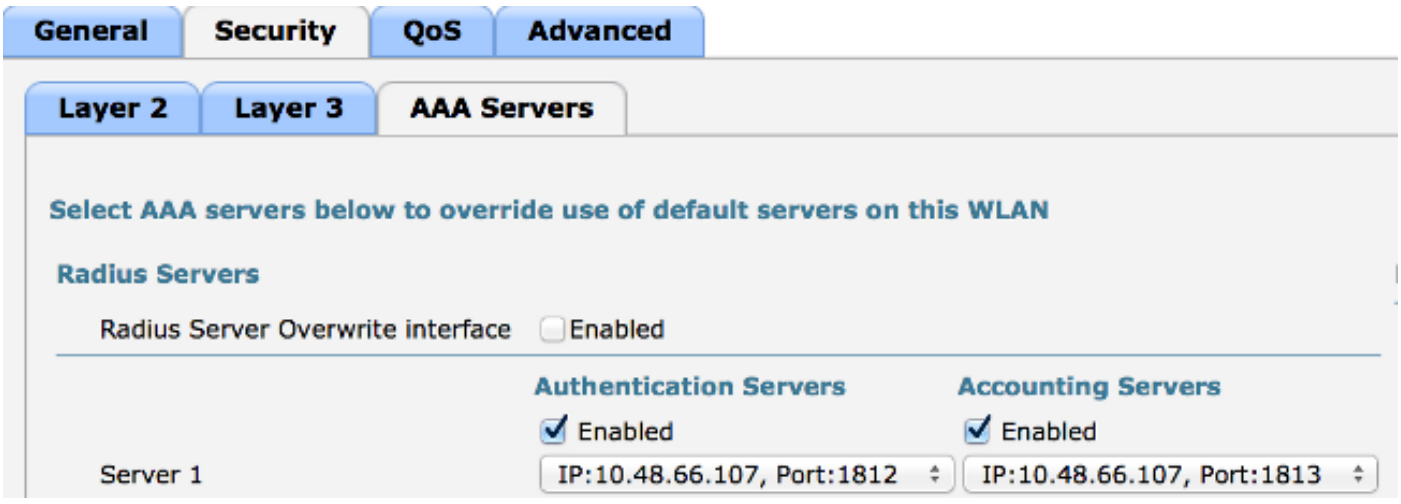
Nota: Si se utiliza la función de conmutación local de FlexConnect, es necesario agregar la asignación de ACL en el nivel AP. Esto se puede encontrar en **Wireless > Access Points (Inalámbrico > Puntos de acceso).** Elija el **nombre AP** adecuado **> FlexConnect > ACLs de WebAuthentication Externas**.



;

Configuración del servidor de autenticación, autorización y contabilidad (AAA)

En este ejemplo, tanto los servidores de autenticación como los de contabilidad apuntan al servidor ISE definido previamente.



Nota: Los valores predeterminados de la ficha **Avanzadas** no necesitan ser agregados.

Configuración de ISE

La configuración de ISE consta de varios pasos.

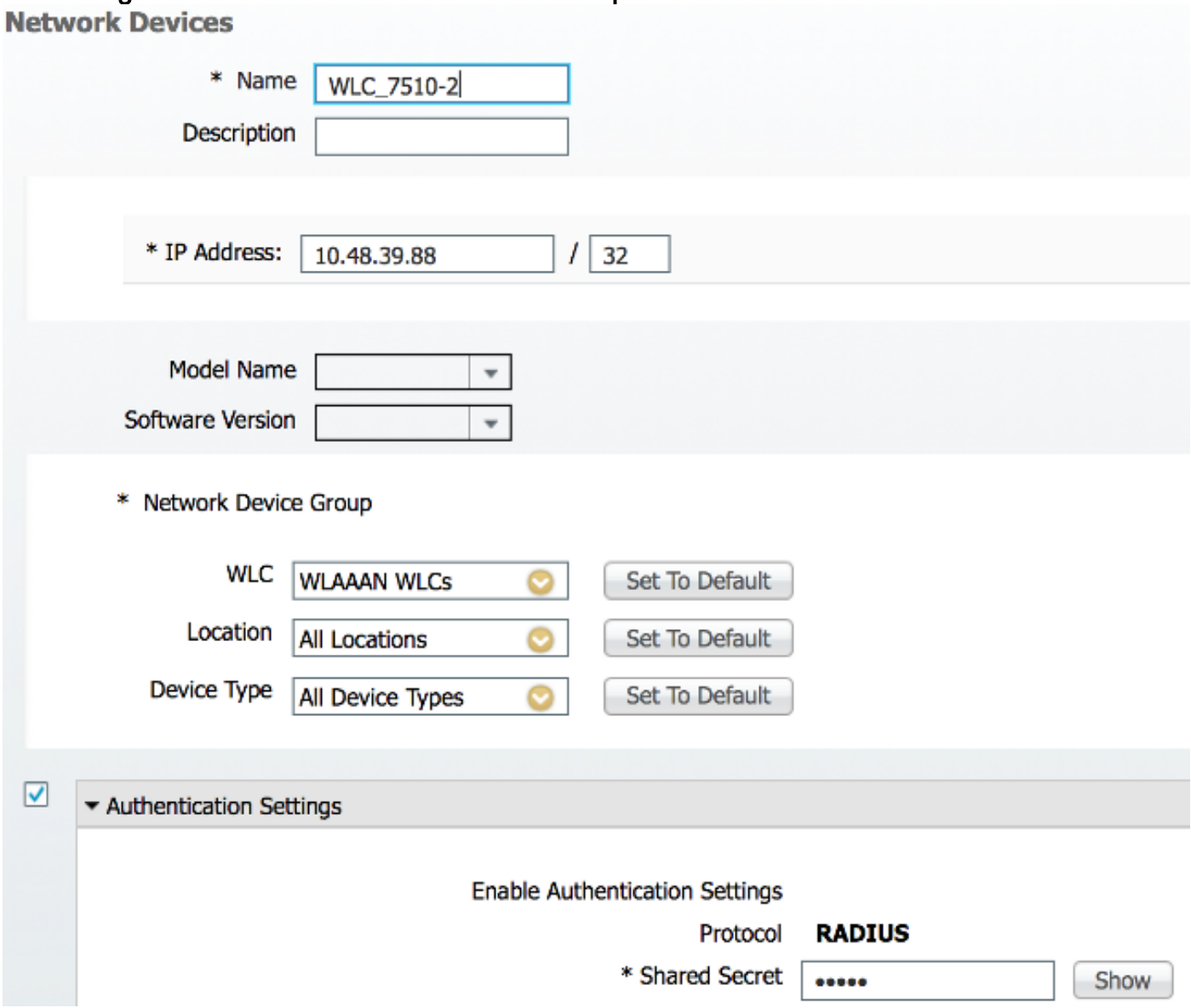
Primero, defina el dispositivo como un dispositivo de red.

A continuación, asegúrese de que existan las reglas de autenticación y autorización que dan cabida a este intercambio.

Definir el dispositivo de red

En **Administración > Recursos de red > Dispositivos de red**, rellene estos campos:

- Nombre del dispositivo
- Dirección IP del dispositivo
- **Configuración de autenticación > Secreto compartido**

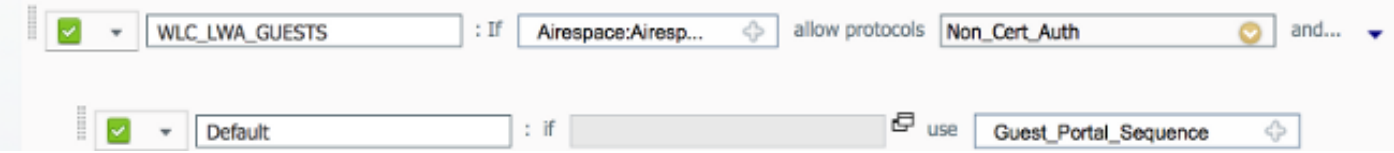


Configurar la política de autenticación

En **Política > Autenticación**, agregue una nueva política de autenticación.

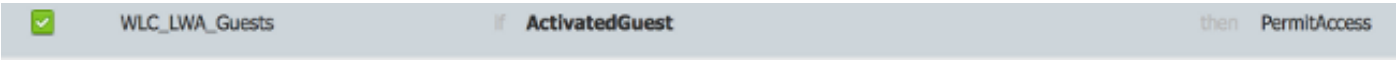
Este ejemplo utiliza estos parámetros:

- Nombre: **WLC_LWA_Invitados**
- Condición: **Airespace:Airespace-Wlan-Id.** Esta condición coincide con el ID de WLAN de 3, que es el ID de la WLAN **mlatosie_LWA** que se definió previamente en el WLC.
- {opcional} Permite protocolos de autenticación que no requieren el certificado **Non_Cert_Auth**, pero se pueden utilizar los valores predeterminados.
- Guest_Portal_Sequence, que define que los usuarios son usuarios invitados definidos localmente.



Configuración de la política de autorización y el resultado

En **Política > Autorización,** defina una nueva política. Puede ser una política muy básica, como:

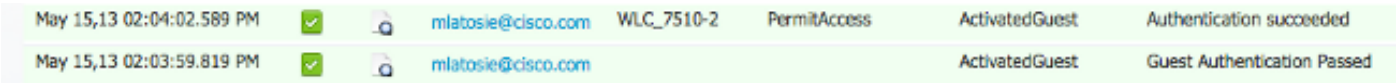


Esta configuración depende de la configuración general de ISE. Este ejemplo se ha simplificado a propósito.

Verificación

En ISE, los administradores pueden supervisar y resolver problemas de sesiones en directo en **Operaciones > Autenticaciones**.

Se deben ver dos autenticaciones. La primera autenticación proviene del portal de invitados en ISE. La segunda autenticación viene como una solicitud de acceso del WLC al ISE.



Puede hacer clic en el icono **Authentication Detail Report** para verificar qué políticas de autorización y políticas de autenticación fueron elegidas.

En el WLC, un administrador puede monitorear clientes bajo **Monitor > Client**.

Este es un ejemplo de un cliente que se autenticó correctamente:

Troubleshoot

Cisco recomienda ejecutar depuraciones por medio del cliente siempre que sea posible.

A través de la CLI, estas depuraciones proporcionan información útil:

```
debug client MA:CA:DD:RE:SS

debug web-auth redirect enable macMA:CA:DD:RE:SS

debug aaa all enable
```

Información Relacionada

- Guía de configuración de Cisco ISE 1.x
- Guía de Configuración de Cisco WLC 7.x
- Soporte Técnico y Documentación - Cisco Systems