

# Configuración de PEAP y EAP-FAST con ACS 5.2 y WLC

## Contenido

[Introducción](#)  
[Prerequisites](#)  
[Requirements](#)  
[Componentes Utilizados](#)  
[Convenciones](#)  
[Configurar](#)  
[Diagrama de la red](#)  
[Suposición](#)  
[Configuration Steps](#)  
[Configuración del servidor RADIUS](#)  
[Configurar recursos de red](#)  
[Configurar usuarios](#)  
[Definición de elementos de política](#)  
[Aplicar políticas de acceso](#)  
[Configurar la WLC](#)  
[Configure el WLC con los detalles del servidor de autenticación](#)  
[Configuración de las interfaces dinámicas \(VLAN\)](#)  
[Configuración de las WLAN \(SSID\)](#)  
[Configuración de la utilidad de cliente inalámbrico](#)  
[PEAP-MSCHAPv2 \(usuario1\)](#)  
[EAP-FAST \(usuario2\)](#)  
[Verificación](#)  
[Comprobar usuario1 \(PEAP-MSCHAPv2\)](#)  
[Verificar usuario2 \(EAP-FAST\)](#)  
[Troubleshoot](#)  
[Comandos para resolución de problemas](#)  
[Información Relacionada](#)

## Introducción

Este documento explica cómo configurar el controlador de LAN inalámbrico (WLC) para la autenticación EAP (Extensible Authentication Protocol) con el uso de un servidor RADIUS externo como Access Control Server (ACS) 5.2.

## Prerequisites

## Requirements

Asegúrese de cumplir estos requisitos antes de intentar realizar esta configuración:

- Tener un conocimiento básico del WLC y los Lightweight Access Points (LAPs)
- Tener un conocimiento funcional del servidor AAA

- Poseer un conocimiento profundo de las redes inalámbricas y de los problemas de seguridad inalámbrica

## Componentes Utilizados

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

- Cisco 5508 WLC que ejecuta la versión 7.0.220.0 del firmware
- LAP de la serie 3502 de Cisco
- Sublicante nativo de Microsoft Windows 7 con controlador Intel 6300-N versión 14.3
- Cisco Secure ACS que ejecuta la versión 5.2
- Switch Cisco serie 3560

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). If your network is live, make sure that you understand the potential impact of any command.

## Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

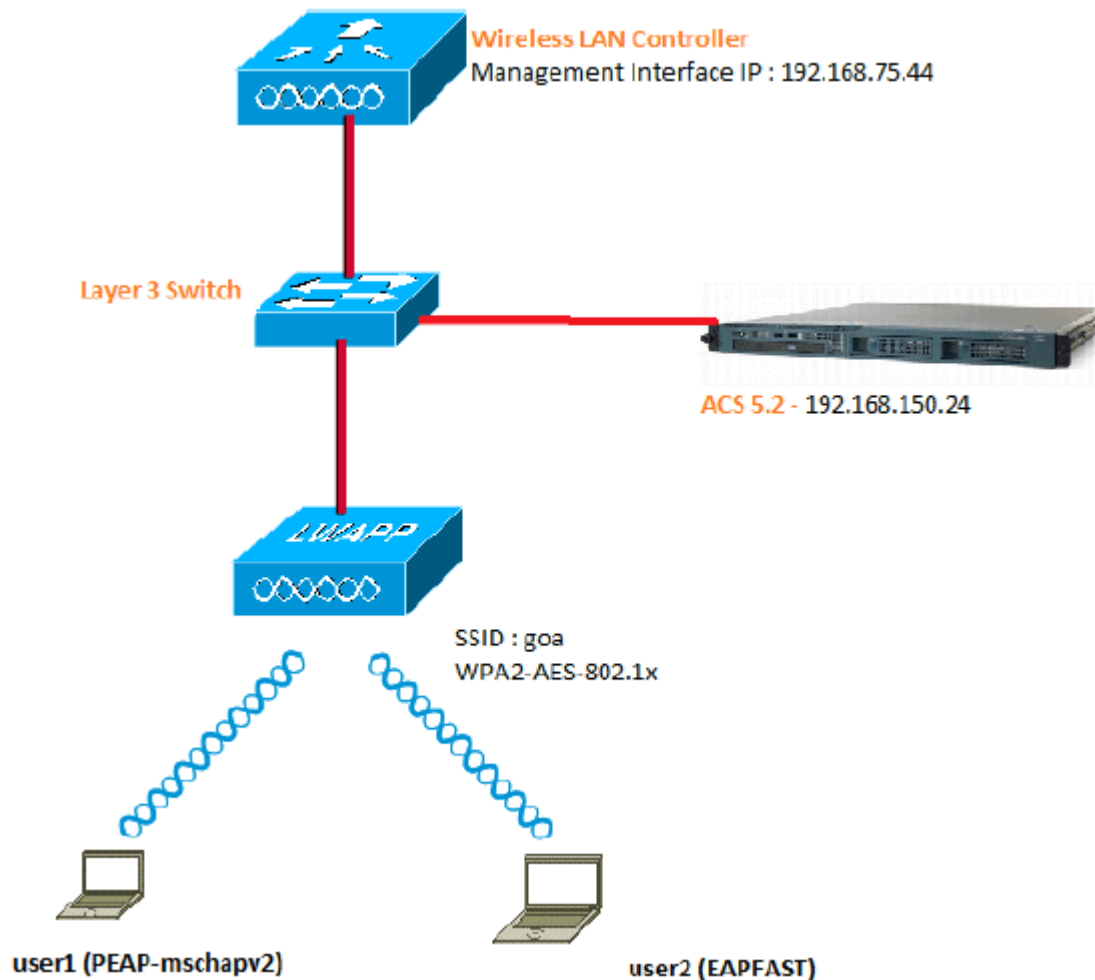
## Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

**Nota:** Utilice la herramienta [Command Lookup](#) (sólo para clientes [registrados](#)) para obtener más información sobre los comandos utilizados en esta sección.

## Diagrama de la red

En este documento, se utiliza esta configuración de red:



Estos son los detalles de configuración de los componentes utilizados en este diagrama:

- La dirección IP del servidor ACS (RADIUS) es 192.168.150.24.
- La dirección de la interfaz de administración y del administrador AP del WLC es 192.168.75.44.
- Los servidores DHCP dirigen 192.168.150.25.
- La VLAN 253 se utiliza en toda esta configuración. Ambos usuarios se conectan al mismo SSID "goa". Sin embargo, el usuario 1 está configurado para autenticarse mediante PEAP-MSCHAPv2 y el usuario 2 mediante EAP-FAST.
- Los usuarios se asignarán en la VLAN 253:
  - VLAN 253: 192.168.153.x/24. Gateway: 192.168.153.1
  - VLAN 75: 192.168.75.x/24. Gateway: 192.168.75.1

## Suposición

- Los switches se configuran para todas las VLAN de Capa 3.
- Al servidor DHCP se le asigna un ámbito DHCP.
- Existe conectividad de capa 3 entre todos los dispositivos de la red.
- El LAP ya está unido al WLC.

- Cada VLAN tiene una máscara /24.
- ACS 5.2 tiene instalado un certificado autofirmado.

## Configuration Steps

Esta configuración se divide en tres pasos de alto nivel:

1. [Configure el servidor RADIUS.](#)
2. [Configure el WLC.](#)
3. [Configuración de la utilidad de cliente inalámbrico.](#)

## Configuración del servidor RADIUS

La configuración del servidor RADIUS se divide en cuatro pasos:

1. [Configure los recursos de red.](#)
2. [Configurar usuarios.](#)
3. [Definir elementos de política.](#)
4. [Aplique políticas de acceso.](#)

ACS 5.x es un sistema de control de acceso basado en políticas. Es decir, ACS 5.x utiliza un modelo de política basado en reglas en lugar del modelo basado en grupos utilizado en las versiones 4.x.

El modelo de políticas basadas en reglas ACS 5.x proporciona un control de acceso más potente y flexible en comparación con el antiguo enfoque basado en grupos.

En el modelo basado en grupos más antiguo, un grupo define la política porque contiene y une tres tipos de información:

- Información de identidad: esta información puede estar basada en la pertenencia a grupos AD o LDAP o en una asignación estática para usuarios internos de ACS.
- Otras restricciones o condiciones: restricciones de tiempo, restricciones de dispositivos, etc.
- Permisos: VLAN o niveles de privilegio de Cisco IOS®.

El modelo de políticas de ACS 5.x se basa en reglas con el formato:

- Si la condición entonces resultado

Por ejemplo, utilizamos la información descrita para el modelo basado en grupos:

- Si identity-condition, restricted-condition, authorization-profile.

Como resultado, esto nos da la flexibilidad de limitar en qué condiciones se permite al usuario acceder a la red, así como qué nivel de autorización se permite cuando se cumplen condiciones específicas.

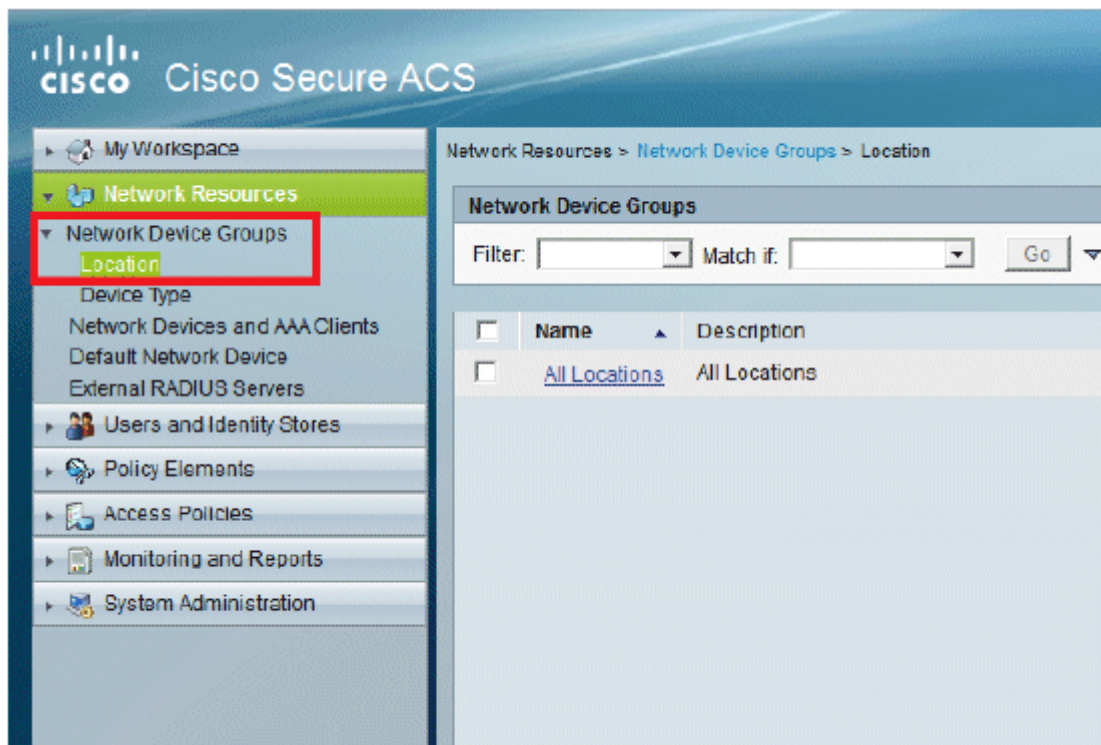
## Configurar recursos de red

En esta sección, configuramos el cliente AAA para el WLC en el servidor RADIUS.

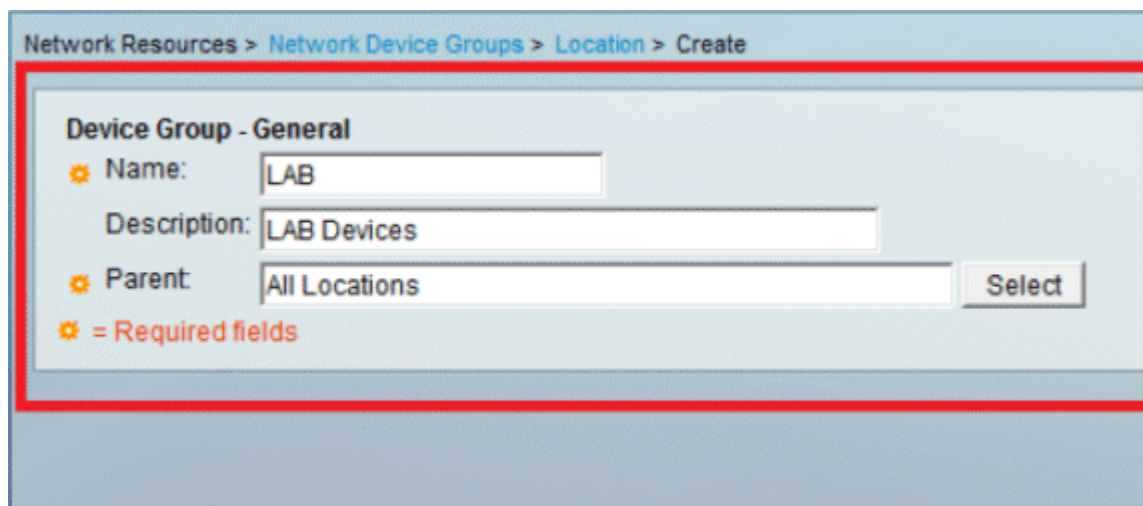
Este procedimiento explica cómo agregar el WLC como cliente AAA en el servidor RADIUS para que el WLC pueda pasar las credenciales del usuario al servidor RADIUS.

Complete estos pasos:

1. Desde la GUI de ACS, vaya a **Network Resources > Network Device Groups > Location**, y haga clic en **Create** (en la parte inferior).

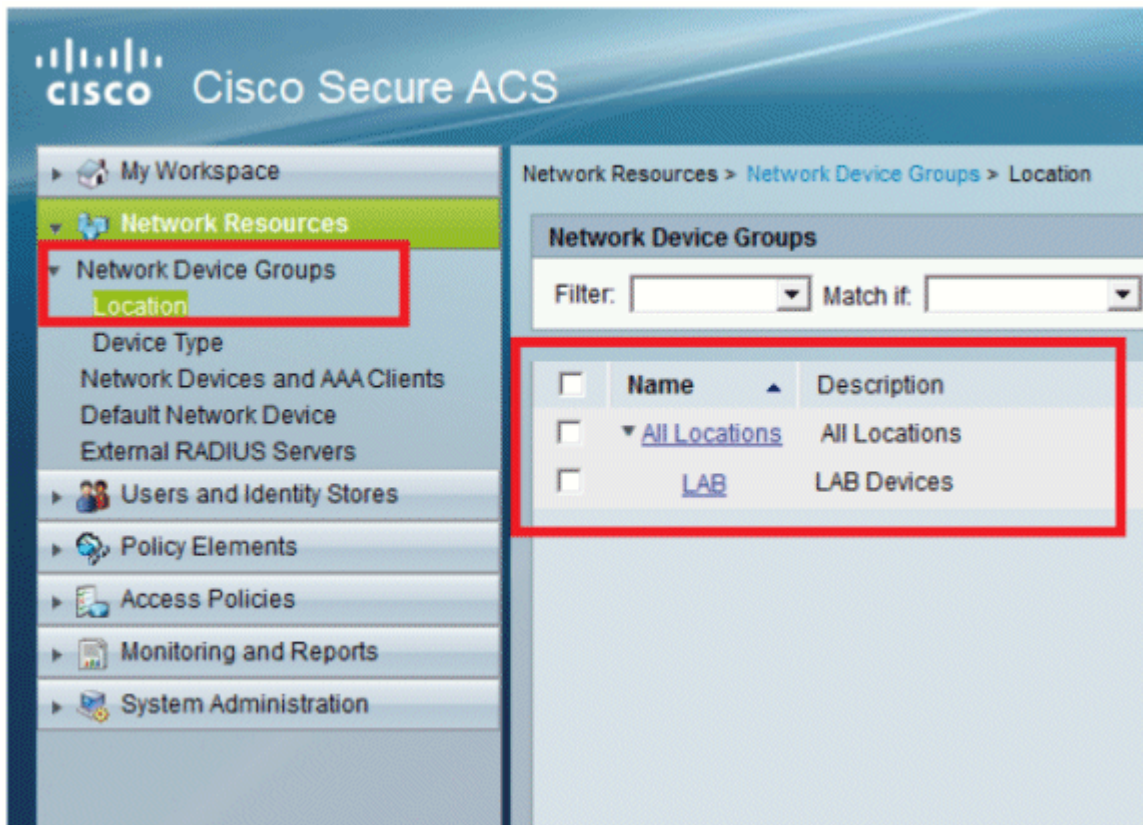


2. Agregue los campos obligatorios y haga clic en **Enviar**.

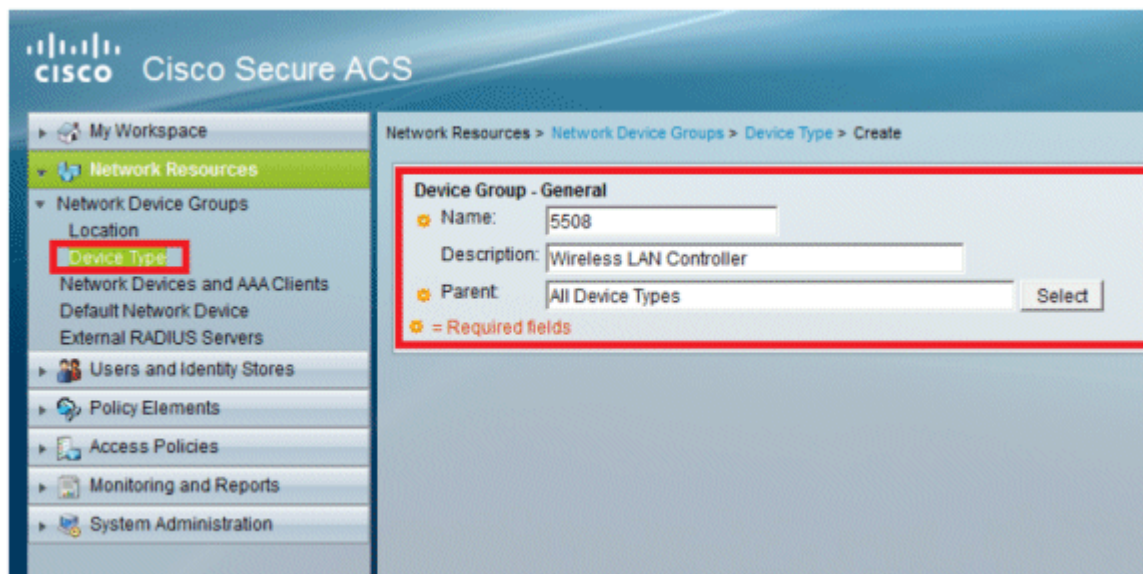


Ahora verá esta pantalla:

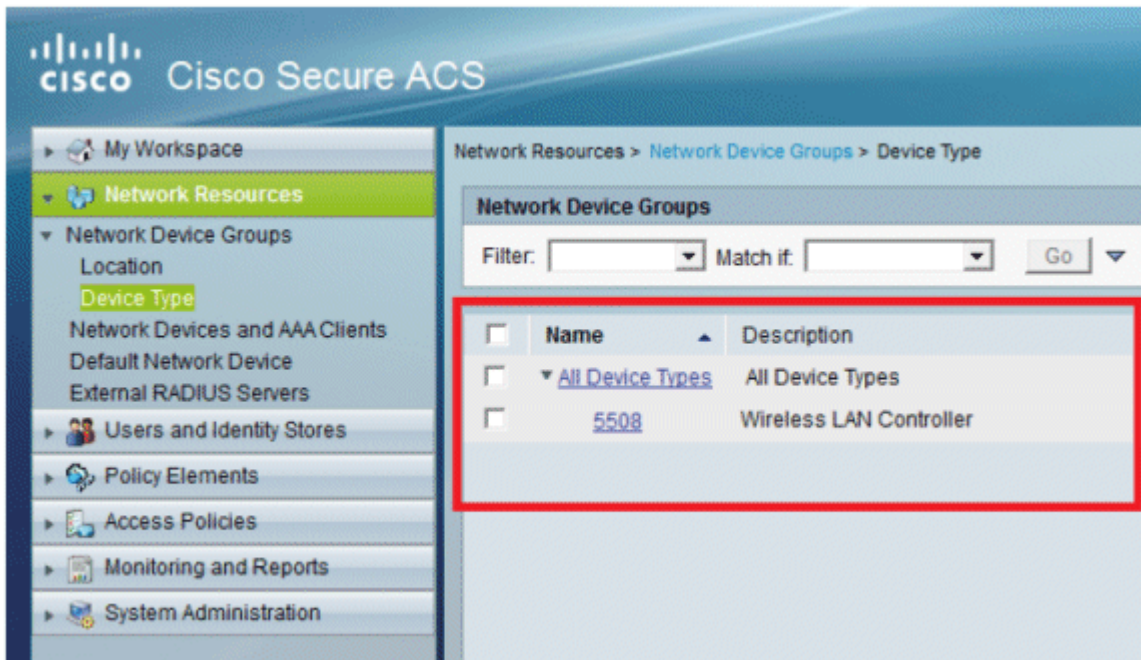




3. Haga clic en **Tipo de dispositivo > Crear**.

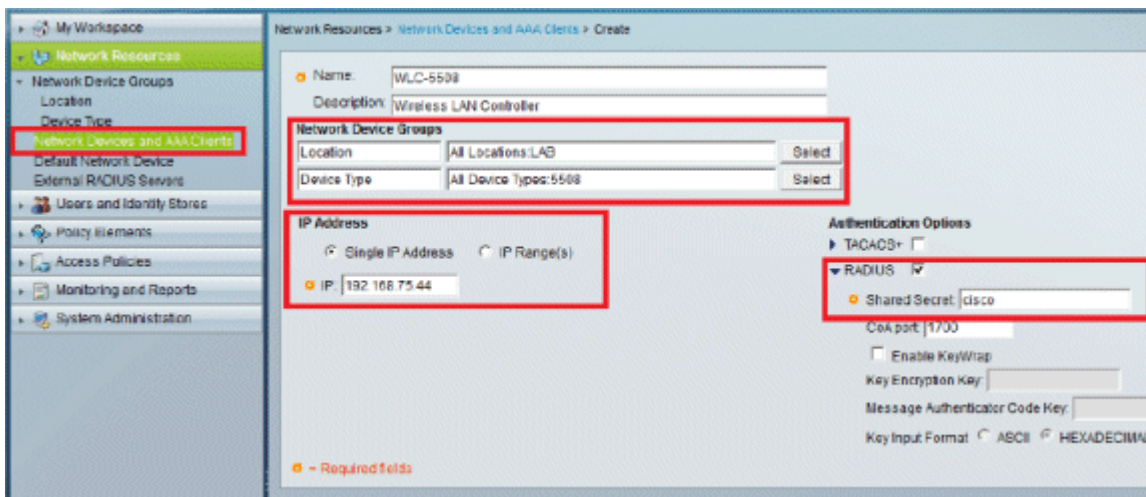


4. Haga clic en Submit (Enviar). Ahora verá esta pantalla:

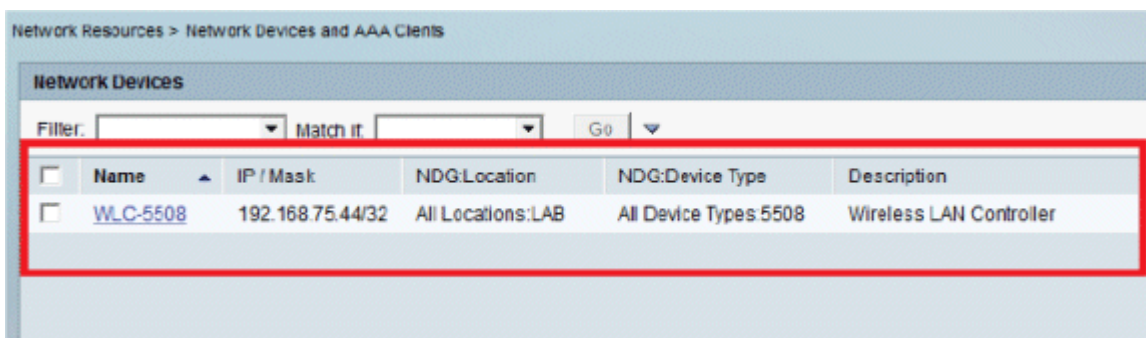


5. Vaya a **Recursos de red > Dispositivos de red y clientes AAA**.

6. Haga clic en **Create** y rellene los detalles como se muestra aquí:



7. Haga clic en Submit (Enviar). Ahora verá esta pantalla:

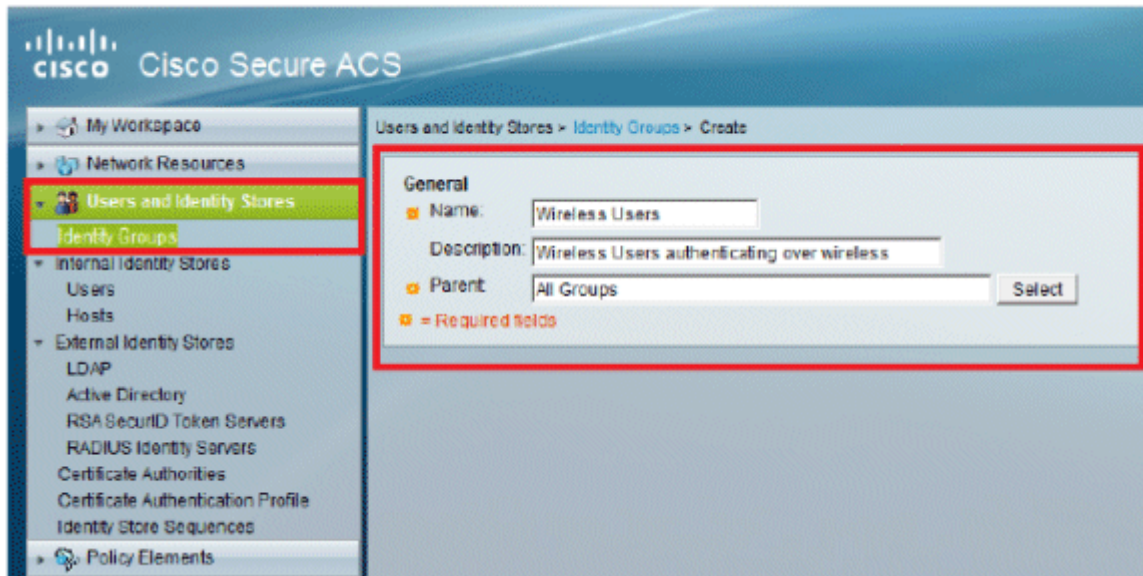


## Configurar usuarios

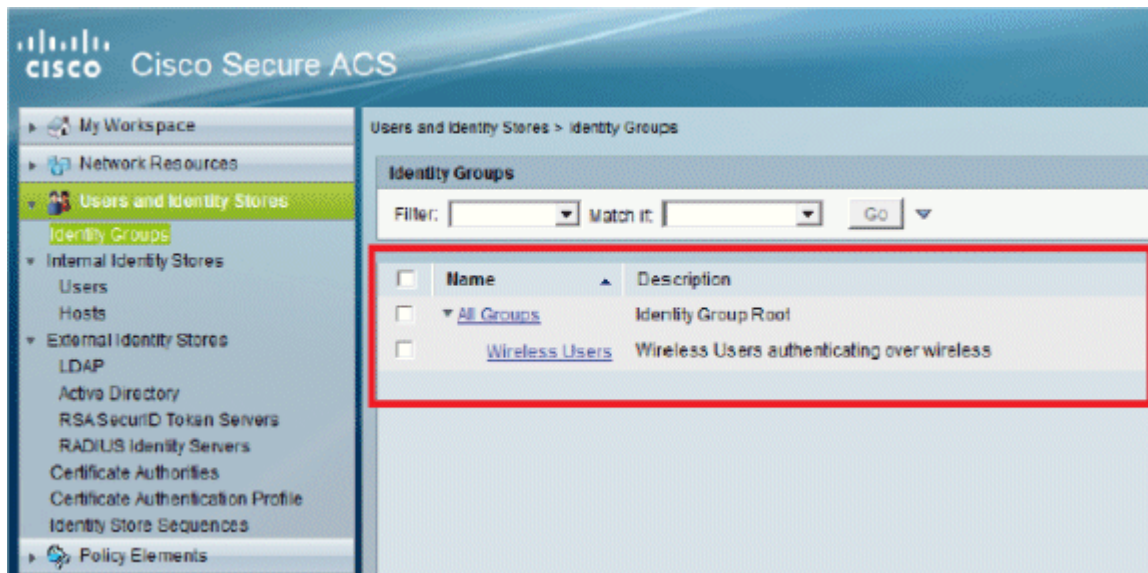
En esta sección, crearemos usuarios locales en ACS. Ambos usuarios (usuario1 y usuario2) están asignados en un grupo denominado "Usuarios inalámbricos".



1. Vaya a **Usuarios y almacenes de identidad > Grupos de identidad > Crear**.



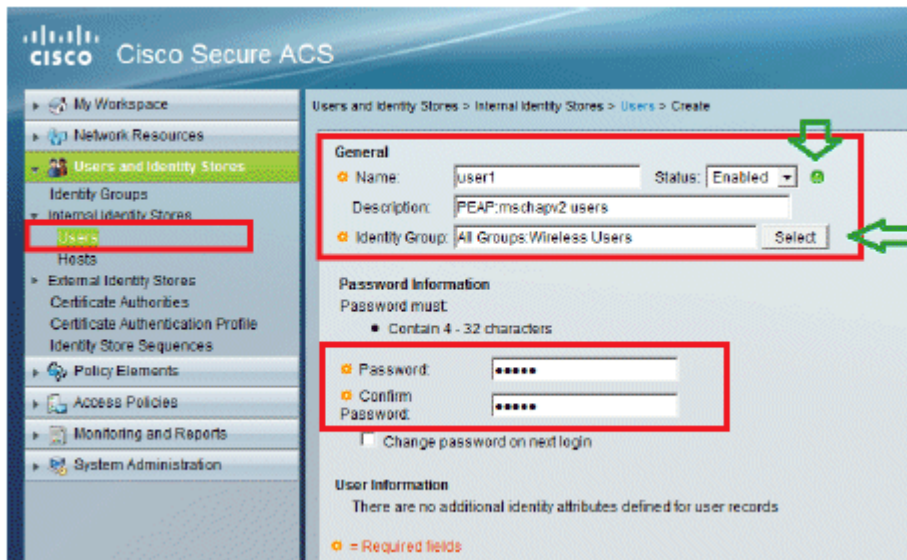
2. Una vez que haga clic en **Submit**, la página tendrá el siguiente aspecto:



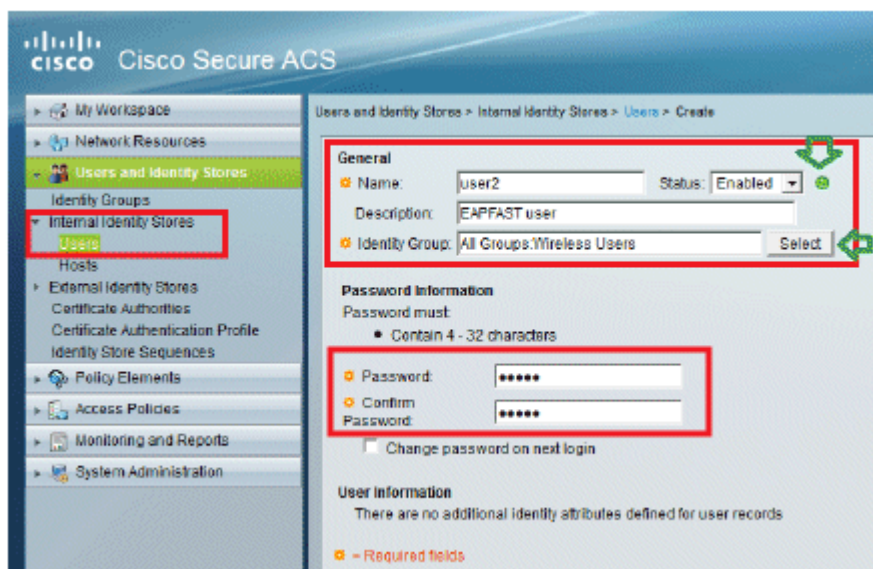
3. Cree los usuarios **user1** y **user2** y asígnelos al grupo "Usuarios inalámbricos".

a. Haga clic en **Usuarios y almacenes de identidad > Grupos de identidad > Usuarios > Crear**.

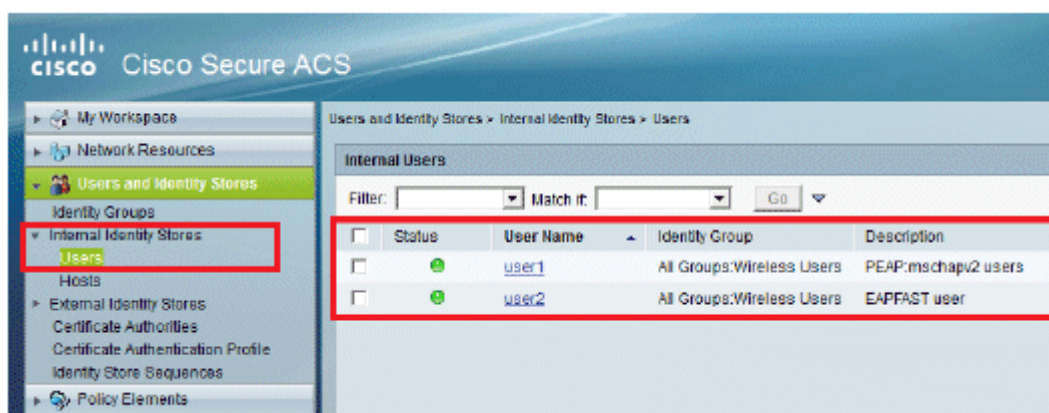




b. De manera similar, cree user2.

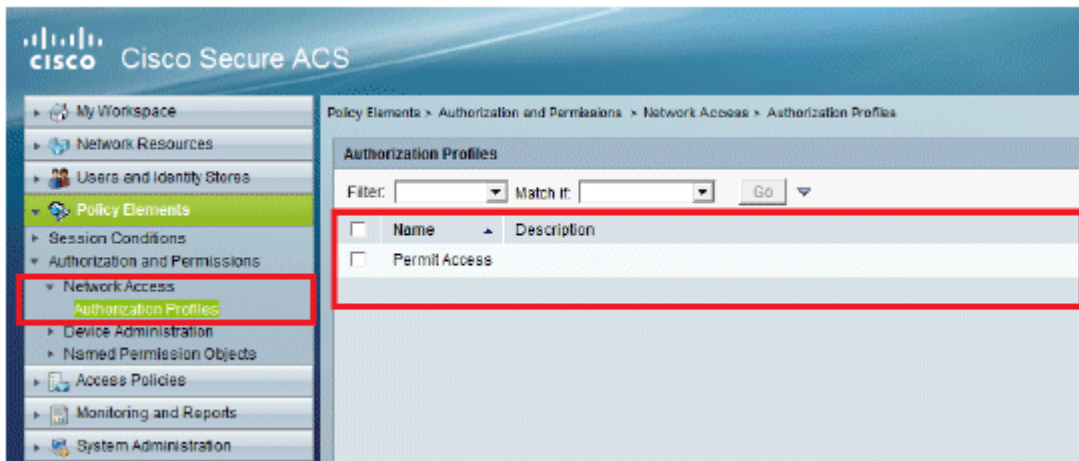


La pantalla tendrá el siguiente aspecto:



## Definición de elementos de política

Verifique que **Permit Access** esté configurado.

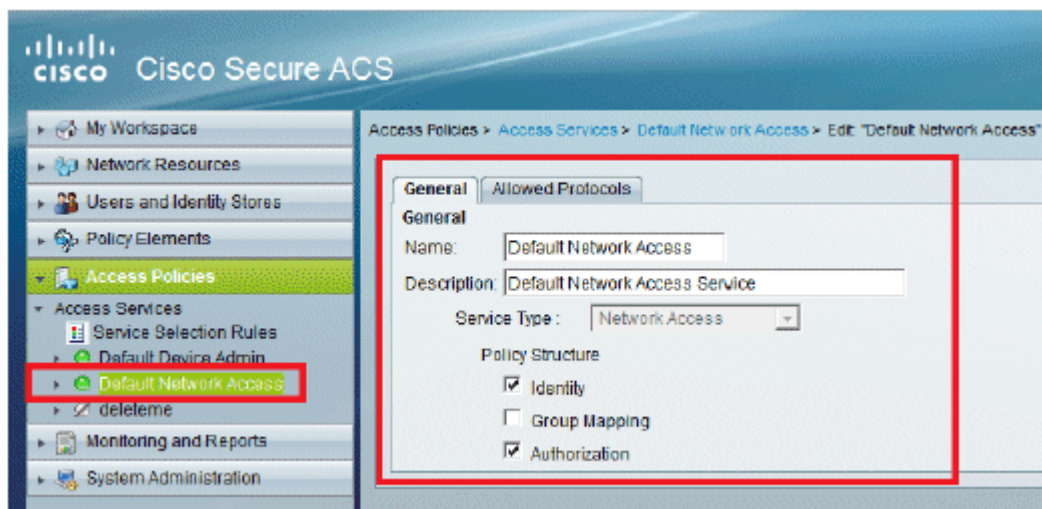


## Aplicar políticas de acceso

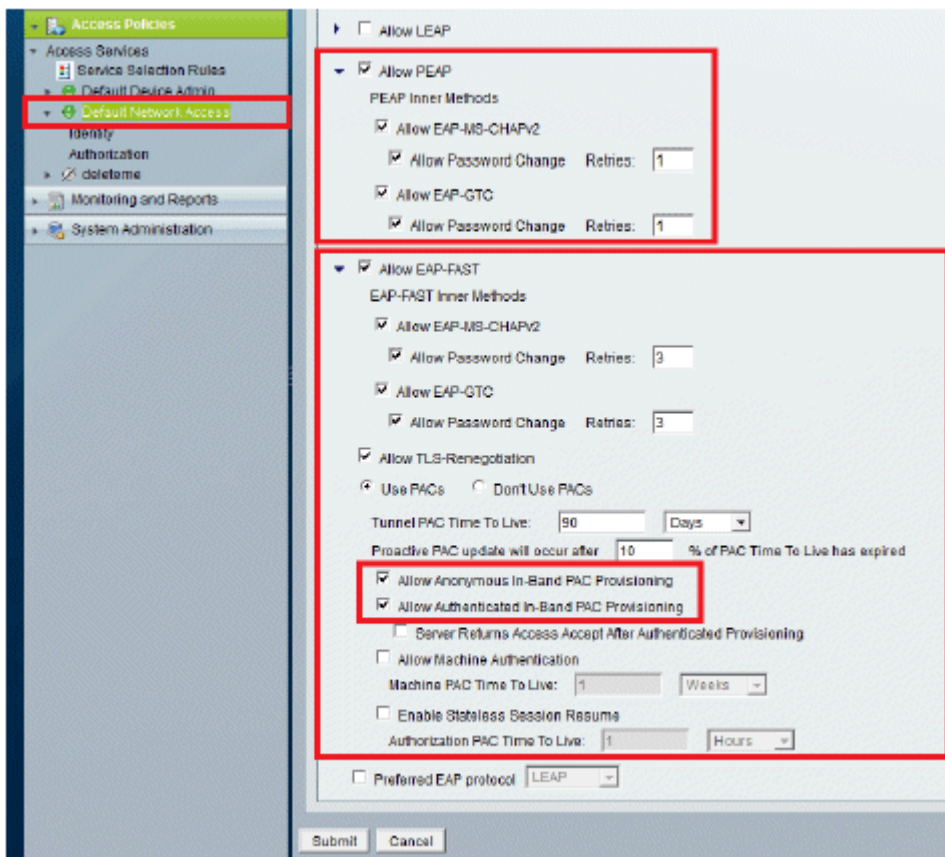
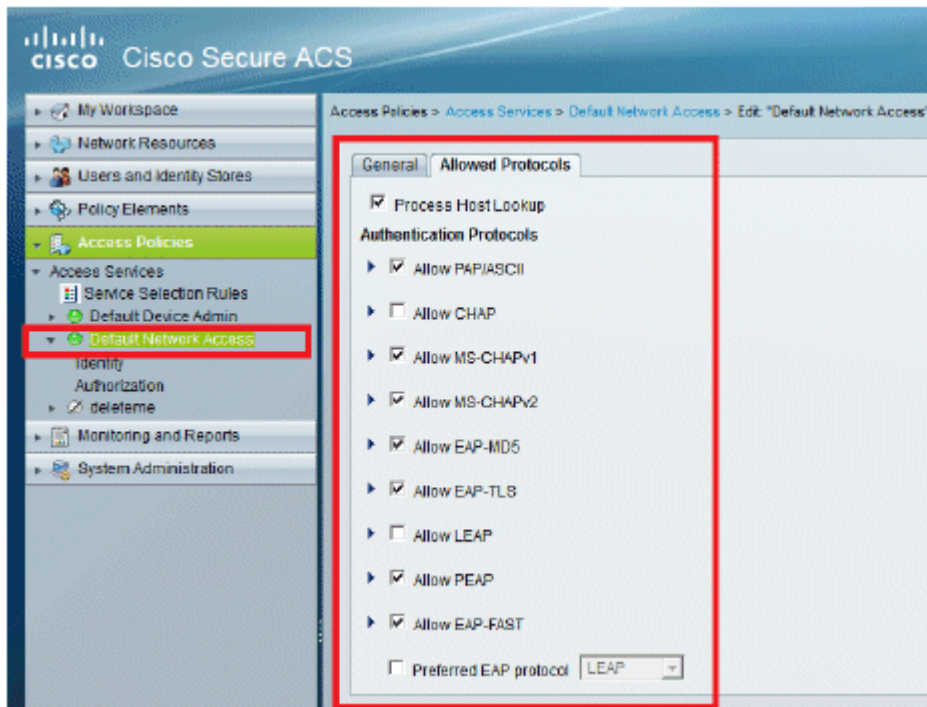
En esta sección, seleccionaremos qué métodos de autenticación se utilizarán y cómo se configurarán las reglas. Crearemos reglas basadas en los pasos anteriores.

Complete estos pasos:

1. Vaya a **Políticas de acceso > Servicios de acceso > Acceso a la red predeterminado > Editar: "Acceso a la red predeterminado"**.



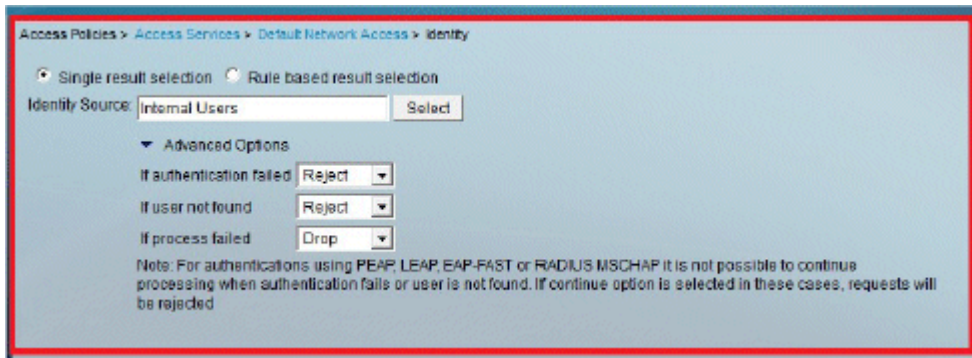
2. Seleccione el método EAP que desea que autenticuen los clientes inalámbricos. En este ejemplo, utilizamos **PEAP- MSCHAPv2** y **EAP-FAST**.



3. Haga clic en Submit (Enviar).

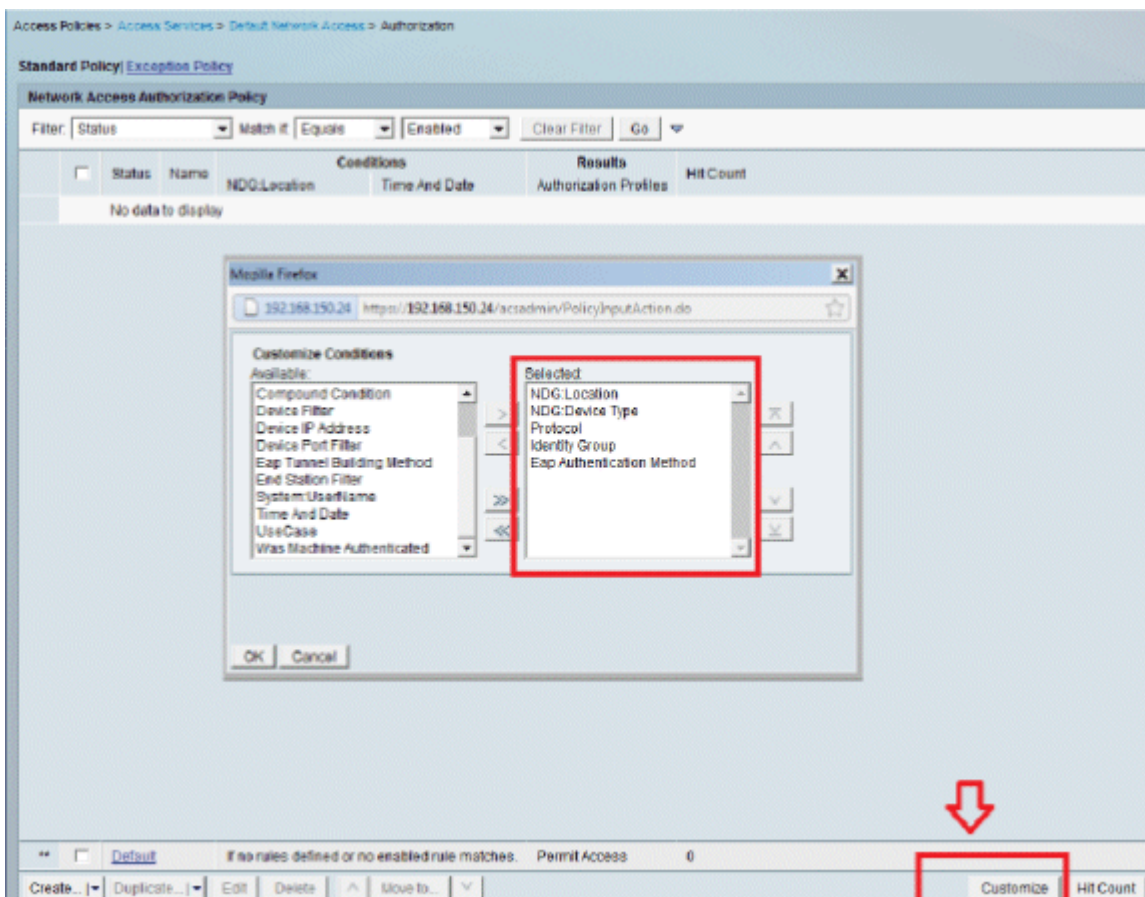
4. Verifique el grupo de identidad que ha seleccionado. En este ejemplo, utilizamos **Internal Users**, que creamos en ACS. **Guarde los cambios.**





5. Para verificar el perfil de autorización, vaya a **Access Policies > Access Services > Default Network Access > Authorization**.

Puede personalizar en qué condiciones permitirá el acceso de los usuarios a la red y qué perfil de autorización (atributos) pasará una vez autenticado. Esta granularidad sólo está disponible en ACS 5.x. En este ejemplo, hemos seleccionado Location, **Device Type**, **Protocol**, **Identity Group** y EAP Authentication Method.

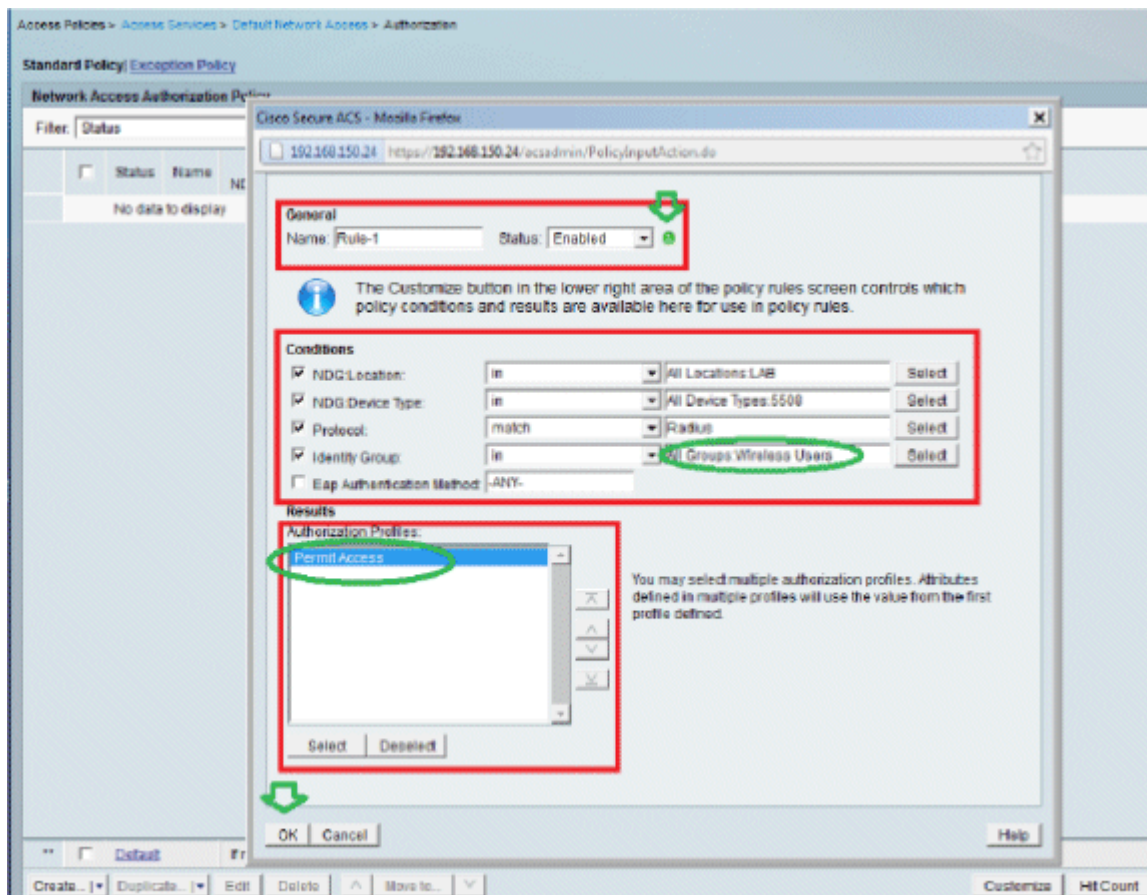


6. Haga clic en **Aceptar y Guardar cambios**.

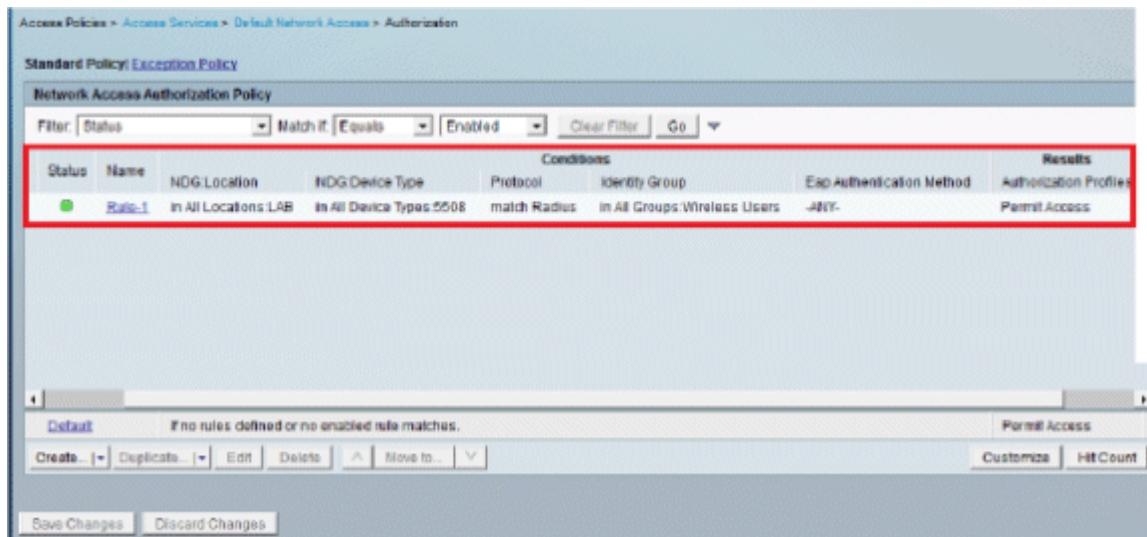
7. El siguiente paso consiste en crear una regla. Si no se define ninguna regla, se permite al cliente el acceso sin condiciones.

Haga clic en **Create > Rule-1**. Esta regla es para usuarios del grupo "Usuarios inalámbricos".



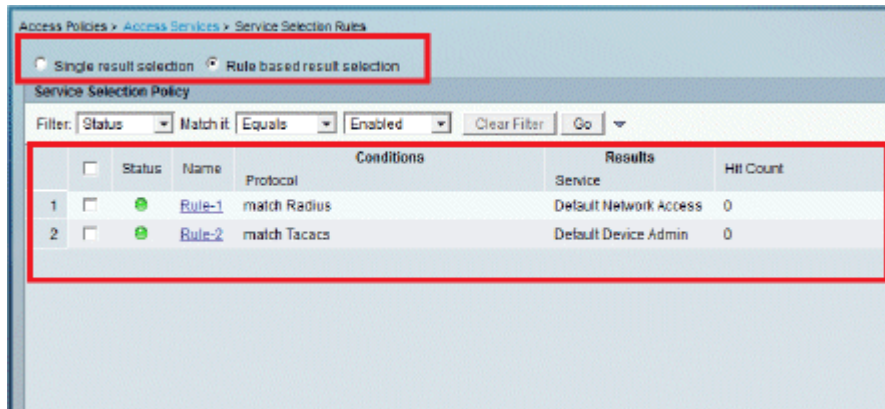


8. Guarde los cambios. La pantalla tendrá el siguiente aspecto:



Si desea que se denieguen los usuarios que no cumplan las condiciones, edite la regla predeterminada para que diga "denegar acceso".

9. Ahora definiremos las **reglas de selección de servicios**. Utilice esta página para configurar una política simple o basada en reglas para determinar qué servicio aplicar a las solicitudes entrantes. En este ejemplo, se utiliza una política basada en reglas.



## Configurar la WLC

La configuración requiere estos pasos:

1. [Configure el WLC con los detalles del servidor de autenticación.](#)
2. [Configure las interfaces dinámicas \(VLAN\).](#)
3. [Configure las WLAN \(SSID\).](#)

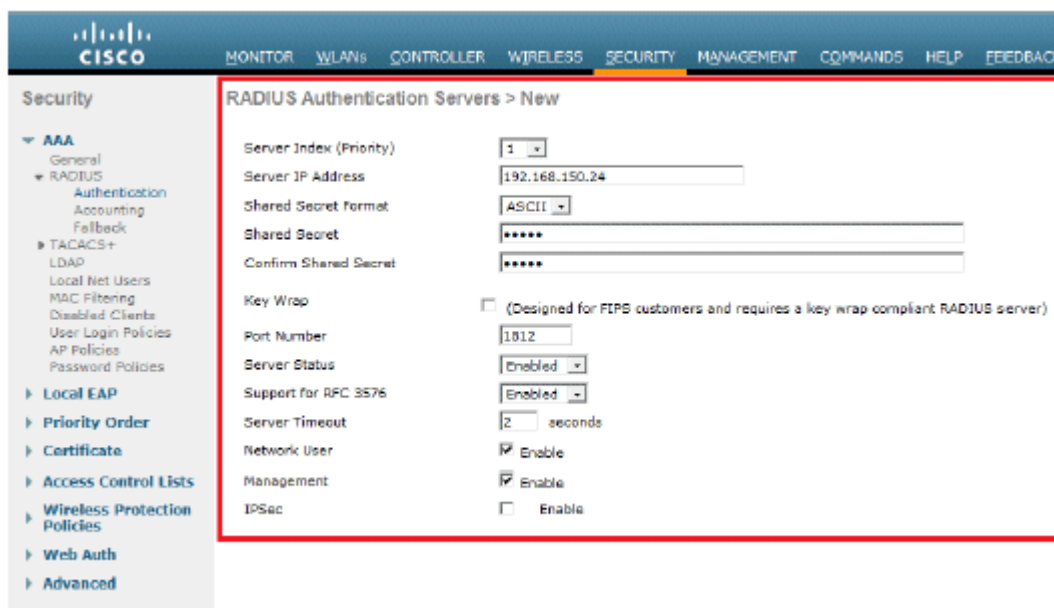
### Configure el WLC con los detalles del servidor de autenticación

Es necesario configurar el WLC para que pueda comunicarse con el servidor RADIUS para autenticar los clientes, y también para cualquier otra transacción.

Complete estos pasos:

1. En la GUI del controlador, haga clic en **Security**.
2. Introduzca la dirección IP del servidor RADIUS y la clave secreta compartida utilizada entre el servidor RADIUS y el WLC.

Esta clave secreta compartida debe ser la misma que la configurada en el servidor RADIUS.

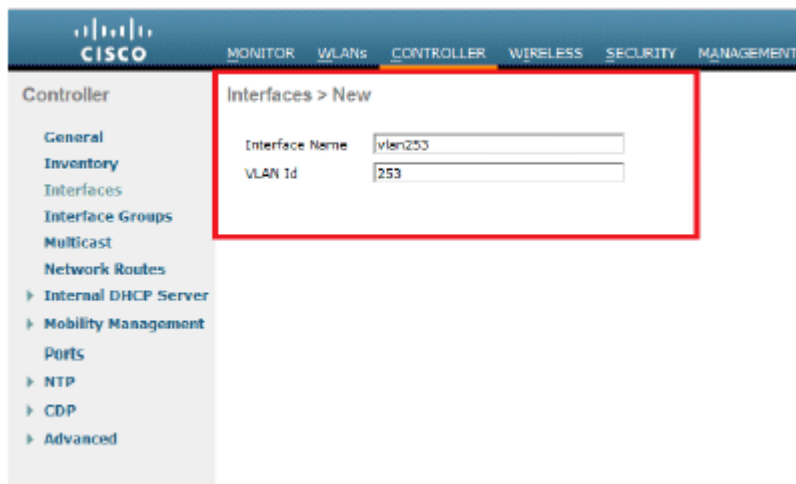


## Configuración de las interfaces dinámicas (VLAN)

Este procedimiento describe cómo configurar las interfaces dinámicas en el WLC.

Complete estos pasos:

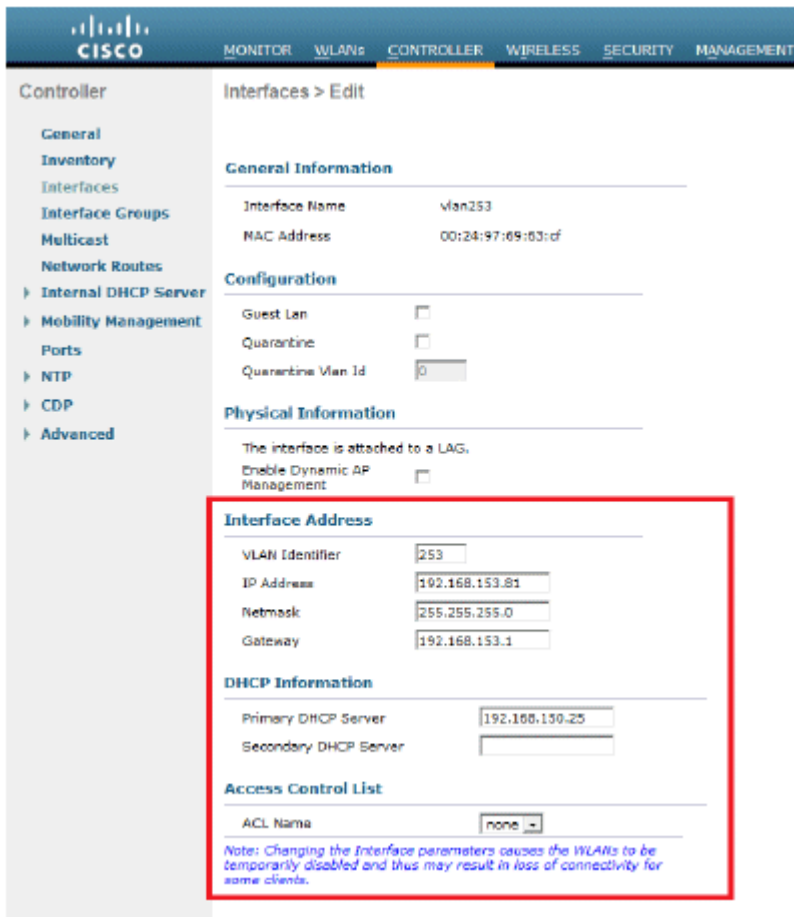
1. La interfaz dinámica se configura desde la GUI del controlador, en la ventana **Controller > Interfaces**.



2. Haga clic en Apply (Aplicar).

Esto lo lleva a la ventana Edit (Editar) de esta interfaz dinámica (VLAN 253 aquí).

3. Introduzca la dirección IP y el gateway predeterminado de esta interfaz dinámica.



4. Haga clic en Apply (Aplicar).

5. Las interfaces configuradas tendrán el siguiente aspecto:



## Configuración de las WLAN (SSID)

Este procedimiento explica cómo configurar las WLANs en el WLC.

Complete estos pasos:

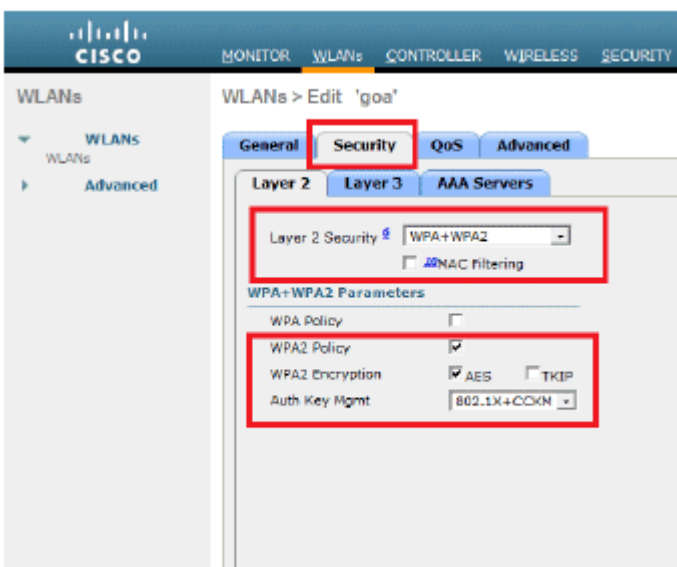
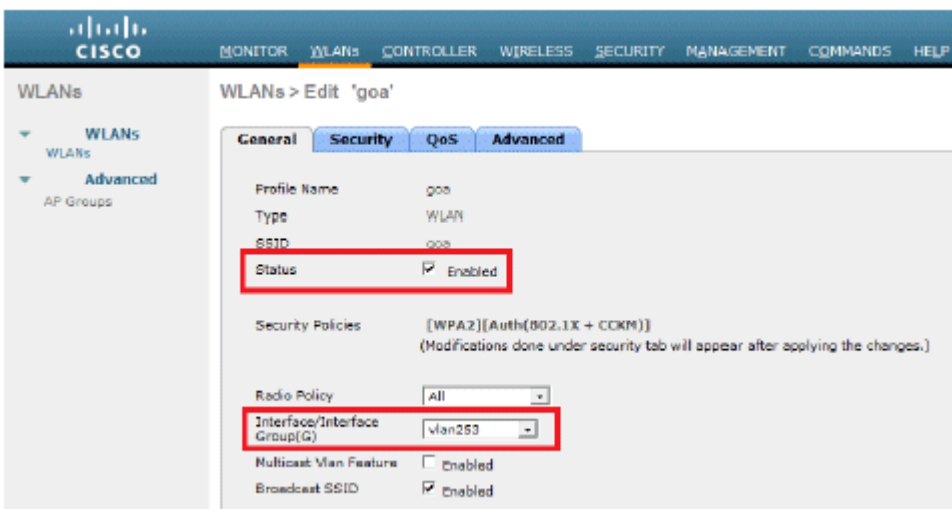
1. Desde el controlador GUI, vaya a **WLANs > Create New** para crear una nueva WLAN. Se muestra la ventana New WLANs (Nuevas WLAN).
2. Introduzca la información de ID de WLAN y SSID de WLAN.

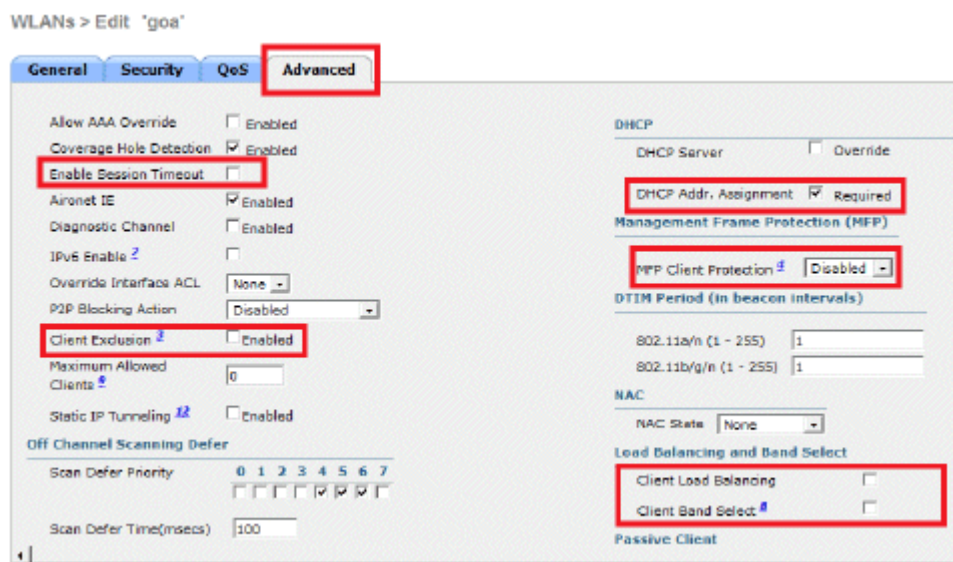
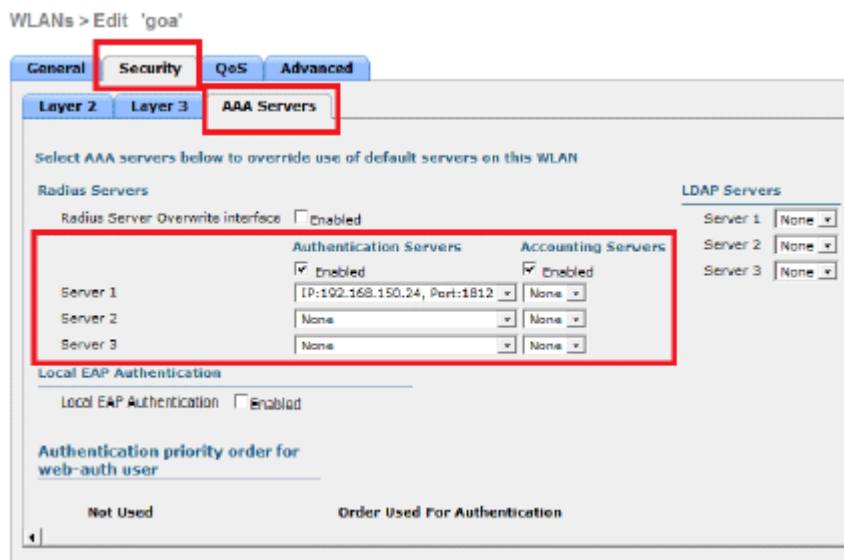


Puede introducir cualquier nombre como SSID de WLAN. Este ejemplo utiliza **goa** como el SSID de WLAN.



3. Haga clic en **Apply** para ir a la ventana Edit del objetivo WLAN.





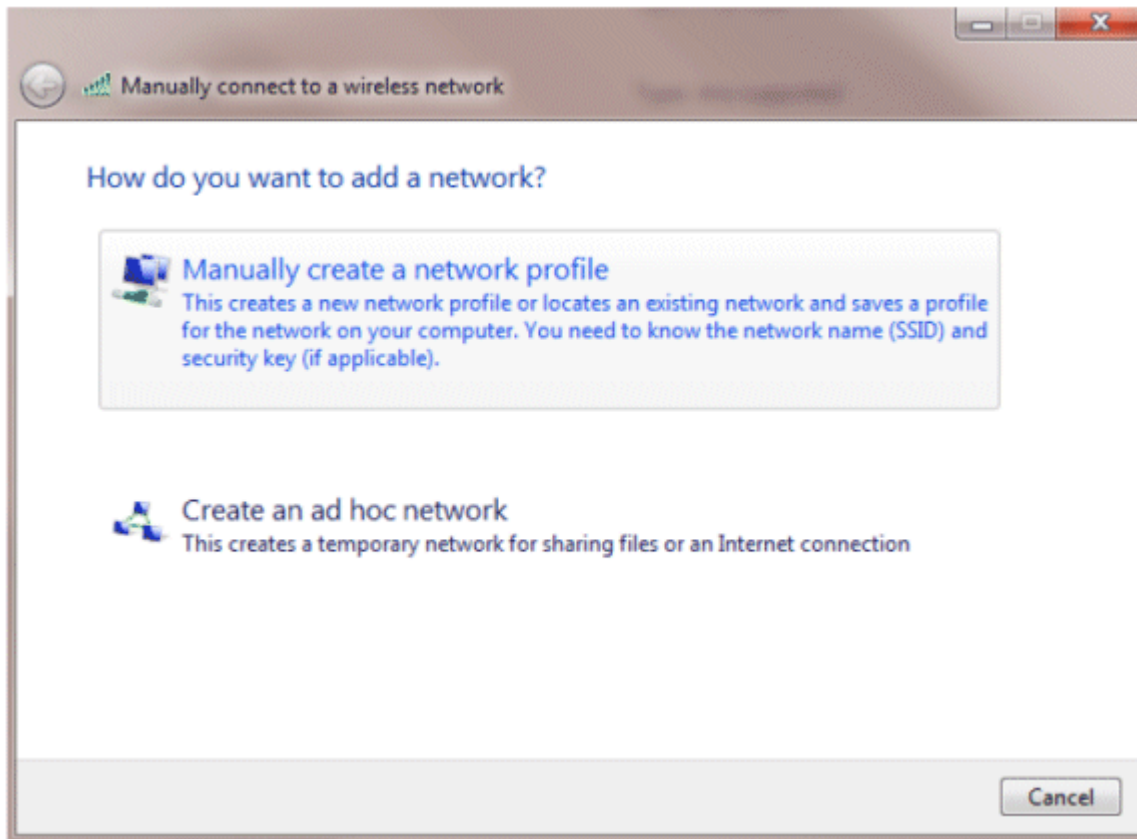
## Configuración de la utilidad de cliente inalámbrico

### PEAP-MSCHAPv2 (usuario1)

En nuestro cliente de prueba, utilizamos el suplicante nativo de Windows 7 con una tarjeta Intel 6300-N que ejecuta la versión de controlador 14.3. Se recomienda probar con los controladores más recientes de los proveedores.

Complete estos pasos para crear un perfil en Windows Zero Config (WZC):

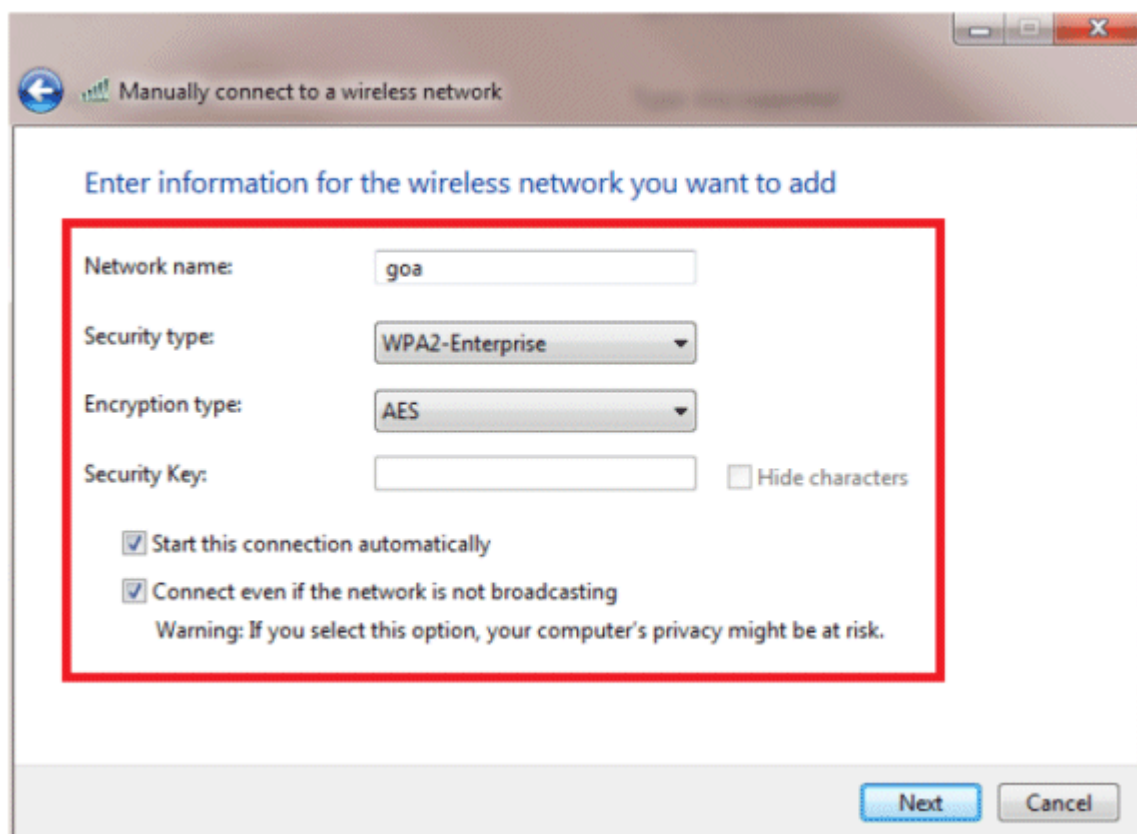
1. Vaya a **Control Panel > Network and Internet > Manage Wireless Networks**.
2. Haga clic en la pestaña **Add**.
3. Haga clic en **Crear manualmente un perfil de red**.



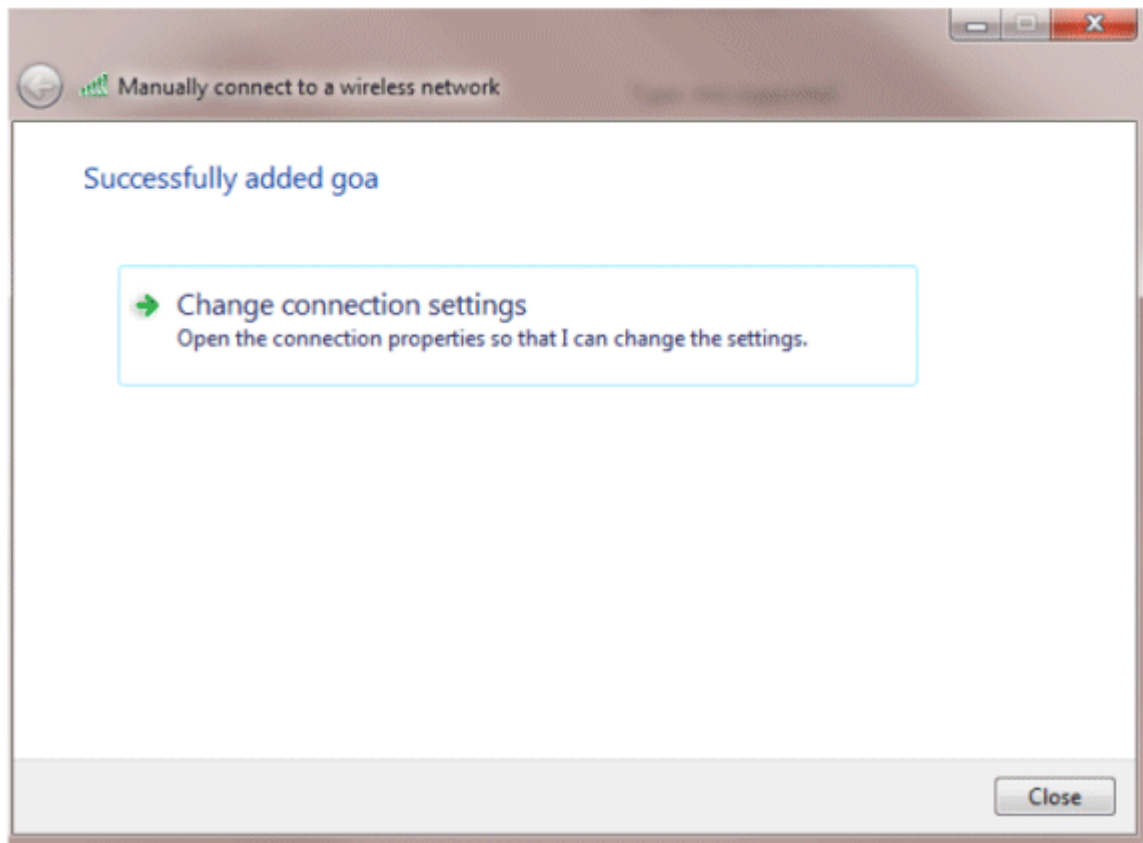
4. Agregue los detalles según lo configurado en el WLC.

**Nota:** El SSID distingue entre mayúsculas y minúsculas.

5. Haga clic en Next (Siguiente).



6. Haga clic en **Cambiar la configuración de la conexión** para volver a verificar la configuración.



7. Asegúrese de que tiene **PEAP** habilitado.



goa Wireless Network Properties



Connection Security

Security type: WPA2-Enterprise

Encryption type: AES

Choose a network authentication method:

Microsoft: Protected EAP (PEAP)

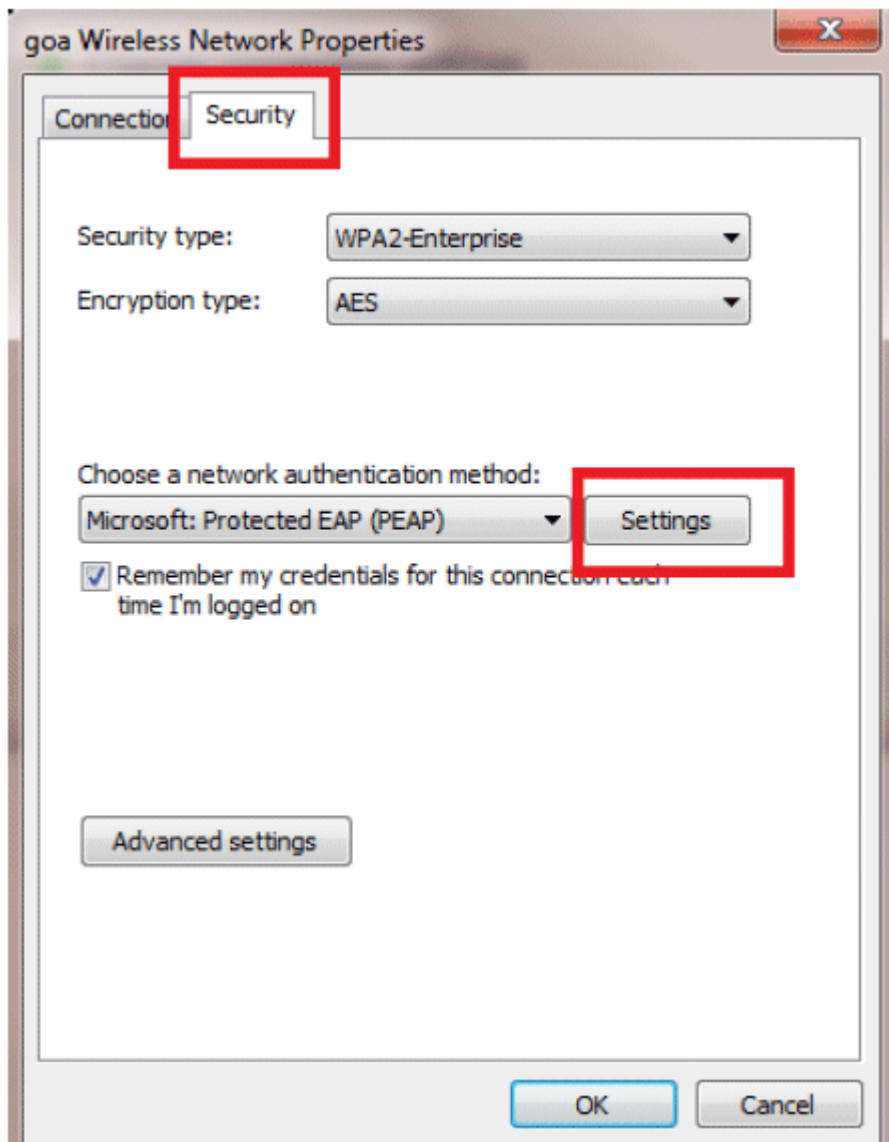
Settings

Remember my credentials for this connection each time I'm logged on

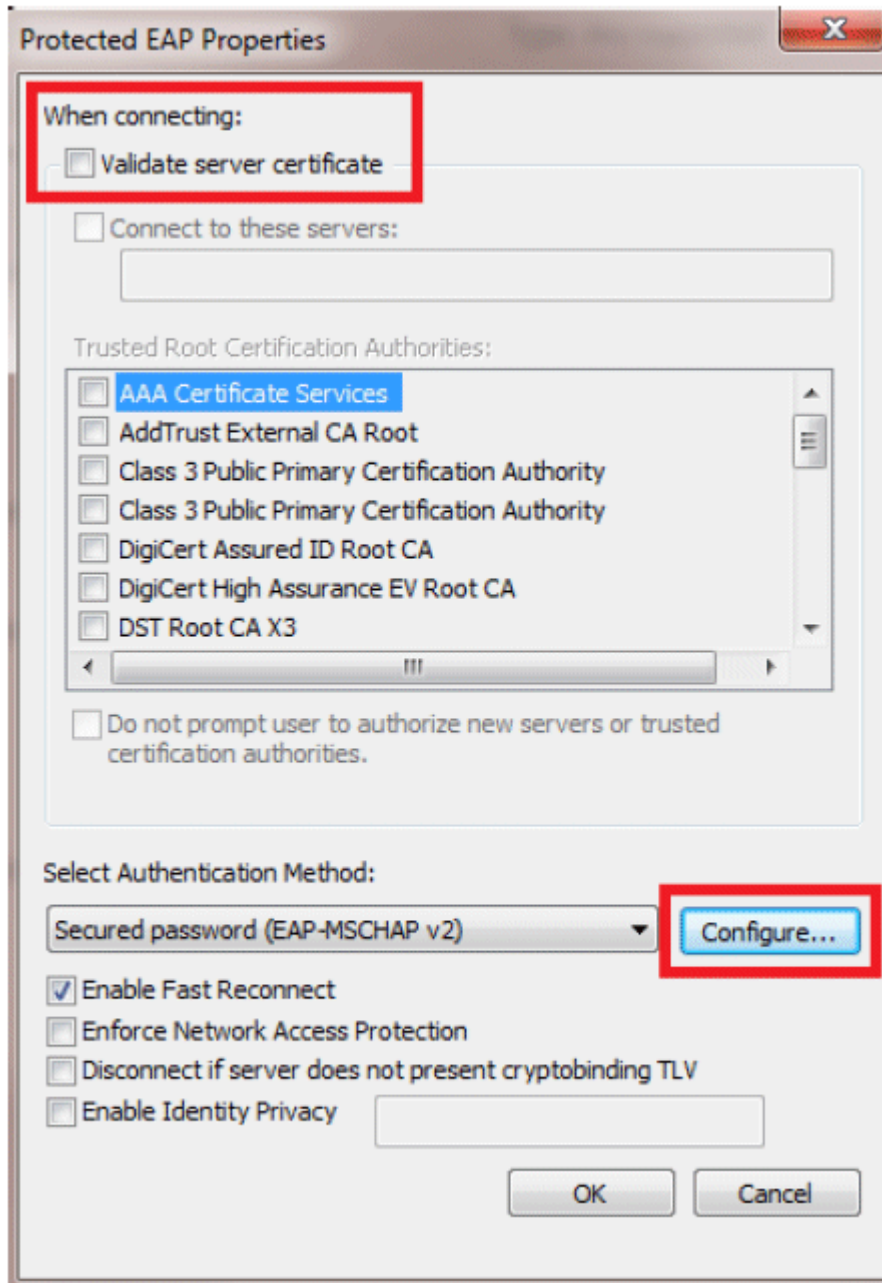
Advanced settings

OK

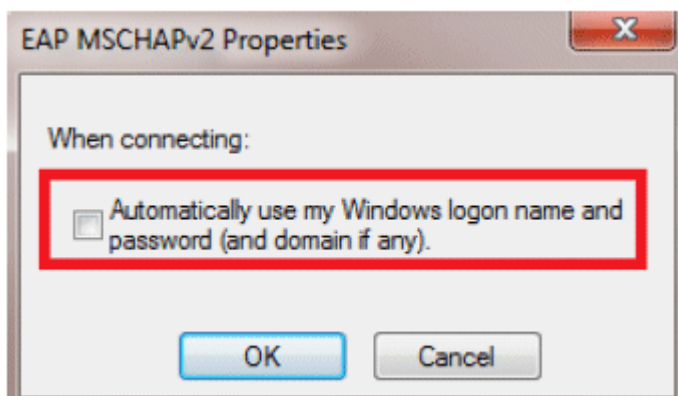
Cancel



8. En este ejemplo, no estamos validando el certificado del servidor. Si marca esta casilla y no puede conectarse, intente desactivar la función y vuelva a realizar la prueba.



9. También puede utilizar sus credenciales de Windows para iniciar sesión. Sin embargo, en este ejemplo no vamos a usar eso. Click OK.



10. Haga clic en **Advanced settings** para configurar el nombre de usuario y la contraseña.

goa Wireless Network Properties



Connection Security

Security type: WPA2-Enterprise

Encryption type: AES

Choose a network authentication method:

Microsoft: Protected EAP (PEAP) Settings

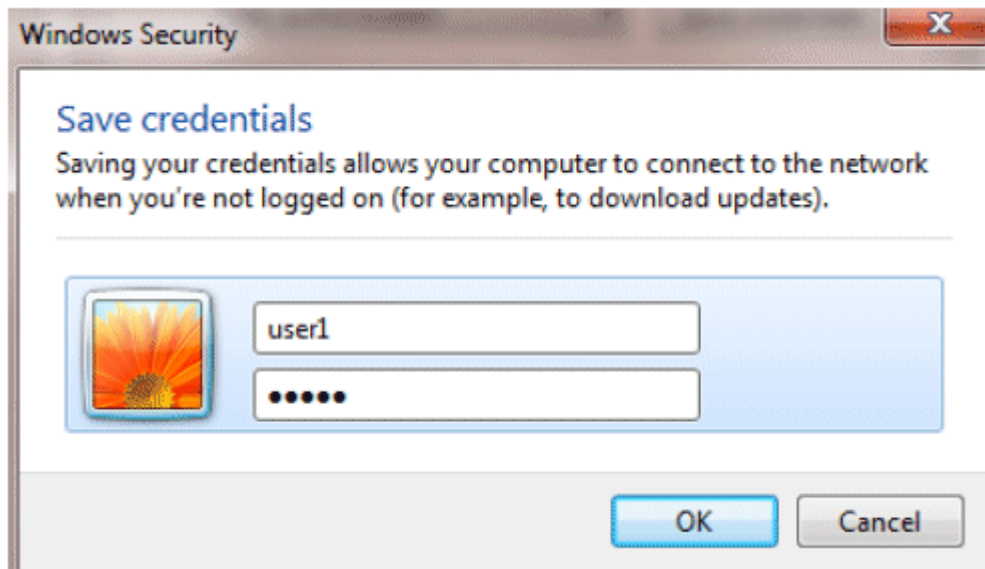
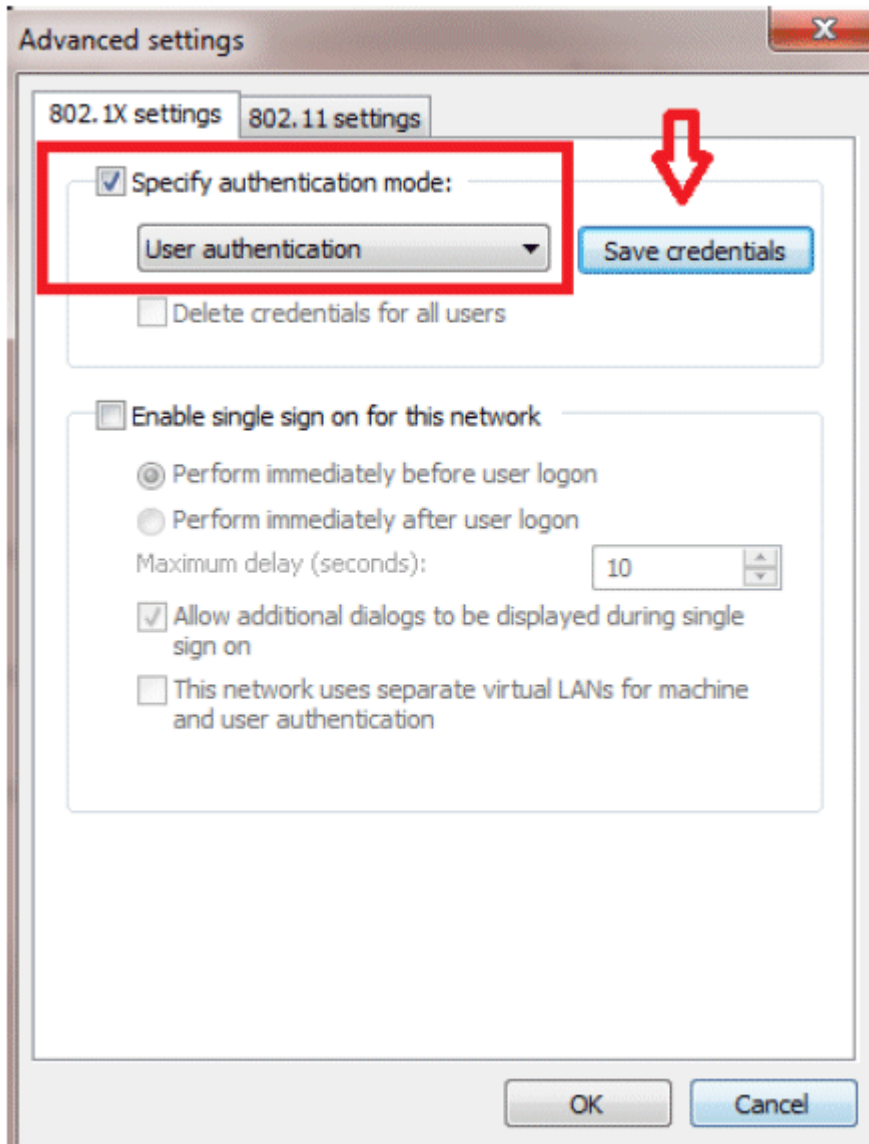
Remember my credentials for this connection each time I'm logged on

Advanced settings

OK

Cancel





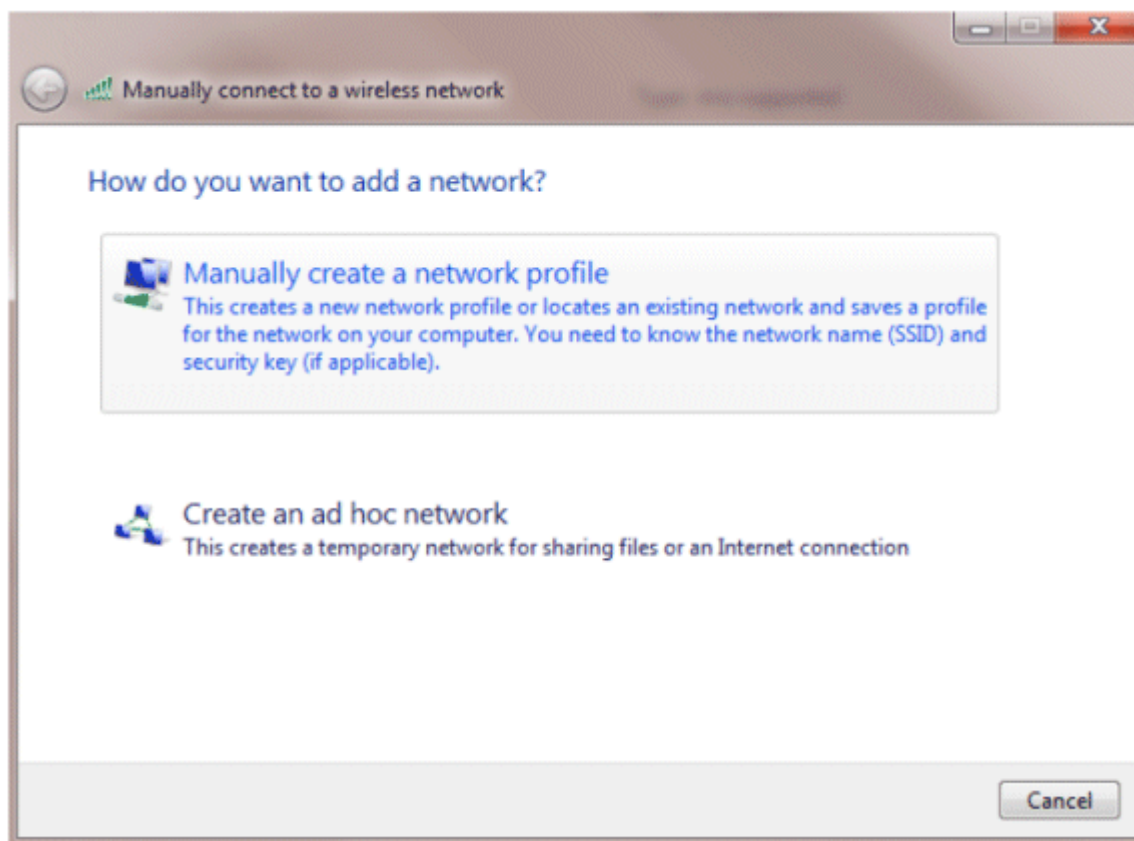
La utilidad de cliente ya está lista para conectarse.

**EAP-FAST (usuario2)**

En nuestro cliente de prueba, utilizamos el suplicante nativo de Windows 7 con una tarjeta Intel 6300-N que ejecuta la versión de controlador 14.3. Se recomienda probar con los controladores más recientes de los proveedores.

Complete estos pasos para crear un perfil en WZC:

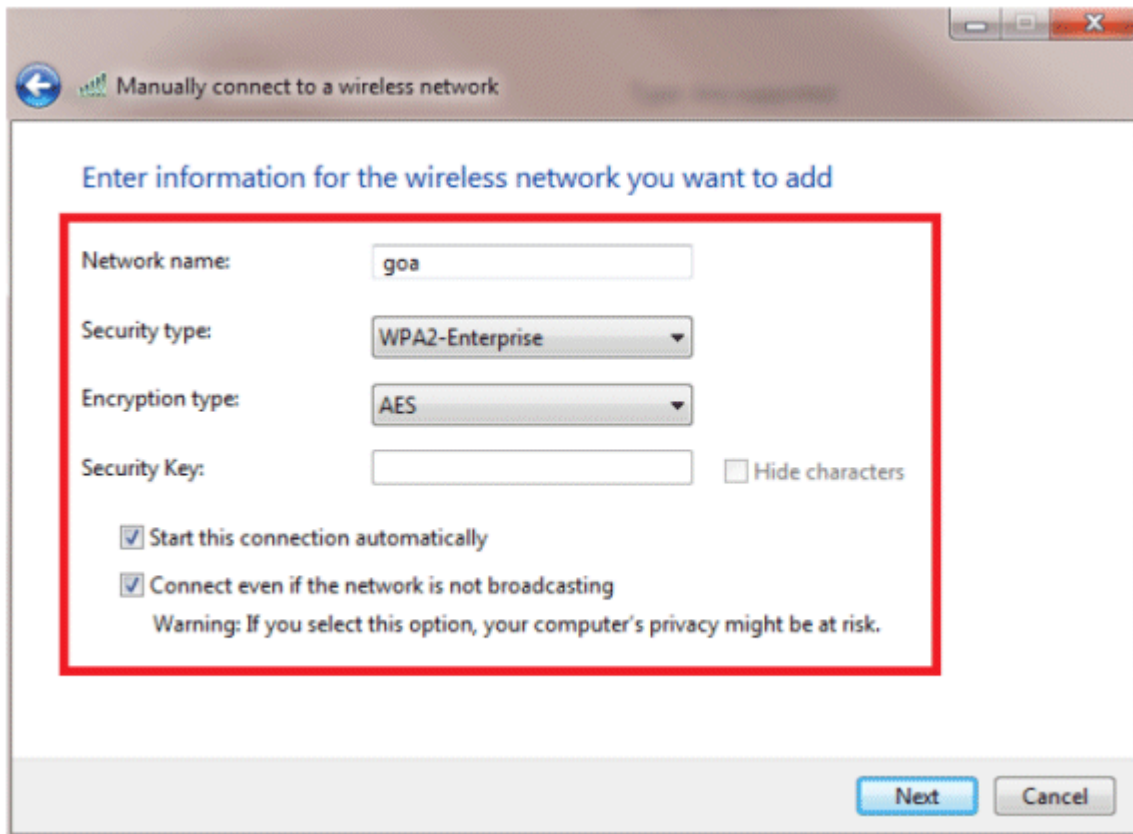
1. Vaya a **Control Panel > Network and Internet > Manage Wireless Networks**.
2. Haga clic en la pestaña **Add**.
3. Haga clic en **Crear manualmente un perfil de red**.



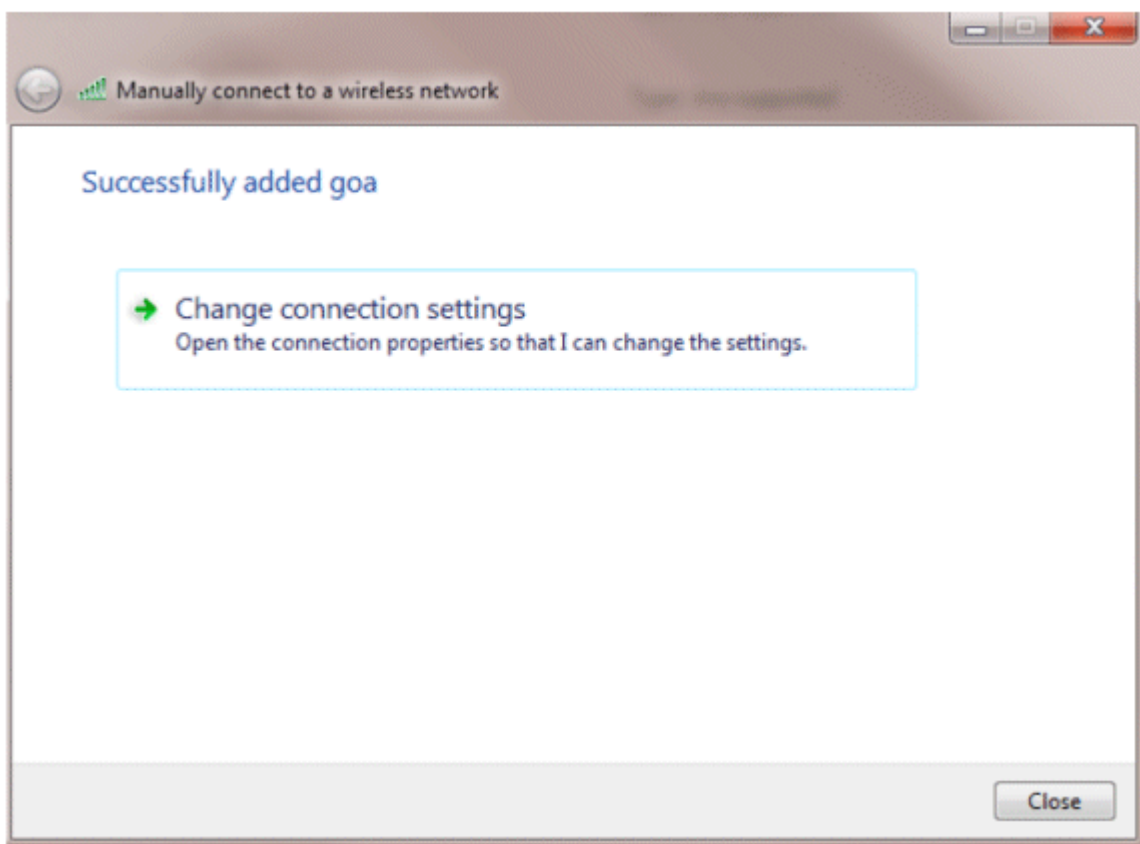
4. Agregue los detalles según lo configurado en el WLC.

**Nota:** El SSID distingue entre mayúsculas y minúsculas.

5. Haga clic en Next (Siguiente).



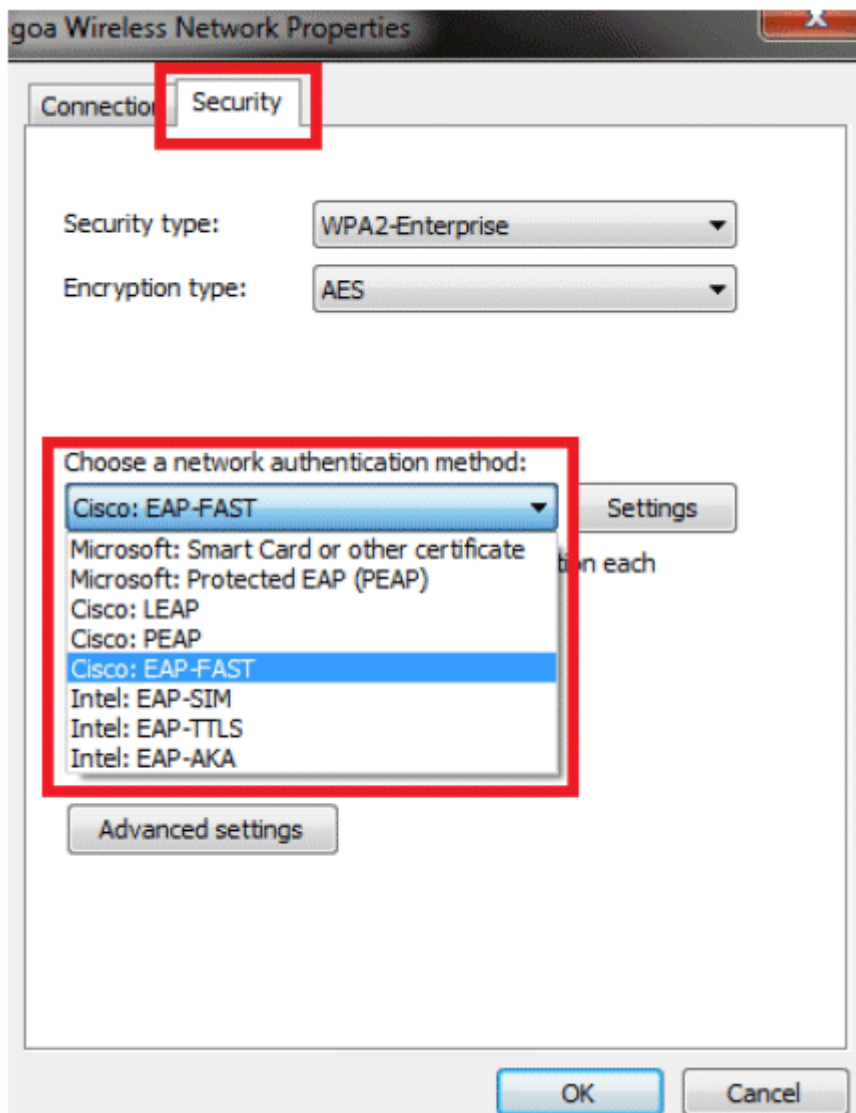
6. Haga clic en **Cambiar la configuración de la conexión** para volver a verificar la configuración.

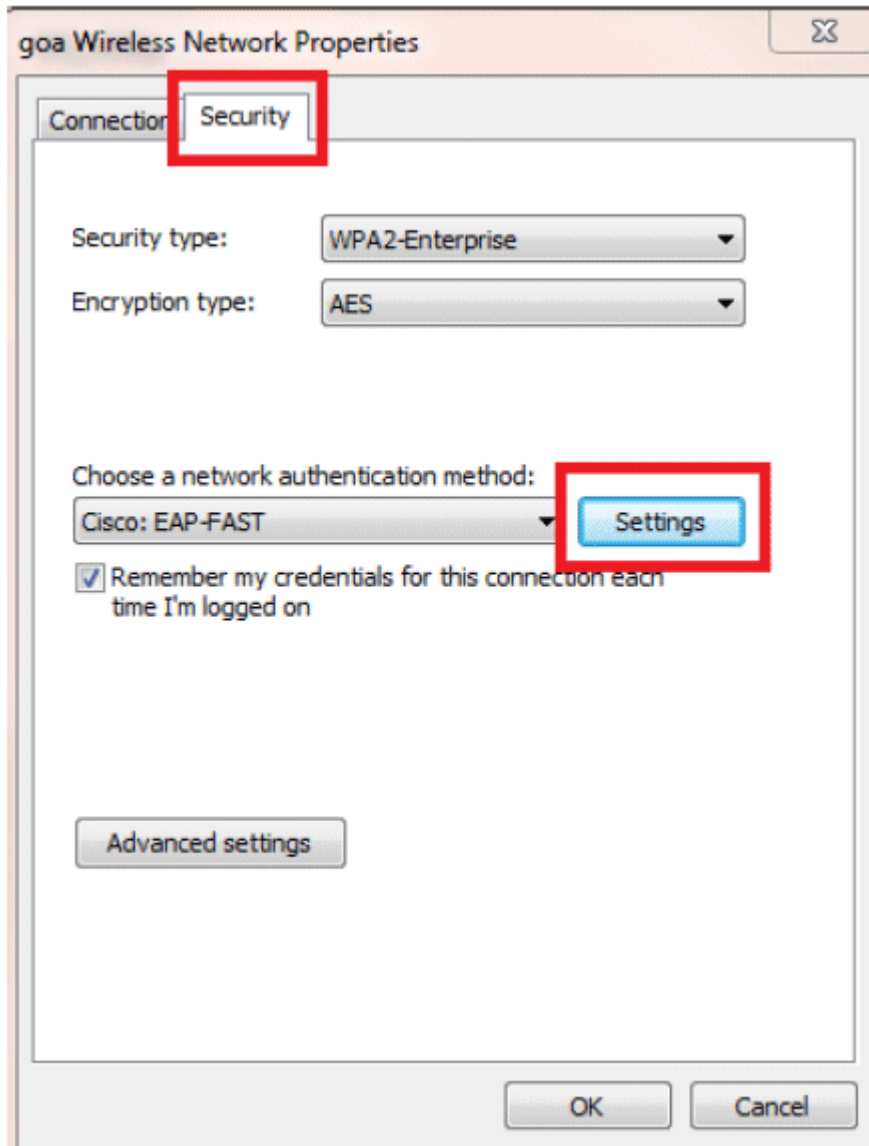


7. Asegúrese de que EAP-FAST está activado.

**Nota:** De forma predeterminada, WZC no tiene EAP-FAST como método de autenticación. Tiene que descargar la utilidad de un proveedor externo. En este ejemplo, como se trata de una tarjeta Intel,

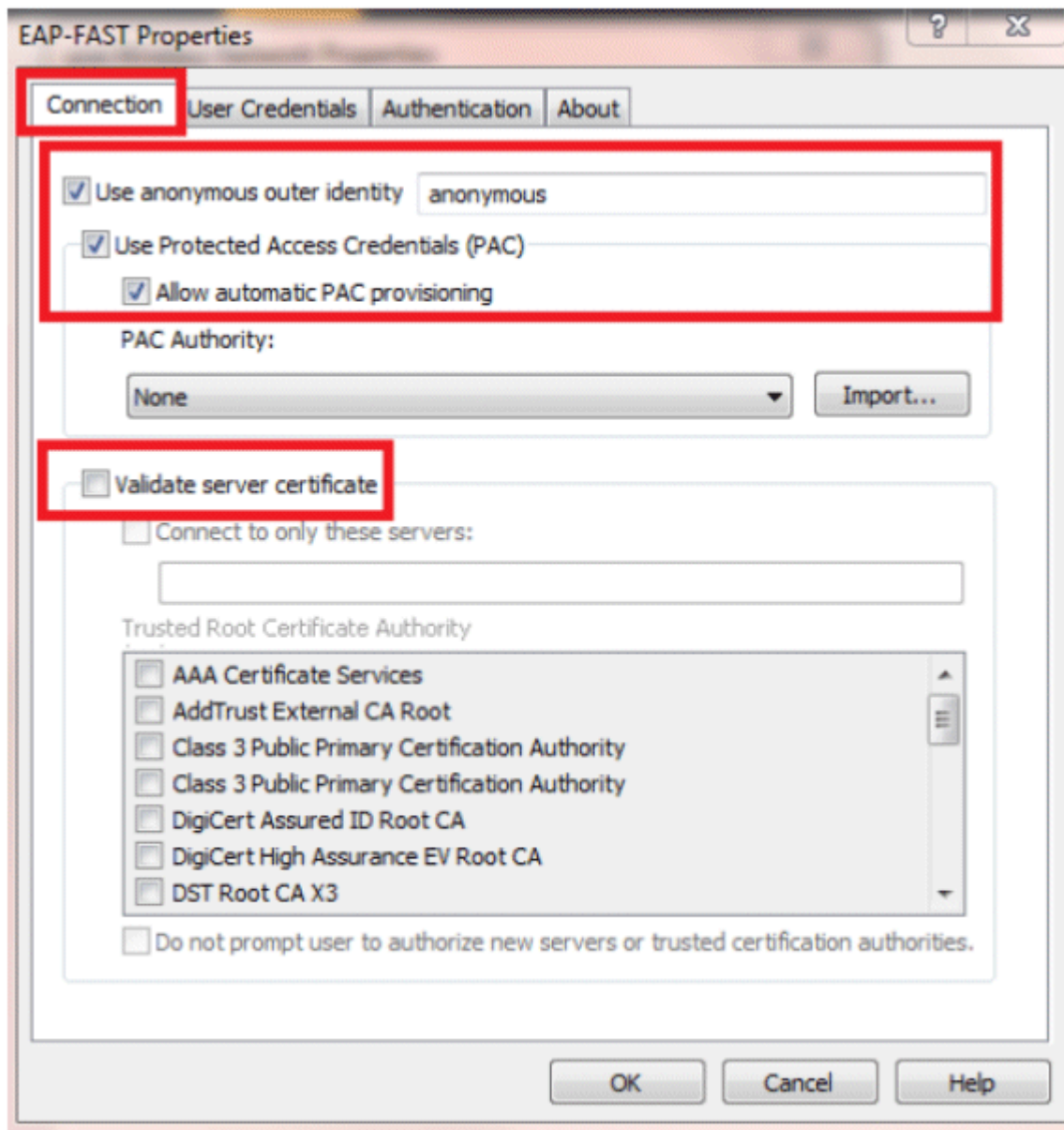
tenemos Intel PROSet instalado en el sistema.



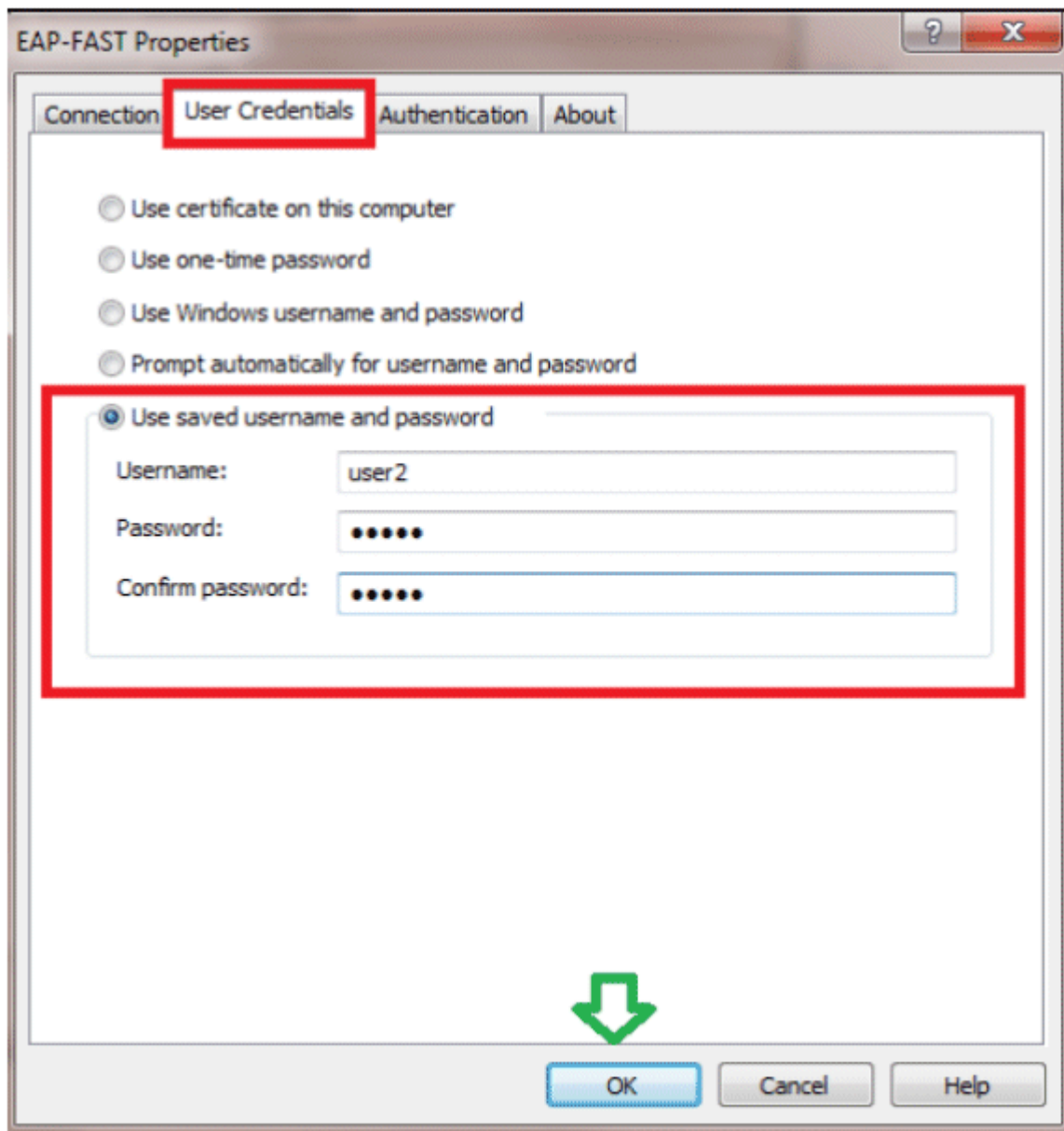


8. Habilite **Allow automatic PAC provisioning** y asegúrese de que la opción **Validate server certificate** esté desactivada.

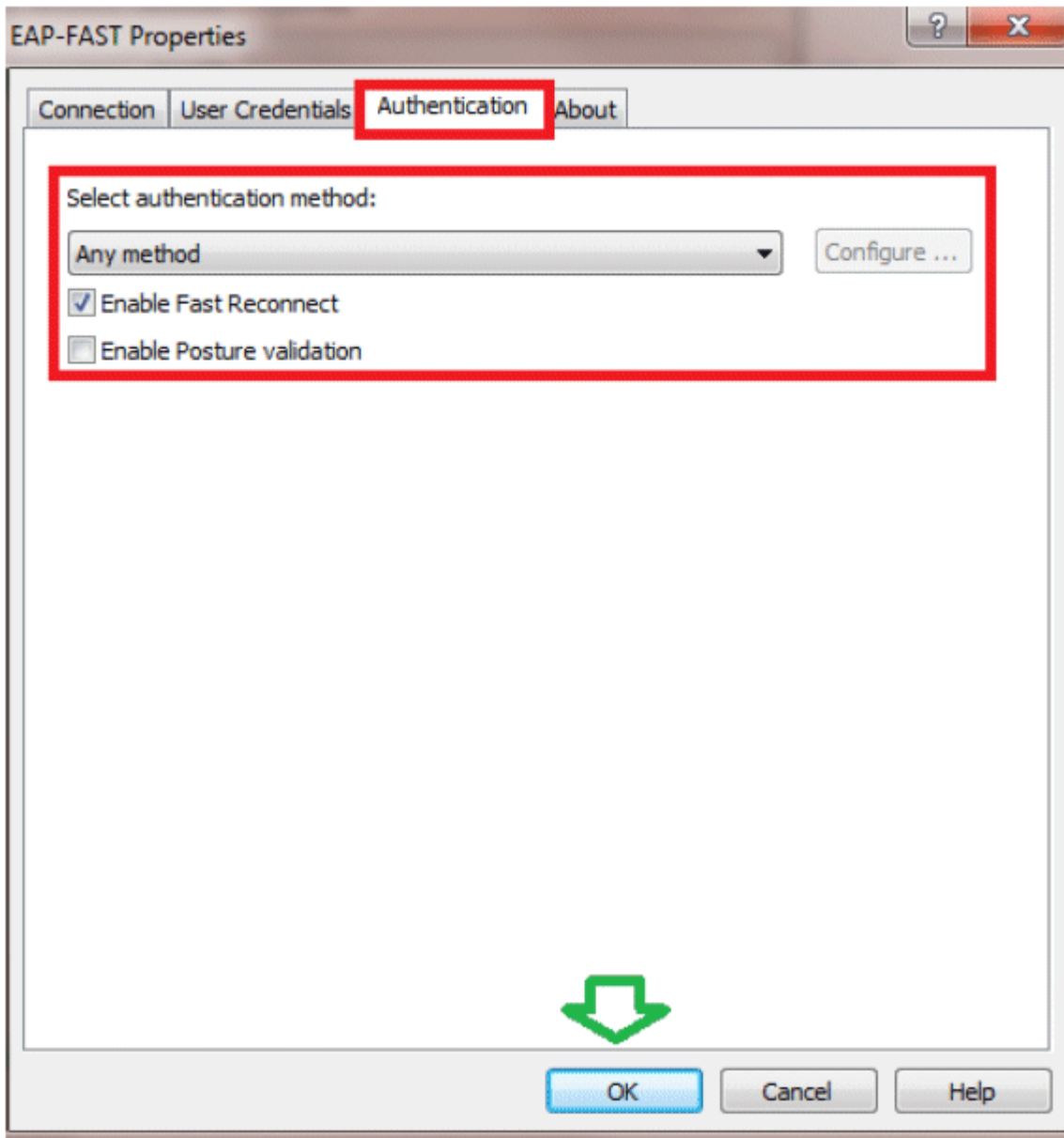




9. Haga clic en la ficha **Credenciales de usuario** e introduzca las credenciales del usuario 2. También puede utilizar sus credenciales de Windows para iniciar sesión. Sin embargo, en este ejemplo no vamos a usar eso.

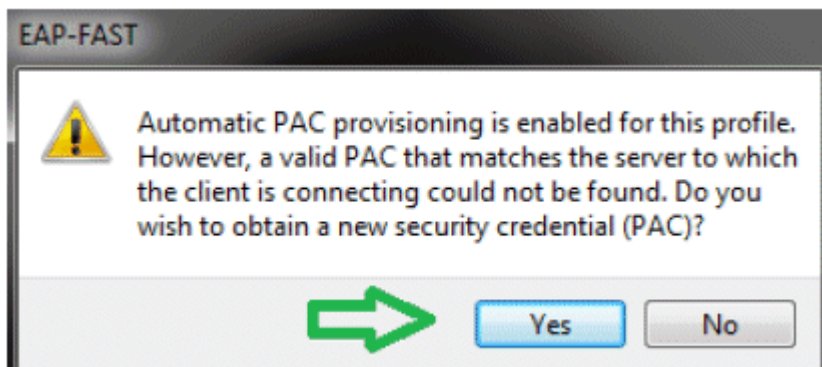


10. Click OK.



La utilidad de cliente ya está lista para conectarse para el usuario 2.

**Nota:** Cuando el usuario 2 intenta autenticarse, el servidor RADIUS enviará una PAC. Acepte la PAC para completar la autenticación.



## Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

[La herramienta Output Interpreter Tool \(clientes registrados solamente\) \(OIT\) soporta ciertos comandos show.](#) Utilice la OIT para ver un análisis del resultado del comando show.

## Comprobar usuario1 (PEAP-MSCHAPv2)

Desde la GUI del WLC, vaya a **Monitor > Clients**, y seleccione la dirección MAC.

The screenshot displays the 'Clients > Detail' page in the Cisco WLC GUI. It is divided into three main sections: Client Properties, AP Properties, and Security Information. Several fields are highlighted with red boxes.

Client Properties	
MAC Address	00:24:d7:ae:f1:98
IP Address	192.168.153.107
Client Type	Regular
User Name	user1
Port Number	13
Interface	vlan253
VLAN ID	253
CCX Version	CCXv4
E2E Version	E2Ev1
Mobility Role	Local
Mobility Peer IP Address	N/A
Policy Manager State	RUN
Management Frame Protection	No
UpTime (Sec)	12
Power Save Mode	OFF
Current TxRateSet	
Data RateSet	6.0,9.0,12.0,18.0,24.0,36.0,48.0,54.0

AP Properties	
AP Address	2c:3f:38:et:3ef0
AP Name	3502e
AP Type	802.11an
WLAN Profile	gona
Status	Associated
Association ID	1
802.11 Authentication	Open System
Reason Code	1
Status Code	0
CF Pollable	Not Implemented
CF Poll Request	Not Implemented
Short Preamble	Not Implemented
PCCC	Not Implemented
Channel Agility	Not Implemented
Re-authentication timeout	86365
Remaining Re-authentication timeout	0
WEP State	WEP Enable

Security Information	
Security Policy Completed	Yes
Policy Type	RSN (WPA2)
Encryption Cipher	CCMP (AES)
EAP Type	PEAP
SNMP NAC State	Access
Radius NAC State	RUN

## Estadísticas RADIUS WLC:

<#root>

(Cisco Controller) >

**show radius auth statistics**

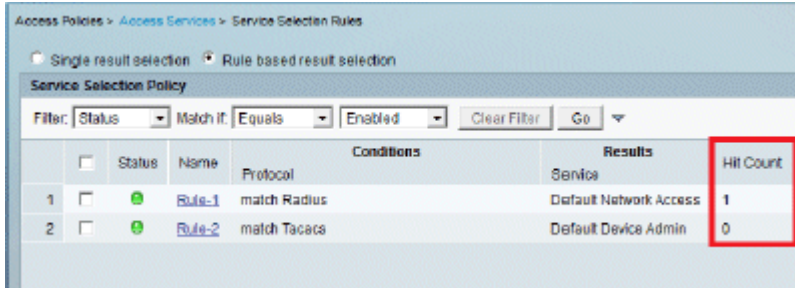
Authentication Servers:

```
Server Index..... 1
Server Address..... 192.168.150.24
Msg Round Trip Time..... 1 (msec)
First Requests..... 8
Retry Requests..... 0
Accept Responses..... 1
Reject Responses..... 0
Challenge Responses..... 7
Malformed Msgs..... 0
Bad Authenticator Msgs..... 0
Pending Requests..... 0
Timeout Requests..... 0
Unknowntype Msgs..... 0
Other Drops..... 0
```

## Registros de ACS:

1. Complete estos pasos para ver los recuentos de aciertos:

- a. Si verifica los registros dentro de los 15 minutos de la autenticación, asegúrese de actualizar el conteo de aciertos.



Access Policies > Access Services > Service Selection Rules

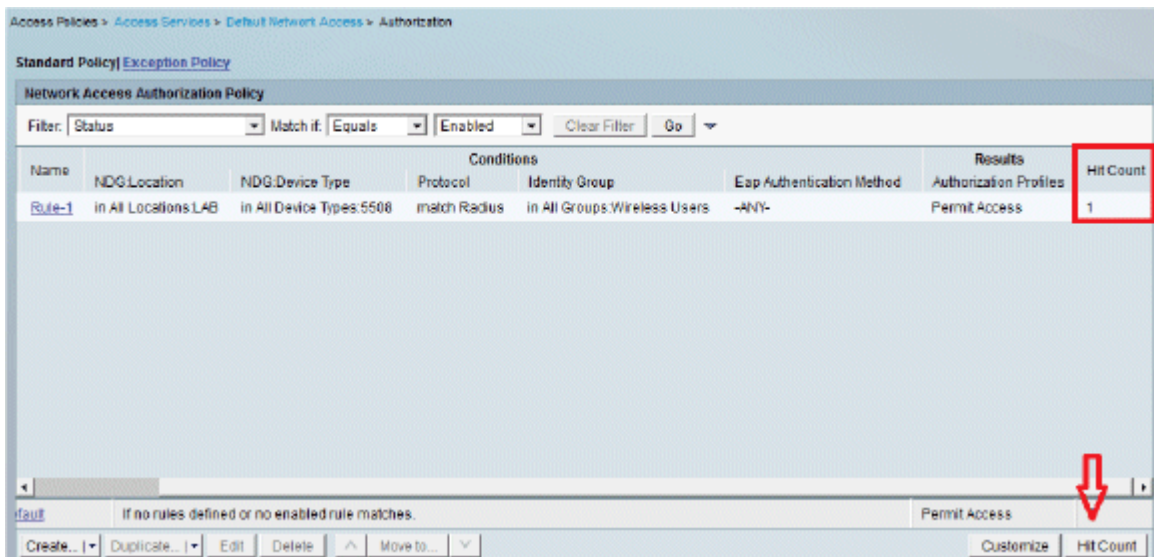
Single result selection | Rule based result selection

Service Selection Policy

Filter: Status Match if: Equals Enabled Clear Filter Go

	Status	Name	Protocol	Conditions	Results	Hit Count
1	<input type="checkbox"/>	<a href="#">Rule-1</a>	match Radius		Default Network Access	1
2	<input type="checkbox"/>	<a href="#">Rule-2</a>	match Tacacs		Default Device Admin	0

- b. Tiene una pestaña para **Recuento de visitas** en la parte inferior de la misma página.



Access Policies > Access Services > Default Network Access > Authorization

Standard Policy | Exception Policy

Network Access Authorization Policy

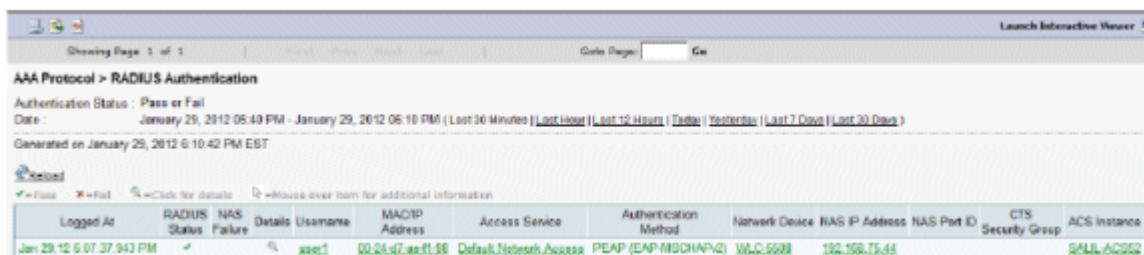
Filter: Status Match if: Equals Enabled Clear Filter Go

Name	NDG Location	NDG Device Type	Protocol	Identity Group	Eap Authentication Method	Results	Hit Count
<a href="#">Rule-1</a>	In All Locations LAB	In All Device Types:5508	match Radius	In All Groups:Wireless Users	-ANY-	Permit Access	1

If no rules defined or no enabled rule matches. Permit Access

Create... Duplicate... Edit Delete Move to... Customize Hit Count

2. Haga clic en **Supervisión e informes** y aparecerá una ventana emergente Nuevo. Vaya a **Autenticaciones - Radio - Hoy**. También puede hacer clic en **Detalles** para verificar qué regla de selección de servicio se aplicó.



Showing Page 1 of 1

AAA Protocol > RADIUS Authentication

Authentication Status: Pass or Fail

Date: January 29, 2012 05:49 PM - January 29, 2012 05:10 PM (Last 30 Minutes) | Last 1 Hour | Last 12 Hours | Today | Yesterday | Last 7 Days | Last 30 Days

Generated on January 29, 2012 5:10:42 PM EST

Logged At	RADIUS Status	NAS Failure	Details Username	MAC/IP Address	Access Service	Authentication Method	Network Device	NAS IP Address	NAS Port ID	CTS Security Group	ACS Instance
Jan 29, 12 5:07:37 943 PM	✓		asa1	00:24:67:ae:f1:88	Default Network Access	PEAP (EAP-MSCHAPv2)	WLC5508	192.168.75.44			SAULACS62

## Verificar usuario2 (EAP-FAST)

Desde la GUI del WLC, vaya a **Monitor > Clients**, y seleccione la dirección MAC.

Client Properties

MAC Address	00:24:d7:1ae1f1:98
IP Address	192.168.153.111
Client Type	Regular
User Name	user2
Port Number	13
Interface	vlan253
VLAN ID	253
CCX Version	CCXv4
E2E Version	E2Ev1
Mobility Role	Local
Mobility Peer IP Address	N/A
Policy Manager State	RUN
Management Frame Protection	No
UpTime (Sec)	29
Power Save Mode	OFF
Current TxRateSet	m15 6.0,9.0,12.0,18.0,24.0,36.0,48.0,54.
Data RateSet	0

AP Properties

AP Address	2c13f1381c113c1f0
AP Name	3502a
AP Type	802.11an
WLAN Profile	gob
Status	Associated
Association ID	1
802.11 Authentication	Open System
Reason Code	1
Status Code	0
CF Pollable	Not Implemented
CF Poll Request	Not Implemented
Short Preamble	Not Implemented
PBCC	Not Implemented
Channel Agility	Not Implemented
Re-authentication timeout	86392
Remaining Re-authentication timeout	0
WEP State	WEP Enable

Security Information

Security Policy Completed	Yes
Policy Type	RSN (WPA2)
Encryption Cipher	CCMP (AES)
EAP Type	EAP-FAST
SNMP NAC State	Access
Radius NAC State	RUN

Registros de ACS:

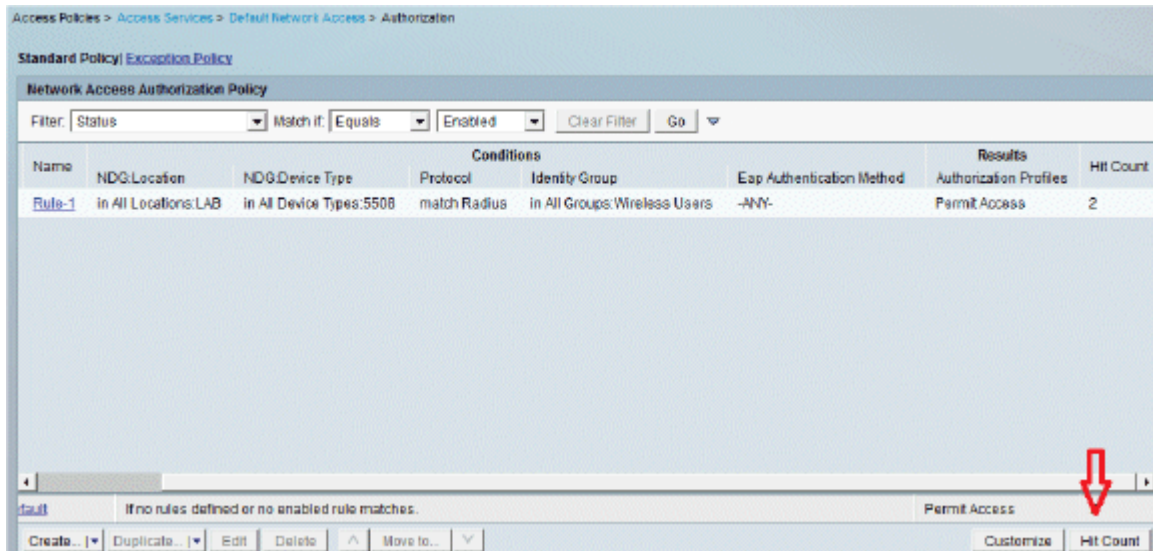
1. Complete estos pasos para ver los recuentos de aciertos:

a. Si verifica los registros dentro de los 15 minutos de la autenticación, asegúrese de actualizar el conteo de HIT.

	Status	Name	Protocol	Conditions	Results	Hit Count
1	✔	Rule-1	match Radius		Default Network Access	3
2	✔	Rule-2	match Tacacs		Default Device Admin	0

b. Tiene una pestaña para **Recuento de visitas** en la parte inferior de la misma página.





- Haga clic en **Supervisión e informes** y aparecerá una ventana emergente Nuevo. Vaya a **Autenticaciones - Radio - Hoy**. También puede hacer clic en **Detalles** para verificar qué regla de selección de servicio se aplicó.

AAA Protocol > RADIUS Authentication

Authentication Status: Pass or Fail

Date: January 29, 2012 01:53 PM - January 29, 2012 06:23 PM (Last 30 Minutes | Last Hour | Last 12 Hours | Today | Yesterday | Last 7 Days | Last 30 Days)

Generated on January 29, 2012 6:23:17 PM EST

Logged At	RADIUS Status	NAS	Details	Username	MAC/IP Address	Access Service	Authentication Method	Network Device	NAS IP Address	NAS Port ID	CTS Security Group	ACS Ins
Jan 29 12 5 19 27 270 PM	✓	Failure		user2	80:24:d7:ae:f1:58	Default Network Access	EAP-FAST (EAP-MSCHAPv2)	WLC-5588	192.168.75.44			SALLA
Jan 29 12 5 07 37 941 PM	✓			user1	80:24:d7:ae:f1:58	Default Network Access	PEAP (EAP-MSCHAPv2)	WLC-5588	192.168.75.44			SALLA

## Troubleshoot

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

### Comandos para resolución de problemas

[La herramienta Output Interpreter Tool \(clientes registrados solamente\) \(OIT\) soporta ciertos comandos show.](#) Utilice la OIT para ver un análisis del resultado del comando show.

**Nota:** Consulte [Información Importante sobre Comandos Debug](#) antes de utilizar los comandos **debug**.

- Si experimenta cualquier problema, ejecute estos comandos en el WLC:
  - debug client** <mac add of the client>
  - debug aaa all enable**
  - show client detail** <mac addr> : **verifique el estado del administrador de políticas.**
  - show radius auth statistics** - Verifique el motivo de la falla.
  - debug disable-all** - Desactiva los debugs.
  - clear stats radius auth all** - Borrar estadísticas de radio en el WLC.

2. Verifique los registros en el ACS y anote el motivo de la falla.

## **Información Relacionada**

- [Soporte Técnico y Documentación - Cisco Systems](#)

## 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).