

# Configuración de un WLC y un ACS para Autenticar Usuarios de Administración

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Configuración de WLC](#)

[Configure el WLC para que acepte la administración a través del servidor Cisco Secure ACS](#)

[Configuración de Cisco Secure ACS](#)

[Agregue el WLC como un cliente AAA al servidor RADIUS](#)

[Configuración de Usuarios y sus Atributos IETF RADIUS Apropriados](#)

[Configuración de un usuario con acceso de lectura y escritura](#)

[Configuración de un usuario con acceso de sólo lectura](#)

[Administre el WLC localmente así como a través del servidor RADIUS](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

---

## Introducción

Este documento describe cómo configurar un WLC y un Cisco Secure ACS para que el servidor AAA pueda autenticar a los usuarios de administración en el controlador.

## Prerequisites

### Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento de cómo configurar los parámetros básicos en WLCs
- Conocimiento de cómo configurar un servidor RADIUS como Cisco Secure ACS

### Componentes Utilizados

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

- Cisco 4400 Wireless LAN Controller que ejecuta la versión 7.0.216.0
- Cisco Secure ACS que ejecuta la versión de software 4.1 y se utiliza como servidor RADIUS en esta configuración.

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.

## Convenciones

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

## Antecedentes

Este documento explica cómo configurar un Wireless LAN Controller (WLC) y un Access Control Server (Cisco Secure ACS) para que el servidor de Autenticación, Autorización y Contabilización (AAA) pueda autenticar a los usuarios de administración en el controlador. El documento también explica cómo diferentes usuarios de administración pueden recibir diferentes privilegios con atributos específicos del proveedor (VSA) devueltos desde el servidor Cisco Secure ACS RADIUS.

## Configurar

En esta sección, se le presenta la información sobre cómo configurar el WLC y el ACS para el propósito descrito en este documento.

### Diagrama de la red

En este documento, se utiliza esta configuración de red:

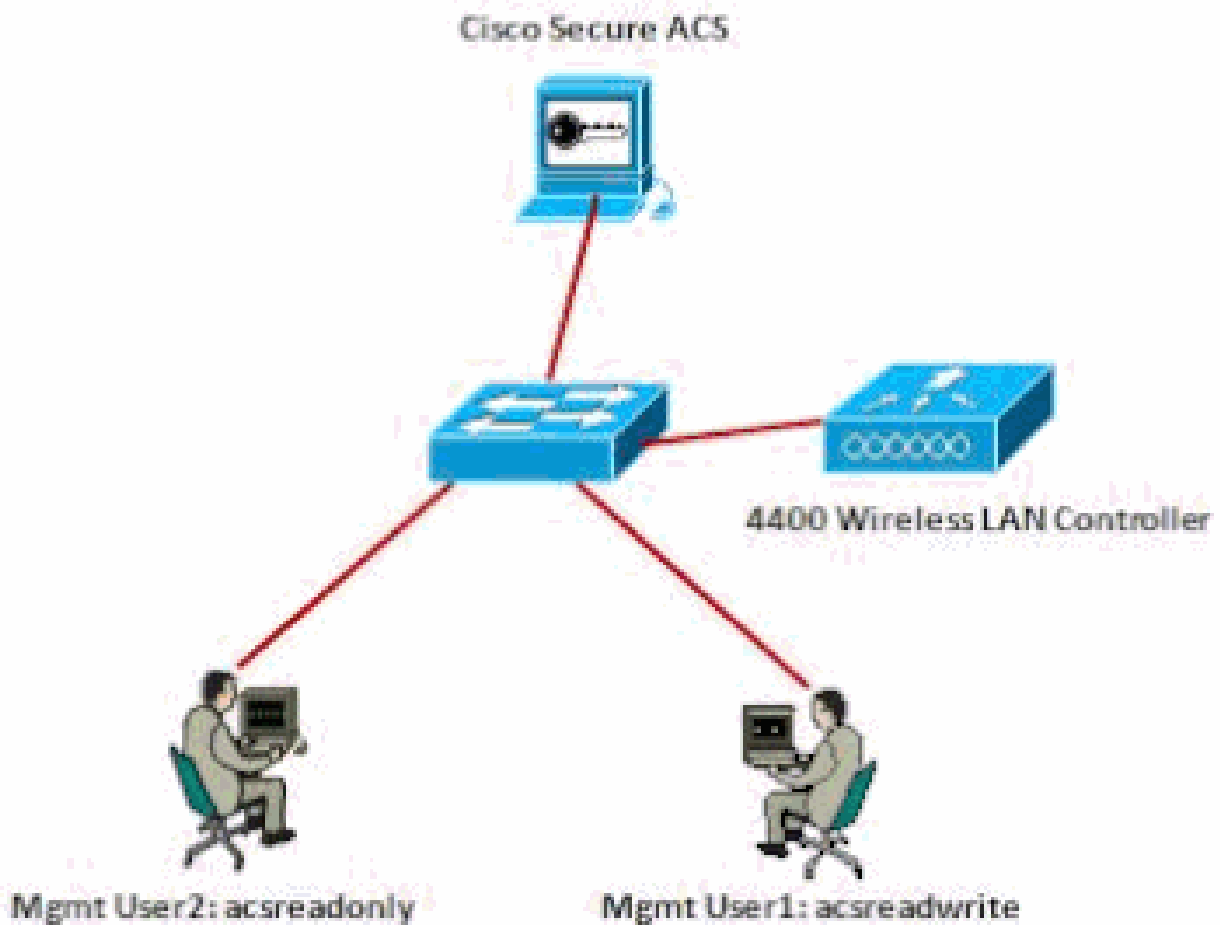


Diagrama de la red

Este ejemplo de configuración utiliza estos parámetros:

- Dirección IP de Cisco Secure ACS —172.16.1.1/255.255.0.0
- Dirección IP de la interfaz de administración del controlador: 172.16.1.30/255.255.0.0
- Clave secreta compartida que se utiliza en el punto de acceso (AP) y el servidor RADIUS: asdf1234
- Estas son las credenciales de los dos usuarios que este ejemplo configura en el ACS:
  1. Nombre de usuario: acsreadwrite  
Contraseña - acsreadwrite
  2. Nombre de usuario: acsreadonly  
Contraseña: acsreadonly

Debe configurar el WLC y Cisco Secure Cisco Secure ACS para:

- Cualquier usuario que inicia sesión en el WLC con el nombre de usuario y la contraseña asacsreadwrite se le da acceso administrativo completo al WLC.
- Cualquier usuario que inicia sesión en el WLC con el nombre de usuario y la contraseña como acsreadonly se le da acceso de solo lectura al WLC.

## Configuraciones

En este documento, se utilizan estas configuraciones:

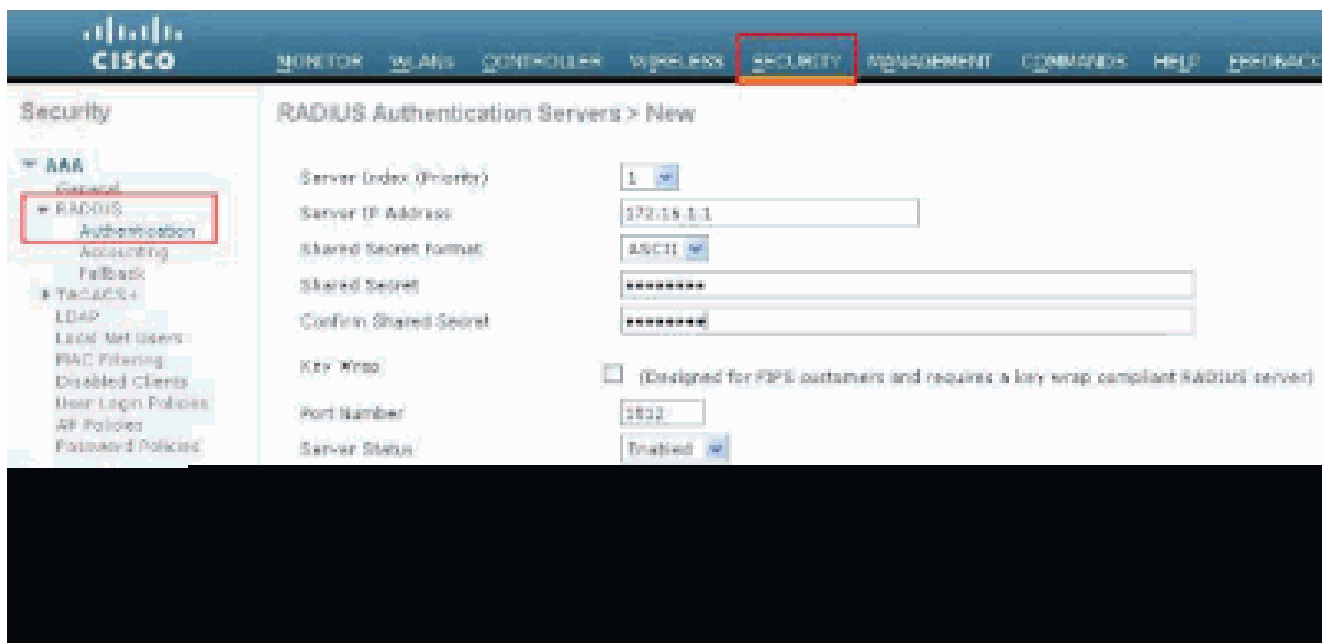
- [Configuración de WLC](#)
- [Configuración de Cisco Secure ACS](#)

## Configuración de WLC

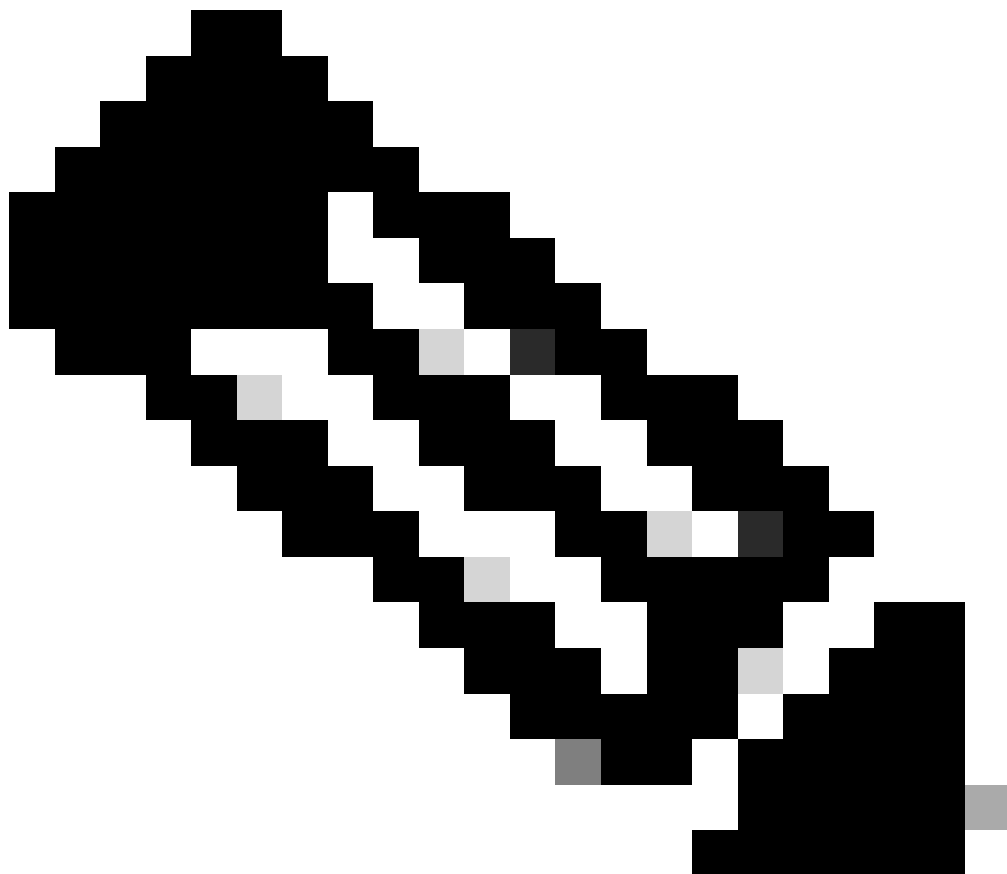
Configure el WLC para que acepte la administración a través del servidor Cisco Secure ACS

Complete estos pasos para configurar el WLC de modo que se comuniquen con el servidor RADIUS:

1. Desde la GUI del WLC, haga clic en Seguridad. En el menú de la izquierda, haga clic en RADIUS > Authentication. Aparece la página Servidores de autenticación RADIUS. Para agregar un nuevo servidor RADIUS, haga clic en Nuevo. En la página RADIUS Authentication Servers > New, ingrese los parámetros específicos para el servidor RADIUS. Aquí está un ejemplo.

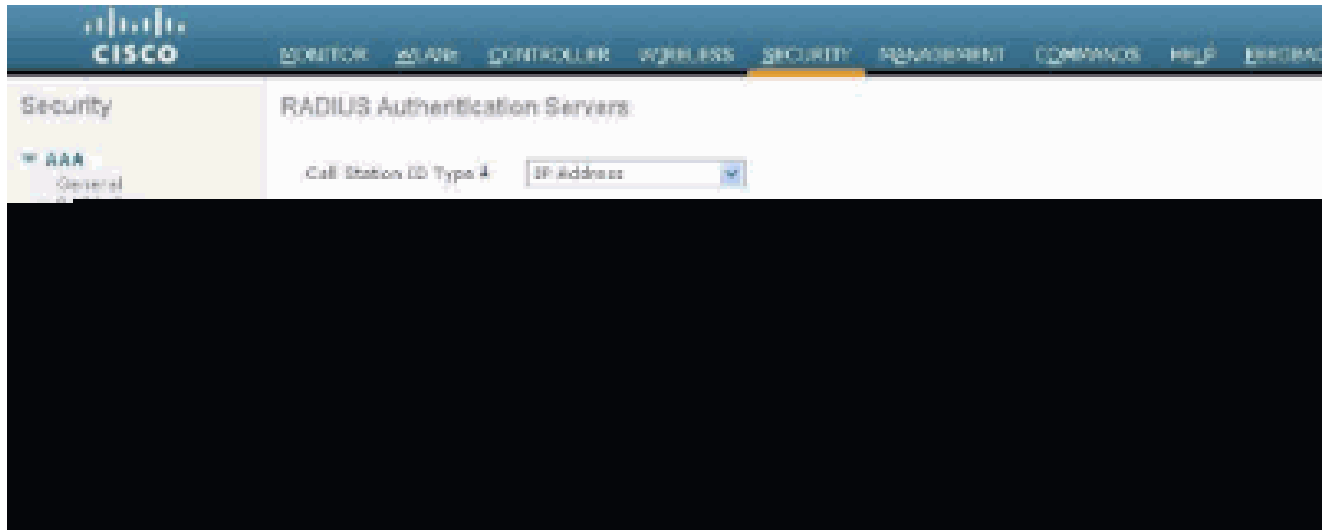


2. Verifique el botón de radio Management para permitir que el servidor RADIUS autentique a los usuarios que inician sesión en el WLC.



Nota: Asegúrese de que el secreto compartido configurado en esta página coincide con el secreto compartido configurado en el servidor RADIUS. Solo entonces puede el WLC comunicarse con el servidor RADIUS.

- 
3. Verifique si el WLC está configurado para ser administrado por Cisco Secure ACS. Para hacer esto, haga clic en Seguridad de la GUI del WLC. La ventana resultante de la GUI aparece de forma similar a este ejemplo.



Puede ver que la casilla de verificación Administración está habilitada para el servidor RADIUS 172.16.1.1. Esto ilustra que ACS está permitido autenticar a los usuarios de administración en el WLC.

## Configuración de Cisco Secure ACS

Complete los pasos de estas secciones para configurar el ACS:

1. [Agregue el WLC como un cliente AAA al servidor RADIUS](#)
2. [Configuración de Usuarios y sus Atributos IETF RADIUS Apropriados](#)
3. [Configuración de un usuario con acceso de lectura y escritura](#)
4. [Configuración de un usuario con acceso de sólo lectura](#)

Agregue el WLC como un cliente AAA al servidor RADIUS

Complete estos pasos para agregar el WLC como un cliente AAA en Cisco Secure ACS:

1. Desde la GUI de ACS, haga clic en Network Configuration.
2. En los clientes AAA, haga clic en Add Entry (Agregar entrada).
3. En la ventana Add AAA Client, ingrese el nombre de host WLC, la dirección IP del WLC y una clave secreta compartida.

En este ejemplo, estas son las configuraciones:

- AAA Client Hostname es WLC-4400.
- 172.16.1.30/16 es la dirección IP del cliente AAA, que, en este caso es el WLC.
- La clave secreta compartida es asdf1234.

**Network Configuration**

### Add AAA Client

AAA Client Hostname:

AAA Client IP Address:

Shared Secret:

---

**RADIUS Key Wrap**

Key Encryption Key:

Message Authenticator Code Key:

Key Input Format:  ASCII  Hexadecimal

---

Authenticate Using:

Single Connect TACACS+ AAA Client (Record stop in accounting on failure)

Log Update/Watchdog Packets from this AAA Client

Log RADIUS Tunneling Packets from this AAA Client

Replace RADIUS Port info with Username from this AAA Client

Match Framed-IP-Address with user IP address for accounting packets from this AAA Client

Ventana Agregar Cliente AAA

Esta clave secreta compartida debe ser la misma que la clave secreta compartida que configure en el WLC.

4. En el menú desplegable Authenticate Using, elija RADIUS (Cisco Airespace).
5. Haga clic en Submit + Restart para guardar la configuración.

#### Configuración de Usuarios y sus Atributos IETF RADIUS Apropriados

Para autenticar a un usuario a través de un servidor RADIUS, para la administración y el inicio de sesión del controlador, debe agregar al usuario a la base de datos RADIUS con el atributo IETF RADIUS Service-Typeset al valor apropiado basado en los privilegios de usuario.

- Para establecer los privilegios de lectura y escritura para el usuario, establezca el atributo Service-Type en Administrative.
- Para establecer privilegios de sólo lectura para el usuario, establezca el atributo Service-TypeAttribute en NAS-Prompt.

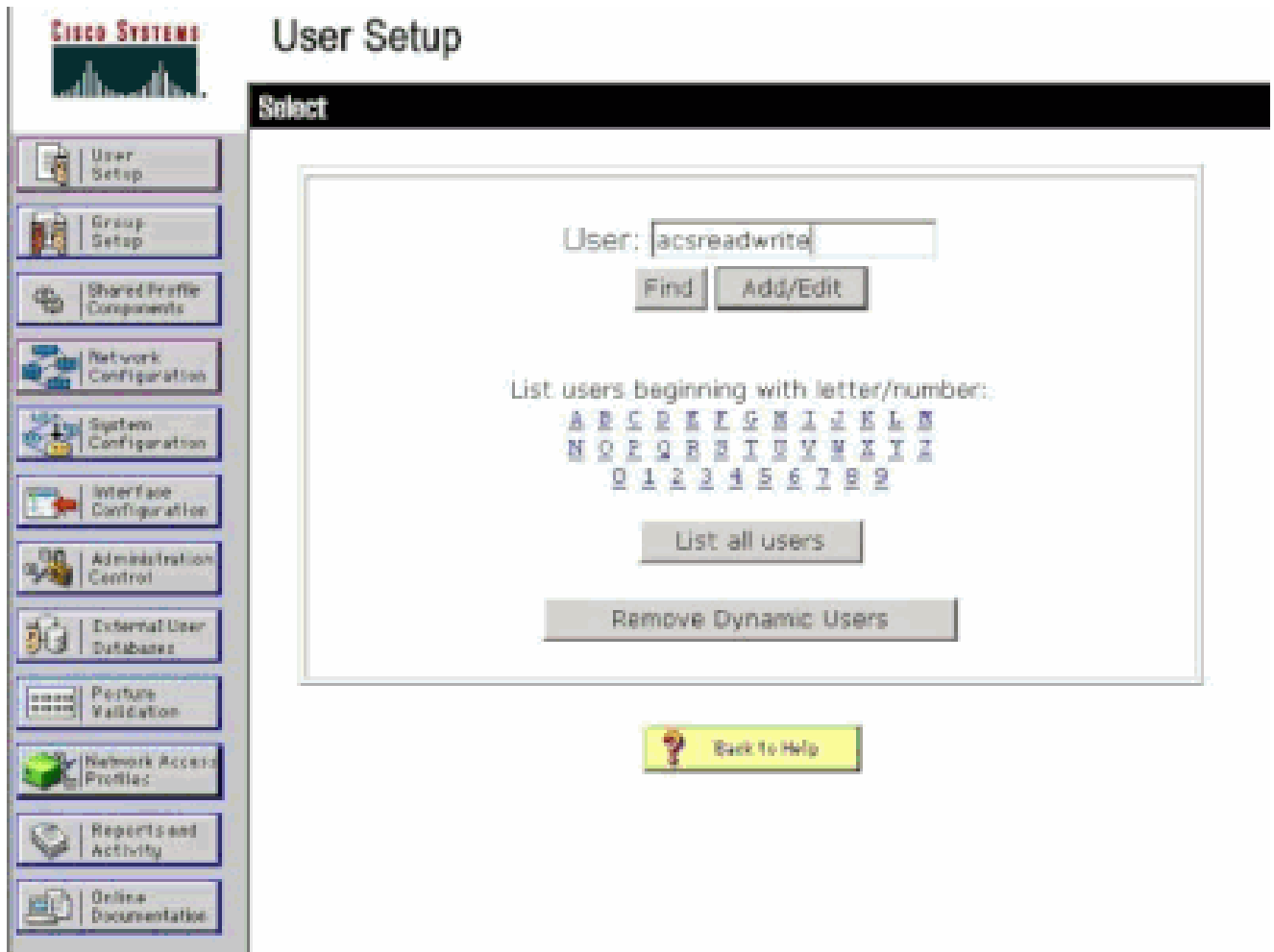
#### Configuración de un usuario con acceso de lectura y escritura

El primer ejemplo muestra la configuración de un usuario con acceso completo al WLC. Cuando este usuario intenta iniciar sesión en el controlador, el servidor RADIUS autentica y proporciona a este usuario acceso administrativo completo.

En este ejemplo, el nombre de usuario y la contraseña son acsreadwrite.

Complete estos pasos en Cisco Secure ACS.

1. Desde la GUI de ACS, haga clic en User Setup.
2. Escriba el nombre de usuario que se agregará al ACS como muestra esta ventana de ejemplo.



Ventana Configuración de usuario

3. Haga clic en Add/Edit para ir a la página User Edit.
4. En la página User Edit (Edición de usuario), proporcione los detalles Real Name, Description y Password de este usuario.
5. Desplácese hacia abajo hasta la configuración IETF RADIUS Attributes y marque Service-Type Attribute.
6. Dado que, en este ejemplo, el usuario acsreadwrite necesita tener acceso completo, elija Administrative en el menú desplegable Service-Type y haga clic en Submit.

Esto asegura que este usuario particular tenga acceso de lectura-escritura al WLC.



Configuración de atributos RADIUS ETF

A veces, este atributo Service-Type no está visible en la configuración del usuario. En tales casos, complete estos pasos para que sea visible.

1. Desde la GUI de ACS, navegue hasta Interface Configuration > RADIUS (IETF) para habilitar los atributos IETF en la ventana User Configuration.

Accederá a la página RADIUS (IETF) Settings (Parámetros de RADIUS).

2. En la página Configuración de RADIUS (IETF), puede habilitar el atributo IETF que debe estar visible en la configuración de usuario o grupo. Para esta configuración, verifique Service-Type para la columna User y haga clic en Submit. Esta ventana muestra un ejemplo.

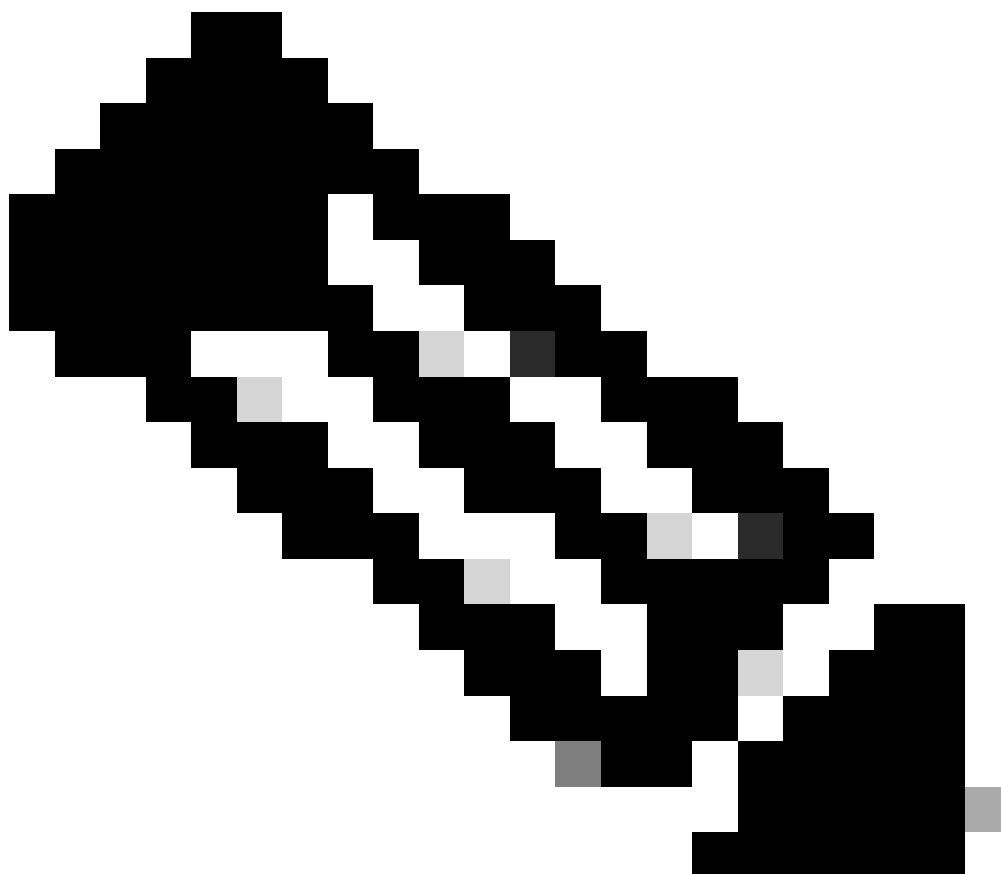


## Interface Configuration

### RADIUS (IETF)



User	Group
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> [006] Service-Type
<input type="checkbox"/>	<input checked="" type="checkbox"/> [007] Framed-Protocol
<input type="checkbox"/>	<input checked="" type="checkbox"/> [009] Framed-IP-Netmask
<input type="checkbox"/>	<input checked="" type="checkbox"/> [010] Framed-Routing
<input type="checkbox"/>	<input checked="" type="checkbox"/> [011] Filter-Id
<input type="checkbox"/>	<input checked="" type="checkbox"/> [012] Framed-MTU
<input type="checkbox"/>	<input checked="" type="checkbox"/> [013] Framed-Compression
<input type="checkbox"/>	<input checked="" type="checkbox"/> [014] Login-IP-Host
<input type="checkbox"/>	<input checked="" type="checkbox"/> [015] Login-Service
<input type="checkbox"/>	<input checked="" type="checkbox"/> [016] Login-TCP-Port
<input type="checkbox"/>	<input checked="" type="checkbox"/> [018] Reply-Message
<input type="checkbox"/>	<input checked="" type="checkbox"/> [020] Callback-Id
<input type="checkbox"/>	<input checked="" type="checkbox"/> [022] Framed-Route
<input type="checkbox"/>	<input checked="" type="checkbox"/> [023] Framed-IPX-Network
<input type="checkbox"/>	<input checked="" type="checkbox"/> [024] State
<input type="checkbox"/>	<input checked="" type="checkbox"/> [025] Class
<input type="checkbox"/>	<input checked="" type="checkbox"/> [027] Session-Timeout
<input type="checkbox"/>	<input checked="" type="checkbox"/> [028] Idle-Timeout



Nota: Este ejemplo especifica la autenticación por usuario. También puede realizar la autenticación basándose en el grupo al que pertenece un usuario determinado. En estos casos, active la casilla de verificación Grupo para que este atributo esté visible en Configuración del grupo. Además, si la autenticación se realiza por grupos, debe asignar usuarios a un grupo determinado y configurar los atributos IETF de configuración de grupo para proporcionar privilegios de acceso a los usuarios de ese grupo. Consulte Administración de grupos para obtener información detallada sobre cómo configurar y administrar grupos.

---

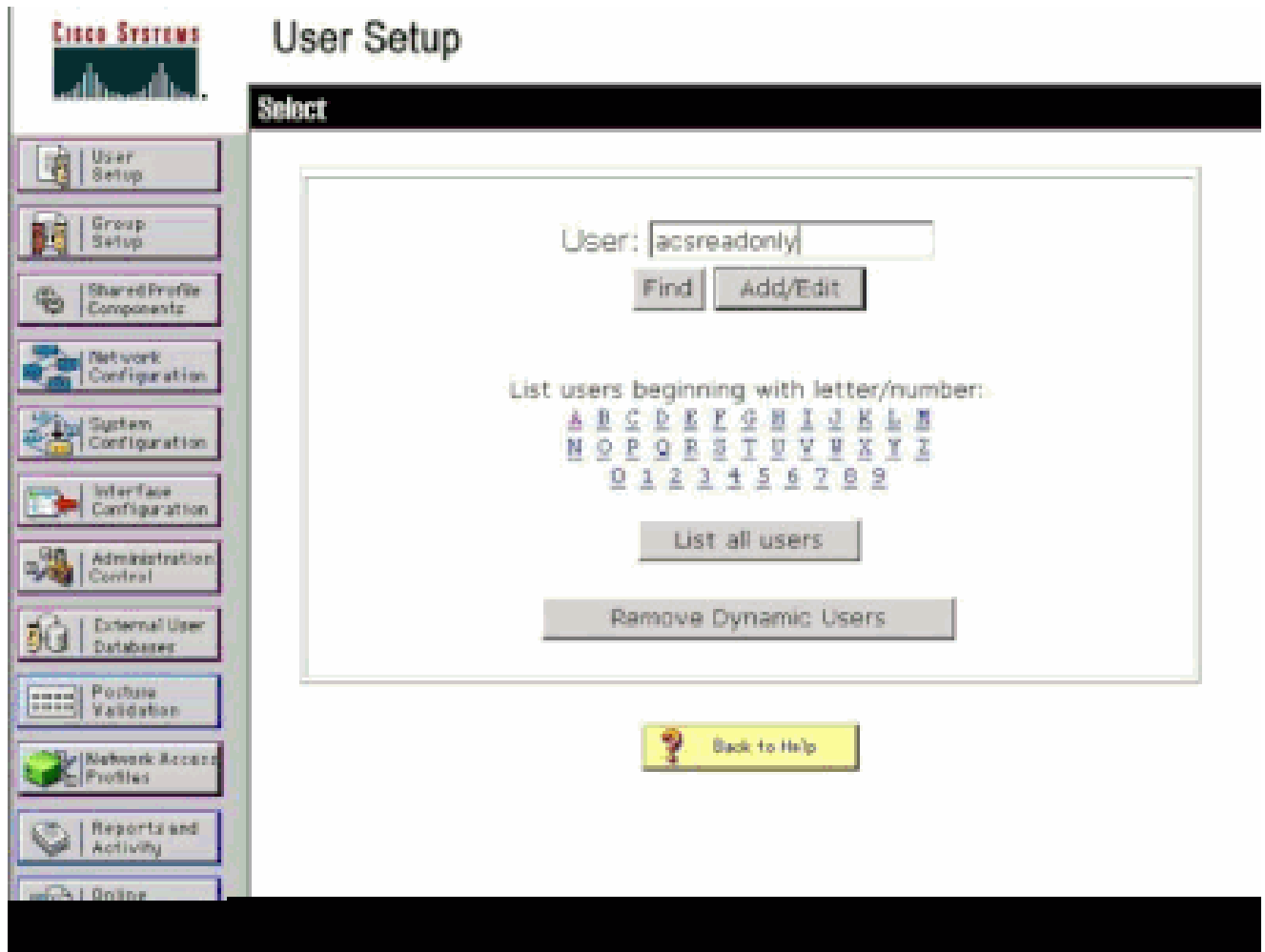
### Configuración de un usuario con acceso de sólo lectura

Este ejemplo muestra la configuración de un usuario con acceso de solo lectura al WLC. Cuando este usuario intenta iniciar sesión en el controlador, el servidor RADIUS autentica y proporciona a este usuario acceso de sólo lectura.

En este ejemplo, el nombre de usuario y la contraseña son acsreadonly.


Complete estos pasos en Cisco Secure ACS:

1. Desde la GUI de ACS, haga clic en User Setup.
2. Escriba el nombre de usuario que desea agregar al ACS y haga clic en Add/Edit para ir a la página User Edit .



Agregar un nombre de usuario

3. Proporcione el nombre real, la descripción y la contraseña de este usuario. Esta ventana muestra un ejemplo.



# User Setup

**Edit**

## User: acsreadonly (New User)

Account Disabled

### Supplementary User Info

Real Name:

Description:

---

### User Setup

Password Authentication:

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password:

Confirm Password:

Separate (CHAP/MS-CHAP/ARAP)

Password:

Confirm Password:

When a token server is used for authentication, supplying a

Proporcione el nombre real, la descripción y la contraseña del usuario agregado

4. Desplácese hacia abajo hasta la configuración IETF RADIUS Attributes y marque Service-Type Attribute.
5. Dado que, en este ejemplo, el usuario acsreadonly necesita tener acceso de solo lectura, elija NAS Prompt en el menú desplegable Service-Type y haga clic en Submit.

Esto asegura que este usuario particular tenga acceso de solo lectura al WLC.

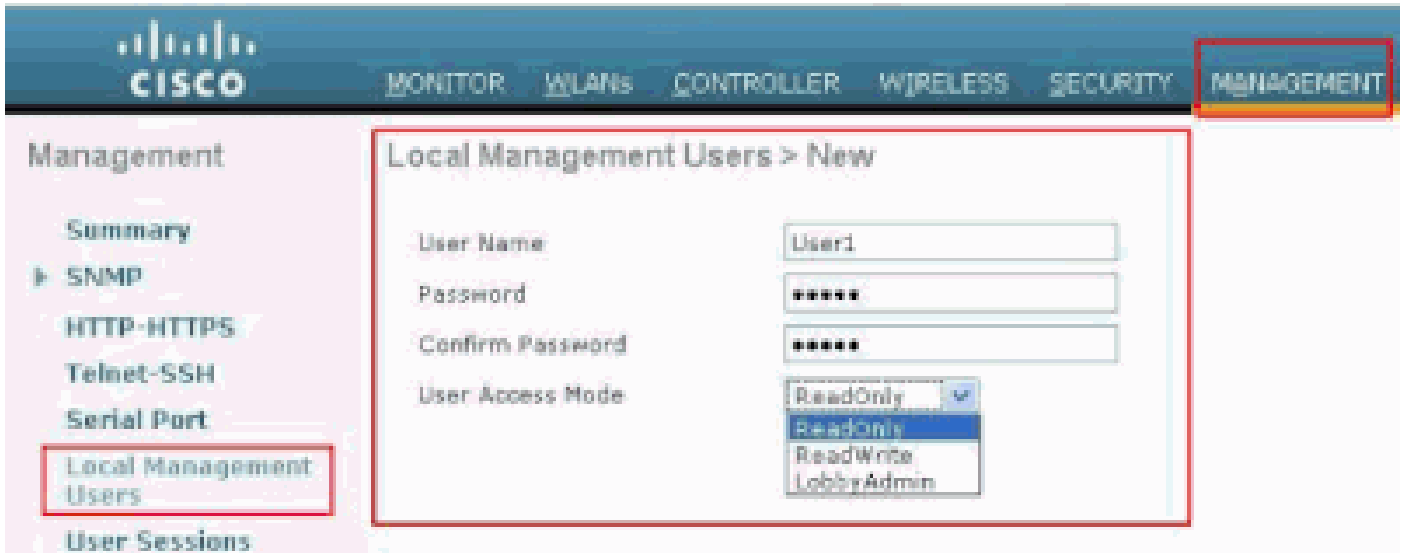
The screenshot shows the Cisco Systems User Setup interface. On the left is a navigation menu with options like User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Profile Validation, Network Access Profiles, Reports and Activity, and Online Documentation. The main content area is divided into two sections:

- Account Disable:** Contains radio buttons for 'Never', 'Disable account if:', and 'Failed attempts exceed:'. The 'Failed attempts exceed:' option has a text input field with the value '5'. Below it, it shows 'Failed attempts since last successful login: 0' and a checkbox for 'Reset current failed attempts count on submit:'. A date selector shows 'Sep 22 2011'.
- IETF RADIUS Attributes:** Contains a checked checkbox for '[006] Service-Type' and a dropdown menu. The dropdown menu is open, showing a list of service types: 'Authenticate only', 'Authenticate only', 'NAS Prompt', 'Outbound', 'Callback NAS Prompt', 'Administrative', 'Callback Administrative', 'Callback login', and 'Framed'. The 'NAS Prompt' option is highlighted with a blue background and is enclosed in a red rectangular box.

Comprobar atributo de tipo de servicio

Administre el WLC localmente así como a través del servidor RADIUS

También puede configurar los usuarios de administración localmente en el WLC. Esto se puede hacer desde la GUI del controlador, bajo Management > Local Management Users.



Configure los usuarios de administración localmente en el WLC

Suponga que el WLC se configura con los usuarios de administración tanto localmente como en el servidor RADIUS con la casilla de verificación Management habilitada. En tal escenario, de forma predeterminada, cuando un usuario intenta iniciar sesión en el WLC, el WLC se comporta de esta manera:

1. El WLC primero mira a los usuarios de administración local definidos para validar el usuario. Si el usuario existe en su lista local, permite la autenticación para este usuario. Si este usuario no aparece localmente, busca en el servidor RADIUS.
2. Si el mismo usuario existe tanto localmente como en el servidor RADIUS, pero con privilegios de acceso diferentes, el WLC autentica al usuario con los privilegios especificados localmente. En otras palabras, la configuración local en el WLC siempre tiene prioridad cuando se compara con el servidor RADIUS.

El orden de la autenticación para los usuarios de administración se puede cambiar en el WLC. Para hacer esto, desde la página Seguridad en el WLC, haga clic en Orden de prioridad > Usuario de administración. En esta página puede especificar el orden de autenticación. Aquí está un ejemplo.

CISCO

MONITOR WLAN CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Security: Priority Order > Management User

AAA

- General
- RADIUS
  - Authentication
  - Accounting
  - Fallback
- TACACS+
  - LDAP
  - Local Net Users
  - MAC Filtering
  - Disabled Clients
  - User Logs Policies
  - AP Policies
  - Password Policies
- Local ERP
- Priority Order
  - Management User
- Certificate
- Access Control Lists

**Authentication:**

Not Used      Order Used for Authentication

TACACS+      LOCAL RADIUS

Up  
Down

*If LOCAL is selected as second priority, then user will be authenticated against LOCAL only if first priority is unreachable.*

Orden de prioridad > Selección de usuario de gestión





Nota: Si se selecciona LOCAL como segunda prioridad, el usuario se autentica con este método sólo si el método definido como la primera prioridad (RADIUS/ TACACS) es inalcanzable.

---

## Verificación

Para verificar si su configuración funciona correctamente, acceda al WLC a través del modo CLI o GUI (HTTP/HTTPS). Cuando aparezca el mensaje de inicio de sesión, escriba el nombre de usuario y la contraseña tal como se configuraron en Cisco Secure ACS.

Si usted tiene las configuraciones correctas, usted está autenticado con éxito en el WLC.

También puede asegurarse de que al usuario autenticado se le proporcionen restricciones de acceso según lo especificado por ACS. Para hacerlo, acceda a la GUI del WLC a través de HTTP/HTTPS (asegúrese de que el WLC esté configurado para permitir HTTP/HTTPS).

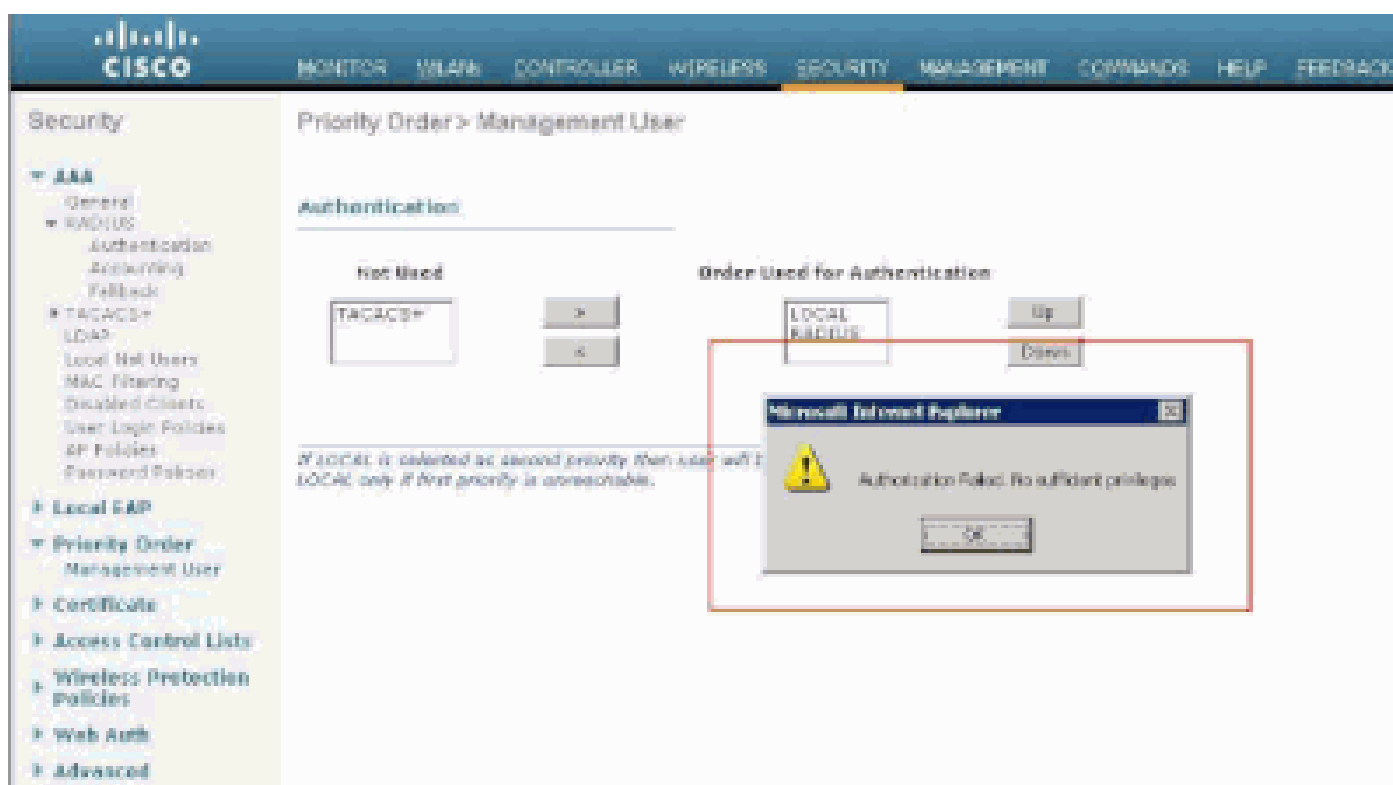
Un usuario con acceso de lectura-escritura establecido en el ACS tiene varios privilegios

configurables en el WLC. Por ejemplo, un usuario de lectura-escritura tiene el privilegio de crear una nueva WLAN bajo la página WLANs del WLC. Esta ventana muestra un ejemplo.



Privilegios Configurables en el WLC

Cuando un usuario con privilegios de sólo lectura intenta alterar la configuración en el controlador, el usuario ve este mensaje.



No se puede modificar el controlador con acceso de sólo lectura

Estas restricciones de acceso también se pueden verificar a través de la CLI del WLC. En este resultado, se muestra un ejemplo.

```
<#root>
```

```
(Cisco Controller) >
```

```
?
```

- debug           Manages system debug options.
- help            Help
- linktest        Perform a link test to a specified MAC address.

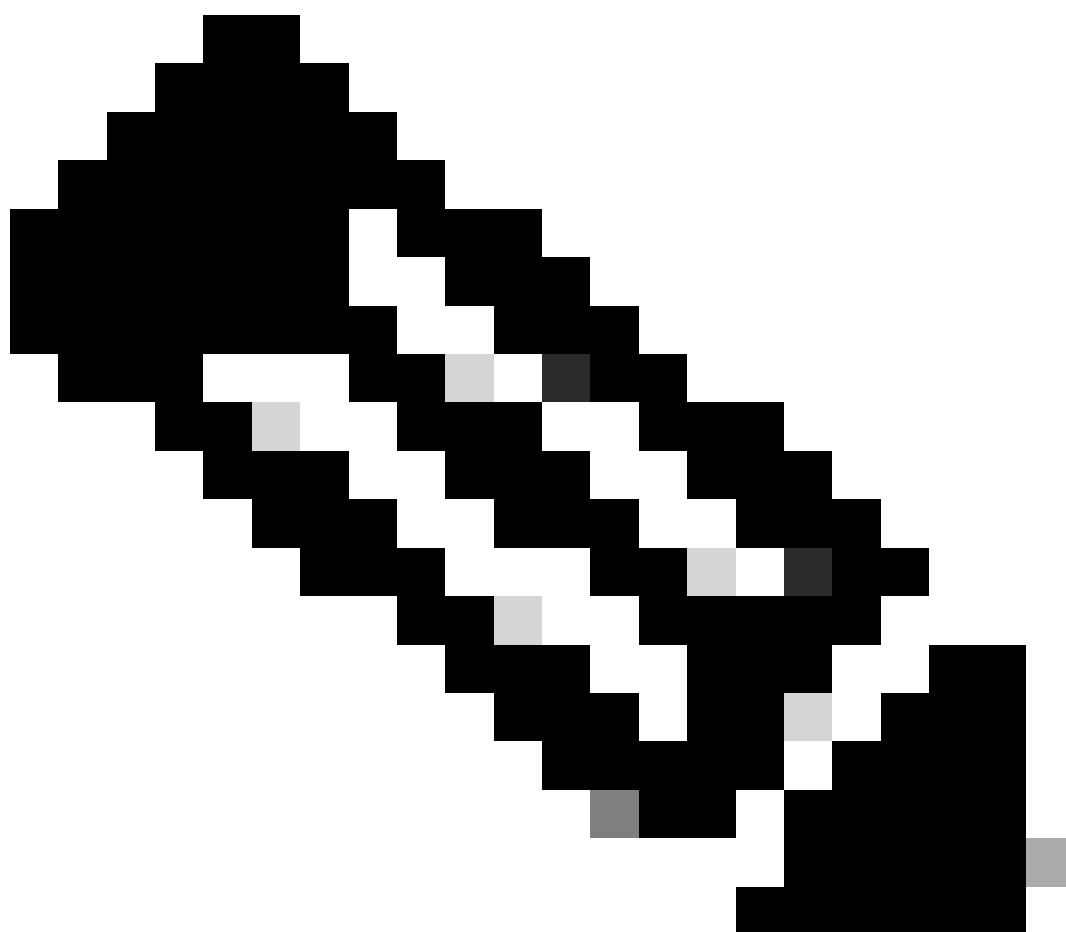
```
Logout          Exit this session. Any unsaved changes are lost.
show           Display switch options and settings.
```

```
(Cisco Controller) >config
```

```
Incorrect usage. Use the '?' or <TAB> key to list commands.
```

Como se muestra en este ejemplo de salida, un ? en la CLI del controlador muestra una lista de comandos disponibles para el usuario actual. Observe también que el **config** comando no está disponible en este resultado de ejemplo. Esto ilustra que un usuario de sólo lectura no tiene el privilegio de hacer ninguna configuración en el WLC. Sin embargo, un usuario de lectura y escritura tiene los privilegios para realizar configuraciones en el controlador (tanto en el modo GUI como CLI).

---



**Nota:** Incluso después de autenticar un usuario WLC a través del servidor RADIUS, mientras navega de página en página, el servidor HTTP[S] aún autentica completamente al cliente cada vez. La única razón por la que no se le solicita la autenticación en cada página es que el explorador almacena en caché y vuelve a reproducir las credenciales.

---

---

## Troubleshoot

Hay ciertas circunstancias cuando un controlador autentica a los usuarios de administración a través del ACS, la autenticación finaliza con éxito (access-accept), y usted no ve ningún error de autorización en el controlador. Pero, al usuario se le pide otra vez para la autenticación.

En tales casos, usted no puede interpretar qué está mal y porqué el usuario no puede iniciar sesión en el WLC con solamente el **debug aaa events enable** comando. En su lugar, el controlador muestra otra solicitud de autenticación.

Una posible razón para esto es que el ACS no está configurado para transmitir el atributo Service-Type para ese usuario o grupo en particular, aunque el nombre de usuario y la contraseña estén correctamente configurados en el ACS.

La salida del **debug aaa events enable** comando no indica que un usuario no tenga los atributos requeridos (para este ejemplo, el atributo Service-Type) aunque un **access-accept** se envíe de vuelta desde el servidor AAA. En este ejemplo, el resultado del **debug aaa events enable** comando muestra un ejemplo.

```
<#root>
```

```
(Cisco Controller) >
```

```
debug aaa events enable
```

```
Mon Aug 13 20:14:33 2011: AuthenticationRequest: 0xa449a8c
```

```
Mon Aug 13 20:14:33 2011: Callback.....0x8250c40
```

```
Mon Aug 13 20:14:33 2011: protocolType.....0x00020001
```

```
Mon Aug 13 20:14:33 2011: proxyState.....1A:00:00:00:00:00-00:00
```

```
Mon Aug 13 20:14:33 2011: Packet contains 5 AVPs (not shown)
```

```
Mon Aug 13 20:14:33 2011: 1a:00:00:00:00:00 Successful transmission of  
Authentication Packet (id 8) to 172.16.1.1:1812, proxy state  
1a:00:00:00:00:00-00:00
```

```
Mon Aug 13 20:14:33 2011: ***Enter processIncomingMessages: response code=2
```

```
Mon Aug 13 20:14:33 2011: ***Enter processRadiusResponse: response code=2
```

```
Mon Aug 13 20:14:33 2011: 1a:00:00:00:00:00 Access-Accept
received from RADIUS server 172.16.1.1 for mobile 1a:00:00:00:00:00 receiveId = 0
```

```
Mon Aug 13 20:14:33 2011: AuthorizationResponse: 0x9802520
```

```
Mon Aug 13 20:14:33 2011: structureSize.....28
```

```
Mon Aug 13 20:14:33 2011: resultCode.....0
```

```
Mon Aug 13 20:14:33 2011: protocolUsed.....0x00000001
```

```
Mon Aug 13 20:14:33 2011: proxyState.....1A:00:00:00:00:00-00:00
```

```
Mon Aug 13 20:14:33 2011: Packet contains 0 AVPs:
```

En este primer resultado del **debug aaa events enable** comando de ejemplo, verá que Access-Accept se recibe con éxito del servidor RADIUS pero el atributo Service-Type no se pasa al WLC. Esto se debe a que el usuario particular no está configurado con este atributo en el ACS.

Cisco Secure ACS debe configurarse para que devuelva el atributo Service-Type después de la autenticación de usuario. El valor del atributo Service-Type debe establecerse en **Administrative** o **NAS-Prompt** en función de los privilegios de usuario.

Este segundo ejemplo muestra de nuevo el resultado del **debug aaa events enable** comando. Sin embargo, esta vez el atributo Service-Type se establece en **Administrative** en ACS.

```
<#root>
```

```
(Cisco Controller)>
```

```
debug aaa events enable
```

```
Mon Aug 13 20:17:02 2011: AuthenticationRequest: 0xa449f1c
```

```
Mon Aug 13 20:17:02 2011: Callback.....0x8250c40
```

```
Mon Aug 13 20:17:02 2011: protocolType.....0x00020001
```

```

Mon Aug 13 20:17:02 2011: proxyState.....1D:00:00:00:00-00:00
Mon Aug 13 20:17:02 2011: Packet contains 5 AVPs (not shown)
Mon Aug 13 20:17:02 2011: 1d:00:00:00:00 Successful transmission of
Authentication Packet (id 11) to 172.16.1.1:1812, proxy state
1d:00:00:00:00-00:00
Mon Aug 13 20:17:02 2011: ****Enter processIncomingMessages: response code=2
Mon Aug 13 20:17:02 2011: ****Enter processRadiusResponse: response code=2

Mon Aug 13 20:17:02 2011: 1d:00:00:00:00 Access-Accept received
from RADIUS server 172.16.1.1 for mobile 1d:00:00:00:00 receiveId = 0

Mon Aug 13 20:17:02 2011: AuthorizationResponse: 0x9802520
Mon Aug 13 20:17:02 2011: structureSize.....100
Mon Aug 13 20:17:02 2011: resultCode.....0
Mon Aug 13 20:17:02 2011: protocolUsed.....0x00000001
Mon Aug 13 20:17:02 2011: proxyState.....1D:00:00:00:00-00:00
Mon Aug 13 20:17:02 2011: Packet contains 2 AVPs:

Mon Aug 13 20:17:02 2011: AVP[01] Service-Type.....0x00000006 (6) (4 bytes)

Mon Aug 13 20:17:02 2011: AVP[02] Class.....
CISCOACS:000d1b9f/ac100128/acserver (36 bytes)

```

Puede ver en este resultado de ejemplo anterior que el atributo Service-Type se pasa al WLC.

Información Relacionada

- [Configurar el controlador de LAN inalámbrica: Guía de configuración](#)

- [Configuración de VLAN en controladores de LAN inalámbrica](#)
- [Configure un servidor RADIUS y un WLC para la asignación de VLAN dinámica](#)
- [Configuración básica de Wireless LAN Controller y Lightweight Access Point](#)
- [Configuración de las VLAN del Grupo AP con los Controladores de LAN Inalámbrica](#)
- [Soporte técnico y descargas de Cisco](#)

## Acerca de esta traducción

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

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

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



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).