Configuración de la red inalámbrica unificada de Cisco TACACS+

Contenido

Introducción

Este documento proporciona un ejemplo de configuración de Terminal Access Controller Access Control System Plus (TACACS+) en un Controlador de LAN inalámbrico Cisco (WLC) y un Cisco

Wireless Control System (WCS) para una red inalámbrica unificada de Cisco. Este documento también proporciona algunos consejos de Troubleshooting básico.

TACACS+ es un protocolo cliente/servidor que proporciona seguridad centralizada a los usuarios que intentan obtener acceso de administración a un router o servidor de acceso a la red. TACACS+ proporciona estos servicios AAA:

- Autenticación de usuarios que intentan iniciar sesión en el equipo de red
- Autorización para determinar qué nivel de acceso deben tener los usuarios
- Contabilidad para realizar un seguimiento de todos los cambios que realiza el usuario

Refiérase a Configuración de TACACS+ para obtener más información sobre los servicios AAA y la funcionalidad TACACS+.

Consulte Comparación de TACACS+ y RADIUS para ver una comparación de TACACS+ y RADIUS.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento de cómo configurar WLC y puntos de acceso ligeros (LAP) para el funcionamiento básico
- Conocimiento del protocolo de punto de acceso ligero (LWAPP) y de los métodos de seguridad inalámbrica
- Conocimiento básico RADIUS y TACACS+
- Conocimiento básico de la configuración de Cisco ACS

Componentes Utilizados

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

- Cisco Secure ACS para la versión 4.0 de Windows
- Controlador de LAN inalámbrica de Cisco que ejecuta la versión 4.1.171.0. La funcionalidad TACACS+ en WLCs es soportada en la versión de software 4.1.171.0 o posterior.
- Cisco Wireless Control System que ejecuta la versión 4.1.83.0. La funcionalidad TACACS+ en WCS se soporta en la versión de software 4.1.83.0 o posterior.

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.

Convenciones

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

Implementación de TACACS+ en el controlador

Autenticación

La autenticación se puede realizar mediante una base de datos local, RADIUS o servidor TACACS+ que utilice un nombre de usuario y una contraseña. La implementación no es completamente modular. Los servicios de autenticación y autorización están vinculados entre sí. Por ejemplo, si la autenticación se realiza mediante RADIUS/base de datos local, la autorización no se realiza con TACACS+. Utilizaría los permisos asociados para el usuario en la base de datos local o RADIUS, como sólo lectura o lectura-escritura, mientras que cuando la autenticación se realiza con TACACS+, la autorización está vinculada a TACACS+.

En los casos en que se configuran varias bases de datos, se proporciona una CLI para dictar la secuencia en la que se debe hacer referencia a la base de datos backend.

Autorización

La autorización se basa en tareas y no en una autorización real basada en comandos. Las tareas se asignan a varias fichas que corresponden a los siete elementos de la barra de menús que se encuentran actualmente en la interfaz gráfica de usuario web. Estos son los elementos de la barra de menús:

- MONITOR
- WLANS
- CONTROLADOR
- TECNOLOGÍA INALÁMBRICA
- SECURITY
- GESTIÓN
- COMANDO

La razón de esta asignación se basa en el hecho de que la mayoría de los clientes utilizan la interfaz web para configurar el controlador en lugar de la CLI.

Hay disponible una función adicional para la gestión de administradores de vestíbulo (LOBBY) para los usuarios que solo necesitan tener privilegios de administrador de vestíbulo.

La tarea a la que tiene derecho un usuario se configura en el servidor TACACS+ (ACS) utilizando los pares Attribute-Value (AV) personalizados. Se puede autorizar al usuario para una o varias tareas. La autorización mínima es sólo MONITOR y el máximo es ALL (autorizado para realizar las siete pestañas). Si un usuario no tiene derecho a una tarea determinada, el usuario podrá acceder a esa tarea en modo de sólo lectura. Si se habilita la autenticación y el servidor de autenticación se vuelve inalcanzable o no puede autorizar, el usuario no puede iniciar sesión en el controlador.

Nota: Para que la autenticación de administración básica a través de TACACS+ se realice correctamente, debe configurar los servidores de autenticación y autorización en el WLC. La configuración de contabilidad es opcional.

Contabilidad

La contabilidad se produce siempre que una acción iniciada por el usuario se realiza

correctamente. Los atributos cambiados se registran en el servidor de contabilidad TACACS+ junto con los siguientes:

- ID de usuario de la persona que realizó el cambio
- El host remoto desde el que el usuario ha iniciado sesión
- La fecha y hora en que se ejecutó el comando
- Nivel de autorización del usuario
- Cadena que proporciona información sobre la acción realizada y los valores proporcionados

Si el servidor de contabilidad se vuelve inalcanzable, el usuario puede continuar con la sesión.

Nota: Los registros contables no se generan a partir de WCS en la versión 4.1 o anterior del software.

Configuración TACACS+ en el WLC

La versión 4.1.171.0 y posteriores del software WLC introducen nuevos CLI y cambios en la GUI web para habilitar la funcionalidad TACACS+ en el WLC. Las CLI introducidas se enumeran en esta sección como referencia. Los cambios correspondientes para la GUI web se agregan en la ficha Seguridad.

Este documento asume que la configuración básica del WLC ya está completa.

Para configurar TACACS+ en el controlador WLC, debe completar estos pasos:

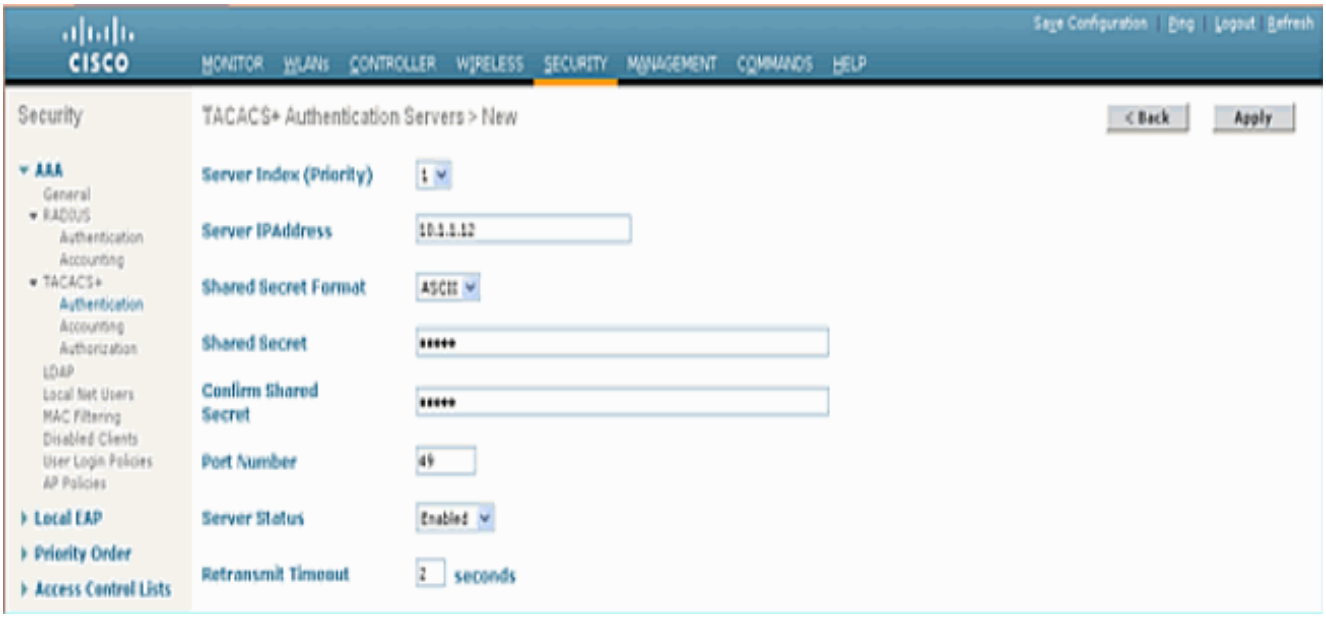
1. Agregar un servidor de autenticación TACACS+
2. Agregar un servidor de autorización TACACS+
3. Agregar un servidor de contabilidad TACACS+
4. Configurar el orden de autenticación

Agregar un servidor de autenticación TACACS+

Complete estos pasos para agregar un servidor de autenticación TACACS+:

1. Utilice la GUI y vaya a **Security > TACACS+ > Authentication**.

2. Agregue la dirección IP del servidor TACACS+ e introduzca la clave secreta compartida. Si es necesario, cambie el puerto predeterminado de TCP/49.



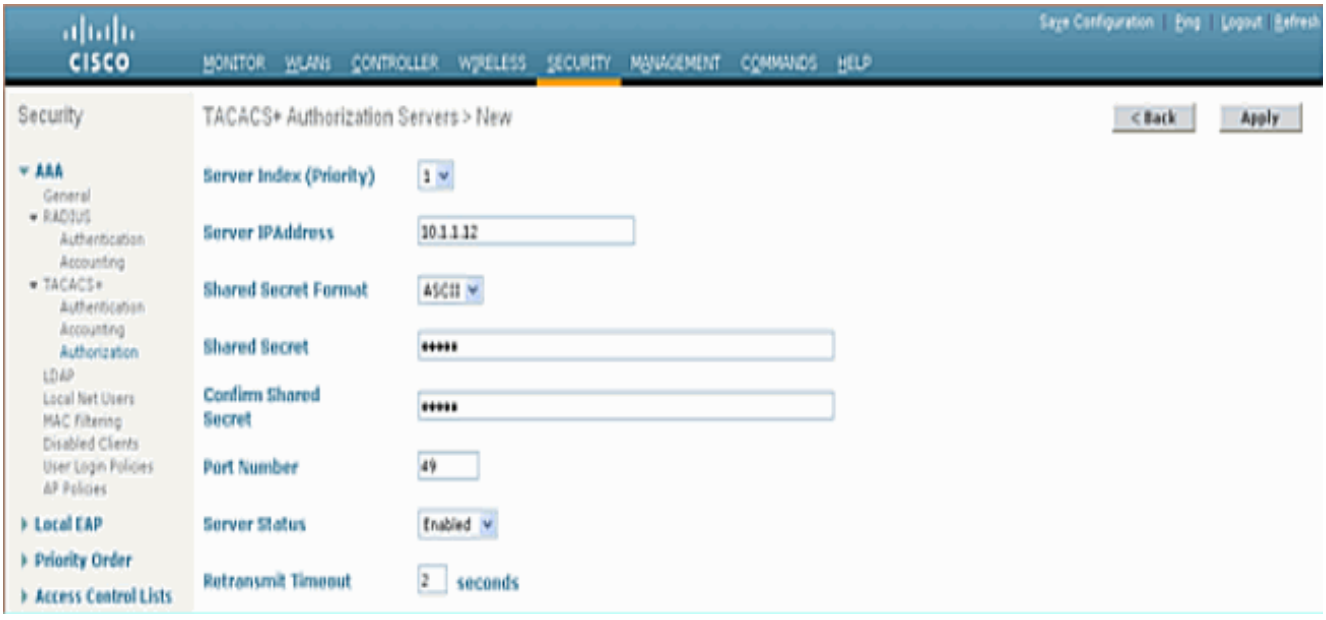
3. Haga clic en Apply (Aplicar).Puede lograr esto desde CLI usando el comando **config tacacs auth add** *<Server Index> <IP addr> <port> [ascii/hex]* **<secret>**:

```
(Cisco Controller) >config tacacs auth add 1 10.1.1.12 49 ascii cisco123
```

Agregar un servidor de autorización TACACS+

Complete estos pasos para agregar un Servidor de Autorización TACACS+:

1. Desde la GUI, vaya a **Security > TACACS+ > Authorization**.
2. Agregue la dirección IP del servidor TACACS+ e introduzca la clave secreta compartida. Si es necesario, cambie el puerto predeterminado de TCP/49.



3. Haga clic en Apply (Aplicar).Puede lograr esto desde CLI usando el comando **config tacacs athr add** *<Server Index> <IP addr> <port> [ascii/hex]* **<secret>**:

```
(Cisco Controller) >config tacacs athr add 1 10.1.1.12 49 ascii cisco123
```

Agregar un servidor de contabilidad TACACS+

Complete estos pasos para agregar un TACACS+ Accounting Server:

1. Utilice la GUI y vaya a **Security > TACACS+ > Accounting**.
2. Agregue la dirección IP del servidor e introduzca la clave secreta compartida. Si es necesario, cambie el puerto predeterminado de TCP/49.

3. Haga clic en Apply (Aplicar).Puede lograr esto desde CLI usando el comando **config tacacs acct add** *<Server Index> <IP addr> <port> [ascii/hex]* **<secret>**:

```
(Cisco Controller) >config tacacs acct add 1 10.1.1.12 49 ascii cisco123
```

Configurar el orden de autenticación

Este paso explica cómo configurar el orden de autenticación AAA cuando hay varias bases de datos configuradas. El orden de autenticación puede ser **local y RADIUS**, o **local y TACACS**. La configuración predeterminada del controlador para el orden de autenticación es *local y RADIUS*.

Complete estos pasos para configurar el orden de autenticación:

1. Desde la GUI, vaya a **Seguridad > Orden de prioridad > Usuario de administración**.
2. Seleccione la prioridad de autenticación.En este ejemplo, se ha seleccionado TACACS+.
3. Haga clic en **Aplicar** para que se realice la selección.

Puede lograr esto desde CLI usando el comando **config aaa auth mgmt** *<server1> <server2>*:

```
(Cisco Controller) >config aaa auth mgmt tacacs local
```

Verificar configuración

Esta sección describe los comandos usados para verificar la configuración de TACACS+ en el WLC. Estos son algunos útiles comandos **show** que ayudan a determinar si la configuración es correcta:

- **show aaa auth**: proporciona información sobre el orden de la autenticación.

```
(Cisco Controller) >show aaa auth
Management authentication server order:
    1..................................... local
    2..................................... Tacacs
```

- **show tacacs summary**—Muestra un resumen de los servicios y estadísticas TACACS+.

```
(Cisco Controller) >show tacacs summary
Authentication Servers

Idx  Server Address    Port    State     Tout
---  ---------------  ------  --------  ----
1    10.1.1.12         49      Enabled   2

Authorization Servers

Idx  Server Address    Port    State     Tout
---  ---------------  ------  --------  ----
1    10.1.1.12         49      Enabled   2

Accounting Servers

Idx  Server Address    Port    State     Tout
---  ---------------  ------  --------  ----
1    10.1.1.12         49      Enabled   2
```

- **show tacacs auth stats**—Muestra las estadísticas del servidor de autenticación TACACS+.

```
(Cisco Controller) >show tacacs auth statistics
Authentication Servers:

Server Index..................................... 1
Server Address..................................... 10.1.1.12
Msg Round Trip Time.............................. 0 (1/100 second)
First Requests................................... 7
Retry Requests................................... 3
Accept Responses................................. 3
Reject Responses................................. 0
Error Responses.................................. 0
Restart Responses................................ 0
Follow Responses................................. 0
GetData Responses................................ 0
Encrypt no secret Responses...................... 0
Challenge Responses.............................. 0
Malformed Msgs................................... 0
Bad Authenticator Msgs........................... 0
Timeout Requests................................. 12
Unknowntype Msgs................................. 0
Other Drops...................................... 0
```

- **show tacacs athr stats**—Muestra las estadísticas del servidor de autorización TACACS+.

```
(Cisco Controller) >show tacacs athr statistics
Authorization Servers:

Server Index..................................... 1
Server Address..................................... 10.1.1.12
```

```
Msg Round Trip Time.......................... 0 (1/100 second)
First Requests............................... 3
Retry Requests............................... 3
Received Responses........................... 3
Authorization Success........................ 3
Authorization Failure........................ 0
Challenge Responses.......................... 0
Malformed Msgs............................... 0
Bad Athrenticator Msgs....................... 0
Timeout Requests............................. 0
Unknowntype Msgs............................. 0
Other Drops.................................. 0
```

- **show tacacs acct stats**—Muestra las estadísticas del servidor de contabilidad TACACS+.

```
(Cisco Controller) >show tacacs acct statistics
Accounting Servers:

Server Index................................. 1
Server Address............................... 10.1.1.12
Msg Round Trip Time.......................... 0 (1/100 second)
First Requests............................... 133
Retry Requests............................... 0
Accounting Response.......................... 0
Accounting Request Success................... 0
Accounting Request Failure................... 0
Malformed Msgs............................... 0
Bad Authenticator Msgs....................... 0
Timeout Requests............................. 399
Unknowntype Msgs............................. 0
Other Drops.................................. 0
```

Configuración de Cisco Secure ACS Server

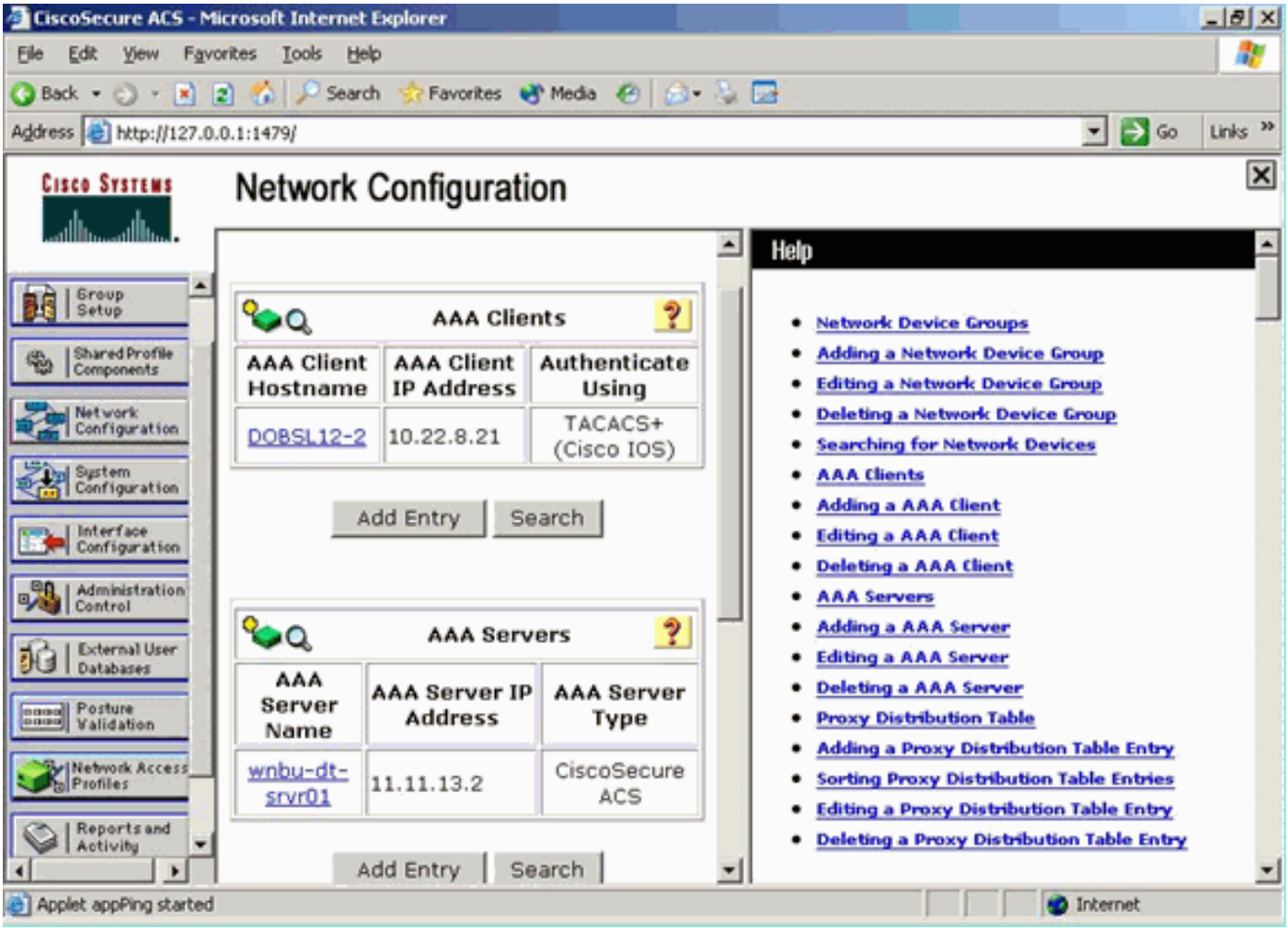
Esta sección proporciona los pasos involucrados en el servidor TACACS+ ACS para crear servicios y atributos personalizados, y asignar las funciones a los usuarios o grupos.

La creación de usuarios y grupos no se explica en esta sección. Se supone que los usuarios y grupos se crean según sea necesario. Refiérase a Guía del Usuario para Cisco Secure ACS para Windows Server 4.0 para obtener información sobre cómo crear usuarios y grupos de usuarios.

Configuración de red

Siga este paso:

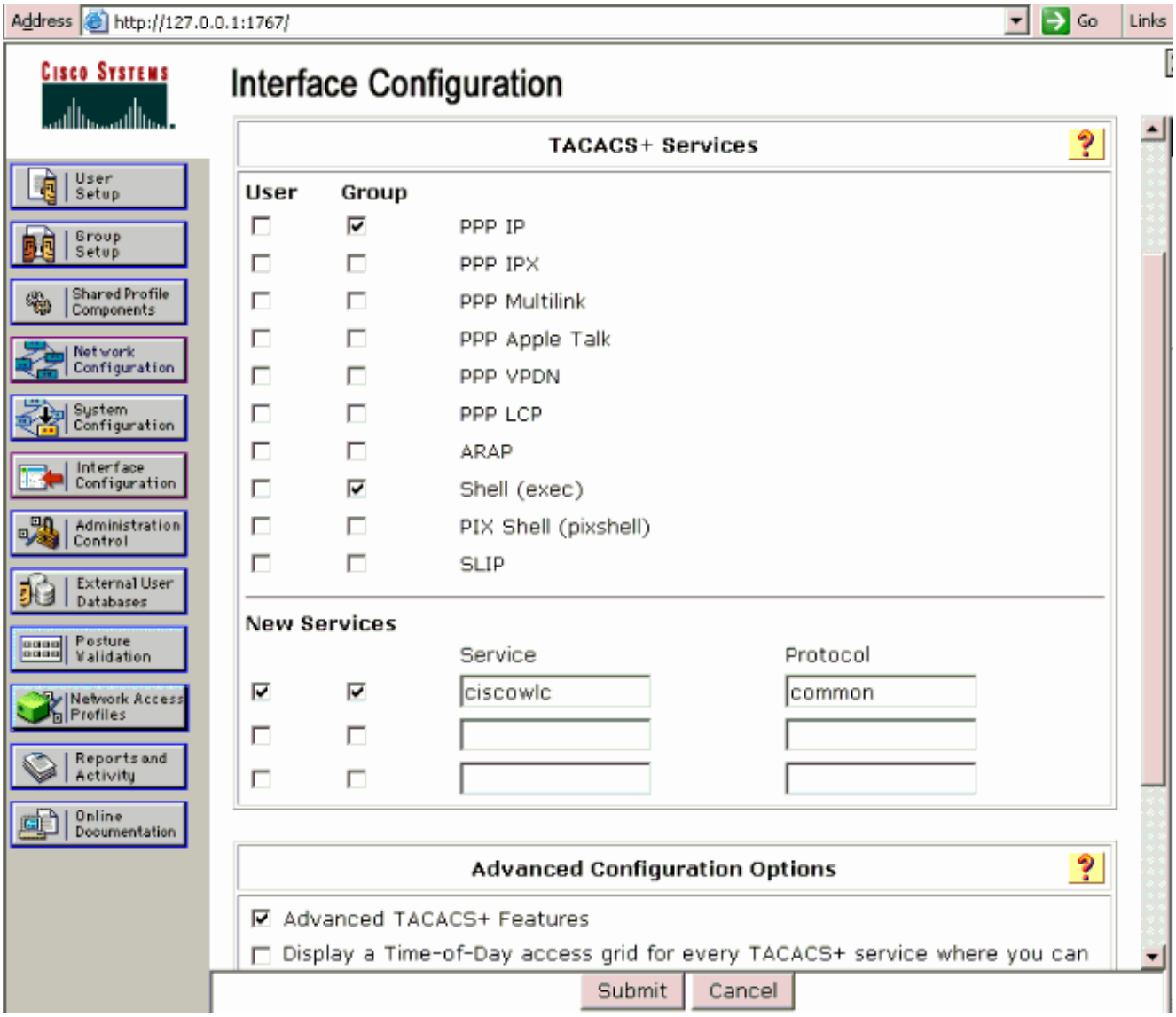
Agregue la dirección IP de administración del controlador como cliente AAA con el mecanismo de autenticación como TACACS+ (Cisco IOS).



Configuración de la Interfaz

Complete estos pasos:

1. En el menú Interface Configuration , seleccione el enlace **TACACS+** (Cisco IOS).
2. Habilite los **Nuevos Servicios**.
3. Marque las casillas de verificación **Usuario** y **Grupo**.
4. Ingrese **ciscowlc** para Service y **common** para Protocol.
5. Habilite las **Funciones avanzadas de TACACS+**.

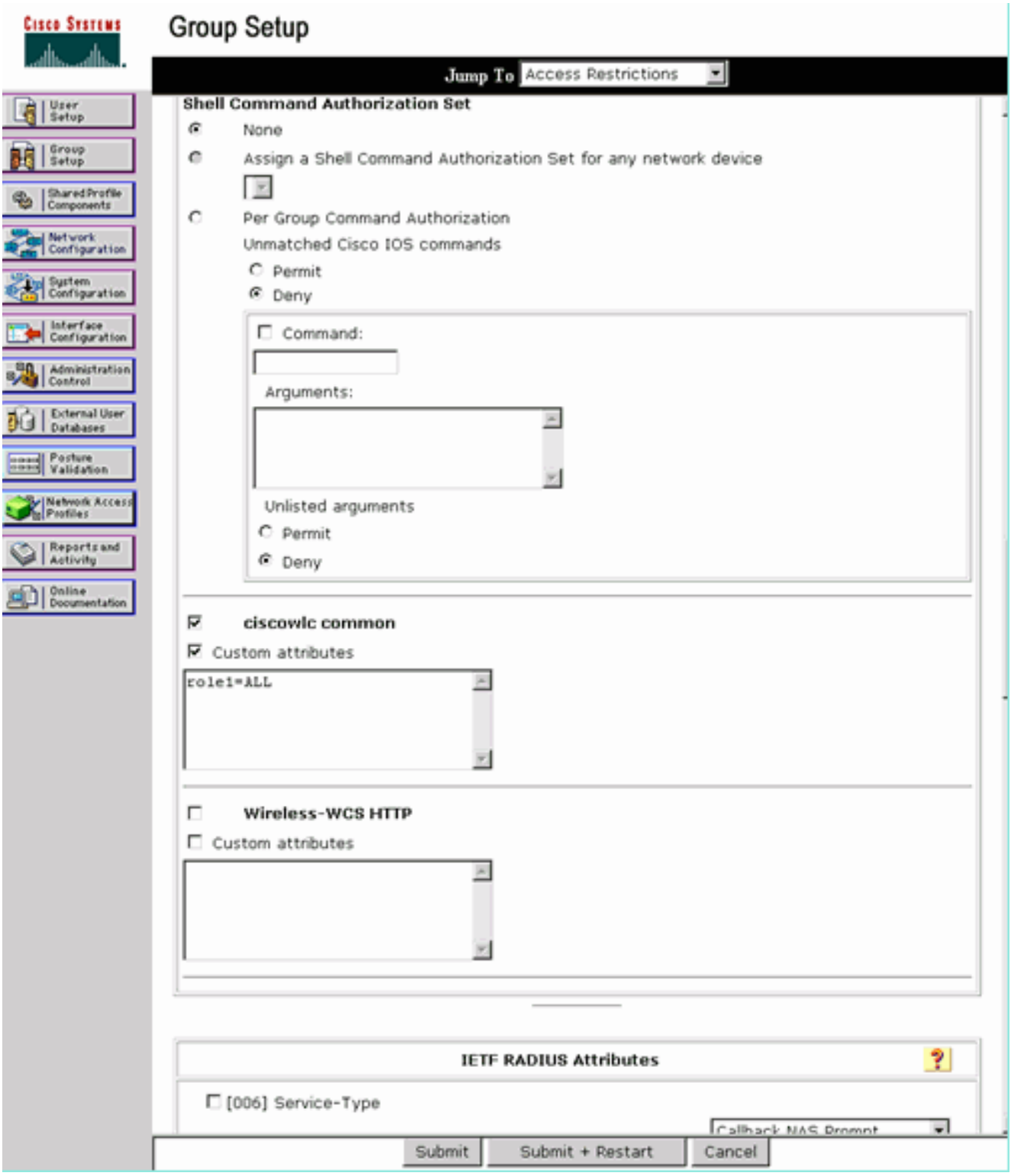


6. Haga clic en **Enviar** para aplicar los cambios.

Configuración de usuario/grupo

Complete estos pasos:

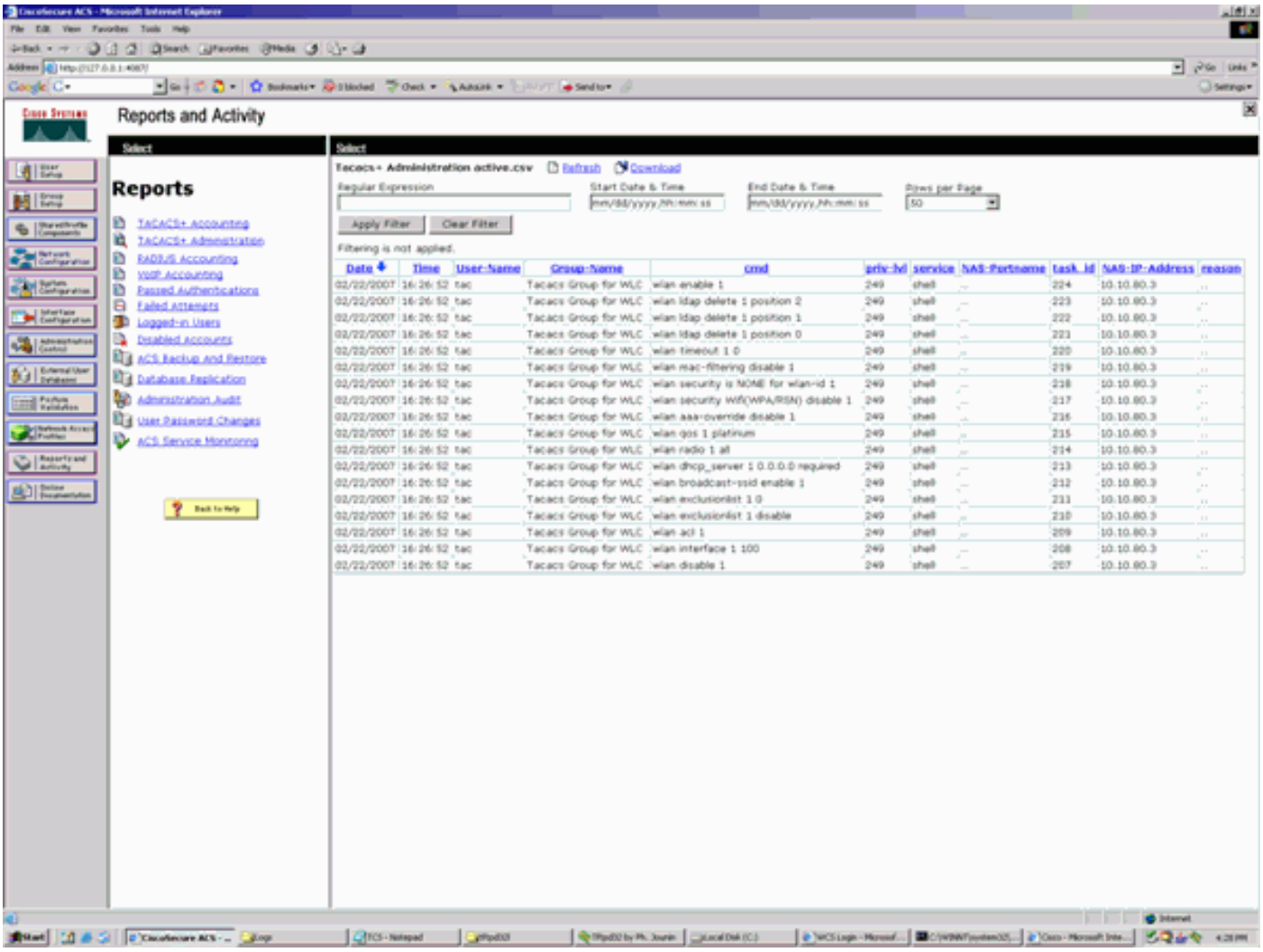
1. Seleccione un usuario o grupo creado previamente.
2. Vaya a **TACACS+ Settings**.
3. Marque la casilla de verificación que corresponde al servicio *ciscowlc* creado en la sección Configuración de la Interfaz.
4. Marque la casilla de verificación **Atributos personalizados**.



5. En el cuadro de texto debajo de Atributos personalizados, introduzca este texto si el usuario creado sólo necesita acceso a WLAN, SEGURIDAD y CONTROLADOR: **role1=WLAN role2=SECURITY role3=CONTROLLER**.Si el usuario sólo necesita acceso a la ficha SECURITY (SEGURIDAD), introduzca este texto: **role1=SEGURIDAD**.La función corresponde a los siete elementos de la barra de menús de la GUI web del controlador. Los elementos de la barra de menús son MONITOR, WLAN, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT y COMMAND.
6. Introduzca la función que un usuario necesita para role1, role2, etc. Si un usuario necesita todas las funciones, la palabra clave **ALL** debe utilizarse. Para la función de administrador del vestíbulo, se debe utilizar la palabra clave **LOBBY**.

Registros de contabilidad en Cisco Secure ACS

Los registros contables TACACS+ del WLC están disponibles en Cisco Secure ACS en la Administración de Informes y Actividad TACACS+:



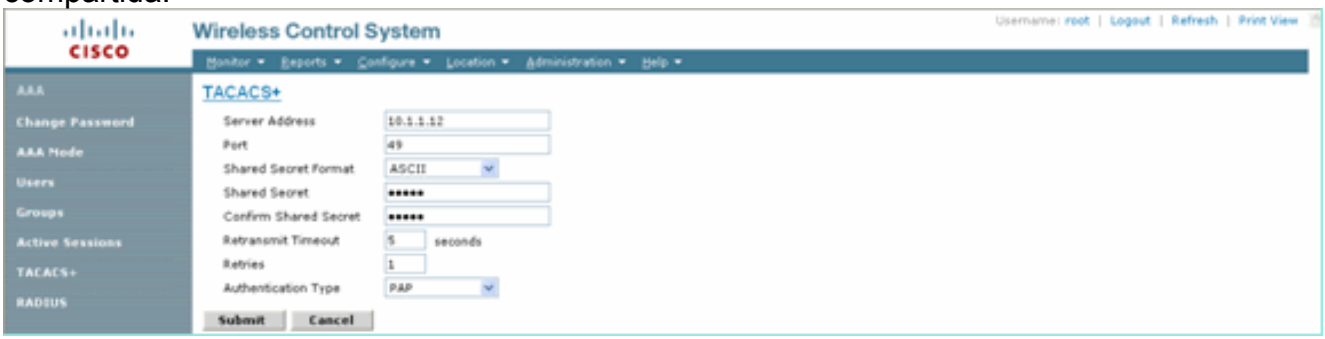
Configuración de TACACS+ en WCS

Complete estos pasos:

1. Desde la GUI, inicie sesión en WCS con la cuenta raíz.
2. Agregue el servidor TACACS+. Vaya a **Administration > AAA > TACACS+ > Add TACACS+ Server**.

3. Agregue los detalles del servidor TACACS+, como la dirección IP, el número de puerto (49 es el valor predeterminado) y la clave secreta

compartida.



4. Habilite la autenticación TACACS+ para la administración en WCS. Vaya a **Administration > AAA > AAA Mode > Select TACACS+**.

WCS con dominios virtuales

Virtual Domain es una nueva función introducida con la versión 5.1 de WCS. Un dominio virtual de WCS consta de un conjunto de dispositivos y mapas y restringe la vista de un usuario a la información relevante para estos dispositivos y mapas. A través de un dominio virtual, un administrador puede asegurarse de que los usuarios solo pueden ver los dispositivos y mapas de los que son responsables. Además, debido a los filtros del dominio virtual, los usuarios pueden configurar, ver alarmas y generar informes sólo para su parte asignada de la red. El administrador especifica un conjunto de dominios virtuales permitidos para cada usuario. Sólo una de estas opciones puede estar activa para ese usuario al iniciar sesión. El usuario puede cambiar el dominio virtual actual seleccionando un dominio virtual permitido diferente en el menú desplegable Dominio virtual de la parte superior de la pantalla. Todos los informes, alarmas y otras funciones se filtran ahora por ese dominio virtual.

Si sólo hay un dominio virtual definido (raíz) en el sistema y el usuario no tiene ningún dominio virtual en los campos de atributos personalizados en el servidor TACACS+/RADIUS, el usuario tiene asignado el dominio virtual raíz de forma predeterminada.

Si hay más de un dominio virtual y el usuario no tiene ningún atributo especificado, se bloqueará el inicio de sesión del usuario. Para permitir que el usuario inicie sesión, los atributos personalizados de dominio virtual deben exportarse al servidor Radius/TACACS+.

La ventana Atributos personalizados de dominio virtual permite indicar los datos específicos del protocolo adecuados para cada dominio virtual. El botón Exportar de la barra lateral de la jerarquía de dominio virtual da formato previo a los atributos RADIUS y TACACS+ del dominio virtual. Puede copiar y pegar estos atributos en el servidor ACS. Esto le permite copiar solamente los dominios virtuales aplicables a la pantalla del servidor ACS y asegura que los usuarios sólo tengan acceso a estos dominios virtuales.

Para aplicar los atributos RADIUS y TACACS+ preformateados al servidor ACS, complete los

pasos explicados en la sección RADIUS de dominio virtual y Atributos TACACS+.

Configuración de Cisco Secure ACS para utilizar WCS

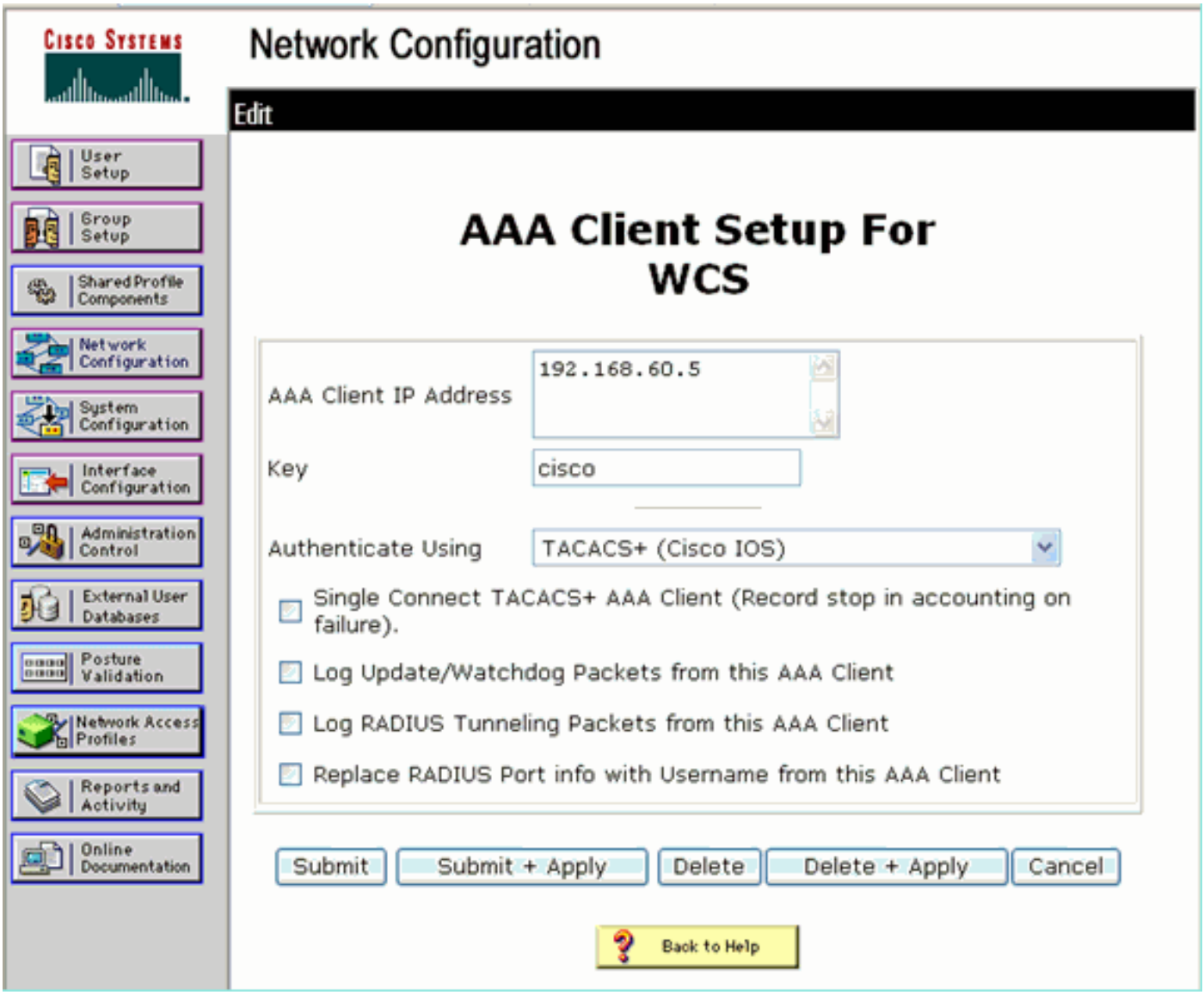
La sección proporciona los pasos involucrados en el servidor TACACS+ ACS para crear servicios y atributos personalizados, y asignar las funciones a los usuarios o grupos.

La creación de usuarios y grupos no se explica en esta sección. Se supone que los usuarios y grupos se crean según sea necesario.

Configuración de red

Siga este paso:

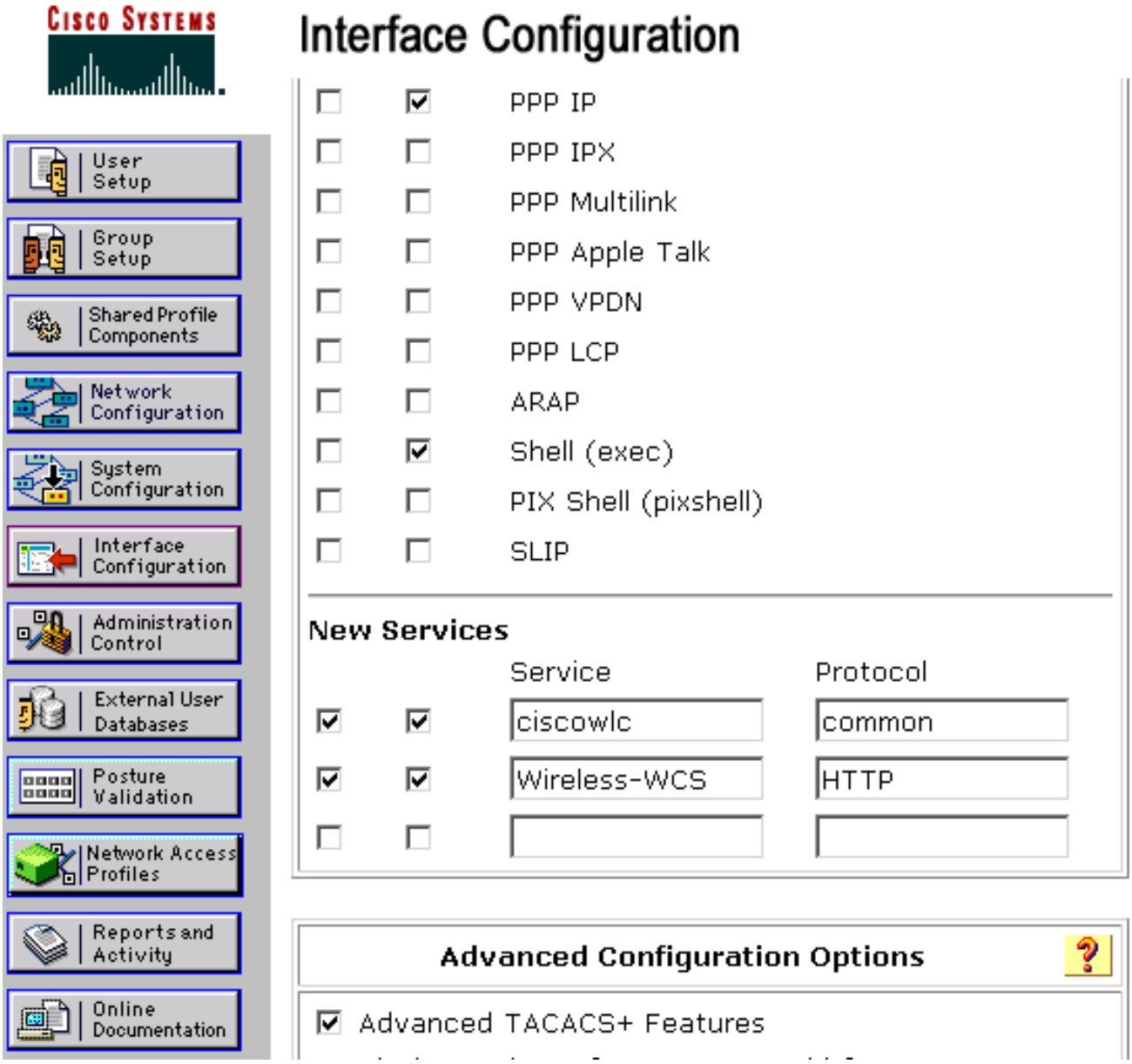
Agregue la dirección IP de WCS como cliente AAA con el mecanismo de autenticación como TACACS+ (Cisco IOS).



Configuración de la Interfaz

Complete estos pasos:

1. En el menú Interface Configuration , seleccione el enlace **TACACS+** (Cisco IOS).
2. Habilite los **Nuevos Servicios**.
3. Marque las casillas de verificación **Usuario** y **Grupo**.
4. Ingrese **Wireless-WCS** para Service y **HTTP** para Protocol.**Nota:** HTTP debe estar en CAPS.
5. Habilite las **Funciones avanzadas de TACACS+**.

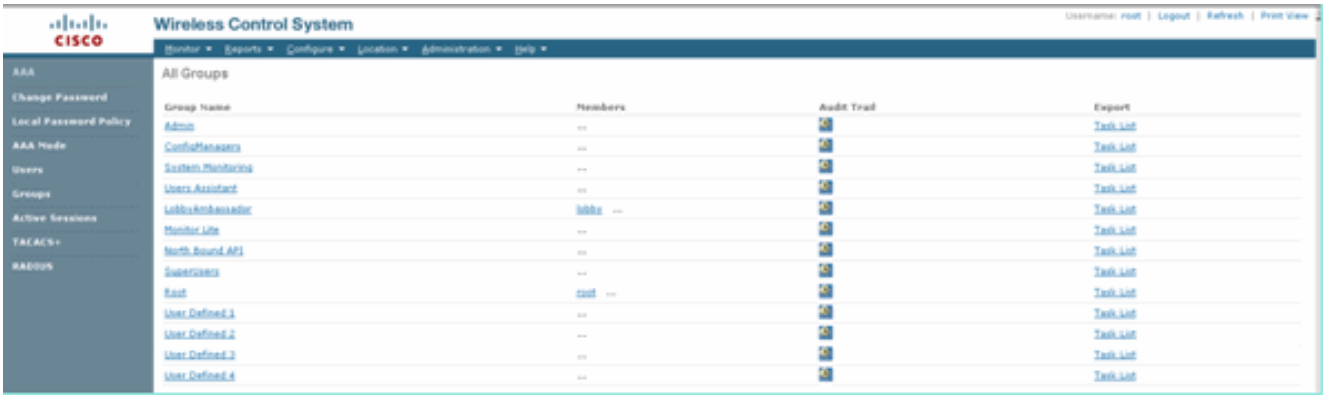


6. Haga clic en **Enviar** para aplicar los cambios.

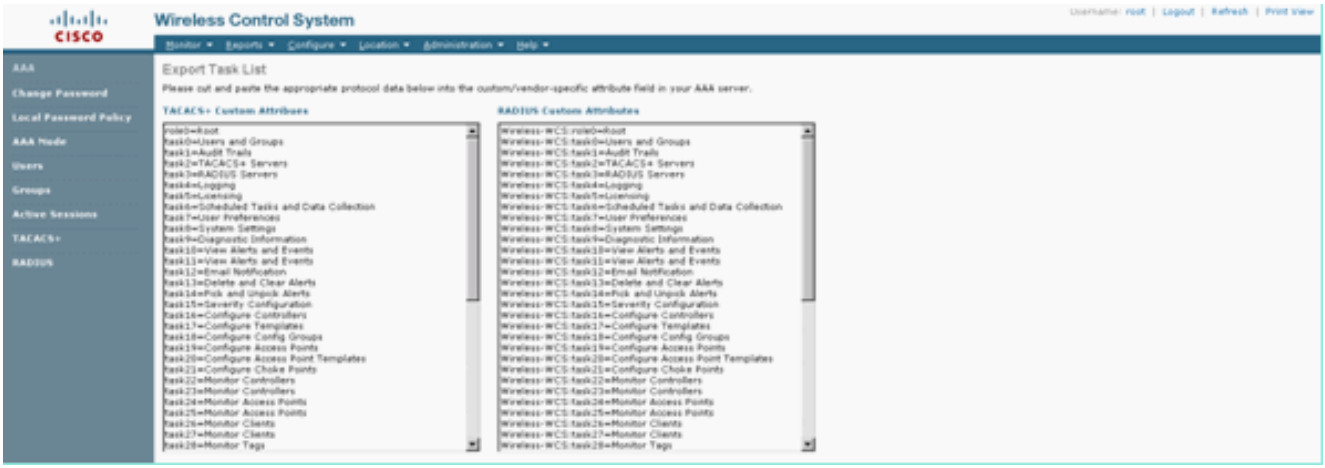
Configuración de usuario/grupo

Complete estos pasos:

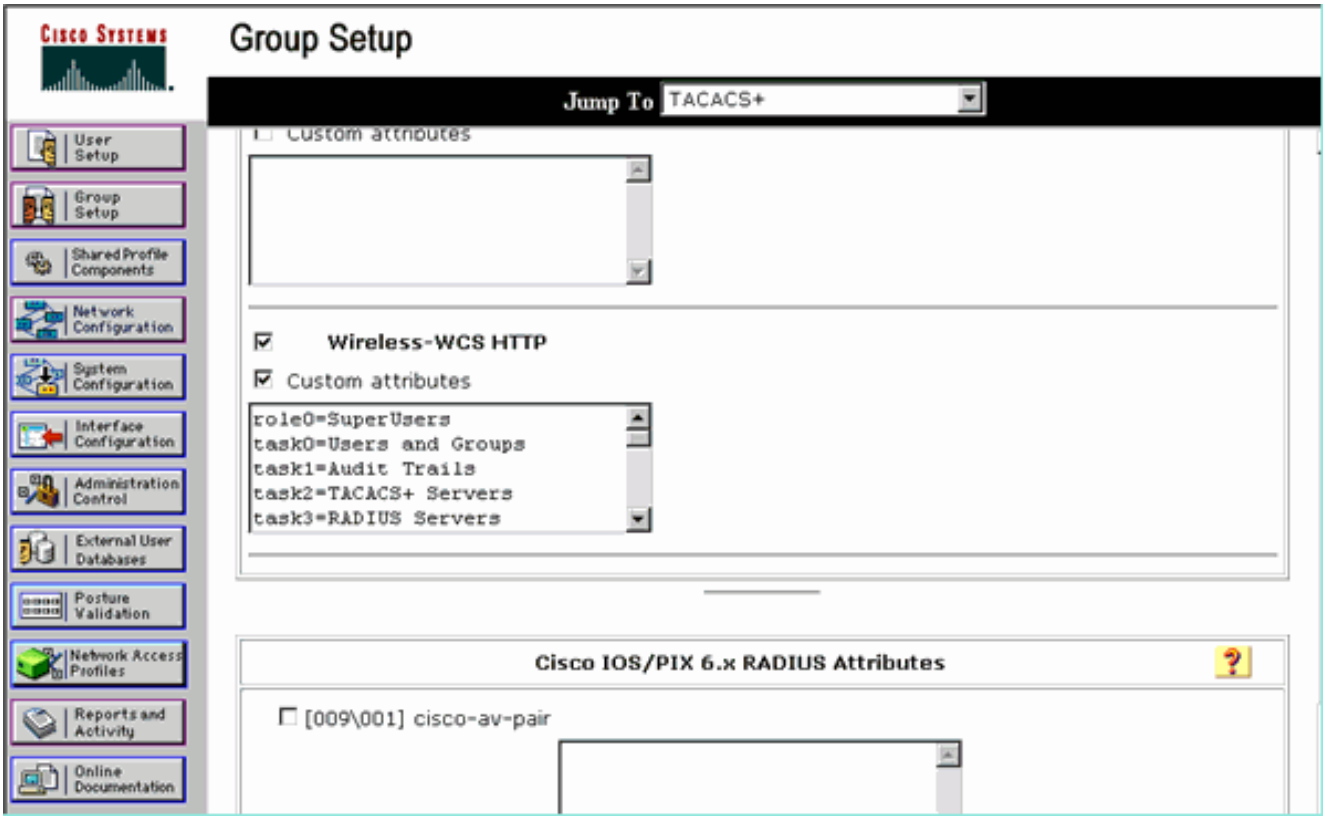
1. En la GUI de WCS, navegue hasta **Administration > AAA > Groups** para seleccionar cualquiera de los grupos de usuarios preconfigurados, como SuperUsers en el WCS.



2. Seleccione la Lista de tareas para los grupos de usuarios preconfigurados y copie y pegue en el
ACS.



3. Seleccione un usuario/grupo creado anteriormente y vaya a **TACACS+ Settings**.
4. En ACS GUI, seleccione la casilla de verificación que corresponde al servicio Wireless-WCS creado anteriormente.
5. En ACS GUI, marque la casilla **Atributos personalizados**.
6. En el cuadro de texto debajo de Atributos personalizados, introduzca esta función e información de tarea copiada de WCS. Por ejemplo, introduzca la lista de tareas permitidas por los
superusuarios.



7. A continuación, inicie sesión en el WCS con el nombre de usuario/contraseña recién creado en el ACS.

Depuraciones

Depuraciones del WLC para role1=ALL

```
(Cisco Controller) >debug aaa tacacs enable

(Cisco Controller) >Wed Feb 28 17:36:37 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:36:37 2007: tplus response: type=1 seq_no=2 session_id=5eaa857e
length=16 encrypted=0
Wed Feb 28 17:36:37 2007: TPLUS_AUTHEN_STATUS_GETPASS
Wed Feb 28 17:36:37 2007: auth_cont get_pass reply: pkt_length=22
Wed Feb 28 17:36:37 2007: processTplusAuthResponse: Continue auth transaction
Wed Feb 28 17:36:37 2007: tplus response: type=1 seq_no=4 session_id=5eaa857e
length=6 encrypted=0
Wed Feb 28 17:36:37 2007: tplus_make_author_request() from tplus_authen_passed returns rc=0
Wed Feb 28 17:36:37 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:36:37 2007: author response body: status=1 arg_cnt=1 msg_len=0 data_len=0
Wed Feb 28 17:36:37 2007: arg[0] = [9][role1=ALL]
Wed Feb 28 17:36:37 2007: User has the following mgmtRole fffffff8
```

Depuraciones del WLC para múltiples roles

```
(Cisco Controller) >debug aaa tacacs enable

Wed Feb 28 17:59:33 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:59:34 2007: tplus response: type=1 seq_no=2
session_id=b561ad88 length=16 encrypted=0
Wed Feb 28 17:59:34 2007: TPLUS_AUTHEN_STATUS_GETPASS
Wed Feb 28 17:59:34 2007: auth_cont get_pass reply: pkt_length=22
Wed Feb 28 17:59:34 2007: processTplusAuthResponse: Continue auth transaction
```

```
Wed Feb 28 17:59:34 2007: tplus response: type=1 seq_no=4 session_id=b561ad88
length=6 encrypted=0
Wed Feb 28 17:59:34 2007: tplus_make_author_request() from tplus_authen_passed
returns rc=0
Wed Feb 28 17:59:34 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:59:34 2007: author response body: status=1 arg_cnt=4 msg_len=0 data_len=0
Wed Feb 28 17:59:34 2007: arg[0] = [11][role1=WLAN]
Wed Feb 28 17:59:34 2007: arg[1] = [16][role2=CONTROLLER]
Wed Feb 28 17:59:34 2007: arg[2] = [14][role3=SECURITY]
Wed Feb 28 17:59:34 2007: arg[3] = [14][role4=COMMANDS]
Wed Feb 28 17:59:34 2007: User has the following mgmtRole 150
```

Depuraciones de un WLC para falla de autorización

```
(Cisco Controller) >debug aaa tacacs enable

Wed Feb 28 17:53:04 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:53:04 2007: tplus response: type=1 seq_no=2 session_id=89c553a1
length=16 encrypted=0
Wed Feb 28 17:53:04 2007: TPLUS_AUTHEN_STATUS_GETPASS
Wed Feb 28 17:53:04 2007: auth_cont get_pass reply: pkt_length=22
Wed Feb 28 17:53:04 2007: processTplusAuthResponse: Continue auth transaction
Wed Feb 28 17:53:04 2007: tplus response: type=1 seq_no=4 session_id=89c553a1
length=6 encrypted=0
Wed Feb 28 17:53:04 2007: tplus_make_author_request() from tplus_authen_passed
returns rc=0
Wed Feb 28 17:53:04 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:53:04 2007: author response body: status=16 arg_cnt=0 msg_len=0 data_len=0
Wed Feb 28 17:53:04 2007:User has the following mgmtRole 0
Wed Feb 28 17:53:04 2007: Tplus authorization for tac failed status=16
```

Información Relacionada

- Ejemplo de Configuración de Cisco Wireless LAN Controller (WLC) y Cisco ACS 5.x (TACACS+) para la Autenticación Web
- Configuración de TACACS+
- Cómo Configurar la Autenticación y Autorización TACACS para Usuarios Admin y no Admin en ACS 5.1
- Comparación de TACACS+ y RADIUS
- Soporte Técnico y Documentación - Cisco Systems