

La administración inalámbrica del sistema de control y del Sistema de control de redes con el ejemplo de configuración ACS 5.x

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configurar](#)

[Paso 1. Agregue el WCS a los clientes AAA ACS.](#)

[Paso 2. Agregue el Cisco Secure ACS como servidor TACACS+ en el WCS.](#)

[Paso 3. Configure el perfil correcto del shell en el ACS.](#)

[Paso 4. Cisco Secure ACS de la configuración para volver los atributos.](#)

[Verificación](#)

[Troubleshooting](#)

[Información Relacionada](#)

[Introducción](#)

Este documento describe cómo utilizar Cisco Secure Access Control Server (ACS) 5.x para configurar la administración de Cisco Wireless Control System (WCS) y de Cisco Prime Network Control System (NCS).

[prerrequisitos](#)

[Requisitos](#)

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Wireless Control System
- Sistema de control de redes de la prima de Cisco
- Cisco Secure Access Control Server

[Componentes Utilizados](#)

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

- Cisco Wireless Control System 7.0.172.0
- Cisco Secure ACS 5.x

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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte [Convenciones de Consejos Técnicos de Cisco](#) para obtener más información sobre las convenciones sobre documentos.

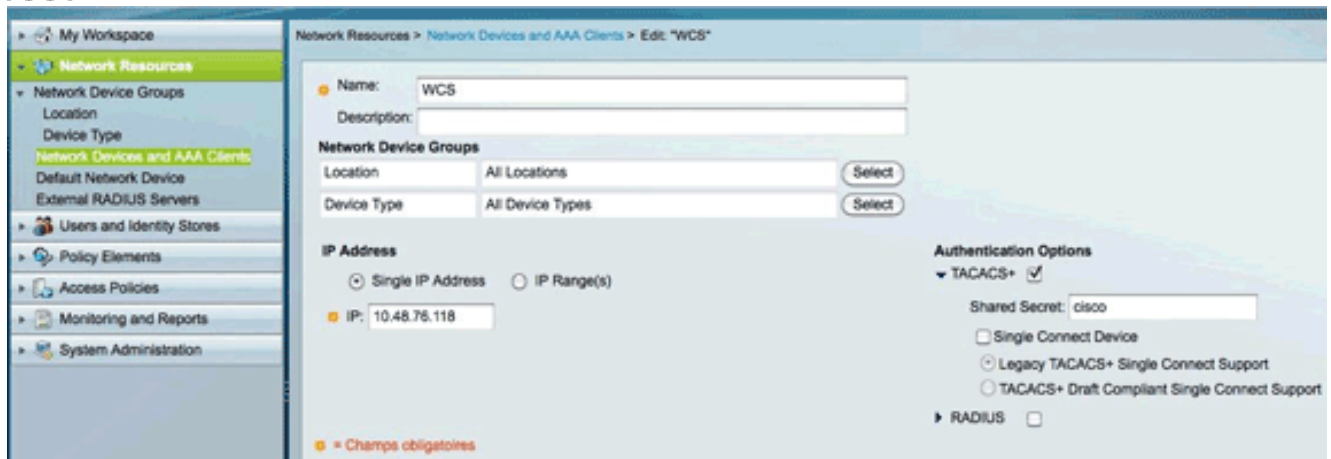
Configurar

Esta configuración de muestra describe cómo autenticar a un usuario con el TACACS+.

Nota: Aunque existan las diversas opciones y posibilidades cuando usted autentica a los usuarios WCS/NCS con el Cisco Secure ACS 5.x, no todas las combinaciones se describen en este documento. Sin embargo, este ejemplo provee de usted la información necesaria entender cómo modificar el ejemplo a la configuración exacta que usted quiere alcanzar.

Paso 1. Agregue el WCS a los clientes AAA ACS.

1. En el Cisco Secure ACS, elija los **recursos de red > los dispositivos de red y a los clientes AAA**.



2. Ingrese un nombre en el campo de nombre.
3. Ingrese el IP Address WCS en el campo del IP Address.
4. Bajo área de las opciones de autenticación, haga clic la casilla de verificación **TACACS+** para habilitar el TACACS+, y después ingrese un término que se utilizará como secreto compartido. **Nota:** Este ejemplo utiliza *Cisco* como el secreto compartido; sin embargo, por razones de seguridad, usted debe utilizar un término menos obvio.

Paso 2. Agregue el Cisco Secure ACS como servidor TACACS+ en el WCS.

1. Inicie sesión al WCS, y elija la **administración >AAA**.
2. Haga clic el **TACACS+**.

3. Ingrese su término secreto compartido en el secreto compartido y confirme los campos secretos compartidos.
4. Elija la dirección IP de Cisco ACS del campo IP de la interfaz local.
5. En el área izquierda de la navegación, haga clic el **modo AAA**.

6. Haga clic el botón de radio **TACACS+**. **Nota:** Por razones de seguridad, Cisco recomienda que usted elige **en el error del auth o ninguna respuesta del servidor del** retraso del permiso a la lista desplegable local. Elegir esta opción evita que usted sea bloqueado hacia fuera en caso de los problemas. Usted puede cambiar la opción que todo trabaja una vez correctamente.

[Paso 3. Configure el perfil correcto del shell en el ACS.](#)

Este paso describe cómo configurar el Cisco Secure ACS para volver los atributos correctos para determinar los privilegios del usuario en el WCS.

1. En el área izquierda de la navegación, **grupos del teclado**. Una lista de tipos de usuario aparece. Este ejemplo autentica a un usuario del tipo de usuario del embajador del pasillo.

- Haga clic el link de la **lista de tareas** al lado del grupo de **LobbyAmbassador**.

Nota: Usted debe configurar el rol del usuario (embajador del pasillo por este ejemplo) y una lista de tareas que pueden realizarse y los elementos de menú pueden acceder. Si usted utiliza una versión reciente del WCS, usted debe también configurar el dominio virtual que el usuario pertenecerá a.

- Elija la **administración > los dominios virtuales**.
- Haga clic la **exportación**.

Virtual Domain Custom Attributes

Please cut and paste the appropriate protocol specific data below into the custom/vendor-specific attribute field in access to.

TACACS+ Custom Attributes

```
virtual-domain0=root
virtual-domain1=w1
```

RADIUS Custom Attributes

```
Wireless-WCS:virtual-domain0=root
Wireless-WCS:virtual-domain1=w1
```

- Elija los **elementos > la autorización y los permisos de la directiva > Device Administration (Administración del dispositivo) > los perfiles del shell** para crear un nuevo perfil del shell.
- Ingrese un nombre significativo (tal como *WCS*), y después haga clic la lengüeta de los **atributos personalizados**.
- Configure los atributos como existen en el WCS.

Manually Entered

Attribute	Requirement	Value
role0	Mandatory	LobbyAmbassador
task0	Mandatory	Configure Guest Users
task1	Mandatory	Lobby Ambassador User Preferences
virtual-domain0	Mandatory	root

Nota: En las versiones del ACS anterior que la corrección 7 de la versión 5.2, usted puede ser que haga frente a los problemas cuando usted ingresa una tarea que contenga la palabra "alerta". Esto se repara en ACS versión posteriores. El mismo problema existe en las versiones del Identity Services Engine (ISE) anterior de 1.2. Aquí está un ejemplo de cómo ingresar manualmente los atributos: -type "role0" in the "Attribute" field
-type "LobbyAmbassador" in the Value field
-click the "add" button.

Etc... for the other attributes. **Nota:** En ACS 4, era copiar posible/goma la lista de atributos del WCS GUI al ACS 4 GUI. En ACS 5, deben ser ingresados uno por uno. En los NC y la infraestructura primera, el atributo se debe ingresar en una orden muy específica. La orden es dominio virtual, papel, y la lista de tareas. Si está ingresado en la orden incorrecta,

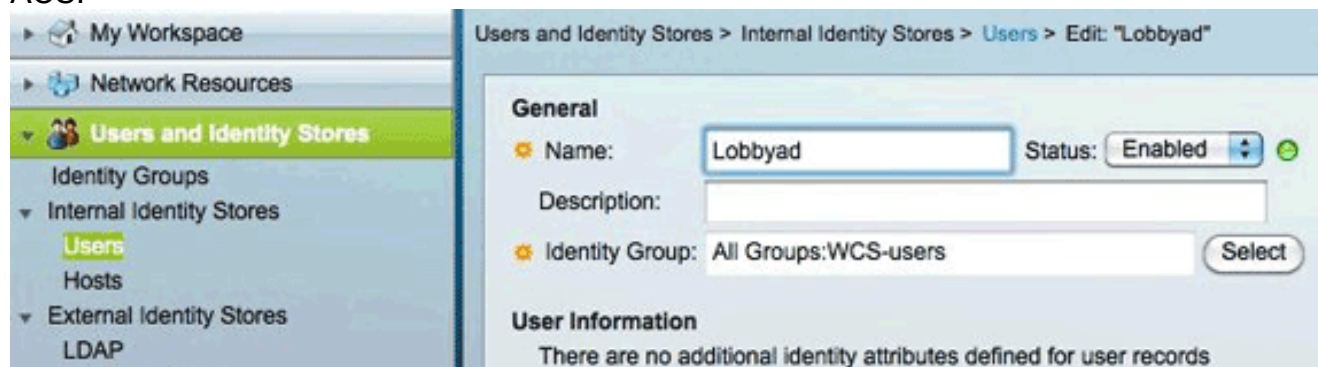
NCS/Prime rechaza la autenticación.NCS:virtual-domain0=ROOT-DOMAIN

NCS:role0=Super Users

NCS:task0=View Alerts and Events

Paso 4. Cisco Secure ACS de la configuración para volver los atributos.

1. Configure a un usuario (este ejemplo utiliza *Lobbyad*) como usuario en el ACS.



Nota: Para la facilidad de la configuración, este ejemplo agrega al usuario de Lobbyad al grupo de los *WCS-usuarios*. (Este paso es opcional.)

2. En políticas de acceso, bajo **dispositivo predeterminado los Admin > la autorización**, configuran una regla para hacer juego la autenticación WCS.



3. Si el Nombre de usuario pertenece a los *WCS-usuarios* agrupe, vuelva el perfil del shell de los *wcs* (que contiene los atributos del grupo).
4. Si usted quiere configurar otros tipos de usuarios (tales como administradores), usted debe configurar otro perfil del shell para volver diversos atributos. Desde entonces, usted debe agrupar a los administradores en un diverso grupo para distinguir y saber qué perfil del shell a volver.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- [Guía de configuración del Cisco Wireless Control System, versión 7.0.172.0](#)
- [Guía del usuario para el Cisco Secure Access Control System 5.2](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)