# La integración del ACS versión 5.4 con Motorola se va volando el ejemplo de configuración 5.X (AP)

## Contenido



## Introducción

Este documento proporciona un ejemplo de configuración con una versión 5.4 del Cisco Secure Access Control Server (ACS) para soportar autenticación de TACACS+, la autorización, y las estadísticas (AAA) en los reguladores inalámbricos y los Puntos de acceso de Motorola. En este documento, los atributos específicos del proveedor y los valores del Motorola se asignan a los grupos en el ACS para determinar el cada papel y los permisos de acceso de usuario. Los atributos y los valores se asignan al grupo con los servicios definidos por el usario y los protocolos habilitados en cada grupo.

## Prerrequisitos

## Requisitos

El ACS versión 5.x se debe conectar con las alas 5.x de Motorola.

## Componentes Utilizados

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

- ACS versión 5.4
- Alas 5.2

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.

# Configurar

## Configuración de ACS

### Tipos de dispositivo

Aquí está un ejemplo de cómo definir los dispositivos del ala 5 como tipos de dispositivo en una versión 5.x del Cisco Secure ACS. Los tipos de dispositivo permiten que los dispositivos sean agrupados en la versión 5.x del Cisco Secure ACS, se utiliza que cuando usted define las directivas de la autorización del dispositivo.

En el ACS GUI, navegue a los **recursos de red > a los grupos de dispositivos de red > al tipo de dispositivo**, y el tecleo **crea**.

Ingrese un **nombre** y una **descripción**, y seleccione a un **padre**. Haga clic en Submit (Enviar).

Esto crea a un **grupo de dispositivos de red** para los dispositivos de las soluciones de Motorola.

### Dispositivos de red y clientes AAA

Aquí está un ejemplo de cómo agregar un dispositivo del ala 5 como cliente AAA en la versión 5.x del Cisco Secure ACS.

En el Cisco Secure ACS, navegue a los **recursos de red > a los dispositivos de red y a los clientes AAA**, y el tecleo **crea**:

Ingrese un **nombre** para los reguladores sin hilos, y seleccione una **ubicación**. Asigne el **tipo de dispositivo** creado en la sección anterior, y marque el checkbox **TACACS+**. Ingrese un **secreto compartido**, y haga clic el botón de radio al lado de la opción apropiada del **IP Address**. En este

ejemplo, el **intervalo de direcciones IP por la máscara** se selecciona, y se define la subred del IPv4 que los reguladores de la Tecnología inalámbrica están conectados con (**192.168.20.0/24**). El tecleo **somete** una vez que usted ingresa toda la información.

Esto define los reguladores inalámbricos como los **dispositivos de red y clientes AAA**:

### Grupos de la identidad

En este ejemplo, definen a dos grupos, MotorolaRO Nombrado y MotorolaRW. Asignan los usuarios asignados al grupo de MotorolaRO al papel del monitor y a los permisos de Acceso Web concedidos, mientras que asignan al papel del superusuario y concedieron los usuarios asignados al grupo de MotorolaRW todos los permisos de acceso.

Navegue a los **usuarios y la identidad salva > los grupos de la identidad > crea**:

Ingrese un **nombre** y una **descripción** para el grupo de acceso del read only, y el tecleo **somete.**

Cree a un segundo grupo. Ingrese un **nombre** y una **descripción** para el grupo de acceso de lectura/grabación, y el tecleo **somete**.

Usted ahora ha creado a dos **grupos de la identidad**.

### Perfiles del shell

Aquí está un ejemplo de cómo definir los perfiles del shell en una versión 5.x del Cisco Secure ACS. En este ejemplo, dos descascan los perfiles, MOTO Nombrado RO y MOTO RW, se definen con los atributos que determinan el papel y los permisos de acceso que asignan cada usuario de administración. El nombre de cada perfil del shell debe hacer juego el nombre autenticación de TACACS+ del servicio definido en la directiva TACACS+ AAA.

Navegue a los **elementos > a la autorización y a los permisos de la directiva > Device Administration (Administración del dispositivo) > los perfiles del shell**. El tecleo **crea**.

En la **ficha general**, defina los servicios requeridos y los protocolos TACACS+ para agregar. Usted puede utilizar los servicios y los protocolos actuales o crear sus los propio. Este ejemplo define los servicios y los protocolos bajo el nombre MOTO RO para proporcionar el acceso del read only para irse volando 5 dispositivos:

En las **tareas comunes** tabule, fije el **privilegio máximo a los parásitos atmosféricos**, y seleccione un valor de **1.**

En la lengueta de los **atributos personalizados**, en los campos del **atributo** y de **valor de atributo**, defina los atributos que se asignarán al usuario. En este ejemplo, asignan los usuarios del read only al papel del monitor y a los permisos de Acceso Web concedidos. Haga clic en Submit (Enviar).

Cree un nuevo **perfil del shell**. En la **ficha general**, defina los servicios requeridos y los protocolos TACACS+ para agregar. Usted puede utilizar los servicios y los protocolos actuales o crear sus los propio. Este ejemplo define los servicios y los protocolos, MOTO Nombrados RW, que proporcionan el acceso de lectura/grabación para los dispositivos del ala 5:

En las **tareas comunes** tabule, fije el **privilegio máximo a los parásitos atmosféricos**, y seleccione un valor de **1.**

En la lengueta de los **atributos personalizados**, en los campos del **atributo** y de **valor de atributo**, defina los atributos que se asignarán al usuario. En este ejemplo, asignan al papel del superusuario y concedieron los usuarios de lectura/grabación todos los permisos de acceso. Haga clic en Submit (Enviar).

Usted ahora ha creado los **perfiles del shell** nombrados MOTO RO y MOTO RW.

### Perfiles de la autorización del dispositivo

Aquí está un ejemplo de cómo definir las directivas de la autorización del dispositivo en una versión 5.x del Cisco Secure ACS. Las directivas de la autorización del dispositivo determinan el perfil del shell que asignan cada usuario de administración basado en el tipo de dispositivo que pide la autenticación, la ubicación, y la calidad de miembro de grupo de la identidad. En este ejemplo, se definen dos directivas de la autorización del dispositivo, MotorolaRO Nombrado y MotorolaRW.

En el Cisco Secure ACS, navegue a las **políticas de acceso > al dispositivo del valor por defecto Admin > autorización > personalizan**:

Agregue las condiciones del personalizar nombradas **Identity Group**, **NDG: Ubicación**, **NDG: Tipo de dispositivo**, y **protocolo**. Bajo personalice los resultados, agregue el **perfil del shell**, y haga clic la **AUTORIZACIÓN**:

El tecleo **crea**. En el **campo de nombre**, ingrese **MotorolaRO**, y seleccione al **grupo de la identidad**, **NDG: Ubicación**, y **tipo de NDGevice**. Fije el protocolo a **Tacacs**, y seleccione el perfil del shell nombrado **MOTO RO**. Haga Click en OK:

El tecleo **crea**. En el **campo de nombre**, ingrese **MotorolaRW**, y seleccione al **grupo de la identidad**, **NDG: Ubicación**, y **tipo de NDGevice**. Fije el protocolo a **Tacacs**, y seleccione el perfil del shell nombrado **MOTO RW**. Haga Click en OK:

Usted ahora ha creado las **directivas de la autorización del dispositivo** nombradas MotorolaRO y MotorolaRW:

## Las soluciones de Motorola se van volando la configuración 5.2

### Directivas AAA TACACS

La directiva AAA TACACS define la configuración del cliente TACACS+ en un dispositivo del ala 5. Cada directiva AAA TACACS puede contener hasta dos entradas del servidor de AAA TACACS+ además de los nombres autenticación de TACACS+ del servicio y de los protocolos definidos en el Cisco Secure ACS. La directiva TACACS+ AAA también determina la información que se remite al servidor de contabilidad.

Este ejemplo de la directiva AAA TACACS define un Cisco Secure ACS para TACACS+ AAA, define los servicios TACACS+ y los protocolos nombrados MOTO RO y MOTO RW, y habilita las

estadísticas del comando CLI y de la sesión.

### Ejemplo de la directiva AAA TACACS

```
aaa-tacacs-policy CISCO-ACS-SERVER

authentication server 1 host 192.168.10.21 secret 0 hellomoto

authorization server 1 host 192.168.10.21 secret 0 hellomoto

accounting server 1 host 192.168.10.21 secret 0 hellomoto

authentication service MOTO protocol RO

authentication service MOTO protocol RW

accounting commands

accounting session

!
```

### Políticas de administración

Una vez que se define una directiva AAA TACACS+, debe ser asignada a una o más políticas de administración antes de que se utilice el TACACS+. Las políticas de administración determinan las interfaces de administración que se habilitan en cada dispositivo del ala 5, usuarios administradores locales, papeles y permisos de acceso, y los servidores externos del RADIO o TACACS+ usados para autenticar a los usuarios administradores.

Por abandono, cada dispositivo del ala 5 se asigna a una política de administración, nombrada el valor por defecto, que se asigna con el uso de los perfiles. El TACACS+ se puede habilitar en la política de administración predeterminada o cualquier política de administración definida por el usario.

La mayoría de las instalaciones típicas incluyen las políticas de administración separadas para los reguladores inalámbricos y los Puntos de acceso. Se recomiendan las políticas de administración separadas, porque diferencian los requerimientos de administración y las interfaces para cada dispositivo. En este caso, el TACACS+ se debe habilitar en cada política de administración para habilitar el TACACS+ en los reguladores inalámbricos y los Puntos de acceso.

Los ejemplos de la política de administración en la siguiente sección habilitan TACACS+ AAA en las políticas de administración definidas por el usario que se asignan a los reguladores inalámbricos y a los Puntos de acceso. El retraso TACACS+ a la autenticación local también se habilita en caso que un dispositivo del ala 5 no pueda alcanzar a ninguna servidores para autentificación definida TACACS+.

### Ejemplos de la política de administración

```
!

management-policy CONTROLLER-MANAGEMENT
```

```
no http server

https server

ssh

user admin password 0 hellomoto role superuser access all

snmp-server user snmptrap v3 encrypted des auth md5 0 hellomoto

snmp-server user snmpoperator v3 encrypted des auth md5 0 hellomoto

snmp-server user snmpmanager v3 encrypted des auth md5 0 hellomoto

aaa-login tacacs fallback

aaa-login tacacs authorization

aaa-login tacacs accounting

aaa-login tacacs policy CISCO-ACS-SERVER

!

!

management-policy AP-MANAGEMENT

ssh

user admin password 0 hellomoto role superuser access all

aaa-login tacacs fallback

aaa-login tacacs authorization

aaa-login tacacs accounting

aaa-login tacacs policy CISCO-ACS-SERVER

!
```

# Verificación

Esta sección proporciona los pasos necesarios requeridos para validar TACACS+ AAA. En este ejemplo, dos cuentas de usuario se definen en cada Cisco Secure ACS y se asignan a los grupos apropiados. La calidad de miembro del grupo de usuario determina el papel y los permisos de acceso asignados al usuario de administración.

```
Username           Role          Access Permissions
-------------------------------------------------
monitor Monitor Web
super user Superuser all
```

## Asignación del papel

Esta sección proporciona los pasos de verificación requeridos para verificar las asignaciones de la autenticación y del papel.

En la red UI, login al regulador inalámbrico con el nombre de usuario y contraseña del **monitor**:

Autentican, se autorizan, y se asignan al usuario al papel del monitor, que proporciona el acceso del read only en el regulador inalámbrico. Seleccione la **configuración > los dispositivos**, e intente editar un dispositivo.

> Nota: Ningún edite las funciones está disponible, porque el usuario es acceso permitido del read only.

Acceso en el dispositivo: (Solamente el **botón View Button** está disponible; **el botón Delete Button** es greyed-hacia fuera.)

En la red UI, login al regulador inalámbrico con el nombre de usuario y contraseña del **superusuario**:

Autentican, se autorizan, y se asignan al usuario al papel del superusuario, que proporciona el acceso total en el regulador inalámbrico. Seleccione la **configuración > los dispositivos**, e intente editar un dispositivo.

> Nota: **El botón Edit** está disponible ahora, porque el usuario es acceso total permitido en el dispositivo.

# Troubleshooting

En la versión 5.X del Cisco Secure ACS, navegue a **monitorear y a los informes > Visualizador a la supervisión y al informe del lanzamiento > los informes > protocolo > autenticación de TACACS selectos del catálogo >AAA > ejecutado**.

Esto presenta los resultados para todo el haber pasado y autenticaciones fallidas para los usuarios e incluye la razón del error. Haga clic el botón de la **lupa** (detalles) para otros detalles.