Configuración de RADIUS en los switches gestionados de la serie 200/300

Objetivo

El servicio de usuario de acceso telefónico de autorización remota (RADIUS) es un servicio de seguridad que se utiliza para la autenticación de usuarios en redes con una arquitectura de seguridad centralizada. Los switches gestionados de la serie 200/300 pueden actuar como un cliente RADIUS en la red y, junto con un servidor RADIUS, puede establecer un sistema centralizado para la autenticación de usuarios en la red. En este artículo se explica cómo configurar un servidor RADIUS y aplicar métodos de autenticación en los switches gestionados de la serie 200/300.

Dispositivos aplicables | Versión de software

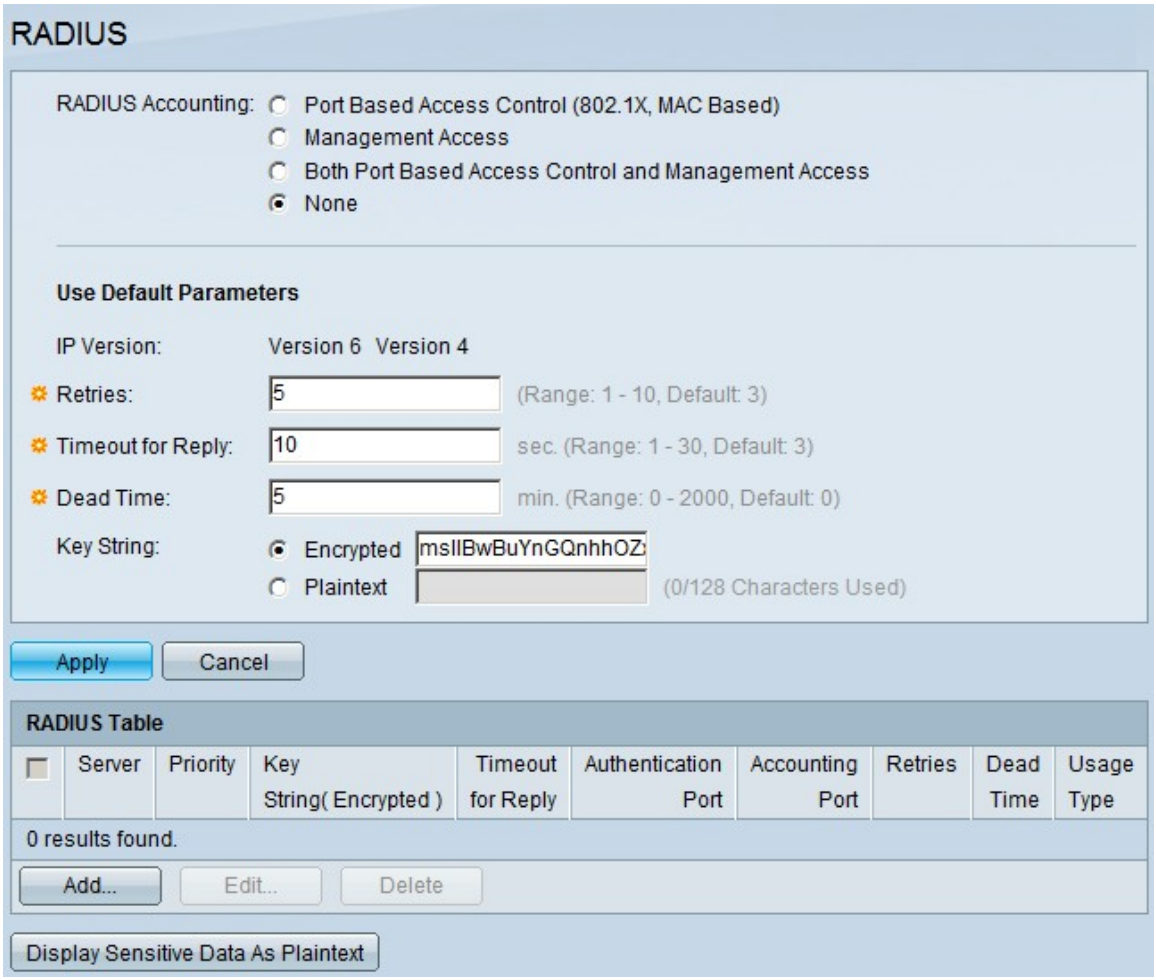
- SF/SG serie 200 - 1.2.9.x
- SF/SG serie 300 - 1.2.9.x

Configuración predeterminada de RADIUS

Esta sección le guía a través de la configuración predeterminada de un servidor RADIUS. Estos valores predeterminados se pueden utilizar para cualquier servidor RADIUS que desee agregar a un switch.

Paso 1

Inicie sesión en la utilidad de configuración web y elija **Security > RADIUS**. Se abre la página *RADIUS*:



Las imágenes de este artículo proceden de un switch modelo SG300.

Paso 2

En el campo RADIUS Accounting (Contabilidad RADIUS), pulse en una de las siguientes opciones:

- Control de acceso basado en puerto (802.1x, basado en MAC): para utilizar el servidor RADIUS para la contabilización de puertos 802.1x.
- Management Access (Acceso a la gestión): Para utilizar el servidor RADIUS para la contabilización de inicio de sesión.
- Control de acceso basado en puerto y acceso a la administración: para utilizar el servidor RADIUS tanto para 802.1x como para la contabilidad de inicio de sesión.
- Ninguno: para no utilizar el servidor RADIUS para la administración de cuentas.

Radius Accounting no está disponible en los switches de la serie SG200.

Paso 3

En la sección Use Default Parameters, en el campo Retries, ingrese el número de reintentos que el switch hizo para autenticar el servidor RADIUS.

Paso 4

En el campo Timeout for Reply (Tiempo de espera para respuesta), introduzca el tiempo en

segundos para cada intento de autenticación realizado en el servidor RADIUS.

Paso 5

En el campo Dead Time (Tiempo muerto), ingrese el tiempo en minutos antes de que el switch declare un servidor RADIUS no responsivo como muerto y se mueva al siguiente servidor disponible para intentar la conexión.

Paso 6

En el campo Key String (Cadena de clave), introduzca la clave utilizada para la autenticación y el cifrado entre el switch y el servidor RADIUS. Esta clave debe coincidir tanto en el servidor RADIUS como en el switch. Haga clic en una de las siguientes opciones:

- Cifrado: si tiene una clave cifrada de otro dispositivo, introdúzcala.
- Texto sin formato: si no dispone de una clave cifrada de otro dispositivo, introduzca la clave como texto sin formato.

Paso 7

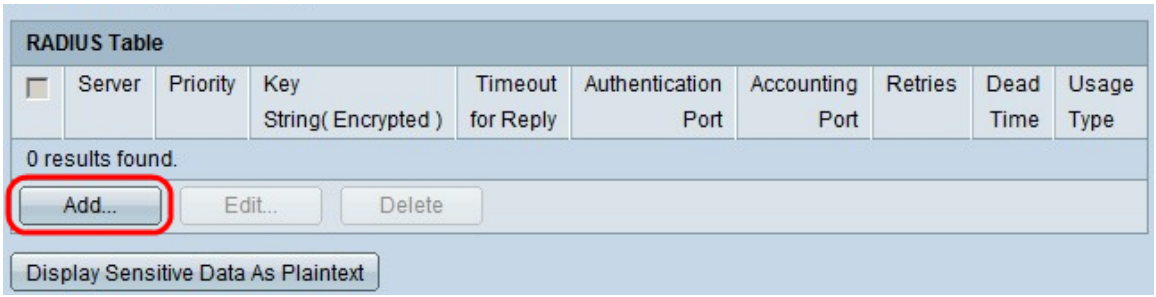
Haga clic en **Apply** para guardar estos valores predeterminados y hacerlos disponibles para un servidor RADIUS.

Agregar/editar un servidor RADIUS

En esta sección, se proporciona un procedimiento paso a paso que explica cómo agregar o editar un servidor RADIUS a un 200/300 Series Managed Switches.

Paso 1

Inicie sesión en la utilidad de configuración web y elija **Security > RADIUS**. Se abre la página *RADIUS*:



Paso 2

En la sección Tabla RADIUS, haga clic en **Agregar**. Aparece la ventana *Add Radius Server*.

Para editar un servidor RADIUS actual, haga clic en **Editar** y edite las propiedades deseadas del servidor RADIUS.

Paso 3

En el campo Definición de servidor, haga clic en una de las siguientes opciones:

- By Name (Por nombre): Indica si el servidor RADIUS está definido con un nombre.
- By IP Address (Por dirección IP): Si el servidor RADIUS está definido con una dirección IP.

Paso 4

En el campo IP Version, haga clic en **Version 6** o en **Version 4** como el tipo de dirección IP del servidor RADIUS.

Paso 5

Si elige la **Versión 6** como dirección IP en el tipo de dirección IPv6, haga clic en una de las siguientes opciones:

- Link Local (Enlace local): Dirección IPv6 que sólo identifica hosts en un único enlace de red.
- Global: dirección IPv6 a la que se puede acceder desde otras redes.

Paso 6

Si elige Link Local como tipo de dirección IPv6, en la lista desplegable Link Local Interface (Interfaz local de enlace), seleccione la interfaz adecuada.

Paso 7

En el campo Server IP Address/Name (Dirección/nombre IP del servidor), introduzca la dirección IP o el nombre del servidor RADIUS.

Paso 8

En el campo Priority (Prioridad), introduzca la prioridad del servidor RADIUS que utilizará el switch. El servidor con la prioridad más alta se consulta primero en el switch. Cero (0) proporciona la prioridad más alta.

Paso 9

En el campo Cadena de clave, haga clic en una de las siguientes opciones:

- Use Default (Utilizar valor predeterminado): para utilizar la clave predeterminada para la autenticación.
- Definido por el usuario (cifrado): si está disponible, introduzca la clave cifrada.
- Definido por el usuario (texto sin formato): si no está disponible, introduzca la clave como texto sin formato.

Paso 10

En el campo Tiempo de espera para respuesta, haga clic en una de las siguientes opciones:

- Use Default (Utilizar valor predeterminado): para utilizar el valor predeterminado.

- User Defined (Definido por el usuario): Introduzca el número en segundos que el switch espera cada intento de conexión al servidor RADIUS.

Paso 11

En el campo Puerto de autenticación, ingrese el puerto UDP que el servidor RADIUS utiliza para la autenticación.

Paso 12

En el campo Puerto de Contabilización, ingrese el puerto UDP que el servidor RADIUS utiliza para la contabilización.

Paso 13

En el campo Reintentos, haga clic en una de las siguientes opciones:

- Use Default (Utilizar valor predeterminado): para utilizar el valor predeterminado.
- Definido por el usuario: para utilizar un valor diferente. Introduzca el número de intentos que realiza el switch antes de que se considere que se ha producido una conexión fallida al servidor RADIUS.

Paso 14

En el campo Tiempo muerto, haga clic en una de las siguientes opciones:

- Use Default (Utilizar valor predeterminado): para utilizar el valor predeterminado.
- Definido por el usuario: para utilizar un valor diferente. Introduzca el tiempo en minutos antes de que el switch declare muerto un servidor RADIUS que no responde y se mueva al siguiente servidor disponible para intentar la conexión.

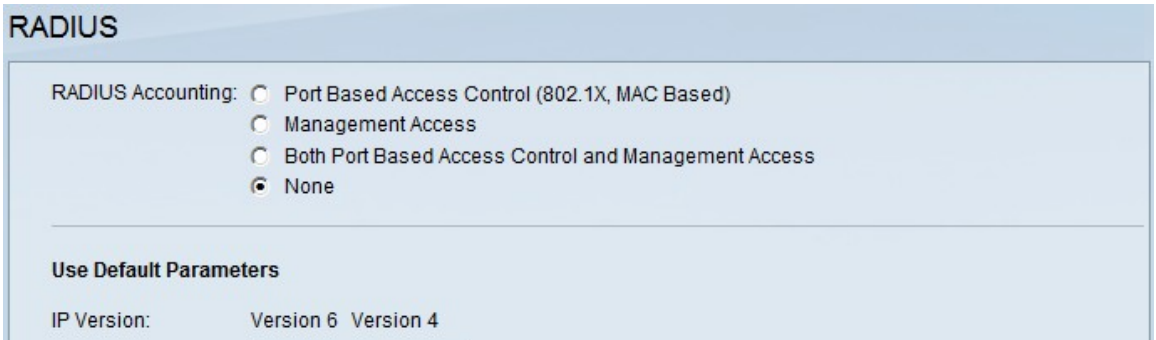
Paso 15

En el campo Tipo de uso, haga clic en una de las siguientes opciones:

- Login: autentica a los administradores del switch.
- 802.1x: El servidor RADIUS comprobará las credenciales de seguridad de los usuarios que soliciten acceso a la red en función del esquema de control de acceso a la red (PNAC) basado en puertos 802.1x.
- Todos: utiliza ambos tipos de autenticaciones.

Paso 16

Haga clic en Apply (Aplicar).



Paso 17

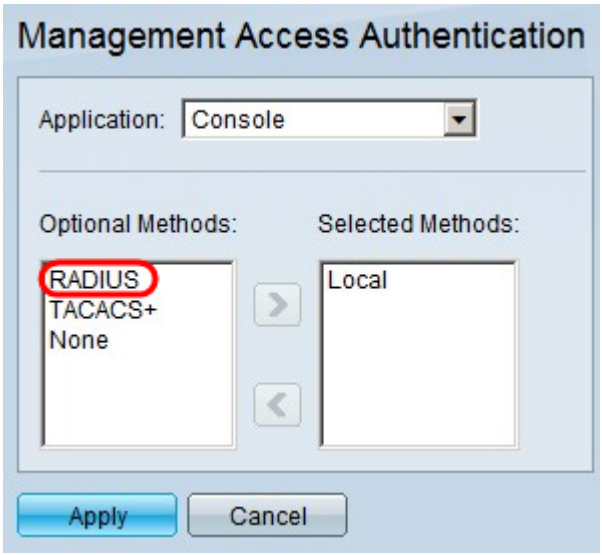
(Opcional) Para eliminar un servidor RADIUS, en la sección Tabla RADIUS, active la casilla de verificación del servidor RADIUS que desea eliminar y haga clic en **Eliminar**.

Autenticación RADIUS

Una vez que el servidor RADIUS está configurado correctamente, debe autenticarlo en el switch. Esta sección explica cómo autenticar un servidor RADIUS en los 200/300 Series Managed Switches.

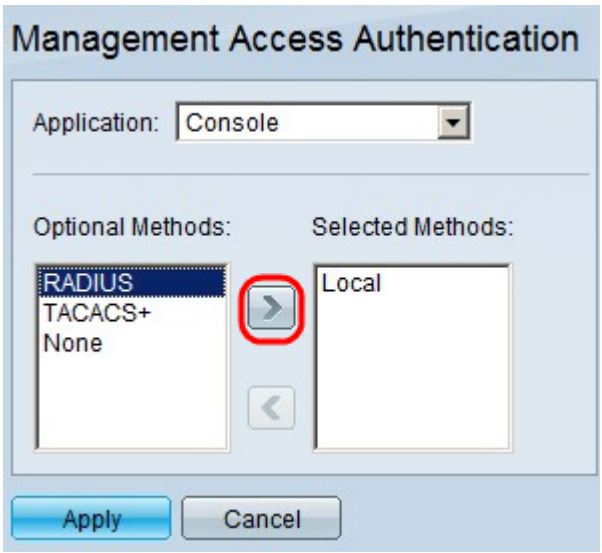
Paso 1

Inicie sesión en la utilidad de configuración web y elija **Security > Management Access Authentication**. Se abre la página *Management Access Authentication*:



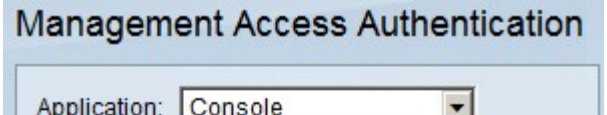
Paso 2

En la lista Métodos opcionales, elija RADIUS.



Paso 3

Haga clic en el botón **>**.



Paso 4

Haga clic en Apply (Aplicar).

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).