Autenticación de acceso a la gestión en los switches gestionados serie 200/300

Objetivo

Los modos de acceso de administración como SSH, Console, Telnet, HTTP y HTTPS permiten que un usuario acceda a un dispositivo. Se puede exigir autenticación a los usuarios para mejorar la seguridad. Los switches gestionados serie 200 y 300 pueden autenticarse localmente o en un servidor TACACS+ o RADIUS. Este documento explica cómo asignar un método de autenticación en los switches gestionados serie 200 y 300.

Dispositivos aplicables

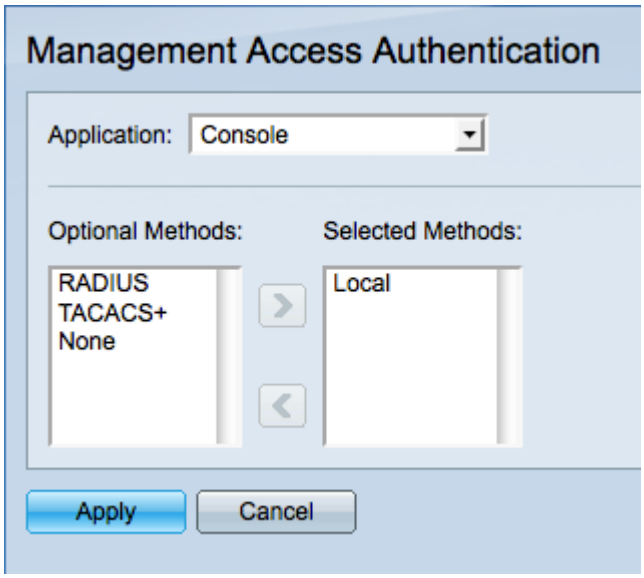
Switches gestionados · SF/SG serie 200 y SF/SG serie 300

Versión del software

•1.3.0.62

Autenticación de acceso a la gestión

Paso 1. Inicie sesión en la utilidad de configuración web y elija **Security > Management Access Authentication**. Se abre la página *Autenticación de Acceso a la Administración*:



Paso 2. Elija el tipo de aplicación al que desea asignar la autenticación en la lista desplegable Aplicación. Las aplicaciones posibles son:

Consola ·: permite administrar el switch con una interfaz de consola. Permite conectarse al switch y realizar algunas configuraciones incluso si no se conoce la dirección IP del switch.

·Telnet: protocolo de comunicación basado en caracteres que permite conectarse de forma remota al switch a través de una red TCP/IP. No se recomienda Telnet debido a la falta de cifrado.

·Secure Telnet (SSH): realiza las mismas funciones que telnet más cifrado. Se recomienda SSH para conexiones remotas.

·HTTP: protocolo que permite acceder a la interfaz gráfica de usuario (GUI) del switch. Esto contrasta con Telnet y SSH que se basan en el símbolo del sistema.

·HTTP seguro (HTTPS): realiza las mismas funciones que HTTP con la adición de una comunicación segura.

Paso 3. Elija un método de autenticación de la lista de Métodos opcionales y, a continuación, haga clic en el botón > para moverlo a la lista Métodos seleccionados. Diferentes métodos proporcionan diferentes niveles de seguridad.

Nota: El orden en que se seleccionan los métodos de autenticación es el orden en que se produce la autenticación de usuario. Si se selecciona RADIUS antes de local, el dispositivo intentará autenticar al usuario mediante un servidor RADIUS antes del método local.

·RADIUS: RADIUS cifra sólo la contraseña. La autenticación se encuentra en un servidor RADIUS y requiere un servidor RADIUS configurado.

·TACACS+: TACACS+ cifra todos los datos durante la autenticación. La autenticación se encuentra en un servidor TACACS+ y requiere un servidor TACACS+ configurado.

·Ninguno: la autenticación no es necesaria para acceder al switch.

·Local: la información del usuario se verifica mediante la información almacenada en el switch.

Paso 4. Haga clic en Aplicar para guardar los parámetros de autenticación o haga clic en Cancelar para cancelar los cambios.