Configuración de la autenticación de servidor de Secure Shell (SSH) en un switch

Objetivo

Este artículo proporciona instrucciones sobre cómo configurar la autenticación del servidor en un switch administrado, no cómo conectarse al switch. Para un artículo sobre la conexión a un switch a través de SSH + masilla, haga clic aquí para ver ese artículo.

Secure Shell (SSH) es un protocolo que proporciona una conexión remota segura a dispositivos de red específicos. Esta conexión proporciona una funcionalidad similar a una conexión Telnet, excepto que está cifrada. SSH permite al administrador configurar el switch a través de la interfaz de línea de comandos (CLI) con un programa de terceros. El switch actúa como un cliente SSH que proporciona funciones SSH a los usuarios de la red. El switch utiliza un servidor SSH para proporcionar servicios SSH. Cuando la autenticación del servidor SSH está inhabilitada, el switch toma cualquier servidor SSH como confiable, lo que disminuye la seguridad en su red. Si el servicio SSH está activado en el switch, se mejora la seguridad.

Dispositivos aplicables

- Serie Sx200
- Serie Sx300
- Serie Sx350
- Serie SG350X
- Serie Sx500
- Serie Sx550X

Versión del software

- 1.4.5.02 - Series Sx200, Sx300 y Sx500
- 2.2.0.66 - Serie Sx350, Serie SG350X, Serie Sx550X

Configuración de la Autenticación del Servidor SSH

Activar servicio SSH

Cuando la autenticación del servidor SSH está habilitada, el cliente SSH que se ejecuta en el dispositivo autentica el servidor SSH mediante el siguiente proceso de autenticación:

- El dispositivo calcula la huella dactilar de la clave pública recibida del servidor SSH.
- El dispositivo busca en la tabla Servidores de Confianza SSH la dirección IP y el nombre de host del servidor SSH. Se puede producir uno de los tres resultados siguientes:

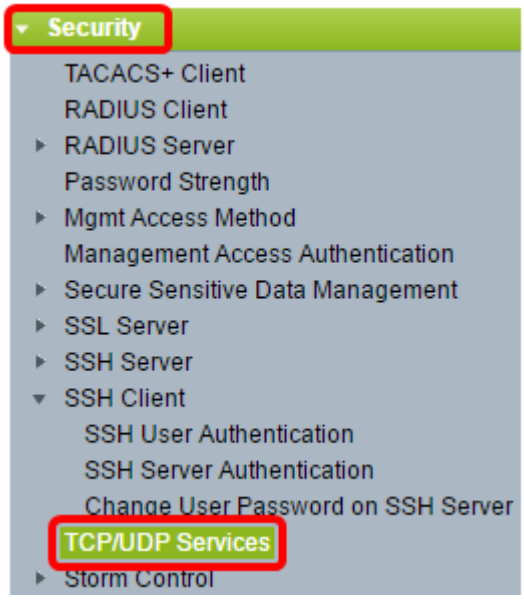
1. Si se encuentra una coincidencia para la dirección y el nombre de host del servidor y su huella dactilar, el servidor se autentica.
2. Si se encuentra una dirección IP y un nombre de host coincidentes, pero no hay ninguna

huella dactilar coincidente, la búsqueda continúa. Si no se encuentra ninguna huella dactilar coincidente, la búsqueda se completa y la autenticación falla.

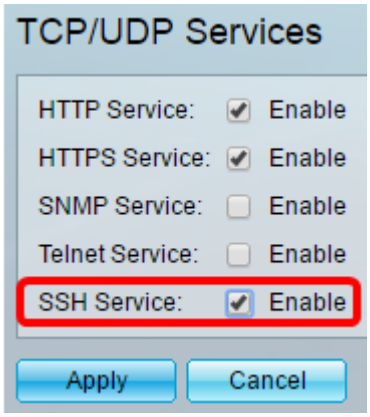
3. Si no se encuentra ninguna dirección IP y nombre de host coincidentes, la búsqueda se completa y la autenticación falla.
   - Si la entrada para el servidor SSH no se encuentra en la lista de servidores de confianza, el proceso falla.

Nota: Para soportar la configuración automática de un switch listo para usar con la configuración predeterminada de fábrica, la autenticación del servidor SSH está inhabilitada por defecto.

Paso 1. Inicie sesión en la utilidad basada en Web y seleccione **Security > TCP/UDP Services**.



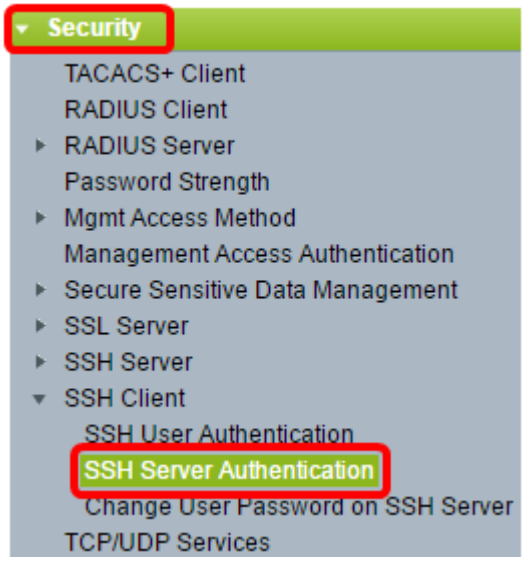
Paso 2. Marque la casilla de verificación **SSH Service** para habilitar el acceso del símbolo del sistema de switches a través de SSH.



Paso 3. Haga clic en **Apply** para habilitar el servicio SSH.

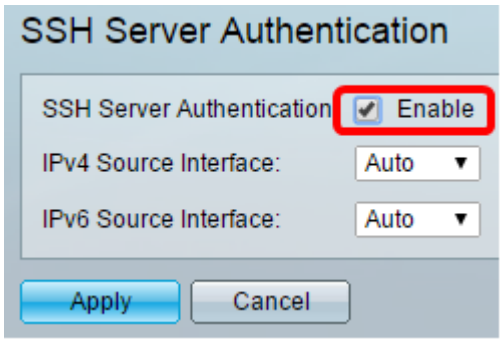
Configuración de la Autenticación del Servidor SSH

Paso 1. Inicie sesión en la utilidad basada en web y elija **Security > SSH Client > SSH Server Authentication**.

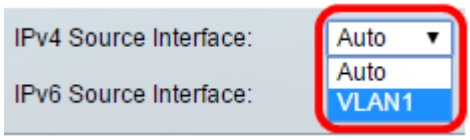


Nota: Si dispone de un Sx350, SG300X o Sx500X, cambie al modo avanzado seleccionando **Avanzado** en la lista desplegable Modo de visualización.

Paso 2. Marque la casilla de verificación **Enable** SSH Server Authentication para habilitar la autenticación del servidor SSH.

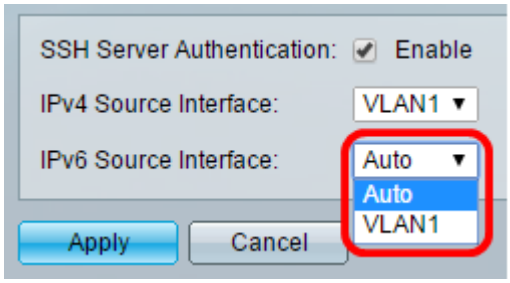


Paso 3. (Opcional) En la lista desplegable Interfaz de origen IPv4, elija la interfaz de origen cuya dirección IPv4 se utilizará como dirección IPv4 de origen para los mensajes utilizados en la comunicación con los servidores SSH IPv4.



Nota: Si se elige la opción Auto (Automático), el sistema toma la dirección IP de origen de la dirección IP definida en la interfaz saliente. En este ejemplo, se elige VLAN1.

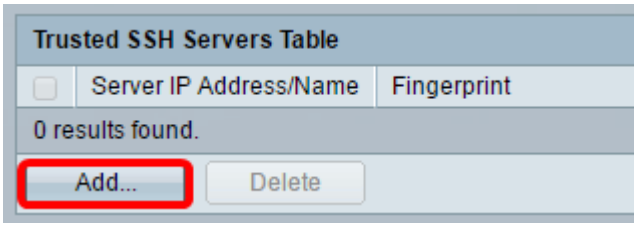
Paso 4. (Opcional) En la lista desplegable IPv6 Source Interface (Interfaz de origen IPv6), elija la interfaz de origen cuya dirección IPv6 se utilizará como dirección IPv6 de origen para los mensajes utilizados en la comunicación con los servidores SSH IPv6.



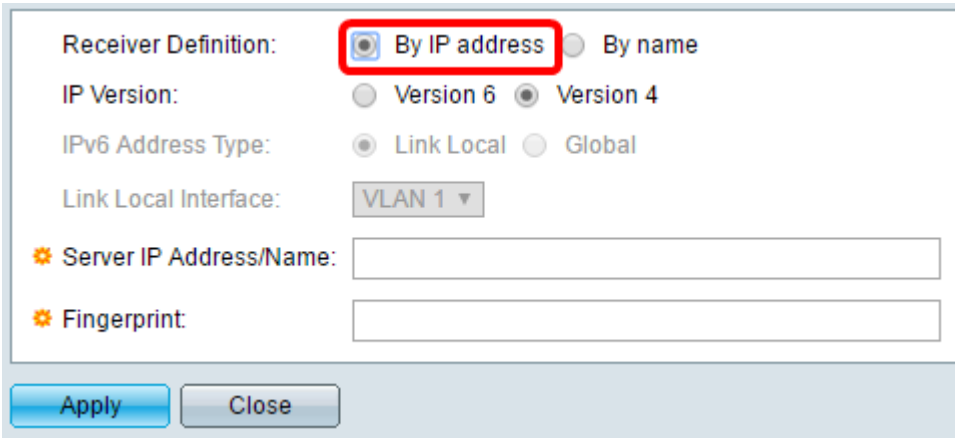
Nota: En este ejemplo, se elige la opción Automático. El sistema tomará la dirección IP de origen de la dirección IP definida en la interfaz saliente.

Paso 5. Haga clic en Apply (Aplicar).

Paso 6. Para agregar un servidor de confianza, haga clic en **Agregar** en la Tabla Servidores SSH de Confianza.



Paso 7. En el área Definición del Receptor, haga clic en uno de los métodos disponibles para definir el servidor SSH:

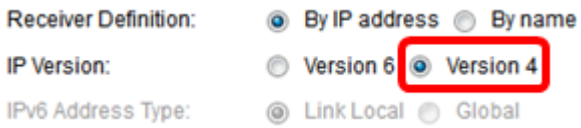


Las opciones son:

- By IP Address (Por dirección IP): esta opción permite definir el servidor SSH con una dirección IP.
- By Name : esta opción permite definir el servidor SSH con un nombre de dominio completo.

Nota: En este ejemplo, se elige Por dirección IP. Si selecciona Por nombre, vaya al paso 11.

Paso 8. (Opcional) Si selecciona Por dirección IP en el Paso 6, haga clic en la versión IP del servidor SSH en el campo IP Version (Versión IP).



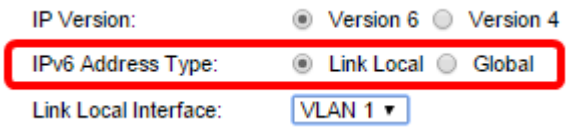
Las opciones disponibles son:

- Versión 6: esta opción permite introducir una dirección IPv6.
- Versión 4: esta opción permite introducir una dirección IPv4.

Nota: En este ejemplo, se elige la versión 4. El botón de opción IPv6 sólo está disponible si se ha configurado una dirección IPv6 en el switch.

Paso 9. (Opcional) Si ha seleccionado la versión 6 como versión de la dirección IP en el

paso 7, haga clic en el tipo de dirección IPv6 en Tipo de dirección IPv6.

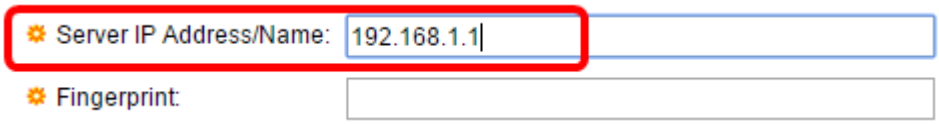


Las opciones disponibles son:

- Enlace local: la dirección IPv6 identifica de forma exclusiva los hosts en un único enlace de red. Una dirección local de link tiene un prefijo de FE80, no es enrutable y se puede utilizar para la comunicación solamente en la red local. Sólo se admite una dirección local de vínculo. Si existe una dirección local de link en la interfaz, esta entrada reemplaza la dirección en la configuración. Esta opción está seleccionada de forma predeterminada.
- Global: la dirección IPv6 es una unidifusión global visible y accesible desde otras redes.

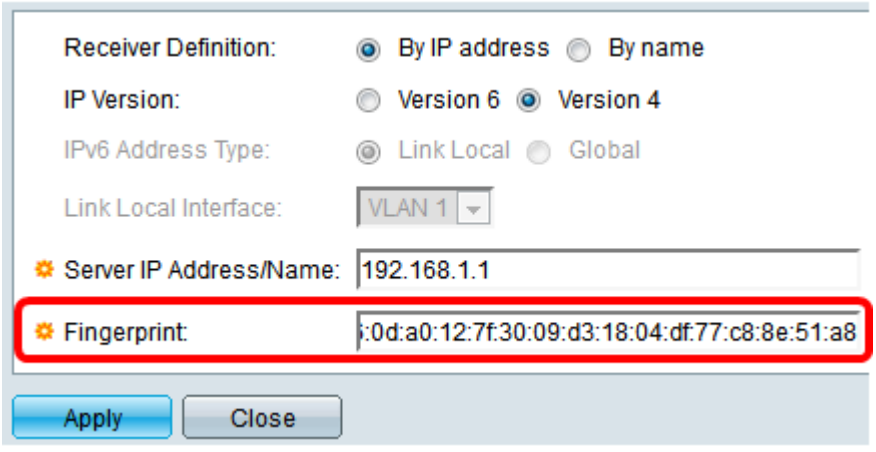
Paso 10. (Opcional) Si ha seleccionado Enlace local como tipo de dirección IPv6 en el paso 9, seleccione la interfaz adecuada en la lista desplegable Interfaz local de enlace.

Paso 11. En el campo *Server IP Address/Name*, ingrese la dirección IP o el nombre de dominio del servidor SSH.



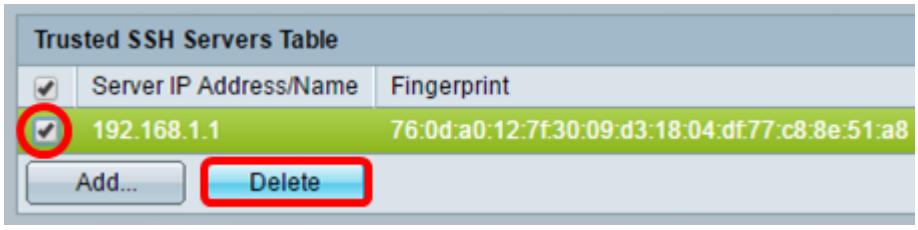
Nota: En este ejemplo, se introduce una dirección IP.

Paso 12. En el campo *Fingerprint*, ingrese la huella digital del servidor SSH. Una huella digital es una clave cifrada que se utiliza para la autenticación. En este caso, la huella dactilar se utiliza para autenticar la validez del servidor SSH. Si existe una coincidencia entre la dirección/nombre IP del servidor y la huella dactilar, el servidor SSH se autentica.

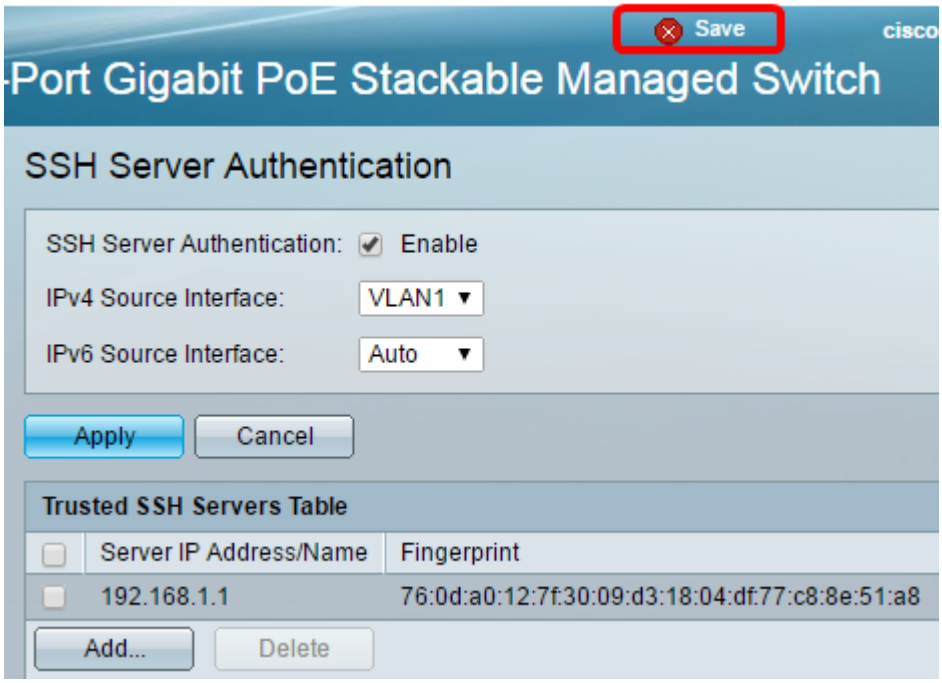


Paso 13. Haga clic en **Apply** para guardar la configuración.

Paso 14. (Opcional) Para eliminar un servidor SSH, active la casilla de verificación del servidor que desea eliminar y, a continuación, haga clic en **Eliminar**.



Paso 15. (Opcional) Haga clic en el botón **Guardar** en la parte superior de la página para guardar los cambios en el archivo de configuración de inicio.



Ahora debería haber configurado los parámetros de autenticación del servidor SSH en su switch administrado.

Ver un vídeo relacionado con este artículo...

[Haga clic aquí para ver otras charlas sobre tecnología de Cisco]

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).