

# Autenticación SSH en un switch Cisco Business 350

## Objetivo

En este artículo se proporcionan instrucciones sobre cómo configurar la autenticación del servidor en un switch Cisco Business de la serie 350.

## Introducción

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 capacidades SSH a los usuarios dentro de la red. El switch utiliza un servidor SSH para proporcionar servicios SSH. Cuando se inhabilita la autenticación del servidor SSH, el switch toma cualquier servidor SSH como de confianza, lo que disminuye la seguridad en su red. Si el servicio SSH está habilitado en el switch, la seguridad se mejora.

## Dispositivos aplicables | Versión de software

- CBS350 ([Ficha técnica](#)) | 3.0.0.69 ([Descargar última](#))
- CBS350-2X ([Ficha técnica](#)) | 3.0.0.69 ([Descargar última](#))
- CBS350-4X ([Ficha técnica](#)) | 3.0.0.69 ([Descargar última](#))

## Configurar la configuración de autenticación del servidor SSH

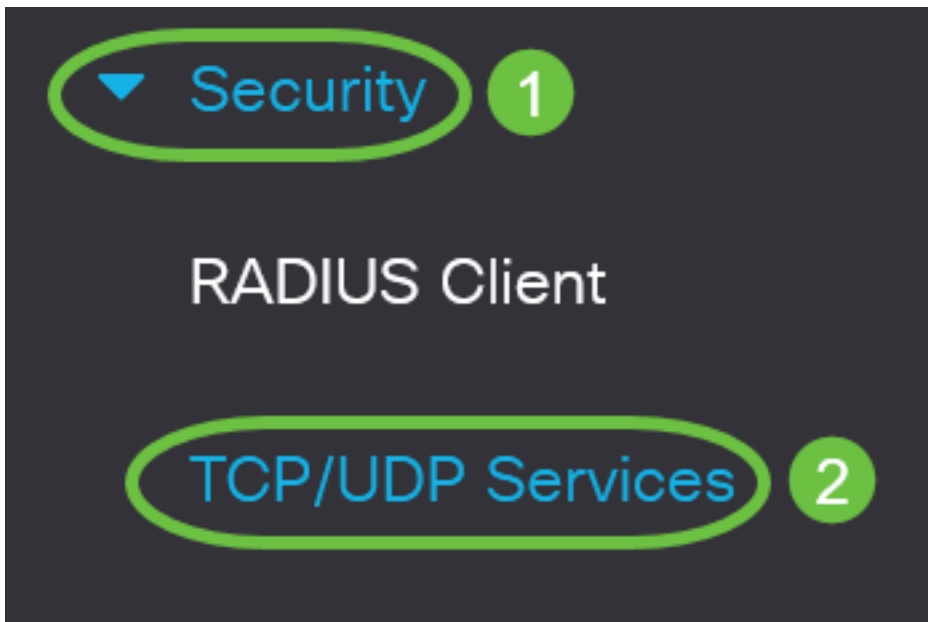
### Habilitar servicio SSH

Cuando se habilita la autenticación del servidor SSH, el cliente SSH que se ejecuta en el dispositivo autentica el servidor SSH usando el siguiente proceso de autenticación:

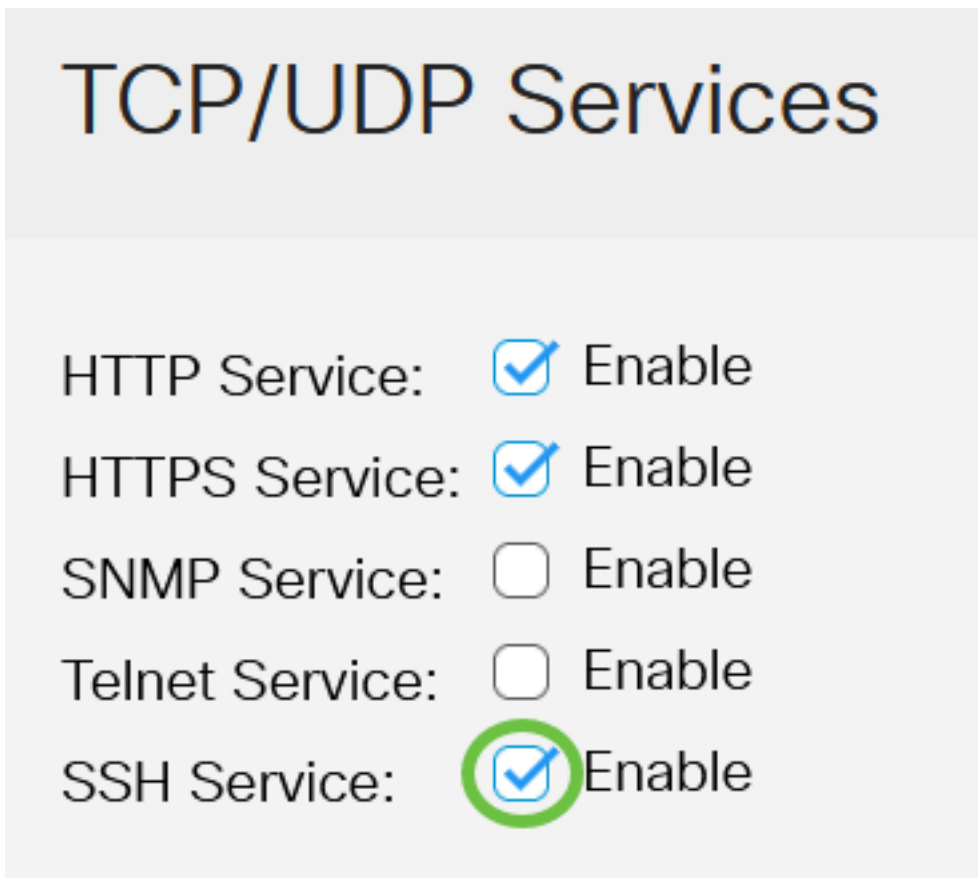
- El dispositivo calcula la huella digital de la clave pública recibida del servidor SSH.
- El dispositivo busca en la tabla SSH Trusted Servers la dirección IP y el nombre de host del servidor SSH. Se puede producir uno de los tres resultados siguientes:
  1. Si se encuentra una coincidencia tanto para la dirección como para el nombre de host del servidor y su huella digital, el servidor se autentica.
  2. Si se encuentra una dirección IP y un nombre de host coincidentes, pero no hay una 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.
  4. Si la entrada para el servidor SSH no se encuentra en la lista de servidores de confianza, el proceso falla.

Para soportar la configuración automática de un switch externo con la configuración predeterminada de fábrica, la autenticación del servidor SSH está inhabilitada de forma predeterminada.

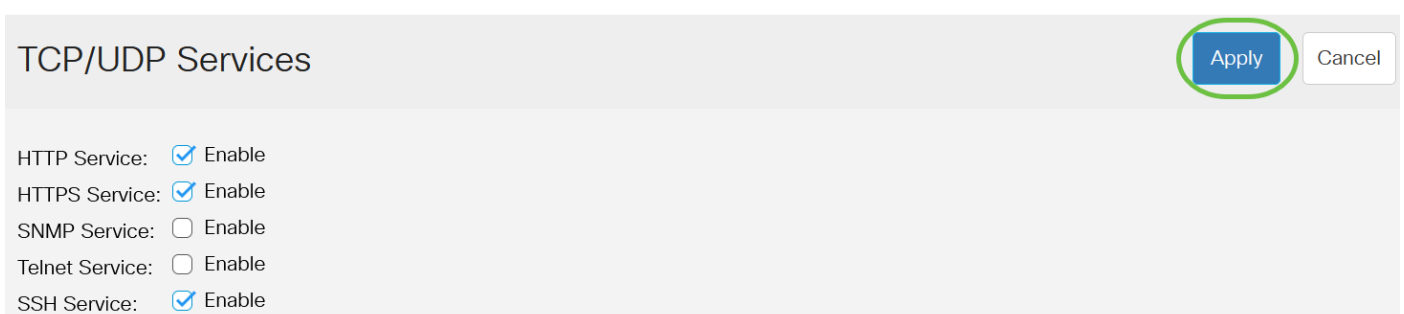
Paso 1. Inicie sesión en la utilidad basada en Web y elija **Security > TCP/UDP Services**.



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

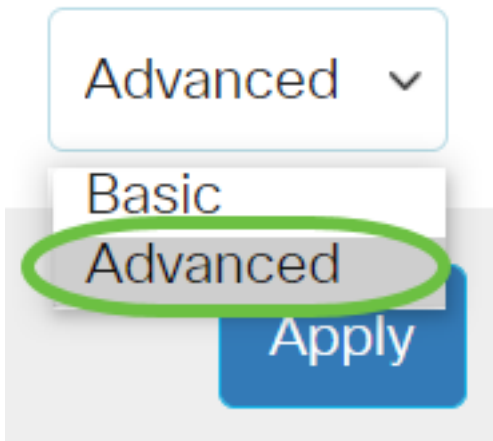


Paso 3. Haga clic en **Aplicar** para habilitar el servicio SSH.



## Configurar la configuración de autenticación del servidor SSH

Paso 1. Inicie sesión en la utilidad basada en Web del switch y, a continuación, seleccione Avanzado en la lista desplegable Modo de visualización.



Paso 2. Elija **Security > SSH Client > SSH Server Authentication**.

▼ Security

1

TACACS+ Client

RADIUS Client

▶ RADIUS Server

Password Strength

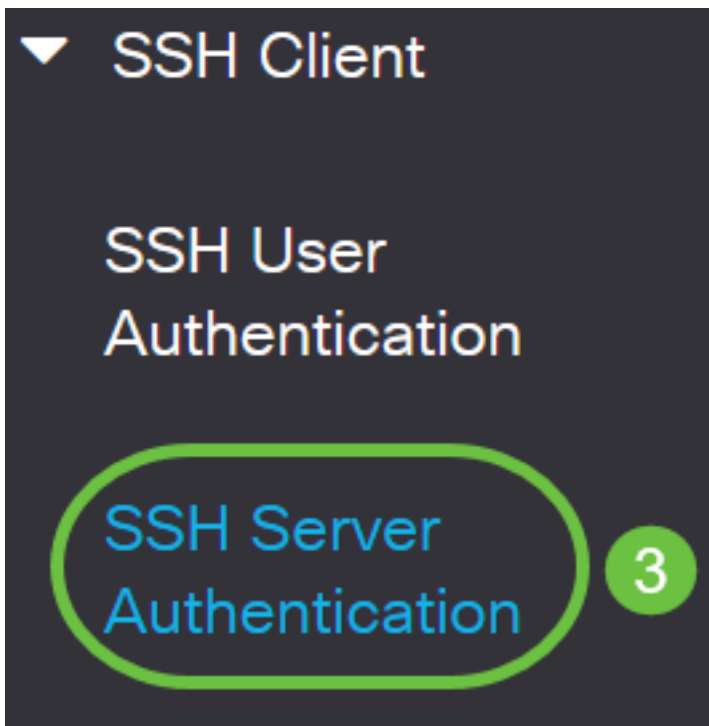
▶ Mgmt Access Method

Management Access  
Authentication

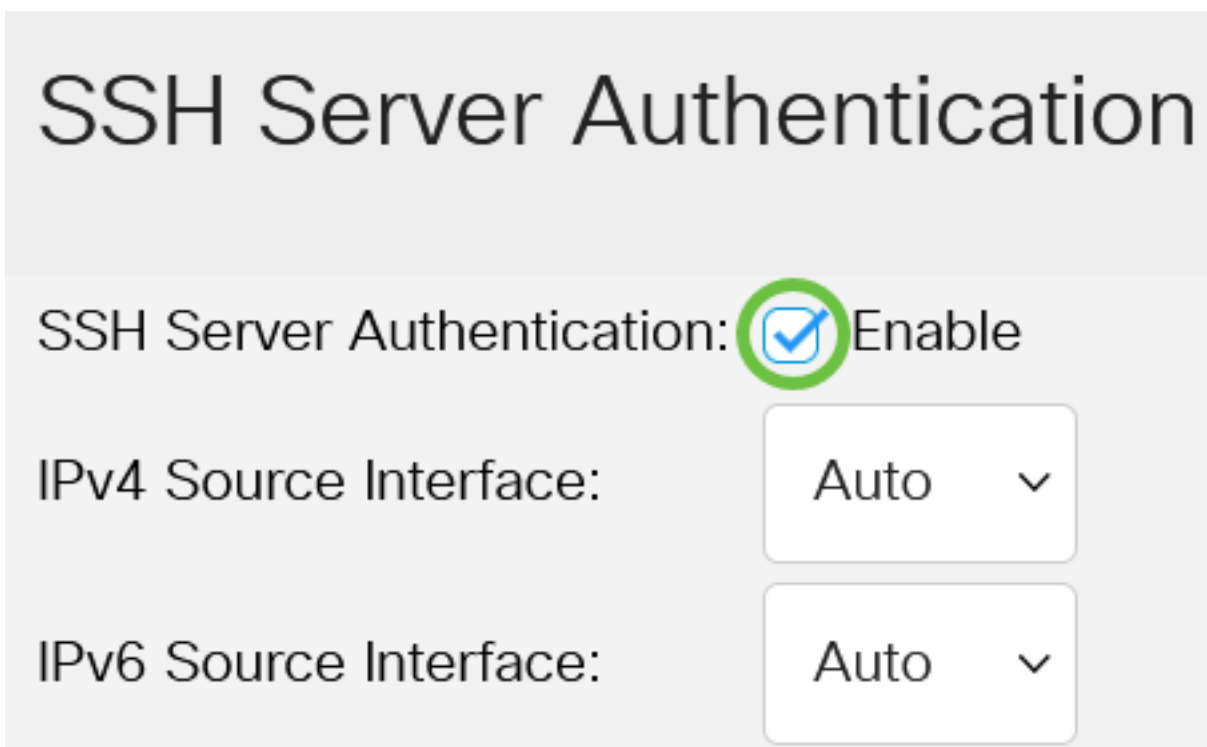
▶ Secure Sensitive Data  
Management

▶ SSL Server

▶ SSH Server



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 IPv4 Source Interface , 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 IPv4 SSH.

# SSH Server Authentication

SSH Server Authentication:  Enable

IPv4 Source Interface:

Auto ▾

IPv6 Source Interface:

Auto

VLAN 1

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

Paso 4. (Opcional) En la lista desplegable IPv6 Source Interface, 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 IPv6 SSH.

SSH Server Authentication:  Enable

IPv4 Source Interface:

VLAN 1 ▾

IPv6 Source Interface:

Auto ▾

Auto

Trusted SSH Servers Ta

VLAN 1

En este ejemplo, se elige la opción Auto (Automático). El sistema tomará la dirección IP de origen de la dirección IP definida en la interfaz de salida.

Paso 5. Haga clic en Apply (Aplicar).

## SSH Server Authentication

Apply

Cancel

SSH Server Authentication:  Enable

IPv4 Source Interface:

IPv6 Source Interface:

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

## Trusted SSH Servers Table



Server IP Address/Name	Fingerprint
------------------------	-------------

0 results found.

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

## Add Trusted SSH Server

Server Definition:



By IP address



By name

Las opciones son:

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

En este ejemplo, se elige By IP address (Por dirección IP). Si se elige Por nombre, vaya directamente al [Paso 11](#).

Paso 8. (Opcional) Si eligió By IP address en el Paso 6, haga clic en la versión IP del servidor SSH en el campo IP Version (Versión IP).

# Add Trusted SSH Server

---

Server Definition:  By IP address  By name

IP Version:  Version 6  Version 4

Las opciones disponibles son:

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

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 eligió la versión 6 como la versión de la dirección IP en el paso 7, haga clic en el tipo de dirección IPv6 en el tipo de dirección IPv6.

# Add Trusted SSH Server

---

Server Definition:  By IP address  By name

IP Version:  Version 6  Version 4

IPv6 Address Type:  Link Local  Global

Las opciones disponibles son:

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

Paso 10. (Opcional) Si eligió Link Local como tipo de dirección IPv6 en el Paso 9, elija la interfaz apropiada en la lista desplegable Link Local Interface .



# Add Trusted SSH Server

Server Definition:  By IP address  By name

IP Version:  Version 6  Version 4

IPv6 Address Type:  Link Local  Global

Link Local Interface:

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

## Add Trusted SSH Server

Server Definition:  By IP address  By name

IP Version:  Version 6  Version 4

IPv6 Address Type:  Link Local  Global

Link Local Interface:

⚙️ Server IP Address/Name:

⚙️ Fingerprint:  (16 pairs of hexadecimal characters)

En este ejemplo, se ingresa una dirección IP.

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

# Add Trusted SSH Server

Server Definition:  By IP address  By name

IP Version:  Version 6  Version 4

IPv6 Address Type:  Link Local  Global

Link Local Interface: VLAN 1 ▾

✦ Server IP Address/Name:

✦ Fingerprint:  (16 pairs of hexadecimal characters)

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

Add Trusted SSH Server

X

Server Definition:  By IP address  By name

IP Version:  Version 6  Version 4

IPv6 Address Type:  Link Local  Global

Link Local Interface: VLAN 1 ▾



✦ Server IP Address/Name:

✦ Fingerprint:  (16 pairs of hexadecimal characters)

**Apply** Close

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**.

## Trusted SSH Servers Table

  2

<span>1</span>	Server IP Address/Name	Fingerprint
<input checked="" type="checkbox"/>	192.168.1.1	76:0d:a0:12:7f:30:09:d3:18:04:df:77:c8:8e:51:a8

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



## SSH Server Authentication

Ahora ha configurado los parámetros de autenticación del servidor SSH en su switch Cisco Business de la serie 350.

¿Desea obtener más artículos sobre su switch CBS350? Consulte cualquiera de los enlaces siguientes para obtener más información.

[Parámetros de dirección IP](#) [Configuración de la pila](#) [Selector de modo de apilamiento](#) [Pautas de apilamiento](#) [Autenticación del servidor SSH](#) [Recuperación de contraseña](#) [Acceso a CLI con PuTTY](#) [Crear VLAN](#) [Restablecer switch](#)