

# Configuración de la Autenticación de Usuario de Secure Shell (SSH) en un Switch

## Objetivo

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.

En el modo CLI mediante SSH, el administrador puede ejecutar configuraciones más avanzadas en una conexión segura. Las conexiones SSH son útiles para solucionar problemas de una red de forma remota, en los casos en los que el administrador de la red no está físicamente presente en el sitio de red. El switch permite que el administrador autentique y administre a los usuarios para que se conecten a la red a través de SSH. La autenticación se realiza a través de una clave pública que el usuario puede utilizar para establecer una conexión SSH a una red específica.

La función de cliente SSH es una aplicación que se ejecuta a través del protocolo SSH para proporcionar autenticación y cifrado de dispositivos. Permite que un dispositivo realice una conexión segura y cifrada a otro dispositivo que ejecute el servidor SSH. Con la autenticación y el cifrado, el cliente SSH permite una comunicación segura a través de una conexión Telnet no segura.

Este artículo proporciona instrucciones sobre cómo configurar la autenticación de usuario de cliente en un switch administrado.

## Dispositivos aplicables

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

## Versión del software

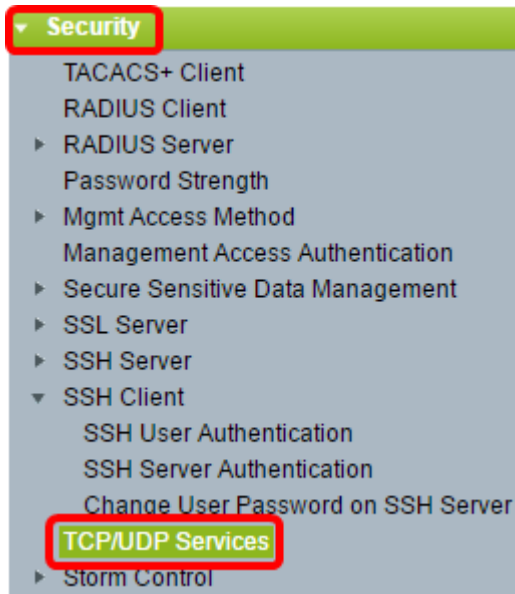
- 1.4.5.02 - Series Sx200, Sx300 y Sx500
- 2.2.0.66 - Serie Sx350, Serie SG350X, Serie Sx550X

## Configuración de la Autenticación de Usuario de Cliente SSH

### Activar servicio SSH

**Nota:** Para soportar la configuración automática de un dispositivo listo para usar (dispositivo 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 seleccione **Seguridad > Servicios TCP/UDP**



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 de Usuario SSH

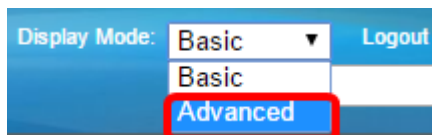
Utilice esta página para elegir un método de autenticación de usuario SSH. Puede establecer un nombre de usuario y una contraseña en el dispositivo si elige el método de contraseña. También puede generar una clave Ron Rivest, Adi Shamir y Leonard Adleman (RSA) o un algoritmo de firma digital (DSA) si se selecciona el método de clave pública o privada.

Los pares de claves RSA y DSA predeterminados se generan para el dispositivo cuando se arranca. Una de estas claves se utiliza para cifrar los datos que se descargan del servidor SSH. La clave RSA se utiliza de forma predeterminada. Si el usuario elimina una de estas claves o ambas, se vuelven a generar.

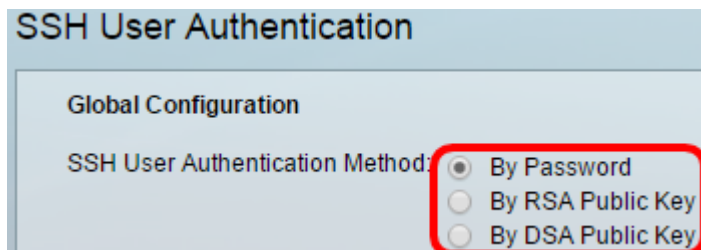
Paso 1. Inicie sesión en la utilidad basada en web y elija **Security > SSH Client > SSH User Authentication**.



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



Paso 2. En Configuración global, haga clic en el Método de autenticación de usuario SSH que desee.



**Nota:** Cuando un dispositivo (cliente SSH) intenta establecer una sesión SSH en el servidor SSH, el servidor SSH utiliza uno de los siguientes métodos para la autenticación del cliente:

- By Password (Por contraseña): esta opción permite configurar una contraseña para la autenticación de usuarios. Éste es el parámetro predeterminado y la contraseña predeterminada es anonymous (anónima). Si se elige esta opción, asegúrese de que las credenciales de nombre de usuario y contraseña se hayan establecido en el servidor SSH.
- By RSA Public Key (Por clave pública RSA): esta opción permite utilizar la clave pública RSA para la autenticación de usuarios. Una clave RSA es una clave cifrada basada en la factorización de enteros grandes. Esta clave es el tipo más común de clave utilizada para la autenticación de usuario SSH.
- By DSA Public Key (Por clave pública DSA): esta opción permite utilizar una clave pública DSA para la autenticación de usuarios. Una clave DSA es una clave encriptada basada en el algoritmo discreto ElGamal. Esta clave no se utiliza comúnmente para la autenticación de usuario SSH, ya que toma más tiempo en el proceso de autenticación.

**Nota:** En este ejemplo, se elige Por contraseña.

Paso 3. En el área Credenciales, introduzca el nombre de usuario en el campo *Nombre de usuario*.

Credentials

Username: ciscosbuser1 (0/70 characters used)

Password:  Encrypted AUy3Nne84DHjTuVuzd1A  
 Plaintext (Default Password)

Apply Cancel Restore Default Credentials Display Sensitive Data as Plaintext

**Nota:** En este ejemplo, se utiliza ciscosbuser1.

Paso 4. (Opcional) Si selecciona Por contraseña en el paso 2, haga clic en el método y, a continuación, introduzca la contraseña en el campo *Cifrado* o *Texto sin formato*.

Password:  Encrypted AUy3Nne84DHjTuVuzd1A  
 Plaintext Ci\$C0SBSwi+ch

Las opciones son:

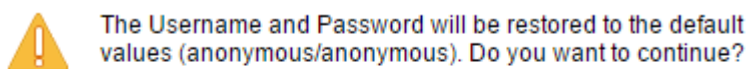
- Encrypted: esta opción permite introducir una versión cifrada de la contraseña.
- Texto sin formato: esta opción permite introducir una contraseña de texto sin formato.

**Nota:** En este ejemplo, se elige texto sin formato y se introduce una contraseña de texto sin formato.

Paso 5. Haga clic en **Apply** para guardar su configuración de autenticación.

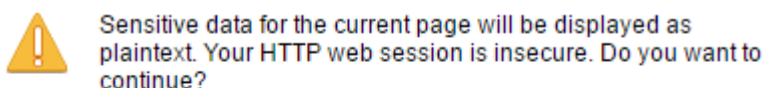
Paso 6. (Opcional) Haga clic en **Restaurar credenciales predeterminadas** para restaurar el nombre de usuario y la contraseña predeterminados y, a continuación, haga clic en **Aceptar** para continuar.

**Nota:** El nombre de usuario y la contraseña se restaurarán a los valores predeterminados: anonymous/anonymous.



OK Cancel

Paso 7. (Opcional) Haga clic en **Mostrar datos confidenciales como texto sin formato** para mostrar los datos confidenciales de la página en formato de texto sin formato y, a continuación, haga clic en **Aceptar** para continuar.



Don't show me this again

OK Cancel

## Configuración de la Tabla de Claves de Usuario SSH

Paso 8. Marque la casilla de verificación de la clave que desea administrar.

SSH User Key Table			
<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	User Defined	60:aa:27:3c:37:52:c2:a5:7c:d0:4a:a5:04:92:47:74
<input type="checkbox"/>	DSA	Auto Generated	1c:54:fe:25:98:fb:d2:1a:45:f5:47:cb:a8:00:be:eb

Generate Edit... Delete Details

**Nota:** En este ejemplo, se elige RSA.

Paso 9. (Opcional) Haga clic en **Generar** para generar una nueva clave. La nueva clave anulará la clave activada y, a continuación, haga clic en **Aceptar** para continuar.



Generating a new key will overwrite the existing key. Do you want to continue?



Paso 10. (Opcional) Haga clic en **Editar** para editar una clave actual.

SSH User Key Table			
<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	User Defined	60:aa:27:3c:37:52:c2:a5:7c:d0:4a:a5:04:92:47:74
<input type="checkbox"/>	DSA	Auto Generated	1c:54:fe:25:98:fb:d2:1a:45:f5:47:cb:a8:00:be:eb

Generate Edit... Delete Details

Paso 11. (Opcional) Elija un tipo de clave en la lista desplegable Tipo de clave.

Key Type:  

Public Key:  

Comment:

**Nota:** En este ejemplo, se elige RSA.

Paso 12. (Opcional) Introduzca la nueva clave pública en el campo *Public Key*.

When a Key is entered, it should contain the "BEGIN" and "END" markers.

Key Type: RSA

Public Key:

```

--- BEGIN SSH2 PUBLIC KEY ---
Comment: RSA Public Key
AAAAB3NzaC1yc2EAAAADAQABAAQDAQDAb0QFu8yktUlebpLhpETIs79pWY+k0F8g4x
ovv+0T55Bq2pys5O7FwoxKTLIXFVW5CFdRw26QS2w0oLnH0TecsC13qzhFuOEVBPhKC
akyEuy6x8fFsKwdLIld8iUVIbyXk4psIDQD2u0U7AHVRH4ITcXpinexS0MQ==
--- END SSH2 PUBLIC KEY ---

```

Private Key:  Encrypted


Plaintext

Apply Close Display Sensitive Data as Plaintext

Paso 13. (Opcional) Introduzca la nueva clave privada en el campo *Private Key*.

**Nota:** Puede editar la clave privada y hacer clic en Cifrada para ver la clave privada actual como texto cifrado, o en Texto sin formato para ver la clave privada actual como texto sin formato.

Paso 14. (Opcional) Haga clic en **Mostrar datos confidenciales como texto sin formato** para mostrar los datos cifrados de la página en formato de texto sin formato y, a continuación, haga clic en **Aceptar** para continuar.

 Sensitive data for the current page will be displayed as plaintext. Your HTTP web session is insecure. Do you want to continue?

Don't show me this again

OK Cancel

Paso 15. Haga clic en **Apply** para guardar los cambios y luego haga clic en **Close**.

Paso 16. (Opcional) Haga clic en **Eliminar** para eliminar la clave marcada.

SSH User Key Table			
<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	User Defined	60:aa:27:3c:37:52:c2:a5:7c:d0:4a:a5:04:92:47:74
<input type="checkbox"/>	DSA	Auto Generated	1c:54:fe:25:98:fb:d2:1a:45:f5:47:cb:a8:00:be:eb

Generate Edit... Delete Details

Paso 17. (Opcional) Una vez que aparezca un mensaje de confirmación como se muestra a continuación, haga clic en **Aceptar** para eliminar la clave.



The selected user defined key will be deleted and replaced by an auto generated key. Do you want to continue?

Paso 18. (Opcional) Haga clic en **Detalles** para ver los detalles de la tecla activada.

### SSH User Key Details

SSH Server Key Type: RSA

Public Key: --- BEGIN SSH2 PUBLIC KEY ---  
Comment: RSA Public Key  
AAAAB3NzaC1yc2EAAAADAQABAAQgQDAb0QFu6yktUlebpLhpETIs79pV  
Rovv+0T55Bq2pys5O7FwoxKTLIXFVW5CFdRw26QS2w0oLnH0TecsCI3qzH  
7LYhakyEuy6x6fFsKwdLlId8iUVlbyXk4psIDQD2u0U7AHVRH4ITcXpinexS0M  
--- END SSH2 PUBLIC KEY ---

Private Key (Encrypted): --- BEGIN SSH2 ENCRYPTED PRIVATE KEY ---  
Comment: RSA Private Key  
UM5POag2XRmC4XxM1VhmxNkAdj+ml75ZsprMYh/PkuAVm40EHk41YQDg  
+zh87iJBUUpwHPId1ivhgjBJuF9sFtKTIU3DKUg1IOrKcM90JapMOyDpD7M+4  
gBd08SbtMQWZdFy7hj6rSTCO0YPKpVhkylBwye44QdjCaCGojE/FIKuMHBz  
dkVPHkwi2ExfbENqD60yc7pFex+oaah/ugmYgjBmOnNbrViXCrHiUSAKUWz  
RUDaVM7V2u67+yw+/yNJ+XvRYkhsQZRON8cOi4ilHV1MImJoRGrdiuR/CjE  
X3zOhmB8o6iyCa32MPlhy08yfPN4YgrHh0cpxeWcY1ZRIG0vZ4lxUJ423xYL  
rdclnoll4EWSk+sj1vzrGidXHCRzQkkMqLp+E5zI9npJc0t6+64tKqAD3CVaHk  
VwR5JXrle2vHdik2af2AO3JZsobtTO0dMSA5zPdN4CCERPLAEaACTCQOkE  
MqHATSyFcG+h0X2MitxV5XsWUaJe/dH/BNeljYrzKRF6y9V37PFBizSLAtE2  
62u0QPBRglLu6lL4j4jCtN54PauVkr48mw3JgsWszKXgHmSx/ok7Tu4gPcn-  
UI37c0vNZwDadMZ/1ZKLEkBOJtJIJevDsWslvclKZAvoSmLu2B20hUM2uor1  
5GngylqcT5vYLMGpDL2k2PzUgFuLvbAOFzIri1c1czqyjy+JCbP/cl7TAOeGA7  
LtCY8DrAo8y5O15CcgUIZJddWLRqunDGpygscAaor050vG3/5A1C8YRMh2F  
86OuHWS+0HHqnJnmgrOICj/O/DiSeRnHkr8juT1sBuwpFDd+wT0L/KzRN1L  
4OwOYCjkdgm7GgOI2eOnY9YvyD/RyjcMm11JFA1RwPCSQWhyPrZgcCQS  
0FLgLKZNZ1XNJkdqDBmb6CfyvXeGP76EH+EQ==  
--- END SSH2 PRIVATE KEY ---

Paso 19. (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.



Port Gigabit PoE Stackable Managed Switch

Save

Language: E

### SSH User Authentication

Success. To permanently save the configuration, go to the [File Operations](#) page or c

**Global Configuration**

SSH User Authentication Method:  By Password  
 By RSA Public Key  
 By DSA Public Key

**Credentials**

Username:  (0/70 characters used)

Password:  Encrypted   
 Plaintext  (Default Password)

Apply Cancel Restore Default Credentials Display Sensitive Data as Plaintext

**SSH User Key Table**

<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input type="checkbox"/>	RSA	User Defined	60:aa:27:3c:37:52:c2:a5:7c:d0:4a:a5:04:92:47:74
<input type="checkbox"/>	DSA	Auto Generated	1c:54:fe:25:98:fb:d2:1a:45:f5:47:cb:a8:00:be:eb

Generate Edit... Delete Details

Ahora debería haber configurado los parámetros de autenticación de usuario de cliente en el switch gestionado.



## 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).