

# Configuración de los parámetros de autenticación de usuario de Secure Shell (SSH) en un switch Cisco Business de la serie 350

## Objetivo

En este artículo se proporcionan instrucciones sobre cómo configurar la autenticación de usuario del cliente en los switches 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.

En el modo CLI a través de 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 que el administrador de la red no está físicamente presente en el sitio de la red. El switch permite al administrador autenticar y administrar usuarios para conectarse a la red a través de SSH. La autenticación se produce 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 sobre el protocolo SSH para proporcionar autenticación y cifrado del dispositivo. 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.

## Dispositivos aplicables | Versión de software

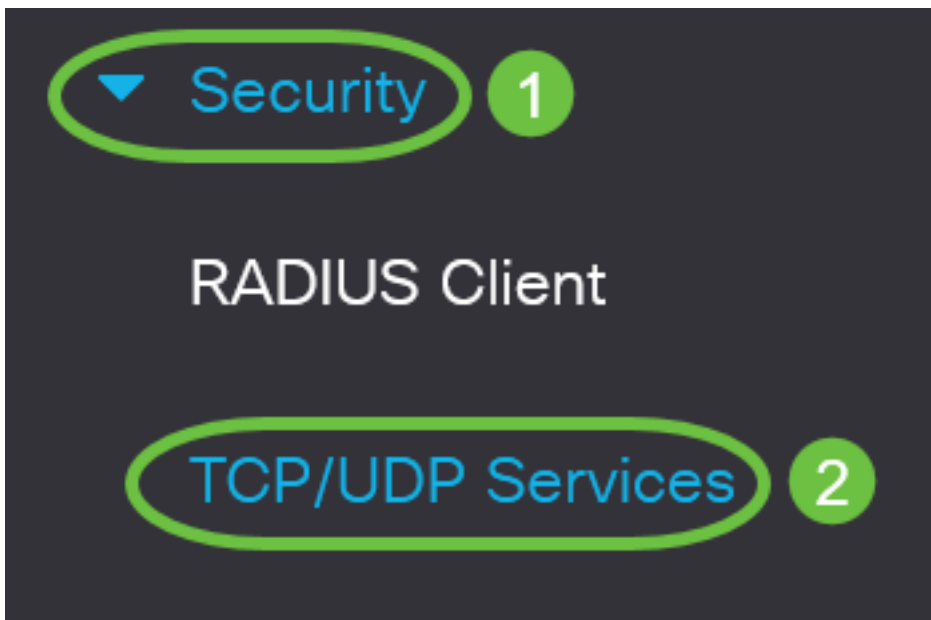
- CBS350 ([Ficha técnica](#)) | 3.0.0.69 ([Descargar última](#))
- CBS350-2X ([Ficha técnica](#)) | 3.0.0.69 ([Descargar última](#))
- CBS350-4X ([Ficha técnica](#)) | 3.0.0.69 ([Descargar última](#))

## Configurar la configuración de autenticación de usuario de cliente SSH

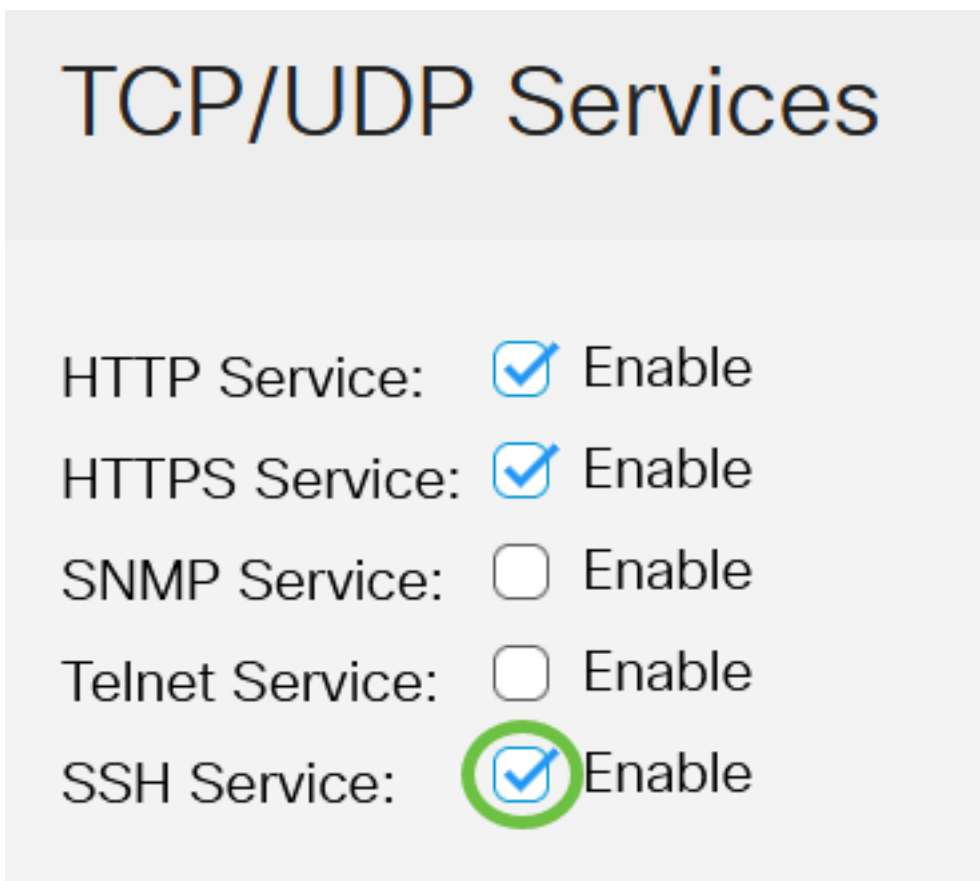
### Habilitar servicio SSH

Para soportar la configuración automática de un dispositivo listo para usar (dispositivo con configuración predeterminada de fábrica), la autenticación del servidor SSH está inhabilitada de forma predeterminada.

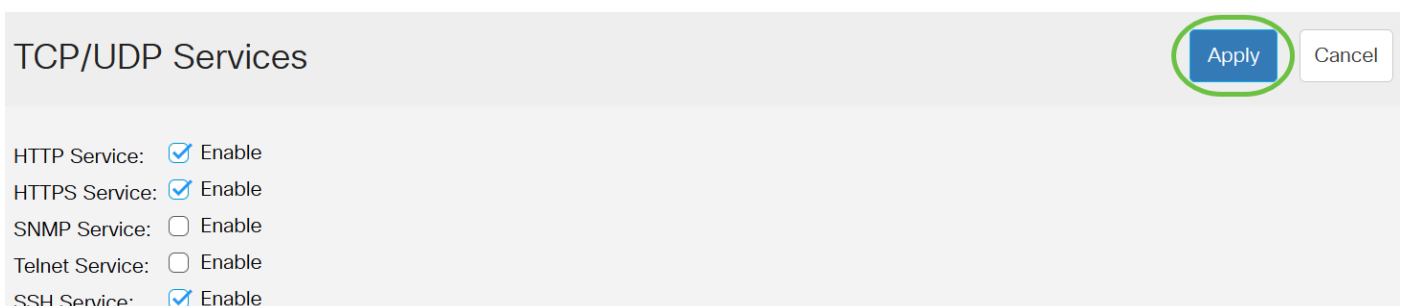
Paso 1. Inicie sesión en la utilidad basada en Web y elija **Security > TCP/UDP Services**



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.

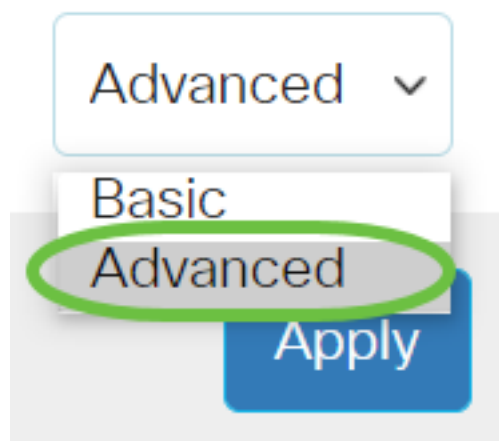


**Configurar la configuración de autenticación de usuario SSH**

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 se elige el método de contraseña. También puede generar una clave Ron Rivest, Adi Shamir y Leonard Adleman (RSA) o Digital Signature Algorithm (DSA) si se selecciona el método de clave pública o privada.

Los pares de claves predeterminados RSA y DSA se generan para el dispositivo cuando se inicia. 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 o ambas claves, se regeneran.

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 User Authentication** en el menú.

## ▼ Security

1

TACACS+ Client

RADIUS Client

▶ RADIUS Server

Password Strength

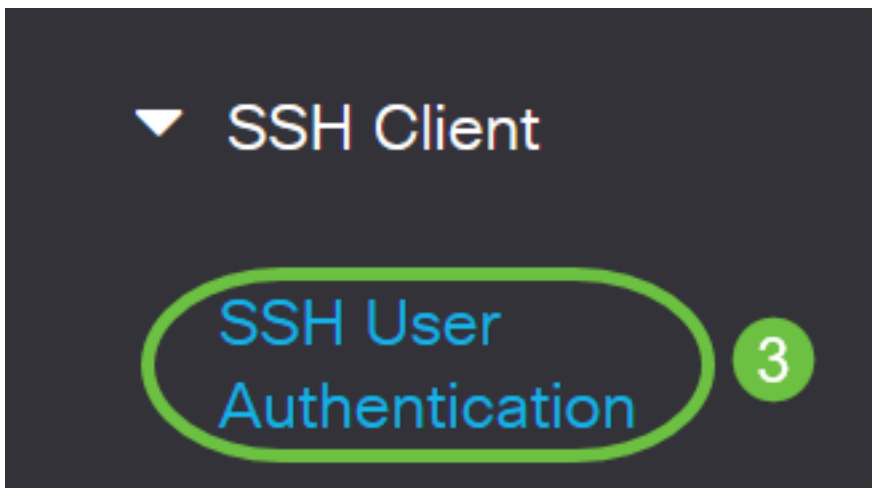
▶ Mgmt Access Method

Management Access  
Authentication

▶ Secure Sensitive Data  
Management

▶ SSL Server

▶ SSH Server



Paso 3. En Configuración global, haga clic en el método de autenticación de usuario SSH deseado.

## Global Configuration

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

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 le permite configurar una contraseña para la autenticación de usuario. Esta es la configuración predeterminada y la contraseña predeterminada es `anonymous`. Si se elige esta opción, asegúrese de que se hayan establecido las credenciales de nombre de usuario y contraseña en el servidor SSH.
- **By RSA Public Key -** Esta opción le permite utilizar la clave pública RSA para la autenticación de usuario. Una clave RSA es una clave cifrada basada en la factorización de enteros grandes. Esta clave es el tipo de clave más común utilizado para la autenticación de usuario SSH.
- **By DSA Public Key (Clave pública DSA):** Esta opción permite utilizar una clave pública DSA para la autenticación de usuario. Una clave DSA es una clave cifrada basada en el algoritmo discreto ElGamal. Esta clave no se utiliza comúnmente para la autenticación de usuario SSH, ya que lleva más tiempo en el proceso de autenticación.

En este ejemplo, se elige **By Password (Por contraseña)**.

Paso 4. En el área Credenciales, ingrese el nombre de usuario en el campo *Nombre de usuario*.

## Credentials

✳ Username:  (12/70 characters used)

✳ Password:  Encrypted

Plaintext  (Default Password: anonymous)

En este ejemplo, se utiliza ciscosbuser1.

Paso 5. (Opcional) Si eligió By Password en el Paso 2, haga clic en el método y escriba la contraseña en los campos *Encrypted* o *Plaintext*.

## Credentials

✳ Username:  (12/70 characters used)

✳ Password:  Encrypted

Plaintext  (Default Password: anonymous)

Las opciones son:

- Encrypted (Cifrado): Esta opción le permite introducir una versión cifrada de la contraseña.
- Texto sin formato - Esta opción le permite introducir una contraseña de texto sin formato.

En este ejemplo, se elige el texto sin formato y se introduce una contraseña de texto sin formato.

Paso 6. Haga clic en **Aplicar** para guardar la configuración de autenticación.

## SSH User Authentication

By RSA Public Key

By DSA Public Key

### Credentials

✳ Username:  (12/70 ch)

✳ Password:  Encrypted

Plaintext


Paso 7. (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.

SSH User Authentication

Global Configuration

## Confirm Restore Default Credentials X

 The Username and Password will be restored to the default values (anonymous/anonymous). Do you want to continue?


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

Paso 8. (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.

SSH User Authentication

Global Configuration



## Confirm Display Method Change X

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

## Configuración de la Tabla de Clave de Usuario SSH

Paso 9. Active la casilla de verificación de la clave que desea administrar.

## SSH User Key Table




Generate   Details

<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	Auto Generated	MD5:c0:b4:8a:25:26:52:56:8f:4e:f5:a4:fa:a7:cc:0a:b2
<input type="checkbox"/>	DSA	Auto Generated	MD5:03:c8:0b:9b:a2:88:86:f8:49:0d:d2:51:81:f3:cd:c6

En este ejemplo, se elige RSA.

Paso 10. (Opcional) Haga clic en **Generar** para generar una nueva clave. La nueva clave reemplazará la clave seleccionada y luego hará clic en **Aceptar** para continuar.

## SSH User Key Table

   Details

<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	Auto Generated	MD5:c0:b4:8a:25:26:52:56:8f:4e:f5:a4:fa:a7:cc:0a:b2
<input type="checkbox"/>	DSA	Auto Generated	MD5:03:c8:0b:9b:a2:88:86:f8:49:0d:d2:51:81:f3:cd:c6

## Confirm Key Generation

X



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

OK

Cancel

Paso 11. (Opcional) Haga clic en **Editar** para editar una clave actual.



## SSH User Key Table

[Generate](#)   [Details](#)

<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	Auto Generated	MD5:c0:b4:8a:25:26:52:56:8f:4e:f5:a4:fa:a7:cc:0a:b2
<input type="checkbox"/>	DSA	Auto Generated	MD5:03:c8:0b:9b:a2:88:86:f8:49:0d:d2:51:81:f3:cd:c6

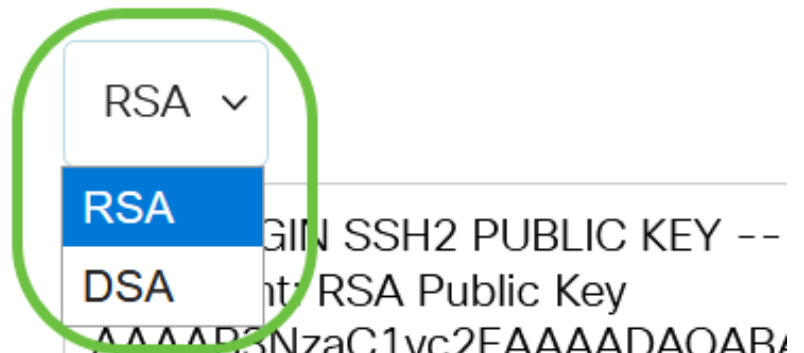
Paso 12. (Opcional) Elija un tipo de clave de la lista desplegable Tipo de clave.

## Edit SSH Client Authentication Settings

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

Key Type:

 Public Key:



The screenshot shows a dropdown menu for the 'Key Type' field. The menu is open, showing three options: 'RSA' (selected and highlighted in blue), 'DSA', and 'SSH2 PUBLIC KEY --'. The 'RSA' option is circled in green. Below the dropdown, the beginning of a public key is visible, starting with 'BEGIN SSH2 PUBLIC KEY --' and 'ssh-rsa Public Key'.

En este ejemplo, se elige RSA.

Paso 13. (Opcional) Introduzca la nueva clave pública en el campo *Clave pública*.

## Edit SSH Client Authentication Settings

X

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

Key Type:

Public Key:

```
----- BEGIN SSH2 PUBLIC KEY -----  
Comment: RSA Public Key  
AAAAB3NzaC1yc2EAAAADAQABAAQCy9BJ+eTyaNva9u8G8VZgLqYuM8NHNoVh9WtPdKmbP004VvhTXfPqGCzg4/IIFlpm  
hf4lmgpX+XB7aLCi3Ch0vsuLJEahjrCS5iRCvEPrh9oUoec/GBCFhe7zXYHprXkoGBC4I0SXBVS5xKpxuSwLIDsxgY10  
/9lpXWKK8uN2r7P2PVJI1APr2RnjlUe1LVZTfrpMSqZ6UB+QtNtvaed46vTowjgCb4+y+zFYpQjlvZCAuMoaWkljQFslXMBOLL  
/D/cydxLa887DJQaMjPnu4G0PuQALWtT88h5hsHpZEhmcptoC00B+Auby0mXG6leE5bKFDpb2UFLJzHodD0fC9b  
----- END SSH2 PUBLIC KEY -----
```

Private Key:  Encrypted

Plaintext

Apply

Close

Display Sensitive Data as Plaintext

Paso 14. (Opcional) Introduzca la nueva clave privada en el campo *Private Key*.

Puede editar la clave privada y hacer clic en Cifrado para ver la clave privada actual como texto cifrado, o bien en Texto sin formato para ver la clave privada actual en texto sin formato.

Paso 15. (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.

## Edit SSH Client Authentication Settings

X

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

Key Type:

Public Key:

```
----- BEGIN SSH2 PUBLIC KEY -----  
Comment: RSA Public Key  
AAAAB3NzaC1yc2EAAAADAQABAAQCy9BJ+eTyaNva9u8G8VZgLqYuM8NHNoVh9WtPdKmbP004VvhTXfPqGCzg4/IIFlpm  
hf4lmgpX+XB7aLCi3Ch0vsuLJEahjrCS5iRCvEPrh9oUoec/GBCFhe7zXYHprXkoGBC4I0SXBVS5xKpxuSwLIDsxgY10  
/9lpXWKK8uN2r7P2PVJI1APr2RnjlUe1LVZTfrpMSqZ6UB+QtNtvaed46vTowjgCb4+y+zFYpQjlvZCAuMoaWkljQFslXMBOLL  
/D/cydxLa887DJQaMjPnu4G0PuQALWtT88h5hsHpZEhmcptoC00B+Auby0mXG6leE5bKFDpb2UFLJzHodD0fC9b  
----- END SSH2 PUBLIC KEY -----
```

Private Key:  Encrypted

Plaintext

Apply

Close

Display Sensitive Data as Plaintext

# Confirm Display Method Change

X



Sensitive data for the current page will be displayed as plaintext. Do you want to continue?

Don't show me this again



Paso 16. Haga clic en **Aplicar** para guardar los cambios y luego haga clic en **Cerrar**.

## Edit SSH Client Authentication Settings

X

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

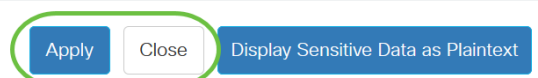
Key Type:

Public Key:

```
----- BEGIN SSH2 PUBLIC KEY -----  
Comment: RSA Public Key  
AAAAB3NzaC1yc2EAAAADAQABAAQCy9BJ+eTyaNva9u8G8VZgLqYuM8NHNoVh9WtPdKmBp004VvhTXfPqGCzg4/IIFlpm  
hf4ImgpX+XB7aLCI3Ch0vsuLJEahjrCS5iRCvEPrh9oUoec/GBCFhe7zXYHpRXkoGBC4I0SXBVS5xKpxuSwLIDsxgY10  
/9lpXWKK8uN2r7P2PVJI1APr2RnjIue1LVZTfrpMSqZ6UB+QtNtvaed46vTOWjgCb4+y+zFYpQjlvZCAuMoaWkljQFsiXMBOLL  
/D/cydxLa887DJQaMjPnu4G0PuQALWtT88h5hsHpZEhmcptoC00B+Auby0mXG6leE5bKFDpb2UFLJzHodD0fC9b  
----- END SSH2 PUBLIC KEY -----
```

Private Key:  Encrypted

Plaintext



Paso 17. (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	MD5:02:26:b2:5c:56:51:b6:cf:db:fa:f7:b5:1a:26:7e:33
<input type="checkbox"/>	DSA	Auto Generated	MD5:03:c8:0b:9b:a2:88:86:f8:49:0d:d2:51:81:f3:cd:c6

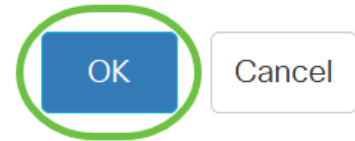
Paso 18. (Opcional) Una vez que se le solicite un mensaje de confirmación como se muestra a continuación, haga clic en **Aceptar** para eliminar la clave.

# Delete User Generated Key

X

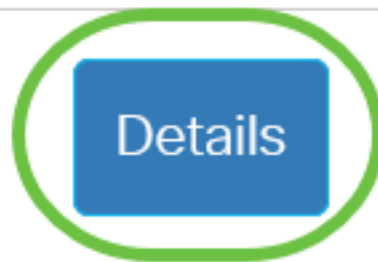


The selected user defined key will be deleted and replaced by an auto generated key. Do you want to continue?



Paso 19. (Opcional) Haga clic en **Detalles** para ver los detalles de la clave marcada.

## SSH User Key Table



Key Type

Key Source

Fingerprint

### SSH User Key Details

Back

SSH Server Key Type: RSA  
Public Key: ----- BEGIN SSH2 PUBLIC KEY -----  
Comment: RSA Public Key  
AAAAB3NzaC1yc2EAAAADAQABAAQ=CxBoUggILUWLBwkarVUG9jbM4OQUDsPdr  
VmHGNkIRJVg3nxO2wmw10xckYy7YZLPaoriNd/obTuGZ4jOqhSgfQckqhibcSNdlaUrw;  
w1v4QBwH8UbGNw1yV/SaECMuFre/VzYdRP  
/RvGDNCNOphqMMJyCQ3D+WG2136l+li+U3Kn9BOBoOsSn+gz7c1OvNoXQ9t+NvtJDF  
3MfMhmvwx0XIEKgMZgV+ennjipMPja0FP8HGblh  
/hOPdhUIPmaRheE3hsDS1S9TJXLu7RnG0TrknL+QUFqZeRT3jSablwZsaGyE8oklpP5E  
K9qsLJZlqeMm2gWjziB  
----- END SSH2 PUBLIC KEY -----  
Private Key (Encrypted): ----- BEGIN SSH2 ENCRYPTED PRIVATE KEY -----  
Comment: RSA Private Key  
AkNK2himPem2VeoSwyp0U+1FXk81mva9RGX2rBMhCDlj/79rYDLBnYKdSHk3A7Hqg0  
aDjeLKVROxyRccQ0UivFp70SYz6mmjfrvwAXgCnZoNkhv8WO+Ktz0tLliHAj2gWaXerYB  
D5suzX+ROnl R0Δ0zI I05G663mEMVcOT

Paso 20. (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.



CBS350-8P-E-2G - swi...



## SSH User Authentication

Apply

Cancel

Res

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