

# Configurar as configurações de autenticação de usuário do Secure Shell (SSH) em um switch Cisco Business 350 Series

## Objetivo

Este artigo fornece instruções sobre como configurar a autenticação de usuário cliente em switches Cisco Business 350 Series.

## Introduction

O Secure Shell (SSH) é um protocolo que fornece uma conexão remota segura para dispositivos de rede específicos. Essa conexão fornece uma funcionalidade semelhante a uma conexão Telnet, exceto que ela é criptografada. O SSH permite que o administrador configure o switch através da interface de linha de comando (CLI) com um programa de terceiros.

No modo CLI via SSH, o administrador pode executar configurações mais avançadas em uma conexão segura. As conexões SSH são úteis na solução de problemas de uma rede remotamente, nos casos em que o administrador da rede não está fisicamente presente no local da rede. O switch permite que o administrador autentique e gereencie usuários para se conectar à rede via SSH. A autenticação ocorre através de uma chave pública que o usuário pode usar para estabelecer uma conexão SSH com uma rede específica.

O recurso de cliente SSH é um aplicativo executado no protocolo SSH para fornecer autenticação e criptografia de dispositivo. Ele permite que um dispositivo faça uma conexão segura e criptografada para outro dispositivo que executa o servidor SSH. Com autenticação e criptografia, o cliente SSH permite uma comunicação segura em uma conexão Telnet não segura.

## Dispositivos aplicáveis | Versão do software

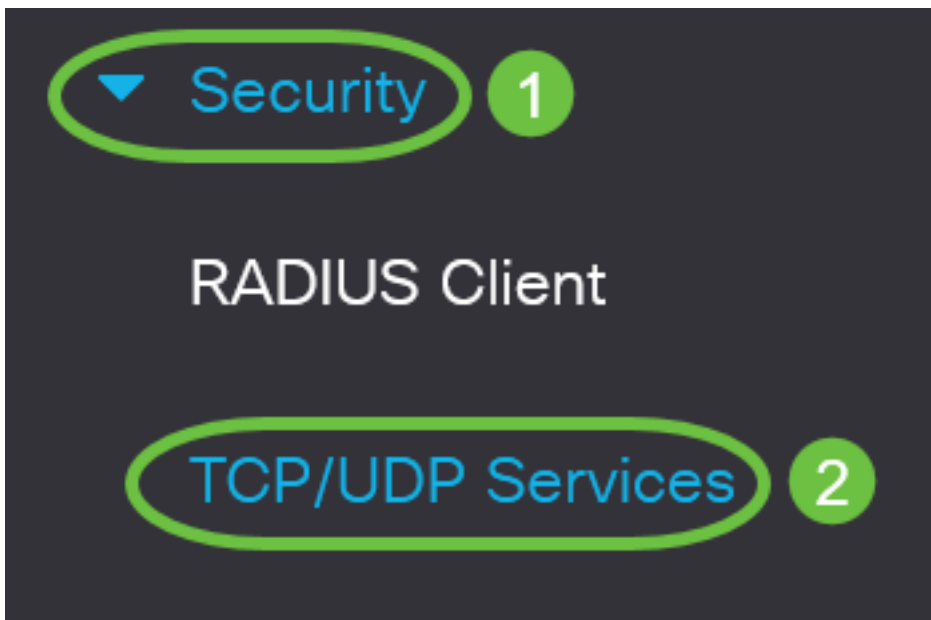
- CBS350 ([Data Sheet](#)) | 3.0.0.69 (Baixe o mais recente)
- CBS350-2X ([Data Sheet](#)) | 3.0.0.69 (Baixe o mais recente)
- CBS350-4X ([Data Sheet](#)) | 3.0.0.69 (Baixe o mais recente)

## Definir as configurações de autenticação de usuário do cliente SSH

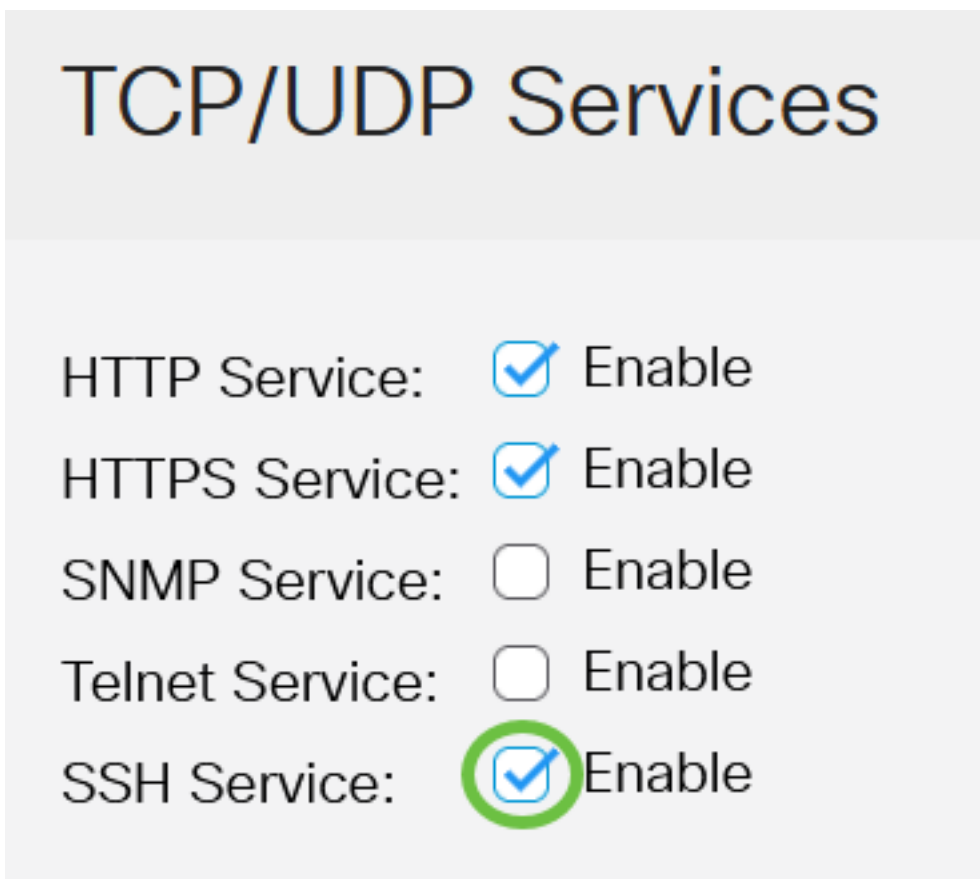
### Habilitar serviço SSH

Para suportar a configuração automática de um dispositivo pronto para uso (dispositivo com configuração padrão de fábrica), a autenticação do servidor SSH é desativada por padrão.

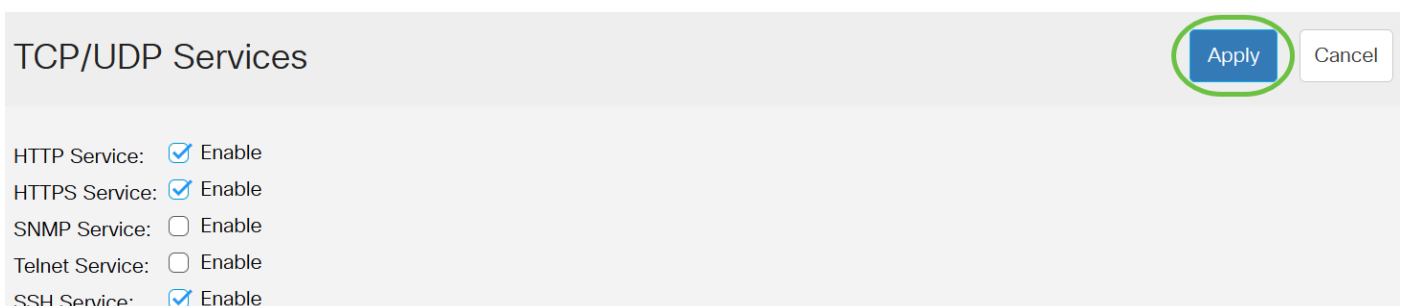
Etapa 1. Faça login no utilitário baseado na Web e escolha **Security > TCP/UDP Services**



Etapa 2. Marque a caixa de seleção **Serviço SSH** para habilitar o acesso do prompt de comando dos switches através do SSH.



Etapa 3. Clique em **Apply** para habilitar o serviço SSH.

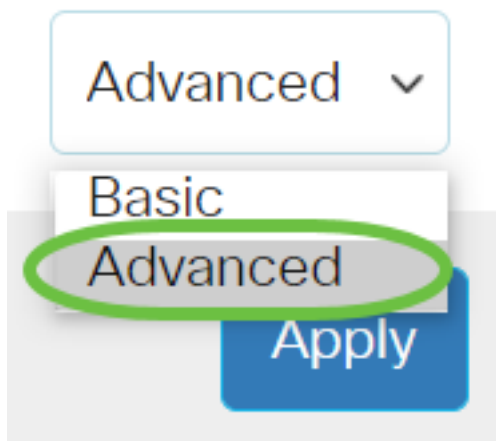


**Definir as configurações de autenticação de usuário SSH**

Use esta página para escolher um método de autenticação de usuário SSH. Você pode definir um nome de usuário e uma senha no dispositivo se o método de senha for escolhido. Você também pode gerar uma chave Ron Rivest, Adi Shamir e Leonard Adleman (RSA) ou Digital Signature Algorithm (DSA) se o método de chave pública ou privada estiver selecionado.

Os pares de chave padrão RSA e DSA são gerados para o dispositivo quando ele é inicializado. Uma dessas chaves é usada para criptografar os dados que estão sendo baixados do servidor SSH. A chave RSA é usada por padrão. Se o usuário excluir uma ou ambas essas chaves, elas serão regeneradas.

Etapa 1. Faça login no utilitário baseado na Web do seu switch e escolha Avançado na lista suspensa Modo de exibição.



Etapa 2. Escolha **Security > SSH Client > SSH User Authentication** no menu.

▼ Security

1

TACACS+ Client

RADIUS Client

▶ RADIUS Server

Password Strength

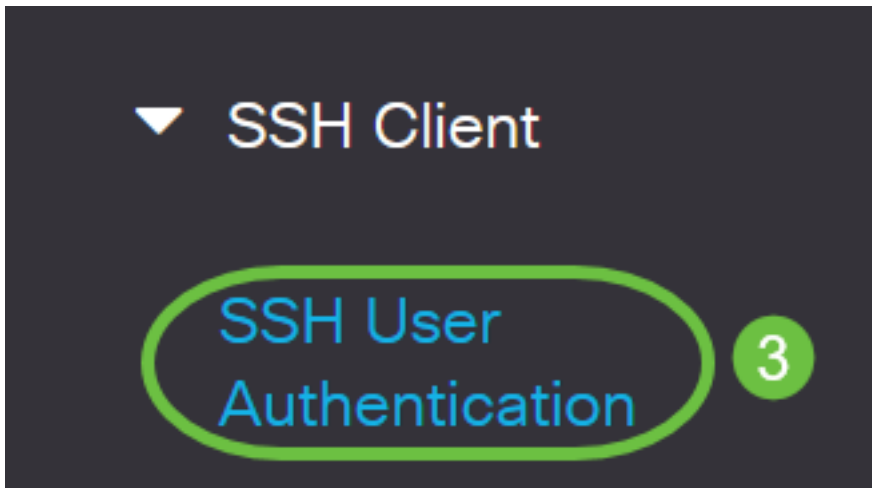
▶ Mgmt Access Method

Management Access  
Authentication

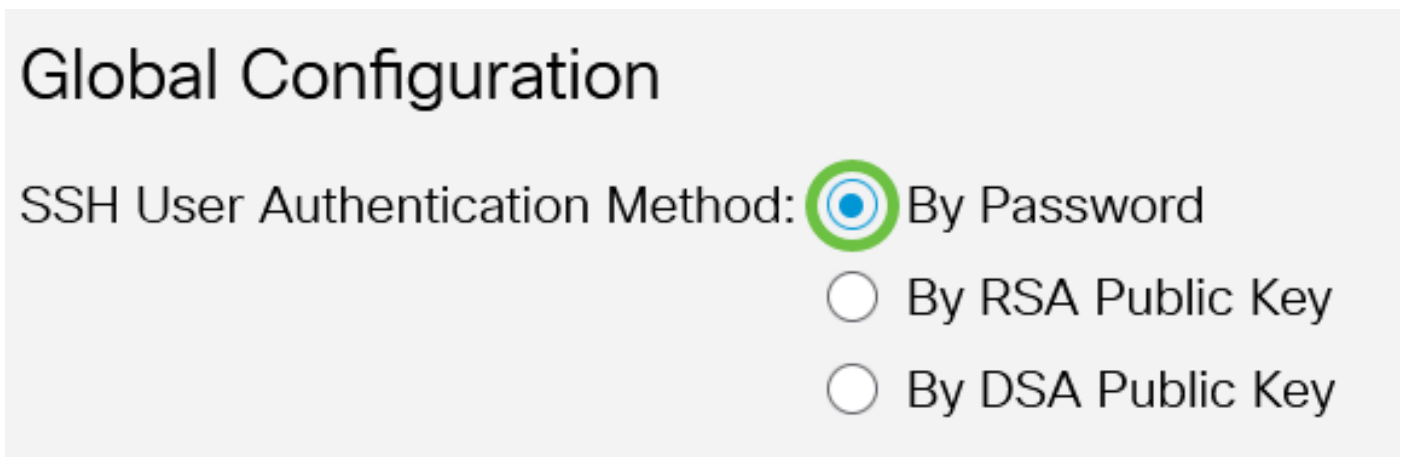
▶ Secure Sensitive Data  
Management

▶ SSL Server

▶ SSH Server



Etapa 3. Em Configuração global, clique no método de autenticação de usuário SSH desejado.



Quando um dispositivo (cliente SSH) tenta estabelecer uma sessão SSH para o servidor SSH, o servidor SSH usa um dos seguintes métodos para autenticação de cliente:

- Por senha - Esta opção permite configurar uma senha para autenticação do usuário. Essa é a configuração padrão e a senha padrão é anônima. Se essa opção for escolhida, verifique se as credenciais de nome de usuário e senha foram estabelecidas no Servidor SSH.
- Por chave pública RSA - Essa opção permite que você use a chave pública RSA para autenticação de usuário. Uma chave RSA é uma chave criptografada com base na fatorização de grandes números. Esta chave é o tipo mais comum de chave usado para autenticação de usuário SSH.
- Por chave pública DSA - Esta opção permite que você use uma chave pública DSA para autenticação do usuário. Uma chave DSA é uma chave criptografada com base no algoritmo discreto ElGamal. Essa chave não é comumente usada para autenticação de usuário SSH, pois leva mais tempo no processo de autenticação.

Neste exemplo, Por senha é escolhido.

Etapa 4. Na área Credenciais, digite o nome do usuário no campo *Nome de usuário*.

## Credentials

✳ Username:  (12/70 characters used)

✳ Password:  Encrypted

Plaintext  (Default Password: anonymous)

Neste exemplo, ciscosbuser1 é usado.

Etapa 5. (Opcional) Se você escolheu Por senha na etapa 2, clique no método e insira a senha no campo *Criptografado* ou *Texto simples*.

## Credentials

✳ Username:  (12/70 characters used)

✳ Password:  Encrypted

Plaintext  (Default Password: anonymous)

As opções são:

- Criptografado - Esta opção permite que você insira uma versão criptografada da senha.
- Texto sem formatação - Esta opção permite inserir uma senha em texto simples.

Neste exemplo, Texto simples é escolhido e uma senha de texto simples é inserida.

Etapa 6. Clique em **Apply** para salvar sua configuração de autenticação.

## SSH User Authentication

By RSA Public Key

By DSA Public Key

### Credentials

✳ Username:  (12/70 ch)

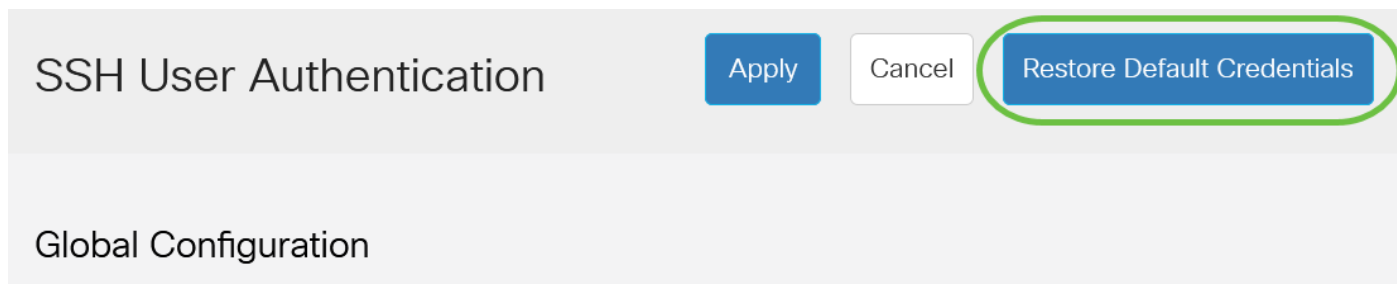
✳ Password:  Encrypted

Plaintext

**Apply** Cancel

Passo 7. (Opcional) Clique em **Restaurar credenciais padrão** para restaurar o nome de usuário e


a senha padrão e clique em **OK** para continuar.



SSH User Authentication Apply Cancel Restore Default Credentials

Global Configuration

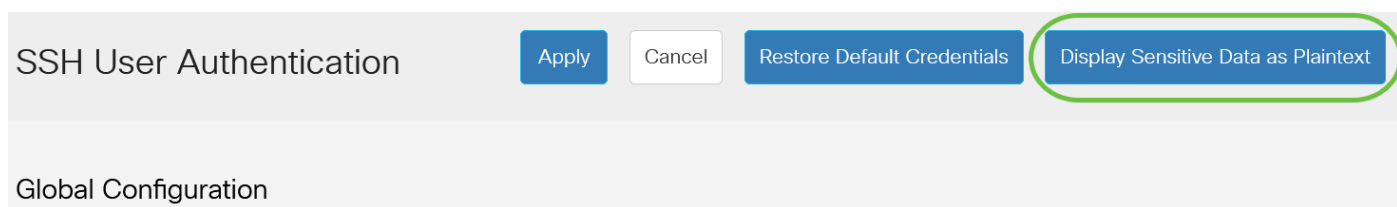
### Confirm Restore Default Credentials X

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

OK Cancel

O nome de usuário e a senha serão restaurados para os valores padrão: anônimo/anônimo.


Etapa 8. (Opcional) Clique em **Exibir dados confidenciais como texto não criptografado** para mostrar os dados confidenciais da página em formato de texto simples e clique em **OK** para continuar.



SSH User Authentication Apply Cancel Restore Default Credentials Display Sensitive Data as Plaintext

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?

OK Cancel

## Configurar tabela de chave de usuário SSH

Etapa 9. Marque a caixa de seleção da chave que deseja gerenciar.

## 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

Neste exemplo, RSA é escolhido.

Etapa 10. (Opcional) Clique em **Gerar** para gerar uma nova chave. A nova chave substituirá a chave selecionada e clique em **OK** 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?

 Cancel

Etapa 11. (Opcional) Clique em **Editar** para editar uma chave atual.



## 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

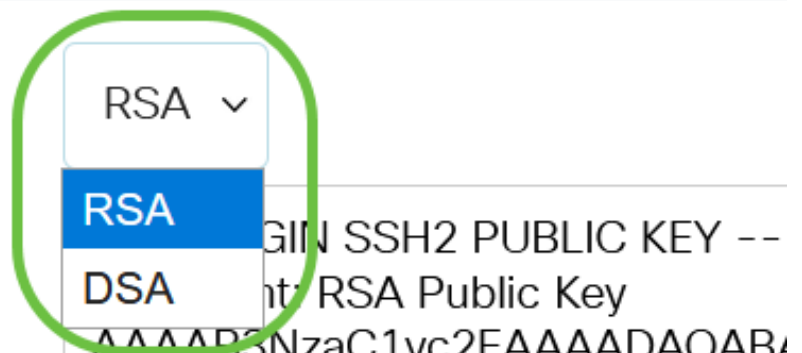
Etapa 12. (Opcional) Escolha um tipo de chave na lista suspensa Tipo de chave.

## 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 'Key Type' with 'RSA' selected. The menu options are 'RSA', 'DSA', and 'Other'. The 'RSA' option is highlighted in blue. The background shows a text field containing a public key starting with 'BEGIN SSH2 PUBLIC KEY --' and 'ssh-rsa'.

Neste exemplo, RSA é escolhido.

Etapa 13. (Opcional) Insira a nova chave pública no campo *Chave pública*.

## Edit SSH Client Authentication Settings

X

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  
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

Etapa 14. (Opcional) Insira a nova chave privada no campo *Private Key*.

Você pode editar a chave privada e clicar em Encrypted (Criptografado) para ver a chave privada atual como um texto criptografado ou Texto sem formatação para ver a chave privada atual em texto simples.

Etapa 15. (Opcional) Clique em **Exibir dados confidenciais como texto não criptografado** para mostrar os dados criptografados da página em formato de texto simples e clique em **OK** para continuar.

## Edit SSH Client Authentication Settings

X

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  
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



Etapa 16. Clique em **Apply** para salvar suas alterações e clique em **Close**.

## Edit SSH Client Authentication Settings

X

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

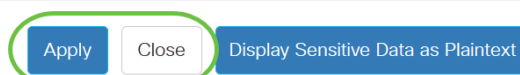
Key Type:

Public Key:

```
----- BEGIN SSH2 PUBLIC KEY -----  
Comment: RSA Public Key  
AAAAB3NzaC1yc2EAAAADAQABAAQCy9BJ+eTyaNva9u8G8VZgLqYuM8NHNoVh9WtPdKmBp004VvhTXfPqGCzg4/IIFlpm  
hf4ImgpX+XB7aLCI3Ch0vsuLJEahjrCS5iRCvEPrh9oUoec/GBCFhe7zXYHpRXkoGBC4I0SXBVS5xKpxuSwLIDsxgY10  
/9lpXWKK8uN2r7P2PVJI1APr2RnjUe1LVZTfrpMSqZ6UB+QtNtvaed46vTOWjgCb4+y+zFYpQjlvZCAuMoaWkljQFsiXMBOLL  
/D/cydxLa887DJQaMjPnu4G0PuQALWtT88h5hsHpZEhmcptoC00B+Auby0mXG6leE5bKFDpb2UFLJzHodD0fC9b  
----- END SSH2 PUBLIC KEY -----
```

Private Key:  Encrypted

Plaintext



Etapa 17. (Opcional) Clique em **Excluir** para excluir a chave selecionada.

## 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

Etapa 18. (Opcional) Depois que uma mensagem de confirmação for exibida, clique em **OK** para excluir a chave.

# 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?

OK

Cancel

Etapa 19. (Opcional) Clique em **Detalhes** para ver os detalhes da chave selecionada.

## SSH User Key Table

Generate



Details



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+RQnlR0Δ0z1I05G663mEMVcOT
```

Etapa 20. (Opcional) Clique no botão **Salvar** na parte superior da página para salvar as alterações no arquivo de configuração de inicialização.



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



## SSH User Authentication

Apply

Cancel

Res

Agora você definiu as configurações de autenticação de usuário cliente no switch Cisco Business 350 Series.