

在思科企业350系列交换机上配置安全外壳 (SSH) 用户身份验证设置

目标

本文提供有关如何在Cisco Business 350系列交换机上配置客户端用户身份验证的说明。

简介

安全外壳(SSH)是一种协议，可提供到特定网络设备的安全远程连接。此连接提供与Telnet连接类似的功能，但是它已加密。SSH允许管理员通过命令行界面(CLI)使用第三方程序配置交换机。

在通过SSH的CLI模式下，管理员可以在安全连接中执行更高级的配置。在网络管理员实际不在网络站点时，SSH连接在远程排除网络故障时非常有用。交换机允许管理员通过SSH对用户进行身份验证和管理，以连接到网络。身份验证通过用户可用于建立到特定网络的SSH连接的公钥进行。

SSH客户端功能是通过SSH协议运行以提供设备身份验证和加密的应用。它使设备能够与运行SSH服务器的另一设备建立安全且加密的连接。通过身份验证和加密，SSH客户端允许通过不安全的Telnet连接进行安全通信。

适用设备 | 软件版本

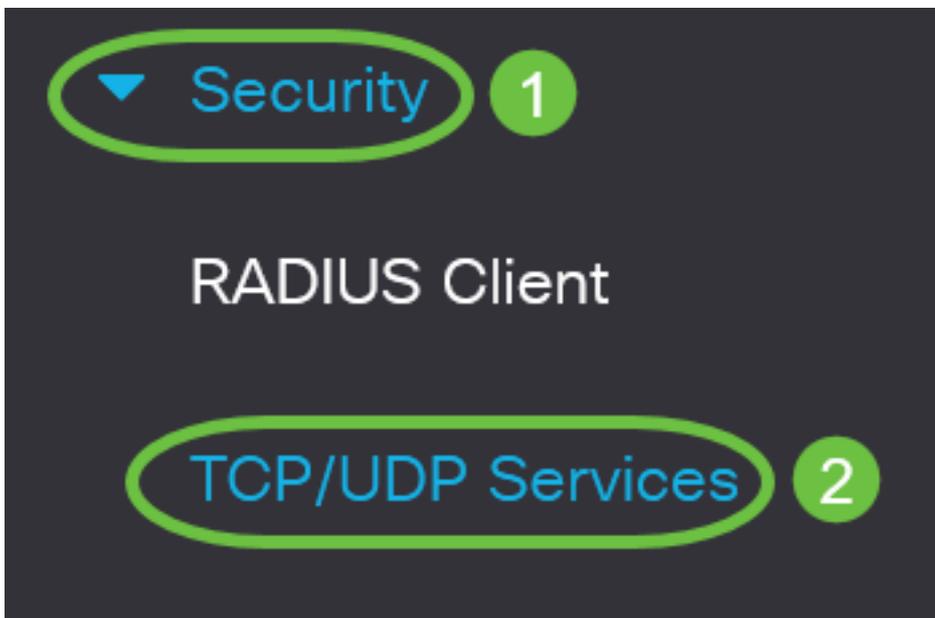
- CBS350 ([产品手册](#)) | 3.0.0.69([下载最新](#))
- CBS350-2X ([产品手册](#)) | 3.0.0.69([下载最新](#))
- CBS350-4X ([产品手册](#)) | 3.0.0.69([下载最新](#))

配置SSH客户端用户身份验证设置

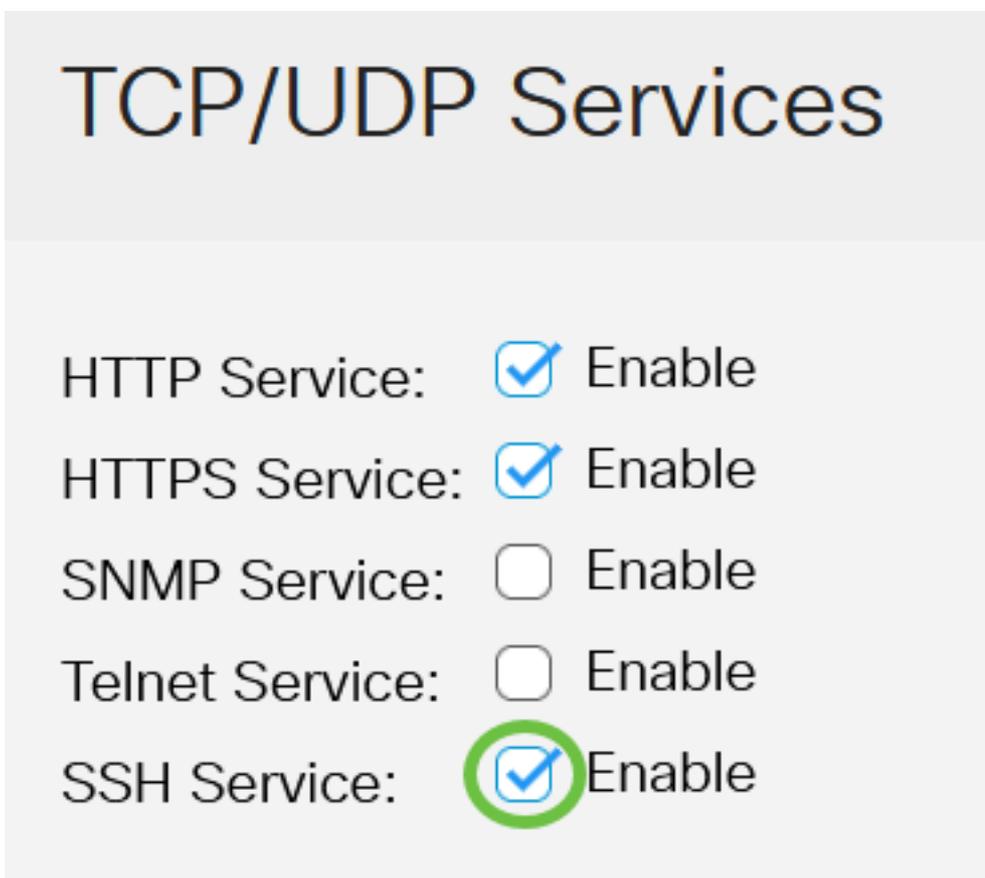
启用SSH服务

为了支持自动配置设备（出厂默认配置的设备），默认情况下禁用SSH服务器身份验证。

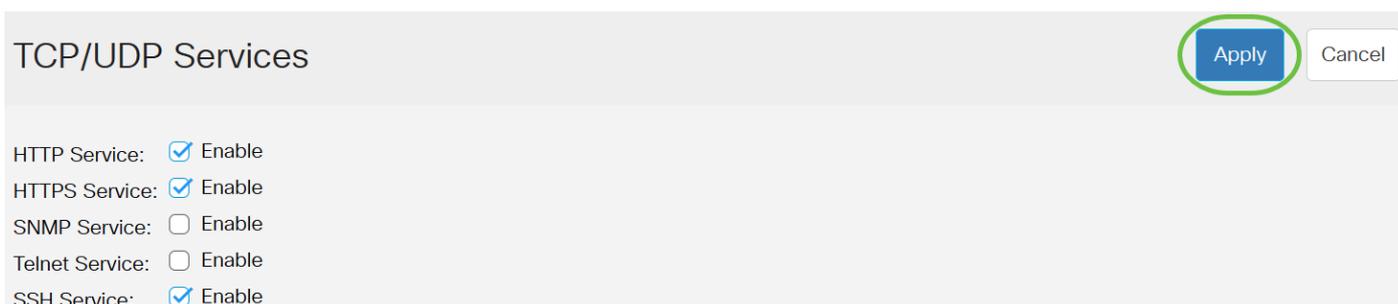
步骤1. 登录基于Web的实用程序，然后选择**Security > TCP/UDP Services**



步骤2.选中SSH Service复选框以通过SSH启用交换机命令提示符的访问。



步骤3.单击Apply以启用SSH服务。

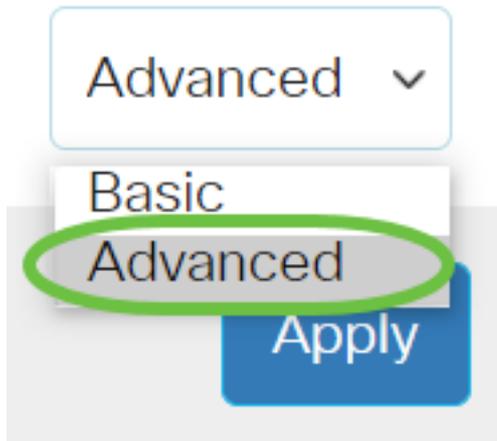


配置SSH用户身份验证设置

使用此页可选择SSH用户身份验证方法。如果选择了密码方法，则可以在设备上设置用户名和密码。如果选择了公钥或私钥方法，您还可以生成Ron Rivest、Adi Shamir和Leonard Adleman(RSA)或数字签名算法(DSA)密钥。

启动设备时，会为设备生成RSA和DSA默认密钥对。其中一个密钥用于加密从SSH服务器下载的数据。默认情况下使用RSA密钥。如果用户删除其中一个或两个密钥，则会重新生成它们。

步骤1.登录交换机的基于Web的实用程序，然后在Display Mode下拉列表中选择Advanced。



步骤2.从菜单中选择Security > SSH Client > SSH User Authentication。

▼ Security

1

TACACS+ Client

RADIUS Client

▶ RADIUS Server

Password Strength

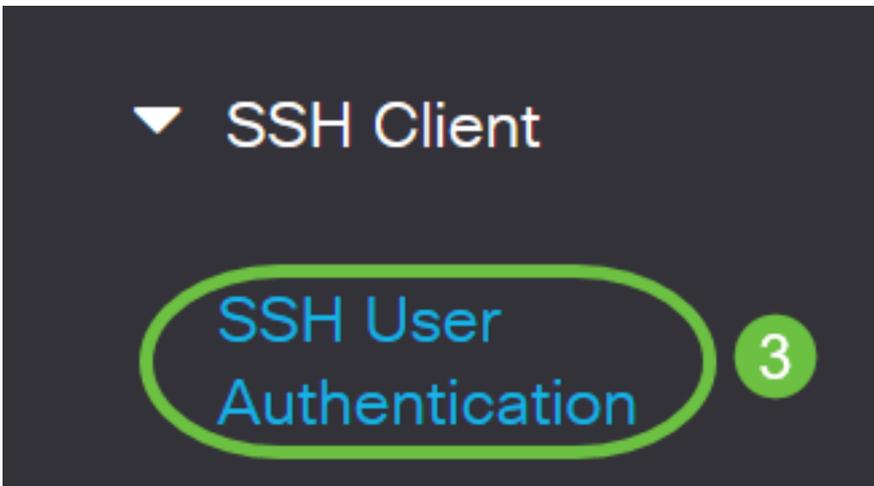
▶ Mgmt Access Method

Management Access
Authentication

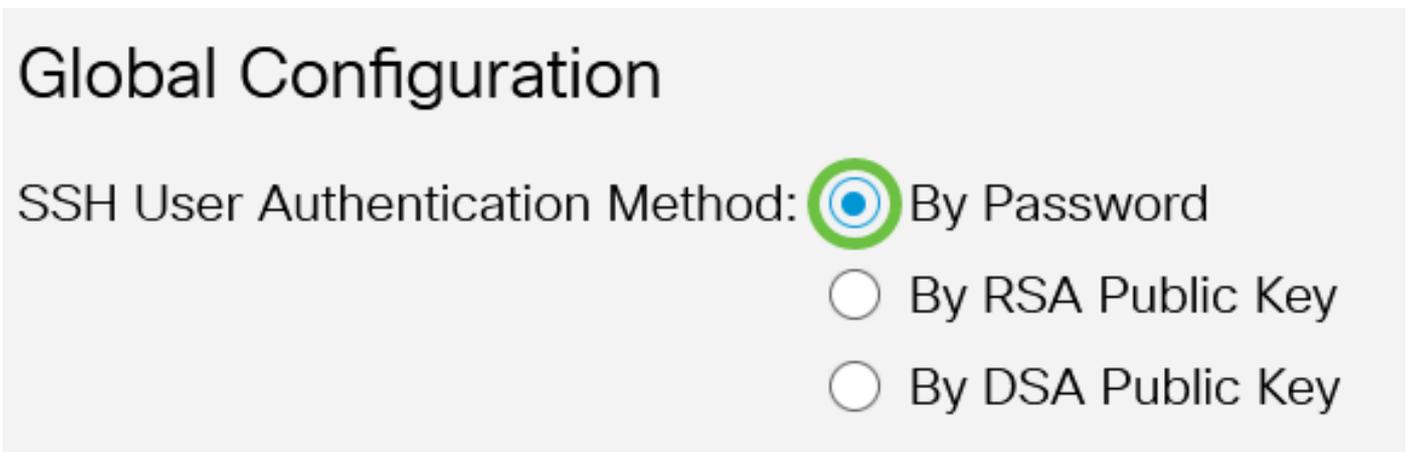
▶ Secure Sensitive Data
Management

▶ SSL Server

▶ SSH Server



步骤3.在Global Configuration (全局配置) 下，点击所需的SSH User Authentication Method (SSH用户身份验证方法)。



当设备 (SSH客户端) 尝试建立到SSH服务器的SSH会话时，SSH服务器使用以下方法之一进行客户端身份验证：

- By Password — 此选项允许您配置用户身份验证的密码。这是默认设置，默认密码为 anonymous。如果选择此选项，请确保已在SSH服务器上建立用户名和密码凭证。
- By RSA Public Key — 此选项允许您使用RSA公钥进行用户身份验证。RSA密钥是基于大整数分解的加密密钥。此密钥是用于SSH用户身份验证的最常见密钥类型。
- By DSA Public Key — 此选项允许您使用DSA公钥进行用户身份验证。DSA密钥是基于 ElGamal离散算法的加密密钥。此密钥不常用于SSH用户身份验证，因为在身份验证过程中需要更多时间。

在本例中，选择By Password。

步骤4.在“凭证”区域的“用户名”字段中输入用户名。



在本例中，使用ciscosobuser1。

步骤5. (可选) 如果您在步骤2中选择了By Password , 请点击方法 , 然后在Encrypted或Plaintext字段中输入密码。

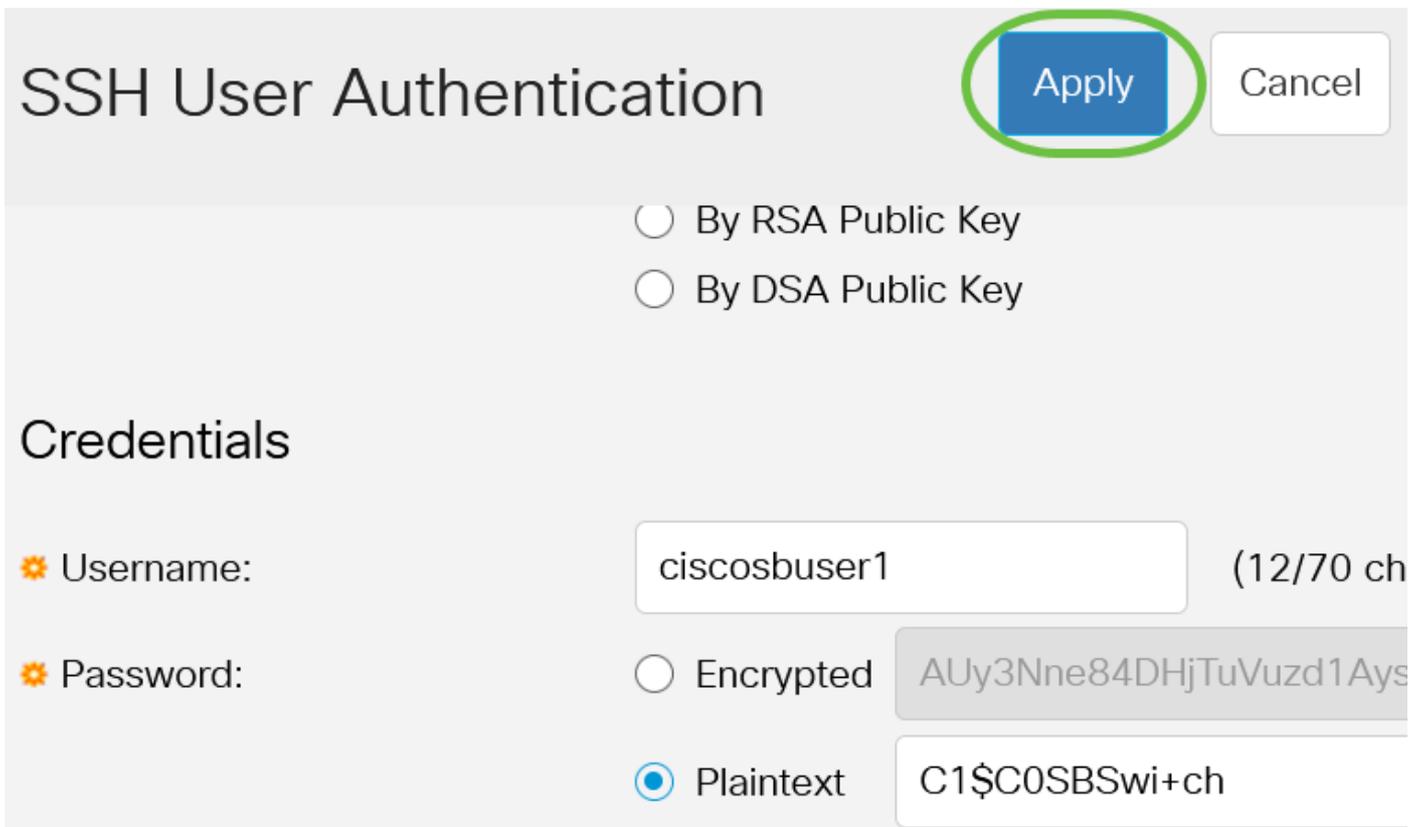


选项有 :

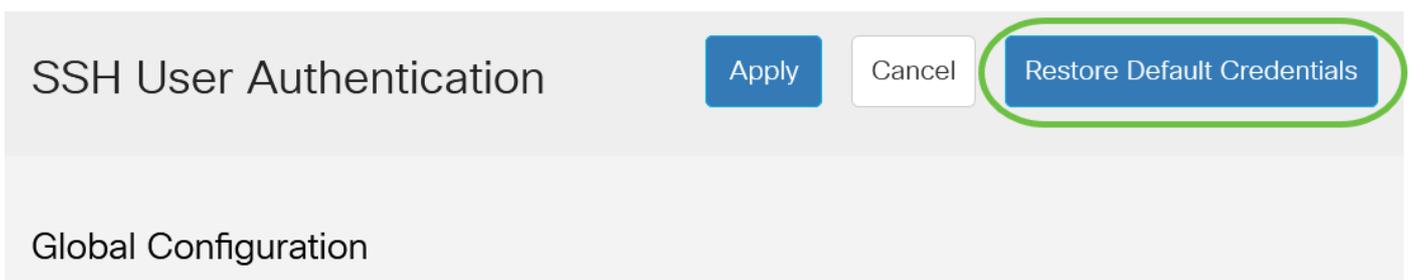
- Encrypted — 此选项允许您输入密码的加密版本。
- 纯文本 — 此选项允许您输入纯文本密码。

在本示例中 , 选择纯文本并输入纯文本密码。

步骤6.单击“应用”保存身份验证配置。



第7步. (可选) 单击“恢复默认凭据”以恢复默认用户名和密码 , 然后单击确定继续操作。

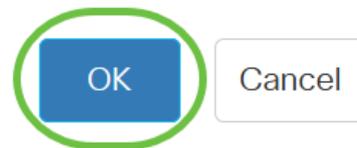


Confirm Restore Default Credentials

X

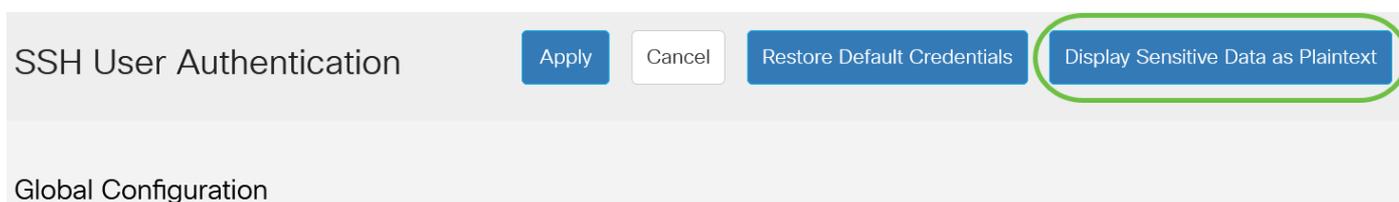


The Username and Password will be restored to the default values (anonymous/anonymous). Do you want to continue?



用户名和密码将恢复为默认值：匿名/匿名。

第8步。(可选)单击**Display Sensitive Data as Plaintext**以纯文本格式显示页面的敏感数据，然后单击**OK**继续。

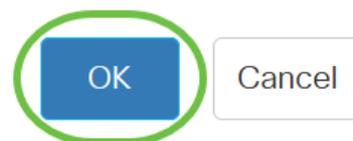


Confirm Display Method Change

X



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



配置SSH用户密钥表

步骤9.选中要管理的密钥的复选框。

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 |

在本例中，选择RSA。

步骤10。(可选)单击**Generate**以生成新密钥。新密钥将覆盖选中的密钥，然后单击**确定**继续。

SSH User Key Table

| <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?

步骤11. (可选) 单击“编辑”以编辑当前密钥。

SSH User Key Table

| <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 |

步骤12. (可选) 从Key Type下拉列表中选择密钥类型。

Edit SSH Client Authentication Settings

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

Key Type:

Public Key:



在本例中，选择RSA。

步骤13. (可选) 在Public Key字段中输入新公钥。

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/llFlpm  
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

步骤14. (可选) 在私钥字段中输入新的私钥。

您可以编辑私钥，并点击Encrypted以将当前私钥显示为加密文本，或点击Plaintext以明文查看当前私钥。

第15步。(可选) 单击Display Sensitive Data as Plaintext(将敏感数据显示为纯文本格式)以显示页面的加密数据，然后单击OK(确定)以继续。

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  
/9lpXWKK8uN2r7P2PVJI1APr2RnjUe1LVZTfrpMSqZ6UB+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

OK

Cancel

步骤16.单击“应用”保存更改，然后单击“关闭”。

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  
hf4ImgpX+XB7aLCi3Ch0vsuLJEahjrCS5iRCvEPrh9oUoec/GBCFhe7zXYHPrXkoGBC4I0SXbVS5xKpxuSwLIDsxgY10  
/9lpXWKK8uN2r7P2PVJI1APr2RnjlUe1LVZTfrpMSqZ6UB+QtNtvaed46vTowjgCb4+y+zFYpQjlvZCAuMoaWkljQfslXMBOLL  
/D/cydxLa887DJQaMjPnu4G0PuQALWtT88h5hsHpZEhmcptoC00B+Auby0mXG6leE5bKFDpb2UFLJzHodD0fC9b  
----- END SSH2 PUBLIC KEY -----
```

Private Key: Encrypted

Plaintext

Apply

Close

Display Sensitive Data as Plaintext

步骤17. (可选) 单击“删除”删除选中的键。

SSH User Key Table

Generate



Details

| <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 |

步骤18. (可选) 在出现确认消息提示后，单击“确定”以删除密钥。

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?

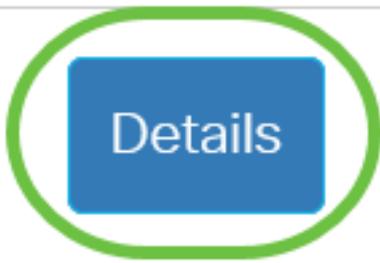
OK

Cancel

步骤19. (可选) 单击**Details**查看选中键的详细信息。

SSH User Key Table

Generate



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=CxBoUggllUWLBwkarVUG9jbM4OQUdSPdr
VmHGNkIRJVg3nxO2wmw10xcYy7YZLPaoriNd/obTuGZ4jOqhSgfQckqhibcSNdlaUrw
w1v4QBwH8UbGNw1yV/SaECMuFre/VzYdRP
/RvGDNCNOphqMMJyCQ3D+WG2136I+li+U3Kn9BObOsSn+gz7c1OvNoXQ9t+NvtJDF
3MfMhmvwX0XIEKgMZgV+ennjipMPja0FP8HGblh
/hOPdhUIPmaRheE3hsDS1S9TJXLu7RnG0TrknL+QUFqZeRT3jSablwZsaGyE8oklpP5E
K9qsLJZlqeMm2gWjziB
----- END SSH2 PUBLIC KEY -----
Private Key (Encrypted): ----- BEGIN SSH2 ENCRYPTED PRIVATE KEY -----
Comment: RSA Private Key
AkNK2himPem2VeoSwyp0U+1FXk81mva9RGX2rBMhCDIj/79rYDLBnYKdSHk3A7Hqg0
aDjeLKVROxyRccQ0UivFp70SYz6mmjfrvwAXgCnZonkhv8WO+Ktz0tLliHAj2gWaXerYB
D5suizX+RQnlR0A0z1I05G663mEMVcOT

步骤20. (可选) 单击页面顶部的 **Save** 按钮，将更改保存到启动配置文件。



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



SSH User Authentication

Apply

Cancel

Res

您现在已在Cisco Business 350系列交换机上配置了客户端用户身份验证设置。