

SG350XG和SG550XG交换机的客户端安全外壳 (SSH)用户身份验证

目标

安全外壳(SSH)是一种协议，可提供到特定设备的安全远程连接。350XG和550XG系列托管交换机允许您对用户进行身份验证和管理，以便通过SSH连接到设备。身份验证通过公钥进行，因此用户可以使用此密钥建立到特定设备的SSH连接。如果网络管理员不在网络站点，SSH连接对远程排除网络故障非常有用。

本文介绍如何在SG350XG和SG550XG系列托管交换机上配置客户端用户身份验证。

适用设备

- SG350XG
- SG550XG

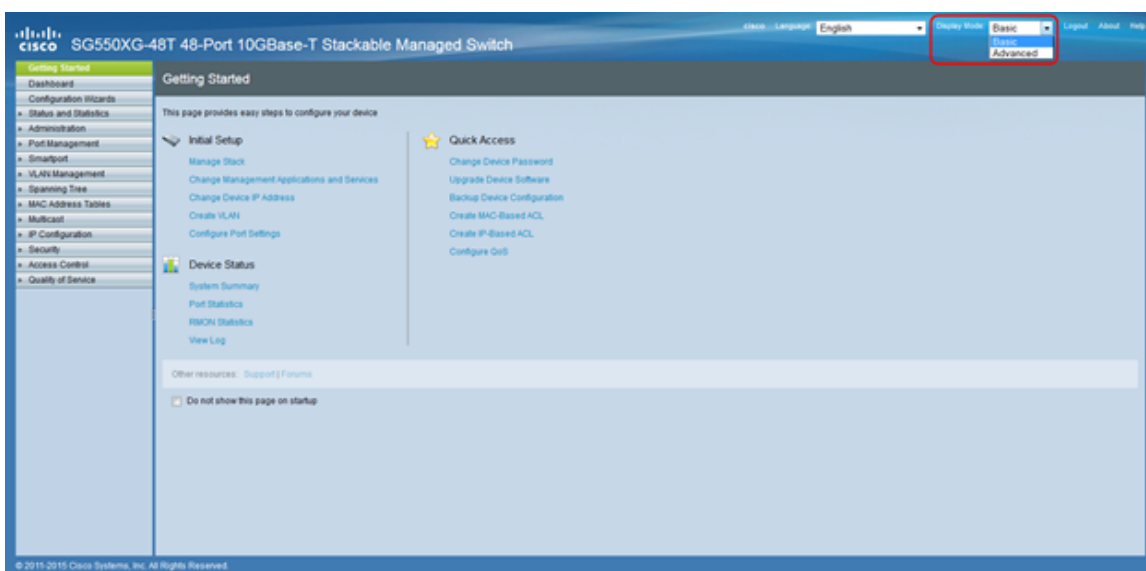
软件版本

- v2.0.0.73

配置SSH 客户端 身份验证

全局配置

注意：以下屏幕截图来自“高级显示”。单击屏幕右上角的 *Display Mode* 下拉列表可切换此选项



步骤1. 登录Web配置实用程序，然后选择Security > SSH Client > SSH User Authentication。“SSH用户身份验证”页面打开：

SSH User Authentication

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: anonymous)

SSH User Key Table

<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input type="checkbox"/>	RSA	Auto Generated	6f:bf:d8:12:60:74:ea:4c:68:a1:76:91:e5:8f:a4:d1
<input type="checkbox"/>	DSA	Auto Generated	24:31:b0:3c:5c:94:74:35:ba:d1:ce:c6:f7:16:84:48

步骤2.在“SSH用户身份验证方法”字段中，单击所需全局身份验证方法的单选按钮。

SSH User Authentication

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: anonymous)

可用选项如下：

- By Password — 此选项允许您配置用户身份验证的密码。输入密码或保留默认密码“anonymous”。
- By RSA Public Key — 此选项允许您使用RSA公钥进行用户身份验证。RSA用于加密和签名。如果选择此选项，请在SSH用户密钥表块中创建RSA公钥和私钥。
- By DSA Public Key — 此选项允许您使用DSA公钥进行用户身份验证。DSA仅用于签名。如果选择此选项，请在SSH用户密钥表块中创建DSA公钥/私钥。

步骤3.找到“凭证”区域。在用户名字段中输入用户名。

SSH User Authentication

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: anonymous)

Apply Cancel Restore Default Credentials Display Sensitive Data as Plaintext

步骤4.如果在步骤2中选择了 [By Password](#)，请单击“Password”字段中所需密码方法的单选按钮。默认密码为“anonymous”。

SSH User Authentication

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: anonymous)

Apply Cancel Restore Default Credentials Display Sensitive Data as Plaintext

可用选项如下所述：

- Encrypted — 输入加密密码。
- 明文 — 输入明文密码。

步骤5.单击“应用”保存身份验证配置。

SSH User Authentication

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: anonymous)

Apply Cancel Restore Default Credentials Display Sensitive Data as Plaintext

步骤6. (可选) 要恢复默认用户名和密码，请点击“恢复默认凭据”。默认密码为“anonymous”。

SSH User Authentication

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: anonymous)

步骤7. (可选) 要将敏感数据显示为明文或加密文本，请点击Display Sensitive Data as Plaintxt/Encrypted。

SSH User Authentication

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: anonymous)

注意：按钮的名称会根据当前设置而改变。该按钮将始终切换数据显示。

SSH用户密钥表

本节介绍如何管理SSH用户表。

步骤1.导航至SSH用户密钥表。在显示的列表中，选中您要管理的密钥左侧的复选框。

SSH User Key Table

<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	User Defined	8e:06:e1:fe:ab:4d:1f:cf:14:5c:e3:11:cd:8f:1e:8a
<input type="checkbox"/>	DSA	User Defined	6a:b3:3e:9e:83:c3:3b:da:57:f7:29:89:15:a7:dc:0c

步骤2. (可选) 单击Generate以生成新密钥。新密钥将覆盖所选密钥。将弹出一个确认窗口。单击 OK 继续。

SSH User Key Table

<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	User Defined	8e:06:e1:fe:ab:4d:1f:cf:14:5c:e3:11:cd:8f:1e:8a
<input type="checkbox"/>	DSA	User Defined	6a:b3:3e:9e:83:c3:3b:da:57:f7:29:89:15:a7:dc:0c

步骤3. (可选) 单击“删除”以删除选定的键。将弹出一个确认窗口。单击 OK 继续。

SSH User Key Table			
<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	User Defined	8e:06:e1:fe:ab:4d:1f:cf:14:5c:e3:11:cd:8f:1e:8a
<input type="checkbox"/>	DSA	User Defined	6a:b3:3e:9e:83:c3:3b:da:57:f7:29:89:15:a7:dc:0c

步骤4. (可选) 单击“详细信息”以查看所选键的详细信息。

SSH User Key Table			
<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	User Defined	8e:06:e1:fe:ab:4d:1f:cf:14:5c:e3:11:cd:8f:1e:8a
<input type="checkbox"/>	DSA	User Defined	6a:b3:3e:9e:83:c3:3b:da:57:f7:29:89:15:a7:dc:0c

系统将显示SSH User Key Details页面。单击Back返回SSH用户密钥表。

SSH User Key Details

SSH Server Key Type: RSA

Public Key: ---- BEGIN SSH2 PUBLIC KEY ----
 Comment: RSA Public Key
 AAAAB3NzaC1yc2EAAAADAQABAAQCAeTjr4/8xsROwDkFBY7efsV5v59RNAwzJdZsxb
 XRqFXeMQ2LNyUTCK8hcu0zVSipsQ8AFRZmpnaVKEgSunFK5YYJ2AckP9NyMikihWfRWm
 UXT6SBOK/Bjk7GPXhcs0JE6II3uPCyiC50vzGRBGhWSH/oGBxMqkavDGpcToaDyKQ==
 ---- END SSH2 PUBLIC KEY ----

Private Key (Encrypted): ---- BEGIN SSH2 ENCRYPTED PRIVATE KEY ----
 Comment: RSA Private Key
 [Blurred Private Key Content]
 ---- END SSH2 PRIVATE KEY ----

步骤5.单击“编辑”以编辑选定的键。

SSH User Key Table			
<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	User Defined	8e:06:e1:fe:ab:4d:1f:cf:14:5c:e3:11:cd:8f:1e:8a
<input type="checkbox"/>	DSA	User Defined	6a:b3:3e:9e:83:c3:3b:da:57:f7:29:89:15:a7:dc:0c

“编辑SSH客户端身份验证设置”(Edit SSH Client Authentication Settings)窗口打开：

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  
AAAAB3NzaC1yc2EAAAADAQABAAQCAeTjr4/8xsROwDkFBY7efsV5v59RNAwzJdZsxbXRqF;  
-----END SSH2 PUBLIC KEY -----
```

Private Key: Encrypted

Plaintext

步骤6.从Key Type下拉列表中选择所需的键类型。

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  
AAAAB3NzaC1yc2EAAAADAQABAAQCAeTjr4/8xsROwDkFBY7efsV5v59RNAwzJdZsxbXRqF;  
-----END SSH2 PUBLIC KEY -----
```

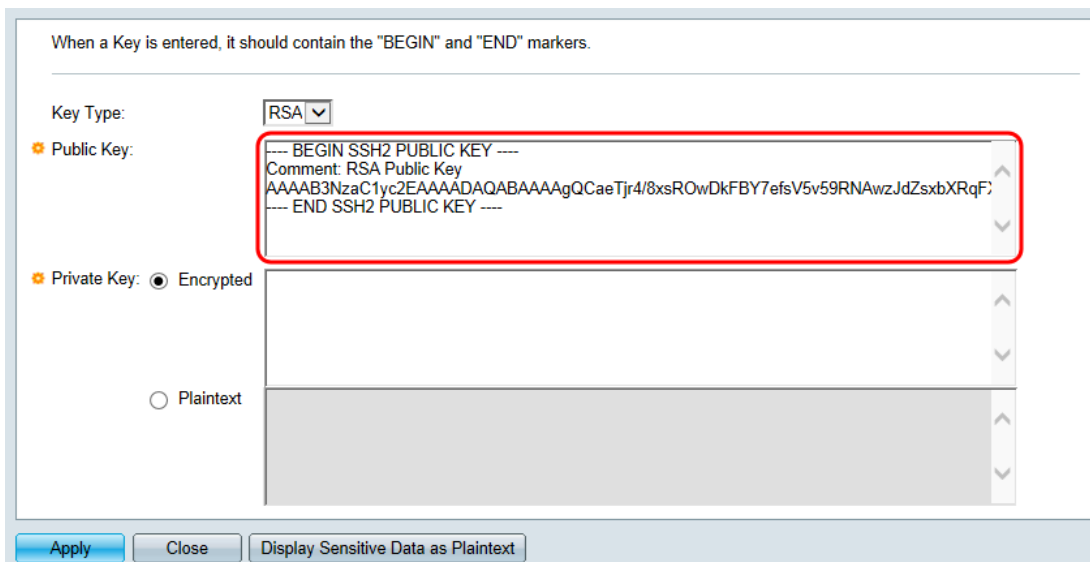
Private Key: Encrypted

Plaintext

可用选项如下：

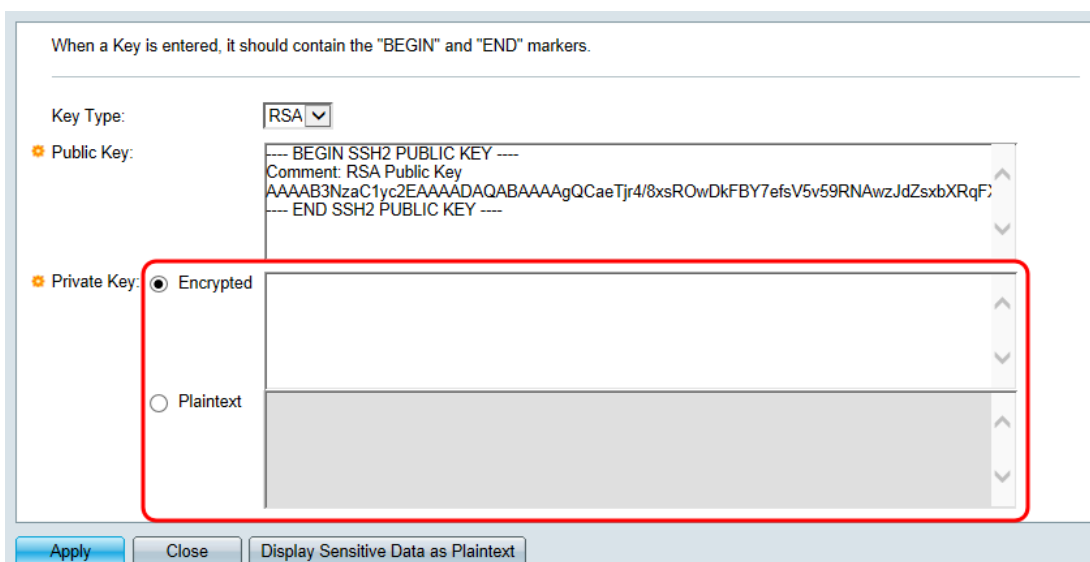
- RSA - RSA用于加密和签名。
- DSA - DSA仅用于签名。

步骤7.在Public Key字段中，可以编辑当前公钥。



步骤8.在私钥字段中，可以编辑当前私钥。单击

加密单选按钮，查看当前私钥是否已加密。否则，单击**Plaintext** 单选按钮以将当前私钥显示为纯文本。



步骤9.单击“应用”保存更改。

