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

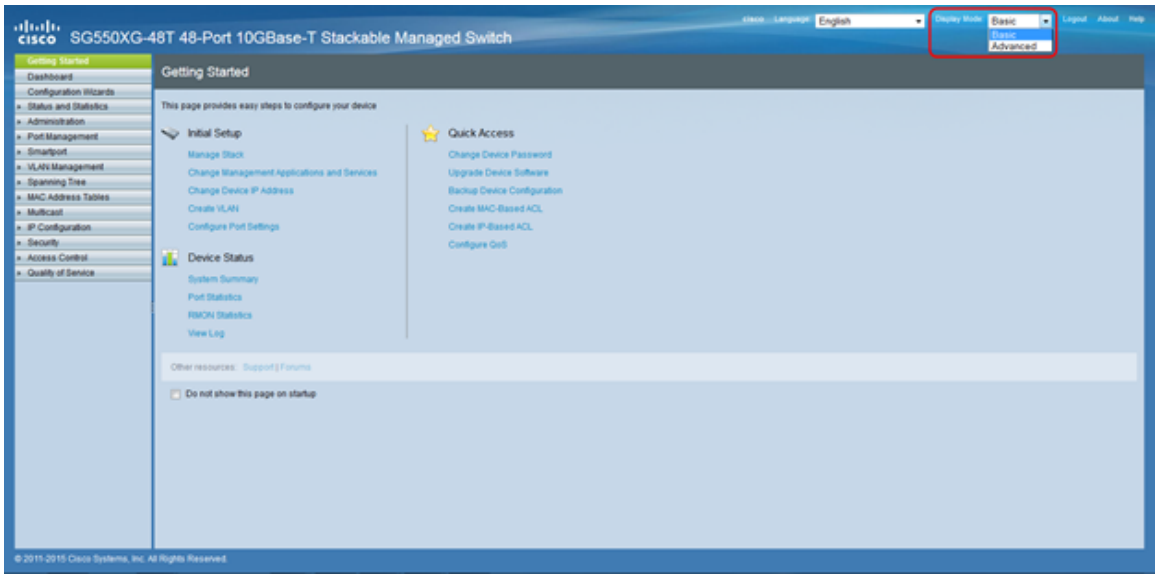
软件版本

- v2.0.0.73

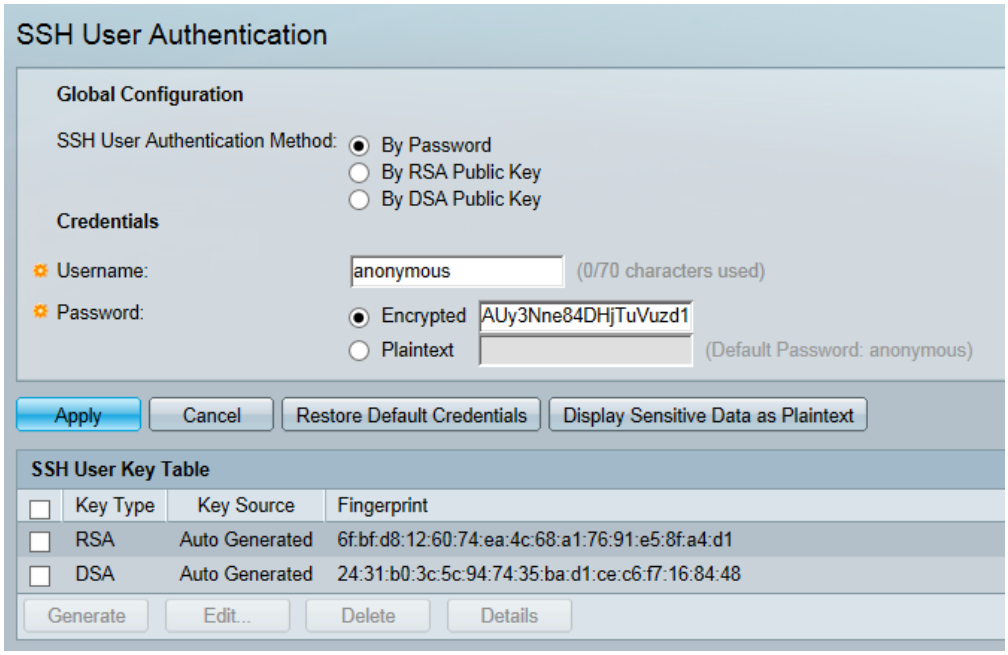
配置SSH 客户端 身份验证

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：



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。

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。

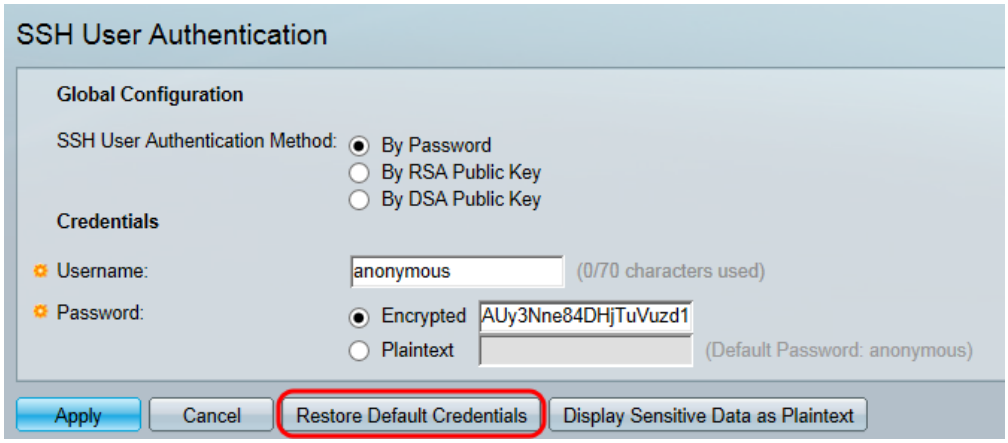
步骤4.如果在**步骤2**中选择了By Password，请单击“Password”字段中所需密码方法的单*选按*钮。默认密码为“anonymous”。

可用选项如下所述：

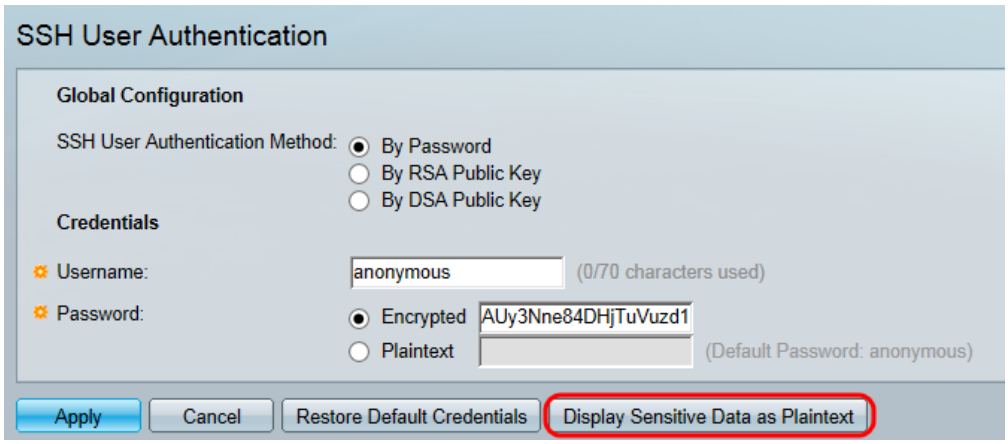
- Encrypted — 输入加密密码。
- 明文 — 输入明文密码。

步骤5.单击“**应用**”保存身份验证配置。

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”。



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。

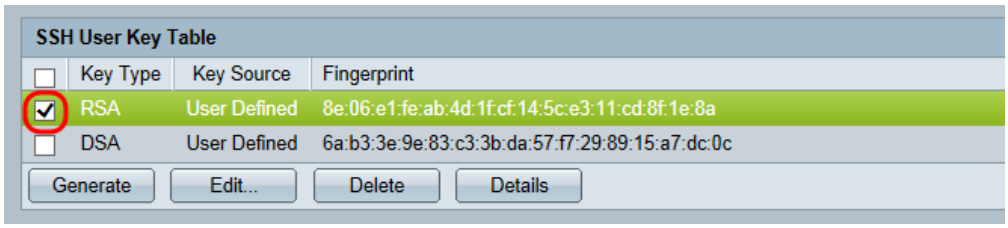


注意：按钮的名称会根据当前设置而改变。该按钮将始终切换数据显示。

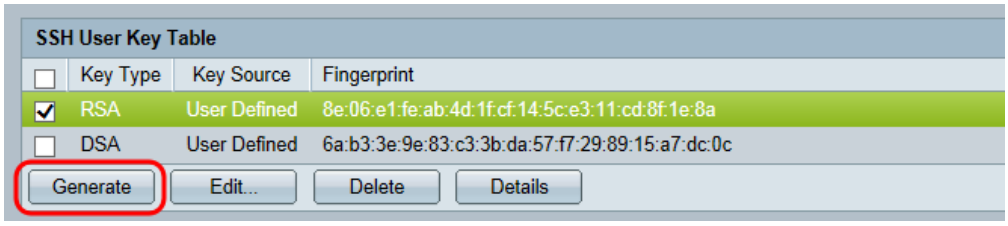
SSH用户密钥表

本节介绍如何管理SSH用户表。

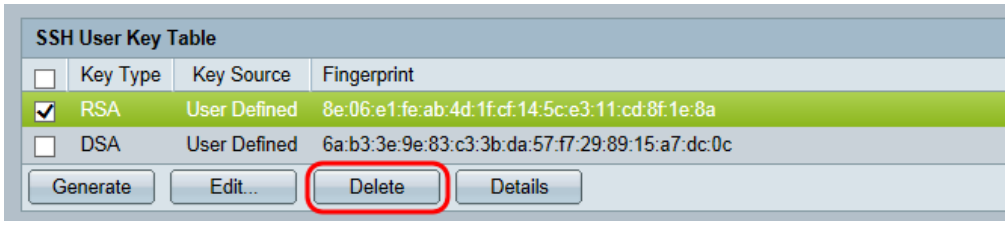
步骤1.导航至SSH*用户密钥表*。在显示的列表中，选中您要管理的密钥左侧的复选框。



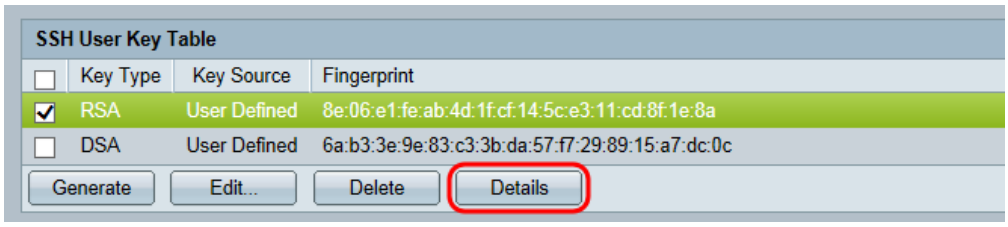
步骤2.（可选）单击**Generate**以生成新密钥。新密钥将覆盖所选密钥。将弹出一个确认窗口。单击 **OK** 继续。



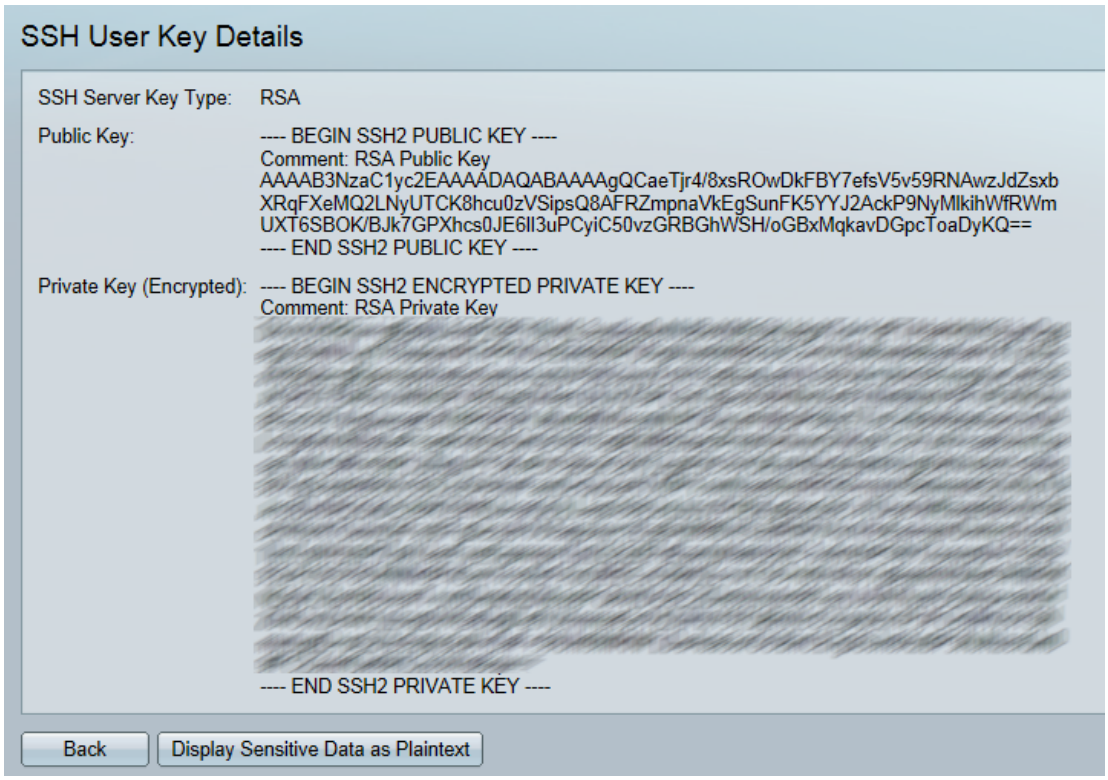
步骤3.（可选）单击“**删除**”以删除选定的键。将弹出一个确认窗口。单击 **OK** 继续。



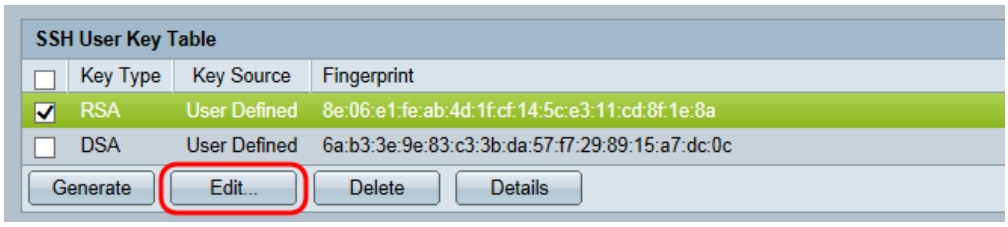
步骤4.（可选）单击“详细**信息**”以查看所选键的详细信息。



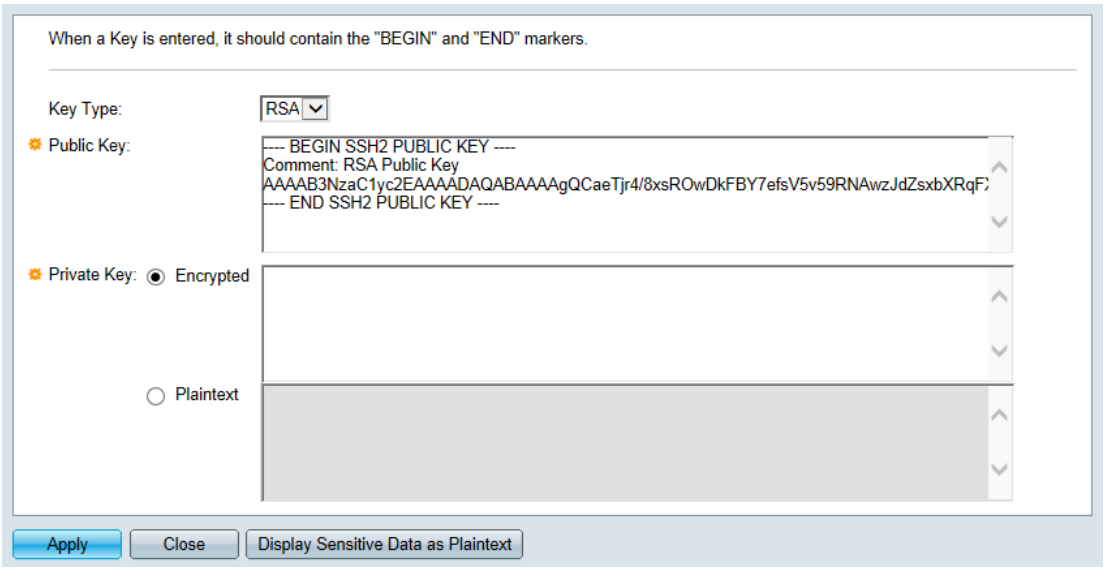
系统将显示SSH User Key Details页面。单击**Back**返回SSH用户密钥表。



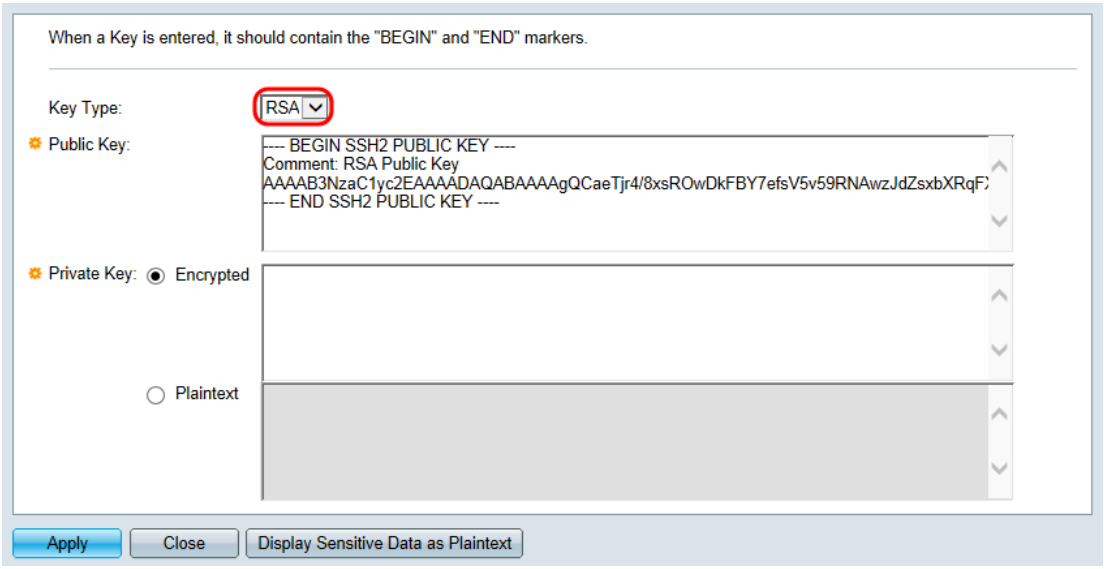
步骤5.单击“编**辑**”以编辑选定的键。



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



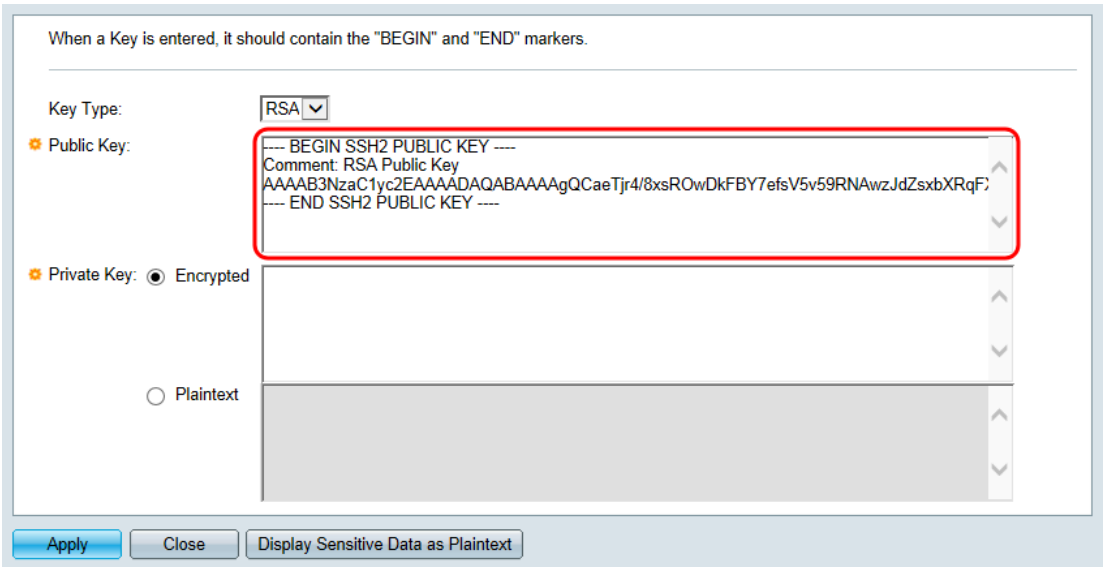
步骤6.从Key Type下拉列表中选*择所需*的键类型。



可用选项如下：

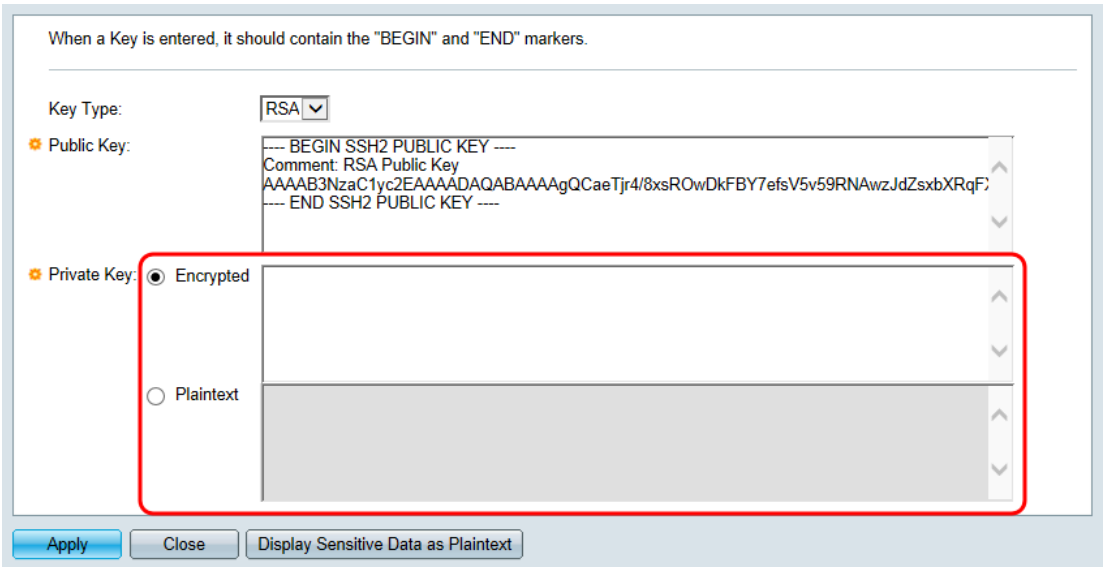
- RSA - RSA用于加密和签名。
- DSA - DSA仅用于签名。

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。