在交换机上配置安全外壳(SSH)用户身份验证设置

目标

Secure Shell(SSH)协议可提供到特定网络设备的远程安全连接。此连接提供的功能与Telnet连接类似，不同之处在于它经过了加密。SSH允许管理员使用第三方程序通过命令行界面(CLI)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。如果网络管理员实际上不在网络站点，则SSH连接对于远程排除网络故障非常有用。交换机让管理员验证和管理用户通过SSH连接到网络。身份验证通过公共密钥进行，用户可以使用公共密钥建立到特定网络的SSH连接。

SSH客户端功能是通过SSH协议运行的应用程序，用于提供设备身份验证和加密。它使设备能够与运行SSH服务器的另一设备建立安全加密连接。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。

本文介绍如何在受管交换机上配置客户端用户身份验证。

适用设备

- Sx200系列
- Sx300系列
- Sx350 系列
- SG350X 系列
- Sx500 系列
- Sx550X 系列

软件版本

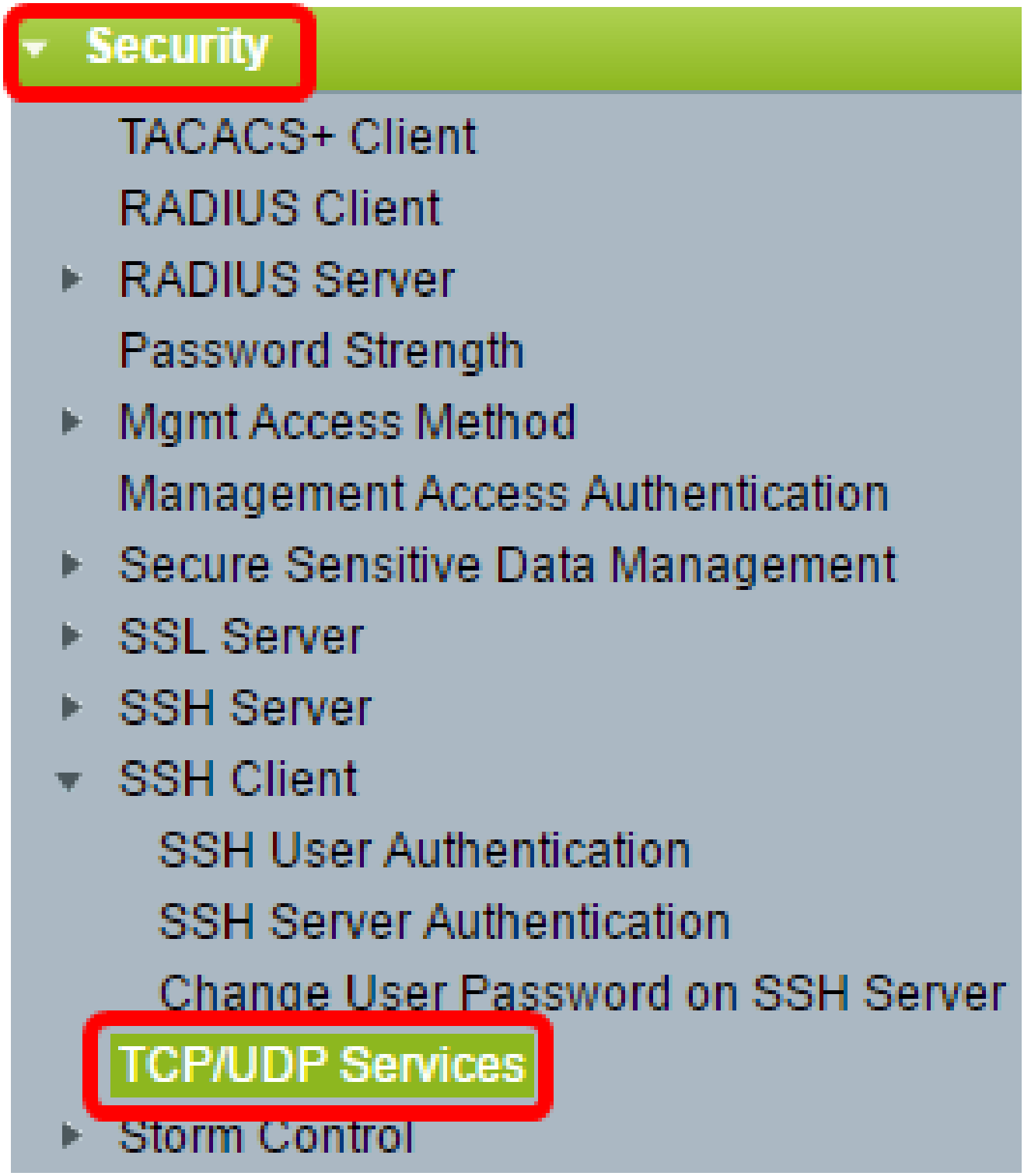
- 1.4.5.02 - Sx200系列、Sx300系列、Sx500系列
- 2.2.0.66 - Sx350系列、SG350X系列、Sx550X系列

配置SSH客户端用户身份验证设置

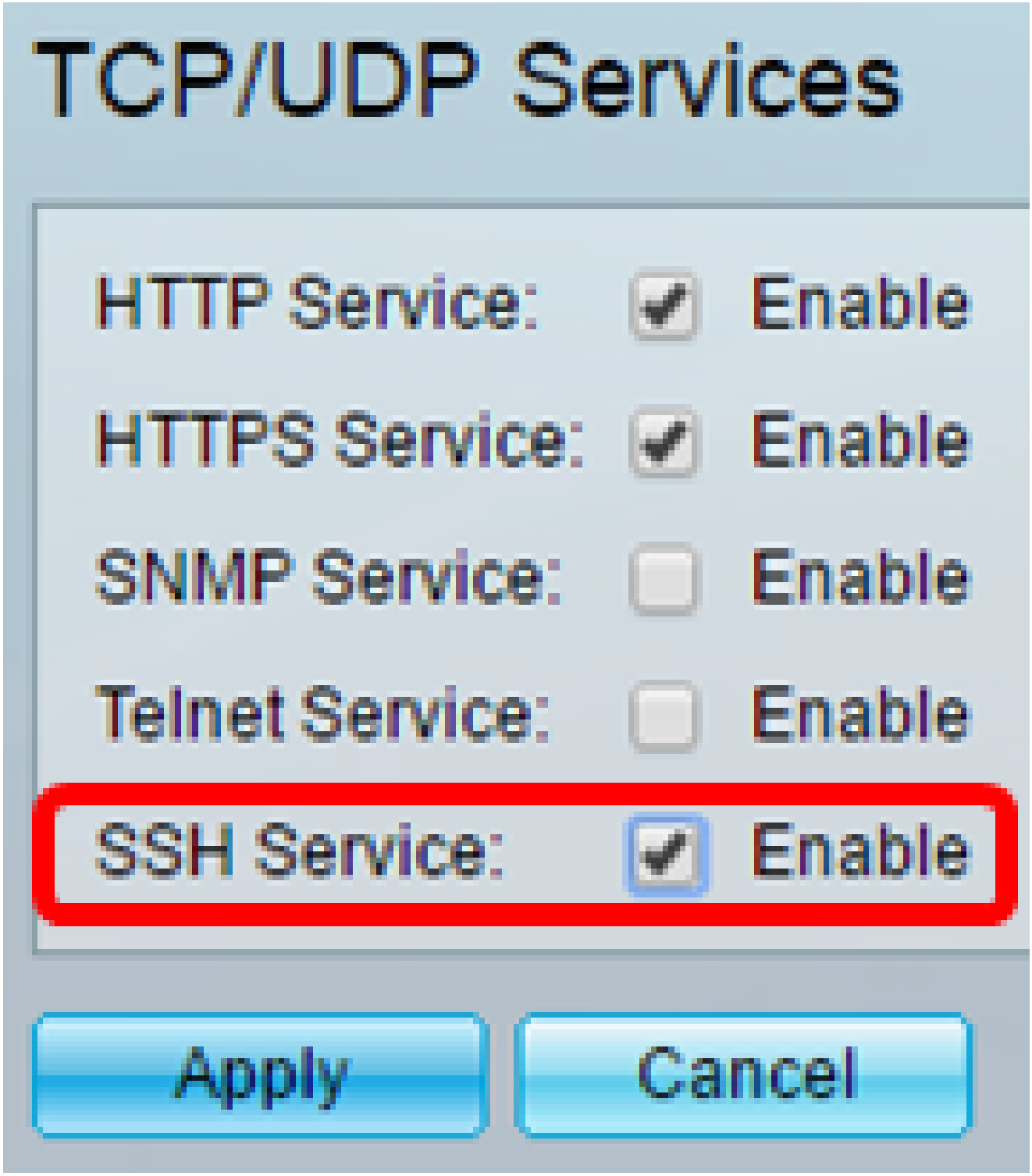
启用SSH服务

注意：为了支持开箱即用设备（出厂默认配置的设备）的自动配置，默认情况下禁用SSH服务器身份验证。

步骤1:登录到基于Web的实用程序并选择安全> TCP/UDP服务



第二步：选中SSH Service复选框以启用通过SSH访问交换机命令提示符。



第三步：单击Apply以启用SSH服务。

配置SSH用户身份验证设置

使用此页可以选择SSH用户身份验证方法。如果选择密码方法，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。

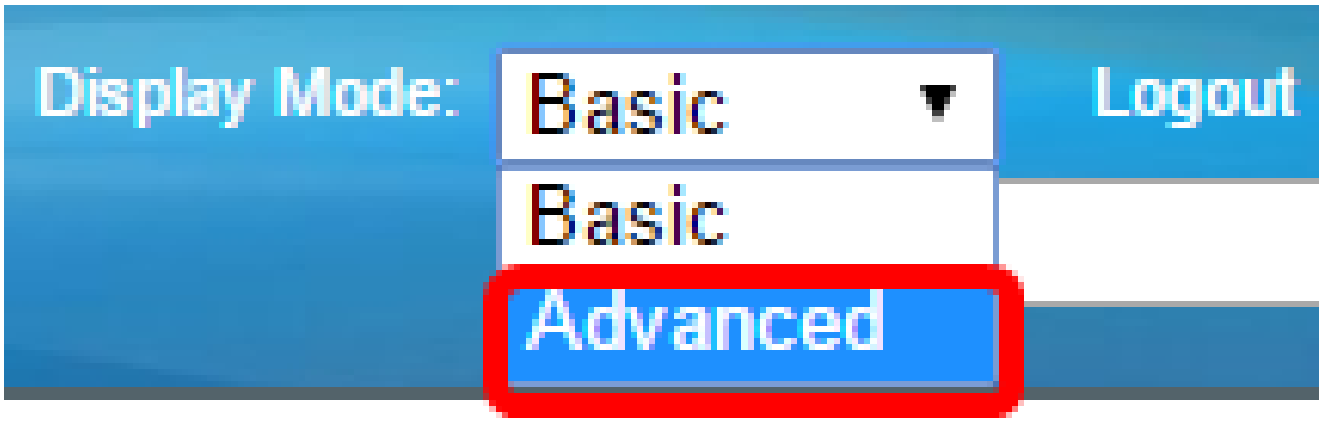
RSA和DSA默认密钥对会在设备启动时生成。其中一个密钥用于加密从SSH服务器下载的数据。默认情况下使用RSA密钥。如果用户删除其中一个或两个密钥，则重新生成这些密钥。

步骤1:登录到基于Web的实用程序，然后选择Security > SSH Client > SSH User Authentication。

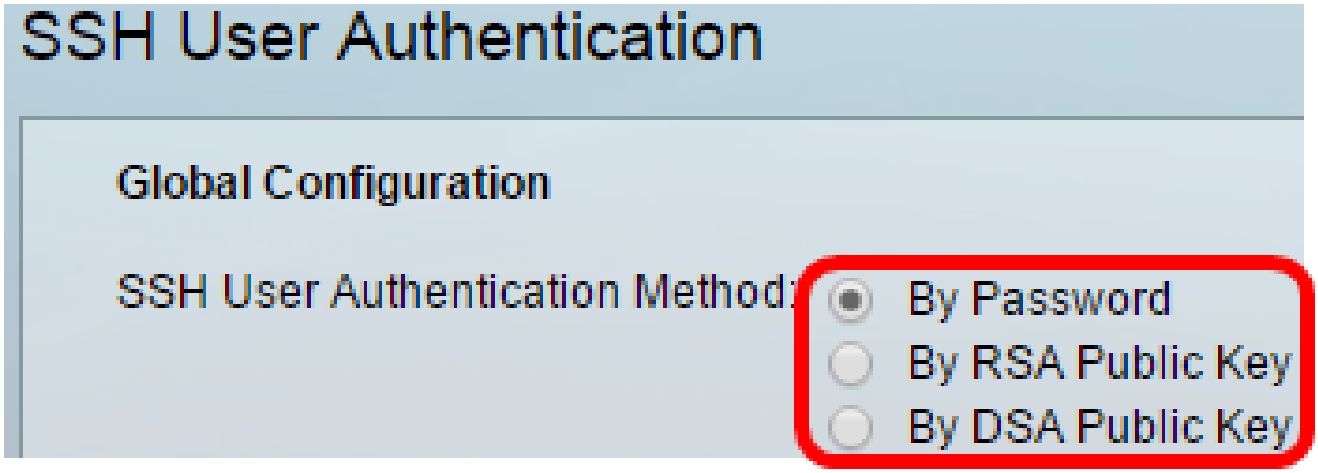


注：如果您有Sx350、SG300X或Sx500X，请从Display Mode下拉列表中选择Advanced，切

换到Advanced模式。



第二步：在Global Configuration下，点击所需的SSH User Authentication Method。

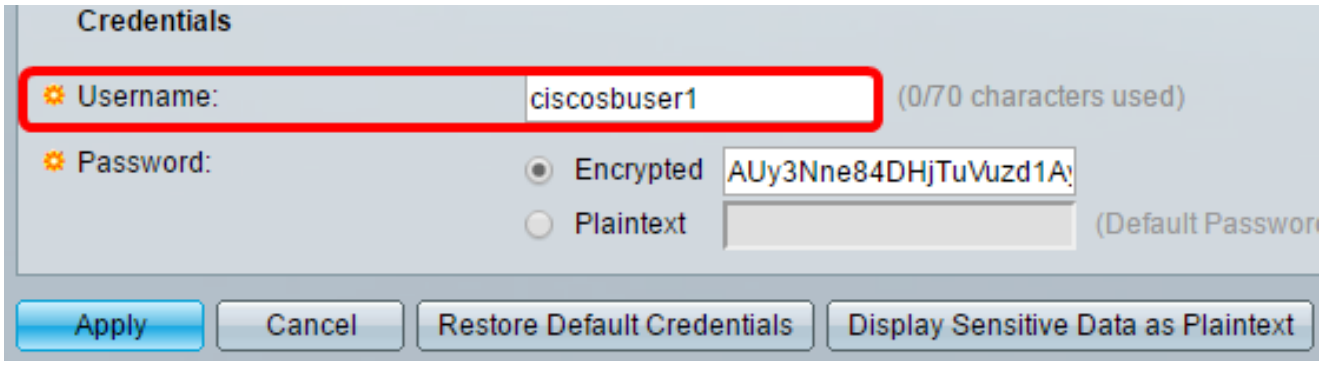


注意：当设备（SSH客户端）尝试建立到SSH服务器的SSH会话时，SSH服务器使用以下方法之一进行客户端身份验证：

- 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，默认密码是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，因为它在身份验证过程中需要花费更多时间。

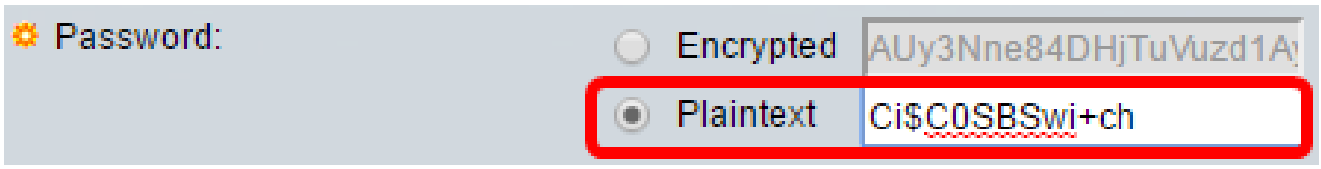
注意：在本示例中，选择By Password。

第三步：在Credentials区域，在Username字段中输入用户名。



注意：在本示例中，使用ciscosbuser1。

第4步。（可选）如果在第2步中选择了按密码，请单击该方法，然后在加密或明文字段中输入密码。



选项有：

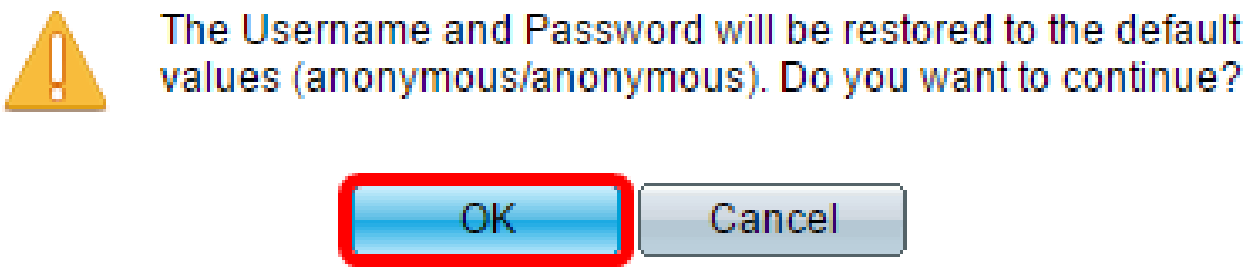
- Encrypted — 此选项允许您输入密码的加密版本。
- 纯文本 — 此选项允许您输入纯文本密码。

注意：在本示例中，选择纯文本并输入纯文本密码。

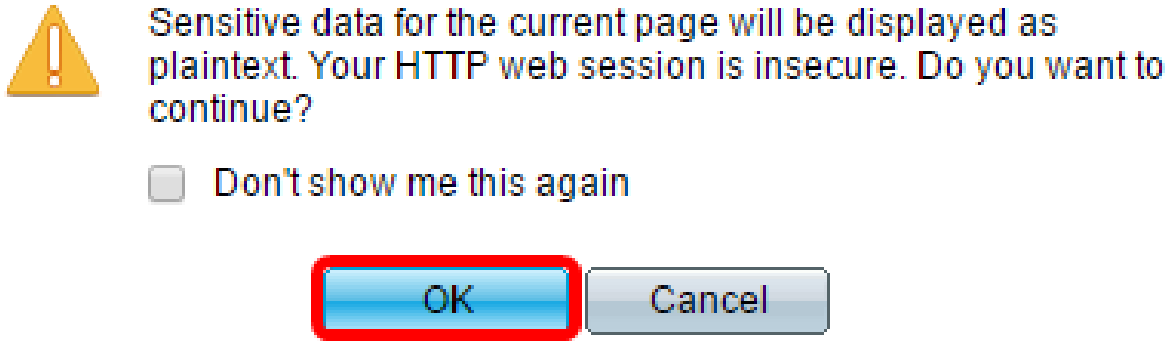
第五步：单击Apply保存身份验证配置。

步骤6.（可选）点击Restore Default Credentials恢复默认用户名和密码，然后点击OK继续。

注意：用户名和密码将恢复为默认值：anonymous/anonymous。

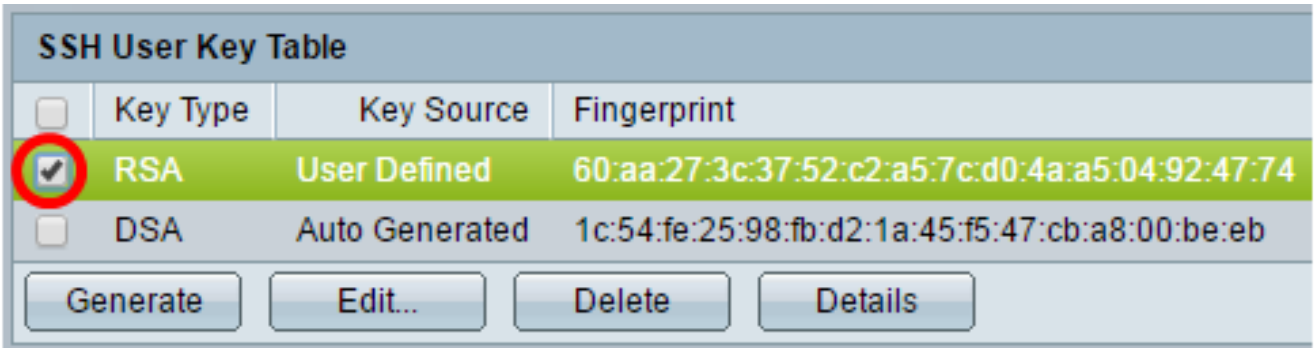


步骤7.（可选）单击将敏感数据显示为明文以纯文本格式显示页面的敏感数据，然后单击确定以继续。



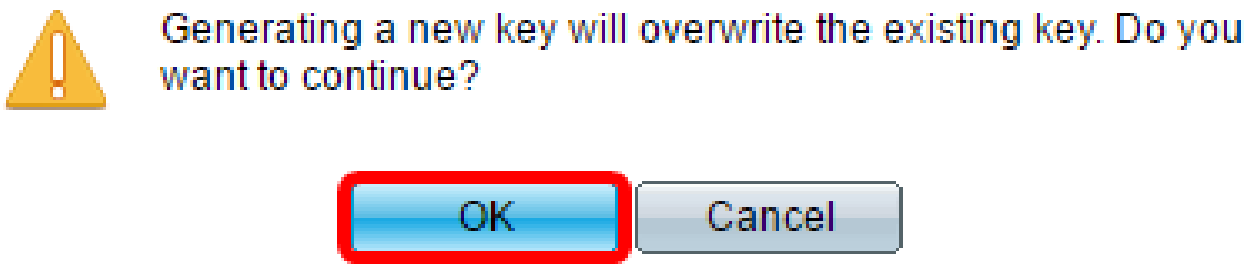
配置SSH用户密钥表

步骤 8选中要管理的密钥的复选框。

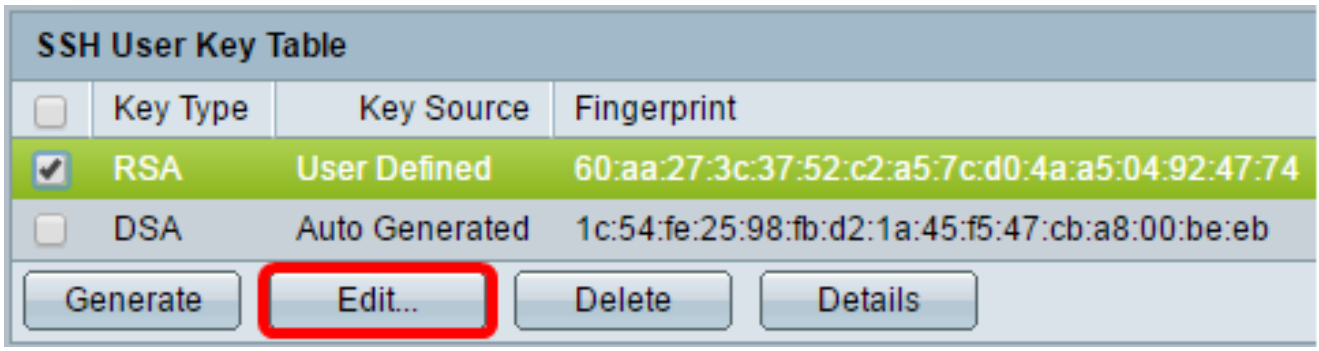


注意：在本示例中，选择了RSA。

步骤9.（可选）单击Generate生成新密钥。新密钥将覆盖选中的密钥，然后单击OK继续。



第10步。（可选）点击Edit以编辑当前密钥。

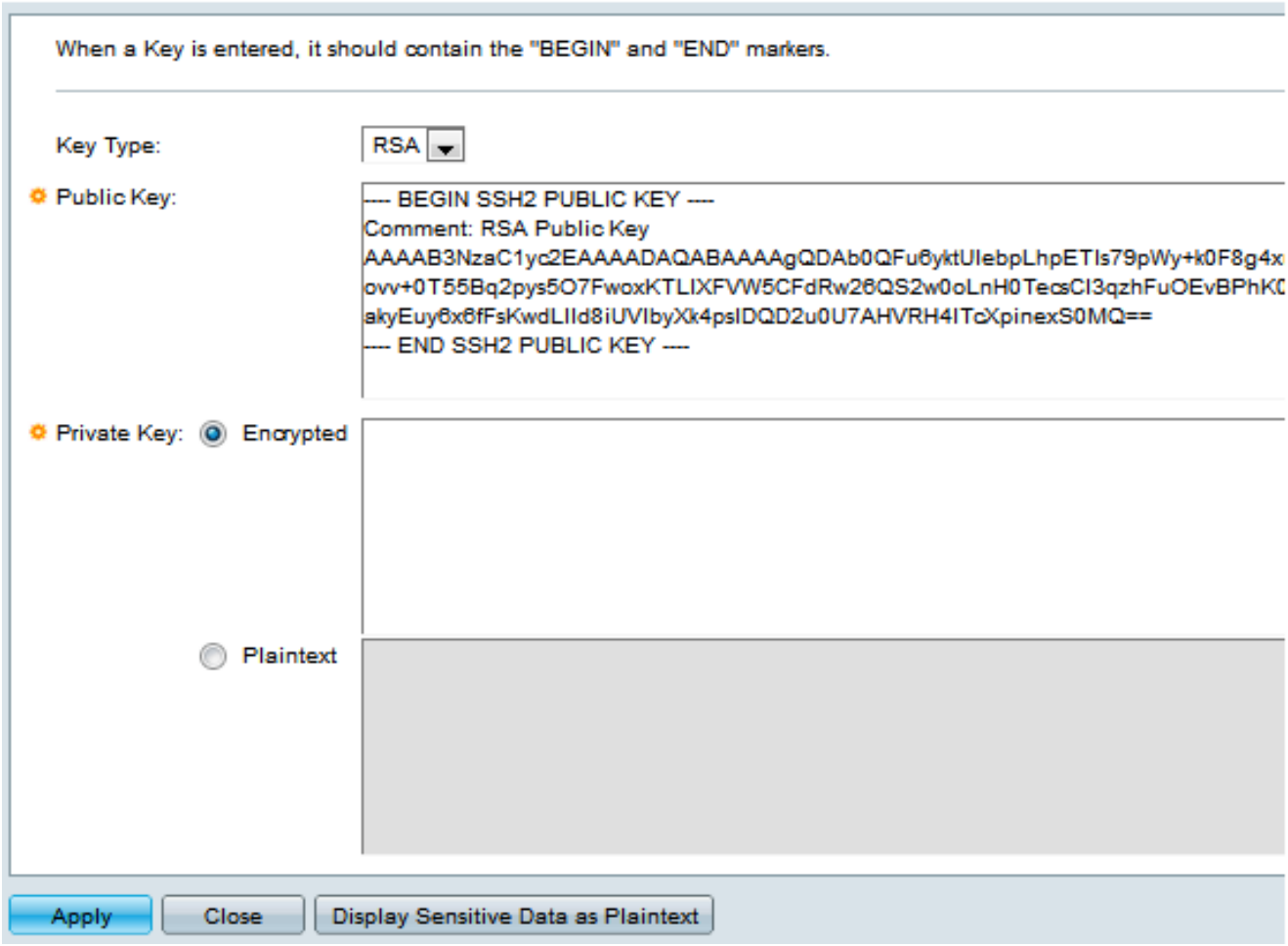


步骤11.（可选）从Key Type下拉列表中选择密钥类型。



注意：在本示例中，选择了RSA。

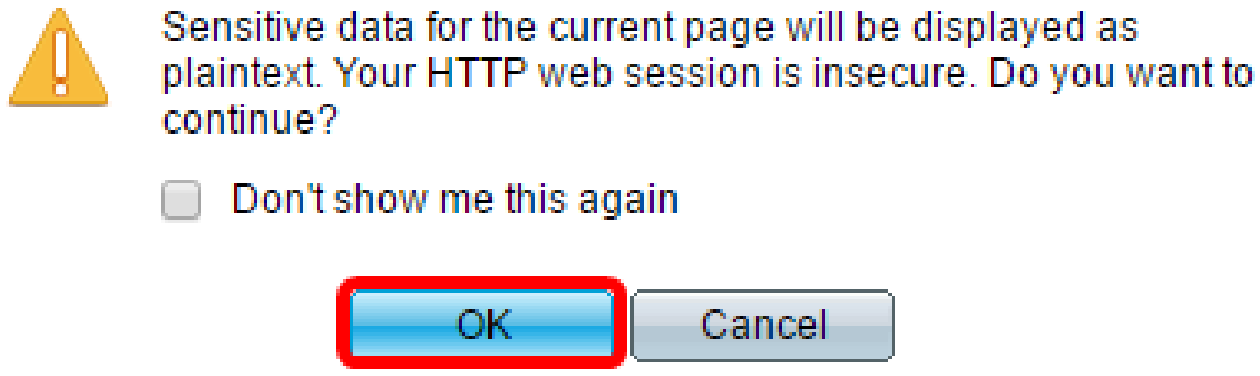
步骤12.（可选）在公钥字段中输入新的公钥。



步骤13.（可选）在Private Key（私钥）字段中输入新的私钥。

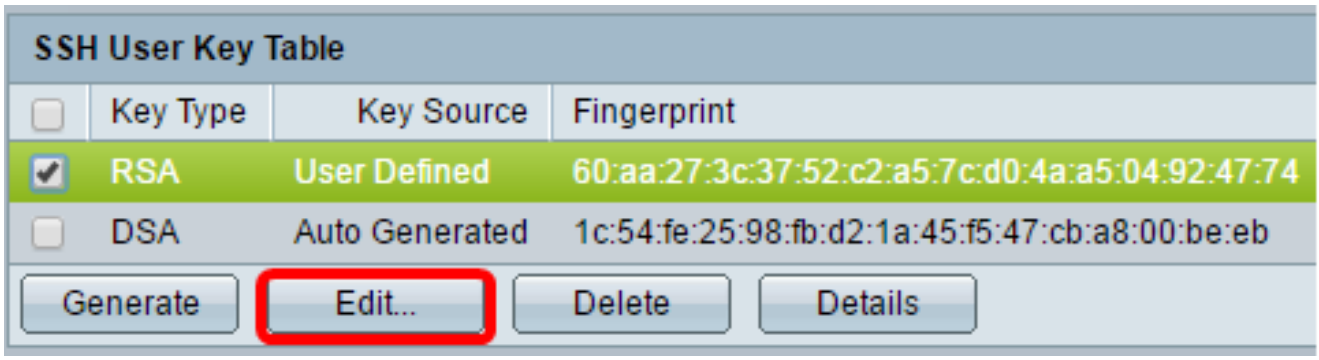
注意：您可以编辑私钥，并且可以点击Encrypted以加密文本形式查看当前私钥，或者点击Plaintext以纯文本形式查看当前私钥。

步骤14.（可选）单击Display Sensitive Data as Plaintext以纯文本格式显示页面的加密数据，然后单击OK继续。

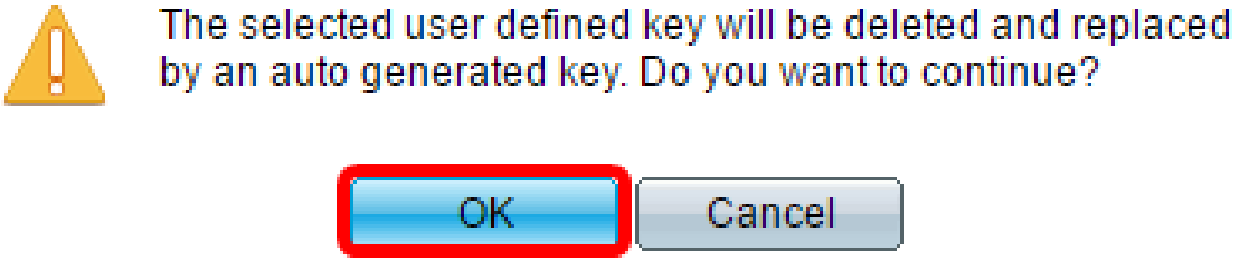


步骤 15单击Apply保存更改，然后单击Close。

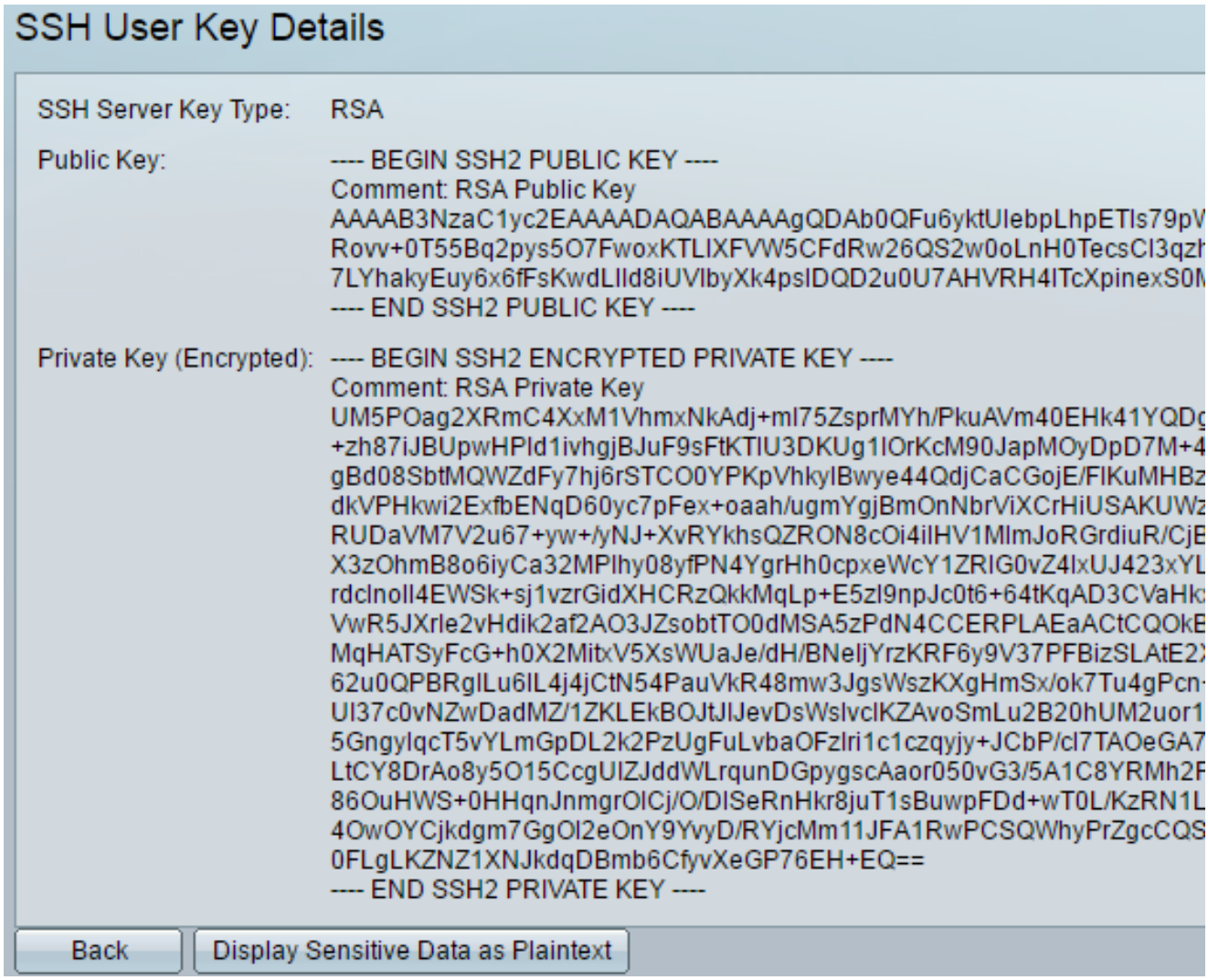
步骤16.（可选）单击Delete删除选中的密钥。



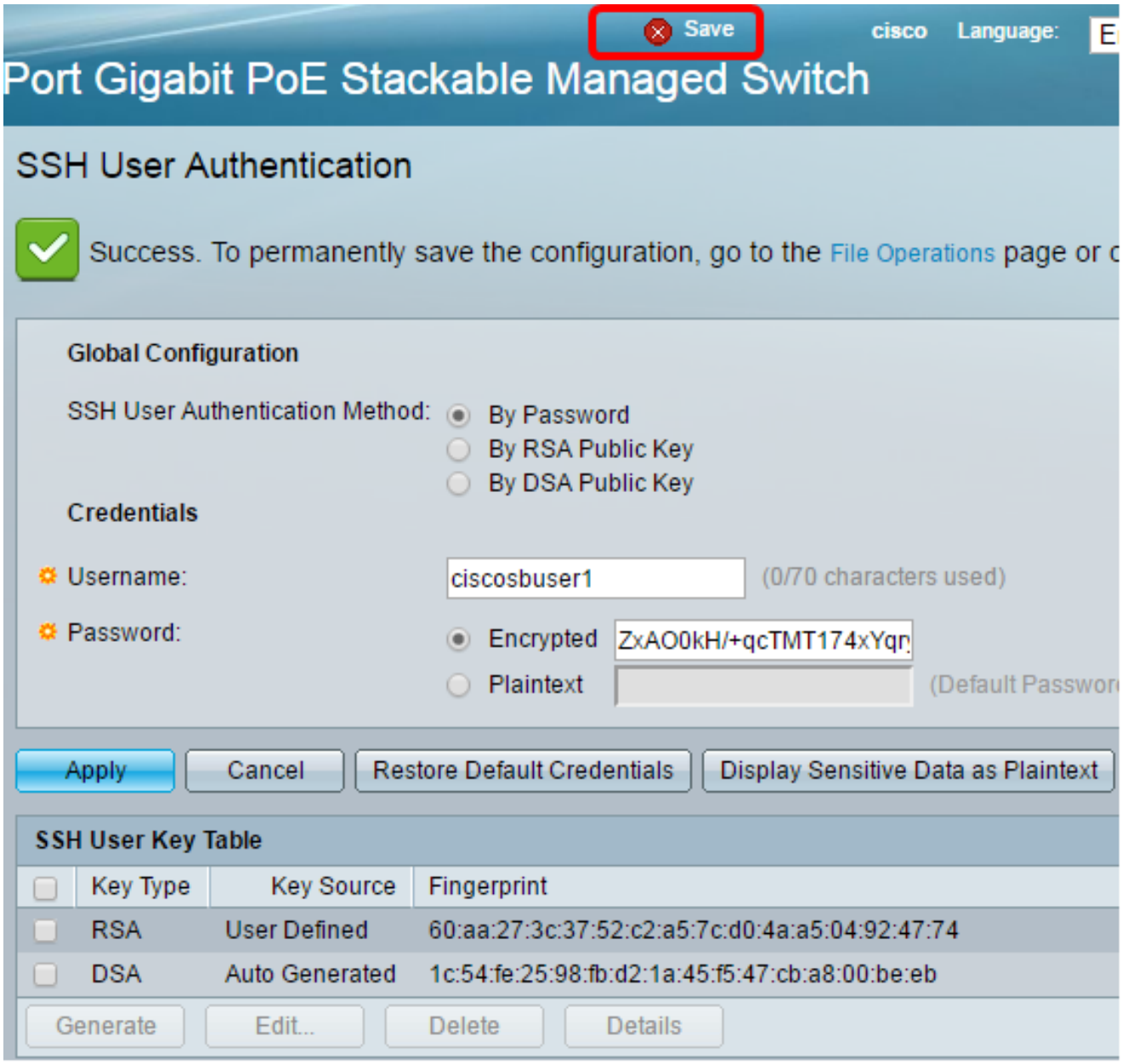
步骤17.（可选）出现如下所示的确认消息提示后，单击OK删除密钥。



步骤18.（可选）单击Details查看选中密钥的详细信息。



步骤19.（可选）点击页面顶部的Save按钮，将更改保存到启动配置文件。



现在，您应该已经在受管交换机上配置了客户端用户身份验证设置。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。