在交换机上配置安全外壳(SSH)服务器身份验证设置

目标

本文介绍如何在受管交换机上配置服务器身份验证，而不是如何连接到交换机。有关通过SSH + Putty连接到交换机的文章，请点击此处查看该文章。

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允许管理员通过命令行界面(CLI)使用第三方程序配置交换机。交换机充当SSH客户端，为网络内的用户提供各种SSH功能。交换机使用SSH服务器提供SSH服务。当禁用SSH服务器身份验证时，交换机将任何SSH服务器视为受信任，这会降低网络的安全性。如果交换机上启用了SSH服务，则安全性会增强。

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服务器身份验证设置

启用SSH服务

当启用SSH服务器身份验证时，设备上运行的SSH客户端使用以下身份验证过程对SSH服务器进行身份验证：

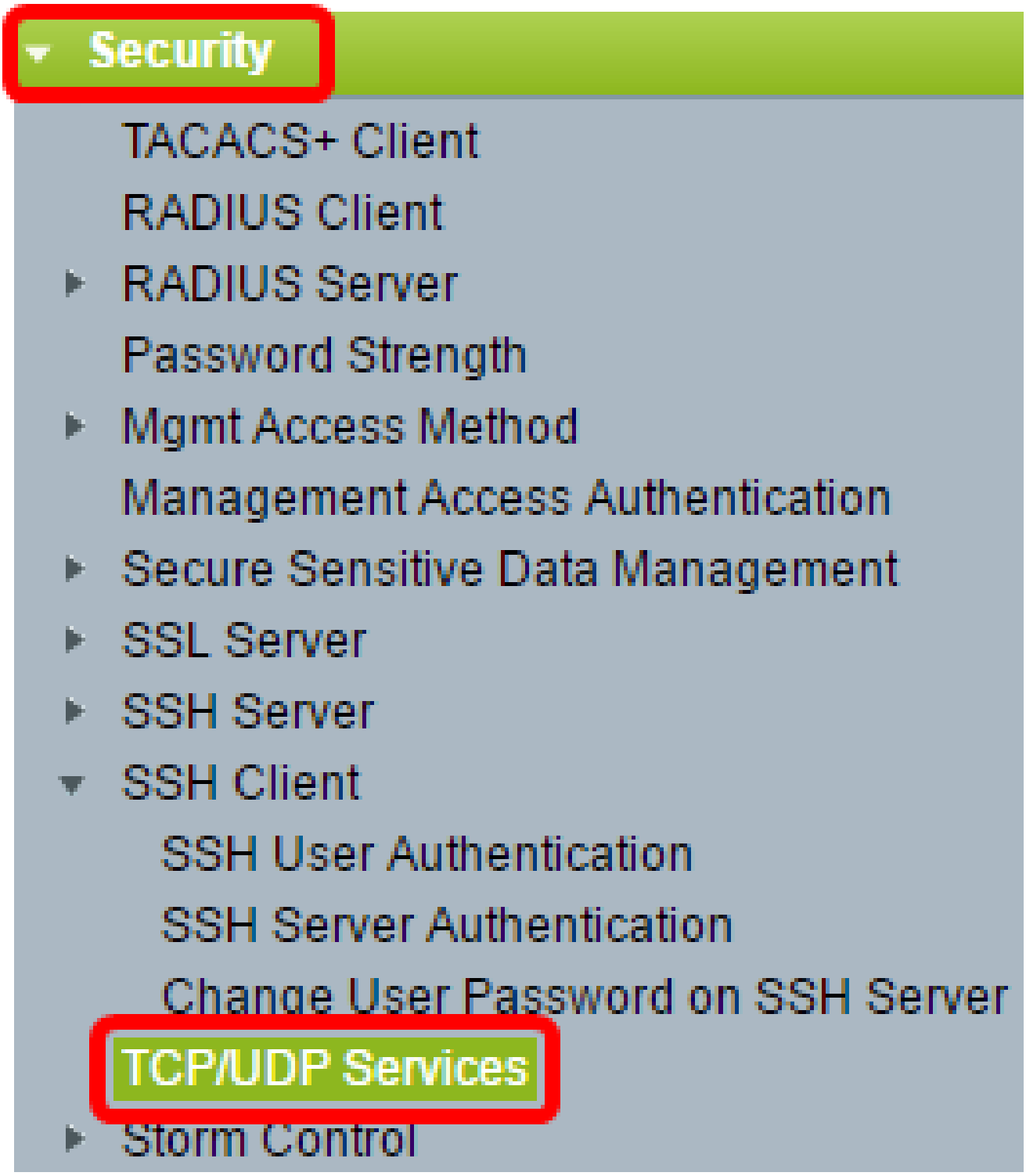
- 设备计算SSH服务器收到的公钥的指纹。
- 设备在“SSH受信任服务器”(SSH Trusted Servers)表中搜索SSH服务器的IP地址和主机名。可

能出现以下三种结果之一：

1. 如果找到服务器的地址和主机名及其指纹的匹配项，则对服务器进行身份验证。
2. 如果找到匹配的IP地址和主机名，但没有匹配的指纹，搜索将继续。如果未找到匹配的指纹，则搜索完成且身份验证失败。
3. 如果未找到匹配的IP地址和主机名，则搜索完成且身份验证失败。
    - 如果在受信任服务器列表中找不到SSH服务器的条目，则进程失败。

注意：为了支持使用出厂默认配置对开箱即用交换机进行自动配置，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，然后选择Security > TCP/UDP Services。

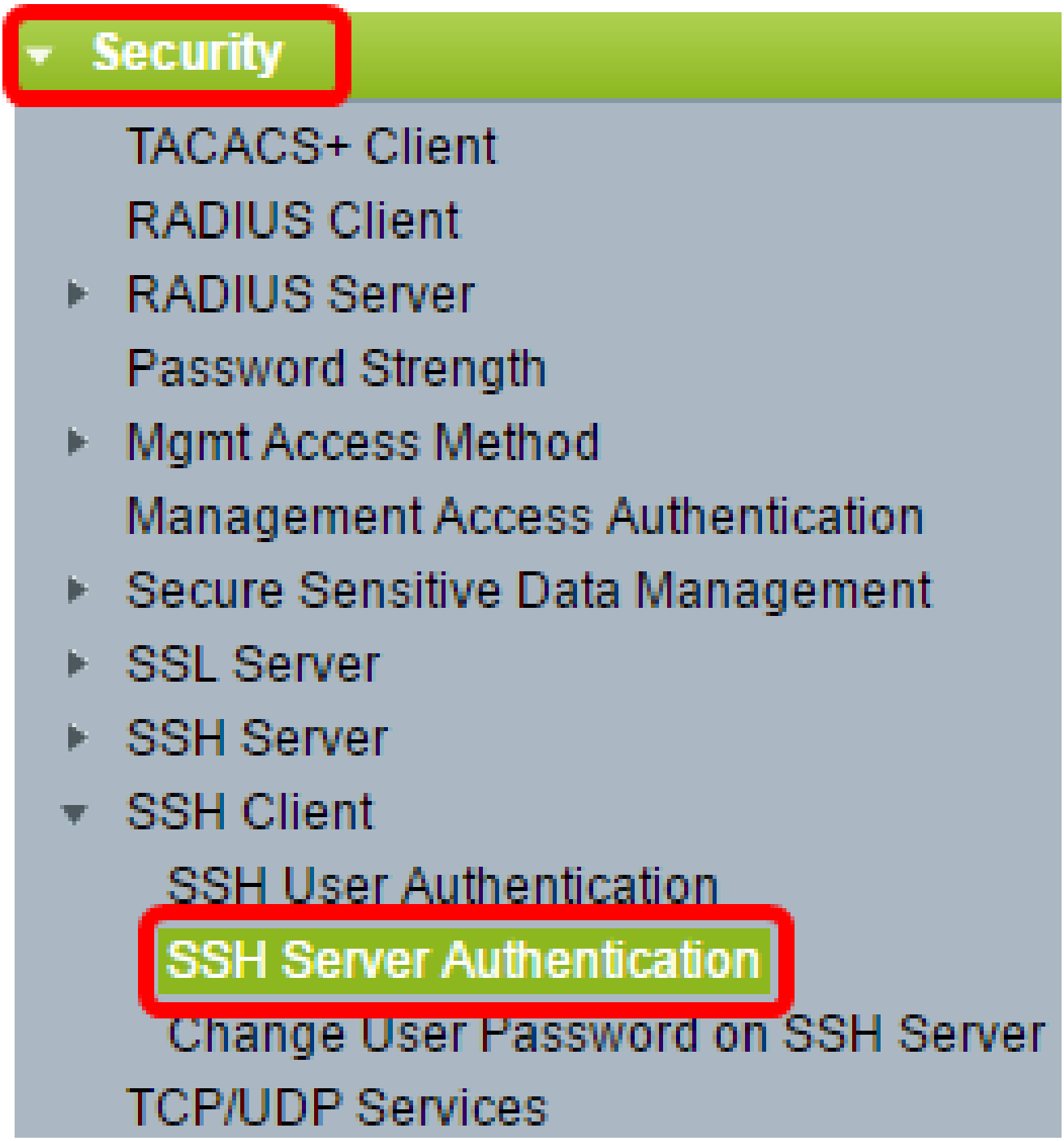


第二步：选中SSH Service复选框以启用通过SSH访问交换机命令提示符。

第三步：单击Apply以启用SSH服务。

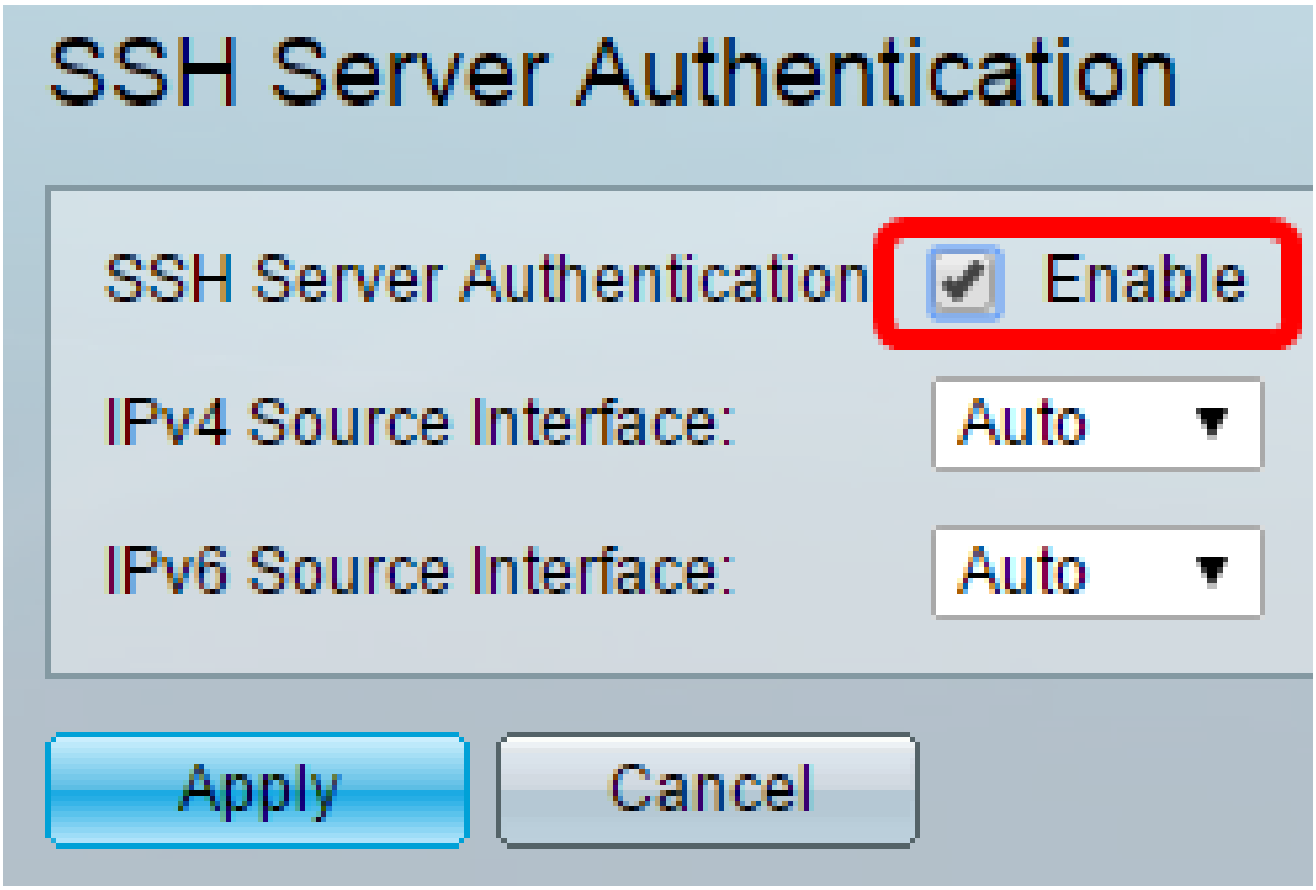
配置SSH服务器身份验证设置

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

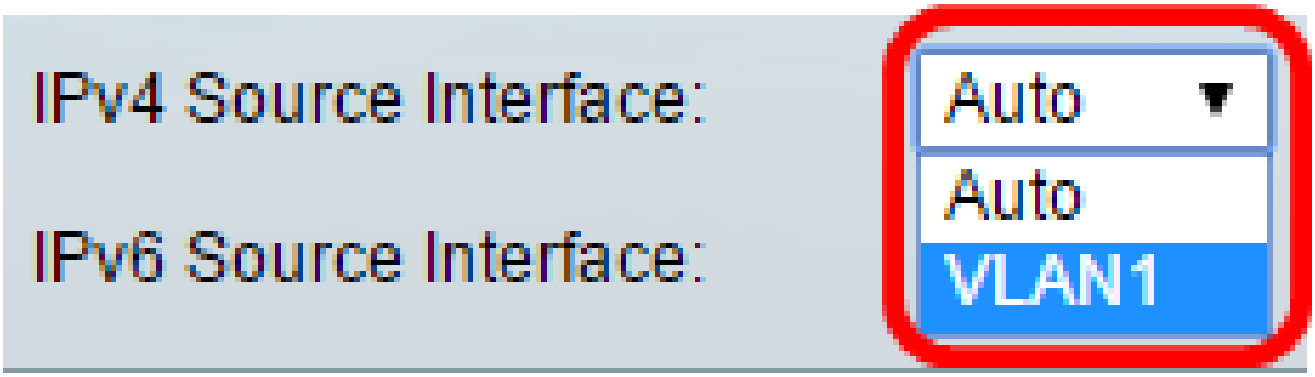


注：如果您有Sx350、SG300X或Sx500X，请从Display Mode下拉列表中选择Advanced，切换到Advanced模式。

第二步：选中Enable SSH Server Authentication复选框以启用SSH服务器身份验证。

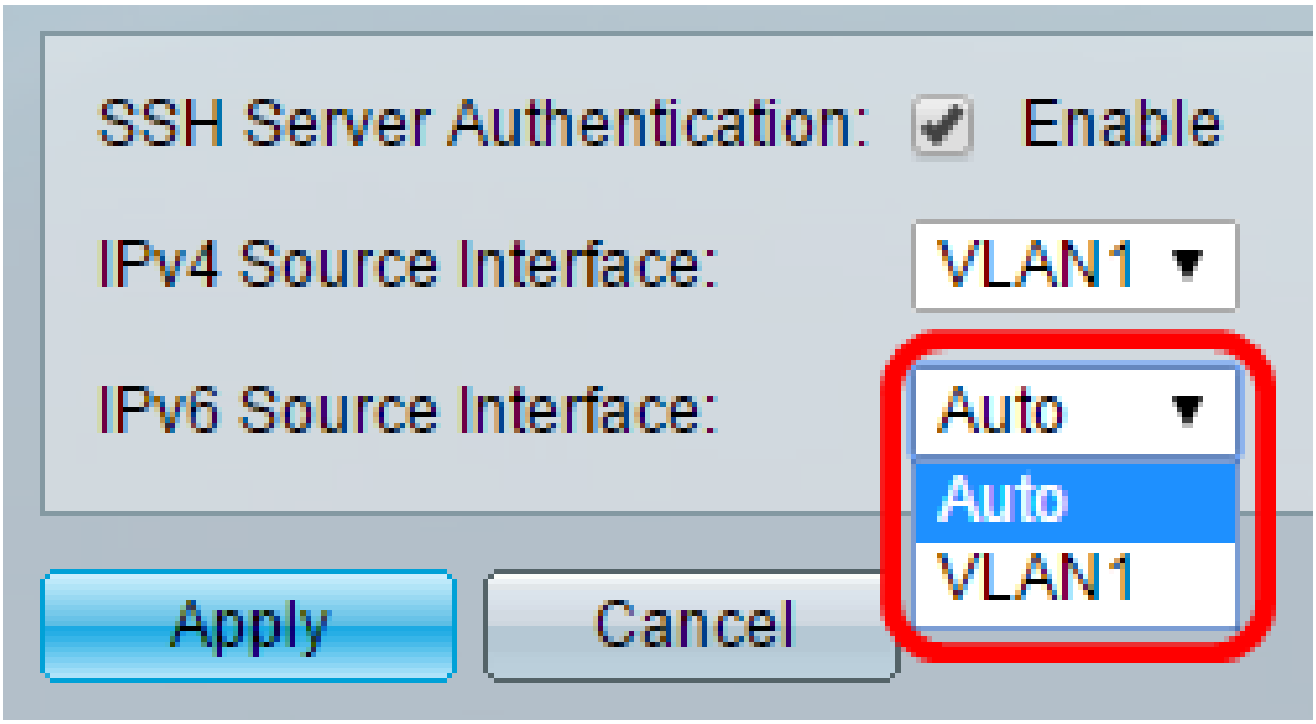


步骤3.（可选）在IPv4 Source Interface下拉列表中，选择其IPv4地址将用作与IPv4 SSH服务器通信所用消息的源IPv4地址的源接口。



注意：如果选择Auto选项，则系统从传出接口上定义的IP地址获取源IP地址。在本例中，选择VLAN1。

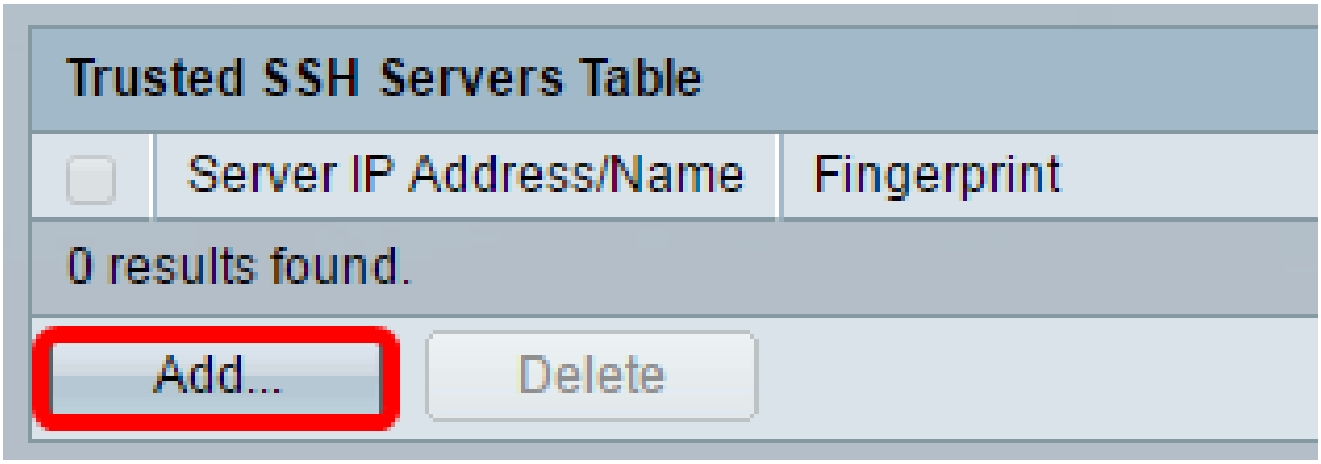
步骤4.（可选）在IPv6 Source Interface下拉列表中，选择其IPv6地址将用作与IPv6 SSH服务器通信所用消息的源IPv6地址的源接口。



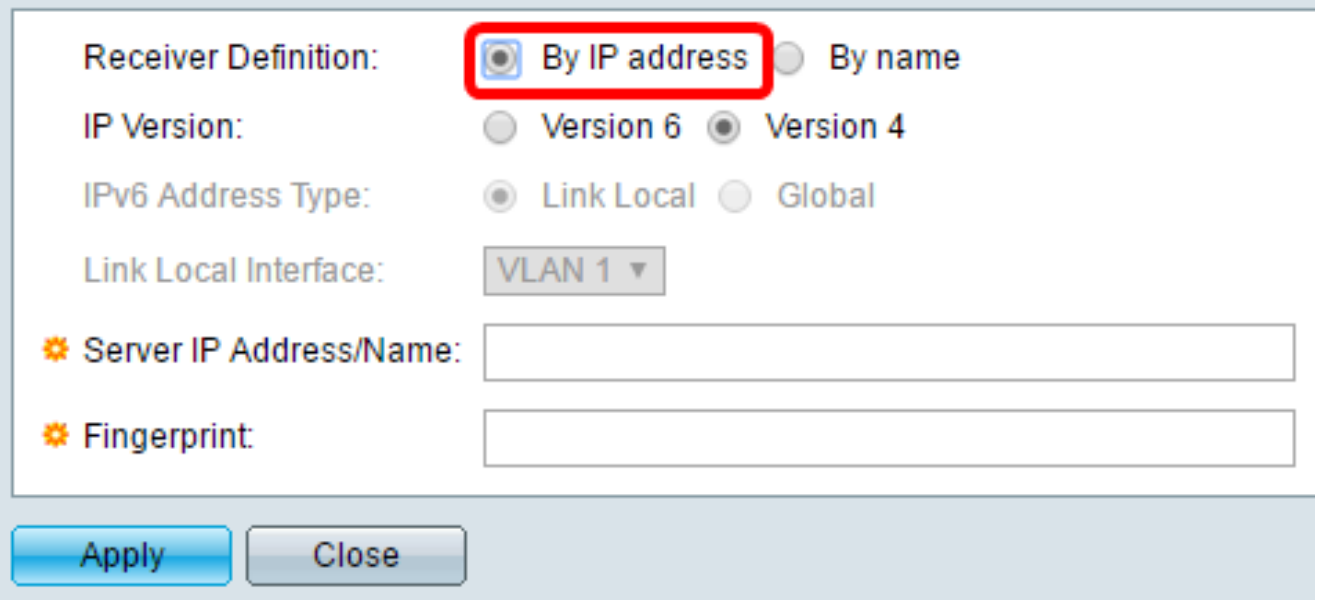
注意：在本例中，选择了“自动”(Auto)选项。系统将从传出接口上定义的IP地址获取源IP地址。

第五步：单击 Apply。

第六步：要添加可信服务器，请点击Trusted SSH Servers Table下的Add。



步骤 7.在Receiver Definition区域中，单击可用方法之一以定义SSH服务器：

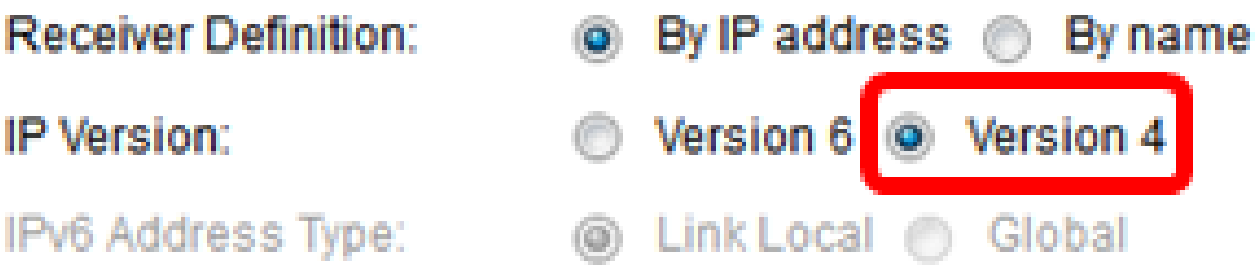


选项有：

- 按IP地址(By IP Address) — 此选项允许您使用IP地址定义SSH服务器。
- 按名称(By Name) — 此选项允许您使用完全限定域名定义SSH服务器。

注意：在本示例中，选择By IP address。如果选择了By name，请跳至步骤11。

步骤8.（可选）如果在步骤6中选择了By IP address，请在IP Version字段中点击SSH服务器的IP版本。



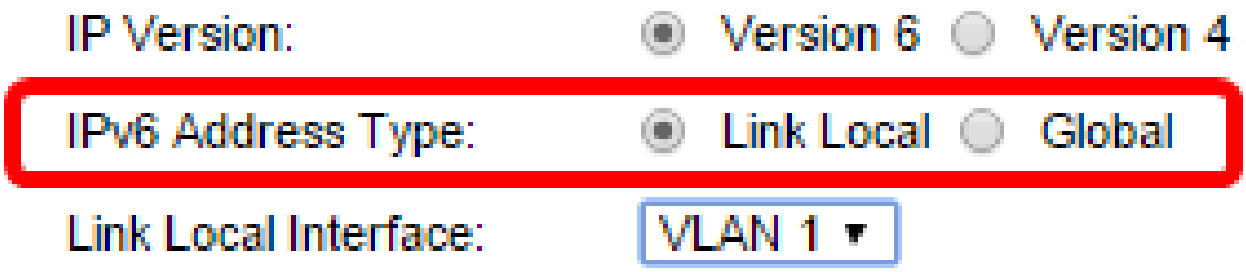
可用选项包括：

- 版本6 — 此选项允许您输入IPv6地址。
- 版本4 — 此选项允许您输入IPv4地址。

注意：在本示例中，选择了版本4。仅当交换机中配置了IPv6地址时，IPv6单选按钮才可用。

步骤9.（可选）如果在步骤7中选择版本6作为IP地址版本，则在IPv6 Address Type中点击IPv6地址

的类型。

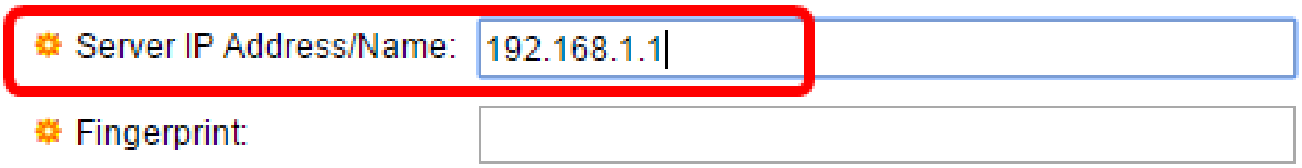


可用选项包括：

- 本地链路 — IPv6地址唯一标识单个网络链路上的主机。链路本地地址的前缀为FE80，不可路由，并且只能用于本地网络上的通信。仅支持一个链路本地地址。如果接口上存在本地链路地址，此条目将替换配置中的地址。默认情况下会选择此选项。
- 全局 — IPv6地址是全局单播，可从其他网络查看和到达。

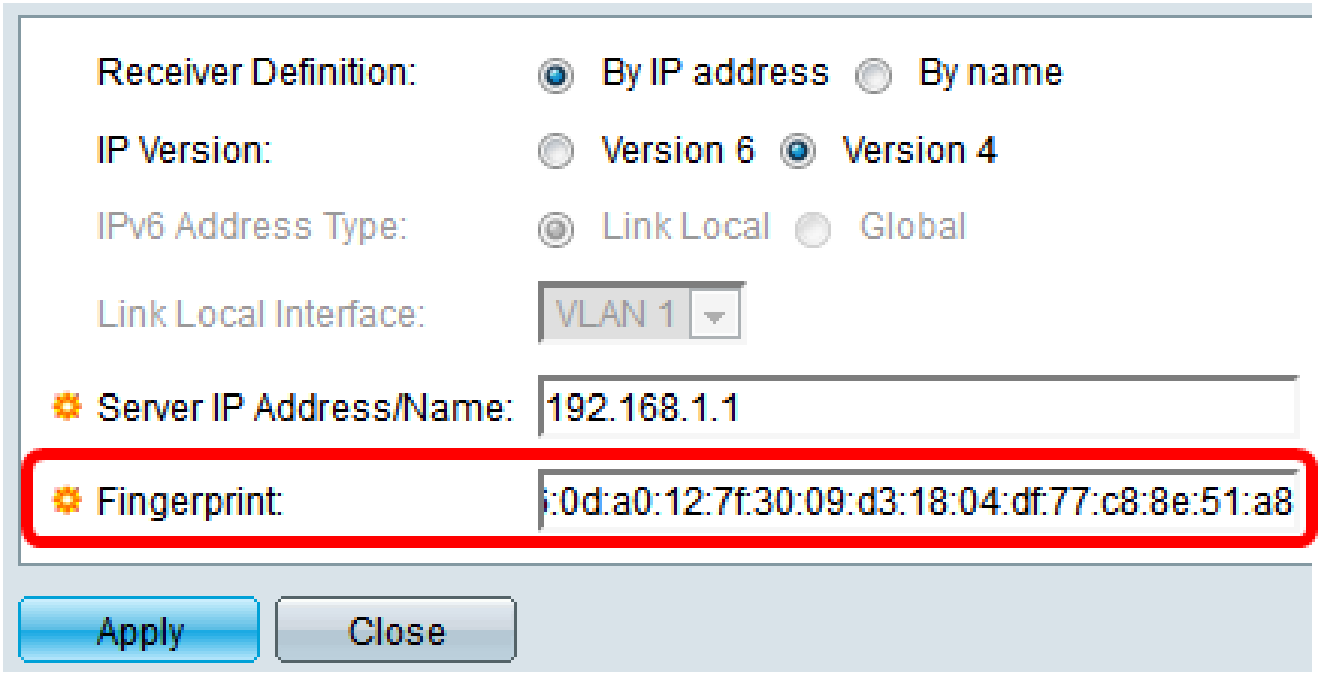
步骤10.（可选）如果在步骤9中选择本地链路作为IPv6地址类型，请在Link Local Interface下拉列表中选择相应的接口。

步骤 11在服务器IP地址/名称字段中，输入SSH服务器的IP地址或域名。



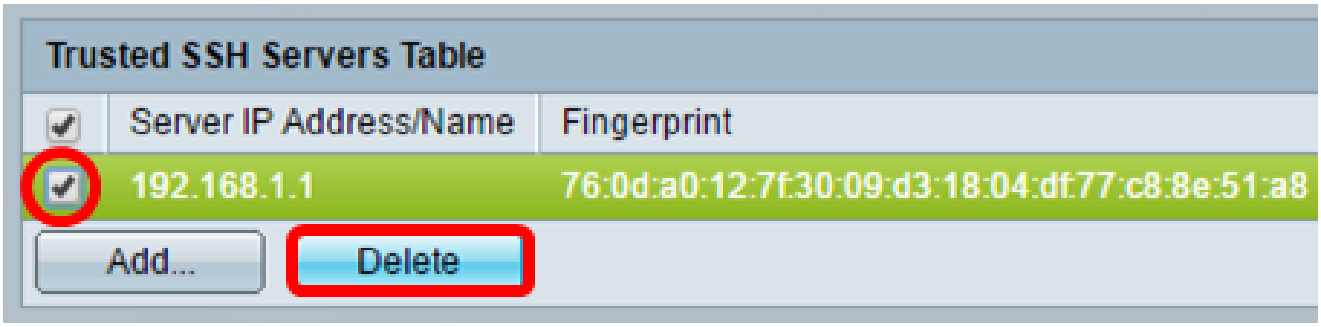
注意：在本示例中，输入了IP地址。

步骤 12在指纹字段中，输入SSH服务器的指纹。指纹是用于身份验证的加密密钥。在这种情况下，指纹用于验证SSH服务器的有效性。如果服务器IP地址/名称与指纹匹配，则对SSH服务器进行身份验证。

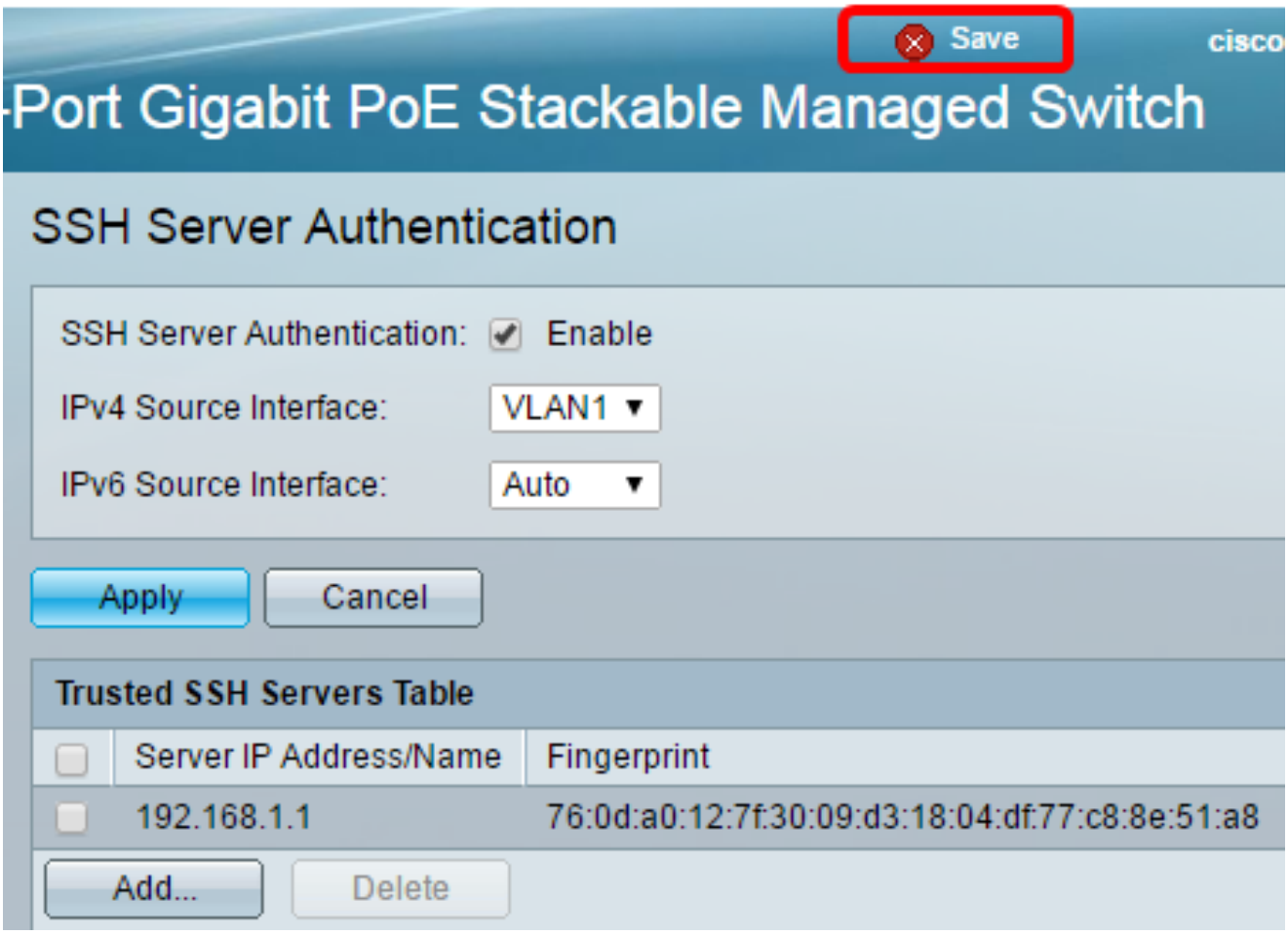


步骤 13单击确定保存所进行的配置。

步骤14.（可选）要删除SSH服务器，请选中要删除的服务器的复选框，然后点击删除。



步骤15.（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SSH服务器身份验证设置。

观看与本文相关的视频...

[点击此处查看思科的其他技术讲座]

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）。