SX500系列堆叠式交换机上的管理访问身份验证设置

目标

身份验证方法可帮助网络管理员通过各种方法（如SSH、Telnet、HTTP等）允许或拒绝设备访问。RADIUS、TACACS+和Local是可在SG500x系列的身份验证设置功能中启用的三种安全类型。此外，交换机上也有不存在安全的选项。RADIUS仅加密从客户端传输到服务器的访问请求数据包中的密码。TACACS+加密数据包的整体。但是，它会留下标准TACACS+报头。 本地只是验证交换机上存储的用户信息。用户身份验证按选择身份验证方法的顺序进行。如果第一种身份验证方法不可用，则使用下一种选择的方法。如果身份验证方法失败或用户权限级别不足，则拒绝用户访问交换机。

本文介绍如何为SG500x系列堆叠式交换机上的SSH、控制台、Telnet、HTTP和HTTPS等访问模式分配身份验证方法。

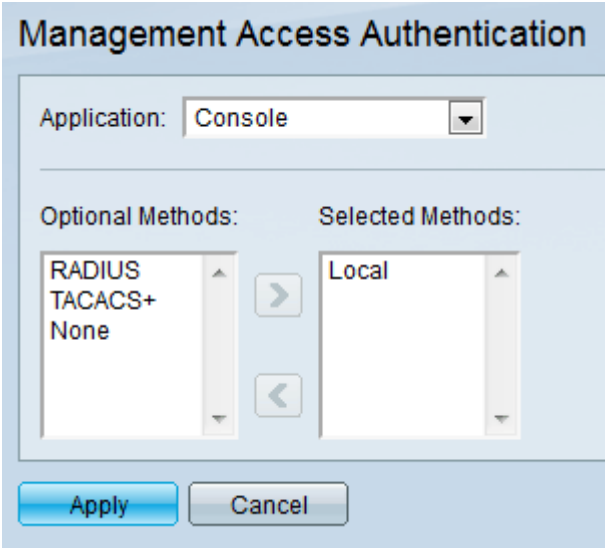
适用设备

·Sx500系列堆叠式交换机

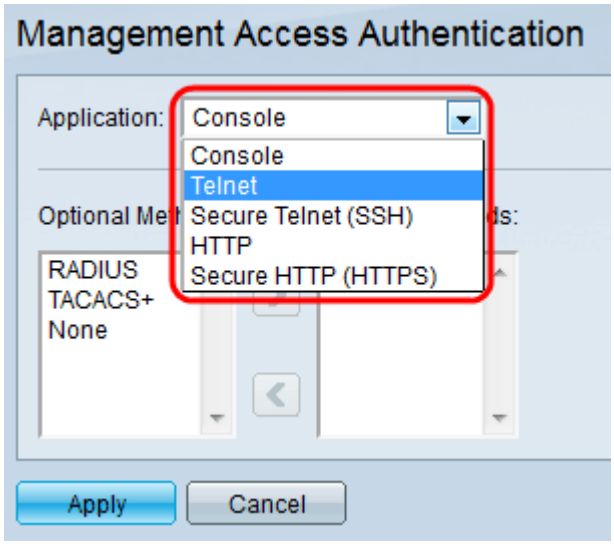
软件版本

•1.3.0.62

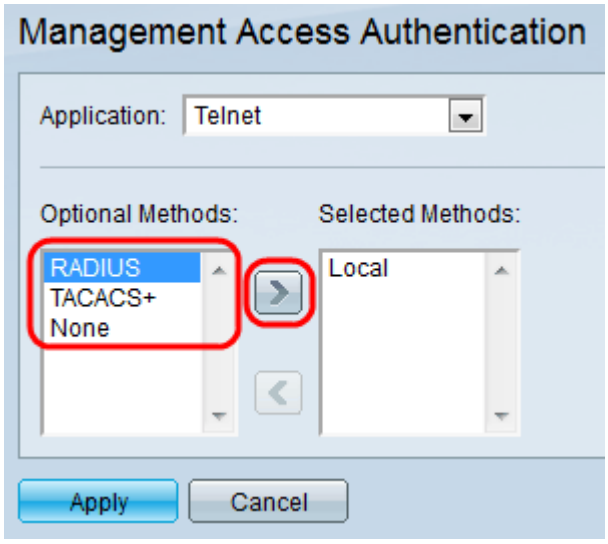
管理访问身份验证设置



步骤1.登录Web配置实用程序，然后选择Security > Management Access Authentication。系统将*打开"管理访问身份验证"*页：



步骤2.从Application下拉列表中选择要向其分配身份验证的应用类型。



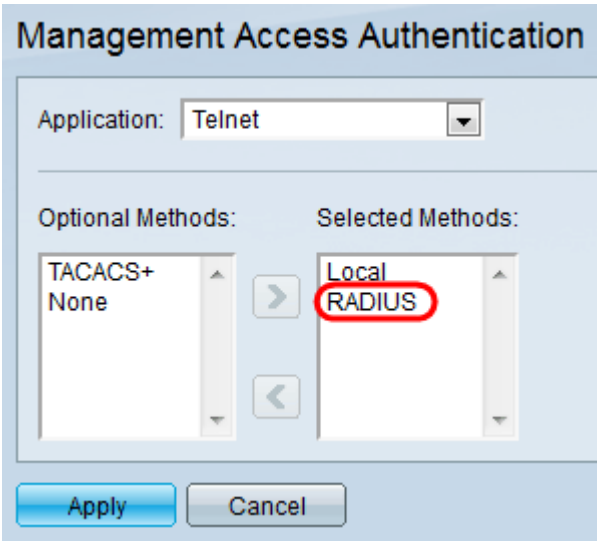
步骤3.从Optional Methods列表中选择身份验证方法，然后单击Right Arrow图**标将**其移至Selected Methods列表。

·RADIUS — 身份验证在RADIUS服务器上。必须配置RADIUS服务器。

·TACACS+ — 身份验证在TACACS+服务器上。必须配置TACACS+服务器。

·本地 — 用户信息由交换机上存储的信息来验证。

·无 — 访问交换机时不需要身份验证。



步骤4.（可选）从“选定方法”中选择方法，然后单击“左箭头”图**标，从**选定方法中删除该方法，并将其移至“可选方法”。

步骤5.单击“**应用**”保存身份验证设置。