200/300系列管理型交换机上的管理访问身份验证

目标

管理访问模式（如SSH、控制台、Telnet、HTTP和HTTPS）允许用户访问设备。 为了提高安全性，可能需要对用户进行身份验证。 200和300系列管理型交换机可以在本地或在TACACS+或RADIUS服务器上进行身份验证。 本文档说明如何在200和300系列管理型交换机上分配身份验证方法。

适用设备

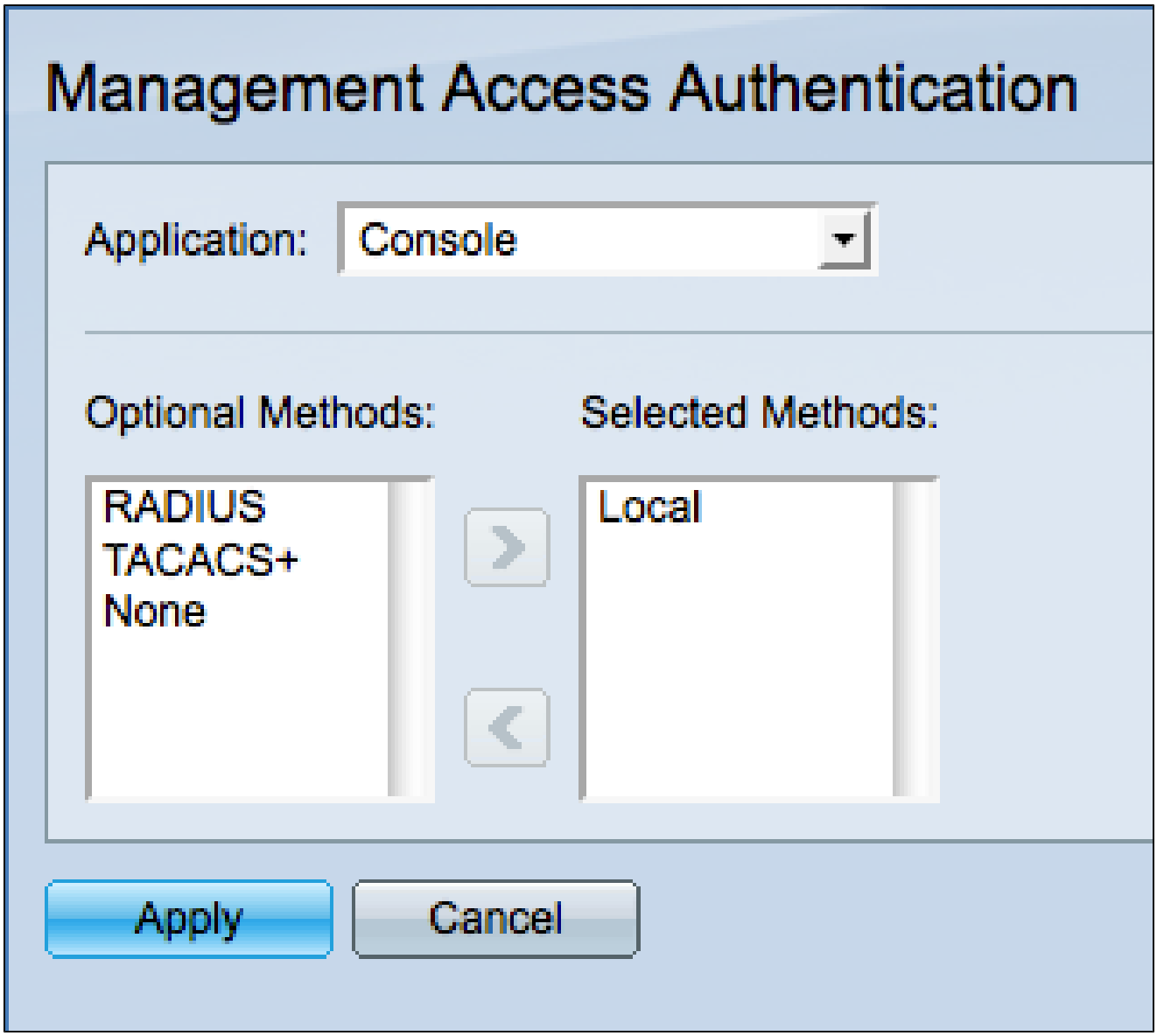
· SF/SG 200和SF/SG 300系列托管交换机

软件版本

•1.3.0.62

管理访问身份验证

步骤1:登录到Web配置实用程序，然后选择Security > Management Access Authentication。将打开Management Access Authentication页面：



第二步：从Application下拉列表中选择要向其分配身份验证的应用类型。 可能的应用有：

·控制台 — 允许您使用控制台界面管理交换机。即使交换机的IP地址未知，也允许您连接到交换机并执行某些配置。

· Telnet — 基于字符的通信协议，允许您通过TCP/IP网络远程连接到交换机。 由于缺少加密，不建议使用Telnet。

·安全Telnet(SSH) — 执行与Telnet和加密相同的功能。 对于远程连接，建议使用SSH。

· HTTP — 允许访问交换机图形用户界面(GUI)的协议。 这与基于命令提示符的Telnet和SSH不同。

·安全HTTP(HTTPS) — 通过添加安全通信执行与HTTP相同的功能。

第三步：从Optional Methods列表中选择一种身份验证方法，然后单击>按钮将其移动到Selected Methods列表。不同的方法提供不同级别的安全性。

注意：身份验证方法的选择顺序是用户身份验证的发生顺序。 如果在本地之前选择RADIUS，设备将尝试在本地方法之前通过RADIUS服务器对用户进行身份验证。

· RADIUS - RADIUS仅加密密码。身份验证在RADIUS服务器上，需要已配置的RADIUS服务器。

· TACACS+ - TACACS+在身份验证期间加密所有数据。 身份验证位于TACACS+服务器上，需要已配置的TACACS+服务器。

·无 — 访问交换机不需要身份验证。

·本地 — 用户信息由存储在交换机上的信息验证。

第四步：单击Apply保存身份验证设置，或单击Cancel取消更改。

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）。