在200/300系列被管理的交换机的管理访问认证

客观

管理接入模式例如SSH、控制台、Telnet、HTTP和HTTPS允许用户访问设备。 认证可以要求用户改进安全。 200和300系列被管理的交换机能验证本地或在TACACS+或RADIUS服务器。 本文解释如何分配在200和300系列被管理的交换机的一个认证方法。

可适用的设备

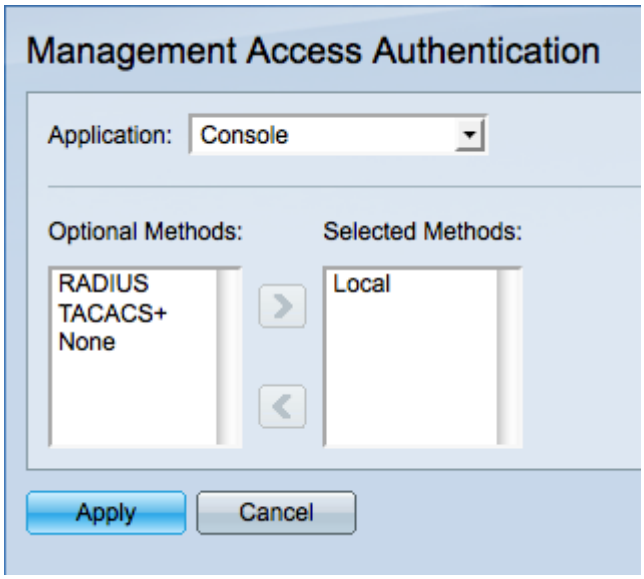
• SF/SG 200和SF/SG 300系列被管理的交换机

软件版本

•1.3.0.62

管理访问认证

步骤1.登陆到Web配置工具并且选择**安全>管理访问认证**。 *管理访问认证*页打开：



步骤2.选择您希望分配认证到从应用程序下拉列表应用程序的种类。 可能的应用程序是：

•控制台—允许您管理有控制台接口的交换机。允许您连接到交换机和执行一些配置，即使交换机的IP地址不知道。

•Telnet —允许您远程连接到在TCP/IP网络的交换机的基于字符通信协议。 Telnet不推荐归结于缺乏加密。

•安全的Telnet (SSH) —执行功能和telnet一样加上加密。 SSH为远程连接是推荐的。

•HTTP —允许您访问图形用户界面的协议(GUI)交换机。 这是与是基于的prompt命令的Telnet和SSH对比。

•安全HTTP (HTTPS) —执行功能和HTTP一样增加安全通信。

步骤3.从可选的方法列表选择验证方法然后点击**>**移动它的按钮向所选的方法列表。不同的方法提供不同的安全级别。

Note:命令认证方法选择是命令用户认证出现。 如果RADIUS在本地前选择，设备将尝试由RADIUS服务器验证用户在本地方法前。

- RADIUS — RADIUS加密密码。认证在RADIUS服务器并且要求一个被配置的RADIUS服务器。
- TACACS+ — TACACS+在认证时加密所有数据。 认证在TACACS+服务器并且要求一个被配置的TACACS+服务器。
- 什么都—没有要求认证访问交换机。
- 本地—用户信息由在交换机存储的信息验证。

步骤4.点击**适用**保存认证设置或点击**取消**取消您的更改。