200/300系列託管交換器上的管理存取驗證

目標

SSH、控制檯、Telnet、HTTP和HTTPS等管理訪問模式允許使用者訪問裝置。 為了提高安全性，可能需要對使用者進行身份驗證。 200和300系列託管交換器可以在本地或在TACACS+或RADIUS伺服器上進行驗證。 本檔案將說明如何在200和300系列託管交換器上指派驗證方法。

適用裝置

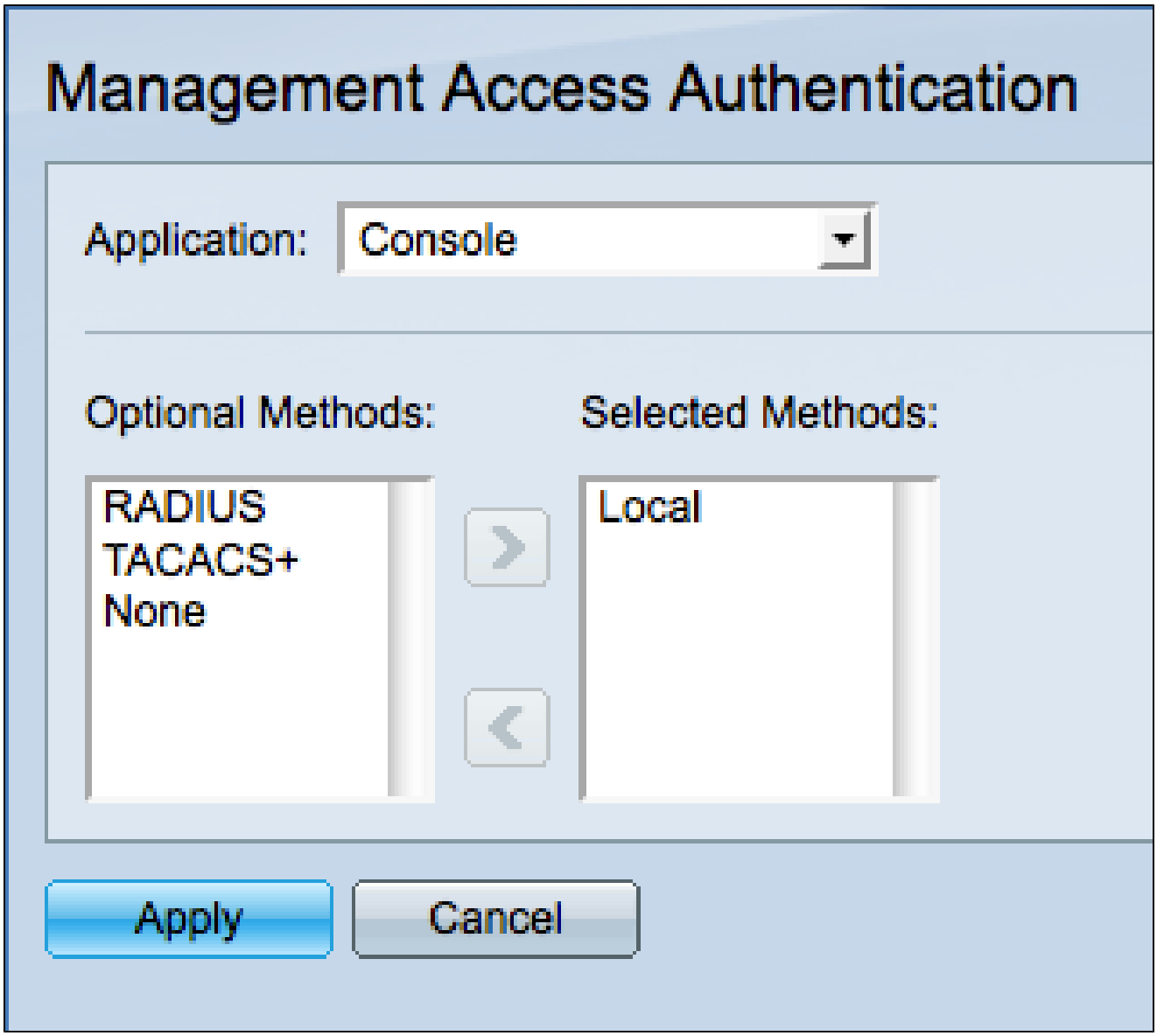
· SF/SG 200和SF/SG 300系列託管交換器

軟體版本

•1.3.0.62

管理訪問身份驗證

步驟 1.登入到Web配置實用程式，然後選擇Security > Management Access Authentication。將開啟Management Access Authentication頁面：



步驟 2.從Application下拉選單中選擇要將身份驗證分配到的應用程式型別。 可能的應用有：

·控制檯 — 允許您使用控制檯介面管理交換機。即使交換機的IP地址未知，也允許您連線到交換機並執行某些配置。

· Telnet — 基於字元的通訊協定，允許通過TCP/IP網路遠端連線到交換機。 由於缺少加密，不建議使用Telnet。

·安全Telnet(SSH) — 執行與telnet和加密相同的功能。 對於遠端連線，建議使用SSH。

· HTTP — 允許您訪問交換機圖形使用者介面(GUI)的協定。 這與基於命令提示符的Telnet和SSH不同。

·安全HTTP(HTTPS) — 通過新增安全通訊執行與HTTP相同的功能。

步驟 3.從Optional Methods清單中選擇一種身份驗證方法，然後按一下>按鈕將其移動到Selected Methods清單中。不同的方法提供不同級別的安全性。

注意：身份驗證方法的選擇順序是使用者進行身份驗證的順序。 如果在本地方法之前選擇RADIUS，則裝置將嘗試在本地方法之前通過RADIUS伺服器驗證使用者。

· RADIUS - RADIUS僅加密密碼。驗證在RADIUS伺服器上，需要已設定的RADIUS伺服器。

· TACACS+ - TACACS+會在驗證期間加密所有資料。 驗證在TACACS+伺服器上，需要已設定的TACACS+伺服器。

·無 — 訪問交換機不需要身份驗證。

·本地 — 使用者資訊由儲存在交換機上的資訊驗證。

步驟 4.按一下Apply儲存身份驗證設定，或按一下Cancel取消更改。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。