# 200/300シリーズマネージドスイッチでの管理アクセス認証

## 目的

SSH、コンソール、Telnet、HTTP、HTTPSなどの管理アクセスモードを使用すると、ユーザはデバイスにアクセスできます。 セキュリティを向上させるために、ユーザに認証を要求できます。 200および300シリーズマネージドスイッチは、ローカルに、またはTACACS+やRADIUSサーバ上で認証できます。 このドキュメントでは、200および300シリーズマネージドスイッチで認証方式を割り当てる方法について説明します。

## 適用可能なデバイス

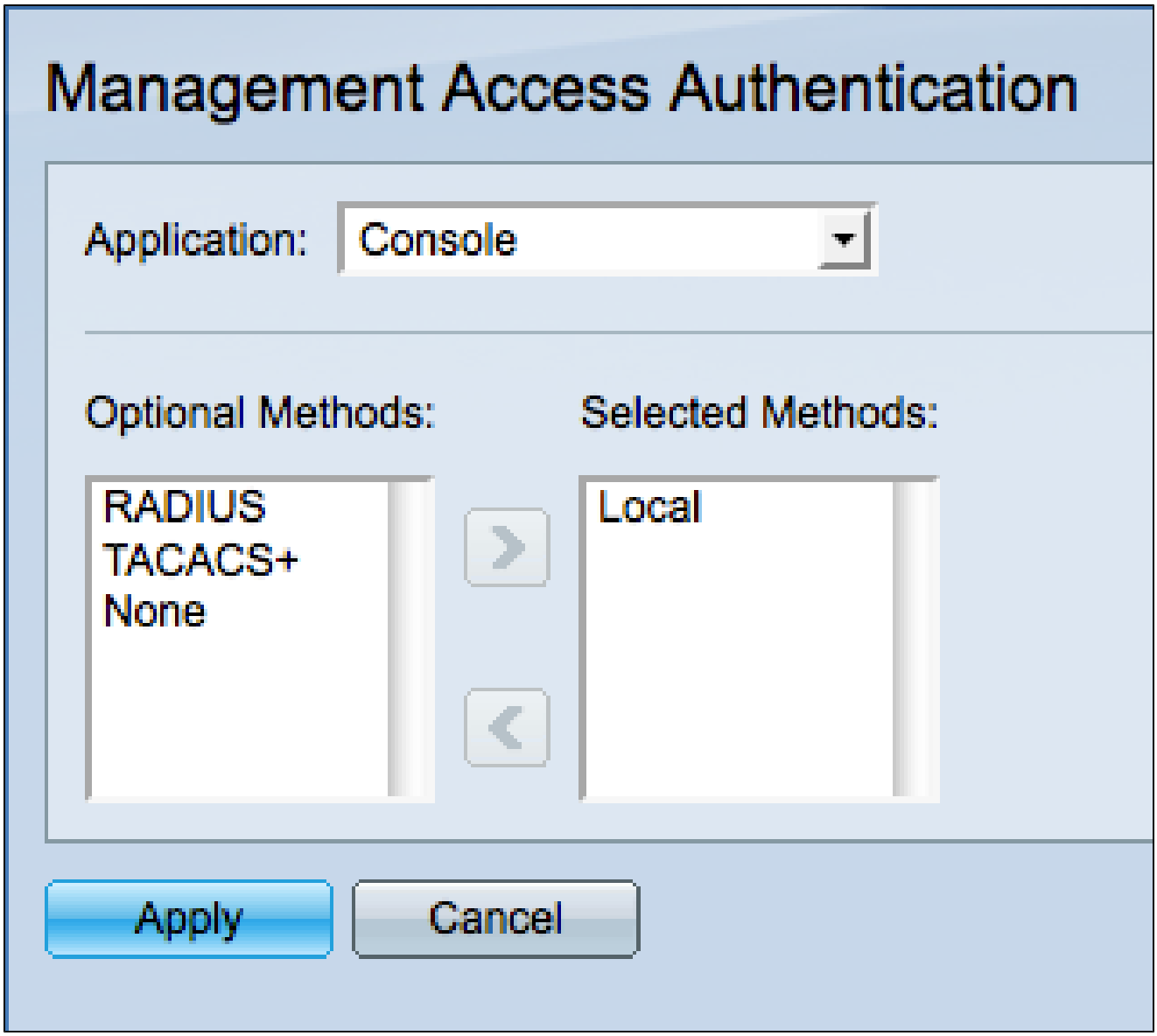
・ SF/SG 200およびSF/SG 300シリーズマネージドスイッチ

## [Software Version]

•1.3.0.62

## 管理アクセス認証

ステップ 1：Web設定ユーティリティにログインし、Security > Management Access Authenticationの順に選択します。 Management Access Authenticationページが開きます。




ステップ 2：Applicationドロップダウンリストから、認証を割り当てるアプリケーションのタイプを選択します。 考えられる用途は次のとおりです。

・ コンソール：コンソールインターフェイスを使用してスイッチを管理できます。スイッチのIPアドレスが不明な場合でも、スイッチに接続して設定を行うことができます。

・ Telnet:TCP/IPネットワークを介してスイッチにリモート接続できる、文字ベースの通信プロトコル。 Telnetは暗号化されないため、推奨されません。

・ セキュアTelnet(SSH):Telnetと暗号化と同じ機能を実行します。 リモート接続にはSSHが推奨されます。

・ HTTP：スイッチのGraphical User Interface（GUI；グラフィカルユーザインターフェイス）にアクセスできるプロトコル。 これは、コマンドプロンプトベースのTelnetおよびSSHとは対照的です。

・ セキュアHTTP(HTTPS)：セキュア通信を追加して、HTTPと同じ機能を実行します。

ステップ 3：Optional Methodsのリストから認証方式を選択し、>ボタンをクリックして Selected Methodsリストに移動します。異なる方法で提供されるセキュリティレベルは異なります。

注：認証方式が選択される順序は、ユーザ認証が発生する順序です。 ローカルの前に RADIUSを選択すると、デバイスはローカル方式の前にRADIUSサーバによってユーザの認証を試みます。

・ RADIUS:RADIUSはパスワードのみを暗号化します。認証はRADIUSサーバ上にあり、設定されたRADIUSサーバが必要です。

・ TACACS+:TACACS+は認証中にすべてのデータを暗号化する。 認証はTACACS+サーバ上にあり、設定されたTACACS+サーバが必要です。

・ なし – スイッチへのアクセスに認証は必要ありません。

・ ローカル：ユーザ情報はスイッチに保存された情報によって確認されます。

ステップ 4：Applyをクリックして認証設定を保存するか、Cancelをクリックして変更をキャンセルします。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。