Authentification d'accès de gestion sur les commutateurs gérés de la gamme 200/300

Objectif

Les modes d'accès à la gestion tels que SSH, Console, Telnet, HTTP et HTTPS permettent à un utilisateur d'accéder à un périphérique. L'authentification peut être requise des utilisateurs pour améliorer la sécurité. Les commutateurs administrables des gammes 200 et 300 peuvent s'authentifier localement ou sur un serveur TACACS+ ou RADIUS. Ce document explique comment attribuer une méthode d'authentification sur les commutateurs gérés des gammes 200 et 300.

Périphériques pertinents

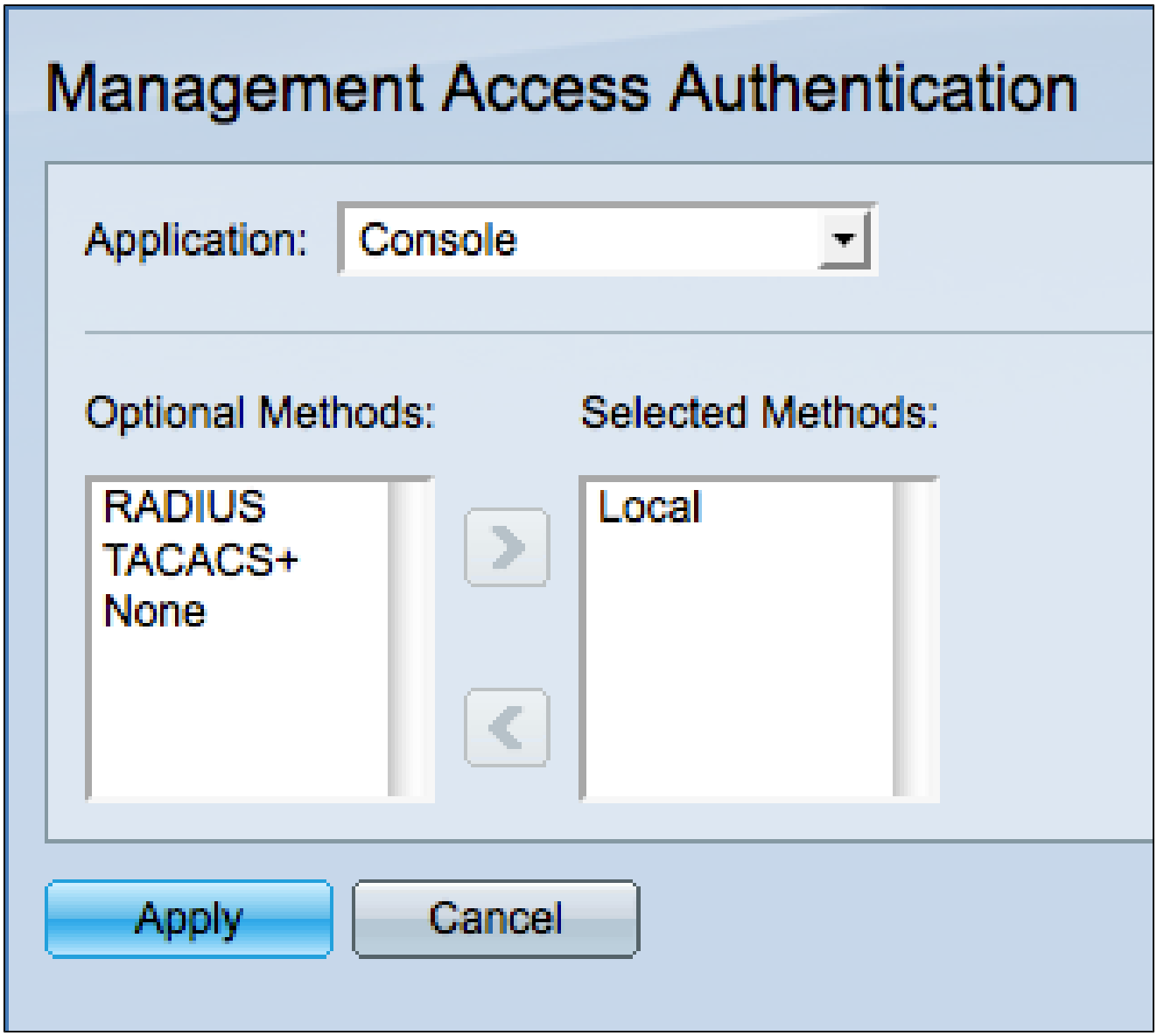
· Commutateurs administrables des gammes SF/SG 200 et SF/SG 300

Version du logiciel

•1.3.0.62

Authentification d'accès de gestion

Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez Security > Management Access Authentication. La page Management Access Authentication s'ouvre :



Étape 2. Sélectionnez le type d'application auquel vous souhaitez attribuer l'authentification dans la liste déroulante Application. Les applications possibles sont :

· Console : permet de gérer le commutateur à l'aide d'une interface de console. Vous permet de vous connecter au commutateur et d'effectuer certaines configurations même si l'adresse IP du commutateur est inconnue.

· Telnet : protocole de communication à base de caractères qui vous permet de vous connecter à distance au commutateur sur un réseau TCP/IP. Telnet n’est pas recommandé en raison du manque de chiffrement.

· Secure Telnet (SSH) : exécute les mêmes fonctions que telnet plus le cryptage. SSH est recommandé pour les connexions à distance.

· HTTP : protocole qui vous permet d'accéder à l'interface graphique utilisateur (GUI) du

commutateur. Contrairement à Telnet et SSH qui sont basés sur une invite de commandes.

· HTTP sécurisé (HTTPS) : exécute les mêmes fonctions que le protocole HTTP avec l'ajout d'une communication sécurisée.

Étape 3. Choisissez une méthode d'authentification dans la liste des méthodes facultatives, puis cliquez sur le bouton > pour la déplacer vers la liste Méthodes sélectionnées. Différentes méthodes offrent différents niveaux de sécurité.

Remarque : l'ordre dans lequel les méthodes d'authentification sont sélectionnées correspond à l'ordre dans lequel l'authentification de l'utilisateur a lieu. Si RADIUS est sélectionné avant local, le périphérique tentera d'authentifier l'utilisateur par un serveur RADIUS avant la méthode locale.

· RADIUS : RADIUS chiffre uniquement le mot de passe. L'authentification se fait sur un serveur RADIUS et nécessite un serveur RADIUS configuré.

· TACACS+ : TACACS+ chiffre toutes les données pendant l'authentification. L'authentification se fait sur un serveur TACACS+ et nécessite un serveur TACACS+ configuré.

· None : l'authentification n'est pas requise pour accéder au commutateur.

· Local : les informations relatives à l'utilisateur sont vérifiées par les informations stockées sur le commutateur.

Étape 4. Cliquez sur Apply pour enregistrer les paramètres d'authentification ou sur Cancel pour annuler vos modifications.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.