Configuration RADIUS sur les commutateurs gérés de la gamme 200/300

Objectif

Le service RADIUS (Remote Authorization Dial-In User Service) est un service de sécurité utilisé pour l'authentification des utilisateurs dans les réseaux dotés d'une architecture de sécurité centralisée. Les commutateurs administrables de la gamme 200/300 peuvent faire office de client RADIUS sur votre réseau et, en association avec un serveur RADIUS, vous pouvez établir un système centralisé pour l'authentification des utilisateurs sur votre réseau. Cet article explique comment configurer un serveur RADIUS et appliquer des méthodes d'authentification sur les commutateurs gérés de la gamme 200/300.

Périphériques pertinents | Version du logiciel

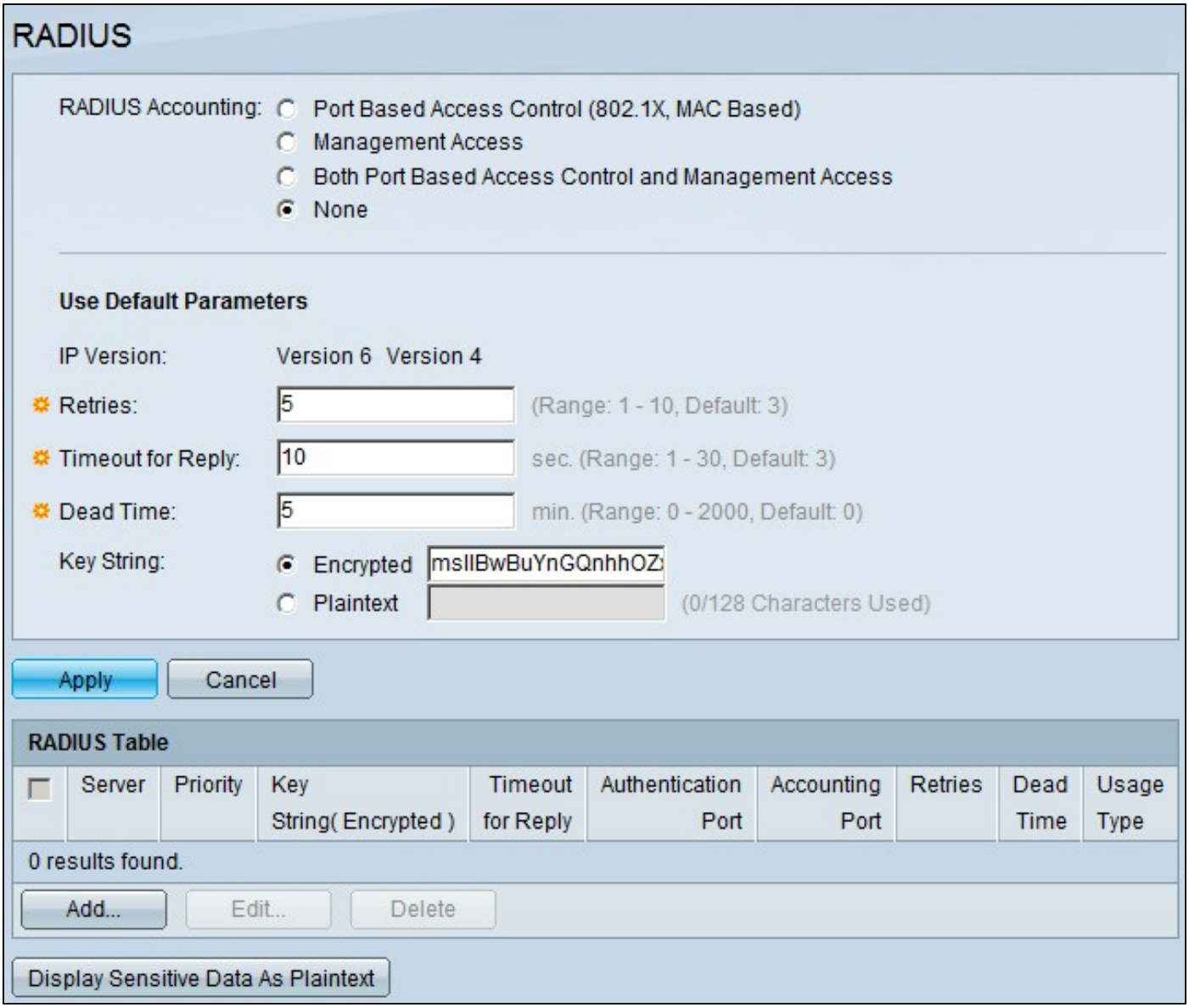
- Série SF/SG 200 - 1.2.9.x
- Série SF/SG 300 - 1.2.9.x

Configuration par défaut RADIUS

Cette section vous guide à travers la configuration par défaut d'un serveur RADIUS. Ces valeurs par défaut peuvent être utilisées pour tout serveur RADIUS que vous souhaitez ajouter à un commutateur.

Étape 1

Connectez-vous à l'utilitaire de configuration Web et choisissez Security > RADIUS. La page RADIUS s'ouvre :



Les images de cet article proviennent d'un commutateur SG300.

Étape 2

Dans le champ RADIUS Accounting, cliquez sur l'une des options suivantes :

- Port Based Access Control (802.1x, MAC) : pour utiliser le serveur RADIUS pour la gestion des comptes de ports 802.1x.
- Accès à la gestion : pour utiliser le serveur RADIUS pour la gestion des connexions.
- Contrôle d'accès basé sur les ports et accès de gestion : pour utiliser le serveur RADIUS pour 802.1x et la gestion des comptes de connexion.
- None : pour ne pas utiliser le serveur RADIUS à des fins de comptabilité.

Radius Accounting n'est pas disponible sur les commutateurs de la gamme SG200.

Étape 3

Dans la section Use Default Parameters, dans le champ Retries, saisissez le nombre de tentatives effectuées par le commutateur pour authentifier le serveur RADIUS.

Étape 4

Dans le champ Délai de réponse, saisissez le délai en secondes de chaque tentative d'authentification effectuée sur le serveur RADIUS.

Étape 5

Dans le champ Dead Time, saisissez le délai en minutes avant que le commutateur déclare un serveur RADIUS sans réponse comme étant mort et passe au serveur disponible suivant pour tenter la connexion.

Étape 6

Dans le champ Key String, saisissez la clé utilisée pour l'authentification et le chiffrement entre le commutateur et le serveur RADIUS. Cette clé doit correspondre sur le serveur RADIUS et sur le commutateur. Cliquez sur l'une des options suivantes :

- Chiffré : si vous disposez d'une clé chiffrée provenant d'un autre périphérique, saisissez la clé.
- Texte brut : si vous ne disposez pas d'une clé chiffrée provenant d'un autre périphérique, saisissez la clé en texte brut.

Étape 7

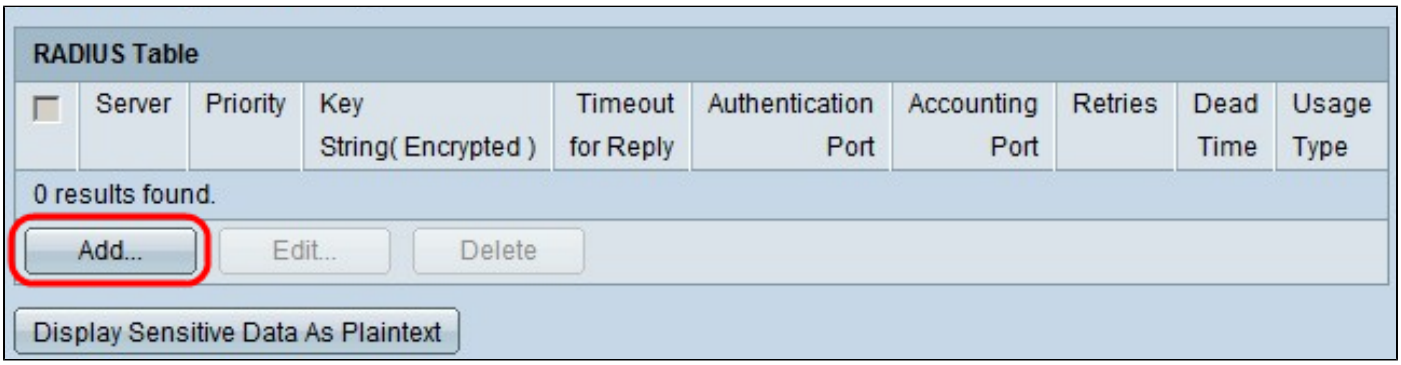
Cliquez sur Apply pour enregistrer ces valeurs par défaut et les rendre disponibles pour un serveur RADIUS.

Ajouter/Modifier un serveur RADIUS

Dans cette section, une procédure pas à pas est présentée qui explique comment ajouter ou modifier un serveur RADIUS à un commutateur géré de la gamme 200/300.

Étape 1

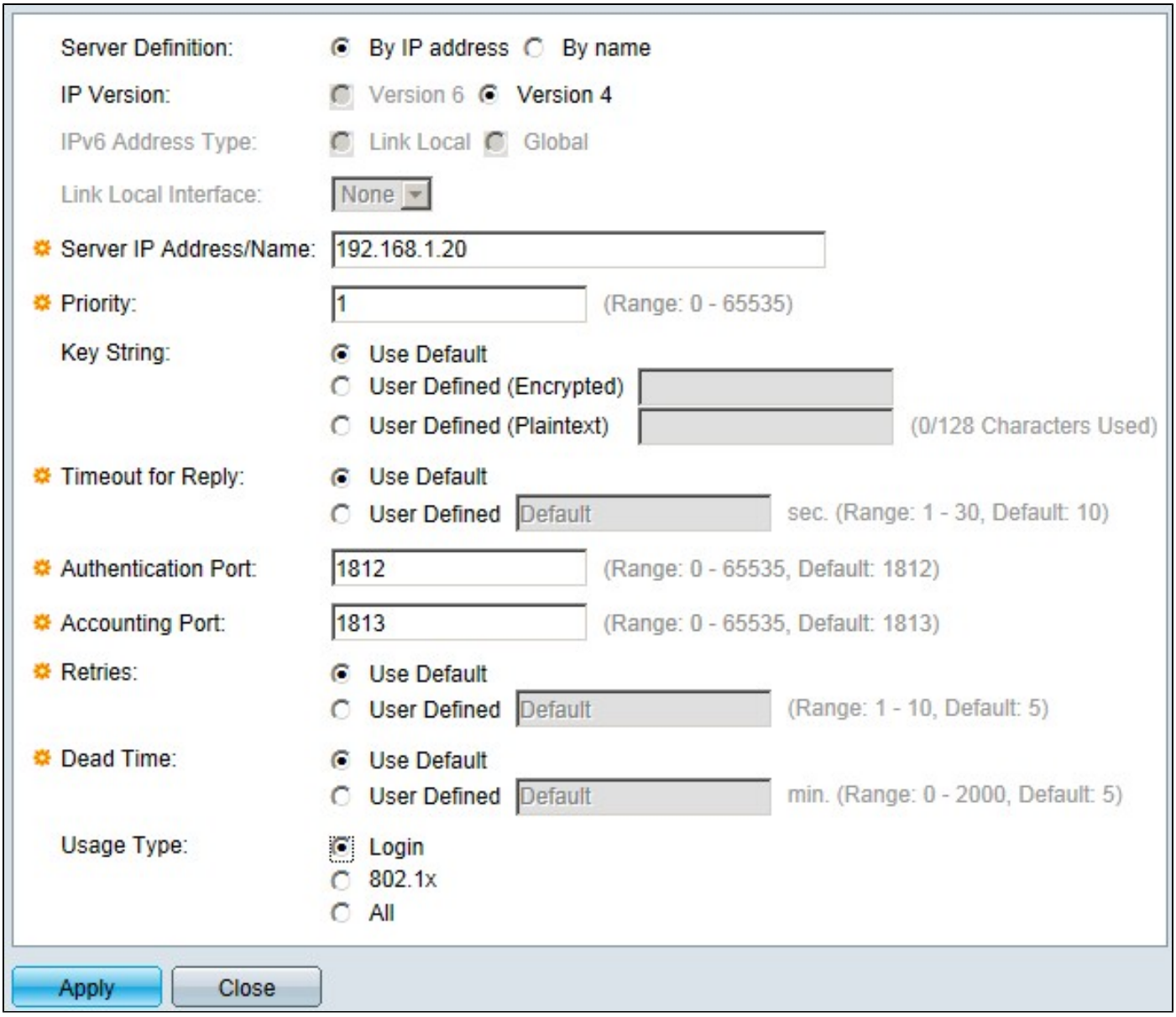
Connectez-vous à l'utilitaire de configuration Web et choisissez Security > RADIUS. La page RADIUS s'ouvre :



Étape 2

Dans la section RADIUS Table, cliquez sur Add. La fenêtre Add Radius Server s'affiche.

Pour modifier un serveur RADIUS en cours, cliquez sur Edit et modifiez les propriétés souhaitées du serveur RADIUS.



Étape 3

Dans le champ Définition du serveur, cliquez sur l'une des options suivantes :

- Par nom : si le serveur RADIUS est défini par un nom.
- By IP Address (Par adresse IP) : si le serveur RADIUS est défini avec une adresse IP.

Étape 4

Dans le champ IP Version, cliquez sur Version 6 ou Version 4 comme type d'adresse IP du serveur RADIUS.

Étape 5

Si la version 6 est choisie comme adresse IP dans le type d'adresse IPv6, cliquez sur l'une des options suivantes :

- Link Local : adresse IPv6 qui identifie uniquement les hôtes sur une liaison réseau unique.
- Global : adresse IPv6 accessible à partir d'autres réseaux.

Étape 6

Si le type d'adresse IPv6 Link Local est sélectionné, dans la liste déroulante Link Local Interface, sélectionnez l'interface appropriée.

Étape 7

Dans le champ Server IP Address/Name, saisissez l'adresse IP ou le nom du serveur RADIUS.

Étape 8

Dans le champ Priority, saisissez la priorité du serveur RADIUS que le commutateur utilisera. Le serveur ayant la priorité la plus élevée est interrogé en premier dans le commutateur. Zéro (0) donne la priorité la plus élevée.

Étape 9

Dans le champ Key String, cliquez sur l'une des options suivantes :

- Use Default : pour utiliser la clé par défaut pour l'authentification.
- Défini par l'utilisateur (chiffré) : si disponible, saisissez la clé chiffrée.
- Défini par l'utilisateur (texte brut) : si cette option n'est pas disponible, saisissez la clé en texte brut.

Étape 10

Dans le champ Délai de réponse, cliquez sur l'une des options suivantes :

- Utiliser la valeur par défaut : pour utiliser la valeur par défaut.
- User Defined (Défini par l'utilisateur) : saisissez le nombre de secondes pendant lequel le commutateur attend chaque tentative de connexion au serveur RADIUS.

Étape 11

Dans le champ Authentication Port, saisissez le port UDP utilisé par le serveur RADIUS pour l'authentification.

Étape 12

Dans le champ Port de gestion, saisissez le port UDP utilisé par le serveur RADIUS pour la gestion des comptes.

Étape 13

Dans le champ Retries, cliquez sur l'une des options suivantes :

- Utiliser la valeur par défaut : pour utiliser la valeur par défaut.
- Défini par l'utilisateur : pour utiliser une valeur différente. Saisissez le nombre de tentatives effectuées par le commutateur avant qu'une connexion défaillante au serveur RADIUS ne soit considérée comme ayant eu lieu.

Étape 14

Dans le champ Dead Time, cliquez sur l'une des options suivantes :

- Utiliser la valeur par défaut : pour utiliser la valeur par défaut.
- Défini par l'utilisateur : pour utiliser une valeur différente. Entrez le délai en minutes avant que le commutateur déclare un serveur RADIUS sans réponse comme étant mort et passe au serveur disponible suivant pour tenter la connexion.

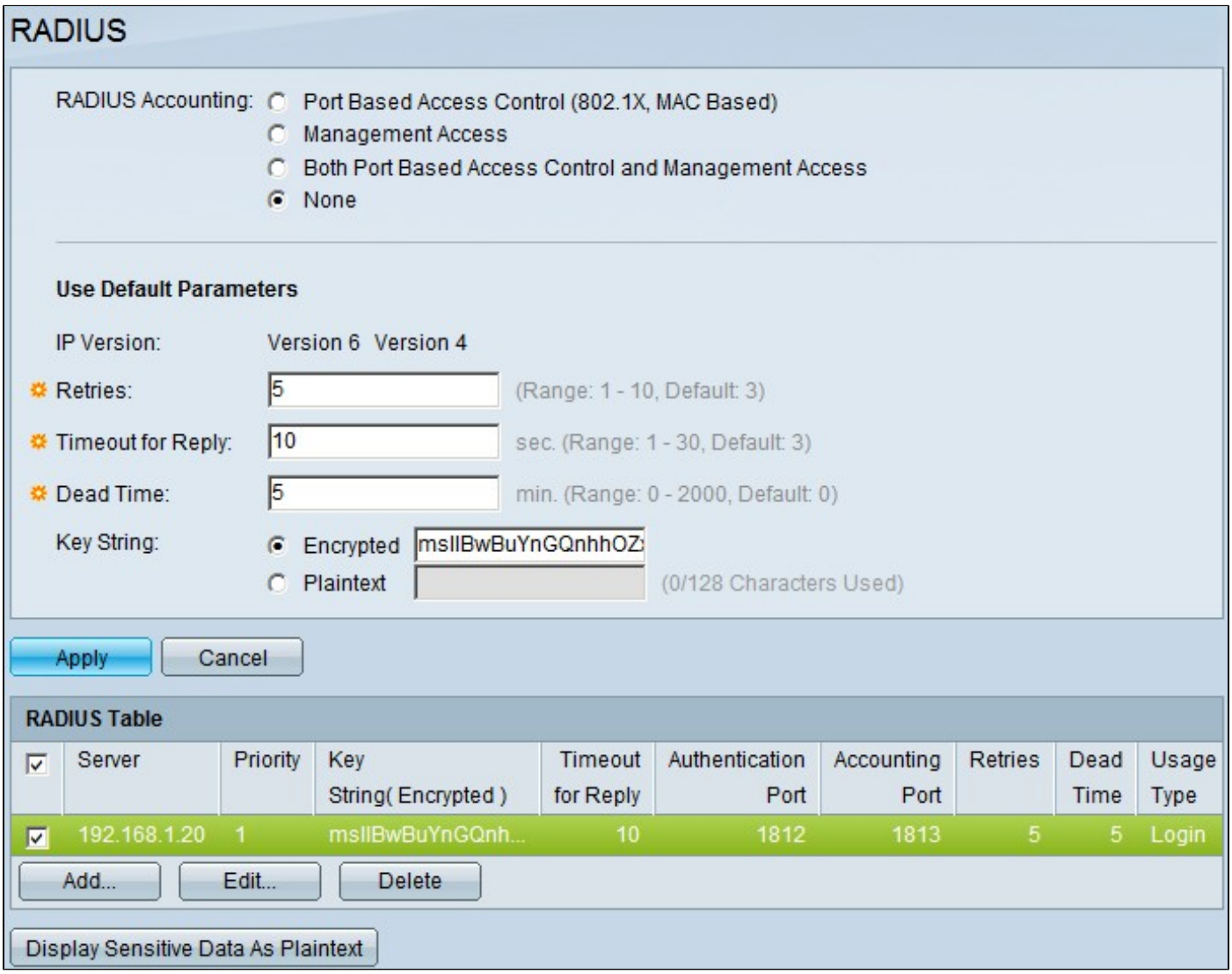
Étape 15

Dans le champ Type d'utilisation, cliquez sur l'une des options suivantes :

- Login (Connexion) : authentifie les administrateurs du commutateur.
- 802.1x : le serveur RADIUS vérifie les informations d'identification de sécurité des utilisateurs qui demandent un accès réseau en fonction du schéma PNAC (Network Access Control) basé sur les ports 802.1x.
- Tous - Utilise les deux types d'authentification.

Étape 16

Cliquez sur Apply.



Étape 17

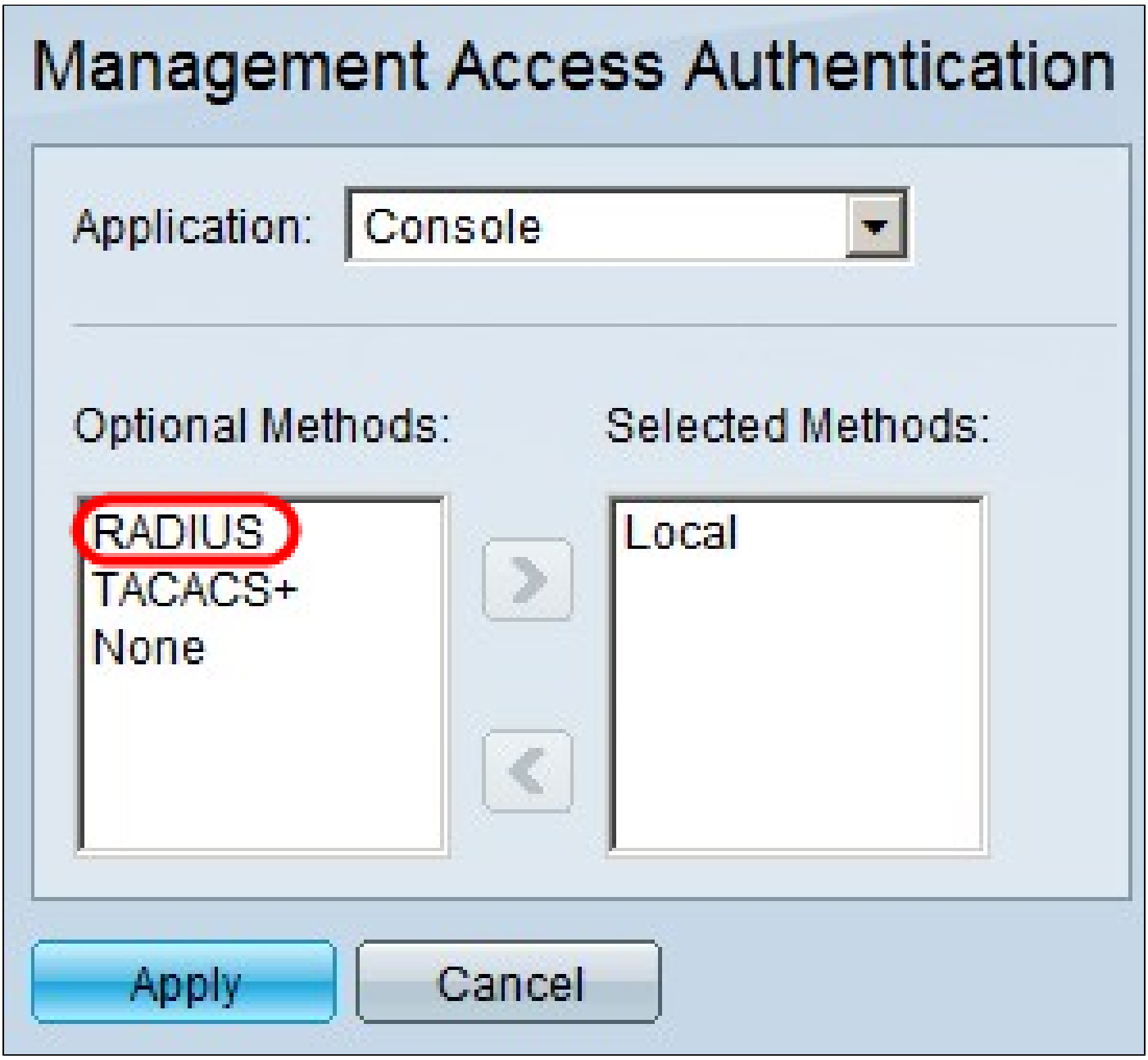
(Facultatif) Pour supprimer un serveur RADIUS, dans la section Table RADIUS, cochez la case du serveur RADIUS que vous souhaitez supprimer et cliquez sur Supprimer.

Authentification RADIUS

Une fois le serveur RADIUS configuré correctement, vous devez l'authentifier sur le commutateur. Cette section explique comment authentifier un serveur RADIUS sur les commutateurs gérés de la gamme 200/300.

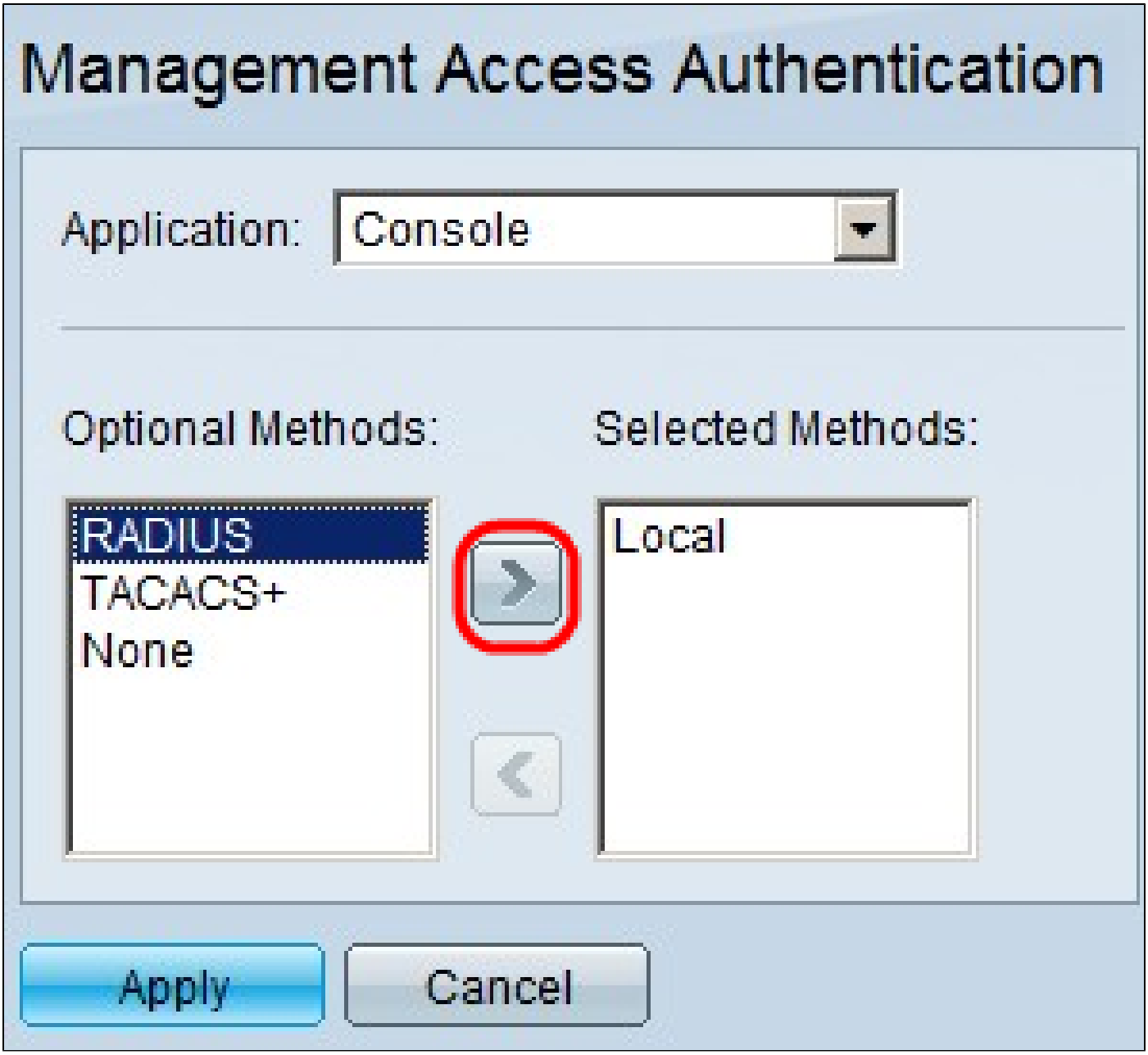
Étape 1

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



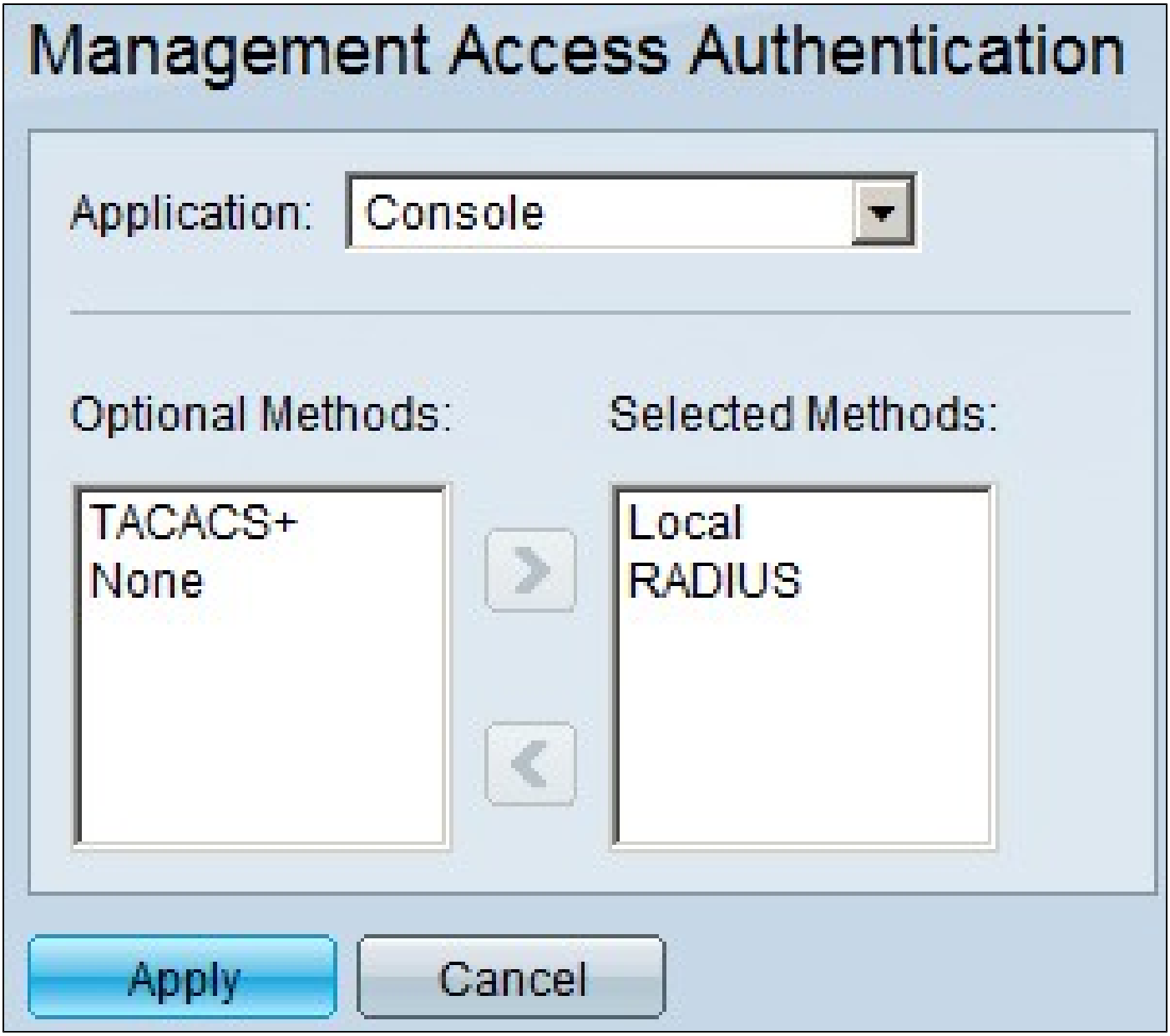
Étape 2

Dans la liste Optional Methods, sélectionnez RADIUS.



Étape 3

Cliquez sur le bouton >.



Étape 4

Cliquez sur Apply.

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.