Configuration de l'authentification de session et de l'hôte 802.1X sur les commutateurs des gammes 200/220/300

Objectif

802.1X est une norme IEEE pour le contrôle d'accès réseau basé sur les ports (PNAC) qui fournit une méthode d'authentification aux périphériques connectés aux ports. La page Host and Session Authentication de l'interface utilisateur graphique d'administration de votre commutateur permet de définir le type d'authentification utilisé par port. L'authentification par port est une fonctionnalité qui permet à un administrateur réseau de diviser les ports de commutateur en fonction du type d'authentification souhaité. La page Authenticated Hosts affiche des informations sur les hôtes qui ont été authentifiés.

Cet article explique comment configurer l'authentification d'hôte et de session par port et comment afficher les hôtes authentifiés dans les paramètres de sécurité 802.1X sur les commutateurs gérés de la gamme 200/220/300.

Périphériques pertinents

- Série Sx200
- Série Sx220
- Gamme Sx300

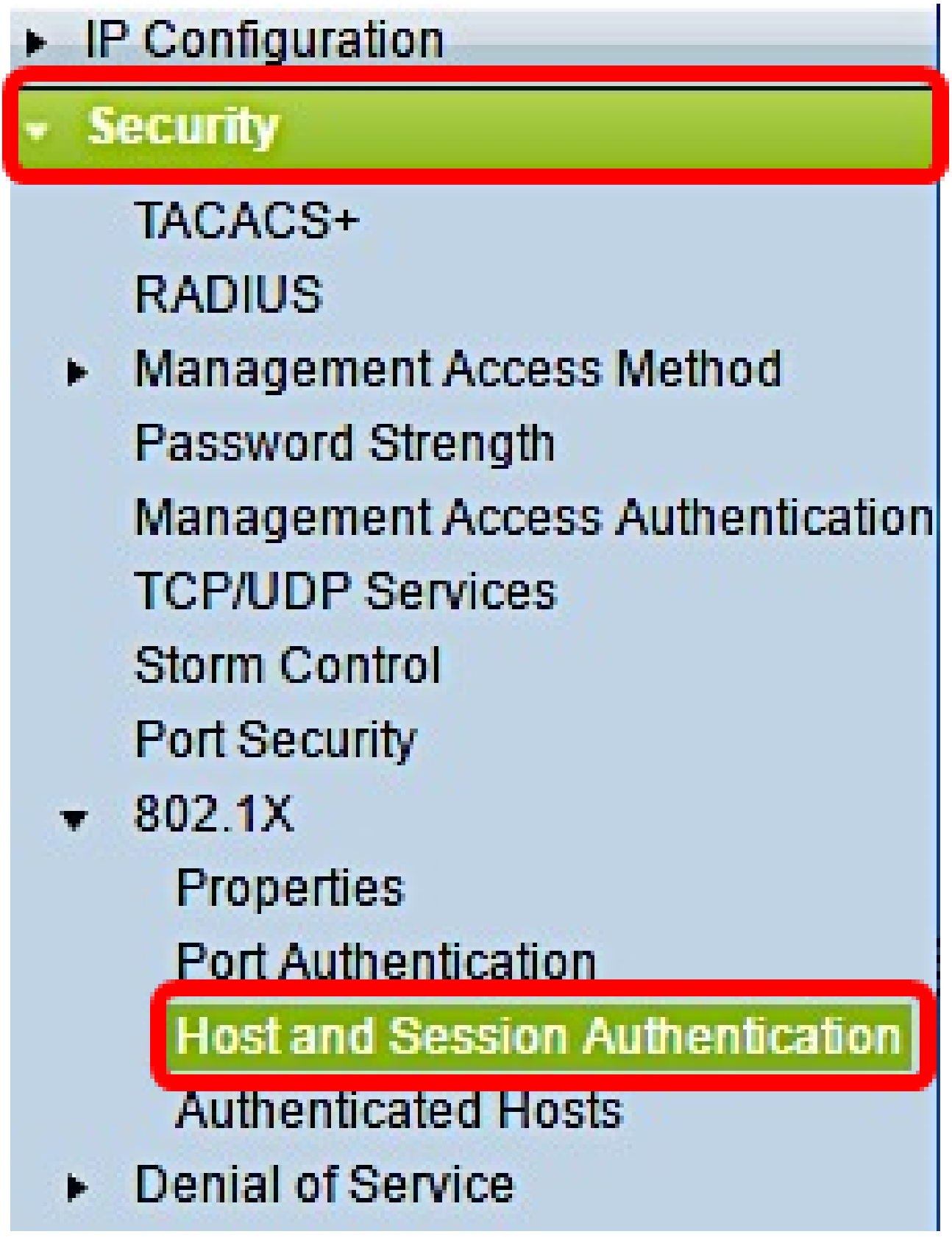
Version du logiciel

- 1.4.5.02 - Série Sx200, Série Sx300
- 1.1.0.14 : Série Sx220

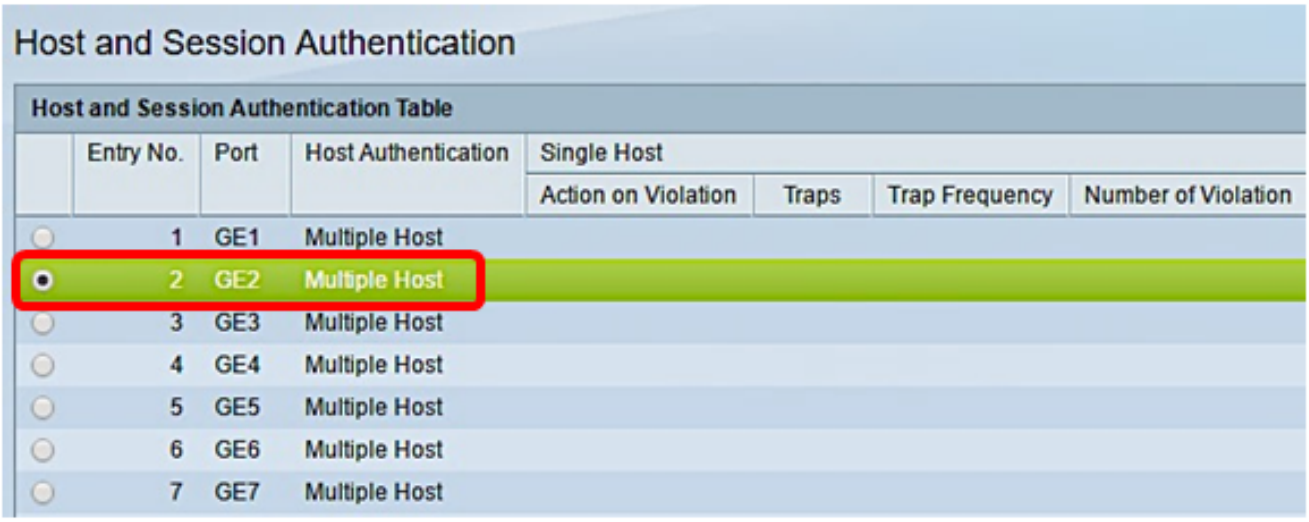
Authentification hôte et session

Étape 1. Connectez-vous à l'utilitaire Web et choisissez Security > 802.1X > Host and Session Authentication.

Remarque : les images ci-dessous proviennent du commutateur intelligent SG220-26P.

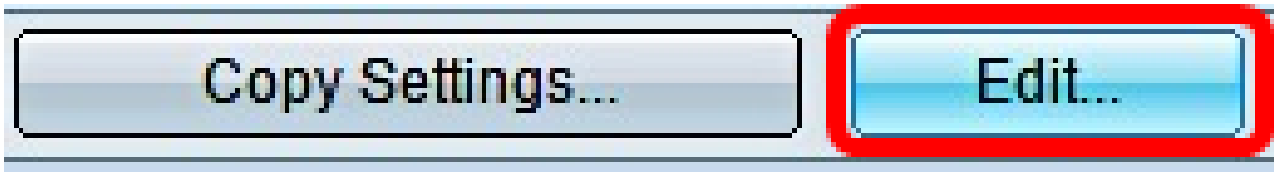


Étape 2. Sélectionnez la case d'option du port que vous souhaitez modifier.

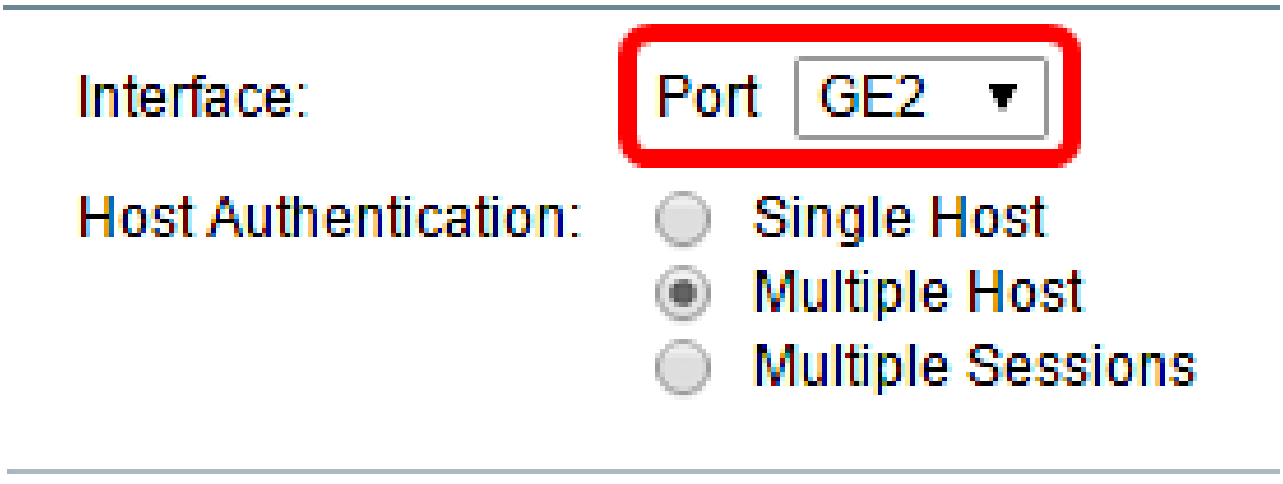


Remarque : dans cet exemple, le port GE2 est choisi.

Étape 3. Cliquez sur Edit pour modifier l'authentification d'hôte et de session pour le port spécifié.



Étape 4. La fenêtre Edit Port Authentication s'affiche alors. Dans la liste déroulante Interface, vérifiez que le port spécifié est celui que vous avez choisi à l'étape 2. Sinon, cliquez sur la flèche de la liste déroulante et sélectionnez le port de droite.

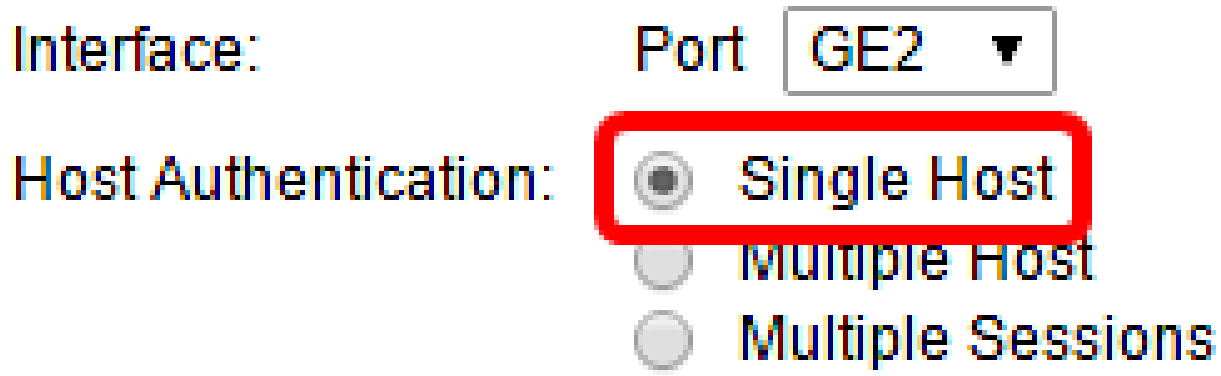


Remarque : si vous utilisez la gamme 200 ou 300, la fenêtre Edit Host and Session Authentication s'affiche.

Étape 5. Cliquez sur la case d'option correspondant au mode d'authentification souhaité dans le champ Host Authentication. Les options sont les suivantes :

- Hôte unique : le commutateur accorde uniquement à un hôte autorisé l'accès au port.
- Hôtes multiples (802.1X) : plusieurs hôtes peuvent accéder au port unique. Il s'agit du mode par défaut. Le commutateur ne nécessite que l'autorisation du premier hôte, puis tous les autres clients connectés au port ont accès au réseau. Si l'authentification échoue, le premier hôte et tous les clients connectés se voient refuser l'accès au réseau.
- Sessions multiples : plusieurs hôtes peuvent accéder au port unique, mais chaque hôte doit être authentifié.

Remarque : dans cet exemple, un hôte unique est choisi.

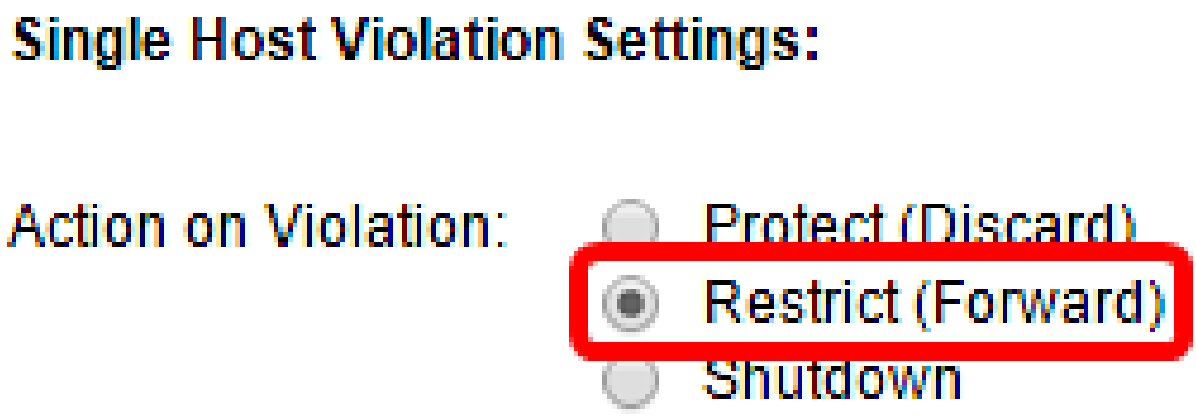


Remarque : si vous avez sélectionné Multiple Host ou Multiple Sessions, passez à l'étape 9.

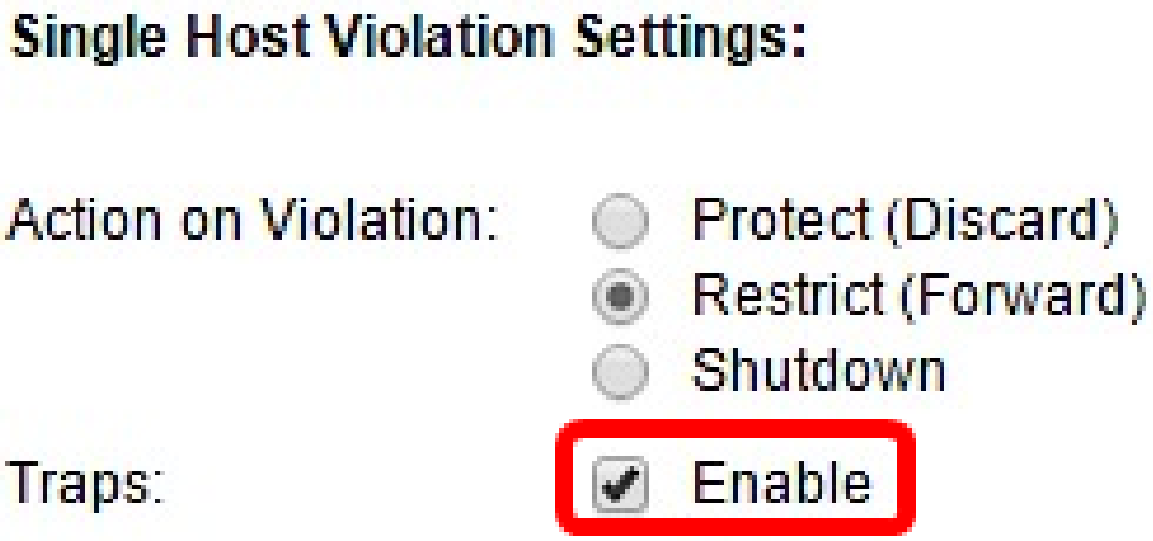
Étape 6. Dans la zone Paramètres de violation d'hôte unique, cliquez sur la case d'option correspondant à l'action souhaitée en cas de violation. Une violation se produit si des paquets arrivent d'un hôte dont l'adresse MAC ne correspond pas à l'adresse MAC du demandeur d'origine. Dans ce cas, l'action détermine ce qui arrive aux paquets qui arrivent des hôtes qui ne sont pas considérés comme le demandeur d'origine. Les options sont les suivantes :

- Protect (Discard) : abandonne les paquets. Il s'agit de l'action par défaut.
- Restrict (Forward) : permet d'accéder aux paquets et de les transférer.
- Shutdown : bloque les paquets et arrête le port. Le port reste inactif jusqu'à ce qu'il soit réactivé ou que le commutateur soit redémarré.

Remarque : dans cet exemple, Restrict (Forward) est sélectionné.



Étape 7. (Facultatif) Cochez Enable dans le champ Traps pour activer les déroutements. Les déroutements sont des messages SNMP (Simple Network Management Protocol) générés qui servent à signaler les événements système. Une interruption est envoyée au gestionnaire SNMP du commutateur lorsqu'une violation se produit.



Étape 8. Saisissez le délai souhaité en secondes entre les déroutements envoyés dans le champ Trap Frequency. Définit la fréquence d'envoi des déroutements.

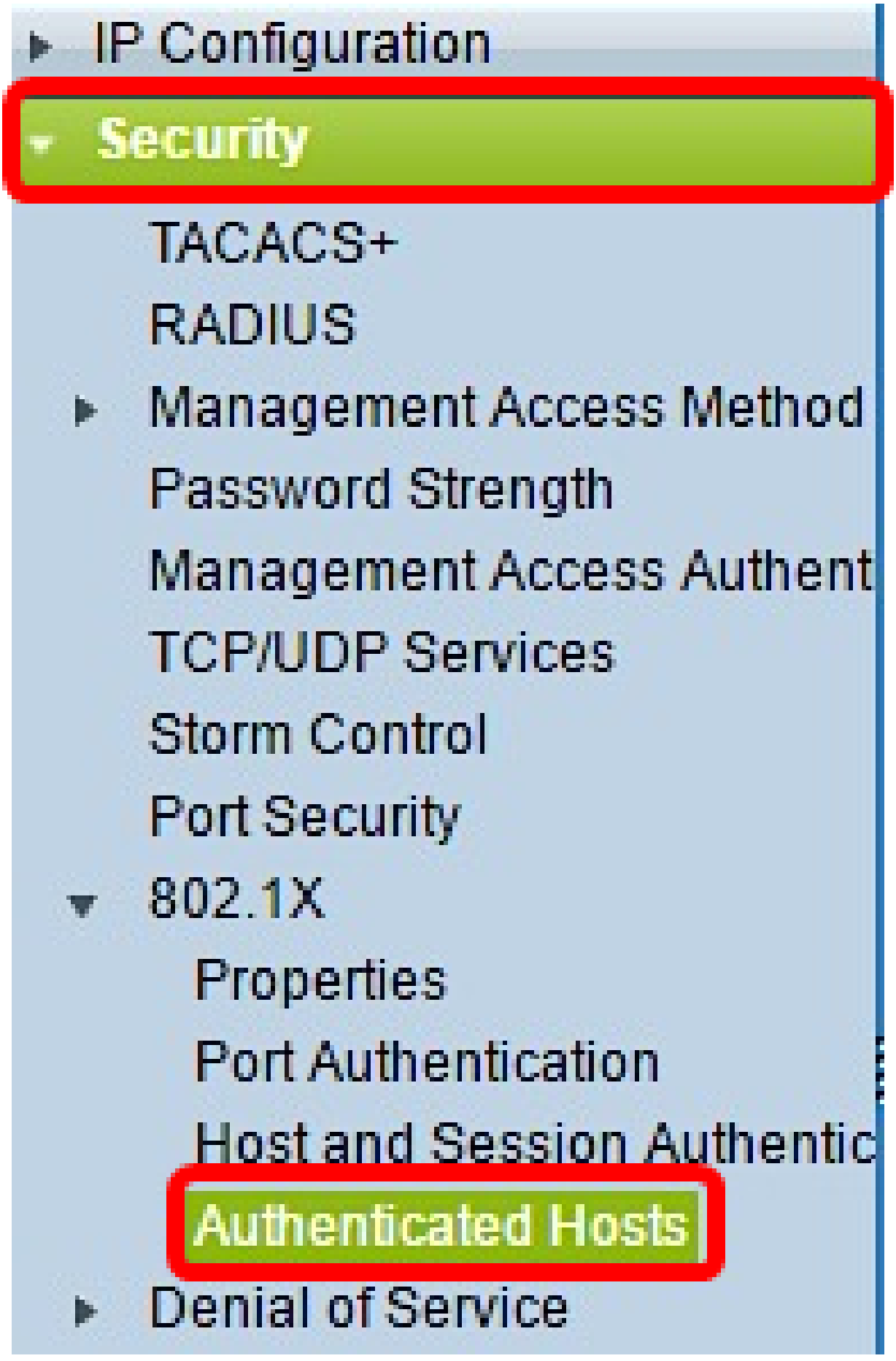
Remarque : dans cet exemple, 30 secondes sont utilisées.

Étape 9. Cliquez sur Apply.

Vous devez maintenant avoir configuré l'authentification de l'hôte et de la session sur votre commutateur.

Affichage des hôtes authentifiés

Étape 1. Connectez-vous à l'utilitaire Web et choisissez Security > 802.1X > Authenticated Host.


IP Configuration
Security
TACACS+
RADIUS
Management Access Method
Password Strength
Management Access Authent
TCP/UDP Services
Storm Control
Port Security
802.1X
Properties
Port Authentication
Host and Session Authentic
Authenticated Hosts
Denial of Service

Le tableau Authenticated Hosts affiche les informations suivantes pour les hôtes authentifiés.

- User Name : spécifie le nom du demandeur qui a été authentifié sur le port.
- Port : indique le numéro de port auquel le demandeur est connecté.
- Session Time : indique la durée totale de connexion du demandeur au port. Le format est JJ:HH:MM:SS (Jour:Heure:Minute:Seconde).
- Authentication Method : spécifie la méthode utilisée pour l'authentification. Les valeurs possibles sont les suivantes :
- None : indique que le demandeur n'a pas été authentifié.
- Radius : indique que le demandeur a été authentifié par le serveur RADIUS.
- MAC Address : spécifie l'adresse MAC du demandeur.
- VLAN ID : spécifie le VLAN auquel l'hôte appartient. La colonne VLAN ID est uniquement disponible dans les commutateurs Smart Plus de la gamme 220.

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.

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.