Configuration de l'authentification 802.1x sur les commutateurs de la gamme Cisco Business 220

Objectif

L'objectif de cet article est de vous montrer comment configurer l'authentification 802.1x sur les commutateurs intelligents de la gamme Cisco Business 220.

Périphériques pertinents | Version du micrologiciel

- Série CBS220 (Fiche technique) |2.0.0.17

Introduction

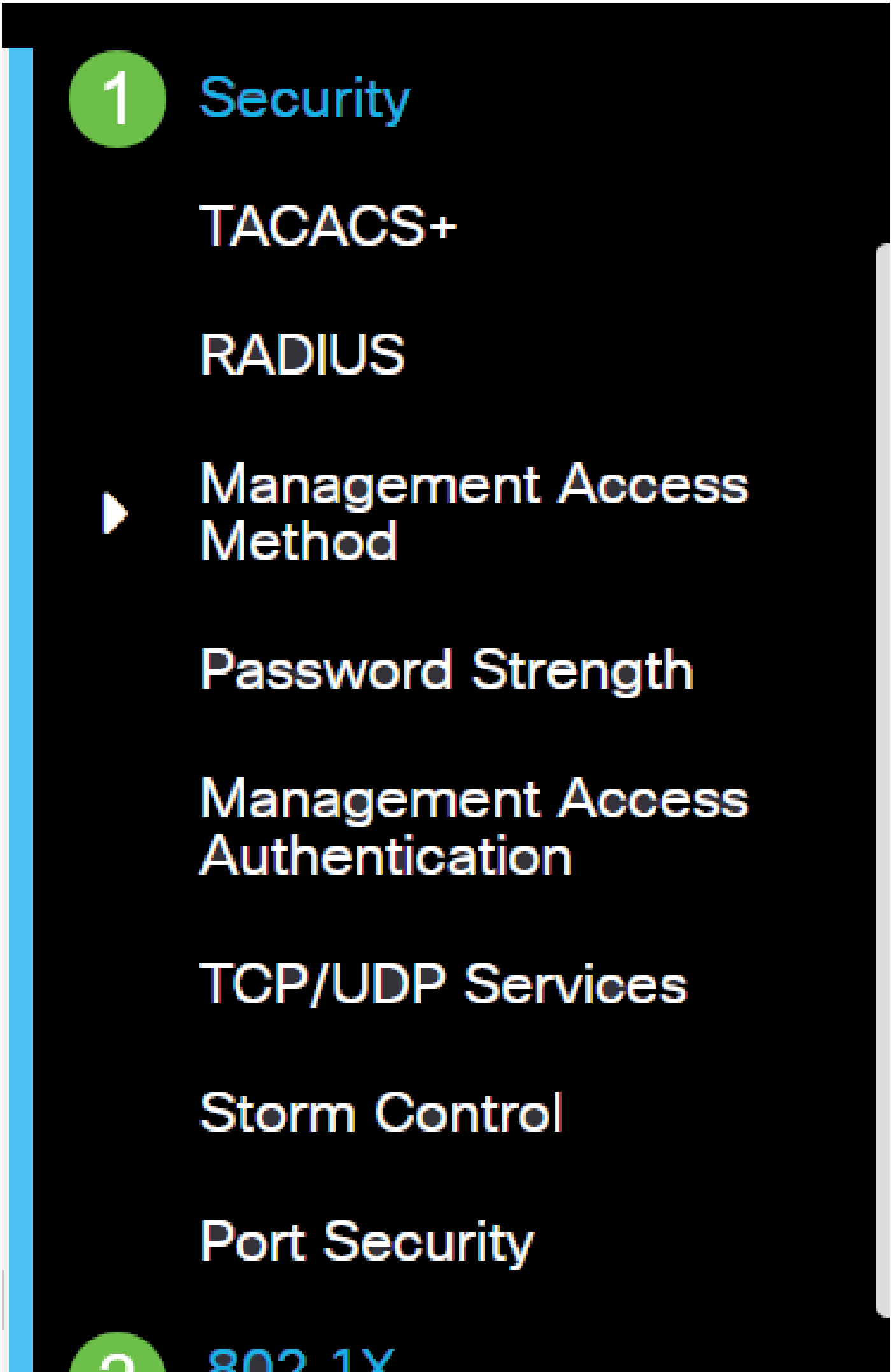
L'authentification de port permet de configurer les paramètres de chaque port. Comme certaines modifications de configuration ne sont possibles que lorsque le port est à l'état Forcer l'autorisation, comme l'authentification de l'hôte, il est recommandé de remplacer le contrôle de port par Forcer l'autorisation avant d'effectuer des modifications. Une fois la configuration terminée, remettez le contrôle de port à son état précédent.

Un port 802.1x défini sur celui-ci ne peut pas devenir membre d'un LAG. 802.1x et la sécurité des ports ne peuvent pas être activés sur le même port en même temps. Si vous activez la sécurité des ports sur une interface, le contrôle de port administratif ne peut pas être modifié en mode Auto.

Configurer l'authentification des ports

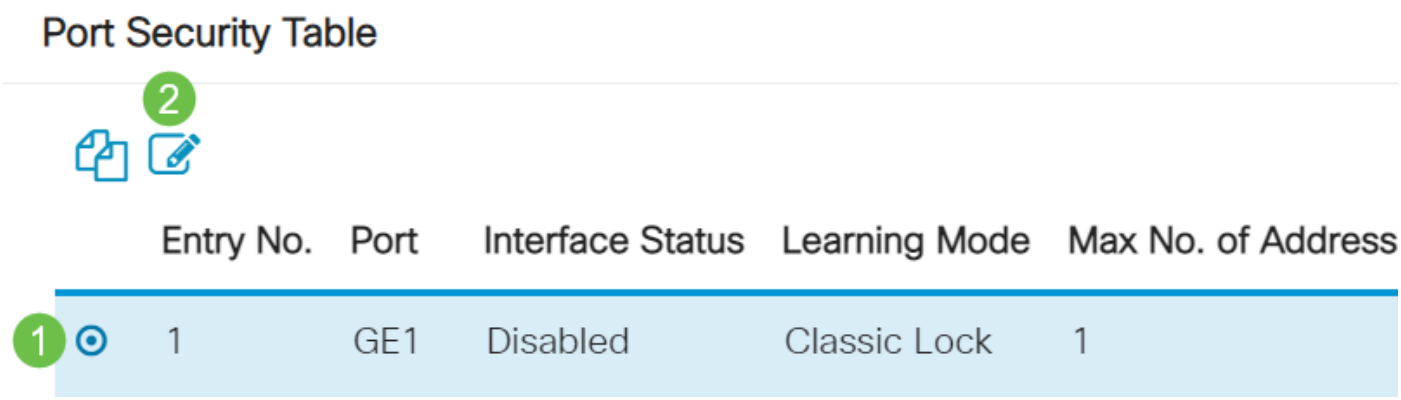
Étape 1

Connectez-vous à l'interface utilisateur Web du commutateur et choisissez Security > 802.1x > Port Authentication.


1
Security
TACACS+
RADIUS
Management Access Method
Password Strength
Management Access Authentication
TCP/UDP Services
Storm Control
Port Security

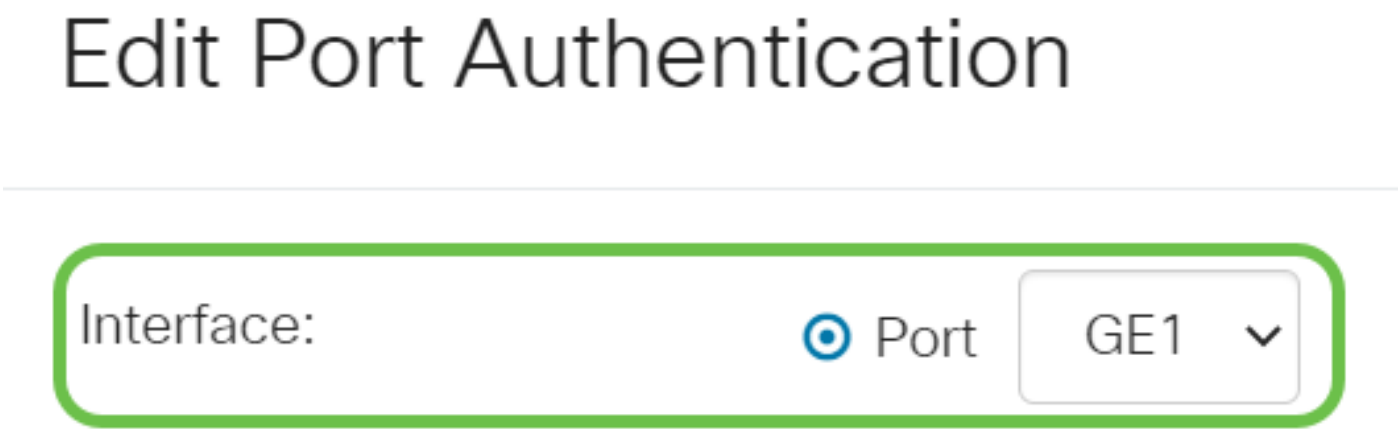
Étape 2

Cliquez sur la case d'option du port que vous souhaitez configurer, puis cliquez sur l'icône de modification.



Étape 3

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 choisissez le port de droite.

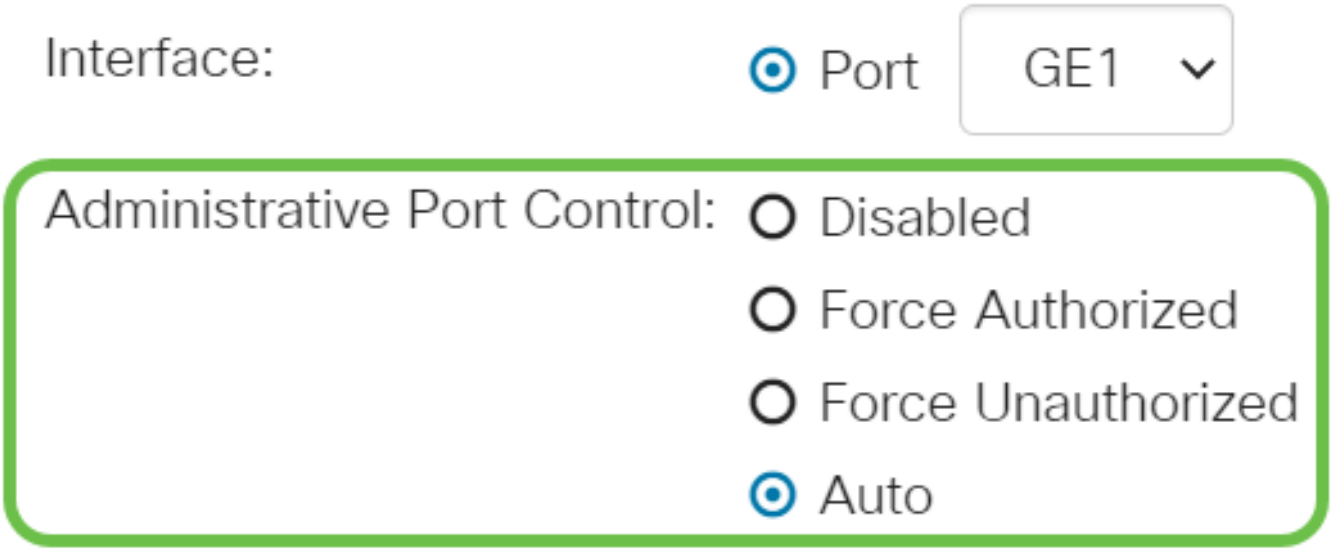


Étape 4

Sélectionnez une case d'option pour le contrôle de port d'administration. Cela déterminera l'état d'autorisation du port. Les options sont les suivantes :

- Disabled : désactive 802.1x. Il s'agit de l'état par défaut.
- Force Unauthorized : refuse l'accès à l'interface en plaçant l'interface dans l'état non autorisé. Le commutateur ne fournit pas de services d'authentification au client via l'interface.
- Auto : active l'authentification et l'autorisation basées sur les ports sur le commutateur.

L’interface passe d’un état autorisé à un état non autorisé en fonction de l’échange d’authentification entre le commutateur et le client.
- Force Authorized : autorise l'interface sans authentification.

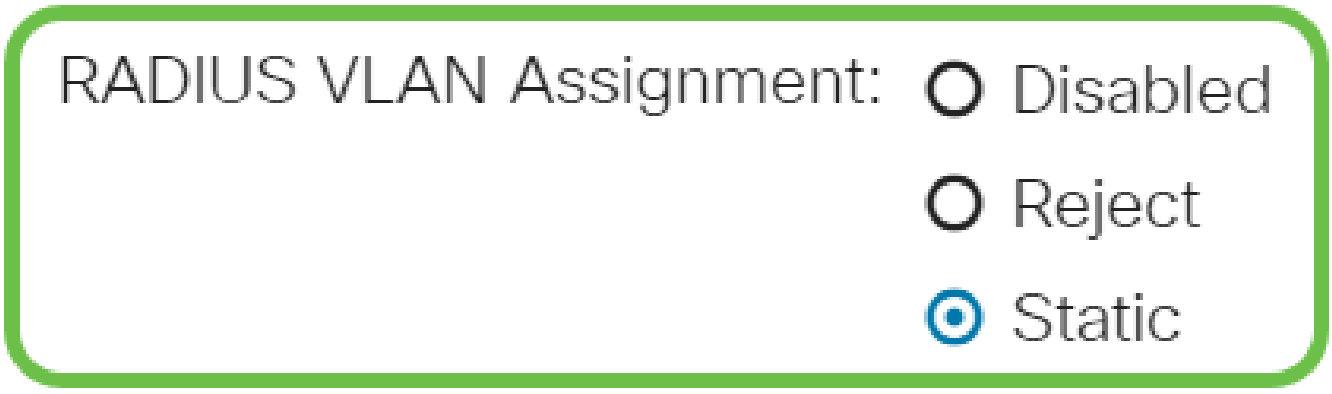


Étape 5 (facultative)

Sélectionnez une case d'option pour l'affectation de VLAN RADIUS. Cela active l'affectation de VLAN dynamique sur le port spécifié. Les options sont les suivantes :

- Disabled : ignore le résultat de l'autorisation VLAN et conserve le VLAN d'origine de l'hôte. Il s'agit de l'action par défaut.
- Reject : si le port spécifié reçoit des informations VLAN autorisées, il les utilise. Cependant, s'il n'y a aucune information autorisée VLAN, il rejette l'hôte et le rend non autorisé.
- Static : si le port spécifié reçoit des informations autorisées VLAN, il les utilise. Cependant, s'il n'y a pas d'informations autorisées VLAN, il conserve le VLAN d'origine de l'hôte.

S'il existe des informations autorisées VLAN provenant de RADIUS, mais que le VLAN n'est pas créé administrativement sur le périphérique testé (DUT), le VLAN est créé automatiquement.



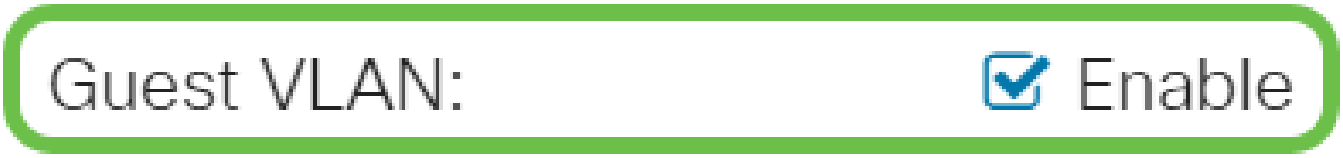
Conseil rapide : pour que la fonction Dynamic VLAN Assignment fonctionne, le commutateur

nécessite que les attributs VLAN suivants soient envoyés par le serveur RADIUS :

- [64] Tunnel-Type = VLAN (type 13)
- [65] Tunnel-Medium-Type = 802 (type 6)
- [81] ID de groupe privé de tunnel = ID de VLAN

Étape 6 (facultative)

Cochez la case Enable pour que le VLAN invité utilise un VLAN invité pour les ports non autorisés.



Étape 7

Cochez la case Enable pour Periodic Reauthentication. Cette opération active les tentatives de réauthentification de port après la période de réauthentification spécifiée.



Étape 8

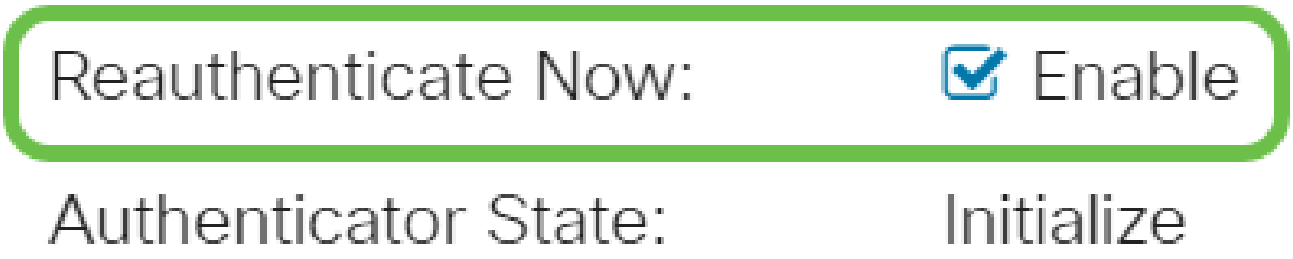
Saisissez une valeur dans le champ Période de réauthentification. Il s'agit du temps en secondes nécessaire pour réauthentifier le port.



Étape 9 (facultative)

Cochez la case Reauthenticate Now pour activer la réauthentification immédiate des ports.

Le champ Authenticator State affiche l'état actuel de l'authentification.



Si le port n'est pas à l'état Forcer l'autorisation ou Forcer l'état Non autorisé, il est en mode Auto et l'authentificateur affiche l'état de l'authentification en cours. Une fois le port authentifié, l'état est affiché comme Authenticated.

Étape 10

Dans le champ Max Hosts, saisissez le nombre maximal d'hôtes authentifiés autorisés sur le port spécifique. Cette valeur prend effet uniquement en mode multisession.



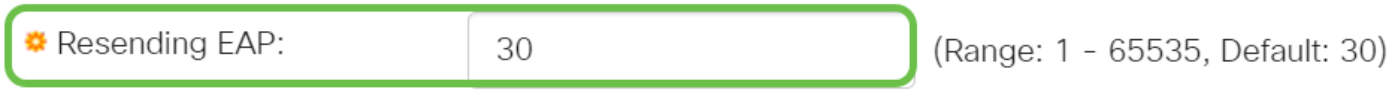
Étape 11

Dans le champ Quiet Period, saisissez le nombre de secondes pendant lesquelles le commutateur reste dans l'état silencieux après un échec de l'échange d'authentification. Lorsque le commutateur est dans un état silencieux, cela signifie qu'il n'écoute pas les nouvelles demandes d'authentification du client.



Étape 12

Dans le champ Resending EAP, entrez le nombre de secondes pendant lequel le commutateur attend une réponse à une demande ou trame d'identité EAP (Extensible Authentication Protocol) du demandeur (client) avant de renvoyer la demande.



Étape 13

Dans le champ Max EAP Requests, saisissez le nombre maximal de demandes EAP qui peuvent

être envoyées. Si aucune réponse n'est reçue après la période définie (délai d'attente du demandeur), le processus d'authentification est redémarré.



Étape 14

Dans le champ Expiration du demandeur, entrez le nombre de secondes qui s'écoulent avant que les demandes EAP soient renvoyées au demandeur.



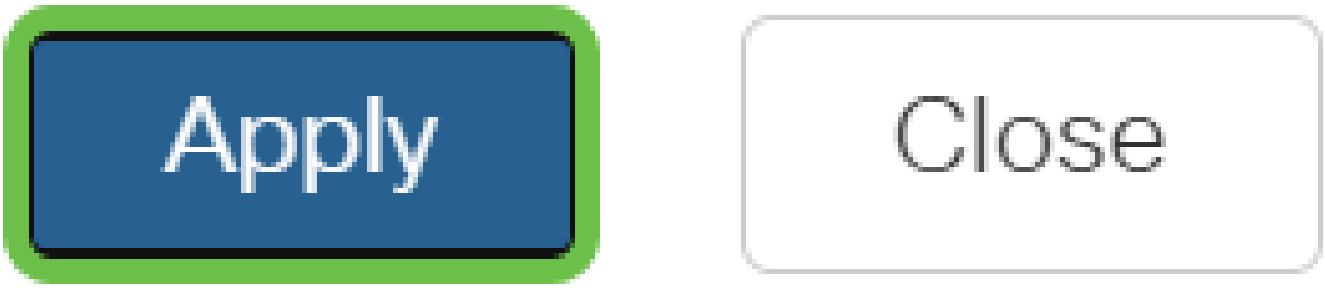
Étape 15

Dans le champ Server Timeout, entrez le nombre de secondes qui s'écoulent avant que le commutateur ne renvoie une requête au serveur d'authentification.



Étape 16

Cliquez sur Apply.



Vous devez maintenant avoir correctement configuré l'authentification 802.1x sur votre commutateur.

Pour plus de configurations, référez-vous au Guide d'administration des commutateurs Cisco Business 220.

Si vous souhaitez consulter d'autres articles, consultez la page d'assistance des commutateurs

Cisco Business 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.