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

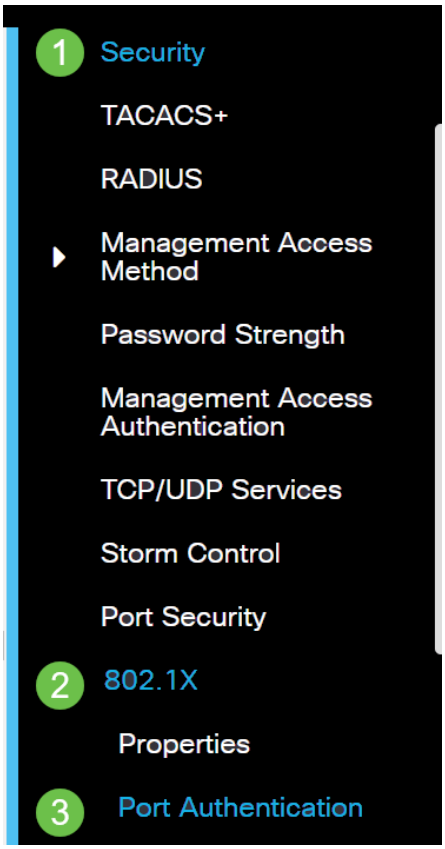
L'authentification de port active la configuration des paramètres pour chaque port. Étant donné que certaines modifications de configuration ne sont possibles que lorsque le port est dans un état Forcer autorisé, tel que l'authentification de l'hôte, il est recommandé de modifier le contrôle de port en Forcer autorisé avant d'apporter 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 Port Security ne peuvent pas être activés simultanément sur le même port. Si vous activez la sécurité des ports sur une interface, le contrôle des ports d'administration ne peut pas être modifié en mode Auto.

Configurer l'authentification des ports

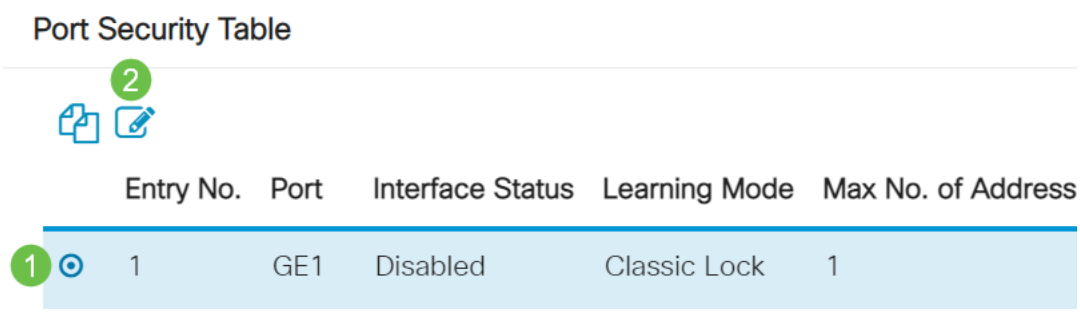
Étape 1

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



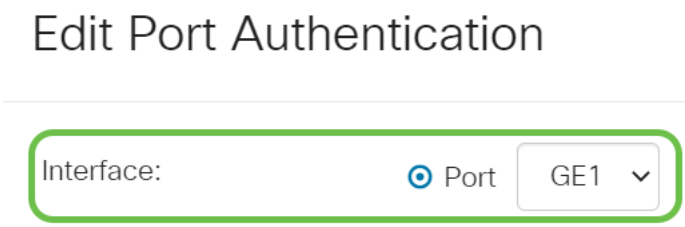
Étape 2

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



Étape 3

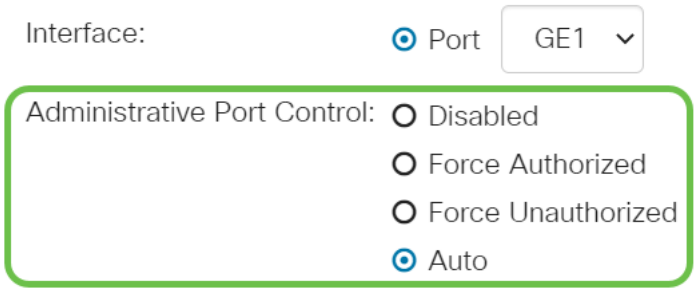
La fenêtre *Edit Port Authentication* s'affiche. Dans la liste déroulante Interface, vérifiez que le port spécifié est celui que vous avez choisi à l'étape 2. Sinon, cliquez sur la flèche de la liste déroulante et sélectionnez le port de droite.



Étape 4

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

- **Disabled** : désactive 802.1x. Il s'agit de l'état par défaut.
- **Forcer Unallowed** : refuse l'accès à l'interface en déplaçant 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 se déplace entre un état autorisé ou non autorisé en fonction de l'échange d'authentification entre le commutateur et le client.
- **Forcer Autorisé** — Autorise l'interface sans authentification.

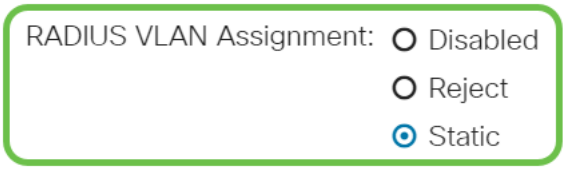


Étape 5 (facultative)

Sélectionnez une case d'option pour l'affectation de VLAN RADIUS. Ceci 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.
- **Rejeter** - Si le port spécifié reçoit des informations VLAN autorisées, il les utilisera. Cependant, s'il n'y a aucune information autorisée par VLAN, il rejettera l'hôte et le rendra non autorisé.
- **Static** : si le port spécifié reçoit des informations VLAN autorisées, il les utilise. Cependant, s'il n'y a aucune information autorisée par le VLAN, il conserve le VLAN d'origine de l'hôte.

S'il existe des informations VLAN autorisées à partir de RADIUS, mais que le VLAN n'est pas créé administrativement sur le périphérique en cours de test (DUT), le VLAN est créé automatiquement.



Astuce rapide : pour que la fonction d'affectation de VLAN dynamique fonctionne, le commutateur nécessite que les attributs de VLAN suivants soient envoyés par le serveur RADIUS :

- [64] Tunnel-Type = VLAN (type 13)
- [65] Tunnel-Medium-Type = 802 (type 6)
- [81] Tunnel-Private-Group-Id = ID VLAN

Étape 6 (facultative)

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

Étape 7

Cochez la case **Activer** pour l'authentification périodique. Cela permettra d'activer les tentatives de réauthentification des ports après la période de réauthentification spécifiée.

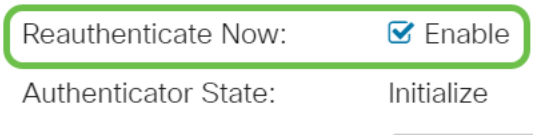
Étape 8

Entrez une valeur dans le champ *Période de réauthentification*. Il s'agit de la durée en secondes pour réauthentifier le port.

Étape 9 (facultative)

Cochez la case **Réauthentifier maintenant** pour activer la réauthentification immédiate du port.

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



Si le port n'est pas en état Autorisé 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 authentifié.

Étape 10

Dans le champ *Nombre maximal d'hôtes*, 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 *Période calme*, saisissez le nombre de secondes pendant lesquelles le commutateur reste à l'état silencieux après un échec de l'échange d'authentification. Lorsque le commutateur est dans un état silencieux, cela signifie que le commutateur n'écoute pas les nouvelles demandes d'authentification du client.

Étape 12

Dans le champ *Renvoyer EAP*, saisissez le nombre de secondes pendant lesquelles le commutateur attend une réponse à une requête ou une trame d'identité EAP (Extensible Authentication Protocol) du demandeur (client) avant de renvoyer la requête.

Étape 13

Dans le champ *Nombre maximal de demandes EAP*, saisissez le nombre maximal de demandes EAP pouvant être envoyées. Si aucune réponse n'est reçue après la période définie (délai d'expiration du demandeur), le processus d'authentification est redémarré.

Étape 14

Dans le champ *Délai d'attente du demandeur*, saisissez le nombre de secondes écoulées avant que les demandes EAP ne soient envoyées au demandeur.

Étape 15

Dans le champ *Délai d'expiration du serveur*, saisissez 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, reportez-vous au Guide d'administration des commutateurs de la gamme Cisco Business 220.

Si vous souhaitez consulter d'autres articles, consultez la page d'assistance pour les commutateurs Cisco Business 220