Configurer l'authentification des ports 802.1X sur les commutateurs intelligents Cisco Sx220

Objectif

L'objectif de cet article est de vous montrer comment configurer l'authentification des ports sur les commutateurs intelligents de la gamme Sx220.

L'authentification de port 802.1X active la configuration des paramètres 802.1X pour chaque port de votre périphérique. Un port qui demande l'authentification est appelé demandeur. L'authentificateur est un commutateur ou un point d'accès qui agit comme un dispositif de protection du réseau pour les supplicants. L'authentificateur transmet les messages d'authentification au serveur RADIUS afin qu'un port puisse être authentifié et puisse envoyer et recevoir des informations.

Périphériques pertinents

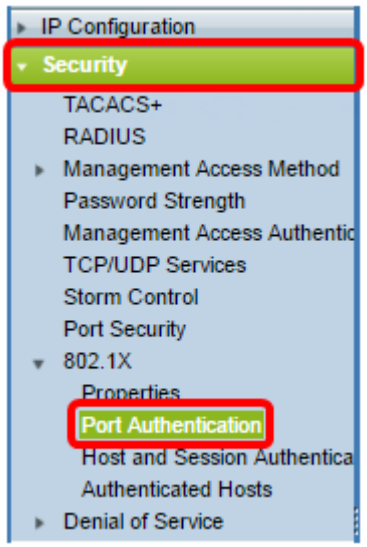
- Série Sx220

Version du logiciel

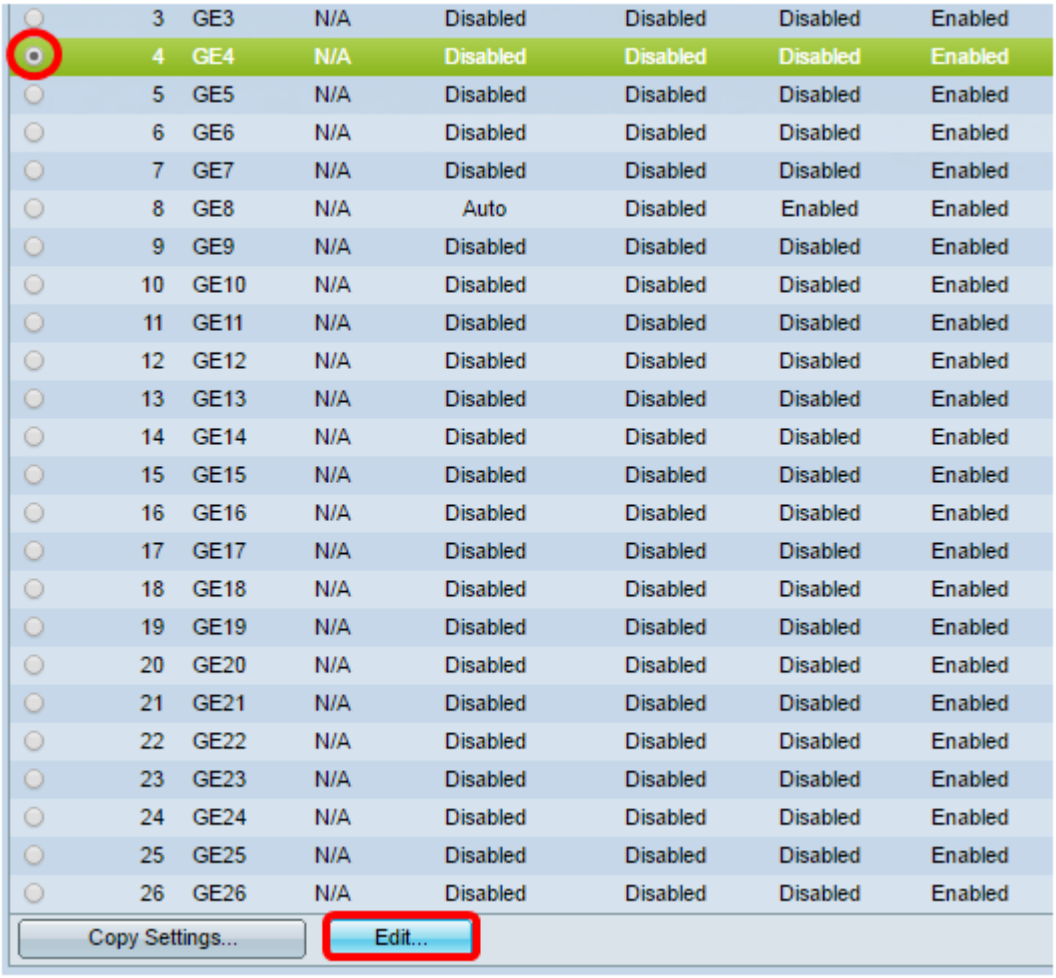
- 1.1.0.14

Configurer l'authentification des ports

Étape 1. Connectez-vous à l'utilitaire 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 **Modifier**.

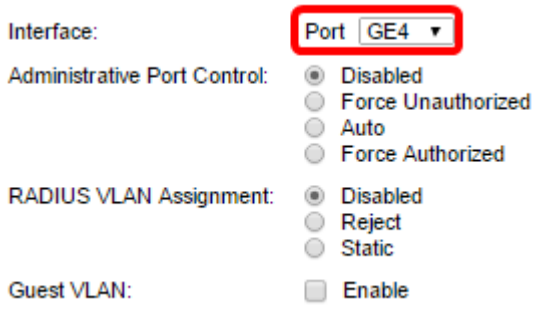


○	3	GE3	N/A	Disabled	Disabled	Disabled	Enabled
◉	4	GE4	N/A	Disabled	Disabled	Disabled	Enabled
○	5	GE5	N/A	Disabled	Disabled	Disabled	Enabled
○	6	GE6	N/A	Disabled	Disabled	Disabled	Enabled
○	7	GE7	N/A	Disabled	Disabled	Disabled	Enabled
○	8	GE8	N/A	Auto	Disabled	Enabled	Enabled
○	9	GE9	N/A	Disabled	Disabled	Disabled	Enabled
○	10	GE10	N/A	Disabled	Disabled	Disabled	Enabled
○	11	GE11	N/A	Disabled	Disabled	Disabled	Enabled
○	12	GE12	N/A	Disabled	Disabled	Disabled	Enabled
○	13	GE13	N/A	Disabled	Disabled	Disabled	Enabled
○	14	GE14	N/A	Disabled	Disabled	Disabled	Enabled
○	15	GE15	N/A	Disabled	Disabled	Disabled	Enabled
○	16	GE16	N/A	Disabled	Disabled	Disabled	Enabled
○	17	GE17	N/A	Disabled	Disabled	Disabled	Enabled
○	18	GE18	N/A	Disabled	Disabled	Disabled	Enabled
○	19	GE19	N/A	Disabled	Disabled	Disabled	Enabled
○	20	GE20	N/A	Disabled	Disabled	Disabled	Enabled
○	21	GE21	N/A	Disabled	Disabled	Disabled	Enabled
○	22	GE22	N/A	Disabled	Disabled	Disabled	Enabled
○	23	GE23	N/A	Disabled	Disabled	Disabled	Enabled
○	24	GE24	N/A	Disabled	Disabled	Disabled	Enabled
○	25	GE25	N/A	Disabled	Disabled	Disabled	Enabled
○	26	GE26	N/A	Disabled	Disabled	Disabled	Enabled

Copy Settings... Edit...

Note: Dans cet exemple, le port GE4 est choisi.

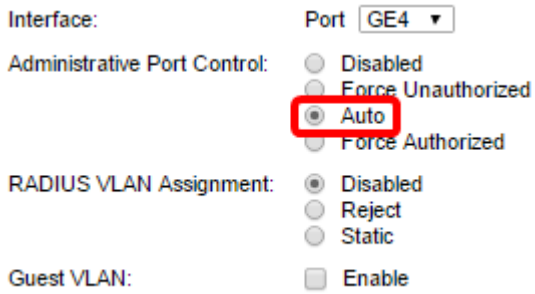
Étape 3. La fenêtre Edit Port Authentication s'affiche. Dans la liste déroulante Interface, vérifiez que le port spécifié est celui que vous avez choisi à l'étape 2. Sinon, cliquez sur la flèche de la liste déroulante et sélectionnez le port de droite.



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.
- Force 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.

- Force Authorized : autorise l'interface sans authentification.

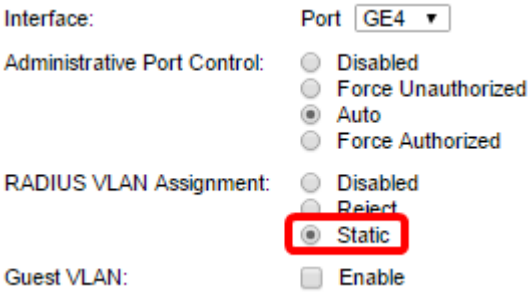


Note: Dans cet exemple, Auto est sélectionné.

Étape 5. (Facultatif) 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.
- Reject : si le port spécifié reçoit des informations VLAN autorisées, il les utilise. 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.

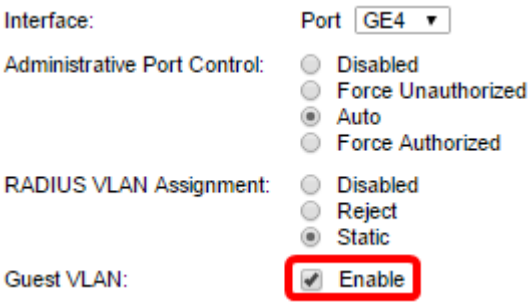
Note: S'il existe une information autorisée de VLAN à partir de RADIUS, mais que le VLAN n'est pas créé administrativement sur le périphérique en cours de test (DUT), le VLAN est créé automatiquement. Dans cet exemple, Static est sélectionné.



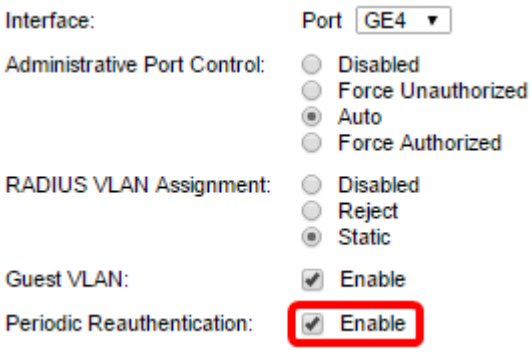
Astuce rapide : Pour que la fonction d'affectation de VLAN dynamique fonctionne, le commutateur nécessite que les attributs de VLAN suivants soient envoyés par le serveur RADIUS :

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

Étape 6. (Facultatif) Cochez la case **Activer** pour que le VLAN invité utilise un VLAN invité pour les ports non autorisés.

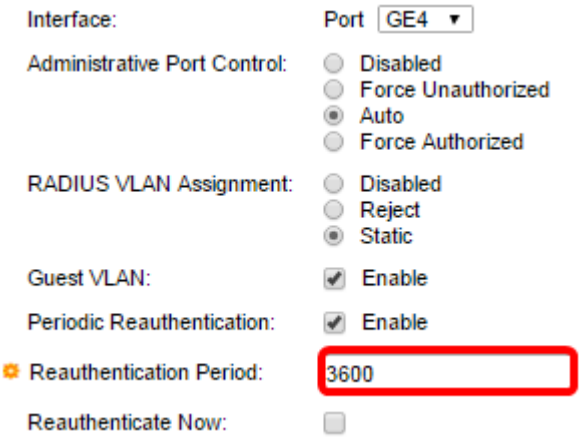


Étape 7. Cochez la case **Activer** pour l'authentification périodique. Cela permettra d'activer les tentatives de réauthentification des ports après la période de réauthentification spécifiée.



Note: Cette fonction est activée par défaut.

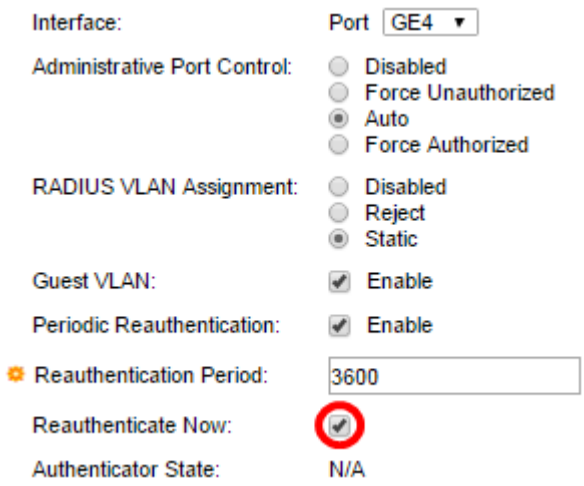
Étape 8. Entrez une valeur dans le champ *Période de réauthentification*. Il s'agit de la durée en secondes pour réauthentifier le port.



Note: Dans cet exemple, la valeur par défaut 3600 est utilisée.

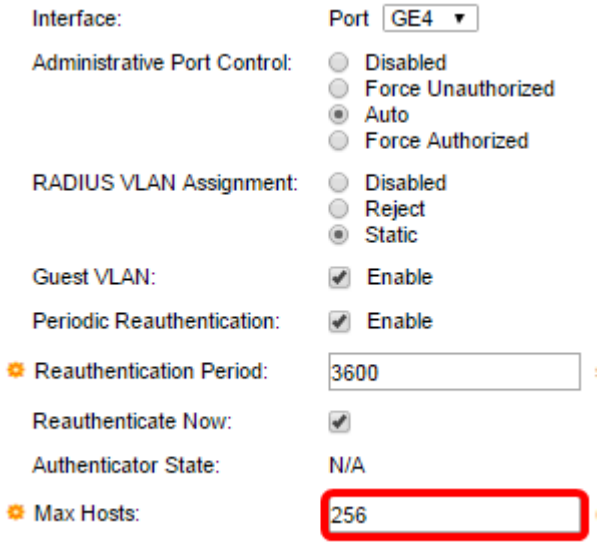
Étape 9. (Facultatif) Cochez la case **Réauthentifier maintenant** pour activer la réauthentification immédiate du port.

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



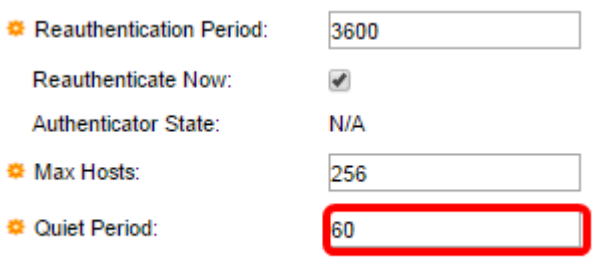
Note: Si le port n'est pas en état Autorisé ou Forcer l'état Non autorisé, il est en mode Auto et l'authentificateur affiche l'état de l'authentification en cours. Une fois le port authentifié, l'état est authentifié.

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 multisessions.



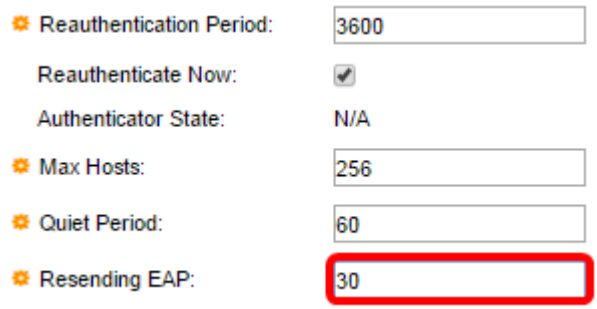
Note: Dans cet exemple, la valeur par défaut 256 est utilisée.

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.



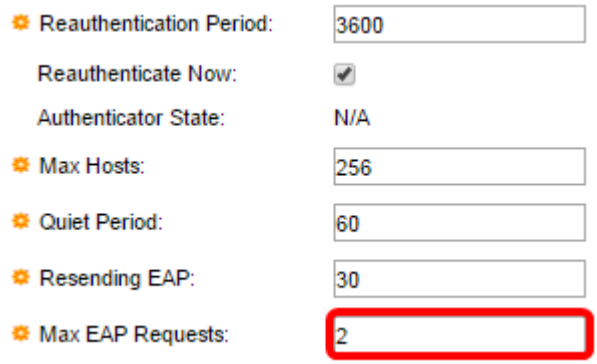
Note: Dans cet exemple, la valeur par défaut 60 est utilisée.

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.



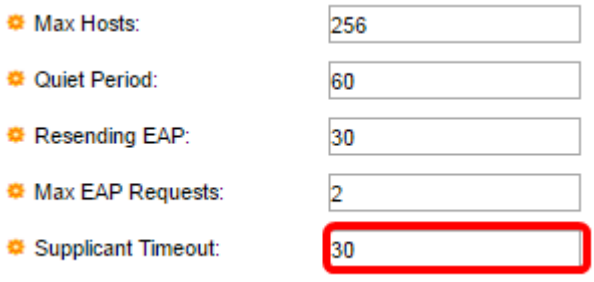
Note: Dans cet exemple, la valeur par défaut 30 est utilisée.

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.



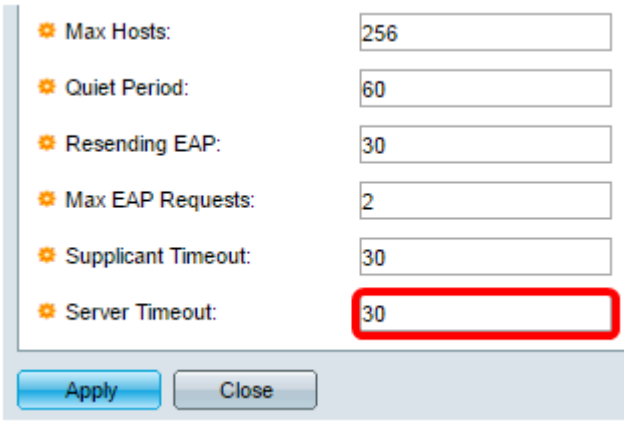
Note: Dans cet exemple, la valeur par défaut 2 est utilisée.

Étape 14. Dans le champ *Délai d'attente du demandeur*, saisissez le nombre de secondes qui s'écoulent avant que les demandes EAP ne soient envoyées au demandeur.



Note: Dans cet exemple, la valeur par défaut 30 est utilisée.

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.



Note: Dans cet exemple, la valeur par défaut 30 est utilisée.

Étape 16. Cliquez sur Apply.

Vous devez maintenant avoir correctement configuré l'authentification de port sur votre commutateur.