Configurez l'authentification de port de 802.1X sur les Commutateurs intelligents de gamme Cisco Sx220

Objectif

L'objectif de cet article est de t'afficher comment configurer l'authentification de port sur les Commutateurs intelligents de gamme Sx220.

l'authentification de port de 802.1X active la configuration des paramètres de 802.1X pour chaque port sur votre périphérique. Un port qui demande l'authentification s'appelle le suppliant. L'authentificateur est un commutateur ou un Point d'accès qui agit en tant que protection de réseau aux suppliants. D'authentificateur les messages d'authentification en avant au serveur de RADIUS de sorte qu'un port puisse être authentifié et puisse envoyer et recevoir les informations.

Périphériques applicables

- Gamme Sx220

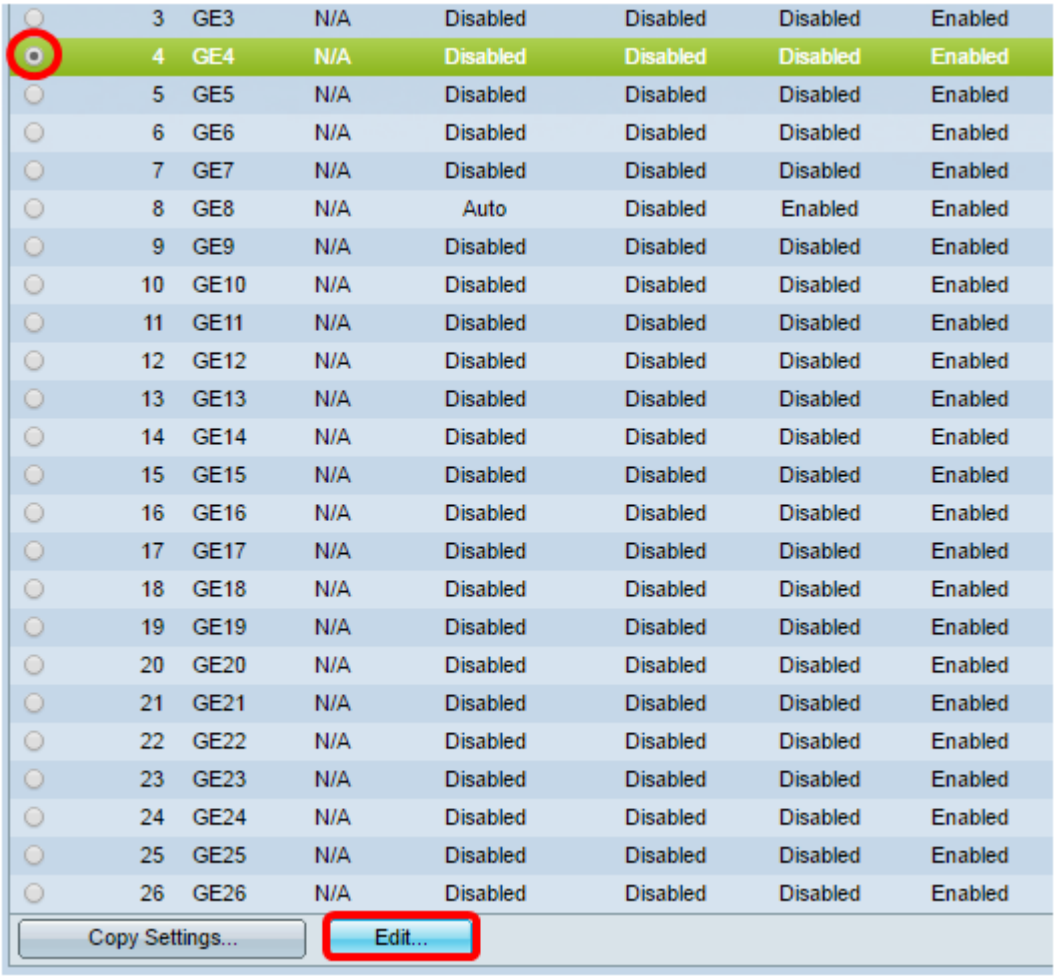
Version de logiciel

- 1.1.0.14

Configurez l'authentification de port

Étape 1. Ouvrez une session à l'utilitaire basé sur le WEB de commutateur et choisissez la **Sécurité > le 802.1X > l'authentification de port**.

Étape 2. Cliquez sur en fonction la case d'option pour le port que vous voulez configurer alors cliquez sur Edit.

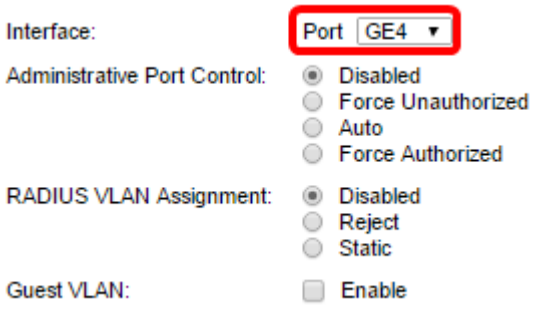


○	3	GE3	N/A	Disabled	Disabled	Disabled	Enabled
◉	4	GE4	N/A	Disabled	Disabled	Disabled	Enabled
○	5	GE5	N/A	Disabled	Disabled	Disabled	Enabled
○	6	GE6	N/A	Disabled	Disabled	Disabled	Enabled
○	7	GE7	N/A	Disabled	Disabled	Disabled	Enabled
○	8	GE8	N/A	Auto	Disabled	Enabled	Enabled
○	9	GE9	N/A	Disabled	Disabled	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...

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

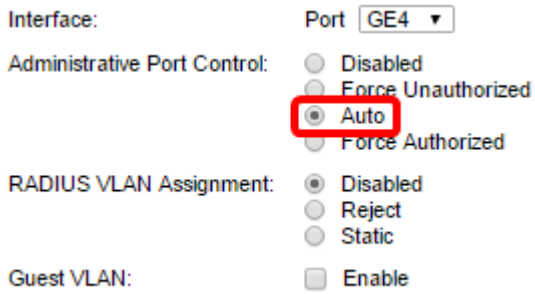
Étape 3. La fenêtre d'authentification de port d'éditer s'affichera alors. De la liste déroulante d'interface, assurez-vous que le port spécifié est celui que vous avez choisi dans l'étape 2. Autrement, cliquez sur la flèche déroulante et choisissez le port droit.



Étape 4. Choisissez une case d'option pour le contrôle administratif de port. Ceci déterminera l'état d'autorisation sur le port. Les options sont :

- Handicapé — Désactive le 802.1X. C'est l'état par défaut.
- Force non autorisée — Refuse l'accès d'interface en entrant l'interface dans l'état non autorisé. Le commutateur ne fournit pas des services d'authentification au client par l'interface.
- Automatique — Authentification et autorisation basées sur port d'enables sur le commutateur. Les mouvements d'interface entre un état autorisé ou non autorisé basé sur l'échange d'authentification entre le commutateur et le client.

- Force autorisée — Autorise l'interface sans authentification.

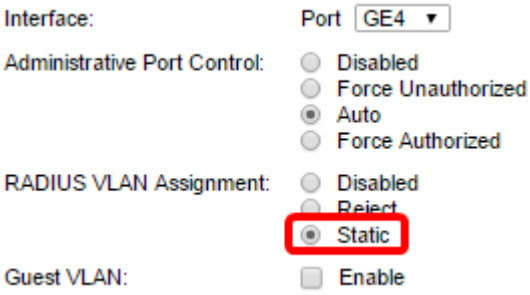


Remarque: Dans cet exemple, l'automatique est choisi.

Étape 5. (facultative) choisissent une case d'option pour l'affectation de RADIUS VLAN. Ceci activera l'affectation dynamique VLAN sur le port spécifié. Les options sont :

- Handicapé — Ignore le résultat d'autorisation VLAN et garde l'original VLAN de l'hôte. C'est l'action par défaut.
- Anomalie — Si le port spécifié reçoit des informations autorisées par VLAN, il utilisera les informations. Cependant, s'il n'y a aucune informations autorisée par VLAN, il rejettera l'hôte et le rendra non autorisé.
- Statique — Si le port spécifié reçoit des informations autorisées par VLAN, il utilisera les informations. Cependant, s'il n'y a aucune informations autorisée par VLAN, il gardera l'original VLAN de l'hôte.

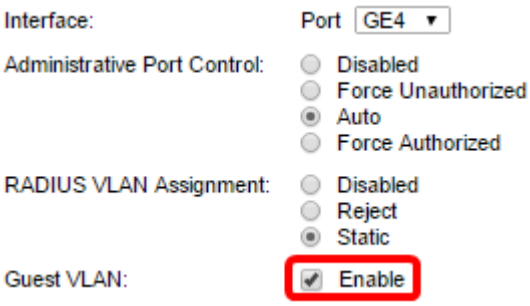
Remarque: S'il y a des informations autorisées par VLAN de RADIUS, mais le VLAN n'est pas administrativement créé sur le périphérique au test (DUT), le VLAN sera créé automatiquement. Dans cet exemple, la charge statique est choisie.



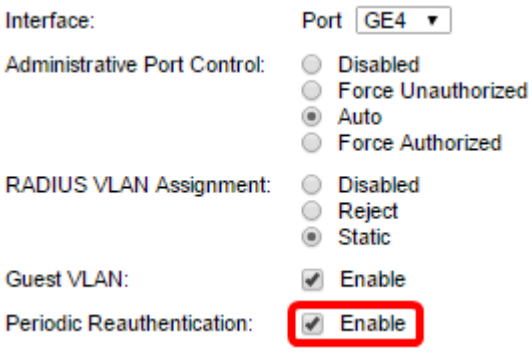
Astuce rapide : Pour que la caractéristique dynamique d'affectation VLAN fonctionne, le commutateur exige des attributs suivants VLAN d'être envoyés par le serveur de RADIUS :

- Tunnel-type [64] = VLAN (type 13)
- Tunnel-Support-type [65] = 802 (type 6)
- Tunnel-Privé-Groupe-id = ID DE VLAN [81]

Contrôle (facultatif) d'étape 6. la case d'**enable** pour l'invité VLAN pour utiliser un VLAN invité pour les ports non autorisés.

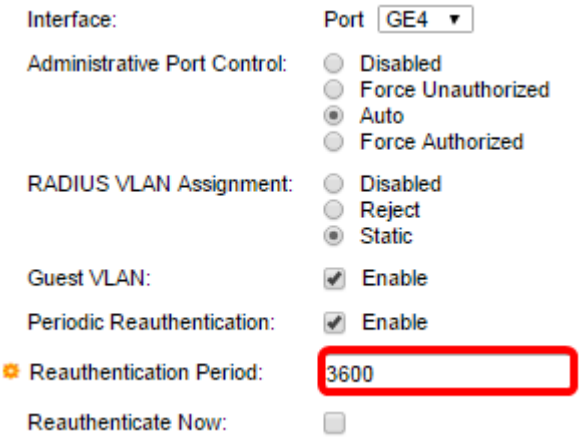


Étape 7. Cochez la case d'**enable** pour la réauthentification périodique. Ceci activera des tentatives de ré-authentification de port après la période spécifiée de réauthentification.



Remarque: Cette caractéristique est activée par défaut.

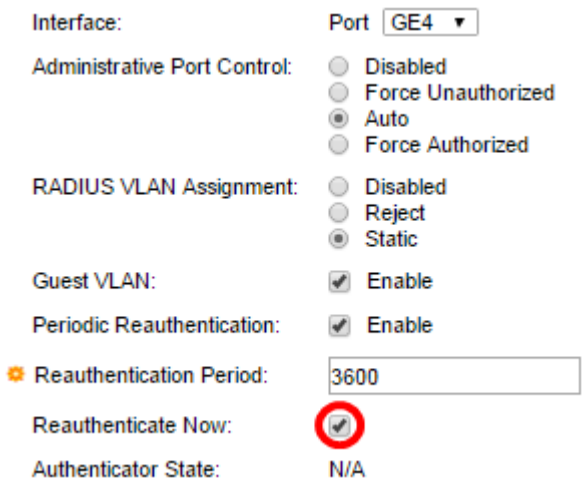
Étape 8. Écrivez une valeur dans le domaine de *période de réauthentification*. C'est l'heure en quelques secondes d'authentifier à nouveau le port.



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

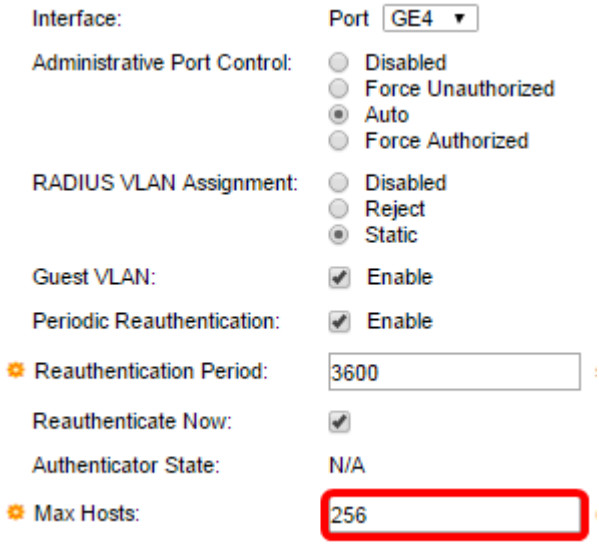
Contrôle (facultatif) d'étape 9. d'**authentifier à nouveau la** case **maintenant** pour activer la ré-authentification immédiate de port.

Remarque: Le champ d'état d'authentificateur affiche l'état actuel de l'authentification.



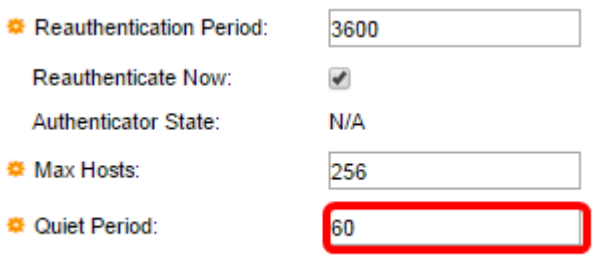
Remarque: Si le port n'est pas en vigueur état non autorisé autorisée ou de force, il est en mode automatique et l'authentificateur affiche l'état de l'authentification en cours. Après que le port soit authentifié, l'état est affiché comme authentifié.

Étape 10. Dans les *hôtes maximum* mettez en place, écrivez le nombre maximal d'hôtes authentifiés permis sur le port spécifique. Cette valeur la prend effet seulement sur le mode de multi-sessions.



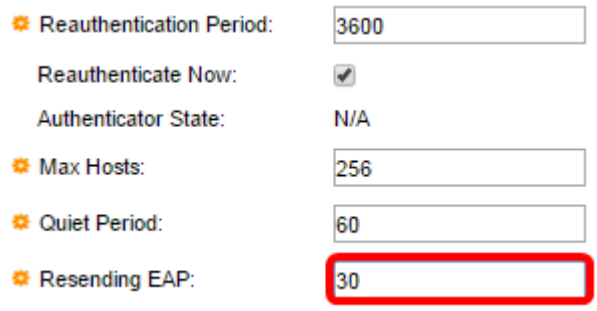
Remarque: Dans cet exemple, la valeur par défaut 256 est utilisée.

Étape 11. Dans le domaine *tranquille de période*, écrivez le nombre de secondes qui le commutateur demeure dans l'état tranquille suivant un échange d'authentification défaillante. Quand le commutateur est dans l'état tranquille, il signifie que le commutateur n'écoute pas de nouvelles demandes d'authentification du client.



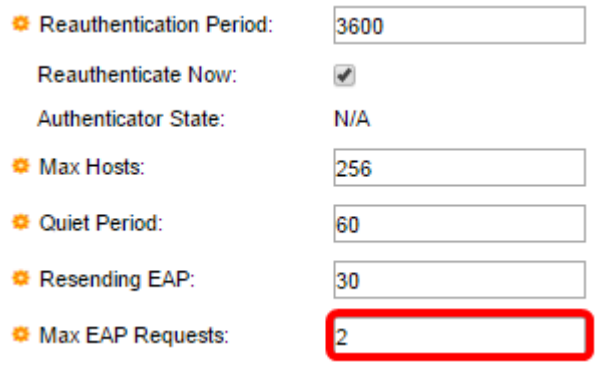
Remarque: Dans cet exemple, la valeur par défaut 60 est utilisée.

Étape 12. Dans le domaine *renvoyant d'EAP*, écrivez le nombre de secondes qui les attentes de commutateur une réponse à une trame de demande ou d'identité de Protocole EAP (Extensible Authentication Protocol) du suppliant (client) avant de renvoyer la demande.



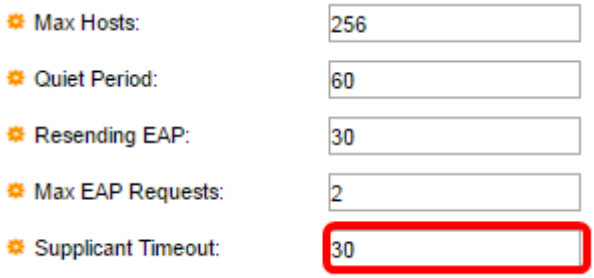
Remarque: Dans cet exemple, la valeur par défaut 30 est utilisée.

Étape 13. Dans l'*EAP maximum les demandes* mettent en place, écrivent le nombre maximal de demandes d'EAP qui peuvent être envoyées. Si une réponse n'est pas reçue après la période définie (délai d'attente de suppliant), la procédure d'authentification est redémarrée.



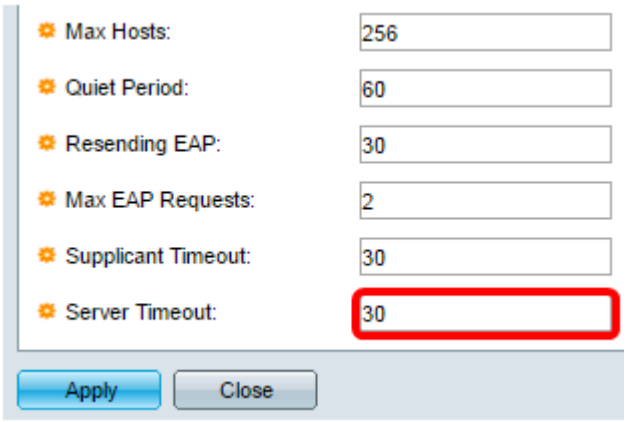
Remarque: Dans cet exemple, la valeur 2 par défaut est utilisée.

Étape 14. Dans le domaine de *délai d'attente de suppliant*, écrivez le nombre de secondes qui passe avant que des demandes d'EAP soient renvoyées au suppliant.



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

Étape 15. Dans le *champ Server Timeout*, écrivez le nombre de secondes qui passe avant que le commutateur renvoie une demande au serveur d'authentification.



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

Étape 16. Cliquez sur **Apply**.

Vous devriez avoir maintenant avec succès configuré l'authentification de port sur votre commutateur.