Configuration du paramètre d'authentification de port 802.1x sur un commutateur

Objectif

IEEE 802.1x est une norme qui facilite le contrôle d'accès entre un client et un serveur. Avant que les services puissent être fournis à un client par un réseau local (LAN) ou un commutateur, le client connecté au port du commutateur doit être authentifié par le serveur d'authentification qui exécute le service d'utilisateur RADIUS (Remote Authentication Dial-In User Service).

L'authentification 802.1x empêche les clients non autorisés de se connecter à un réseau local via des ports accessibles à la publicité. L'authentification 802.1x est un modèle client-serveur. Dans ce modèle, les périphériques réseau ont les rôles spécifiques suivants :

Client ou demandeur : un client ou demandeur est un périphérique réseau qui demande l'accès au réseau local. Le client est connecté à un authentificateur.

Authentificateur : un authentificateur est un périphérique réseau qui fournit des services réseau et auquel les ports du demandeur sont connectés. Les méthodes d'authentification suivantes sont prises en charge :

Basé sur 802.1x — Pris en charge dans tous les modes d'authentification. Dans l'authentification basée sur 802.1x, l'authentificateur extrait les messages EAP (Extensible Authentication Protocol) des messages 802.1x ou des paquets EAPoL (EAPoL) et les transmet au serveur d'authentification, à l'aide du protocole RADIUS.

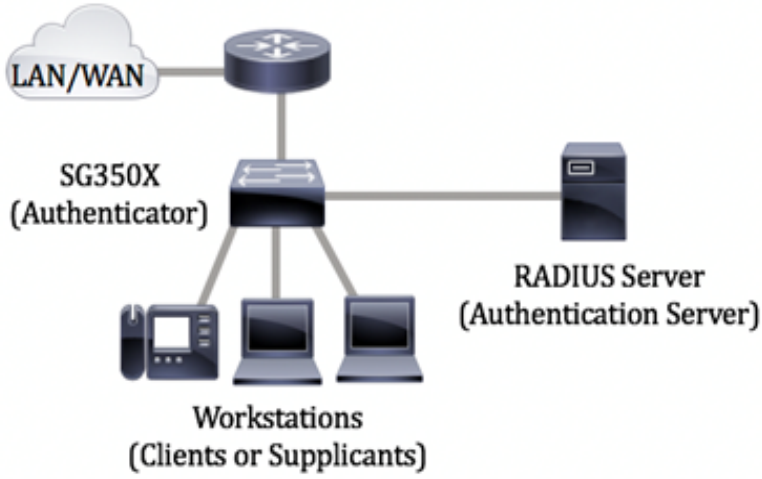
MAC-based : pris en charge dans tous les modes d'authentification. Avec le contrôle d'accès au support (MAC), l'authentificateur exécute lui-même la partie client EAP du logiciel au nom des clients qui cherchent à accéder au réseau.

Web-based : pris en charge uniquement en mode multisessions. Avec l'authentification basée sur le Web, l'authentificateur exécute lui-même la partie client EAP du logiciel au nom des clients qui cherchent à accéder au réseau.

Serveur d'authentification : un serveur d'authentification effectue l'authentification réelle du client. Le serveur d'authentification du périphérique est un serveur d'authentification RADIUS avec des extensions EAP.

Note: Un périphérique réseau peut être un client ou un demandeur, un authentificateur ou les deux par port.

L'image ci-dessous affiche un réseau qui a configuré les périphériques en fonction des rôles spécifiques. Dans cet exemple, un commutateur SG350X est utilisé.



Instructions de configuration de 802.1x :

Créer un réseau d'accès virtuel (VLAN). Pour créer des VLAN à l'aide de l'utilitaire Web de votre commutateur, cliquez ici. Pour obtenir des instructions basées sur l'interface de ligne de commande, cliquez ici.

Configurez les paramètres Port to VLAN sur votre commutateur. Pour configurer à l'aide de l'utilitaire Web, cliquez ici. Pour utiliser l'interface de ligne de commande, cliquez ici.

Configurez les propriétés 802.1x sur le commutateur. 802.1x doit être globalement activé sur le commutateur pour activer l'authentification basée sur les ports 802.1x. Pour des instructions, cliquez ici.

(Facultatif) Configurez la plage de temps sur le commutateur. Pour savoir comment configurer les paramètres de plage de temps sur votre commutateur, cliquez ici.

Configurez l'authentification de port 802.1x. Cet article explique comment configurer les paramètres d'authentification de port 802.1x sur votre commutateur.

Pour savoir comment configurer l'authentification mac sur un commutateur, cliquez ici.

Périphériques pertinents

Série Sx300

Gamme Sx350

Gamme SG350X

Série Sx500

Gamme Sx550X

Version du logiciel

1.4.7.06 - Sx300, Sx500

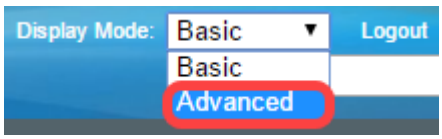
2.2.8.04 - Sx350, SG350X, Sx550X

Configurer les paramètres d'authentification de port 802.1x sur un commutateur

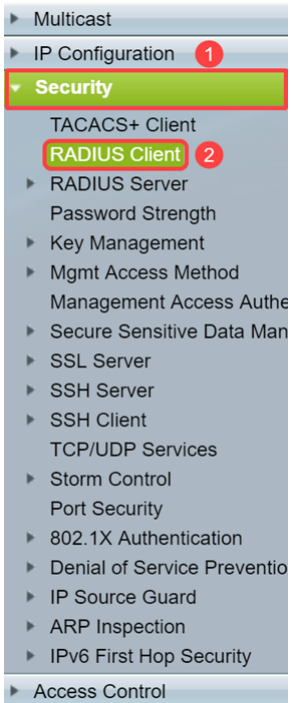
Configuration des paramètres du client RADIUS

Étape 1. Connectez-vous à l'utilitaire Web de votre commutateur, puis sélectionnez **Avancé** dans la liste déroulante Mode d'affichage.

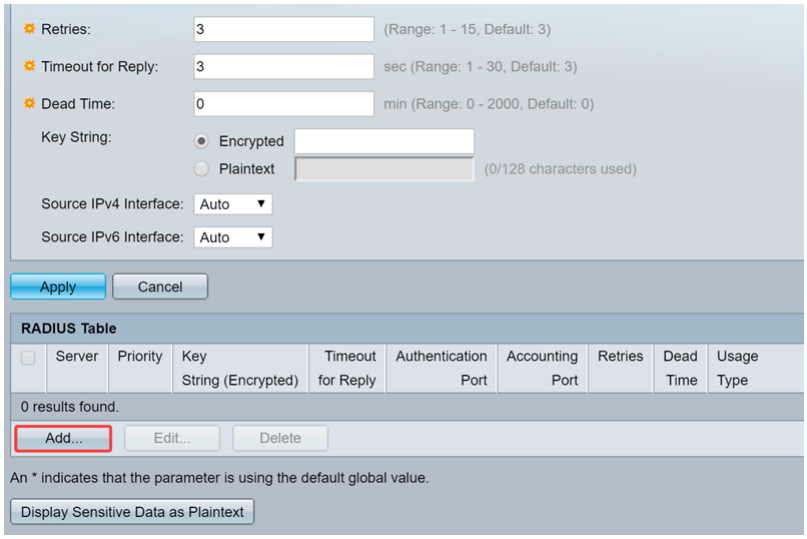
Note: Les options de menu disponibles peuvent varier en fonction du modèle de périphérique. Dans cet exemple, SG550X-24 est utilisé.



Étape 2. Accédez à **Security > RADIUS Client**.

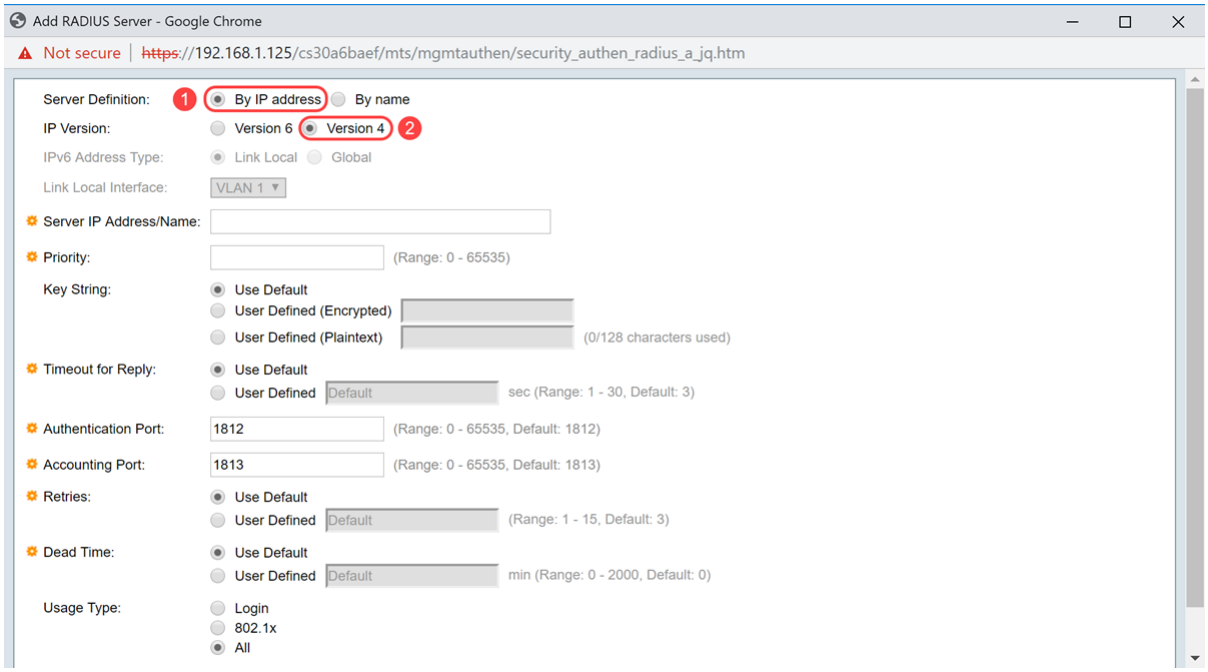


Étape 3. Faites défiler jusqu'à la section *Table RADIUS* et cliquez sur **Ajouter...** pour ajouter un serveur RADIUS.



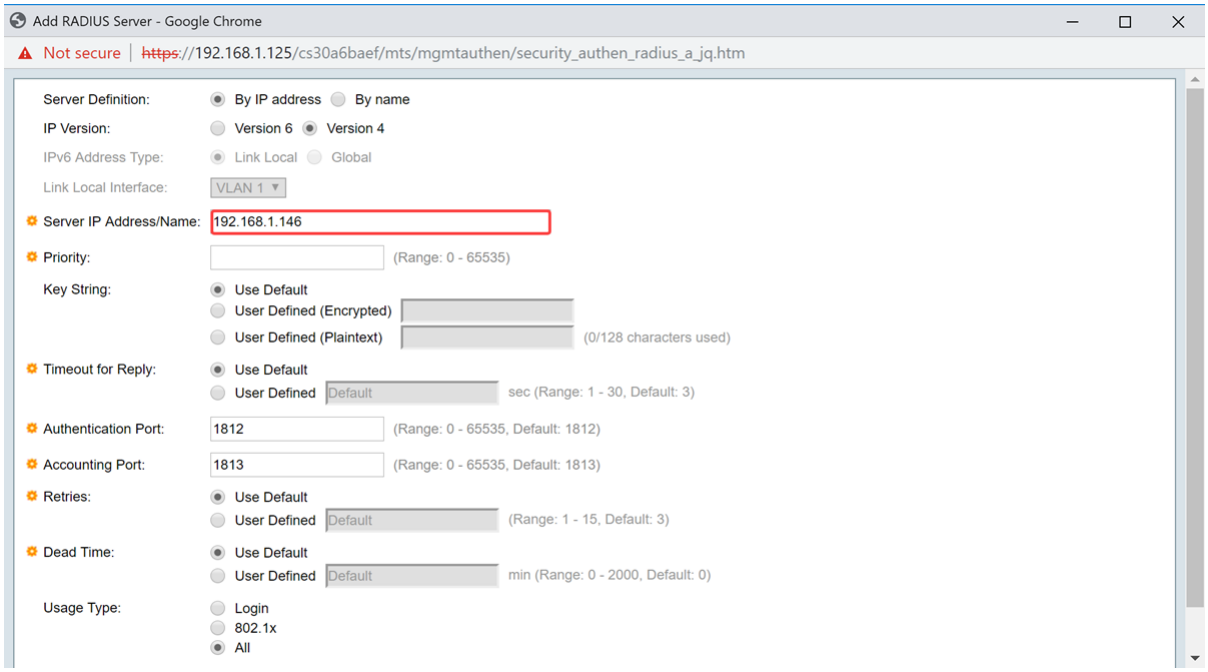
Étape 4. Indiquez si vous voulez spécifier le serveur RADIUS par adresse IP ou par nom dans le champ *Définition du serveur*. Sélectionnez la version de l'adresse IP du serveur RADIUS dans le champ *IP Version*.

Note: Nous allons utiliser **By IP address** et **Version 4** dans cet exemple.

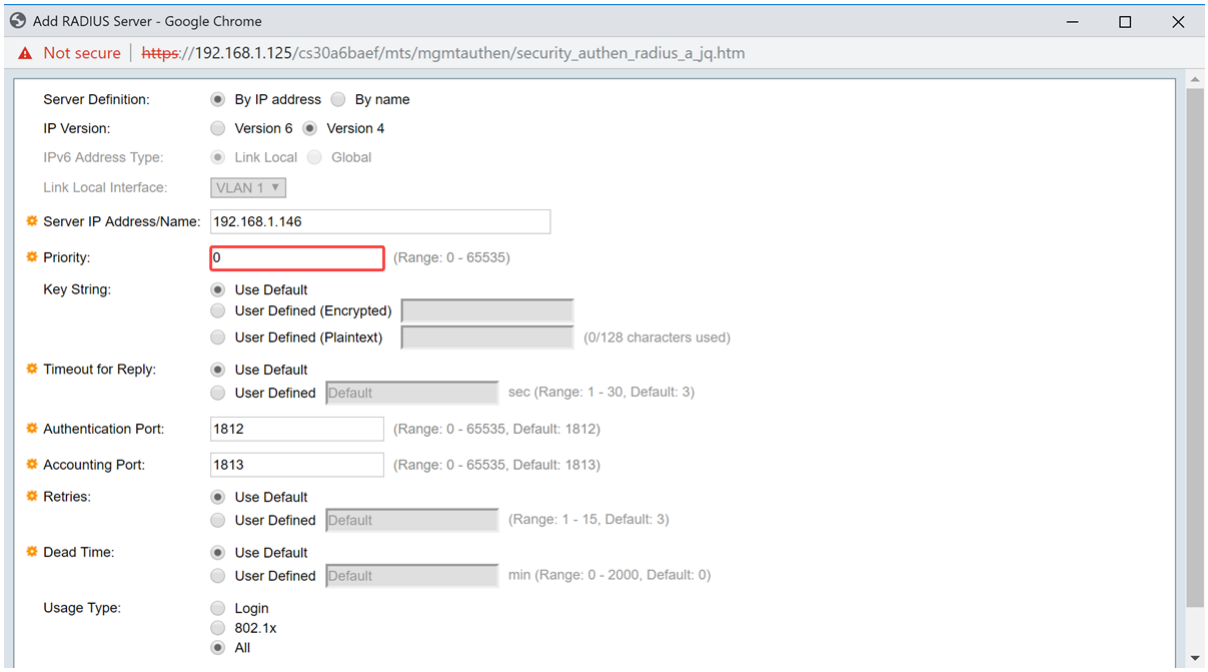


Étape 5. Saisissez l'adresse IP ou le nom du serveur RADIUS.

Note: Nous allons entrer l'adresse IP **192.168.1.146** dans le champ *Adresse IP/Nom du serveur*.



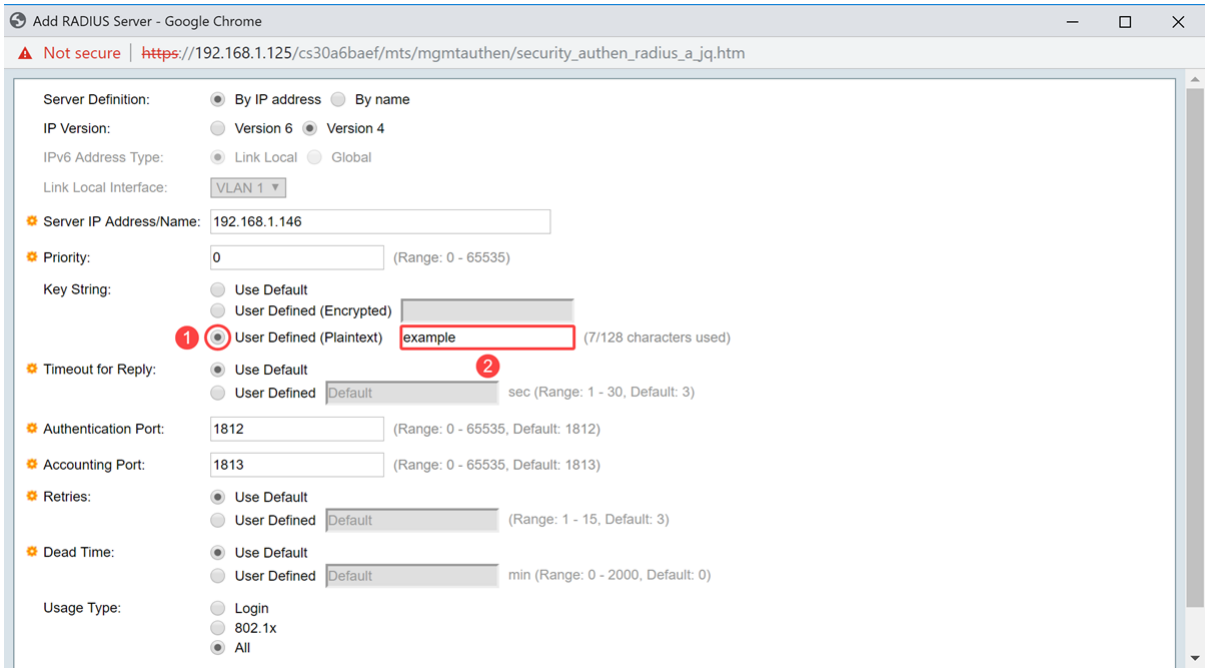
Étape 6. Saisissez la priorité du serveur. La priorité détermine l'ordre dans lequel le périphérique tente de contacter les serveurs pour authentifier un utilisateur. Le périphérique commence par le serveur RADIUS de priorité la plus élevée. 0 est la priorité la plus élevée.



Étape 7. Entrez la chaîne de clé utilisée pour authentifier et chiffrer la communication entre le périphérique et le serveur RADIUS. Cette clé doit correspondre à la clé configurée sur le serveur RADIUS. Il peut être entré au format **Chiffré** ou **Texte clair**. Si **Use Default** est sélectionné, le périphérique tente de s'authentifier auprès du serveur RADIUS à l'aide de la chaîne de clé par défaut.

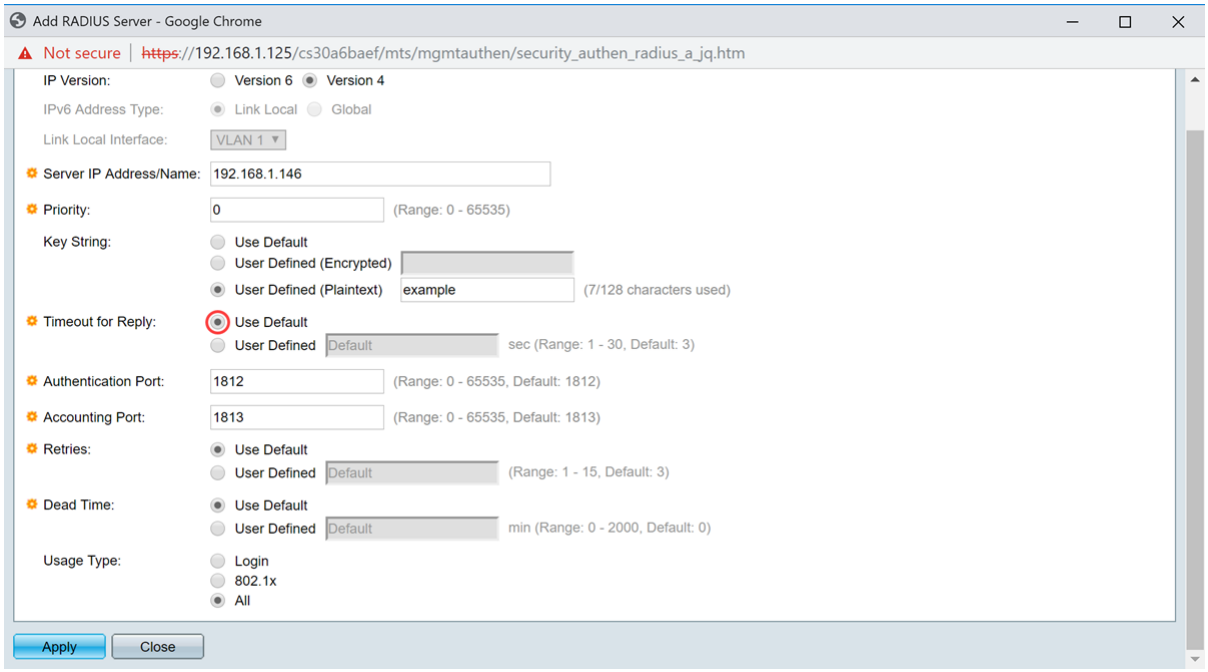
Note: Nous utiliserons le **texte défini par l'utilisateur (texte clair)** et saisirons l'**exemple** clé.

Pour savoir comment configurer les paramètres du serveur RADIUS sur votre commutateur, cliquez ici.



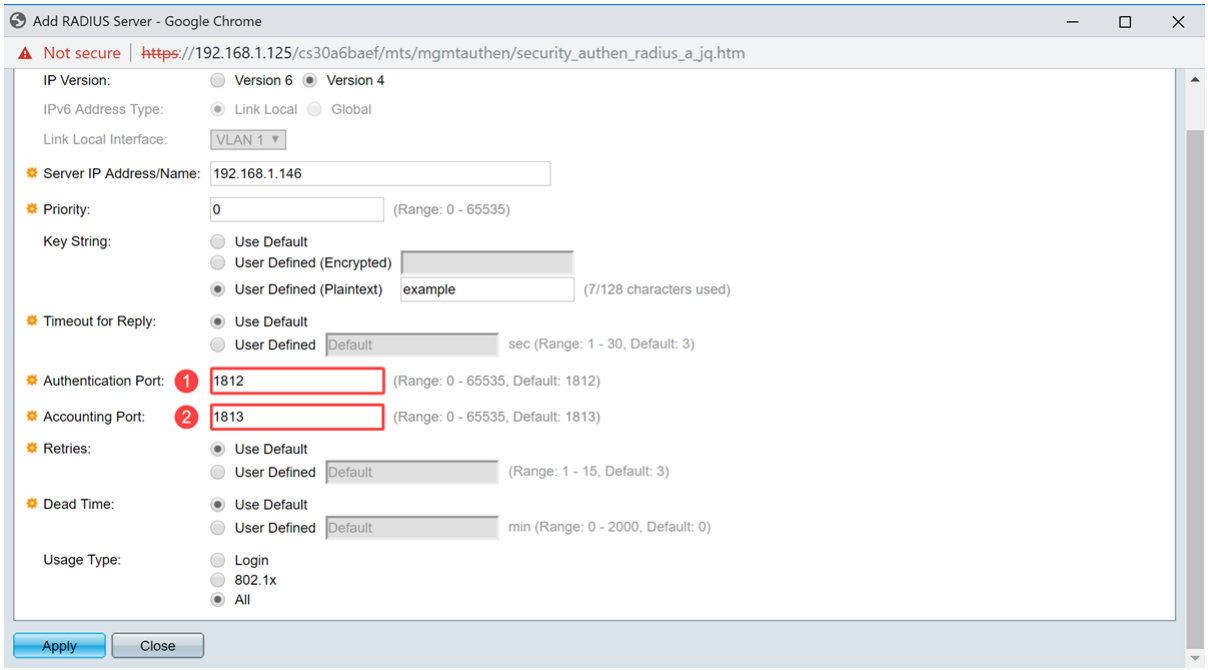
Étape 8. Dans le champ *Expiration de réponse*, sélectionnez **Utiliser par défaut** ou **Défini par l'utilisateur**. Si **Défini par l'utilisateur** a été sélectionné, saisissez le nombre de secondes pendant lesquelles le périphérique attend une réponse du serveur RADIUS avant de réessayer la requête, ou passez au serveur suivant si le nombre maximal de tentatives est atteint. Si **Use Default** est sélectionné, le périphérique utilise la valeur de délai d'attente par défaut.

Note: Dans cet exemple, **Utiliser par défaut** a été sélectionné.



Étape 9. Entrez le numéro de port UDP du port du serveur RADIUS pour la demande d'authentification dans le champ *Port d'authentification*. Entrez le numéro de port UDP du port du serveur RADIUS pour les demandes de comptabilité dans le champ *Port de comptabilité*.

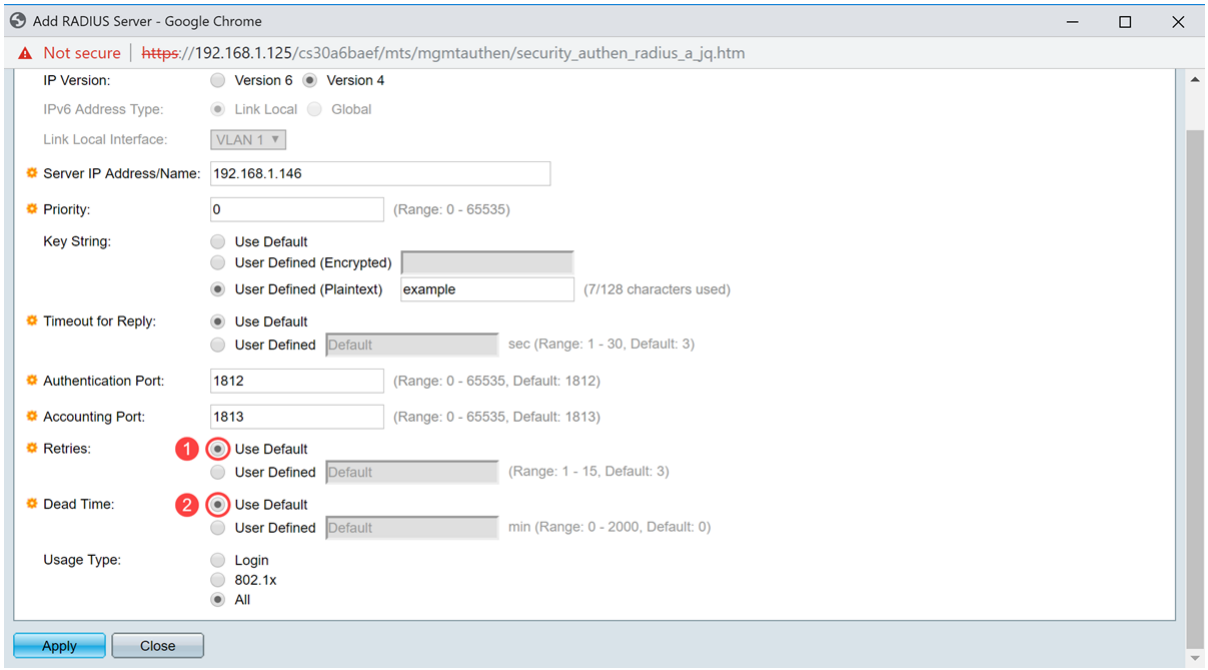
Note: Dans cet exemple, nous utiliserons la valeur par défaut pour le port d'authentification et le port de comptabilité.



Étape 10. Si le champ **Défini par l'utilisateur** est sélectionné pour *les tentatives*, saisissez le nombre de demandes envoyées au serveur RADIUS avant qu'une erreur ne soit considérée comme ayant eu lieu. Si **Use Default** a été sélectionné, le périphérique utilise la valeur par défaut pour le nombre de tentatives.

Si **User Defined** est sélectionné pour *Dead Time*, saisissez le nombre de minutes qui doivent passer avant qu'un serveur RADIUS ne répondant pas ne soit contourné pour les demandes de service. Si **Use Default** a été sélectionné, le périphérique utilise la valeur par défaut pour l'heure d'arrêt. Si vous avez entré 0 minute, il n'y a pas de temps mort.

Note: Dans cet exemple, nous allons sélectionner **Utiliser par défaut** pour ces deux champs.

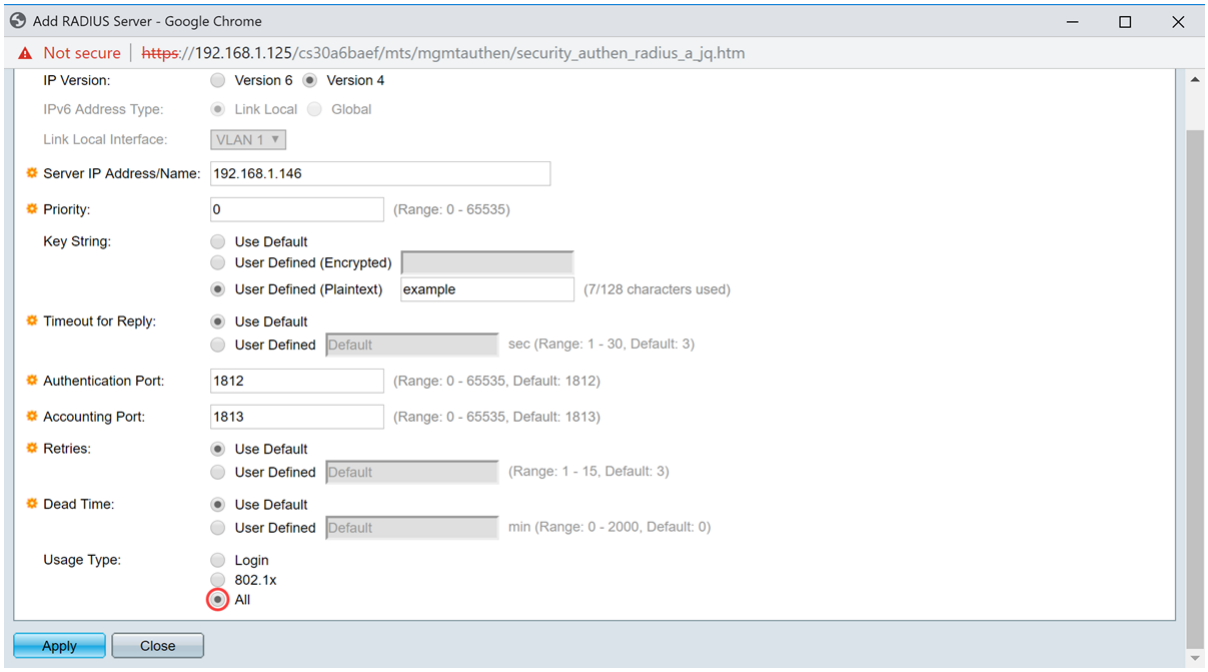


Étape 11. Dans le champ *Type d'utilisation*, saisissez le type d'authentification du serveur RADIUS. Les options sont les suivantes :

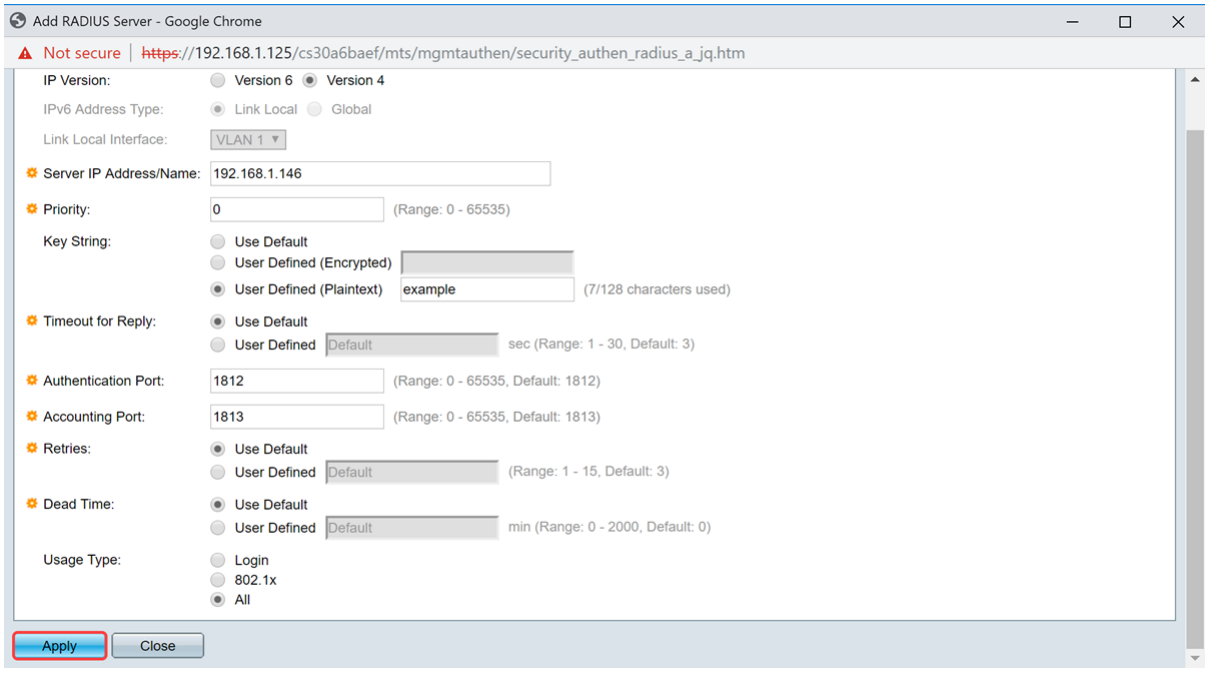
Connexion : le serveur RADIUS est utilisé pour authentifier les utilisateurs qui demandent à administrer le périphérique.

802.1x : serveur RADIUS utilisé pour l'authentification 802.1x.

Tout : le serveur RADIUS est utilisé pour l'authentification des utilisateurs qui demandent à administrer le périphérique et pour l'authentification 802.1x.



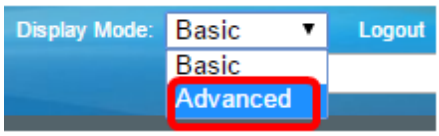
Étape 12. Cliquez sur Apply.



Configuration des paramètres d'authentification de port 802.1x

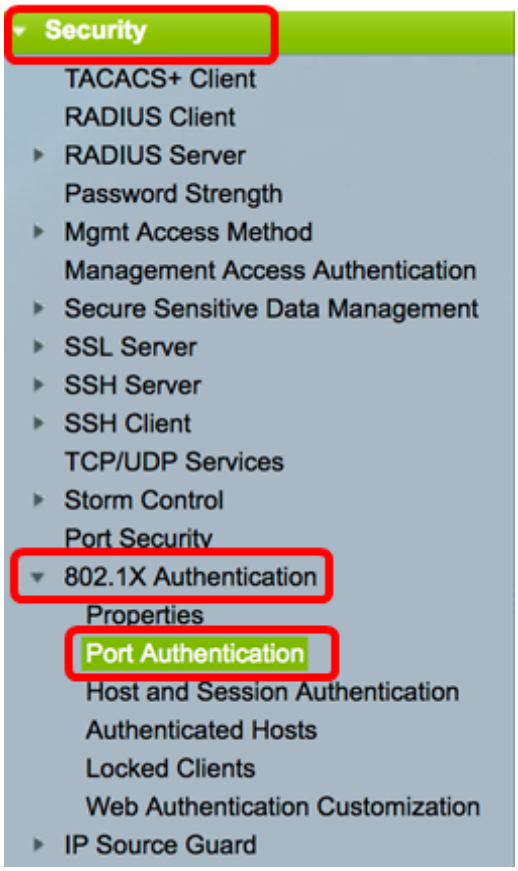
Étape 1. Connectez-vous à l'utilitaire Web de votre commutateur, puis sélectionnez **Avancé** dans la liste déroulante Mode d'affichage.

Note: Les options de menu disponibles peuvent varier en fonction du modèle de périphérique. Dans cet exemple, SG350X-48MP est utilisé.



Note: Si vous disposez d'un commutateur Sx300 ou Sx500, passez à l'étape 2.

Étape 2. Choisissez **Security > 802.1X Authentication > Port Authentication**.

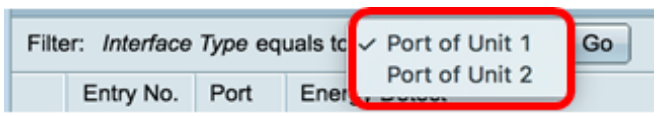


Étape 3. Choisissez une interface dans la liste déroulante *Type d'interface*.

Port : dans la liste déroulante *Type d'interface*, sélectionnez **Port** si un seul port doit être choisi.

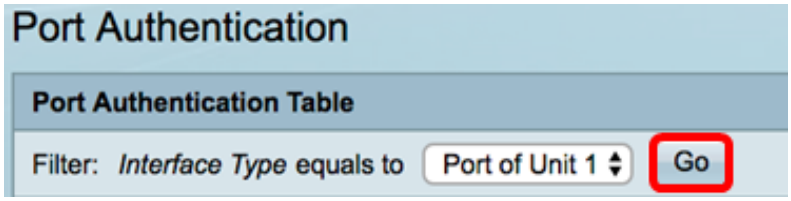
LAG — Dans la liste déroulante *Type d'interface*, sélectionnez le LAG à configurer. Cela affecte le groupe de ports défini dans la configuration LAG.

Note: Dans cet exemple, le port de l'unité 1 est choisi.

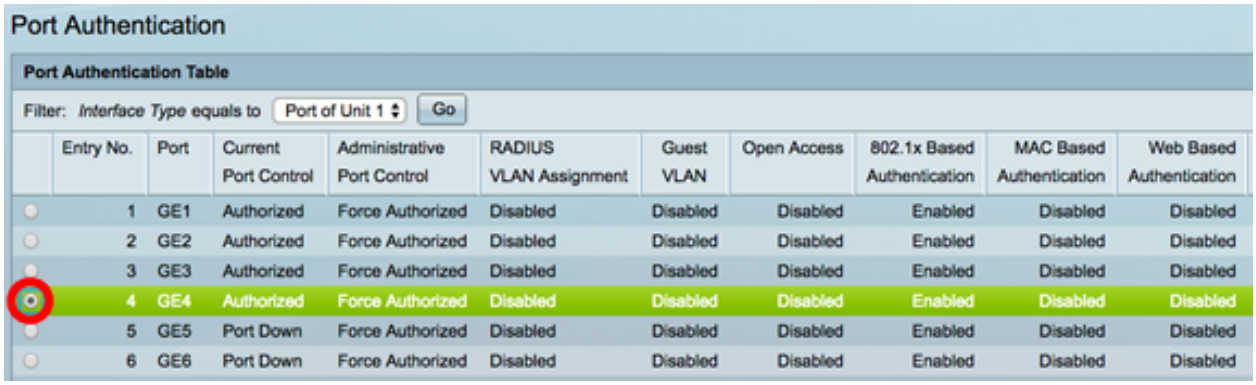


Note: Si vous disposez d'un commutateur non empilable tel qu'un commutateur Sx300, passez à l'étape 5.

Étape 4. Cliquez sur **Aller** pour afficher une liste de ports ou de LAG sur l'interface.



Étape 5. Cliquez sur le port à configurer.



Note: Dans cet exemple, GE4 est sélectionné.

Étape 6. Faites défiler la page vers le bas, puis cliquez sur **Modifier**.

Étape 7. (Facultatif) Si vous souhaitez modifier une autre interface, choisissez dans les listes déroulantes Unité et Port.

Note: Dans cet exemple, le port GE4 de l'unité 1 est choisi.

Étape 8. Sélectionnez la case d'option correspondant au contrôle de port souhaité dans la zone Administrative Port Control. Les options sont les suivantes :

Force Unallowed : refuse l'accès à l'interface en déplaçant le port dans l'état non autorisé. Le port abandonne le trafic.

Auto : le port se déplace entre un état autorisé ou non autorisé en fonction de l'authentification du demandeur.

Force Authorized : autorise le port sans authentification. Le port transfère le trafic.

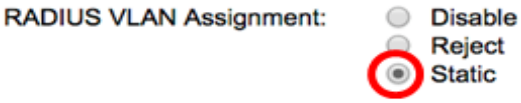
Note: Dans cet exemple, Auto est sélectionné.

Étape 9. Cliquez sur la case d'option Affectation de VLAN RADIUS pour configurer l'affectation de VLAN dynamique sur le port sélectionné. Les options sont les suivantes :

Disable : la fonction n'est pas activée.

Rejeter — Si le serveur RADIUS a autorisé le demandeur, mais n'a pas fourni de VLAN de demandeur, le demandeur est rejeté.

Static : si le serveur RADIUS a autorisé le demandeur, mais n'a pas fourni de VLAN de demandeur, le demandeur est accepté.



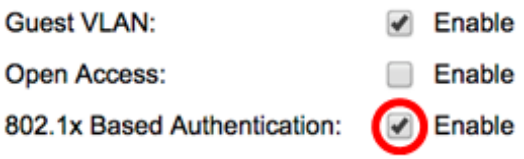
Note: Dans cet exemple, Static est sélectionné.

Étape 10. Cochez la case **Activer** dans le VLAN invité pour activer le VLAN invité pour les ports non autorisés. Le VLAN invité fait en sorte que le port non autorisé se connecte automatiquement au VLAN choisi dans la zone ID de VLAN invité des propriétés 802.1.

Étape 11. (Facultatif) Cochez la case **Activer l'**accès ouvert pour activer l'accès libre. Open Access vous aide à comprendre les problèmes de configuration des hôtes se connectant au réseau, à surveiller les mauvaises situations et à résoudre ces problèmes.

Note: Lorsque l'accès ouvert est activé sur une interface, le commutateur traite toutes les défaillances reçues d'un serveur RADIUS comme des réussites et autorise l'accès au réseau pour les stations connectées aux interfaces, quels que soient les résultats de l'authentification. Dans cet exemple, Open Access est désactivé.

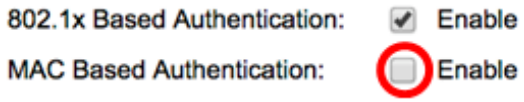
Étape 12. Cochez la case **Activer l'**authentification basée sur 802.1x pour activer l'authentification 802.1X sur le port.



Étape 13. Cochez la case **Enable** MAC Based Authentication pour activer l'authentification de port en fonction de l'adresse MAC du demandeur. Seules huit authentifications MAC

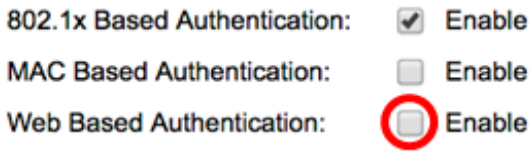
peuvent être utilisées sur le port.

Note: Pour que l'authentification MAC réussisse, le nom d'utilisateur et le mot de passe du demandeur du serveur RADIUS doivent être l'adresse MAC du demandeur. L'adresse MAC doit être en minuscules et saisie sans le . ou - séparateurs (tels que 0020aa00bbcc).



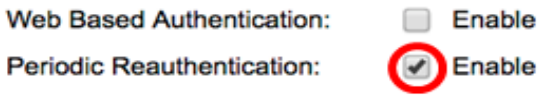
Note: Dans cet exemple, l'authentification basée sur MAC est désactivée.

Étape 14. Cochez la case **Activer** l'authentification Web pour activer l'authentification Web sur le commutateur. Dans cet exemple, l'authentification Web est désactivée.



Note: Dans cet exemple, l'authentification Web est désactivée.

Étape 15. (Facultatif) Cochez la case **Activer la** réauthentification périodique pour forcer le port à se réauthentifier après un certain temps. Cette heure est définie dans le champ *Période de réauthentification*.



Note: Dans cet exemple, la réauthentification de période est activée.

Étape 16. (Facultatif) Entrez une valeur dans le champ *Période de réauthentification*. Cette valeur représente la durée en secondes avant que l'interface ne réauthentifie le port. La valeur par défaut est 3600 secondes et la plage est comprise entre 300 et 4294967295 secondes.

Note: Dans cet exemple, 6 000 secondes sont configurées.

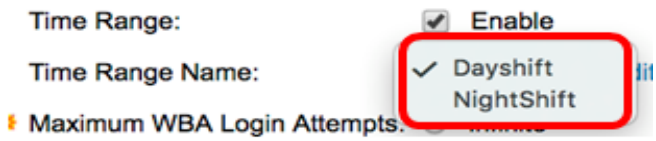
Étape 17. (Facultatif) Cochez la case **Activer** la nouvelle authentification maintenant pour forcer une réauthentification immédiate du port. Dans cet exemple, la réauthentification immédiate est désactivée.

La zone Authenticator State affiche l'état d'autorisation du port.

Étape 18. (Facultatif) Cochez la case **Activer la** plage de temps pour activer une limite sur la durée d'autorisation du port.

Note: Dans cet exemple, la plage de temps est activée. Si vous préférez ignorer cette fonction, passez à l'étape 20.

Étape 19. (Facultatif) Dans la liste déroulante Nom de la plage de temps, sélectionnez une plage de temps à utiliser.



Note: Dans cet exemple, Dayshift est choisi.

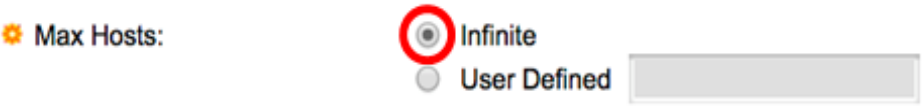
Étape 20. Dans la zone Nombre maximal de tentatives de connexion WBA, cliquez sur Infinite pour aucune limite ou sur User Defined pour définir une limite. Si l'option Défini par l'utilisateur est sélectionnée, saisissez le nombre maximal de tentatives de connexion autorisées pour l'authentification Web.

Note: Dans cet exemple, Infinite est choisi.

Étape 21. Dans la zone Maximum WBA Silence Period, cliquez sur Infinite pour aucune limite ou sur User Defined pour définir une limite. Si l'option Défini par l'utilisateur est sélectionnée, saisissez la longueur maximale de la période silencieuse pour l'authentification Web autorisée sur l'interface.

Note: Dans cet exemple, Infinite est choisi.

Étape 22. Dans la zone Nombre maximal d'hôtes, cliquez sur Infinite (Infinite) pour ne pas limiter ou sur User Defined (Défini par l'utilisateur) pour définir une limite. Si l'option User Defined est sélectionnée, saisissez le nombre maximal d'hôtes autorisés autorisés sur l'interface.



Note: Définissez cette valeur sur 1 pour simuler le mode hôte unique pour l'authentification Web en mode multisessions. Dans cet exemple, Infinite est choisi.

Étape 23. Dans le champ *Période calme*, saisissez l'heure à laquelle le commutateur reste dans l'état silencieux après un échec de l'échange d'authentification. Lorsque le

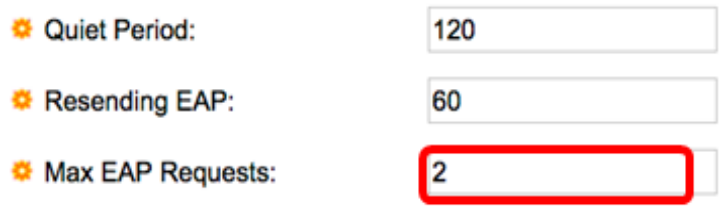
commutateur est dans un état silencieux, cela signifie que le commutateur n'écoute pas les nouvelles demandes d'authentification du client. La valeur par défaut est 60 secondes et la plage est comprise entre 1 et 65 535 secondes.

Note: Dans cet exemple, la période de silence est définie sur 120 secondes.

Étape 24. Dans le champ *Renvoyer EAP*, saisissez l'heure à laquelle le commutateur attend un message de réponse du demandeur avant de renvoyer une demande. La valeur par défaut est 30 secondes et la plage est comprise entre 1 et 65 535 secondes.

Note: Dans cet exemple, le renvoi du protocole EAP est défini sur 60 secondes.

Étape 25. Dans le champ *Nombre maximal de demandes EAP*, saisissez le nombre maximal de demandes EAP pouvant être envoyées. EAP est une méthode d'authentification utilisée dans 802.1X qui fournit un échange d'informations d'authentification entre le commutateur et le client. Dans ce cas, les requêtes EAP sont envoyées au client pour authentification. Le client doit ensuite répondre et faire correspondre les informations d'authentification. Si le client ne répond pas, une autre requête EAP est définie en fonction de la valeur EAP de renvoi et le processus d'authentification est redémarré. La valeur par défaut est 2 et la plage est comprise entre 1 et 10.

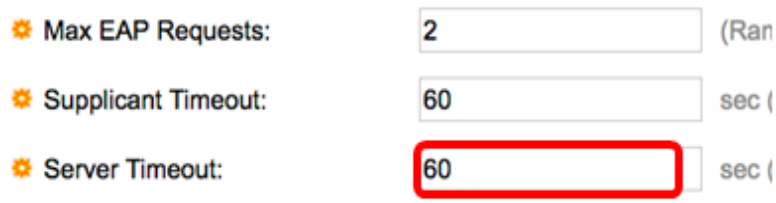


Note: Dans cet exemple, la valeur par défaut de 2 est utilisée.

Étape 26. Dans le champ *Délai d'attente du demandeur*, saisissez l'heure avant le renvoi des demandes EAP au demandeur. La valeur par défaut est 30 secondes et la plage est comprise entre 1 et 65 535 secondes.

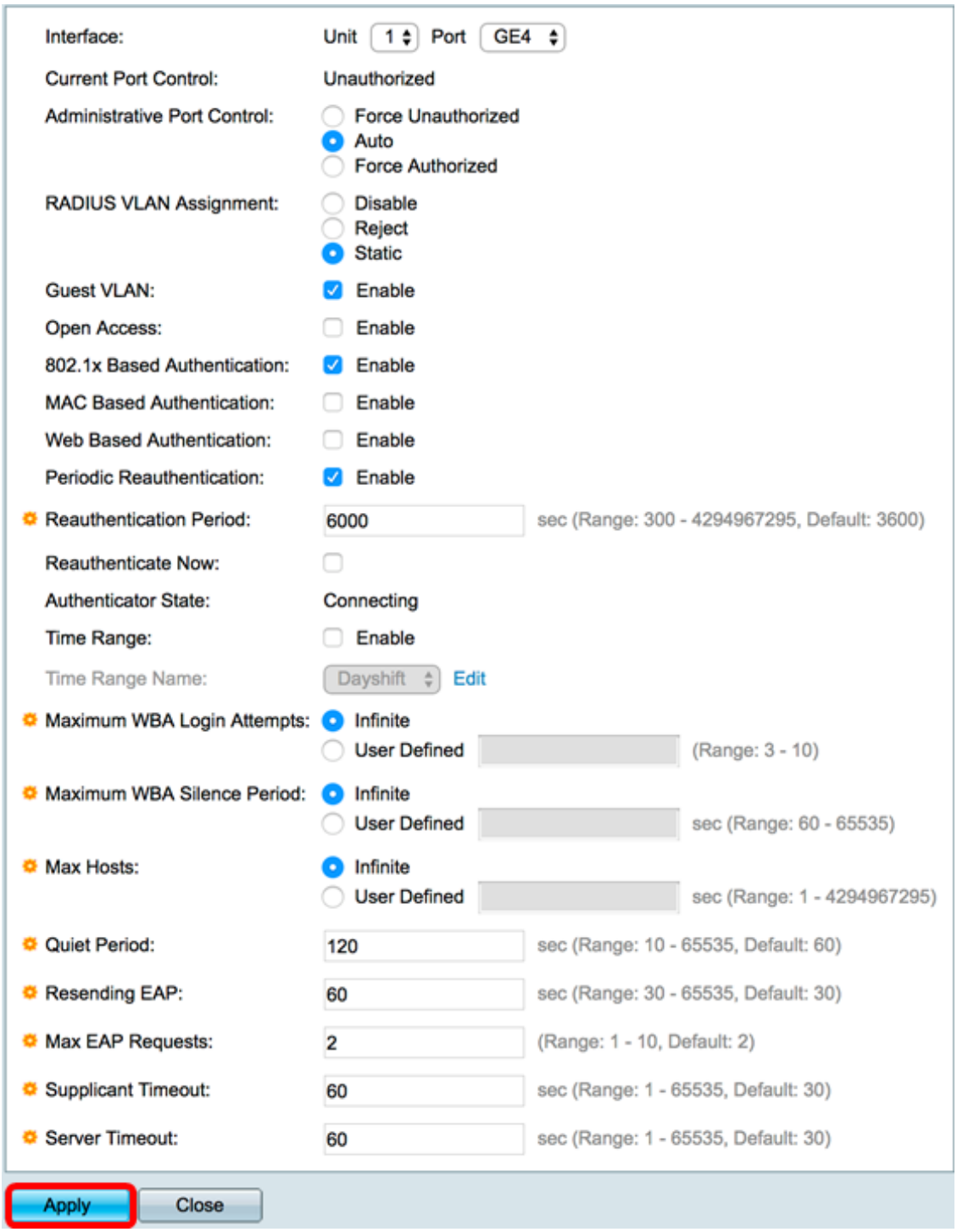
Note: Dans cet exemple, le délai d'attente du demandeur est défini sur 60 secondes.

Étape 27. Dans le champ *Délai d'expiration du serveur*, saisissez l'heure qui s'écoule avant que le commutateur n'envoie une nouvelle demande au serveur RADIUS. La valeur par défaut est 30 secondes et la plage est comprise entre 1 et 65 535 secondes.

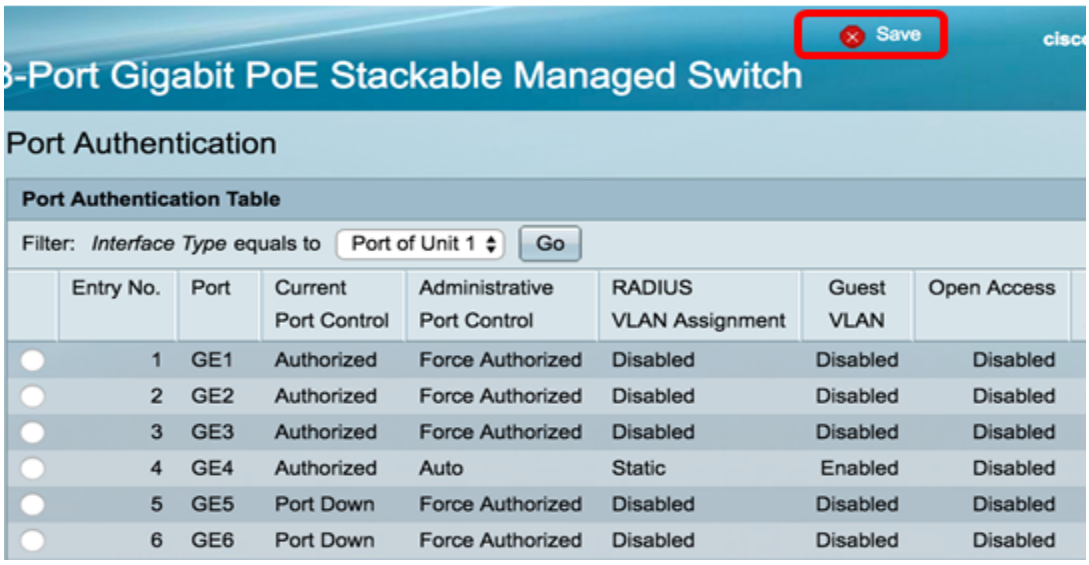


Note: Dans cet exemple, le délai d'attente du serveur est défini sur 60 secondes.

Étape 28. Cliquez sur **Appliquer**, puis sur **Fermer**.



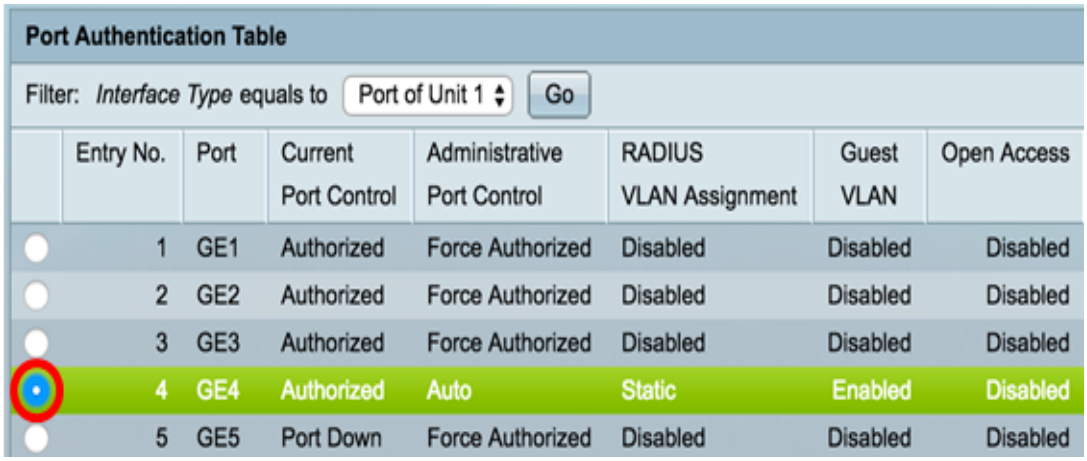
Étape 29. (Facultatif) Cliquez sur **Enregistrer** pour enregistrer les paramètres dans le fichier de configuration initiale.



Vous devez maintenant avoir correctement configuré les paramètres d'authentification de port 802.1x sur votre commutateur.

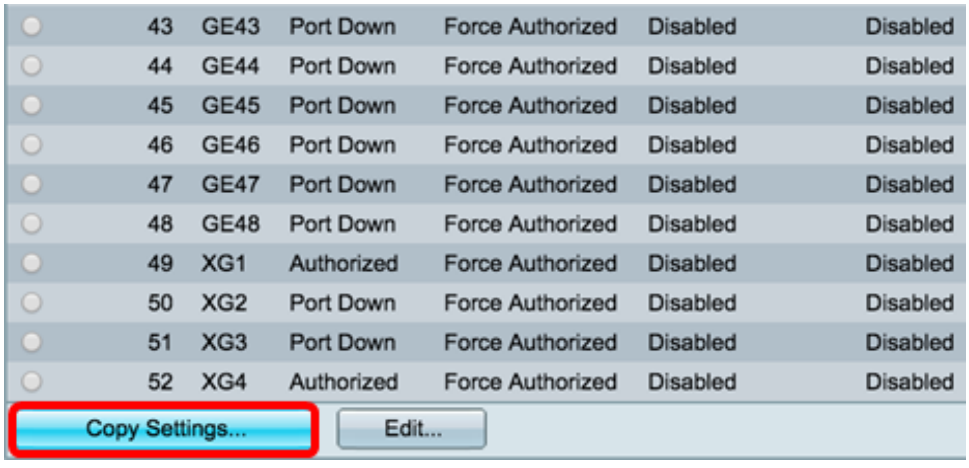
Appliquer les paramètres de configuration d'interface à plusieurs interfaces

Étape 1. Cliquez sur la case d'option de l'interface à laquelle vous voulez appliquer la configuration d'authentification à plusieurs interfaces.



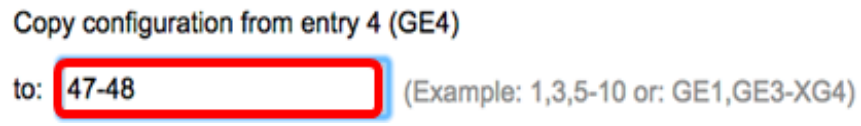
Note: Dans cet exemple, GE4 est sélectionné.

Étape 2. Faites défiler la page vers le bas, puis cliquez sur **Copier les paramètres**.



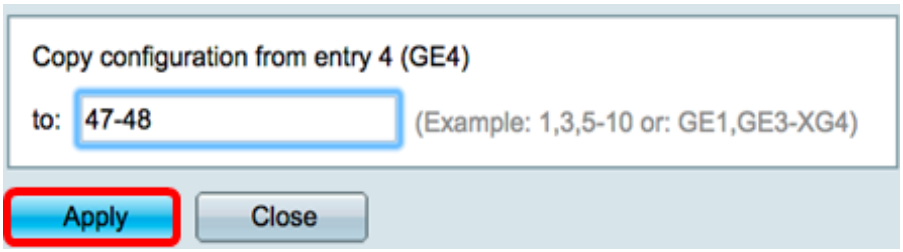
Étape 3. Dans le champ *to*, saisissez la plage d'interfaces à appliquer à la configuration de

l'interface choisie. Vous pouvez utiliser les numéros d'interface ou le nom des interfaces en entrée. Vous pouvez entrer chaque interface séparée par une virgule (par exemple 1, 3, 5 ou GE1, GE3, GE5) ou saisir une plage d'interfaces (par exemple 1-5 ou GE1-GE5).

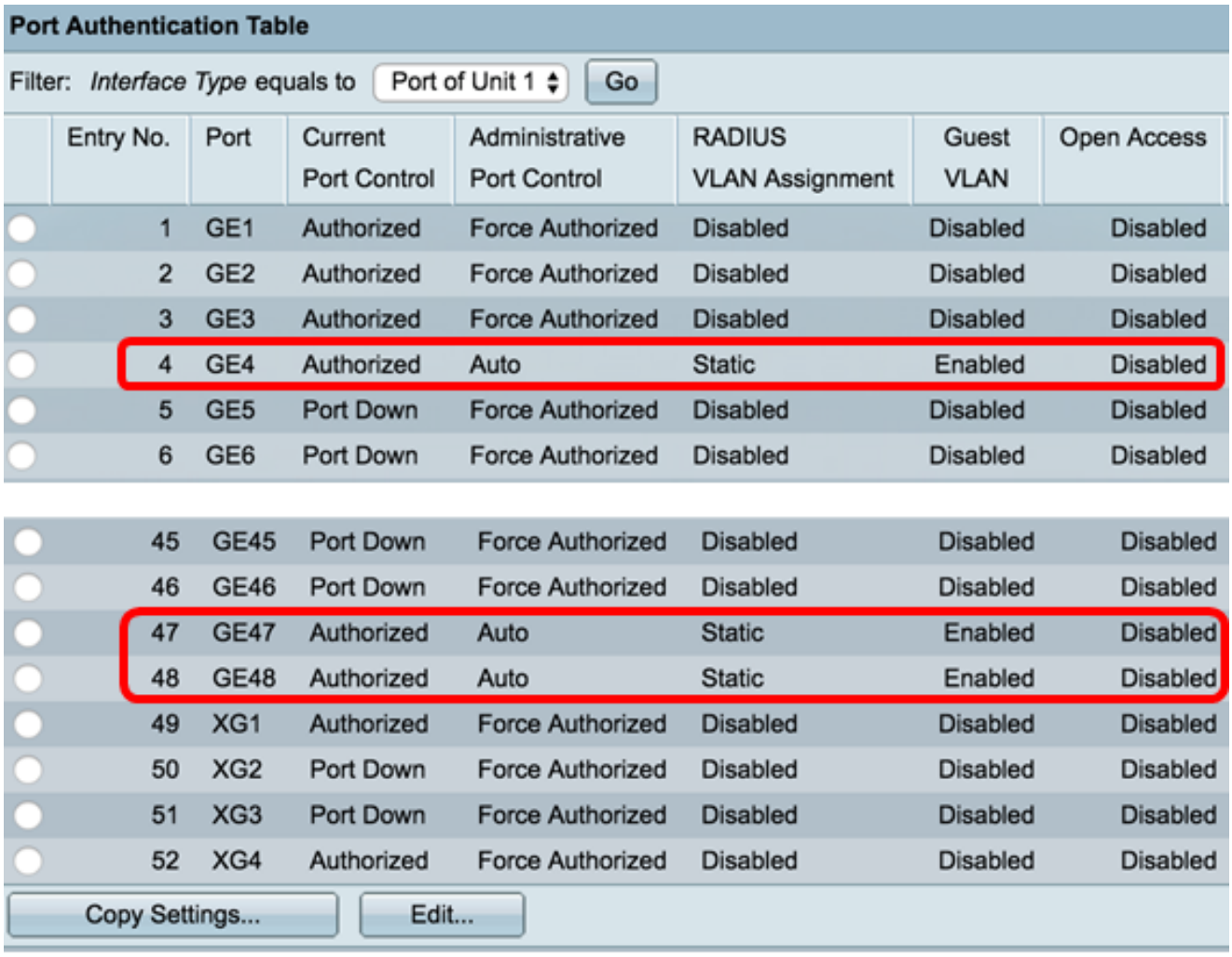


Note: Dans cet exemple, les paramètres de configuration seront appliqués aux ports 47 à 48.

Étape 4. Cliquez sur **Appliquer**, puis sur **Fermer**.



L'image ci-dessous illustre les modifications après la configuration.



Vous devez maintenant avoir copié les paramètres d'authentification 802.1x d'un port et les avoir appliqués à d'autres ports de votre commutateur.