Configurer les paramètres d'authentification d’un utilisateur SSH sur un commutateur

Objectif

Secure Shell (SSH) est un protocole qui fournit une connexion à distance sécurisée à des périphériques réseau spécifiques. Cette connexion offre des fonctionnalités similaires à une connexion Telnet, à ceci près qu’elle est chiffrée. SSH permet à l'administrateur de configurer le commutateur via l'interface de ligne de commande (CLI) à l'aide d'un programme tiers.

En mode CLI via SSH, l'administrateur peut exécuter des configurations plus avancées dans une connexion sécurisée. Les connexions SSH sont utiles pour dépanner un réseau à distance, dans les cas où l’administrateur réseau n’est pas physiquement présent sur le site réseau. Le commutateur permet à l'administrateur d'authentifier et de gérer les utilisateurs pour se connecter au réseau via SSH. L'authentification s'effectue via une clé publique que l'utilisateur peut utiliser pour établir une connexion SSH à un réseau spécifique.

La fonctionnalité de client SSH est une application qui s'exécute sur le protocole SSH pour fournir l'authentification et le chiffrement des périphériques. Elle permet à un périphérique d'établir une connexion sécurisée et chiffrée avec un autre périphérique qui exécute le serveur SSH. Avec l'authentification et le chiffrement, le client SSH permet une communication sécurisée sur une connexion Telnet non sécurisée.

Cet article présente la marche à suivre pour configurer l’authentification d’un utilisateur client sur un commutateur géré.

Périphériques pertinents

- Série Sx200
- Gamme Sx300
- Gamme Sx350
- Gamme SG350X
- Gamme Sx500
- Gamme Sx550X

Version du logiciel

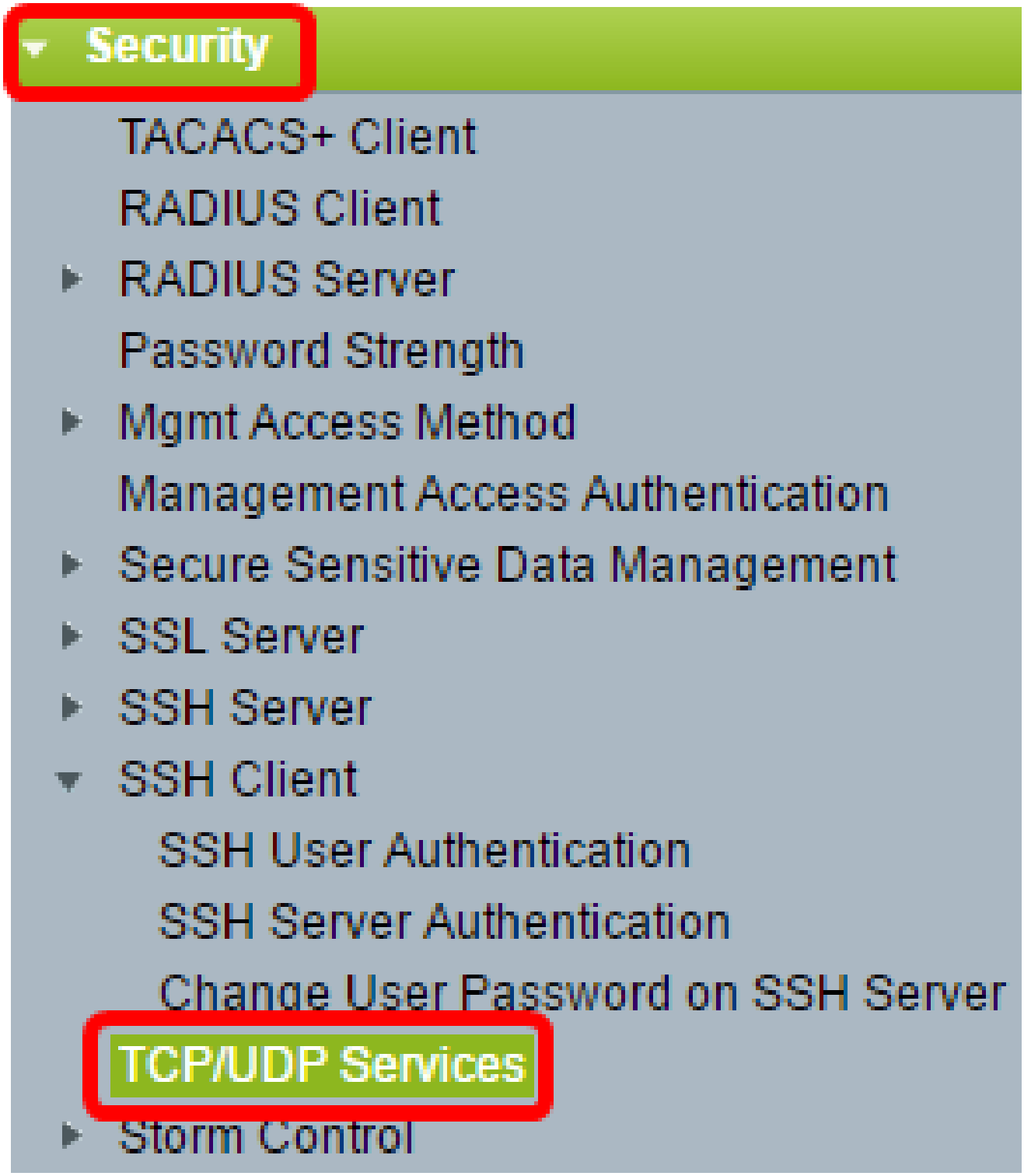
- 1.4.5.02 - Série Sx200, Sx300, Sx500
- 2.2.0.66 - Série Sx350, Série SG350X, Série Sx550X

Configuration des paramètres d'authentification utilisateur du client SSH

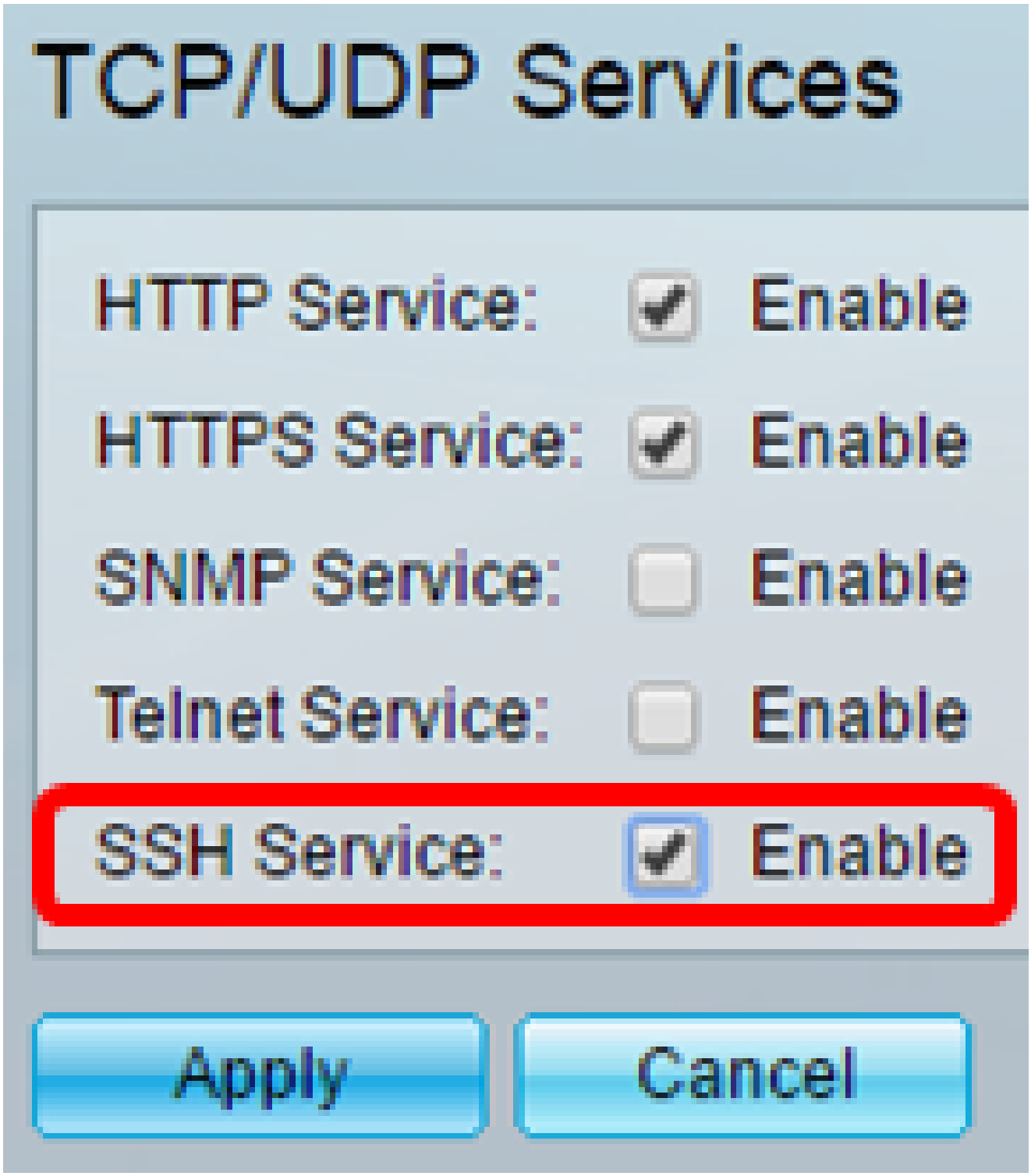
Activer le service SSH

Remarque : afin de prendre en charge la configuration automatique d'un périphérique prêt à l'emploi (périphérique avec la configuration d'usine par défaut), l'authentification du serveur SSH est désactivée par défaut.

Étape 1. Connectez-vous à l'utilitaire Web et choisissez Security > TCP/UDP Services



Étape 2. Cochez la case SSH Service pour activer l'accès de l'invite de commande des commutateurs via SSH.



Étape 3. Cliquez sur Apply pour activer le service SSH.

Configuration des paramètres d'authentification utilisateur SSH

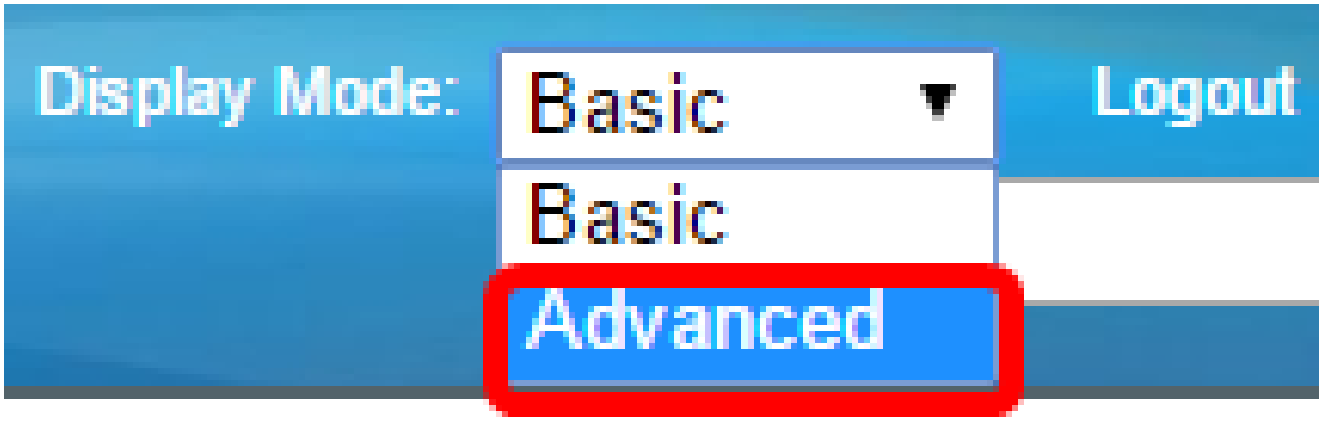
Utilisez cette page pour choisir une méthode d'authentification utilisateur SSH. Vous pouvez définir un nom d'utilisateur et un mot de passe sur le périphérique si la méthode de mot de passe est choisie. Vous pouvez également générer une clé Ron Rivest, Adi Shamir et Leonard Adleman (RSA) ou un algorithme de signature numérique (DSA) si la méthode de

clé publique ou privée est sélectionnée.

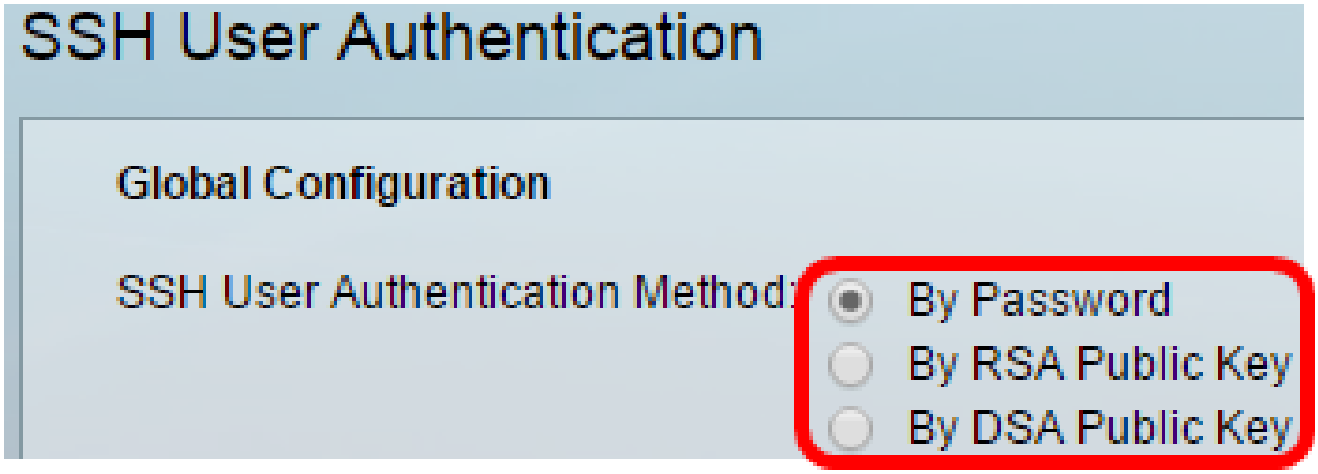
Les paires de clés par défaut RSA et DSA sont générées pour le périphérique lors de son démarrage. L'une de ces clés est utilisée pour chiffrer les données téléchargées à partir du serveur SSH. La clé RSA est utilisée par défaut. Si l'utilisateur supprime l'une de ces clés ou les deux, elles sont régénérées.

Étape 1. Connectez-vous à l'utilitaire Web et choisissez Security > SSH Client > SSH User Authentication.

Remarque : si vous disposez d'un commutateur Sx350, SG300X ou Sx500X, passez en mode avancé en sélectionnant Avancé dans la liste déroulante Mode d'affichage.



Étape 2. Sous Configuration globale, cliquez sur la méthode d'authentification de l'utilisateur SSH souhaitée.



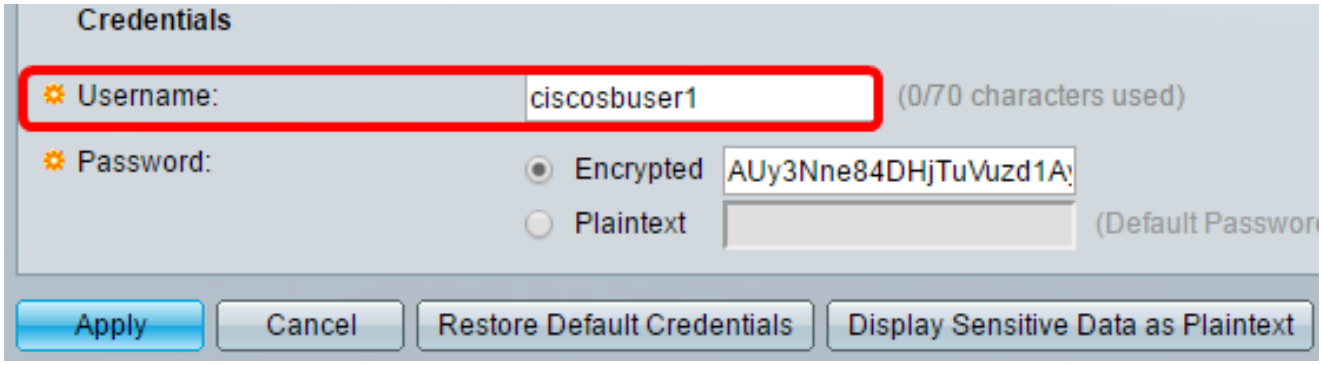
Remarque : lorsqu'un périphérique (client SSH) tente d'établir une session SSH avec le serveur SSH, le serveur SSH utilise l'une des méthodes suivantes pour l'authentification du client :

- Par mot de passe : cette option vous permet de configurer un mot de passe pour l'authentification des utilisateurs. Il s'agit du paramètre par défaut et le mot de passe par défaut est anonymous. Si cette option est sélectionnée, assurez-vous que le nom d'utilisateur et le mot de passe ont été définis sur le serveur SSH.
- By RSA Public Key : cette option vous permet d'utiliser la clé publique RSA pour l'authentification des utilisateurs. Une clé RSA est une clé chiffrée basée sur la factorisation de grands entiers. Cette clé est le type de clé le plus courant utilisé pour l'authentification des utilisateurs SSH.
- By DSA Public Key : cette option vous permet d'utiliser une clé publique DSA pour l'authentification des utilisateurs. Une clé DSA est une clé chiffrée basée sur l'algorithme discret ElGamal. Cette clé n'est généralement pas utilisée pour l'authentification des

utilisateurs SSH, car elle prend plus de temps dans le processus d'authentification.

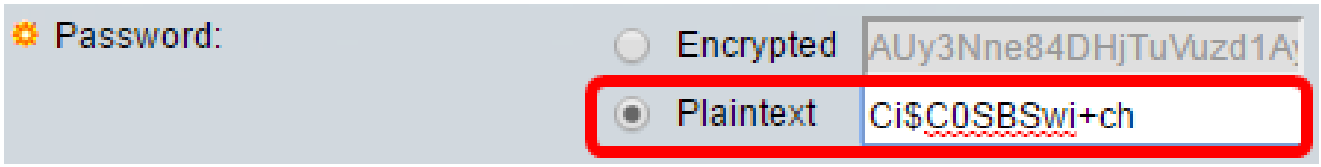
Remarque : dans cet exemple, l'option Par mot de passe est sélectionnée.

Étape 3. Dans la zone Informations d'identification, saisissez le nom d'utilisateur dans le champ Nom d'utilisateur.



Remarque : dans cet exemple, ciscosbuser1 est utilisé.

Étape 4. (Facultatif) Si vous avez sélectionné Par mot de passe à l'étape 2, cliquez sur la méthode, puis saisissez le mot de passe dans le champ Chiffré ou Texte clair.



Les options sont les suivantes :

- Encrypted : cette option vous permet d'entrer une version chiffrée du mot de passe.
- Plaintext : cette option vous permet d'entrer un mot de passe en texte clair.

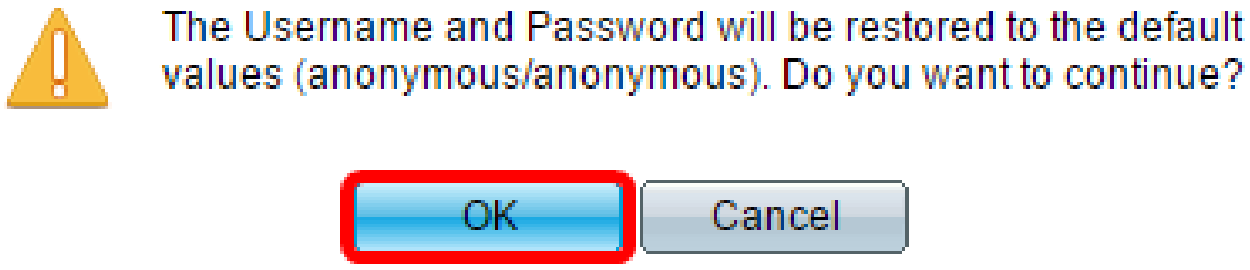
Remarque : dans cet exemple, le texte en clair est choisi et un mot de passe en texte clair est entré.

Étape 5. Cliquez sur Apply pour enregistrer votre configuration d'authentification.

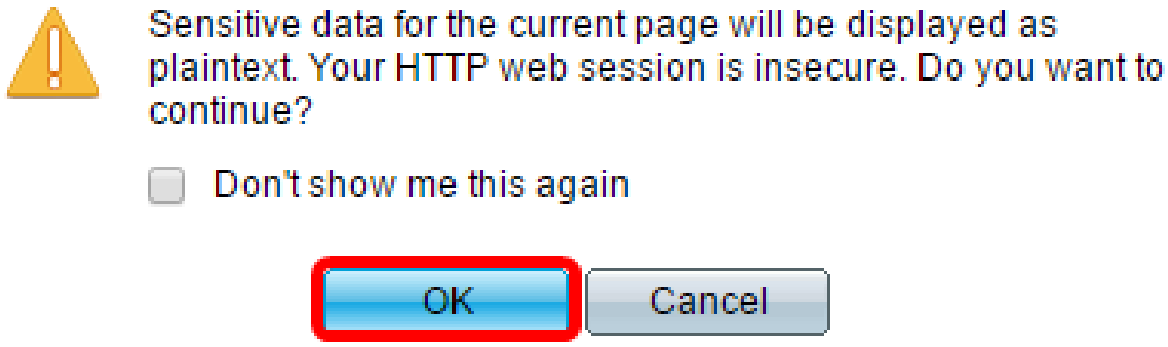
Étape 6. (Facultatif) Cliquez sur Restore Default Credentials pour restaurer le nom d'utilisateur et le mot de passe par défaut, puis cliquez sur OK pour continuer.

Remarque : le nom d'utilisateur et le mot de passe seront restaurés aux valeurs par défaut :

anonymous/anonymous.

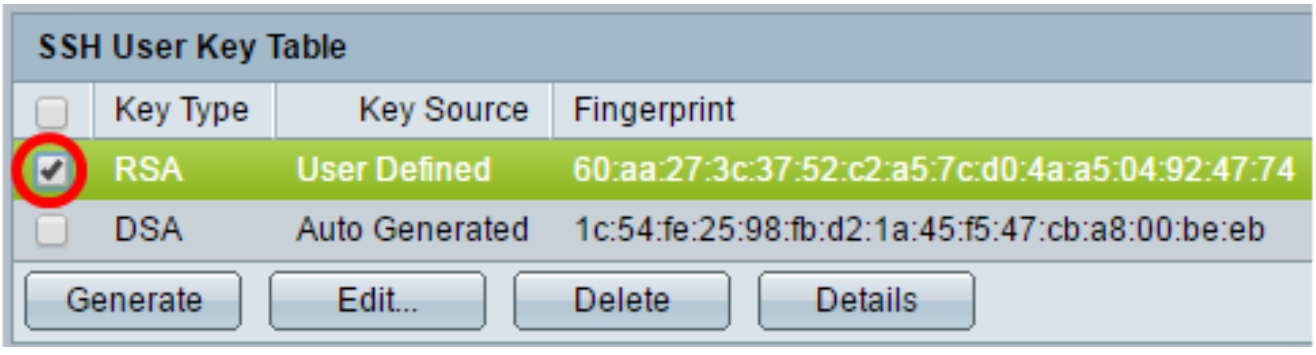


Étape 7. (Facultatif) Cliquez sur Afficher les données sensibles en texte clair pour afficher les données sensibles de la page en texte clair, puis cliquez sur OK pour continuer.



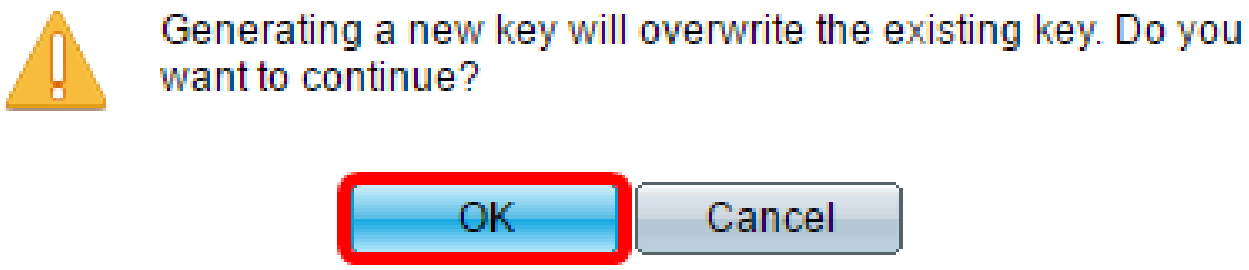
Configuration de la table des clés utilisateur SSH

Étape 8. Cochez la case de la clé que vous souhaitez gérer.

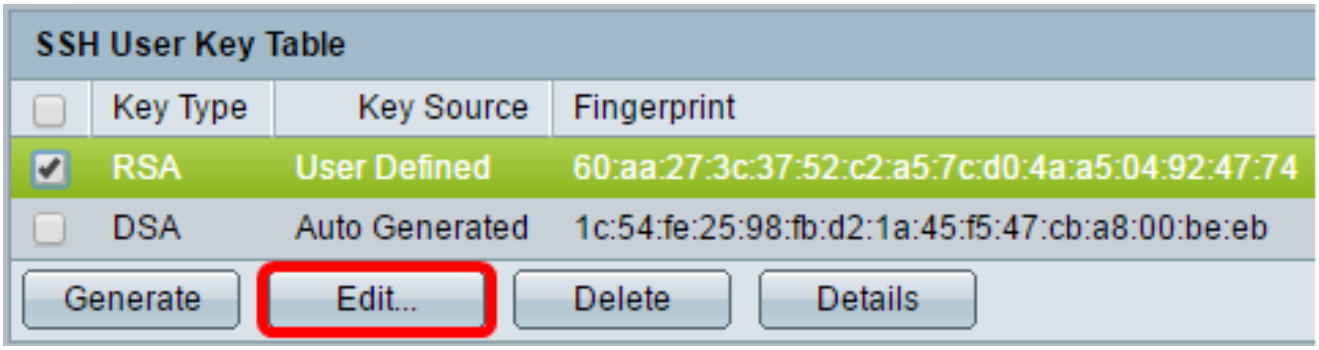


Remarque : dans cet exemple, RSA est sélectionné.

Étape 9. (Facultatif) Cliquez sur Generate pour générer une nouvelle clé. La nouvelle clé remplacera la clé cochée, puis cliquez sur OK pour continuer.



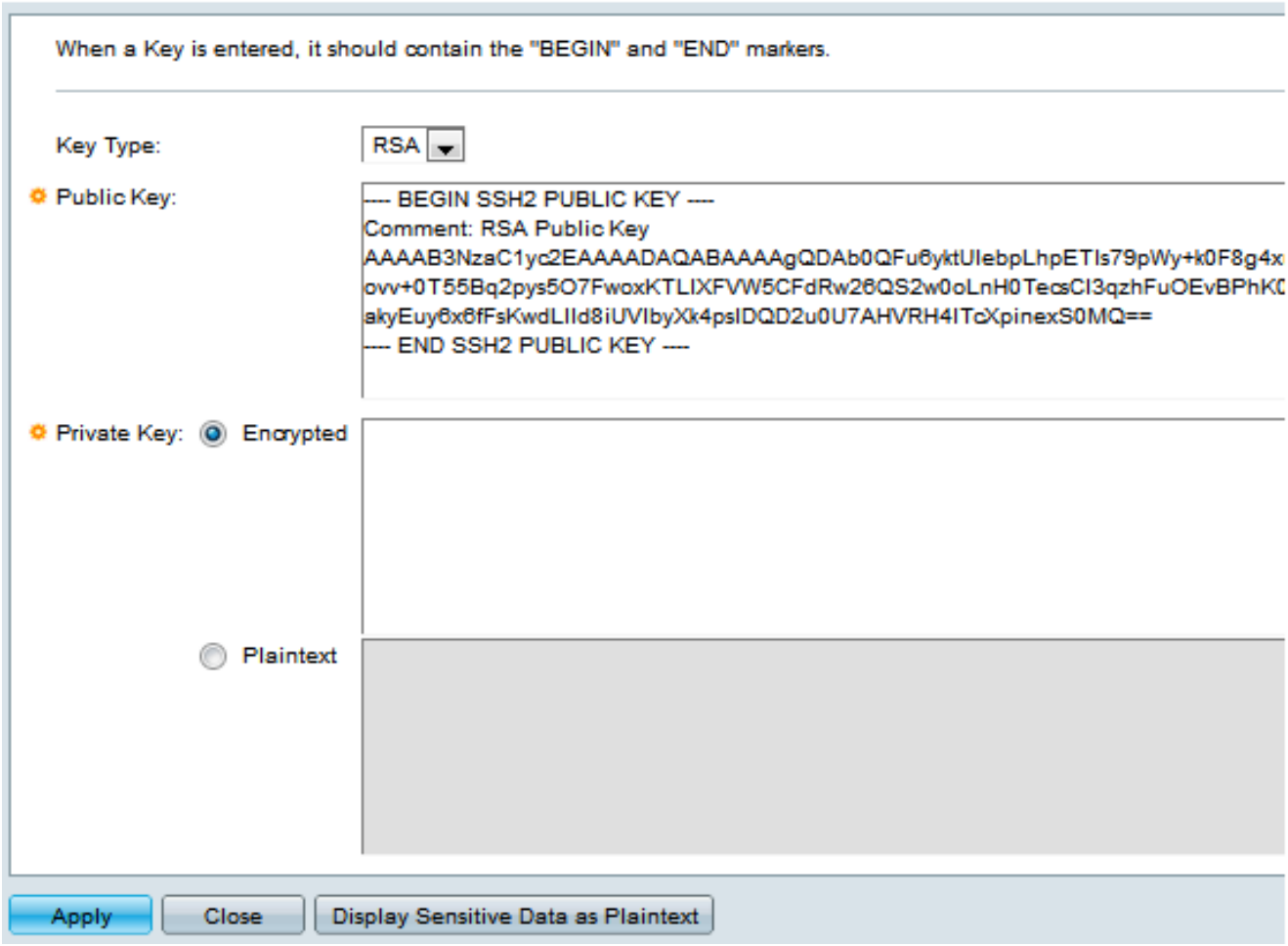
Étape 10. (Facultatif) Cliquez sur Edit pour modifier une clé actuelle.



Étape 11. (Facultatif) Choisissez un type de clé dans la liste déroulante Type de clé.

Remarque : dans cet exemple, RSA est sélectionné.

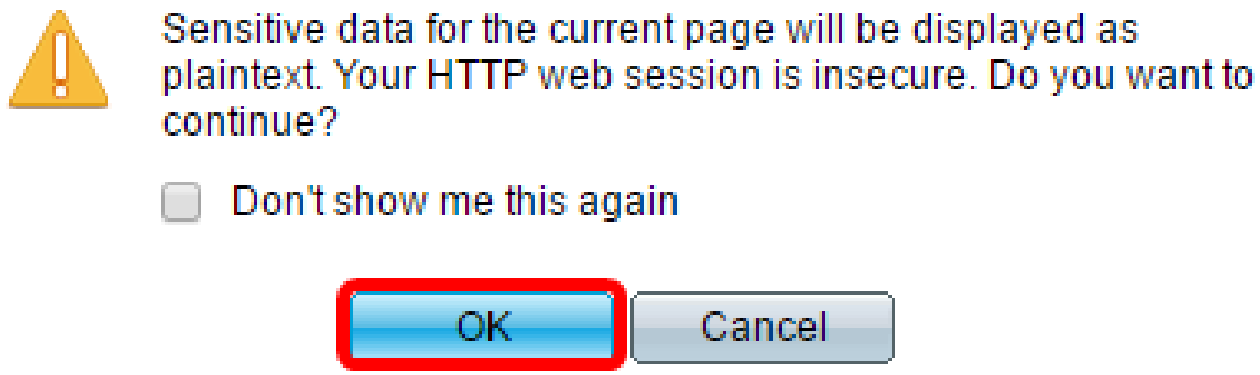
Étape 12. (Facultatif) Entrez la nouvelle clé publique dans le champ Clé publique.



Étape 13. (Facultatif) Entrez la nouvelle clé privée dans le champ Private Key (Clé privée).

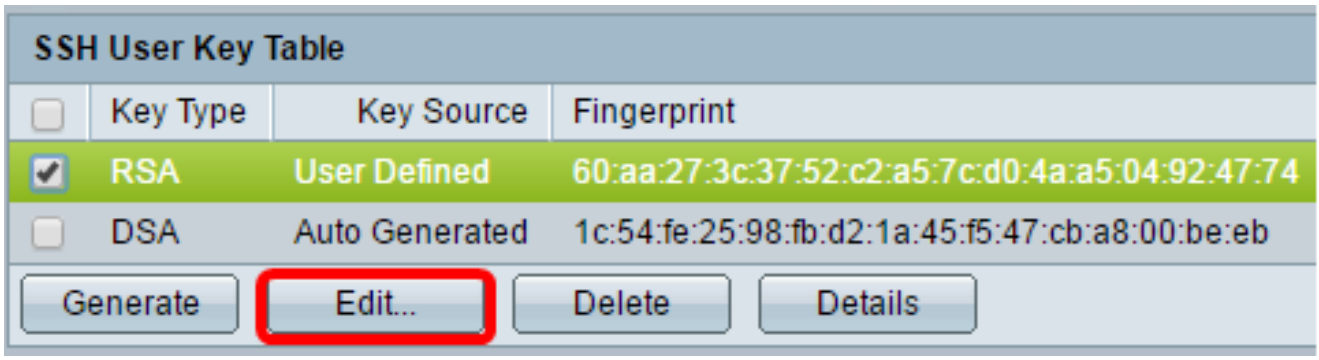
Remarque : vous pouvez modifier la clé privée et cliquer sur Chiffré pour afficher la clé privée actuelle sous forme de texte chiffré ou sur Texte brut pour afficher la clé privée actuelle en texte brut.

Étape 14. (Facultatif) Cliquez sur Display Sensitive Data as Plaintext pour afficher les données chiffrées de la page au format texte brut, puis cliquez sur OK pour continuer.

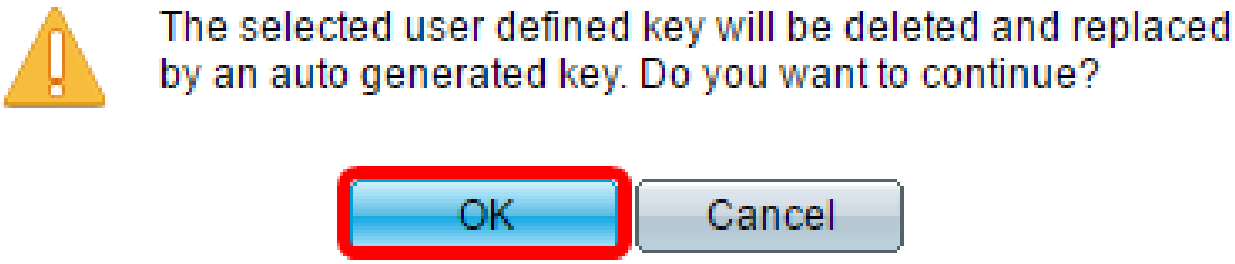


Étape 15. Cliquez sur Apply pour enregistrer vos modifications, puis cliquez sur Close.

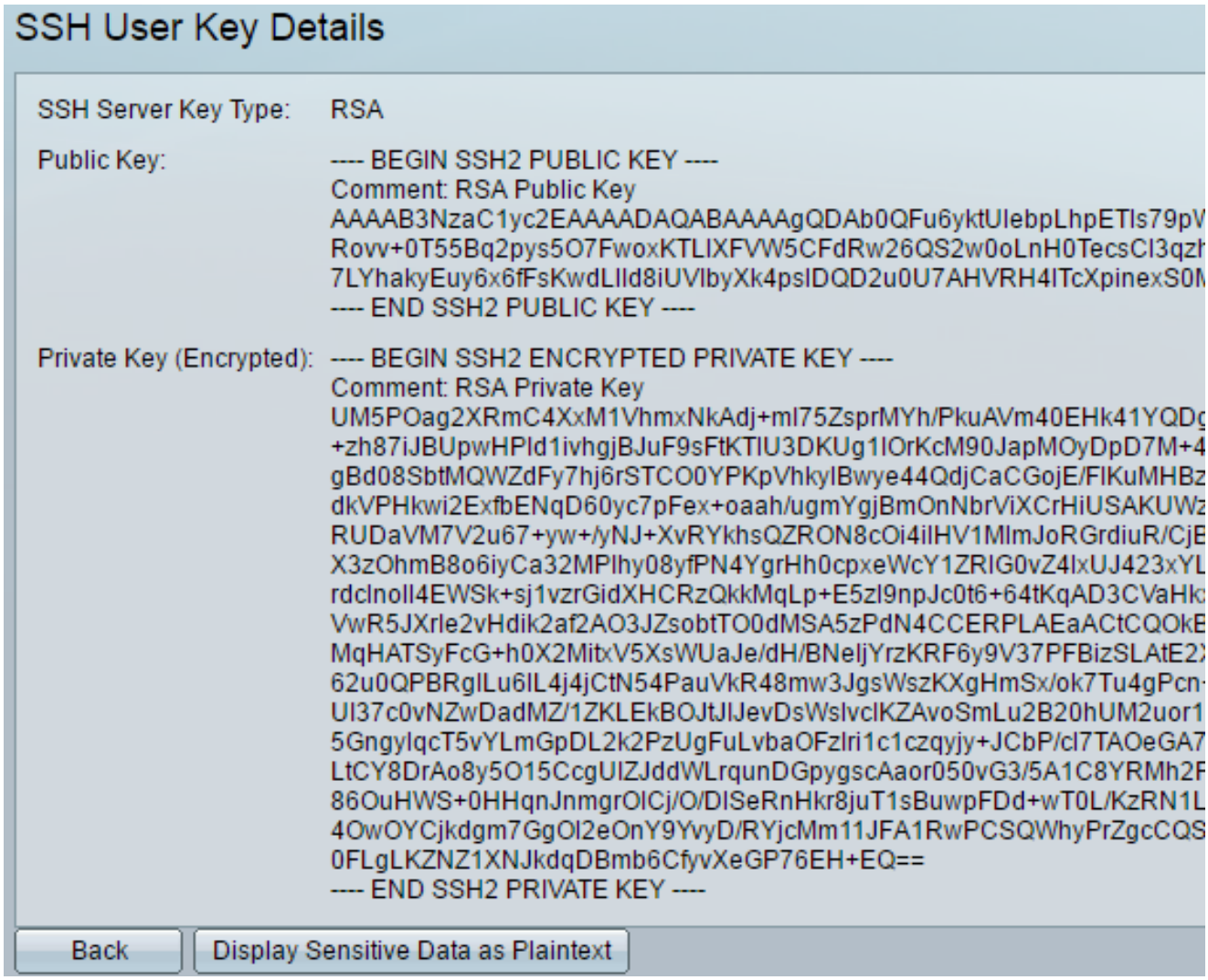
Étape 16. (Facultatif) Cliquez sur Delete pour supprimer la clé cochée.



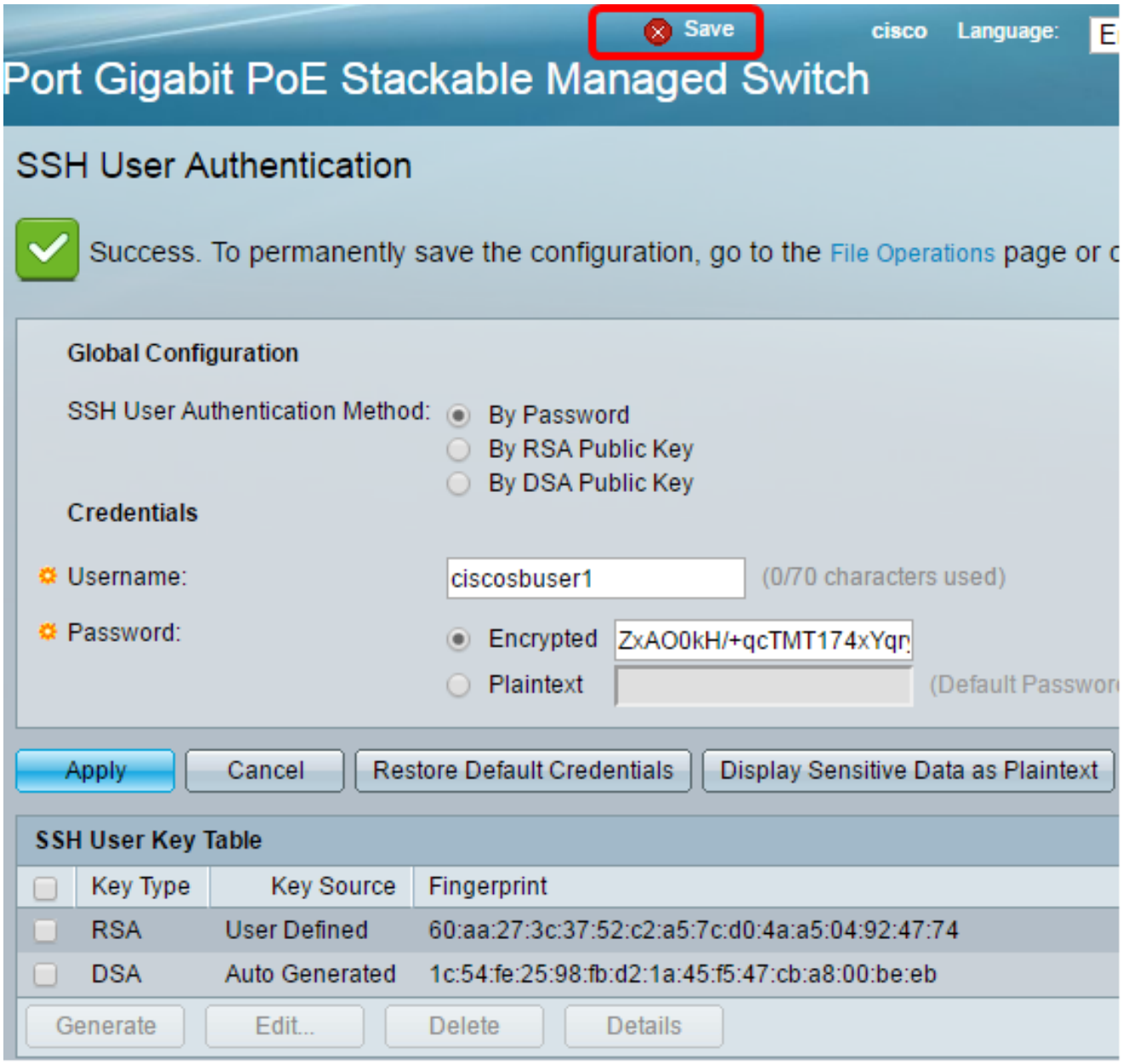
Étape 17. (Facultatif) Lorsque vous êtes invité à confirmer, comme indiqué ci-dessous, cliquez sur OK pour supprimer la clé.



Étape 18. (Facultatif) Cliquez sur Details pour afficher les détails de la clé cochée.



Étape 19. (Facultatif) Cliquez sur le bouton Save en haut de la page pour enregistrer les modifications apportées au fichier de configuration initiale.



Vous devez maintenant avoir configuré les paramètres d'authentification de l'utilisateur client sur votre commutateur géré.

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.

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.

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.

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.

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.

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.

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.

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.