Configurer les paramètres d'authentification utilisateur Secure Shell (SSH) sur un commutateur de la gamme Cisco Business 350

Objectif

Cet article explique comment configurer l'authentification des utilisateurs clients sur les commutateurs de la gamme Cisco Business 350.

Introduction

Secure Shell (SSH) est un protocole qui fournit une connexion à distance sécurisée à des périphériques réseau spécifiques. Cette connexion fournit une fonctionnalité similaire à une connexion Telnet, sauf qu'elle est chiffrée. SSH permet à l'administrateur de configurer le commutateur via l'interface de ligne de commande (CLI) avec 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 se produit via une clé publique que l'utilisateur peut utiliser pour établir une connexion SSH à un réseau spécifique.

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

Périphériques pertinents | Version du logiciel

- CBS350 (fiche technique) | 3.0.0.69 (Télécharger la dernière version)
- CBS350-2X (fiche technique) | 3.0.0.69 (Télécharger la dernière version)
- CBS350-4X (fiche technique) | 3.0.0.69 (Télécharger la dernière version)

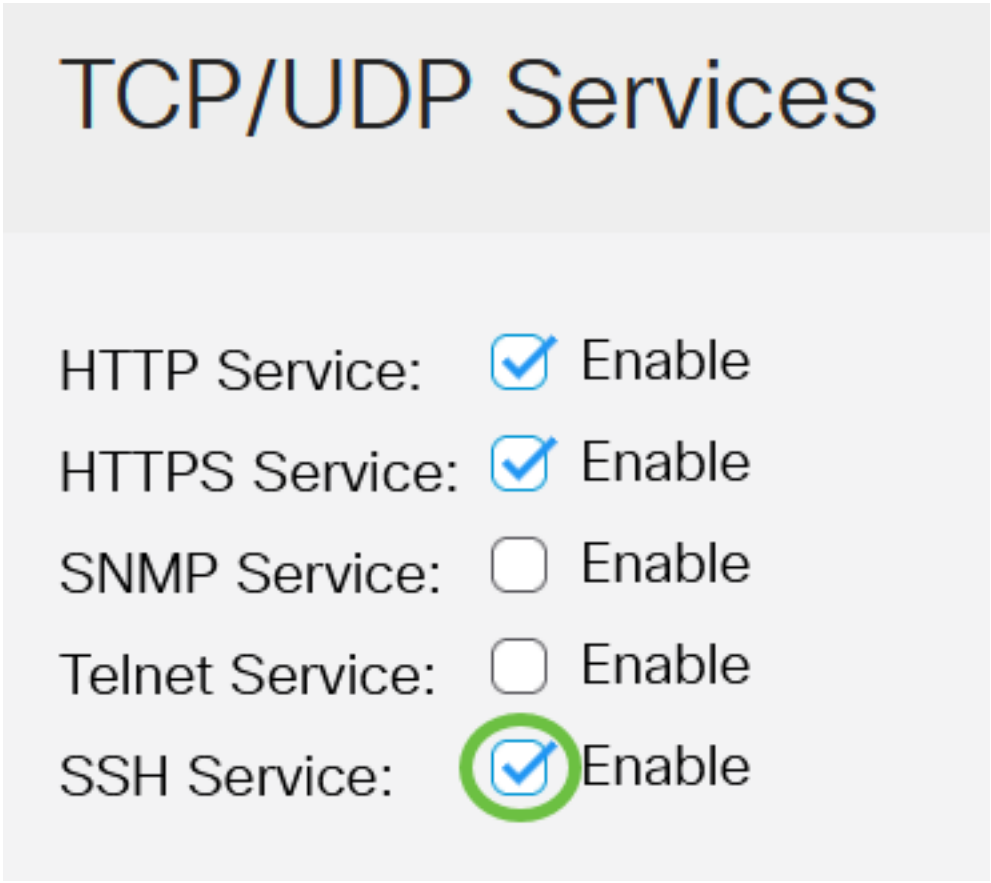
Configuration des paramètres d'authentification utilisateur du client SSH

Activer le service SSH

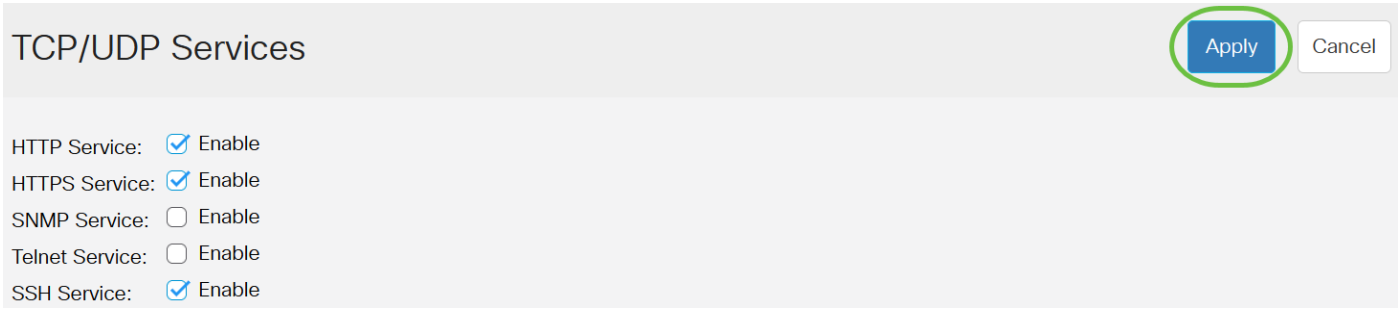
Afin de prendre en charge la configuration automatique d'un périphérique prêt à l'emploi (périphérique avec configuration par défaut en usine), l'authentification du serveur SSH est désactivée par défaut.

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.

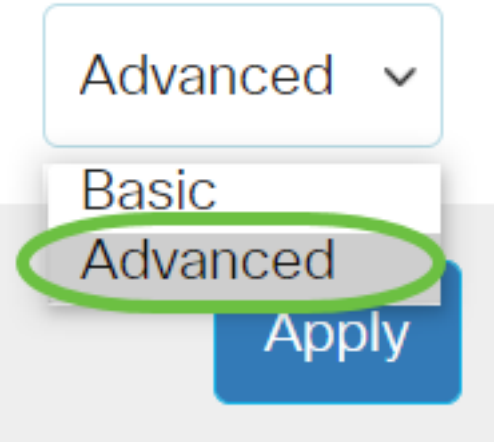


Configuration des paramètres d'authentification utilisateur SSH

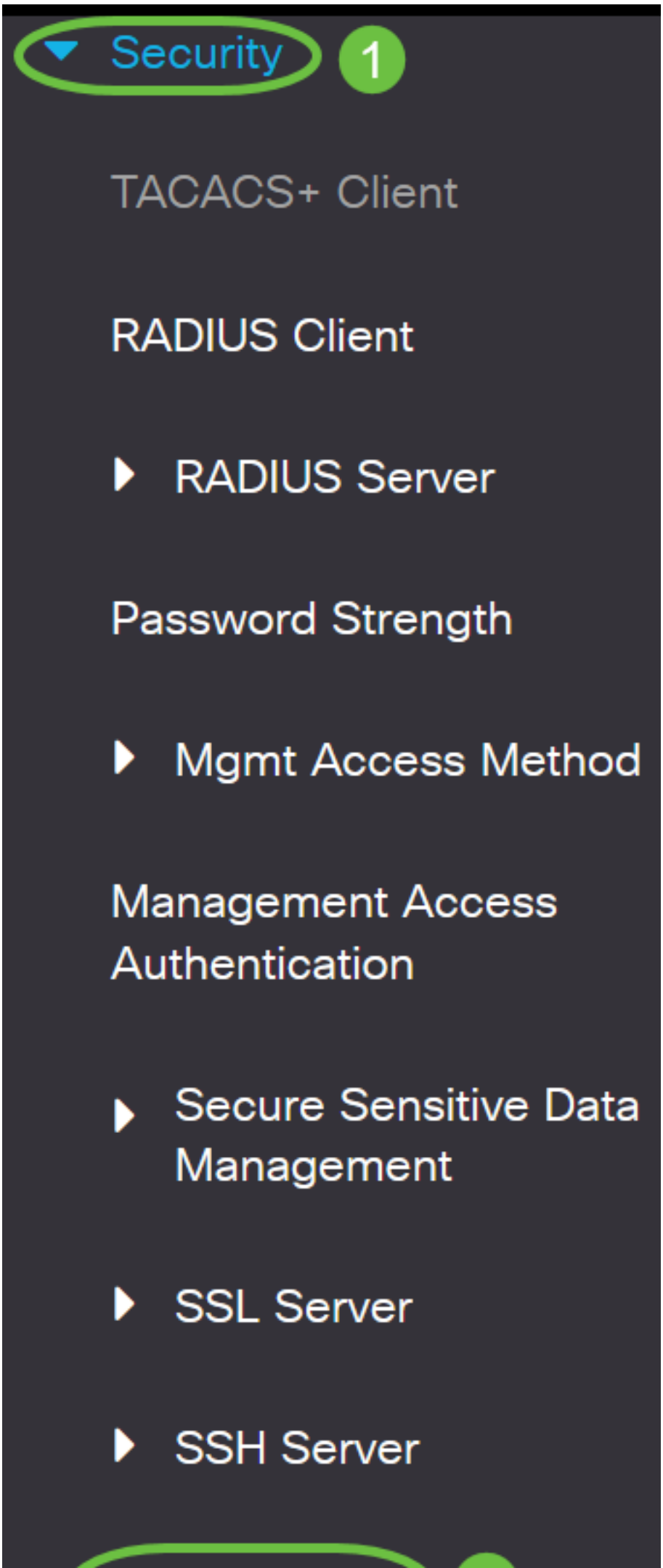
Utilisez cette page pour choisir une méthode d'authentification utilisateur SSH. Vous pouvez définir un nom d'utilisateur et un mot de passe sur le périphérique si la méthode de mot de passe est choisie. Vous pouvez également générer une clé Ron Rivest, Adi Shamir et Leonard Adleman (RSA) ou DSA (Digital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

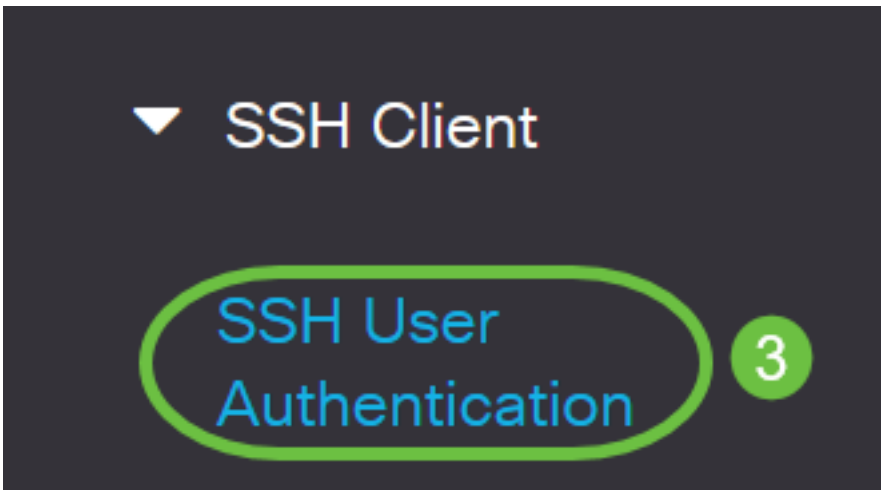
Les paires de clés par défaut RSA et DSA sont générées pour le périphérique au démarrage. Une de ces clés est utilisée pour chiffrer les données téléchargées à partir du serveur SSH. La clé RSA est utilisée par défaut. Si l'utilisateur supprime une ou les deux clés, elles sont régénérées.

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

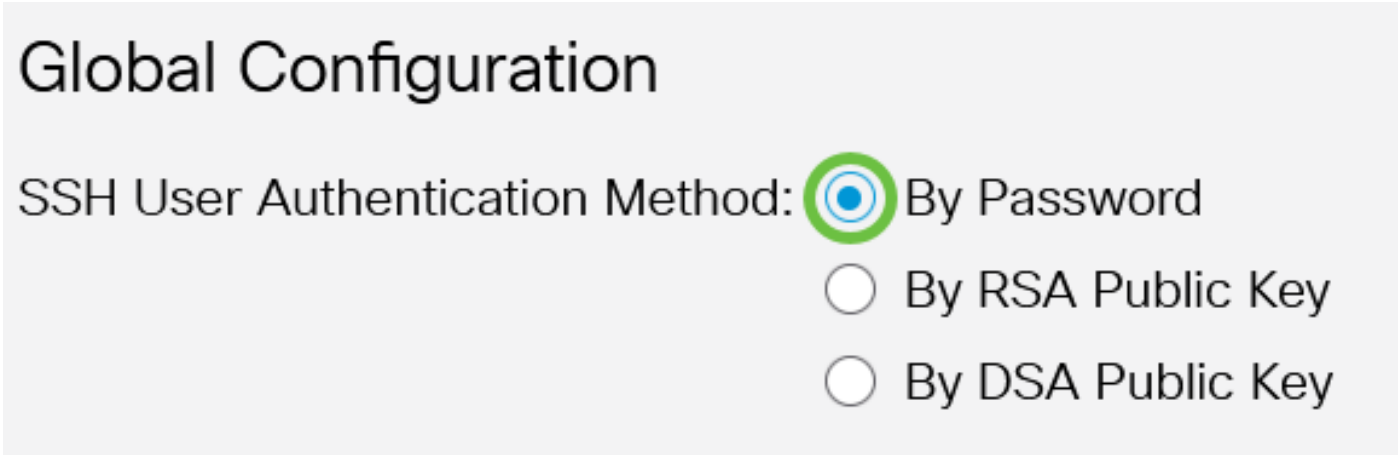


Étape 2. Choisissez **Security > SSH Client > SSH User Authentication** dans le menu.


Security
1
TACACS+ Client
RADIUS Client
RADIUS Server
Password Strength
Mgmt Access Method
Management Access Authentication
Secure Sensitive Data Management
SSL Server
SSH Server



Étape 3. Sous Configuration globale, cliquez sur la méthode d'authentification utilisateur SSH souhaitée.



Lorsqu'un périphérique (client SSH) tente d'établir une session SSH sur 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 anonyme. Si cette option est sélectionnée, assurez-vous que le nom d'utilisateur et le mot de passe ont été définis sur le serveur SSH.
- Par clé publique RSA : cette option vous permet d'utiliser la clé publique RSA pour l'authentification des utilisateurs. Une clé RSA est une clé cryptée basée sur la factorisation de gros entiers. Cette clé est le type de clé le plus utilisé pour l'authentification utilisateur SSH.
- By DSA Public Key (Par clé publique DSA) : cette option vous permet d'utiliser une clé publique DSA pour l'authentification des utilisateurs. Une clé DSA est une clé cryptée basée sur l'algorithme discret ElGamal. Cette clé n'est pas couramment utilisée pour l'authentification des utilisateurs SSH car elle prend plus de temps dans le processus d'authentification.

Dans cet exemple, Par mot de passe est sélectionné.

Étape 4. Dans la zone Informations d'identification et de connexion, saisissez le nom d'utilisateur dans le champ *Nom d'utilisateur*.

Dans cet exemple, ciscosbuser1 est utilisé.

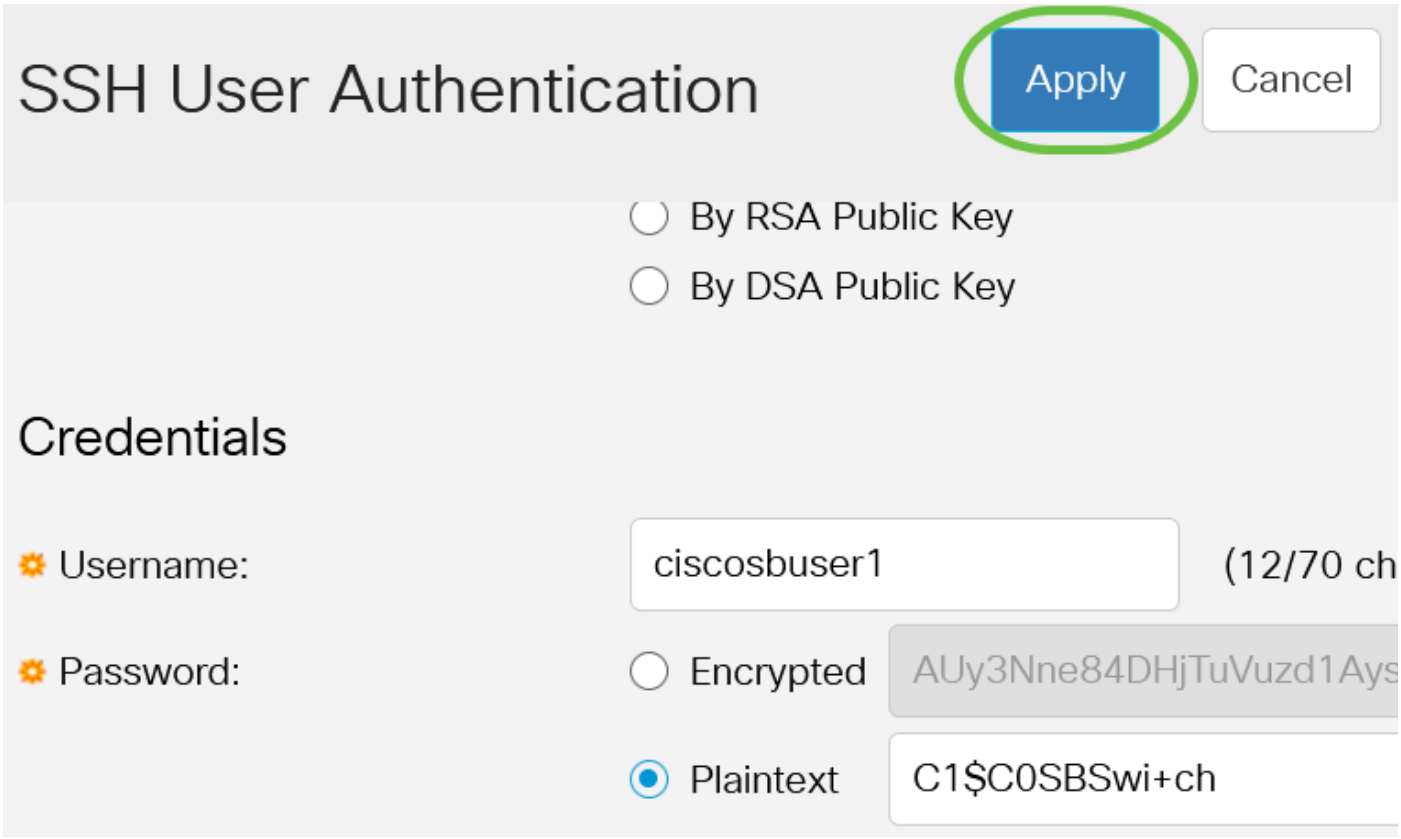
Étape 5. (Facultatif) Si vous avez choisi Par mot de passe à l'étape 2, cliquez sur la méthode, puis entrez le mot de passe dans le champ *Chiffré* ou *Texte clair*.

Les options sont les suivantes :

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

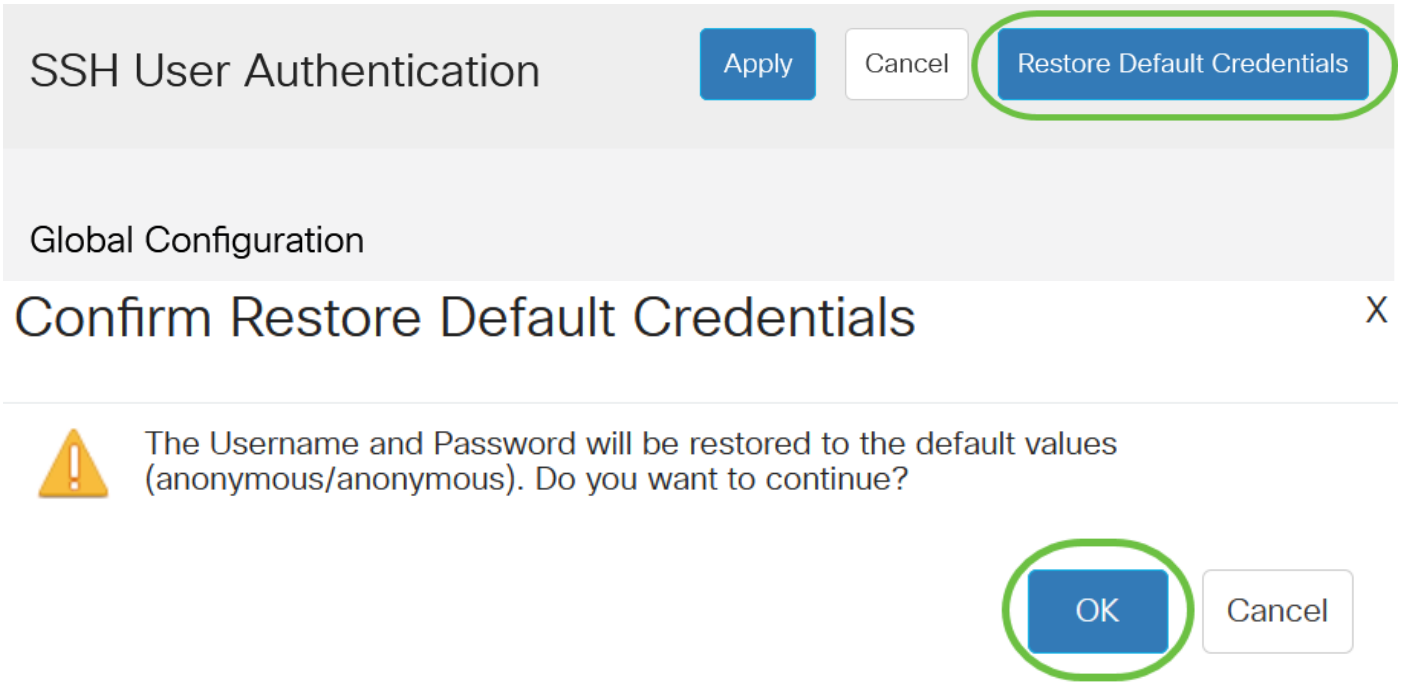
Dans cet exemple, le texte clair est sélectionné et un mot de passe en texte clair est saisi.

Étape 6. Cliquez sur **Apply** pour enregistrer votre configuration d'authentification.



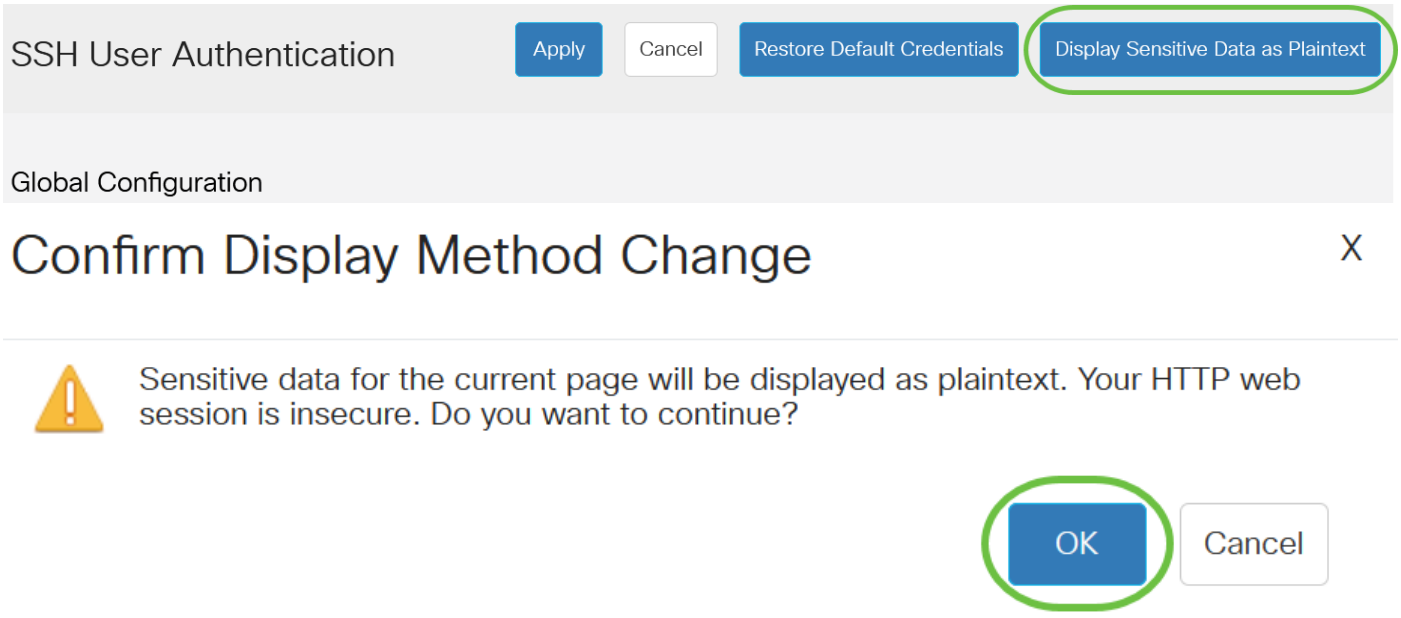
Étape 7. (Facultatif) Cliquez sur **Restaurer les informations d'identification par défaut** pour

restaurer le nom d'utilisateur et le mot de passe par défaut, puis cliquez sur **OK** pour continuer.



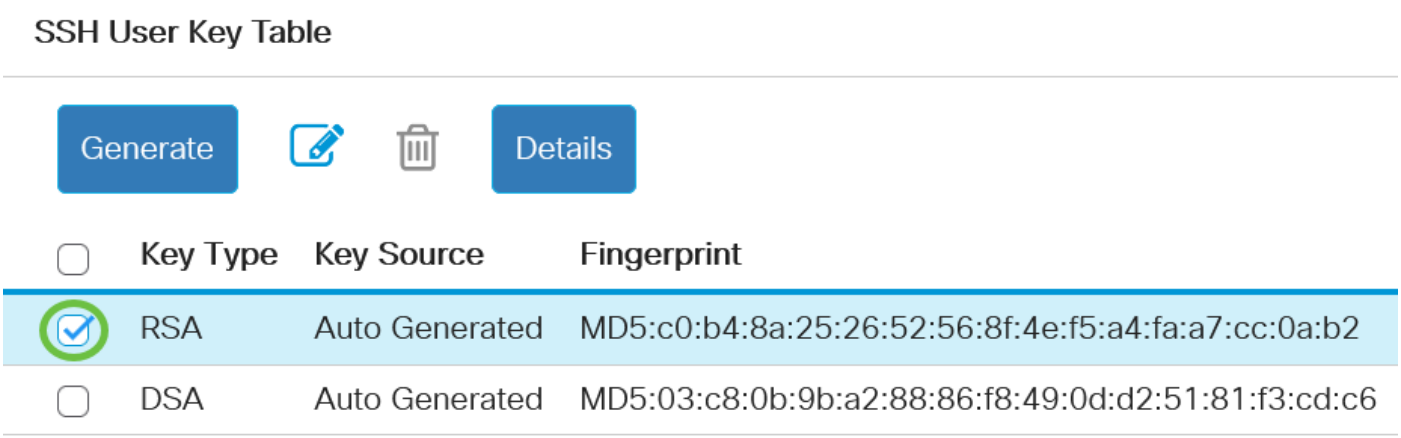
Le nom d'utilisateur et le mot de passe sont restaurés aux valeurs par défaut : anonyme/anonyme.

Étape 8. (Facultatif) Cliquez sur **Afficher les données sensibles en texte clair** pour afficher les données sensibles de la page en format texte brut, puis cliquez sur **OK** pour continuer.



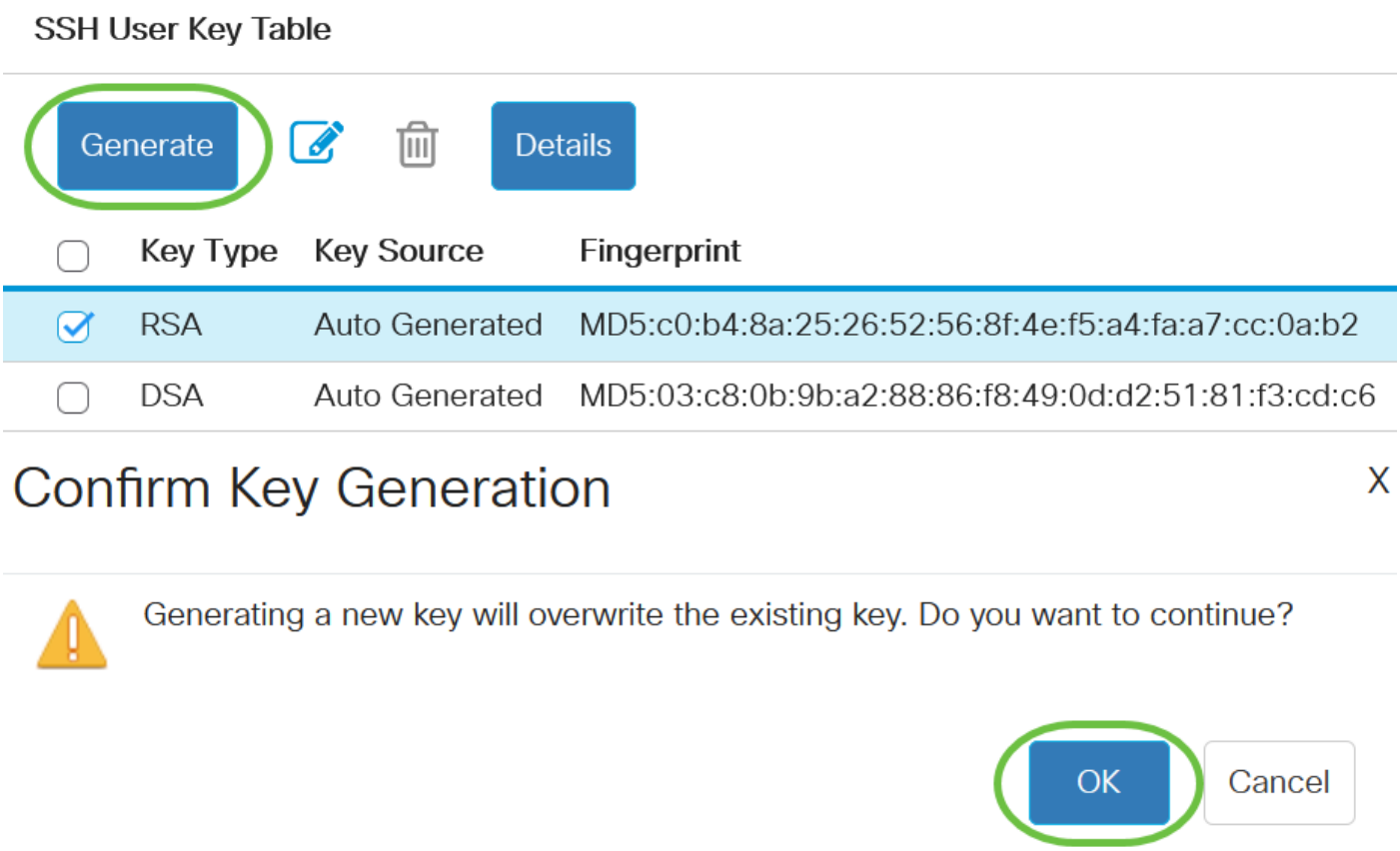
Configurer la table des clés utilisateur SSH

Étape 9. Cochez la case de la clé que vous souhaitez gérer.

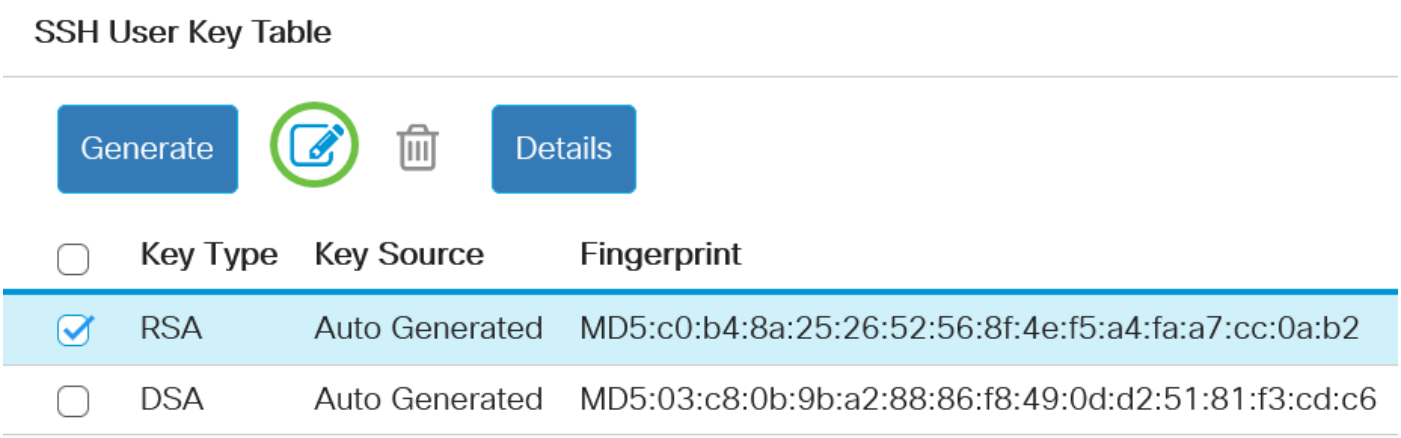


Dans cet exemple, RSA est choisi.

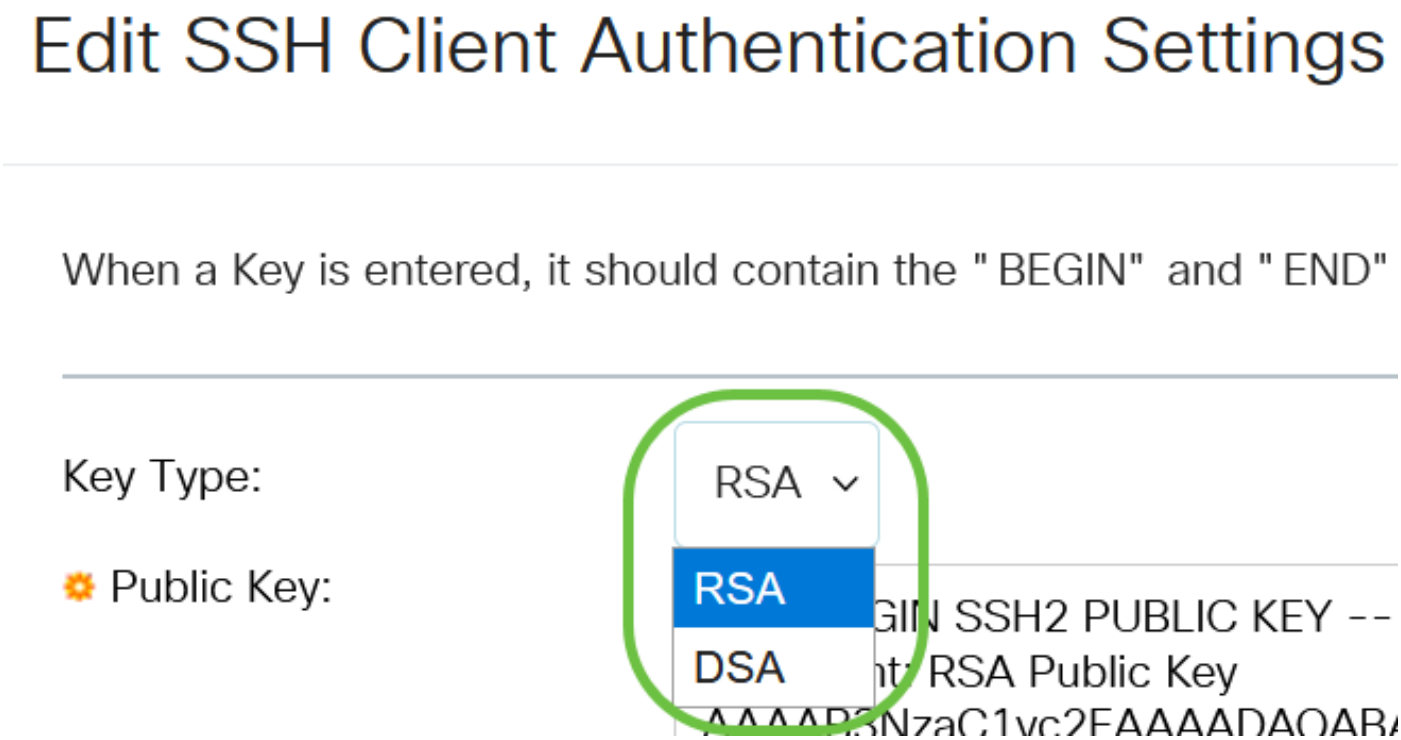
Étape 10. (Facultatif) Cliquez sur **Generate** pour générer une nouvelle clé. La nouvelle clé remplacera la clé cochée, puis cliquez sur **OK** pour continuer.



Étape 11. (Facultatif) Cliquez sur **Modifier** pour modifier une clé actuelle.

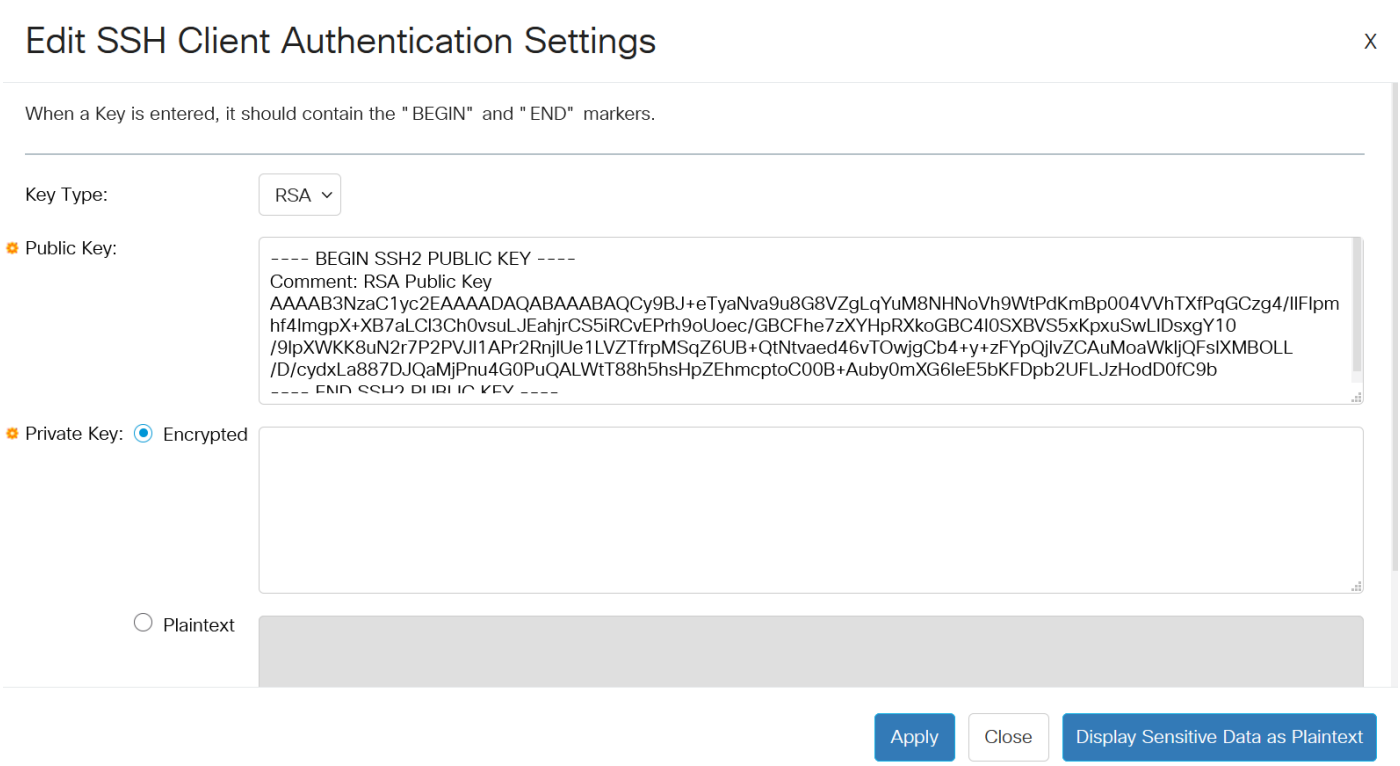


Étape 12. (Facultatif) Choisissez un type de clé dans la liste déroulante Type de clé.



Dans cet exemple, RSA est choisi.

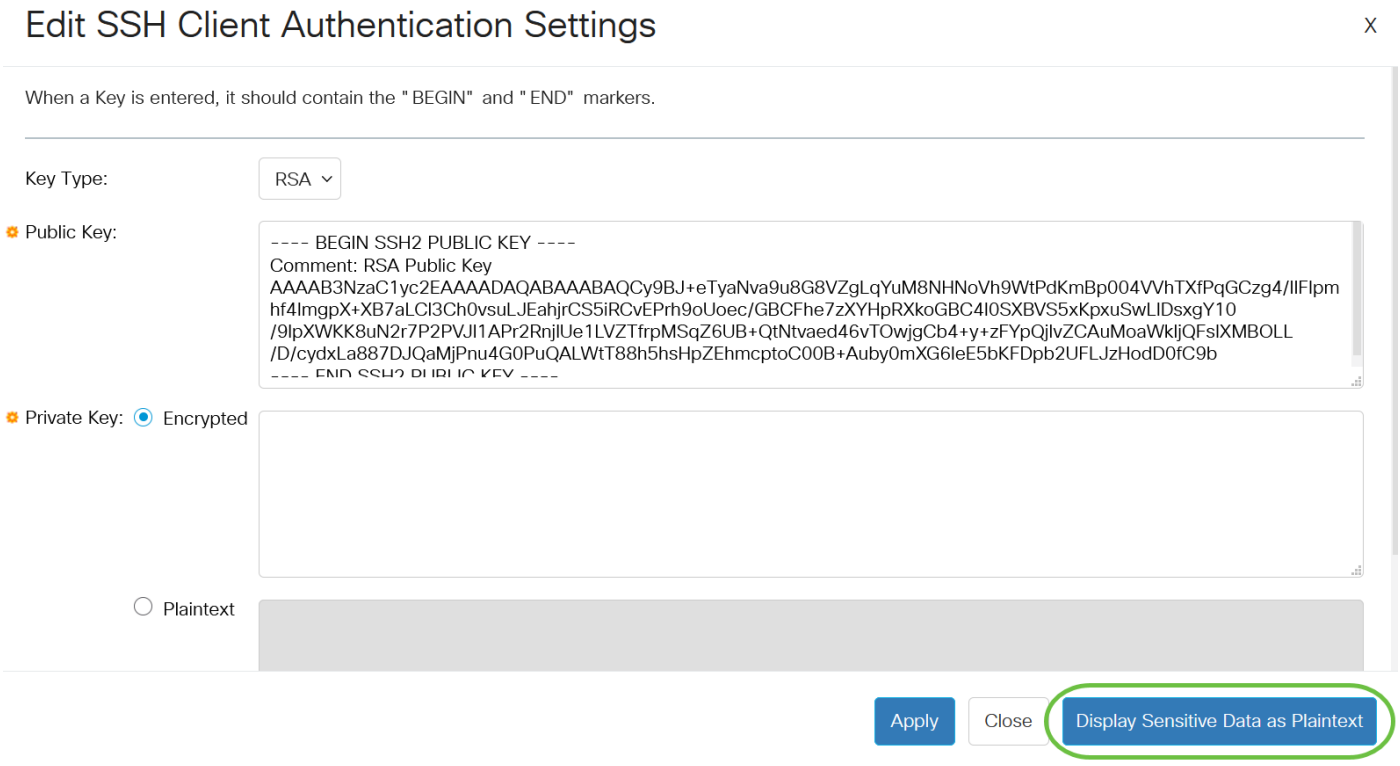
Étape 13. (Facultatif) Saisissez la nouvelle clé publique dans le champ *Clé publique*.

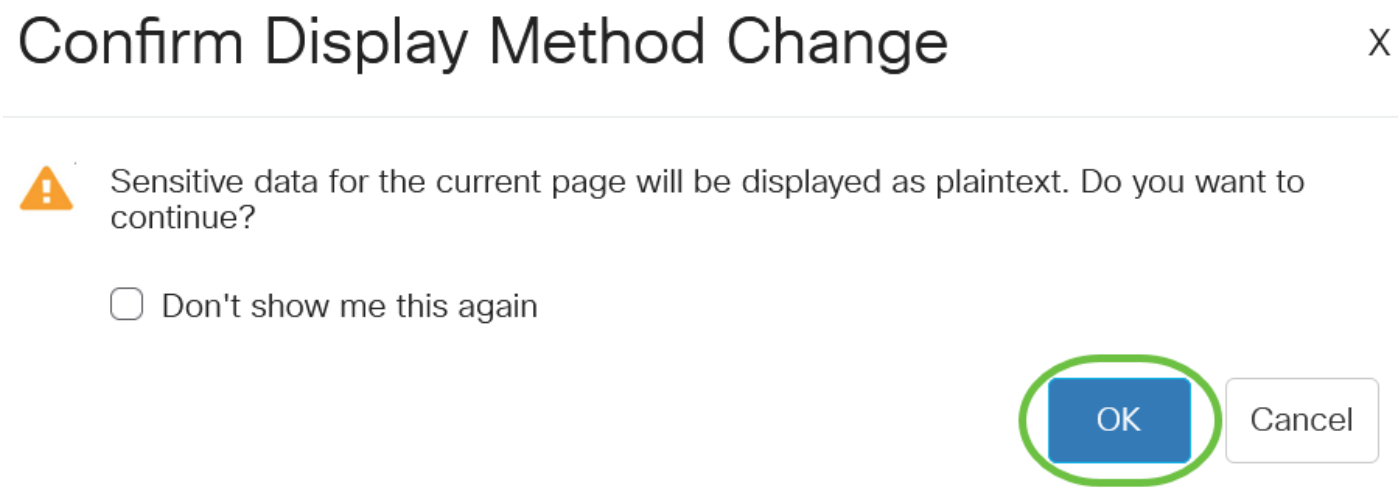


Étape 14. (Facultatif) Saisissez la nouvelle clé privée dans le champ *Private Key*.

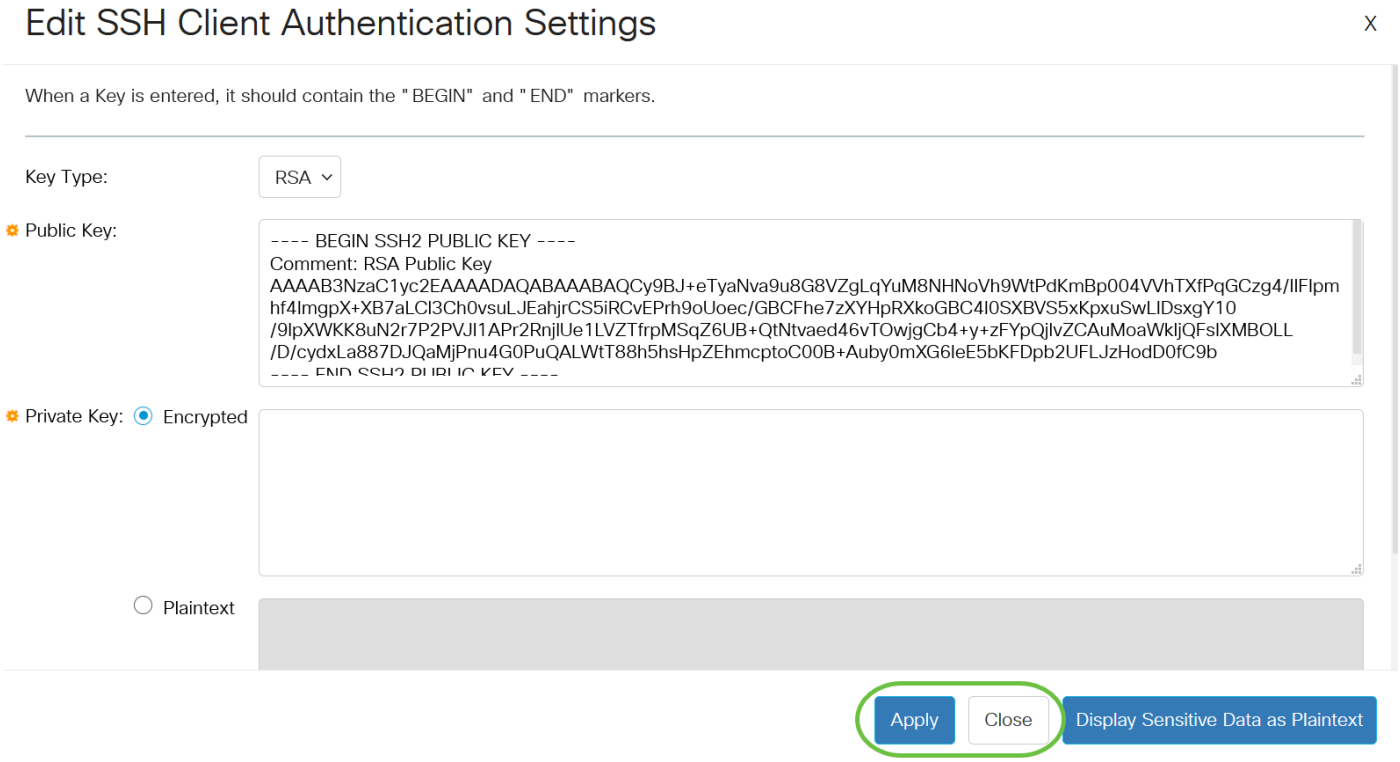
Vous pouvez modifier la clé privée et cliquer sur Chiffré pour afficher la clé privée actuelle en tant que texte chiffré, ou en texte clair pour afficher la clé privée actuelle en texte clair.

Étape 15. (Facultatif) Cliquez sur **Afficher les données sensibles en texte clair** pour afficher les données chiffrées de la page en format texte brut, puis cliquez sur **OK** pour continuer.

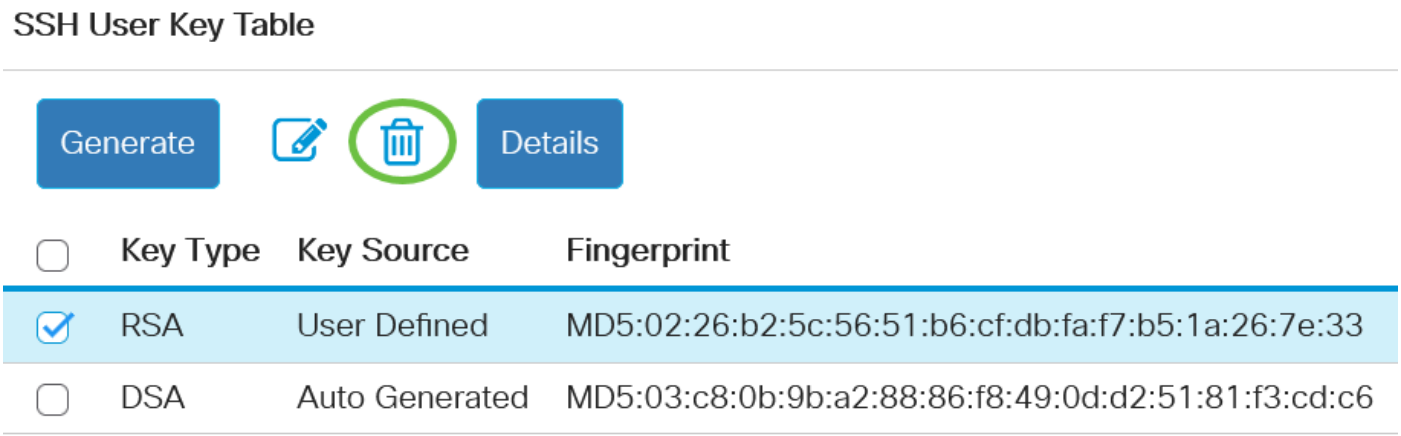




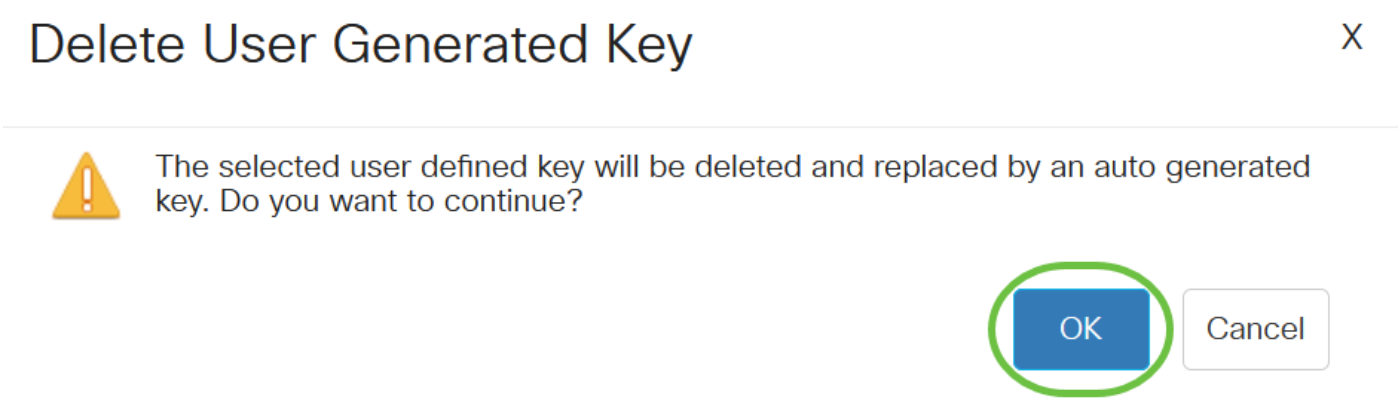
Étape 16. Cliquez sur **Apply** pour enregistrer vos modifications, puis cliquez sur **Close**.



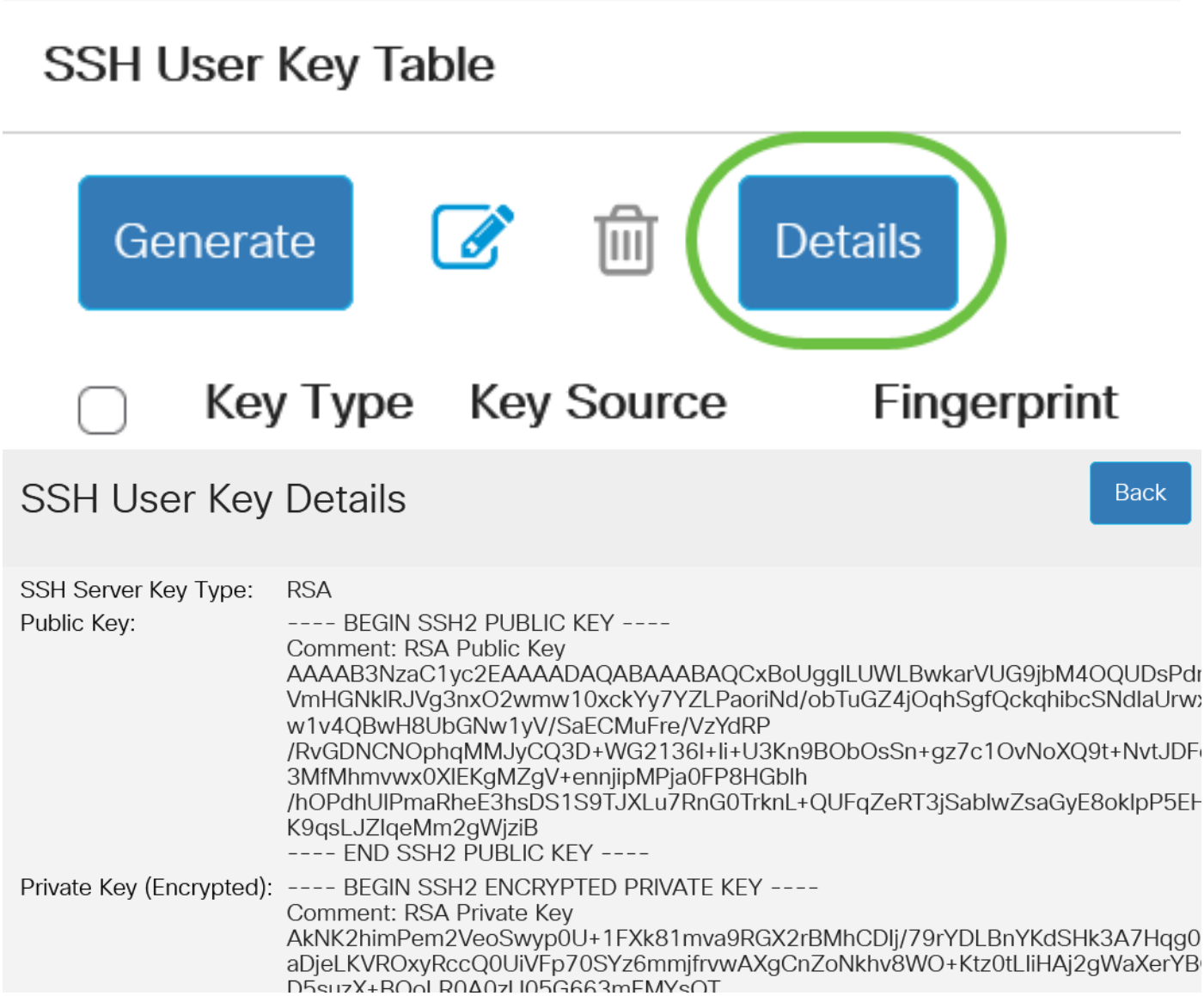
Étape 17. (Facultatif) Cliquez sur **Supprimer** pour supprimer la clé cochée.



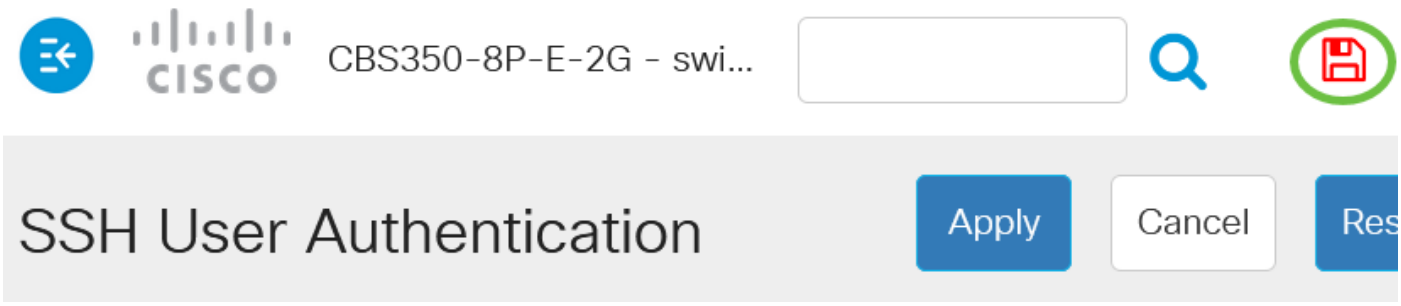
Étape 18. (Facultatif) Lorsque vous y êtes invité par un message de confirmation comme indiqué ci-dessous, cliquez sur **OK** pour supprimer la clé.



Étape 19. (Facultatif) Cliquez sur **Détails** pour afficher les détails de la clé cochée.



Étape 20. (Facultatif) Cliquez sur le bouton **Enregistrer** dans la partie supérieure de la page pour enregistrer les modifications apportées au fichier de configuration initiale.



Vous avez maintenant configuré les paramètres d'authentification des utilisateurs clients sur votre commutateur de la gamme Cisco Business 350.