Authentification utilisateur SSH (Client Secure Shell) pour les commutateurs SG350XG et SG550XG

Objectif

Secure Shell (SSH) est un protocole qui fournit une connexion à distance sécurisée à un périphérique spécifique. Les commutateurs gérés des gammes 350XG et 550XG vous permettent d'authentifier et de gérer les utilisateurs pour qu'ils se connectent au périphérique via SSH. L'authentification se produit via une clé publique, de sorte que l'utilisateur peut utiliser cette clé pour établir une connexion SSH à un périphérique spécifique. Les connexions SSH sont utiles pour dépanner un réseau à distance, dans le cas où l'administrateur réseau ne se trouve pas sur le site réseau.

Cet article explique comment configurer l'authentification des utilisateurs clients sur les commutateurs gérés SG350XG et SG550XG.

Périphériques pertinents

- SG350XG
- SG550XG

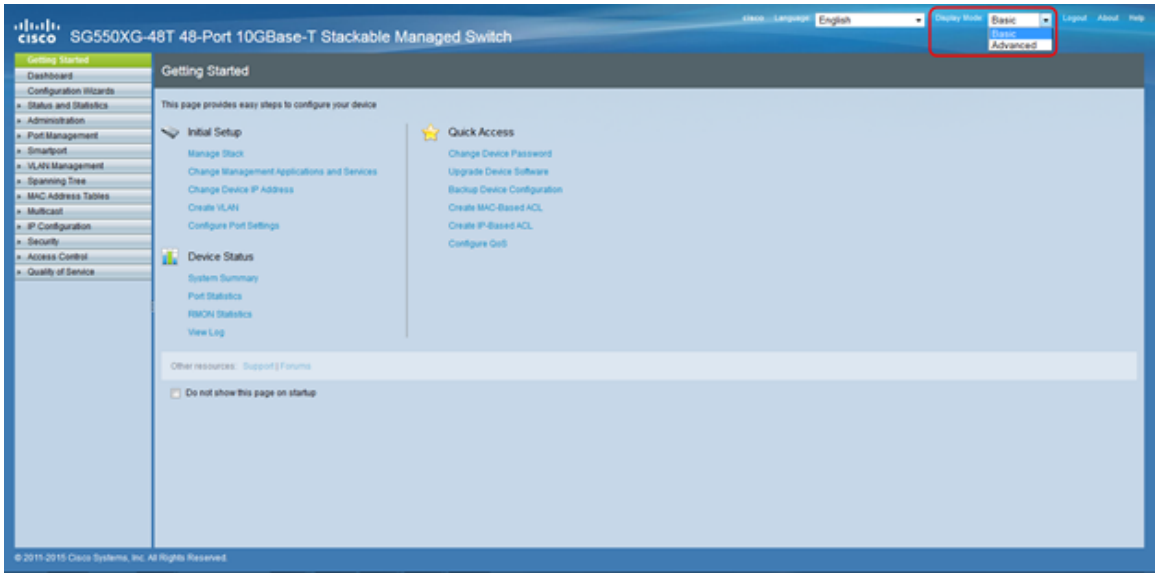
Version du logiciel

- v 2.0.0.73

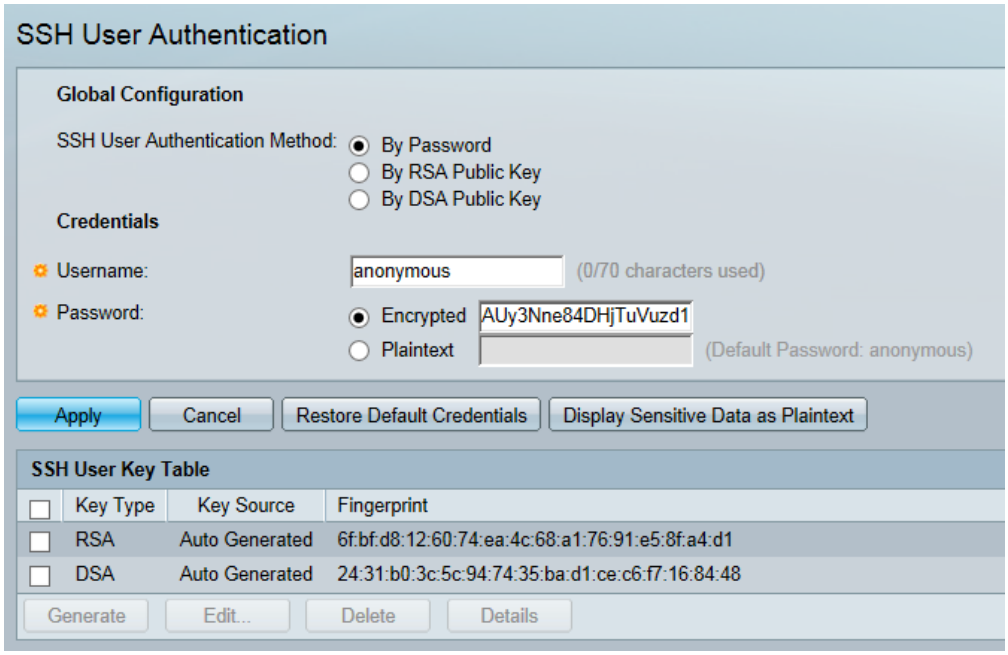
Configurer SSH Client Authentification

Configuration globale

Note: Les captures d'écran suivantes proviennent de l'affichage avancé. Vous pouvez basculer en cliquant sur la liste déroulante *Mode d'affichage* située en haut à droite de l'écran



Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez **Security > SSH Client > SSH User Authentication**. La page *Authentification utilisateur SSH* s'ouvre :



Étape 2. Dans le champ *SSH User Authentication Method*, cliquez sur la case d'option correspondant à la méthode d'authentification globale souhaitée.

Les options disponibles sont les suivantes :

- Par mot de passe : cette option vous permet de configurer un mot de passe pour l'authentification des utilisateurs. Entrez un mot de passe ou conservez le ” anonyme par défaut “.
- Par clé publique RSA : cette option vous permet d'utiliser une clé publique RSA pour l'authentification des utilisateurs. RSA est utilisé pour le chiffrement et la signature. Si cette option est sélectionnée, créez une clé publique et privée RSA dans le bloc de la table des clés 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. DSA est utilisé uniquement pour la signature. Si cette option est sélectionnée, créez une clé publique/privée DSA dans le bloc de la table des clés utilisateur SSH.

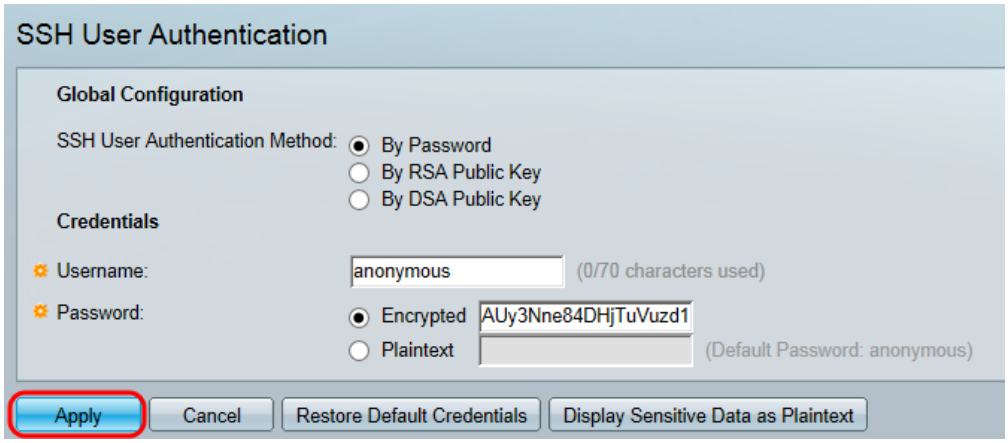
Étape 3. Recherchez la zone *Informations d'identification*. Dans le champ *Nom d'utilisateur*, saisissez le nom d'utilisateur.

Étape 4. Si **Par mot de passe** a été sélectionné à l'étape 2, cliquez sur la case d'option correspondant à la méthode de mot de passe souhaitée dans le champ *Mot de passe*. Le mot de passe par défaut est “ anonyme ”.

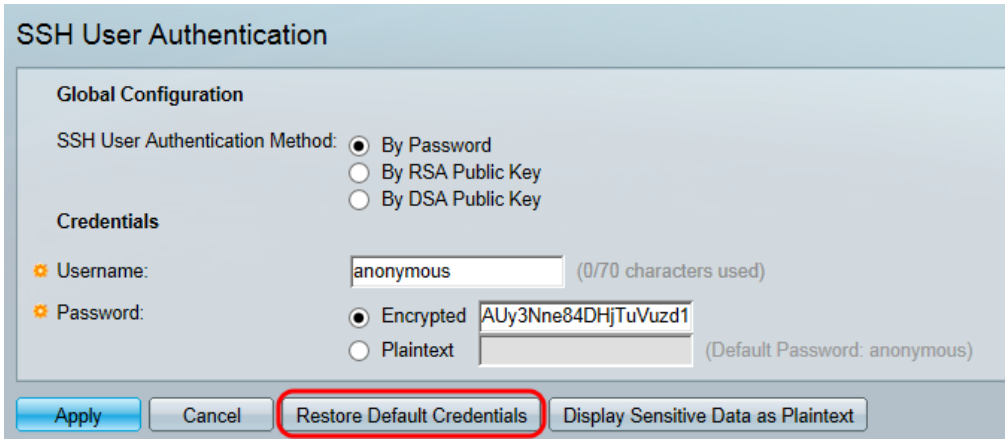
Les options disponibles sont décrites comme suit :

- Encrypted : saisissez un mot de passe chiffré.
- Texte clair : saisissez un mot de passe en texte brut.

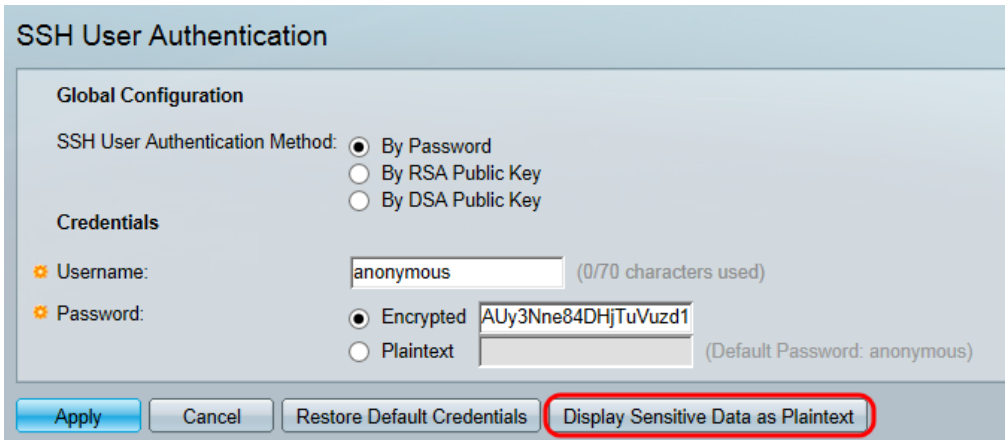
Étape 5. Cliquez sur **Apply** pour enregistrer la configuration d'authentification.



Étape 6. (Facultatif) Pour restaurer le nom d'utilisateur et le mot de passe par défaut, cliquez sur **Restaurer les informations d'identification par défaut**. Le mot de passe par défaut est “ anonyme ”.



Étape 7. (Facultatif) Pour afficher les données sensibles en texte clair ou en texte chiffré, cliquez sur **Afficher les données sensibles en texte clair/chiffré.**

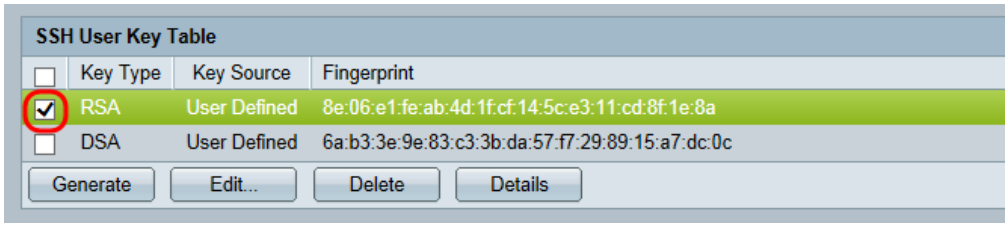


Note: Le nom du bouton change en fonction du paramètre actuel. Le bouton bascule toujours sur l'affichage des données.

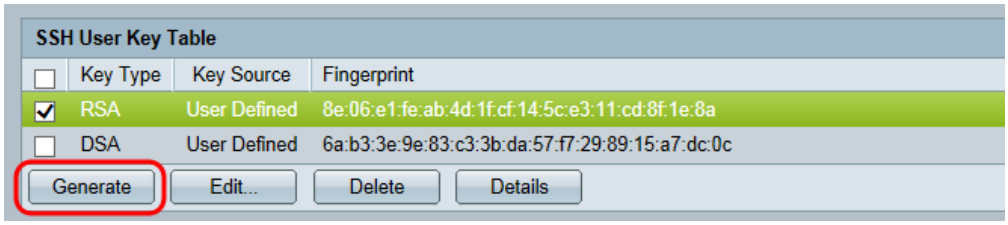
Table des clés utilisateur SSH

Cette section explique comment gérer la table d'utilisateurs SSH.

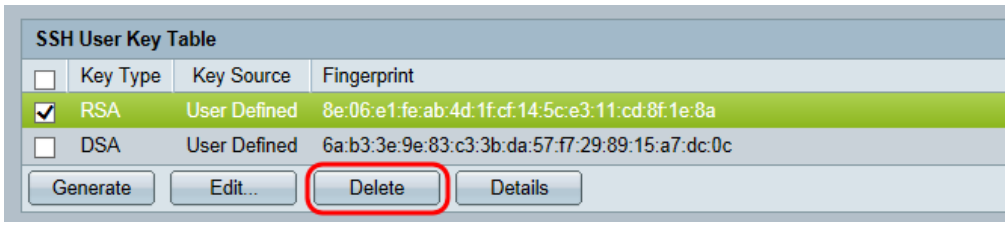
Étape 1. Accédez à la *table de clés utilisateur SSH*. Dans la liste affichée, cochez la ou les cases laissées à la clé que vous souhaitez gérer.



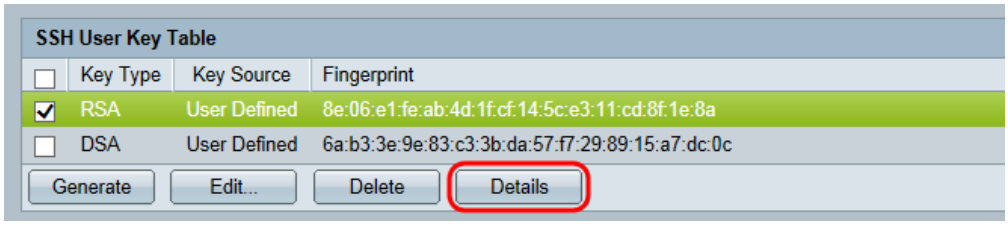
Étape 2. (Facultatif) Cliquez sur **Generate** pour générer une nouvelle clé. La nouvelle clé remplace la clé sélectionnée. Une fenêtre de confirmation s'affiche. Cliquez sur **OK** pour continuer.



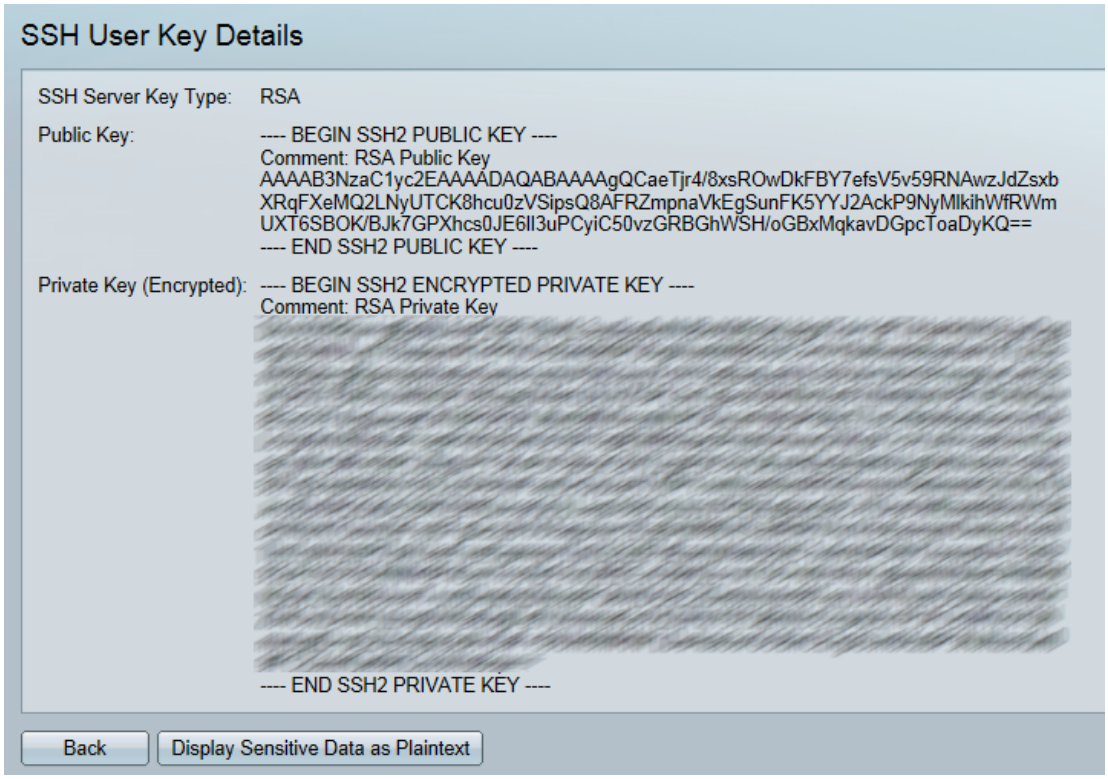
Étape 3. (Facultatif) Cliquez sur **Supprimer** pour supprimer la clé sélectionnée. Une fenêtre de confirmation s'affiche. Cliquez sur **OK** pour continuer.



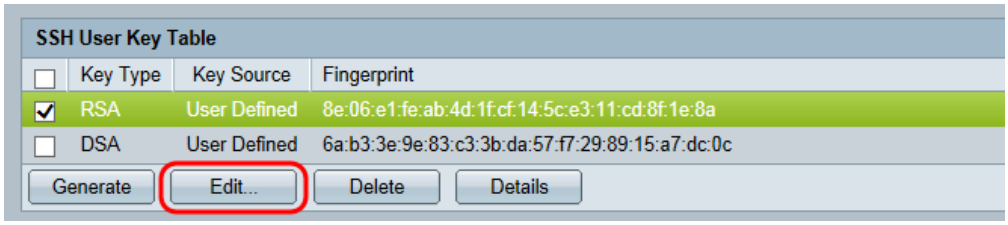
Étape 4. (Facultatif) Cliquez sur **Détails** pour afficher les détails de la clé sélectionnée.



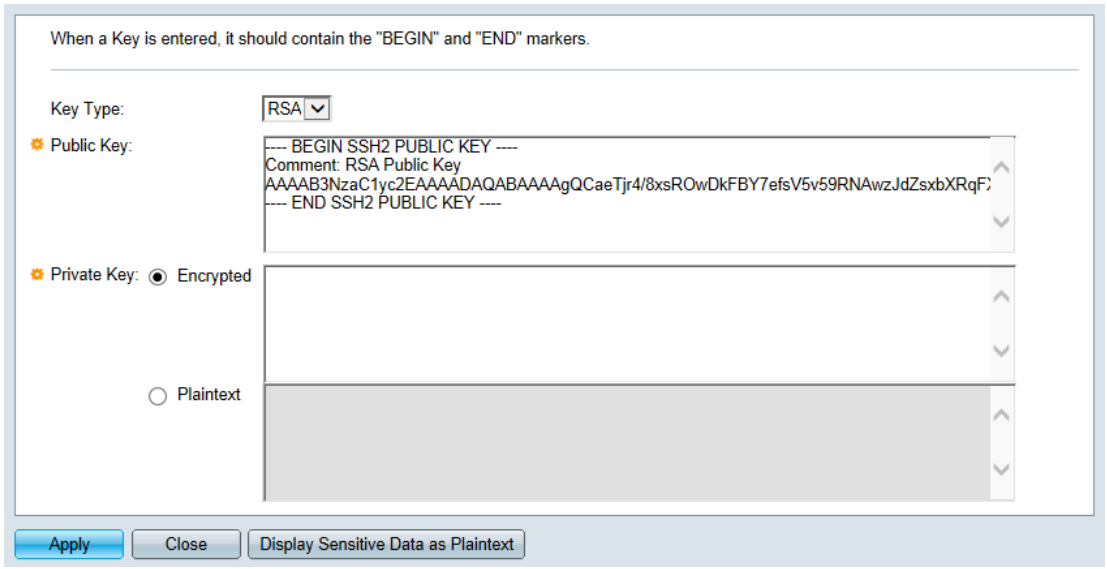
La page Détails de la clé utilisateur SSH s'affiche. Cliquez sur **Précédent** pour revenir à la table des clés utilisateur SSH.



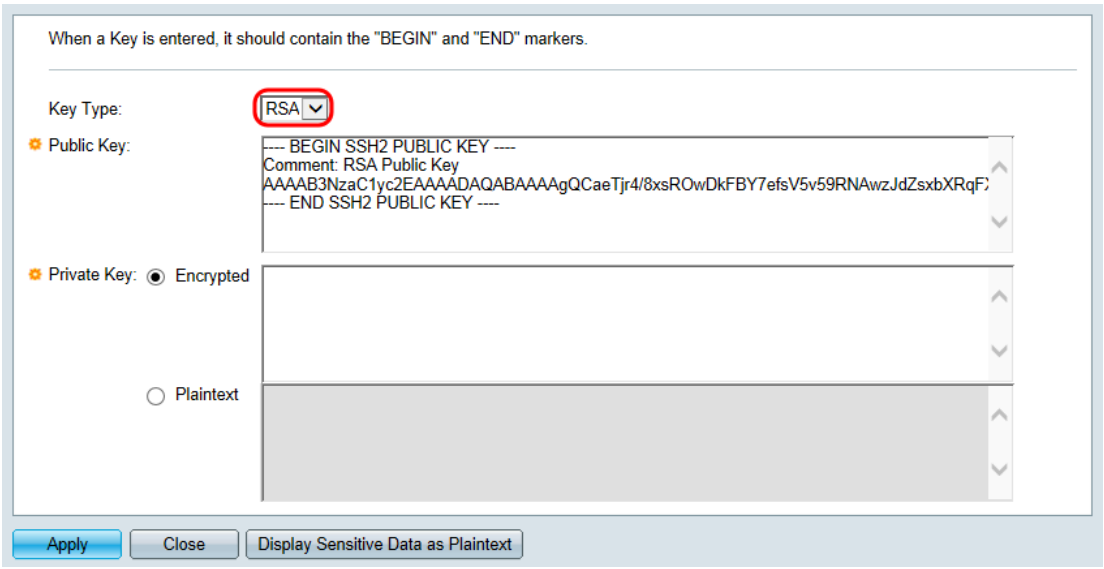
Étape 5. Cliquez sur **Modifier** pour modifier la clé choisie.



La fenêtre *Edit SSH Client Authentication Settings* s'ouvre :



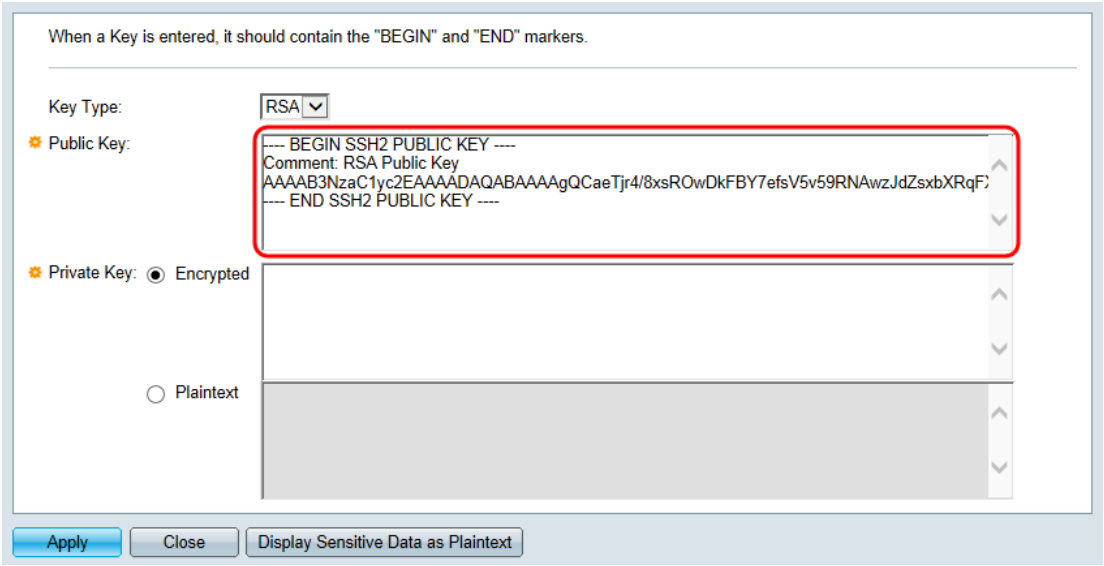
Étape 6. Sélectionnez le type de clé souhaité dans la liste déroulante *Type de clé*.



Les options disponibles sont les suivantes :

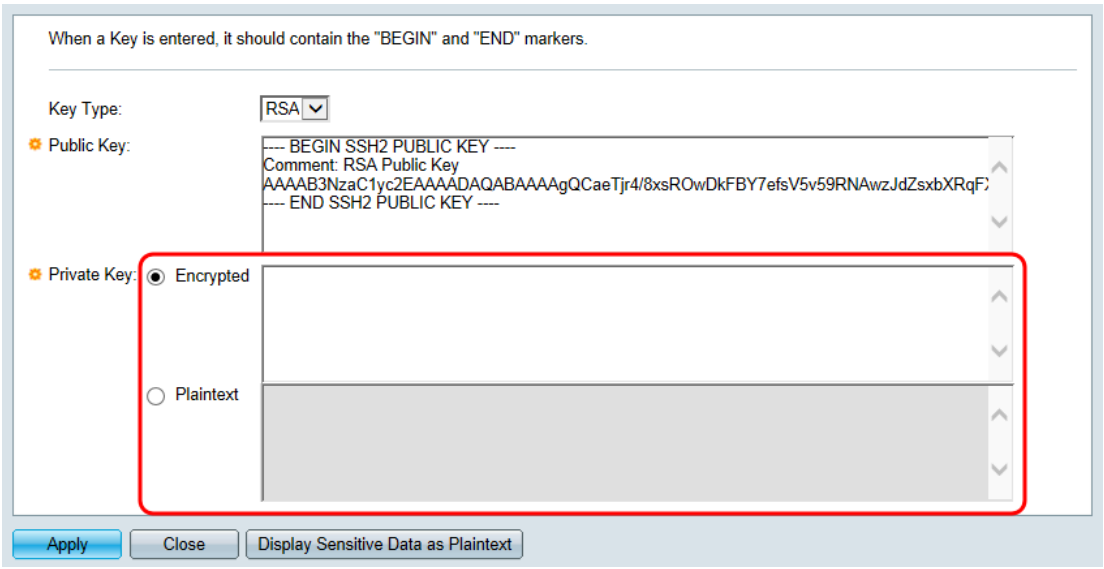
- RSA : RSA est utilisé pour le chiffrement et la signature.
- DSA - DSA est utilisé uniquement pour la signature.

Étape 7. Dans le champ *Clé publique*, vous pouvez modifier la clé publique actuelle.



Étape 8. Dans le champ *Clé privée*, vous pouvez modifier la clé privée actuelle. Cliquez sur le bouton

Bouton d'option **chiffré** pour voir la clé privée actuelle comme chiffrée. Sinon, cliquez sur la case d'option **Texte clair** pour afficher la clé privée actuelle en texte brut.



Étape 9. Cliquez sur **apply** pour enregistrer vos modifications.