

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

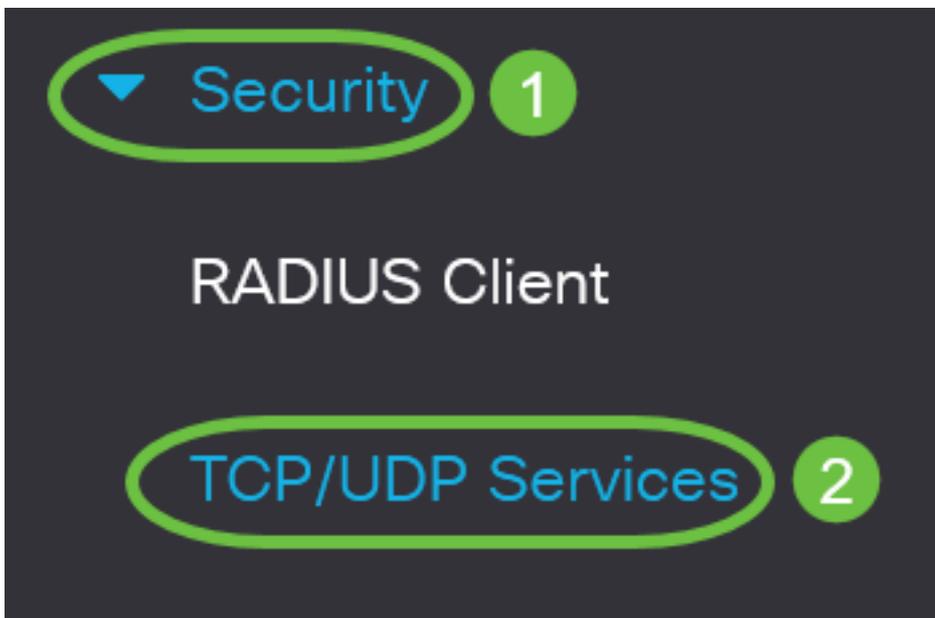
- CBS350 ([fiche technique](#)) | 3.0.0.69 ([Télécharger la dernière version](#))
- CBS350-2X ([fiche technique](#)) | 3.0.0.69 ([Télécharger la dernière version](#))
- CBS350-4X ([fiche technique](#)) | 3.0.0.69 ([Télécharger la dernière version](#))

Configuration des paramètres d'authentification utilisateur du client SSH

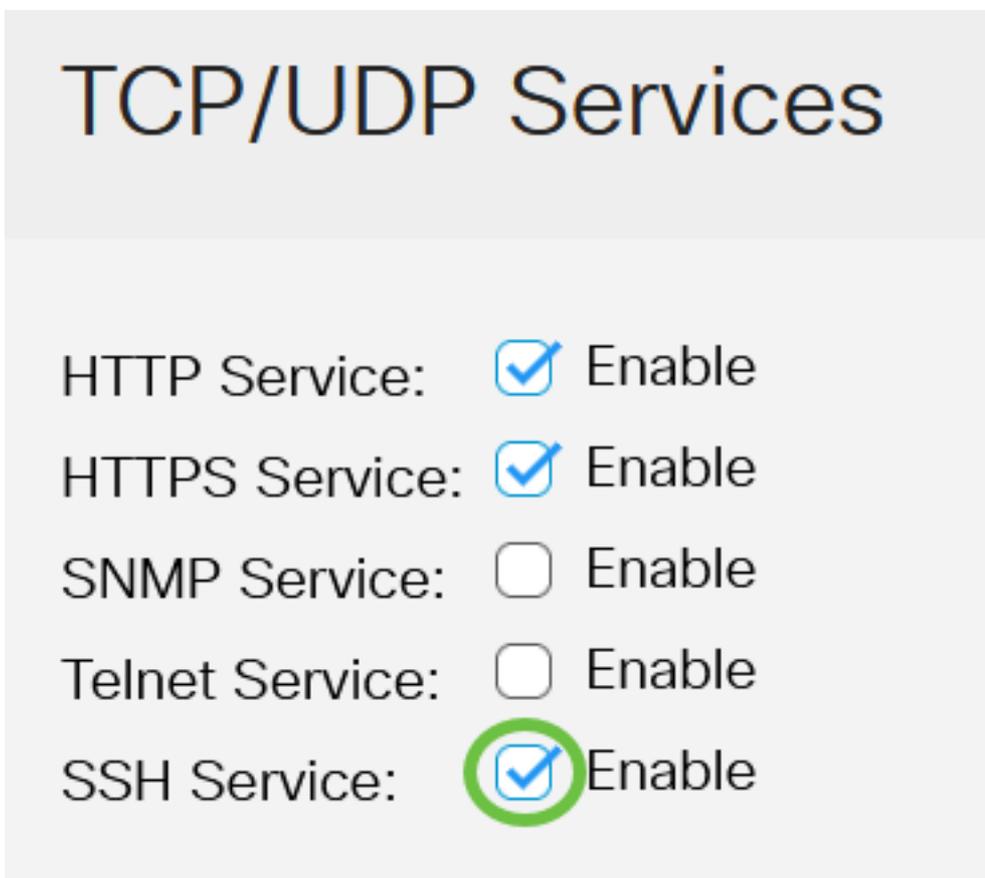
Activer le service SSH

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.

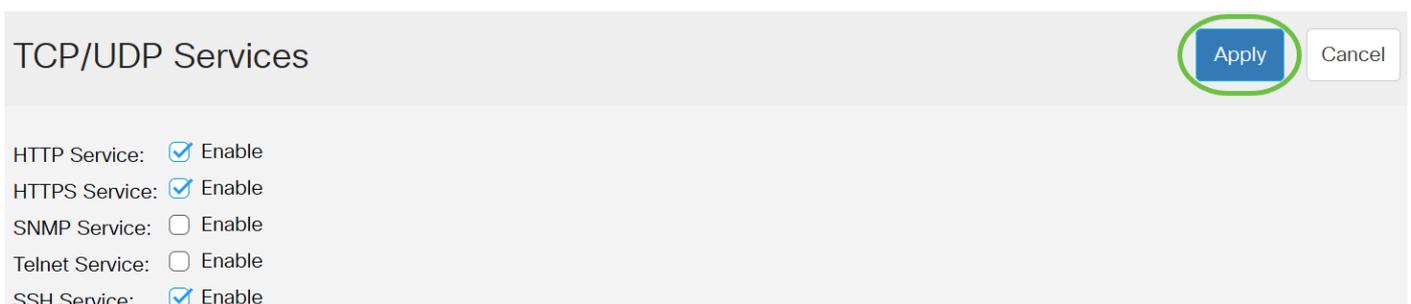
Étape 1. Connectez-vous à l'utilitaire Web et choisissez **Security > TCP/UDP Services**



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.

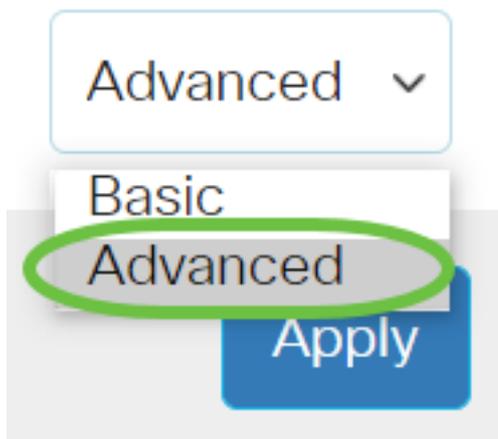


Configuration des paramètres d'authentification utilisateur SSH

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

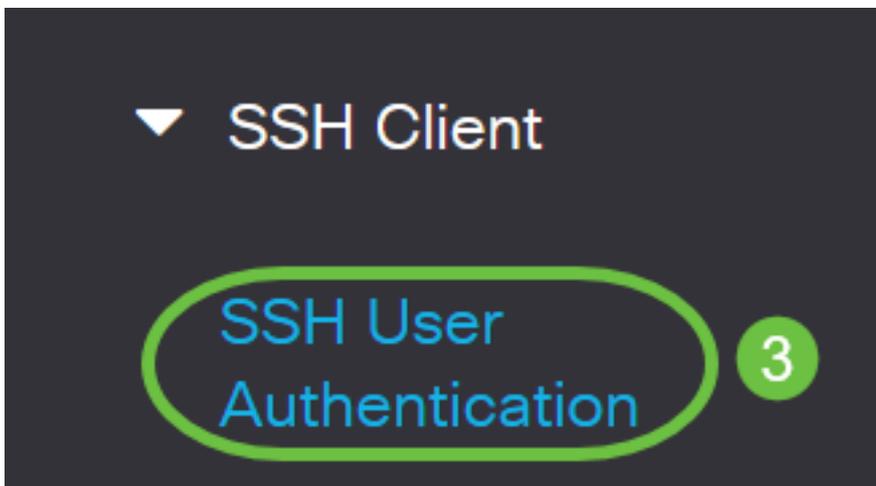
▶ Mgmt Access Method

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.

Global Configuration

SSH User Authentication Method: By Password
 By RSA Public Key
 By DSA Public Key

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*.

Credentials

✱ Username: (12/70 characters used)

✱ Password: Encrypted

Plaintext (Default Password: anonymous)

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*.

Credentials

✱ Username: (12/70 characters used)

✱ Password: Encrypted

Plaintext (Default Password: anonymous)

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.

SSH User Authentication

By RSA Public Key

By DSA Public Key

Credentials

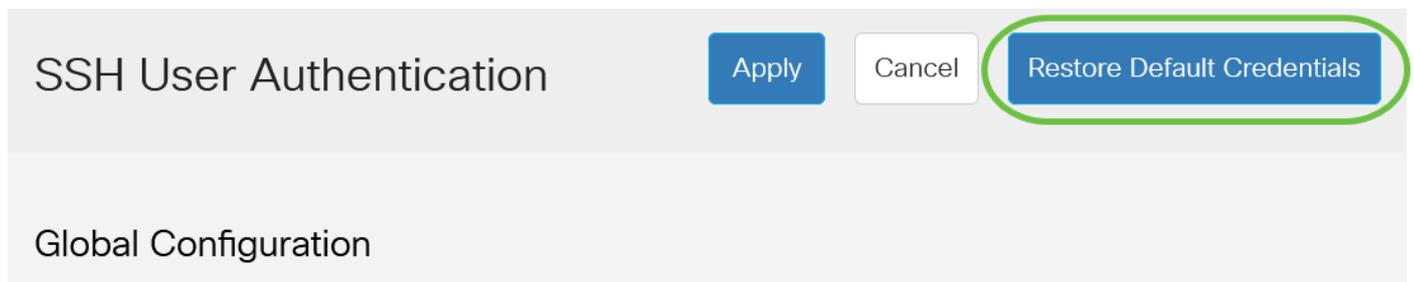
✱ Username: (12/70 ch)

✱ Password: Encrypted

Plaintext

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.



SSH User Authentication Apply Cancel Restore Default Credentials

Global Configuration

Confirm Restore Default Credentials X

 The Username and Password will be restored to the default values (anonymous/anonymous). Do you want to continue?

OK Cancel

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.



SSH User Authentication Apply Cancel Restore Default Credentials Display Sensitive Data as Plaintext

Global Configuration

Confirm Display Method Change X

 Sensitive data for the current page will be displayed as plaintext. Your HTTP web session is insecure. Do you want to continue?

OK Cancel

Configurer la table des clés utilisateur SSH

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

SSH User Key Table

Generate   Details

<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	Auto Generated	MD5:c0:b4:8a:25:26:52:56:8f:4e:f5:a4:fa:a7:cc:0a:b2
<input type="checkbox"/>	DSA	Auto Generated	MD5:03:c8:0b:9b:a2:88:86:f8:49:0d:d2:51:81:f3:cd:c6

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.

SSH User Key Table

   Details

<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	Auto Generated	MD5:c0:b4:8a:25:26:52:56:8f:4e:f5:a4:fa:a7:cc:0a:b2
<input type="checkbox"/>	DSA	Auto Generated	MD5:03:c8:0b:9b:a2:88:86:f8:49:0d:d2:51:81:f3:cd:c6

Confirm Key Generation

X



Generating a new key will overwrite the existing key. Do you want to continue?

OK

Cancel

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

SSH User Key Table

[Generate](#)   [Details](#)

<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	Auto Generated	MD5:c0:b4:8a:25:26:52:56:8f:4e:f5:a4:fa:a7:cc:0a:b2
<input type="checkbox"/>	DSA	Auto Generated	MD5:03:c8:0b:9b:a2:88:86:f8:49:0d:d2:51:81:f3:cd:c6

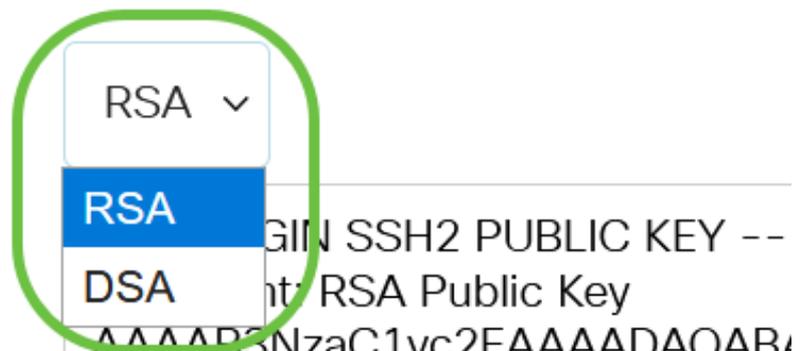
Étape 12. (Facultatif) Choisissez un type de clé dans la liste déroulante Type de clé.

Edit SSH Client Authentication Settings

When a Key is entered, it should contain the "BEGIN" and "END"

Key Type:

 Public Key:



The screenshot shows a dropdown menu for 'Key Type' with 'RSA' selected. The menu is circled in green. The background text is partially visible, showing 'BEGIN SSH2 PUBLIC KEY --' and 'RSA Public Key'.

Dans cet exemple, RSA est choisi.

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

Edit SSH Client Authentication Settings

X

When a Key is entered, it should contain the "BEGIN" and "END" markers.

Key Type:

Public Key:

```
----- BEGIN SSH2 PUBLIC KEY -----  
Comment: RSA Public Key  
AAAAB3NzaC1yc2EAAAADAQABAAQCy9BJ+eTyaNva9u8G8VZgLqYuM8NHNoVh9WtPdKmbp004VvhTXfPqGCzg4/IIFlpm  
hf4lmgpX+XB7aLCi3Ch0vsuLJEahjrCS5iRCvEPrh9oUoec/GBCFhe7zXYHpRXkoGBC4I0SXbVS5xKpxuSwLIDsxgY10  
/9lpXWKK8uN2r7P2PVJI1APr2RnjlUe1LVZTfrpMSqZ6UB+QtNtvaed46vTowjgCb4+y+zFYpQjlvZCAuMoaWkljQFslXMBOLL  
/D/cydxLa887DJQaMjPnu4G0PuQALWtT88h5hsHpZEhmcptoC00B+Auby0mXG6leE5bKFDpb2UFLJzHodD0fC9b  
----- END SSH2 PUBLIC KEY -----
```

Private Key: Encrypted

Plaintext

Apply

Close

Display Sensitive Data as Plaintext

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.

Edit SSH Client Authentication Settings

X

When a Key is entered, it should contain the "BEGIN" and "END" markers.

Key Type:

Public Key:

```
----- BEGIN SSH2 PUBLIC KEY -----  
Comment: RSA Public Key  
AAAAB3NzaC1yc2EAAAADAQABAAQCy9BJ+eTyaNva9u8G8VZgLqYuM8NHNoVh9WtPdKmbp004VvhTXfPqGCzg4/IIFlpm  
hf4lmgpX+XB7aLCi3Ch0vsuLJEahjrCS5iRCvEPrh9oUoec/GBCFhe7zXYHpRXkoGBC4I0SXbVS5xKpxuSwLIDsxgY10  
/9lpXWKK8uN2r7P2PVJI1APr2RnjlUe1LVZTfrpMSqZ6UB+QtNtvaed46vTowjgCb4+y+zFYpQjlvZCAuMoaWkljQFslXMBOLL  
/D/cydxLa887DJQaMjPnu4G0PuQALWtT88h5hsHpZEhmcptoC00B+Auby0mXG6leE5bKFDpb2UFLJzHodD0fC9b  
----- END SSH2 PUBLIC KEY -----
```

Private Key: Encrypted

Plaintext

Apply

Close

Display Sensitive Data as Plaintext

Confirm Display Method Change

X



Sensitive data for the current page will be displayed as plaintext. Do you want to continue?

Don't show me this again

OK

Cancel

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

Edit SSH Client Authentication Settings

X

When a Key is entered, it should contain the "BEGIN" and "END" markers.

Key Type:

RSA

Public Key:

```
----- BEGIN SSH2 PUBLIC KEY -----  
Comment: RSA Public Key  
AAAAB3NzaC1yc2EAAAADAQABAAQCy9BJ+eTyaNva9u8G8VZgLqYuM8NHNoVh9WtPdKmBp004VvhTXfPqGCzG4/IIFlpm  
hf4ImgpX+XB7aLCI3Ch0vsuLJEahjrCS5iRCvEPrh9oUoec/GBCFhe7zXYHpRXkoGBC4I0SXBVS5xKpxuSwLIDsxgY10  
/9lpXWKK8uN2r7P2PVJI1APr2RnjIue1LVZTfrpMSqZ6UB+QtNtvaed46vTOWjgCb4+y+zFYpQjlvZCAuMoaWkljQFsiXMBOLL  
/D/cydxLa887DJQaMjPnu4G0PuQALWtT88h5hsHpZEhmcptoC00B+Auby0mXG6leE5bKFDpb2UFLJzHodD0fC9b  
----- END SSH2 PUBLIC KEY -----
```

Private Key: Encrypted

Plaintext

Apply

Close

Display Sensitive Data as Plaintext

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

SSH User Key Table

Generate



Details



Key Type

Key Source

Fingerprint



RSA

User Defined

MD5:02:26:b2:5c:56:51:b6:cf:db:fa:f7:b5:1a:26:7e:33



DSA

Auto Generated

MD5:03:c8:0b:9b:a2:88:86:f8:49:0d:d2:51:81:f3:cd:c6

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

Delete User Generated Key

X

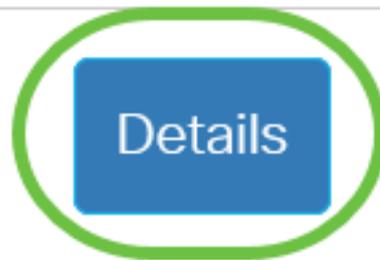


The selected user defined key will be deleted and replaced by an auto generated key. Do you want to continue?



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

SSH User Key Table



Key Type

Key Source

Fingerprint

SSH User Key Details

Back

SSH Server Key Type: RSA
Public Key: ----- BEGIN SSH2 PUBLIC KEY -----
Comment: RSA Public Key
AAAAB3NzaC1yc2EAAAADAQABAAQ=CxBoUggILUWLBwkarVUG9jbM4OQUDsPdr
VmHGNkIRJVg3nxO2wmw10xckYy7YZLPaoriNd/obTuGZ4jOqhSgfQckqhibcSNdlaUrw;
w1v4QBwH8UbGNw1yV/SaECMuFre/VzYdRP
/RvGDNCNOphqMMJyCQ3D+WG2136l+li+U3Kn9BOBoOsSn+gz7c1OvNoXQ9t+NvtJDF
3MfMhmvwx0XIEKgMZgV+ennjipMPja0FP8HGblh
/hOPdhUIPmaRheE3hsDS1S9TJXLu7RnG0TrknL+QUFqZeRT3jSablwZsaGyE8oklpP5E
K9qsLJZlqeMm2gWjziB
----- END SSH2 PUBLIC KEY -----
Private Key (Encrypted): ----- BEGIN SSH2 ENCRYPTED PRIVATE KEY -----
Comment: RSA Private Key
AkNK2himPem2VeoSwyp0U+1FXk81mva9RGX2rBMhCDlj/79rYDLBnYKdSHk3A7Hqg0
aDjeLKVROxyRccQ0UivFp70SYz6mmjfrvwAXgCnZoNkhv8WO+Ktz0tLliHAj2gWaXerYB
D5suzX+RQnl R0Δ0zI I05G663mEMVcOT

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.



CBS350-8P-E-2G - swi...



SSH User Authentication

Apply

Cancel

Res

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