Authentification SSH sur un commutateur Cisco Business 350

Objectif

Cet article explique comment configurer l'authentification du serveur sur un commutateur 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.Le commutateur agit en tant que client SSH qui fournit des fonctionnalités SSH aux utilisateurs du réseau. Le commutateur utilise un serveur SSH pour fournir des services SSH. Lorsque l'authentification du serveur SSH est désactivée, le commutateur prend n'importe quel serveur SSH comme approuvé, ce qui diminue la sécurité sur votre réseau. Si le service SSH est activé sur le commutateur, la sécurité est améliorée.

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 du serveur SSH

Activer le service SSH

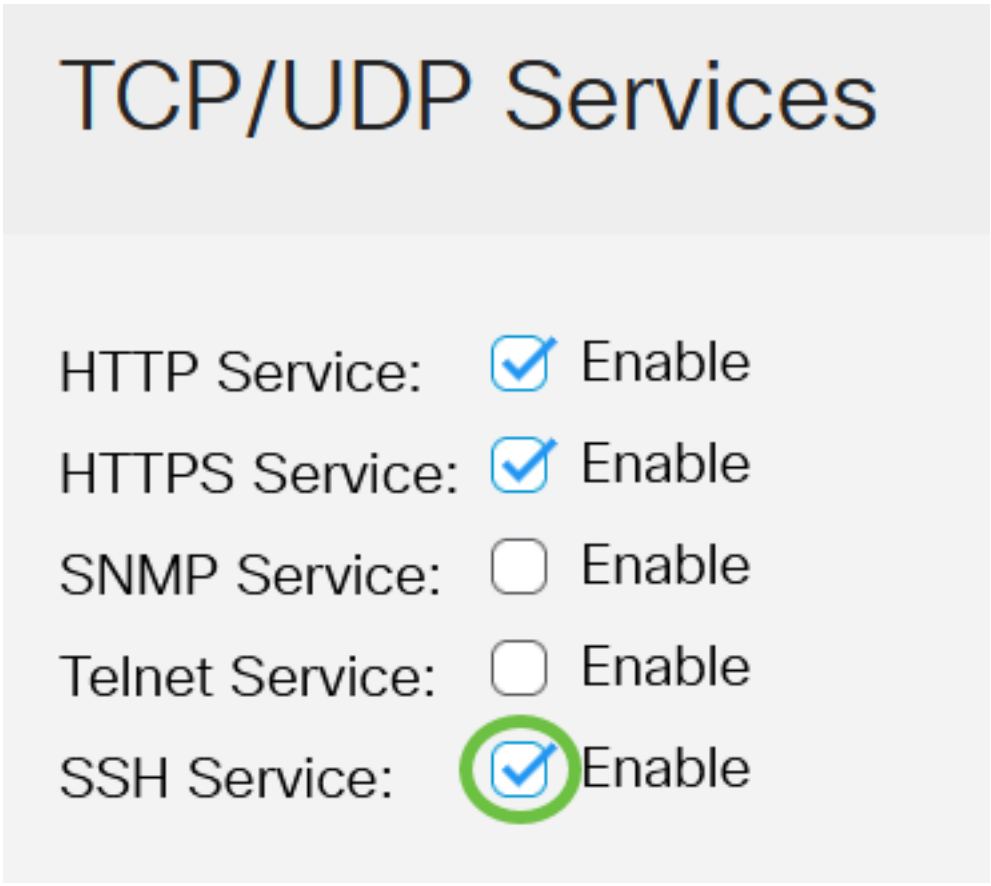
Lorsque l'authentification du serveur SSH est activée, le client SSH exécuté sur le périphérique authentifie le serveur SSH à l'aide du processus d'authentification suivant :

- Le périphérique calcule l'empreinte de la clé publique reçue du serveur SSH.
- Le périphérique recherche dans la table SSH Trusted Servers l'adresse IP et le nom d'hôte du serveur SSH. L'un des trois résultats suivants peut se produire :
    1. Si une correspondance est trouvée pour l'adresse et le nom d'hôte du serveur et son empreinte digitale, le serveur est authentifié.
    2. Si une adresse IP et un nom d'hôte correspondants sont trouvés, mais qu'il n'y a pas d'empreinte correspondante, la recherche se poursuit. Si aucune empreinte digitale correspondante n'est trouvée, la recherche est terminée et l'authentification échoue.
    3. Si aucune adresse IP et aucun nom d'hôte ne correspondent n'ont été trouvés, la recherche est terminée et l'authentification échoue.
    4. Si l'entrée du serveur SSH est introuvable dans la liste des serveurs approuvés, le processus échoue.

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

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

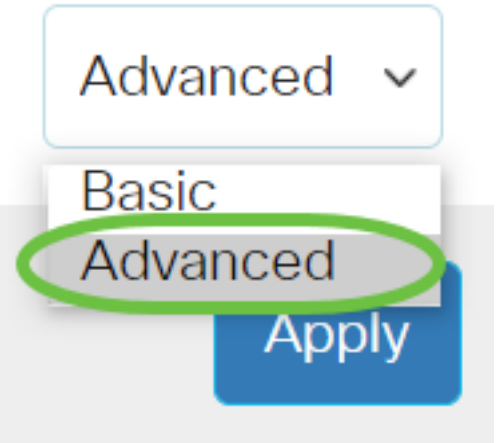
Étape 2. Cochez la case **SSH Service** pour activer l'accès de l'invite de commande des commutateurs via SSH.



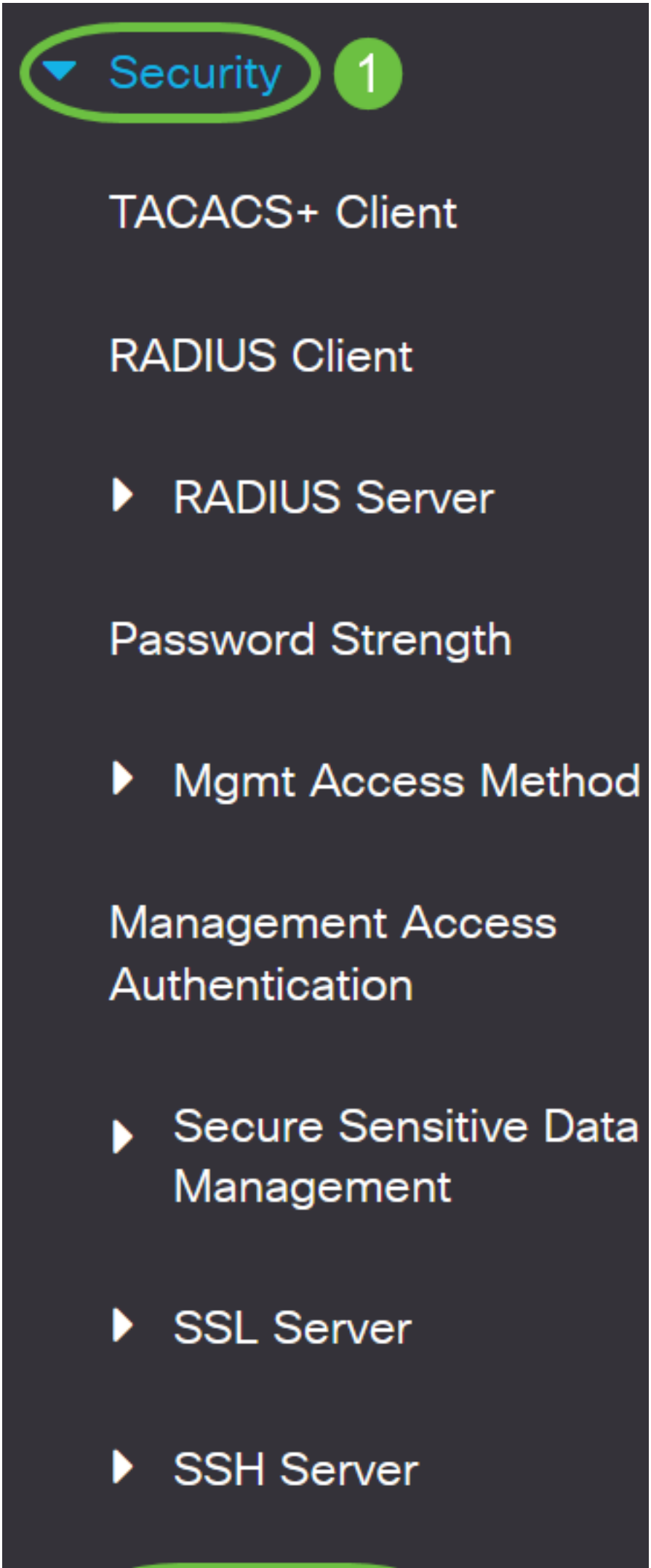
Étape 3. Cliquez sur **Apply** pour activer le service SSH.

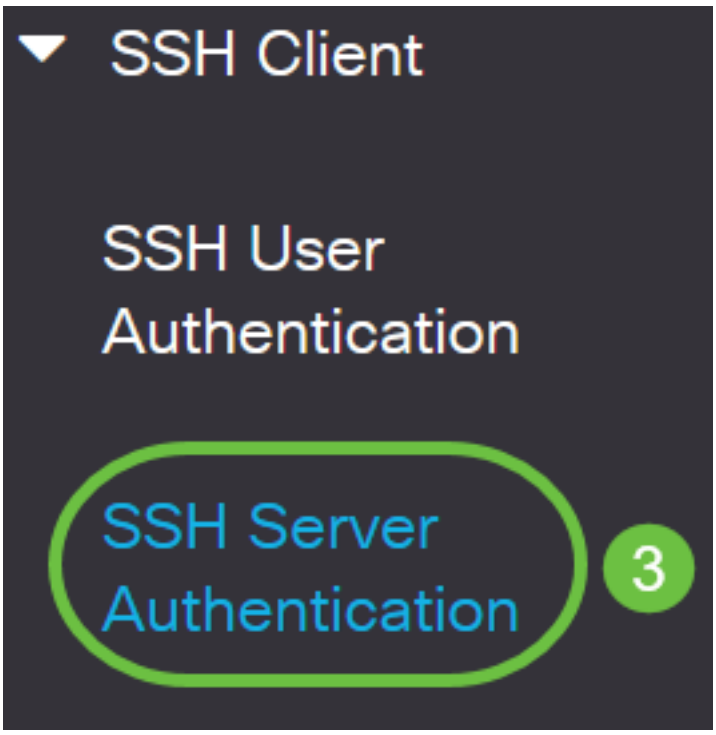
Configuration des paramètres d'authentification du serveur SSH

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

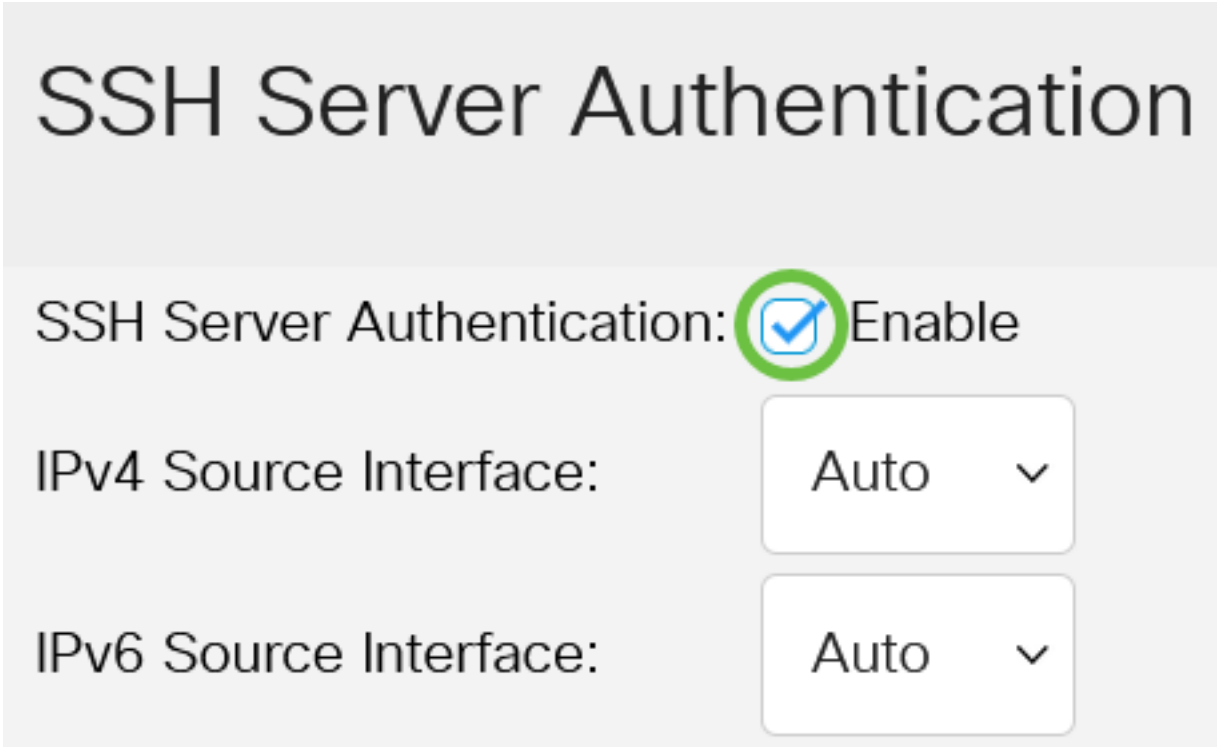


Étape 2. Choisissez **Security > SSH Client > SSH Server Authentication**.

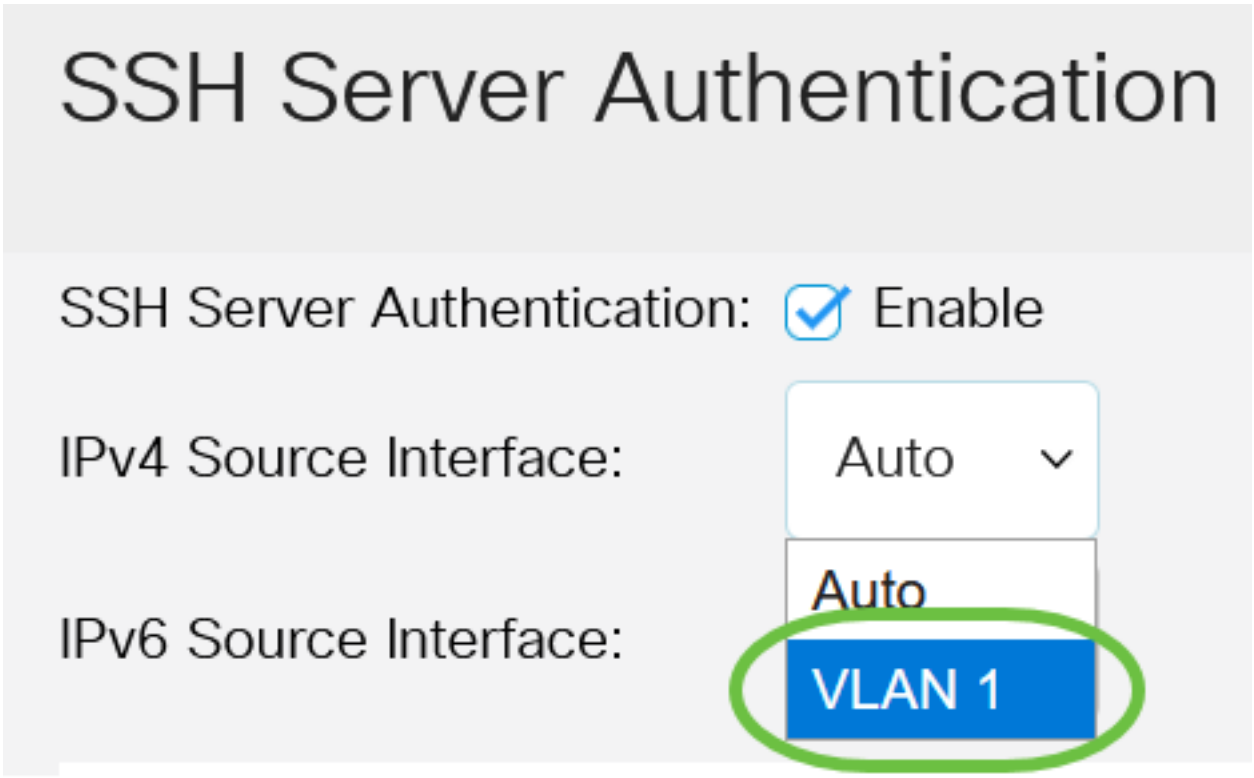

Security
1
TACACS+ Client
RADIUS Client
RADIUS Server
Password Strength
Mgmt Access Method
Management Access Authentication
Secure Sensitive Data Management
SSL Server
SSH Server



Étape 2. Cochez la case **Enable** SSH Server Authentication pour activer l'authentification du serveur SSH.

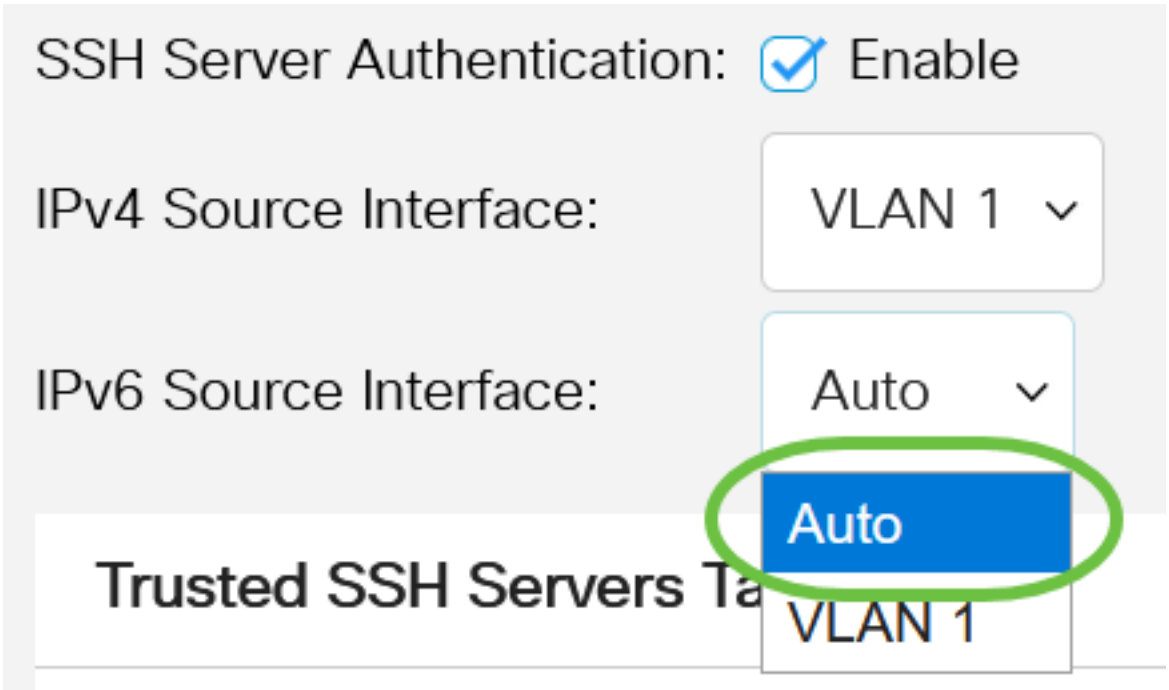


Étape 3. (Facultatif) Dans la liste déroulante IPv4 Source Interface, sélectionnez l'interface source dont l'adresse IPv4 sera utilisée comme adresse IPv4 source pour les messages utilisés dans la communication avec les serveurs SSH IPv4.



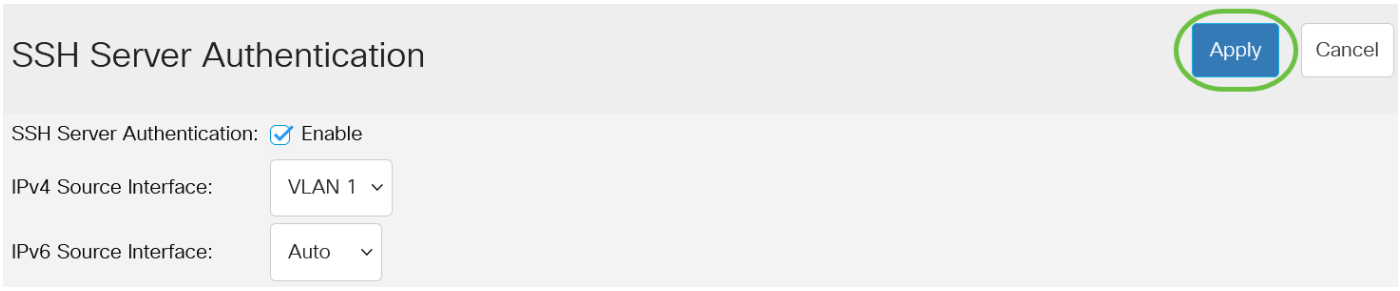
Si l'option Auto est sélectionnée, le système prend l'adresse IP source à partir de l'adresse IP définie sur l'interface sortante. Dans cet exemple, VLAN1 est sélectionné.

Étape 4. (Facultatif) Dans la liste déroulante IPv6 Source Interface, sélectionnez l'interface source dont l'adresse IPv6 sera utilisée comme adresse IPv6 source pour les messages utilisés dans la communication avec les serveurs SSH IPv6.

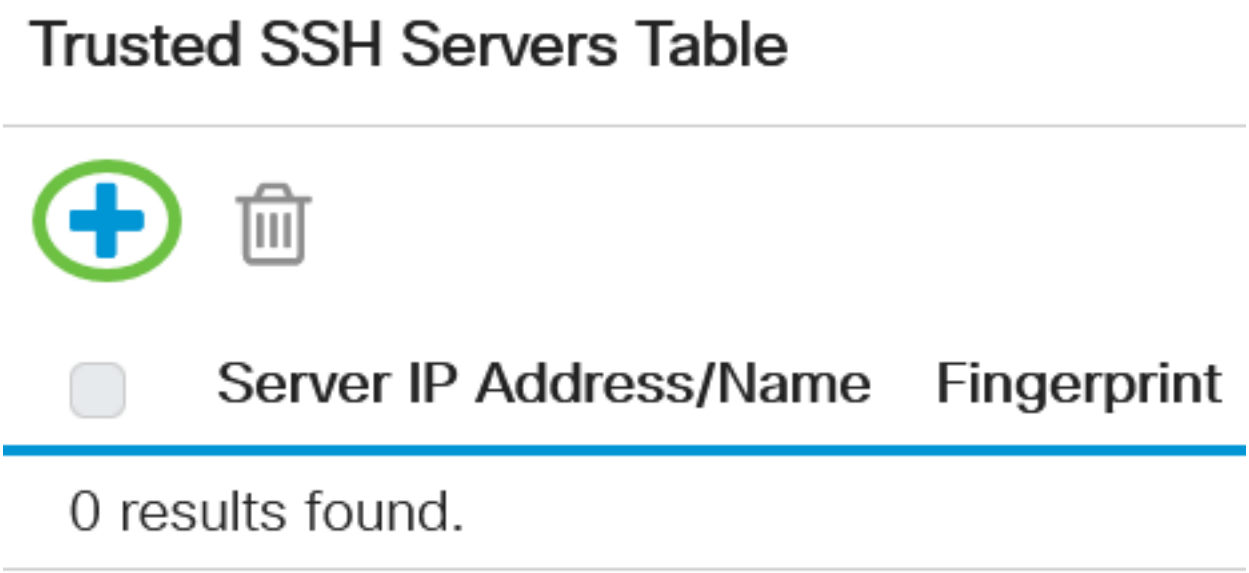


Dans cet exemple, l'option Auto est sélectionnée. Le système prend l'adresse IP source à partir de l'adresse IP définie sur l'interface sortante.

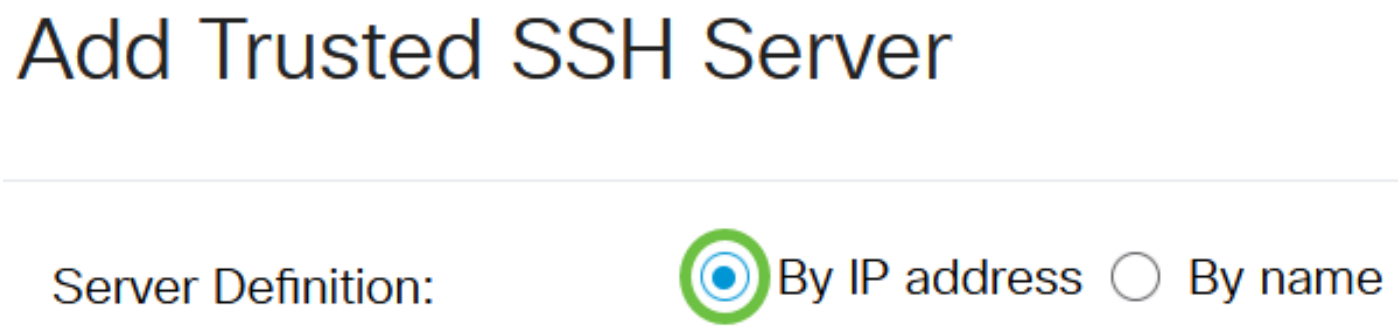
Étape 5. Cliquez sur Apply.



Étape 6. Pour ajouter un serveur approuvé, cliquez sur **Ajouter** sous la table Serveurs SSH approuvés.



Étape 7. Dans la zone Server Definition, cliquez sur l'une des méthodes disponibles pour définir le serveur SSH.

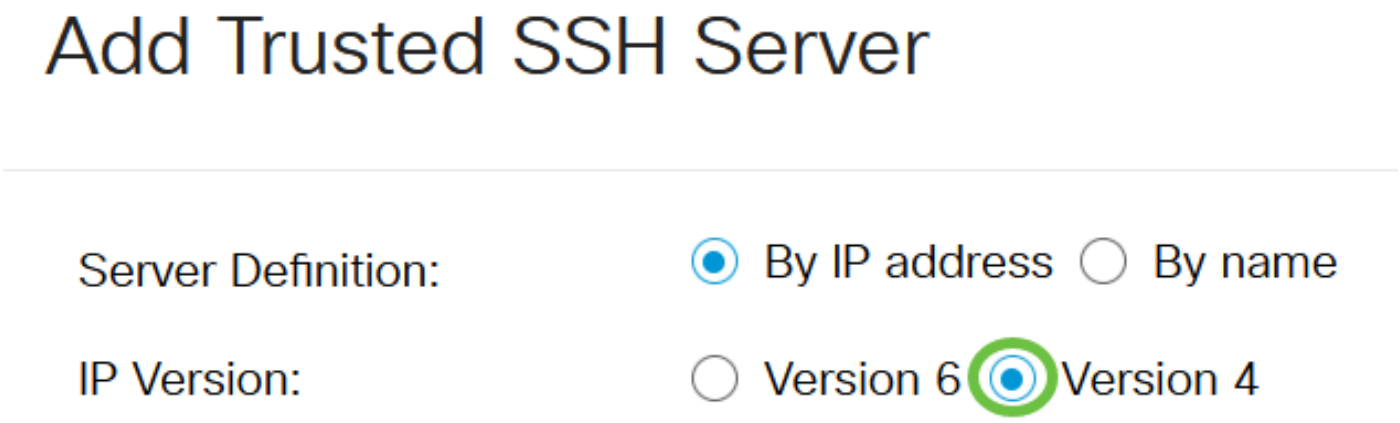


Les options sont les suivantes :

- Par adresse IP : cette option vous permet de définir le serveur SSH avec une adresse IP.
- Par nom : cette option vous permet de définir le serveur SSH avec un nom de domaine complet.

Dans cet exemple, l'option Par adresse IP est sélectionnée. Si Par nom est sélectionné, passez à l'étape 11.

Étape 8. (Facultatif) Si vous avez sélectionné Par adresse IP à l'étape 6, cliquez sur la version IP du serveur SSH dans le champ IP Version.

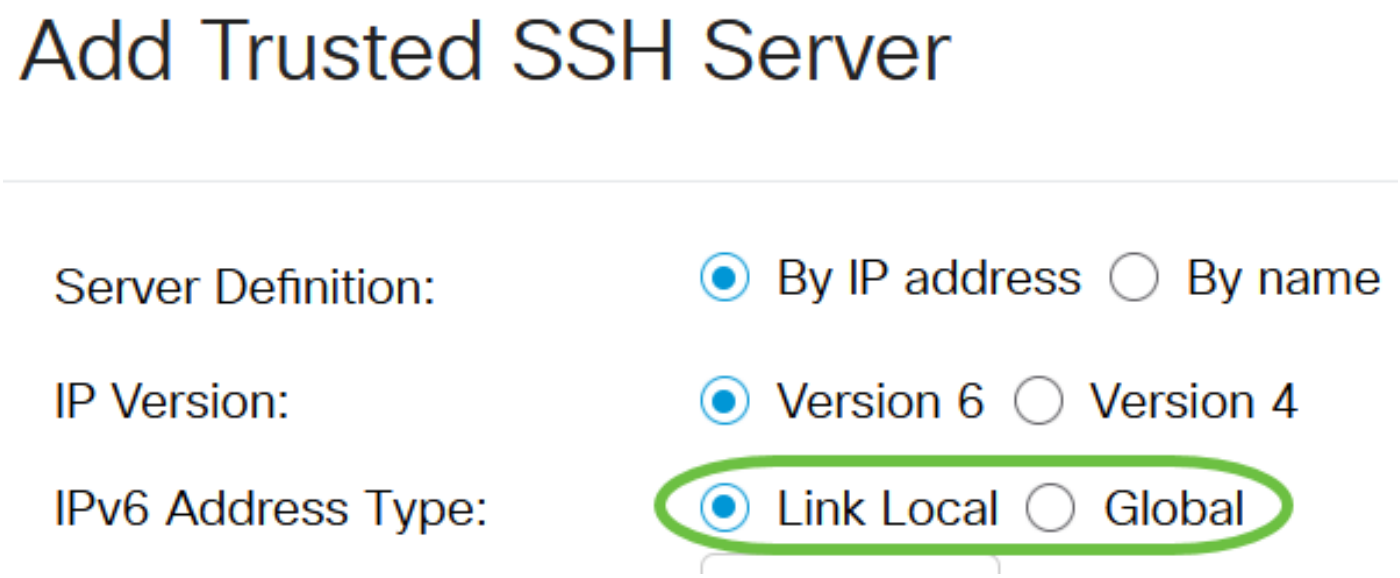


Les options disponibles sont les suivantes :

- Version 6 : cette option vous permet de saisir une adresse IPv6.
- Version 4 : cette option vous permet de saisir une adresse IPv4.

Dans cet exemple, la version 4 est choisie. La case d'option IPv6 n'est disponible que si une adresse IPv6 est configurée dans le commutateur.

Étape 9. (Facultatif) Si vous avez choisi la version 6 comme version d'adresse IP à l'étape 7, cliquez sur le type de l'adresse IPv6 dans le type d'adresse IPv6.

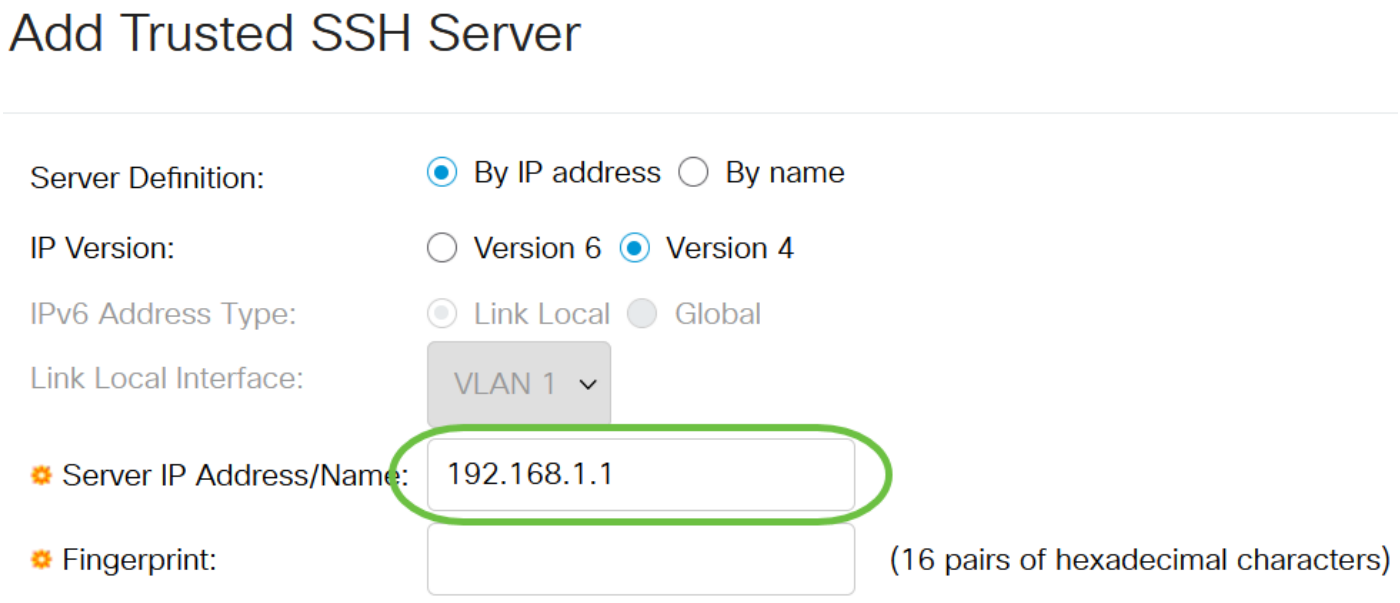


Les options disponibles sont les suivantes :

- Link Local : l'adresse IPv6 identifie de manière unique les hôtes sur une liaison réseau unique. Une adresse link-local a un préfixe FE80, n'est pas routable et ne peut être utilisée que pour la communication sur le réseau local. Une seule adresse link-local est prise en charge. Si une adresse link-local existe sur l'interface, cette entrée remplace l'adresse dans la configuration. Cette option est choisie par défaut.
- Global : l'adresse IPv6 est une monodiffusion globale visible et accessible à partir d'autres réseaux.

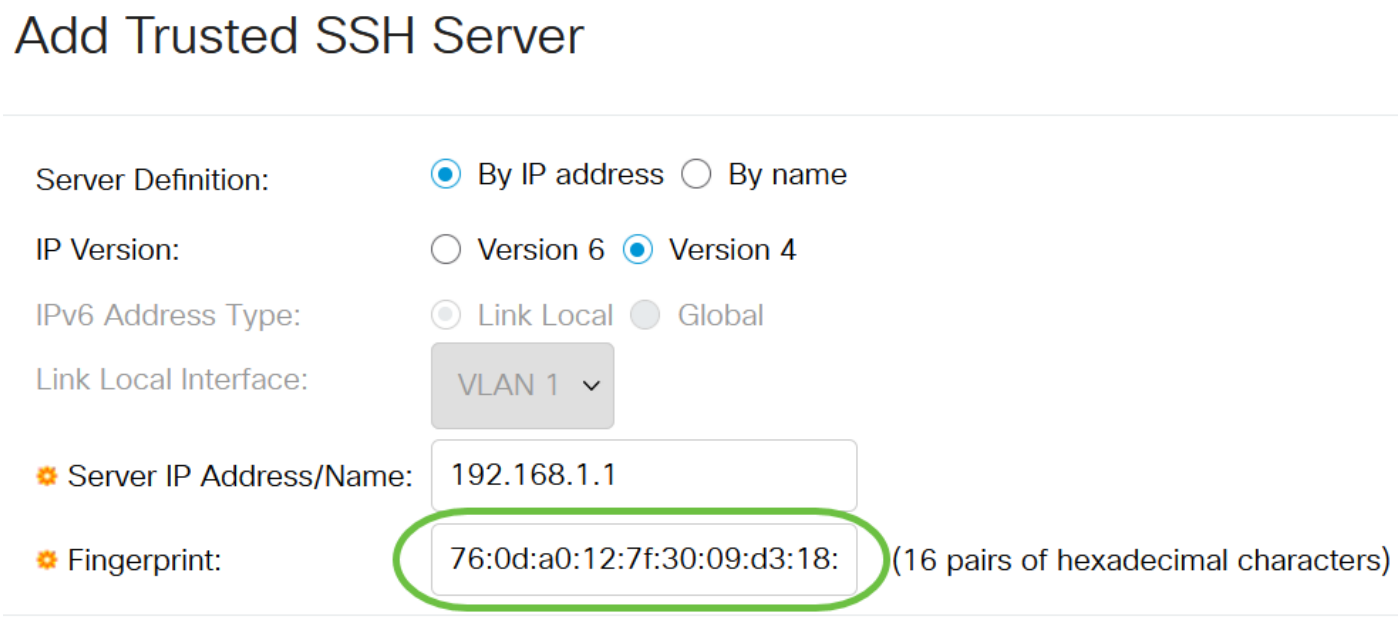
Étape 10. (Facultatif) Si vous avez choisi Link Local comme type d'adresse IPv6 à l'étape 9, sélectionnez l'interface appropriée dans la liste déroulante Link Local Interface.

Étape 11. Dans le champ *Server IP Address/Name*, saisissez l'adresse IP ou le nom de domaine du serveur SSH.

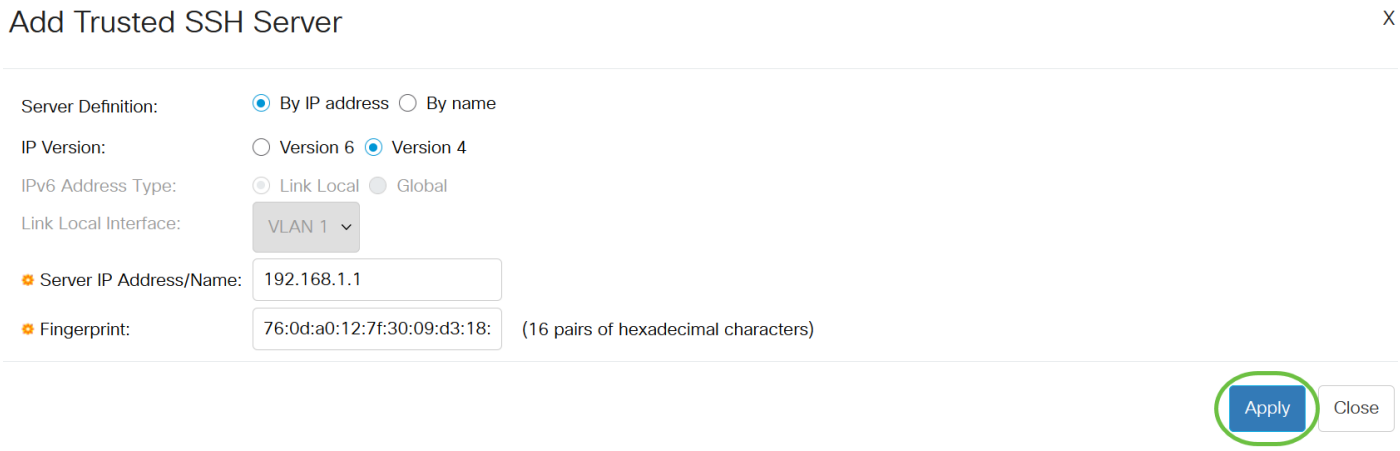


Dans cet exemple, une adresse IP est entrée.

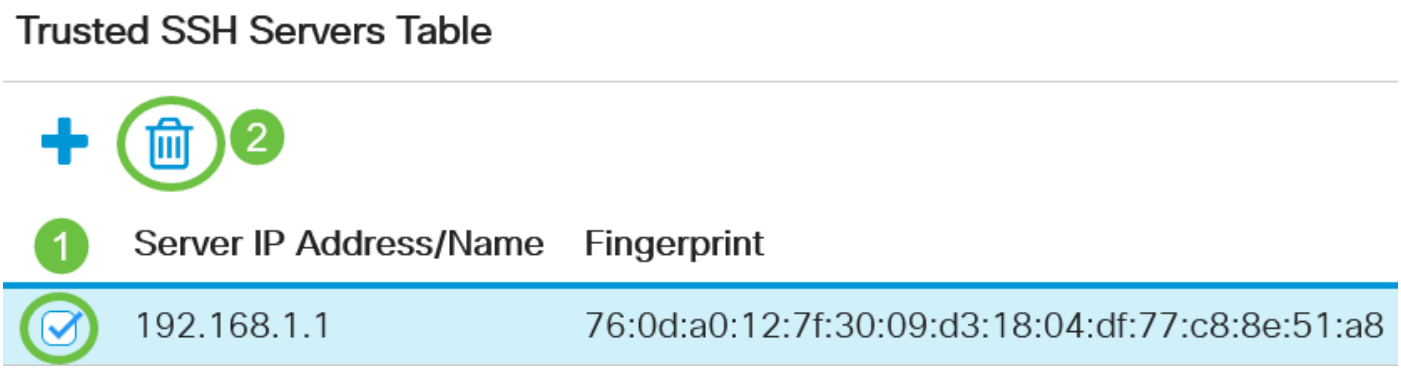
Étape 12. Dans le champ *Empreinte*, saisissez l'empreinte du serveur SSH. Une empreinte digitale est une clé cryptée utilisée pour l'authentification. Dans ce cas, l'empreinte digitale est utilisée pour authentifier la validité du serveur SSH. S'il existe une correspondance entre l'adresse IP/le nom du serveur et l'empreinte digitale, le serveur SSH est authentifié.



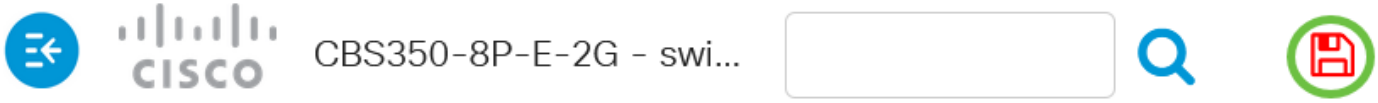
Étape 13. Cliquez sur **Apply** pour enregistrer votre configuration.



Étape 14. (Facultatif) Pour supprimer un serveur SSH, cochez la case du serveur à supprimer, puis cliquez sur **Supprimer**.



Étape 15. (Facultatif) Cliquez sur le bouton **Enregistrer** dans la partie supérieure de la page pour enregistrer les modifications apportées au fichier de configuration initiale.



SSH Server Authentication

Vous avez maintenant configuré les paramètres d'authentification du serveur SSH sur votre commutateur de la gamme Cisco Business 350.

Vous recherchez d'autres articles sur votre commutateur CBS350 ? Consultez les liens ci-dessous pour en savoir plus!

Paramètres d'adresse IP Paramètres de la pile Sélecteur de mode d'empilage Instructions d'empilage Authentification du serveur SSH Récupération de mot de passe Accès CLI avec PuTTY Créer des VLAN Réinitialiser le commutateur