

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

▼ Security

TACACS+ Client

RADIUS Client

▶ RADIUS Server

Password Strength

▶ Mgmt Access Method

Management Access Authentication

▶ Secure Sensitive Data Management

▶ SSL Server

▶ SSH Server

▼ SSH Client

SSH User Authentication

SSH Server Authentication

Change User Password on SSH Server

TCP/UDP Services

▶ Storm Control

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

TCP/UDP Services

HTTP Service: ☒ Enable

HTTPS Service: ☒ Enable

SNMP Service: ☐ Enable

Telnet Service: ☐ Enable

SSH Service: ☒ Enable

Apply

Cancel

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

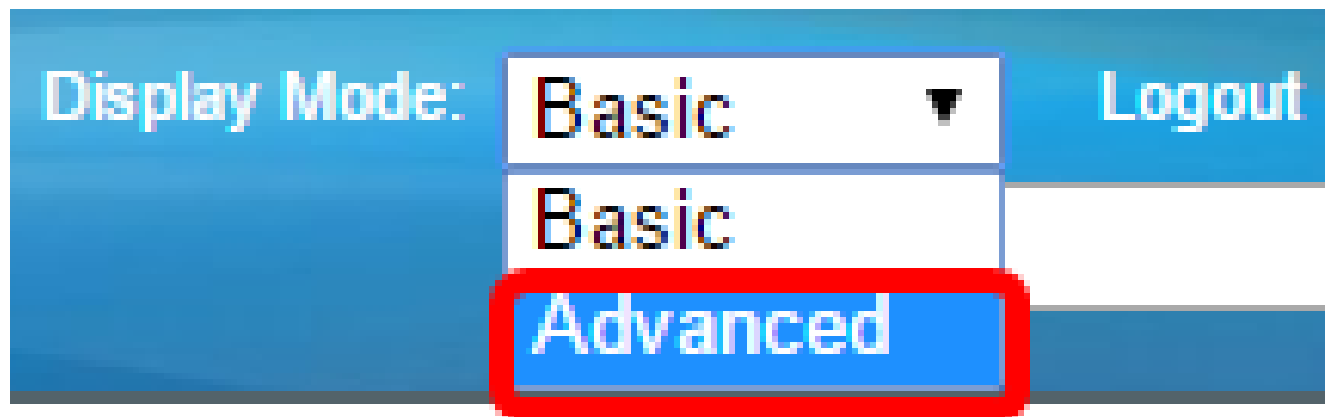
clé publique ou privée est sélectionnée.

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.

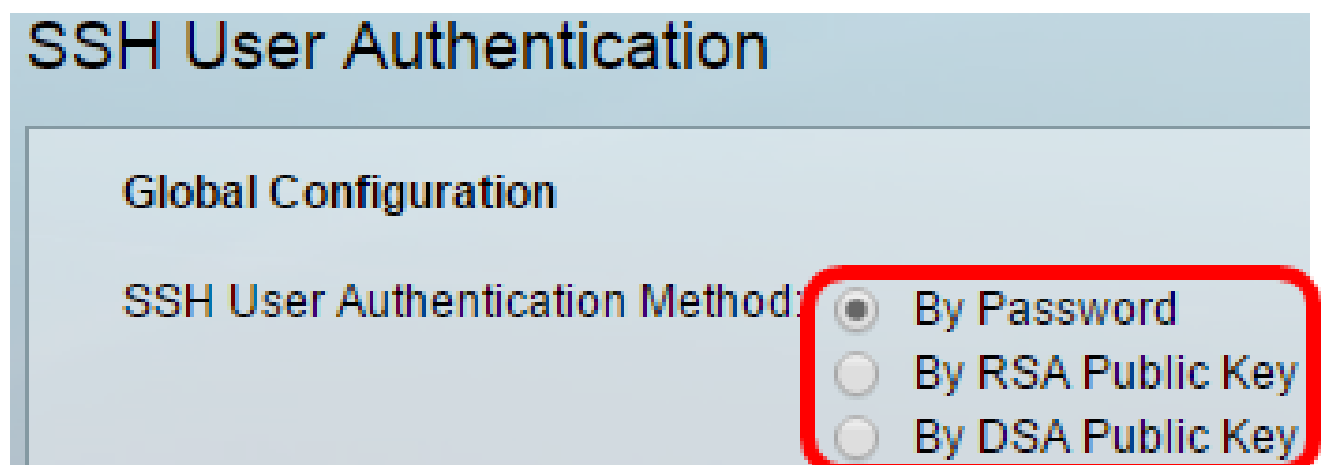
Étape 1. Connectez-vous à l'utilitaire Web et choisissez Security > SSH Client > SSH User Authentication.



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.



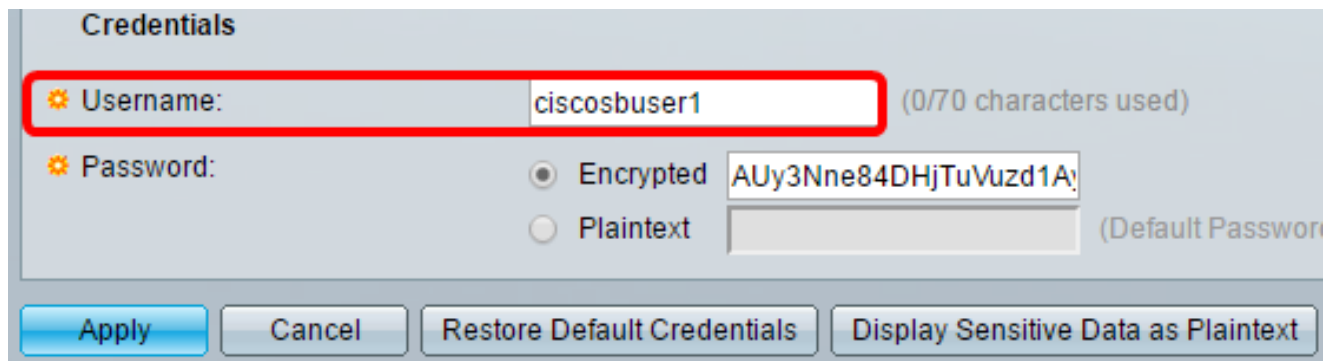
Remarque : lorsqu'un périphérique (client SSH) tente d'établir une session SSH avec le serveur SSH, le serveur SSH utilise l'une des méthodes suivantes pour l'authentification du client :

- 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.

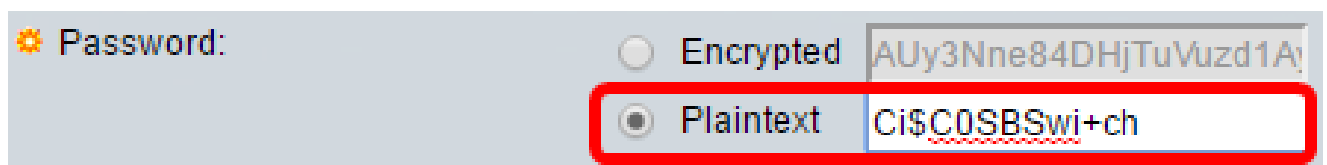
Remarque : dans cet exemple, l'option Par mot de passe est sélectionnée.

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



Remarque : dans cet exemple, ciscosuser1 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.



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

OK

Cancel

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.



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

☐ Don't show me this again

OK

Cancel

Configuration de la table des clés utilisateur SSH

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

SSH User Key Table			
<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	User Defined	60:aa:27:3c:37:52:c2:a5:7c:d0:4a:a5:04:92:47:74
<input type="checkbox"/>	DSA	Auto Generated	1c:54:fe:25:98:fb:d2:1a:45:f5:47:cb:a8:00:be:eb
<div>Generate Edit... Delete Details</div>			

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.



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



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

SSH User Key Table			
<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	User Defined	60:aa:27:3c:37:52:c2:a5:7c:d0:4a:a5:04:92:47:74
<input type="checkbox"/>	DSA	Auto Generated	1c:54:fe:25:98:fb:d2:1a:45:f5:47:cb:a8:00:be:eb
<div><button>Generate</button><button>Edit...</button><button>Delete</button><button>Details</button></div>			

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

Key Type:

⚙️ Public Key:



Remarque : dans cet exemple, RSA est sélectionné.

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

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  
AAAAB3NzaC1yc2EAAAADAQABAAQgQDAb0QFu6yktUlebpLhpETIs79pWy+k0F8g4x  
ovv+0T55Bq2pys5O7FwoxKTLIXFVW5CFdRw26QS2w0oLnH0TecsCI3qzhFuOEVBPhK0  
akyEuy6x6fFsKwdLIld8iUVIbyXk4psIDQD2u0U7AHVRH4ITcXpinexS0MQ==  
-----END SSH2 PUBLIC KEY -----
```

☒ Private Key: ☒ Encrypted ☐ Plaintext

☐ Plaintext

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.



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

☐ Don't show me this again

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

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

SSH User Key Table			
<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	User Defined	60:aa:27:3c:37:52:c2:a5:7c:d0:4a:a5:04:92:47:74
<input type="checkbox"/>	DSA	Auto Generated	1c:54:fe:25:98:fb:d2:1a:45:f5:47:cb:a8:00:be:eb
<div>Generate Edit... Delete Details</div>			

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



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



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

SSH User Key Details

SSH Server Key Type: RSA

Public Key:

---- BEGIN SSH2 PUBLIC KEY ----

Comment: RSA Public Key

AAAAB3NzaC1yc2EAAAADAQABAAQgQDAb0QFu6yktUlebpLhpETIs79pV
Rovv+0T55Bq2pys5O7FwoxKTLIXFVW5CFdRw26QS2w0oLnH0TecsCI3qzF
7LYhakyEuy6x6fFsKwdLIld8iUVIbyXk4psIDQD2u0U7AHVRH4ITcXpinexS0M
---- END SSH2 PUBLIC KEY ----

Private Key (Encrypted):

---- BEGIN SSH2 ENCRYPTED PRIVATE KEY ----

Comment: RSA Private Key

UM5POag2XRmC4XxM1VhmxNkAdj+ml75ZsprMYh/PkuAVm40EHk41YQDg
+zh87iJBUpwHPId1ivhgjBJuF9sFtKTIU3DKUg1lOrKcM90JapMOyDpD7M+4
gBd08SbtMQWZdFy7hj6rSTCO0YPKpVhkyIBwye44QdjCaCGojE/FIKuMHBz
dkVPHkwi2ExfbENqD60yc7pFex+oaah/ugmYgjBmOnNbrViXCrHiUSAKUWz
RUDaVM7V2u67+yw+/yNJ+XvRYkhsQZRON8cOi4ilHV1MImJoRGrdiuR/CjE
X3zOhmB8o6iyCa32MPlhy08yfPN4YgrHh0cpxeWcY1ZRIG0vZ4lxUJ423xYL
rdclnoll4EWSk+sj1vzrGidXHCzQkkMqLp+E5zI9npJc0t6+64tKqAD3CVaHk
VwR5JXrle2vHdik2af2AO3JZsobtTO0dMSA5zPdN4CCERPLAEaActCQOkE
MqHATSyFcG+h0X2MitxV5XsWUaJe/dH/BNeljYrzKRF6y9V37PFBizSLAtE2
62u0QPBRglLu6IL4j4jCtN54PauVkr48mw3JgsWszKXgHmSx/ok7Tu4gPcn
UI37c0vNZwDadMZ/1ZKLEkBOJtJIJevDsWslvclKZAvoSmLu2B20hUM2uor1
5GngylqcT5vYLMGpDL2k2PzUgFuLvbaOFzIri1c1czqyjj+JCbP/cl7TAOeGA7
LtCY8DrAo8y5O15CcgUIZJddWlrqunDGpygscAaor050vG3/5A1C8YRMh2F
86OuHWS+0HHqnJnmgrOICj/O/DiSeRnHkr8juT1sBuwpFDd+wT0L/KzRN1L
4OwOYCjkdgm7GgOI2eOnY9YvyD/RyjCmm11JFA1RwPCSQWhyPrZgcCQS
0FLgLKZNZ1XNJkdqDBmb6CfyvXeGP76EH+EQ==
---- END SSH2 PRIVATE KEY ----

Back


Display Sensitive Data as Plaintext

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

Save
cisco
Language: E

Port Gigabit PoE Stackable Managed Switch

SSH User Authentication


 Success. To permanently save the configuration, go to the [File Operations](#) page or c

Global Configuration

SSH User Authentication Method:

☒ By Password
☐ By RSA Public Key
☐ By DSA Public Key

Credentials

Username: (0/70 characters used)

Password:

☒ Encrypted

☐ Plaintext (Default Password)

SSH User Key Table

<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input type="checkbox"/>	RSA	User Defined	60:aa:27:3c:37:52:c2:a5:7c:d0:4a:a5:04:92:47:74
<input type="checkbox"/>	DSA	Auto Generated	1c:54:fe:25:98:fb:d2:1a:45:f5:47:cb:a8:00:be:eb

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.