Konfigurieren der Authentifizierungseinstellungen für den Secure Shell (SSH)-Server auf einem Switch

Ziel

Dieser Artikel enthält Anweisungen zum Konfigurieren der Serverauthentifizierung auf einem verwalteten Switch, nicht zum Herstellen einer Verbindung mit dem Switch. Für einen Artikel über die Verbindung zu einem Switch über SSH + Putty, klicken Sie bitte hier, um diesen Artikel anzuzeigen.

Secure Shell (SSH) ist ein Protokoll, das eine sichere Remoteverbindung zu bestimmten Netzwerkgeräten bereitstellt. Diese Verbindung stellt Funktionen bereit, die einer Telnet-Verbindung ähneln, nur dass sie verschlüsselt ist. Mit SSH kann der Administrator den Switch über die Befehlszeilenschnittstelle (CLI) mit einem Drittanbieterprogramm konfigurieren.Der Switch fungiert als SSH-Client, der den Benutzern im Netzwerk SSH-Funktionen bereitstellt. Der Switch verwendet einen SSH-Server, um SSH-Dienste bereitzustellen. Wenn die SSH-Serverauthentifizierung deaktiviert ist, betrachtet der Switch jeden SSH-Server als vertrauenswürdig, wodurch die Sicherheit im Netzwerk beeinträchtigt wird. Wenn der SSH-Dienst auf dem Switch aktiviert ist, wird die Sicherheit erhöht.

Unterstützte Geräte

- Sx200-Serie
- Sx300-Serie
- Sx350-Serie
- SG350X-Serie
- Sx500-Serie
- Sx550X-Serie

Software-Version

- 1.4.5.02 - Serie Sx200, Serie Sx300, Serie Sx500
- 2.2.0.66 - Serie Sx350, Serie SG350X, Serie Sx550X

Authentifizierungseinstellungen für den SSH-Server konfigurieren

SSH-Dienst aktivieren

Wenn die SSH-Serverauthentifizierung aktiviert ist, authentifiziert der auf dem Gerät ausgeführte SSH-Client den SSH-Server mithilfe des folgenden Authentifizierungsprozesses:

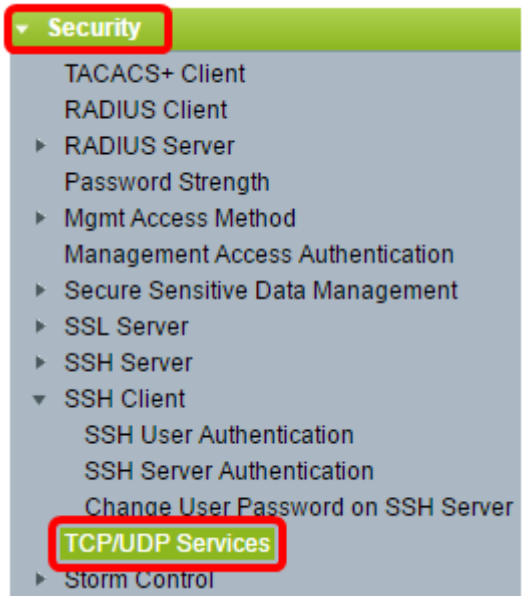
- Das Gerät berechnet den Fingerabdruck des empfangenen öffentlichen Schlüssels des SSH-Servers.
- Das Gerät durchsucht die Tabelle der vertrauenswürdigen SSH-Server nach der IP-Adresse

und dem Hostnamen des SSH-Servers. Eines der folgenden drei Ergebnisse kann eintreten:

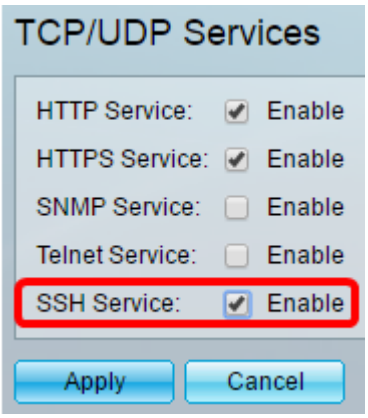
1. Wenn eine Übereinstimmung für die Adresse und den Hostnamen des Servers und dessen Fingerabdruck gefunden wird, wird der Server authentifiziert.
2. Wenn eine übereinstimmende IP-Adresse und ein übereinstimmender Hostname gefunden werden, aber kein übereinstimmender Fingerabdruck vorhanden ist, wird die Suche fortgesetzt. Wenn kein passender Fingerabdruck gefunden wird, ist die Suche abgeschlossen, und die Authentifizierung schlägt fehl.
3. Wenn keine übereinstimmenden IP-Adressen und Hostnamen gefunden werden, ist die Suche abgeschlossen, und die Authentifizierung schlägt fehl.
    - Wenn der Eintrag für den SSH-Server nicht in der Liste der vertrauenswürdigen Server gefunden wird, schlägt der Vorgang fehl.

Hinweis: Um die automatische Konfiguration eines Switch mit werkseitiger Standardkonfiguration zu unterstützen, ist die SSH-Serverauthentifizierung standardmäßig deaktiviert.

Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm an, und wählen Sie **Security > TCP/UDP Services aus**.



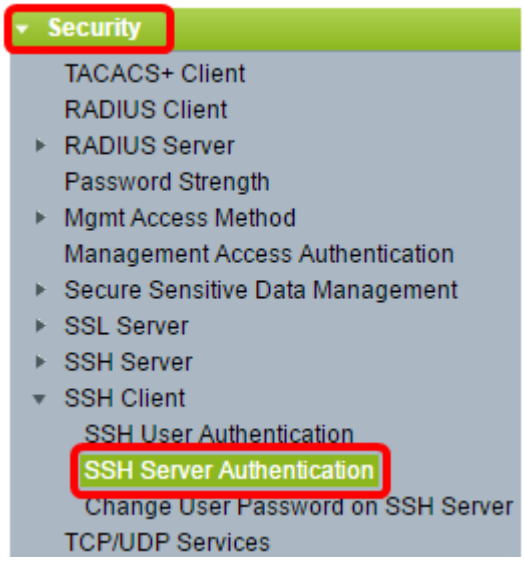
Schritt 2: Aktivieren Sie das Kontrollkästchen **SSH-Dienst**, um den Zugriff auf die Switch-Eingabeaufforderung über SSH zu aktivieren.



Schritt 3: Klicken Sie auf **Apply**, um den SSH-Dienst zu aktivieren.

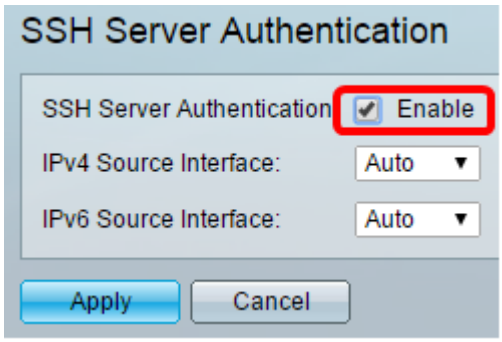
Authentifizierungseinstellungen für den SSH-Server konfigurieren

Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm an, und wählen Sie **Security > SSH Client > SSH Server Authentication aus**.

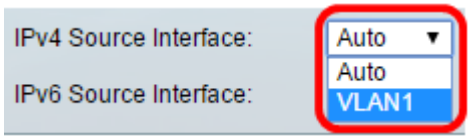


Hinweis: Wenn Sie über einen Sx350, SG300X oder Sx500X verfügen, wechseln Sie in den erweiterten Modus, indem Sie **Erweitert** aus der Dropdown-Liste Anzeigemodus auswählen.

Schritt 2: Aktivieren Sie das Kontrollkästchen SSH-Serverauthentifizierung **aktivieren**, um die SSH-Serverauthentifizierung zu aktivieren.

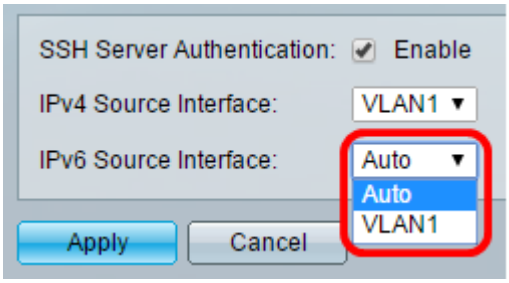


Schritt 3. (Optional) Wählen Sie in der Dropdown-Liste "IPv4 Source Interface" die Quellschnittstelle aus, deren IPv4-Adresse als Quell-IPv4-Adresse für Nachrichten verwendet wird, die in Verbindung mit IPv4-SSH-Servern verwendet werden.



Hinweis: Wenn die Option Auto (Automatisch) ausgewählt ist, bezieht das System die Quell-IP-Adresse aus der IP-Adresse, die auf der Ausgangsschnittstelle definiert wurde. In diesem Beispiel wird VLAN1 ausgewählt.

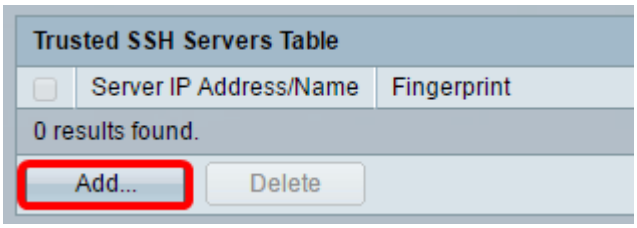
Schritt 4 (Optional) Wählen Sie in der Dropdown-Liste "IPv6 Source Interface" die Quellschnittstelle aus, deren IPv6-Adresse als IPv6-Quelladresse für Nachrichten verwendet wird, die für die Kommunikation mit IPv6-SSH-Servern verwendet werden.



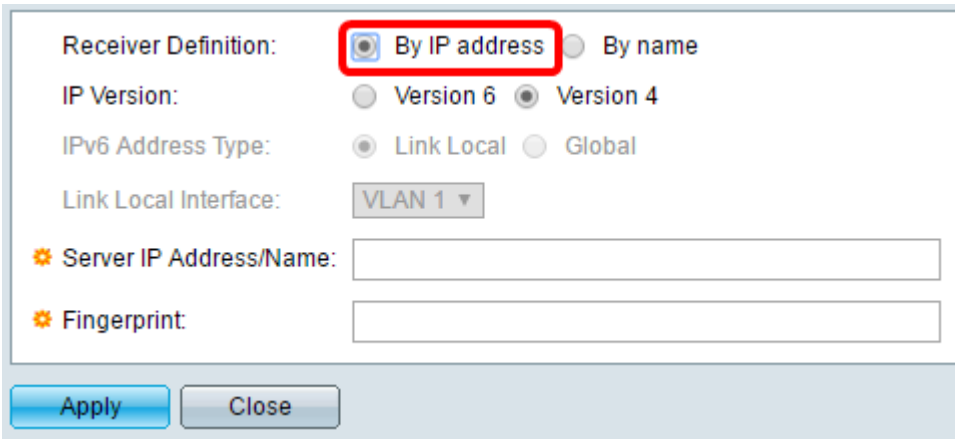
Hinweis: In diesem Beispiel ist die Option Auto (Automatisch) ausgewählt. Das System nimmt die Quell-IP-Adresse von der IP-Adresse, die auf der Ausgangsschnittstelle definiert ist.

Schritt 5: Klicken Sie auf **Apply** (Anwenden).

Schritt 6: Um einen vertrauenswürdigen Server hinzuzufügen, klicken Sie unter der Tabelle Vertrauenswürdige SSH-Server auf **Hinzufügen**.



Schritt 7. Klicken Sie im Bereich Receiver Definition (Empfängerdefinition) auf eine der verfügbaren Methoden, um den SSH-Server zu definieren:

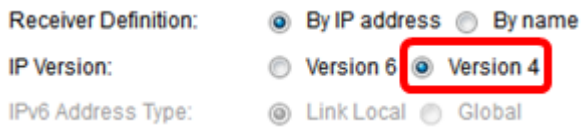


Folgende Optionen sind verfügbar:

- By IP Address (Nach IP-Adresse) - Mit dieser Option können Sie den SSH-Server mit einer IP-Adresse definieren.
- By Name (Nach Name) - Mit dieser Option können Sie den SSH-Server mit einem vollqualifizierten Domänennamen definieren.

Hinweis: In diesem Beispiel wird "Nach IP-Adresse" ausgewählt. Wenn "Nach Name" ausgewählt ist, fahren Sie mit Schritt 11 fort.

Schritt 8. (Optional) Wenn Sie In Schritt 6 Nach IP-Adresse ausgewählt haben, klicken Sie im Feld IP-Version auf die IP-Version des SSH-Servers.



Folgende Optionen sind verfügbar:

- Version 6: Über diese Option können Sie eine IPv6-Adresse eingeben.
- Version 4: Über diese Option können Sie eine IPv4-Adresse eingeben.

Hinweis: In diesem Beispiel wird Version 4 ausgewählt. Das Optionsfeld IPv6 ist nur verfügbar, wenn auf dem Switch eine IPv6-Adresse konfiguriert ist.

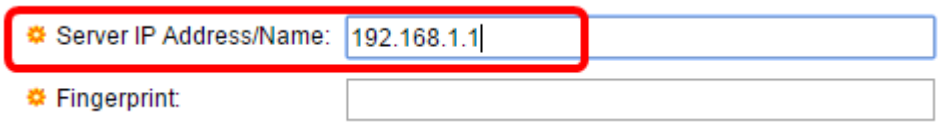
Schritt 9. (Optional) Wenn Sie in Schritt 7 Version 6 als IP-Adressversion ausgewählt haben, klicken Sie im Feld IPv6 Address Type (IPv6-Adresstyp) auf den IPv6-Adresstyp.

Folgende Optionen sind verfügbar:

- Link Local (Lokale Verbindung): Die IPv6-Adresse identifiziert Hosts auf einer einzelnen Netzwerkverbindung eindeutig. Eine lokale Adresse einer Verbindung hat das Präfix FE80, kann nicht geroutet werden und kann nur für die Kommunikation im lokalen Netzwerk verwendet werden. Es wird nur eine lokale Verbindungsadresse unterstützt. Wenn auf der Schnittstelle eine lokale Adresse für die Verbindung vorhanden ist, ersetzt dieser Eintrag die Adresse in der Konfiguration. Diese Option ist standardmäßig ausgewählt.
- Global - Die IPv6-Adresse ist ein globales Unicast, das von anderen Netzwerken aus sichtbar und erreichbar ist.

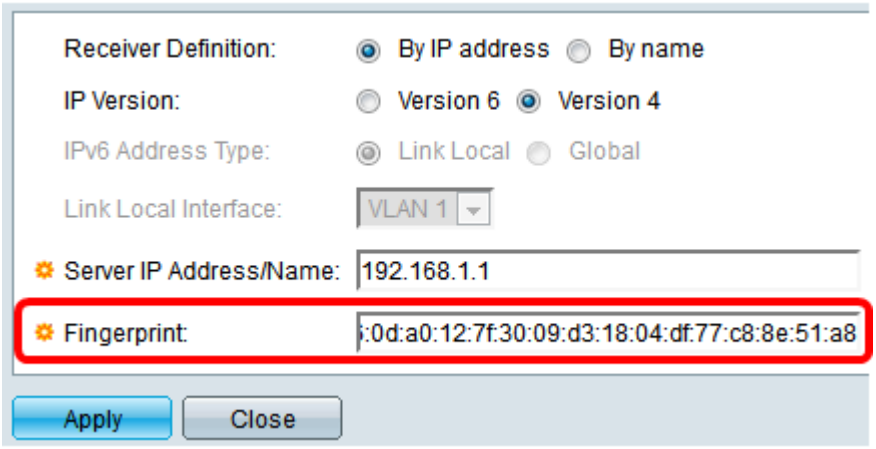
Schritt 10. (Optional) Wenn Sie in Schritt 9 Link Local (Lokale Verbindung) als IPv6-Adresstyp ausgewählt haben, wählen Sie in der Dropdown-Liste Link Local Interface (Lokale Verbindung) die entsprechende Schnittstelle aus.

Schritt 11. Geben Sie im Feld *Server IP Address/Name (Server-IP-Adresse/Name*) die IP-Adresse oder den Domänennamen des SSH-Servers ein.



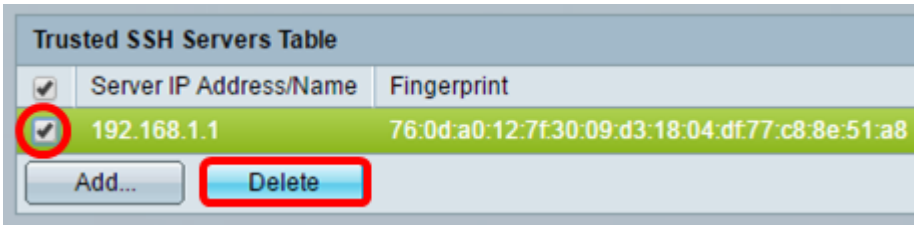
Hinweis: In diesem Beispiel wird eine IP-Adresse eingegeben.

Schritt 12: Geben Sie im Feld *Fingerprint* (Fingerabdruck) den Fingerabdruck des SSH-Servers ein. Ein Fingerabdruck ist ein verschlüsselter Schlüssel für die Authentifizierung. In diesem Fall wird der Fingerabdruck zur Authentifizierung der Gültigkeit des SSH-Servers verwendet. Wenn die IP-Adresse/der Name des Servers mit dem Fingerabdruck übereinstimmt, wird der SSH-Server authentifiziert.

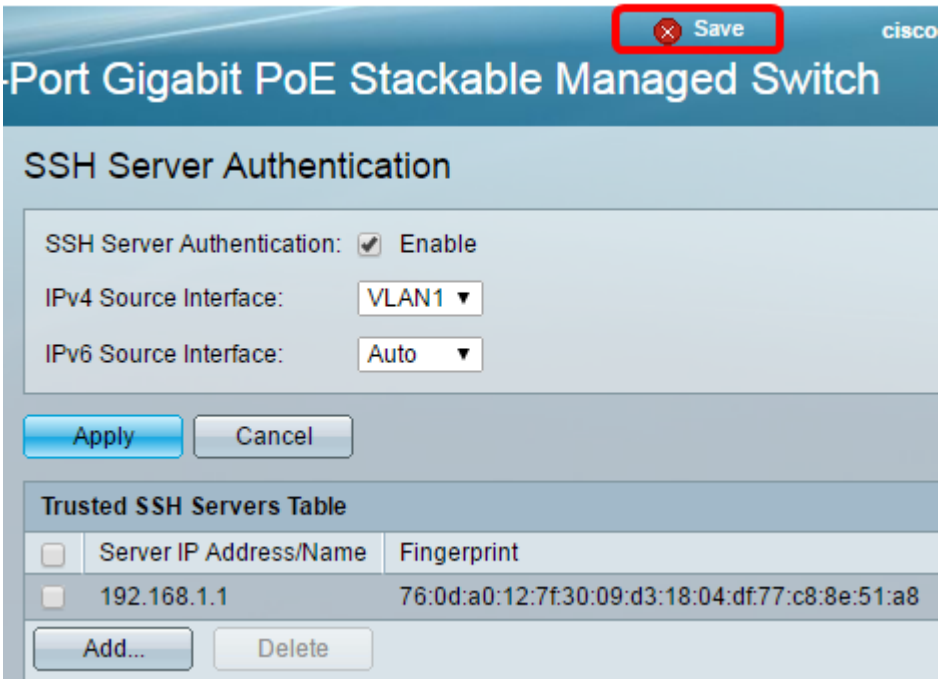


Schritt 13: Klicken Sie auf **Apply**, um die Konfiguration zu speichern.

Schritt 14. (Optional) Um einen SSH-Server zu löschen, aktivieren Sie das Kontrollkästchen des Servers, den Sie löschen möchten, und klicken Sie dann auf **Löschen**.



Schritt 15. (Optional) Klicken Sie oben auf der Seite auf die Schaltfläche **Speichern**, um die Änderungen in der Startkonfigurationsdatei zu speichern.



Sie sollten jetzt die Authentifizierungseinstellungen für den SSH-Server auf dem verwalteten Switch konfiguriert haben.

Video zu diesem Artikel anzeigen ...

Klicken Sie hier, um weitere Tech Talks von Cisco anzuzeigen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.