

# Konfigurieren der Secure Shell (SSH)-Serverauthentifizierungseinstellungen auf einem Cisco Business Switch der Serie 350

## Ziel

Dieser Artikel enthält Anweisungen zum Konfigurieren der Serverauthentifizierung auf einem Cisco Business-Switch der Serie 350.

## Einführung

Secure Shell (SSH) ist ein Protokoll, das eine sichere Remote-Verbindung mit bestimmten Netzwerkgeräten ermöglicht. Diese Verbindung stellt Funktionen bereit, die einer Telnet-Verbindung ähnlich sind, jedoch verschlüsselt sind. Mithilfe von 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, übernimmt der Switch jeden SSH-Server als vertrauenswürdig, was die Sicherheit in Ihrem Netzwerk verringert. Wenn der SSH-Dienst auf dem Switch aktiviert ist, wird die Sicherheit erhöht.

## Unterstützte Geräte | Softwareversion

- CBS 350 ([Datenblatt](#)) | 3.0.0.69 ([Laden Sie die aktuelle Version herunter](#))
- CBS350-2X ([Datenblatt](#)) | 3.0.0.69 ([Laden Sie die aktuelle Version herunter](#))
- CBS350-4X ([Datenblatt](#)) | 3.0.0.69 ([Laden Sie die aktuelle Version herunter](#))

## Konfigurieren der Authentifizierungseinstellungen für den SSH-Server

### SSH-Dienst aktivieren

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

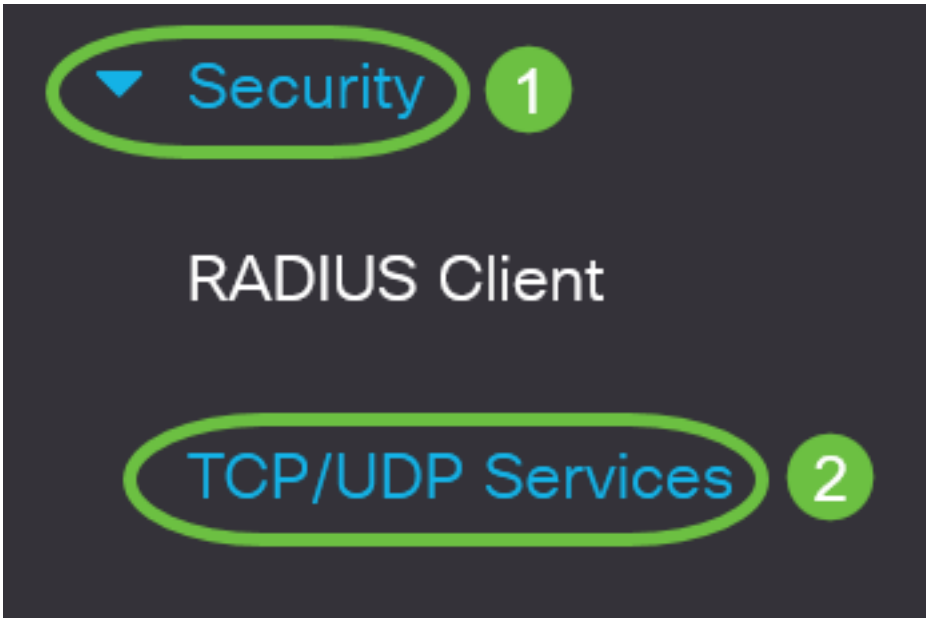
- Das Gerät berechnet den Fingerabdruck des empfangenen öffentlichen Schlüssels des SSH-Servers.
- Das Gerät sucht in der Tabelle mit vertrauenswürdigen SSH-Servern nach der IP-Adresse und dem Hostnamen des SSH-Servers. Eines der folgenden drei Ergebnisse kann auftreten:
  1. Wenn eine Übereinstimmung sowohl für die Adresse als auch für 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 übereinstimmender Fingerabdruck gefunden wird, wird die Suche abgeschlossen, und die Authentifizierung schlägt fehl.
  3. Wenn keine übereinstimmende IP-Adresse und kein Hostname gefunden werden, wird

die Suche abgeschlossen, und die Authentifizierung schlägt fehl.

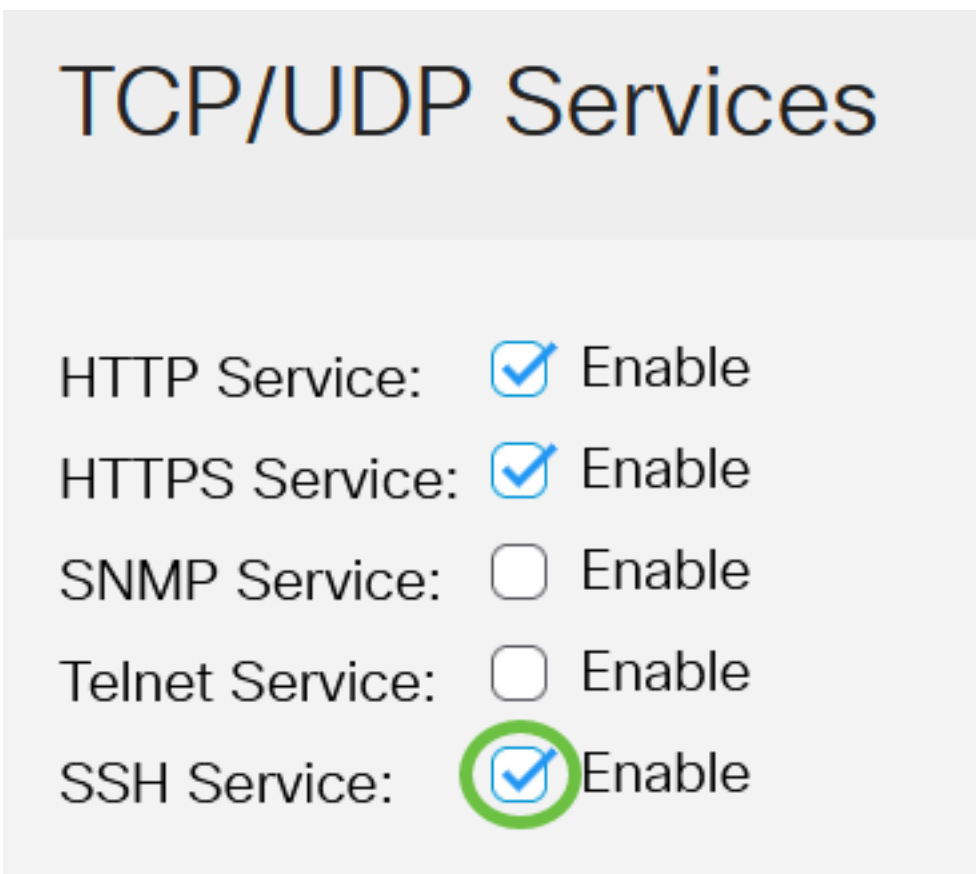
4. Wenn der Eintrag für den SSH-Server nicht in der Liste der vertrauenswürdigen Server gefunden wird, schlägt der Prozess fehl.

Um die automatische Konfiguration eines Out-of-Box-Switches mit werksseitiger 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-Service**, um den Zugriff auf die Switch-Eingabeaufforderung über SSH zu aktivieren.



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

## TCP/UDP Services

Apply

Cancel

HTTP Service:  Enable

HTTPS Service:  Enable

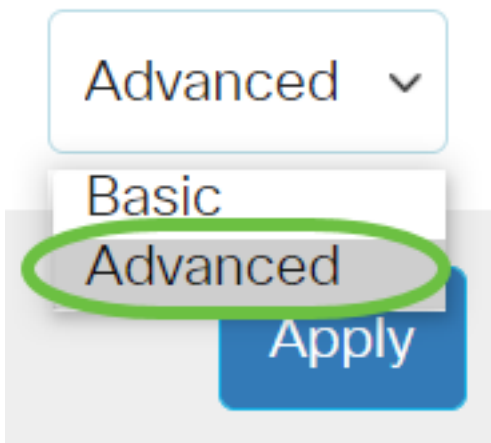
SNMP Service:  Enable

Telnet Service:  Enable

SSH Service:  Enable

## Konfigurieren der Authentifizierungseinstellungen für den SSH-Server

Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm Ihres Switches an, und wählen Sie dann in der Dropdown-Liste Anzeigemodus die Option Erweitert aus.



Schritt 2: Wählen Sie **Security > SSH Client > SSH Server Authentication** aus.

▼ Security

1

TACACS+ Client

RADIUS Client

▶ RADIUS Server

Password Strength

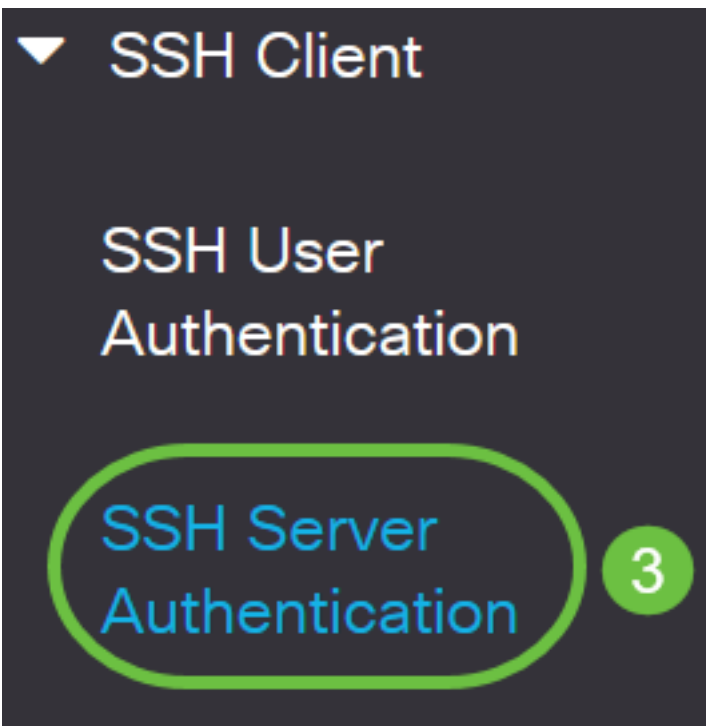
▶ Mgmt Access Method

Management Access  
Authentication

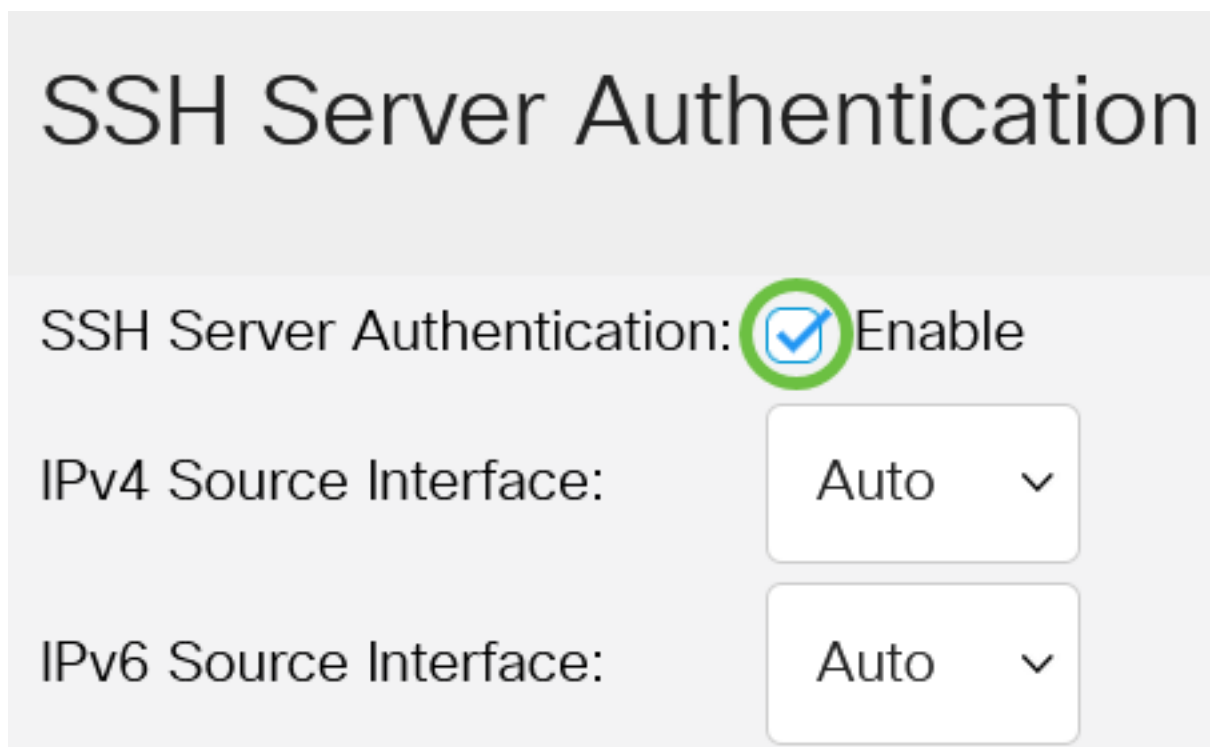
▶ Secure Sensitive Data  
Management

▶ SSL Server

▶ SSH Server



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 (IPv4-Quellschnittstelle) die Quellschnittstelle aus, deren IPv4-Adresse als Quell-IPv4-Adresse für Nachrichten verwendet wird, die in Verbindung mit IPv4-SSH-Servern verwendet werden.

# SSH Server Authentication

SSH Server Authentication:  Enable

IPv4 Source Interface:

Auto ▾

IPv6 Source Interface:

Auto

VLAN 1

Wenn die Option Auto (Automatisch) ausgewählt ist, bezieht das System die Quell-IP-Adresse von der IP-Adresse, die auf der ausgehenden Schnittstelle definiert ist. In diesem Beispiel wird VLAN1 ausgewählt.

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

SSH Server Authentication:  Enable

IPv4 Source Interface:

VLAN 1 ▾

IPv6 Source Interface:

Auto ▾

Auto

Trusted SSH Servers Ta

VLAN 1

In diesem Beispiel wird die Option Automatisch ausgewählt. Das System bezieht die Quell-IP-Adresse von der IP-Adresse, die auf der ausgehenden Schnittstelle definiert ist.

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

## SSH Server Authentication

Apply

Cancel

SSH Server Authentication:  Enable

IPv4 Source Interface:

IPv6 Source Interface:

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

## Trusted SSH Servers Table



Server IP Address/Name    Fingerprint

0 results found.

Schritt 7: Klicken Sie im Bereich Serverdefinition auf eine der verfügbaren Methoden, um den SSH-Server zu definieren.

## Add Trusted SSH Server

Server Definition:



By IP address



By name

Folgende Optionen sind verfügbar:

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

In diesem Beispiel wird By IP address (Nach IP-Adresse) ausgewählt. Wenn By name (Nach Name) ausgewählt ist, fahren Sie mit [Schritt 11 fort](#).

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

# Add Trusted SSH Server

---

Server Definition:

By IP address  By name

IP Version:

Version 6  Version 4

Folgende Optionen stehen zur Verfügung:

- Version 6 - Mit dieser Option können Sie eine IPv6-Adresse eingeben.
- Version 4 - Mit dieser Option können Sie eine IPv4-Adresse eingeben.

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

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

# Add Trusted SSH Server

---

Server Definition:

By IP address  By name

IP Version:

Version 6  Version 4

IPv6 Address Type:

Link Local  Global

Folgende Optionen stehen zur Verfügung:

- Link Local (Lokale Verbindung) - Die IPv6-Adresse identifiziert eindeutig Hosts in einer einzelnen Netzwerkverbindung. Eine lokale Adresse einer Verbindung hat das Präfix FE80, ist nicht routbar und kann nur für die Kommunikation im lokalen Netzwerk verwendet werden. Es wird nur eine lokale Adresse für eine Verbindung unterstützt. Wenn auf der Schnittstelle eine lokale Adresse für die Verbindung vorhanden ist, ersetzt dieser Eintrag die Adresse in der Konfiguration. Diese Option wird 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 die entsprechende Schnittstelle in der Dropdown-Liste Link Local Interface (Lokale Verbindungsschnittstelle) aus.



# Add Trusted SSH Server

Server Definition:  By IP address  By name

IP Version:  Version 6  Version 4

IPv6 Address Type:  Link Local  Global

Link Local Interface:

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

## Add Trusted SSH Server

Server Definition:  By IP address  By name

IP Version:  Version 6  Version 4

IPv6 Address Type:  Link Local  Global

Link Local Interface:

Server IP Address/Name:

Fingerprint:  (16 pairs of hexadecimal characters)

In diesem Beispiel wird eine IP-Adresse eingegeben.

Schritt 12: Geben Sie im *Fingerabdruck*-Feld den Fingerabdruck des SSH-Servers ein. Ein Fingerabdruck ist ein verschlüsselter Schlüssel, der für die Authentifizierung verwendet wird. In diesem Fall wird der Fingerabdruck verwendet, um die Gültigkeit des SSH-Servers zu authentifizieren. Wenn eine Übereinstimmung zwischen der Server-IP-Adresse/-Name und dem Fingerabdruck besteht, wird der SSH-Server authentifiziert.

# Add Trusted SSH Server

Server Definition:  By IP address  By name

IP Version:  Version 6  Version 4

IPv6 Address Type:  Link Local  Global

Link Local Interface: VLAN 1 ▾

✦ Server IP Address/Name:

✦ Fingerprint:  (16 pairs of hexadecimal characters)

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

Add Trusted SSH Server

X

Server Definition:  By IP address  By name

IP Version:  Version 6  Version 4

IPv6 Address Type:  Link Local  Global

Link Local Interface: VLAN 1 ▾



✦ Server IP Address/Name:

✦ Fingerprint:  (16 pairs of hexadecimal characters)

**Apply** Close

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**.

## Trusted SSH Servers Table

  2

<span>1</span>	Server IP Address/Name	Fingerprint
<input checked="" type="checkbox"/>	192.168.1.1	76:0d:a0:12:7f:30:09:d3:18:04:df:77:c8:8e:51:a8

Schritt 15: (Optional) Klicken Sie auf die Schaltfläche **Speichern** am oberen Seitenrand, um die Änderungen in der Startkonfigurationsdatei zu speichern.



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



## SSH Server Authentication

Sie haben jetzt die Authentifizierungseinstellungen für den SSH-Server auf Ihrem Cisco Business Switch der Serie 350 konfiguriert.