

Secure Shell (SSH) Service für Managed Switches der Serien 300 und 500 aktivieren

Ziel

Standardmäßig kann ein Managed Switch der Serie 300 oder 500 über das Konfigurationsprogramm über einen Webbrowser konfiguriert werden. Mit Secure Shell (SSH) kann der Administrator den Switch über eine Kommandozeile (CLI) mit einem Drittanbieterprogramm konfigurieren. Im CLI-Modus über SSH kann der Administrator erweiterte Konfigurationen in einer sicheren Verbindung ausführen. In diesem Artikel wird erläutert, wie der SSH-Dienst auf den Managed Switches der Serien 300 und 500 aktiviert wird.

Anwendbare Geräte | Softwareversion

- Serie Sx300 | 1.3.0.62 ([Download zuletzt](#))
- Serie Sx500 | 1.3.0.62 ([Download zuletzt](#))

SSH-Dienst aktivieren

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Security > TCP/UDP Services aus**. Die Seite *TCP/UDP-Dienste* wird geöffnet:



TCP/UDP Services	
HTTP Service:	<input checked="" type="checkbox"/> Enable
HTTPS Service:	<input checked="" type="checkbox"/> Enable
SNMP Service:	<input type="checkbox"/> Enable
Telnet Service:	<input type="checkbox"/> Enable
SSH Service:	<input checked="" type="checkbox"/> Enable

Apply Cancel

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 sofort zu aktivieren.

Sehen Sie sich ein Video zu diesem Artikel an..

[Klicken Sie hier, um weitere Tech Talks von Cisco anzuzeigen.](#)