

Firmware-Upgrade/Backup und Image-Swap auf SG350XG und SG550XG

Ziele

In diesem Dokument wird erläutert, wie die Firmware auf den SG350XG- und SG550XG-Switches aktualisiert, gesichert oder ausgetauscht wird.

Die Verwendung der neuesten Firmware ist ein Best Practice für Sicherheit und Leistung. Es können mehrere Firmware-Versionen auf dem Switch gespeichert und bei Bedarf ausgetauscht werden. Firmware-Versionen können ebenfalls gesichert werden. Dies kann hilfreich sein, um Sicherungskopien der Firmware zu speichern, falls das Gerät ausfällt.

Anwendbare Geräte

- SG350XG
- SG550XG

Softwareversion

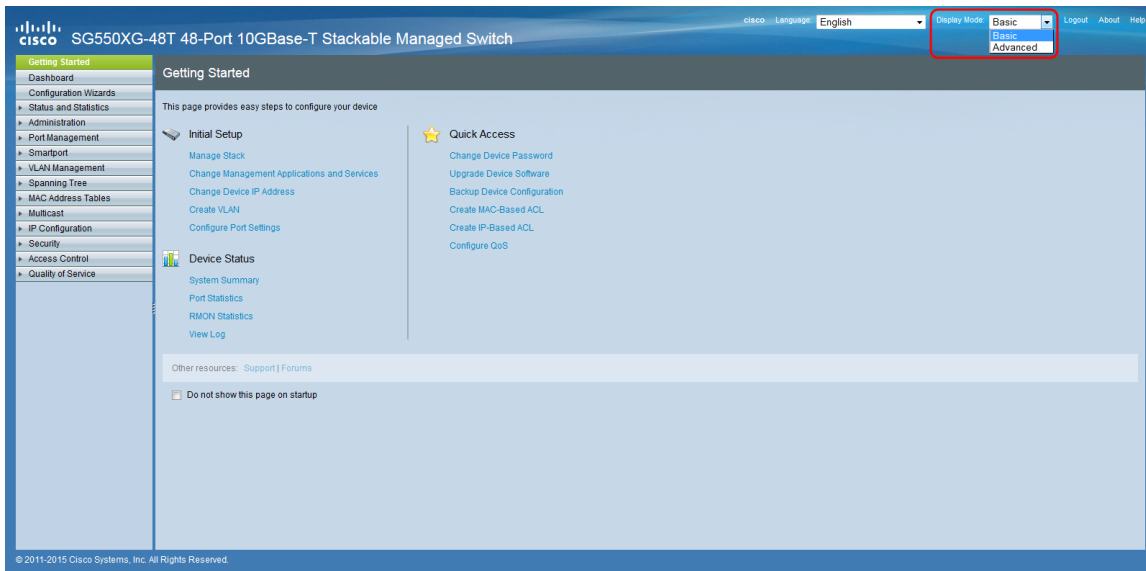
- V2.0.0.73

Tabelle der Schritte

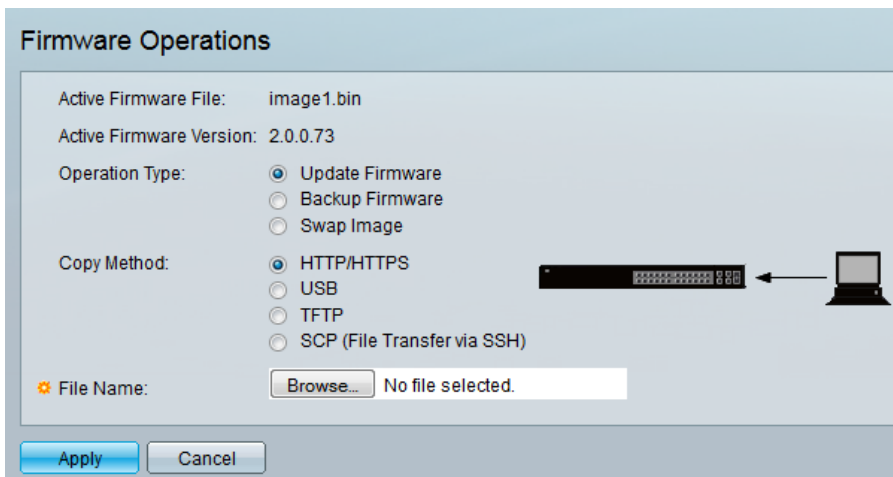
1. Anmeldung
2. [Update-/Backup-Firmware](#)
 - [Methode: HTTP/HTTPS](#)
 - [Methode: USB](#)
 - [Methode: TFTP](#)
 - [Methode: SCP](#)
3. [Bild austauschen](#)

Anmeldung

Hinweis: Die folgenden Screenshots stammen aus dem Advanced Display. Sie können dies umschalten, indem Sie auf die Dropdown-Liste *Anzeigemodus* oben rechts im Bildschirm klicken.

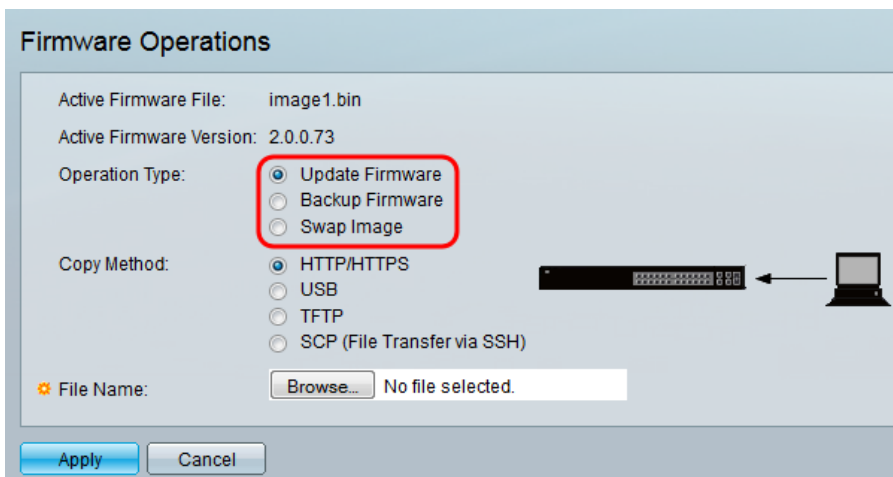


Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und **wählen Sie Administration > File Management > Firmware Operations (Verwaltung > Dateiverwaltung > Firmware-Betrieb)**. Die Seite *Firmware-Betrieb* wird geöffnet.



Hinweis: Sie können die aktuelle Firmware-Datei und -Version im Feld *Aktive Firmware-Datei* und im Feld *Aktive Firmware-Version* sehen.

Schritt 2: Klicken Sie im Bereich *Betriebstyp* auf das gewünschte Optionsfeld.



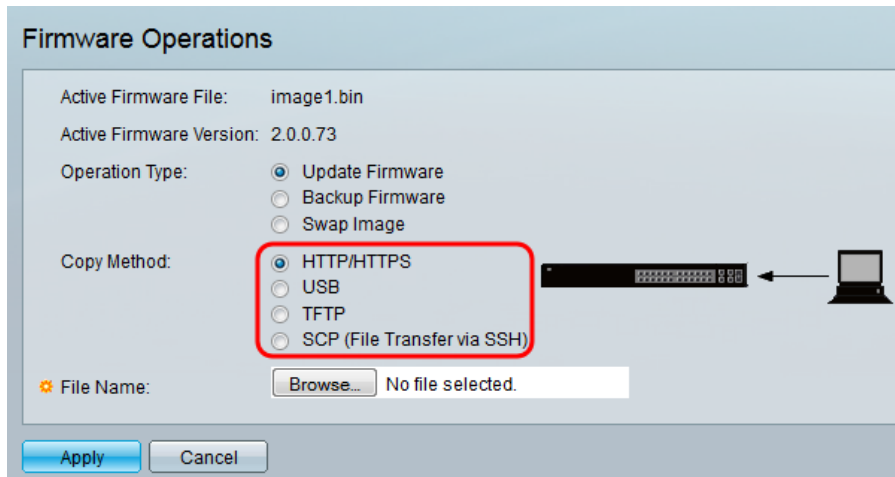
Die Optionen werden wie folgt beschrieben:

- [Firmware aktualisieren](#) - Aktualisiert die Firmware des Geräts.

- [Backup-Firmware](#) - Erstellt ein Backup der Firmware des Geräts.
- [Swap Image \(Image austauschen\)](#): Ändert die Firmware des Geräts mit einer Firmware, die im Flash-Speicher des Geräts gespeichert ist.

Update-/Backup-Firmware

Schritt 1: Klicken Sie auf das Optionsfeld im Abschnitt *Copy Method (Kopiermethode)*, um die gewünschte Übertragungsmethode für die Datei anzugeben.



Die Optionen werden wie folgt beschrieben:

- [HTTP/HTTPS](#): Verwendet die vom Browser bereitgestellten Funktionen.
- [USB](#) - Verwendet den USB-Port des Switches.
- [TFTP](#) - Trivial File Transfer Protocol (TFTP) ist ein einfaches Dateiübertragungsprotokoll, das es einem Client ermöglicht, eine Datei von einem Remotehost abzurufen oder auf diesen abzulegen.
- [SCP \(File Transfer via SSH\)](#) - Secure Copy Protocol (SCP) unterstützt Dateiübertragungen zwischen Hosts in einem Netzwerk. Sie verwendet Secure Shell (SSH) für die Datenübertragung und verwendet die gleichen Authentifizierungsmechanismen, um die Authentizität und Vertraulichkeit der übertragenen Daten sicherzustellen.

HTTP/HTTPS

Schritt 1: Klicken Sie im Feld *Dateiname auf die* Schaltfläche **Durchsuchen**, um die zu aktualisierende Bilddatei auszuwählen. Dieser Schritt ist nicht relevant für Backup by HTTP/HTTPS.

Copy Method: HTTP/HTTPS
 USB
 TFTP
 SCP (File Transfer via SSH)

File Name:

Schritt 2: Klicken Sie auf **Übernehmen**.

Copy Method: HTTP/HTTPS
 USB
 TFTP
 SCP (File Transfer via SSH)

File Name:

Schritt 3: Navigieren Sie zu **Administration > Reboot**. Die Seite *Neustart* wird geöffnet.

Reboot

To reboot the device, click the 'Reboot' button.

Reboot: Immediate
 Date Time HH:MM
 In Days Hours Minutes

Restore to Factory Defaults
 Clear Startup Configuration File

Schritt 4: Klicken Sie auf **Neustart**. Ein Bestätigungsfenster wird angezeigt.

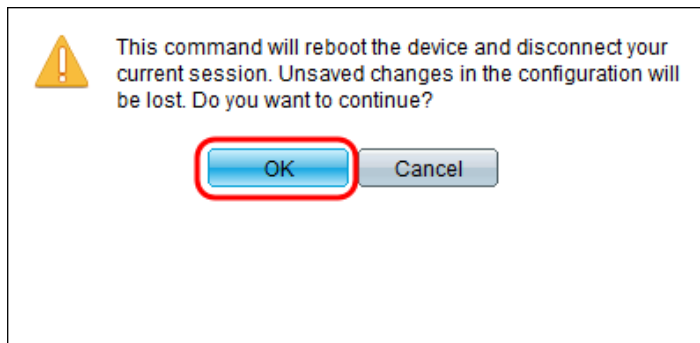
Reboot

To reboot the device, click the 'Reboot' button.

Reboot: Immediate
 Date Time HH:MM
 In Days Hours Minutes

Restore to Factory Defaults
 Clear Startup Configuration File

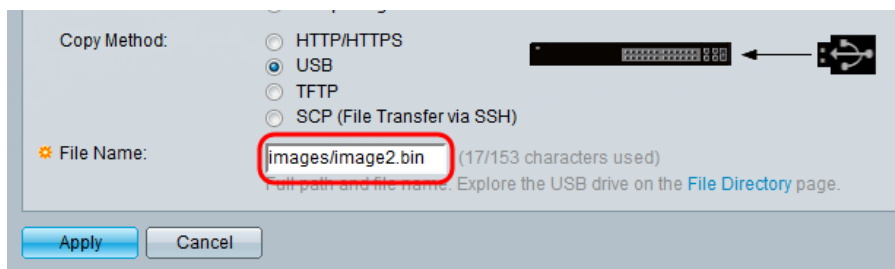
Schritt 5: Klicken Sie auf **OK**.



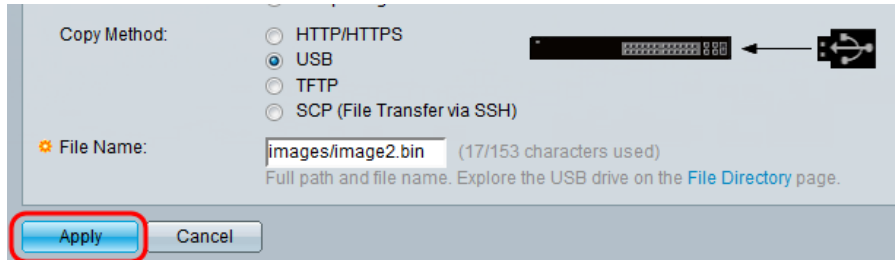
Hinweis: Das Gerät wird jetzt neu gestartet, wodurch die Verbindung zur aktuellen Sitzung getrennt wird. Sobald der Neustart abgeschlossen ist, wird eine neue Sitzung verbunden.

USB

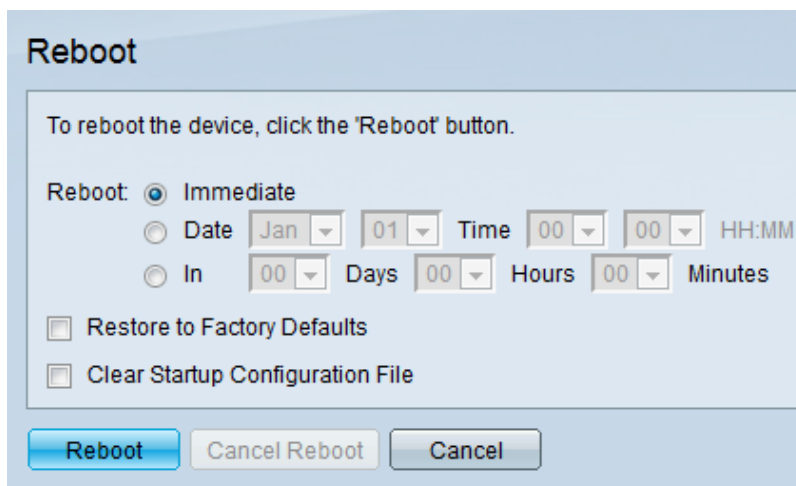
Schritt 1: Geben Sie den Pfad der Bilddatei auf dem USB-Stick im Feld *Dateiname ein*.



Schritt 2: Klicken Sie auf **Übernehmen**.



Schritt 3: Wählen Sie im Webkonfigurationsprogramm **Administration > Reboot (Verwaltung > Neustart)**. Die Seite *Neustart* wird geöffnet.



Schritt 4: Klicken Sie auf **Neustart**.

Reboot


To reboot the device, click the 'Reboot' button.

Reboot: Immediate
 Date Time HH:MM
 In Days Hours Minutes

Restore to Factory Defaults
 Clear Startup Configuration File

Reboot Cancel Reboot Cancel

Schritt 5: Ein Bestätigungsfenster wird angezeigt. Klicken Sie auf **OK**.

 This command will reboot the device and disconnect your current session. Unsaved changes in the configuration will be lost. Do you want to continue?

OK Cancel

Hinweis: Das Gerät wird jetzt neu gestartet, wodurch die Verbindung zur aktuellen Sitzung getrennt wird. Sobald der Neustart abgeschlossen ist, wird eine neue Sitzung verbunden.

TFTP

Schritt 1: Wählen Sie die entsprechende Optionsschaltfläche für die Definition des TFTP-Servers aus. Der Server kann entweder **nach IP-Adresse** oder **nach Namen** definiert werden. Wenn Sie **Nach Name** ausgewählt haben, fahren Sie mit [Schritt 5 fort](#).

Copy Method: Swap image
 HTTP/HTTPS
 USB
 TFTP
 SCP (File Transfer via SSH)

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:

Source File Name: (0/160 characters used)

Apply Cancel

Schritt 2: (Optional) Wählen Sie die Version der IP-Adresse des Servers aus. Wenn **Version 4** ausgewählt ist, fahren Sie mit [Schritt 5 fort](#).

Die Optionen werden wie folgt beschrieben:

- IPv4 - Eine 32-Bit-Adresse (vier Byte).
- IPv6 - Ein Nachfolger von IPv4 besteht aus einer 128-Bit-Adresse (8 Byte).

Schritt 3: (Optional) Wählen Sie den Typ der IPv6-Adresse aus. Sie können für Ihren Adresstyp entweder **Link Local (Lokale Verbindung)** oder **Global** auswählen. Wenn **Global** ausgewählt wurde, fahren Sie mit [Schritt 5 fort](#).

Schritt 4: (Optional) Wählen Sie das gewünschte VLAN aus der Dropdown-Liste *Lokale Schnittstelle der Verbindung* aus.

Schritt 5: Geben Sie den Namen oder die IP-Adresse des Servers in das Feld *IP-Adresse/Name des Servers* ein.

Copy Method: HTTP/HTTPS USB TFTP SCP (File Transfer via SSH)

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: 192.0.2.1

Source File Name: (0/160 characters used)

Apply Cancel

Hinweis: Das folgende Feld hängt von der in [Schritt 1](#) ausgewählten Option ab.

Schritt 6: Geben Sie den Dateinamen in das Feld *Source/Destination File Name (Quelle/Ziel-Dateiname)* ein.

Copy Method: HTTP/HTTPS USB TFTP SCP (File Transfer via SSH)

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: 192.0.2.1

Source File Name: image2.bin (10/160 characters used)

Apply Cancel

Hinweis: Das folgende Feld trägt den Titel *Name der Zieldatei* für Backup by TFTP.

Schritt 7: Klicken Sie auf **Übernehmen**.

Copy Method: HTTP/HTTPS USB TFTP SCP (File Transfer via SSH)

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: 192.0.2.1

Source File Name: image2.bin (10/160 characters used)

Apply Cancel

SCP (Dateiübertragung über SSH)

Schritt 1: Um die SSH-Serverauthentifizierung zu aktivieren (die standardmäßig deaktiviert ist), klicken Sie auf **Edit by Remote SSH Server Authentication**. Dadurch gelangen Sie zur Seite *Client SSH UserAuthentication*, um den SSH-Benutzer zu konfigurieren.

Remote SSH Server Authentication: Disabled [Edit](#)

SSH Client Authentication: Use SSH Client [System Credentials](#)
 Use SSH Client One-Time Credentials:

Username:

Password:

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:

Source File Name: (0/160 characters used)

[Apply](#) [Cancel](#)

Hinweis: Weitere Informationen zu Anmeldeinformationen des SSH-Client-Systems finden Sie im Artikel [SSH User Authentication \(SSH-Benutzerauthentifizierung\)](#).

Schritt 2: Wählen Sie die gewünschte SSH-Authentifizierung im Feld *SSH-Client-Authentifizierung* aus.

Remote SSH Server Authentication: Disabled [Edit](#)

SSH Client Authentication: Use SSH Client [System Credentials](#)
 Use SSH Client One-Time Credentials:

Username:

Password:

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:

Source File Name: (0/160 characters used)

[Apply](#) [Cancel](#)

Die verfügbaren Optionen sind wie folgt definiert:

- SSH-Clientsystem-Anmeldeinformationen verwenden - Legt permanente SSH-Benutzeranmeldeinformationen fest. Klicken
- **Systemanmeldedaten**, um zur Seite *SSH-Benutzerauthentifizierung* zu gelangen, auf der Benutzer/Kennwort einmal für die zukünftige Verwendung festgelegt werden können.
- SSH-Client Einmalanmeldedaten verwenden - Legt einmalige SSH-Benutzeranmeldeinformationen fest.

Hinweis: Weitere Informationen zu Anmeldeinformationen des SSH-Client-Systems finden Sie im Artikel [SSH User Authentication \(SSH-Benutzerauthentifizierung\)](#).

Schritt 3: (Optional) Geben Sie den gewünschten *Benutzernamen* und das gewünschte *Kennwort* in die entsprechenden Felder ein.

Remote SSH Server Authentication: Disabled [Edit](#)

SSH Client Authentication:
 Use SSH Client [System Credentials](#)
 Use SSH Client One-Time Credentials:

Username:
Password:

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:
✦ Source File Name: (0/160 characters used)

[Apply](#) [Cancel](#)

Schritt 4: Wählen Sie das entsprechende Optionsfeld für die Definition des SCP-Servers aus. Der Server kann entweder **nach IP-Adresse** oder **nach Namen** definiert werden. Wenn Sie **By name (Nach Namen)** ausgewählt haben, fahren Sie mit [Schritt 8 fort](#).

Remote SSH Server Authentication: Disabled [Edit](#)

SSH Client Authentication:
 Use SSH Client [System Credentials](#)
 Use SSH Client One-Time Credentials:

Username:
Password:

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:
✦ Source File Name: (0/160 characters used)

[Apply](#) [Cancel](#)

Schritt 5: (Optional) Wählen Sie die Version der IP-Adresse des Servers aus. Wenn **Version 4** ausgewählt ist, fahren Sie mit [Schritt 8 fort](#).

Remote SSH Server Authentication: Disabled [Edit](#)

SSH Client Authentication:
 Use SSH Client [System Credentials](#)
 Use SSH Client One-Time Credentials:

Username:
Password:

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:
✦ Source File Name: (0/160 characters used)

[Apply](#) [Cancel](#)

Die Optionen werden wie folgt beschrieben:

- IPv4 - Eine 32-Bit-Adresse (vier Byte).
- IPv6 - Ein Nachfolger von IPv4 besteht aus einer 128-Bit-Adresse (8 Byte).

Schritt 6: (Optional) Wählen Sie den Typ der IPv6-Adresse aus. Sie können für Ihren

Adresstyp entweder **Link Local (Lokale Verbindung)** oder **Global** auswählen. Wenn **Global** ausgewählt wurde, fahren Sie mit [Schritt 8 fort](#).

Remote SSH Server Authentication: Disabled [Edit](#)

SSH Client Authentication: Use SSH Client [System Credentials](#)
 Use SSH Client One-Time Credentials:

Username:

Password:

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:

Source File Name: (0/160 characters used)

[Apply](#) [Cancel](#)

Schritt 7: (Optional) Wählen Sie das gewünschte VLAN aus der Dropdown-Liste *Lokale Schnittstelle der Verbindung* aus.

Remote SSH Server Authentication: Disabled [Edit](#)

SSH Client Authentication: Use SSH Client [System Credentials](#)
 Use SSH Client One-Time Credentials:

Username:

Password:

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:

Source File Name: (0/160 characters used)

[Apply](#) [Cancel](#)

Schritt 8: Geben Sie den Namen oder die IP-Adresse des Servers in das Feld *IP-Adresse/Name des Servers* ein.

Remote SSH Server Authentication: Disabled [Edit](#)

SSH Client Authentication: Use SSH Client [System Credentials](#)
 Use SSH Client One-Time Credentials:

Username:

Password:

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:

Source File Name: (0/160 characters used)

[Apply](#) [Cancel](#)

Schritt 9: Geben Sie den Dateinamen in das Feld *Quelle/Ziel Dateiname* ein.

Remote SSH Server Authentication: Disabled [Edit](#)

SSH Client Authentication: Use SSH Client [System Credentials](#)
 Use SSH Client One-Time Credentials:

Username:

Password:

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:

Source File Name: (10/160 characters used)

Hinweis: Das Feld trägt den Titel *Name der Zieldatei* für die Sicherung durch SCP.

Schritt 10: Klicken Sie auf **Übernehmen**.

Remote SSH Server Authentication: Disabled [Edit](#)

SSH Client Authentication: Use SSH Client [System Credentials](#)
 Use SSH Client One-Time Credentials:

Username:

Password:

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:

Source File Name: (10/160 characters used)

Bild austauschen

Schritt 1: Wählen Sie in der Dropdown-Liste *Active Image After Reboot (Active Image After Reboot)* die Firmware-Datei aus, die Sie nach dem Neustart aktivieren möchten.

Firmware Operations

Active Firmware File: image1.bin

Active Firmware Version: 2.0.0.73

Operation Type: Update Firmware
 Backup Firmware
 Swap Image

Active Image After Reboot:

Active Image Version Number After Reboot:

Schritt 2: Klicken Sie auf **Übernehmen**.

Firmware Operations

Active Firmware File:	image1.bin
Active Firmware Version:	2.0.0.73
Operation Type:	<input type="radio"/> Update Firmware <input type="radio"/> Backup Firmware <input checked="" type="radio"/> Swap Image
Active Image After Reboot:	image1.bin
Active Image Version Number After Reboot:	2.0.0.73

Schritt 3: Wählen Sie im Webkonfigurationsprogramm **Administration > Reboot (Administration > Neustart)**. Die Seite *Neustart* wird geöffnet.

Reboot

To reboot the device, click the 'Reboot' button.

Reboot: Immediate
 Date Time HH:MM
 In Days Hours Minutes

Restore to Factory Defaults
 Clear Startup Configuration File

Schritt 4: Klicken Sie auf **Neustart**. Ein Bestätigungsfenster wird angezeigt.

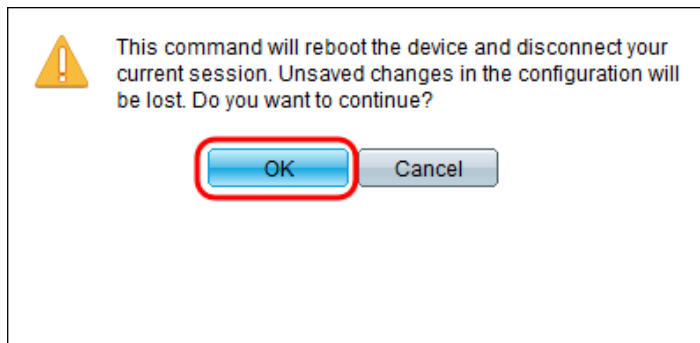
Reboot

To reboot the device, click the 'Reboot' button.

Reboot: Immediate
 Date Time HH:MM
 In Days Hours Minutes

Restore to Factory Defaults
 Clear Startup Configuration File

Schritt 5: Klicken Sie auf **OK**.



Hinweis: Das Gerät wird jetzt neu gestartet, wodurch die Verbindung zur aktuellen Sitzung getrennt wird. Sobald der Neustart abgeschlossen ist, wird eine neue Sitzung verbunden.

Sehen Sie sich ein Video zu diesem Artikel an..

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