

# Mise à niveau/sauvegarde du micrologiciel et échange d'images sur les modèles SG350XG et SG550XG

## Objectifs

L'objectif de ce document est d'expliquer comment mettre à niveau, sauvegarder ou échanger le micrologiciel sur les commutateurs SG350XG et SG550XG.

L'utilisation du dernier micrologiciel est une bonne pratique pour la sécurité et les performances. Plusieurs versions du micrologiciel peuvent être enregistrées sur le commutateur et peuvent être échangées si nécessaire. Les versions de microprogramme peuvent également être sauvegardées. Cela peut être utile pour enregistrer des copies de sauvegarde du micrologiciel en cas de défaillance du périphérique.

## Périphériques pertinents

- SG350XG
- SG550XG

## Version du logiciel

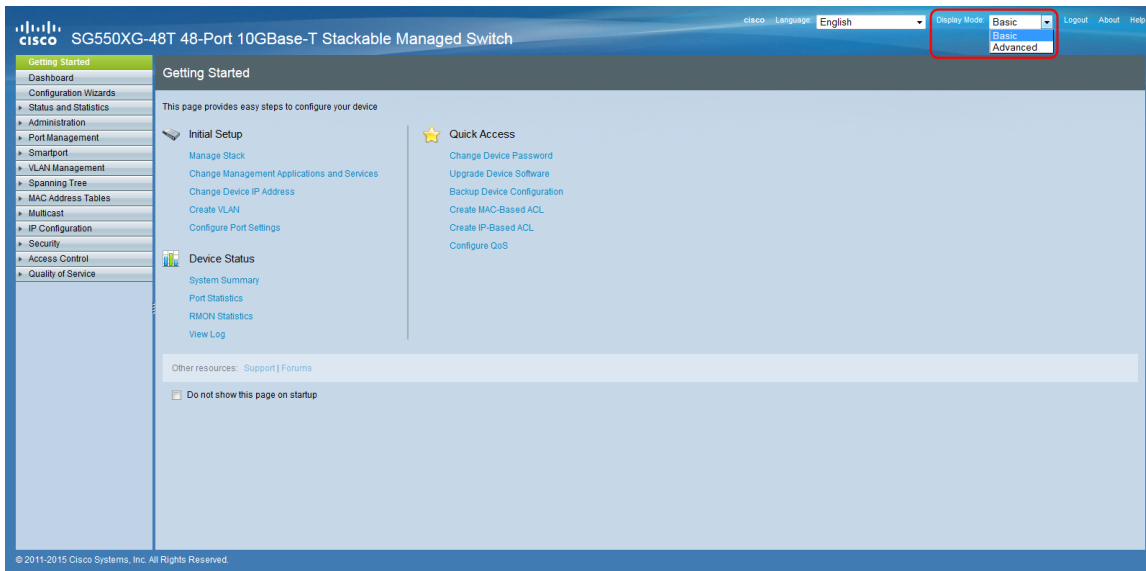
- v 2.0.0.73

## Tableau des étapes

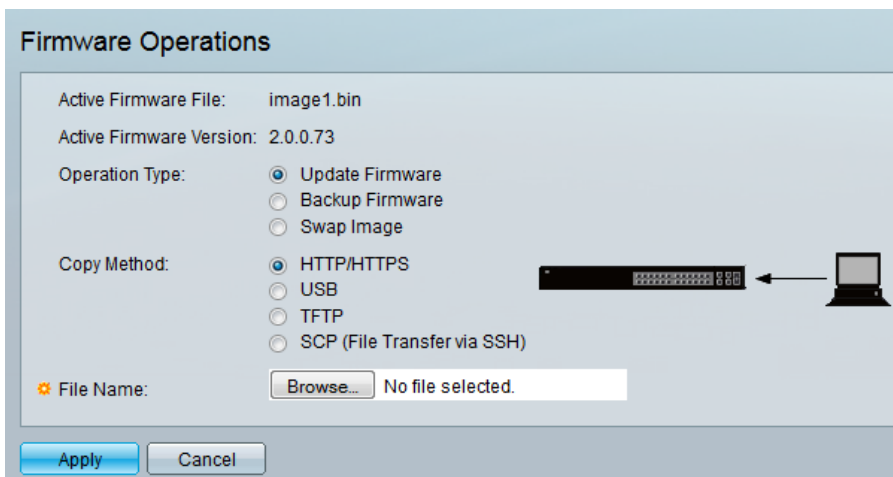
1. Connexion
2. [Mise à jour/sauvegarde du micrologiciel](#)
  - [Méthode : HTTP/HTTPS](#)
  - [Méthode : USB](#)
  - [Méthode : TFTP](#)
  - [Méthode : SCP](#)
3. [Échanger l'image](#)

## Connexion

**Note:** Les captures d'écran suivantes proviennent de l'affichage avancé. Vous pouvez basculer en cliquant sur la liste déroulante *Mode d'affichage* située en haut à droite de l'écran

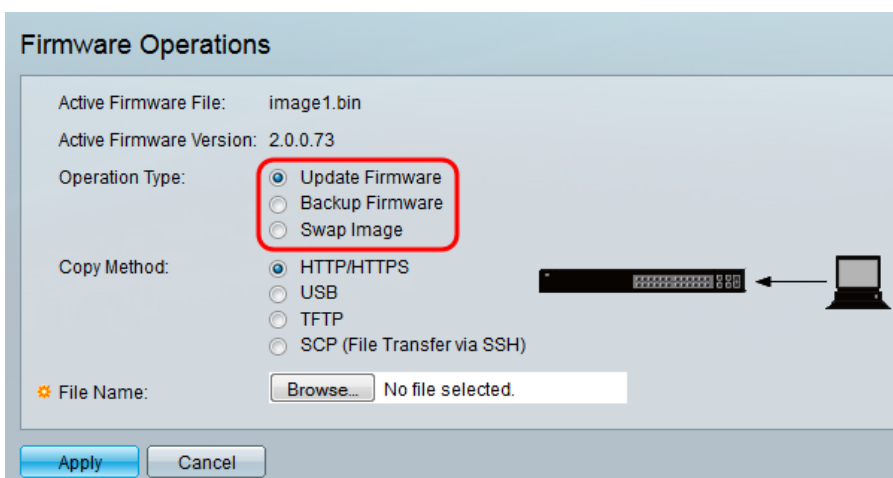


Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez **Administration > File Management > Firmware Operations**. La page *Firmware Operations* s'affiche.



**Remarque :** vous pouvez voir le fichier et la version actuels du microprogramme dans le champ *Fichier du microprogramme actif* et le champ *Version du microprogramme actif*.

Étape 2. Activez la case d'option souhaitée dans la zone *Type d'opération*.



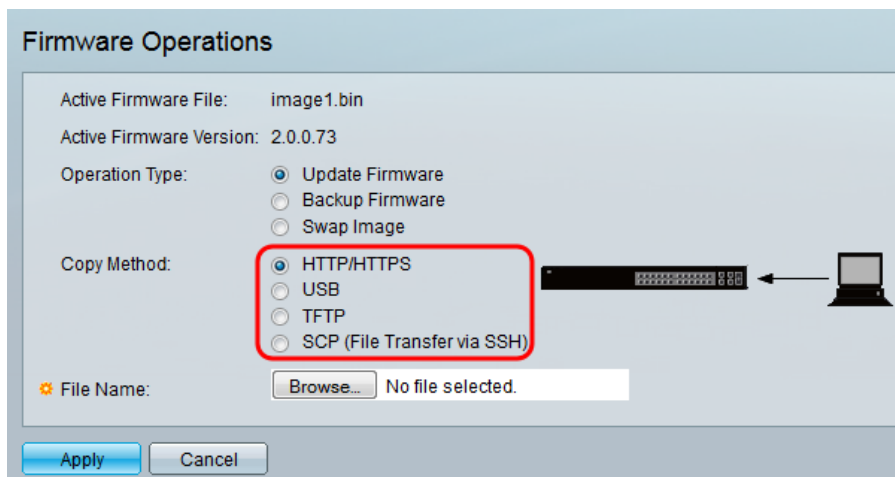
Les options sont décrites comme suit :

- [Mettre à jour le micrologiciel](#) - Met à jour le micrologiciel du périphérique.

- [Backup Firmware](#) : crée une sauvegarde du micrologiciel du périphérique.
- [Swap Image](#) - Modifie le micrologiciel du périphérique avec un micrologiciel stocké dans la mémoire flash du périphérique.

## Mise à jour/sauvegarde du micrologiciel

Étape 1. Cliquez sur la case d'option de la section *Méthode de copie* pour connaître la méthode de transfert souhaitée.



Les options sont décrites comme suit :

- [HTTP/HTTPS](#) - Utilise les fonctionnalités fournies par le navigateur.
- [USB](#) - Utilise le port USB des commutateurs.
- [TFTP](#) - Le protocole TFTP (Trivial File Transfer Protocol) est un protocole de transfert de fichiers simple qui permet à un client d'obtenir ou de placer un fichier sur un hôte distant.
- [SCP](#) (File Transfer via SSH) - Secure Copy Protocol (SCP) prend en charge les transferts de fichiers entre les hôtes d'un réseau. Il utilise Secure Shell (SSH) pour le transfert de données et utilise les mêmes mécanismes d'authentification, assurant ainsi l'authenticité et la confidentialité des données en transit.

## HTTP/HTTPS

Étape 1. Cliquez sur le bouton **Parcourir** dans le champ *Nom du fichier* pour sélectionner le fichier image à mettre à jour. Cette étape n'est pas pertinente pour la sauvegarde par HTTP/HTTPS.

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

File Name:

Étape 2. Cliquez sur **Apply**.

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

File Name:

Étape 3. Accédez à **Administration > Reboot**. La page *Reboot* s'affiche.

### 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

Étape 4. Cliquez sur **Redémarrer**. Une fenêtre de confirmation s'affiche.

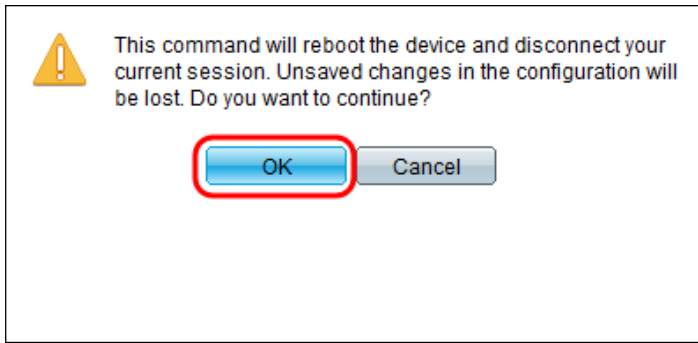
### Reboot

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

Étape 5. Cliquez sur **OK**.



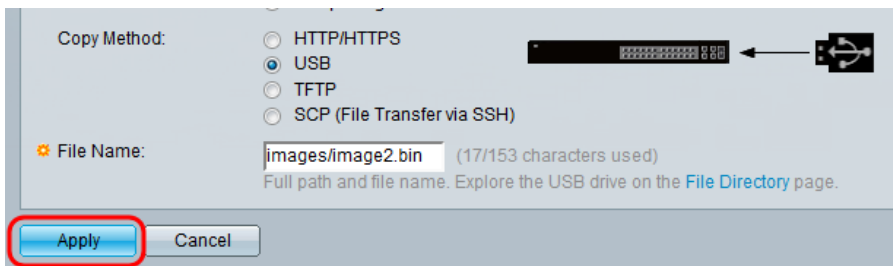
**Note:** Le périphérique redémarre et déconnecte la session en cours. Une fois le redémarrage terminé, une nouvelle session se connecte.

## USB

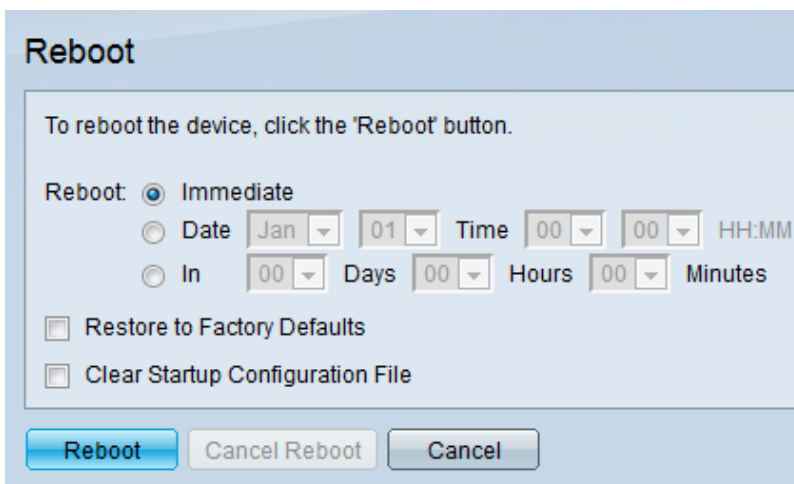
Étape 1. Entrez le chemin d'accès du fichier image situé sur l'USB dans le champ *Nom du fichier*.



Étape 2. Cliquez sur Apply.



Étape 3. Dans l'utilitaire de configuration Web et choisissez **Administration > Reboot**. La page *Reboot* s'affiche.



Étape 4. Cliquez sur **Redémarrer**.

## 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

Étape 5. Une fenêtre de confirmation s'affiche. Click 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

**Note:** Le périphérique redémarre et déconnecte la session en cours. Une fois le redémarrage terminé, une nouvelle session se connecte.

## TFTP

Étape 1. Sélectionnez la case d'option correspondante pour définir le serveur TFTP. Le serveur peut être défini **Par adresse IP** ou **Par nom**. Si vous avez sélectionné **Par nom**, passez à l'[étape 5](#).

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

Étape 2. (Facultatif) Sélectionnez la version de l'adresse IP du serveur. Si la **version 4** est sélectionnée, passez à l'[étape 5](#).

Les options sont décrites comme suit :

- IPv4 : adresse 32 bits (quatre octets).
- IPv6 : successeur d'IPv4, se compose d'une adresse de 128 bits (8 octets).

Étape 3. (Facultatif) Sélectionnez le type d'adresse IPv6. Vous pouvez sélectionner **Link Local** ou **Global** pour votre type d'adresse. Si **Global** a été sélectionné, passez à l'[étape 5](#).

Étape 4. (Facultatif) Sélectionnez le VLAN souhaité dans la liste déroulante *Link Local Interface*.

Étape 5. Entrez le nom ou l'adresse IP du serveur dans le champ *Adresse IP/Nom du serveur*.

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

**Note:** Le champ suivant dépend de l'option sélectionnée à l'[étape 1](#).

Étape 6. Entrez le nom du fichier dans le champ *Source/Destination File Name*.

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

**Note:** Le champ suivant est intitulé *Nom du fichier de destination* pour la sauvegarde par TFTP.

Étape 7. Cliquez sur Apply.

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 (File Transfer via SSH)

Étape 1. Pour activer l'authentification du serveur SSH (qui est désactivée par défaut), cliquez sur **Modifier** par *Authentification du serveur SSH distant*. Cela vous amène à la page *Client SSH UserAuthentication* pour configurer l'utilisateur SSH.



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

**Note:** Pour plus d'informations sur les informations d'identification du système client SSH, reportez-vous à l'article [Authentification utilisateur SSH](#).

Étape 2. Sélectionnez l'authentification SSH souhaitée dans le champ *SSH Client Authentication*.

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

Les options disponibles sont définies comme suit :

- Utiliser les informations d'identification du système client SSH - Définit les informations d'identification permanentes de l'utilisateur SSH. Cliquez sur
- **Informations d'identification système** pour accéder à la page *Authentification utilisateur SSH* où l'utilisateur/mot de passe peut être défini une fois pour toute utilisation future
- Utiliser les informations d'identification et de connexion uniques du client SSH - Définit les informations d'identification utilisateur SSH uniques.

**Note:** Pour plus d'informations sur les informations d'identification du système client SSH, reportez-vous à l'article [Authentification utilisateur SSH](#).

Étape 3. (Facultatif) Saisissez le *nom d'utilisateur* et le *mot de passe* souhaités dans leurs champs respectifs.

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](#)

Étape 4. Sélectionnez la case d'option correspondante pour définir le serveur SCP. Le serveur peut être défini **par adresse IP** ou **par nom**. Si vous avez sélectionné **Par nom**, passez à [l'étape 8](#).

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](#)

Étape 5. (Facultatif) Sélectionnez la version de l'adresse IP du serveur. Si la **version 4** est sélectionnée, passez à [l'étape 8](#).

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](#)

Les options sont décrites comme suit :

- IPv4 : adresse 32 bits (quatre octets).
- IPv6 : successeur d'IPv4, se compose d'une adresse de 128 bits (8 octets).

Étape 6. (Facultatif) Sélectionnez le type d'adresse IPv6. Vous pouvez sélectionner **Link**

**Local** ou **Global** pour votre type d'adresse. Si **Global** a été sélectionné, passez à l'[étape 8](#).

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](#)

Étape 7. (Facultatif) Sélectionnez le VLAN souhaité dans la liste déroulante *Link Local Interface*.

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](#)

Étape 8. Entrez le nom ou l'adresse IP du serveur dans le champ *Adresse IP/Nom du serveur*.

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](#)

Étape 9. Entrez le nom du fichier dans la zone *Source/Destination Nom de fichier* champ.

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)

**Note:** Le champ est intitulé *Nom du fichier de destination* pour la sauvegarde par SCP.

Étape 10. Cliquez sur Apply.

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)

## Échanger l'image

Étape 1. Sélectionnez le fichier de microprogramme que vous souhaitez activer après le redémarrage dans la liste déroulante *Image active après redémarrage*.

**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:

Étape 2. Cliquez sur Apply.

### 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

Étape 3. Dans l'utilitaire de configuration Web, sélectionnez **Administration > Reboot**. La page *Reboot* s'affiche.

### 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

Étape 4. Cliquez sur **Redémarrer**. Une fenêtre de confirmation s'affiche.

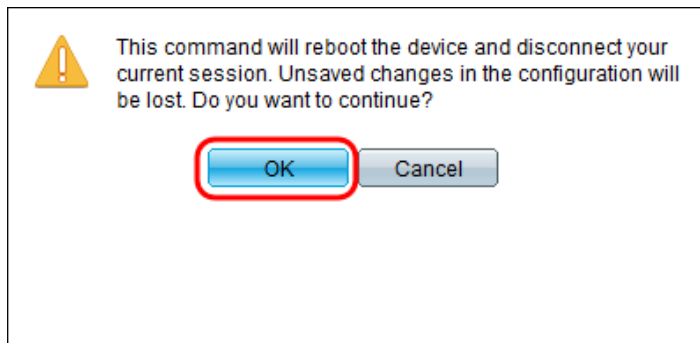
### Reboot

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

Étape 5. Cliquez sur **OK**.



**Note:** Le périphérique redémarre et déconnecte la session en cours. Une fois le redémarrage terminé, une nouvelle session se connecte.

**Afficher une vidéo relative à cet article...**

[Cliquez ici pour afficher d'autres présentations techniques de Cisco](#)