Download or Back Up Configuration Files on a Switch

Objective

The Backup Configuration File or log of the switch is useful for troubleshooting or if the device accidentally gets reset. This contains manual copies of files used for protection against system shutdown or for the maintenance of a specific operating state. For instance, you can copy and save the Mirror Configuration, Startup Configuration, or Running Configuration to a Backup file. You can use this file to update or restore the switch back to its functional state.

The Backup Configuration File can be saved on the Internal Flash memory or a USB device attached on your switch, a Trivial File Transfer Protocol (TFTP) server, a Secure Copy (SCP) server, or on your computer. This article will guide you on how to download or back up a system configuration file through any of the following methods:

- Via TFTP — The Trivial File Transfer Protocol (TFTP) method is chosen to download or back up configuration file via TFTP. TFTP is mainly used to boot up computers in LAN, and is also suitable to download files.
- Via HTTP/HTTPS — The Hyper Text Transfer Protocol (HTTP) or Hyper Text Transfer Protocol Secure (HTTPS) method is chosen to download or back up configuration file via HTTP/HTTPS. This method is more popular for file downloads as it is more secure.
- Via SCP (Over SSH) — The Secure Copy (SCP) (Over (SSH)) method is chosen to download or back up configuration file via Secure Shell (SSH). This download or back up of configuration files are done over a secure network.
- Via USB or Internal Flash — This method is chosen to download or back up the source file into the internal flash memory or a connected USB drive on the switch.

Applicable Devices

- Sx250 Series
- Sx350 Series
- SG350X Series
- Sx550X Series

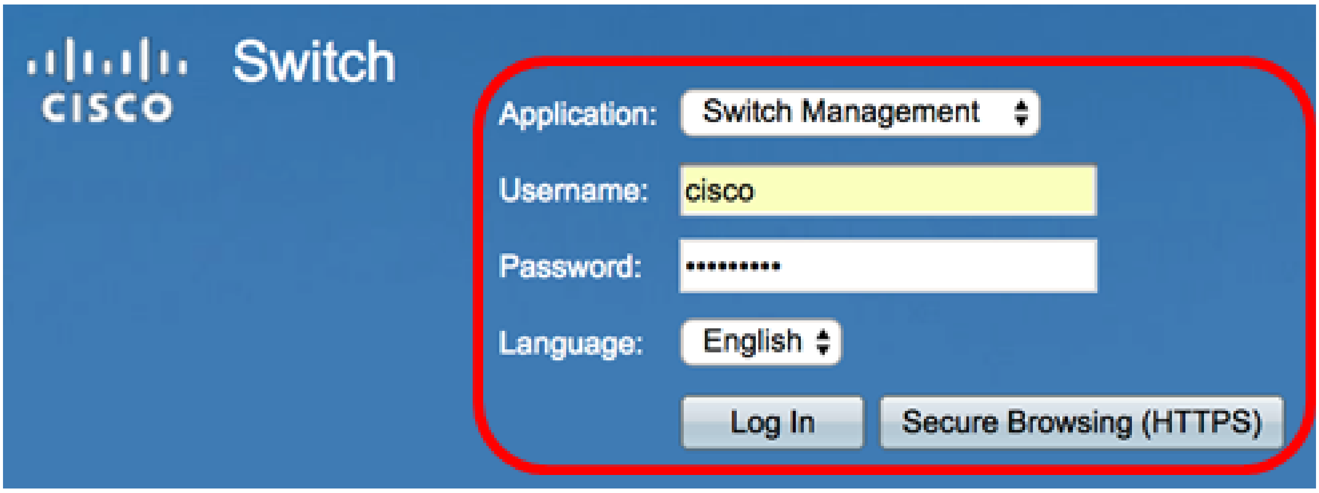
Software Version

- 2.3.0.130

Back Up Configuration Files

Step 1. Log in to the web-based utility of your switch. The default username and password is cisco/cisco.

Note: If you already have changed the password or created a new account, enter your new credentials instead.



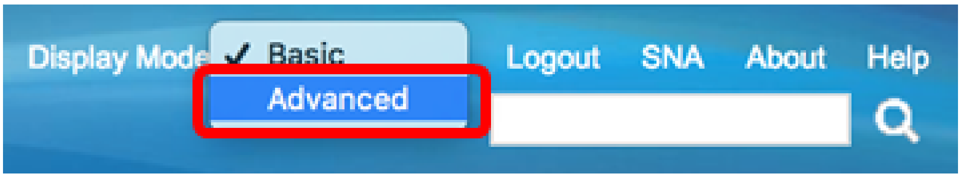
Application: Switch Management

Username: cisco

Password: *********

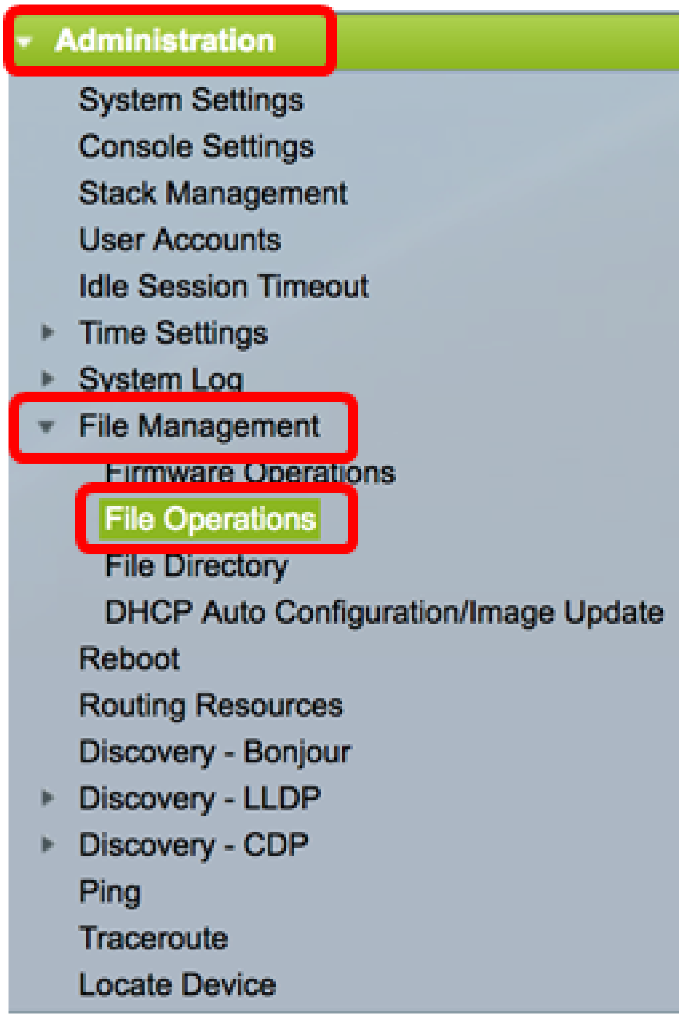
Language: English

Step 2. Choose **Advanced** from the Display Mode drop-down list.

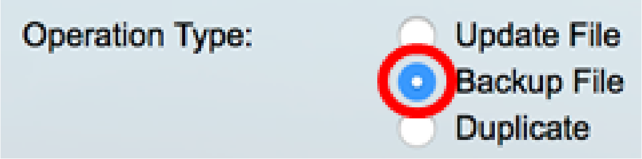


Step 3. Click **Administration > File Management > File Operations**.

Note: The available menu options may vary depending on the device model. In this example, SG350X-48MP switch is used.



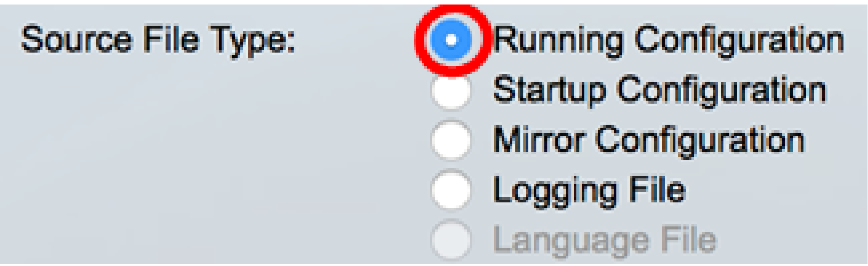
Step 4. Click the **Backup File** radio button to back up a configuration file.



Operation Type: ○ Update File ● Backup File ○ Duplicate

Step 5. In the *Source File Type* area, click the radio button of the type of file that you want to be backed up. The switch maintains the following configuration files.

- *Running Configuration* - The configuration file that contains the current configuration, including any changes applied in any management sessions since the last reboot.
- *Startup Configuration* - The configuration file that is saved to flash memory.
- *Mirror Configuration* - The running configuration file is automatically saved to the mirror configuration file type if it is not modified for at least 24 hours.
- *Logging File* - This is where the switch stores all of its logs.
- *Language File* - This is where the switch stores language information.



Source File Type: ● Running Configuration ○ Startup Configuration ○ Mirror Configuration ○ Logging File ○ Language File

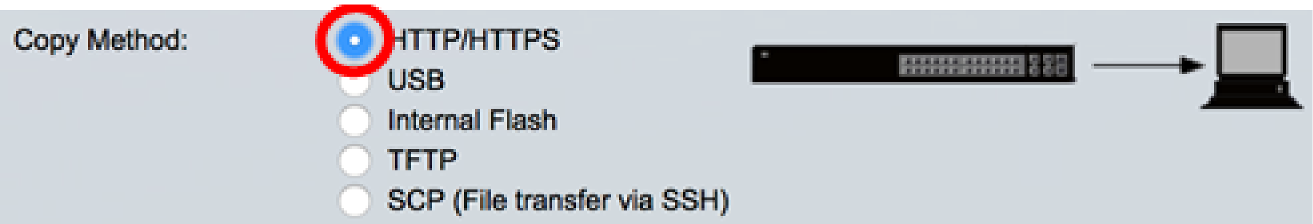
Note: In this example, **Running Configuration** is chosen.

Step 6. Choose one from the following backup methods:

- Via HTTP/HTTPS
- Via USB or Internal Flash
- Via TFTP
- Via SCP (Over SSH)

Back Up a System Configuration File via HTTP/HTTPS

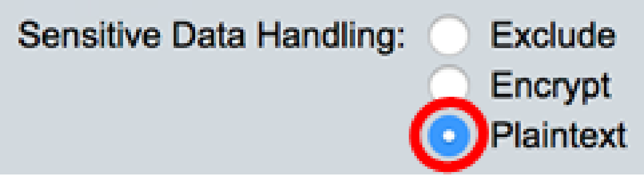
Step 1. Click the **HTTP/HTTPS** button to back up a configuration file on your local computer.



Copy Method: ● HTTP/HTTPS ○ USB ○ Internal Flash ○ TFTP ○ SCP (File transfer via SSH)

Step 2. In the *Sensitive Data Handling* area, choose how sensitive data should be included in the backup file. The options are:

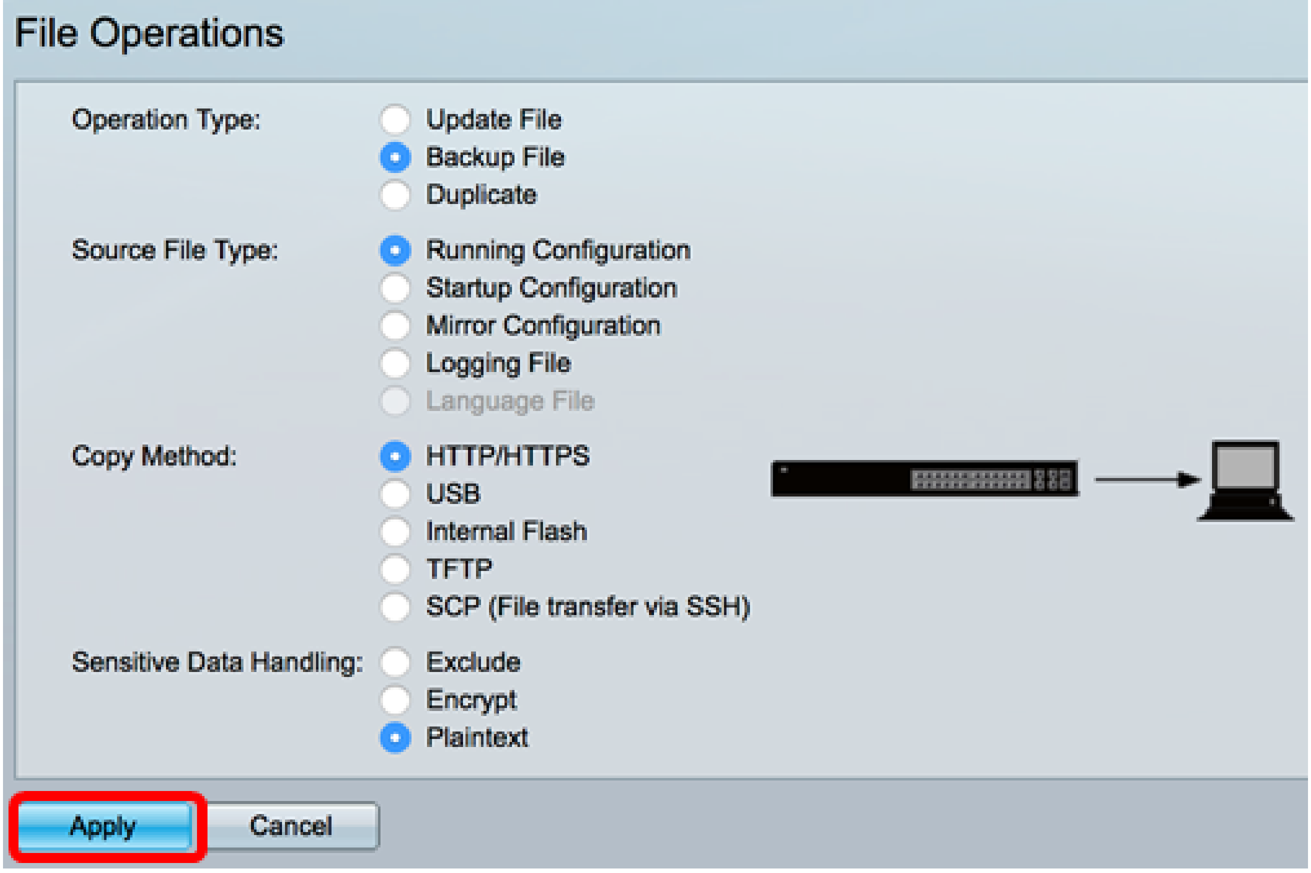
- *Exclude* - Do not include sensitive data in the backup.
- *Encrypt* - Include sensitive data in the backup in its encrypted form.
- *Plaintext* - Include sensitive data in the backup in its plaintext form.



Sensitive Data Handling: ○ Exclude ○ Encrypt ● Plaintext

Note: In this example, **Plaintext** is chosen. This will back up all data in plaintext form.

Step 3. Click **Apply**.



File Operations

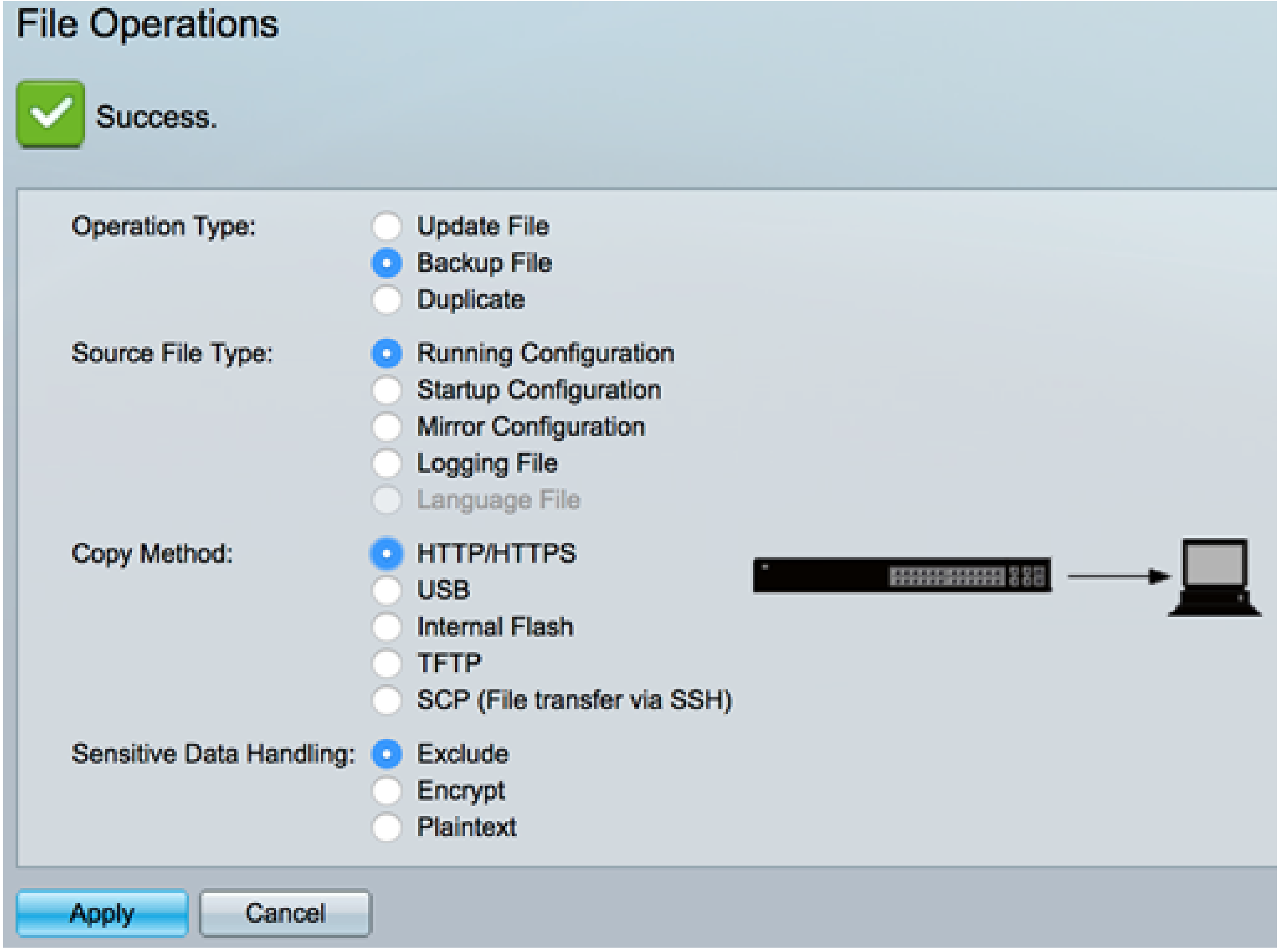
Operation Type: ○ Update File ● Backup File ○ Duplicate

Source File Type: ● Running Configuration ○ Startup Configuration ○ Mirror Configuration ○ Logging File ○ Language File

Copy Method: ● HTTP/HTTPS ○ USB ○ Internal Flash ○ TFTP ○ SCP (File transfer via SSH)

Sensitive Data Handling: ○ Exclude ○ Encrypt ● Plaintext

Once the operation is finished, a Success message will be displayed in the *File Operations* page.



File Operations

✓ Success.

Operation Type: ○ Update File ● Backup File ○ Duplicate

Source File Type: ● Running Configuration ○ Startup Configuration ○ Mirror Configuration ○ Logging File ○ Language File

Copy Method: ● HTTP/HTTPS ○ USB ○ Internal Flash ○ TFTP ○ SCP (File transfer via SSH)

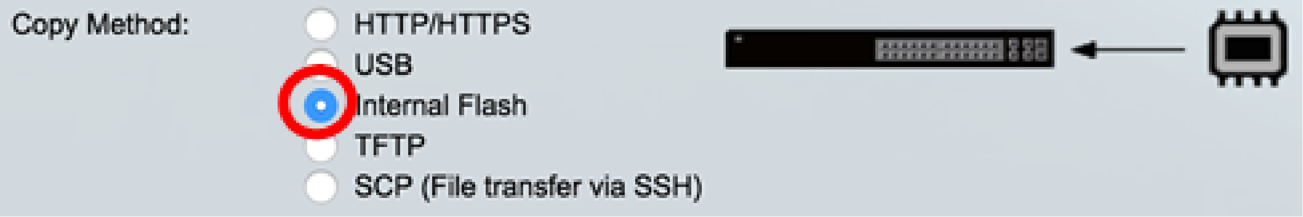
Sensitive Data Handling: ● Exclude ○ Encrypt ○ Plaintext

You should now have successfully backed up the configuration file of your switch through the HTTP/HTTPS transfer method.

[Back to Top]

Back Up a System Configuration File via USB or Internal Flash

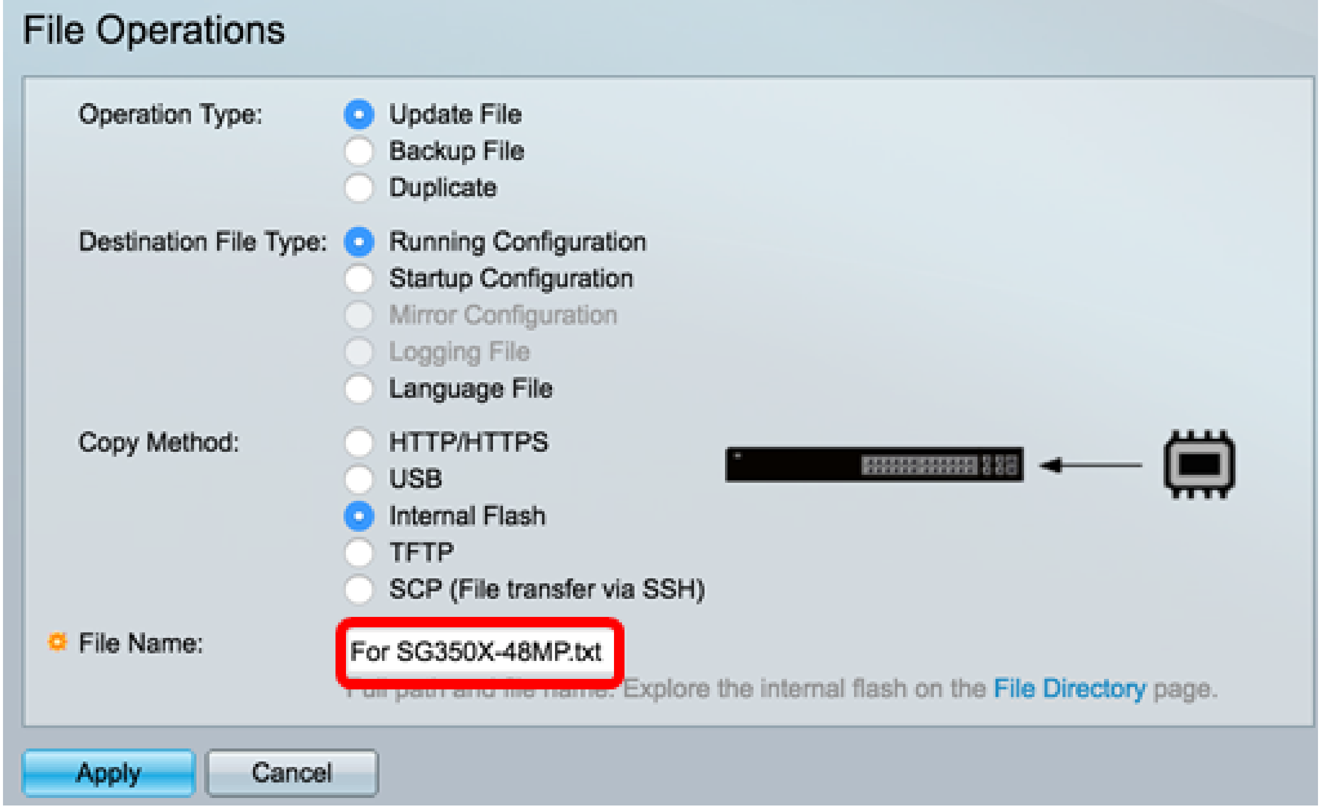
Step 1. Choose either **USB** or **Internal Flash** as the copy method. In this example, Internal Flash is chosen.



Copy Method: ○ HTTP/HTTPS ○ USB ● Internal Flash ○ TFTP ○ SCP (File transfer via SSH)

Step 2. In the *File Name* field, enter name of destination file.

Note: In this example, the running configuration file named SG350X-48MP.txt will be saved in the Internal Flash memory of the switch.



File Operations

Operation Type: ● Update File ○ Backup File ○ Duplicate

Destination File Type: ● Running Configuration ○ Startup Configuration ○ Mirror Configuration ○ Logging File ○ Language File

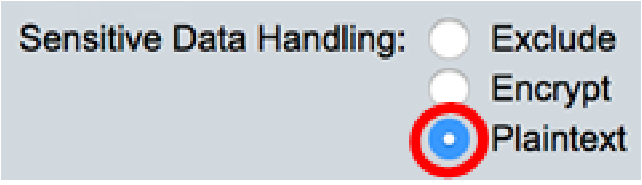
Copy Method: ○ HTTP/HTTPS ○ USB ● Internal Flash ○ TFTP ○ SCP (File transfer via SSH)

File Name: For SG350X-48MP.txt

Full path and file name. Explore the internal flash on the File Directory page.

Step 3. In the Sensitive Data Handling area, choose how sensitive data should be included in the backup file. The options are:

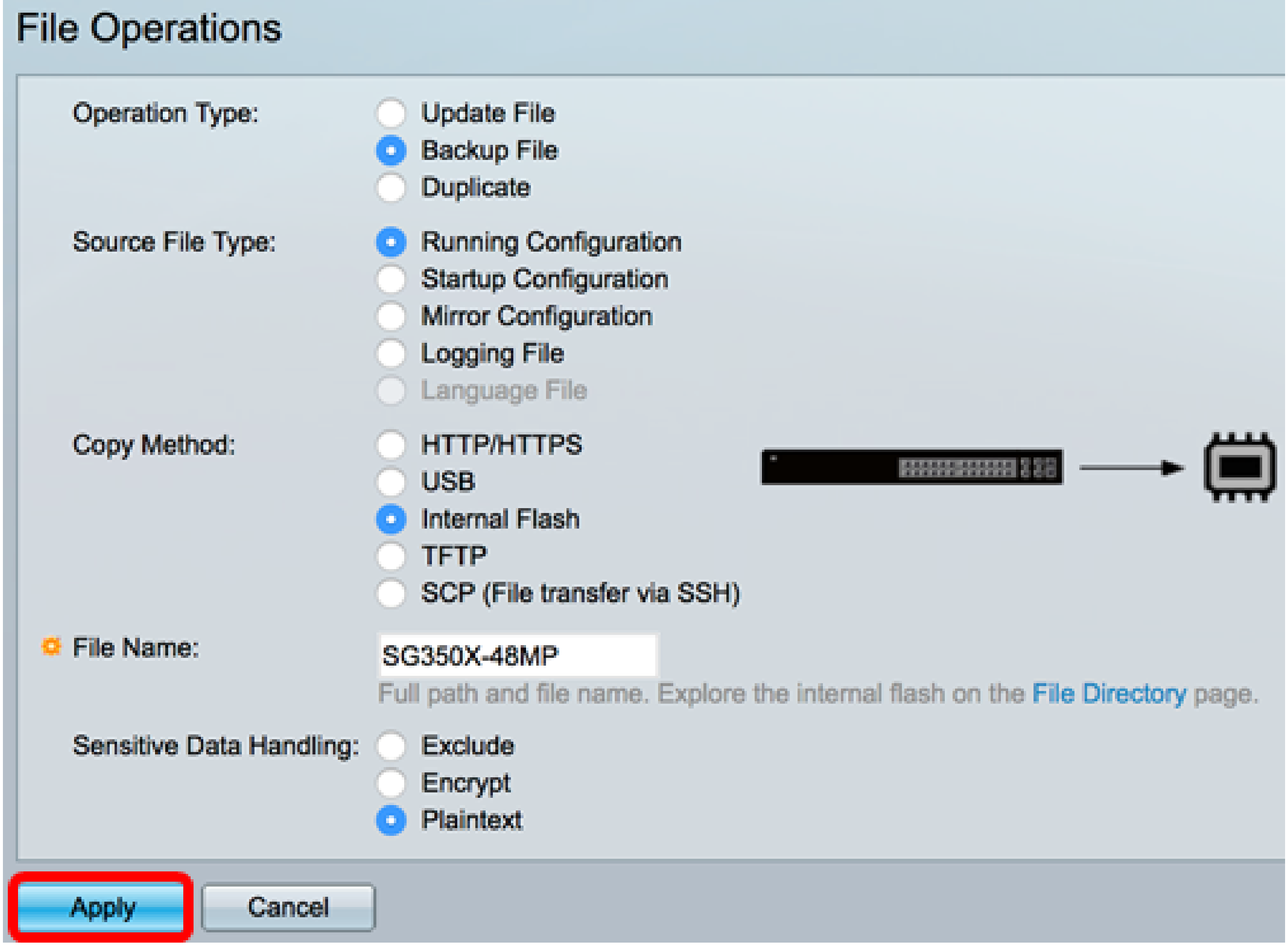
- Exclude — Do not include sensitive data in the backup.
- Encrypt — Include sensitive data in the backup in its encrypted form.
- Plaintext — Include sensitive data in the backup in its plaintext form.



Sensitive Data Handling: ○ Exclude ○ Encrypt ● Plaintext

Note: In this example, Plaintext is chosen. This will back up all data in plaintext form.

Step 4. Click **Apply** to copy the configuration file from the Internal Flash to your switch.



File Operations

Operation Type:
○ Update File
● Backup File
○ Duplicate

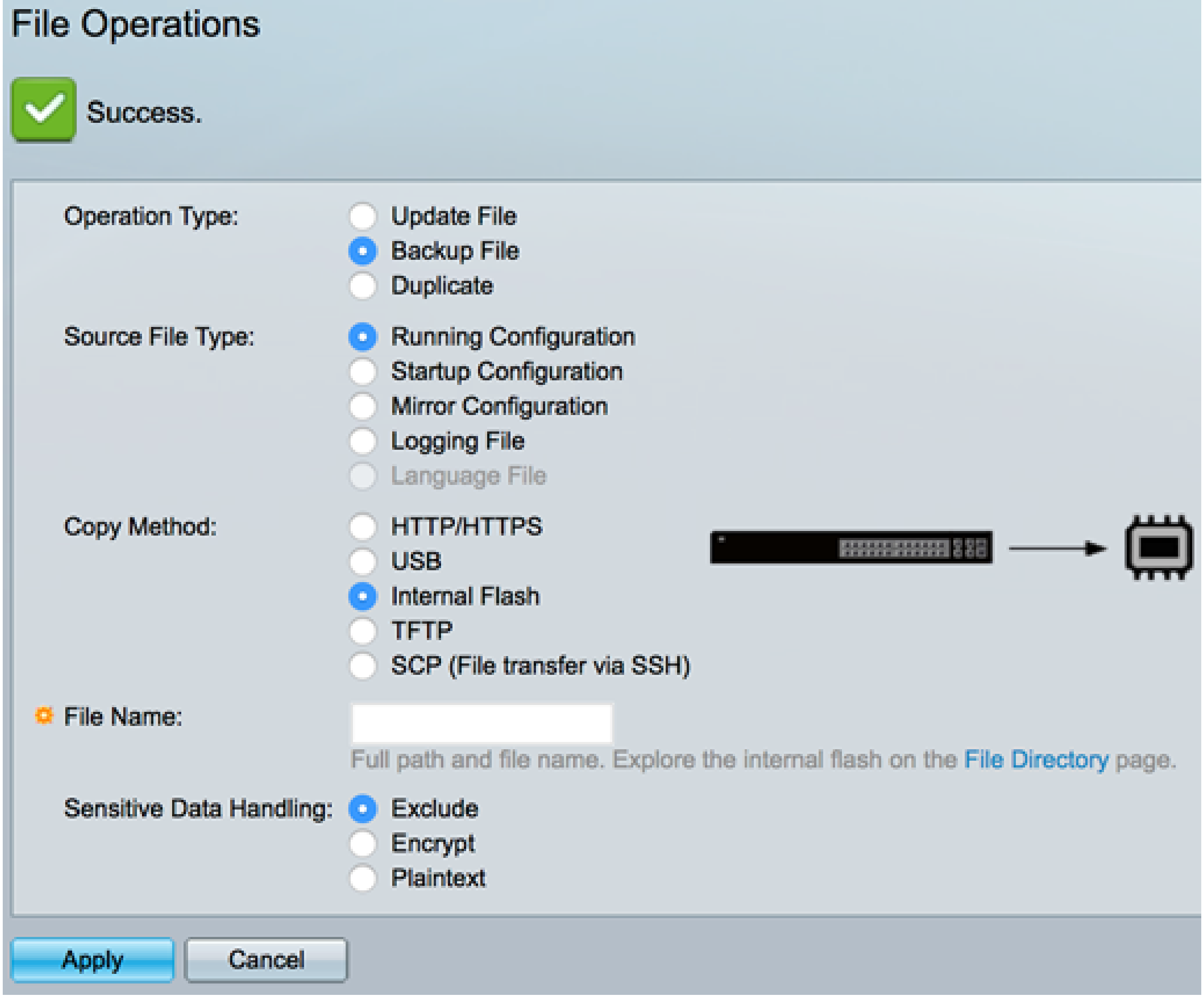
Source File Type:
● Running Configuration
○ Startup Configuration
○ Mirror Configuration
○ Logging File
○ Language File

Copy Method:
○ HTTP/HTTPS
○ USB
● Internal Flash
○ TFTP
○ SCP (File transfer via SSH)

File Name: SG350X-48MP
Full path and file name. Explore the internal flash on the File Directory page.

Sensitive Data Handling:
○ Exclude
○ Encrypt
● Plaintext

Once the operation is finished, a Success message will be displayed in the File Operations page.



File Operations

Success.

Operation Type: ○ Update File ● Backup File ○ Duplicate

Source File Type: ● Running Configuration ○ Startup Configuration ○ Mirror Configuration ○ Logging File ○ Language File

Copy Method: ○ HTTP/HTTPS ○ USB ● Internal Flash ○ TFTP ○ SCP (File transfer via SSH)

File Name:

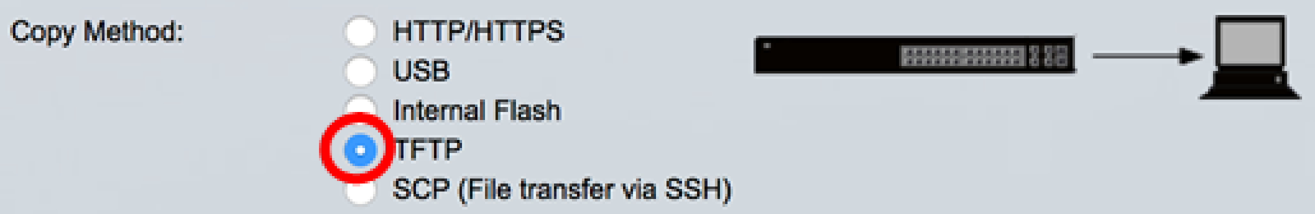
Full path and file name. Explore the internal flash on the File Directory page.

Sensitive Data Handling: ● Exclude ○ Encrypt ○ Plaintext

You should now have successfully backed up the system configuration file on your switch through the Internal Flash or USB copy method.

Back Up a System Configuration File via TFTP

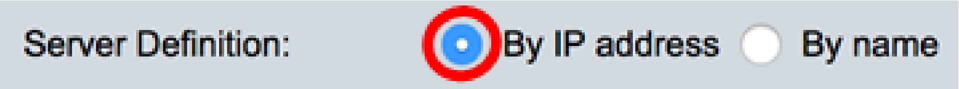
Step 1. In the *Copy Method* area, click the **TFTP**radio button. The TFTP method is chosen to download or back up configuration file via TFTP server. This download or back up of configuration files are done over a secure network.



Copy Method: ○ HTTP/HTTPS ○ USB ○ Internal Flash ● TFTP ○ SCP (File transfer via SSH)

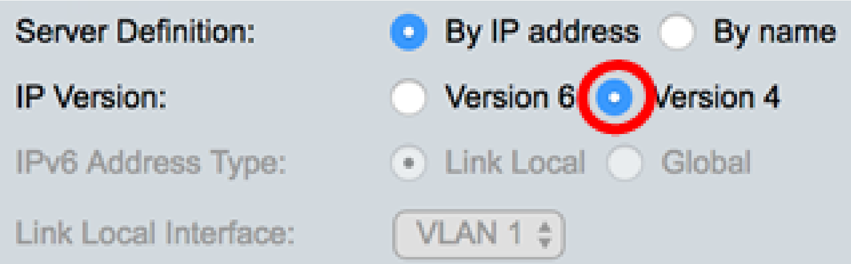
Step 2. Click a radio button in the TFTP *Server Definition* area. The options are:

- *By IP address* - Choose to enter the IP address of the TFTP server. In this example, this option is chosen.
- *By name* - Choose to enter the hostname of the TFTP server. If this option is chosen, skip to Step 4.



Server Definition: ● By IP address ○ By name

Step 3. (Optional) If you chose By IP address, choose either **Version 4** (IPv4) or **Version 6** (IPv6) from the IP Version area. If you chose Version 6, specify whether the IPv6 is a Link Local or Global address in the IPv6 Address Type area. If it is a link local address, choose the interface from the Link Local Interface drop-down list. If Version 4 is chosen, skip to Step 4.



Server Definition: ● By IP address ○ By name

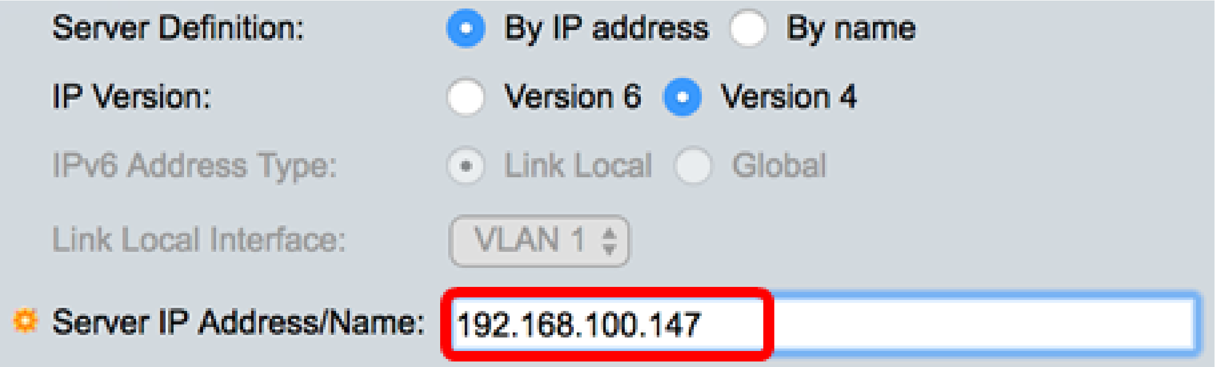
IP Version: ○ Version 6 ● Version 4

IPv6 Address Type: ● Link Local ○ Global

Link Local Interface: VLAN 1

Note: In this example, IP Version 4 is chosen.

Step 4. (Optional) If you selected By name in Step 2, enter the hostname of the TFTP server in the *Server IP Address/Name* field. Otherwise, enter the IP address.



Server Definition: ● By IP address ○ By name

IP Version: ○ Version 6 ● Version 4

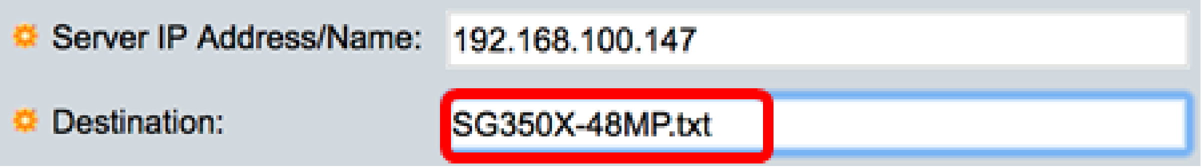
IPv6 Address Type: ● Link Local ○ Global

Link Local Interface: VLAN 1

Server IP Address/Name: 192.168.100.147

Note: In this example, the configuration file will be saved into the TFTP server with 192.168.100.147 IP address.

Step 5. Enter the backup file name in the *Destination* field. In this example, SG350X-48MP.txt is used.

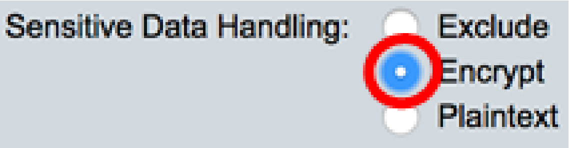


Server IP Address/Name: 192.168.100.147

Destination: SG350X-48MP.txt

Step 6. In the *Sensitive Data Handling* area, choose how sensitive data should be included in the backup file. The options are:

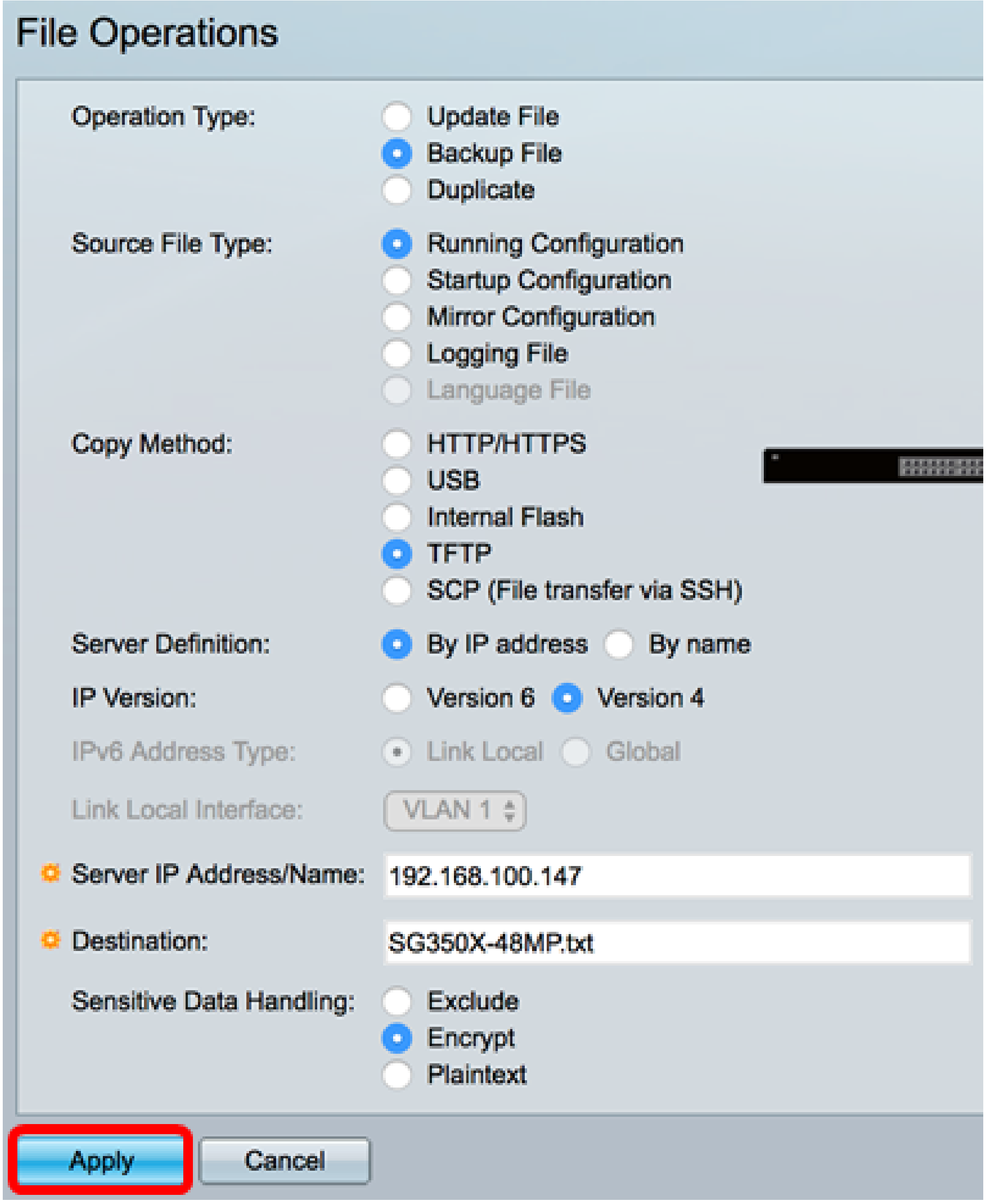
- *Exclude* - Do not include sensitive data in the backup.
- *Encrypt* - Include sensitive data in the backup in its encrypted form.
- *Plaintext* - Include sensitive data in the backup in its plaintext form.



Sensitive Data Handling: ○ Exclude ● Encrypt ○ Plaintext

Note: In this example, Encrypt is chosen. This will back up all data in encrypted form.

Step 7. Click **Apply** to start the backup operation.



File Operations

Operation Type: ○ Update File ● Backup File ○ Duplicate

Source File Type: ● Running Configuration ○ Startup Configuration ○ Mirror Configuration ○ Logging File ○ Language File

Copy Method: ○ HTTP/HTTPS ○ USB ○ Internal Flash ● 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

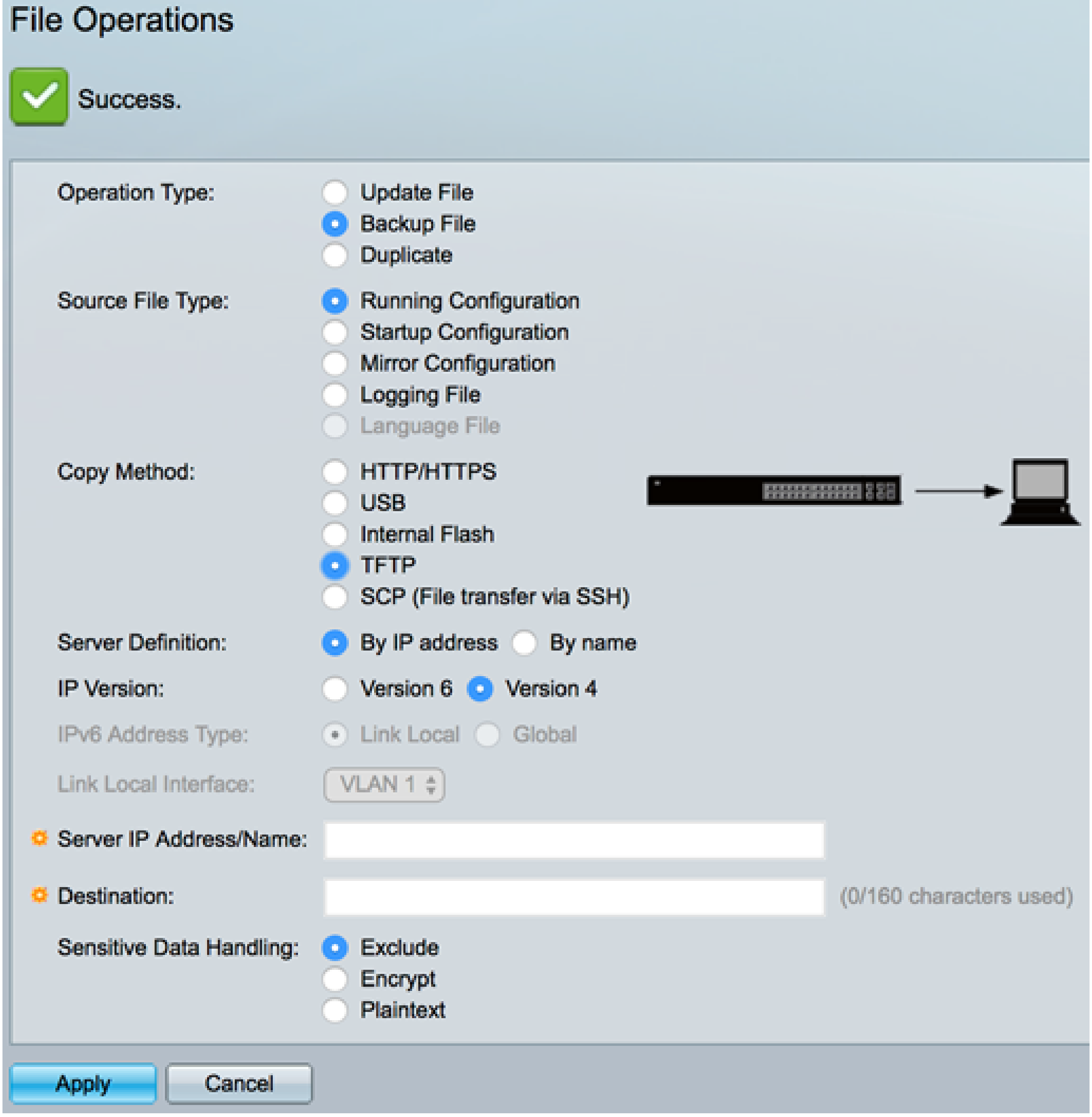
Link Local Interface: VLAN 1

Server IP Address/Name: 192.168.100.147

Destination: SG350X-48MP.txt

Sensitive Data Handling: ○ Exclude ● Encrypt ○ Plaintext

Once the operation is finished, a Success message will be displayed in the File Operations page.



File Operations

✓ Success.

Operation Type: ○ Update File ● Backup File ○ Duplicate

Source File Type: ● Running Configuration ○ Startup Configuration ○ Mirror Configuration ○ Logging File ○ Language File

Copy Method: ○ HTTP/HTTPS ○ USB ○ Internal Flash ● 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:

Destination: (0/160 characters used)

Sensitive Data Handling: ● Exclude ○ Encrypt ○ Plaintext

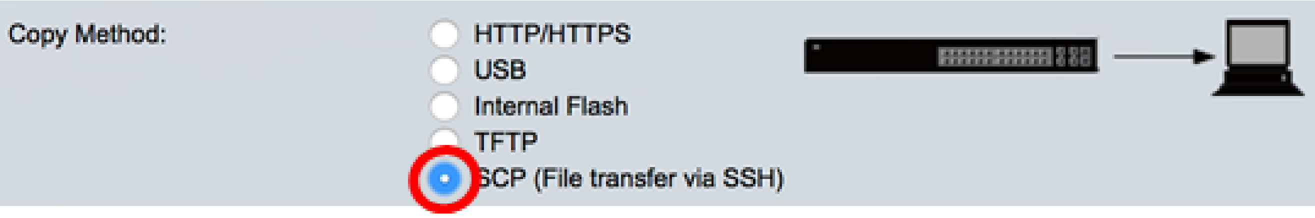
You should now have successfully backed up the configuration file of your switch through the TFTP copy method.

[Back to Top]

Back Up a System Configuration File using SCP (Over SSH)

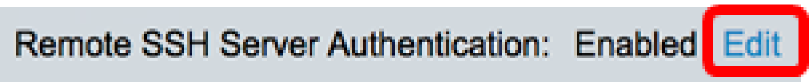
Important: Before you proceed with the SCP method, make sure that SSH server authentication is enabled and the corresponding settings have been configured. For instructions on how to configure SSH authentication settings on your switch, click here.

Step 1. In the Copy Method area, click the **SCP (File transfer via SSH)** radio button. The SCP method is chosen to download or back up configuration file via Secure Shell (SSH). This download or back up of configuration files are done over a secure network.



Copy Method: ○ HTTP/HTTPS ○ USB ○ Internal Flash ○ TFTP ● SCP (File transfer via SSH)

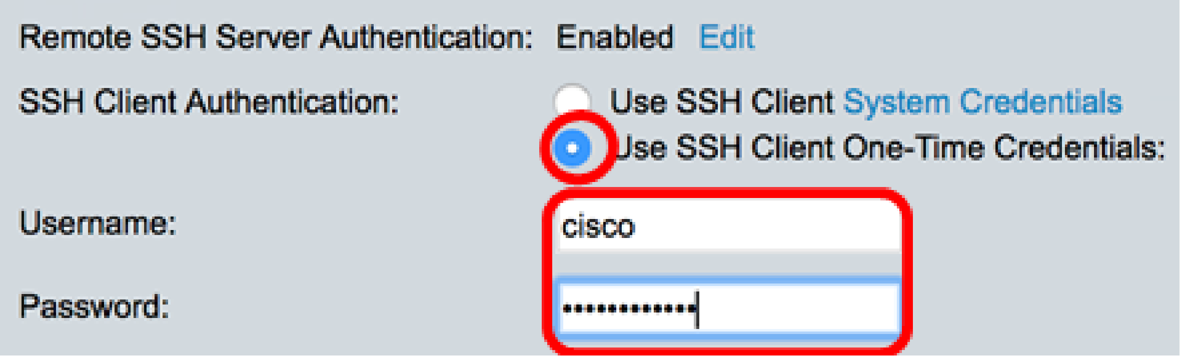
Step 2. Make sure that the Remote SSH Server Authentication is set to **Enabled**. This feature authenticates SSH servers, making sure that the expected SSH server is the correct one. It is disabled by default. Even when disabled, this feature will not affect SSH communications for file operations. If disabled, click **Edit** to enable the feature.



Remote SSH Server Authentication: Enabled Edit

Step 3. Choose a radio button in the SSH Client Authentication area to specify which SSH credentials to use when contacting the remote host. Choose **Use SSH Client System Credentials** to use the permanent SSH credentials stored on the switch (these credentials can be set for future use by clicking System Credentials, which opens the SSH User Authentication page, or choose **Use SSH Client One-Time Credentials** to use temporary credentials.

Note: The username and password for one-time credential will not be saved in configuration file.



Remote SSH Server Authentication: Enabled Edit

SSH Client Authentication: ○ Use SSH Client System Credentials ● Use SSH Client One-Time Credentials:

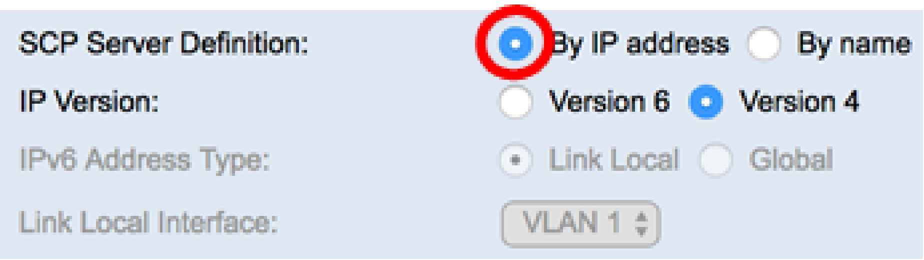
Username: cisco

Password: ••••••••••••

Note: In this example, Use SSH Client One-Time Credentials is chosen and the username and password details are entered accordingly.

Step 4. Click a radio button in the *SCP Server Definition* area. The options are:

- *By IP address* - Choose to enter the IP address of the SCP server. In this example, this option is chosen.
- *By name* - Choose to enter the hostname of the SCP server. If this option is chosen, skip to Step 6.



SCP Server Definition: ● By IP address ○ By name

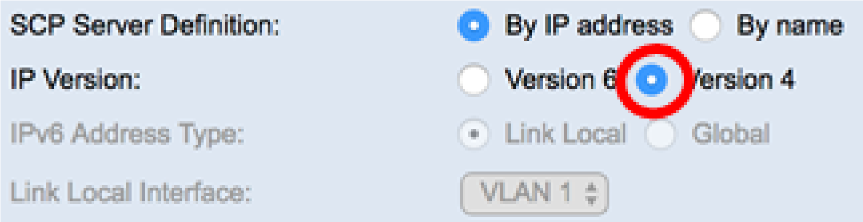
IP Version: ○ Version 6 ● Version 4

IPv6 Address Type: ● Link Local ○ Global

Link Local Interface: VLAN 1

Step 5. (Optional) If you chose By IP address, choose either **Version 4** (IPv4) or **Version 6** (IPv6) from the IP Version area. If you chose Version 6, specify whether the IPv6 is a Link

Local or Global address in the IPv6 Address Type area. If it is a link local address, choose the interface from the Link Local Interface drop-down list. If Version 4 is chosen, skip to Step 6.



SCP Server Definition: ● By IP address ○ By name

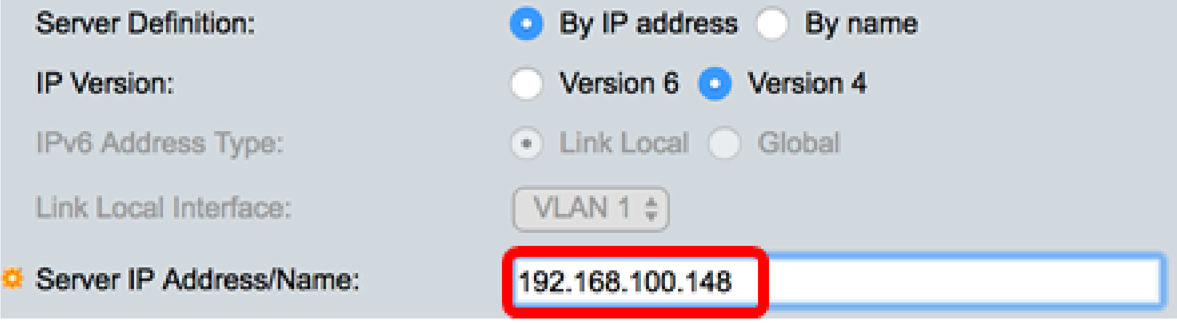
IP Version: ○ Version 6 ● Version 4

IPv6 Address Type: ● Link Local ○ Global

Link Local Interface: VLAN 1

Note: In this example, IP Version 4 is chosen.

Step 6. (Optional) If you selected By name in Step 4, enter the hostname of the TFTP server in the *Server IP Address/Name* field. Otherwise, enter the IP address.



Server Definition: ● By IP address ○ By name

IP Version: ○ Version 6 ● Version 4

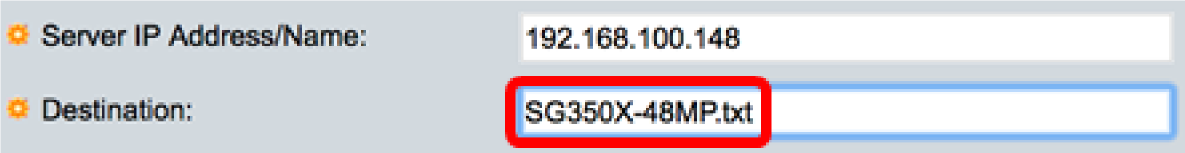
IPv6 Address Type: ● Link Local ○ Global

Link Local Interface: VLAN 1

Server IP Address/Name: 192.168.100.148

Note: In this example, the configuration file will be saved into the SCP server with 192.168.100.148 IP address.

Step 7. Enter the backup file name in the *Destination* field. In this example, the backup configuration file will be saved in the SG350X-48MP.txt file.

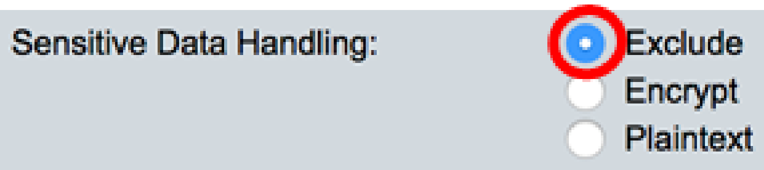


Server IP Address/Name: 192.168.100.148

Destination: SG350X-48MP.txt

Step 8. In the Sensitive Data Handling area, choose how sensitive data should be included in the backup file. The options are:

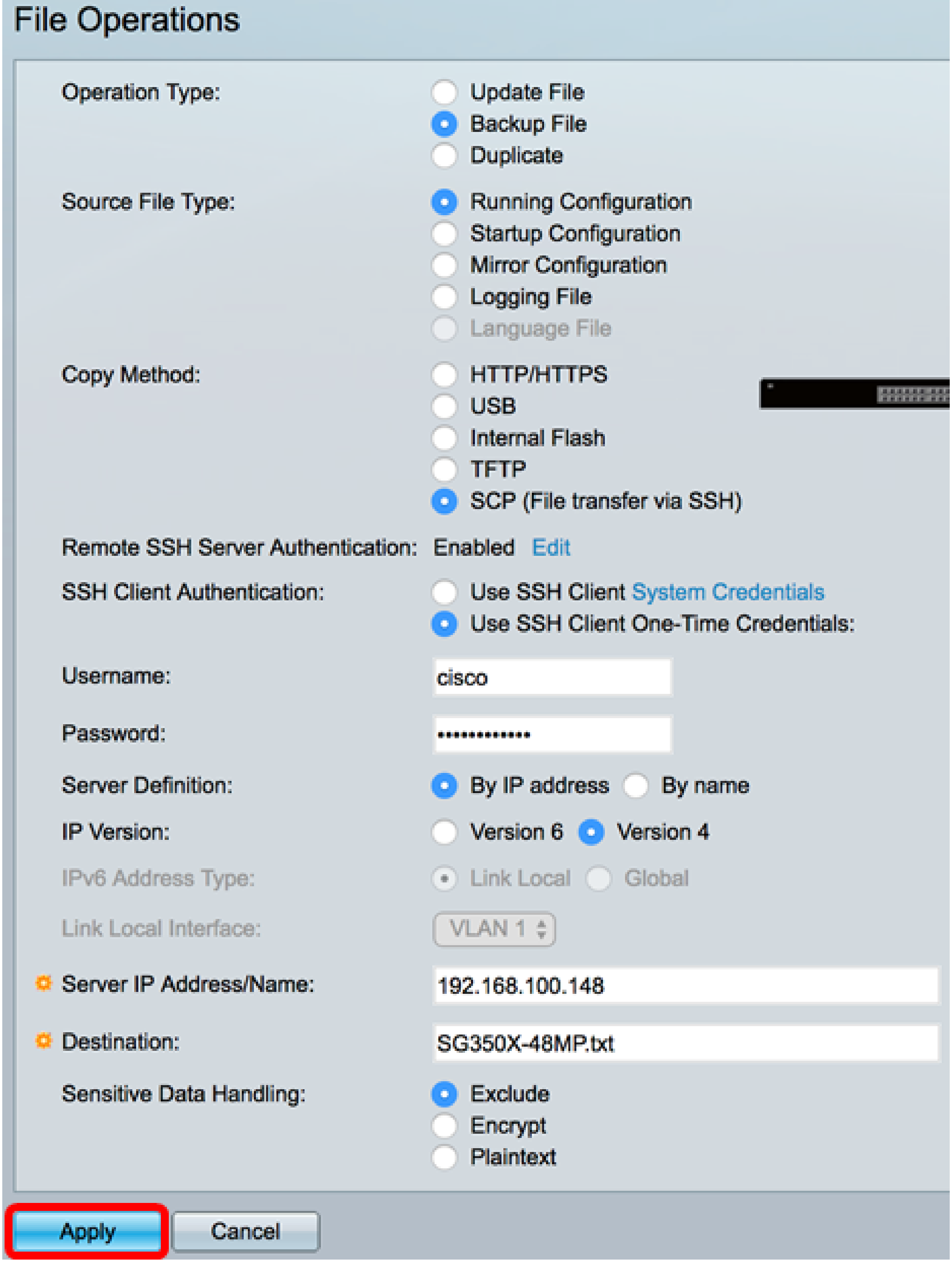
- *Exclude* - Do not include sensitive data in the backup.
- *Encrypt* - Include sensitive data in the backup in its encrypted form.
- *Plaintext* - Include sensitive data in the backup in its plaintext form.



Sensitive Data Handling: ● Exclude ○ Encrypt ○ Plaintext

Note: In this example, Exclude is chosen. The backup file will not include sensitive data.

Step 9. Click **Apply** to start the backup operation.



File Operations

Operation Type: ○ Update File ● Backup File ○ Duplicate

Source File Type: ● Running Configuration ○ Startup Configuration ○ Mirror Configuration ○ Logging File ○ Language File

Copy Method: ○ HTTP/HTTPS ○ USB ○ Internal Flash ○ TFTP ● SCP (File transfer via SSH)

Remote SSH Server Authentication: Enabled Edit

SSH Client Authentication: ○ Use SSH Client System Credentials ● Use SSH Client One-Time Credentials:

Username: cisco

Password: •••••••••••••

Server Definition: ● By IP address ○ By name

IP Version: ○ Version 6 ● Version 4

IPv6 Address Type: ● Link Local ○ Global

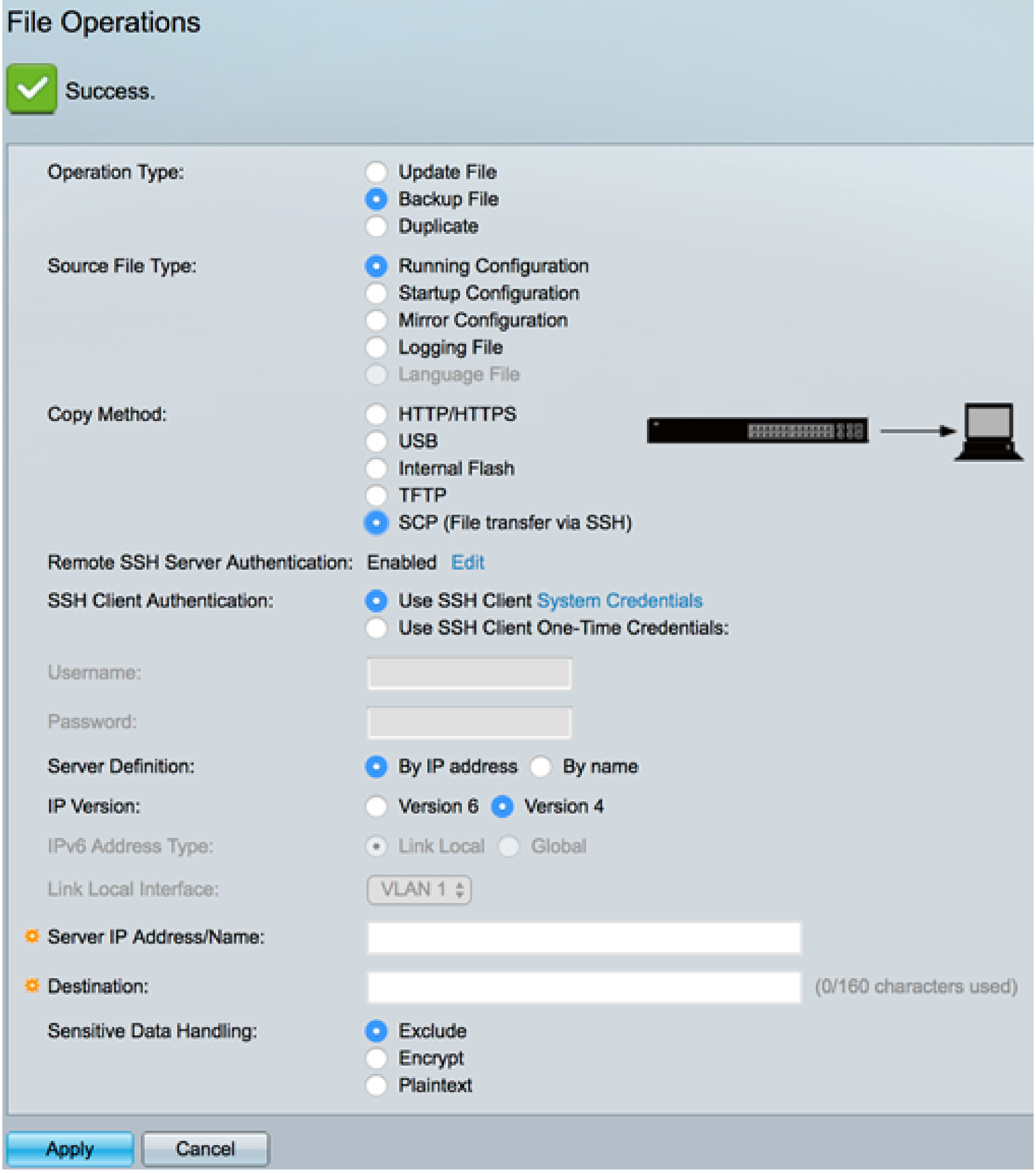
Link Local Interface: VLAN 1

Server IP Address/Name: 192.168.100.148

Destination: SG350X-48MP.txt

Sensitive Data Handling: ● Exclude ○ Encrypt ○ Plaintext

Once the operation is finished, a Success message will be displayed in the File Operations page.



File Operations

✓ Success.

Operation Type:	○ Update File ● Backup File ○ Duplicate
Source File Type:	● Running Configuration ○ Startup Configuration ○ Mirror Configuration ○ Logging File ○ Language File
Copy Method:	○ HTTP/HTTPS ○ USB ○ Internal Flash ○ TFTP ● SCP (File transfer via SSH)
Remote SSH Server Authentication:	Enabled 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:	VLAN 1
Server IP Address/Name:	
Destination:	(0/160 characters used)
Sensitive Data Handling:	● Exclude ○ Encrypt ○ Plaintext

You should now have successfully backed up the configuration file of your switch through the SCP copy method.

[Back to Top]

To know how to update a configuration file on a switch, click here. To duplicate a configuration file, click here for instructions.