

Configuration of Download and Backup Configuration Settings and Logs on 200/300 Series Managed Switches

Objective

This document explains how to download and backup configurations and logs on the 200/300 switch series. When you download the configurations and logs, it allows you to download previously saved configurations to the switch. When you backup the configuration and logs, the switch saves a copy of the desired configuration and logs onto another device.

Applicable Devices

- SF/SG 200 and SF/SG 300 Series Managed Switches

Software Version

- 1.3.0.62

Download/Backup Configuration/Log

Via TFTP

Step 1. Log in to the web configuration utility and choose **Administration > File Management > Download/Backup Configuration/Log**. The *Download/Backup Configuration/Log* window appears:

Download/Backup Configuration/Log

Transfer Method: via TFTP
 via HTTP/HTTPS
 via SCP (Over SSH)

Save Action: Download
 Backup

TFTP Server Definition: By IP address By name

IP Version: Version 6 Version 4

IPv6 Address Type: Link Local Global

Link Local Interface:

⚠ TFTP Server IP Address/Name:

⚠ Source File Name: (0/160 Characters Used)

Destination File Type: Running configuration file
 Startup configuration file
 Backup configuration file

Step 2. Click **via TFTP** to use trivial file transfer protocol as your download and backup transfer method.

Step 3. Click the radio button of an action in the Save Action field. The available actions are:

- Download - This option specifies that the file on the switch will be replaced by a file on another device.
- Backup - This option specifies that the file on the switch will be copied to another device.

Step 4. Click the radio button of a type of TFTP server definition in the TFTP Server Definition field. The available options are:

- By IP address - This option allows you can connect to the TFTP server by IP address.
- By name - This option allows you can connect to the TFTP server by domain name.

Timesaver: If you chose By Name in Step 4, skip to Step 8.

Step 5. If you chose By IP address in Step 4, click the radio button of an IP version in the IP Version field. The available options are:

- Version 6 - Select this if a IPv6 type address is used.
- Version 4 - Select this if a IPv4 type address is used.

Timesaver: If you chose Version 4 in Step 5, skip to Step 8.

Step 6. If you chose Version 6 in Step 5, then click the radio button of type of version 6 address in the IPv6 Type address field. The available options are:

- Link Local - This option allows you to select an IPv6 address on the local network.
- Global - This option allows you to select an IPv6 address that is visible on all networks.

Timesaver: If you chose Global in Step 6, skip to Step 8.

Step 7. If you chose Link Local in Step 6, then from the Link Local Interface drop-down list, choose the local port for file transfer.

Step 8. In the TFTP Server IP Address/Name field, enter the IP address or the domain name of the TFTP server.

Timesaver: If you chose Backup in Step 3, skip to Step 11.

Step 9. If you chose Download in Step 3, then in the Source File Name field, enter the name of the source file that will be downloaded onto the switch.

Step 10. If you chose Download in Step 3, then click the radio button of the type of file in the Destination File Type field. The available options are:

- Running configuration file - The configuration that is currently being used by the switch.
- Startup configuration - The configuration that is used when the switch is rebooted.
- Backup Configuration — The configuration that is manually saved for backup.

Download/Backup Configuration/Log

Transfer Method: via TFTP
 via HTTP/HTTPS
 via SCP (Over SSH)

Save Action: Download
 Backup

TFTP Server Definition: By IP address By name

IP Version: Version 6 Version 4

IPv6 Address Type: Link Local Global

Link Local Interface:

⚠ TFTP Server IP Address/Name:

Source File Type: Running configuration file
 Startup configuration file
 Backup configuration file
 Mirror configuration file
 Flash Log

Sensitive Data: Exclude
 Encrypted
 Plaintext
Available sensitive data options are determined by the current user's SSD rules

⚠ Destination File Name: (6/160 Characters Used)

Step 11. If you chose Backup in Step 3, then click the radio button of the type of file in the Source File Type field. The available options are:

- Running configuration - The configuration that is currently being used by the switch.
- Startup configuration - The configuration that is used by the switch after reboot.
- Backup configuration - The configuration that is manually saved for backup.
- Mirror configuration - This is a copy of the Startup configuration that is made when the switch

has been operating continuously for 24 hours, has had no changes made to the running configuration in the past 24 hours, or if the startup configuration is identical to the running configuration.

- Flash log - This is the log of system messages that are stored in flash memory.

Step 12. Click the radio button of a type of sensitive data in the Sensitive Data field. The available options are:

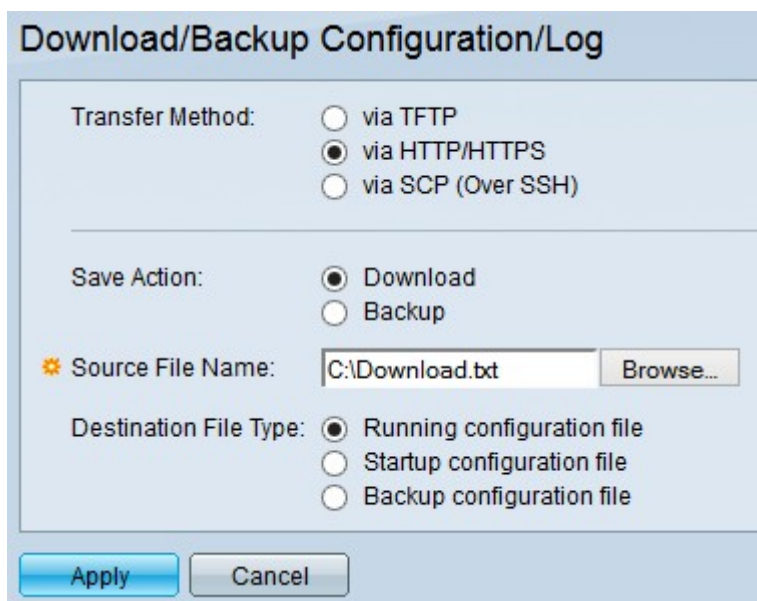
- Exclude - This option does not include sensitive data in the backup.
- Encrypted - This option encrypts sensitive data in the backup.
- Plaintext - This option includes the sensitive data in the backup in plain text form.

Step 13. In the Destination File Name field, enter the desired name of the file that will be downloaded onto the other device.

Step 14. Click **Apply** to save your configuration.

HTTP/HTTPS Configuration

Step 1. Log in to the web configuration utility and choose **Administration > File Management > Download/Backup Configuration/Log**. The *Download/Backup Configuration/Log* page opens:



Step 2. Click **via HTTP/HTTPS** to use HTTP/HTTPS as your download and backup transfer method.

Step 3. Click the radio button of an action in the Save Action field. The available actions are:

- Download - This option specifies that the file on the switch will be replaced by a file on another device.
- Backup - This option specifies that the file on the switch will be copied to another device.

Timesaver: If you chose Backup in Step 3, skip to Step 5.

Step 4. If you chose Download in Step 3, then click **Browse** in the Source File Name field and choose a source file from your computer to be loaded onto the switch.

Step 5. If you chose Download in Step 3, then click the radio button of the type of file in the

Destination File Type field. The available options are:

- Running configuration file - The configuration that is currently being used by the switch.
- Startup configuration - The configuration that is used when the switch is rebooted.
- Backup Configuration - The configuration that is manually saved for backup.

Download/Backup Configuration/Log

Transfer Method: via TFTP
 via HTTP/HTTPS
 via SCP (Over SSH)

Save Action: Download
 Backup

Source File Type: Running configuration file
 Startup configuration file
 Backup configuration file
 Mirror configuration file
 Flash Log

Sensitive Data: Exclude
 Encrypted
 Plaintext

Available sensitive data options are determined by the current user's SSD rules

Apply Cancel

Step 6. If you chose Backup in Step 3, then click the radio button of the type of file in the Source File Type field. The available options are:

- Running configuration - The configuration that is currently being used by the switch.
- Startup configuration - The configuration that is used by the switch after reboot.
- Backup configuration - The configuration that is manually saved for backup.
- Mirror configuration - This is a copy of the Startup configuration that is made when the switch has been operating continuously for 24 hours, has had no changes made to the running configuration in the past 24 hours, or if the startup configuration is identical to the running configuration.
- Flash log - This is the log of system messages that are stored in flash memory.

Step 7. If you chose Backup in Step 3, then click the radio button of a type of sensitive data in the Sensitive Data field. The available options are:

- Exclude - This option does not include sensitive data in the backup.
- Encrypted - This option encrypts sensitive data in the backup.
- Plaintext - This option includes the sensitive data in the backup in plain text form.

Step 8. Click **Apply** to save your configuration.

Via SCP (Over SSH)

Step 1. Log in to the web configuration utility and choose **Administration > File Management > Download/Backup Configuration/Log**. The *Download/Backup Configuration/Log* page opens:

SSH User Authentication

Transfer Method:

via TFTP
 via HTTP/HTTPS
 via SCP (Over SSH)

SSH Settings For SCP:

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

SSH Client Authentication:

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

Username (The username is not saved in the configuration file)

Password (The password is not saved in the configuration file)

Save Action:

Download
 Backup

SCP Server Definition:

By IP address By name

IP Version:

Version 6 Version 4

IPv6 Address Type:

Link Local Global

Link Local Interface:

SCP Server IP Address/Name:

Source File Name: (8/160 Characters Used)

Destination File Type:

Running configuration file
 Startup configuration file
 Backup configuration file

Step 2. Click **via SCP (Over SSH)** to use Secure Copy Protocol over Secure Shell as your download and backup transfer method.

Note: The Remote SSH Server Authentication field displays the status of the SSH server. The Edit button takes you to the *SSH Server Authentication* page. For more information on how to configure the SSH server, refer to the article [Secure Shell \(SSH\) Server Authentication on the 300 Series Managed Switches](#).

Step 3. Click the radio button SSH client authentication method in the SSH Client Authentication field. The available options are:

- Use SSH Client - This option lets you establish permanent SSH credentials for users.

Note: The System Credentials button takes you to the *SSH User Authentication* page. For more information about the configuration of SSH User Authentication, refer to the article [Secure Shell \(SSH\) Client User Authentication on the 300 Series Managed Switches](#).

- Use SSH Client One-Time Credentials - This option lets you enter a specific user credential for this action only:
 - Username - Enter the user name to be use for this action.
 - Password - Enter the password to be use for this action.

Step 4. Click the radio button of an action in the Save Action field. The available actions are:

- Download - This option specifies that the file on the switch will be replaced by a file on another device.
- Backup - This option specifies that the file on the switch will be copied to another device.

Step 5. Click the radio button of a type of SCP server definition in the SCP Server Definition field. The available options are:

- By IP address - This option makes it so that you can connect to the SCP server by IP address.
- By name - This option makes it so that you can connect to the SCP server by domain name.

Timesaver: If you chose By Name in Step 5, skip to Step 9.

Step 6. If you chose By IP address in Step 5, then click the radio button of an IP version in the IP Version field. The available options are:

- Version 6 - Select this if a IPv6 type address is used.
- Version 4 - Select this if a IPv4 type address is used.

Timesaver: If you chose Version 4 in Step 6, skip to Step 9.

Step 7. If you chose Version 6 in Step 6, then click the radio button of type of version 6 address in the IPv6 Type address field. The available options are:

- Link Local - This option allows you to select an IPv6 address on the local network.
- Global - This option allows you to select an IPv6 address that is visible on all networks.

Timesaver: If you chose Global in Step 7, skip to Step 9.

Step 8. If you chose Link Local in Step 7, then from the Link Local Interface drop-down list, choose the local port for file transfer.

Step 9. In the SCP Server IP Address/Name field, enter the IP address or the domain name of the SCP server.

Timesaver: If you chose Backup in Step 4, skip to Step 12.

Step 10. If you chose Download in Step 4, then in the Source File Name field, enter the name of the source file that will be downloaded onto the switch.

Step 11. If you chose Download in Step 4, then click the radio button of the type of file in the Destination File Type field. The available options are:

- Running configuration file - The configuration that is currently being used by the switch.
- Startup configuration - The configuration that is used when the switch is rebooted.
- Backup Configuration - The configuration that is manually saved for backup.

SSH User Authentication

Transfer Method:

via TFTP
 via HTTP/HTTPS
 via SCP (Over SSH)

SSH Settings For SCP:

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

SSH Client Authentication:

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

Username (The username is not saved in the configuration file)

Password (The password is not saved in the configuration file)

Save Action:

Download
 Backup

SCP Server Definition: By IP address By name

IP Version: Version 6 Version 4

IPv6 Address Type: Link Local Global

Link Local Interface:

SCP Server IP Address/Name:

Source File Type:

Running configuration file
 Startup configuration file
 Backup configuration file
 Mirror configuration file
 Flash Log

Sensitive Data:

Exclude
 Encrypted
 Plaintext

Available sensitive data options are determined by the current user's SSD rules

Destination File Name: (6/160 Characters Used)

Step 12. If you chose Backup in Step 4, then click the radio button of the type of file in the Source File Type field. The available options are:

- Running configuration - The configuration that is currently being used by the switch.
- Startup configuration - The configuration that is used by the switch after reboot.
- Backup configuration - The configuration that is manually saved for backup.
- Mirror configuration - This is a copy of the Startup configuration that is made when the switch has been operating continuously for 24 hours, has had no changes made to the running configuration in the past 24 hours, or if the startup configuration is identical to the running configuration.
- Flash log - This is the log of system messages that are stored in flash memory.

Step 13. Click the radio button of a type of sensitive data in the Sensitive Data field. The available options are:

- Exclude - This option does not include sensitive data in the backup.
- Encrypted - This option encrypts sensitive data in the backup.
- Plaintext - This option includes the sensitive data in the backup in plain text form.

Step 14. In the Destination File Name field, enter the desired name of the file that will be

downloaded onto the other device.

Step 15. Click **Apply** to save your configuration.