



Brocade[®] Fabric OS[®] Software Upgrade Guide, 9.2.x

User Guide
April 28, 2023

Table of Contents

Introduction.....	4
About This Document.....	4
Supported Hardware and Software.....	4
Contacting Technical Support for Your Brocade® Product.....	4
Document Feedback.....	5
Obtaining Firmware.....	6
Download Prerequisites.....	6
Finding the Switch Firmware Version.....	8
Brocade TruFOS Certificates.....	9
Downloading Firmware.....	11
Enabling the USB Device.....	12
Staging Firmware.....	13
Validating the Firmware Download.....	14
Downloading Firmware from a USB Device.....	14
Viewing the USB File System.....	15
Downloading Firmware from a USB Device Using a Relative Path.....	15
Upgrading and Downgrading Firmware.....	16
Supported Upgrade Paths.....	17
Supported Blades.....	18
Upgrade or Downgrade Prerequisites.....	18
Connected Switches.....	19
General Upgrade Considerations.....	19
General Downgrade Considerations.....	20
Upgrading Firmware on Fixed-Port Switches.....	21
Firmware Download with Legacy Mode.....	21
FPGA Firmware Upgrade Utility.....	22
Upgrading Firmware on Directors (Including Blades).....	23
Validating the Firmware Version and Firmware Signature.....	26
Verifying the Device and Fabric Connections.....	26
Testing Firmware.....	27
Testing and Restoring Firmware on Switches.....	27
Testing a Different Firmware Version on a Switch.....	27
Committing Evaluation Firmware.....	27
Reverting Evaluation Firmware.....	28
Testing and Restoring Firmware on Directors.....	28
Testing a Different Firmware Version on a Director.....	28

Test-Driving a New Firmware Version on a Director.....	30
Revision History.....	32
Documentation Legal Notice.....	33

Introduction

This section provides the step-by-step procedures to prepare, perform, and verify the upgrade or downgrade of the Fabric OS® firmware.

About This Document

It is assumed that the reader of this document is familiar with establishing console access and entering commands using the Fabric OS CLI. Although many different software and hardware configurations are tested and supported by Broadcom for Fabric OS v9.2.x firmware, documenting all possible configurations and scenarios is beyond the scope of this document.

Supported Hardware and Software

The following hardware platforms are supported by Brocade Fabric OS 9.2.x.

Brocade Gen 7 (64G) Fixed-Port Switches

- Brocade G720 Switch
- Brocade G730 Switch
- Brocade 7850 Extension Switch

Brocade Gen 7 (64G) Directors

- Brocade X7-4 Director
- Brocade X7-8 Director

Brocade Gen 6 (32G) Fixed-Port Switches

- Brocade G610 Switch
- Brocade G620 Switch
- Brocade G630 Switch
- Brocade 7810 Extension Switch
- Brocade G648 Blade Server SAN I/O Module
- Brocade MXG610 Blade Server SAN I/O Module

Brocade Gen 6 (32G) Directors

- Brocade X6-4 Director
- Brocade X6-8 Director

Contacting Technical Support for Your Brocade® Product

If you purchased Brocade® product support from a Broadcom® OEM or solution provider, contact your OEM or solution provider for all your product support needs.

- OEM and solution providers are trained and certified by Broadcom to support Brocade products.
- Broadcom provides backline support for issues that cannot be resolved by the OEM or solution provider.
- Brocade Supplemental Support augments your existing OEM support contract, providing direct access to Brocade expertise. For more information on this option, contact Broadcom or your OEM.
- For questions regarding service levels and response times, contact your OEM or solution provider.

If you purchased Brocade product support directly from Broadcom, use one of the following methods to contact the Technical Assistance Center 24x7. For product support information and the latest information on contacting the Technical Assistance Center, go to www.broadcom.com/support/fibre-channel-networking/contact-brocade-support.

Online	Telephone
For nonurgent issues, the preferred method is to log on to the Support portal at support.broadcom.com. (You must initially register to gain access to the Support portal.) Once registered, log on and then select Brocade Products. You can now navigate to the following sites: • Case Management • Software Downloads • Licensing • SAN Reports • Brocade Support Link • Training & Education	For Severity 1 (critical) issues, call Brocade Fibre Channel Networking Global Support at one of the phone numbers listed at www.broadcom.com/support/fibre-channel-networking/contact-brocade-support.

Document Feedback

Quality is our first concern. We have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission or if you think that a topic needs further development, we want to hear from you. Send your feedback to documentation.pdl@broadcom.com. Provide the publication title; topic heading; publication number and page number (for PDF documents); URL (for HTML documents); and as much detail as possible.

Obtaining Firmware

This section provides an overview of the procedures you must perform to complete a firmware upgrade or downgrade.

The Fabric OS firmware upgrade process consists of the following major procedures:

1. Choose one of the following options to download the Fabric OS firmware files to a fixed-port switch or director:
 - Download the Fabric OS firmware files from the Broadcom® website.
 - Download the firmware from a USB stick that is attached to the switch.
2. Choose one of the following options to upgrade or downgrade to the newer version of Fabric OS firmware:
 - Upgrade the firmware on a fixed-port switch.
 - Upgrade the firmware on a director.

Fabric OS v9.2.x supports the Platform Specific Download (PSD) versions that load on specific Brocade supported platforms. For example, a Fabric OS `v9.2.0_G7_ENTP` file can be installed only on a Brocade G730 Switch. Fabric OS PSD releases are full versions of a given Fabric OS release that can be loaded only on a single hardware platform. You must download the Fabric OS PSD images separately for each platform that the Fabric OS release will be used on.

For a specific list of supported Fabric OS PSD versions, refer to the corresponding version of Fabric OS release notes.

Fabric OS versions are made available periodically to add features or to remedy defects. Contact your switch support provider to obtain information about available firmware versions.

NOTE

- Broadcom does not supply individual RPM files, only packaged installation file sets (distributions).
- Starting simultaneous firmware downloads on adjacent fixed-port switches might result in a traffic disruption.

Do not power-cycle the switch or chassis during the firmware download. For more information on troubleshooting a firmware download, refer to the *Brocade Fabric OS Troubleshooting and Diagnostics Reference Manual*.

ATTENTION

Complete the firmware download process on the current switch before issuing the `firmwaredownload` command on the next switch. This process ensures that traffic between switches in your fabric is not disrupted. To verify that the firmware download process is complete, enter the `firmwaredownloadstatus` command on the switch, verify that the process is complete, and then proceed to the next switch.

Download Prerequisites

This section describes the following types of chassis with Fabric OS v9.2.x:

- **Gen 6 (X6) Chassis** – An X6 chassis containing CPX6 CP blades and CR32 core blades that ships from the factory and can be upgraded to Fabric OS v9.2.x. This chassis also ships from the factory with CPX blades and CR32 core blades with switch type 165.5 or 166.5.
- **Gen 7 Upgraded Chassis** – An X6 chassis containing CPX6 blades that can be upgraded to Gen 7 by replacing the CR32 core blades with Gen 7 (CR64) core blades. After the upgrade to Gen 7, the model name is displayed as CPX6+. A nondisruptive upgrade from Fabric OS v9.1.x to Gen 7 (X7) is supported.
- **Gen 7 (X7) Chassis** – This chassis ships from the factory with Gen 7 CR64 core blades. It contains CPX7 or CPX CP blades and is not backward compatible with a Gen 6 chassis and Fabric OS v8.2.x.

The following prerequisites are for an existing customer with a Gen 6 chassis that wants to upgrade to a Gen 7 chassis:

- Upgrade the Fabric OS version to v9.1.1x.
- Replace the Gen 6 core blades with Gen 7 core blades.
- Install the Brocade Trusted FOS (TruFOS) Certificate – A TruFOS Certificate with a valid expiration date is required for the following tasks:
 - To install Fabric OS v9.2.x or later when running any version of Fabric OS.
 - To install any version of Fabric OS, including pre- Fabric OS v9.2.x versions when running Fabric OS v9.2.x or later.

For more information about Brocade TruFOS Certificates, see [Brocade TruFOS Certificates](#).

NOTE

Once upgraded to Gen 7, you cannot downgrade to any Fabric OS version lower than Fabric OS v9.1.x.

Perform the following tasks before downloading the firmware. The following preparatory tasks allow you to provide your switch support provider with the required information for troubleshooting the firmware download if there is a failure or timeout.

1. Read the updates related to the firmware download process in the release notes.

NOTE

The Fabric OS software does not support nondisruptive upgrades from any release more than one major release earlier than the one being installed. For example, nondisruptive upgrades to Fabric OS v9.2.x is only supported from Fabric OS v9.1.x. Upgrading from an earlier version of the Fabric OS software (for example, 9.0.x), is not supported.

2. Enter the `firmwaredownload -v` command to verify if disk space is sufficient before proceeding with the firmware upgrade steps. If sufficient space is not available, the following warning message is displayed:

```
switch:admin> firmwaredownload -v
Required space available on the switch to proceed firmwaredownload.
```

Perform the disk cleanup and proceed with the further steps to download the firmware.

3. Log the telnet session to record the information shown during the download process. You can use this information to validate the installation. Connect to the switch and log on using an account with admin permissions.

For additional support:

- a) Connect the switch directly to a computer using a serial console cable. Use mini USB console cables for Gen 7 series switches.
- b) Ensure that all serial console sessions for both control processors (CPs) on directors and any open network connection sessions such as telnet sessions are being logged.

4. Enter the `firmwareshow` command to verify the current version of the Fabric OS software.
5. Enter the `hashow` command to check the HA synchronization status if you are downloading the firmware on chassis. If HA is not synchronized, the lack of HA synchronization can be related to any of the following events:
 - A firmware download is in progress.
 - The device is recovering from a reboot or power-cycle.

If the local CP and remote CP have different firmware versions, retry the firmware download. See [Downloading Firmware](#) for information about downloading the Fabric OS software.

6. Enter the `firmwaredownloadstatus` command to confirm that there is no firmware download already in progress. If there is a download in progress, wait until that download process is complete.
7. Ensure that all switches in the fabric are running a version of Fabric OS software that is compatible with the release of Fabric OS software that you are planning to install.
 - a) Validate the existing fabric by running the commands `nsshow`, `nsallshow`, and `fabricshow`. These commands provide a record of the existing fabric, which you can use to validate the installation.

NOTE

All connected servers, storage devices, and switches should be present in the output of the commands in this step. If there is a discrepancy, it is possible that a device or a switch cannot connect to the fabric, and further troubleshooting is required.

- b) Enter the `switchshow` command to verify that no ports are running as G_Ports.
8. Back up the configuration file and retrieve all current core files before downloading the new firmware to the device. You should keep individual backup files for all switches in the fabric and should avoid copying configurations from one switch to another.
9. Enter the `configupload` command to save the configuration file to your FTP or SSH server or to a USB memory device. The `configupload` command, by default, uploads only the switch context configuration for the logical switch context in which the command is executed.
10. Use the `configupload -all` command to include the switch and the chassis information in non-Virtual Fabric mode. In Virtual Fabric mode, the `configupload -all` command can be selected to upload all logical switches and the chassis configuration. Only administrators with chassis permissions are allowed to upload other FIDs or the chassis configuration.

NOTE

Alternately, you can run the `configupload -vf` command followed by the `configupload -all` command on a Virtual Fabric mode enabled switch.

11. Enter the `supportsave` command to retrieve all current core files. This information is useful to troubleshoot the firmware download process if a problem occurs.
12. Enter the `errclear` command to clear all existing messages, including internal messages.
13. Enter the `supportsave -R` command (uppercase *R*). This action clears all core and trace files.
14. Continue with the firmware download.

Finding the Switch Firmware Version

Perform the following steps to find the firmware version of the switch:

1. Connect to the switch and log on using an account with admin permissions.
2. Enter the `version` command.

The following information is displayed:

- `Kernel` – Displays the version of the switch kernel operating system.
- `Fabric OS` – Displays the Fabric OS software version of the switch.
- `Made on` – Displays the build date of the firmware running on the switch.
- `Flash` – Displays the install date of the firmware that is stored in the non-volatile memory.
- `BootProm` – Displays the version of the firmware that is stored in the boot PROM.

The following sample is output from the `version` command.

```
switch:admin> version
Kernel:      5.4.66_rt38
```

```

Fabric OS:  v9.2.0
Made on:    Thu Feb 2 18:20:59 2023
Flash:      Fri Feb 3 04:53:50 2023
BootProm:   4.0.22-sb

```

Brocade TruFOS Certificates

Brocade TruFOS Certificates ensure the integrity and authenticity of the Fabric OS firmware by validating the digital signature. This validation is useful during critical operations such as firmware upgrades or migrations.

Brocade TruFOS Certificates are factory-installed certificates that are supplied with the platforms. Brocade TruFOS Certificates can be requested and provided free of charge for entitled switches from your switch vendor's Assist Portal or Broadcom Support Portal. The digitally signed certificate ensures that the Brocade switch installs only a validated genuine Fabric OS version.

All Brocade Switches and Directors (except embedded switches) require a valid Brocade TruFOS Certificate before upgrading to Fabric OS v9.2.x. When you request a Brocade TruFOS Certificate, you must supply the switch license ID (LID) of each switch on your vendor's Assist site or on the Broadcom Support Portal. You can request up to 100 Brocade TruFOS Certificates at a time by uploading a file listing the LIDs, or you can request up to 10 Brocade TruFOS Certificates by entering the LIDs manually.

The following table describes the Brocade TruFOS Certificate support in various upgrade and downgrade scenarios:

Table 1: Support for Brocade TruFOS Certificates in Various Fabric OS Upgrade and Download Scenarios

Fabric OS Upgrade/Downgrade Scenarios	TruFOS Enforcement
Upgrade from Fabric OS v9.2.0 to a later version of Fabric OS v9.2.x.	A Brocade TruFOS Certificate is enforced.
Upgrade from Fabric OS v9.1.x to Fabric OS v9.2.0	A Brocade TruFOS Certificate is enforced.
Upgrade from Fabric OS v9.1.1b to Fabric OS v9.2.0	A Brocade TruFOS Certificate is enforced.
Upgrade from Fabric OS v9.0.1x to Fabric OS v9.2.0	The upgrade is blocked. You must upgrade to Fabric OS v9.1.x with a Brocade TruFOS Certificate and then upgrade to Fabric OS v9.2.0.
Downgrade from Fabric OS v9.2.0 to Fabric OS v9.1.x	A Brocade TruFOS Certificate is enforced and the installation is blocked with the following Brocade TruFOS Certificate error message: Firmwaredownload failed. TruFOS validation Failed.
Downgrade from Fabric OS v9.2.0 to Fabric OS v9.0.x	The downgrade is blocked. You must downgrade to Fabric OS v9.1.x and then proceed with the downgrade to Fabric OS v9.0.x. A Brocade TruFOS Certificate is enforced.

Perform the following steps to request Brocade TruFOS Certificates from the Broadcom website:

- From the website support.broadcom.com, click **LOGIN**, and enter your username and password.
If you do not have an account, click **REGISTER** to set up your account.
- Once logged on, click **Brocade Storage Networking** in the top navigation menu and select **License Management** from the listed menu options. The following options appear:
 - Licensing Portal
 - TruFOS Certificate Request
 - Beware of Counterfeit Licenses
- Click **TruFOS Certificate Request**. The **Trusted FOS Certificate Request** page appears.
- Follow the instructions given on the **Trusted FOS Certificate Request** page to request Brocade TruFOS Certificates.

Brocade TruFOS Certificate management uses the same function as a license management in Fabric OS. You can use the `license --install {-h <hostip> -t <protocol> [-m <server_port_number>] -u <user> [-p <password>] -f <filepath/xmlfile>}` command to install the Brocade TruFOS Certificate (provided as an XML file).

The following example shows a sample from the `license --install` command and the RASLog message.

```
switch:admin> license --install -h 192.0.2.0 -t scp -u UserName -p
Password -f /repository/20211013171159568_10_00_c4_f5_7c_64_5b_60.xml
License Installed [FOS-87-0-04-11209683]
```

The following example shows the output from the `license --show` command.

You can use the `license --show` command to verify that a Brocade TruFOS Certificate is installed and when it expires.

```
switch:admin> license --show
License Id : 10:00:d8:1f:cc:b7:fa:32
License 1 :
-----
License serial number   : FOS-86-0-03-11304460
License features        : Trunking
Generation date         : 09/09/2021
License 2 :
-----
License serial number   : FOS-87-0-04-11222265
License features        : Trusted FOS (TruFOS) Certificate
Generation date         : 09/27/2022
Expiry date             : 09/27/2023
License 3 :
-----
License serial number   : FOS-86-0-03-11304455
License features        : Extended Fabric
Generation date         : 09/09/2021
License 4 :
-----
License serial number   : FOS-86-0-01-11304458
License features        : Inter Chassis Link (ICL)
License Capacity        : 64 ICL links per CR blade (16 QSFPs per CR blade)
Generation date         : 09/09/2021
License 5 :
-----
License serial number   : FOS-86-0-03-11304456
License features        : Fabric Vision and IO Insight
Generation date         : 09/09/2021
License 6 :
-----
License serial number   : FOS-86-0-03-11304457
License features        : FICON_CUP
Generation date         : 09/09/2021
License 7 :
-----
License serial number   : FOS-86-0-03-11304459
License features        : Integrated Routing
Generation date         : 09/09/2021
```

Once the Brocade TruFOS Certificate is installed, you can proceed with the firmware download process.

Downloading Firmware

Firmware upgrades are available for partners and for customers with support service contracts on the website at <https://support.broadcom.com/>.

Perform the following steps to download firmware and documentation files from the website and then download the firmware to a switch or a director:

1. From the website <https://support.broadcom.com/>, click **LOGIN**, and enter your user name and password.
If you do not have an account, click **REGISTER** to set up your account.
2. Click **Brocade Storage Networking** in the top navigation menu and then select **Software & Documentation > Software Downloads**. The **Search Downloads** page appears, where all the firmware and documentation resources are located.
3. From the **Search Downloads** page, click in the **Product Search** box. A drop-down list of products appears.
4. Select **Brocade Storage Networking** to view documentation and firmware related to Brocade products.
5. Enter the product name or the firmware version number in the **Search** box. For example, if you search with the version number 9.2.0, it lists the firmware and documentation files available for the product with the Fabric OS v9.2.0. Click the **Download** button to download the required firmware.
6. Uncompress the firmware file using the UNIX `tar` command for TAR files, the `gunzip` command for GZ files, or a Windows unzip program for ZIP files.

NOTE

For each switch in your fabric, complete all firmware download changes on the current switch before issuing the `firmwaredownload` command on the next switch. This process ensures that the traffic between the switches in your fabric is not disrupted.

7. Enter the `license --show` command to verify whether a valid TruFOS certificate has been installed. If the Brocade TruFOS Certificate is not installed, obtain the license key from your vendor or the Broadcom Support Portal. If the TruFOS validation fails because the Brocade TruFOS Certificates are not available or have expired, the following warning message appears: `Firmwaredownload failed. TruFOS Certificate validation failed.` For more information about Brocade TruFOS Certificates, see [Brocade TruFOS Certificates](#).
Once the Brocade TruFOS license is installed, proceed with the firmware download process.
8. Use the `firmwaredownload` command to download the firmware to the switch by using FTP, SFTP, SCP, or HTTP to connect to an FTP or SSH server, or use a USB device with the downloaded firmware.
 - If you are using FTP, SFTP, SCP, or HTTP, verify that the FTP or SSH server is running on the host server and that you have a valid user ID, password, and permissions for that server. If you plan to use the Challenge-Response Authentication (CRA) protocol with either SFTP or SCP, you must first enable this protocol on the host server side.
 - If you are using a USB memory device, verify that it is connected and running.
 - a) Visually confirm that the device is connected.
 - b) Enter the `usbstorage -e` command to mount the USB device.
 - c) Enter the `usbstorage -l` command to display the space on USB storage. This also lists the content from the USB device or folder path in USB storage.

The `firmwaredownload` command supports both non-interactive and interactive modes. If this command is issued without any operands or any syntax errors in the parameters, the command enters an interactive mode to prompt you for input.

9. Unpack the downloaded firmware. The firmware expands into a directory that is named according to the version of Fabric OS software in the file name. For example, if you download and unzip a file named `v9.2.0_G6G7_DIR.zip` for an X6/X7 director, it expands into a directory that is named `v9.2.0_G6G7_DIR`.
10. Specify the complete path and include the `v9.2.0` directory name using the interactive commands for the `firmwaredownload` command. When you enter the `firmwaredownload` command, there is an automatic search for the correct package file type associated with the switch.

<Firmware Server Name or IP Address>, <User_Account>, <File Name>, <Your_Password>

The following example shows the complete path for the `firmwaredownload` command:

```
switch:admin> firmwaredownload -s
Server Name or IP Address: 192.0.2.0
User Name: admin
File Name: /repository/fos/v9.2.0/v9.2.0_G6G7_DIR
```

NOTE

If DNS is enabled and a server name is specified instead of a server IP address in the command line, the `firmwaredownload` command automatically determines whether IPv4 or IPv6 should be used. Use on an FTP server by name, you must configure at least one DNS server using the `dnsconfig` command.

The following example shows the initial portion of an interactive firmware download. After this portion is complete, a scrolling list of the firmware elements being installed is displayed.

```
switch:admin> firmwaredownload
Server Name or IP Address: 192.0.2.0
User Name: admin
File Name: /repository/fos/v9.2.0/v9.2.0_G6G7_DIR
Network Protocol(1-auto-select, 2-FTP, 3-SCP, 4-SFTP, 5-HTTP) [1]: 4
Password: <hidden>
```

```
Do you accept and agree to the terms outlined in the End User License Agreement(EULA) for this product?
Please respond with (Y/y) to Accept, (N/n) to Not accept, or (D/d) to display the EULA : y
```

```
Server IP: 192.0.2.0, Protocol IPv4
Checking system settings for firmwaredownload...
```

NOTE

Do not use Linux utilities to expand files that are destined for a Windows server.

Enabling the USB Device

Perform the following steps to enable the USB device:

1. Log on to the switch using an account with admin permissions.

NOTE

Ensure that USB devices have been pre-formatted with FAT32 file system.

2. Plug a USB drive into the USB port of the Brocade switch. If it is a Brocade chassis, plug the USB drive into the active CP where the blue active CP light is illuminated.

3. Enter the `usbstorage -e` command.

This command enables the USB device. You can now use it to install the firmware.

Staging Firmware

Firmware that is downloaded to the secondary partition using the `firmwaredownload` command with either the remote (`-r`) or local (`-lr`) source option can be activated later using the `firmwareactivate` command. After the firmware is downloaded, the update is incomplete until the new firmware is activated.

Perform any desired configuration changes before activating the new firmware. If the switch is rebooted or power-cycled, the downloaded firmware is not affected because it is stored in the secondary partition. Any `firmwarerestore` or `firmwarecommit` process starts when the firmware is activated. You can use the `firmwareactivate` command in both single-CP and dual-CP environments.

NOTE

If you are downloading Fabric OS v9.1.x firmware using the `firmwaredownload -sf` command, you must commit it before downloading Fabric OS v9.2.0 firmware.

To stage the firmware, perform the following steps:

1. Download the firmware using one of the previously mentioned options.
2. Enter the `firmwareshow` command to find the status of the download.

```
switch:admin> firmwareshow
```

Slot	Name	Appl	Primary/Secondary Versions	Status
1	CP0	FOS	v9.2.0 v9.2.0	STANDBY *
2	CP1	FOS	v9.2.0 v9.2.0	ACTIVE

Activating Firmware

After downloading the firmware to a platform, the upgrade is incomplete until the firmware is activated.

Perform the following steps to activate the firmware:

1. Download the firmware to the secondary partition of the platform using the `firmwaredownload -r` or `firmwaredownload -lr` command.
2. Enter the `firmwareshow` command to view the current firmware version on each partition.

```
switch:admin> firmwareshow
```

Appl	Primary/Secondary Versions
Fabric OS	v9.1.1 v9.2.0

3. Enter the `firmwareactivate` command to activate the firmware.

```
switch:admin> firmwareactivate
```

This command will activate the firmware on the secondary partition
but will require that existing telnet, secure telnet or SSH sessions be restarted.

Do you want to continue (Y/N) [Y]:

Once the firmware is activated, the output similar to the following is displayed:

```
switch:admin> firmwareshow
```

Appl	Primary/Secondary Versions
Fabric OS	v9.2.0 v9.2.0

You can use the `firmwareactivate -l` option to activate only the secondary partition firmware version of the local CP.

Validating the Firmware Download

No matter which download process you use, the firmware install process automatically validates that the downloaded file sets are complete and correct. There is no need to perform a manual validation.

Downloading Firmware without a Password

To download the firmware without a password, perform the following steps:

1. Enter the `sshutil` command for public key authentication when SSH is selected.
2. Configure the switch to install the private key and export the public key to the remote host.
3. Configure the SSH protocol to permit password-less logons for outgoing authentication before running the `firmwaredownload` command. For more information, refer to the "Configuring Outgoing SSH Authentication" section of the *Brocade Fabric OS Administration Guide*.

Downloading Firmware from a USB Device

You can download new versions of Fabric OS firmware to a switch or chassis from a USB device. The following Brocade devices support downloading firmware from a USB stick attached to the chassis or active control processor:

- Brocade G610
- Brocade G620
- Brocade G630
- Brocade X6-4
- Brocade X6-8
- Brocade G720
- Brocade G730
- Brocade X7-4
- Brocade X7-8
- Brocade 7810
- Brocade 7850

Perform the following steps to download the firmware from a USB device depending on the operating system that you use:

1. Perform any of the following tasks depending on the operating system:
 - a. If you are using Windows, open a file browser and navigate to the directory on the USB device. Drag the unzipped firmware image files from where you downloaded them to this directory. You can store multiple images under this directory.
 - b. If you are using Linux, enable and mount the USB device as a file system . After mounting, copy the unzipped firmware images to be downloaded to the directory.
2. Enter the `firmwaredownload` command with the `-U` (uppercase U) option to download the specified firmware image from the USB device. When you specify a path to a firmware image in the USB device, specify the relative path.

NOTE

To ensure file integrity, use the `usbstorage -d` command to unmount the USB device before physically unplugging it from the switch or director. If you update a USB device on an external server, ensure that it is properly ejected from the server before physically unplugging it.

All types of USB flash drives are supported on Brocade Gen 6 and Gen 7 platforms. However, the following USB flash drives are certified by Broadcom:

NOTE

Ensure that USB devices have been pre-formatted with FAT32 file system.

- SanDisk 32 CZ48 USB 3.0 Flash Drive (SDCZ48-032G-UAM46)
- SanDisk 64 CZ48 USB 3.0 Flash Drive (SDCZ48-064G-UAM46)
- Kingston 32GB DataTraveler 100 G3 USB 3.0 Flash Drive (DT100G3/32GB)
- Kingston 32GB DataTraveler G4 USB 3.0 Flash Drive (DTIG4/32GB)
- PNY Turbo Attache 4 USB 3.0 32GB Flash Drive (P-FD32GTBAT4-GE)
- PNY Attache 4 USB 3.0 64GB Flash Drive (P-FD64GTBAT4-GE)

Viewing the USB File System

1. Connect to the device and log on using an account with admin permissions.
2. Enter the `usbstorage -l` command.

```
switch:admin> usbstorage -l
v9.2.0\                1126MB    2023 January 30 15:33
Available space on USB storage 96%
```

Downloading Firmware from a USB Device Using a Relative Path

Downloading firmware from a USB device using a relative path is the preferred method. Perform the following steps to download the firmware from a USB using a relative path.

1. Connect to the device and log on using an account with admin permissions.
2. Enter the `firmwaredownload -U` (uppercase U) command, followed by the name of the firmware directory. In the following example, the directory is `9.2.0_G7_ENTP`.

```
switch:admin> firmwaredownload -U brocade/firmware/v9.2.0_G7_ENTP
```

Upgrading and Downgrading Firmware

In this document, upgrading means installing a newer version of firmware than the one that is running; alternatively, downgrading means installing an older firmware version. The procedures in this document assume that you are upgrading firmware. These procedures also work for downgrading if the old and new firmware versions are compatible.

Consider the following two methods before upgrading or downgrading a switch to the newer or older firmware version:

- Perform the upgrade or downgrade process directly to the desired firmware version. For more information, see [Upgrading Firmware on Fixed-Port Switches](#) or [Upgrading Firmware on Directors \(Including Blades\)](#).
- Evaluate a newer or older version before actual deployment. This evaluation allows you to assess the features, capabilities, and potential risks, and it helps to determine the upgrade or downgrade to a newer or older firmware version. For more information, see [Testing and Restoring Firmware on Switches](#).

All Brocade systems maintain two partitions (a primary and a secondary) of a nonvolatile storage to store the firmware. The firmware download process first copies the replacement files (which might contain an updated kernel) into the secondary partition. Then, the process swaps the partitions so that the secondary partition becomes the primary. It then performs a nondisruptive HA reboot of the system. For directors, the standby is rebooted; this does not affect the system traffic. For fixed-port platforms, the system attempts to restore the previous machine state after the reboot is completed, also called a warm reboot. When the system boots, it boots using the revised Fabric OS firmware in the primary partition. The firmware download process then copies the updated files from the primary partition to the secondary partition.

NOTE

Most firmware upgrades and downgrades are not disruptive to device operations; however, always refer to the latest Fabric OS release notes for updates on upgrading and downgrading.

The following table lists the currently supported Fabric OS downgrade versions and platforms.

Table 2: Gen 6 and Gen 7 Platforms and Supported Firmware Downgrade Versions from Fabric OS v9.2.x

Platforms	Fabric OS v9.2.x	Fabric OS v9.1.x	Fabric OS v9.0.x
Brocade Gen 7 (64G) Fixed-Port Switches			
Brocade G720	Supported	Supported	Supported
Brocade G730	Supported	Supported	Not Supported
Brocade 7850 Extension Switch	Supported	Not Supported	Not Supported
Brocade Gen 7 (64G) Directors			
Brocade X7-4 Director	Supported	Supported	Supported
Brocade X7-8 Director	Supported	Supported	Supported
Brocade Gen 6 (32G) Fixed-Port Switches			
Brocade G610 (Switch Type 170.0 to 170.3)	Supported	Supported	Supported
Brocade G610 (Switch Type 170.4 or higher)	Supported	Supported	Supported (Fabric OS v9.0.1b and later)
Brocade G620 (Switch Type 162)	Supported	Supported	Supported
Brocade G620 (Switch Type 183)	Supported	Supported	Supported

Platforms	Fabric OS v9.2.x	Fabric OS v9.1.x	Fabric OS v9.0.x
Brocade G630 (Switch Type 173)	Supported	Supported	Supported
Brocade G630 (Switch Type 184)	Supported	Supported	Supported
Brocade 7810 Extension Switch	Supported	Supported	Supported
Brocade G648 Blade Server SAN I/O Module	Supported	Supported	Supported
Brocade MXG610 Blade Server SAN I/O Module	Supported	Supported	Supported
Brocade Gen 6 (32G) Directors			
Brocade X6-4	Supported	Supported	Supported
Brocade X6-8	Supported	Supported	Supported

The following table lists the upgrade and downgrade considerations for various features and the guides to refer to for more information.

Table 3: Upgrade and Downgrade Considerations for Various Features

Feature	Guides for Reference
Flow Vision	The Brocade Flow Vision feature has specific firmware upgrade and downgrade considerations. For the firmware upgrade and downgrade considerations that apply to Flow Vision and the respective version of Fabric OS software, refer to the upgrade and downgrade sections of the "Administering Flow Vision" section in the <i>Brocade Fabric OS Administration Guide</i> .
Monitoring and Alerting Policy Suite (MAPS)	The MAPS feature has specific firmware upgrade and downgrade considerations. For the firmware upgrade and downgrade considerations that apply to MAPS and the respective version of Fabric OS software, refer to the <i>Brocade Fabric OS MAPS User Guide</i> .
IP Extension	Brocade IP Extension configuration has specific firmware upgrade and downgrade considerations. For the firmware upgrade and downgrade considerations that apply to IP Extension configuration and the respective version of Fabric OS software, refer to the <i>Brocade Fabric OS Extension User Guide</i> .
FCoE	The Brocade FCoE feature has specific firmware upgrade and downgrade considerations. For the firmware upgrade and downgrade considerations that apply to FCoE and the respective version of Fabric OS software, refer to the upgrade and downgrade sections of the <i>Brocade Fabric OS FCoE User Guide</i> .

Supported Upgrade Paths

The following table provides details on supported upgrade paths and steps for upgrading through multiple versions of Fabric OS software. For the specific Fabric OS versions, refer to the Fabric OS release notes of the corresponding version.

Table 4: Supported Upgrade Paths to Fabric OS v9.2.x

Current Fabric OS Version	Upgrade Procedure
Fabric OS v9.1.x	Upgrade to Fabric OS with a valid Brocade TruFOS Certificate. This is a nondisruptive direct upgrade.
Fabric OS v9.0.x	Upgrade to Fabric OS v9.1.x, and then upgrade to the Fabric OS v9.2.x version with a valid Brocade TruFOS Certificate. This is a nondisruptive upgrade.

Supported Link Modes

Fabric OS v9.2.x supports the following link modes:

- 10BASE-T/Full
- 100BASE-T/Full
- 1000BASE-T/Full

Supported Blades

The following table provides details on the blades supported in Brocade Gen 7 Directors or in the existing Brocade Gen 6 Directors upgraded to Gen 7 Directors that are running Fabric OS v9.2.x.

Table 5: Supported Blades in Fabric OS v9.2.x

Blade	Brocade X7 Director	Brocade X6 Director Upgraded to X7	Brocade X6 Director
FC64-48	Yes	Yes	No
FC32-X7-48	Yes	Yes	No
FC32-48	Yes	Yes	Yes
FC32-64	Yes	Yes	Yes
FC64-64	Yes	Yes	No
SX6	Yes	Yes	Yes
CR64-8/CR64-4	Yes	Yes	No
CR32-8/CR32-4	No	No	Yes
CP X6	No	Yes	Yes
CP X7	Yes	No	No

Upgrade or Downgrade Prerequisites

Perform the following mandatory tasks before upgrading the firmware on your switch or director:

- Ensure compatibility with the new Fabric OS version and with any older versions of Fabric OS.
- Make sure that your enterprise switch or director has a valid Brocade TruFOS Certificate installed before upgrading to Fabric OS v9.2.0 and later versions.
- Make sure that the OpenSSL version is upgraded to version 3.0.7 or later on applications that access Fabric OS v9.2.x.
- Make sure that all entries in the `msConfigure` command are removed and configurations are transferred to the `portcfgmsacl` command before upgrading to Fabric OS v9.2.0. The upgrade is blocked during the preinstall check if any configuration is available in the `msConfigure` command.
- Remove the following zones:
 - Traffic Isolation zones
 - Frame Redirection zones
 - Broadcast zones
 - Fabric Assist zones
 - Quick loop zones

Perform the following mandatory tasks before downgrading the firmware on your switch or director:

- Make sure that the Fibre Channel Link Aggregation (FC-LAG) configurations are removed before downgrading. The FC-LAG configuration blocks a firmware downgrade from Fabric OS v9.2.x. This is a disruptive operation.
- Disable VMID+ on the ports of the logical fabric and disable XISL usage before downgrading to the pre-Fabric OS v9.2.x versions.
- Make sure that FIPS-Inside mode is disabled before downgrading to a target version that is not FIPS-Inside compliant.
- Remove user-defined rules for the TXP or RXP monitoring system with actions FENCE or DECOM before downgrading.
- Set all Management Server ACL values to the default access on all ports before downgrading to the requested firmware.

Connected Switches

Before you upgrade the firmware on your switch or director, review the connected switches in your fabric to ensure compatibility with the new Fabric OS version and that any older Fabric OS versions are supported. Refer to the Fabric OS release notes for the recommended firmware version.

NOTE

Starting simultaneous firmware downloads on adjacent fixed-port switches might result in traffic disruption.

To determine whether you must upgrade other switches connected to your switch, use the `version` command on each connected switch to view the firmware information and build dates.

General Upgrade Considerations

This section provides information to be considered before upgrading a device to Fabric OS v9.2.x with reference to configuration and functionality.

Configuration

Consider the following information before upgrading a device to Fabric OS v9.2.x with reference to configuration:

- Upgrading to Fabric OS v9.2.x allows you to extend the length of the chassis name up to 31 characters.
- FIPS mode is disabled and not supported when upgrading to Fabric OS v9.2.x. After completing a successful upgrade, you can configure FIPS-Inside mode in Fabric OS v9.2.x.

Functionality

Consider the following information before upgrading a device to Fabric OS v9.2.x with reference to functionality:

- If both Gen 6 core blades (CR32-4 and CR32-8) and Gen 7 core blades (CR64-4 and CR64-8) are present on the same chassis, the last inserted (second) core blade is faulted. Do not install both versions at the same time. If a director is being migrated, power it off and follow the migration procedure.
- If you do not accept the end-user license agreement (EULA) terms and conditions, the Fabric OS v9.2.x upgrade is blocked.
- The Boot LUN zoning feature is supported in Fabric OS v9.2.0. However, the `bootLunCfg` CLI command displays a warning message that the Boot LUN zoning feature will be deprecated in future versions.
- The FA PWWN feature is supported in Fabric OS v9.2.0. However, the `fapwwn` command displays a warning message that the FA PWWN feature will be deprecated in future versions.
- The Rule Quiet Time and Global Quiet Time configurations from the pre-Fabric OS v9.2.x release are supported in the default notification mode with a warning message. When you enable the adaptive notification feature, the Rule Quiet

Time and Global Quiet Time configurations are no longer supported and are only available in the default notification mode.

- If cryptographic ciphers that are not supported in the Fabric OS v9.2.x version are configured, a firmware upgrade is not allowed. For more information about supported ciphers, refer to the *Brocade Fabric OS Administration Guide*.
- When you upgrade an existing Gen 7 chassis with the Fabric Vision® license that is running Fabric OS v9.1.x to Fabric OS v9.2.x, Traffic Optimizer is scheduled to change from the Sys_TrafOpt_Version1 profile to the Sys_TrafOpt_Version2 profile after 30 days. The scheduled change of the Traffic Optimizer profile can be modified using the `trafopt` command to cancel or change the schedule or invoke an immediate change to the Sys_TrafOpt_Version2 profile. Factory-shipped Gen 7 platforms with the Fabric OS v9.2.x firmware have the Sys_TrafOpt_Version2 profile that is enabled by default. For more information, refer to *Brocade Fabric OS Administration Guide*.

General Downgrade Considerations

This section provides information to be considered before downgrading a device to Fabric OS v9.1.x with reference to configuration and functionality.

Configuration

Consider the following information before downgrading a device to Fabric OS v9.1.x with reference to configuration:

- A Fabric OS downgrade is blocked in the following cases:
 - The Maintenance role is mapped to an LDAP role.
 - Access time is configured for the Maintenance role.
 - The password expiration policy is configured for the Maintenance role.
 - Brocade FC64-64 blades are installed. Remove them before a downgrade.
- A Fabric OS firmware downgrade is not supported if the FPGA of the CP is already upgraded as part of the Gen 6 to Gen 7 Director conversion.
- If ciphers or protocols that apply to only the Fabric OS v9.2.x version are configured, the Fabric OS downgrade is blocked. Ensure that the ciphers are updated based on the target firmware before downgrading.

Functionality

Consider the following information before downgrading a device to Fabric OS v9.1.x with reference to functionality:

- If you are downgrading to an earlier version of the Fabric OS software, the collective zone configuration database size across all logical partitions must not exceed the maximum supported limits of the target firmware version. If the zone database size exceeds the limit, downgrading is blocked until the configured zone databases are reduced to meet the zone size limits of the target firmware version.
- A Fabric OS downgrade from v9.2.x to v9.1.x is not supported when the TrafOpt_Custom profile is active. If you want to downgrade below Fabric OS v9.2.x, first migrate the Traffic Optimizer profile to Sys_TrafOpt_Version2 or Sys_TrafOpt_Version1, which is a disruptive operation. Then Fabric OS can be downgraded nondisruptively.
- If you insert a CP with Fabric OS v9.1.x on standby when the active CP runs Fabric OS v9.2.x with the TrafOpt_Custom profile, the HA state goes out of sync unless autoleveling is enabled.
- Upon downgrading to the pre-Fabric OS v9.2.x versions with adaptive notification enabled, a warning message appears. Default and custom Quiet Time configurations created in default notification mode will be supported after downgrading.
- Upon downgrading from Fabric OS v9.2.0 to a lower version, the `dflt_always_active_policy` is removed.
- The custom rules configured for the STATE_CHG monitoring system with the CIRCUIT QOS group are not supported in the pre-Fabric OS v9.2.x releases.
- The custom rules configured for the ZONE_CFGSZ_PER monitoring system with the CHASSIS group are not supported in the pre-Fabric OS v9.2.x releases.
- The MEMORY_USAGE_STATE monitoring system is not supported in the pre-Fabric OS v9.2.x releases.

Upgrading Firmware on Fixed-Port Switches

The firmware download is an incremental process in Fabric OS v9.2.x. During the firmware download process, the checksum of a package to be downloaded is compared with the existing checksum files on the switch. The checksum files already present are skipped if they are the same, and only the new and modified packages are downloaded on the switch.

Before you begin, see [Connected Switches](#) and confirm that all connected switches in the fabric are running a supported Fabric OS version before starting any upgrade. If they are not, you should upgrade the deficient switches before proceeding. You can use the `firmwareshow` command to determine the current firmware version on each switch.

1. Connect to the switch that you want to upgrade, and log in using an account with admin permissions.
2. Enter the `firmwaredownload` command. Enter `y` at the following EULA prompt and respond to the successive interactive prompts.

```
Please acknowledge that you have read and accept Broadcom's EULA stipulations.
Please respond (Y/y=accept, N/n=do not accept, or (S/s) to show the EULA) : Y
```

NOTE

If DNS is enabled and a server name instead of a server IP address is specified in the command line, the `firmwaredownload` command automatically determines whether IPv4 or IPv6 should be used. To mention an FTP server by name, you must configure at least one DNS server using the `firmwaredownload` command.

3. Enter `y` at the `Do you want to continue [y/n]` prompt.
4. After the high availability (HA) reboot, reconnect to the switch and log in again using an account with admin permissions.

NOTE

During the brief period of (HA) reboot on fixed-port switches, exchanges involving Fibre Channel Generic Services might experience a delay. Fixed-port switches must retry the operations in this case.

5. Enter the `firmwaredownloadstatus` command to determine if the firmware download process has completed. It takes several minutes for this process to complete.
6. After the firmware commit is completed, enter the `firmwareshow` command to verify that the firmware level of both partitions is the same.

```
switch:admin> firmwareshow
Appl      Primary/Secondary Versions
-----
FOS       v9.2.0
          v9.2.0
```

Firmware Download with Legacy Mode

The number of packages installed on a switch is reduced with an incremental firmware download based on the checksum value of the packages. Gen 6 and Gen 7 platforms with checksum files can do an incremental firmware download to the next supported build. If you prefer, you can skip the incremental download and opt for the firmware download using legacy mode.

NOTE

The legacy mode is slower due to the increased load on package files.

To enable a legacy firmware download and skip the incremental upgrade, enter the `firmwaredownload -L` command. The following example shows a firmware download with legacy mode using interactive commands.

```
switch:admin> firmwaredownload -L
Server Name or IP Address: 192.0.2.0
```

```
User Name:admin
File Name: /repository/fos/v9.1.0/v9.1.0_G7_MID
Network Protocol(1-auto-select, 2-FTP, 3-SCP, 4-SFTP, 5-HTTP) [1]: 1
Password:
```

```
Please acknowledge that you have read and accept Broadcom's EULA stipulations.
Please respond (Y/y=accept, N/n=do not accept, or (S/s) to show the EULA) : y
-----Output truncated-----
```

FPGA Firmware Upgrade Utility

The FPGA firmware upgrade utility allows you to upgrade the field-programmable gate array (FPGA) firmware on Brocade platforms, and it verifies that the updated image is correctly installed.

NOTE

- For any product or platform requiring an FPGA upgrade, separate instructions are provided with the product and/or in Release Notes for a given version.
- FPGA images are specific to an individual platform and are packaged in the Fabric OS firmware download. Appropriate FPGA firmware images are copied to the system when you run the `firmwaredownload` command.

The firmware download does not automatically update the FPGA firmware into the FPGA flash memory of the system. If an updated FPGA version is included in a Fabric OS firmware update, after the firmware download is completed, you must enter the `fpgaupgrade` command to update the FPGA firmware. Once the FPGA upgrade is successful, you must power-cycle the entire device (not just an HA failover or a reboot) for the new FPGA firmware to be active. If the FPGA upgrade is not successful, an error message is displayed. In this case, you should not power-cycle the device until you have resolved the error condition.

If your device is already running the latest FPGA image, entering the `fpgaupgrade` command displays a message that the image is up to date, and the utility does not update the FPGA flash memory. The following example illustrates a switch that is running the latest FPGA version:

```
switch:admin> fpgaupgrade
The switch is already running the latest FPGA version
```

You can use the `fpgaupgrade --latest` command to verify whether the running FPGA image is the latest. The following example shows a down-level FPGA.

```
switch:admin> fpgaupgrade --latest
Current      Latest
-----
0x05.05      0x06.06
```

If your device is not running the latest FPGA image, running the `fpgaupgrade` command updates the FPGA flash memory with the new image and then verifies that the updated image is correctly installed. The following example illustrates a switch that needs the latest FPGA version upgrade:

NOTE

The `fpgaupgrade` command output might vary depends on the platform.

```
switch:admin> fpgaupgrade
This is a disruptive operation and will require a power-cycle after the completion of the operation.
Do you want to continue (y/n) ?
y
Programming new FPGA, this may take a few minutes ...
```

```

Device #1 IDCODE is 0310A0DD
full-chip erasing Max 10 FPGA device(s) ...
programming Max 10 FPGA CFM0 block at sector 5 ...
programming Max 10 FPGA CFM1 block at sector 3 ...
programming Max 10 FPGA CFM1 block at sector 4 ...
programming Max 10 FPGA UFM block at sector 2 ...
verifying Max 10 FPGA CFM0 block at sector 5 ...
verifying Max 10 FPGA CFM1 block at sector 3 ...
verifying Max 10 FPGA CFM1 block at sector 4 ...
verifying Max 10 FPGA UFM block at sector 2 ...
programming Max 10 FPGA DSM block ...
DONE
Test time elapsed = 162.764267 sec
Exit code = 0... Success
Programmed new FPGA successfully. Please power-cycle for it to take effect.

```

Enter the `fpgaupgrade <slot number>` command to verify that the updated image is correctly installed in directors.

```

switch:admin> fpgaupgrade --slot 3
FPGA: Curr = (0x1, 0xb), Latest = (0x1,0xb)
CPLD: Curr = (0x1, 0x2), Latest = (0x1,0x2)
JTAG: Curr = (0x1, 0x3), Latest = (0x1,0x3)
The switch is already running the latest FPGA version

```

Depending on the error, you might be requested not to power-cycle the system until the corrective action is taken. The following example shows an FPGA update failure:

```

switch:admin> fpgaupgrade
This is a disruptive operation and will require a power-cycle after the completion of the operation.
Do you want to continue (y/n) ?
y
Programming new FPGA, this may take a few minutes ...
Exit code = 6... Device verify failure
FPGA update failed. Avoid doing power cycle
Failed to program new FPGA (-1)

```



CAUTION

If there is an error, do not power-cycle the affected blade or switch before contacting your switch supplier. You can retry the `fpgaupgrade` command and it can succeed on a retry. However, do not power-cycle if the error persists after a retry. A failed FPGA update can result in an outage for the affected blade or the entire switch (if it is a nonbladed chassis).

Upgrading Firmware on Directors (Including Blades)

You can obtain the firmware file for the version of Fabric OS software that you want to load onto the director from <https://www.broadcom.com/mybroadcom>. See [Downloading Firmware](#) for details on the process of downloading the firmware files from the website and downloading the firmware to a switch or a director.

NOTE

If the director being upgraded does not support HA (either due to a synchronization issue or because the director has been disabled), you can still upgrade the CPs one at a time. However, this process might disrupt traffic if the sync feature is not available. To upgrade the CPs, follow the directions for fixed-port switch upgrades.

Before you begin, see [Connected Switches](#) and confirm that all connected switches in the fabric are running a supported version of the Fabric OS firmware before starting any upgrades. If they are not, you should upgrade the deficient switches before proceeding. Use the `firmwareshow` command to determine the current firmware version on each switch.

1. Verify that the Ethernet interfaces CP0 and CP1 are plugged into your network.
2. Verify that the FTP, SCP, SFTP, or HTTP server is running on the host server and that you have full access (a valid user ID, a password, and permissions) on that server.
3. Unpack the compressed files, preserving the directory structures.
See [Downloading Firmware](#) for details on this process for your environment. If you plan to use a USB device for the `firmwaredownload` command, you should copy the uncompressed release folder to the device now.
4. Connect to the chassis IP management interface or active control processor and log in using an account with admin permissions.

NOTE

- A Brocade director has only one chassis management IP address.
- Synchronization of the CPs is not the same as the synchronization of the firmware. The CPs can differ in firmware versions and still be in sync. See the `firmwaresync` command to trigger a sync of the actual firmware from the active CP to the standby CP.

5. Enter the `hashow` command to confirm that the two CP blades are synchronized.

In the following example, the active CP blade is CP0, and the standby CP blade is CP1:

```
switch:admin> hashow
Local CP (Slot 1, CP0): Active, Cold Recovered
Remote CP (Slot 2, CP1): Standby, Healthy
HA enabled, Heartbeat Up, HA State synchronized
```

If the CP blades are not synchronized, enter the `hasyncstart` command to synchronize them. If the CPs remain unsynchronized, contact your switch service provider.

For further troubleshooting, refer to the *Brocade Fabric OS Troubleshooting and Diagnostics Reference Manual*.

6. Enter the `firmwaredownload` command. Enter `y` at the following EULA prompt and respond to the successive interactive prompts.

```
Please acknowledge that you have read and accept Broadcom's EULA stipulations. Please
respond (Y/y=accept, N/n=do not accept, or (S/s) to show the EULA) :
```

7. Enter `y` at the `Do you want to continue [Y]` prompt.

The firmware is downloaded to one CP blade at a time, beginning with the standby CP blade. During the process, the active CP blade fails over. After the firmware is downloaded, a firmware commit starts on both CP blades. The entire firmware download and commit process takes approximately 17 minutes.

On the Brocade X6-4/X6-8 Director, if a Brocade SX6 Extension Blade is present: Upon failover, an autoleveling process is activated. Autoleveling is triggered when the active CP detects a blade that contains a different firmware version, regardless of which version is older. Once the autoleveling is triggered, it performs the following:

1. Downloads the firmware to the internal BP processor of the blade.
2. Swaps partitions.
3. Reboots the blade.
4. Copies the new firmware from the primary partition to the secondary partition.

If you have multiple Brocade SX6 Extension Blades, they are updated simultaneously; however, the downloads might occur at different rates.

Autoleveling occurs in parallel with the firmware download being performed on the CPs, but it does not impact performance. Fibre Channel traffic is not disrupted during autoleveling, but Gigabit Ethernet (GbE) traffic on application processor (AP) blades might be affected. If there is an active FCIP tunnel on the Brocade SX6 Extension Blade, the FCIP tunnel traffic is impacted for at least 2 minutes.

```
switch:admin> firmwaredownload
Server Name or IP Address: 192.0.2.0
User Name: admin
File Name: /home/user/9.2.0
Network Protocol (1-auto-select, 2-FTP, 3-SCP, 4-SFTP, 5-HTTP) [1]: 1
Password:
```

```
Please acknowledge that you have read and accept Broadcom's EULA stipulations. Please respond (Y/y=accept,
N/n=do not accept, or (S/s) to show the EULA) : y
```

```
Checking system settings for firmwaredownload...
```

```
-----Output Truncated-----
```

8. After the failover, connect to the switch and log in again using an admin account.
9. Using a separate session to connect to the switch, enter the `firmwaredownloadstatus` command to monitor the firmware download status.

```
switch:admin> firmwaredownloadstatus
[1]: Fri Jan 24 16:25:49 2023Slot 2 (CP1, active): Firmware is being downloaded to standby CP. This step
may take up to 30 minutes.
[2]: Fri Jan 24 16:31:49 2023Slot 2 (CP1, active): Firmware has been downloaded successfully to Standby
CP.
[3]: Fri Jan 24 16:31:51 2023Slot 2 (CP1, active): Standby CP is going to reboot with new firmware.
[4]: Fri Jan 24 16:35:41 2023Slot 1 (CP0, active): Forced failover succeeded. New Active CP is running new
firmware
[5]: Fri Jan 24 16:36:48 2023Slot 1 (CP0, active): Firmware is being downloaded to standby CP. This step
may take up to 30 minutes.
[6]: Fri Jan 24 16:39:27 2023Slot 1 (CP0, active): Firmware has been downloaded successfully on Standby
CP.
[7]: Fri Jan 24 16:39:27 2023Slot 1 (CP0, active): Standby CP reboots.
[8]: Fri Jan 24 16:41:59 2023Slot 1 (CP0, active): Firmware commit operation has started on both active
and standby CPs.
[9]: Fri Jan 24 16:42:00 2023Slot 1 (CP0, active): The firmware commit operation has started. This may
take up to 10 minutes.
[10]: Fri Jan 24 16:42:00 2023Slot 1 (CP0, active): Standby CP booted successfully with new firmware.
[11]: Fri Jan 24 16:46:08 2023Slot 1 (CP0, active): The commit operation has completed successfully.
[12]: Fri Jan 24 16:46:08 2023Slot 1 (CP0, active): Firmware commit operation has completed successfully
on active CP.
```

10. Enter the `firmwareshow` command to display the installed firmware version. The output allows you to confirm that the firmware has been correctly installed.

```
switch:admin> firmwareshow
Appl      Primary/Secondary Versions
-----
FOS       v9.2.0
          v9.2.0
```

Validating the Firmware Version and Firmware Signature

You can validate the firmware version and the change to a fixed-port switch or chassis-based platform by running the `firmwareshow` and `firmwaredownloadstatus` commands. A signed firmware download is the default behavior; however, you can use the `firmwarekeyshow` command to view the contents of the public key that is used for validating the firmware signature.

Table 6: Commands Used for Validating Firmware Downloads and Version

Command	Description
<code>firmwareshow</code>	Displays the current firmware level on the switch, including any states in transition during the firmware download process. For Brocade chassis-based devices, this command displays the firmware that is loaded on both partitions (primary and secondary) for all control processor (CP) and application processor (AP) blades. Maintain the same firmware level on both partitions of each CP within the device.
<code>firmwaredownload -v</code>	Displays a warning message if disk space is insufficient before proceeding with the firmware upgrade. If the sufficient space is not available, the following warning message is displayed: <code>Required space available on the switch to proceed firmwaredownload.</code>
<code>firmwaredownloadstatus</code>	Displays an event log that records the progress and status of events during Fabric OS firmware downloads. An event log is created by the current <code>firmwaredownload</code> command and is kept until another <code>firmwaredownload</code> command is issued. A timestamp is associated with each event. When downloading to devices with two control processors, you can run this command only on the active CP.

Verifying the Device and Fabric Connections

Use the `nsshow`, `nsallshow`, and `fabricshow` commands to ensure that the fabric and the connections to the attached devices have been restored correctly. Use the `switchshow` command to verify that no ports are coming up as `G_Ports`.

NOTE

All connected servers, storage devices, and switches should be present in the output of these commands. If there is a discrepancy, it is possible that a device or switch cannot connect to the fabric and further troubleshooting is necessary.

Table 7: Commands Used for Validating Firmware and Fabric Functionality

Command	Description
<code>nsshow</code>	Displays all devices directly connected to the switch that have logged on to the name server. This command displays <code>Connected through AG: Yes</code> if devices are connected to the fabric through an Access Gateway, and it displays <code>Real device behind AG: Yes</code> if a real device is connected behind the Access Gateway device. After the firmware download, ensure that the number of attached devices is the same as the number of attached devices before the firmware download.
<code>nsallshow</code>	Displays the port IDs for all devices connected to fabric. After the firmware download, ensure that the number of attached devices is the same as the number of attached devices before the firmware download.
<code>fabricshow</code>	Displays all devices in a fabric. After the firmware download, ensure that the number of devices in the fabric is the same as the number of attached devices before the firmware download.

Testing Firmware

This section provides steps to restore a switch to the original firmware version after evaluating a newer version and perform a firmware download on each control processor on Brocade Directors and restore the former Fabric OS firmware image.

Testing and Restoring Firmware on Switches

Typically you restore (downgrade) a switch to the original firmware version after evaluating a newer or different version. Testing firmware in this manner allows you to easily restore a switch to the existing firmware version because the evaluation version occupies only one partition on the switch.

**CAUTION**

When you evaluate new firmware, be sure to disable all features supported by the newer firmware before restoring the original firmware.

Testing a Different Firmware Version on a Switch

Perform the following steps to download and install the new firmware version that you want to evaluate:

1. Enter the `firmwaredownload -sbn` command to download the firmware to a single partition and to disable autocommit mode. See [Downloading Firmware](#) for details on this process for your environment.
2. Connect to the switch and log on using an account with admin permissions.
3. Enter the `firmwareshow` command to view the current firmware.
4. If the firmware level change is only one level up or down, the system will attempt a nondisruptive high availability (HA) reboot. If the firmware level change is greater than one level up or down, the reboot will be disruptive, and traffic on that switch and possibly on its fabric might be affected. This is by design. The switch performs a complete reboot and comes up with the new firmware to be tested. Your current switch session is automatically disconnected as part of the reboot.
5. Reconnect to the switch and log on using an account with admin permissions.
6. Enter the `firmwaredownloadstatus` command to view the status of the firmware download.

Once you have downloaded and installed the new firmware version, you can evaluate it. Once you complete your evaluation, you can either commit the firmware (install it fully) or revert to the previously installed version.

Committing Evaluation Firmware

If you want to commit (fully install) the firmware that you have been evaluating, complete the following steps:

1. Enter the `firmwareshow` command to confirm that the primary partition of the switch contains the new firmware.
2. Enter the `firmwarecommit` command to update the secondary partition with the new firmware.
It takes several minutes to complete the commit operation.
3. Enter the `firmwaredownloadstatus` command to view the status of the firmware download.
4. Enter the `firmwareshow` command to confirm that both partitions on the switch contain the new firmware.

When you complete this step, you have committed the firmware to the switch and completed the firmware download procedure.

Reverting Evaluation Firmware

If you want to remove the firmware that you have been evaluating and revert to the previously installed firmware, complete the following steps:

1. Enter the `firmwarerestore` command to reboot the switch and restore the original firmware.

This command automatically begins to copy the original firmware from the primary partition to the secondary partition. At the end of the process, both partitions will have the original firmware. It takes several minutes to restore the firmware.

2. Wait at least 5 minutes after running the `firmwarerestore` command to ensure that all processes have been completed and that the switch is fully up and operational.
3. Reconnect to the switch, and log on using an account with admin permissions.
4. Enter the `firmwareshow` command and verify that both partitions on the switch have the original firmware.

Testing and Restoring Firmware on Directors

The procedures described in [Testing a Different Firmware Version on a Director](#) and [Test-Driving a New Firmware Version on a Director](#) enable you to perform a firmware download on each control processor (CP) and to verify that the procedure was successful before committing to the new firmware. The previous firmware is saved in the secondary partition of each CP until you enter the `firmwarecommit` command. If you decide to back out of the installation before the firmware commit, you can enter the `firmwarerestore` command to restore the former Fabric OS firmware image.

ATTENTION

- The `firmwarerestore` command can run only if the autocommit functionality was disabled during the firmware download.
- Under normal operating conditions, maintain the same firmware version on both CPs and on both partitions of each CP. This enables you to evaluate firmware before you commit. Do not run mixed firmware levels on CPs.

Testing a Different Firmware Version on a Director

NOTE

The `firmwarerestore` command is local to the control processor (CP). If you run this command on the standby CP, it reboots the standby as expected, swaps partitions, and then runs the `firmwarecommit` command to complete the effective removal of the previous firmware. If, however, you run the `firmwarerestore` command on the active CP, it performs the same actions as for the standby. Then, it automatically triggers a failover to the standby CP, because you have effectively rebooted the active CP with the `firmwarerestore` command.

1. Connect to the director and log on using an account with admin permissions.
2. Enter the `ipaddrshow` command and note the addresses for CP0 and CP1.
3. Enter the `hashow` command and note which CP is the active CP and which CP is the standby CP.
4. Confirm that both CPs are in sync. This is indicated by the text `HA State synchronized` in the following `hashow` output:

```
switch:admin> hashow
Local CP (Slot 1, CP0): Active, Cold Recovered
Remote CP (Slot 2, CP1): Standby, Healthy
HA enabled, Heartbeat Up, HA State synchronized
```

If the CPs are not in sync, see [Downloading Firmware](#) for instructions on synchronizing them.

5. Enter the `firmwareshow` command and confirm that the current firmware on both partitions on both CPs is listed as expected.
6. Exit the session.
7. Update the firmware on the standby CP.
 - a) Connect to the director and log on as admin to the standby CP.
 - b) Enter the `firmwaredownload` command and respond to the prompts.

At this point, the firmware downloads to the standby CP only. When the download to the standby CP has completed, reboot the CP. The current session is disconnected.
8. Fail over to the standby CP.
 - a) Connect to the active CP.
 - b) Enter the `hashow` command and verify that high availability (HA) synchronization is complete. It typically takes a minute or two for the standby CP to reboot and synchronize with the active CP.
 - c) Enter the `firmwareshow` command and confirm that the primary partition of the standby CP contains the new firmware.
 - d) Enter the `hafailover` command. The active CP reboots, and the current session is disconnected.

If a Brocade SX6 Extension Blade is installed: At the point of failover, an autoleveling process is activated to match the firmware on the blade with the firmware on the active CP. Both blade partitions must always contain the same firmware version. The firmware is stored on the compact flash card of the blade and is always synchronized with the firmware of the active CP. This is why the blade firmware is automatically downloaded (autoleveled) to become consistent with the CP firmware.
9. Verify that the failover succeeded.
 - a) Connect to the active CP (the former standby CP).
 - b) Enter the `hashow` command and verify that the HA synchronization is complete. It takes a minute or two for the standby CP, which is the old active CP, to reboot and synchronize with the active CP.

NOTE

If the CPs fail to synchronize, you can still proceed because the version being tested is already present on the active CP; subsequent steps ensure that the standby CP is updated to the same version as the active CP.

 - c) Enter the `firmwareshow` command to confirm that the evaluation firmware version is now running on the active CP.
10. Update the firmware on the standby CP. This allows you to test and validate HA failover using the new firmware.
 - a) Connect to the standby CP (the former active CP).
 - b) Enter the `firmwaredownload -sbn` command. This command ensures that the following steps are successful.

The firmware is downloaded to the standby CP only, and that CP is rebooted. This causes the current logon session to be disconnected.
 - c) Wait until the HA is synchronized, and connect to the director and log on as admin.
 - d) Enter the `firmwareshow` command and confirm that both primary partitions have the test-drive firmware.

You are now ready to evaluate the new firmware version.

ATTENTION

Stop! If you want to *restore* the firmware, stop here and skip to Step 13. Otherwise, continue to Step 11 to commit the firmware on both CPs; this completes the firmware download.

11. Enter the `firmwarecommit` command to update the secondary partition on the standby CP with the new firmware.



CAUTION

Do not do anything on the director while this operation is in process. It takes several minutes to complete the commit operation.

12. Perform a commit on the active CP.

- a) Enter the `firmwareshow` command in the current session on the active CP, and confirm that only the active CP secondary partition contains the old firmware.
- b) Enter the `firmwarecommit` command to update the secondary partition with the new firmware. It takes several minutes to complete the commit operation.



CAUTION

Do not do anything on the director while this operation is in process.

- c) Enter the `firmwareshow` command and confirm that both partitions on both CPs contain the new firmware when the `firmwarecommit` command completes.
- d) Enter the `hashow` command and confirm that the HA state is in sync.

ATTENTION

Stop! If you have completed both Steps 11 and 12, the firmware has been committed to both CPs, and the firmware download procedure is complete.

13. Enter the `firmwarerestore` command in the current session on the standby CP to restore the firmware on that CP.

The standby CP reboots, and the current session ends. After several minutes, both partitions should have the same Fabric OS version.

14. Run HA failover on the active CP.

- a) Enter the `hashow` command in the current session on the active CP, and verify that HA synchronization is complete.

It typically takes a minute or two for the standby CP to reboot and synchronize with the active CP.

- b) Enter the `hafailover` command.

The active CP reboots, and the current session ends. The director is now running the original firmware on the original active CP.

15. Restore the firmware on the *new* standby CP.

- a) Wait 1 minute, and then connect to the director on the new standby CP, which is the former active CP.
- b) Enter the `firmwarerestore` command.

The standby CP reboots, and the current session ends. After several minutes, both partitions should have the same Fabric OS version.

- c) Wait 5 minutes, and then log back on to the director.

- d) Enter the `firmwareshow` command and verify that all partitions have the original firmware.

Your system is now restored to the original partitions on both CPs. You should confirm that all servers using the fabric can access their storage devices. See [Validating the Firmware Version and Firmware Signature](#) for information on this task.

If a Brocade SX6 Extension Blade is installed: Both blade partitions must always contain the same firmware version. The firmware is stored on the compact flash card of the blade and is always synchronized with the active firmware of the CP. Thus, if you restore the active CP firmware, the blade firmware is automatically downloaded (autoleveled) to become consistent with the active CP firmware (the blade firmware is restored).

If you want to upgrade a director that has only one CP installed, follow the procedures in [Testing and Restoring Firmware on Directors](#). Be aware that upgrading a director with only one CP is disruptive to switch traffic.

Test-Driving a New Firmware Version on a Director

This procedure shows how you might install a firmware version to *test-drive* it without either overwriting the version that you are currently using or rebooting your active control processor (CP).

NOTE

The information in this procedure is written at a moderately high level of abstraction, so you might need to look at the more detailed steps in [Testing a Different Firmware Version on a Director](#) if you have questions.

1. Enter the `firmwaredownload -sn` command to download the firmware to the standby CP without committing it.
2. Reboot the standby CP.
3. Enter the `hafailover` command on the active CP to cause the standby CP to come up as the active CP with the “test-drive” firmware active.
4. Run tests as desired on the new firmware on the active CP.
5. Once you have completed your testing, you have two options; neither will disrupt the traffic on the director.
 - Option 1: *I want to restore the firmware I had before.*
 - a. Enter the `hafailover` command on the active CP to get back to the original CP (running the original firmware).
 - b. Enter the `firmwarerestore` command on the standby CP.
This will reboot the standby, swap the partitions, and then run the `firmwarecommit` command on the standby CP.
 - Option 2: *I want to fully install the new firmware.*
 - a. Enter the `firmwaredownload -sb` command on the current standby CP (running the original firmware).
This loads new firmware, reboots the director, and then commits the firmware on the standby.
 - b. Enter the `firmwarecommit` command on the current active CP (running the new firmware).
You are now done. Both CPs have the latest firmware committed and active.

Revision History

The revision history provides a list of the important changes made in each version of the document.

FOS-92x-UPG-UG100; April 28, 2023

Initial document version.

Documentation Legal Notice

This notice provides copyright and trademark information as well as legal disclaimers.

Copyright © 2023. Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. For more information, go to www.broadcom.com. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.

The product described by this document may contain open source software covered by the GNU General Public License or other open source license agreements. To find out which open source software is included in Brocade products or to view the licensing terms applicable to the open source software, please download the open source attribution disclosure document in the Broadcom Support Portal. If you do not have a support account or are unable to log in, please contact your support provider for this information.

