Brocade® Fabric OS® Software Upgrade Guide, 9.0.x

User Guide
30 April 2021

Table of Contents

Copyright Statement

Introduction

About This Document

This document provides the step-by-step procedures to prepare, perform, and verify the upgrade or downgrade of the Fabric OS® firmware. 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 9.0.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 9.0.x.

Brocade Gen 7 (64G) Fixed-Port Switches

- Brocade G720 Switch

Brocade Gen 7 (64G) Directors

For ease of reference, Brocade chassis-based storage systems are standardizing on the term *director*. The legacy term *backbone* can be used interchangeably with the term *director*.

- 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

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

Online	Telephone
For nonurgent issues, the preferred method is to log in to myBroadcom at https://www.broadcom.com/mybroadcom. (You must initially register to gain access to the Customer Support Portal.) Once there, select **Customer Support Portal** > **Support Portal**. You will now be able to navigate to the following sites: • **Knowledge Search**: Clicking the top-right magnifying glass brings up a search bar. • **Case Management**: The legacy MyBrocade case management tool (MyCases) has been replaced with the Fibre Channel Networking case management tool. • **DocSafe**: You can download software and documentation. • **Other Resources**: Licensing Portal (top), SAN Health (top and bottom), Communities (top), Education (top).	Required for Severity 1 (critical) issues: Please call Fibre Channel Networking Global Support at one of the numbers listed at https://www.broadcom.com/support/fibre-channel-networking/.

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

- OEM/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/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/solution provider.

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, publication number, topic heading, page number, and as much detail as possible.

Obtaining Firmware

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

1. Download the Fabric OS firmware files to a fixed-port switch or director. For more information, see the following sections:
   – Downloading Firmware for downloading the Fabric OS firmware files from the Broadcom® website.
   – Downloading Firmware from a USB Device for downloading the firmware from a USB stick that is attached to the switch.
2. Upgrade or downgrade to the newer version of Fabric OS firmware. For more information, see the following sections:
   – Upgrading Firmware on Fixed-Port Switches to upgrade the firmware on a fixed-port switch.
   – Upgrading Firmware on Directors (Including Blades) to upgrade the firmware on a director.

Fabric OS firmware is delivered in RPM Package Manager packages that contain tested and supported .rpm files, along with other needed files. These packages 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).

NOTE
Starting simultaneous firmware downloads on adjacent fixed-port switches may result in 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 document discusses the following types of chassis with the Fabric OS 9.0.x release:

- **Gen 6 (X6) Chassis** – Fabric OS 8.x shipped from the factory that can be upgraded to Fabric OS 9.0.x. This chassis contains the CPX6 CP blades and CR32 core blades.
- **Gen 6 Chassis Upgraded to Gen 7 (X7)** – Fabric OS upgraded to v9.0.x or later. This chassis contains the CPX6 CP blades with new FPGA firmware and is not backward compatible with CR32 core blades and Fabric OS 8.x. The Gen 6 chassis upgraded to Gen 7 is compatible only with the CR64 core blades.
- **Gen 7 (X7) Chassis** – The chassis that is shipped from the factory with Fabric OS 9.0.x. This chassis contains new model CP blades and is not backward compatible with Gen 6 chassis and Fabric OS 8.x. The Gen 7 chassis is compatible only with CR64 core blades.

The following are the prerequisites if you are an existing customer with a Gen 6 chassis and want to upgrade to a Gen 7 chassis:

- Upgrading the Fabric OS version to 9.0.x.
- Replacing the Gen 6 core blades with Gen 7 core blades.

For more information on upgrading to Gen 7, refer to the *Brocade X6 Field Migration Guide*.

NOTE
Once upgraded to Gen 7, you cannot downgrade to any Fabric OS version lower than Fabric OS 9.0.x.

Before downloading the firmware, perform the following tasks. The following preparatory tasks allow you to provide your switch support provider with the information required to troubleshoot the firmware download in case of a failure or timeout.

NOTE
Downloading firmware using Secure File Transfer Protocol (SFTP) is not supported on the multispeed management port if it is set to 1000Mb/s.

1. Read the release notes for the new firmware to find out if there are any updates related to the firmware download process.

   NOTE
   The Fabric OS software does not support nondisruptive upgrades from any release more than one major release earlier than the one being installed. This means that nondisruptive upgrading to Fabric OS 9.0.x is supported from Fabric OS 8.2.x only. If you try to upgrade from an earlier version of Fabric OS software (for example, 8.1.x), perform a disruptive upgrade.

2. Log the telnet session to record the information shown during this process, because you can use this information to validate the correctness of the installation. Connect to the switch and log in using an account with admin permissions.

   For additional support:

   a) Connect the switch directly to a computer using a serial console cable.
   b) Ensure that all serial console sessions (for both CPs on directors) and any open network connection sessions such as telnet sessions are being logged.

3. Enter `firmwareshow` to verify the current version of Fabric OS software.
4. Enter `hashow` 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:
   – 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 downloading Fabric OS software.
4. Enter `firmwaredownloadstatus` 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.
5. 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 that the installation was correct and complete.

      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 `switchshow` to verify that no ports are running as G_Ports.
6. Back up the configuration file and retrieve all current core files before downloading the new firmware to the device.
   a) Enter `configupload` to save the configuration file to your FTP or SSH server or to a USB memory device.
   b) Enter `supportsave` to retrieve all current core files. This information is useful to troubleshoot the firmware download process if a problem occurs.
7. Enter `errclear` to clear all existing messages, including internal messages.
8. Enter `supportsave -R` (uppercase *R*). This action clears all core and trace files.
9. Continue with the firmware download.

Finding the Switch Firmware Version

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

   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 firmware stored in non-volatile memory.
   - **BootProm** – Displays the version of the firmware stored in the boot PROM.

   The following example shows the output of the `version` command.

```
switch:admin> version
Kernel:     4.1.35rt41
Fabric OS:  v9.0.0
Made on:    Thu Jan 16 19:48:47 2020
Flash:      Mon Jan 20 05:06:28 2020
BootProm:   sb-4.0.10
```

Downloading Firmware

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

Perform the following procedure to download the firmware and documentation files from the website and download the firmware to a switch or a director.

1. From the website https://www.broadcom.com/mybroadcom, click **LOGIN**, and enter your username and password.

   If you do not have an account, click **REGISTER** to set up your account.
2. Select **Customer Support Portal** > **Documents and Software**.
3. Do one of the following:
   a) Enter the product name or the firmware version number in the **Search** box. For example, the following search is for firmware and documentation files for firmware version 8.2.1.
   b) Click the **Product Search** box, select **FIBRE CHANNEL NETWORKING**, and select a product from the product lists.

   The list of firmware and documents available for the product appears. Click the **Download** button to download the required firmware.
4. 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 traffic between switches in your fabric is not disrupted.
5. Use the `firmwaredownload` command to download the firmware to the switch by using FTP, SFTP, or SCP to connect to an FTP or SSH server or use a Brocade-branded USB device to which the firmware is downloaded. If you are using FTP, SFTP, or SCP, verify that the FTP or SSH server is running on the host server and you have a valid

user ID, password, and permissions for that server. If you are planning to use the Challenge Response Authentication (CRA) protocol with either SFTP or SCP, you must first enable this protocol on the host server side.

6. 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 `usbstorage -e` to mount the USB device.
   c) Enter `usbstorage -l` to verify that it is running.
7. The `firmwaredownload` command supports both non-interactive and interactive modes. If this command is issued without any operands or if there is any syntax error in the parameters, the command enters an interactive mode to prompt you for input.
8. Unpack the downloaded firmware, and it expands into a directory that is named according to the version of Fabric OS software that it contains. For example, when you download and unzip the file named `8.2.1.zip` , it expands into a directory that is named 8.2.1.
9. Specify the complete path up to and including the 8.2.1 directory name using the interactive commands for the `firmwaredownload` command to work properly. When you issue 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 displays the complete path for the `firmwaredownload` command:

```
switch:admin> firmwaredownload -s
Server Name or IP Address: 10.1.2.3
User Name: admin
File Name: /pub/sre/SQA/fos/v8.2.1/v8.2.1
```

   NOTE
   If DNS is enabled and a server name instead of a server IP address is specified in the command line, `firmwaredownload` 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 `dnsconfig` command.

10. The following example illustrates 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: 10.1.2.3
User Name: admin
File Name: /home/SAN/fos/8.2.1/8.2.1
Network Protocol(1-auto-select, 2-FTP, 3-SCP, 4-SFTP) [1]: 4
Verifying if the public key authentication is available.Please wait ... The public key authentication is
 not available.
Password: <hidden>
Server IP: 10.0.0.0, Protocol IPv4
Checking system settings for firmwaredownload...
```

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

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` processes do not start until the firmware is activated. You can use the `firmwareactivate` command in both single-CP and dual-CP environments.

To stage the firmware:

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
Appl     Primary/Secondary Versions
---------------------------------
FOS           v8.2.1
              V8.2.1a
```

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 to be restarted.
Do you want to continue (Y/N) [Y]:
```

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. You can run `firmwaredownloadstatus` to monitor the status of the firmware download.

Downloading Firmware without a Password

To download the firmware without a password:

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 logins 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*.

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 `firmwaredownload -r` or `firmwaredownload -lr`.
2. Enter `firmwareshow` to view the current firmware version on each partition.

```
switch:admin> firmwareshow
Appl     Primary/Secondary Versions
---------------------------------
Fabric OS     v8.2.1
              v8.2.1
```

3. Enter `firmwareactivate` 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]:
```

Downloading Firmware from a USB Device

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

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

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

1. Open a file browser and navigate to the directory on the USB device if you are using Windows. Drag the unzipped firmware image files from where you downloaded them to this directory. You can store multiple images under this directory.
2. Enable and mount the USB device as a file system if you are using Linux. After completing this, copy the unzipped firmware images to be downloaded to the directory.
3. Enter the `firmwaredownload` command with the `-U` (uppercase U) option to download the specified firmware image from the USB device. When specifying a path to a firmware image in the USB device, you can 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 are updating a USB device on an external server, ensure that the device is properly ejected from the server before physically unplugging it.

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

- SanDisk 32 CZ48 USB 3.0 Flash Drive (SDCZ48-032G-UAM46)
- SanDisk 16 CZ48 USB 3.0 Flash Drive (SDCZ48-016G-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 Attache 3.0 4 USB 32GB Flash Drive
- PNY Attache 3.0 4 USB 16GB Flash Drive

Enabling the USB Device

1. Log in to the switch using an account with admin permissions.
2. Enter the `usbstorage -e` command.
   This enables the USB device. You can now use it to install the firmware.

Viewing the USB File System

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

```
switch:admin> usbstorage -l
     v8.2.1\              1126MB    2020 January 30 15:33
Available space on USB storage 96%
```

Downloading from the USB Device Using a Relative Path

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

1. Connect to the device and log in using an account with admin permissions.
2. Enter `firmwaredownload -U` (uppercase U), followed by the name of the firmware directory. In the following example, the directory is 9.0.0.

```
switch:admin> firmwaredownload -U 9.0.0
```

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, but they 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 firmware. The firmware download process first copies the replacement files (which may 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 1: Gen 6 and Gen 7 Platforms and Supported Firmware Downgrade Versions from Fabric OS 9.0.x

Platforms	Fabric OS 9.0.x	Fabric OS 8.2.x	Fabric OS 8.1.x
Brocade Gen 7 (64G) Fixed-Port Switches			
Brocade G720	Supported	Not Supported	Not Supported
Brocade Gen 7 (64G) Directors			
Brocade X7-4 Director	Supported	Not Supported	Not Supported
Brocade X7-8 Director	Supported	Not Supported	Not 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 (Fabric OS 9.0.1b and later)	Not Supported	Not Supported
Brocade G620 (Switch Type 162)	Supported	Supported	Supported
Brocade G620 (Switch Type 183)	Supported	Not Supported	Not Supported
Brocade G630 (Switch Type 173)	Supported	Supported	Not Supported
Brocade G630 (Switch Type 184)	Supported	Not Supported	Not Supported

Platforms	Fabric OS 9.0.x	Fabric OS 8.2.x	Fabric OS 8.1.x
Brocade 7810 Extension Switch	Supported	Supported (Fabric OS 8.2.1 and later)	Not Supported
Brocade G648 Blade Server SAN I/O Module	Supported	Supported	Not Supported
Brocade MXG610 Blade Server SAN I/O Module	Supported	Supported	Not 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 2: 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 9.0.x version of Fabric OS software, refer to the upgrade and downgrade sections of the *Brocade Fabric OS Flow Vision User Guide*.
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 9.0.x version of Fabric OS software, refer to the *Brocade Fabric OS MAPS User Guide*.
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 9.0.x version of Fabric OS software, refer to the *Brocade Fabric OS Extension User Guide*.
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 9.0.x version of Fabric OS software, refer to the upgrade and downgrade sections of the *Brocade Fabric OS FCoE User Guide*.

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 3: Supported Upgrade Paths to Fabric OS 9.0.x

Current Fabric OS Version	Upgrade Procedure
Fabric OS 8.2.x	A nondisruptive direct upgrade is possible.
Fabric OS 8.1.x	A disruptive direct upgrade is possible by using the `firmwaredownload -s` command.

Supported Link Modes

Fabric OS 9.0.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 Gen 7 directors or in the existing Gen 6 directors upgraded to Gen 7 directors that are running Fabric OS 9.0.x.

Table 4: Supported Blades in Fabric OS 9.0.x

Blade	X7 Director	X6 Director Upgraded to X7	X6 Director
FC64-48	Yes	Yes	No
FC32-X7-48	Yes	Yes	No
FC32-48	Yes	Yes	Yes
FC32-64	Yes	Yes	Yes
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

Before you upgrade the firmware on your switch or director, ensure that the following steps are verified to ensure compatibility with the new Fabric OS version and any older Fabric OS version.

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 may result in traffic disruption.

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

Blades Not Supported in Gen 7 Directors

Gen 7 directors that run Fabric OS 9.0.x do not support the following blades:

- CR32-4
- CR32-8

Currently, if you are running any Brocade Gen 6 director with these blades, you must physically remove those blades before upgrading it to Fabric OS 9.0.x. The firmware upgrade process will be blocked if any one of these blades is present. If any of these blades is installed after upgrading to Fabric OS 9.0.x, the slot that the blade is in will fault, and the blade will not be available; all other blades will function normally.

For more information on replacing Gen 6 core blades with Gen 7 core blades, refer to the *Brocade X6 Field Migration Guide*.

General Upgrade Considerations

Consider the following information before upgrading a device to Fabric OS 9.0.x:

- If the chassis contains Gen 6 core blades during the firmware upgrade, any Gen 7 port blades present will be faulted.
- Changing the default passwords for admin and all user accounts before upgrading to Fabric OS 9.0.x is mandatory.
- If the active or defined IP Filter policies are configured with Packet Forwarding rules, the Fabric OS 9.0.x firmware download will be blocked. IP Filter forwarding is not supported in Fabric OS 9.0.x.
- If both C4 (CR32-4 and CR32-8) and C5 core blades (CR64-4 and CR64-8) are present on the same chassis, the last inserted (second) core will be faulted. A power off/on of the switch is required when the last enabled C4 core blades are replaced with C5 core blades or in reverse.
- If you do not accept the end-user license agreement (EULA) terms and conditions, the Fabric OS 9.0.x upgrade will be blocked.
- Disabling LDAP authentication (if enabled) on the switch before upgrading is mandatory. If Brocade VSAs are not configured for users on the LDAP server, LDAP authentication mandates role mapping in the target Fabric OS version. Ensure that the Brocade VSA configuration exists on the server or map the AD group to a switch role with the `ldapcfg --maprole` command to avoid the probable login failure for LDAP users after the upgrade.
- Deleting the users and roles with the name "Maintenance" is mandatory before upgrading to Fabric OS 9.0.x.
- The SSH option to generate authorized keys with a passphrase is disabled. If authorized keys are already generated with a passphrase, generate new keys without a passphrase.
- Setting the protocol to Any for HTTP in a template translates to the max protocol version of TLSv1.3. You can use any TLS protocols from TLSv1 to TLSv1.3. In the case of a chassis, the configurations applied using a template need to be supported on both active and standby CP versions. If the chassis is running different firmware versions on both CPs and the configuration applied is not valid for the standby CP, then the `seccryptocfg` configuration will fail.
- Upgrading to Fabric OS 9.0.x allows you to extend the length of the chassis name up to 31 characters.
- Gen 5 platforms and packages, including the older versions of the OSS packages, are not supported in Fabric OS 9.0.x.
- FIPS mode is disabled and not supported when upgrading to Fabric OS 9.0.x. After completing a successful upgrade, you can configure "FIPS-Inside" mode in Fabric OS 9.0.x.
- If the cryptographic ciphers that are not supported in the Fabric OS 9.0.x version are configured, a firmware upgrade is not allowed. For more information on supported ciphers, refer to the *Brocade Fabric OS Administration Guide*.
- Disabling the Management IPsec before upgrading to Fabric OS 9.0.x is mandatory.
- If the root password on a device is set to the default value during an upgrade, the root account will retain its previous status. That is, if the root account was disabled in the earlier Fabric OS version, it will remain disabled; but if it is enabled in the earlier version, it will remain enabled after the upgrade. Be aware that the root account is disabled by default on all devices shipped directly from the factory or if you use the `firmwarecleaninstall` command to update the device, assuming that the earlier release is supported on the platform.

  NOTE

  Not all systems ship with a root account. If your device does not ship with a root account, this account cannot be enabled.
- When you upgrade to a Fabric OS 9.0.x version, if the switch is already configured with an IP address, you must change the IP address to permit registered organization name (RON) configuration.

General Downgrade Considerations

Consider the following information before attempting to downgrade a device from Fabric OS 9.0.x to an earlier version of Fabric OS software:

- A Fabric OS firmware downgrade is not supported if the FPGA is already upgraded.
- A Fabric OS version downgrade will be blocked if the SSH identity keys are present with the openSSH key format.
- If new SSH identity keys are generated in the Fabric OS 9.0.x version, the downgrade will be blocked. You can delete those private keys using `sshutil delprivkey` before downgrading.
- A Fabric OS downgrade will be blocked if Elliptic Curve Digital Signature Algorithm (ECDSA) certificates or Certificate-Signing Requests (CSRs) were created.
- A Fabric OS downgrade will be blocked if the IPv6 RADIUS server is configured with PEAP-MSCHAPv2 authentication.
- A Fabric OS downgrade to earlier releases will be blocked if the Session-Timeout feature is enabled. You can disable the Session-Timeout feature using the `timeout --session 0` command.
- If ciphers or protocols that are applicable to only the Fabric OS 9.0.x version are configured, the Fabric OS downgrade will be blocked. Ensure that the ciphers are updated based on the target firmware before downgrading.
- The root access level settings do not block a downgrade irrespective of the configuration that exists for the root access (Console only, None, or All). Also, the root account setting (enabled or disabled) persists after a downgrade.
- A downgrade is not allowed if one or more ports are configured with encryption. You must disable the encryption configuration before the downgrade.
- If you are downgrading to an earlier version of 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 will be blocked in the following cases:
  - The maintenance role is mapped to an LDAP role.
  - The access-time is configured for the Maintenance role.
  - The password expiration policy is configured for the Maintenance role.
- Changing default passwords for admin and user accounts is mandatory before downgrading from Fabric OS 9.0.x.

Upgrading Firmware on Fixed-Port Switches

The firmware download is an incremental process in Fabric OS 9.0.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 `firmwaredownload` . 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, `firmwaredownload` 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 may experience a delay. Fixed-port switches may need to retry the operation(s) in this case.

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

```
switch:admin> firmwareshow
Appl     Primary/Secondary Versions
------------------------------------------
FOS      v9.0.0
         v9.0.0
```

Firmware Download with Legacy Mode

The number of packages installed on a switch is reduced with the 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. You can preferably skip the incremental download and opt for the firmware download using the legacy mode.

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

```
switch:admin> firmwaredownload -L
Server Name or IP Address: 10.01.02.03
User Name:admin
File Name: /pub/sre/SQA/fos/v9.0.0/v9.0.0_bld72
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
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 `firmwaredownload`.

The firmware download does not automatically update the FPGA firmware into the system's FPGA flash memory. If an updated FPGA version is included in a Fabric OS firmware update, after the firmware download is completed, you must enter `fpgaupgrade` 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 will be 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 `fpgaupgrade` displays a message that the image is up to date, and the utility will 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
```

If your device is not running the latest FPGA image, running `fpgaupgrade` 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:

```
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.
```

You can use `fpgaupgrade --latest` to verify if the running FPGA image is the latest or not. The following example shows a down-level FPGA.

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

Depending on the error, you may be requested not to power-cycle the system until the corrective action is taken. The following is an example of such 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
Do not power-cycle the affected blade or switch before contacting your switch supplier if there is an error. A failed FPGA update can result in an outage for the affected blade or the entire switch (in the case of 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 may 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 located on 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 `firmwaredownload` , you should copy the uncompressed release folder to the device at this time.
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.

   NOTE
   Synchronization of the CPs is not the same as 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 an SX6 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 SX6 blades, they will be updated simultaneously; however, the downloads may 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 may be affected. If there is an active FCIP tunnel on the SX6 blade, the FCIP tunnel traffic will be impacted for at least 2 minutes.

```
switch:admin> firmwaredownload
Server Name or IP Address: 10.01.02.03
User Name: admin
File Name: /home/user/9.0.0
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 `firmwaredownloadstatus` to monitor the firmware download status.

```
switch:admin> firmwaredownloadstatus
[1]: Fri Jan 24 16:25:49 2020Slot 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 2020Slot 2 (CP1, active): Firmware has been downloaded successfully to Standby
 CP.
[3]: Fri Jan 24 16:31:51 2020Slot 2 (CP1, active): Standby CP is going to reboot with new firmware.
[4]: Fri Jan 24 16:35:41 2020Slot 1 (CP0, active): Forced failover succeeded. New Active CP is running new
 firmware
[5]: Fri Jan 24 16:36:48 2020Slot 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 2020Slot 1 (CP0, active): Firmware has been downloaded successfully on Standby
 CP.
[7]: Fri Jan 24 16:39:27 2020Slot 1 (CP0, active): Standby CP reboots.
[8]: Fri Jan 24 16:41:59 2020Slot 1 (CP0, active): Firmware commit operation has started on both active
 and standby CPs.
[9]: Fri Jan 24 16:42:00 2020Slot 1 (CP0, active): The firmware commit operation has started. This may
 take up to 10 minutes.
[10]: Fri Jan 24 16:42:00 2020Slot 1 (CP0, active): Standby CP booted successfully with new firmware.
[11]: Fri Jan 24 16:46:08 2020Slot 1 (CP0, active): The commit operation has completed successfully.
[12]: Fri Jan 24 16:46:08 2020Slot 1 (CP0, active): Firmware commit operation has completed successfully
 on active CP.
```

10. Enter `firmwareshow` 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      v9.0.0
         v9.0.0
```

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. Signed firmware download is the default behavior; however, you can use the `firmwarekeyshow` command to view the contents of the public key used for validating the firmware signature.

Table 5: Commands Used for Validating Firmware Downloads and Version

Command	Description
`firmwareshow`	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 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.
`firmwaredownloadstatus`	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 `firmwaredownload` command and is kept until another `firmwaredownload` 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.
`firmwarekeyshow`	Displays the contents of the public key used for validating the integrity of firmware images. A firmware key should be installed on every switch as a part of the Fabric OS installation. Signed firmware download is the default behavior. During firmware download, if the validation succeeds, firmware download proceeds normally. If the firmware is not signed or if the signature validation fails, the firmware download fails. For information on `firmwarekeyshow` commands, refer to *Brocade Fabric OS Command Reference Manual*.

Verifying the Device and Fabric Connections

Use the `nsshow` , `nsallshow` , and `fabricshow` commands to ensure that the fabric and connections to the attached devices are 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 6: Commands Used for Validating Firmware and Fabric Functionality

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

Testing Firmware

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 quickly 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

1. Enter `firmwaredownload -sn` to download the firmware to a single partition and to disable the autocommit mode. See Downloading Firmware for details on this process for your environment.
2. Connect to the switch and log in using an account with admin permissions.
3. Enter `firmwareshow` to view the current firmware.
4. If the firmware level change is only one level up or down, the system will attempt a non-disruptive 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 may 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 in using an account with admin permissions.
6. Enter `firmwaredownloadstatus` to view the status of the firmware download.

Once you have downloaded and installed the new firmware version, you can evaluate it. Once you have completed 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 `firmwareshow` to confirm that the primary partition of the switch contains the new firmware.
2. Enter `firmwarecommit` to update the secondary partition with the new firmware.
   It takes several minutes to complete the commit operation.
3. Enter `firmwaredownloadstatus` to view the status of the firmware download.
4. Enter `firmwareshow` to confirm that both partitions on the switch contain the new firmware.

   When you have completed this step, you have committed the firmware to the switch and have 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 `firmwarerestore` to reboot the switch and restore the original firmware.

   This 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 `firmwarerestore` to ensure that all processes have completed and that the switch is fully up and operational.
3. Reconnect to the switch and log in using an account with admin permissions.
4. Enter `firmwareshow` 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 allow 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 `firmwarerestore` 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.

NOTE
Under normal operating conditions, maintain the same firmware version on both CPs and both partitions of each CP. This enables you to evaluate firmware before you commit. As a standard practice, 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 `firmwarecommit` to complete the effective removal of the previous firmware. If, however, you run `firmwarerestore` on the active CP, it performs the same actions as for the standby. Then, it automatically triggers a failover to the standby CP, because effectively you have rebooted the active CP with the `firmwarerestore` command.

1. Connect to the director and log in using an account with admin permissions.
2. Enter `ipaddrshow` and note the addresses for CP0 and CP1.
3. Enter `hashow` 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 `firmwareshow` 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 in as admin to the standby CP.
   b) Enter `firmwaredownload` 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 `hashow` 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 `firmwareshow` and confirm that the primary partition of the standby CP contains the new firmware.
   d) Enter `hafailover` . The active CP reboots, and the current session is disconnected.

      If an SX6 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 `hashow` 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, and subsequent steps ensure that the standby CP is updated to the same version as the active CP.
   c) Enter `firmwareshow` 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 `firmwaredownload -sbn` . This 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 login session to be disconnected.
    c) Wait until the HA is synchronized, and connect to the director and log in as admin.
    d) Enter `firmwareshow` 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 `firmwarecommit` 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 `firmwareshow` in the current session on the active CP, and confirm that only the active CP secondary partition contains the old firmware.
    b) Enter `firmwarecommit` 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 `firmwareshow` and confirm that both partitions on both CPs contain the new firmware when the `firmwarecommit` command completes.
    d) Enter `hashow` 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 `firmwarerestore` 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 `hashow` 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 `hafailover` .

    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 `firmwarerestore` .

    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 in to the director.
    d) Enter `firmwareshow` 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 for information on this task.

If an SX6 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

The following procedure shows how you can 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 may need to look at the more detailed steps in Testing a Different Firmware Version on a Director if you have questions.

1. Enter `firmwaredownload -sn` to download the firmware to the standby CP without committing it.
2. Reboot the standby CP.
3. Enter `hafailover` 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 `hafailover` on the active CP to get back to the original CP (running the original firmware).
     b. Enter `firmwarerestore` on the standby CP.
     This will reboot the standby, swap the partitions, and then run `firmwarecommit` on the standby CP.
   - Option 2: *I want to fully install the new firmware.*
     a. Enter `firmwaredownload -sb` 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 `firmwarecommit` on the current active CP (running the new firmware).
     You are now done. Both CPs have the latest firmware committed and active.

Revision History

FOS-90x-UPG-UG101; 30 April 2021

- Updated the table in the Upgrading and Downgrading Firmware section with the new Brocade G610 switch types.
- Standardized all references to the Fabric OS 9.0.x version.
- Made editorial updates.

FOS-90x-UPG-UG100; 30 April 2020

Initial document version.


BROADCOM®