BROCADE

SOFTWARE UPGRADE GUIDE

Brocade Fabric OS Upgrade Guide

Supporting Fabric OS 8.0.1

53-1004124-01
22 April 2016

Contents

Preface

Document conventions

The document conventions describe text formatting conventions, command syntax conventions, and important notice formats used in Brocade technical documentation.

Text formatting conventions

Text formatting conventions such as boldface, italic, or Courier font may be used in the flow of the text to highlight specific words or phrases.

Format	Description
bold text	Identifies command names
	Identifies keywords and operands
	Identifies the names of user-manipulated GUI elements
	Identifies text to enter at the GUI
italic text	Identifies emphasis
	Identifies variables
	Identifies document titles
`Courier font`	Identifies CLI output
	Identifies command syntax examples

Command syntax conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
value	In Fibre Channel products, a fixed value provided as input to a command option is printed in plain text, for example, **--show** WWN.
[ ]	Syntax components displayed within square brackets are optional.
	Default responses to system prompts are enclosed in square brackets.
{ **x** | **y** | **z** }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
	In Fibre Channel products, square brackets may be used instead for this purpose.
x | **y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.

Convention	Description
...	Repeat the previous element, for example, *member*[*member*...].
\	Indicates a "soft" line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Notes, cautions, and warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

NOTE
A Note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION
An Attention statement indicates a stronger note, for example, to alert you when traffic might be interrupted or the device might reboot.

CAUTION
A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER
A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Brocade resources

Visit the Brocade website to locate related documentation for your product and additional Brocade resources.

You can download additional publications supporting your product at www.brocade.com. Select the Brocade Products tab to locate your product, then click the Brocade product name or image to open the individual product page. The user manuals are available in the resources module at the bottom of the page under the Documentation category.

To get up-to-the-minute information on Brocade products and resources, go to MyBrocade. You can register at no cost to obtain a user ID and password.

Release notes are available on MyBrocade under Product Downloads.

White papers, online demonstrations, and data sheets are available through the Brocade website.

Contacting Brocade Technical Support

As a Brocade customer, you can contact Brocade Technical Support 24x7 online, by telephone, or by e-mail. Brocade OEM customers contact their OEM/Solutions provider.

Brocade customers

For product support information and the latest information on contacting the Technical Assistance Center, go to http://www.brocade.com/services-support/index.html.

If you have purchased Brocade product support directly from Brocade, use one of the following methods to contact the Brocade Technical Assistance Center 24x7.

Online	Telephone	E-mail
Preferred method of contact for non-urgent issues: • My Cases through MyBrocade • Software downloads and licensing tools • Knowledge Base	Required for Sev 1-Critical and Sev 2-High issues: • Continental US: 1-800-752-8061 • Europe, Middle East, Africa, and Asia Pacific: +800-AT FIBREE (+800 28 34 27 33) • For areas unable to access toll free number: +1-408-333-6061 • Toll-free numbers are available in many countries.	support@brocade.com Please include: • Problem summary • Serial number • Installation details • Environment description

Brocade OEM customers

If you have purchased Brocade product support from a Brocade OEM/Solution Provider, contact your OEM/Solution Provider for all of your product support needs.

- OEM/Solution Providers are trained and certified by Brocade to support Brocade® products.
- Brocade 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, contact Brocade or your OEM.
- For questions regarding service levels and response times, contact your OEM/Solution Provider.

Document feedback

To send feedback and report errors in the documentation you can use the feedback form posted with the document or you can e-mail the documentation team.

Quality is our first concern at Brocade and we have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission, or you think that a topic needs further development, we want to hear from you. You can provide feedback in two ways:

- Through the online feedback form in the HTML documents posted on www.brocade.com.
- By sending your feedback to documentation@brocade.com.

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

About this document

Supported hardware and software

The following hardware platforms are supported by Fabric OS 8.0.1.

NOTE
Although many different software and hardware configurations are tested and supported by Brocade Communication Systems, Inc for Fabric OS 8.0.1, documenting all possible configurations and scenarios is beyond the scope of this document.

Brocade Gen 5 (16-Gbps) fixed-port switches

- Brocade 6505 switch
- Brocade 6510 switch
- Brocade 6520 switch
- Brocade M6505 blade server SAN I/O module
- Brocade 6543 blade server SAN I/O module
- Brocade 6545 blade server SAN I/O module
- Brocade 6546 blade server SAN I/O module
- Brocade 6547 blade server SAN I/O module
- Brocade 6548 blade server SAN I/O module
- Brocade 6558 blade server SAN I/O module
- Brocade 7840 Extension Switch

Brocade Gen 5 (16-Gbps) DCX 8510 Directors

NOTE
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 DCX 8510-4 Director
- Brocade DCX 8510-8 Director

Brocade Gen 6 fixed-port switches

- Brocade G620 switch

Brocade Gen 6 Directors

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

Fabric OS support for the Brocade Analytics Monitoring Platform (AMP) device depends on the specific version of the software running on that platform. Refer to the AMP Release Notes and documentation for more information.

Supported upgrade paths

The following table gives you details on supported upgrade paths and steps to upgrade through multiple versions of Fabric OS. For specific Fabric OS builds, refer to the *Fabric OS Release Notes* for that build of Fabric OS. For upgrading to other versions of Fabric OS, refer to the *Fabric OS Upgrade Guide* for the version of Fabric OS you want to upgrade to.

TABLE 1 Supported upgrade paths to Fabric OS 8.0.1

Upgrading from	Upgrade procedure
Fabric OS 7.1.x	A direct upgrade is not possible. You must upgrade first to Fabric OS 7.2.x, then to Fabric OS 7.3.x and then to Fabric OS 7.4.x before upgrading to Fabric OS 8.0.1.
Fabric OS 7.2.x	A direct upgrade is not possible. You must upgrade first to Fabric OS 7.3.x and then to Fabric OS 7.4.x before upgrading to Fabric OS 8.0.1.
Fabric OS 7.3.x	A non-disruptive direct upgrade is not possible. To upgrade non-disruptively, you must do a non-disruptive upgrade to Fabric OS 7.4.x before upgrading to Fabric OS 8.0.1. A disruptive direct upgrade is possible by using the **firmwaredownload -s** command.
Fabric OS 7.4.x	A nondisruptive direct upgrade is possible.
Fabric OS 8.0.0	A nondisruptive direct upgrade is possible.

Upgrade and downgrade considerations

Upgrading and downgrading firmware

In this publication, *upgrading* means installing a newer version of firmware, while *downgrading* means installing an older firmware version.

In most cases, you will be *upgrading* firmware; that is, installing a newer firmware version than the one you are currently running. However, some circumstances may require installing an older version; that is, *downgrading* the firmware. The procedures in this section assume that you are upgrading firmware, but they work for downgrading as well, provided the old and new firmware versions are compatible. Most firmware upgrades and downgrades are non-disruptive to device operations, but Brocade strongly recommends that you always refer to the latest Fabric OS release notes for updates regarding up- and downgrading.

TABLE 2 Currently supported Fabric OS versions and platforms

Platforms	Fabric OS 7.4.x	Fabric OS 8.0.0	Fabric OS 8.0.1
Gen 5 switches and Directors	Supported	Not Supported	Supported
G620 Switch	Not Supported	Supported	Supported
X6 Directors	Not Supported	Not Supported	Supported

For instructions about testing firmware without fully installing it, refer to Testing firmware on page 33.

Flow Vision upgrade and downgrade considerations

The Brocade Flow Vision application has specific firmware upgrade and downgrade considerations.

For firmware upgrade and downgrade considerations that apply to Flow Vision and Fabric OS 8.0.1, refer to the upgrade and downgrade sections of the *Flow Vision Administrator's Guide*.

Upgrade and downgrade considerations for MAPS

The Brocade Monitoring and Alerting Policy Suite (MAPS) has specific firmware upgrade and downgrade considerations.

For firmware upgrade and downgrade considerations that apply to MAPS and Fabric OS 8.0.1, refer to the upgrade and downgrade sections of the *Monitoring and Alerting Policy Suite Administrator's Guide*.

General upgrade considerations

The following general items should be taken into consideration before upgrading a device to Fabric OS 8.0.1.

- On a Brocade G620 with online EX_Ports, you must have the "Integrated Routing" license installed when you upgrade from Fabric OS 8.0.0 to Fabric OS 8.0.1. You should retain the 8.0.0-level Integrated Routing license if you want to downgrade to Fabric OS 8.0.0. All other Gen 6 switches require the "Integrated Routing Port on Demand" license to enable EX_Ports.

- During the firmware upgrade, a configuration file uploaded from firmware versions Fabric OS 7.3.x and Fabric OS 7.4.x can be used to configure Fabric OS 8.0.1.
- If the root password on a device is set to the default value when you upgrade, the root account will retain its previous status. That is, if it was disabled in the previous version, it will remain disabled, but if it is enabled in the previous 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.

  Refer to Enabling the root password on page 13 for instructions on setting the root password.

General downgrade considerations

The following general items should be taken into consideration before attempting to downgrade a device from Fabric OS 8.0.1 to an earlier version of Fabric OS.

- Root access level settings will not block a downgrade, no matter what configuration exists for root access (consoleonly, none, or all). Root-level access is allowed on all interfaces after a downgrade. In addition, the root account setting (enabled or disabled) persists after a downgrade.
- You cannot downgrade any Brocade Gen 6 or later device other than the Brocade G620 to any version of Fabric OS earlier than Fabric OS 8.0.1. The Brocade G620 is the only device that can be downgraded to Fabric OS 8.0.0.
- If you are downgrading a Gen 5 platform to a version of Fabric OS earlier than Fabric OS 7.4.x, refer to the *Fabric OS Upgrade Guide* for that Fabric OS version to confirm that the hardware supports that version of the firmware.
- Fabric OS 7.4.0 and later include the Europe/Samara, Asia/Srednekolymsk, and Asia/Anadyr time zones. If these time zones are configured on a switch, the downgrading to any version of Fabric OS earlier than 7.4.0 is blocked because the earlier versions do not support these time zones. To perform a downgrade in this situation, you will need to first remove these time zones from the platform configuration.
- During the firmware downgrade, a configuration file uploaded from Fabric OS 8.0.1 can configure firmware versions Fabric OS 7.3.x and Fabric OS 7.4.x.
- Downgrading from Fabric OS 8.0.1 to earlier versions of Fabric OS may require changes to the default password hash and the level of root access. Specifically, when you attempt a downgrade from Fabric OS 8.0.1 to Fabric OS 8.0.0 or earlier, you may be presented with a message to change the password hash to MD5 before you can downgrade the device. To do this, enter **passwdcfg --hash md5** and then change **all** account passwords so that their passwords are now stored using MD5 to hash the passwords. This is required because versions of Fabric OS prior to 8.0.1 can only read MD5 hashes.

  

  CAUTION
  When you do this, the stored non-MD5 password history will be permanently lost. Although no confirmation is required, a warning message is displayed.

- Fabric OS 8.0.1 allows you to restrict user access time. If there are user accounts with access time configurations on a device, you will not be able to downgrade the OS until the access time for every account is set to "00:00-00:00". This can be done using the **userconfig** command.
- Fabric OS 8.0.1 provides support for user-defined port name formatting for dynamic port names. Prior to 8.0.1, only the default dynamic port name format was supported. As a result, downgrading from Fabric OS 8.0.1 to earlier versions is blocked if the dynamic port name feature is enabled and there is a dynamic portname format other than the default format. In this case, the following message is displayed:

```
Dynamic portname format is not set to default in one or more partitions. Please run "portname
-d -default" in the corresponding partitions to set default portname format.
```

- If peer zoning exists in the zone configuration, downgrading from Fabric OS 8.0.1 to versions prior to Fabric OS 7.3.0 displays the following warning message:

  ```
  WARNING: You are downgrading to a version of Fabric OS that does not support Peer Zoning. The
  peer zone(s) or target driven peer zone(s) enabled in the effective configuration will be
  treated as regular zones after downgrade.
  ```

- Fabric OS 8.0.x, 7.4.x, and 7.3.x automatically detect mismatches between the active control processor (CP) firmware and application processor (AP) blade firmware and triggers the autoleveling process. This autoleveling process automatically updates the AP blade firmware to match the active CP. At the end of the autoleveling process, the active CP and the AP blade will be running the same firmware version.

Enabling the root password

To ensure proper device security after you have upgraded a Brocade device, you should enable the root password and change it from its default value.

NOTE
If you have lost or forgotten the root password, contact your service provider for password reset/recovery procedures.

To enable and change the root password after you have upgraded, complete the following procedure:

1. Login as admin (using console, SSH, Telnet, or other supported means) using the active admin password.

   While you are not required to change the admin password as part of this login, Brocade strongly recommends that you do so. Always remember to record the new password in a secure location.
2. Enter **userconfig --change root -e yes** to enable the root account.
3. Use the command **rootaccess --set** *required mode* to specify the mode that can be used to access the device. The default mode is “consoleonly”.
4. Log out and then log back in as root using the mode you just specified.
5. Enter the default root password, and then set the new root password.

   Changing the default root password is required for all scenarios (upgrades, running the **firmwarecleaninstall** command, and).

Firmware installation and maintenance

Firmware download process overview

You can download Fabric OS to a chassis-based system (Director); or to a nonchassis-based system, also referred to as a fixed-port switch. The difference in the download process is that Directors have two control processors (CPs) and fixed-port switches have one CP. In Directors the firmware download process sequentially upgrades the firmware image on both CPs using High Availability (HA) failover to prevent disruption to traffic flowing through the platform. This operation depends on the HA status on the Director.

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

Fabric OS firmware is delivered in RPM Package Manager (RPM) 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
> Brocade does not supply individual .rpm files, only packaged installation file sets (distributions).

You can use either the **firmwaredownload** command to download the firmware from either an FTP or SSH server by using FTP, SFTP, or SCP to the switch, or you can use a Brocade-branded USB device that the firmware has been downloaded to.

All Brocade systems maintain two partitions (a primary and a secondary) of 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 swaps the partitions so that the secondary partition becomes the primary. It then performs a non-disruptive HA reboot of the system. For directors, the standby is rebooted; this does not affect 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 up, it boots up 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.

If the firmware download process is interrupted by an unexpected reboot or power-cycle, the system automatically repairs and recovers the secondary partition. You must wait for the recovery to complete before entering **firmwaredownload** again.

> NOTE
> For more information on troubleshooting a firmware download, refer to the *Fabric OS Troubleshooting and Diagnostics Guide*.

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, which prompts you for input.

> ATTENTION
> 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. To verify the firmware download process is complete, enter the **firmwaredownloadstatus** command on the switch, verify the process is complete, and then move to the next switch.

Blades supported in Brocade X6 Directors

The following table lists the blades supported in Brocade X6 Directors when running Fabric OS 8.0.1.

TABLE 3 Blades supported by Fabric OS 8.0.1 in Brocade X6 Directors

Blade type	Description	Supported blades
Extension blades	These contain extra processors and both FC and IP ports for FCIP.	Brocade SX6 Extension blade
CP blades	These have a control processor used to control an entire Brocade X6 Director.	Brocade CPX6 Control Processor blade This blade type can only be inserted into slot 1 or slot 2.
CR blades	These core routing blades provides switching functionality among supported blades using backplane and Inter-Chassis Link (ICL) functionality. This enables connections between Brocade X6 Directors, or from a Brocade X6 Director to a Brocade DCX 8510 Director.	Brocade CR32-4 and CR32-8 Core Routing blades • A CR32-4 blade goes only into slots 5 or 6 on a Brocade X6-4 • A CR32-8 blade goes only into slots 7 or 8 on a Brocade X6-8
FC port blades	These are blades that contain only Fibre Channel ports.	Brocade FC32-48 FC blade

Blades supported in Brocade DCX 8510 Directors

The following table lists the blades supported in Brocade DCX 8510 Directors when running Fabric OS 8.0.1.

TABLE 4 Blades supported by Fabric OS 8.0.1 in Brocade DCX 8510 Directors

Blade type	Description	Supported blades
Extension blades	These contain extra processors and both FC and IP ports for FCIP.	Brocade FX8-24 Extension blade
CP blades	These blades have a control processor used to control an entire Brocade DCX 8510 Director.	Brocade CP8 Control Processor blade This blade type goes only into slots 4 or 5 in a Brocade DCX 8510-4, or slots 6 or 7 in a Brocade DCX 8510-8.
CR blades	These core routing blades provides switching functionality among supported blades using backplane and Inter-Chassis Link (ICL) functionality. This enables connections between Brocade DCX 8510 Directors, or between a Brocade DCX 8510 Director and a Brocade X6 Director.	CR16-4 and CR16-8 Core Routing blades • A CR16-4 blade goes only into slots 3 or 6 in a Brocade DCX 8510-4 Director. • A CR16-8 blade goes only into slots 5 or 8 in a Brocade DCX 8510-8 Director.
FC port blades	These are blades that contain only Fibre Channel ports.	• Brocade FC16-32 port blade • Brocade FC16-48 port blade • Brocade FC16-64 port blade

Unsupported blades

Fabric OS 8.0.1 does not support the following blades:

- FC8-32E
- FC8-48E
- FC8-64
- FS8-18
- FCOE10-24

These blades must be physically removed from any Brocade DCX 8510 chassis before upgrading it to Fabric OS 8.0.1. The firmware upgrade process will be blocked if any of these blades are present. If any these blades are installed after upgrading to Fabric OS 8.0.1, the slot that the blade is in will fault and the blade will not be available; all other blades will function normally.

Considerations for FICON CUP environments

To prevent channel errors during a nondisruptive firmware installation, the switch CUP port must be offline on all host systems.

Preparing for a firmware download

Download prerequisites

Before executing a firmware download, Brocade recommends that you perform the tasks listed in this section. In the unlikely event of a failure or timeout, these preparatory tasks enable you to provide your switch support provider the information required to troubleshoot the firmware download. Brocade recommends

Brocade recommends that you log the Telenet session to record the information shown in this process, as this information can be used to validate the correctness of the installation, and that you use the **configupload** command to back up the current configuration before you download firmware to a switch. Refer to the "Configuration file backup" section in the *Fabric OS Administrator's Guide* for details.

NOTE

Firmware downloading using Secure File Transfer Protocol (SFTP) is not supported on the multi-speed management port if it is set to 10 Mbps.

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

   NOTE

   Fabric OS does not support non-disruptive upgrades from any release more than one release earlier than the one being installed. This means that non-disruptive upgrading to Fabric OS 8.0.1 is supported from Fabric OS 7.4.x or later only. If you are trying to upgrade from any earlier version of Fabric OS, you will need to perform a disruptive upgrade.
2. 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 consoles (for both CPs on Directors) and any open network connection sessions such as Telnet sessions are being logged so that these can be included with any trouble reports.
3. Enter **firmwareshow** to verify the current version of Fabric OS.
4. Enter **firmwaredownloadstatus** to confirm that there is no firmware download already in progress. If there is, wait until that process is complete.
5. Confirm that all switches in the fabric are running a version of Fabric OS that is compatible with the version of Fabric OS you are planning on installing.

   NOTE

   All of the 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.

   a) Validate the existing fabric by running the following commands: **nsshow**, **nsallshow**, and **fabricshow**. This also will provide a record of the existing fabric which you can use to validate that the installation was correct and complete.

b) Enter **switchshow** to verify that no ports are running as G_Ports.

6. Back up the configuration file and retrieve all the 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 USB memory device).
   Refer to Special characters in FTP server credentials on page 21 for information on use of special characters.

   b) Enter **supportsave** to retrieve all current core files.
   This information will help in troubleshooting the firmware download process if a problem is encountered.

7. Optional: Enter **errclear** to erase all existing messages, including internal messages.
8. Enter **supportsave -R** (uppercase "R").
   This clears all core and trace files.
9. Continue with the firmware download.

Obtaining and decompressing firmware

Firmware upgrades are available for customers with support service contracts and for partners on the Brocade website at http://www.brocade.com.

Before you can use the **firmwaredownload** command to update the firmware, you must uncompress the firmware file. Use the UNIX **tar** command for .tar files, the **gunzip** command for .gz files, or a Windows unzip program for .zip files. When you unpack the downloaded firmware, it expands into a directory that is named according to the version of Fabric OS it contains. For example, when you download and unzip the file "8.0.1.zip", it expands into a directory named "8.0.1". When you issue the **firmwaredownload** command, there is an automatic search for the correct package file type associated with the switch. For this command to work correctly, you must specify the complete path up to and including the 8.0.1 directory name.

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

Firmware staging

Firmware that has been 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.

Brocade recommends that you perform any desired configuration changes before activating the new firmware. If the switch is rebooted or power-cycled, the downloaded firmware will not be affected as it is stored in the secondary partition. Any **firmwarerestore** or **firmwarecommit** processes will not start until the firmware is activated. The **firmwareactivate** command can be used in both single-CP and dual-CP environments. Refer to Activating firmware on page 22 for instructions on activating firmware.

Firmware download validation

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.

Passwordless firmware download

You can download firmware without a password using the **sshutil** command for public key authentication when SSH is selected. The switch must be configured to install the private key, and then you must export the public key to the remote host. Before running the

firmwareDownload command, you must first configure the SSH protocol to permit passwordless logins for outgoing authentication as described in the *Configuring outgoing SSH authentication* section in the *Fabric OS Administrator's Guide*.

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 and that any older OS versions are supported. Refer to the "Fabric OS Compatibility" section of the *Brocade Fabric OS Release Notes* for the recommended firmware version.

> ATTENTION
> Starting simultaneous firmware downloads on adjacent fixed-port switches may result in traffic disruption.

To determine if you need to upgrade switches that are connected to the switch you are upgrading, use the procedure described in Finding the switch firmware version on page 21 on each connected switch to display the firmware information and build dates.

Finding the switch firmware version

1. Connect to the switch and log in 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 version of the switch Fabric OS.
   - **Made on**: Displays the build date of the firmware running on the switch.
   - **Flash**: Displays the install date of firmware stored in nonvolatile memory.
   - **BootProm**: Displays the version of the firmware stored in the boot PROM.

Special characters in FTP server credentials

FTP server credentials may include special characters (also referred to as meta-characters), that are members of a special character set that are interpreted differently when used in command line mode. These characters have an alternate meaning, or are designated to carry out a special instruction. Here is a list of some of the more commonly-used special characters and their alternate meanings.

> NOTE
> This list is not exhaustive and alternate meanings for some characters is contextual. For detailed information on using special characters in FTP credentials, refer to Linux scripting information available on the internet.

- **&** is used to put a command in background/batch mode.
- **!** is used to recall the last invocation of the command matching the pattern that follows the character.
- **|** is used to direct (pipe) output to the command that follows the character.
- **;** is used to concatenate multiple commands.
- ***** is used to represent a wildcard character.
- **?** is used as a match for any single character in the specified position.
- **()** is used for integer expansion.

- **<** and **>** are used for redirection. **<** represents input and **>** represents output.
- **$** is used to represent shell variable.
- **`** is used for command substitution or assign output of a command to a variable.
- **"** is used for partial quoting.
- **'** is used for full quoting.
- Spaces are used as a separation character.
- **#** when preceded by a space, treats all characters through the end of the line as a comment rather than commands.

These special characters may be used to enhance user credential security. However, in order for these characters to be properly interpreted, you must use one of the following methods:

- Escape each instance of the special character by preceding it with the escape character (****).
- Enclose the credentials containing special characters within single quotes (**'**).

  If single quotes are themselves part of the credential, precede each instance of the single quote with the escape character (****). Alternately, the string may be enclosed in double quotes (**"**) if a more intricate bash substitution is desired to further strengthen the security measure of the credentials.

You can test the representation of the credentials by logging in with root-level permissions and using the **echo** command.

Activating firmware

After the firmware is downloaded to a switch or Director, the update is incomplete until the new firmware is activated.

1. Download the firmware to the secondary partition of the platform using either **firmwaredownload –r**, or **firmwaredownload –lr**.
2. Enter **firmwareshow** to view the current firmware version on each partition.

```
switch:admin> firmwareshow
Appl     Primary/Secondary Versions
----------------------------------
FOS      v8.0.1v00
         v8.0.1v00
```

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 to be restarted.

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

Firmware download scenarios

General firmware download considerations

NOTE

This section only applies when upgrading from Fabric OS 7.4.x to 8.0.1 or downgrading from Fabric OS 8.0.1 to 7.4.x. If you are attempting to upgrade from Fabric OS 7.2.x to 8.0.1 or downgrading from Fabric OS 8.0.1 to 7.2.x, you must enter the **firmwaredownload -s** command as described in Testing and restoring firmware on switches on page 33.

The following items apply to all firmware downloads, whether for Directors or for fixed-port switches.

- You cannot upgrade any Brocade Gen 5 or earlier device to Fabric OS 8.0.0, only to Fabric OS 8.0.1 and later.
- You cannot downgrade any Brocade Gen 6 or later device other than the Brocade G620 to any version of Fabric OS earlier than Fabric OS 8.0.1.
- Fabric OS 8.0.0 can only be installed on the Brocade G620 switch.
- You cannot download firmware to migrate from Fabric OS 8.0.1 to 7.2.x (or earlier) or from Fabric OS 7.2.x (or earlier) to 8.0.1.
- All Brocade Directors and fixed-port switches maintain primary and secondary partitions for firmware.
- By default the **firmwaredownload** command automatically copies the firmware from one partition to the other. Under normal circumstances you should use the default settings and not override this option. By default, **firmwaredownload** performs a full install, along with an automatic reboot and automatic commit. These alternate modes are only selectable when the platform is in single control processor (**-s**) mode, in which case autoreboot is OFF by default.

Overriding the autocommit option in downloads

ATTENTION

This option should only be used by experienced administrators for specific situations (such as evaluating a new version of the firmware).

The **firmwarerestore** command can only run if autocommit was disabled during the initial firmware download. To download firmware with the autocommit option disabled, enter **firmwaredownload** and use the **-s** and **-n** options. Refer to the *Fabric OS Command Reference* for a complete description of the **firmwaredownload** and available options.

Firmware download considerations for fixed-port switches

The following paragraph is specific to firmware downloads for Brocade 7840 fixed-port switches.

A VE_Port on a Brocade 7840 that does not have HA configured can go down due to external events during hot code load. In such scenario, traffic will be disrupted on that particular VE port. After the hot code load completes, it may be possible that the VE_Port will come up as a G_Port, and consequently, traffic will not resume. In such scenario, you will need to perform an explicit **portdisable** and **portenable** command combination on that VE_Port to recover it.

Switch firmware download process overview

When you run the **firmwaredownload** command without options on Brocade fixed-port switches, the following behaviors occur:

1. The firmware is downloaded to the secondary partition.
2. The system performs a High Availability reboot (**hareboot**). After the **hareboot**, the former secondary partition is the primary partition.
3. The system replicates the firmware from the primary to the secondary partition.

While the upgrade is proceeding, you can start a session on the switch and use the **firmwaredownloadstatus** command to observe the upgrade progress.

CAUTION

After you start the process, do not enter any disruptive commands (such as reboot) that will interrupt the process. Any external disruption to the switch during the switch's internal reboot interval will result in a "cold reboot" which is likely to be disruptive to any traffic on the switch. The entire firmware download and commit process can take up to 20 minutes, and any existing Telnet sessions will be dropped during the normal internal reboot. If there is a problem, wait for the timeout (30 minutes for network problems) before issuing firmwaredownload again. Disrupting the process can render the switch inoperable and require you to seek help from your switch service provider. Do not disconnect the switch from power during the process, as the switch could be inoperable when it reboots.

Upgrading firmware on fixed-port switches

Before you start, refer to Connected switches on page 21 and confirm that all connected switches in the fabric are running a supported version of Fabric OS before starting any upgrading. 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. Take the following appropriate action based on what service you are using:
   - If you are using FTP, SFTP, or SCP, 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 are using a USB memory device, verify that it is connected and running.
     1. Visually confirm that the device is connected.
     2. Enter **usbstorage -e** to mount the USB device.
     3. Enter **usbstorage -l** to verify that it is running.
2. Obtain the firmware file for the version of Fabric OS you want to load onto the switch from the Brocade website at http://www.brocade.com. You can store the file on your FTP or SSH server or under the “firmware” directory on a pre-formatted Brocade USB storage device.
3. Unpack the compressed files, preserving the directory structures.

   Refer to Obtaining and decompressing firmware on page 20 for details on this process for your environment.
4. Connect to the switch you want to upgrade, and log in using an account with admin permissions.
5. Enter **firmwaredownload** and respond to the prompts.

   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 enter at least one DNS server using the **dnsconfig** command.

6. Enter **y** at the `Do you want to continue [y/n]` prompt.
7. After the High Availability (HA) reboot, reconnect to the switch and log in again using an account with admin permissions.
8. Enter **firmwaredownloadstatus** to determine if the firmware download process has completed.
9. After the firmware commit is completed, which takes several minutes, enter the **firmwareshow** command to verify the firmware level of both partitions is the same.

The following example illustrates the initial portion of an interactive firmware download. After this portion is complete, you will see a scrolling list of the firmware elements being installed.

```
switch:admin> firmwaredownload
Server Name or IP Address: 10.7.7.7
User Name: admin
File Name: /home/SAN/fos/8.0.1/8.0.1
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:
Server IP: 10.7.7.7, Protocol IPv4
Checking system settings for firmwaredownload...
```

Firmware download considerations for Directors

The following items are specific to firmware downloads for Brocade Directors.

> ATTENTION
> To successfully download firmware, you must have an active Ethernet connection for each control processor (CP) in the chassis.

You can download firmware to a Director without disrupting the overall fabric if both CP blades are installed and fully synchronized. To determine if they are synchronized, enter **hashow** before initiating the firmware download process. If the CP blades are synchronized, the command will produce a response similar to the following:

```
Local CP (Slot 7, CP1) : Active, Warm Recovered
Remote CP (Slot 6, CP0) : Standby, Healthy
HA Enabled, Heartbeat Up, HA State Synchronized
```

The last line indicates that the blades are synchronized. In addition, the slot numbers shown for the CPs are determined the Director type, so those for your Director may not match the example.

> NOTE
> If only one CP blade is inserted, powered on or plugged into the network, you can run **firmwaredownload -s** to upgrade the CP. **This will disrupt the network traffic.**

If there are two CPs, but they are not in sync, run **hasyncstart**, and then enter **hashow** to view their status. If the CPs are still not in sync after this, refer to the *Fabric OS Troubleshooting and Diagnostics Guide*. If the troubleshooting information fails to help resolve the issue, contact your switch service provider.

Alternatively, you can run the **firmwaredownload** command separately on each CP to upgrade it, and manually switch the CPs between active and standby. These operations are disruptive when run on the primary CP first, but are not disruptive if you run it on the standby CP first.

In most cases, after the standby CP comes up, it will resynchronize with the active CP. At that point, a manual failover can be executed on the active CP non-disruptively and then **firmwaredownload -s** can be performed on the new standby CP. This is actually a common operation carried out by many field personnel to upgrade firmware.

NOTE
During the default firmware download process (using **firmwaredownload** without the **-s** option), the chassis fails over to its standby CP blade and the IP address for the device transfers to that CP blade's Ethernet port. This may cause informational ARP address reassignment messages to appear on other switches in the fabric. This is normal behavior, because the association between the IP addresses and MAC addresses has changed.

Firmware download process for Directors

The following summary describes the default behavior of the **firmwaredownload** command (without options) on a Director. After you enter **firmwaredownload** on the active control processor (CP) blade, the following actions occur:

1. The standby CP blade downloads the firmware.
2. The standby CP blade reboots and comes up with the new Fabric OS version.
3. The active CP blade synchronizes its state with the standby CP blade.
4. The active CP blade forces a failover and reboots to become the standby CP blade.
5. The new active CP blade synchronizes its state with the new standby CP blade.
6. The new standby CP blade (the active CP blade before the failover) downloads firmware.
7. The new standby CP blade reboots and comes up with the new Fabric OS version.
8. The new active CP blade synchronizes its state with the new standby CP blade.
9. The **firmwarecommit** command runs automatically on both CP blades.

The entire firmware download and commit process takes approximately 17 minutes. If there is a problem, wait for the timeout (30 minutes for network problems) before entering the **firmwaredownload** command again.

CAUTION
After you start the process, do not enter any disruptive commands (such as reboot) that interrupt the process. Disrupting the process can render the switch inoperable and require you to seek help from your switch service provider. Do not disconnect the switch from power during the process, as doing so could render the switch inoperable when it reboots.

Upgrading firmware on Directors (including blades)

Before you start, refer to Connected switches on page 21 and confirm that all connected switches in the fabric are running a supported version of Fabric OS before starting any upgrading. 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.

NOTE
If there are any unsupported blades in a Brocade DCX 8510-4 or Brocade DCX 8510-8 Director, the download will be blocked. Refer to Unsupported blades on page 16 for a list of blades that are not supported on these devices when running Fabric OS 8.0.1.

1. Verify that the Ethernet interfaces located on CP0 and CP1 are plugged into your network.
2. Verify that the FTP, SFTP, or SSH server is running on the host server and that you have full accessibility (a valid user id, password, and permissions) on that server.
3. Obtain the firmware file for the version of Fabric OS you want to load onto the Director from the Brocade website at http://www.brocade.com and store the file on the FTP or SSH server.
4. Unpack the compressed files, preserving the directory structures.

Refer to Obtaining and decompressing firmware on page 20 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.

5. Connect to the chassis IP management interface or active control processor (CP) and log in using an account with admin permissions.

   NOTE
   A Brocade Director has only one chassis management IP address.

6. 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 5, CP0): Active, Warm Recovered
   Remote CP (Slot 6, CP1): Standby, Healthy
   HA enabled, Heartbeat Up, HA State synchronized
   ```

   The two CP blades must be synchronized and running Fabric OS 7.4.0 or later to provide a nondisruptive download. If the CP blades are not synchronized, enter the **hasyncstart** command to synchronize them. If the CPs still are not synchronized, contact your switch service provider.

   For further troubleshooting, refer to the *Fabric OS Troubleshooting and Diagnostics Guide*.

7. Enter the **firmwaredownload** command and respond to the interactive prompts.
8. At the `Do you want to continue [y/n]` prompt, enter **y**.

   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 DCX 8510 Directors, if an FX8-24 blade is present: At the point of the failover, an *autoleveling* process is activated. Autoleveling is triggered when the active CP detects a blade that contains a different version of the firmware, regardless of which version is older. Autoleveling downloads firmware to the blade's internal BP processor, swaps partitions, reboots the blade, and copies the new firmware from the primary partition to the secondary partition. If you have multiple FX8-24 blades, they will be updated simultaneously; however, the downloads may occur at different rates.

   Autoleveling takes place in parallel with the firmware download being performed on the CPs, but does not impact performance. Fibre Channel traffic is not disrupted during autoleveling, but Gigabit Ethernet (GbE) traffic on AP blades may be affected. If there is an active FCIP tunnel on the FX8-24 blade, the FCIP tunnel traffic will be impacted for at least two minutes.

   ```
   switch:admin> firmwaredownload
   Server Name or IP Address: 10.1.2.3
   User Name: userfoo
   File Name: /home/userfoo/8.0.1
   Network Protocol (1-auto-select, 2-FTP, 3-SCP, 4-SFTP)) [1]:
   Password: <hidden>
   Checking version compatibility...
   Version compatibility check passed.
   The following AP blades are installed in the system.
   Slot Name      Versions                      Traffic Disrupted
   ------------------------------------------------------------------
   8    FX8-24    8.0.1                         GigE

   This command will upgrade the firmware on both CPs and all AP blade(s) above.
   If you want to upgrade firmware on a single CP only, please use -s option.
   You may run firmwaredownloadstatus to get the status of this command.
   This command will cause a warm/non-disruptive boot on the active CP,
   but will require that existing telnet, secure telnet or SSH sessions be restarted.
   Do you want to continue [Y]: y
   . . .
   The firmware is being downloaded to the Standby CP. It may take up to 10 minutes.
   ```

If an X6 Director has a combination of tunnels with and without HA configurations, the message shown in the following example appears during a non-disruptive firmware download:

```
X6-225:admin> firmwaredownload 10.7.7.7,,/downloads/fos/8.0.1/release.plist
. . .

Checking FCIP Tunnel HA Status.
Tunnel 12/19 (FID:7) HA configure but HA Offline. Traffic will be disrupted.
Tunnel 12/30 (FID:128) Not HA configured. Traffic will be disrupted.

System settings check passed.

This command will upgrade the firmware on both CP blades. If you want to
upgrade firmware on a single CP only, please use -s option.

You may run firmwaredownloadstatus to get the status of this command.

This command will cause a warm/non-disruptive boot on the active CP, but will require that existing
telnet, secure telnet or SSH sessions be restarted.

. . .
```

NOTE

If all the tunnels are configured for high availability, no warning regarding traffic disruption is displayed.

9. After the failover, connect to the switch, and log in again as admin.
10. Using a separate session to connect to the switch, enter **firmwaredownloadstatus** to monitor the firmware download status.

```
switch:admin> firmwaredownloadstatus
[1]: Mon Mar 22 04:27:21 2016
Slot 7 (CP1, active): Firmware is being downloaded to the switch. This step may take up to 30
minutes.
[2]: Mon Mar 22 04:34:58 2016
Slot 7 (CP1, active): Relocating an internal firmware image on the CP blade.
[3]: Mon Mar 22 04:35:29 2016
Slot 7 (CP1, active): The internal firmware image is relocated successfully.
[4]: Mon Mar 22 04:35:30 2016
Slot 7 (CP1, active): Firmware has been downloaded to the secondary partition of the switch.
[5]: Mon Mar 22 04:37:24 2016
Slot 7 (CP1, standby): The firmware commit operation has started. This may take up to 10 minutes.
[6]: Mon Mar 22 04:41:59 2016
Slot 7 (CP1, standby): The commit operation has completed successfully.
[7]: Mon Mar 22 04:41:59 2016
Slot 7 (CP1, standby): Firmwaredownload command has completed successfully. Use firmwareshow to
verify the firmware versions.
```

11. Enter **firmwareshow** to display the installed firmware version, so you can confirm that it has been correctly installed.

Firmware download from a USB device

The following Brocade devices support firmware downloading from a Brocade-branded USB device attached to the switch or active CP. Suitably preformatted USB sticks are available from Brocade technical support.

- Brocade 6505 switch
- Brocade 6510 switch
- Brocade 6520 switch
- Brocade 7840 switch
- Brocade DCX 8510-4 and Brocade DCX 8510-8 Directors
- Brocade G620 switch

- Brocade X6-4 and Brocade X6-8 Directors

If you are using Windows, open a file browser and navigate to the `brocade/firmware` directory on the USB device. You can then drag the unzipped firmware image files from where you downloaded them to this directory. Multiple images can be stored under this directory.

If you are using Linux, the USB device must be enabled and mounted as a file system. Once you have done this, copy the unzipped firmware images to be downloaded to `/usb/usbstorage/brocade/firmware`. Alternatively, you can use the absolute path in the USB file system to the same directory.

When you enter **firmwaredownload** with the **-U** (uppercase 'U') option, the **firmwaredownload** command downloads the specified firmware image from the USB device. When specifying a path to a firmware image in the USB device, you can only specify the relative path to `/firmware` or the absolute path.

NOTE
Before removing the USB device from the switch or Director, you must unmount the USB device using either the "eject" command in Windows or **usbstorage -d** in Linux.

Enabling the USB device

1. Log in to the switch using an account assigned to the admin role.
2. Enter the **usbStorage -e** command.

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
firmware\               381MB    2016 April 22 15:33
  8.0.1\                381MB    2016 April 22 10:39
config\                   0B     2016 April 22 15:33
support\                  0B     2016 April 22 15:33
firmwarekey\              0B     2016 April 22 15:33
Available space on usbstorage 69%
```

Downloading from the USB device using the relative path

This is the preferred method.

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, that directory is '8.0.1'.

```
switch:admin> firmwaredownload -U 8.0.1
```

Downloading from the USB device using the absolute path

1. Connect to the device and log in using an account with admin permissions.

2. Enter **firmwaredownload -U** followed by the full path of the firmware directory. In the following example, that path is '/usb/usbstorage/brocade/firmware/8.0.1'.

```
switch:admin> firmwaredownload -U /usb/usbstorage/brocade/firmware/8.0.1
```

Validating a firmware installation

You can validate the firmware installation on a switch or Director by running the following commands: **firmwareshow** and **firmwaredownloadstatus**.

NOTE
There is no way to perform a checksum validation on a direct firmware installation; the files are directly transferred and installed from the Brocade file servers.

TABLE 5 Commands used for validating a firmware download

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. Brocade recommends that you 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 time stamp is associated with each event. When downloading to devices with two control processors, you can only run this command on the active CP. When downloadingFabric OS, the event logs in the two CPs are synchronized. This command can be run from either CP.

Confirming that the switch and fabric are working properly together

Use the following commands to ensure that the fabric and connections to the attached devices have been restored correctly: **nsshow**, **nsallshow**, and **fabricshow**. Also, you can verify that no ports are coming up as G_Ports by using the **switchshow** command.

NOTE
All of the 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. Make sure the number of attached devices after the firmware download is exactly the same as the number of attached devices prior to the firmware download.
nsallshow	Displays all devices connected to a fabric. Make sure the number of attached devices after the firmware download is exactly the same as the number of attached devices prior to the firmware download.
fabricshow	Displays all switches in a fabric. Make sure the number of switches in the fabric after the firmware download is exactly the same as the number of attached devices prior to the firmware download.

Testing firmware

Testing and restoring firmware on switches

Typically, you restore (downgrade) a switch back 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, as 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. Verify that the FTP, SFTP, or SSH server is running on the host server and that you have full accessibility (a valid user id, password, and permissions) on that server.
2. Obtain the firmware file from the Brocade website (http://www.brocade.com) or your switch support provider and store the file on your FTP or SSH server.
3. Unpack the compressed files, preserving the directory structures.

   Refer to Obtaining and decompressing firmware on page 20 for details on this process for your environment.
4. Connect to the switch and log in using an account with admin permissions.
5. Enter **firmwareshow** to view the current firmware.
6. Enter **firmwaredownload -s**, and respond to the prompts.

   The following is an example of a firmware download to a single partition using this command.

   NOTE
   If the firmware level change is only one level up or down, the system will attempt a non-disruptive HA reboot. If it is a two-level change, the reboot will be disruptive, and traffic on that switch and possibly the fabric it is part of may be affected. This is by design.

```
switch:admin> firmwaredownload -s
Server Name or IP Address: 10.1.2.3
Network Protocol (1-auto-select, 2-FTP, 3-SCP, 4-SFTP) [1]:
User Name: userfoo
File Name: /home/userfoo/8.0.1
Password: <hidden>
Do Auto-Commit after Reboot [Y]: n
Reboot system after download [N]: y
Firmware is being downloaded to the switch. This step may take up to 30 minutes.
Checking system settings for firmwaredownload...
```

   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.
7. Reconnect to the switch and log in using an account with admin permissions.

   You are now ready to evaluate the new version of the firmware.

8. Enter **firmwaredownloadstatus** to view the status of the firmware download.
9. Enter **firmwareshow** to confirm that the primary partition of the switch contains the new firmware.

   You can now evaluate the new firmware.

   Once you have completed your evaluation of the firmware, you can either commit the firmware (install it fully) or revert to the previously-installed version.

   - If you want to commit the firmware (fully install it), complete the following steps.

   a) Enter **firmwarecommit** to update the secondary partition with new firmware. It will take several minutes to complete the commit operation.

   b) Enter **firmwaredownloadstatus** to view the status of the firmware download.

   c) Enter **firmwareshow** to confirm both partitions on the switch contain the new firmware.

      ATTENTION
      If you have completed this step, you have committed the firmware to the switch and have completed the firmware download procedure.

   - If you want to revert to the previously-installed firmware, complete the following steps.

   a) Enter **firmwarerestore** to reboot the switch and restore the original firmware.

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

   b) Wait at least five minutes after to ensure that all processes have completed and the switch is fully up and operational.

   c) Reconnect to the switch and log in using an account with admin permissions.

   d) Enter **firmwareshow** and verify that both partitions on the switch have the original firmware.

Testing and restoring firmware on Directors

This procedure enables you to perform a firmware download on each control processor (CP) and 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 prior to the firmware commit, you can enter **firmwarerestore** to restore the former active Fabric OS firmware image.

ATTENTION
The **firmwarerestore** command can only run if autocommit was disabled during the firmware download.

NOTE
Brocade recommends that under normal operating conditions you maintain the same firmware version on both CPs, and on 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 it 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, but then it automatically triggers a failover to the standby CP since effectively you have rebooted the active CP with the **firmwarerestore** command.

1. Connect to the IP address for the Director.
2. Enter **ipaddrshow** and note the addresses for CP0 and CP1.
3. Enter **hashow** and note which CP is the active one, and which CP is the standby one.
4. Confirm that both CPs are in sync.

   If the CPs are not in sync, refer to Firmware download process for Directors on page 26 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 -sfn** and respond to the prompts.

      At this point, the firmware downloads to the standby CP only. When it has completed the download to that CP, reboot it. The current session is disconnected.
8. Failover 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 FX8-24 blade is installed (Brocade DCX 8510 only): At the point of the failover, an *autoleveling* process is activated to match the firmware on the blade with that on the CP. Blade partitions must always contain the same version of the firmware on both partitions. The firmware is stored on the blade's compact flash card and is always synchronized with the active CP's firmware. 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 will cause the current login session to be disconnected.

c) Wait one minute for the standby CP to reboot, and then connect to the Director and log in as admin.

d) Enter **firmwareshow** and confirm that *both* primary partitions have the test drive firmware in place.

You are now ready to evaluate the new firmware version.

ATTENTION
Stop! If you want to *restore* the firmware, stop here and skip ahead to step 13; otherwise, continue to step 11 to commit the firmware on both CPs, which 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 will take 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) When the **firmwarecommit** command completes, enter **firmwareshow** and confirm both partitions on both CPs contain the new firmware.

d) Enter **hashow** and confirm that the HA state is in sync.

ATTENTION
Stop! If you have completed step 11, then you have committed the firmware on both CPs and you have completed the firmware download procedure.

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 firmware on the "new" standby CP.

a) Wait one minute and 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 five minutes and log 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 the servers using the fabric can access their storage devices. Refer to Validating a firmware installation on page 31 for information on this task.

If an FX8-24 blade is installed (Brocade DCX 8510 only): Blade partitions must always contain the same version of the firmware on both partitions. The firmware is stored on the blade's compact flash card and is always synchronized with the active CP's firmware. Thus, if you restore the active CP firmware, the blade firmware is automatically downloaded (autoleveled) to become consistent with the new 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 switches on page 33. 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 example shows how you might install a firmware version to "test drive" it without either overwriting the version you are currently using or rebooting your active CP. It is written at a moderately high level of abstraction, so you may need to look at the more detailed steps above 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" firmware active.
4. Run tests as desired on the new firmware (active CP).
5. Once you have completed your testing, you have two choices:
   - **Option 1:** "My tests are finished on the new firmware, but I want to go back to what I had before."
     1. Enter **hafailover** on the active CP to get back to the original CP (running the original firmware).
     2. Enter **firmwarerestore** on the standby CP.

        This will reboot the standby, swap the partitions and then run commit on the standby CP.
   - **Option 2:** "My tests are finished on the new firmware, and I want to install it fully."
     1. Enter **firmwaredownload -sb** on the current standby CP (with old code)

        This loads new firmware, reboots and then commits the firmware on standby.
     2. Enter **firmwarecommit** on the current active CP (with new code).

        You are now done and both CPs have latest firmware committed and active.

   Both options are non-disruptive to Director traffic.