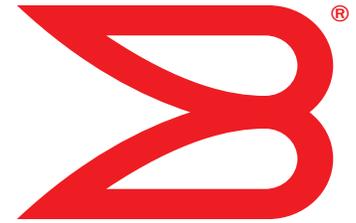


53-1000114-05
13 February 2012



Fabric OS

Password Recovery Notes

Supporting Fabric OS v6.x, v5.x, v4.x, v3.x, v2.6.x

BROCADE

Copyright © 2012 Brocade Communications Systems, Inc. All Rights Reserved.

Brocade, the B-wing symbol, BigIron, DCX, Fabric OS, FastIron, NetIron, SAN Health, ServerIron, and Turbolron are registered trademarks, and Brocade Assurance, Brocade NET Health, Brocade One, CloudPlex, MLX, VCS, VDX, and When the Mission Is Critical, the Network Is Brocade are trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. Other brands, products, or service names mentioned are or may be trademarks or service marks of their respective owners.

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

The authors and Brocade Communications Systems, Inc. shall have no liability or responsibility to any person or entity with respect to any loss, cost, liability, or damages arising from the information contained in this book or the computer programs that accompany it.

The product described by this document may contain "open source" software covered by the GNU General Public License or other open source license agreements. To find out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit <http://www.brocade.com/support/oscd>.

Brocade Communications Systems, Incorporated

Corporate and Latin American Headquarters
Brocade Communications Systems, Inc.
130 Holger Way
San Jose, CA 95134
Tel: 1-408-333-8000
Fax: 1-408-333-8101
E-mail: info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems China HK, Ltd.
No. 1 Guanghua Road
Chao Yang District
Units 2718 and 2818
Beijing 100020, China
Tel: +8610 6588 8888
Fax: +8610 6588 9999
E-mail: china-info@brocade.com

European Headquarters
Brocade Communications Switzerland Sàrl
Centre Swissair
Tour B - 4ème étage
29, Route de l'Aéroport
Case Postale 105
CH-1215 Genève 15
Switzerland
Tel: +41 22 799 5640
Fax: +41 22 799 5641
E-mail: emea-info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems Co., Ltd. (Shenzhen WFOE)
Citic Plaza
No. 233 Tian He Road North
Unit 1308 - 13th Floor
Guangzhou, China
Tel: +8620 3891 2000
Fax: +8620 3891 2111
E-mail: china-info@brocade.com

Document History

Title	Publication number	Summary of changes	Date
<i>Fabric OS Password Recovery Notes</i>	53-1000114-01	New document	March 2006
<i>Fabric OS Password Recovery Notes</i>	53-1000114-02	Updated for next release	December 2008
<i>Fabric OS Password Recovery Notes</i>	53-1000114-03	Corrected and restructured	November 2010
<i>Fabric OS Password Recovery Notes</i>	53-1000114-04	Caution added	December 2010
<i>Fabric OS Password Recovery Notes</i>	53-1000114-05	Defect fixed	February 2012

Fabric OS Password Recovery Notes

In this chapter

- [Password recovery overview](#) 1
- [Password recovery using root account](#) 2
- [Password recovery using the Boot PROM interface](#) 3
- [Obtaining the boot PROM recovery password](#) 17
- [Password recovery using Password Recovery firmware](#) 18

Password recovery overview

Several methods exist for recovering passwords on a Brocade Fabric OS switch or director. The correct approach depends on the version of Fabric OS you are using, which passwords you have, and on the hardware platform you are using.

[Table 1](#) lists the procedures described in this document and the conditions under which you would use each procedure to recover passwords. These conditions are a combination of Fabric OS version and account access availability.

TABLE 1 Password recovery procedures and when to use them

Condition (Fabric OS version and account access availability)	Use these procedures
<ul style="list-style-type: none"> • Access to root account on any supported version of Fabric OS 	“Password recovery using root account” on page 2
<ul style="list-style-type: none"> • Fabric OS v4.1x, 4.2x, 4.4x, 4.x, 5.x, or 6.x • no root account access • Boot PROM interface access 	“Password recovery using the Boot PROM interface” on page 3
<ul style="list-style-type: none"> • Fabric OS v4.1x, 4.2x, 4.4x, 4.x, 5.x, or 6.x • no root account access • no Boot PROM interface access 	“Obtaining the boot PROM recovery password” on page 17, and then “Password recovery using the Boot PROM interface” on page 3
<ul style="list-style-type: none"> • Fabric OS v2.6.x or 3.x • no root account access 	“Password recovery using Password Recovery firmware” on page 18

NOTE

You cannot perform password recovery procedures on FIPS-enabled switches because these procedures require access to a serial port. The serial port is disabled on FIPS-enabled switches.

NOTE

When connected through a serial cable to the console, always save the output using the capture functionality under Windows, or script functionality for UNIX or Linux.

1 Password recovery using root account

Password recovery on Fabric OS v4.x, v5.x, and v6.x

If you have access to the root account you can reset the passwords for all other accounts on the system including the factory, admin, and user accounts. The root account can reset the root, factory, and admin accounts. Admin can reset the user login. See [“Password recovery using root account”](#) on page 2.

If you do not have access to the root account, you can use the boot PROM method. This option is only available on Fabric OS v4.1 or later. See [“Password recovery using the Boot PROM interface”](#) on page 3. If the password is set on the boot PROM and is unknown, contact your switch service provider for a Boot PROM recovery string to regain access to the switch. See [“Obtaining the boot PROM recovery password”](#) on page 17.

Password recovery on Fabric OS v2.6.x and v3.x

If you have access to the root account you can reset the passwords for all other accounts on the system including the factory, admin, and user accounts. The root account can reset the root, factory, and admin accounts. Admin can reset the user login. See [“Password recovery using root account”](#) on page 2.

If you do not have access to the root account, you can use Password Recovery firmware, available from your switch support provider. See [“Password recovery using Password Recovery firmware”](#) on page 18.

Password recovery using root account

If you have access to the root account, you can reset the passwords on the switch to default. This feature is available for all currently supported versions of the Fabric OS.

To reset any account password from the root account, follow these steps:

1. Open a CLI session (serial or telnet for an unsecured system and sectelnet for a secure system) to the switch.
2. Log in as root.
3. At the prompt, enter the **passwddefault** command as shown below:

```
switch:root> passwddefault
```

4. Follow the prompts to reset the password for the selected account. For example:

```
switch:root> passwddefault
All account passwords have been successfully set to factory default.
```

Once the passwords have been reset, log into the switch as admin, and change your default passwords. Make sure to keep a hardcopy of your switch passwords in a secure location. [Table 2](#) lists the default passwords for Fabric OS switches.

TABLE 2 Default Passwords

Account	Default password
factory	shuntang (older switches) password (newer switches)
root	fibranne

TABLE 2 Default Passwords (Continued)

Account	Default password
admin	password
user	password

Password recovery using the Boot PROM interface



CAUTION

Enter commands at the boot PROM interface exactly as shown. Incorrectly entered commands at the boot PROM interface can render your switch unstable or unusable. To recover, you would need to seek help from your switch service provider or return your switch to the factory for repair.

You can use this procedure if you need to recover passwords on a device running Fabric OS v4.1.x, 4.2.x, 4.4.x, 5.x, or 6.x and the root account is not accessible. If the root account is accessible, use [“Password recovery using root account”](#) on page 2, instead.

To use this procedure, you must have access to the Boot PROM interface; that is, its password must be available or not set. If you do not have access to the Boot PROM interface, use [“Obtaining the boot PROM recovery password”](#) on page 17 before using this procedure.

If you are attempting to recover passwords for Fabric OS v4.4.0, you must review [“Password recovery for Fabric OS v4.4.0”](#) on page 16 before beginning this procedure.

The specific steps required to recover passwords using the Boot PROM interface depend on several factors, including:

- The Boot ROM environment—Two Boot ROM environments exist, the original “440” processor types and the newer Freescale processor type, which uses U-Boot.
- Location of the Linux kernel—On earlier products, the Linux kernel was maintained on separate hardware chips. For these products, these procedures make references to MEM()0xF0000000. Later products place the kernel on the compact flash. For these products, these procedures make references to ATA()0xb689f type structures.
- Whether the platform has a single CP, or has active and standby CPs—This procedure is disruptive to traffic on the 3250, 3850, 3900, 4100, 200E, 4900, 5000, 7500, 7600, 300, 5100, and 5300 switches and Brocade Encryption Switches, because it requires you to reboot the switch; traffic resumes after the switch is rebooted. On a Brocade 12000, 24000, 48000 director, DCX, or DCX-4S platforms you can reset the passwords without disruption by performing this procedure on the standby CP.

To reset the passwords on the active CP from the standby CP, extra steps are necessary to communicate with the active CP.

- Throughput of the switch or director—8 Gbps devices, including the Brocade 300, 5100, 5300, DCX, and DCX-4S devices, requires the creation of a temporary boot environment variable.

1 Password recovery using the Boot PROM interface

Table 3 lists the types of combinations. Each combination has a separate password recovery procedure, described later in this section.

TABLE 3 Factor combinations and associated Brocade devices

Factor combinations	Associated Brocade Fabric OS devices
<ul style="list-style-type: none">• ATA()0xa64g• U-Boot ROM• active and standby CPs• 8 Gbps platform	Brocade DCX and DCX-4S
<ul style="list-style-type: none">• ATA()0xa64g• U-Boot ROM• single CP• 8 Gbps platform	Brocade 300, 5100, 5300
<ul style="list-style-type: none">• ATA()0xa64g• original Boot ROM• single CP	Brocade 200E, 4900, 5000, 7500, 7600
<ul style="list-style-type: none">• MEM()0xF0000000• original Boot ROM• active and backup CPs	Brocade 12000, 24000, 48000
<ul style="list-style-type: none">• MEM()0xF0000000• original Boot ROM• single CP	Brocade 3250, 3850, 3900, 4100

This section provides detailed procedures for performing password recovery on each group of related devices as well as a quick reference for advanced users who need only a reminder of the basic steps:

- [“Password recovery procedure: quick reference”](#) on page 4
- [“Password recovery procedure for Brocade DCX and DCX-4S”](#) on page 5
- [“Password recovery procedure for Brocade 300, 5100, 5300 switches and the Brocade Encryption Switch”](#) on page 8
- [“Password recovery procedure for Brocade 200E, 4900, 5000, 7500, and 7600 switches”](#) on page 10
- [“Password recovery procedure for Brocade 12000, 24000, and 48000 switches”](#) on page 11
- [“Password recovery procedure for Brocade 3250, 3850, 3900, and 4100 switches”](#) on page 14

Password recovery procedure: quick reference

Advanced users who need only a reminder of the basic steps can use this quick reference to recover passwords:

1. Press ESC during reboot.
2. Choose option **3**.
3. **printenv**
4. For 8 Gbps platforms only:
`setenv OSLoadOptions "single"`

5. For 8 Gbps platforms only:

```
boot
```

For Non-8 Gbps platforms:

```
boot ATA()0x77588 -s
```

Where the argument to the boot command is the first parameter shown for OSLoader in the **printEnv** output.

6. `mount -o remount,rw,noatime /`

7. `mount /dev/hda1 /mnt`

For step 7, choose the 2nd parameter shown for OSRootPartition.

8. `/etc/init.d/network start`

Step 8 required only for devices with active and standby CPs.

9. `/sbin/passwddefault`

10. `bootenv OSLoadOptions "quiet;quiet"`

11. `reboot -f`

Password recovery procedure for Brocade DCX and DCX-4S

1. Connect to the standby CP of the Brocade DCX or DCX-4S backbone.

To determine which CP is standby, use one of the following methods:

- If you have the appropriate passwords, use the **haShow** command.

NOTE

You cannot use the **haShow** command if you have lost all passwords.

- Use the active LED to identify the active and standby CPs.

2. Reboot the standby CP using either the **fastBoot** command or the **reboot** command. Enter:

```
> fastboot
```

Or:

```
> /sbin/reboot
```

3. When prompted to stop test or stop AutoBoot, press ESC.

The Boot PROM menu is displayed with the following options:

- Start system
Used to reboot the system.
- Recover password.
Used to generate a character string for your support provider to recover the Boot PROM password. Use this feature only when directed by technical support personnel.
- Enter command shell.
Used to enter the command shell, to reset all passwords on the system.

```
Checking system RAM - press any key to stop test
```

1 Password recovery using the Boot PROM interface

```
Checking memory address: 00100000
System RAM test terminated by keyboard
set_bootstatus: BS_LOAD_OS, platform_idx = 6
Hit ESC to stop autoboot: 0
1) Start system.
2) Recover password.
3) Enter command shell.
```

Option?

4. Enter **3** at the prompt to open the command shell.

Option? **3**

5. Type the Boot PROM password, if prompted, and then press Enter. The Boot PROM has a password only if one was defined.

NOTE

If you are prompted to enter a new Boot PROM password, make sure it is at least 8 characters in length. Do not select this option unless specifically instructed by support personnel.

6. To change the “OSLoadOptions=quiet;quiet” setting so that the switch boots into single user mode, enter the following command:

```
=> setenv OSLoadOptions "single"
```

7. Enter the **printEnv** command to verify the change:

```
=> printenv
AutoLoad=yes
BootromVerbose=no
InitTest=MEM()
LoadIdentifiers=Fabric Operating System;Fabric Operating System
OSLoadOptions=single
(output truncated)
```

8. Save the changes:

```
=> saveenv
Saving Environment to Flash.....Done
```

9. Enter the **boot** command with no parameters to bring up the device in the single user mode:

```
=> boot
ATA device vendor STI Flash 8.0.0, product
STI1M73108114125534, revision 01/17/07
Map file at LBA sector 0x5003f
(output truncated)
```

10. Enter the **mount** command with the following parameters to remount the root partition as read/write capable:

```
sh-2.04# mount -o remount,rw /
EXT3 FS on hda1, internal journal
```

11. Mount the secondary partition.

If the previous command returns hda2, then use hda1 in this command. If the previous command returns hda 1, use hda2.

```
sh-2.04# mount /dev/hda2 /mnt
kjournald starting.
```

```
Commit interval 5 seconds
EXT3 FS on hda2, internal journal
EXT3-fs: recovery complete.
EXT3-fs: mounted filesystem with ordered data mode.
```

12. From the serial connection to the standby CP, view the `/etc/hosts` file to determine the hostname of the CPs:

```
sh-2.04# /bin/cat /etc/hosts
127.0.0.1 localhost
10.64.148.23 swd77 #sw0 255.255.240.0
10.64.148.24 swd76 #sw1 255.255.240.0
10.64.128.25 mycp0 #cp0 255.255.240.0 < CP0 SLOT 5
10.64.148.26 cp1 #cp1 255.255.240.0 < CP1 SLOT 6
0.0.0.0 #fc0 0.0.0.0
0.0.0.0 #fc1 0.0.0.0
10.0.0.5 cp_0_inteth #cp_0_internaeth
10.0.0.6 cp_1_inteth #cp_1_internaeth
```

NOTE

The hostnames for CPO and CP1 are user definable, and might be different for each installation.

13. From the serial connection to the standby CP, set the appropriate hostname to the CP. Use the hostname displayed in the previous step. In the above example, `mycp0` is the standby CP.

```
sh-2.04# hostname mycp0
```

14. Start networking on the standby CP to enable communication with the active CP:

```
sh-2.04# /etc/init.d/network start
```

15. From the standby CP, enter the `rsh` command to run a remote shell on the active CP and reset its password with the `passwddefault` command:

For DCX

- If the standby CP card is in slot 6 (CPO), enter:

```
sh-2.04# rsh 127.1.1.8 /sbin/passwddefault
```
- If the standby CP card is in slot 7 (CP1), enter:

```
sh-2.04# rsh 127.1.1.7 /sbin/passwddefault
```

For DCX-4S

- If the standby CP card is in slot 4 (CPO), enter:

```
sh-2.04# rsh 127.1.1.6 /sbin/passwddefault
```
- If the standby CP card is in slot 5 (CP1), enter:

```
sh-2.04# rsh 127.1.1.5 /sbin/passwddefault
```

16. Reset the `OSLoadOptions` to “`quiet;quiet`”:

```
sh-2.04# bootenv OSLoadOptions "quiet;quiet"
```

17. Reboot the standby CP using the `reboot -f` command.

```
sh-2.04# reboot -f
```

18. Log in to the active CP as `admin` from a telnet or serial connection, and set new passwords for all accounts, when prompted.

1 Password recovery using the Boot PROM interface

The password recovery procedure is now complete.

Password recovery procedure for Brocade 300, 5100, 5300 switches and the Brocade Encryption Switch

To recover a password on a Brocade 300, 5100, 5300, or a Brocade Encryption Switch, follow these steps:

1. Connect to the serial console port of the switch.
2. Reboot the switch using either the **fastBoot** command or the **reboot** command. Enter:

```
> fastboot
```

Or:

```
> /sbin/reboot
```

3. When prompted to stop test or stop AutoBoot, press ESC.

The Boot PROM menu is displayed with the following options:

- Start system
Used to reboot the system.
- Recover password.
Used to generate a character string for your support provider to recover the Boot PROM password. Use this feature only when directed by technical support personnel.
- Enter command shell.
Used to enter the command shell, to reset all passwords on the system.

```
Checking system RAM - press any key to stop test
Checking memory address: 00100000
System RAM test terminated by keyboard
set_bootstatus: BS_LOAD_OS, platform_idx = 6
Hit ESC to stop autoboot: 0
```

- ```
1) Start system.
2) Recover password.
3) Enter command shell.
```

```
Option?
```

4. Type **3** at the prompt to open the command shell:

```
Option? 3
```

5. Type the Boot PROM password, if prompted, and press Enter.

The Boot PROM has a password only if one was defined.

---

### NOTE

If you are prompted to enter a new Boot PROM password, make sure it is at least 8 characters in length. Do not select this option unless specifically instructed by support personnel.

---

6. To change the “OSLoadOptions=quiet;quiet” setting so that the switch boots into single user mode, enter the following command:

```
=> setenv OSLoadOptions "single"
```

7. Enter the **printEnv** command to verify the change:

```
=> printenv
AutoLoad=yes
BootromVerbose=no
InitTest=MEM()
LoadIdentifiers=Fabric Operating System;Fabric Operating System
OSLoadOptions=single
(output truncated)
```

8. Save the changes:

```
=> saveenv
Saving Environment to Flash.....Done
```

9. Enter the **boot** command with no parameters to bring up the device in the single user mode:

```
=> boot
Map file at LBA sector 0x17da68
Booting image at 00400000 ...
(output truncated)
```

10. Enter the **mount** command with the following parameters to remount the root partition as read/writecapable:

```
sh-2.04# mount -o remount,rw /
EXT3 FS on hda1, internal journal
```

11. Mount the secondary partition.

If the previous command returns hda2, then use hda1 in this command. If the previous command returns hda 1, use hda2.

```
sh-2.04# mount /dev/hda2 /mnt
kjournald starting. Commit interval 5 seconds
EXT3 FS on hda2, internal journal
EXT3-fs: mounted filesystem with ordered data mode.
```

12. Enter the **passwddefault** command to reset all passwords to default values as follows:

```
sh-2.04# /sbin/passwddefault
All account passwords have been successfully set to factory default.
```

If additional user accounts existed, they are deleted. Only the default accounts and passwords remain.

13. Reset the OSLoadOptions to "quiet;quiet":

```
sh-2.04# bootenv OSLoadOptions "quiet;quiet"
```

14. Reboot the switch using the **reboot -f** command.

```
sh-2.04# reboot -f
```

Traffic flow resumes when the switch completes rebooting. If you do not use the **-f** option you will have to manually reboot the switch.

15. Log in as root to the switch by the serial interface or telnet and set new passwords for all accounts.

The password recovery procedure is now complete.

## Password recovery procedure for Brocade 200E, 4900, 5000, 7500, and 7600 switches

To recover a password on a Brocade 200E, 4900, 5000, 7500, or 7600 switch, follow these steps:

1. Connect to the serial console port of the switch.
2. Reboot the switch using either the **fastBoot** command or the **reboot** command. Enter:

```
> fastboot
```

Or:

```
> /sbin/reboot
```

3. When you see the message "Press escape within 4 seconds...", press ESC.

The Boot PROM menu is displayed with the following options:

- Start system  
Used to reboot the system.
- Recover password.  
Used to generate a character string for your support provider to recover the Boot PROM password. Use this feature only when directed by technical support personnel.
- Enter command shell.  
Used to enter the command shell, to reset all passwords on the system.

```
The system is coming up, please wait...
Checking system RAM - press any key to stop test
01a00000
System RAM check terminated by keyboard
System RAM check complete
Press escape within 4 seconds to enter boot interface.
```

```
1) Start system.
2) Recover password.
3) Enter command shell.
```

```
Option? 3
```

4. Type **3** at the prompt to open the command shell.
5. Type the Boot PROM password, if prompted, and press Enter.

The Boot PROM has a password only if one was defined.

---

### NOTE

If you are prompted to enter a new Boot PROM password, make sure it is at least 8 characters in length. Do not select this option unless specifically instructed by support personnel.

---

6. Enter the **printEnv** command and make a note of the following values from its output. You will need these values later in this procedure:

- From the OSLoader field, the first of the two ATA memory addresses shown
- From the OSRootPartition field, the second partition value shown

These values are shown in red in the following example:

```
> printenv
```

```

AutoLoad=yes
ENET_MAC=00051E905AF0
InitTest=MEM()
LoadIdentifiers=Fabric Operating System;Fabric Operating System.
OSLoadOptions=quiet
OSLoader=ATA() 0xb009f;ATA() 0x141480
OSRootPartition=hda1;hda2
SkipWatchdog=yes

```

7. Enter the **boot** command with the first ATA memory address you obtained in [step 6](#) and the **-s** option:

```

> boot ATA() 0xb009f -s
Booting "Manually selected OS" image.
Entry point at 0x00800000 ...

```

8. Enter the **mount** command with the following parameters to remount the root partition as read/write:

```

> mount -o remount,rw,noatime /

```

9. Enter the **mount** command with the following parameters where hda is followed by the second partition value (such as hda1 or hda2) from the OSRootpartition field in the **printEnv** output you obtained in [step 6](#):

```

> mount /dev/hda2 /mnt

```

---

#### NOTE

OSRootPartition has not changed in any of the releases. It either points to the first partition (hda1) or 2nd partition (hda2). You simply swap the order, for example OSRootPartition=hda1;hda2 or OSRootPartition=hda2;hda1. The first entry is assigned as the root or bootable partition. Normally, either partition is bootable unless there was a firmware download in progress that went wrong or there is corruption in the partition.

---

10. Enter the **passwddefault** command to reset all passwords to default values as follows:

```

> /sbin/passwddefault

```

If additional user accounts existed, they are deleted. Only the default accounts and passwords remain.

11. Reboot the switch using the **reboot -f** command.

```

> reboot -f

```

Traffic flow resumes when the switch completes rebooting. If you do not use the **-f** option you will have to manually reboot the switch.

12. Log in as root to the switch by serial or telnet and set new passwords for all accounts.

The password recovery procedure is now complete.

## Password recovery procedure for Brocade 12000, 24000, and 48000 switches

To recover a password on a Brocade 12000, 24000, or 48000 director, follow these steps:

# 1 Password recovery using the Boot PROM interface

1. Connect to the standby CP of the Brocade 12000, 24000, or 48000 director.

To determine which CP is standby, use one of the following methods:

- If you have the appropriate passwords, use the **haShow** command.

---

**NOTE**

You cannot use the **haShow** command if you have lost all passwords.

---

- Use the active LED to identify the active and standby CP.

2. Reboot the standby CP using either the **fastBoot** command or the **reboot** command. Enter:

```
> fastboot
```

Or:

```
> /sbin/reboot
```

3. When you see the message "Press escape within 4 seconds..." , press ESC.

The Boot PROM menu is displayed with the following options:

- Start system  
Used to reboot the system.
- Recover password.  
Used to generate a character string for your support provider to recover the Boot PROM password. Use this feature only when directed by technical support personnel.
- Enter command shell.  
Used to enter the command shell, to reset all passwords on the system.

```
The system is coming up, please wait...
Checking system RAM - press any key to stop test
01a00000
System RAM check terminated by keyboard
System RAM check complete
Press escape within 4 seconds to enter boot interface.
```

- ```
1) Start system.
2) Recover password.
3) Enter command shell.
```

```
Option? 3
```

4. Enter **3** at the prompt to open the command shell.
5. Type the Boot PROM password, if prompted, and then press Enter. The Boot PROM has a password only if one was defined.

NOTE

If you are prompted to enter a new Boot PROM password, make sure it is at least 8 characters in length. Do not select this option unless specifically instructed by support personnel.

6. Enter the **printEnv** command and make a note of the following values from its output. You will need these values later in this procedure:

- From the OSLoader field, the first of the two ATA memory addresses shown
- From the OSRootPartition field, the second partition value shown

These values are shown in red in the following example:

```
> printenv
AutoLoad=yes
ENET_MAC=0060696019B4
InitTest=MEM()
LoadIdentifiers=Fabric Operating System;Fabric Operating System
OSBooted=MEM() 0xF0000000
OSLoadOptions=quiet;quiet
OSLoader=MEM() 0xF0000000;MEM() 0xF0800000
OSRootPartition=hda1;hda2
SkipWatchdog=yes
```

7. Run the **boot** command with the first memory address (obtained in [step 6](#)) and the **-s** option.

```
> boot MEM() 0xF0000000 -s
Booting "Manually selected OS" image.
Entry point at 0x00800000 ...
```

8. Enter the **mount** command with the following parameters to remount the root partition as read/write:

```
> mount -o remount,rw,noatime /
```

9. Enter the **mount** command with the following parameters where hda is followed by the second partition value (such as hda1 or hda2) from the OSRootpartition field in the **printEnv** output you obtained in [step 6](#):

```
> mount /dev/hda2 /mnt
```

NOTE

OSRootPartition has not changed in any of the releases. It either points to the first partition (hda1) or 2nd partition (hda2). You simply swap the order, for example OSRootPartition=hda1;hda2 OR OSRootPartition=hda2;hda1. The first entry is assigned as the root or bootable partition. Normally, either partition is bootable unless there was a firmwaredownload in progress that went wrong or there is corruption in the partition.

10. From the serial connection to the standby CP, view the /etc/hosts file to determine the hostname of the CPs:

```
# /bin/cat /etc/hosts
127.0.0.1 localhost
10.64.148.23 swd77 #sw0 255.255.240.0
10.64.148.24 swd76 #sw1 255.255.240.0
10.64.128.25 mycp0 #cp0 255.255.240.0 < CP0 SLOT 5
10.64.148.26 cp1 #cp1 255.255.240.0 < CP1 SLOT 6
0.0.0.0 #fc0 0.0.0.0
0.0.0.0 #fc1 0.0.0.0
10.0.0.5 cp_0_inteth #cp_0_internaeth
10.0.0.6 cp_1_inteth #cp_1_internaeth
```

NOTE

The hostnames for CPO and CP1 are user definable, and might be different for each installation.

11. From the serial connection to the standby CP, set the appropriate hostname to the CP. Use the hostname displayed in the previous step. In the above example, mycp0 is the standby CP.

1 Password recovery using the Boot PROM interface

```
# hostname mycp0
```

12. Start networking on the standby CP to enable communication with the active CP:

```
> /etc/init.d/network start
```

13. From the standby CP, enter the **rsh** command to run a remote shell on the active CP and reset its password with the **passwddefault** command:

- If the standby CP card is in slot 5 (CP0), enter:

```
> rsh 10.0.0.5 /sbin/passwddefault
```

- If the standby CP card is in slot 6 (CP1), enter:

```
> rsh 10.0.0.6 /sbin/passwddefault
```

14. Reboot the standby CP using the **reboot -f** command.

```
> reboot -f
```

15. Log in to the active CP as admin from a telnet or serial connection, and set new passwords for all accounts, when prompted.

The password recovery procedure is now complete.

Password recovery procedure for Brocade 3250, 3850, 3900, and 4100 switches

To recover a password on a Brocade 3250, 3850, 3900, or 4100 switch, follow these steps:

1. Connect to the serial console port of the switch.
2. Reboot the switch using either the **fastBoot** command or the **reboot** command. Enter:

```
> fastboot
```

Or:

```
> /sbin/reboot
```

3. When you see the message "Press escape within 4 seconds..." , press ESC.

The Boot PROM menu is displayed with the following options:

- Start system
Used to reboot the system.
- Recover password.
Used to generate a character string for your support provider to recover the Boot PROM password. Use this feature only when directed by technical support personnel.
- Enter command shell.
Used to enter the command shell, to reset all passwords on the system.

```
The system is coming up, please wait...  
Checking system RAM - press any key to stop test  
01a00000  
System RAM check terminated by keyboard  
System RAM check complete  
Press escape within 4 seconds to enter boot interface.
```

```
1) Start system.
```

- 2) Recover password.
- 3) Enter command shell.

Option? **3**

4. Type **3** at the prompt to open the command shell.
5. Type the Boot PROM password, if prompted, and press Enter.

The Boot PROM has a password only if one was defined.

NOTE

If you are prompted to enter a new Boot PROM password, make sure it is at least 8 characters in length. Do not select this option unless specifically instructed by support personnel.

6. Enter the **printEnv** command and make a note of the following values from its output. You will need these values later in this procedure:

- From the OSLoader field, the first of the two MEM memory addresses shown
- From the OSRootPartition field, the second partition value shown

These values are shown in red in the following example:

```
> printenv
AutoLoad=yes
ENET_MAC=0060696019B4
InitTest=MEM()
LoadIdentifiers=Fabric Operating System;Fabric Operating System
OSBooted=MEM() 0xF0000000
OSLoadOptions=quiet;quiet
OSLoader=MEM() 0xF0000000;MEM() 0xF0800000
OSRootPartition=hda1;hda2
SkipWatchdog=yes
```

7. Run the **boot** command with the first memory address (obtained in [step 6](#)) and the **-s** option.

```
> boot MEM() 0xF0000000 -s
Booting "Manually selected OS" image.
Entry point at 0x00800000 ...
```

8. Enter the **mount** command with the following parameters to remount the root partition as read/write:

```
> mount -o remount,rw,noatime /
```

9. Enter the **mount** command with the following parameters where hda is followed by the second partition value (such as hda1 or hda2) from the OSRootpartition field in the **printEnv** output you obtained in [step 6](#):

```
> mount /dev/hda2 /mnt
```

NOTE

OSRootPartition has not changed in any of the releases. It either points to the first partition (hda1) or 2nd partition (hda2). You simply swap the order, for example OSRootPartition=hda1;hda2 or OSRootPartition=hda2;hda1. The first entry is assigned as the root or bootable partition. Normally, either partition is bootable unless there was a firmwaredownload in progress that went wrong or there is corruption in the partition.

1 Password recovery using the Boot PROM interface

10. Enter the **passwddefault** command to reset all passwords to default values as follows:

```
> /sbin/passwddefault
```

If additional user accounts existed, they are deleted. Only the default accounts and passwords remain.

11. Reboot the switch using the **reboot -f** command.

```
> reboot -f
```

Traffic flow resumes when the switch completes rebooting. If you do not use the **-f** option you will have to manually reboot the switch.

12. Log in as root to the switch by serial or telnet and set new passwords for all accounts.

The password recovery procedure is now complete.

Password recovery for Fabric OS v4.4.0

In Fabric OS v4.4.0, you must take additional steps before and after performing the [“Password recovery using the Boot PROM interface”](#) on page 3. Otherwise, the switch is left in single-user mode.

Password recovery steps before root command

When running Fabric OS v4.4.0, you must save the output of the **printEnv** command before booting the switch in the single user mode. Saving this information is necessary because booting the system from the Boot PROM command shell in Fabric OS 4.4.0 erases all Boot PROM parameters. You will reenter these parameter values later, after the password recovery process is complete.

A skeletal procedure is provided here. For procedural details, see [“Password recovery using the Boot PROM interface”](#) on page 3, and find the procedure for your specific switch, and remember to save the printEnv output.

1. Connect to the serial port of the switch or the standby CP.
2. Reboot the switch and press ESC within 4 seconds after the message "Press escape within 4 seconds...".
3. Enter **3** at the prompt to enter the command shell.
4. Enter the Boot PROM password.
5. Enter the **printEnv** command and save the output. For example:

```
The system is coming up, please wait...
Checking system RAM - press any key to stop test

Checking memory address: 01300000
System RAM check terminated by keyboard
System RAM check complete
Press escape within 4 seconds to enter boot interface.
```

- 1) Start system.
- 2) Recover password.
- 3) Enter command shell.

```
Option? 3
Password:
```

```
=> printenv
AutoLoad=yes
ENET_MAC=006069602BD6
InitTest=MEM()
LoadIdentifiers=Fabric Operating System;Fabric Operating System
OSLoader=MEM() 0xF0000000;MEM() 0xF0800000
OSLoadOptions=quiet;quiet
OSRootPartition=hda1;hda2
SkipWatchdog=yes
```

- From the output of the `printEnv` command, record the value for OSLoader.

OSLoader _____

Password recovery steps after root command

After you have recovered the passwords, you must perform these steps:

- Connect to the serial port interface of the switch or standby CP.
- Reboot the switch and press ESC within 4 seconds after the message "Press escape within 4 seconds..." displays.
- Enter **3** at the prompt to enter the command shell.


```
"Enter Boot PROM interface:"
```
- Enter the Boot PROM password.
- Enter the following command strings, one at a time, to the Boot PROM parameters you saved before booting from the Boot PROM command shell:

NOTE

The value of the OSLoader= string should be set to the exact value from [step 6 on page 17](#)

```
unsetenv OSBooted
setenv LoadIdentifiers=Fabric Operating System;Fabric Operating System
setenv OSLoadOptions=quiet;quiet
setenv OSLoader=MEM() 0xF0000000;MEM() 0xF0800000
saveenv
printenv
reset
```

Obtaining the boot PROM recovery password

Use this procedure on devices running Fabric OS v4.1.x, v5.x, and v6.x when you do not have a Boot PROM password.

This procedure obtains a Boot PROM recovery password. It does not reset the Fabric OS passwords on the switch. Once the Boot PROM password has been recovered, you must go through the Boot PROM command shell to reset the Fabric OS passwords on the switch.

This section explains how to gather the information you need to send to your switch support provider in order to get a Boot PROM recovery password. Once you have received the Boot PROM recovery password, and gained access to the Boot PROM, you must reset the passwords using ["Password recovery using the Boot PROM interface"](#) on page 3.

1 Password recovery using Password Recovery firmware

To obtain the Boot PROM recovery password from your switch support provider:

1. Connect to the serial port interface of the switch or standby CP.
2. Reboot the switch or standby CP.
3. Press ESC within four seconds after the message "Press escape within 4 seconds...".
4. Enter **2** at the prompt. A character string is displayed, shown in red in the following example:

```
1) Start system.
2) Recover password.
3) Enter command shell.
```

```
Option? 2
```

```
Send the following string to Customer Support for password recovery:
```

```
/uasLR1raCqT3FToqy0ZjA==
```

5. Send the character string to your switch support provider to obtain a Boot PROM recovery password.
6. Perform the appropriate steps to set the Boot PROM password if it was not set, as prompted:

```
Recovery password is NOT set. Please set it now.
```

7. Enter the Recovery Password that is generated from your support provider when prompted, and re-enter it when prompted.

```
Enter the supplied recovery password.
```

```
Recovery Password: YnFG9DDr1FMDVknM0RkPtg== < Supplied by your support provider
```

```
Re-enter Recovery Password: YnFG9DDr1FMDVknM0RkPtg==
```

8. When prompted with "New password:", enter the new Boot PROM password and re-enter it when prompted:

```
New password: xxx
```

```
Re-enter new password: xxx
```

9. Record the new password for future reference.
10. Enter the **saveEnv** command.

Follow these steps to recover a complete recovery entry. The output is related to the steps above as well.

- a. Enter the **resetPw** command to clear boot PROM password usage.
- b. Enter the **saveEnv** command. Passwords will no longer be required for Boot PROM access.

```
> saveenv
```

You are now ready to recover passwords as described in "[Password recovery using the Boot PROM interface](#)" on page 3.

Password recovery using Password Recovery firmware

This procedure applies only to Brocade switches and directors running Fabric OS v2.6.x and v3.x.

This procedure requires Password Recovery firmware, available from your switch support provider. The Password Recovery firmware is effective only for the first time it is launched. You cannot use the Password Recovery firmware to perform any other switch functions.

These procedures require switch downtime. Brocade recommends removing the switch from the fabric and rejoining it after the recovery process is complete.

In order to complete the steps in this section you need the following:

- Password Recovery firmware: Provide the exact Fabric OS version and the WWN of the switch to your support provider with a request for the Password Recovery firmware. This firmware can be launched only once, and it recovers the password for the specific switch only.
- Ethernet connection between host and switch. It can be a network connection from a host to the switch or a direct connection with an Ethernet crossover cable.
- Serial connection to the switch.

NOTE

The Brocade SilkWorm 2800 does not have a serial port on the switch. Password recovery on a Brocade SilkWorm 2800 is not supported.

Password recovery for Fabric OS v2.6.x and v3.x

To reset the passwords on a Fabric OS v2.6.x and v3.x switch using the Password Recovery firmware, follow these steps:

1. Copy the Password Recovery firmware to a host that is accessible to the switch; either an FTP server or a laptop (running an FTP server) directly connected to the ethernet port. You must use either FTP or RSHD to copy the firmware. If FTP is used, the password cannot be blank.
2. Connect to the console port.
3. Power the switch off and back on.
4. Set the boot parameters on your switch to perform a netboot:
 - a. At the “[VxWorks Boot]” prompt for the switch, enter **c**.
 - b. Type the requested information at the prompts. To accept the default value for a parameter, press Enter.

The parameters are defined as follows:

host name	Name of machine on which Password Recovery firmware is located
file name	Full pathname where Password Recovery firmware is located
inet on ethernet	Switch IP address
host inet	The IP address for the FTP or RSHD host
gateway inet	Gateway address
user	Login name of user account on host machine

Press any key to stop auto-boot...

```
[VxWorks Boot]: c
'.' = clear field; '-' = go to previous field; ^D = quit
boot device : fe1
processor number : 0
```

1 Password recovery using Password Recovery firmware

```
host name : host
file name : /usr/switch/firmware resetPasswd303f6f
inet on ethernet (e) : 192.168.132.217:255.255.240.0
inet on backplane (b):
host inet (h) : 192.168.132.133
gateway inet (g) : 192.168.132.133
user (u) : user
ftp password (pw) (blank = use rsh):
flags (f) : 0x0
target name (tn) : sw2800
startup script (s) :
other (o) :
```

5. Press @ at the [VxWorks Boot] prompt to begin booting the Password Recovery version of the firmware from the network.

```
[VxWorks Boot]: @
boot device : fei
processor number : 0
host name : host
file name : resetPasswd303f6f
inet on ethernet (e) : 192.168.132.217:fffff000
host inet (h) : 192.168.132.133
gateway inet (g) : 192.168.132.133
user (u) : user
flags (f) : 0x0
target name (tn) : sw2800
Attaching network interface fei0... done.
Attaching network interface lo0... done.
host is alive <-----CONNECTION TO HOST PROVIDING FIRMWARE IMAGE
Loading... 4407608 + 329564 + 1153796
Starting at 0x10400000...
Attaching network interface fei0... done.
Attached TCP/IP interface to fei unit 0
Attaching network interface lo0... done.
telnetInit: telnetd initialized.
NFS client support not included.
efwHookAdd: Added Ethernet Hook
Adding 9407 symbols for standalone.
Model: 4
flash time 0, creation time 1048818644
Committing configuration...done.
setting passwd to defaults <-----FIRMWARE IMAGE RESETS PASSWORD TO BROCADE
DEFAULTS
Time Bomb has been set
RESTRICTED ONE TIME USE
Passwords have been reset. Please power cycle the switch.
```

The user, admin, factory, and root passwords are reset to the default values.

6. Turn off the switch and turn it on again.
7. Press any key when you see the message "Press any key to stop autoboot..." This provides access to the boot prompt.
8. Set the switch to boot from the flash again:

- a. At the [VxWorks Boot] prompt, enter **c** to begin resetting the boot parameters to the default settings.
 - b. Remove the values that you added by typing a period (.) after each parameter, then pressing Enter. The boot parameters are returned to the default settings.
9. Turn off the switch and turn it on again to reload the original firmware from flash. The switch resumes normal operation.
 10. Log in to the switch by telnet or serial as root, and set new passwords for all accounts.

1 Password recovery using Password Recovery firmware