BROCADE

Secure Fabric OS

QuickStart Guide

Supporting Fabric OS v3.2.0, v4.4.0

Supporting SilkWorm 3016, 3200, 3250, 3800, 3850, 3900, 4100, 12000, 24000

Publication Number: 53-0000352-04

Publication Date: 09/03/04

Brocade, the Brocade B weave logo, Secure Fabric OS, and SilkWorm are registered trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. FICON, IBM eserver BladeCenter are registered trademarks of IBM Corporation in the U.S. and other countries. All other brands, products, or service names are or may be trademarks or service marks of, and are used to identify, products or services of their respective owners.

Notice: The information in this document is provided "AS IS," without warranty of any kind, including, without limitation, any implied warranty of merchantability, noninfringement or fitness for a particular purpose. Disclosure of information in this material in no way grants a recipient any rights under Brocade's patents, copyrights, trade secrets or other intellectual property rights. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use.

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.

Notice: 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*.

Export of technical data contained in this document may require an export license from the United States government. SECURITY NOTICE: Secure Fabric OS includes security features that you can use, along with other security tools, to design and implement a more secure storage area network ("SAN"), as part of your overall network and information security infrastructure. However, simply installing Secure Fabric OS does not guarantee the security of your SAN or your overall network. There are numerous factors that affect the security of a SAN, including, without limitation, proper security policies and procedures, hardware and software selection (including network security tools), proper installation, configuration, and maintenance of the hardware and software, the interoperability of the various components of your SAN and your network, and a proper, secure operating environment. In addition, Secure Fabric OS utilizes digital certificates in connection with its access control features. Although digital certificates are a useful authentication security measure that improves overall security, they do not guarantee authenticity or security. To help you evaluate the digital certificate functionality of Secure Fabric OS, you can obtain details in the Certificate Practices Statement, which is included with the documentation you received with this product. In designing the security of your SAN, it is your responsibility to evaluate all of these factors to ensure your SAN will meet your security needs. Your experience may vary based on these and other factors. Your use of Secure Fabric OS, including the digital certificates, is subject to and governed by the terms of the applicable license agreement and to your compliance with the policies and procedures for the use of Secure Fabric OS and digital certificates made available to you by Brocade from time to time. If Brocade becomes aware of a breach of the security of its digital certificate infrastructure, Brocade reserves the right to re-issue digital certificates. In that event, you will be required to submit new certificate signing requests and install reissued certificates across your SAN. You should plan for any network disruption that this may cause.

YOU ACKNOWLEDGE THAT YOU HAVE ACCESS TO SUFFICIENT INFORMATION TO ENSURE THAT YOU CAN MAKE AN INFORMED DECISION AS TO THE EXTENT TO WHICH YOU CHOOSE TO RELY ON DIGITAL CERTIFICATES AND OTHER SECURITY FEATURES IN SECURE FABRIC OS ("SECURITY"). THE SECURITY IS PROVIDED "AS IS," WITHOUT WARRANTIES OF ANY KIND, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. BROCADE SHALL HAVE NO LIABILITY WITH RESPECT TO YOUR USE OF AND RELIANCE ON THE SECURITY.

Brocade Communications Systems, Incorporated

Corporate Headquarters
1745 Technology Drive
San Jose, CA 95110
T: (408) 333-8000
F: (408) 333-8101
Email: info@brocade.com

Latin America Headquarters
5201 Blue Lagoon Drive
Miami, FL 33126
T: (305) 716-4165
Email: latinam-sales@brocade.com

European Headquarters
2 ème étage 29, route de l'Aéroport
Case Postale 105
CH-1215 Gèneva 15,
Switzerland
T: +41 22 799 56 40
F: +41 22 799 56 41
Email: emea-info@brocade.com

Asia-Pacific Headquarters
Shiroyama JT Trust Tower 36th Floor
4-3-1 Toranomon, Minato-ku
Tokyo, Japan 105-6036
T: +81 35402 5300
F: +81 35402 5399
Email: japan-info@brocade.com

Document History

The following table lists all published versions of the *Secure Fabric OS QuickStart Guide*.

Document Title	Publication Number	Summary of Changes	Publication Date
Secure Fabric OS QuickStart Guide, v4.1.0	53-0000352-02	First release.	April 2003
Secure Fabric OS QuickStart Guide, v2.6.2/v3.1.2/v4.2.0	53-0000352-03	Addition of "Security Notice" to the back of title page. Updated references to v3.1.x and v4.1.x to v3.1.2 and v4.2.x, as appropriate. Added references to SilkWorm 3250, 3850, and 24000, as appropriate. Added a short glossary. Some minor edits.	December 2003
Secure Fabric OS QuickStart Guide	53-0000352-04	Reorganize and edit. Add references to SilkWorm 3016, SilkWorm 4100, and Fabric OS v4.4.0.	September 2004

Overview of Secure Fabric OS

Brocade Secure Fabric OS is an optional licensed software product that you can use to increase the security of a SilkWorm platform fabric. Secure Fabric OS is supported by Brocade Fabric OS v2.6.2, v3.2.0, and v4.4.0, and can be implemented in fabrics that contain any combination of these versions.

The intent of the *Secure Fabric OS QuickStart Guide* is to provide the initial steps required to build a basic Secure Fabric OS SAN. For comprehensive instructions on building a Secure Fabric OS SAN, refer to the *Secure Fabric OS User's Guide*.

To implement Secure Fabric OS in a fabric, each switch in the fabric must have the following:

- A compatible version of the Fabric OS
- An activated Secure Fabric OS license key
- An activated Brocade Zoning license key (zoning is essential to Secure Fabric OS mechanisms)
- The required public key infrastructure (PKI) objects
- A digital certificate

Obtaining these items for each platform might require access to the Web site of your switch supplier. If your supplier is Brocade, you can access the Brocade Partner Web site by navigating to *www.brocade.com* and clicking Partner Network at the top of the page.

Note

If you do not already have a Partner login, follow the instructions on the Web site to receive a user ID and password.

From the Brocade Partner Web site, click **For Technical Professionals > Tools > Secure Fabric OS Upgrade** to access the Secure Fabric OS - Field Upgrade Process Web page. This Web page includes all the links and resources you might need to build a basic Secure Fabric OS SAN.

Secure Fabric OS uses PKI technology that requires digital certificates installed on switches to uniquely identify their credentials. Brocade hosts PKI Certificate Authority and provides a Web-based field upgrade process to receive certificate signing requests (CSRs) and deliver digital certificates to the reseller.

An enhancement to the field upgrade process that addresses reseller requirements is implemented, allowing the request for digital certificates from reseller end customers to be routed through the reseller. The current field upgrade process can only accept requests from the Brocade Partner Web site.

This document includes the Secure Fabric OS basics for the following:

- "Upgrading Secure Fabric OS"
- "Enabling Secure Mode in the Fabric"
- "Using PKI Objects"
- "Merging Fabrics"
- "Creating and Activating Memberless Policies"
- "Preventing a LUN Connection"

Upgrading Secure Fabric OS

To perform a field upgrade:

1. Ensure the installed version of Fabric OS (on each switch) supports Secure Fabric OS.

   There are two methods to obtain the Fabric OS version information on a Brocade platform:

   - Using Advanced Web Tools, point your browser to the platform IP address (or DNS alias). This utility displays information about all switches in the fabric, including the OS version running on each.
   - Using telnet, connect to the switch, log in, and run the **version** command. The second line of output, which reads "Fabric OS: ...," contains the OS version information (for example, Fabric OS v4.4.0).

   Table 1 Supported Platforms and Fabric OS Versions

Platform	Fabric OS
SilkWorm 2000-series	v2.6.1 or later
SilkWorm 3200 and 3800	v3.1.x or later
SilkWorm 3900 and 12000	v4.1.x or later
SilkWorm 3016, 3250, 3850, and 24000	v4.2.x or later
SilkWorm 4100	v4.4.0

2. Upgrade the Fabric OS version, if necessary.

   Download the desired Fabric OS version from the Brocade Partner Web site. Refer to the *Fabric OS Procedures Guide* that corresponds to your version of Fabric OS for firmware download instructions.

   Note

   After downloading the firmware to the switch, reboot or fastboot your switch to activate the new firmware.

   If your SAN is already in secure mode, you do not need to disable secure mode to upgrade the Fabric OS.

   If the switch being upgraded is the primary fabric configuration server (FCS), it temporarily becomes the backup FCS switch during the firmware reboot procedure; however, it reverts to primary FCS switch at the conclusion of the reboot.

   Rebooting a switch to activate new firmware causes I/O to be disrupted unless the switch runs Fabric OS v4.x.

3. Obtain software license keys for Brocade Secure Fabric OS and Brocade Zoning.

   If you do not have a Secure Fabric OS license and a Zoning license for each switch you want in your secure fabric, provide your switch supplier with the WWN of the switches that need licenses. The switch supplier will provide you with a "Paper Pack" for the Secure Fabric OS and Zoning licenses. Follow the instructions in the Paper Pack and use the Brocade Partner Web site to submit your transaction keys to receive your unique switch license keys.

4. Use the **licenseAdd** command (or Advanced Web Tools) to add the software license keys for Secure Fabric OS and Zoning to each switch.

5. Download and run the PKICert utility and generate a CSR:

   a. From the Brocade Partner Web site, click **For Technical Professionals > Tools > Secure Fabric OS Upgrade** to access the Secure Fabric OS - Field Upgrade Process Web page.

   b. Click the **PKICert** link to begin downloading the utility to your PC or workstation.

   c. Extract and run the PKICert utility.

   d. Select option 1 and follow the directions to generate a CSR file for each switch or fabric.

   Note
   You can generate a CSR file for all switches for a fabric or multiple fabrics using this utility.

   Starting with Fabric OS v3.2.0 and v4.4.0, Fabric OS also uses PKI certificates for Secure Fabric OS instead of SSL; the SSL certificates are independent of the Secure Fabric OS certificates and are obtained through a separate process. This procedure is for PKI certificates for Secure Fabric OS only.

6. Obtain digital certificates:

   a. From the Brocade Partner Web site, click **For Technical Professionals > Tools > Secure Fabric OS Upgrade** to access the Secure Fabric OS - Field Upgrade Process Web page.

   b. Click the **Request Certificates** link and follow the instructions.

   c. Request certificates for your switches by submitting the corresponding CSRs you generated.

      You should receive an email within 30 minutes that contains a file with unique digital certificates for each switch listed in the CSR file that you submitted.

   Note
   If you do not receive the certificates, contact your switch supplier.

7. Distribute certificates to the fabric.

   Select option 2 in the PKICert utility to distribute the certificates.

8. Download the **sectelnet** utility:

   Note
   You can skip this step if you only connect to your switches through the switch serial console interface.

   a. From the Brocade Partner Web site, click **For Technical Professionals > Tools > Secure Fabric OS Upgrade** to access the Secure Fabric OS - Field Upgrade Process Web page.

   b. Click the **Secure Telnet Client** link and follow the instructions.

   c. Select the appropriate format to download (Windows NT or Solaris).

   Note
   If any switches in the Secure Fabric OS fabric are running Fabric OS v4.1.x or later, you have the option of using an SSH client that supports protocol version 2.

Enabling Secure Mode in the Fabric

Secure mode is enabled on a fabric-wide basis. When secure mode is enabled, one or more switches become FCS switches. You determine which switches are FCS switches either by specifying that all switches become FCS switches or providing a list. When you specify all switches, the local switch (the switch on which you run the **secModeEnable** command) is the primary FCS switch. When you provide a list, the primary FCS switch is the first one on the list.

Enabling secure mode:

- Creates an FCS_POLICY policy containing the WWNs for the FCS switches.
- Distributes the fabric management policy set (FMPS) to all switches in the fabric.
- Activates the FMPS.
- Reboots switches not running Fabric OS v3.2.0 or v4.4.0.

The primary FCS switch:

- Distributes the default policy sets to all switches in the fabric.
- Distributes and applies the zoning configuration.
- Applies the FMPS.

Note

Refer to the *Secure Fabric OS User's Guide* for additional information about enabling secure mode and setting policies.

Before you enable secure mode in the fabric, you must determine which switches are going to be backup FCS switches and which one will be the primary FCS switch.

To enable security:

1. Build the fabric.

   The administrator builds the fabric with switches that are identified to be in the secure fabric.

   You should record all your passwords and store them in a safe place prior to enabling security. For detailed information about this procedure, refer to the *Secure Fabric OS User's Guide* that corresponds to the version of the Fabric OS on your switch.

2. Determine the primary FCS switch, the backup FCS switch, and any non-FCS switches.

   Any non-FCS switches cannot manage the secure fabric.

3. Connect to the switch that will become the primary FCS switch, using **sectelnet** or the serial port.

   Note

   If the primary FCS switch is running Fabric OS v4.1 or later, you can use an SSH client that supports version 2 of the protocol.

4. Run the **secModeEnable** command to enable security on the fabric.

   Starting in Fabric OS v3.2.0 and v4.4.0, you have the choice of a simplified secure mode enable process or an interactive specification of the FCS switches by WWN, switch name, or domain ID and passwords.

To use the simplified secure mode enable process, type the following:

```
zebra011:admin> secmodeenable --quickmode

Your  use of  the certificate-based  security features  of the  software
installed on this equipment is subject to the End User License Agreement
provided  with the equipment and the Certification  Practices Statement,
which you may review at http://www.switchkeyactivation.com/cps. By using
these security features, you are consenting to be bound by the  terms of
these  documents.  If you  do not agree to the terms of these documents,
promptly contact the entity from which you obtained this software and do
not use these security features.
Do you agree to these terms?  (yes, y, no, n): [no] y

This command requires Switch Certificate,  Security license and Zoning license to
be installed on  every switch in the fabric.

PLEASE NOTE: On successful completion of this command, login sessions may be
closed and some switches may go through a reboot to form a secure fabric.

Non-FCS admin password will be set the same as FCS admin password.
ARE YOU SURE  (yes, y, no, n): [no] y
Please enter current admin account password:
Enabling secure mode, this may take several minutes, please wait...
Secure mode is enabled.
```

The **secModeEnable** command:

- Creates a default FMPS with the policy (FCS_POLICY) that contains the FCS switch WWNs.
- Distributes the policy set to all of the switches in the fabric.
- Activates the policy set.

Refer to the *Fabric OS Command Reference Manual* for your primary FCS switch for other options available with the **secModeEnable** command.

Note

When security is enabled, all switches in the fabric *not running Fabric OS v3.2.0 or v4.4.0* are automatically rebooted. In these cases, all I/O should be stopped prior to running the **secModeEnable** command.

5. Verify that your fabric is now running in secure mode by running the **secModeShow** or **secFabricShow** command and examining the output:

```
zebra011:admin> secmodeshow
Secure Mode: ENABLED.
Version Stamp: 849437394, Fri May  7 16:29:19 2004.
Pos   Primary WWN                     DId swName.
=================================================
  1   Yes     10:00:00:60:69:00:02:5c   1 zebra011.
  2   No      10:00:00:05:1e:34:00:7a   2 Dazzler16.
  3   No      10:00:00:60:69:80:48:a5   3 zebra007.
  4   No      10:00:00:60:69:90:02:f2   4 zebra052.
  5   No      10:00:00:60:69:c0:21:34   5 zebra071.
  6   No      10:00:00:60:69:80:48:a4   6 zebra006.
  7   No      10:00:00:60:69:c0:21:14   7 zebra072.
  8   No      10:00:00:60:69:51:42:31   8 zebra061.
  9   No      10:00:00:60:69:90:02:ed   9 zebra053.
 10   No      10:00:00:60:69:c0:1f:57  10 zebra074.
 11   No      10:00:00:60:69:c0:20:db  11 zebra077.
 12   No      10:00:00:05:1e:34:00:7d  12 Dazzler8.
 13   No      10:00:00:60:69:c0:21:73  13 zebra075.
 14   No      10:00:00:60:69:c0:21:85  14 zebra073.
 15   No      10:00:00:60:69:51:42:26  15 zebra062.
 16   No      10:00:00:60:69:51:43:00  16 zebra064.
 17   No      10:00:00:60:69:c0:0b:5d  17 zebra076.
 18   No      10:00:00:60:69:c0:06:85  18 zebra078.
 19   No      10:00:00:60:69:90:03:19  38 zebra051.
 20   No      10:00:00:60:69:51:0c:62 163 zebra065.
```

```
zebra011:admin> secfabricshow
Role    WWN                     DId Status  Enet IP Addr    Name
================================================================
Primary 10:00:00:60:69:00:02:5c   1 Ready   10.32.170.96    “zebra011”
Backup  10:00:00:05:1e:34:00:7a   2 Ready   10.32.170.56    “Dazzler16”
Backup  10:00:00:60:69:80:48:a5   3 Ready   10.32.170.92    “zebra007”
Backup  10:00:00:60:69:90:02:f2   4 Ready   10.6.3.59       “zebra052”
Backup  10:00:00:60:69:c0:21:34   5 Ready   10.32.170.71    “zebra071”
Backup  10:00:00:60:69:80:48:a4   6 Ready   10.32.170.91    “zebra006”
Backup  10:00:00:60:69:c0:21:14   7 Ready   10.32.170.72    “zebra072”
Backup  10:00:00:60:69:51:42:31   8 Ready   10.32.170.61    “zebra061”
Backup  10:00:00:60:69:90:02:ed   9 Ready   10.32.170.53    “zebra053”
Backup  10:00:00:60:69:c0:1f:57  10 Ready   10.32.170.74    “zebra074”
Backup  10:00:00:60:69:c0:20:db  11 Ready   10.32.170.77    “zebra077”
Backup  10:00:00:05:1e:34:00:7d  12 Ready   10.32.170.57    “Dazzler8”
Backup  10:00:00:60:69:c0:21:73  13 Ready   10.32.170.75    “zebra075”
Backup  10:00:00:60:69:c0:21:85  14 Ready   10.32.170.73    “zebra073”
Backup  10:00:00:60:69:51:42:26  15 Ready   10.32.170.62    “zebra062”
Backup  10:00:00:60:69:51:43:00  16 Ready   10.32.170.64    “zebra064”
Backup  10:00:00:60:69:c0:0b:5d  17 Ready   10.32.170.76    “zebra076”
Backup  10:00:00:60:69:c0:06:85  18 Ready   10.32.170.78    “zebra078”
Backup  10:00:00:60:69:90:03:19  38 Ready   10.32.170.51    “zebra051”
Backup  10:00:00:60:69:51:0c:62 163 Ready   10.32.170.65    “zebra065”
________________________________________________________________

Secured switches in the fabric: 20
```

If you encounter difficulties, refer to the *Secure Fabric OS User's Guide* for troubleshooting information.

After you have installed a default secure mode fabric, it is time to decide which policies you want to implement in your Secure Fabric OS. These policies are site-specific. Refer to the *Secure Fabric OS User’s Guide* for information about all the available policies and using them in your Secure Fabric OS.

Using PKI Objects

This section includes the following:

- “Locating PKI Objects”
- “Identifying PKI Objects”
- “Removing PKI Objects”

Locating PKI Objects

Before enabling secure mode, you should verify that your PKI objects are in place. If you are missing one of your PKI objects, remove all PKI objects, regenerate the complete set, and generate a new CSR. You can use the **pkiCreate** command in Fabric OS v4.1.x or later. In v3.1.x, use the **fastboot** command to generate the PKI objects.

Identifying PKI Objects

If your switch is running Fabric OS v4.1.x or later, type **pkiShow** from the command line to display all the PKI objects. For all other versions of the Fabric OS, type **configShow "pki"**.

To display PKI objects on a SilkWorm 12000 running Secure Fabric OS v4.4.0:

```
sec_core_0:root> pkishow
Passphrase      : Exist
Private Key     : Exist
CSR             : Exist
Certificate     : Exist
Root Certificate: Exist
```

To display PKI objects on a SilkWorm 3200 running Secure Fabric OS v3.2.0:

```
switch:admin> configshow “pki”
Passphrase      : Exist
Private Key     : Exist
CSR             : Exist
Certificate     : Exist
Root Certificate: Exist
```

Removing PKI Objects

To remove PKI objects in nonsecure mode:

```
switch:admin> pkiremove

WARNING!!!

Removing Pki objects will impair the security functionality
of this fibre channel switch. If you want secure mode enabled,
you will need to get the switch certificate again.

About to remove Pki objects.
ARE YOU SURE (yes, y, no, n): [no] y
All PKI objects removed.
```

If run in secure mode, the following error message is displayed:

```
switch:admin> pkiremove

This Switch is in secure mode.
Removing Pki objects is not allowed. Exiting...
```

Merging Fabrics

The switch that succeeds as the primary FCS switch distributes its the zoning information to all the switches in the newly merged fabric. Before merging fabrics, back up the zoning configurations and ensure that the switch that will succeed as the primary FCS switch has the desired zoning configuration.

As a guideline to merging secure fabrics, reset the version stamp on the secure-mode fabric that is merging with the other Secure Fabric OS fabric.

Refer to the *Brocade Secure Fabric OS User's Guide* for additional information about merging fabrics.

Creating and Activating Memberless Policies

You cannot create and activate an FCS policy without members. For some policies, such as TELNET_POLICY or SERIAL_POLICY, creating memberless a policy locks you out of your secure fabric through telnet or prevents setting up a serial connection. In these cases, you need to leave a way into your fabric (for example, through a SERIAL_POLICY) so that you can manage your Secure Fabric OS fabric.

Preventing a LUN Connection

It might be necessary to prevent someone from connecting a host and mounting a logical unit number (LUN) connection to your secure fabric. Besides hardware-enforced zoning, you need to create options and DCC policies on each switch in the secure fabric after configuring it in all your hosts and storage. This locks down anything that is connected to the secure fabric. If someone subsequently plugs in a *rogue* host, that port becomes disabled. Alternatively, if your primary FCS switch is running Fabric OS v3.2.0 or v4.4.0, you can use **secModeEnable --quickmode**, **--lockdown**, or **--lockdown=dcc** to enable secure mode; either option creates DCC policies for each port in the fabric.

Note

If you change the PID format used on the fabric (for example, from native mode to core PID mode), you need to create new DCC policies on each switch.