Secure Fabric OS

User's Guide

Supporting Fabric OS v3.2.0, v4.4.0

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

Publication Number: 53-0000526-04
Publication Date: 09/03/04

 Publication Number: 53-0000526-04

Brocade Communications Systems, Incorporated

Corporate Headquarters
Brocade Communications Systems, Inc.
1745 Technology Drive
San Jose, CA 95110
Tel: 1-408-333-8000
Fax: 1-408-333-8101
E-mail: info@brocade.com

Latin America Headquarters
Brocade Communications System, Inc.
5201 Blue Lagoon Drive
Miami, FL 33126
Tel: 1-305-716-4165
E-mail: latinam-sales@brocade.com

European Headquarters
Brocade Communications Switzerland Sàrl
Centre Swissair
Tour A - 2ème étage
29, Route de l'Aéroport
Case Postale 105
CH-1215 Genève 15
Switzerland
Tel: +41 22 799 56 40
Fax: +41 22 799 56 41
E-mail: emea-info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems K.K.
Shiroyama JT Trust Tower 36th FL.
4-3-1 Toranomon, Minato-ku
Tokyo, Japan 105-6036
Tel: +81-3-5402-5300
Fax: +81-3-5402-5399
E-mail: japan-info@brocade.com

Document History

The following table lists all versions of the *Secure Fabric OS User's Guide*.

Document Title	Publication Number	Summary of Changes	Publication Date
Secure Fabric OS User's Guide v2.6	53-0000195-02	First release.	January 2001
Secure Fabric OS User's Guide v3.1.0/4.1.0	53-0000526-02	Examples, information about new features, and new procedures were added. The book was reorganized for greater ease of use. Glossary was removed; detailed procedure for downloading from Web site was removed.	April 2003
Secure Fabric OS User's Guide v2.6.2/3.1.2/4.2.0	53-0000526-03	Addition of "Security Notice" to the back of title page. Updated references to 2.6.1, 3.1 and 4.1 to 2.6.2, 3.1.2 and 4.2, as appropriate. Added references to SilkWorm 3250, 3850 and 24000, as appropriate. Some minor edits. Rewording of core PID passages to reflect new PID mode. Wording of caution against running two halves of a 12000 differently under Secure OS clarified. There was some rewording of compatibility requirements.	December 2003
Secure Fabric OS User's Guide	53-0000526-04	Add SilkWorm 3016, SilkWorm 4100, and Fabric OS v4.4.0 references, new and revised content from defects, and minor edits.	September 2004

Contents

About This Document

This document is written for a SAN administrator setting up and managing a Brocade Secure Fabric OS SAN. This document is specific to Brocade Fabric OS versions v3.2.0 and v4.4.0 and all switches running Fabric OS v3.2.0 and v4.4.0, including:

- Brocade SilkWorm 3016 switch
- Brocade SilkWorm 3200 switch
- Brocade SilkWorm 3250 switch
- Brocade SilkWorm 3800 switch
- Brocade SilkWorm 3850 switch
- Brocade SilkWorm 3900 switch
- Brocade SilkWorm 4100 switch
- Brocade SilkWorm 12000 director
- Brocade SilkWorm 24000 director

In those instances in which procedures or parts of procedures documented here apply to some switches but not to others, this guide identifies exactly which switches are supported and which are not.

"About This Document" contains the following sections:

How This Document Is Organized

This document is organized to help you find the particular information that you want as quickly and easily as possible.

This document contains both information and procedures organized in roughly chronological order. Starting from an introduction to Secure Fabric OS, it continues with system requirements, initial implementation, adjusting to your own environment, and continued operation; also included is a summary of the Secure Fabric OS commands, as well as the steps necessary to remove Secure Fabric OS.

The document contains the following components:

- Chapter 1, "Introducing Secure Fabric OS" provides basic information about Secure Fabric OS.
- Chapter 2, "Adding Secure Fabric OS to the Fabric" allows you to set up and get started using Secure Fabric OS.
- Chapter 3, "Creating Secure Fabric OS Policies" helps you create the security policies needed for your SAN.
- Chapter 4, "Managing Secure Fabric OS" provides information for routine administration of your Secure Fabric OS.
- Appendix A, "Secure Fabric OS Commands and Secure Mode Restrictions" summarizes Secure Fabric OS commands.
- Appendix B, "Removing Secure Fabric OS Capability" provides information and procedures for removing Secure Fabric OS from your SAN.
- The glossary defines both terms specific to Brocade technology and common industry terms with uses specific to Brocade technology.
- The index points you to the exact pages on which specific information is located.

Supported Hardware and Software

This document has been updated to include information specific to the Secure Fabric OS on Fabric OS v3.2.0 and v4.4.0, including:

- Additional functionality or support in the software from Fabric OS v3.1.2 and v4.2.0.
- Changes to functionality or support in the software from Fabric OS v3.1.2 and v4.2.0.

Although many different software and hardware configurations are tested and supported by Brocade Communications Systems, Inc. for Secure Fabric OS v3.2.0 and v4.4.0, documenting all possible configurations and scenarios is beyond the scope of this document; however, this document does specify when procedures or steps of procedures apply only to specific switches.

This document does not support all Fabric OS versions. This document is specific to Secure Fabric OS v3.2.0 and v4.4.0. To obtain information about an OS version other than these, refer to the documentation specific to your OS version.

What's New in This Document

The following changes have been made since this document was last released:

- Information that was added:
  - Use of an enhanced version of the **secModeEnable** command
  - Configuration and use of CHAP and DH-CHAP authentication
  - Support information for the SilkWorm 3016 and 4100.
- Information that was changed:
  - Clarified when switches fastboot. Fabric OS v3.2.0 and v4.4.0 switches no longer need to reboot when the fabric enters secure mode.
- Information that was deleted:
  - Removed references to Fabric OS v2.6.2 because there are further code releases for v2.x, unless the reference is regarding interoperability between Fabric OS versions.

For further information, refer to release notes.

Document Conventions

This section describes text formatting conventions and important notices formats.

Text Formatting

The following table describes the narrative-text formatting conventions that are used in this document.

Table Preface-1 Text Formatting Conventions

Convention	Purpose
bold text	• Identifies command names • Identifies GUI elements • Identifies keywords/operands • Identifies text to enter at the GUI or CLI
italic text	• Provides emphasis • Identifies variables • Identifies paths and internet addresses • Identifies document titles and cross references
`code` text	• Identifies CLI output • Identifies syntax examples

For readability, command names in the narrative portions of this guide are presented in mixed lettercase: for example, **switchShow**. In actual examples, command lettercase is often all lowercase. Otherwise, this manual specifically notes those cases in which a command is case sensitive.

Notes, Cautions, and Warnings

The following notices appear in this document.

Note
A note provides a tip, emphasizes important information, or provides a reference to related information.

Caution
A caution alerts you to potential damage to hardware, firmware, software, or data.

Warning
A warning alerts you to potential danger to personnel.

Special Term Uses

For definitions of SAN-specific terms, visit the Storage Networking Industry Association online dictionary at *http://www.snia.org/education/dictionary.*

Additional Information

This section lists additional Brocade and industry-specific documentation that you might find helpful.

Brocade Resources

The following related documentation is provided on the Brocade Documentation CD-ROM and on the Brocade Web site, through Brocade Connect.

Note
Go to *http://www.brocade.com* and click **Brocade Connect** to register at no cost for a user ID and password.

Fabric OS

- *Brocade Fabric OS Features Guide*
- *Brocade Fabric OS Procedures Guide*
- *Brocade Fabric OS Command Reference Manual*
- *Brocade Fabric OS MIB Reference Manual*
- *Brocade System Error Message Reference Manual*
- *Brocade QuickLoop User's Guide (v3.x only)*

Fabric OS Optional Features

- *Brocade Advanced Web Tools Administrator's Guide*
- *Brocade Fabric Watch User's Guide*

SilkWorm 24000

- *SilkWorm 24000 QuickStart Guide*
- *SilkWorm 24000 Hardware Reference Manual*

SilkWorm 12000

- *SilkWorm 12000 QuickStart Guide*
- *SilkWorm 12000 Hardware Reference Manual*

SilkWorm 4100

- *SilkWorm 4100 Hardware Reference Manual (for v4.4.x software)*
- *SilkWorm 4100 QuickStart Guide (for v4.4.x software)*

SilkWorm 3900

- *SilkWorm 3900 Hardware Reference Manual (for v4.x software)*
- *SilkWorm 3900 QuickStart Guide (for v4.x software)*

SilkWorm 3800

- *SilkWorm 3800 Hardware Reference Manual (for v3.x software)*
- *SilkWorm 3800 QuickStart Guide (for v3.x software)*

SilkWorm 3250/3850

- *SilkWorm 3250/3850 Hardware Reference Manual (for v4.x software)*
- *SilkWorm 3250/3850 QuickStart Guide (for v4.x software)*

SilkWorm 3200

- *SilkWorm 3200 Hardware Reference Manual (for v3.x software)*
- *SilkWorm 3200 QuickStart Guide (for v3.x software)*

SilkWorm 3016

- *SilkWorm 3016 Hardware Reference Manual (for v4.2.1 and later software)*
- *SilkWorm 3016 QuickStart Guide (for v4.2.1 and later software)*

For practical discussions about SAN design, implementation, and maintenance, you can obtain *Building SANs with Brocade Fabric Switches* through:

http://www.amazon.com

For additional Brocade documentation, visit the Brocade SAN Info Center and click the Resource Library location:

http://www.brocade.com

Release notes are bundled with the Fabric OS.

Other Industry Resources

For additional resource information, visit the Technical Committee T11 Web site. This Web site provides interface standards for high-performance and mass storage applications for Fibre Channel, storage management, as well as other applications:

http://www.t11.org

For information about the Fibre Channel industry, visit the Fibre Channel Industry Association Web site:

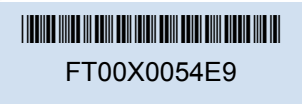
http://www.fibrechannel.org

Getting Technical Help

Contact your switch support supplier for hardware, firmware, and software support, including product repairs and part ordering. To expedite your call, have the following information available:

1. General Information
   - Technical Support contract number, if applicable
   - Switch model
   - Switch operating system version
   - Error numbers and messages received
   - **supportSave** command output
   - Detailed description of the problem and specific questions
   - Description of any troubleshooting steps already performed and results
2. Switch Serial Number

   The switch serial number and corresponding bar code are provided on the serial number label, as shown here:

   The serial number label is located as follows:

   - *SilkWorm 3200 and 3800 switches:* Back of chassis.
   - *SilkWorm 3250, 3850, and 3900 switches*: Bottom of chassis.
   - *SilkWorm 4100 switches:* On the switch ID pull-out tab located on the port side and on the inside of the chassis, near power supply 1 (on the right when looking at the nonport side).
   - *SilkWorm 12000 and 24000 directors:* Inside the front of the chassis, on the wall to the left of the ports.

3. World Wide Name (WWN)
    - *SilkWorm 3016, 3250, 3850, 3900 and 4100 switches, and SilkWorm 12000 and 24000 directors:* Provide the license ID. Use the **licenseIdShow** command to display the license ID.
    - *All other SilkWorm switches:* Provide the switch WWN. Use the **wwn** command to display the switch WWN.

Document Feedback

Because quality is our first concern at Brocade, 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. Forward your feedback to *documentation@brocade.com*. Provide the title and version number and as much detail as possible about your issue, including the topic heading and page number and your suggestions for improvement.

Chapter

1

Introducing Secure Fabric OS

Brocade Secure Fabric OS is an optionally licensed product that provides customizable security restrictions through local and remote management channels on a SilkWorm fabric. Secure Fabric OS provides the ability to:

- Create policies to customize fabric management access.
- Specify which switches and devices can join the fabric.
- View statistics related to attempted policy violations.
- Manage the fabric-wide Secure Fabric OS parameters through a single switch.
- Create temporary passwords specific to a login account and switch.
- Enable and disable Secure Fabric OS as desired.

Secure Fabric OS uses digital certificates based on PKI or Diffie-Hellman with Challenge-Handshake Authentication Protocol (DH-CHAP) shared secrets to provide switch-to-switch authentication.

This chapter contains the following sections:

Management Channel Security

Secure Fabric OS can be used to provide policy-based access control of local and remote management channels, including Fabric Manager, Web Tools, standard SNMP applications, and management server.

Access through a channel can be restricted by customizing the Secure Fabric OS policy for that channel. Secure Fabric OS policies are available for telnet (includes sectelnet and Secure Shell), SNMP, management server, HTTP, and API.

Fabric Manager, Web Tools, and API all use both HTTP and API to access the switch. To use any of these management tools to access a fabric that has secure mode enabled, ensure that the workstation computers can access the fabric by both API and HTTP. If an API or HTTP policy has been created, it must include the IP addresses of all the workstation computers.

After a digital certificate has been installed on the switch, Fabric OS v3.2.0 and v4.4.0 encrypt sectelnet, API, and HTTP passwords automatically, regardless of whether Secure Fabric OS is enabled.

Note

The **Telnet** button in Web Tools can be used to launch telnet only (not sectelnet or Secure Shell) and is disabled when secure mode is enabled.

On two-domain directors, messages (such as notifications of password changes) that are sent to the whole secure fabric are seen on both domains, even if the other domain is not part of the secure fabric.

Secure Shell (SSH)

Fabric OS v4.4.0 supports SSH, enabling fully encrypted telnet sessions. Use of SSH requires installation of a SSH client on the host computer; use of SSH does not require a digital certificate on the switch.

Secure Shell access is configurable by the Telnet Policy that is available through Secure Fabric OS. However, Fabric OS v4.4.0 supports Secure Shell whether or not Secure Fabric OS is licensed.

To restrict CLI access to Secure Shell over the network, disable telnet as described in "Telnet," later in this section.

Secure Shell clients are available in the public domain and can be located by searching the Internet. Use clients that support version 2 of the protocol, such as OpenSSH or F-Secure.

Fabric OS v4.4.0 also supports the following ciphers for session encryption and HMACs (hash function-based message authentication codes):

- Ciphers: AES128-CBC, 3DES-CBC, Blowfish-CBC, Cast128-CBC, and RC4
- HMACs: HMAC-MD5, HMAC-SHA1, HMAC-SHA1-96, and HMACMD5-96

Note

The first time a Secure Shell client is launched, a message is displayed, indicating that the server's host key is not cached in the registry. You will also see this message the first time a Secure Shell client is launched after you upgrade switch firmware.

For more information about Secure Shell, refer to the *Fabric OS Procedures Guide*.

Sectelnet

The sectelnet client is a secure form of telnet that encrypts passwords only. It is available from your switch supplier. Fabric OS v4.4.0 includes the sectelnet server; the sectelnet client must be installed on the workstation computer.

The sectelnet client can be used as soon as a digital certificate is installed on the switch. sectelnet access is configurable by the Telnet Policy.

Telnet

Standard telnet is not available when secure mode is enabled.

To remove all telnet access to the fabric, disable telnet through the **telnetd** option of the **configure** command. This configure option does not require disabling the switch. For more information about the **configure** command, refer to the *Fabric OS Command Reference Manual*.

Switch-to-Switch Authentication

Switch-to-switch authentication supports the following:

- "Using PKI"
- "Using DH-CHAP"

Using PKI

Secure Fabric OS can use digital certificates based on public key infrastructure (PKI) and switch WWNs and the SLAP or FCAP protocols to identify the authorized switches and prevent the addition of unauthorized switches to the fabric. A PKI certificate installation utility (PKICert) is provided for generating certificate signing requests (CSRs) and installing digital certificates on switches. For information about how to use the PKICert utility, see "Adding Secure Fabric OS to Switches That Require Upgrading" on page 2-5.

Support for FCAP is first provided in Secure Fabric OS v3.2.0 and v4.4.0 and is used instead of SLAP when both switches support it. PKI authentication automatically falls back to SLAP when a switch does not support FCAP.

Note

PKI digital certificates are used also by Fabric OS v4.4.0. Secure Fabric OS and secure sockets layer (SSL) use different digital certificates and different methods of obtaining and installing the certificates. PKI digital certificates are used for the secure fabric, and SSL digital certificates are not. The methods described in this manual are specific to Secure Fabric OS. Refer to the *Fabric OS Procedures Guide* for information about SSL and digital certificates.

Using DH-CHAP

Starting with Fabric OS v3.2.0 and v4.4.0, Secure Fabric OS can use Diffie-Hellman with Challenge-Handshake Authentication Protocol (DH-CHAP) shared secrets to provide switch-to-switch authentication and prevent the addition of unauthorized switches to the fabric. (DH-CHAP is not available with Fabric OS v2.6.x.) The default is to use FCAP or SLAP (refer to "Switch-to-Switch Authentication"). To authenticate using DH-CHAP, it should be explicitly enabled.

You control which authentication protocols can be used by a switch with the **authUtil** CLI command. Using this command, you can specify that FCAP only, DH-CHAP only, or either be used. If both are permitted, the default order (FCAP, DH-CHAP) is used. The actual protocol is selected during dynamic negotiation.

DH-CHAP requires a pair of shared secret keys—*shared secrets*—between each pair of switches authenticating with DH-CHAP. Use the **secAuthSecret** command to manage shared secrets. Refer to the *Fabric OS Command Reference Manual* for details of the **authUtil** and **secAuthSecret** commands and refer to "Configuring Authentication" on page 2-27 for a basic procedure for configuring DH-CHAP.

Fabric Configuration Server Switches

Fabric configuration server (FCS) switches are one or more switches that are specified as “trusted” switches for use in managing Secure Fabric OS. These switches should be both electronically and physically secure. At least one FCS switch must be specified to act as the primary FCS switch, and one or more backup FCS switches are recommended to provide failover ability in case the primary FCS switch fails.

If your primary FCS switch runs Fabric OS v3.2.0 or v4.4.0, you should not use a Fabric OS v2.6.2 switch (or a switch running older versions of Fabric OS v3.x.x or v4.x.x) as a backup FCS switch. Fabric OS v3.2.0 and v4.4.0 introduce new features, such as a larger secure database (128K in v3.2.0 and 256K in v4.4.0), centralized login authentication (AAA), RADIUS, and a SSL certificate, not supported by older releases.

FCS switches are specified by listing their WWNs in a specific policy called the FCS policy. The first switch that is listed in this policy and participating in the fabric acts as the primary FCS switch; it distributes the following information to the other switches in the fabric:

- Zoning configuration
- Secure Fabric OS policies
- Fabric password database
- SNMP community strings
- System date and time

Note

The role of the FCS switch is separate from the role of the principal switch, which assigns domain IDs. The role of the principle switch is not affected by whether secure mode is enabled.

When secure mode is enabled, only the primary FCS switch can propagate management changes to the fabric. When a new switch joins the fabric, the primary FCS switch verifies the digital certificate; then it provides the current configuration, overwriting the existing configuration of the new switch.

Because the primary FCS switch distributes the zoning configuration, zoning databases do not merge when new switches join the fabric. Instead, the zoning information on the new switches is overwritten when the primary FCS switch downloads zoning to these switches, if secure mode is enabled on all of them. For more information about zoning, refer to the *Fabric OS Procedures Guide*. For more information about merging fabrics, refer to “Adding Switches and Merging Fabrics with Secure Mode Enabled” on page 4-14.

The remaining switches listed in the FCS policy act as backup FCS switches. If the primary FCS switch becomes unavailable for any reason, the next switch in the list becomes the primary FCS switch. You should have at least one backup FCS switch, to reduce the possibility of having no primary FCS switch available. You can designate as many backup FCS switches as you like; however, all FCS switches should be physically secure.

Any switches not listed in the FCS policy are defined as non-FCS switches. The root and factory accounts are disabled on non-FCS switches.

For information about customizing the FCS policy, see “Enabling Secure Mode” on page 3-2. For information about configuration download restrictions while in secure mode, refer to “Enabling Secure Mode” on page 3-2.

Fabric Management Policy Set

Using Secure Fabric OS, you can create several types of policies to customize various aspects of the fabric. By default, only the FCS policy exists when secure mode is first enabled. Use the CLI or Fabric Manager to create and manage Secure Fabric OS policies.

Secure Fabric OS policies can be created, displayed, modified, and deleted. They can also be created and saved without being activated immediately, to allow implementation at a future time. Saved policies are persistent, meaning that they are saved in flash memory and remain available after switch reboot or power cycle.

The group of existing policies is referred to as the "fabric management policy set" or FMPS, which contains an *active* policy set and a *defined* policy set. The active policy set contains the policies that are activated and currently in effect. The defined policy set contains all the policies that have been defined, whether activated or not. Both policy sets are distributed to all switches in the fabric by the primary FCS switch. Secure Fabric OS recognizes each type of policy by a predetermined name.

Secure Fabric OS supports the following policies:

- FCS policy

  Use to specify the primary FCS and backup FCS switches. This is the only required policy.

- Management Access Control (MAC) policies

  Use to restrict management access to switches. The following specific MAC policies are provided:

  - Read and Write SNMP policies. Use to restrict which SNMP hosts are allowed read and write access to the fabric.
  - Telnet policy. Use to restrict which workstations can use sectelnet or Secure Shell to connect to the fabric (telnet is not available when Secure Fabric OS is enabled).
  - HTTP policy. Use to restrict which workstations can use HTTP to access the fabric.
  - API policy. Use to restrict which workstations can use API to access the fabric.
  - SES policy. Use to restrict which devices can be managed by SES.
  - Management Server policy. Use to restrict which devices can be accessed by management server.
  - Serial Port policy. Use to restrict which switches can be accessed by serial port.
  - Front Panel policy. Use to restrict which switches can be accessed by front panel.

- Options policy

  Use to restrict the types of WWNs that can be used for zoning.

- Device Connection Control (DCC) policies

  Use to restrict which Fibre Channel device ports can connect to which Fibre Channel switch ports.

- Switch Connection Control (SCC) policy

  Use to restrict which switches can join the fabric.

Note
A SCC policy is required if FICON is enabled.

Adding Secure Fabric OS to the Fabric

Chapter 2

Secure Fabric OS is supported by Fabric OS v2.6.2, v3.1.0, and v4.1.0 and later; it can be added to fabrics that contain any combination of these versions. This manual applies to v3.2.0 and v4.4.0, and assumes that these versions are running before adding Secure Fabric OS. The procedure for adding Secure Fabric OS to a switch depends on whether the switch is shipped with one of these versions installed or requires upgrading.

The following switches can be upgraded for use with Secure Fabric OS:

- SilkWorm 2000-series switches from Fabric OS v2.3.x to v2.6.2
- SilkWorm 3200 or 3800 switches from Fabric OS v3.0.x to v3.2.0
- SilkWorm 3900 or 12000 switches from Fabric OS v4.0.x to v4.4.0
- SilkWorm 3250, 3850, and 24000 switches from Fabric OS v4.2.0 to v4.4.0
- SilkWorm 3016 switch from Fabric OS v4.2.1 to v4.4.0

The SilkWorm 4100 switch ships with Fabric OS v4.4.0.

This chapter contains the following sections:

Adding Secure Fabric OS to a Fabric

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

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

Note

Adding Secure Fabric OS to the fabric might require access to the Web site of the switch support supplier. If the supplier is Brocade, navigate to *http://partner.brocade.com* (if a partner login is not already assigned, follow the instructions to receive a user name and password).

The following tasks are required to set up a fabric for use with Secure Fabric OS:

- Identify the versions of Fabric OS currently installed on each switch and determine which switches require upgrading to support Secure Fabric OS. Instructions are provided in "Identifying the Current Version of Fabric OS" on page 2-2.
- For each switch (except SilkWorm 12000 and SilkWorm 24000 with dual-virtual switches) that was shipped with Fabric OS v3.1.2 or later or v4.2.0 or later installed, follow the instructions provided in "Adding Secure Fabric OS to v3.2.0 or v4.4.0 Switches" on page 2-3.
- For each switch that must be upgraded for use with Secure Fabric OS, follow the instructions provided in "Adding Secure Fabric OS to Switches That Require Upgrading" on page 2-5.
- For SilkWorm 12000 directors, and SilkWorm 24000 directors configured with two logical switches, with any version of Fabric OS v4.x, follow the instructions provided in "Adding Secure Fabric OS to a SilkWorm 12000 or SilkWorm 24000" on page 2-24.
- Install a supported CLI client on each computer workstation that will be used to access the fabric. Instructions are provided in "Installing a Supported CLI Client on a Computer Workstation" on page 2-26.

Note

If one or more switches are incapable of enforcing security, secure mode is not enabled in the entire fabric.

Identifying the Current Version of Fabric OS

Before continuing, identify the version of Fabric OS on each switch in the fabric and determine which switches must be upgraded.

To identify the current version of Fabric OS installed on each switch in the fabric:

1. Open a CLI connection (serial or telnet) to one of the switches in the fabric.
2. Log in to the switch as admin. The default password is "password".
3. Type the **version** command.

   For example, entering the **version** command on a SilkWorm 3900:

```
switch3900:admin> version
Kernel: 2.4.2
Fabric OS: v4.2
Made on: Fri Jan 3 23:02:08 2003
Flash: Jan 3 18:03:35 2003
BootProm: 4.2.17
```

4. Repeat step 1 through step 3 for each switch in the fabric.

Adding Secure Fabric OS to v3.2.0 or v4.4.0 Switches

This section applies to the following switches:

- SilkWorm 3200 or 3800 switches shipped with Fabric OS v3.2.0
- SilkWorm 3016, 3250, 3850, 3900, 4100, 12000, and 24000 (configured with one logical switch) switches shipped with Fabric OS v4.4.0

All switches that are shipped with Fabric OS v3.2.0 or v4.4.0 installed already have the required PKI objects and a digital certificate. If a switch no longer has the required PKI objects, refer to section "Recreating PKI Objects if Required" on page 2-18 for information on recreating the PKI objects. If a switch no longer has the required digital certificate, refer to section "Obtaining the Digital Certificate File" on page 2-13 for information on obtaining digital certificates.

Switch digital certificates are checked when a switch joins a fabric, either because the switch is added to the fabric or because the switch is booting. Changes to the certificate—for example, if the certificate is removed or corrupted—might not be noticed until the switch is rebooted.

To set up Secure Fabric OS on a switch shipped with Fabric OS v3.2.0 or v4.4.0:

1. Change the account passwords from default values as described in "Customizing the Account Passwords" on page 2-4.

   Note

   The SilkWorm 3016 switch has a different default user name than all other SilkWorm switches. As a result, use the **userRename** command to rename the SilkWorm 3016 default "USERID" user account to "admin" before connecting the switch to a secure fabric made up of other Brocade SilkWorm switches. Refer to the *Fabric OS Command Reference Manual* for more command details.

2. If switches running Fabric OS v2.6.2 or v3.2.0 will be in same fabric as switches running Fabric OS v4.4.0, refer to the *Fabric OS Procedures Guide* for instructions on configuring compatible PID modes across the switches.

   Switch digital certificates are checked when a switch joins a fabric, either because the switch is added to the fabric or because the switch is booting. Changes to the certificate, for example, if the certificate is removed or corrupted, might not be noticed until the switch is rebooted.

   Note

   Changing the PID format causes an update to the DCC policies. If you change the PID format, use the **configUpload** command to create a new backup configuration file. Do not download the old file.

3. Ensure that the switch has activated Secure Fabric OS and Advanced Zoning software licenses as described in "Verifying or Activating the Secure Fabric OS and Advanced Zoning Licenses" on page 2-4.

Customizing the Account Passwords

The user is prompted to customize the account passwords at the first login. The prompts continue to display at each login and the **passwd** command remains disabled until the passwords prompts are answered. Immediately changing the passwords is recommended.

Note

In addition to customizing the passwords for the user, admin, factory, and root accounts, setting both the boot PROM and recovery passwords is strongly recommended. For instructions on setting these passwords, refer to the *Fabric OS Procedures Guide*.

To log in and change the passwords:

1. Open a CLI connection (serial or telnet) to the switch.
2. Log in to the switch as admin. The default password is **password**. The firmware prompts to change all passwords.
3. Change all the passwords to secure passwords, using between 8 and 40 alphanumeric characters for each password, with a different password for each account. The new passwords must be different from the default values.

Note

The initial login prompt accepts a maximum password length of eight characters. Any characters beyond the eighth character are ignored. Only the default password is subject to the eight character limit. Any password set by the user can have a length from 8 to 40 characters.

Record the passwords and store them in a secure place; recovering passwords can require significant effort and result in fabric downtime.

Verifying or Activating the Secure Fabric OS and Advanced Zoning Licenses

The Secure Fabric OS and Advanced Zoning features are part of the Fabric OS and can be activated by entering a corresponding license key, available from the switch supplier. A license must be activated on each switch that will be implementing Secure Fabric OS.

Licenses can be activated through the CLI or through Web Tools. This section provides CLI instructions only. For instructions on activating a license through Web Tools, refer to the *Advanced Web Tools User's Guide*.

To verify or activate a software license through the CLI:

1. Open a command line interface (CLI), serial or telnet, to the switch.
2. Log in to the switch as admin. The default password is **password**.
3. Type the **licenseShow** command to determine whether the license is already activated.

   A list of all the activated licenses displays. The Secure Fabric OS license displays as "Security license"; for example:

```
switch:admin> licenseshow
 1A1AaAaaaAAAA1a:
     Web license
     Zoning license
     SES license
     Trunking license
     Security license
```

4. If the Secure Fabric OS and Advanced Zoning licenses are already listed, the features are already available and the remaining steps are not required; continue if either license is not listed.
5. Contact the switch supplier to purchase the required license key.
6. After the key is received, type **licenseAdd "***key***"**.

   key is the license key string exactly as provided by the switch supplier; it is case sensitive. You can copy it from the email in which it was provided directly into the CLI. For example:

```
switch:admin> licenseadd "aAaaaaAaAaAaAaA"
adding license key "aAaaaaAaAaAaAaA"
```

7. Type the **licenseShow** command to verify that the license was successfully activated.

   If the license is listed, the feature is immediately available (the Secure Fabric OS license displays as "Security license").

Adding Secure Fabric OS to Switches That Require Upgrading

This section applies to the following switches:

- SilkWorm 3200 or 3800 switches running a Fabric OS previous to v3.1.2
- SilkWorm 3900 switches and SilkWorm 12000 directors running a Fabric OS previous to v4.2.0

To set up Secure Fabric OS on a switch that was not shipped with Fabric OS v3.1.2 or v4.2.0 (or later):

1. If switches running Fabric OS v3.2.0 will be in same fabric as switches running Fabric OS v4.4.0, refer to the *Fabric OS Procedures Guide* for instructions on configuring compatible PID modes.

Note

Changing the PID format causes an update to the DCC policies. If you change the PID format, use the **configDownload** command to create a new backup configuration file. Do not upload the old file.

2. Back up the configuration and upgrade the switch to Fabric OS v3.2.0 or v4.4.0, as appropriate to the switch, as described in "Upgrading to a Compatible Version of Fabric OS" on page 2-6.
3. Change the account passwords from the default values, as described in "Customizing the Account Passwords" on page 2-7.
4. The remaining steps are determined by whether Secure Fabric OS was already in use on the switch (such as on a 2000-series switch that was running Fabric OS v2.6):
   - If Secure Fabric OS was already in use on the switch, the upgrade is complete; do not proceed further. To verify the existing policy set, enter the **secPolicyShow** command.
   - If Secure Fabric OS was not already in use on the switch, continue with step 5.
5. Verify or activate the Secure Fabric OS and Advanced Zoning licenses, as described in "Verifying or Activating the Secure Fabric OS and Advanced Zoning Licenses" on page 2-8.
6. Download and install the PKICert utility on the computer workstation, as described in "Installing the PKICert Utility" on page 2-8.
7. Create a file containing the certificate signing requests (CSRs) from all the switches that require certificates, as described in "Using the PKICert Utility" on page 2-8.
8. Obtain digital certificates from the switch supplier, as described in "Obtaining the Digital Certificate File" on page 2-13.
9. Distribute the certificates to the switches, as described in "Distributing Digital Certificates to the Switches" on page 2-14.
10. Verify that digital certificates are installed on all the switches, as described in "Verifying Installation of the Digital Certificates" on page 2-17.

Upgrading to a Compatible Version of Fabric OS

Secure Fabric OS is supported by 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 following switches can be upgraded for use with Secure Fabric OS:

- SilkWorm 2000-series switches from Fabric OS v2.3.x to v2.6.2
- SilkWorm 3200 or 3800 switches from Fabric OS v3.0.x to v3.2.0
- SilkWorm 12000 or 3900 switches from Fabric OS v4.0.x to v4.4.0
- SilkWorm 3016, 3250, 3850, and 24000 switches from Fabric OS v4.2.x to v4.4.0

The SilkWorm 4100 switch ships with Fabric OS v4.4.0.

Note

Combinations of switches running Fabric OS v2.6.2 or v3.2.0 and Fabric OS v4.4.0 must use compatible PID modes. Refer to the *Fabric OS Procedures Guide* for information about PID modes.

Changing the PID format causes an update to the DCC policies. If you change the PID format, use the **configDownload** command to create a new backup configuration file. Do not upload the old file.

If a switch already has a Secure Fabric OS license (such as a switch running Fabric OS v2.6) and secure mode is enabled, the switch can remain in secure mode during the firmware upgrade.

To install the required versions of Fabric OS on each switch in the fabric:

1. Obtain the required firmware from the switch provider, according to the type of switch.
2. Open a CLI connection (serial or telnet) to one of the switches in the fabric.
3. Back up the configuration by entering the **configUpload** command and completing the prompts. This also backs up the security policies, if the switch is an FCS switch.
4. Log in to the switch as admin. The default password is "password".
5. Download the firmware to the computer workstation or server.
6. Download the required firmware from the computer to the switch. The download process depends on the *type of switch* and *management interface*. Refer to the *Fabric OS Procedures Guide* for download instructions specific to the type of switch and management interface.

Note

If secure mode is already enabled on the switch (such as on a 2000-series switch that was running v2.6), secure mode can remain enabled during the download to preserve the policies. For information about merging fabrics that have secure mode enabled, refer to "Adding Switches and Merging Fabrics with Secure Mode Enabled" on page 4-14.

7. Reboot the switch.

Note

The required PKI objects are automatically generated when the switch is rebooted in the new version of Fabric OS. See "Verifying Installation of the Digital Certificates" on page 2-17 for steps you can take to verify the existence of the PKI objects.

8. Repeat this procedure for each switch in the fabric.

Customizing the Account Passwords

After installing a new version of Fabric OS, the user is prompted to customize the account passwords at the first login. These prompts display at each login and the **passwd** command remains disabled until the passwords are changed from the default values.

Note

Only the first eight characters are checked.

In addition to customizing the passwords for the user, admin, factory, and root accounts, setting the boot PROM and recovery passwords is strongly recommended for Fabric OS v4.4.0 (this does not apply to v3.2.0). For instructions on setting these passwords, refer to the *Fabric OS Procedures Guide*.

To log in and change the passwords:

1. Open a CLI, serial or telnet, to the switch.
2. Log in to the switch as admin. The default password is **password**. The firmware prompts the user to change all passwords.

3. Change all the passwords to secure passwords, using between 8 and 40 alphanumeric characters for each password, with a different password for each account. The new passwords must be different from the default values.

Note

Record the passwords and store them in a secure place; recovering passwords can require significant effort and result in fabric downtime.

Verifying or Activating the Secure Fabric OS and Advanced Zoning Licenses

Refer to the instructions provided in "Verifying or Activating the Secure Fabric OS and Advanced Zoning Licenses" on page 2-4.

Installing the PKICert Utility

The PKI certificate installation utility (PKICert utility) version 1.0.6 or later is provided by the switch supplier and is used to collect certificate signing requests (CSRs) and install digital certificates on switches. The utility must be installed on a computer workstation.

To install the PKICert utility on a Solaris workstation, follow the instructions provided in the PKICert utility ReadMe file.

To install the PKICert utility on a PC workstation, perform the following steps:

1. Obtain the PKICert utility from the switch supplier.
2. Extract all the files from the utility zip file into into a directory.
3. Execute the **setup.exe**; it installs a utility in a location specified during the installation.
4. Review the ReadMe file for current information about the utility.

Using the PKICert Utility

The PKICert utility makes it possible to retrieve certificate signing requests (CSRs) from all the switches in the fabric and save them into a CSR file in XML format. PKICert also allows the user to create license reports, and it provides online help. (CSRs and PKI digital certificates are also used in Fabric OS v4.4.0 with SSL certificates. The utility to retrieve certificates, the CSRs themselves, and the digital certificates for these two uses are different. Refer to the *Fabric OS Procedures Guide* for information on SSL.)

Note

If this procedure is interrupted by a switch reboot, the CSR file is not generated and the procedure must be repeated. This procedure provides PC-specific examples.

The PKICert utility can be used only in nonsecure mode to generate or install certificates.

To obtain the CSR file for the fabric:

1. Open the PKICert utility. On a PC, double-click **pkicert.exe**.

   The utility prompts for the events log file name.

2. Type a file name for the events log and press **Enter** or just press **Enter** to accept the default. The log file is automatically created in the same directory as **pkicert.exe**.

```
PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.6

All events and errors will be recorded in an event/error log file.
If the file already exists, new event/error information will be
appended to it.

Enter a log file name [or just press Enter to accept the default].

[pki_events.log] => pki_events_fabric1.log
```

   The utility prompts for the desired function.

3. Type **1** to select CSR retrieval and press **Enter**.

```
PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.6
FUNCTIONS

1)   Retrieve CSRs from switches & write a CSR file
2)   Install Certificates contained in a Certificate file
3)   Generate a Licensed-Product/Installed-Certificates report
4)   Help using PKI-Cert to get & install certificates
q)   Quit PKI Certificate installation utility

Enter choice> 1
```

   The utility prompts for the method of specifying fabric addresses.

4. Type the desired method for entering the fabric addresses.

```
PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.6
Choose a method for providing fabric addresses

1)   Manually enter fabric address
2)   Read addresses from a file (name to be given)
r)   Return to Main menu

Enter choice>
```

   To manually enter the fabric address:

   a. Type **1** and press **Enter**.

      The utility prompts for the IP address or switch name of a switch in the fabric. Only one switch name or IP address is required for each fabric.

   b. Type the IP address or switch name of one of the switches in the fabric and press **Enter**. At least one valid IP address must be entered to continue, and the corresponding switch must be operating and available. When all the IP addresses have been entered, press **Enter** again to end the list.

      The utility prompts for the username and password for this switch.

c. Type the username and password, then press **Enter** to continue.

```
PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.6

Only one address per fabric is needed to get to all switches.
Enter a list of one or more IP or DNS addresses (aliases) you
wish to use (one per line). End the list with an empty item.

1 -->  10.32.142.167
2 -->

Connecting to Fabric(s) ...

Login to fabric 1. principal switch WWN = 10:00:00:60:69:80:46:00

Username: admin
Password:

Logged into fabric 1. principal switch WWN = 10:00:00:60:69:80:46:00

Press Enter to continue >
```

To read the fabric addresses from a file:

a. Type **2** and press **Enter**.

The utility prompts for the path and file name of the file. The addresses in the file must be IP addresses or switch names, each on a separate line.

b. Type the path and file name of the file that contains the fabric addresses and press **Enter**.

```
Enter the file-name of the Fabric Address file.
File Name ===> \\server\Working\FabricAddresses.txt

Connecting to Fabric(s) ...

Login to fabric 1. principal switch WWN = 10:00:00:60:69:80:46:00
Username:admin
Password:

Logged into fabric 1. principal switch WWN = 10:00:00:60:69:80:46:00

Press Enter to continue >
```

The utility prompts for information about the CSR file to be created.

5. Type the requested information:

a. Enter path and file name for the CSR file to be created; then type **y** if the address was entered correctly, or enter **n** and reenter the address, if not.

b. Type **y** to include licensed product data in the file. Otherwise, type **n**.

c. Type **y** to retrieve CSRs from all switches in the fabric or **n** to retrieve CSRs only from switches that do not already have a digital certificate.

```
PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.6
GET CERTIFICATE SIGNING REQUESTS

You must enter the file-name of the CSR output file to create.
       _____________________________________________________
       | Note:                                             |
       |   * The named file will be created                |
       |   * The file-name may include a directory path    |
       |     that must already exist.                      |
       |   * An extension of '.xml' will be appended to    |
       |     the file name if not already present.         |
       |   * If the file already exists, it will be        |
       |     overwritten.                                  |
        -----------------------------------------------------

File Name ===> test
Is the filename "test.xml" correct? (y/n):  y
**** WARNING, file, "test.sml", already exists!! ****
Do you want to overwrite it <y/n>? > y
Include (optional) licensed product data (y/n)? > y
Get CSRs even from switches with certificates (y/n)? > y
```

Note

If CSRs are retrieved and digital certificates are requested for switches that already have digital certificates, the same digital certificates are provided again.

The utility prompts for which fabrics to retrieve CSRs from.

6. Type **1** to retrieve CSRs only from the fabric identified earlier or **a** to retrieve CSRs from all discovered fabrics; then press **Enter**.

```
PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.6

Choose a Fabric On Which to Operate

Fabric   World Wide Name         # Switches  Principal
------  ----------------------  ----------  -----------
1)    10:00:00:60:69:80:46:00      34      host1_sw0
a)    All Fabrics
r)    Return to Functions menu

enter your choice> 1
```

The utility displays the success or failure of CSR retrieval.

7. Press **Enter** to continue.

```
       PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.6

Retrieving CSR's from 1 fabric(s)
1. Got a CSR for Switch: Name="sw_129", IP="10.32.142.129"
2. Got a CSR for Switch: Name="sw_128", IP="10.32.142.128"
3. Got a CSR for Switch: Name="sw_139", IP="10.32.142.139"
4. Got a CSR for Switch: Name="sw_143", IP="10.32.142.143"
5. Got a CSR for Switch: Name="sw_138", IP="10.32.142.138"
6. Got a CSR for Switch: Name="sw_142", IP="10.32.142.142"
7. Got a CSR for Switch: Name="Core_sw0", IP="10.32.142.166"

Wrote 12824 bytes of switch data to file: "\\server\Working\CSR_Fabric1.xml"

Success getting CSRs  & writing them to a CSR file

Press Enter to continue >
```

The **Functions** menu is displayed.

8. If you are ready to install digital certificate(s), type **2** from the list shown in the following **Functions** menu; do not quit PKICert.

```
       PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.6
       FUNCTIONS

1)   Retrieve CSRs from switches & write a CSR file
2)   Install Certificates contained in a Certificate file
3)   Generate a Licensed-Product/Installed-Certificates report
4)   Help using PKI-Cert to get & install certificates
q)   Quit PKI Certificate installation utility

Enter choice> 2
```

After you type 2, the following information is displayed:

```
PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.6
Currently Connected Fabrics

Fabric   World Wide Name         # Switches  Principal
------  ----------------------  ----------  -----------
*      10:00:00:60:69:11:f8:f9         15      sec237

_____________________________________________________
       Use Currently Connected Fabrics?

y) Yes, continue with current fabric(s)
n) No, input different Fabric addresses(es)

enter your choice> y
```

Select **n** (no) to input different fabric addresses. After you select **y** (yes), the following information is displayed:

```
PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.6
LOAD CERTIFICATES

  Enter the file-name of the Certificate input file.
File Name ===> c:/6821.xml

Is the filename "c:/6821.xml" correct? (y/n): y
```

After you select **y** (yes) the following information is displayed:

```
PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.6

Choose a Fabric On Which to Operate

Fabric   World Wide Name         # Switches  Principal
------  ----------------------  ----------  -----------
1)    10:00:00:60:69:11:f8:f9         15      sec237
a)    All Fabrics
r)    Return to Functions menu

enter your choice> 1
```

9. To quit installation, type **q** to quit the utility; then type **y** and press **Enter** to verify that you want to quit.

```
       PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.6
       FUNCTIONS

1)   Retrieve CSRs from switches & write a CSR file
2)   Install Certificates contained in a Certificate file
3)   Generate a Licensed-Product/Installed-Certificates report
4)   Help using PKI-Cert to get & install certificates
q)   Quit PKI Certificate installation utility

Enter choice> q

QUIT? (y/n) y
```

Obtaining the Digital Certificate File

The switch supplier provides the digital certificates in an XML file that is generated in response to the CSRs. Generally, the digital certificate file is provided by email.

To obtain the digital certificate file, contact the switch supplier and provide the following information:

- The CSR file generated in the previous procedure
- Email address
- Technical contact
- Phone
- Country

The switch supplier provides a confirmation number and the digital certificate file, which contains a certificate for each CSR submitted.

Save the digital certificate file on a secure workstation. The recommended location is in the directory with the CSR file. Making a backup copy of the digital certificate file and storing it in a secure location is recommended.

Distributing Digital Certificates to the Switches

You can use PKICert utility to distribute the digital certificates to the switches in the fabric. The utility ensures that each digital certificate is installed on the corresponding switch.

If you run the utility without any task argument, it defaults to interactive mode, in which it prompts for the required input.

Note

If this procedure is interrupted by a switch reboot, the certificate is not loaded and the procedure must be repeated.

To load digital certificates onto one or more switches while retrieving CSRs, go to step 8 of the previous section, "Using the PKICert Utility".

To manually load digital certificates onto one or more switches:

1. Open the PKICert utility. On a PC, double-click **pkicert.exe**.

   The utility prompts for the events log file name.

2. Type a file name for the events log and press **Enter**; alternatively, press **Enter** to accept the default. The log file is automatically created in the same directory as **pkicert.exe**.

```
PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.6

All events and errors will be recorded in an event/error log file.
If the file already exists, new event/error information will be
appended to it.

Enter a log file name [or just press Enter to accept the default].

[pki_events.log] => pki_events_fabric1.log
```

   The utility prompts for the desired function.

3. Type **2** to install the certificates and press **Enter**.

```
PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.6
FUNCTIONS

1)   Retrieve CSRs from switches & write a CSR file
2)   Install Certificates contained in a Certificate file
3)   Generate a Licensed-Product/Installed-Certificates report
4)   Help using PKI-Cert to get & install certificates
q)   Quit PKI Certificate installation utility

Enter choice> 2
```

The utility prompts for the method of specifying fabric addresses.

4. Type the desired method for entering the fabric addresses.

```
PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.6
Choose a method for providing fabric addresses

1)   Manually enter fabric address
2)   Read addresses from a file (name to be given)
r)   Return to Main menu

Type choice>
```

To manually enter the fabric address:

a. Type **1** and press **Enter**.

   The utility prompts for the IP address or switch name of a switch in the fabric. Only one switch name or IP address is required for each fabric.

b. Type the IP address or switch name of one of the switches in the fabric and press **Enter**. At least one valid IP address must be entered to continue; the corresponding switch must be operating and available. When all the IP addresses have been entered, press **Enter** again to end the list.

   The utility prompts for the username and password for this switch.

c. Type the username and password; then press **Enter** to continue.

```
PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.6

Only one address per fabric is needed to get to all switches.
Enter a list of one or more IP or DNS addresses (aliases) you
wish to use (one per line). End the list with an empty item.

1 -->  10.32.142.167
2 -->

Connecting to Fabric(s) ...

Login to fabric 1. principal switch WWN = 10:00:00:60:69:80:46:00

Username: admin
Password:

Logged into fabric 1. principal switch WWN = 10:00:00:60:69:80:46:00

Press Enter to continue >
```

To read the fabric addresses from a file:

a. Type **2** and press **Enter**.

   The utility prompts for the path and file name of the file. The addresses in the file must be IP addresses or switch names, each on a separate line.

b. Type the path and file name of the file that contains the fabric addresses and press **Enter**.

```
Enter the file-name of the Fabric Address file.
File Name ===> \\server\Working\FabricAddresses.txt

Connecting to Fabric(s) ...

Login to fabric 1. principal switch WWN = 10:00:00:60:69:80:46:00
Username: admin
Password:

Logged into fabric 1. principal switch WWN = 10:00:00:60:69:80:46:00

Press Enter to continue >
```

The utility prompts for the path and file name of the digital certificate file provided by the switch supplier.

5. Type the path and file name of the digital certificate file and press **Enter**.

   If the returned path and file name is correct, type **y** and press **Enter**; if not, type **n**, press **Enter**, retype the path and file name, and verify it is correct.

```
       PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.6
LOAD CERTIFICATES

Enter the file-name of the Certificates input file.

File Name ===> \\server\Working\DC_Fabric1.xml
Is the filename "\\server\Working\DC_Fabric1.xml" correct? (y/n):  y
```

The utility prompts for which fabrics to install digital certificates to.

6. Type **1** to distribute certificates only to the fabric identified earlier or **a** to install certificates to all discovered fabrics; then press **Enter**.

```
PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.6

Choose a Fabric On Which to Operate

Fabric   World Wide Name         # Switches  Principal
------  -----------------------  ----------  -----------
1)    10:00:00:60:69:80:46:00      7         host1_sw0
a)    All Fabrics
r)    Return to Functions menu

enter your choice> 1
```

The new certificates are loaded onto the switches and the success or fail of each certificate is displayed.

7. Press **Enter** to continue.

```
       PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.6
Load Certificates onto 1 fabric(s)

1. Loaded Certificate on Switch primaryfcsswitch: WWN-10:00:00:60:69:11:fc:52
2. Loaded Certificate on Switch backupfcsswitch: WWN-10:00:00:60:69:11:fc:53
3. Loaded Certificate on Switch backupfcsswitch: WWN-10:00:00:60:69:11:fc:54
4. Loaded Certificate on Switch nonfcsswitch: WWN-10:00:00:60:69:11:fc:55
5. Loaded Certificate on Switch nonfcsswitch: WWN-10:00:00:60:69:11:fc:56
6. Loaded Certificate on Switch nonfcsswitch: WWN-10:00:00:60:69:11:fc:57
7. Loaded Certificate on Switch nonfcsswitch: WWN-10:00:00:60:69:11:fc:58

7 Certificates were loaded,
0 Certificate loads failed

Press Enter to Continue.
```

Note

The sectelnet application can be used as soon as a digital certificate is installed on the switch.

8. Press **Enter**.

   The Functions menu is displayed.

9. Type **q** to quit the utility; then type **y** and press **Enter** to verify that you want to quit.

```
       PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.6
       FUNCTIONS

1)   Retrieve CSRs from switches & write a CSR file
2)   Install Certificates contained in a Certificate file
3)   Generate a Licensed-Product/Installed-Certificates report
4)   Help using PKI-Cert to get & install certificates
q)   Quit PKI Certificate installation utility

Enter choice> q

QUIT? (y/n) y
```

Verifying Installation of the Digital Certificates

The installation of the digital certificates can be verified through the CLI.

To verify that digital certificates are installed on all the switches in the fabric:

1. Log in to one of the switches in the fabric as admin.
2. Display the PKI objects:
   - For Fabric OS v4.4.0, enter **pkiShow**. If the switch is a SilkWorm 12000 or a two-domain SilkWorm 24000, enter this command on both logical switches.
   - For Fabric OS v3.2.0, enter **configShow "pki"**.

The command displays the status of the PKI objects.

Note
"Root Certificate" is an internal PKI object. "Certificate" is the digital certificate.

Displaying PKI objects on Fabric OS v4.4.0:

```
switch:admin> pkishow
Passphrase      : Exist
Private Key     : Exist
CSR             : Exist
Certificate     : Exist
Root Certificate: Exist
```

Displaying PKI objects on Fabric OS v3.2.0:

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

3. Verify that **Certificate** displays **Exist**.

   If the certificate shows **Empty** but the other objects show **Exist**, repeat the procedure provided in "Distributing Digital Certificates to the Switches" on page 2-14.

   If any of the other objects show **Empty** or the command displays an error message, re-create the objects as described in "Recreating PKI Objects if Required" on page 2-18.

4. Repeat for the remaining switches in the fabric.

Recreating PKI Objects if Required

The PKI objects (except for the digital certificate) are automatically generated the first time Fabric OS v3.2.0 or v4.4.0 is booted. If any of the PKI objects appear to be missing, in secure mode, the switch segments from the fabric and disables security.

The PKI objects on Fabric OS v3.2.0 and v4.4.0 can be regenerated by rebooting the switch. The PKI objects on Fabric OS v4.4.0 can also be regenerated through the following procedure.

Note
Secure mode must be disabled to perform this procedure.

To use the CLI to re-create the PKI objects on Fabric OS v4.4.0:

1. Log in to the switch as admin.
2. Type the **pkiRemove** command. If the switch is a SilkWorm 12000 or a two-domain SilkWorm 24000, enter this command on both logical switches.

3. Type the **pkiCreate** command to create new PKI objects. New PKI objects are created without digital certificates. If the switch is a SilkWorm 12000 or a two-domain SilkWorm 24000, enter this command on both logical switches. The **pkiCreate** command does not work if secure mode is already enabled.
4. Type the **pkiShow** command. If the switch is a SilkWorm 12000 or a two-domain SilkWorm 24000, enter this command on both logical switches.

   The command displays the status of the PKI objects.

   Recreating PKI objects on Fabric OS v4.4.0:

```
switch:admin> pkicreate
Installing Private Key and Csr...
Switch key pair and CSR generated...
Installing Root Certificate...

switch:admin> pkishow
Passphrase      : Exist
Private Key     : Exist
CSR             : Exist
Certificate     : Empty
Root Certificate: Exist
```

5. Repeat for any other switches, as required.

Creating PKI Certificate Reports

Reports for PKI certification provide information about the number of licenses and switches enabled on your secured fabric. The reports can also be used to audit the fabric.

1. To create a PKI report, type **3** (shown in the following example), and follow the screen prompts.

```
        PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.6
        FUNCTIONS

1)   Retrieve CSRs from switches & write a CSR file
2)   Install Certificates contained in a Certificate file
3)   Generate a Licensed-Product/Installed-Certificates report
4)   Help using PKI-Cert to get & install certificates
q)   Quit PKI Certificate installation utility

Enter choice> 3
```

2. Type the desired method for entering the fabric addresses.

```
PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.6
Choose a method for providing fabric addresses

1)   Manually enter fabric address
2)   Read addresses from a file (name to be given)
r)   Return to Main menu

Enter choice> 1
```

To manually enter the fabric address:

a. Type **1** and press **Enter**.

   The utility prompts for the IP address or switch name of a switch in the fabric. Only one switch name or IP address is required for each fabric.

b. Type the IP address or switch name of one of the switches in the fabric and press **Enter**. At least one valid IP address must be entered to continue, and the corresponding switch must be operating and available. When all the IP addresses have been entered, press **Enter** again to end the list.

   The utility prompts for the username and password for this switch.

c. Type the username and password; then press **Enter** to continue.

```
PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.6

Only one address per fabric is needed to get to all switches.
Enter a list of one or more IP or DNS addresses (aliases) you
wish to use (one per line). End the list with an empty item.

1 -->  192.168.156.73_
```

After you enter the IP address or name the utility logs in to the fabric.

```
Connecting to Fabric(s) ...

Login to fabric 1. principal switch WWN = 10:00:00:60:69:50:0d:9f

Username: root
Password:

Logged into fabric 1. principal switch WWN = 10:00:00:60:69:50:0d:9f

Press Enter to continue >
```

The utility prompts for information about the report file to be created.

3. Enter the requested information:

   a. Type the path and file name for the report file to be created. Then, type **y** if the address was entered correctly; if not, type **n** and reenter the address.

   b. Type **y** to include licensed product data in the file; otherwise, type **n**.

c. Type **y** to retrieve reports from all switches in the fabric or type **n** to retrieve reports only from switches that do not already have a digital certificate.

```
PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.6
CREATE REPORT ON LICENSED PRODUCTS

You must enter the file-name of the report file to write.
       _____________________________________________________
       | Note:                                             |
       |   * The named file will be created                |
       |   * The file-name may include a directory path    |
       |     that must already exist.                      |
       |   * An extension of '.xml' will be appended to    |
       |     the file name if not already present.         |
       |   * If the file already exists, it will be        |
       |     overwritten.                                  |
        -----------------------------------------------------

File Name ===> SFOS_FAB
Is the filename "SFOS_FAB.xml" correct? (y/n):  y
```

The utility prompts for which fabrics to write reports to.

4. Type **1** to write certificate reports only to the fabric identified earlier or **a** to write certificate reports to all discovered fabrics; then press **Enter**.

```
PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.6

Choose a Fabric On Which to Operate

Fabric   World Wide Name         # Switches  Principal
------  ----------------------  ----------  -----------
1)    10:00:00:60:69:50:0d:9f         2       sec_edge_2
a)    All Fabrics
r)    Return to Functions menu

enter your choice> 1
```

```
PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.6

Reporting on Licensed Products of these Fabrics:

Fabric   World Wide Name         # Switches  Principal
------  ----------------------  ----------  -----------
1>      10:00:00:60:69:50:0d:9f      2      sec_edge_2

Wrote 545 bytes of Lic Prod info to file: "SFOS_FAB.xml"
Success compiling and writing license report.
Press enter to continue.
```

5. Press **Enter**.

The Functions screen is displayed.

6. Type **q** to quit the utility; then type **y** and press **Enter** to verify you want to quit.

```
        PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.6
        FUNCTIONS

1)   Retrieve CSRs from switches & write a CSR file
2)   Install Certificates contained in a Certificate file
3)   Generate a Licensed-Product/Installed-Certificates report
4)   Help using PKI-Cert to get & install certificates
q)   Quit PKI Certificate installation utility

Enter choice> q
```

Accessing PKI Certificate Help

The purpose of PKI help is to obtain command line information about PKICert and obtain advice on advanced options for advanced users.

To access PKI help:

1. Select option **4** (as shown in the following example) and follow the screen prompts.

```
        PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.6
        FUNCTIONS

1)   Retrieve CSRs from switches & write a CSR file
2)   Install Certificates contained in a Certificate file
3)   Generate a Licensed-Product/Installed-Certificates report
4)   Help using PKI-Cert to get & install certificates
q)   Quit PKI Certificate installation utility

Enter choice> 4
```

```
        HELP USING PKI-CERT TO GET & INSTALL DIGITAL CERTIFICATIONS

        NOTE:This utility will only work with switches running a FAB-OS version
        that supports Fabric Security (e.g. >= v2.6, v3.2, v4.3)

1)   Use PKI-Cert to get CSR's (Certificate Signing Requests) which will be
     written to a data file. The XML format file will contain CSR's for each
     switch (identified by its WWN).

2)   Next, Upload the CSR file to the Brocade Security Upgrade website. A data
     file will be emailed to you containing a set of digital Certificates, one for
     each switch, in XML format.

3)   Finally, use PKI-Cert to install the Certificates. You will be prompted for
     the name of the data file containing the certificates.

Some options may be given on the command line such as "Log-Level."
Read help for Batch/Command-Line mode usage (y/n)? > y
```

```
       HELP WITH COMMAND LINE USEAGE OF PKI CERTIFICATE UTILITY

pkicert [-gGil] [_e log-file] [-d data-file] [-a addr-file] [-A switch-addr] [-L
log-level] [-u user-login -p password]

Task Options:
          -g Get CSRs & generate a CSR data file
          -G Get CSRs (even from switches with certificates)
          -i Install Certificates from a data file
          -l Licensed Product Report compile & generate
If none of the above "task" options is given, Pki-Cert will operate in
"Interactive" rather than "Batch" mode.

Other OPtions:

Log-file: -e (events/errors log)
  Path/file-name of log file created and written to (or if it already exists,
  apprended to ) with event/error data
     <Press Enter to Continue>
```

```
Data-file: -d
   Path/file-name of input or output file
   * If the task is "Get-CSRs" or "License Rpt", the file is an output file
     created and written to with CSR or License report data.
   * If the task is "Install Certificates", dat is read from it.

Address-file: -a
   Path/file-name of optional input file containing IP addresses or aliases of
fabrics to which sessions should be established. If this argument is not provided,
this data is read from the file indicated by environment variable
'FABRIC_CONFIG_FILE'.

Address--IP: -A
   IP address of switch/fabric with which to connect for the given task.

Log-Level: -L
   Level of information to write to the event log file:
   0 = Silent, 1 = Errors, 2 = Events + Errors, 3 = Debug-info +Events + ...

     <Press Enter to Continue>
```

2. To end help, press **Enter.**

```
User Login: -u
   User name or account login for switch given with _A option or for use as
   default for all switches given.

Password: -p
   Password must accompany "-u UserLogin" if provided. It must be more than 5
   characters.
        ----- END Of HELP with Batch Usage -----

     <Press Enter to Continue>
```

Adding Secure Fabric OS to a SilkWorm 12000 or SilkWorm 24000

The two logical switches in SilkWorm 12000 and SilkWorm 24000 (configured as two domains) directors require a slightly different procedure from other Fabric OS switches. This procedure applies whether the directors are shipped with or upgraded to Fabric OS v4.4.0.

Caution
Placing the two switches from the same director in separate fabrics is not supported if secure mode is enabled on one or both switches.

Note
Status messages from any logical switch are broadcast to the serial console and telnet sessions on all logical switches. All broadcast messages display the switch instance. Messages that originate from a switch instance other than the one to which the telnet session is logged in can be ignored.

To set up Secure Fabric OS on a SilkWorm 12000 or two-domain SilkWorm 24000:

1. Open a telnet or Secure Shell session to the IP address of either of the logical switches.

   sectelnet can also be used if the switch was shipped with Fabric OS v4.4.0 (and therefore already has a digital certificate).

   Note
   Fabric OS v4.4.0 maintains separate login accounts for each logical switch.

2. Type the **version** command. This shows the firmware version installed on the active CP.

   If the firmware is Fabric OS v4.0.0c or later, the **firmwareShow** command can be entered for more detailed information about which firmware versions are installed.

```
SW12000:admin> version
Kernel: 2.4.2
Fabric OS: v4.0.2
Made on: Fri Feb 1 23:02:08 2002
Flash: Fri Feb 1 18:03:35 2002
BootProm: 4.2.13b

SW12000:admin> firmwareshow
Local CP (Slot 5, CP0): Active
Primary partition: v4.0.2
Secondary Partition: v4.0.2
Remote CP (Slot 6, CP1): Standby
Primary partition: v4.0.2
Secondary Partition: v4.0.2
```

3. If the firmware version is not Fabric OS v4.4.0 or later, back up the configuration and install Fabric OS v4.4.0 on both CPs. For instructions, refer to "Upgrading to a Compatible Version of Fabric OS" on page 2-6.
4. Log in to one logical switch and change the account passwords from the default values, as described in "Customizing the Account Passwords" on page 2-7; then, log in to the other logical switch and change the passwords from the default values.

5. If the logical switches are in separate fabrics, synchronize the fabrics by connecting them to a common external network time protocol (NTP) server.

Note
If the fabric contains any switches running Fabric OS v4.4.0, the server must support a full NTP client. For switches running Fabric OS v3.2.0, the server can be SNTP or NTP.

   a. Open a telnet or Secure Shell session to either of the logical switches.

   b. Type **tsclockserver "***IP address of NTP server***"**.

   c. The IP address can be verified by reentering the command with no operand, which displays the current setting.

   d. Repeat for the other logical switch.

```
SW12000switch0:admin> tsclockserver "132.163.135.131"
switch:admin> tsclockserver
132.163.135.131

SW12000switch0:admin> login
login: admin
Password: xxxxxx

12000switch1:admin> tsclockserver "132.163.135.131"
12000switch1:admin> tsclockserver
132.163.135.131
```

6. Ensure that both logical switches have a Secure Fabric OS license activated, as described in "Verifying or Activating the Secure Fabric OS and Advanced Zoning Licenses" on page 2-4.

Note
Only one license key is required to enable the same feature on both logical switches.

7. Ensure that both logical switches have a Advanced Zoning license activated, as described in "Verifying or Activating the Secure Fabric OS and Advanced Zoning Licenses" on page 2-4.

8. If the firmware was upgraded, perform the following steps:

   a. Download and install the PKICert utility on the computer workstation, if not already installed, as described in "Installing the PKICert Utility" on page 2-8.

   b. Use the PKICert utility to create a file containing the certificate signing requests (CSRs) of all the switches in the fabric, as described in "Using the PKICert Utility" on page 2-8.

   c. Obtain digital certificates from the switch supplier, as described in "Obtaining the Digital Certificate File" on page 2-13.

   d. Use the PKICert utility to load the certificates onto both logical switches, as described in "Distributing Digital Certificates to the Switches" on page 2-14.

   e. Verify that the digital certificates are installed on both logical switches, as described in "Verifying Installation of the Digital Certificates" on page 2-17. The **pkiShow** command referenced in this procedure must be executed from both logical switches.

Installing a Supported CLI Client on a Computer Workstation

Standard telnet sessions work only until secure mode is enabled. The following telnet clients are supported after secure mode has been enabled:

- sectelnet

  sectelnet is a secure form of telnet that is available for switches running Fabric OS v3.2.0 or v4.4.0. For instructions on installing the sectelnet client, refer to the following procedures.

- SSH

  SSH is a secure form of telnet that is supported only for switches running Fabric OS v4.1.x and later. You can use SSH clients that use version 2 of the protocol (for example, OpenSSH or F-Secure). Refer to the *Fabric OS Procedures Guide* for client installation instructions.

sectelnet is provided on the Brocade Partner Web site. It can be used as soon as a digital certificate is installed on the switch.

Caution
Ensure that all intermediate hops are secure when accessing a switch by way of sectelnet or SSH; otherwise, user passwords might be compromised.

To install the sectelnet client on a Solaris workstation:

1. Obtain the Solaris version of the sectelnet file from the switch supplier and copy the file onto the workstation computer.
2. Decompress the tar file and install it to a location that is "known" to the computer, such as in the directory containing the standard telnet file. The location must be defined in the *i* environmental variable.

   sectelnet is immediately available.

To install the sectelnet client on a PC workstation:

1. Obtain the PC version of the sectelnet file from the switch supplier and copy the file onto the workstation computer.
2. Double-click the zipped file to decompress it.
3. Double-click the **setup.exe** file.
4. Install **sectelnet.exe** to a location that is "known" to the computer, such as in the directory containing telnet.exe. The location must be defined in the *path* environmental variable.

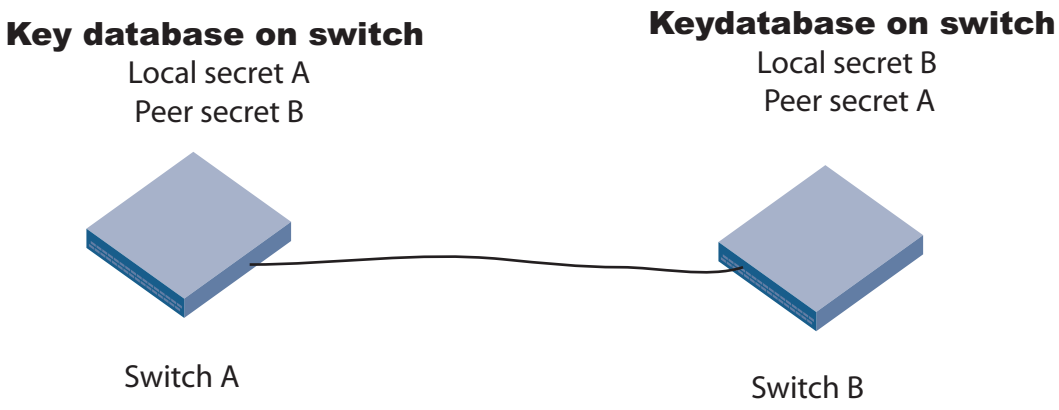
   sectelnet.exe is available as soon as setup completes.

Configuring Authentication

By default Secure Fabric OS on Fabric OS v3.2.0 and v4.4.0 uses SLAP or FCAP protocols for authentication. These protocols use digital certificates, based on switch WWN and PKI technology to authenticate switches. Support for FCAP is provided in Secure Fabric OS v3.2.0 and v4.4.0 and is used when both switches support it. Authentication automatically defaults to SLAP when a switch does not support FCAP

Alternatively, you can configure Secure Fabric OS to use DH-CHAP authentication. Use the **authUtil** command to configure the authentication parameters used by the switch. When you configure DH-CHAP, authentication, you also must define a pair of *shared secrets* known to both switches. Figure 2-1 on page 2-27 shows how the secrets are configured. In the pair, one is the local switch secret and the other is the peer switch secret. (Terms local and peer are relative to an initiator, or one who initiates authentication is local, and the one who responds is peer.) Use **secAuthSecret** to set shared secrets on the switch. Configured, shared secrets are used at the next authentication. Authentication occurs whenever secure mode is enabled or whenever there is a state change for the switch or port. The state change can be due to a switch reboot, or a switch or port enable or disable.

Figure 2-1 DH-CHAP Authentication



Selecting Authentication Protocols

Use the **authUtil** command to

- Display the current authentication parameters
- Select the authentication protocol used between switches
- Select the Diffie-Hellman (DH) group for a switch

Authentication is only performed when secure mode is enabled, but you can run the **authUtil** command either while secure mode is enabled, or not. Run the command on the switch you want to view or change.

This section illustrates using the **authUtil** command to display the current authentication parameters and to set the authentication protocol to DH-CHAP. Refer to the *Fabric OS Command Reference Manual* for more details on the **authUtil** command.

To view the current authentication parameter settings for a switch:

1. Login to the switch as admin
2. On a switch running Fabric OS v4.x, type **authUtil --show**; on a switch running Fabric OS v3.x, type **authUtil "--show"**.

   Output similar to the following displays:

```
AUTH TYPE     HASH TYPE     GROUP TYPE
-------------------------------------
dhchap          sha1,md5     0,1,2,3,4
```

To set the authentication protocol used by the switch to DH-CHAP:

1. Log in to the switch as admin
2. On a switch running Fabric OS v4.x, type **authUtil --set -a dhchap**; on a switch running Fabric OS v3.x, type **authUtil "--set -a dhchap"**.

   Output similar to the following displays:

```
Authentication is set to dhchap.
```

When using DH-CHAP, make sure that you configure the switches at both ends of a link.

Note
If you set the authentication protocol to DH-CHAP, have not yet configured shared secrets and authentication is checked (for example you enable the switch), switch authentication fails.

Managing Shared Secrets

When you configure the switches at both ends of a link to use DH-CHAP for authentication, you must also define a pair of shared secrets—one for each end of the link. Use the **secAuthSecret** command to

- View the WWN of switches with shared secrets
- Set the shared secrets for switches
- Remove the shared secret for one or more switches

This section illustrates using the **secAuthSecret** command to display the list of switches in the current switch's shared secret database and to set the pair of shared secrets for the current switch and a connected switch. Refer to the *Fabric OS Command Reference Manual* for more details on the **secAuthSecret** command.

Note
A Secure Fabric OS license is required to use the **secAuthSecret** command.

When setting shared secrets, note that you are entering the shared secrets in plain text. Use a secure channel (for example, SSH or the serial console), to connect to the switch on which you are setting the secrets.

To view the list of switches with shared secrets in the current switches database:

1. Log in to the switch as admin.
2. On a switch running Fabric OS v4.x, type **secAuthSecret --show**; on a switch running Fabric OS v3.x, type **secAuthSecret "--show"**.

   The output displays the WWN, domain ID and name (if known) of the switches with defined shared secrets, for example:

```
WWN                     DId    Name
-----------------------------------------------
10:00:00:60:69:80:07:52         Unknown
10:00:00:60:69:80:07:5c    1    switchA
```

To set shared secrets:

1. Login to the switch as admin
2. On a switch running Fabric OS v4.x, type **secAuthSecret --set**; on a switch running Fabric OS v3.x, type **secAuthSecret "--set"**.

This enters command interactive mode. The command returns a description of itself and needed input; then it loops through a sequence of switch specification, peer secret entry and local secret entry. To exit the loop, type **Enter** for the switch name.

```
switchA:admin> secAuthSecret --set

This command is used to set up secret keys for the DH-CHAP authentication.
The minimum length of a secret key is 8 characters and maximum 40
characters. Setting up secret keys does not initiate DH-CHAP
authentication. If switch is configured to do DH-CHAP, it is performed
whenever a port or a switch is enabled.

Warning: Please use a secure channel for setting secrets. Using
an insecure channel is not safe and may compromise secrets.

Following inputs should be specified for each entry.

1. WWN for which secret is being set up.
2. Peer secret: The secret of the peer that authenticates to peer.
3. Local secret: The local secret that authenticates peer.

Press Enter to start setting up shared secrets > <cr>

Enter WWN, Domain, or switch name (Leave blank when done):
10:20:30:40:50:60:70:80

Enter peer secret: <hidden>
Re-enter peer secret: <hidden>
Enter local secret: <hidden>
Re-enter local secret: <hidden>

Enter WWN, Domain, or switch name (Leave blank when done):
10:20:30:40:50:60:70:81

Enter peer secret: <hidden>
Re-enter peer secret: <hidden>
Enter local secret: <hidden>
Re-enter local secret: <hidden>

Enter WWN, Domain, or switch name (Leave blank when done): <cr>
Are you done? (yes, y, no, n): [no] y

Saving data to key store… Done.
```

Chapter

3

Creating Secure Fabric OS Policies

Secure Fabric OS policies make it possible to customize access to the fabric. The FCS policy is the only required policy; all other policies are optional.

To implement Secure Fabric OS policies:

- Determine which trusted switches to use as FCS switches to manage Secure Fabric OS.
- Enable secure mode in the fabric and specify the FCS switch and one or more backup FCS switches. This automatically creates the FCS policy.
- Determine which additional Secure Fabric OS policies to implement in the fabric; then create and activate those policies. An access policy must be created for each management channel that are used.
- Verify that the Secure Fabric OS policies are operating as intended. Testing a variety of scenarios to verify optimal policy settings is recommended. For troubleshooting information, refer to "Troubleshooting" on page 4-18.

Secure mode is enabled by the **secModeEnable** command. You can use optional arguments to the command to automate some policy-creation tasks. Refer to the *Fabric OS Command Reference Manual* for more information.

This chapter contains the following sections:

Default Fabric and Switch Accessibility

Following is the default fabric and switch access when secure mode is enabled but no additional Secure Fabric OS policies have been created:

- Switches:
  - Only the primary FCS switch can be used to make Secure Fabric OS changes.
  - Any SilkWorm switch can join the fabric, provided it is connected to the fabric, a SilkWorm 2000-series switch or later, and meets the minimum Secure Fabric OS requirements (such as a Security and Advanced Zoning licenses, and digital certificates).
  - All switches in the fabric can be accessed through a serial port.
  - All switches in the fabric that have front panels (SilkWorm 2000-series switches) can be accessed through the front panel.

Note

The SilkWorm 3016 switch has a different default user name than all other SilkWorm switches. As a result, use the **userRename** command to rename the SilkWorm 3016 default "USERID" user account to "admin" before connecting the switch to a secure fabric made up of other Brocade SilkWorm switches. Refer to the *Fabric OS Command Reference Manual* for more command details.

- Computer hosts and workstations:
  - Any host can access the fabric by using SNMP.
  - Any host can access any switch in the fabric by using the CLI (such as by sectelnet or Secure Shell).
  - Any host can establish an HTTP connection to any switch in the fabric.
  - Any host can establish an API connection to any switch in the fabric.
- Devices:
  - All device ports can access SES.
  - All devices can access the management server.
  - Any device can connect to any Fibre Channel port in the fabric.
- Zoning: node WWNs can be used for WWN-based zoning.

Enabling Secure Mode

Secure mode is enabled and disabled on a fabric-wide basis. Secure mode can be enabled and disabled as often as desired; however, all Secure Fabric OS policies, including the FCS policy, are deleted each time secure mode is disabled, and they must be re-created the next time it is enabled. The Secure Fabric OS database can be backed up using the **configUpload** command. For more information about this command, refer to the *Fabric OS Command Reference Manual*.

Secure mode is enabled using the **secModeEnable** command. This command must be entered through a sectelnet, Secure Shell, or serial connection to the switch designated as the primary FCS switch. The command fails if any switch in the fabric is not capable of enforcing Secure Fabric OS policies. If the primary FCS switch fails to participate in the fabric, the role of the primary FCS switch moves to the next available switch listed in the FCS policy.

The **secModeEnable** command performs the following actions:

- Creates and activates the FCS policy.
- Distributes the policy set (initially consisting of only the FCS policy) to all switches in the fabric.
- Activates and distributes the local zoning configurations.
- Fastboots any switches needing a reboot to bring the fabric up in secure mode. (Switches running Fabric OS v3.2.0 and v4.4.0 do not need to be rebooted to enable secure mode.)

Note

After running **secModeEnable** from a switch with Fabric OS v3.2.0 or v4.4.0, switches with previous OS versions reboot. Wait until the reboot of those switches completes, and then run **secFabricShow** to verify that all switches in the fabric are in a "Ready" state before running any commands that change security policies, passwords, or SNMP.

Depending on whether optional arguments are specified or not, the command might also request new passwords for secure mode.

By default: the only policy created is the FCS policy; this policy is implemented; no other Secure Fabric OS-related changes occur to the fabric. Other Secure Fabric OS policies can be created after the fastboots are complete.

Caution

Placing the two switches from the same SilkWorm 12000 or placing the two switches of a two-domain SilkWorm 24000 in separate fabrics is not supported if secure mode is enabled on one or both switches.

The following restrictions apply when secure mode is enabled:

- Standard telnet cannot be used after secure mode is enabled; however, sectelnet can be used as soon as a digital certificate is installed on the switch. Secure Shell can be used at any time; however, telnet sessions opened prior to issuing **secModeEnable** remain open if secure mode is enabled using the option to preserve passwords. If telnet is completely prohibited, the telnet protocol should be disabled on each switch, using the **configure** command, prior to enabling secure mode.
- A number of commands can only be entered from the FCS switches. Refer to "Command Restrictions in Secure Mode" on page A-4 for a list of these commands.

- If downloading a configuration to the switch:
  - Download the configuration to the primary FCS switch. A configuration downloaded to a backup FCS switch or non-FCS switch is overwritten by the next fabric-wide update from the primary FCS switch.
  - If the configdownload file contains an RSNMP policy, it must also contain a WSNMP policy.
  - The defined policy set in the configdownload file must have the following characteristics:
    - The defined policy set must exist.
    - The FCS policy must be the first policy.
    - The FCS policy must have at least one switch in common with the current defined FCS policy in the fabric.
  - The active policy set in the configdownload file must have the following characteristics:
    - The active policy set must exist.
    - The FCS policy must be the first policy.
    - The FCS policy must be identical to the active FCS policy in the fabric.

Note

If any part of the configuration download process fails, resolve the source of the problem and repeat the **configDownload** command. For information about troubleshooting the configuration download process, refer to the *Fabric OS Procedures Guide*.

After **configDownload**, the policy database might require up to 8 minutes to download.

For information about displaying the existing Secure Fabric OS policies, see "Displaying Individual Secure Fabric OS Policies" on page 4-3.

Note

Enabling secure mode fastboots all Fabric OS v2.6.x switches in the fabric.

To enable secure mode in the fabric:

1. Ensure that all switches in the fabric have the following:
   - Fabric OS v2.6.2, v3.2.0, or v4.4.0
   - An activated Secure Fabric OS license
   - An activated Advanced Zoning license
   - Digital certificate
2. Ensure that any zoning configuration downloads have completed on all switches in the fabric. For information specific to zoning, refer to the *Advanced Zoning User's Guide* for Fabric OS v2.6.x and v3.2.0 or the *Fabric OS Procedures Guide* for Fabric OS v4.4.0.
3. Open a sectelnet or Secure Shell connection to the switch that will be the primary FCS switch. The login prompt is displayed.

Note

Most Secure Fabric OS commands must be executed on the primary FCS switch. The **secModeEnable** command must be entered through a sectelnet or Secure Shell session.

4. Log in to the switch as admin.

5. Terminate any other sectelnet or Secure Shell sessions in the fabric (when using the **secModeEnable** command, no other sessions should be active) and ensure that any other commands entered in the current session have completed.
6. Use the **secModeEnable** command to enable secure mode.

   Several optional arguments are available. This step illustrates three forms of the command:

   - Type **secmodeenable --quickmode**.

     Note

     The **secModeEnable** command might fail if a switch running Fabric OS v2.6.x is in the fabric. Fabric OS v2.6.x supports a maximum security database size of 16 Kb. If you use **--lockdown=dcc** or **--quickmode**, a security database greater than 16 Kb can be created. Enable security successful using other **secModeEnable** operands. Refer to the *Fabric OS Command Reference Manual* for detailed command and operand information.

     Do not use the **secModeEnable --currentpwd** command until the passwords are changed from the factory defaults by answering the password prompts during the login.

   - Type **secmodeenable**.

     This version invokes the command's interactive mode; then, identify each FCS switch at the prompts, (as shown in the next example). Press **Enter** with no data to end the FCS list.

   - Type **secmodeenable "***fcsmember;...;fcsmember***"**.

     fcsmember is the domain ID, WWN, or switch name of the primary and backup FCS switches, with the primary FCS switch listed first.

   Refer to the *Fabric OS Command Reference Manual* for other forms of the **secModeEnable** command.

To enable secure mode using **--quickmode**:

```
switch: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:

 Secure mode is enabled.
```

To enable secure mode using **--lockdown=scc**, **--currentpwd**, and **--fcs** options:

```
switch:admin> secmodeenable --lockdown=scc --currentpwd --fcs "*"

 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:

 Secure mode is enabled.
```

The command requests active consent to the terms of the license, requests the identity of the FCS switches, and requests the new passwords required for secure mode.

7. Skip this step if you used the **--quickmode** or **--currentpwd** options; otherwise, type the following passwords at the prompts, using unique passwords that are different from the default values and contain between 8 and 40 alphanumeric characters:

   - Root password for the FCS switch
   - Factory password for the FCS switch
   - Admin password for the FCS switch
   - User password for the fabric
   - Admin password for the non-FCS switches

   Note

   The root and factory accounts are disabled on the non-FCS switches. If either of these logins is attempted on a non-FCS switch, an error message is displayed.

   For example, to enter passwords after enabling secure mode:

```
New FCS switch root password:
Re-enter new password:
New FCS switch factory password:
Re-enter new password:
New FCS switch admin password:
Re-enter new password:
New FCS switch user password:
Re-enter new password:
New Non FCS switch admin password:
Re-enter new password:
Saving passwd...done.
Saving Defined FMPS ...
done
Saving Active FMPS ...
done
Committing configuration...done.
Secure mode is enabled.
Saving passwd...done.
Rebooting...
```

   All passwords are saved. The command distributes the new FCS policy and passwords to all switches in the fabric, activates the local zoning configurations, and fastboots all Fabric OS 2.6.2 the switches in the fabric.

Note

Record the passwords and store them in a secure place. Recovering passwords might require significant effort and result in fabric downtime.

Modifying the FCS Policy

Only one FCS policy can exist, and it cannot be empty or deleted if secure mode is enabled. The FCS policy is named FCS_POLICY.

Changes made to the FCS policy are saved to permanent memory only after the changes have been saved or activated; they can be aborted later if desired (see “Managing Secure Fabric OS Policies” on page 3-24).

The FCS policy can be modified through any of the following methods:

- Using the **secPolicyFCSMove** command to change the position of a switch in the list, as described in "Changing the Position of a Switch Within the FCS Policy" on page 3-8
- Using the **secFCSFailover** command to fail over the primary FCS switch role to the backup FCS switch from which the command is entered, as described in "Failing Over the Primary FCS Switch" on page 3-9
- Using the **secPolicyAdd** command to add members, as described in "Adding a Member to an Existing Policy" on page 3-26
- Using the **secPolicyRemove** command to remove members, as described in "Removing a Member from a Policy" on page 3-27

Note

If the last FCS switch is removed from the fabric, secure mode remains enabled but no primary FCS switch is available. To specify a new primary FCS switch, enter the **secModeEnable** command again and specify the primary and backup FCS switches. This is the only instance in which the **secModeEnable** command can be entered when secure mode is already enabled.

The possible FCS policy states are shown in Table 3-1.

Table 3-1 FCS Policy States

Policy State	Characteristics
No policy, or policy with no entries	Not possible if secure mode is enabled.
Policy with one entry	A primary FCS switch is designated but there are no backup FCS switches. If the primary FCS switch becomes unavailable for any reason, the fabric is left without an FCS switch.
Policy with multiple entries	A primary FCS switch and one or more backup FCS switches are designated. If the primary FCS switch becomes unavailable, the next switch in the list becomes the primary FCS switch.

You might not want to put Fabric OS v2.6.x switches in the FCS policy if your primary FCS switch is running Fabric OS v3.2.0 or v4.4.0 and using multiple user accounts (MUA) because Fabric OS v2.6.x does not support MUA. Refer to the *Fabric OS Procedures Guide* for more information on MUA.

Changing the Position of a Switch Within the FCS Policy

The **secPolicyFCSMove** command can be used to change the order in which switches are listed in the FCS policy. The list order determines which backup FCS switch becomes the primary FCS switch if the current primary FCS switch fails.

To modify the order of FCS switches:

1. From a sectelnet or Secure Shell session, log in to the primary FCS switch as admin.
2. Type **secPolicyShow "Defined", "FCS_POLICY"**.

   This displays the WWNs of the current primary FCS switch and backup FCS switches.

3. Type **secPolicyFCSMove**, then provide the current position of the switch in the list and the desired position at the prompts.

   Alternatively, enter **secPolicyFCSMove "***From, To***"**. *From* is the current position in the list of the FCS switch and *To* is the desired position in the list for this switch.

   For example, to move a backup FCS switch from position 2 to position 3 in the FCS list, using interactive mode:

```
primaryfcs:admin> secpolicyfcsmove
Pos Primary WWN                   DId     swName.
================================================
1   Yes     10:00:00:60:69:10:02:181      switch5.
2   No      10:00:00:60:69:00:00:5a2      switch60.
3   No      10:00:00:60:69:00:00:133      switch73.
Please enter position you'd like to move from : (1..3) [1] 2
Please enter position you'd like to move to : (1..3) [1] 3
_____________________________________________________
DEFINED POLICY SET
FCS_POLICY
Pos Primary WWN                   DId swName
_____________________________________________________
1   Yes     10:00:00:60:69:10:02:181  switch5.
2   No      10:00:00:60:69:00:00:133  switch73.
3   No      10:00:00:60:69:00:00:5a2  switch60.
_____________________________________________________
```

4. Type **secPolicyActivate**.

Failing Over the Primary FCS Switch

The **secFCSFailover** command is used to fail over the role of the primary FCS switch to the backup FCS switch from which the command is entered. This can be used to recover from events such as a lost Ethernet connection to the primary FCS switch.

In addition to failing over the role of the primary FCS switch, this command moves the new primary FCS switch to the top of the list in the FCS policy.

Note

Disabling a switch or removing it from the fabric does not change the order of the FCS policy.

Before issuing the **secFCSFailover** command, ensure no other operations are simultaneously performed that cause the fabric to reconfigure; for example, **haFailover** or another **secFCSFailover**. Otherwise, **secFCSFailover** might hang.

During FCS failover to a backup FCS switch, all transactions in process on the current primary FCS switch are aborted, and any further transactions are blocked until failover is complete.

To fail over the primary FCS switch:

1. Log in as admin to the current primary FCS switch from a sectelnet or SSH session.
1. If desired, view the current FCS list typing **secPolicyShow "active","FCS_POLICY"**.

   For example, type **secPolicyShow** from the current primary FCS switch, “fcsswitcha”:

```
fcsswitcha:admin> secpolicyshow "active","FCS_POLICY"
_____________________________________________________
ACTIVE POLICY SET
FCS_POLICY
Pos Primary WWN                    DId     swName
_____________________________________________________
1   Yes     10:00:00:00:00:00:11:1c1      fcsswitcha
2   No      10:00:00:00:00:00:22:2c2      fcsswitchb
3   No      10:00:00:00:00:00:33:3c3      fcsswitchc
```

2. From a sectelnet or SSH session, log in as admin to the backup FCS switch to be designated as the new primary FCS switch and type **secFCSFailover**.

   For example, type **secFCSFailover** from the backup FCS switch “fcsswitchc” and then type **secPolicyShow**:

```
fcsswitchc:admin> secfcsfailover
This switch is about to become the primary FCS switch.
All transactions of the current Primary FCS switch will be aborted.
ARE YOU SURE (yes, y, no, n): [no] y
WARNING!!!
The FCS policy of Active and Defined Policy sets have been changed.
Review them before you issue secpolicyactivate again.

fcsswitchc:admin> secpolicyshow "active","FCS_POLICY"
_____________________________________________________
ACTIVE POLICY SET
FCS_POLICY
Pos PrimaryWWN                     DId     swName
_____________________________________________________
1   Yes     10:00:00:00:00:00:33:3c3      fcsswitchc
2   No      10:00:00:00:00:00:11:1c1      fcsswitcha
3   No      10:00:00:00:00:00:22:2c2      fcsswitchb
```

   The backup FCS switch becomes the new primary FCS switch, and the FCS policy is modified so that the new and previous primary FCS switches have exchanged places.

Creating Secure Fabric OS Policies Other Than the FCS Policy

The FCS policy is automatically created when secure mode is enabled; other Secure Fabric OS policies can be created after secure mode is enabled. (Using the quickmode or lockdown options to the **secModeEnable** command also creates an SCC policy and a DCC policy.) The member list of each policy determines the devices or switches to which the policy applies.

If a policy does not exist, then no Secure Fabric OS controls are in effect for that aspect of the fabric. If a policy exists but has no members, that functionality is disabled for all switches in the fabric. As soon as a policy has been created, that functionality becomes disabled for all switches except the members listed in the policy.

Note

Save policy changes frequently; changes are lost if the switch is rebooted before the changes are saved.

Each supported policy is identified by a specific name, and only one policy of each type can exist (except for DCC policies). The policy names are case sensitive and must be entered in all uppercase. Multiple DCC policies can be created using the naming convention DCC_POLICY*_nnn*, with *nnn* representing a unique string.

Note

Uploading and saving a copy of the Secure Fabric OS database after creating the desired Secure Fabric OS policies is strongly recommended. The **configUpload** command can be used to upload a copy of the configuration file, which contains all the Secure Fabric OS information. For more information about this command, refer to the *Fabric OS Command Reference Manual*.

Policy members can be specified by IP address, device port WWN, switch WWN, domain IDs, or switch names, depending on the policy. The valid methods for specifying policy members are listed in Table 3-2.

Table 3-2 Valid Methods for Specifying Policy Members

Policy Name	IP address	Device Port WWN	Switch WWN	Domain IDs	Switch names
FCS_POLICY	No	No	Yes	Yes	Yes
MAC Policies:					
RSNMP_POLICY	Yes	No	No	No	No
WSNMP_POLICY	Yes	No	No	No	No
TELNET_POLICY	Yes	No	No	No	No
HTTP_POLICY	Yes	No	No	No	No
API_POLICY	Yes	No	No	No	No
SES_POLICY	No	Yes	No	No	No
MS_POLICY	No	Yes	No	No	No
SERIAL_POLICY	No	No	Yes	Yes	Yes
FRONTPANEL_POLICY	No	No	Yes	Yes	Yes
OPTIONS_POLICY	For information about valid input, refer to "Creating an Options Policy" on page 3-20.				
DCC_POLICY_nnn	No	Yes	Yes	Yes	Yes
SCC_POLICY	No	No	Yes	Yes	Yes

Note

If IP addresses are used, "0" used for an octet indicates that any number can be matched for that octet. For example, 192.168.11.0 allows access for all IP devices in the range 192.168.11.0 through 192.168.11.255. If domain IDs or switch names are used, the corresponding switches must be in the fabric for the command to succeed.

Creating a MAC Policy

Management Access Control (MAC) policies can be used to restrict the following management access to the fabric:

- Access by hosts using SNMP, telnet/sectelnet/Secure Shell, HTTP, API
- Access by device ports using SCSI Enclosure Services (SES) or management server
- Access through switch serial ports and front panels

The individual MAC policies and how to create them are described in the following sections. By default, all MAC access is allowed; no MAC policies exist until they are created.

Note

An empty MAC policy blocks all access through that management channel. When creating policies, ensure that all desired members are added to each policy.

Providing fabric access to proxy servers is strongly discouraged. When a proxy server is included in a MAC policy for IP-based management, such as the HTTP_POLICY, all IP packets leaving the proxy server appear to originate from the proxy server. This could result in allowing any hosts that have access to the proxy server to access the fabric.

Serial, Telnet, and API violations that occur on the standby CP of a chassis-based platform do not display on the active CP. Also, during an HA failover, security violation counters and events are not propagated from the former active CP to the current active CP.

Creating an SNMP Policy

Read and write SNMP policies can be used to specify which SNMP hosts are allowed read and write access to the fabric. The SNMP hosts must be identified by IP address.

- RSNMP_POLICY (read access)
  Only the specified SNMP hosts can perform read operations to the fabric.
- WSNMP_POLICY (write access)
  Only the specified SNMP hosts can perform write operations to the fabric.

Any host granted write permission by the WSNMP policy is automatically granted read permission by the RSNMP policy.

How to create SNMP policies is described in "To create an SNMP policy:" on page 3-14.

Table 3-3 lists the expected read and write behaviors resulting from combinations of the RSNMP and WSNMP policies.

Table 3-3 Read and Write Behaviors of SNMP Policies

RSNMP Policy	WSNMP Policy	Read Result	Write Result
Nonexistent	Nonexistent	Any host can read	Any host can write
Nonexistent	Empty	Any host can read	No host can write
Nonexistent	Host B in policy	Any host can read	Only B can write
Empty	Nonexistent	This combination is not supported. If the WSNMP policy is not defined, the RSNMP policy cannot be created.	
Empty	Empty	No host can read	No host can write

Table 3-3 Read and Write Behaviors of SNMP Policies (Continued)

RSNMP Policy	WSNMP Policy	Read Result	Write Result
Empty	Host B in policy	Only B can read	Only B can write
Host A in policy	Nonexistent	This combination is not supported. If the WSNMP policy is not defined, the RSNMP policy cannot be created.	
Host A in policy	Empty	Only A can read	No host can write
Host A in policy	Host B in policy	A and B can read	Only B can write

To create an SNMP policy:

1. From a sectelnet or Secure Shell session, log in to the primary FCS switch as admin.
2. Type **secPolicyCreate "***policy_name***", "***member;...;member***"**.

   Policy name is WSNMP_POLICY or RSNMP_POLICY. *Member* is one or more IP addresses in dot-decimal notation. "0" can be entered in an octet to indicate that any number can be matched in that octet.

   For example, to create an WSNMP and an RSNMP policy to only allow IP addresses that match 192.168.5.0 read and write access to the fabric:.

```
primaryfcs:admin> secpolicycreate "WSNMP_POLICY", "192.168.5.0"
WSNMP_POLICY has been created.

primaryfcs:admin> secpolicycreate "RSNMP_POLICY", "192.168.5.0"
RSNMP_POLICY has been created.
```

3. To save or activate the new policy, enter either the **secPolicySave** or the **secPolicyActivate** command.

   If neither of these commands is entered, the changes are lost when the session is logged out. For more information about these commands, refer to "Saving Changes to Secure Fabric OS Policies" on page 3-25 and "Activating Changes to Secure Fabric OS Policies" on page 3-26.

Telnet Policy

The Telnet policy can be used to specify which workstations can use sectelnet or Secure Shell to connect to the fabric. The policy is named TELNET _POLICY and contains a list of the IP addresses for the trusted workstations (workstations that are in a physically secure area).

When a SilkWorm 12000 or 24000 director is in secure mode, sectelnet or SSH sessions cannot be opened to the active CP. This prevents potential violation of the Telnet policy, since the active CP can be used to access either of the logical switches on the SilkWorm 12000, or a two-domain SilkWorm 24000. However, sectelnet or SSH sessions can be established to the IP addresses of the logical switches and to the standby CP, if allowed by the Telnet policy. If the active CP fails over, any sectelnet or SSH sessions to the standby CP are automatically terminated when the standby CP becomes the active CP.

How to create a Telnet policy is described after Table 3-4.

Note

Static host IP addresses are required to implement the Telnet policy effectively. Do *not* use DHCP for hosts that are in the TELNET_POLICY, because as soon as the IP addresses change, the hosts will no longer be able to access the fabric. Restricting output (such as placing a session on "hold" by use of a command or keyboard shortcut) is not recommended.

This policy pertains to sectelnet and Secure Shell. It does not pertain to telnet access, because telnet is not available in secure mode. Use sectelnet as soon as a digital certificate is installed on the switch.

Note

An empty TELNET_POLICY blocks all telnet access. To prevent this, keep one or more members in the Telnet policy. If an empty Telnet policy is absolutely required, leave a meaningful entry in the API, HTTP, or SERIAL policies (or do not create these policies) to ensure that some form of management access is available to the switch. To restrict CLI access over the network to Secure Shell, disable telnet as described in "Telnet" on page 1-2.

The possible Telnet policy states are shown in Table 3-4.

Table 3-4 Telnet Policy States

Policy State	Description
No policy	Any host can connect by sectelnet or SSH to the fabric.
Policy with no entries	No host can connect by sectelnet or SSH to the fabric.
Policy with entries	Only specified hosts can connect by sectelnet or SSH to the fabric.

To create a Telnet policy:

1. From a sectelnet or Secure Shell session, log in to the primary FCS switch as admin.
2. Type **secPolicyCreate "***policy_name***", "***member;...;member***"**.

   Policy_name is TELNET_POLICY. *Member* is one or more IP addresses in dot-decimal notation. "0" can be entered in an octet to indicate that any number can be matched in that octet.
3. To save or activate the new policy, enter either the **secPolicySave** or the **secPolicyActivate** command.

   If neither of these commands is entered, the changes are lost when the session is logged out. For more information about these commands, refer to "Saving Changes to Secure Fabric OS Policies" on page 3-25 and "Activating Changes to Secure Fabric OS Policies" on page 3-26.

   For example, to create a Telnet policy to allow anyone on network 192.168.5.0 (where 0 can be any number) to access the fabric through a sectelnet or Secure Shell session:

```
primaryfcs:admin> secpolicycreate "TELNET_POLICY", "192.168.5.0"
TELNET_POLICY has been created.
```

HTTP Policy

The HTTP policy can be used to specify which workstations can use HTTP to access the fabric. This is useful for applications that use Internet browsers, such as Web Tools.

The policy is named HTTP_POLICY and contains a list of IP addresses for devices and workstations that are allowed to establish HTTP connections to the switches in the fabric.

How to create an HTTP policy is described in after Table 3-5 which shows the possible HTTP policy states.

Table 3-5 HTTP Policy States

Policy State	Characteristics
No policy	All hosts can establish an HTTP/HTTPS connection to any switch in the fabric.
Policy with no entries	No host can establish an HTTP/HTTPS connection to any switch in the fabric. **Note:** An empty policy causes the message "The page cannot be displayed" to display when HTTP/HTTPS access is attempted.
Policy with entries	Only specified hosts can establish an HTTP/HTTPS connection to any switch in the fabric.

To create an HTTP policy:

1. From a sectelnet or Secure Shell session, log in to the primary FCS switch as admin.
2. Type **secPolicyCreate "***policy_name***", "***member;...;member***"**.

   Policy_name is HTTP_POLICY. *Member* is one or more IP addresses in dot-decimal notation. "0" can be entered in an octet to indicate that any number can be matched in that octet.
3. To save or activate the new policy, enter either the **secPolicySave** or the **secPolicyActivate** command.

   If neither of these commands is entered, the changes are lost when the session is logged out. For more information about these commands, see "Saving Changes to Secure Fabric OS Policies" on page 3-25 and "Activating Changes to Secure Fabric OS Policies" on page 3-26.

   For example, to create an HTTP policy to allow anyone on the network with IP address of 192.168.5.0 (where "0" can be any number) to establish an HTTP connection to any switch in the fabric:.

```
primaryfcs:admin> secpolicycreate "HTTP_POLICY", "192.168.5.0"
HTTP_POLICY has been created.
```

API Policy

The API policy can be used to specify which workstations can use API to access the fabric and which ones can write to the primary FCS switch.

The policy is named API_POLICY and contains a list of the IP addresses that are allowed to establish an API connection to switches in the fabric.

How to create an API policy is described after Table 3-6 which shows the possible API policy states.

Table 3-6 API Policy States

Policy State	Characteristics
No policy	All workstations can establish an API connection to any switch in the fabric.
Policy with no entries	No host can establish an API connection to any switch in the fabric.
Policy with entries	Only specified hosts can establish an API connection to any switch in the fabric, and write operations can only be performed on the primary FCS switch.

To create an API policy:

1. From a sectelnet or Secure Shell session, log in to the primary FCS switch as admin.
2. Type **secPolicyCreate "***policy_name***", "***member;...;member***"**.

   Policy_name is API_POLICY. *Member* is one or more IP addresses in dot-decimal notation. "0" can be entered in an octet to indicate that any number can be matched in that octet.
3. To save or activate the new policy, enter either the **secPolicySave** or the **secPolicyActivate** command.

   If neither of these commands is entered, the changes are lost when the session is logged out. For more information about these commands, refer to "Saving Changes to Secure Fabric OS Policies" on page 3-25 and "Activating Changes to Secure Fabric OS Policies" on page 3-26.

   For example, to create an API policy to allow anyone on the network with an IP address of 192.168.5.0 (where "0" can be any number) to establish an API connection to any switch in the fabric:

```
primaryfcs:admin> secpolicycreate "API_POLICY", "192.168.5.0"
API_POLICY has been created.
```

SES Policy

The SES policy can be used to restrict which devices can be managed by SES commands. The policy is named SES_POLICY and contains a list of device port WWNs that are allowed to access SES and from which SES commands are accepted and acted upon.

If secure mode is enabled, the SES client must be directly attached to the primary FCS switch. Then the SES client can be used to manage all the switches in the fabric through the SES product for SilkWorm switches. Refer to the *SES User's Guide* for more information.

The current SES implementation does not support the SES commands **Read Buffer** or **Write Buffer** for remote switches. To direct these commands to a switch that is not the primary FCS switch, designate that switch as the primary FCS switch and attach the SES client directly to it.

How to create an SES policy is described after Table 3-7, which shows the possible SES policy states.

Table 3-7 SES Policy States

Policy State	Characteristics
No policy	All device ports can access SES.
Policy with no entries	No device port can access SES.
Policy with entries	The specified devices can access SES.

To create an SES policy:

1. From a sectelnet or Secure Shell session, log in to the primary FCS switch as admin.
2. Type **secPolicyCreate "***policy_name***", "***member;...;member***"**.

   Policy_name is SES_POLICY. *Member* is a device port WWN.
3. To save or activate the new policy, enter either **secPolicySave** or **secPolicyActivate**.

   If neither of these commands is entered, the changes are lost when the session is logged out. For more information about these commands, refer to "Saving Changes to Secure Fabric OS Policies" on page 3-25 and "Activating Changes to Secure Fabric OS Policies" on page 3-26.

   For example, to create an SES_POLICY that allows access through a device that has a WWN of 12:24:45:10:0a:67:00:40:

```
primaryfcs:admin> secpolicycreate "SES_POLICY", "12:24:45:10:0a:67:00:40"
SES_POLICY has been created.
```

Management Server Policy

The Management Server policy can be used to restrict which devices can be accessed by the management server. Fabric configuration and control functions can be performed only by requesters that are directly connected to the primary FCS switch. The policy is named MS_POLICY and contains a list of device port WWNs for which the management server implementation in Fabric OS (designed according to FC-GS-3 standard) accepts and acts on requests.

How to create a Management Server policy is described after Table 3-8, which shows the possible Management Server policy states.

Table 3-8 Management Server Policy States

Policy State	Characteristics
No policy	All devices can access the management server.
Policy with no entries	No devices can access the management server.
Policy with entries	Specified devices can access the management server.

To create a Management Server policy:

1. From a sectelnet or Secure Shell session, log in to the primary FCS switch as admin.
2. Type **secPolicyCreate "***policy_name***", "***member;...;member***"**.

   Policy_name is MS_POLICY. *Member* is a device WWN.

3. To save or activate the new policy, enter either **secPolicySave** or **secPolicyActivate**.

   If neither of these commands is entered, the changes are lost when the session is logged out. For more information about these commands, see "Saving Changes to Secure Fabric OS Policies" on page 3-25 and "Activating Changes to Secure Fabric OS Policies" on page 3-26.

   For example, to create an MS_POLICY that allows access through a device that has a WWN of 12:24:45:10:0a:67:00:40:

```
primaryfcs:admin> secpolicycreate "MS_POLICY", "12:24:45:10:0a:67:00:40"
MS_POLICY has been created.
```

Serial Port Policy

The Serial Port policy can be used to restrict which switches can be accessed by serial port. The policy is named SERIAL_POLICY and contains a list of switch WWNs, domain IDs, or switch names for which serial port access is enabled.

The serial policy is checked before the account login is accepted. If the Serial Port Policy exists and the switch is not included in the policy, the session is terminated.

How to create a Serial Port policy is described after Table 3-9, which displays the possible serial port policy states.

Table 3-9 Serial Port Policy States

Policy State	Characteristics
No policy	All serial ports of the switches in the fabric are enabled.
Policy with no entries	All serial ports of the switches in the fabric are disabled.
Policy with entries	Only specified switches can be accessed through the serial ports.

To create a Serial Port policy:

1. From a sectelnet or Secure Shell session, log in to the primary FCS switch as admin.
2. Type **secPolicyCreate "***policy_name***", "***member;...;member***"**.

   Policy_name is SERIAL_POLICY. *Member* is a switch WWN, domain ID, or switch name. If a domain ID or switch name is used to specify a switch, the associated switch must be present in the fabric for the command to succeed.
3. To save or activate the new policy, enter either **secPolicySave** or **secPolicyActivate**.

   If neither of these commands is entered, the changes are lost when the session is logged out. For more information about these commands, see "Saving Changes to Secure Fabric OS Policies" on page 3-25 and "Activating Changes to Secure Fabric OS Policies" on page 3-26.

   For example, to create a SERIAL_POLICY that allows serial port access to a switch that has a WWN of 12:24:45:10:0a:67:00:40:

```
primaryfcs:admin> secpolicycreate "SERIAL_POLICY", "12:24:45:10:0a:67:00:40"
SERIAL_POLICY has been created.
```

Front Panel Policy

The Front Panel policy can be used to restrict which switches can be accessed through the front panel. This policy only applies to SilkWorm 2800 switches, since no other switches contain front panels. The policy is named FRONTPANEL_POLICY and contains a list of switch WWNs, domain IDs, or switch names for which front panel access is enabled.

How to create a Front Panel policy is described after Table 3-10, which displays the possible Front Panel policy states.

Table 3-10 Front Panel Policy States

Policy State	Characteristics
No policy	All the switches in the fabric have front panel access enabled.
Policy with no entries	All the switches in the fabric have front panel access disabled.
Policy with entries	Only specified switches in the fabric have front panel access enabled.

To create a Front Panel policy:

1. From a sectelnet or Secure Shell session, log in to the primary FCS switch as admin.
2. Type **secPolicyCreate "***policy_name***", "***member;...;member***"**.

   Policy_name is FRONTPANEL_POLICY. *Member* is a switch WWN, domain ID, or switch name. If a domain ID or switch name is used to specify a switch, the associated switch must be present in the fabric for the command to succeed.
3. To save or activate the new policy, enter either the **secPolicySave** or the **secPolicyActivate** command.

   If neither of these commands is entered, the changes are lost when the session is logged out. For more information about these commands, see "Saving Changes to Secure Fabric OS Policies" on page 3-25 and "Activating Changes to Secure Fabric OS Policies" on page 3-26.

   For example, to create a Front Panel policy to allow only domains 3 and 4 to use the front panel:

```
primaryfcs:admin> secpolicycreate "FRONTPANEL_POLICY", "3; 4"
FRONTPANEL_POLICY has been created.
```

Creating an Options Policy

The Options policy can be used to prevent the use of node WWNs to add members to zones. This policy is named OPTIONS_POLICY and has only one valid value, "NoNodeWWNZoning". Adding this value to the policy prevents use of Node WWNs for WWN-based zoning.

The use of node WWNs can introduce ambiguity because the node WWN might also be used for one of the device ports, as might be true with a host bus adapter (HBA). If the policy does not exist or is empty, node WWNs can be used for WWN-based zoning. Only one Options policy can be created. This policy cannot be used to control use of port WWNs for zoning.

By default, use of node WWNs is allowed; the Options policy does not exist until it is created by the administrator.

How to create an Options policy is described after Table 3-11, which displays the possible Options policy states.

Table 3-11 Options Policy States

Policy State	Characteristics
No policy	Node WWNs can be used for WWN-based zoning.
Policy with no entries	Node WWNs can be used for WWN-based zoning.
Policy with entries	Node WWNs cannot be used for WWN-based zoning.

To create an Options policy:

1. Log in to the primary FCS switch as admin from a sectelnet or Secure Shell session.
2. Type **secPolicyCreate "OPTIONS_POLICY", "NoNodeWWNZoning"**.
3. To save or activate the new policy, enter either the **secPolicySave** or the **secPolicyActivate** command.

   If neither of these commands is entered, the changes are lost when the session is logged out. For more information about these commands, refer to "Saving Changes to Secure Fabric OS Policies" on page 3-25 and "Activating Changes to Secure Fabric OS Policies" on page 3-26.
4. To apply the change to current transactions, disable the switch then re-enable it by entering the **switchDisable** and **switchEnable** commands. This stops any current traffic between devices that are zoned using node names.

```
primaryfcs:admin> secpolicycreate "OPTIONS_POLICY", "NoNodeWWNZoning"
OPTIONS_POLICY has been created.
```

Creating a DCC Policy

Multiple DCC policies can be used to restrict which device ports can connect to which switch ports. The devices can be initiators, targets, or intermediate devices such as SCSI routers and loop hubs. By default, all device ports are allowed to connect to all switch ports; no DCC policies exist until they are created by the administrator.

Each device port can be bound to one or more switch ports; the same device ports and switch ports might be listed in multiple DCC policies. After a switch port is specified in a DCC policy, it permits connections only from designated device ports. Device ports that are not specified in any DCC policies are allowed to connect only to switch ports that are not specified in any DCC policies.

Note

Some older private loop HBAs do not respond to port login from the switch and are not enforced by the DCC policy. However, this does not create a security problem because these HBAs cannot contact any device outside of their immediate loop.

DCC policies must follow the naming convention "DCC_POLICY_*nnn*," where *nnn* represents a unique string. To save memory and improve performance, one DCC policy per switch or group of switches is recommended.

Device ports must be specified by port WWN. Switch ports can be identified by the switch WWN, domain ID, or switch name followed by the port or area number. To specify an allowed connection, enter the device port WWN, a semicolon, and the switch port identification. Following are the possible methods of specifying an allowed connection:

- deviceportWWN;switchWWN (port or area number)
- deviceportWWN;domainID (port or area number)
- deviceportWWN;switchname (port or area number)

How to create a DCC policy is described after Table 3-12, which shows the possible DCC policy states.

Table 3-12 DCC Policy States

Policy State	Characteristics
No policy	Any device can connect to any switch port in the fabric.
Policy with no entries	Any device can connect to any switch port in the fabric. An empty policy is the same as no policy.
Policy with entries	If a device WWN is specified in a DCC policy, that device is only allowed access to the fabric if connected to a switch port listed in the same policy. If a switch port is specified in a DCC policy, it only permits connections from devices that are listed in the policy. Devices with WWNs that are not specified in a DCC policy are allowed to connect to the fabric at any switch ports that are not specified in a DCC policy. Switch ports and device WWNs may exist in multiple DCC policies.

Note
When a DCC violation occurs, the related port is automatically disabled and must be re-enabled using the **portEnable** command.

To create a DCC policy:

1. From a sectelnet or Secure Shell session, log in to the primary FCS switch as admin.
2. Type **secPolicyCreate "DCC_POLICY_***nnn***", "***member;...;member***"**.

   DCC_POLICY_nnn is the name of the DCC policy to be created; *nnn* is a string consisting of up to 19 alphanumeric or underscore characters to differentiate it from any other DCC policies. *Member* contains device or switch port information: *deviceportWWN;switch(port)*:

   - *deviceportWWN* is the WWN of the device port.
   - *switch* can be the switch WWN, domain ID, or switch name. The port can be specified by port or area number. Designating ports automatically includes the devices currently attached to those ports. The ports can be specified using any of the following syntax methods:

     (1-6) Selects ports 1 through 6.

     (*) Selects all ports on the switch.

     [*] Selects all ports and all devices attached to those ports.

     [3, 9] Selects ports 3 and 9 and all devices attached to those ports.

     [1-3, 9] Selects ports 1, 2, 3, 9, and all devices attached to those ports.

3. To save or activate the new policy, enter either the **secPolicySave** or the **secPolicyActivate** command.

   If neither of these commands is entered, the changes are lost when the session is logged out. For more information about these commands, see "Saving Changes to Secure Fabric OS Policies" on page 3-25 and "Activating Changes to Secure Fabric OS Policies" on page 3-26.

   For example, to create a DCC policy "DCC_POLICY_server" that includes device "11:22:33:44:55:66:77:aa" and port 1 and port 3 of switch domain 1:

```
primaryfcs:admin> secpolicycreate "DCC_POLICY_server",
"11:22:33:44:55:66:77:aa;1(1,3)"
DCC_POLICY_xxx has been created
```

   To create a DCC policy "DCC_POLICY_storage" that includes device port WWN "22:33:44:55:66:77:11:bb," all ports of switch domain 2, and all currently connected devices of switch domain 2:

```
primaryfcs:admin> secpolicycreate "DCC_POLICY_storage",
"22:33:44:55:66:77:11:bb;2[*]"
DCC_POLICY_xxx has been created
```

   To create a DCC policy "DCC_POLICY_abc" that includes device "33:44:55:66:77:11:22:cc" and ports 1-6 and port 9 of switch domain 3:

```
primaryfcs:admin> secpolicycreate "DCC_POLICY_abc", "33:44:55:66:77:11:22:cc;3(1-
6,9)"
DCC_POLICY_xxx has been created
```

   To create a DCC policy "DCC_POLICY_example" that includes devices 44:55:66:77:22:33:44:dd and 33:44:55:66:77:11:22:cc, ports 1-4 of switch domain 4, and all devices currently connected to ports 1-4 of switch domain 4:

```
primaryfcs:admin> secpolicycreate "DCC_POLICY_example",
"44:55:66:77:22:33:44:dd;33:44:55:66:77:11:22:cc;4[1-4]"
DCC_POLICY_xxx has been created
```

Creating an SCC Policy

The SCC policy is used to restrict which switches can join the fabric. Switches are checked against the policy each time secure mode is enabled, the fabric is initialized with secure mode enabled, or an E_Port-to-E_Port connection is made.

The policy is named SCC_POLICY, and accepts members listed as WWNs, domain IDs, or switch names. Only one SCC policy may be created.

By default, any switch is allowed to join the fabric; the SCC policy does not exist until it is created by the administrator.

Note

When an SCC policy is activated, any non-FCS switches in the fabric not included in the policy member list, will be segmented from the fabric.

The possible SCC policy states are shown in Table 3-13.

Table 3-13 SCC Policy States

Policy State	SCC Policy Enforcement
No policy specified	All switches may join the fabric.
Policy specified, but with no members	The SCC policy includes all FCS switches. All non-FCS switches are excluded. Only FCS switches may join the fabric.
Policy specified, with members	The SCC policy contains all FCS switches and any switches specified in the member list. Any non-FCS switches not explicitly specified are excluded. Only FCS switches and explicitly specified non-FCS switches may join the fabric.

To create an SCC policy:

1. Log in to the primary FCS switch as admin from a sectelnet or Secure Shell *session.*
2. Type **secPolicyCreate "SCC_POLICY", "***member;...;member***"**.

   Member indicates a switch that is permitted to join the fabric. Switches can be specified by WWN, domain ID, or switch name. An asterisk (*) can be entered to indicate all the switches in the fabric.
3. To save or activate the new policy, enter either the **secPolicySave** or the **secPolicyActivate** command.

   If neither of these commands is entered, the changes are lost when the session is logged out. For more information about these commands, see "Saving Changes to Secure Fabric OS Policies" on page 3-25 and "Activating Changes to Secure Fabric OS Policies" on page 3-26.

   For example, to create an SCC policy that allows switches that have domain IDs 2 and 4 to join the fabric:

```
primaryfcs:admin> secpolicycreate "SCC_POLICY", "2;4"
SCC_POLICY has been created
```

Managing Secure Fabric OS Policies

All Secure Fabric OS transactions must be performed through the primary FCS switch only, except for the **secTransAbort**, **secFCSFailover**, **secStatsReset**, and **secStatsShow** commands.

Multiple sessions can be created to the primary FCS switch from one or more hosts. However, the software allows only one Secure Fabric OS transaction at a time. If a second Secure Fabric OS transaction is started, it fails. The only secondary transaction that can succeed is the **secTransAbort** command.

All policy modifications are only saved in volatile memory until the changes are saved or activated.

The following functions can be performed on existing Secure Fabric OS policies:

- Saving Changes to Secure Fabric OS Policies

  Save changes to flash memory without actually implementing the changes within the fabric. This saved but inactive information is known as the "defined policy set."

- Activating Changes to Secure Fabric OS Policies

  Simultaneously save and implement all the policy changes made since the last time changes were activated. The activated policies are known as the "active policy set."

- Adding a Member to an Existing Policy

  Add one or more members to a policy. The aspect of the fabric covered by each policy is closed to access by all devices/switches that are not listed in that policy.

- Removing a Member from a Policy

  Remove one or more members from a policy. If all members are removed from a policy, that aspect of the fabric becomes closed to all access. The last member of the FCS_POLICY cannot be removed, because a primary FCS switch must be designated.

- Deleting a Policy

  Delete an entire policy; however, keep in mind that doing so opens up that aspect of the fabric to all access.

- Aborting All Uncommitted Changes

  Abort all the changes to the Secure Fabric OS policies since the last time changes were saved or activated.

- Aborting a Secure Fabric OS Transaction

  From any switch in the fabric, abort a Secure Fabric OS-related transaction that has become frozen (such as due to a failed host) and is preventing other Secure Fabric OS transactions.

Each of these tasks is described in the subsections that follow.

Saving Changes to Secure Fabric OS Policies

You can save changes to Secure Fabric OS policies without activating them by entering the **secPolicySave** command. This saves the changes to the defined policy set.

Note

Until the **secPolicySave** or **secPolicyActivate** command is issued, all policy changes are in volatile memory only and are lost if the switch reboots or the current session is logged out.

To save changes to the Secure Fabric OS policies without activating them:

1. From a sectelnet or Secure Shell session, log in to the primary FCS switch as admin.
2. Type the **secPolicySave** command.

```
primaryfcs:admin> secpolicysave
Committing configuration...done.
Saving Define FMPS ...
done
```

Activating Changes to Secure Fabric OS Policies

Changes to the Secure Fabric OS policies can be implemented using the **secPolicyActivate** command. This saves the changes to the active policy set and activates all policy changes since the last time the command was issued. Policies cannot be activated on an individual basis; all changes to the entire policy set are activated by the command.

Note

Until a **secPolicySave** or **secPolicyActivate** command is issued, all policy changes are in volatile memory only and are lost upon rebooting.

To activate changes to the Secure Fabric OS policies:

1. From a sectelnet or Secure Shell session, log in to the primary FCS switch as admin.
2. Type the **secPolicyActivate** command:

```
primaryfcs:admin> secpolicyactivate
About to overwrite the current Active data.
ARE YOU SURE (yes, y, no, n): [no] y
Committing configuration...done.
Saving Defined FMPS ...
done
Saving Active FMPS ...
done
```

Adding a Member to an Existing Policy

You can add members to policies by using the **secPolicyAdd** command. As soon as a policy has been created, the aspect of the fabric managed by that policy is closed to access by all devices that are not listed in the policy.

To add a member to an existing Secure Fabric OS policy:

1. From a sectelnet or Secure Shell session, log in to the primary FCS switch as admin.
2. Type **secPolicyAdd "***policy_name***", "***member;...;member***"**.

   Policy_name is the name of the Secure Fabric OS policy. *Member* is the item to be added to the policy, identified by device or switch IP address, switch domain ID, device or switch WWN, or switch name.
3. To implement the change immediately, enter the **secPolicyActivate** command.

   For example, to add a member to the MS_POLICY using the device port WWN:

```
primaryfcs:admin> secpolicyadd "MS_POLICY", "12:24:45:10:0a:67:00:40"
Member(s) have been added to MS_POLICY.
```

   To add an SNMP manager to WSNMP_POLICY:

```
primaryfcs:admin> secpolicyadd "WSNMP_POLICY", "192.168.5.21"
Member(s) have been added to WSNMP_POLICY.
```

To add two devices to the DCC policy, to attach domain 3 ports 1 and 3 (WWNs of devices are 11:22:33:44:55:66:77:aa and 11:22:33:44:55:66:77:bb):

```
primaryfcs:admin> secpolicyadd "DCC_POLICY_abc",
"11:22:33:44:55:66:77:aa;11:22:33:44:55:66:77:bb;3(1,3)"
```

Removing a Member from a Policy

If all the members are removed from a policy, that policy becomes closed to all access. The last member cannot be removed from the FCS_POLICY, because a primary FCS switch must be designated.

To remove a member from a Secure Fabric OS policy:

1. From a sectelnet or Secure Shell session, log in to the primary FCS switch as admin.
2. Type **secPolicyRemove "***policy_name***", "***member;...;member***"**.

   Policy_name is the name of the Secure Fabric OS policy. *Member* is the device or switch to be removed from the policy, identified by IP address, switch domain ID, device or switch WWN, or switch name.
3. To implement the change immediately, enter the **secPolicyActivate** command.

   For example, to remove a member that has a WWN of 12:24:45:10:0a:67:00:40 from MS policy:

```
primaryfcs:admin> secpolicyremove "MS_POLICY", "12:24:45:10:0a:67:00:40"
Member(s) have been removed from MS_POLICY.
```

Deleting a Policy

If an entire Secure Fabric OS policy is deleted, that aspect of the fabric becomes open to all access.

To delete a Secure Fabric OS policy:

1. From a sectelnet or Secure Shell session, log in to the primary FCS switch as admin.
2. Type **secPolicyDelete "***policy_name***"**.

   policy_name is the name of the Secure Fabric OS policy.
3. To implement the change immediately, enter the **secPolicyActivate** command.

Note
The FCS_POLICY cannot be deleted.

```
primaryfcs:admin> secpolicydelete "MS_POLICY"
About to delete policy MS_POLICY.
Are you sure (yes, y, no, n):[no] y
MS_POLICY has been deleted.
```

Aborting All Uncommitted Changes

You can use the **secPolicyAbort** command to abort all Secure Fabric OS policy changes that have not yet been saved. This function can only be performed from the primary FCS switch.

To abort all unsaved changes:

1. From a sectelnet or Secure Shell session, log in to the primary FCS switch as admin.
2. Type the **secPolicyAbort** command.

   All changes since the last time the **secPolicySave** or **secPolicyActivate** commands were entered are aborted.

```
primaryfcs:admin> secpolicyabort
Unsaved data has been aborted.
```

Aborting a Secure Fabric OS Transaction

You can use the **secTransAbort** command to abort a single Secure Fabric OS transaction from any switch in the fabric. This makes it possible to abort a transaction that has become frozen due to a failed host. If the switch itself fails, the transaction aborts by default. This command cannot be used to abort an active transaction.

To abort a Secure Fabric OS transaction:

1. From a sectelnet or Secure Shell session, log in to the primary FCS switch as admin.
2. Type the **secTransAbort** command.

   Any Secure Fabric OS transaction that was in process is aborted (except for the transaction of entering this command).

```
primaryfcs:admin> sectransabort
Transaction has been aborted.
```

Chapter

4

Managing Secure Fabric OS

Secure Fabric OS v2.6.2, v3.2.0, and v4.4.0 can be managed through Fabric Manager and sectelnet. In addition, Secure Shell is supported for Fabric OS v4.4.0. When secure mode is enabled for a fabric, all Secure Fabric OS administrative operations, all zoning commands, and some management server commands must be executed on the primary FCS switch. For a list of the commands and related restrictions, see "Secure Fabric OS Commands and Secure Mode Restrictions" on page A-1.

This chapter contains the following sections:

Viewing Secure Fabric OS Information

You can display the following Secure Fabric OS information:

- General Secure Fabric OS-related information about a fabric
- Secure Fabric OS policy sets (active and defined)
- Information about one or more specific Secure Fabric OS policies

For information about viewing the Secure Fabric OS statistics, see "Displaying and Resetting Secure Fabric OS Statistics" on page 4-5.

Displaying General Secure Fabric OS Information

You can use the **secFabricShow** command to display general Secure Fabric OS-related information about a fabric.

To display general Secure Fabric OS-related information:

1. Open a sectelnet or Secure Shell session to the primary FCS switch and log in as admin.
2. Type the **secFabricShow** command. The command displays the switches in the fabric and their status (Ready, Error, Busy, or NoResp, for no response from the switch).

```
primaryfcs:admin> secfabricshow
Role    WWN                     DId Status  Enet IP Addr    Name
==========================================================================
non-FCS 10:00:00:60:69:10:03:23   1 Ready   192.168.100.148 "nonfcs"
Backup  10:00:00:60:69:00:12:53   2 Ready   192.168.100.147 "backup"
Primary 10:00:00:60:69:22:32:83   3 Ready   192.168.100.135 "primaryfcs"
__________________________________________________________________________

Secured switches in the fabric: 3
```

Viewing the Secure Fabric OS Policy Database

Use the **secPolicyDump** command to display the Secure Fabric OS policy database, which consists of the active and defined policy sets. This command displays information without page breaks.

To view the Secure Fabric OS policy database:

1. From a sectelnet or Secure Shell session, log in to the primary FCS switch as admin.
2. Type **secpolicydump "***listtype***", "***policy_name***"**.

   Listtype is the type of Secure Fabric OS policy set. It can be **active**, **defined**, or an asterisk (*****), which displays both versions of the policy. If a list type is not entered, both versions of the Secure Fabric OS policy display. *Policy_name* is the name of the Secure Fabric OS policy. If you do not specify a policy name, the command displays all the policies in the specified policy set.

   If you do not specify any operands, the command displays all policies in both the active and defined policy sets.

For example, to display all policies in both active and defined policy sets:

```
primaryfcs:admin> secpolicydump
_____________________________________________________
                DEFINED POLICY SET
FCS_POLICY
Pos Primary WWN DId swName
_____________________________________________________
1 Yes 10:00:00:60:69:30:15:5c 1 primaryfcs
HTTP_POLICY
IpAddr
_____________________________________________________
192.155.52.0
_____________________________________________________
_____________________________________________________
                 ACTIVE POLICY SET
FCS_POLICY
Pos Primary WWN DId swName
_____________________________________________________
1 Yes 10:00:00:60:69:30:15:5c 1 primaryfcs
HTTP_POLICY
IpAddr
_____________________________________________________
192.155.52.0
192.155.53.1
192.155.54.2
192.155.55.3
_____________________________________________________
```

Displaying Individual Secure Fabric OS Policies

Use the **secPolicyShow** command to display information about one or more specified Secure Fabric OS policies. This command displays information, with page breaks.

To display information about a specific Secure Fabric OS policy:

1. From a sectelnet or Secure Shell session, log in to the primary FCS switch as admin.
2. Type **secpolicyshow "***listtype***", "***policy_name***"**.

   listtype is the type of Secure Fabric OS policy set. It can be **active**, **defined**, or an asterisk (*), which displays both versions of the specified policy. *policy_name* is the name of the Secure Fabric OS policy. If you do not specify a policy name, the command displays all the policies in the specified policy set.

   If you do not specify any operands, the command displays all policies in both the active and defined policy sets.

For example, to display all the policies in the defined policy set:

```
primaryfcs:admin> secpolicyshow "defined"
_____________________________________________________
               DEFINED POLICY SET

FCS_POLICY
   Pos    Primary WWN                    DId swName
   _____________________________________________________
     1    Yes     10:00:00:60:69:30:15:5c   1 primaryfcs

HTTP_POLICY
   IpAddr
   _____________________________________________________
   192.155.52.0
   192.155.53.1
   192.155.54.2
   192.155.55.3
   192.155.56.4


_____________________________________________________
```

To display the active version of the FCS policy:

```
primaryfcs:admin> secpolicyshow "active","FCS_POLICY"
_____________________________________________________
               ACTIVE POLICY SET

FCS_POLICY
   Pos    Primary WWN                    DId swName
   _____________________________________________________
     1    Yes     10:00:00:60:69:30:15:5c   1 primaryfcs


_____________________________________________________
```

Displaying Status of Secure Mode

Use the **secModeShow** command to determine whether secure mode is enabled.

To determine whether secure mode is enabled:

1. From a sectelnet or Secure Shell session, log in to the primary FCS switch as admin.
2. Type the **secModeShow** command. The command displays the status of secure mode, the version number and time stamp, and the list of switches in the FCS policy.

```
switch:admin> secmodeshow

    Secure Mode: ENABLED.
    Version Stamp: 9182, Wed Mar 13 16:37:01 2001.
    POS Primary WWN                   DId swName.
    ============================================
    1   Yes     10:00:00:60:69:00:00:5a 21 switch47.
    2   No      12:00:00:60:60:03:23:5b 5  switch12.
```

Table 4-1 identifies the information that displays if secure mode is enabled.

Table 4-1 Secure Mode Information

Table Heading	Indicates
Pos	Position of switch in FCS list
Primary	"Yes" if switch is primary FCS, "no" if not
WWN	WWN of each FCS switch
DId	Domain ID of each FCS switch
swName	Switch name of each FCS switch

Displaying and Resetting Secure Fabric OS Statistics

Secure Fabric OS provides several statistics regarding attempted policy violations. This includes events such as the following:

- A DCC policy exists that defines which devices are authorized to access which switch (port) combinations, and a device that is not listed in the policy tries to access one of the defined switch (port) combinations.
- An attempt is made to log in to an account with an incorrect password.

The statistics for all DCC policies are added together.

Note

Rebooting the switch resets all the statistics. Secure Fabric OS statistics can also be monitored through Fabric Watch.

Each statistic indicates the number of times the monitored event has occurred since the statistics were last reset (**secStatsReset** command). For the Telnet policy, this includes all the automated login attempts made by the sectelnet or Secure Shell client software, in addition to the actual attempts made by the user.

On dual-CP directors, statistics are maintained separately on each CP and are counted only on the active CP. If a director fails over from the active to the standby CP, statistics are not replicated to the standby CP.

The names of the Secure Fabric OS statistics and their definitions are provided in Table 4-2.

Table 4-2 Secure Fabric OS Statistics

Statistic	Definition
TELNET_POLICY	The number of attempted violations to the Telnet policy (includes automated attempts made by client software).
HTTP_POLICY	The number of attempted violations to the HTTP policy.
API_POLICY	The number of attempted violations to the API policy (includes automated attempts made by client software).
RSNMP_POLICY	The number of attempted violations to the RSNMP policy.
WSNMP_POLICY	The number of attempted violations to the WSNMP policy.
SES_POLICY	The number of attempted violations to the SES policy.
MS_POLICY	The number of attempted violations to the MS policy.
SERIAL_POLICY	The number of attempted violations to the Serial policy.
FRONTPANEL_POLICY	The number of attempted violations to the Front Panel policy.
SCC_POLICY	The number of attempted violations to the SCC policy.
DCC_POLICY	The number of attempted violations to the DCC policy. **Note:** Fabric OS v4.4.0 increases the counter by 1 for each drive in a JBOD; Fabric OS v3.2.0 increases the counter by 1 for the entire JBOD.
LOGIN	The number of invalid login attempts.
INVALID_TS (invalid timestamps)	A received packet has a time stamp that differs from the time of the receiving switch by more than the maximum allowed difference.
INVALID_SIGN (invalid signatures)	A received packet has a bad signature.
INVALID_CERT (invalid certificates)	A received certificate is not properly signed by the root CA of the receiving switch.
AUTH_FAIL (SLAP* failures)	The switch received a SLAP that it could not verify, possibly due to bad certificates, bad signature, the other side not performing SLAP, or SLAP packets that were received out of sequence. This counter is not advanced if SLAP protocol does not complete, which can happen when a switch that does not have secure mode enabled is attached to a switch that does.
SLAP_BAD_PKT (SLAP* bad packets)	SLAP packets are received with a bad transaction ID.

Table 4-2 Secure Fabric OS Statistics (Continued)

Statistic	Definition
TS_OUT_SYNC (TS out of synchronization)	The time server is out of synchronization with the primary FCS switch.
NO_FCS (no fabric configuration server)	The number of times the switch has simultaneously lost contact with all the switches in the FCS list.
INCOMP_DB (incompatible Secure Fabric OS database)	Secure Fabric OS databases are incompatible; might be due to different version numbers, time stamps, FCS policies, or secure mode status.
ILLEGAL_CMD (illegal command)	The number of times a command is issued on a switch where it is not allowed (such as entering **secmodedisable** on a non-FCS switch).

* *SLAP (Switch Link Authentication Protocol) is the switch-to-switch authentication process.*

Displaying Secure Fabric OS Statistics

Use the **secStatsShow** command to display statistics for one or all Secure Fabric OS policies, depending on the operand entered. This command can only be issued from the primary FCS switch if the "list" operand is specified. If the "list" operand is not specified, this command can be entered from any switch in the fabric.

Note

On dual-CP directors, statistics are maintained separately on each CP and are counted only on the active CP. If a director fails over from the active to the standby CP, statistics are not replicated to the standby CP.

To display Secure Fabric OS statistics:

1. Log in to the primary FCS switch as admin from a sectelnet or Secure Shell session.
2. Type **secStatsShow "***name***", "***list***"**.

   Name is the name of a Secure Fabric OS statistic or the policy that relates to the statistic. The valid statistic names are listed in Table 4-2. An asterisk (*) can be entered to indicate all statistics. *List* is a list of the Domain IDs for which to display the statistics. You can enter an asterisk (*) to indicate all switches in the fabric. The default value is that of the local switch. If neither operand is specified, all statistics for all policies are displayed.

   The statistic and number of related attempted policy violations are displayed.

   For example, to display Secure Fabric OS statistics for the Management Server policy:

```
primaryfcs:admin> secstatsshow "MS_POLICY"
Name Value
====================
MS 20
```

Resetting Secure Fabric OS Statistics

The **secStatsReset** command can be used to reset statistics for a particular policy or all policies to 0. This command can be issued on any switch. Recording and resetting the statistics allows you to identify changes in traffic patterns since the statistics were last reset. This command can only be issued from the primary FCS switch if the "list" operand is specified. If the "list" operand is not specified, this command can be entered from any switch in the fabric.

To reset a statistic counter to 0:

1. Log in to the primary FCS switch as admin from a sectelnet or Secure Shell session.
2. If desired, enter the **secStatsShow** command and record the current statistics.
3. Type **secStatsReset "***name***", "***list***"** to reset the statistics.

   name is the name of the statistic or the policy that relates to the statistic. The valid statistic names are listed in Table 4-2. You can enter an asterisk (*) to indicate all Secure Fabric OS statistics.

   list is a list of the domain IDs for which to reset the statistics. You can enter an asterisk (*) to indicate all switches in the fabric. The default value is that of the local switch.

   If neither operand is specified, all statistics for all Secure Fabric OS policies are reset to 0.

   The specified statistics are reset to 0.

   For example, to reset all statistics on a local switch:

```
primaryfcs:admin> secstatsreset
About to reset all security counters.
Are you sure (yes, y, no, n):[no] y
Security statistics reset to zero.
```

   To reset the DCC_POLICY statistics on domains 1 and 69:

```
primaryfcs:admin> secstatsreset "DCC_POLICY", "1;69"
Reset DCC_POLICY statistic.
```

Managing Passwords

This section provides the following information:

When secure mode is enabled, the following conditions apply:

- The **passwd** command can only be entered on the primary FCS switch.
- The root and factory accounts can only be accessed from the FCS switches. Attempting to access them from a non-FCS switch generates an error message.
- The admin account (or roles) remain available from all switches, but two passwords are implemented: one for all FCS switches and one for all non-FCS switches.
- Temporary passwords can be created for specific switches, making it possible to provide temporary access to another user.

The user account (or roles) remain available fabric-wide regardless of whether secure mode is enabled. The characteristics of the different accounts when secure mode is enabled and disabled are described in Table 4-3.

You can use the multiple user account (MUA) feature of Fabric OS v3.2.0 and v4.4.0 if the primary FCS switch is running either Fabric OS version. The other switches do not need to be running a version of Fabric OS supporting MUA.

If a digital certificate is installed, the sectelnet and API passwords are automatically encrypted, regardless of whether secure mode is enabled. HTTP only encrypts passwords if secure mode is enabled.

Note

Record passwords and store them in a secure place; recovering passwords might require significant effort and result in fabric downtime.

Table 4-3 on page 4-10 summarizes login account behavior with secure mode disabled and enabled.

Table 4-3 Login Account Behavior with Secure Mode Disabled and Enabled

Login Account	Secure Mode Disabled	Secure Mode Enabled
User Recommended for all non-administrative options. Can use to modify user password.	Available on all switches. Password is specific to each switch; can modify using **passwd** command.	Available on all switches. Can create temporary passwords. Password is fabric wide; can modify using **passwd** command on the primary FCS switch.
Admin Recommended for all administrative options. Can use to modify admin and user passwords.	Available on all switches. Password is specific to each switch; can modify using **passwd** command.	Available on all switches. Can create temporary passwords. Two passwords: • One for all FCS switches; can modify using **passwd** command on the primary FCS switch. • One for all non-FCS switches; can modify using **secNonFCSPasswd** command on the primary FCS switch.
Factory Created for switch initialization purposes; not recommended for administrative operations. Can use to modify factory, admin, and user passwords.	Available on all switches. Password is specific to each switch; can modify using **passwd** command.	Available on FCS switches only. However, can temporarily enable root and factory accounts on non-FCS switches by creating a temporary password. Password is common to all FCS switches; can modify using **passwd** command on the primary FCS switch.
Root Creating for debugging purposes; not recommended for administrative operations. Can use to modify root, factory, admin, and user passwords.	Available on all switches. Password is specific to each switch; can modify using **passwd** command.	Available on FCS switches only. However, can temporarily enable root and factory accounts on non-FCS switches by creating a temporary password. Password is common to all FCS switches; can modify using **passwd** command on the primary FCS switch.

Modifying Passwords in Secure Mode

The **passwd** command can be used to modify the fabric-wide user password and the passwords for the FCS switches. The **secNonFCSPasswd** can be used to modify the admin password for non-FCS switches.

Note

If the password is changed for a login account, all open sessions using that account are terminated, including the session from which the **passwd** command was executed, if applicable.

Modifying the FCS Switch Passwords or the Fabric-Wide User Password

The **passwd** command can be used to modify the passwords for the following accounts when secure mode is enabled:

- The fabric-wide user account
- The admin, root, and factory accounts on the FCS switches
- Multiple user account (MUA) passwords for user-defined accounts

To modify the passwords:

1. From a sectelnet or Secure Shell session, log in to the primary FCS switch as admin, root, or factory, depending on which password you want to modify (use the account for which you want to modify a password or a higher-level account).
2. Type the **passwd** command.
3. Type the new passwords at the prompts. The passwords can be anywhere between 8 and 40 alphanumeric characters in length.

   The passwords are distributed to all switches in the fabric and saved in the Secure Fabric OS database. Any existing telnet connections to the switches are terminated and must be reinitiated if access is required.

```
switch:admin> passwd "admin"
Changing password for admin
Enter new password:
Re-type new password:
Password changed.
Saving password to stable storage.
Password saved to stable storage successfully.
```

Modifying the Non-FCS Switch Admin Password

The **secNonFCSPasswd** command can be used to modify the password for the admin account on non-FCS switches. Secure mode must be enabled to use this command.

To modify the admin password for non-FCS switches:

1. From a sectelnet or Secure Shell session, log in to the primary FCS switch as admin.
2. Type the **secNonFCSPasswd** command.

3. Type the new non-FCS admin password at the prompt. The password can be anywhere from 8 to 40 alphanumeric characters in length.

   This password becomes the admin password for all non-FCS switches in the fabric.

4. Reenter the new non-FCS admin password at the prompt. The password is distributed to all switches in the fabric and saved in the Secure Fabric OS database. Any existing admin-level telnet connections to these non-FCS switches are terminated.

```
primaryfcs:admin> secnonfcspasswd
Non FCS switch password:
Re-enter new password:
Committing configuration...done.
```

Using Temporary Passwords

Temporary passwords can be created to grant temporary access to a specific switch and login account without compromising the confidentiality of the permanent passwords; the permanent passwords also remain in effect. Temporary passwords can be removed; they are also automatically removed after a switch reboot.

Note

If a temporary password is set on a backup FCS switch, and the backup FCS switch then becomes the primary FCS switch, the temporary password remains in effect on that switch until the **secTempPasswdReset** command is entered.

Creating a Temporary Password for a Switch

The **secTempPasswdSet** command can be used to create a temporary password. You must specify a login account and a switch Domain ID.

To create a temporary admin password on a non-FCS switch:

1. From a sectelnet or Secure Shell session, log in to the primary FCS switch as admin.
2. Type **secTempPasswdSet** *domain*, **"***login_name***"**.

   Domain is the Domain ID of the switch for which you want to set a temporary password.
   Login_name is the login account for which you want to set the temporary password.
3. Type the admin password at the prompt.
4. Type an alphanumeric password between 8 and 40 characters in length.
5. Reenter the password exactly as entered the first time.

   For example, to create a temporary password for the admin account on a switch that has a Domain ID of 2:

```
primaryfcs:admin> sectemppasswdset 2, "admin"
Set remote switch admin password: swimming
Re-enter remote switch admin password: swimming
Committing configuration........done
Password successfully set for domain 2 for admin.
```

Removing a Temporary Password from a Switch

The **secTempPasswdReset** command can be used to remove the temporary password. The permanent password remains in effect.

To remove the temporary password from a switch:

1. From a sectelnet or Secure Shell session, log in to the primary FCS switch as admin.
2. Type **secTempPasswdReset** *domain*, "*login_name*".

   Domain is the domain ID of the switch for which you want to remove the temporary password. *Login_name* is the login account to which the temporary password applies.

   You can enter the command with no parameters to reset all temporary passwords in the fabric.

   For example, to removing a temporary password for the admin account from a switch that has a domain ID of 2:

```
switch:admin> sectemppasswdreset 2, "admin"
Committing configuration.....done
Password successfully reset on domain 2 for admin
```

Resetting the Version Number and Time Stamp

When a change is made to any information in the Secure Fabric OS database (zoning, policies, passwords, or SNMP), the current time stamp and a version number are attached to the Secure Fabric OS database.

This information is used to determine which database is preserved when two or more fabrics are merged. The database of the fabric with a nonzero version stamp is kept. When merging fabrics, ensure that the version stamp of the database you want to preserve is nonzero; then, set the version stamp of all other fabrics to 0. To ensure that the time stamp of a fabric is nonzero, modify a policy and enter the **secPolicySave** or **secPolicyActivate** command.

To display the version number and time stamp of a fabric:

1. From a sectelnet or Secure Shell session, log in to the primary FCS switch as admin.
2. Type the **secModeShow** command.

To reset the time stamp of a fabric to 0:

1. From a sectelnet or Secure Shell session, log in to the primary FCS switch as admin.
2. Type the **secVersionReset** command. If the fabric contains no FCS switch, you can enter the **secVersionReset** command on any switch.

Adding Switches and Merging Fabrics with Secure Mode Enabled

To merge fabrics, all switches must be in the same state regarding secure mode and must have an identical FCS policy. Any switches that do not having a matching FCS policy or are in a different state regarding secure mode are segmented. For example, two fabrics that both have secure mode disabled can be merged, and two fabrics that both have secure mode enabled can be merged.

When fabrics are merged, the fabric that contains the desired configuration information must have a nonzero version stamp, and all the other fabrics being merged must have zero version stamps. The Security policy set, zoning configuration, password information, multiple user account information, and SNMP community strings are overwritten by the fabric whose version stamp is nonzero. Before merging, verify that the fabric that contains all the desired information has the nonzero stamp.

Note

As an exception to the rule of secure fabric mergers, when a non-FCS switch merges with a secure fabric, the primary switch propagates its secure database to the non-FCS switch. Propagation from the primary switch occurs even if the secure fabric has a zero version stamp and the non-FCS switch has nonzero version stamp.

For general information about merging fabrics and instructions for merging fabrics that are not in secure mode, refer to the *Fabric OS Procedures Guide*.

Table 4-4 indicates the results of moving switches in and out of fabrics with secure mode enabled or disabled.

Table 4-4 Moving Switches Between Fabrics

Initial State of Switch	If set up as a standalone switch:	If moved into a fabric that has Secure Mode enabled and a functioning primary FCS switch:	If moved into a fabric that has Secure Mode enabled but no FCS switches are available:	If moved into a non-secure fabric:
Has secure mode enabled and is primary FCS switch in the FCS policy stored on switch.	Forms a one switch fabric with secure mode enabled, and acts as primary FCS switch.	Segments unless FCS policies are identical. If identical, switch is primary FCS switch unless other FCS switch is higher in the FCS policy.	Segments unless FCS policies are identical. If policies are identical, switch becomes primary FCS switch.	Segments from fabric.
Has secure mode enabled and is backup FCS switch in the FCS policy stored on switch.	Forms a one switch fabric with secure mode enabled, and acts as primary FCS switch.	Segments unless FCS policies are identical. If policies are identical, switch is backup FCS switch.	Segments unless FCS policies are identical. If policies are identical, switch becomes primary FCS switch.	Segments from fabric.
Has secure mode enabled and is non-FCS switch in the FCS policy stored on switch.	Forms a one switch fabric with secure mode enabled but no FCS switch (to specify primary FCS switch, enter **secModeEnable**).	Segments unless FCS policies are identical. If policies are identical, switch is non-FCS switch.	Segments unless FCS policies are identical. If policies are identical, switch is a non-FCS switch.	Segments from fabric.
Has secure mode disabled.	Standard operation.	Segments from fabric.	Segments from fabric.	Standard operation.

Note

Although the following procedure does not require rebooting the fabric, there is potential for segmentation or other disruption to the fabric due to the number of factors involved in the merge process.

To merge two or more fabrics that have Secure Fabric OS implemented:

1. As a precaution, back up the configuration of each fabric to be merged by entering the **configUpload** command and completing the prompts. This also backs up the policies if Secure Fabric OS was already in use on the switch (such as on a 2000-series switch running v2.6.x).
2. Ensure that all switches to be merged are running Fabric OS v2.6.2, v3.2.0, or v4.4.0.
   a. Open a CLI connection (serial or telnet) to one of the switches in the fabric.
   b. Log in to the switch as admin. The default password is **password**.
   c. Type the **version** command. If the switch is a SilkWorm 12000 or 24000, you can alternatively enter the **firmwareShow** command.
   d. If the switch is not running Fabric OS v2.6.2, v3.2.0, or v4.4.0, upgrade the firmware as required. For information on upgrading firmware, refer to the *Fabric OS Procedures Guide*.
   e. Customize the account passwords from the default values, as described in "Customizing the Account Passwords" on page 2-4.
   f. Repeat for each switch that you intend to include in the final merged fabric.
3. If the final merged fabric will contain switches running Fabric OS v2.6.2 or v3.2.0 and switches running Fabric OS v4.4.0, the PID mode on all switches must be compatible; for more information about PID modes, refer to the *Fabric OS Procedures Guide*.

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.

4. Ensure that the Management Server Platform Service is consistently enabled or disabled across all the switches to be merged. For information about management server support provided by Fabric OS, refer to the *Fabric OS Command Reference Manual*.
5. Ensure that all switches to be merged have activated Secure Fabric OS and Zoning licenses, as described in "Verifying or Activating the Secure Fabric OS and Advanced Zoning Licenses" on page 2-4.
6. Ensure that all switches to be merged have the required PKI objects (private key passphrase, switch private key, CSR, and root certificate) and a digital certificate installed.
   a. Log in to the switch as admin.
   b. Type the command supported by the Fabric OS installed on the switch:
      - For Fabric OS v4.4.0, enter **pkiShow**.
      - For Fabric OS v2.6.2 and v3.2.0, enter **configShow "pki"**.

      A list displays the PKI objects currently installed on the switch.

Note

"Root Certificate" is an internal PKI object. "Certificate" is the digital certificate.

   c. Verify that all of the objects display "Exist".

If the digital certificate displays "Empty," repeat the procedure provided in "Distributing Digital Certificates to the Switches" on page 2-14. If any of the PKI objects other than the digital certificate displays "Empty", you can either reboot the switch to automatically re-create the objects or re-create them as described in "Recreating PKI Objects if Required" on page 2-18.

d. Repeat for the remaining switches in the fabric.

7. Install a supported CLI client on the computer workstations that you will be using to manage the merged fabric. Supported CLI clients include sectelnet and Secure Shell and are discussed in "Installing a Supported CLI Client on a Computer Workstation" on page 2-26.
8. Enable secure mode on all switches to be merged by entering the **secModeEnable** command on the primary FCS switches of any fabrics that do not already have secure mode enabled. For more information about enabling secure mode, refer to "Enabling Secure Mode" on page 3-2.
9. Determine which switches you want to designate as primary FCS switch and backup FCS switches for the merged fabric; then, modify the FCS policy for *each* fabric to list these switches as the primary FCS switch and backup FCS switches. Ensure that all the FCS policies are an *exact* match; they must list the same switches, with the switches identified in the same manner and listed in the same order.

   If a fabric has become segmented with secure mode enabled but no FCS switches available, enter the **secModeEnable** command and modify the FCS policy to specify FCS switches. This is the only instance in which this command can be entered when secure mode is already enabled.
10. Modify the SCC policy on the final primary FCS switch (the one that will succeed as the primary FCS switch in the final merged fabric) to include all switches that are being merged.
11. Ensure that the final primary FCS switch has the desired Secure Fabric OS policy set, zoning configuration, password information, multiple user account information, and SNMP community strings. The primary FCS switch will distribute this information fabric-wide.

    For information about managing zoning configurations, refer to the *Advanced Zoning User's Guide*.
12. Verify that the fabric that contains the final primary FCS switch has a nonzero version stamp by logging into the fabric and entering the **secModeShow** command. If this fabric does not show a nonzero version stamp, modify a policy and enter either the **secPolicySave** or **secPolicyActivate** command to create a nonzero version stamp. Set the version stamp of the other fabrics to 0 by logging in to each fabric and entering the **secVersionReset** command.
13. If fabrics are to be rejoined after a segmentation, enter the **switchDisable** and **switchEnable** commands on each switch that was segmented from the primary FCS switch. For each ISL connected to the segmented switch, enter the **portDisable** and **portEnable** commands on both ISL ports.
14. Physically connect the fabrics. The fabrics automatically merge and the Secure Fabric OS configuration associated with the primary FCS switch that has the *non*zero version stamp is kept.

Troubleshooting

Some of the most likely issues with Secure Fabric OS management and the recommended actions are described in Table 4-5. The information in the table is based on the assumption that the fabric was originally fully functional and secure mode was enabled.

Note

Some of the recommended actions might interrupt data traffic.

Table 4-5 Recovery Processes

Symptom	Possible Causes	Recommended Actions
Secure Fabric OS policies do not appear to be in effect.	Secure mode is not enabled.	Type the **secModeShow** command. If secure mode is disabled, enter the **secModeEnable** command on the switch that you want to become the primary FCS switch and specify the FCS switches at the prompts.
	Policy changes have not been applied.	Type the **secPolicyShow** command and review the differences between the active and defined policy sets. If desired, enter the **secPolicyActivate** command to activate all recent policy changes.
	Fabric has segmented.	See possible causes and actions for "One or more switches has segmented from the fabric," later in this table.
Commands cannot be executed from any switch in the fabric.	All FCS switches have failed but secure mode is still enabled, preventing access to fabric.	Type the **secModeEnable** command from the switch that you want to become the new primary FCS switch, and specify the FCS switches. **Note**: Specify adequate backup FCS switches to prevent a recurrence of this problem.
Cannot access some or all switches in the fabric.	The MAC policies are restricting access. **Note:** An empty MAC policy blocks all access through that management channel.	Use a serial cable to connect to the primary FCS switch; then, enter the **secPolicyShow** command to review the MAC policies. Modify policies as necessary by either entering valid entries or deleting the empty policies.
Cannot access primary FCS switch by any management method.	Primary FCS switch has failed or lost all connections.	Log in to the backup FCS switch that you want to become the new primary FCS switch and enter the **secFCSFailover** command to reassign the primary FCS role to a backup FCS switch. If no backup FCS switches are available, enter the **secModeEnable** command to specify a new primary FCS switch. Specify adequate backup FCS switches to prevent a recurrence. Troubleshoot the previous primary FCS switch as required.
A device or switch port listed in the SCC or in a DCC policy cannot be accessed.	Switch port might be disabled.	Type the **switchShow** command. If the port in question is disabled, enter the **portEnable** command. If the switch port still cannot be accessed, enter the **portEnable** command for the port on the other switch.

Table 4-5 Recovery Processes (Continued)

Symptom	Possible Causes	Recommended Actions
One or more CLI sessions is automatically logged out.	Password might have been modified for login account in use, the **secModeEnable** command might have been issued, or switches might have changed switch roles (primary to backup, backup to primary and so forth).	Try closing and reopening CLI session.
On chassis-based platforms, status messages from any logical switch are broadcast to the serial console and telnet sessions on all other logical switches.	The status messages from any logical switch are normally broadcast to the serial console and telnet sessions on all logical switches.	All broadcast messages display the switch instance. Messages that originate from a switch instance other than the one to which the telnet session is logged in can be ignored.
CLI session freezes or cannot be established after secure mode is enabled.	CP failed over and network routing cache(s) require updating.	Try closing and reopening CLI session. If this fails, request that your LAN administrator refresh the network router cache(s).
A policy that has been created is not listed by the **secPolicyShow** command.	The new policy was not saved or activated.	Save or activate the policy changes by entering the **secPolicySave** or **secPolicyActivate** command.
	Incorrect policy name used.	Verify that the correct policy name was used. Policy names must be entered in all uppercase characters.
The message “The page cannot be displayed” is displayed when HTTP access is attempted, and response time is slow.	An HTTP policy has been created but has no members.	Add the desired members to the HTTP policy.
Unable to establish a sectelnet/SSH session to the IP address of the active CP of a SilkWorm 12000/24000, or a session to the standby CP is disconnected when it becomes the active CP.	sectelnet/SSH sessions cannot be established to the IP address of the active CP in secure mode. This enables enforcement of Telnet policy for each logical switch.	Establish a sectelnet/SSH session to the IP addresses of the logical switches or the standby CP instead (if allowed by Telnet policy).
A security transaction appears to have been lost.	One of the switches in the fabric rebooted while the transaction was in progress.	Wait for the switch to complete booting; then, reenter the security command on the new primary FCS switch to complete the transaction.
Fabric segments after secure mode is enabled on a SilkWorm 12000/ 24000 director.	CPs failed over during process of enabling secure mode.	Type **secModeEnable** again on the segmented switch, using the same FCS list as used before.

Table 4-5 Recovery Processes (Continued)

Symptom	Possible Causes	Recommended Actions
One or more switches is segmented from the fabric. **Note:** For instructions on rejoining fabrics, refer to the instructions in "Adding Switches and Merging Fabrics with Secure Mode Enabled" on page 4-14.	SCC_POLICY is excluding the segmented switches.	Use the **secPolicyAdd** command on the primary FCS switch to add the switches to the SCC_POLICY.
	Management server services on the segmented switches are inconsistent with rest of fabric.	Ensure that the Management Server Platform Service is consistently enabled or disabled across all the switches in the fabric. For information about the management server support provided by Fabric OS, refer to the *Fabric OS Command Reference Manual*.
	The segmented switches are missing PKI objects.	Determine the status of the PKI objects by following the procedure in "Verifying Installation of the Digital Certificates" on page 2-17. If any objects are missing, replace as described in "Recreating PKI Objects if Required" on page 2-18.
	ISLs to the segmented switches are interrupted or a port failure occurred.	Check the hardware connections and the port status for all ISLs between the segmented switches and the fabric.
	Configurations of the segmented switches diverged from rest of the fabric.	Disable the segmented switches, reset the configuration parameters to match the rest of the fabric, and reenable the switches.
	FCS policies on the segmented switches are not identical to the FCS policy of the fabric.	If one or more switches is segmented without any FCS switches, enter the **secModeEnable** command on a segmented switch and specify an FCS policy that is identical to the FCS policy of the rest of the fabric. The segmented switch or group of switches is automatically fastbooted. If one or more switches is segmented along with a primary FCS switch, modify the FCS policy as required until it is identical to the FCS policy in the rest of the fabric.
	The fabric contains more than one version stamp. Might be due to no primary FCS switch being available to propagate changes across fabric.	Type the **secModeEnable** command to specify a new primary FCS switch. Specify adequate backup FCS switches to prevent a recurrence. Then, for each segmented portion of the fabric that does not contain the new primary FCS switch, reset the version stamp to 0 by entering **switchDisable**, **secVersionReset**, and **switchEnable**.

Table 4-5 Recovery Processes (Continued)

Symptom	Possible Causes	Recommended Actions
When the SCC policy is created after a fabric segmentation, it automatically includes the segmented FCS switches.	The segmented FCS switches are still listed in the FCS policy.	Modify FCS policy to remove segmented FCS switches; then, modify or create the SCC policy as required.
Passwords that should be consistent across the fabric are not consistent.	A password recovery operation might have been performed on one or more switches.	To make the passwords the same, log in to the switch that had the password recovered and enter the **switchDisable** command, followed by **secVersionReset** and **switchEnable** commands.
Unsaved changes to the policies are lost.	The primary FCS switch might have failed over.	Reenter the changes; then, enter the **secPolicySave** or **secPolicyActivate** command.
During sectelnet sessions, security does not enable and a hex dump displays.	During the active sectelnet session, PKI objects (key and certificate) are removed and reinstalled from another login session. This results in the certificate in the current sectelnet session becoming invalid and displaying errors.	Log out from your current sectelnet session and log back in.

Frequently Asked Questions

This section organizes the frequently asked questions into the following groups:

- General
- Management Access
- Digital Certificates and PKI Objects
- Merging Fabrics
- Passwords

General

Is Secure Fabric OS standards-based?

Yes. Secure Fabric OS uses standards-based security mechanisms and protocols.

What additional information is available for Secure Fabric OS?

In addition to this document, the following information about fabric security and the Secure Fabric OS product is available:

- Secure Fabric OS Course (SFO200), offered by Brocade Communications Systems, Inc. The class schedule is provided at *http://www.brocade.com/education_services/index.jhtml.*
- White papers, online demos, and data sheets are available through the Brocade Web site at *http://www.brocade.com/products/software.jhtml.*
- Best practice guides, white papers, online demos, data sheets, and other documentation is available through the Brocade Partner Web site, including the *SAN Security Best Practice Guide*.
- The CERT® Coordination Center of Carnegie Mellon University provides industry-level information about certification; visit *http://www.cert.org*.

Which switches and fabrics support Secure Fabric OS?

Any SilkWorm switch that is running Fabric OS v2.6.2, v3.2.0, or v4.4.0, as appropriate to the switch. This includes SilkWorm 2000-series, 3200, 3250, 3800, 3850, 3900, 4100, 6400, 12000, and 24000 switches.

Secure Fabric OS might be implemented across fabrics containing any mixture of 1 Gbit/sec or 2 Gbit/sec switches running v2.6.2, v3.2.0, or v4.4.0. If SilkWorm 2000-series switches is in the same fabric as switches running Fabric OS v3.2.0 or v4.4.0, then the 2000-series switches must be running Fabric OS v2.6.2.

Can you enable Secure Fabric OS on some switches but not others in the same fabric?

No. Secure Fabric OS is enabled on a fabric-wide basis. All switches in the fabric must support Secure Fabric OS for it to be effective. Any switches that do not have Secure Fabric OS installed are segmented from the rest of the fabric.

How is Secure Fabric OS managed?

Secure Fabric OS can be managed through the following methods:

- A supported CLI client

  Secure Fabric OS v2.6.2, v3.2.0, and v4.4.0 support the sectelnet client. Secure Fabric OS v4.4.0 also supports Secure Shell v2 clients.

- Fabric Manager
- Web Tools
- Fabric Access (API)

Does Secure Fabric OS prevent all unauthorized access?

There is no 100 percent protection in any network; however, the Secure Fabric OS product makes it possible for the administrator to create a significantly increased level of security that is customized to the fabric.

After Secure Fabric is turned on, can it be turned off again?

Yes, by using the **secModeDisable** command. Turning secure mode off does not disrupt traffic.

What happens if I create a policy with no members in it?

You cannot create an empty FCS Policy, but you can create other types of policies with no members. However, creating a policy with no members closes all access to that aspect of the fabric, which can result in preventing administrative access to the fabric. Before setting a policy, read all the information provided about that policy in "Creating Secure Fabric OS Policies Other Than the FCS Policy" on page 3-11.

How do I prevent someone from adding a computer to the fabric and mounting a LUN?

The following approaches can be used in conjunction, although no guarantees can be made of absolute security:

- Store all the FCS switches in a physically secure area.
- Use hardware-based zoning.
- Create a DCC policy for each switch in the fabric.
- Create an Options policy.

Management Access

What version of SSH and the SSH clients does Fabric OS v4.4.0 support?

Fabric OS v4.4.0 supports version 2 of the SSH protocol. Use a SSH client that supports version 2 of the protocol such as OpenSSH or F-Secure.

Can I use standard telnet when secure mode is enabled?

No, standard telnet is not supported when secure mode is enabled. However, sectelnet is available for Fabric OS v2.6.2, v3.2.0, and v4.4.0; SSH is also available for v4.4.0.

Is SSH part of the Secure Fabric OS feature?

No, SSH is automatically included with Fabric OS v4.4.0, regardless of whether the Secure Fabric OS license is activated.

Digital Certificates and PKI Objects

What is PKI?

PKI stands for Pubic Key Infrastructure; it refers to the use of cryptography to provide security (authentication, encryption, and so on.).

Can digital certificates be duplicated or installed on other switches?

No; digital certificates correspond to the switch WWN and the private/public key pair generated by the switch.

Does the digital certificate have to be reinstalled if the motherboard is replaced?

This depends on the version of Fabric OS on the new motherboard. Hardware shipped with Fabric OS v3.2.0 or v4.4.0 automatically includes digital certificates. To determine whether the new motherboard already has a digital certificate, follow the instructions for verifying the PKI objects.

Do all switches already have a digital certificate?

No, only switches that were shipped with v3.2.0 or v4.4.0 installed have digital certificates. For switches that are upgraded, follow the procedures provided in "Adding Secure Fabric OS to Switches That Require Upgrading" on page 2-5.

How can I tell whether the digital certificate or PKI objects are available on a switch?

For Fabric OS v4.4.0, enter the **pkiShow** command. For Fabric OS v3.2.0, enter **configShow "pki"**.

What happens if the PKI objects are deleted?

PKI objects cannot be deleted in secure mode. If they are deleted when secure mode is disabled, secure mode cannot be reenabled until they are regenerated. If any PKI objects are missing, all the PKI objects should be deleted using the **pkiRemove** command and then regenerated using the **pkiCreate** command or by rebooting the switch (any missing PKI objects, except the digital certificate, are automatically regenerated when the switch is rebooted). If the digital certificate is deleted, it must be reinstalled on the switch according to the instructions provided in "Distributing Digital Certificates to the Switches" on page 2-14.

For Fabric OS v3.2.0, use **configRemove** to remove all the PKI objects, **configUpload**, and then fastboot the switch. After the switch reboots, all PKI objects are available except for the certificate.

Are PKI objects required for any switch operations other than Secure Fabric OS?

The PKI objects are only required for Secure Fabric OS and the sectelnet client.

Why can I issue the **secModeEnable** command with an invalid certificate?

Web Tools and Fabric OS are not consistent in reporting switch certificate status. Web Tools reports a valid certificate with extra characters appended as invalid, whereas Fabric OS accepts the certificate and allows the **secModeEnable** command to complete successfully.

Merging Fabrics

Which switch becomes the primary FCS switch when fabrics are merged?

The first switch that is listed in the shared FCS policy for the merged fabric. If the FCS policies of the fabrics do not match before the merge, the fabrics segment.

What happens to the zoning information when fabrics are merged?

The switch that succeeds as the primary FCS switch distributes its 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.

Passwords

What if I forget the root password?

Refer to "Managing Passwords" on page 4-8 for general guidelines on password management. Refer to the section "Password Recovery," in *Fabric OS Procedures Guide* for more information.

Appendix

A

Secure Fabric OS Commands and Secure Mode Restrictions

Secure Fabric OS commands, zoning commands, and some management server commands must be entered through the primary FCS switch.

This appendix provides the following information:

For more detailed information about commands, refer to the *Fabric OS Command Reference Manual*.

Secure Fabric OS Commands

The Secure Fabric OS commands provide the following capabilities:

- Enable and disable secure mode
- Fail over the primary FCS switch
- Create and modify Secure Fabric OS policies
- View all Secure Fabric OS-related information
- Modify passwords
- Create and remove temporary passwords
- View and reset Secure Fabric OS statistics
- View and reset version stamp information

Most Secure Fabric OS commands must be executed on the primary FCS switch when secure mode is enabled. For a list of restricted commands, see "Command Restrictions in Secure Mode" on page A-4.

A

Table A-1 lists all the commands available for managing Secure Fabric OS.

Table A-1 Secure Fabric OS Commands

Command	Access Level	Description	Available in Secure Mode or Non-Secure Mode?	Available on Which Switches in Secure Mode?
authUtil	admin	Displays current authentication parameters and lets you set the protocol used to authenticate switches.	Both	Any
pkiCreate	admin	Re-creates the PKI objects on the switch. See "Recreating PKI Objects if Required" on page 2-18.	Nonsecure mode	n.a.
pkiRemove	admin	Removes the PKI objects from the switch.	Nonsecure mode	n.a.
pkiShow	All users	Displays the status of the PKI objects and digital certificate on the switch. See "Verifying Installation of the Digital Certificates" on page 2-17.	Both	Any
secActiveSize	admin	Displays the size of the active Secure Fabric OS database.	Both	Any
secAuthSecret	admin	Displays, sets, and removes secret key information from the database or deletes the entire database.	Both	Any
secDefineSize	admin	Displays the size of the defined Secure Fabric OS database.	Both	Any
secFabricShow	admin	Displays Secure Fabric OS-related fabric information. See "Displaying General Secure Fabric OS Information" on page 4-2.	Secure mode	Any
secFCSFailover	admin	Transfers the role of the primary FCS switch to the next switch in the FCS policy. See "Failing Over the Primary FCS Switch" on page 3-9.	Secure mode	Backup FCS switch
secGlobalShow	admin	Displays current state information for Secure Fabric OS, such as version stamp and status of transaction in progress.	Both	Any
secHelp	admin	Displays a list of Secure Fabric OS commands. To use, enter the **secHelp** command at the CLI prompt.	Both	Any
secModeDisable	admin	Disables secure mode. See "Disabling Secure Mode" on page B-2.	Secure mode	Primary FCS switch
secModeEnable	admin	Enables secure mode. See "Enabling Secure Mode" on page 3-2. This command cannot be entered if secure mode is already enabled unless all the FCS switches have failed.	Nonsecure mode Available in secure mode if no FCS switches are left	Enter from intended primary FCS switch
secModeShow	admin	Shows current mode of Secure Fabric OS. See "Displaying Status of Secure Mode" on page 4-4.	Both	Any

Table A-1 Secure Fabric OS Commands (Continued)

Command	Access Level	Description	Available in Secure Mode or Non-Secure Mode?	Available on Which Switches in Secure Mode?
secNonFCSPasswd	admin	Sets non-FCS admin account password. See "Modifying the Non-FCS Switch Admin Password" on page 4-11.	secure mode	Primary FCS switch
secPolicyAbort	admin	Aborts all policy changes since changes were last saved. See "Aborting All Uncommitted Changes" on page 3-28.	secure mode	Primary FCS switch
secPolicyActivate	admin	Activates all policy changes since this command was last issued. All activated policy changes are stored in the active policy set. See "Activating Changes to Secure Fabric OS Policies" on page 3-26.	secure mode	Primary FCS switch
secPolicyAdd	admin	Adds members to a policy. See "Adding a Member to an Existing Policy" on page 3-26.	secure mode	Primary FCS switch
secPolicyCreate	admin	Creates a policy. See "Creating Secure Fabric OS Policies Other Than the FCS Policy" on page 3-11.	secure mode	Primary FCS switch
secPolicyDelete	admin	Deletes a policy. See "Deleting a Policy" on page 3-27.	secure mode	Primary FCS switch
secPolicyDump	admin	Displays the Secure Fabric OS policy database. See "Viewing the Secure Fabric OS Policy Database" on page 4-2.	secure mode	Primary or backup FCS switch
secPolicyFCSMove	admin	Moves an FCS member in the FCS list. See "Changing the Position of a Switch Within the FCS Policy" on page 3-8.	secure mode	Primary FCS switch
secPolicyRemove	admin	Removes members from a policy. See "Removing a Member from a Policy" on page 3-27.	secure mode	Primary FCS switch
secPolicySave	admin	Saves all policy changes since either **secPolicySave** or **secPolicyActivate** were last issued. All policy changes that are saved but not activated are stored in the defined policy set. See "Saving Changes to Secure Fabric OS Policies" on page 3-25.	secure mode	Primary FCS switch
secPolicyShow	admin	Shows members of one or more policies. See "Displaying Individual Secure Fabric OS Policies" on page 4-3.	secure mode	Primary or backup FCS only
secStatsReset	admin	Resets Secure Fabric OS statistics to 0. See "Resetting Secure Fabric OS Statistics" on page 4-8.	Both	Any
secStatsShow	admin	Displays Secure Fabric OS statistics. See "Displaying Secure Fabric OS Statistics" on page 4-7.	Both	Any

Table A-1 Secure Fabric OS Commands (Continued)

Command	Access Level	Description	Available in Secure Mode or Non-Secure Mode?	Available on Which Switches in Secure Mode?
secTempPasswdReset	admin	Removes temporary passwords. See "Removing a Temporary Password from a Switch" on page 4-13.	Secure mode	Primary FCS switch
secTempPasswdSet	admin	Sets a temporary password for a switch. See "Creating a Temporary Password for a Switch" on page 4-12.	Secure mode	Primary FCS switch
secTransAbort	admin	Aborts the current Secure Fabric OS transaction. See "Aborting a Secure Fabric OS Transaction" on page 3-28.	Both	Any
secVersionReset	admin	Resets version stamp. See "Resetting the Version Number and Time Stamp" on page 4-13.	Secure mode	Primary FCS switch; if not available, then non-FCS switch.

Command Restrictions in Secure Mode

This section provides information about the restrictions that secure mode places on commands. Any commands not listed here can be executed on any switch, whether or not secure mode is enabled.

Zoning Commands

All zoning commands must be executed on the primary FCS switch, except for the **cfgShow** command, which can also be executed on the backup FCS switch. Table A-2 lists the zoning commands.

Table A-2 Zoning Commands

Command	Primary FCS Switch	Backup FCS Switch	Non-FCS Switch
aliAdd	Yes	No	No
aliCreate	Yes	No	No
aliDelete	Yes	No	No
aliRemove	Yes	No	No
aliShow	Yes	Yes	No
cfgAdd	Yes	No	No
cfgClear	Yes	No	No

Table A-2 Zoning Commands (Continued)

Command	Primary FCS Switch	Backup FCS Switch	Non-FCS Switch
cfgCreate	Yes	No	No
cfgDelete	Yes	No	No
cfgDisable	Yes	No	No
cfgEnable	Yes	No	No
cfgRemove	Yes	No	No
cfgSave	Yes	No	No
cfgShow	Yes	Yes	No
cfgSize	Yes	Yes	Yes
cfgTransAbort	Yes	No	No
cfgTransShow	Yes	Yes	No
faZoneAdd	Yes	No	No
faZoneCreate	Yes	No	No
faZoneDelete	Yes	No	No
faZoneRemove	Yes	No	No
faZoneShow	Yes	Yes	No
qloopAdd	Yes	No	No
qloopCreate	Yes	No	No
qloopDelete	Yes	No	No
qloopRemove	Yes	No	No
qloopShow	Yes	No	No
zoneAdd	Yes	No	No
zoneCreate	Yes	No	No
zoneDelete	Yes	No	No
zoneRemove	Yes	No	No
zoneShow	Yes	No	No

Miscellaneous Commands

Table A-3 lists which miscellaneous commands, including management server and SNMP commands, can be executed on which switches. Commands not listed here (or in the preceding two tables) can be executed on any switch.

Table A-3 Miscellaneous Commands

Command	Primary FCS Switch	Backup FCS Switch	Non-FCS Switch
agtcfgDefault	Yes	Yes (except cannot modify community strings)	Yes (except cannot modify community strings)
agtcfgSet	Yes	Yes (except cannot modify community strings)	Yes (except cannot modify community strings)
configUpload	Yes	Yes	Not recommended. The zoning and Secure Fabric OS configurations are not uploaded if entered on a non-FCS switch.
date	Yes	Yes (read only)	Yes (read only)
date *<operand to set time>*	Yes	No	No
msCapabilityShow	Yes	Yes	Yes
msConfigure	Yes (except ACL does not display)	Yes (except ACL does not display)	Yes (except ACL does not display)
msPlatShow	Yes	Yes	Yes
msplClearDB	Yes	No	No
msplMgmtActivate	Yes	No	No
msplMgmtDeactivate	Yes	No	No
mstdDisable	Yes	Yes	Yes
mstdDisable "all"	Yes	No	No
mstdEnable	Yes	Yes	Yes
mstdEnable "all"	Yes	No	No
mstdReadConfig	Yes	Yes	Yes
passwd	Yes	No	No

Table A-3 Miscellaneous Commands (Continued)

Command	Primary FCS Switch	Backup FCS Switch	Non-FCS Switch
tsClockServer	Yes	Yes (read only)	Yes (read only)
tsClockServer <*IP address of network time protocol (NTP) server*>	Yes	No	No
userConfig	Yes	No (only allows display)	No (only allows display)
wwn (display only; cannot modify WWNs in secure mode)	Yes	Yes	Yes

Removing Secure Fabric OS Capability

Appendix

B

Secure Fabric OS capability can be removed from a fabric by disabling secure mode and deactivating the Secure Fabric OS license keys on the individual switches. Removing Secure Fabric OS capability is not recommended unless absolutely required. If at all possible, consider disabling only secure mode and leaving the Secure Fabric OS feature available so that secure mode can be reenabled if desired.

One possible reason for disabling secure mode or removing Fabric OS capability includes the addition of new switches to the fabric that do not support Secure Fabric OS.

Disabling secure mode includes the following steps:

- "Preparing the Fabric for Removal of Secure Fabric OS Policies," next
- "Disabling Secure Mode" on page B-2

In addition, the following steps can be taken if desired:

- "Deactivating the Secure Fabric OS License on Each Switch" on page B-3
- "Uninstalling Related Items from the Host" on page B-3

Preparing the Fabric for Removal of Secure Fabric OS Policies

Note

This section provides very general recommendations only. For best-practice information, refer to the SOLUTIONware and other documentation provided on the Brocade Partner Web site.

The following tasks are recommended to prepare the fabric before disabling secure mode:

- Review the current Secure Fabric OS policies and the devices and users affected by each policy. The current policy set can be displayed by entering the **secPolicyDump** command.
- Review the types of attempted policy violations that have been occurring. The current Secure Fabric OS statistics can be displayed by entering the **secStatsShow** command.
- Evaluate the zoning configuration and other aspects of the fabric for any changes that could be implemented to decrease the chance of security violations when Secure Fabric OS is disabled.
- Educate users to minimize security risks and the impact of any security violations.

Disabling Secure Mode

Secure mode is enabled and disabled on a fabric-wide basis and can be enabled and disabled as often as desired. However, all Secure Fabric OS policies, including the FCS policy, are deleted each time secure mode is disabled, and must be re-created the next time it is enabled. The policies can be backed up using the **configUpload** and **configDownload** commands. For more information about these commands, refer to the *Fabric OS Command Reference Manual*.

Secure mode can be disabled only through a sectelnet, Secure Shell, or serial connection to the primary FCS switch. When secure mode is disabled, all current login sessions are automatically terminated.

For information about reenabling secure mode, see "Enabling Secure Mode" on page 3-2.

To disable secure mode, perform the following tasks:

1. From a sectelnet, Secure Shell, or serial session, log in to the primary FCS switch as admin.
2. Type **secModeDisable**.
3. Type the password when prompted.
4. Type **y** to confirm that secure mode should be disabled.

   Secure mode is disabled, all *current login* sessions are terminated, and the passwords are modified as follows:

   - On the switches that were FCS switches, the user, admin, factory, and root passwords remain the same as in secure mode.
   - On the switches that were non-FCS switches, the root, factory, and admin passwords become the same as the non-FCS admin password.

```
primaryfcs:admin> secmodedisable

Warning!!!
About to disable security.
ARE YOU SURE (yes, y, no, n): [no] y
Committing configuration...done.
Removing Active FMPS...
done
Removing Defined FMPS...
done
Disconnecting current session.
```

Deactivating the Secure Fabric OS License on Each Switch

Deactivating the Secure Fabric OS license is not required to disable Secure Fabric OS functionality.

Note

If the user installs and activates a feature license and then removes the license, the feature is not disabled until the next time system is rebooted or a switch enable/disable is performed.

To deactivate the software license:

1. Open a CLI connection (serial or telnet) to the switch.
2. Type the **licenseShow** command to display the Secure Fabric OS license key.

   Copy the license key from the **licenseShow** output directly into the CLI for the next step.
3. Type **licenseRemove "***key***"**.

   key is the license key and is case sensitive.
4. Repeat for each switch in the fabric.

```
switch:admin> licenseremove "1A1AaAaaaAAAA1a"
removing license-key "1A1AaAaaaAAAA1a"
Committing configuration...done.
For license to take effect, Please reboot switch now....
```

Uninstalling Related Items from the Host

The following items can optionally be removed from the host:

- PKICert utility
- sectelnet
- Secure Shell client

These items do not have to be uninstalled to disable Secure Fabric OS functionality.

Follow the standard procedure for uninstalling software from the workstation. On a Windows host computer, use the **Add/Remove Programs** control panel or just delete the folder. On a Solaris host, use the **rm** command to remove the folder.

Glossary

A

address identifier A 24-bit or 8-bit value used to identify the source or destination of a frame. *See also* S_ID *and* D_ID.

Advanced Fabric Services, Brocade A Brocade proprietary feature.

Advanced Performance Monitoring, Brocade A Brocade proprietary feature.

Advanced Zoning, Brocade A Brocade proprietary feature.

AL_PA Arbitrated-loop physical address. A unique 8-bit value assigned during loop initialization to a port in an arbitrated loop. Alternately, "arbitrated-loop parameters."

alias A logical grouping of elements in a fabric. An alias is a collection of port numbers and connected devices, used to simplify the entry of port numbers and WWNs when creating zones.

alias AL_PA An AL_PA value recognized by an L_Port in addition to the AL_PA assigned to the port. *See also* AL_PA.

ANSI American National Standards Institute.

area number In Brocade Fabric OS v4.0 and above, ports on a switch are assigned a logical area number. Port area numbers can be viewed by entering the **switchShow** command. They are used to define the operative port for many Fabric OS commands: for example, area numbers can be used to define the ports within an alias or zone.

ASIC Application-specific integrated circuit.

ATM Asynchronous Transfer Mode. A transport used for transmitting data over LANs or WANs that transmit fixed-length units of data. Provides any-to-any connectivity and allows nodes to transmit simultaneously.

authentication The process of verifying that an entity in a fabric (such as a switch) is what it claims to be. *See also* digital certificate, switch-to-switch authentication.

autocommit A feature of the **firmwareDownload** command. Enabled by default, autocommit commits new firmware to both partitions of a control processor.

autoreboot Refers to the **-b** option of the **firmwareDownload** command. Enabled by default.

B

backup FCS switch Relates to the Brocade Secure Fabric OS feature. The backup fabric configuration server serves as a backup in case the primary FCS switch fails. *See also* FCS switch, primary FCS switch.

bloom The code name given to the third-generation Brocade Fabric ASIC. This ASIC is used in SilkWorm switches 3000 series and beyond.

BOFMS Brocade open fabric management services.

C

CA Certificate authority. A trusted organization that issues digital certificates. *See also* digital certificate.

CFG Configuration.

CHAP Challenge-Handshake Authentication Protocol. Allows remote servers and clients to securely exchange authentication credentials. Both the server and client are configured with the same shared secret.

chassis The metal frame in which the switch and switch components are mounted.

CLI Command line interface. An interface that depends entirely on the use of commands, such as through telnet or SNMP, and does not involve a GUI.

client An entity that, using its common transport (CT), makes requests of a server.

configuration (1) A set of parameters that can be modified to fine-tune the operation of a switch. Use the **configShow** command to view the current configuration of your switch.

(2) In Brocade Zoning, a zoning element that contains a set of zones. The Configuration is the highest-level zoning element and is used to enable or disable a set of zones on the fabric. *See also* zone configuration.

core PID Core switch port identifier. The core PID must be set for v3.1 and earlier switches included in a fabric of v4.1 switches. This parameter is located in the **configure** command of firmware versions v3.1 and earlier. All v4.1 switches and above use the core PID format by default; this parameter is not present in the **configure** command for these switches.

CP Control processor.

D

D_ID Destination identifier. A 3-byte field in the frame header, used to indicate the address identifier of the N_Port to which the frame is headed.

DAS Direct attached storage.

DCC Direct cable connection. DCC does not require network interface cards (NICs), making it relatively inexpensive and simple; however, it provides a limited connection between two PCs, and the data transfer rate is slower than with a true LAN.

DCE Data Communications Equipment. Usually refers to a modem.

defined zone configuration The complete set of all zone objects defined in the fabric. Can include multiple zone configurations. *See also* effective zone configuration, enabled zone configuration, zone configuration.

DH-CHAP Diffie-Hellman Challenge-Handshake Authentication Protocol. An implementation of CHAP using Diffie-Hellman encryption. *See also* CHAP.

digital certificate An electronic document issued by a CA (certificate authority) to an entity, containing the public key and identity of the entity. Entities in a secure fabric are authenticated based on these certificates. *See also* authentication, CA, public key.

director A Brocade SilkWorm 12000 or 24000 switch.

domain ID A unique identifier for all switches in a fabric, used in routing frames. Usually automatically assigned by the principal switch but can be assigned manually. The domain ID for a Brocade SilkWorm switch can be any integer between 1 and 239.

E

E_Port Expansion port. A standard Fibre Channel mechanism that enables switches to network with each other, creating an ISL. *See also* ISL.

edge fabric A Fibre Channel fabric connected to an FC router via an EX_Port (where hosts and storage are attached in a meta-SAN).

effective zone configuration A subset of the defined zone configuration, containing only the zone configuration object that is currently enabled. Only one configuration can be active at a time, but since multiple configurations can be *defined* in the database, a new configuration can be easily switched. *See also* defined zone configuration.

embedded port An embedded port (or domain controller) communicates and get updates from other switches' embedded ports. The well-known address is *fffcdd*, where *dd* = domain number.

enabled zone configuration The currently enabled configuration of zones. Only one configuration can be enabled at a time. *See also* defined zone configuration, zone configuration.

EOF End of frame. A group of ordered sets used to mark the end of a frame.

error As it applies to the Fibre Channel industry, a missing or corrupted frame, timeout, loss of synchronization, or loss of signal (link errors).

Ethernet Popular protocols for LANs.

EX_Port A type of E_Port that connects an FC router to an edge fabric. EX_Ports limit the scope of fabric services scope but provide device connectivity using FC-NAT.

F

fabric A collection of Fibre Channel switches and devices, such as hosts and storage. Also referred to as a "switched fabric." *See also* SAN, topology.

Fabric Manager An optionally licensed Brocade software. Fabric Manager is a GUI that allows for fabric-wide administration and management. Switches can be treated as groups, and actions such as firmware downloads can be performed simultaneously.

Fabric Mode One of two possible modes for an L_Port, in which the L_Port is connected to another port that is not loop capable, using fabric protocol.

fabric name The unique identifier assigned to a fabric and communicated during login and port discovery.

fabric port count The number of ports available for connection by nodes in a fabric.

fabric services Codes that describe the communication to and from any well-known address.

fabric topology The arrangement of switches that form a fabric.

Fabric Watch An optionally licensed Brocade software. Fabric Watch can be accessed through either the command line or Advanced Web Tools, and it provides the ability to set thresholds for monitoring fabric conditions.

failover Describes the Brocade SilkWorm 12000 and 24000 process of one CP passing active status to another CP. A failover is nondisruptive.

FC-0 Lowest layer of Fibre Channel transport. Represents physical media.

FC-1 Layer of Fibre Channel transport that contains the 8b/10b encoding scheme.

FC-2 Layer of Fibre Channel transport that handles framing and protocol, frame format, sequence/exchange management, and ordered set usage.

FC-3 Layer of Fibre Channel transport that contains common services used by multiple N_Ports in a node.

FC-4 Layer of Fibre Channel transport that handles standards and profiles for mapping upper-level protocols such as SCSI and IP onto the Fibre Channel Protocol.

FC-CT Fibre Channel common transport.

FC-FG Fibre Channel generic requirements.

FC-FLA The Fibre Channel fabric loop-attach standard defined by ANSI.

FC-FS Fibre Channel framing and signaling.

FC-GS Fibre Channel generic services.

FC-GS-2 Fibre Channel generic services, second generation.

FC-GS-3 Fibre Channel Generic Services, third generation.

FCIP Fibre Channel over IP.

FC-NAT Fibre Channel network address translation.

FC-PH The Fibre Channel physical and signaling standard for FC-0, FC-1, and FC-2 layers of the Fibre Channel Protocol. Indicates signaling used for cable plants, media types, and transmission speeds.

FC-PH-2 Fibre Channel Physical Interface, second generation.

FC-PH-3 Fibre Channel Physical Interface, third generation.

FC-PI Fibre Channel Physical Interface standard, defined by ANSI.

FC-PLDA The Fibre Channel Private Loop Direct Attach standard defined by ANSI. Applies to the operation of peripheral devices on a private loop.

FC_SB Fibre Channel single bytes.

FC_VI Fibre Channel virtual interface.

FCA Flow-control acknowledgement (DLSW).

FCIA Fibre Channel Industry Association. An international organization of Fibre Channel industry professionals. Provides oversight of ANSI and industry-developed standards, among other tasks.

FCS Fibre Channel switch; alternatively, Fabric Configuration Server.

FCS switch Relates to the Brocade Secure Fabric OS feature. One or more designated switches that store and manage security parameters and configuration data for all switches in the fabric. They also act as a set of backup switches to the primary FCS switch. *See also* primary FCS switch.

FC-SW-2 The second-generation Fibre Channel Switch Fabric standard defined by ANSI. Specifies tools and algorithms for the interconnection and initialization of Fibre Channel switches to create a multiswitch Fibre Channel fabric.

Fibre Channel The primary protocol used for building SANs to transmit data between servers, switches, and storage devices. Unlike IP and Ethernet, Fibre Channel was designed to support the needs of storage devices of all types. It is a high-speed, serial, bidirectional, topology-independent, multiprotocol, and highly scalable interconnection between computers, peripherals, and networks.

Fibre Channel transport A protocol service that supports communication between Fibre Channel service providers. *See also* FSP.

FICON® A protocol used on IBM mainframes. Brocade SilkWorm switch FICON support enables a SilkWorm fabric to transmit FICON format data between FICON-capable servers and storage.

FID Fabric ID. Unique identifier of a fabric in a meta-SAN.

FIFO First in, first out. Refers to a data buffer that follows the first in, first out rule.

firmware The basic operating system provided with the hardware.

firmware watermarking A Brocade SilkWorm switch feature that prevents an incompatible version of the Brocade Fabric OS to be downloaded to the SilkWorm 3000 series of switches.

FL_Port Fabric loop port. A port that is able to transmit under fabric protocol and also has arbitrated-loop capabilities. Can be used to connect an NL_Port to a switch. *See also* Fx_Port.

flash Programmable nonvolatile RAM (NVRAM) memory that maintains its contents without power.

FLOGI Fabric login. The process by which an N_Port determines whether a fabric is present and, if so, exchanges service parameters with it. *See also* PLOGI.

FMPS Fabric management policy set.

frame The Fibre Channel structure used to transmit data between ports. Consists of a start-of-frame delimiter, header, optional headers, data payload, cyclic redundancy check (CRC), and end-of-frame delimiter. There are two types of frames: link control frames (transmission acknowledgements and so forth) and data frames.

frame relay A protocol that uses logical channels, as used in X.25. Provides very little error-checking ability. Discards frames that arrive with errors. Allows a certain level of bandwidth between two locations (known as a "committed information rate": CIR) to be guaranteed by service provider. If CIR is exceeded for short periods (known as "bursts"), the network accommodates the extra data, if spare capacity is available. Frame relay is therefore known as "bandwidth on demand."

FS Fibre Channel service. A service that is defined by Fibre Channel standards and exists at a well-known address. For example, the Simple Name Server is a Fibre Channel service. *See also* FSP.

FSP Fibre Channel Service Protocol. The common protocol for all fabric services, transparent to the fabric type or topology. *See also* FS.

FSPF Fabric shortest path first. The Brocade routing protocol for Fibre Channel switches.

FSS Fabric OS state synchronization. The FSS service is related to high availability (HA). The primary function of FSS is to deliver state update messages from active components to their peer standby components. FSS determines if fabric elements are synchronized (and thus FSS "compliant").

FTP File Transfer Protocol.

FTS Fiber Transport Services.

full fabric The Brocade software license that allows multiple E_Ports on a switch, making it possible to create multiple ISL links.

full fabric citizenship A loop device that has an entry in the Simple Name Server.

full duplex A mode of communication that allows the same port to simultaneously transmit and receive frames. *See also* half duplex.

Fx_Port A fabric port that can operate as either an F_Port or FL_Port. *See also* FL_Port.

G

G_Port Generic port. A port that can operate as either an E_Port or an F_Port. A port is defined as a G_Port when it is not yet connected or has not yet assumed a specific function in the fabric.

gateway Hardware that connects incompatible networks by providing translation for both hardware and software. For example, an ATM gateway can be used to connect a Fibre Channel link to an ATM connection.

Gbit/sec Gigabits per second (1,062,500,000 bits/second).

GB/sec Gigabytes per second (1,062,500,000 bytes/second).

GMT Greenwich Mean Time. An international time zone. Also known as "UTC."

GUI A graphic user interface, such as Brocade Advanced Web Tools.

H

HA High availability. A set of features in Brocade SilkWorm switches that is designed to provide maximum reliability and nondisruptive replacement of key hardware and software modules.

half duplex A mode of communication that allows a port to either transmit or receive frames at any time except simultaneously (with the exception of link control frames, which can be transmitted at any time). *See also* full duplex.

header A Fibre Channel frame has a header and a payload. The header contains control and addressing information associated with the frame.

host A computer system that provides end users with services like computation and storage access.

HTTP Hypertext Transfer Protocol. The standard TCP/IP transfer protocol used on the World Wide Web.

hub A Fibre Channel wiring concentrator that collapses a loop topology into a physical star topology. Nodes are automatically added to the loop when active and removed when inactive.

HW Hardware.

I

ID_ID Insistent domain ID. A parameter of the **configure** command in the Brocade Fabric OS.

iFCP Internet Fibre Channel Protocol. Supports Fibre Channel Layer 4 FCP-Over-TCP/IP. It is a gateway-to-gateway protocol in which TCP/IP switching and routing components enhance/replace Fibre Channel fabric.

iFCS IP storage fabric configuration server.

Insistent Domain ID Mode Sets the domain ID of a switch as insistent, so that it remains the same over reboots, power cycles, failovers, and fabric reconfigurations. This mode is required to support FICON® traffic.

integrated fabric The fabric created by a Brocade SilkWorm 6400, consisting of six SilkWorm 2250 switches cabled together and configured to handle traffic seamlessly as a group.

interswitch link *See* ISL.

IOD In-order delivery. A parameter that, when set, guarantees that frames are either delivered in order or dropped.

IP Internet Protocol. The addressing part of TCP.

ISL Interswitch link. A Fibre Channel link from the E_Port of one switch to the E_Port of another. *See also* E_Port.

ISL oversub-scription ratio The ratio of the number of free ports (non-ISL) to the number of ISLs on a switch.

isolated E_Port An E_Port that is online but not operational due to overlapping domain IDs or nonidentical parameters (such as E_D_TOVs). *See also* E_Port.

ISP Internet service provider.

IU Information unit. A set of information as defined by either an upper-level process protocol definition or upper-level protocol mapping.

K

key A string of data (usually a numeric value) shared between two entities and used to control a cryptographic algorithm. Usually selected from a large pool of possible keys to make unauthorized identification of the key difficult. *See also* key pair.

key pair In public key cryptography, a pair of keys consisting of an entity's public and private key. The public key can be publicized, but the private key must be kept secret. *See also* public key cryptography.

L

L_Port Loop port. A node port (NL_Port) or fabric port (FL_Port) that has arbitrated-loop capabilities. An L_Port can be in either Fabric Mode or Loop Mode.

LAN Local area network. A network in which transmissions typically take place over fewer than 5 kilometers (3.4 miles).

login server The unit that responds to login requests.

Loom The code name given to the second-generation Brocade Fabric ASIC. This is the ASIC used in the SilkWorm 2xxx series of switches.

LUN Logical unit number.

M

MB/sec Megabytes per second.

Mbit/sec Megabits per second.

metric A relative value assigned to a route to aid in calculating the shortest path (1000 @ 1 Gbit/sec, 500 @ 2 Gbits/sec).

MS Management Server. The Management Server allows a storage area network (SAN) management application to retrieve information and administer the fabric and interconnected elements, such as switches, servers, and storage devices. The MS is located at the Fibre Channel well-known address FFFFFAh.

MSD Management Server daemon. Monitors the MS. Includes the Fabric Configuration Service and the Unzoned Name Server.

N

N_Port Node port. A port on a node that can connect to a Fibre Channel port or to another N_Port in a point-to-point connection. *See also* NL_Port, Nx_Port.

Name Server Simple Name Server (SNS). A switch service that stores names, addresses, and attributes for up to 15 minutes and provides them as required to other devices in the fabric. SNS is defined by Fibre Channel standards and exists at a well-known address. Also referred to as "directory service."

NAS Network-attached storage. A disk array connected to a controller that gives access via a LAN.

NL_Port Node loop port. A node port that has arbitrated-loop capabilities. Used to connect an equipment port to the fabric in a loop configuration through an FL_Port. *See also* N_Port, Nx_Port.

node A Fibre Channel device that contains an N_Port or NL_Port.

NS Name Server. The service provided by a fabric switch that stores names, addresses, and attributes related to Fibre Channel objects. Can cache information for up to 15 minutes. Also known as "Simple Name Server" or as a "directory service." *See also* Simple Name Server (SNS).

Nx_Port A node port that can operate as either an N_Port or NL_Port.

P

packet A set of information transmitted across a network. *See also* frame.

Performance Monitoring A Brocade SilkWorm switch feature that monitors port traffic and includes frame counters, SCSI read monitors, SCSI write monitors, and other types of monitors.

PID Port identifier. *See also* core PID.

PKI Public key infrastructure. An infrastructure that is based on public key cryptography and CA (certificate authority) and that uses digital certificates. *See also* CA, digital certificate, public key cryptography.

PKI certification utility Public key infrastructure certification utility. A utility that makes it possible to collect certificate requests from switches and to load certificates to switches. *See also* digital certificate, PKI.

PLOGI Port login. The port-to-port login process by which initiators establish sessions with targets. *See also* FLOGI.

port In a Brocade SilkWorm switch environment, an SFP or GBIC receptacle on a switch to which an optic cable for another device is attached.

port address In Fibre Channel technology, the port address is defined in hexadecimal. In the Brocade Fabric OS, a port address can be defined by a domain and port number combination or by area number. In an ESCON Director, an address used to specify port connectivity parameters and to assign link addresses for attached channels and control units.

port card A hardware component that provides a platform for field-replaceable, hot swappable ports.

port group A group of adjacent ports that share a common pool of frame buffers for long distance connections.

port-level zoning Defines a zone member by “domain,port”, which is the physical port to which the member is connected. *See also* zone member, WWN-level zoning.

port log A record of all activity on a switch, kept in volatile memory.

port log dump A view of what happens on a switch, from the switch's point of view. The **portlogdump** command is used to read the port log.

port name A user-defined alphanumeric name for a port.

port swapping Port swapping is the ability to redirect a failed port to another port. This feature is available in Fabric OS v4.1.0 and later.

port_name The unique identifier assigned to a Fibre Channel port. Communicated during login and port discovery.

POST Power-on self-test. A series of tests run by a switch after it is turned on.

primary FCS switch Relates to the Brocade Secure Fabric OS feature. The primary fabric configuration server switch actively manages security and configurations for all switches in the fabric. *See also* FCS switch.

principal switch The first switch to boot up in a fabric. Ensures unique domain IDs among roles.

private key The secret half of a key pair. *See also* key, key pair.

protocol A defined method and set of standards for communication. Determines the type of error-checking, the data-compression method, how sending devices indicate an end of message, and how receiving devices indicate receipt of a message.

public device A device that supports arbitrated-loop protocol, can interpret 8-bit addresses, and can log in to the fabric.

public key The public half of a key pair. *See also* key, key pair.

public key cryptography A type of cryptography that uses a key pair, with the two keys in the pair called at different points in the algorithm. The sender uses the recipient's public key to encrypt the message, and the recipient uses the recipient's private key to decrypt it. *See also* key pair, PKI.

Q

QoS Quality of service.

queue A mechanism for each AL_PA address that allows for collecting frames prior to sending them to the loop.

R

radius The greatest "distance" between any edge switch and the center of a fabric. A low-radius network is better than a high-radius network.

redundancy Having multiple occurrences of a component to maintain high availability (HA).

remote switch An optional feature for long-distance fabrics, requiring a Fibre Channel-to-ATM or SONET gateway.

S

S_ID Source ID. Refers to the native port address (24-bit address).

SAN Storage area network. A network of systems and storage devices that communicate using Fibre Channel protocols. *See also* fabric.

SAN architecture The overall design of a storage network solution, which includes one or more related fabrics, each of which has a topology.

SAN port count The number of ports available for connection by nodes in the entire SAN.

SCC SC connector. An SC connector is a fiber-optic cable connector that uses a push-pull latching mechanism similar to common audio and video cables. For bidirectional transmissions, two fiber cables and two SC connectors (dual SC) are generally used. SC is specified by the TIA as FOCIS-3.

SCN State change notification. Used for internal state change notifications, not external changes. This is the switch logging that the port is online or is an Fx_Port, not what is sent from the switch to the Nx_Ports.

SCR State change registration. Extended Link Service (ELS) requests the fabric controller to add the N_Port or NL_Port to the list of N_Ports and NL_Ports registered to receive the Registered State Change Notification (RSCN) Extended Link Service.

SCSI Small Computer Systems Interface. A parallel bus architecture and a protocol for transmitting large data blocks to a distance of 15 to 25 meters.

sectelnet A protocol similar to telnet but with encrypted passwords for increased security.

Secure Fabric OS An optionally licensed Brocade feature that provides advanced, centralized security for a fabric.

security policy Rules that determine how security is implemented in a fabric. Security policies can be customized through Brocade Secure Fabric OS or Brocade Fabric Manager.

serial The transmission of data bits in sequential order over a single line.

server A computer that processes end-user applications or requests.

SES SCSI Enclosure Services. A subset of the SCSI protocol used to monitor temperature, power, and fan status for enclosed devices.

SilkWorm The brand name for the Brocade family of switches.

Simple Name Server (SNS) A switch service that stores names, addresses, and attributes for up to 15 minutes and provides them as required to other devices in the fabric. SNS is defined by Fibre Channel standards and exists at a well-known address. Also referred to as “directory service” or “name server.”

Single CP Mode The **-s** option of the Fabric OS **firmwaredownload** command. Using **firmwaredownload -s** enables Single CP Mode. In the SilkWorm 12000 and 24000, Single CP Mode enables a user to upgrade a single CP and to select full install, autoreboot, and autocommit.

SLAP Switch Link Authentication Protocol.

SNMP Simple Network Management Protocol. An Internet management protocol that uses either IP for network-level functions and UDP for transport-level functions, or TCP/IP for both. Can be made available over other protocols, such as UDP/IP, because it does not rely on the underlying communication protocols.

SNS Simple Name Server.

SOF Start of frame. A group of ordered sets that marks the beginning of a frame and indicates the class of service the frame will use.

SONET Synchronous optical network. A standard for optical networks that provides building blocks and flexible payload mappings.

SSH Secure shell. Used starting in Brocade Fabric OS v4.1 to support encrypted telnet sessions to the switch. SSH encrypts all messages, including the client sending the password at login.

SSL Secure sockets layer.

Standard Translative Mode Allows public devices to communicate with private devices that are directly connected to the fabric.

storage A device used to store data, such as a disk or tape.

switch A fabric device providing bandwidth and high-speed routing of data via link-level addressing.

switch name The arbitrary name assigned to a switch.

switch port A port on a switch. Switch ports can be E_Ports, F_Ports, or FL_Ports.

switch-to-switch authentication The process of authenticating both switches in a switch-to-switch connection using digital certificates. *See also* authentication, digital certificate.

T

T10 A standards committee chartered with creating standards for SCSI.

T11 A standards committee chartered with creating standards for Fibre Channel.

tachyon A chip that supports FC-0 through FC-2 on a single chip.

TCP/IP Transmission Control Protocol Internet Protocol.

telnet A virtual terminal emulation used with TCP/IP. “Telnet” is sometimes used as a synonym for the Brocade Fabric OS CLI.

Time Server A Fibre Channel service that allows for the management of all timers.

topology As it applies to Fibre Channel technology, the configuration of the Fibre Channel network and the resulting communication paths allowed. There are three possible topologies:

Point to point. A direct link between two communication ports.

Switched fabric. Multiple N_Ports linked to a switch by F_Ports.

Arbitrated loop. Multiple NL_Ports connected in a loop.

trunking In Fibre Channel technology, a feature that enables distribution of traffic over the combined bandwidth of up to four ISLs between adjacent switches, while preserving in-order delivery.

trunking group A set of up to four trunked ISLs.

trunking ports The ports in a set of trunked ISLs.

TS Time Server.

TX Transmit.

U

U_Port Universal port. A switch port that can operate as a G_Port, E_Port, F_Port, or FL_Port. A port is defined as a U_Port when it is not connected or has not yet assumed a specific function in the fabric.

UDP User Datagram Protocol. A protocol that runs on top of IP and provides port multiplexing for upper-level protocols.

UL Underwriter's Laboratories. A product-safety testing and certification organization; independent, not-for-profit.

UTC Universal Time Conversion. Also known as “Coordinated Universal Time,” which is an international standard of time. UTC is 8 hours behind Pacific Standard Time and 5 hours behind Eastern Standard Time. See also GMT.

W

WAN Wide area network.

watchdog A software daemon that monitors Fabric OS modules on the kernel.

well-known address As it pertains to Fibre Channel technology, a logical address defined by Fibre Channel standards as assigned to a specific function and stored on the switch.

workstation A computer used to access and manage the fabric. Also referred to as a “management station” or “host.”

WWN World Wide Name. An identifier that is unique worldwide. Each entity in a fabric has a separate WWN.

WWN-level zoning Defines a zone member using WWW port or WWN node. Defining a zone member as WWN allows the member (device) to be attached without regard to its physical location.

Z

zone A set of devices and hosts attached to the same fabric and configured as being in the same zone. Devices and hosts within the same zone have access to others in the zone but are not visible to any outside the zone.

zone configuration A specified set of zones. Enabling a configuration enables all zones in that configuration. *See also* defined zone configuration, enabled zone configuration, and effective zone configuration.

zone configuration object Defines a list of zone *objects*. The zone database can contain several zone configuration objects, but only one zone configuration object can be enabled and enforced at a time.

zone member Defines a device. A zone member can belong to more than one zone at a time.A zone member can be defined by either *port-level zoning* (domain,port: the physical port to which it is connected) or *WWN-level zoning* (using WWW port or WWN node).

zone object Defines a list of zone *members*. A zone object can exist across multiple zone configuration objects. zoning

A feature in fabric switches or hubs that allows segmentation of a node by physical port, name, or address.

zoning, port-level *See* port-level zoning.

zoning, WWN-level *See* WWN-level zoning.

Index

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V

W

Z