BROCADE

Brocade Secure Fabric

User's Guide Version 3.1.0/4.1.0

Publication Number: 53-0000526-02
Publication Date: 04/25/03

Publication Number: 53-0000526-02

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

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

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

Export of technical data contained in this document may require an export license from the United States Government.

Brocade Communications Systems, Incorporated

Corporate Headquarters
1745 Technology Drive
San Jose, CA 95110
T: (408) 487-8000
F: (408) 487-8101
Email: info@brocade.com

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

European Headquarters
29, route de l'Aeroport
Case Postale 105
CH-1211 Geneva 15,
Switzerland
T: +41 22 799 56 40
F: +41 22 799 56 41
Email: europe-info@brocade.com

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

Document History

The table below lists all versions of the Brocade Secure Fabric OS User’s Guide.

Document Title	Publication Number	Publication Date
Brocade Secure Fabric OS User’s Guide Version 2.6	53-0000195-02	January 2001
Brocade Secure Fabric OS User’s Guide Version 3.1.0/4.1.0	53-0005225-02	April 2003

Contents

Preface

Chapter 1 Introducing Secure Fabric OS

Chapter 2 Adding Secure Fabric OS to the Fabric

Chapter 3 Creating Secure Fabric OS Policies

Preface

This manual provides comprehensive information to help you administer your SilkWorm switch and storage area network (SAN). This manual was developed to help technical experts operate, maintain, and troubleshoot networked SAN products. This manual can be used with the other product user manuals referenced or as a standalone document. A list of additional SAN resource reference materials is also included. Thank you for purchasing our product(s). The sections that follow provide:

- A summary of updates to this document.
- The intended audience for this document.
- Information to help you use Brocade documentation.
- Information on additional SAN resources.
- How to get Technical Support.

What's New in This Book

The following changes have been made since this book was last released (part number 53-0000195-02):

- Information that was added:
  - Examples of command output
  - Information about the new Secure Shell feature
  - Recommendation to set the Boot PROM and Recovery passwords (Fabric OS v4.1.0 only)
  - Information about restrictions when downloading firmware in Secure Mode
  - List of commands restricted to the FCS switches when Secure Mode is enabled
  - Procedure for setting up Secure Fabric OS on a SilkWorm 12000
  - Procedure for removing Secure Fabric OS capability from the switch
  - PKI Certificate Utility version 1.0.5 is supported
  - How to auto install digital certificates
  - How to create a PKI Certificate Utility Report
  - How to access PKI Cert Help
  - Secure Fab OS Quick Start Guide is a new reference book
- Information that was modified:
  - The book was reorganized for greater ease of use
- Information that was removed:
  - The specific steps for downloading items from the Web site; contact the switch supplier for the required steps
  - The glossary is now provided as a separate document

Intended Audience

This document is intended for use by systems administrators and technicians experienced with networking, Fibre Channel, and SAN technologies.

Manual Conventions

This section lists text formatting conventions and important notices formats used in this document.

Formatting

The following table describes the formatting conventions that are used in this book:

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 book titles and cross references
`code` text	• identifies CLI output • identifies syntax examples

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.

Related Publications

This section lists additional documentation that you may find helpful.

Brocade Documentation

The following related publications are provided on the Brocade Documentation CD-ROM and on the Brocade Partner Web site:

- **Brocade Fabric OS documentation**
  - *Brocade Diagnostic and System Error Message Reference*
  - *Brocade Fabric OS Procedures Guide*
  - *Brocade Fabric OS Reference*
- **Brocade Fabric OS optional features documentation**
  - *Brocade Advanced Performance Monitoring User's Guide*
  - *Brocade Advanced Web Tools User's Guide*
  - *Brocade Advanced Zoning User's Guide*
  - *Brocade Distributed Fabrics User's Guide*
  - *Brocade Fabric Watch User's Guide*
  - *Brocade ISL Trunking User's Guide*
  - *Brocade QuickLoop User's Guide (v 3.1 only)*
  - *Secure Fabric OS QuickStart Guide*
- **Brocade Hardware documentation**
  - *Brocade SilkWorm 12000 Hardware Reference (for v.4.1 software)*
  - *Brocade SilkWorm 12000 QuickStart Guide (for v4.1 software)*
  - *Brocade SilkWorm 3900 Hardware Reference (for v.4.1 software)*
  - *Brocade SilkWorm 3800 Hardware Reference (for v.3.1 software)*
  - *Brocade SilkWorm 3200 Hardware Reference (for v.3.1 software)*

Release notes are available on the Brocade Partner Web site and are also bundled with the Fabric OS.

Additional Resource Information

For practical discussions about SAN design, implementation, and maintenance, *Building SANs with Brocade Fabric Switches* is available 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

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

How to Get Technical Support

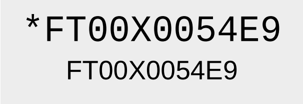
Contact your switch support supplier for hardware, firmware, and software support, including product repairs and part ordering. To assist your support representative and to expedite your call, have the following three sets of information immediately available when you call:

1. **General Information**

   - Technical Support contract number, if applicable
   - switch model
   - switch operating system version
   - error messages received
   - **supportshow** 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 below.

   *FT00X0054E9

   FT00X0054E9

   The serial number label is located as follows:

   - *SilkWorm 2000 series switches:* Bottom of chassis
   - *SilkWorm 3200 and 3800 switches:* Back of chassis
   - *SilkWorm 3900 switches:* Bottom of chassis
   - *SilkWorm 6400 and 12000 switches:* Inside front of chassis, on wall to left of ports

3. **Worldwide Name (WWN)**

   - *SilkWorm 3900 and 12000 switches:* 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.

Introducing Secure Fabric OS

1

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 do the following:

- 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 to provide switch-to-switch authentication.

Overview

This chapter contains the following sections:

Security of Management Channels

Secure Fabric OS can be used to increase the security of the local and remote management channels, including Fabric Manager, Web Tools, standard SNMP applications, Management Server, SES, and a supported command line interface (CLI) client such as sectelnet.

The 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, SES, 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 v2.6.1, v3.1.0, and v4.1.0 all 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.

Secure Shell

Fabric OS v4.1.0 supports Secure Shell, which is a fully encrypted protocol for CLI. Use of Secure Shell requires installation of a Secure Shell client on the host computer. It 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 v4.1.0 supports Secure Shell whether or not Secure Fabric OS is licensed.

To restrict CLI access over the network to Secure Shell, disable telnet as described in *Telnet* on page 1-2.

Secure Shell clients are available in the public domain, and can be located by searching on the internet. Any client that supports Version 2 of the protocol is supported, such as PuTTy or F-Secure.

Fabric OS v4.1.0 also supports the following ciphers for session encryption and HMACs (hash function based message authentication code):

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

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

Sectelnet

Sectelnet is a secure form of telnet that encrypts passwords only. It is available in the public domain and through the switch supplier. Fabric OS v4.1.0 includes the sectelnet server; the sectelnet client must be installed on the workstation computer.

Sectelnet 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 Reference*.

Switch-to-Switch Authentication Using PKI

Secure Fabric OS uses digital certificates based on public key infrastructure (PKI) and switch WWNs 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.

Fabric Configuration Server Switches

Fabric Configuration Server (FCS) switches are one or more switches that are specified as “trusted” switches (switches that are in a physically secure area) 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.

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 is participating in the fabric acts as the primary FCS switch, and 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 provides the current configuration, overwriting the existing configuration of the new switch.

Since the primary FCS switch distributes the zoning configuration, zoning databases do not merge when new switches join the fabric. Instead, the zoning info on the new switches is overwritten when the primary FCS switch downloads zoning to these switches, if Secure Mode is enabled on all the switches. For more information about zoning, refer to the *Advanced Zoning User’s Guide*. For more information about merging fabrics, see *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. A minimum of one backup FCS switch is strongly recommended to reduce the possibility of having no primary FCS switch available. It is possible to designate as many backup FCS switches as desired; 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

Secure Fabric OS supports the creation of several types of policies that can be used to customize various aspects of the fabric. By default, only the FCS policy exists when Secure Mode is first enabled. Secure Fabric OS policies can be created and managed by CLI (serial or telnet) or Fabric Manager.

Secure Fabric OS policies can be created, displayed, modified, and deleted. They can also be created and saved a policy 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 (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.

Available Secure Fabric OS Policies

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.

Chapter

2

Adding Secure Fabric OS to the Fabric

Secure Fabric OS is supported by Fabric OS v2.6.1, v3.1.0, and v4.1.0, and can be added to fabrics that contain any combination of these versions. 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+ to v2.6.1
- SilkWorm 3200 or 3800 switches from Fabric OS v3.0+ to v3.1.0
- SilkWorm 12000 or 3900 switches from Fabric OS v4.0+ to v4.1.0

Overview

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 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 may require access to the website of the switch support supplier. If the supplier is Brocade, navigate to www.brocade.com and click “partner login” at the top of the page (if a partner login is not already assigned, follow the instructions to receive a username and password).

The following steps 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 that was shipped with Fabric OS v3.1.0 or v4.1.0 installed, follow the instructions provided in *Adding Secure Fabric OS to Switches Shipped with Fabric OS v3.1.0 or v4.1.0* 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 switches with any version of Fabric OS v4.x, follow the instructions provided in *Adding Secure Fabric OS to a SilkWorm 12000* on page 2-23.
- 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 not capable of enforcing the Secure Fabric OS policies, then they may segment from the 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 into the switch as admin. The default password is “password”.
3. Enter the **version** command.

   Example

   Entering the **version** command on a SilkWorm 3900:

   ```
   switch3900:admin> version
   Kernel: 2.4.2
   Fabric OS: v4.1
   Made on: Fri Jan 3 23:02:08 2003
   Flash: Jan 3 18:03:35 2003
   BootProm: 4.1.17
   switch3900:admin>
   ```

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

Adding Secure Fabric OS to Switches Shipped with Fabric OS v3.1.0 or v4.1.0

This section applies to the following switches:

- SilkWorm 3200 or 3800 switches shipped with Fabric OS v3.1.0
- SilkWorm 3900 switches shipped with Fabric OS v4.1.0

All switches that are shipped with Fabric OS v3.1.0 or v4.1.0 installed already have the required PKI objects and a digital certificate.

To set up Secure Fabric OS on a switch shipped with Fabric OS v3.1.0 or v4.1.0:

1. Change the account passwords from default values as described in *Customizing the Account Passwords* on page 2-3.
2. If switches running Fabric OS v3.1.0 will be in same fabric as switches running Fabric OS v4.1.0, set the Core PID on the v3.1.0 switches accordingly. Refer to the *Fabric OS Procedures Guide* for instructions.
3. Ensure that the switch has an activated Secure Fabric OS and Zoning software license as described in *Verifying or Activating the Secure Fabric OS and 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 log in and the **passwd** command remains disabled until the passwords are changed from the default values. Changing the passwords immediately 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 into 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 to 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 in a secure place. Recovering passwords can require significant effort and result in fabric downtime.

Verifying or Activating the Secure Fabric OS and Zoning Licenses

The Secure Fabric OS and 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 CLI connection (serial or telnet) to the switch.
2. Log into the switch as admin. The default password is "password".
3. Enter the **licenseshow** command to determine whether the license is already activated.
   A list of all the activated licenses is displayed. The Secure Fabric OS license is displayed as **Security license**.

   Example

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

4. If the Secure Fabric OS and Zoning licenses are already listed, the features are already available and the remaining steps are not required. If either license is not listed, continue with step 5.
5. Contact the switch supplier to purchase the required license key.
6. After the key is received, enter the following:

   ```
   licenseadd "key"
   ```

   key is the license key string exactly as provided by the switch supplier, and is case sensitive. It can be copied from the email in which it was provided directly into the CLI.

   Example

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

7. Enter 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 is displayed as **Security license**).

Adding Secure Fabric OS to Switches that Require Upgrading

This section applies to the following switches:

- SilkWorm 2000-series switches
- SilkWorm 3200 or 3800 switches running a Fabric OS previous to v3.1.0
- SilkWorm 3900 switches running a Fabric OS previous to v4.1.0

To set up Secure Fabric OS on a switch that was not shipped with Fabric OS v3.1.0 or v4.1.0:

1. If switches running Fabric OS v2.6.1 or v3.1.0 will be in same fabric as switches running Fabric OS v4.1.0, set the Core PID on the v2.6.1 and v3.1.0 switches accordingly. Refer to the *Fabric OS Procedures Guide* for instructions.

2. Back up the configuration and upgrade the switch to Fabric OS v2.6.1, v3.1.0, or v4.1.0, 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. 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 Zoning licenses, as described in *Verifying or Activating the Secure Fabric OS and Zoning Licenses* on page 2-7.

6. Download and install the PKICERT utility on the computer workstation, as described in *Installing the PKICERT Utility* on page 2-7.

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 2-13.

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, v2.6.1, v3.1.0, and v4.1.0, 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+ to v2.6.1
- SilkWorm 3200 or 3800 switches from Fabric OS v3.0+ to v3.1.0
- SilkWorm 12000 or 3900 switches from Fabric OS v4.0+ to v4.1.0

Note: Switches running Fabric OS v2.6.1 or v3.1.0 must have the Core PID set to 1 to join a fabric with switches running Fabric OS v4.1.0. For information on setting the Core PID, refer to the *Fabric OS Procedures Guide*.

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 Secure Fabric OS was already in use on the switch (such as on a 2000-series switch running 2.6).
4. Log into 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.
   The required PKI objects are automatically generated when the switch is rebooted in the new version of Fabric OS.
8. Repeat this procedure for each switch in the fabric.

   Note: The PKI objects that are required by Secure Fabric OS are created automatically the first time the switch is booted up.

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 log in and the **passwd** command remains disabled until the passwords are changed from the default values.

Note: 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 v4.1.0 (does not apply to v2.6.1 or v3.1.0). For instructions on setting these passwords, refer to the *Fabric OS Procedures Guide*.

To log in and change the passwords:

1. Open a CLI connection (serial or telnet) to the switch.
2. Log into 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 to 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 in a secure place. Recovering passwords can require significant effort and result in fabric downtime.

Verifying or Activating the Secure Fabric OS and Zoning Licenses

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

Installing the PKICERT Utility

The PKI Certificate Installation utility (named PKICert Utility) version 1.0.5 or later is provided by the switch supplier and is used to generate 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 the same location. The default location is `c:`\security. The utility is installed to a subdirectory named nt_pki. For example, `c:`\security\nt_pki.
3. 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 reports and provides online help.

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.

To obtain the CSR file for the fabric:

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

   The utility prompts for the events log file name.

2. Enter a filename 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.

   Example

   ```
                    PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5

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

   Example

   ```
                    PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5
                                       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. Enter the desired method for entering the fabric addresses.

Example

```
                PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5
                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. Enter **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. Enter 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. Enter the username and password, then press **Enter** to continue.

Example

```
                PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5

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. Enter **2** and press **Enter**.

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

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

Example

```
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. Enter the requested information.

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

   b. Enter **y** to include licensed product data in the file. Otherwise, enter n.

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

Example

```
               PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5
                      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.xml
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. This is not a problem except for the time that might be required to retrieve CSRs and load digital certificates in a very large fabric.

The utility prompts for which fabrics to retrieve CSRs from.

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

Example

```
                  PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5

                        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/failure of CSR retrieval.

7. Press **Enter** to continue.

Example

```
         PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5

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** screen is displayed.

8. To continue installation:

If the user is ready to install their digital certificate(s), select option #2 shown in the **Functions** screen below. Do not quit PKICERT.

Example

```
         PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5
                        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 selection 2 is entered, the following information is displayed.

Example

```
                 PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5
                           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
```

After selecting y (yes), the following information is displayed.

Example

```
                 PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5
                                LOAD CERTIFICATES

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

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

After selecting y (yes) the following information is displayed.

Example

```
                 PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5

                       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

   Enter “**q**” to quit the utility, then enter **y** and press **Enter** to verify you want to quit.

Example

```
       PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5
                      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 Secure Fabric OS directory, for example c:\security\nt_pki\<confirmation number>.xml. Making a backup copy of the digital certificate file and storing it in a secure location is recommended.

Distributing Digital Certificates to the Switches

The PKICERT utility can be used to distribute the digital certificates to the switches in the fabric. The utility ensures that each digital certificate is installed on the correctly corresponding switch.

If the utility is run 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 automatically load digital certificates onto one or more switches while retrieving CSR’s go to step 8 of the previous section titled “Using the PKI Cert Utility”.

To manually load digital certificates onto one or more switches:

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

   The utility prompts for the events log file name.

2. Enter a filename 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.

   Example

   ```
                    PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5

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

   Example

   ```
                    PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5
                                       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. Enter the desired method for entering the fabric addresses.

   Example

   ```
                  PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5
                   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. Enter **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. Enter 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. Enter the username and password, then press **Enter** to continue.

Example

```
                PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5

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. Enter **2** and press **Enter**.

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

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

Example

```
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 filename of the digital certificate file provided by the switch supplier.

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

If the returned path and filename is correct, enter **y** and press **Enter**. If not, enter “**n**”, press **Enter**, reenter the path and filename, then verify it is correct.

Example

```
       PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5
                      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. Enter **1** to distribute certificates only to the fabric identified earlier, or **a** to install certificates to all discovered fabrics, then press **Enter**.

Example

```
                  PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5

                        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.

Example

```
       PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5
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: Sectelnet can be used as soon as a digital certificate is installed on the switch.

8. Press **Enter**.

The **Functions** screen is displayed.

9. Enter “**q**” to quit the utility, then enter **y** and press **Enter** to verify you want to quit.

   Example

```
        PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5
                       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 into one of the switches in the fabric as admin.
2. Display the PKI objects:
   - For Fabric OS v4.1.0, enter **pkishow**. If the switch is a SilkWorm 12000, enter this command on both logical switches.
   - For Fabric OS v2.6.1 and v3.1.0, 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.

Example

Displaying PKI objects on Fabric OS v4.1.0:

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

Displaying PKI objects on Fabric OS v3.1.0:

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

3. Verify that **Certificate** shows **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 2-13.

   If any of the other objects show **Empty** or the command displays an error message, recreate 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 v2.6.0c, v2.6.1, v3.1.0, or v4.1.0 is booted. If any of the PKI objects appears to be missing, the switch segments from the fabric. The PKI objects on Fabric OS v2.6.1, v3.1.0, and v4.1.0 can be regenerated by rebooting the switch. The PKI objects on Fabric OS v4.1.0 can also be regenerated through the following procedure.

To use the CLI to recreate the PKI objects on Fabric OS v4.1.0:

Note: Secure Mode must be disabled to perform this procedure.

1. Log into the switch as admin.
2. Enter the **pkiremove** command. If the switch is a SilkWorm 12000, enter this command on both logical switches.
3. Enter the **pkicreate** command to create new PKI objects. New PKI objects are created without digital certificates. If the switch is a SilkWorm 12000, enter this command on both logical switches. The **pkicreate** command does not work if Secure Mode is already enabled
4. Enter the **pkishow** command. If the switch is a SilkWorm 12000, enter this command on both logical switches.

   The command displays the status of the PKI objects.

   Example

   Recreating PKI objects on Fabric OS v4.1.0:

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

5. Repeat for any other switches, as required.
6. If the switch was segmented from the fabric, log into the switch and enter the **switchdisable** and **switchenable** commands.

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 at any given time.

1. To create a PKI report select option 3 shown in the example below, then follow the screen prompts.

   Example

   ```
          PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5
                         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. Enter the desired method for entering the fabric addresses.

   Example

   ```
                   PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5
                   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. Enter **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. Enter 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. Enter the username and password, then press **Enter** to continue.

Example

```
               PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5

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_
```

Example

```
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. Enter path and filename for the report file to be created, then enter **y** if the address was entered correctly. If not, enter **n** and reenter the address.

b. Enter **y** to include licensed product data in the file. Otherwise, enter n.

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

Example

```
               PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5
                      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. Enter **1** to write certificate reports only to the fabric identified earlier, or **a** to write certificate reports to all discovered fabrics, then press **Enter**.

   Example

```
                  PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5

                        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
```

   Example

```
                  PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5

                  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. Enter “**q**” to quit the utility, then enter **y** and press **Enter** to verify you want to quit.

   Example

```
         PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5
                        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 (CLI) information about PKI Cert and obtain advice on advanced options for power users.

1. To access PKI help select option 4 as shown in the example below, then follow the screen prompts.

Example

```
        PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5
                       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
```

Example

```
       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, v3.1, v4.1)

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_
```

Example

```
       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> y_
```

Example

```
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.**

Example

```
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

This procedure applies to all SilkWorm 12000 switches, whether they are shipped with Fabric OS v4.1.0 or require upgrading to Fabric OS v4.1.0.

Caution: If one or both of the logical switches in a SilkWorm 12000 is in Secure Mode, it is strongly recommended that the logical switches be in the same fabric. Placing the two switches from the same SilkWorm 12000 in separate fabrics is not supported if Secure Mode is enabled on one or both switches.

To set up Secure Fabric OS on a SilkWorm 12000:

Note: The CLI messages from each logical switch may display in both CLI sessions.

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 v4.1.0 (and therefore already has a digital certificate).

   Note: Fabric OS v4.1.0 maintains separate login accounts for each logical switch.

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

   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.

   Example

   ```
   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: 4.1.13b
   SW12000:admin>
   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
   SW12000:admin>
   ```

3. If the firmware version is not Fabric OS v4.1.0 or later, back up the configuration and install Fabric OS v4.1.0 on both CP cards. For instructions, refer to *Upgrading to a Compatible Version of Fabric OS* on page 2-6.

4. Log into 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 into 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 v4.1.0, the server must support a full NTP client. For switches running Fabric OS v2.6.1 or 3.1.0, the server can be SNTP or NTP.

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

   b. Enter the following:

      `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.

Example

```
SW12000switch0:admin> tsclockserver "132.163.135.131"
switch:admin> tsclockserver
132.163.135.131
SW12000switch0:admin>
SW12000switch0:admin>login
login: admin
Password: xxxxxx
12000switch1:admin> tsclockserver "132.163.135.131"
12000switch1:admin> tsclockserver
132.163.135.131
SW12000switch1:admin>
```

6. Ensure that both logical switches have a Secure Fabric OS license activated, as described in *Verifying or Activating the Secure Fabric OS and 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 Zoning license activated, as described in *Verifying or Activating the Secure Fabric OS and 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 2-7.

   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 2-13.

   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 supported for switches running Fabric OS v2.6.1, v3.1.0, or v4.1.0. For instructions on installing the sectelnet client, see *Installing the Sectelnet Client on a Computer Workstation* on page 2-26.
- SSH
  SSH is a secure form of telnet that is supported only for switches running Fabric OS v4.1.0. Fabric OS v4.1.0 supports any SSH client that supports version 2 of the protocol (for example, PuTTy or F-Secure). Refer to the *Fabric OS Procedures Guide* for client installation instructions.

Installing the Sectelnet Client on a Computer Workstation

Sectelnet is provided on the Brocade partner website. It can be used as soon as a digital certificate is installed on the switch.

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 **path** 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.

Chapter

3

Creating Secure Fabric OS Policies

The 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.

Implementing Secure Fabric OS policies requires the following steps:

- Determining which trusted switches to use as FCS switches to manage Secure Fabric OS. These switches should be in a physically secure area.
- Enabling Secure Mode in the fabric, and specifying the trusted switch and one or more backup trusted switches. This automatically creates the FCS policy.
- Determining which additional Secure Fabric OS policies to implement in the fabric, then creating and activating those policies. An access policy must be created for each management channel that will be used.
- Verifying 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, see *Troubleshooting* on page 4-18.

Overview

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 and is a SilkWorm 2000-series switch or later.
  - All switches in the fabric can be accessed through serial port.
  - All switches in the fabric that have front panels (SilkWorm 2000 series switches) can be accessed through front panel.
- Computer hosts and workstations:
  - Any computer can access the fabric by SNMP.
  - Any computer can access any switch in the fabric by CLI (such as by sectelnet or Secure Shell).
  - Any computer can establish an HTTP connection to any switch in the fabric.
  - Any computer 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 recreated 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 Reference*.

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:

- Requests the password for the current login
- Requests new passwords for Secure Mode
- Creates and activates the FCS policy
- Distributes the policy set (initially consisting only of FCS policy) to all switches in the fabric
- Activates and distributes the local zoning configurations
- Fastboots all switches in the fabric to bring the fabric up in Secure Mode (for the SilkWorm 12000, this causes the active CP card to fail over to the standby)

No other policies are created except for the FCS policy, and no other Secure Fabric OS-related changes occur to the fabric other than the implementation of the FCS policy. Other Secure Fabric OS policies can be created after the fastboots are complete.

Caution: If one or both of the logical switches in a SilkWorm 12000 is in Secure Mode, it is strongly recommended that the logical switches be in the same fabric. Placing the two switches from the same SilkWorm 12000 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.
- A number of commands can only be entered from the FCS switches. Refer to *Command Restrictions in Secure Mode* on page A-5 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*.

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

To enable Secure Mode in the fabric:

Note: Enabling Secure Mode fastboots all the switches in the fabric.

1. Ensure that all switches in the fabric have the following items:
   - Fabric OS v2.6, v2.6.1, v3.1.0, or v4.1.0
   - An activated Secure Fabric OS license
   - An activated 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*.
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 into 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. Enter the **secmodeenable** command with no operands to use the command's interactive mode, then identify each FCS switch at the prompts (see example). Press **Enter** with no data to end the FCS list.

   Alternatively, enter the command followed by the FCS switches:

   ```
   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.

Example

Enabling Secure Mode and specifying three FCS switches, one each by domain ID, WWN, and switch name, on Fabric OS v3.1.0 (v4.1.0 may differ slightly), using the command's interactive mode

```
primaryfcs:admin> secmodeenable
This is an interactive session to create a FCS list.

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

Current FCS list is empty
Enter WWN, Domain, or switch name(Leave blank when done): 2
Switch WWN is 10:00:00:60:69:11:fc:54

Current FCS list:
  10:00:00:60:69:11:fc:54

Enter WWN, Domain, or switch name(Leave blank when done): 10:00:00:60:69:11:fc:55
Switch WWN is 10:00:00:60:69:11:fc:55

Current FCS list:
  10:00:00:60:69:11:fc:54
  10:00:00:60:69:11:fc:55

Enter WWN, Domain, or switch name(Leave blank when done): SilkWorm 24
Switch WWN is 10:00:00:60:69:11:fc:56

Current FCS list:
  10:00:00:60:69:11:fc:54
  10:00:00:60:69:11:fc:55
  10:00:00:60:69:11:fc:56

Enter WWN, Domain, or switch name(Leave blank when done):
Are you done?  (yes, y, no, n): [no] y
Is the FCS correct?  (yes, y, no, n): [no] y
```

The command requests active consent to the terms of the license, requests the identity of the FCS switches, then requests the new passwords required for Secure Mode.

7. Enter the following passwords at the prompts, using unique passwords that are different from the default values and contain between 8 to 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.

   Example

   Entering 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...
primaryfcs:admin>
```

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

   Note: Record the passwords and store in a secure place. Recovering passwords may 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, and can be aborted 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 3-7.
- Using the **secfcsfailover** command to fail over the primary FCS switch to the next switch in the list, as described in *Failing Over the Primary FCS Switch* on page 3-8.
- 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 3-10.

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 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.

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 into the primary FCS switch as admin.
2. Enter the following:

```
secpolicyshow “Defined”, “FCS_POLICY”
```

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

3. Enter the **`secpolicyfcsmove`** command, 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.

   To is the desired position in the list for this switch.

   Example

   Moving 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.
____________________________________________________
primaryfcs:admin>
```

4. Enter the **secpolicyactivate** command.

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.

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. If desired, view the current FCS list by logging in as admin to the current primary FCS switch from a sectelnet or Secure Shell session and entering the following:

   ```
   secpolicyshow "active","FCS_POLICY"
   ```

   Example

   Entering **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
   fcsswitcha:admin> logout
   ```

2. From a sectelnet or Secure Shell session, log in as admin to the backup FCS switch to be designated as the new primary FCS switch and enter the **secfcsfailover** command.

   Entering **secfcsfailover** from the backup FCS switch “fcsswitchc”, then **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>
   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
   fcsswitchc:admin>
   ```

   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 in the list.

Creating Secure Fabric OS Policies Other Than the FCS Policy

The FCS policy is automatically created when Secure Mode is enabled, and other Secure Fabric OS policies can be created after Secure Mode is enabled. 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 upper case. 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 Reference*.

Policy members can be specified by device port WWN, switch WWN, domain IDs, or switch WWN, 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:	No	No	No	No	No
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, see *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” can be used in an octet to indicate that any number can be matched for that octet. For example, 192.168.11.0 would allow access for all IP devices in the network 192.168.11.
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.

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 *Creating an SNMP Policy* on page 3-13.

Note: If an SNMP policy is created, it must contain the primary FCS switch and backup FCS switches to ensure consistent read/write access to the primary FCS switch, even in the event of a failover.

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
Non-existent	Non-existent	Any host can read	Any host can write
Non-existent	Empty	Any host can read	No host can write
Non-existent	Host B in policy	Any host can read	Only B can write
Empty	Non-existent	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
Empty	Host B in policy	Only B can read	Only B can write
Host A in policy	Non-existent	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

Creating an SNMP Policy

1. From a sectelnet or Secure Shell session, log into the primary FCS switch as admin.
2. Enter the following:

   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.

   Example

   Creating an WSNMP and an RSNMP policy to only allow IP addresses that match 192.168.5.0 to read and write access to the fabric.

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

3. To save or activate the new policy, enter the **secpolicysave** or the **secpolicyactivate** command.

   If neither of these commands are 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 3-25.

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 is in Secure Mode, sectelnet / SSH sessions cannot be opened to the active CP card. This prevents potential violation of the Telnet policy, since the active CP card can be used to access either of the logical switches on the SilkWorm 12000. However, sectelnet / SSH sessions can be established to the IP addresses of the logical switches and to the standby CP card, if allowed by the Telnet policy. If the active CP card fails over, any sectelnet / SSH sessions to the standby CP card are automatically terminated when the standby CP card becomes the active CP card.

How to create a Telnet policy is described in *Creating a Telnet Policy* on page 3-14.

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. Sectelnet can be used 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.

Creating a Telnet Policy

1. From a sectelnet or Secure Shell session, log into the primary FCS switch as admin.
2. Enter the following:

   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 the **secpolicysave** or the **secpolicyactivate** command.

   If neither of these commands are 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 3-25.

   Example

   Creating a Telnet policy to allow anyone on a network “192.168.5.0/24” 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.
   primaryfcs:admin>
   ```

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 *Creating an HTTP Policy* on page 3-15.

The possible HTTP policy states are shown in Table 3-5.

Table 3-5 HTTP Policy States

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

Creating an HTTP Policy

1. From a sectelnet or Secure Shell session, log into the primary FCS switch as admin.
2. Enter the following:

   ```
   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 the **secpolicysave** or the **secpolicyactivate** command.

   If neither of these commands are 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 3-25.

   #### Example

   Creating 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.
   primaryfcs:admin>
   ```

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 in *Creating an API Policy* on page 3-16.

The possible API policy states are shown in Table 3-6.

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.

Creating an API Policy

1. From a sectelnet or Secure Shell session, log into the primary FCS switch as admin.
2. Enter the following:

   `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 the **secpolicysave** or the **secpolicyactivate** command.

   If neither of these commands are 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 3-25.

   Example

   Creating 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.
   primaryfcs:admin>
   ```

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 the switch.

How to create an SES policy is described in *Creating an SES Policy* on page 3-17.

The possible SES policy states are shown in Table 3-7.

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.

Creating an SES Policy

1. From a sectelnet or Secure Shell session, log into the primary FCS switch as admin.
2. Enter the following:

    `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 the **secpolicysave** or the **secpolicyactivate** command.

    If neither of these commands are 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 3-25.

    Example

    Creating 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.
primaryfcs:admin>
```

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 in *Creating a Management Server Policy* on page 3-18. The possible Management Server policy states are shown in Table 3-8.

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.

Creating a Management Server Policy

1. From a sectelnet or Secure Shell session, log into the primary FCS switch as admin.
2. Enter the following:

   secpolicycreate *“policy_name”, “member;...;member”*

   Policy_name is MS_POLICY.

   Member is a device WWN.

3. To save or activate the new policy, enter the **secpolicysave** or the **secpolicyactivate** command.

   If neither of these commands are 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 3-25.

   Example

   Creating 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.
primaryfcs:admin>
```

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 in *Creating a Serial Port Policy* on page 3-18.

The possible serial port policy states are shown in Table 3-9.

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.

Creating a Serial Port Policy

1. From a sectelnet or Secure Shell session, log into the primary FCS switch as admin.
2. Enter the following:

   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 the **secpolicysave** or the **secpolicyactivate** command.

   If neither of these commands are 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 3-25.

   Example

   Creating 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.
primaryfcs:admin>
```

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 in *Creating a Front Panel Policy* on page 3-19.

The possible Front Panel policy states are shown in Table 3-10.

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.

Creating a Front Panel Policy

1. From a sectelnet or Secure Shell session, log into the primary FCS switch as admin.
2. Enter the following:

   `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 the **secpolicysave** or the **secpolicyactivate** command.

   If neither of these commands are 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 3-25.

Example

Creating 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.
primaryfcs:admin>
```

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 may also be used for one of the device ports, as may 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 in *Creating an Options Policy* on page 3-20.

The possible Options policy states are shown in Table 3-10.

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.

Creating an Options Policy

1. Log into the primary FCS switch as admin from a sectelnet or Secure Shell session.
2. Enter the following:

   ```
   secpolicycreate “OPTIONS_POLICY”, “NoNodeWWNZoning”
   ```

3. To save or activate the new policy, enter the **secpolicysave** or the **secpolicyactivate** command.

   If neither of these commands are 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 3-25.

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.

   Example

   ```
   primaryfcs:admin> secPolicyCreate “OPTIONS_POLICY”, “NoNodeWWNZoning”
   OPTIONS_POLICY has been created.
   primaryfcs:admin>
   ```

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, and the same device ports and switch ports may 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.

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, instead of a separate DCC policy for each port.

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, then a semicolon, then 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 in *Creating a DCC Policy* on page 3-22.

The possible DCC policy states are shown in Table 3-12.

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. 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 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.

Creating a DCC Policy

1. From a sectelnet or Secure Shell session, log into the primary FCS switch as admin.
2. Enter the following:

   secpolicycreate *“DCC_POLICY_nnn”, “member;...;member”*

   DCC_POLICY_nnn is the name of the DCC policy to be created, and *nnn* is a string consisting of up to 19 alphanumeric or underscore characters to differentiate it from any other DCC policies.

   Member contains device and switch port information: deviceportWWN;switch(port).

   - The “deviceportWWN” is the WWN of the device port.
   - The “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 the **secpolicysave** or the **secpolicyactivate** command.

   If neither of these commands are 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 3-25.

Examples

Creating 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)”
primaryfcs:admin>
```

Creating 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[*]”
primaryfcs:admin>
```

Creating 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)”
primaryfcs:admin>
```

Creating 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]”
primaryfcs:admin>
```

Creating an SCC Policy

The SCC policy can be 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 can accept members listed as WWNs, domain IDs, or switch names. Only create one SCC policy can 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.

How to create an SCC policy is described in *Creating an SCC Policy* on page 3-23.

Note: If an SCC policy is created, it must list all the switches in the fabric to prevent switches from being segmented from the fabric.
In particular, ensure that the SCC policy lists all the members of the FCS policy, to ensure consistent access to the primary FCS switch.

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

Table 3-13 SCC Policy States

Policy State	Characteristics
No policy	All switches can be in the fabric.
Policy with no entries	The SCC policy cannot be empty. The policy must contain all the FCS switches.
Policy with entries	The SCC policy must contain all the FCS switches, and can also contain additional switches.

Creating an SCC Policy

1. Log into the primary FCS switch as admin from a sectelnet or Secure Shell session.
2. Enter the following:

   ```
   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 the **secpolicysave** or the **secpolicyactivate** command.

   If neither of these commands are 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 3-25.

   Example

   Creating an SCC policy that allows switches that have domain IDs 2 and 4 to join the fabric:

```
primaryfcs:admin> secPolicyCreate "SCC_POLICY", “2;4”
primaryfcs:admin>
```

Managing Secure Fabric OS Policies

All Secure Fabric OS transactions can 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.

Saving Changes to Secure Fabric OS Policies

It is possible to 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 the changes:

1. From a sectelnet or Secure Shell session, log into the primary FCS switch as admin.
2. Enter the **secpolicysave** command.

Example

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

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 into the primary FCS switch as admin.
2. Enter the **secpolicyactivate** command.

Example

```
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
primaryfcs:admin>
```

Adding a Member to an Existing Policy

Members can be added to policies 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 into the primary FCS switch as admin.
2. Enter the following:

   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.

Examples

Adding 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.
primaryfcs:admin>
```

Adding an SNMP manager to WSNMP_POLICY:

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

Adding 2 devices to the DCC policy, to attach domain 3’s 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)"
primaryfcs:admin>
```

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 into the primary FCS switch as admin.
2. Enter the following:

   `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, and is identified by IP address, switch domain ID, device or switch WWN, or switch name.
3. To implement the change immediately, enter the **secpolicyactivate** command.

Example

Removing 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. .
primaryfcs:admin>
```

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 into the primary FCS switch as admin.
2. Enter the following:

   `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.

Example

```
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.
primaryfcs:admin>
```

Aborting All Uncommitted Changes

The **secpolicyabort** command can be used 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 into the primary FCS switch as admin.
2. Enter the **secpolicyabort** command.

   All changes since the last time the **secpolicysave** or **secpolicyactivate** commands were entered are aborted.

   ### Example

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

Aborting a Secure Fabric OS Transaction

The **sectransabort** command can be used 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 into the primary FCS switch as admin.
2. Enter the **sectransabort** command.

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

   ### Example

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

Chapter

4

Managing Secure Fabric OS

Secure Fabric OS v2.6.1, 3.1.0, and 4.1.0 can be managed through Fabric Manager and sectelnet. In addition, Secure Shell is supported for Fabric OS v4.1.0. 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 command and related restrictions, see *Secure Fabric OS Commands and Secure Mode Restrictions* on page A-1.

Overview

This chapter contains the following sections:

- *Viewing Secure Fabric OS Information* on page 4-1
- *Displaying and Resetting Secure Fabric OS Statistics* on page 4-5
- *Managing Passwords* on page 4-9
- *Resetting the Version Number and Time Stamp* on page 4-13
- *Adding Switches and Merging Fabrics with Secure Mode Enabled* on page 4-14
- *Troubleshooting* on page 4-18
- *Frequently Asked Questions* on page 4-21

Viewing Secure Fabric OS Information

The following Secure Fabric OS information is available:

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

The **secfabricshow** command can be used 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. Enter the **secfabricshow** command.
   The command displays the switches in the fabric and their status (ready, error, busy).

   Example

```
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
primaryfcs:admin>
```

Viewing the Secure Fabric OS Policy Database

The **secpolicydump** command can be used 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 into the primary FCS switch as admin.
2. Enter the following:

   `secpolicydump` *`“listtype”, “policy_name”`*

   Listtype is the type of Secure Fabric OS policy set, and 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.

Example

Displaying 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
____________________________________________________
primaryfcs:admin>
```

Displaying Individual Secure Fabric OS Policies

The **secpolicyshow** command can be used to view 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 into the primary FCS switch as admin.
2. Enter the following:

   `secpolicyshow` *`“listtype”, “policy_name”`*

   Listtype is the type of Secure Fabric OS policy set, and 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.

Example

Showing 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

____________________________________________________
primaryfcs:admin>
```

Showing 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

____________________________________________________
primaryfcs:admin>
```

Displaying Status of Secure Mode

The **secmodeshow** command can be used to determine whether Secure Mode is enabled.

To determine whether Secure Mode is enabled:

1. From a sectelnet or Secure Shell session, to the primary FCS switch and log in as admin.
2. Enter 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.

Example

```
primaryfcs:admin> secmodeshow
Secure Mode: ENABLED.
Version Stamp: 10354, Thu Oct  4 10:23:32 2001.
Pos   Primary WWN                     DId swName.
=================================================
1   Yes     10:00:00:60:69:11:fc:53   2 primaryfcs.
2   No      10:00:00:60:69:11:fc:55   1 backupswitch.
primaryfcs:admin>
```

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 into 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.

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 v4.1.0 increases the counter by 1 for each drive in a JBOD; Fabric OS v3.1.0 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 timestamp 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
SLAP 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; may 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

The **secstatsshow** command can be used 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 “list” operand is specified. If the “list” operand is not specified, this command can be entered from any switch in the fabric.

To display Secure Fabric OS statistics:

1. Log into the primary FCS switch as admin from a sectelnet or Secure Shell session.
2. Enter the following:

   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.

Example

Displaying Secure Fabric OS statistics for the Management Server Policy:

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

Resetting Secure Fabric OS Statistics

The **secstatsreset** command can be used to reset statistics for a particular policy or all policies to zero. 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 zero:

1. Log into 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. Reset the statistics by entering the following:

   ```
   secstatsreset “name”, “list”
   ```

   - *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 zero.

   The specified statistics are reset to zero.

   Example

   Resetting 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.
   primaryfcs:admin>
   ```

   Resetting the DCC_POLICY statistics on domains 1 and 69:

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

Managing Passwords

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 remains 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 remains 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.

If a digital certificate is installed, the sectelnet, API, and HTTP passwords are automatically encrypted, regardless of whether Secure Mode is enabled.

Note: Record the passwords and store in a secure place; recovering passwords may require significant effort and result in fabric downtime.
For information about recovering lost passwords, refer to the *Fabric OS Procedures Guide*.

This section provides the following information:

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

To modify the passwords:

1. From a sectelnet or Secure Shell session, log into 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. Enter the **passwd** command.
3. Enter the new passwords at the prompts. The passwords can be anywhere from 8 to 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 re-initiated if access is required.

   Example

```
primaryfcs:admin> passwd
For username - admin
Old password:
New password:
Re-enter new password:
For username - user
New password:
Re-enter new passwd:
primaryfcs:admin>
```

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 into the primary FCS switch as admin.
2. Enter the **secnonfcspasswd** command.
3. Enter 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. Re-enter 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.

   Example

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

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 regular passwords. The regular passwords also remains in effect. Temporary passwords can be removed and are also automatically lost 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 into the primary FCS switch as admin.
2. Enter the following:

   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. Enter the admin password at the prompt.
4. Enter an alphanumeric password between 8 and 40 characters in length.
5. Re-enter the password exactly as entered the first time.

Example

Creating 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.
primaryfcs:admin>
```

Removing a Temporary Password from a Switch

The **sectemppasswdreset** command can be used to remove the temporary password. The regular password remains in effect.

To remove the temporary password from a switch:

1. From a sectelnet or Secure Shell session, log into the primary FCS switch as admin.
2. Enter the following:

   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.

Example

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
switch: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 the oldest time stamp is kept. When merging fabrics, ensure that the time stamp of the database you want to preserve is non-zero, then set the time stamp of all other fabrics to zero. To ensure that the time stamp of a fabric is non-zero, 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 into the primary FCS switch as admin.
2. Enter the **secmodeshow** command.

To reset the time stamp of a fabric to zero:

1. From a sectelnet or Secure Shell session, log into the primary FCS switch as admin.
2. Enter 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 non-zero stamp, and all the other fabrics being merged must have zero version stamps. The Security policy set, zoning configuration, password information, and SNMP community strings are overwritten by the fabric whose version stamp is non-zero. Before merging, verify that the fabric that contains all the desired information has the non-zero stamp.

Note: 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 act 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; cannot join fabric until a primary FCS switch is available (to specify primary FCS switch, enter secmodeenable).	Segments from fabric.
Has Secure Mode disabled.	Standard operation.	Segments from fabric.	Segments from fabric.	Standard operation.

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

Note: Although this 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.

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).
2. Ensure that all switches to be merged are running Fabric OS v2.6.1, v3.1.0, or v4.1.0.
   a. Open a CLI connection (serial or telnet) to one of the switches in the fabric.
   b. Log into the switch as admin. The default password is “password”.
   c. Enter the **version** command. If the switch is a SilkWorm 12000, you can also enter the **firmwareshow** command.
   d. If the switch is not running Fabric OS v2.6.1, v3.1.0, or v4.1.0, 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 2-3.
   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 v2.6.1 or v3.1.0 and switches running Fabric OS v4.1.0, the switches running v2.6.1 or v3.1.0 must have the Core PID set to 1. This parameter is available through the **configure** command; for more information about the Core PID, refer to the *Fabric OS Procedures Guide*.
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 Reference*.
5. Ensure that all switches to be merged have an activated Secure Fabric OS and Zoning license, as described in *Verifying or Activating the Secure Fabric OS and 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, root certificate) and a digital certificate installed.
   a. Log into the switch as admin.
   b. Enter the command supported by the Fabric OS installed on the switch:
      - For Fabric OS v4.1.0, enter **pkishow**.
      - For Fabric OS v2.6.1 and v3.1.0, 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 the objects show **Exist**.
      If the digital certificate shows as **Empty**, repeat the procedure provided in *Distributing Digital Certificates to the Switches* on page 2-13. If any of the PKI objects other than the digital certificate show as **Empty**, you can either reboot the switch to automatically recreate the objects, or recreate 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, 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 non-zero version stamp, by logging into the fabric and entering the **secstatsshow** command. If this fabric does not show a non-zero version stamp, modify a policy and enter either the **secpolicysave** or **secpolicyactivate** command to create a non-zero stamp. Set the version stamp of the other fabrics to zero by logging into each fabric and entering the **secversionreset** command.

13. If fabrics are being 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 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 may 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.	Enter 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.	Enter 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 are segmented from the fabric.”
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.	Enter 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 into 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.

Table 4-5 Recovery Processes

Symptom	Possible Causes	Recommended Actions
A device or switch port listed in the SCC or in a DCC policy cannot be accessed.	Switch port may be disabled.	Enter the **switchshow** command. If the port in question is disabled, enter the **portenable** command. If the port still cannot be accessed, enter the **portenable** command for the port on the other switch.
One or more CLI sessions are automatically logged out.	Password may have been modified for login account in use, or the **secmodeenable** command may have been issued.	Try closing and reopening CLI session.
On a SilkWorm 12000, the CLI messages do not reflect switch status.	The CLI messages are pertaining to the other logical switch.	Verify switch or policy status by entering the **switchshow** or **secpolicyshow** commands.
CLI session freezes or cannot be established after Secure Mode is enabled.	CP card failed over and network routing cache(s) require updating.	Try closing and reopening CLI session. If this fails, request that 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 the correct policy name was used. Policy names must be entered in all upper case 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 card of a SilkWorm 12000. Or, a session to the standby CP card is disconnected when it becomes the active CP card.	Sectelnet/SSH sessions cannot be established to the IP address of the active CP card in Secure Mode. This enables enforcement of Telnet policy for each logical switch.	Establish a sectelnet/SSH sessions to the IP addresses of the logical switches or the standby CP card 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, and 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.	CP cards failed over during process of enabling Secure Mode.	Enter secmodeenable again on the segmented switch, using the same FCS list as used before.

Table 4-5 Recovery Processes

Symptom	Possible Causes	Recommended Actions
One or more switches are 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 Reference*.
	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 re-enable the switches.
	FCS policies on the segmented switches are not identical to the FCS policy of the fabric.	If one or more switches are 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 are automatically fastbooted. If one or more switches are 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. May be due to no primary FCS switch being available to propagate changes across fabric.	Enter the **secmodeenable** command to specify a new primary FCS switch. Specify adequate backup FCS switches to prevent a recurrence. Then, for each segmented portions of the fabric that does not contain the new Primary FCS switch, reset the version stamp to “0” by entering the following commands: **switchdisable**, **secversionreset**, and **switchenable**.
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.

Table 4-5 Recovery Processes

Symptom	Possible Causes	Recommended Actions
Passwords that should be consistent across the fabric are not consistent.	A password recovery operation may have been performed on one or more switches.	To make the passwords the same, log into the switch that had the password recovered and enter the **secversionreset** command, followed by **switchdisable** and **switchenable** commands.
Unsaved changes to the policies are lost.	The primary FCS switch may have failed over.	Reenter the changes then enter the **secpolicysave** or **secpolicyactivate** command.

Frequently Asked Questions

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 (SFO100), 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 website at http://www.brocade.com/products/software.jhtml.
- Best practice guides, SOLUTIONware, white papers, online demos, data sheets, and other documentation is available through the Brocade Partner website, including the *SAN Security Best Practice Guide*.
- The CERT® Coordination Center of Carnegie Mellon University provides industry level information about certification, and is located at *http://www.cert.org*

Which switches and fabrics support Secure Fabric OS?

Any SilkWorm switch that is running Fabric OS v2.6.0.c, v2.6.1, v3.1.0, or v4.1.0, as appropriate to the switch. This includes Silkworm 2000-series, 6400, 3200, 3800, 3900, and 12000 switches.

Secure Fabric OS may be implemented across fabrics containing any mixture of 1 Gbit/sec or 2 Gbit/sec switches running v2.6.1, v3.1.0, or v4.1.0. If SilkWorm 2000-series switches will be in the same fabric as switches running Fabric OS v3.1.0 or v4.1.0, then the 2000-series switches must be running Fabric OS v2.6.1.

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 v2.6.1, v3.1.0, and v4.1.0 support the sectelnet client.
  Secure Fabric OS v4.1.0 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% 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 3-10.

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 v4.1.0 support?

Fabric OS v4.1.0 supports version 2 of the SSH protocol. Any SSH client that supports version 2 of the protocol is supported. For example, PuTTy 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 supported for Fabric OS v2.6.1, v3.1.0, and v4.1.0, and SSH is also supported for v4.1.0.

Is SSH part of the Secure Fabric OS feature?

No, SSH is automatically included with Fabric OS v4.1.0, regardless of whether the Secure Fabric OS license is activated.

Digital Certificates and PKI Objects

What is PKI?

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

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 v2.6.0, v2.6.1, v3.1.0, or v4.1.0 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 v2.6.0, v3.1.0, or v4.1.0 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 v4.1.0, enter the **pkishow** command. For earlier versions, 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 re-enabled until they are regenerated. If any PKI objects are missing, all the PKI objects should be deleted using the **pkiremove** command, 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 2-13.

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.

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 will segment.

What happens to the zoning information when fabrics are merged?

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

Passwords

What if I forget the root password?

Refer to *Managing Passwords* on page 4-9.

Secure Fabric OS Commands and Secure Mode Restrictions

A

Secure Fabric OS commands, zoning commands, and some Management Server commands must be entered through the primary FCS switch.

Overview

This appendix provides the following information:

- *Secure Fabric OS Commands* on page A-1
- *Command Restrictions in Secure Mode* on page A-5

For more detailed information about commands, refer to the *Fabric OS Reference*.

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-5.

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?
pkicreate	Admin	Recreates the PKI objects on the switch. See *Recreating PKI Objects If Required* on page 2-18.	Non-secure Mode	N/A
pkiremove	Admin	Removes the PKI objects from the switch.	Non-secure 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 FOS database.	Both	Any
secdefinesize	Admin	Displays the size of the defined Secure FOS 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 3-8.	Secure Mode	Backup FCS switch
secglobalshow	Admin	Displays current state information for Secure FOS, 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.	Non-secure Mode Avail. 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 n the active policy set. See *Activating Changes to Secure Fabric OS Policies* on page 3-25.	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 3-10.	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 3-7.	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

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?
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 zero. 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
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	No	No
cfgadd	Yes	No	No
cfgclear	Yes	No	No
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
cfgtransabort	Yes	No	No
cfgtransshow	Yes	No	No
fazoneadd	Yes	No	No
fazonecreate	Yes	No	No
fazonedelete	Yes	No	No
fazoneremove	Yes	No	No
fazoneshow	Yes	No	No
qloopadd	Yes	No	No
qloopcreate	Yes	No	No
qloopdelete	Yes	No	No

Table A-2 Zoning Commands (Continued)

Command	Primary FCS switch	Backup FCS switch	Non-FCS switch
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
cfgshow	Yes	Yes	No
cfgsize	Yes	Yes	Yes
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, but read only	Yes, but 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

Table A-3 Miscellaneous Commands (Continued)

Command	Primary FCS switch	Backup FCS switch	Non-FCS switch
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
tsclockserver	Yes	Yes	Yes
tsclockserver <IP address of network time protocol (NTP) server>	Yes	No	No
wwn (display only; cannot modify WWNs in Secure Mode)	Yes	Yes	Yes

Removing Secure Fabric OS Capability

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 only disabling Secure Mode and leaving the Secure Fabric OS feature available so that Secure Mode can be re-enabled 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.

Overview

Disabling Secure Mode includes the following steps:

- *Preparing the Fabric for Removal of Secure Fabric OS Policies* on page B-1
- *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-2
- *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 website.

The following steps 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 recreated 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 Reference*.

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 re-enabling Secure Mode, see *Enabling Secure Mode* on page 3-2.

1. From a sectelnet, Secure Shell, or serial session, log into the primary FCS switch as admin.
2. Enter **secmodedisable**.
3. Enter the password when prompted.
4. Enter **y** to verify 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.

Example

```
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.
primaryfcs:admin>
```

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 licence 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. Enter the **licenseidshow** command to display the Secure Fabric OS license key.
3. Enter the following:

   `licenseremove` “*key*”

   key is the license key, and is case sensitive. It can be copied from the **licenseshow** output directly into the CLI.
4. Repeat for each switch in the fabric.

   Example

```
switch:admin> licenseremove “1A1AaAaaaAAAA1a”
removing license-key “1A1AaAaaaAAAA1a”
Committing configuration...done.
For license to take effect, Please reboot switch now....
switch:admin>
```

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.

Index