Secure Fabric OS

QuickStart Guide

Publication Number *53-0000352-01*

 Publication Number *53-0000352-01*

Corporate Headquarters
Brocade Communications Systems, Incorporated
1745 Technology Drive
San Jose, CA 95110
U.S.A.
T: (408) 487-8000
F: (408) 487-8101
info@brocade.com

European Headquarters
Brocade Communications Switzerland Sàrl
29, route de l’Aéroport
Case Postale 105
1215 Genève 15,
Switzerland
T: +41 22 799 56 40
F: +41 22 799 56 41
europe-info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems K.K.
The Imperial Tower 15th Floor
1-1-1 Uchisaiwaicho
Chiyoda-ku, Tokyo 100-0011
Japan
T: +81 33507 5802
F: +81 33507 5900
apac-info@brocade.com

Overview

Brocade Secure Fabric OS is an optional licensed software product that you can use to increase the security of a SilkWorm switch fabric. Secure Fabric OS is supported by Brocade Fabric OS v2.6.1, v3.1, and v4.1, and can be implemented in fabrics that contain any combination of these versions.

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

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

1. A compatible version of the Fabric OS
2. An activated Secure Fabric OS license key
3. An activated Zoning license key (zoning is essential to Secure Fabric OS mechanisms)
4. The required Public Key Infrastructure (PKI) objects
5. A digital certificate

Obtaining these items for each switch may require access to the website of your switch supplier. If your supplier is Brocade, you can access the Brocade Partner Site by navigating to www.brocade.com and clicking "partner login" at the top of the page.

Note: If you do not already have a Partner login, follow the instructions to receive a username and password.

From the Brocade Partner site, select: *For Technical Professionals\Tools\Secure Fabric OS Upgrade* to access the *Secure Fabric OS - Field Upgrade Process* web page. This web page includes all the links/resources you may need to build a basic Secure Fabric OS SAN.

Follow the procedure outlined in the *Field Upgrade Process* section of this guide to set up a fabric for use with Secure Fabric OS, and then enable the Secure Fabric OS SAN (see *Enabling Secure Mode in the Fabric*). Refer to *Where to Go From Here* and *Frequently Asked Questions* for additional information about Secure Fabric OS SANs.

Field Upgrade Process

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

   There are two methods you can use to obtain version information about Fabric OS on a Brocade Switch:

   - Use the switch's "WebTools" utility by pointing your browser to the switch IP address (or DNS alias). This utility will display information about all switches in the fabric including the OS version running on each.
   - Use "telnet" to connect to the switch and login. Run the command "version". The second line of output which reads: "Fabric OS: ..." contains the OS version information (for example, Fabric OS v4.1).

   For SilkWorm 2000 series switches, only Fabric OS versions at or above v2.6.1 support Fabric Security. For SilkWorm 3200 and 3800 switches, the Fabric OS version must be v3.1 or above. For SilkWorm 3900 and 12000 switches, the Fabric OS version must be v4.1 or above.

   Note: Fabric OS versions prior to v2.6.1, v3.1, and v4.1 do not support Secure Fabric OS.

2. Upgrade Fabric OS version (if necessary).

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

   Note: After downloading the firmware to the switch, a reboot or fastboot is required to activate the new firmware.

   Note: If your SAN is already in Secure Mode, you do not need to disable Secure Mode to upgrade the Fabric OS.

   Note: If the switch being upgraded is the Primary Fabric Configuration Server (FCS), it temporarily becomes the Backup FCS switch during the firmware reboot procedure. However, it does revert to being the Primary FCS switch at the conclusion of the reboot.

   Note: Rebooting a switch to activate new firmware will cause I/O to be disrupted unless the switch is a Silkworm 3900 or 12000.

3. Obtain Software License Key(s) for Secure Fabric OS and Zoning.

   If you do not have a Secure Fabric OS license and a Zoning license for each switch you want in your secure fabric, provide your switch supplier with the WWN of the switch(es) that need licenses. The switch supplier will then provide you with a “Paper Pak” for the Secure Fabric OS and Zoning license(s). Follow the instructions in the “Paper Pak” and use the Brocade Partner site to submit your transaction keys to receive your unique switch license key(s).

4. Add the Software License Key(s) provided for Secure Fabric OS and Zoning to each switch.

   Use the LicenseAdd command (or the “WebTools” interface) to add the Software License key(s) for Secure Fabric OS and Zoning to each switch.

5. Download and run the PKICert utility, and generate a Certificate Signing Request (CSR).

   a. From the Brocade Partner site, select: *For Technical Professionals\Tools\Secure Fabric OS Upgrade* to access the *Secure Fabric OS - Field Upgrade Process* web page.

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

   c. Extract and run the PKICert utility.

   d. Select Option 1 (see below) and follow the directions to generate a CSR file for each switch or fabric:

      ```
      1)Retrieve CSRs from switches & write a CSR file
      ```

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

6. Obtain digital certificates.

   a. From the Brocade Partner site, select: *For Technical Professionals\Tools\Secure Fabric OS Upgrade* to access the *Secure Fabric OS - Field Upgrade Process* web page.

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

   c. Request valid certificate(s) for your switch(es) by submitting the corresponding CSR(s) that were generated.

      You should receive an E-mail within 30 minutes that contains a file with unique "Digital Certificates" for each switch listed in the CSR file that you submitted.

Note: If you do not receive the certificate(s), contact your switch supplier.

---

7. Distribute certificates to the fabric.

   Select option 2 (see below) in the PKICert Utility to distribute the certificates:

   ```
   2)Install Certificates contained in a Certificate file.
   ```

8. Obtain the sectelnet utility.

   a. From the Brocade Partner site, select: *For Technical Professionals\Tools\Secure Fabric OS Upgrade* to access the *Secure Fabric OS - Field Upgrade Process* web page.

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

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

Note: If any switch(es) in the Secure Fabric OS fabric are running Fabric OS v4.1 or later, you have the option of using an SSH client that supports v2 of the protocol.

---

9. Enable Security on your fabric (refer to the *Enabling Secure Mode in the Fabric* section for additional information):

   Secure mode is enabled on a fabric-wide basis. When secure mode is enabled, a list of one or more switches (that will become FCS switches) is specified. The primary FCS switch is the first one on the list that is part of the fabric.

Note: All I/O should be stopped before you enable Secure Mode. Each switch in the fabric is automatically rebooted during the enable process.

Enabling Secure Mode in the Fabric

Secure mode is enabled on a fabric-wide basis. When secure mode is enabled, a list of one or more switches (that will become FCS switches) is specified. The primary FCS switch is the first one on the list that is part of the fabric.

Enabling secure mode:

- Creates a default Fabric Management Policy Set (FMPS) using the FCS policy containing the WWNs that are specified in the list.
- Distributes the FMPS to all switches in the fabric
- Activates the FMPS
- Reboots all switches

The Primary FCS switch:

- Distributes the default policy sets to all switches in the fabric
- Activates the zoning configurations and any future zone management
- Applies the FMPS policy set

Note: Refer to the Brocade Secure Fabric OS User's Guide for additional information about enabling Secure Mode and setting Policies.

Note: Before you enable Secure Mode in the fabric, you must determine which switches are going to be FCS switches, and which one will be the Primary FCS switch.

The first switch entered when enabling security becomes the Primary FCS switch. The basic process to enable security is to perform the following:

1. Build the fabric.

   The administrator builds the fabric with switches that are identified to be in the secure fabric. This includes setting the Recovery and Boot PROM passwords. You should record all your passwords and store then in a safe place prior to enabling security. For detailed information about this procedure, refer to the *Brocade Secure Fabric OS User's Guide* that corresponds to the version of the Fabric OS on your switch.

2. Determine the Primary FCS switch, the Backup FCS switch, and any Non-FCS switch(es). Any Non-FCS switch(es) cannot manage the secure fabric.

3. Connect to the switch that will become the Primary FCS switch using sectelnet or serial port.

   Note: If the Primary FCS switch is running Fabric OS v4.1 or later, you can use an SSH client that supports v2 of the protocol.

4. Run the *secModeEnable* command to enable security on the fabric. This is where you specify the FCS switches by WWN or Domain ID.

   The secModeEnable command:

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

   Note: To activate security, all switches in the fabric are automatically rebooted. All I/O should be stopped prior to running the *secModeEnable* command.

Where to Go From Here

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

Frequently Asked Questions

1. What is the PKI Digital Certificate Web Service?

   Secure Fabric OS uses Public Key Infrastructure (PKI) technology that requires digital certificates installed on switches to uniquely identify their credentials. Brocade hosts PKI Certificate Authority and provides a web-based field upgrade process to receive Certificate Signing Requests (CSRs) and deliver digital certificates to OEMs.

   An enhancement to the field upgrade process that addresses OEM requirements is implemented allowing the request for digital certificates from their end customer(s) to be routed through them. Our current field upgrade process can only accept requests from the Brocade Partner site. Refer to the *Client Programmers Guide for PKI Digital Certificate Web Services* for additional information.

2. How can I tell what PKI objects I have on my switch?

   If your switch is running Fabric OS v4.1 or later, you can type *pkishow* from the command line to see all the PKI objects. For all other versions of the Fabric OS, type *configshow "pki"*. Below are two examples:

   From a Silkworm 12000 running Secure Fabric OS v4.1:

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

   From a Silkworm 2250 running Secure Fabric OS v2.6.1:

   ```
   poc200:root> configshow "pki"
   pki.CSR:                Exist
   pki.Certificate:        Exist
   pki.Private_Key:        Exist
   pki.Root_CA_Cert:       Exist
   value = 2031619 = 0x1f0003
   ```

3. What if I remove my PKI objects?

   If you are in Secure Mode, you will not be able to do this. When doing this in non-Secure Mode, you will need to reboot your switch in order to generate the PKI objects.

4. What if one of my PKI objects is missing?

   Before enabling Secure Mode, you should verify that your PKI objects are in place. If you are missing one of your PKI objects, you can use the *pkicreate* command in Fabric OS v4.1 or later. In v3.1 or v2.6.1, you need to fastboot the switch to generate the PKI objects.

5. If I'm merging two secure fabrics and they each have zoning information I want to keep, will anything happen after I merge the two secure fabrics?

   Yes, and this is important. The switch that will be the Primary FCS after the two fabrics merge WILL distribute the zoning information that it has to ALL switches in the newly merged fabric. If you need to keep the zoning information active from the other fabric that is being merged, you need to integrate it into the other secured fabric zone configuration so when the two fabrics merge, you will have your zone configuration prior to merging fabrics. Refer to the *Brocade Secure Fabric OS User's Guide* for additional information about merging fabrics.

6. Are there any guidelines as it relates to policies and merging secure fabrics?

   Yes. You will need to reset the version stamp on the secure mode fabric that is merging with the other Secure Fabric OS fabric. Refer to the *Brocade Secure Fabric OS User's Guide* for additional information.

7. What happens if I created a policy with no members in it and made it an active policy?

   You cannot do this with an FCS Policy, but for another policy (for example, Telnet_Policy) what you have just done is locked yourself out of your secure fabric via telnet. You can certainly do this, but you need to leave a way into your fabric (for example, via HTTP) to manage your Secure Fabric OS fabric.

8. What if I forgot my secure fabric root password?

   Refer to the *Secure Fabric OS User's Guide*, specifically the section on password recovery.

9. I just built my Secure Fabric OS SAN, is there a way to prevent someone from plugging in a host and mounting a LUN from my secure fabric?

   Besides Hardware Enforced zoning, you need to create a DCC policy on each switch in the secure fabric after configuring it in all your hosts and storage. This will lock down anything that is connected to the secure fabric. So if someone then plugged in a "rogue" host, that port will become disabled.

10. What version of SSH does Fabric OS v4.1 support?

    Currently, version 2 of the SSH protocol and two popular SSHv2 clients that were tested (PuTTy and F-Secure) are supported.

11. Can I use standard telnet with my secure fabric?

    Sectelnet, serial port, or SSH.

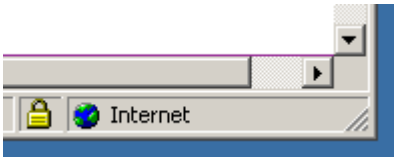
12. Does SSH come with Secure Fabric OS?

    No, SSH is part of the base Fabric OS in v4.1 or later.

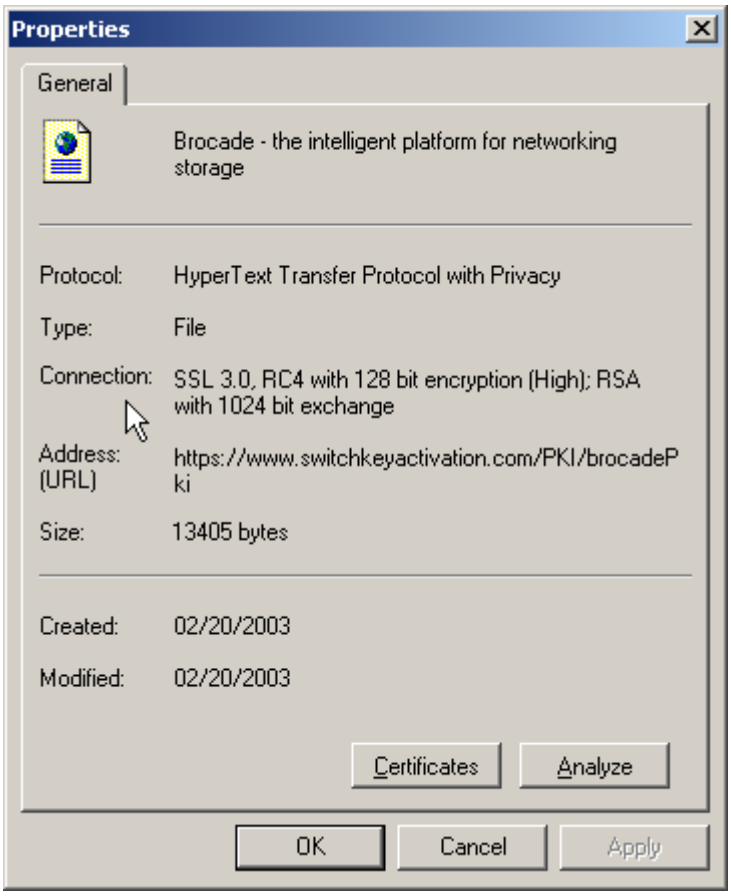
13. What is SLAP?

    SLAP stands for Switch Link Authentication Protocol. Brocade switches in secure mode use the SLAP protocol to authenticate all pending ISL (E_Port) links before making them active.

14. When I click on the "*Secure Fabric OS Upgrade*" link from the Partner web site, I see a little gold lock in the bottom right hand corner of my web browser (see below). What is that lock for?



In the URL of your browser, you will see you are at the *switchkeyactivation.com* web site. If you are using Internet Explorer, you can go under the File menu and select Properties. A window appears with information about the connection type, which in this example is SSL v3 with 128b-bit encryption (see below). You can also click the "Certificate" button and look at information related to the certificate you are using for the connection session (see next page).




Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended to:
•Ensures the identity of a remote computer
* Refer to the certification authority's statement for details.
Issued to: www.switchkeyactivation.com
Issued by: www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign
Valid from 7/16/2002 to 8/2/2004
Install Certificate...
Issuer Statement
OK