Brocade® Fabric OS® Common Criteria User Guide, 9.1.x

User Guide
January 19, 2023

Table of Contents

Introduction

Brocade Fabric OS® firmware uses the Brocade Fabric OS Common Criteria (CC) standards with Fabric OS 9.1.1 Network Device Colloborative Protection Profile (NDcPP) to perform cryptographic functions.

Supported Hardware and Software

The following table lists the CC-compliant operational environments for Brocade Fabric OS software and hardware platforms.

Table 1: Supported Hardware and Software

Hardware Platform	Operating System
Brocade G730 Switch	Fabric OS v9.1.1
Brocade G720 Switch	Fabric OS v9.1.1
Brocade X7-8 Director	Fabric OS v9.1.1
Brocade X7-4 Director	Fabric OS v9.1.1
Brocade G630 Switch	Fabric OS v9.1.1
Brocade G620 Switch	Fabric OS v9.1.1
Brocade G610 Switch	Fabric OS v9.1.1
Brocade X6-8 Director	Fabric OS v9.1.1
Brocade X6-4 Director	Fabric OS v9.1.1
Brocade 7810 Extension Switch	Fabric OS v9.1.1

Contacting Technical Support for Your Brocade® Product

If you purchased Brocade® product support from a Broadcom® OEM or solution provider, contact your OEM or solution provider for all your product support needs.

- OEM and solution providers are trained and certified by Broadcom to support Brocade products.
- Broadcom provides backline support for issues that cannot be resolved by the OEM or solution provider.
- Brocade Supplemental Support augments your existing OEM support contract, providing direct access to Brocade expertise. For more information on this option, contact Broadcom or your OEM.
- For questions regarding service levels and response times, contact your OEM or solution provider.

If you purchased Brocade product support directly from Broadcom, use one of the following methods to contact the Technical Assistance Center 24x7. For product support information and the latest information on contacting the Technical Assistance Center, go to www.broadcom.com/support/fibre-channel-networking/contact-brocade-support.

Online	Telephone
For nonurgent issues, the preferred method is to log on to the Support portal at support.broadcom.com. (You must initially register to gain access to the Support portal.) Once registered, log on and then select **Brocade Products**. You can now navigate to the following sites: • **Case Management** • **Software Downloads** • **Licensing** • **SAN Reports** • **Brocade Support Link** • **Training & Education**	For Severity 1 (critical) issues, call Brocade Fibre Channel Networking Global Support at one of the phone numbers listed at www.broadcom.com/support/fibre-channel-networking/contact-brocade-support.

Document Feedback

Quality is our first concern. We have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission or if you think that a topic needs further development, we want to hear from you. Send your feedback to documentation.pdl@broadcom.com. Provide the publication title; topic heading; publication number and page number (for PDF documents); URL (for HTML documents); and as much detail as possible.

Common Criteria Certification

This section explains steps for configuring the Brocade Fabric OS switch for Common Criteria (CC) standards with Fabric OS 9.1.1 Network Device Collaborative Protection Profile (NDcPP v2.2e). Common Criteria certification for a device enforces a set of security standards and feature limitations to be compliant with the Common Criteria standards.

Brocade Fabric OS switches provide switching functionality that is used in the Fibre Channel domain. The Fabric OS device management functions are isolated through authentication. Once administrators log in with specific credentials, their access is limited to commands for which they have privileges and role-based permissions. Also, network management communication paths are protected against modification and disclosure using SSHv2.

Brocade switches that are running Fabric OS 9.1.1 are designed to support FIPS-compliance mode. All cryptographic algorithms that are required and used in CC are certified by FIPS.

Network Interface

The Target of Evaluation (TOE) is managed through a CLI for administration, which can be accessed through the local console or through SSH where the following processes respond to process the network packets. All these processes run under the admin privilege.

- TCP/IP stack: The Fabric OS IP stack from the kernel that accepts all packets from the network interface.
- Syslog: The process that supports logging of audit messages through a TLS tunnel to a remote server.
- SSH: The process available on port 22 that provides a terminal session after authentication using the SSHv2 protocol. SSH session rekey occurs after every 1 GB of data (incoming + outgoing) of the SSH session or after a configured time interval has elapsed. When both the data limit and the time interval are configured, rekey occurs when either condition is met. On rekey, both the timer and the byte count are reset.
- LDAPS: Lightweight Directory Access Protocol (LDAP) with Transport Layer Security (TLS) uses a certificate authority (CA). By importing signed certificates, you can make LDAP traffic confidential and secure by using Secure Sockets Layer (SSL)/TLS technology with LDAP.

The product operating environment should include the ability for DNS resolution, an NTP server, and a protected management network for admin connections. By default, no services are offered on the TOE management network before user authentication.

Firmware Update

Firmware upgrades are available for partners and for customers with support service contracts at https://www.broadcom.com/mybroadcom.

Firmware packages are signed using the platform-specific 4096-bit RSA key with SHA-256 during the firmware build, and they are verified during the firmware installation as specified in the following steps.

1. RPM packages are signed with the platform-specific 4096-bit RSA key to create an SHA-256 digest when the firmware package is generated.
2. A public key is packaged in an RPM package as part of the firmware.
3. As part of the firmware download, each package is validated by verifying the signature.
4. Installation begins after the packages are validated.
5. The switch restarts after successful installation.

NOTE
If the installation fails, an error with details is displayed and the download procedure is terminated.

NOTE
Once the firmware download is completed, the system reboots and the newly installed firmware runs immediately.

Evaluated firmware is verified during the update using the 4096-bit RSA key on the individual RPMs.

NOTE
To enable a legacy firmware download and skip the incremental upgrade, enter the `firmwaredownload -L` command.

Finding the Firmware Switch Version

This section describes the steps to identify the firmware switch version.

1. Connect to the switch and log in using an account with admin permissions.
2. Enter `version` .

   The following information is displayed:

   - **Kernel** – Displays the version of the switch kernel operating system.
   - **Fabric OS** – Displays the Fabric OS firmware version of the switch.
   - **Made on** – Displays the build date of the firmware that is running on the switch.
   - **Flash** – Displays the installation date of firmware that is stored in non-volatile memory.
   - **BootProm** – Displays the version of the firmware that is stored in the boot PROM.

   The following example shows the output of the `version` command.

```
switch:admin> version
Kernel:     4.1.35rt41
Fabric OS:  v9.1.1
Made on:    Thu Jan 16 19:48:47 2022
Flash:      Mon Jan 20 05:06:28 2022
BootProm:   sb-4.0.10
```

Configuring the Fabric OS Switch for Common Criteria

Fabric OS provides three default user accounts such as `admin` , `user` , and `maintenance` . The `admin` and `user` accounts are enabled by default. The maintenance account is disabled by default, and it is enabled for only maintenance or switch service. You must not use the maintenance account for any administrative actions. The TOE has default roles, such as admin, zoneadmin, basicswitchadmin, switchadmin, securityadmin, fabricadmin, operator, maintenance, and user with varying privileges. All users with the above roles should have their own user account, and their password should be protected.

The switch automatically prompts you to change the default account password after logging in for the first time. When you initially log in as admin, or user, you must immediately change the password for the default accounts. For a maintenance user, you must enable the user first and log in as maintenance to change the password. If you cancel the password change using `Ctrl+C`, the system logs out, and once you log in, you are again prompted to change the password. For more information on changing the default password, see Default Account Password.

New user-defined roles with administrative privileges can also be created on the TOE using the `roleconfig` command. All such users are considered switch administrators. Users can be associated with the default roles using the `userconfig` command. The users with administrative privileges can manage the TOE both locally and remotely by logging the TOE through the local console or SSHv2. The user login passwords that are entered during the login are protected by default.

To configure the Brocade Fabric OS switch to operate in Common Criteria mode, perform the following tasks:

1. Log in to the switch as the default admin user through SSH or the local console. You must provide the required user credentials.
2. Enter the `firmwarecheck --enable -boot` command to enable the check of firmware at boot.
3. Enter the `seccryptocfg --apply -group Compliance -attr Zeroize -val yes` command to zeroize the critical security parameters (CSPs).
4. Configure the system for crypto compliance to limit the cryptographic algorithms. The algorithms are used by the TOE for TLS and SSH sessions, which are allowed in adherence with common criteria evaluation using the `seccryptocfg --apply default_cc` command.
5. Enable the switch in FIPS mode using the `seccryptocfg` command.

```
switch:admin> seccryptocfg --apply -group Compliance -attr FIPSInside -value yes
You are enabling fipsinside.This will be effective on each cp after reboot of respective cp.
Please confirm and provide the preferred option
Press Yes(Y,y), No(N,n) [N]:yes
FIPS inside mode has been set to : Enabled
```

6. To be compliant with CC mode, you must set the validation mode value to `strict` using the `seccryptocfg` command.

```
switch:admin> seccryptocfg --apply -group X509v3 -attr Validation -value Strict
This operation will terminate existing SSH sessions.
Please confirm and provide the preferred option
Press Yes(Y,y), No(N,n) [N]:Y
Config change is Successful
Terminating all SSH/SCP sessions running
Broadcast message from root@admin123 (pts/0) (Tue Jan  3 06:02:58 2023):

All SSH accounts will be logged out
```

7. Power-cycle the module.
8. Use the `ipfilter` commands to block Telnet, HTTP, and SNMP ports, and allow only SSH, HTTPS, and NTP ports.
   a. `ipfilter --clone IP_v4 -from default_ipv4`
   b. `ipfilter --delrule IP_v4 -rule 2`
   c. `ipfilter --delrule IP_v4 -rule 2`
   d. `ipfilter --delrule IP_v4 -rule 2`
   e. `ipfilter --delrule IP_v4 -rule 2`
   f. `ipfilter --activate IP_v4`
   g. Repeat steps a through f for default IPv6 address as well.
9. To generate an ECDSA P521 host key, enter the `sshutil genhostkey` command.

```
switch:admin> sshutil genhostkey -ecdsa
ecdsa host key already exists.
Do you want to proceed(yes, y, no, n)[no]?y
switch:admin>
```

10. To ensure that SSH sessions are rekeyed to an interval less than or equal to one hour, configure time-based SSH rekeying with the `sshutil rekeyinterval` command.

```
switch:admin> sshutil rekeyinterval 3000
SSH daemon will be restarted and all SSH session will be terminated
Do you want to proceed(yes, y, no, n)[no]?y
Rekey Time Interval Configured to 3000 seconds.
```

NOTE
You do not have to configure SSH rekeying based on traffic. The system default is configured to 1 GB of transmitted traffic.

11. Perform the following steps to configure the switch for the secure communication.
    a. Enable secure mode for the secure upload and signature verification check using the `configurechassis` command to ensure secure communication. Ensure that the FTP mode of transfer is not selected for the following operations.
        a. Upload the system configuration.
        b. Download the system configuration.
        c. Save the RASLog, TRACE, supportshow, core file, FFDC data, and other support information.
        d. Download the firmware.

```
switch:admin> configurechassis

Configure...

  cfgload attributes (yes, y, no, n): [no] y

        Enforce secure config Upload/Download (yes, y, no, n): [yes] y
        Add Suffix to the uploaded file name (yes, y, no, n): [no]
        Do you want to enable auto firmwaresync (yes, y, no, n): [yes]

 ssl attributes (yes, y, no, n): [no]
 webtool attributes (yes, y, no, n): [no]
 Custom attributes (yes, y, no, n): [no]
 system attributes (yes, y, no, n): [no]
 fos attributes (yes, y, no, n): [no]
```

12. Run the `portenccompshow` command to check if any ports are enabled for compression or encryption, then disable in-flight encryption using the `portcfgencrypt --disable portnumber` command.
13. Configure the SNMP access list for no access using the `snmpconfig --set seclevel` command.

```
switch:admin> snmpconfig --set seclevel
Select SNMP GET Security Level(0 = No security, 1 = Authentication only, 2 = Authentication and Privacy, 3
 = No Access): (0..3) [0] 3
Warning: Modifying the security access level to No Access for GET operation might impact the SNMP GET /
 SNMP Walk query triggered by the applications monitoring the system.Select SNMP SET Security Level(0 = No
 security, 1 = Authentication only, 2 = Authentication and Privacy, 3 = No Access): (3..3) [3] 3
2022/07/14-14:17:05 (GMT), [SNMP-1005], 347, FID 3, INFO, G620_1, SNMP configuration attribute, SNMP GET
 Security Level, has changed from 0 to 3.
```

14. Set up the certificates to identify the client for secure communications. The SAN switch generates a certificate signing request (CSR). This CSR must be exported from the switch to a certificate authority (CA). The CA must use the CSR to create a certificate (which the CA signs). The signed certificate is used by the switch and must be loaded into the switch along with its root CA certificate. A root CA certificate is always self-signed. The SAN switch needs a signed certificate to authenticate itself to the LDAP server and another signed certificate to authenticate itself to the syslog server. The CA can issue multiple signed certificates or can let intermediate CAs issue certificates. The certificates have a hierarchical structure of relationship. The root certificate is the top-most in the hierarchy tree and its private key is used to sign other certificates. Intermediate certificates are signed by the root certificate with the CA field set to true. The intermediate certificates, in turn, are used to authenticate certificates further down the tree. Server and client identity certificates are signed by the root CA or intermediary CAs. The server/client CA is the chain of certificates from the trusted root, including all intermediaries, which sign the server/client identity certificate.
    When creating a certificate chain, all certificates starting from the leaf, until the root is included into one file. The entire certificate chain that signed the CSR is imported, before importing the identity certificates. To validate peer certificate during the session establishment, the trusted root CA certificate is imported.
15. Import and authenticate the public key using the `sshutil importpubkey` command.

```
switch:admin> sshutil importpubkey
Enter user name for whom key is imported:admin
```

```
Enter IP address:172.16.5.8
Enter remote directory:/root/.ssh
Enter public key name(must have .pub suffix):id_ecdsa.pub
Enter login name:root
root@172.16.5.8's password:
2014/03/27-11:43:43, [SEC-3050], 908, FID 128, INFO, G720, Event: sshutil, Status: success, Info: Imported
 public key from host 172.16.5.8
public key is imported successfully.
```

16. Install the certificates to authenticate the SAN switch to the LDAP server.
    a. Generate and export the CSR.

```
switch:admin> seccertmgmt generate -csr ldap
Generating a CSR will automatically do the following:
Delete all existing CSRs.

Warning:
        Key-pair generation is CPU intensive and can cause high CPU usage
        Private IPs and hostnames should not be part of SCN and/or SAN per CA/Browser forum.

Continue (yes, y, no, n): [no] y
Country Name (2 letter code, eg, US):US
State or Province Name (full name, eg, California):California
Locality Name (eg, city name):San Jose
Organization Name (eg, company name):*******
Organizational Unit Name (eg, department name):***
Common Name (Fully qualified Domain Name, or IP address):**.**.**.**
Email Address:abc@xyz.com
Subject Alternative Name, DNS (Fully Qualified Domain Name, or IP address):*******.com
Subject Alternative Name, DNS (Fully Qualified Domain Name, or IP address):<enter>
Subject Alternative Name, IPAddress (IP v4 or v6 address): 10.1.1.5
Subject Alternative Name, IPAddress (IP v4 or v6 address): <enter>

Generating CSR, file name is: 10.1.1.5.csr
switch:admin> seccertmgmt export -csr ldap -protocol scp -ipaddr 10.1.1.5 -remotedir /certs/keys -login
 user2
```

NOTE
The email address and the SAN fields are optional.

    b. Import the root CA in the chain that signed the client certificate.

```
switch:admin> seccertmgmt import -ca -client ldap -protocol scp -ipaddr  10.1.1.5 -remotedir /etc/
ldap1g/key.d/OCSP/quaternary/certs -login user2 -certname ca-chain5.pem
```

    c. Import the signed certificate.

```
switch:admin> seccertmgmt import -cert ldap -protocol scp -ipaddr  10.1.1.5 -remotedir /certs/keys -
login user2 -certname ldap.pem
```

17. Install the certificates to authenticate the SAN switch to the syslog server.
    a. Generate and export the CSR.

```
switch:admin> seccertmgmt generate -csr syslog
Generating a CSR will automatically do the following:
Delete all existing CSRs.

Warning:
        Key-pair generation is CPU intensive and can cause high CPU usage
        Private IPs and hostnames should not be part of SCN and/or SAN per CA/Browser forum.
```

```
Continue (yes, y, no, n): [no] y
Country Name (2 letter code, eg, US):US
State or Province Name (full name, eg, California):California
Locality Name (eg, city name):San Jose
Organization Name (eg, company name):*******
Organizational Unit Name (eg, department name):***
Common Name (Fully qualified Domain Name, or IP address):**.**.**.**
Email Address:abc@xyz.com
Subject Alternative Name, DNS (Fully Qualified Domain Name, or IP address):*******.com
Subject Alternative Name, DNS (Fully Qualified Domain Name, or IP address):<enter>
Subject Alternative Name, IPAddress (IP v4 or v6 address): 10.1.1.4
Subject Alternative Name, IPAddress (IP v4 or v6 address): <enter>

Generating CSR, file name is: 10.1.1.4.csr
switch:admin> seccertmgmt export -csr syslog -protocol scp -ipaddr 10.1.1.4 -remotedir /certs/keys -
login user1
```

b. Import the root CA in the chain that signed the client certificate.

```
switch:admin> seccertmgmt import -ca -client syslog -protocol scp -ipaddr  10.1.1.4 -remotedir /etc/
syslog-ng/key.d/OCSP/quaternary/certs -login user1 -certname ca-chain.pem
```

c. Import the signed certificate.

```
switch:admin> seccertmgmt import -cert syslog -protocol scp -ipaddr  10.1.1.4 -remotedir /certs/keys -
login user1 -certname syslog.pem
```

18. Configure and install the certificates in the TOE to allow authentication for the LDAP and syslog servers. The authentication occurs when the SAN switch connects to the LDAP and syslog servers.
    a. Import the root certificate and CA certificate chain that is signed on the LDAP and syslog server certificate.

```
switch:admin> seccertmgmt import -ca -server ldap -protocol scp -ipaddr  172.20.1.4 -remotedir /etc/
ldap1g/key.d/OCSP/certs -login user5 -certname ca.cert.pem
switch:admin> seccertmgmt import -ca -server syslog -protocol scp -ipaddr  172.20.1.4 -remotedir /etc/
syslog-ng/key.d/OCSP/certs -login user1 -certname ca.cert.pem
```

    b. Perform the following steps to configure an LDAP server.
        a. Add an LDAP server using the `aaaconfig --add <ldap_server_ip> -conf ldap -d<domain> -tls_mode ldaps` command.
        b. Set the switch authentication mode using the `aaaconfig --authspec` command.
    c. Configure a syslog server using the `syslogadmin` command.

```
switch:admin> syslogadmin --set -ip server.domain -secure -port 6514
```

> **NOTE**
> The Fabric OS switch automatically reconnects TLS communication pathways when a connection is unintentionally broken.

19. Enable auditing of security events using the `auditcfg --class 1,2,3,4,5,7,8,9;auditcfg --enable -all` command.
20. Perform the following steps to configure the NTP server from where the TOE receives time updates.
    a. Add the symmetric authentication key to identify the secure NTP server.

```
switch:admin> tsclockserver --addkey -index 16 -type HMAC-SHA256 -key
 b0630baf4ba7d3997382298e0d81729e734a150ab0630baf4ba7d3934a1501de

Adding authentication key ...
```

    b. Map the clock server with a symmetric authentication key index.

```
switch:admin> tsclockserver --set "172.16.1.2" -index 16
Updating Clock Server configuration...
```

```
switch:admin> tsclockserver
Active NTP Server               172.16.1.2
Configured NTP Server List      172.16.1.2
Configured NTP Key Index List   16
Configured NTP Authspec Mode    NTP AUTHENTICATION DISABLED
Configured NTP Legacy Mode      LEGACY MODE ENABLED
```

c. Enable symmetric key authentication for the clock server.

```
switch:admin> tsclockserver --authspec symmetric
Updating Clock Server authspec...

switch:admin> tsclockserver
Active NTP Server               172.16.1.2
Configured NTP Server List      172.16.1.2
Configured NTP Key Index List   16
Configured NTP Authspec Mode    SYMMETRIC AUTHENTICATION ENABLED
Configured NTP Legacy Mode      LEGACY MODE ENABLED
```

NOTE

The system time on the switch can be modified manually using `date` command provided that the switch is not configured to synchronize with the external NTP server. You cannot change the date within 64 seconds of a previous change. Fabric OS supports the system to be monitored and protected from disproportionate time change; therefore the date cannot be changed beyond plus or minus seven days.

```
date MMDDhhmm[YY]
date [-u|--utc|--universal] MMDDhhmm[YY]
For example:
date -u 01040900
```

NOTE

Fabric OS supports NTP (NTPv4) synchronizing its system clock with external NTP servers. The switch can have a maximum of eight NTP servers that are configured at any point using the `tsclockserver` command. By default, the switch runs the `ntp` service in client mode accepting time sync only from the configured NTP servers and not accepting the broadcast and multicast NTP packets. The switch is used to configure the NTP servers for symmetric authentication using HMAC-SHA1 and HMAC-SHA256 keys. The minimum and maximum key length for HMAC-SHA1 is 40 and 255. The minimum and maximum key length for HMAC-SHA256 is 64 and 255. The keys must use only hexadecimal characters (0 1 2 3 4 5 6 7 8 9 A B C D E F a b c d e f).

Default Account Password

The prompt to change the default account password is a string that begins with the message `Please change passwords for switch default accounts now`. User-defined passwords are 8 through 40 characters. They are case-sensitive and are not displayed when entered on the command line.

NOTE

If you are changing the password string for the admin, user, and maintenance account to `password` , the system sends the warning message `You have chosen the default password and it must be changed at the next switch login. Please acknowledge the temporary use of the password or use Control+C to exit` . The system detects that the password is set to the manufacturer's default password. Even though you are allowed to set the default password at the next login, it prompts you to change the password immediately.

Changing the Default Account Password of the Switch

Use the following procedure to change the default account password of the switch:

1. Connect to the switch and log in using the default administrative account.
2. At `Enter new password` and `Re-type new password` prompts, enter the new password.

   The following example shows the output for changing the default password.

```
Fabric OS (sw0)
sw0 login: admin
Password:
Please change passwords for switch default accounts now.
for user - admin
Changing password for admin
Enter old password:
Enter new password:
Re-type new password:
passwd: all authentication tokens updated successfully
Please change passwords for switch default accounts now.
for user - user
Changing password for user
Enter new password:
Re-type new password:
passwd: all authentication tokens updated successfully
Saving passwords to stable storage.
Passwords saved to stable storage successfully
```

Changing the Password for the Current Login Account

To change the password for the current login account, perform the following steps:

1. Connect to the switch and log in using an account with admin permissions.
2. Enter the `passwd` command.
3. Enter the requested information at the prompts.

   The following example shows the output for changing password using the `passwd` command.

```
sw0 login: admin
Password:####
sw0:FID128:admin> passwd
Changing password for admin
Enter old password: ####
Enter new password: ####
Re-type new password: ####
passwd: all authentication tokens updated successfully
Saving password to stable storage.
Password saved to stable storage successfully.
```

Password Policy

Users in the admin role can configure password policies. The length of the password must be from 8 through 40 characters. By default the minimum length of the password is 8 characters. The passwords can contain any combination of upper and lower case letters, numbers, and the following special characters: ['!', '@', '#', '$', '%', '^', '&', '*','(', ')'];. You must create a stronger password with a longer length and multiple characters.

The `passwdcfg` command is used to configure strong password policies.

```
passwdcfg --set  {[-lowercase <value>] [-uppercase <value>] [-charset <value>]
        [-allowuser {Yes | No}] [-digits <value>] [-punctuation <value>]
        [-minlength <value>] [-history <value>] [-minpasswordage <value>]
        [-maxpasswordage <value>] [-warning <value>] [-lockoutthreshold <value>]
        [-lockoutduration <value>] [-repeat <value>] [-sequence <value>]
        [-reverse <value>] [-expire] [-minDiff <value>]}
```

The password length can be set with the `passwdcfg --set -minlength` command. For example, the following command sets the minimum length of a password to 15 characters and generates a log.

```
passwdcfg --set -minlength 15
2022/04/20-17:27:53, [SEC-1312], 155, FID 3, INFO, G720, passwdcfg params changed as (minlength:8->15)
 (status:0->1).
```

User passwords are protected by storing a hashed password. sha512 is the default hashing algorithm. The current configured hashing algorithm can be verified with the `passwdcfg --showhash` command. You can configure the password hashing algorithm using the `passwdcfg --hash` command.

```
passwdcfg --hash sha512
```

NOTE
If the hashing algorithm is changed, the password must be reset.

Deleting Cryptographic Parameters

This section describes configuration steps to delete cryptographic parameters such as SSH hostkeys, user authentication public and private keys, TLS certificates, and the CSR used for syslog and LDAP.

Deleting the SSH Hostkeys

To delete the SSH hostkeys, perform the following steps:

1. Connect to the switch and log in using an account with admin permissions.
2. Use the `sshutil delhostkey [-rsa | -dsa | -ecdsa]` command to delete the SSH hostkeys on the switch.

Deleting the Public Keys from the Switch

To delete the public keys from the switch, perform the following steps:

1. Connect to the switch and log in using an account with admin permissions.
2. Use the `sshutil delpubkeys -all` command to delete the public keys.

The following example shows deleting the public keys on the switch:

```
switch:admin> sshutil delpubkeys -all
WARNING: It deletes all the ssh public keys for all users. Do you want to proceed(yes, y, no, n)[no]?yes
ssh public keys associated to all users are deleted.
```

Deleting the Private Keys from the Switch

To delete the private keys from the switch, perform the following steps:

1. Log in to the switch as the allowed user.
2. Use the `sshutil delprivkey [-rsa|-dsa|-ecdsa]` command to delete the private key.

The following example shows deleting the private keys on the switch:

```
switch:alloweduser> sshutil delprivkey -rsa
private key is deleted successfully.
```

Deleting the CSR Keys from the Switch

To delete the CSR keys from the switch, perform the following steps:

1. Connect to the switch and log in using an account with admin permissions.
2. Use the `seccertmgmt delete -csr ldap` command to delete the CSR LDAP keys.

Deleting the TLS Certificates

To delete the TLS certificates from the switch, perform the following steps:

1. Connect to the switch and log in using an account with admin permissions.
2. Use the `seccertmgmt delete -cert ldap` command to delete the LDAP client certificate.

Zeroizing All Cryptographic Parameters

To zeroize all the cryptographic parameters from the switch, perform the following steps:

1. Connect to the switch and log in using an account with admin permissions.
2. Use the `seccryptocfg --apply -group Compliance -attr Zeroize -value yes` command to zeroize all the cryptographic parameters.

The following example shows zeroizing all the cryptographic parameters such as SSH keys, TLS keys and certificates, and passwords:

```
switch:admin> seccryptocfg --apply -group Compliance -attr Zeroize -value yes

Please confirm and provide the preferred option
Press Yes(Y,y), No(N,n) [N]:
```

Account Lockout Policy

A user in the admin role can set a lockout failure count for remote login attempts. If the count is exceeded, the targeted account is locked.

The TOE supports unlocking an account that is based on either a configured lockout duration or an explicit admin action. Remote login attempts using SSH are blocked entirely for an account when that account is locked. The valid passwords of the user admin always allow a successful login from the local console, even when the local admin account is locked, when the `adminlockout` console access is enabled. This ensures that access to the TOE CLI is available at the local console despite the potential locking of all administrator accounts by a malicious remote attacker.

The account lockout policy disables a user account when the user exceeds a specified number of failed login attempts, and it is enforced across all user accounts. You can configure this policy to keep the account locked until explicit administrative action is taken to unlock it, or the locked account can be automatically unlocked after a specified period. Administrators can unlock a locked account at any time.

A failed login attempt counter is maintained for each user on each switch instance. The counters for all user accounts are reset to zero when the account lockout policy is enabled. The counter for an individual account is reset to zero when the account is unlocked after a lockout duration period expires or when the account user logs in successfully.

The admin account can also have the lockout policy enabled on it. The admin account lockout policy is disabled by default and uses the same lockout threshold and duration as the other accounts. The admin account can be automatically unlocked after the lockout duration passes or when it is manually unlocked by a user account that has securityAdmin or other admin permissions.

Use the following attributes to set up the account lockout policy:

- Lockout Threshold

Specifies the number of times that a user can attempt to log in using an incorrect password before the account is locked. The number of failed login attempts is counted from the last successful login. Lockout threshold values range from 0 through 999, and the default value is 0. Setting the value to 0 disables the lockout mechanism. To set the lockout threshold of three minutes, use the following command:

```
switch:admin> passwdcfg --set -lockoutthreshold 3
```

- Lockout Duration
  Specifies the time, in minutes, after which a previously locked account is automatically unlocked. Lockout duration values range from 0 through 99999, and the default value is 30. Setting the value to 0 disables lockout duration and requires a user to seek administrative action to unlock the account. The lockout duration begins with the first login attempt after the lockout threshold has been reached. Subsequent failed login attempts do not extend the lockout period. To set the lockout duration of 15 minutes, use the following command:

```
switch:admin> passwdcfg --set -lockoutduration 15
```

Enabling the Admin Lockout Policy

To enable the admin lockout, perform the following steps:

1. Log in to the switch using an account with admin or securityAdmin permissions.
2. Enter the `passwdcfg --enableadminlockout` command.

Disabling the Admin Lockout Policy

To disable the admin lockout policy, perform the following steps:

1. Log in to the switch using an account with admin or securityAdmin permissions.
2. Enter the `passwdcfg --disableadminlockout` command.

Enabling an Account

To enable an account, perform the following steps:

1. Log in to the switch using an account with admin or securityAdmin permissions.
2. Enter the `userconfig --change <account_name> -e yes` command to enable the account.

Disabling an Account

To disable an account, perform the following steps:

1. Log in to the switch using an account with admin or securityAdmin permissions.
2. Enter the `userconfig --change <account_name> -e no` command to disable the account.

Unlocking an Account

To unlock an account, perform the following steps:

1. Log in to the switch using an account with admin or securityAdmin permissions.
2. Enter the `userconfig --change <account_name> -u` command to unlock the account.

Session Management

This section explains the SSH session timeout and configuration of banner.

The switch can be configured for idle (inactivity) timeout for both console session and SSH session separately. By default, console session timeout is 10 minute, the SSH sessions timeout is not set. On the expiry of idle timeout, user is logged out of the sessions automatically. The console session and SSH session timeout can be disabled by setting the timeout value to 0.

To configure session idle timeout for 10 minutes, perform the following command:

```
timeout 10
```

To configure SSH session idle timeout for 10 minutes, perform the following command:

```
timeout --session 10
```

NOTE
The user can log out of an active session using the `logout` command.

The banner on the switch can be configured using the `bannerset` command, which is displayed before a user logs in to the switch. A maximum of length 1022 characters are supported. The banner is displayed at both the local console and remote SSH logins.

Cryptographic Configurations in Common Criteria

This section lists the TLS cryptographic configuration, SSH cryptographic configuration, and X509v3 certification validation.

TLS Cryptographic Configurations

The devices in Common Criteria mode supports the following cryptographic configurations:

- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246.
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246.
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246.
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246.
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289.
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289.
- TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288.
- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288.
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288.
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288.
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289.
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289.
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289.
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289.
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289.
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289.
- TLSv1.2 is supported for LDAP and syslog communication.
- The AES-128 and AES-256 encryption algorithms (with SHA-1 and SHA-256 as MAC) are supported.
- The TOE can offer only an RSA certificate to its peer during authentication, but it will accept either RSA or ECDSA certificates, which chain to a trusted root.
- DES-based cipher suites are not supported.

SSH Cryptographic Configurations

Any algorithms that are not in the list cannot be considered as the evaluated configuration. The following algorithms are supported:

- Host authentication
  - ssh-rsa
  - rsa-sha2-512
  - rsa-sha2-256
  - ecdsa-sha2-nistp521
- Ciphers
  - aes128-cbc
  - aes256-cbc
  - aes128-ctr
  - aes256-ctr
  - aes128-gcm@openssh.com
  - aes256-gcm@openssh.com
- hash-based message authentication code (HMAC)
  - hmac-sha1
  - hmac-sha2-256
  - hmac-sha2-512
- Key exchange
  - ecdh-sha2-nistp256
  - ecdh-sha2-nistp384
  - ecdh-sha2-nistp521
  - diffie-hellman-group14-sha1
  - diffie-hellman-group14-sha256

X509v3 Certificate Validation

Both CA certificates and identity certificates must be validated for Common Criteria compliance. The following table provides more details.

Table 2: X509v3 Certificate Validation Table

X509 Fields	Valid NDcPP 2.2e Values	Validation Behavior During Certificate Import	Validation Behavior During TLS Session Establishment
Not Before Not After	The certificate that is validated for time and date during import and is accepted only if the time and date are within the allowed range.	The certificates that are expired or invalid are not allowed to be imported. Import fails.	The session establishment fails if the CA certificate or identity certificate that is used has expired or is not yet valid.
CN	Must be an FQDN device name or IP. Wildcards are allowed only for one level of subdomain and are not allowed for the main domain.	Validates identity certificates against the IP or host name of the host during import. If the common name does not match the IP or host name or has a wildcard in any field other than the first level of sub-domain, then import fails. The validation does not apply to commoncert.	Validates identity certificates against the IP or host name of the host. Applies to all identity certificates that are used for session establishment including commoncert. Wild cards are allowed only for the first level of sub-domain.
Public-Key	CC-compliant configuration values are documented. However, no restriction is imposed on using non-compliant values.	No validation is performed or no audit log is generated and the import is successful.	Audit logs are generated for certificates that have a `keysize` less than 2048. The session is established successfully.

X509 Fields	Valid NDcPP 2.2e Values	Validation Behavior During Certificate Import	Validation Behavior During TLS Session Establishment
CA	The field must be TRUE for CA certificates.	Validated for CA certificates at import. Import fails if this is not true.	Validated for all CAs used during session establishment.
Key Usage	Must have `Certificate Sign` if there are CA certificates and `Digital Signature` if there are identity certificates. To support RSA-based ciphers for TLS sessions, Key encipherment must be set.	Validated for CA certificates and identity certificates (for `Certificate Sign` and `Digital Signature`). If validation fails, import fails.	Validated for CA certificates and identity certificates (for `Certificate Sign` and `Digital Signature`. If validation fails, session establishment fails.
X509v3 Extended Key Usage	You must correctly indicate whether it is for use as a `serverAuth` certificate or a `clientAuth` certificate. If it is incorrect, connection is not allowed.	Validated for correct EKU (`serverAuth` for identity certificates of servers and `clientAuth` for identity certificates of clients). If incorrect, import fails.	Validated for correct EKU (`serverAuth` for identity certificates for servers and `clientAuth` for identity certificates of clients). If incorrect, session establishment fails.
Authority Information Access	You must have the valid OCSP server respond affirmatively. If this field is unavailable, an OCSP check is not performed.	Checked during the import of LDAPS and syslog certificates. If present, a revocation check is performed. If the revocation check fails, import fails. If the OCSP URL is not found in the certificate, a check is not performed. If the URL is provided but not reachable, the certificate is rejected and the import fails.	Checked for the OCSP URL in the certificate during session establishment. If present, a revocation check is performed and a connection is established only if the revocation check passes. If no OCSP URL is found in the certificate, then a connection is established successfully. If the URL is provided but not reachable, the certificate is rejected and a session is not established.
Signature Algorithm	CC-compliant configuration values are documented. However no restriction is imposed on using non-compliant values.	No validations are performed at import.	No validations are performed during session establishment.

X509 Fields	Valid NDcPP 2.2e Values	Validation Behavior During Certificate Import	Validation Behavior During TLS Session Establishment
Subject Alternative Name	Not a mandatory attribute. If present, the values that are stored in the SAN take priority over the CN in the Subject attribute.	Validated during import for all certificates. Validates identity certificates against the name of the host during import. If the SAN DNS does not match the host name or has a wildcard in any field other than the first level of subdomain, then the check fails. The validation applies to LDAPS and syslog only.	Validated during sessions for all certificates. Validates identity certificates against the name of the host if the reference ID is the FQDN or against the IP address of the host if the reference ID is the IP address. Applies to all identity certificates that are used for session establishment. Wildcards are allowed only for the first level of sub-domain. When the reference ID is the IP address and the SAN IP address does not match the IP address of the host or when the reference ID is the SAN DNS and the SAN DNS does not match the host name or has a wildcard in any field other than the first level of subdomain, then the check fails. Not applicable to FCAP or commoncert.
Basic Constraints Attribute	The attribute must be present and must have a CA field.	Validated for CA certificates at import. Import fails if the attribute does not exist or the attribute is not set to TRUE.	Validated for all CA certificates that are used during session establishment. Validation fails if the attribute does not exist or the attribute is not set to TRUE.

NOTE

The certification extensions `KeyUsage (KU)` , `ExtendedKeyUsage(EKU)` , and `BasicConstraints` are mandatory only in strict mode. However, if these extensions are present in basic mode, validation is performed during the certificate import operation. If the validation fails, the import fails.

NOTE

The `switchname` of the default FID taken from the `switchshow` CLI, along with the domain set with the `dnsconfig` CLI specifies the TOE's reference identifier.

NOTE

Identity verification using the FQDN offers more flexibility than using IP addresses.

The following steps are applicable for certificates that are generated using the openssl conf file.

- The openssl conf file that is used for generating the server or client identity certificate should have the following mandatory entry (other keyUsages are allowed too, but digitalSignature should be present):
  keyUsage=digitalSignature
- The openssl conf file that is used for generating the server identity certificate should have the following mandatory entry:
  extendedKeyUsage=serverAuth
- The openssl conf file that is used for generating the client identity certificate should have the following mandatory entry:
  extendedKeyUsage=clientAuth
- The openssl conf file for generating CA certificates should have the following mandatory entries:

basicConstraints=CA:TRUE
keyUsage = keyCertSign

Certificate Revocation Check Enforcement

Enforcement of the certificate revocation check is achieved using the Online Certificate Status Protocol (OCSP).

If a certificate contains an OCSP Uniform Resource Identifier (URI), a revocation check is performed during the certificate import and TLS session establishment when validation is set to `strict` .

- All TLS-based applications on the switch that support certificate validation of the peer, verify the peer certificate with the OCSP responder for revocation, if the OCSP URI is already present as part of the peer certificate.
- If the peer certificate does not have an OCSP URI, the certificate is not verified for revocation and the connection status depends on other pre-existing validations of the peer certificate alone.
- The OCSP revocation check is implicit based on the peer certificate having an OCSP URI in it. There are no changes to any user interfaces or CLIs.
- The certificate that signs the OCSP response for a peer is the same as the CA certificate that is imported for that peer. No separate OCSP certificate is on the switch for verifying the OCSP response.
- The switch certificates that are sent by the switch to its peer for validation do not have an OCSP URI and do not support the revocation check by the peer.

The TLS session is established only if the OCSP response is good. The following table describes the responses and the outcome.

OCSP Responder Status	Certificate Import or TLS Session Establishment Status
Reachable; Response = Good	Pass
Reachable; Response = Signature verification fails	Fail
Reachable; Response = Revoked	Fail
Reachable; Response = Unknown	Fail
Reachable; No Response	Fail
Not reachable	Fail

Self-Tests

This section details the information on the tests that are executed during the bootup of the switch to confirm the authenticity of the NIST-approved algorithms.

The following table provides detailed information about the tests that are executed during the bootup of the switch:

NOTE
During a self-test failure, you must restart the system and test again. If the failure persists, proceed with the Return Materials Authorization (RMA) request for the device.

Algorithm	Description
TDES	This module implements a known answer test (KAT) for the encrypt and decrypt operations of Triple DES in the CBC mode of operation. The test passes only if the calculated output equals the known output for both operations. The Triple DES KAT must execute successfully before the Triple DES functionality is used.
AES	This module implements a KAT for the encrypt and decrypt operations of AES-128 in the CBC mode of operation. The test passes only if the calculated result equals the known result for both encryption and decryption. The AES KAT must execute successfully before the AES functionality is accessed.
HMAC-SHA1, HMAC-SHA224, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512	This module implements the short messages test as part of the KAT for SHA1, SHA224, SHA256, SHA384, and SHA512 and later the HMAC validation testing is done. The short messages test tests the ability to correctly generate message digests for messages of smaller length.
DRBG	This module tests whether the generated random number is deterministic. This test compares a known seed and known output against the generated random number.
RSA sign/verify	This module implements a KAT for signing and verifiying the operation of RSA. The test passes only if the signature is verified. The KAT must execute successfully before the operator can access the RSA functionality.
AES GCM	This module implements a KAT for AES encryption and decryption using GCM.
SHA1, SHA256, SHA384, SHA512, SHA3	This module implements the SHA1, SHA256, SHA384, SHA-512, and SHA3 short message test as part of the KAT.
ECDSA	This module implements the ECDSA pair-wise consistency test.
ECDH	This module implements the ECDH test.

Audit Messages

Audit messages are generated based on security events. All Audit messages include the ID, time, module ID, switch name, and message. All commands entered have an associated audit record.

Commands that include private data such as passwords have the CLI log redacted to not include private information. Fabric OS supports the last 8192 messages, which are persistently saved in the audit log and are not configurable. Audit records are sent to an external syslog server as soon as they are generated. The syslog server must support TLSv1.2. RASLog messages are sent to the syslog server as well.

Reading an Audit Message

AUDIT messages provide user and system-related information of interest for post-event auditing and troubleshooting.

The following example shows the format of an audit event message.

```
<Sequence Number> AUDIT, <timestamp>, [<Event ID>], <Severity>, <Event Class>, <User ID>/<Role>/<IP Address>/
<Interface>/<Application Name>, <Admin Domain>/<Switch Name>, <Reserved field for future expansion>, <Event-
Specific Information>
```

The following is a sample audit event message.

```
0 AUDIT, 2005/12/10-09:54:03, [SEC-1000], WARNING, SECURITY, JohnSmith/root/192.0.2.2/Telnet/CLI, Domain A/
JohnsSwitch, , Incorrect password during login attempt.
```

The following table describes the audit message fields.

Table 3: Audit message field description

Variable Name	Description
Sequence Number	The error message position in the log.
Audit flag	Identifies the message as an audit message.
Timestamp	The system time (UTC) when the message was generated on the switch. The RASLog subsystem supports an internationalized timestamp format based on the “LOCAL” setting.
Event ID	The message module and number. These values uniquely identify each message in the Fabric OS and reference the cause and actions recommended in this manual. Note that not all message numbers are used; there can be gaps in the numeric message sequence.
Severity	The severity of the error, which can be one of the following: • 1 – CRITICAL • 2 – ERROR • 3 – WARNING • 4 – INFO
Event Class	The event class, which can be one of the following: • CFG • CLI • FABRIC • FIRMWARE • LS • MAPS • RAS • SECURITY • ZONE
User ID	The user ID.
Role	The role of the user.
IP Address	The IP address or the resolved host name, if applicable.
Interface	The interface being used.
Application Name	The application name being used on the interface.
Admin Domain	The admin domain, if there is one.
Switch Name	The defined switch name or the chassis name of the switch depending on the action; for example, HA messages typically show the chassis name and login failures typically show the logical switch name. This value is truncated if it is over 16 characters in length. Use the `chassisName` command to name the chassis or the `switchName` command to rename the logical switch.
Reserved field for future expansion	This field is reserved for future use and contains a space character (null value).
Event-Specific Information	A text string that explains the error encountered and provides parameters supplied by the software at runtime.

Sample Audit Records

- The audit message indicates that the time was updated using the date CLI:

```
2022/11/11-18:06:55 (GMT), [RAS-3005], INFO, CLI, admin/admin/NONE/console/CLI,NA/Audit1/CHASSIS, , CLI:
 date -s "Fri Nov 11 18:06:42 GMT 2022"
2022/11/11-18:07:02 (GMT), [TS-1009], INFO, SECURITY, admin/admin/NONE/console/CLI,NA/Audit1/FID 3, , Date
 changed by user from 11/11/22-18:07:47 to 11/11/22-18:07:00.
```

- Audit start and stop:

```
2023/01/18-21:44:43 (GMT), [RAS-3005], INFO, CLI, admin/admin/NONE/console/CLI,NA/G720-/CHASSIS, , CLI:
 auditcfg --disable
2023/01/18-21:44:47 (GMT), [RAS-2002], INFO, RAS, admin/admin/NONE/console/CLI,NA/G720-F128/FID 128, ,
 Audit message log is disabled.
2023/01/18-21:44:56 (GMT), [RAS-2001], INFO, RAS, admin/admin/NONE/console/CLI,NA/G720-F128/FID 128, ,
 Audit message log is enabled.
2023/01/18-21:44:56 (GMT), [RAS-3005], INFO, CLI, admin/admin/NONE/console/CLI,NA/G720-/CHASSIS, , CLI:
 auditcfg --enable  -all
```

- Adding NTP keys:

```
2022/11/11-18:09:16 (GMT), [TS-1015], INFO, SECURITY, admin/admin/NONE/console/CLI,NA/Audit1/FID 3, , NTP
 Key with index 65530 and key type AES128CMAC added.
2022/11/11-18:09:16 (GMT), [RAS-3005], INFO, CLI, admin/admin/NONE/console/CLI,NA/Audit1/CHASSIS, , CLI:
 tsclockserver --addkey -index 65530 -type CMAC-AES-128
2022/11/11-18:10:17 (GMT), [TS-1015], INFO, SECURITY, admin/admin/NONE/console/CLI,NA/Audit1/FID 3, , NTP
 Key with index 17 and key type SHA1 added.
2022/11/11-18:10:18 (GMT), [RAS-3005], INFO, CLI, admin/admin/NONE/console/CLI,NA/Audit1/CHASSIS, , CLI:
 tsclockserver --addkey -index 17 -type HMAC-SHA1
```

- Configuring NTP server:

```
2022/11/11-18:10:33 (GMT), [TS-1002], INFO, SECURITY, admin/admin/NONE/console/CLI,NA/Audit1/FID
 3, ,External Clock Server used instead of LOCL: locl: 0x45585400 remote: 0x4c4f434c.
2022/11/11-18:10:33 (GMT), [TS-1013], INFO, SECURITY, admin/admin/NONE/console/CLI,NA/Audit1/FID
 3, ,NTP Clock Server List modified to tl27-16b.example.com; tl28-16b.example.com; tl29-16b.example.com;
 2620:100:4:e200::80;2620:100:4:e200::81;172.16.2.80; tl30-16b.example.com from LOCL.
2022/11/11-18:10:33 (GMT), [TS-1014], INFO, SECURITY, admin/admin/NONE/console/CLI,NA/Audit1/FID 3, , NTP
 Key Index List modified to 60000;17;16;NONE;NONE;NONE;60000 from NONE;NONE;NONE;NONE;NONE;NONE;NONE.
2022/11/11-18:10:34 (GMT), [RAS-3005], INFO, CLI, admin/admin/NONE/console/CLI,NA/Audit1_G6plus/
CHASSIS, , CLI: tsclockserver --set "tl27-16b.example.com; tl28-16b.example.com; tl29-16b.example.com;
 2620:100:4:e200::80;2620:100:4:e200::81;172.16.2.80; tl30-16b.example.com" -index
 "60000;17;16;NONE;NONE;NONE;60000"
```

- Time updated from NTP server:

```
2022/11/11-18:07:59 (GMT), [MAPS-1020], WARNING, MAPS, NONE/root/NONE/none/CLI,NA/Audit1-CA/FID 101, ,
 Switch wide status has changed from CRITICAL to HEALTHY.
2022/11/11-18:22:52 (GMT), [MAPS-1146], INFO, MAPS, NONE/root/NONE/none/CLI,NA/Audit1/FID 3, , Time changed
 on switch re-starting MAPS monitoring.
2023/01/04-12:33:32 (GMT), [TS-1010], INFO, SECURITY, NONE/root/NONE/none/CLI,NA/G720/FID 128,
 9.1.1b_bld03, , , , , , , NTP Server Time Update from 23/01/04-12:24:32 to 23/01/04-12:33:32
```

- Certificate Management:

```
2023/01/16-17:04:50 (GMT), [SEC-3030], INFO, SECURITY, admin/admin/tl27-16b.example.com/ssh/CLI,NA/G720/
FID 128, 9.1.1b_bld03, , , , , , , Event: secCertMgmt, Status: success, Info: Imported syslog switch ca
 certificate - rootca-rsa.pem(2048/sha256) from host 192.168.144.253.
2023/01/16-17:03:18 (GMT), [SEC-3030], INFO, SECURITY, admin/admin/tl27-16b.example.com/ssh/CLI,NA/G720/
FID 128, 9.1.1b_bld03, , , , , , , Event: secCertMgmt, Status: success, Info: Deleted syslog switch ca
 certificate  - Clntca.pem.
2023/01/17-13:46:06 (GMT), [RAS-3005], INFO, CLI, admin/admin/tl27-16b.example.com/ssh/CLI,NA/swd77/
CHASSIS, 9.1.1b_bld03, , , , , , , CLI: seccertmgmt generate -csr fcap
```

```
2023/01/17-13:46:05 (GMT), [AUTH-3003], INFO, SECURITY, admin/admin/tl27-16b.example.com/ssh/CLI,NA/G720/
FID 128, 9.1.1b_bld03, , , , , , , Event: pkiCreate, Status: success, Info: Created the PKI objects.
```

- OpenSSL errors, presented as is:

```
2022/11/11-18:31:58 (GMT), [SEC-3081], INFO, SECURITY, admin/admin/NONE/console/CLI,NA/Audit1/CHASSIS, ,
 Event: X509v3, Certificate Validation failed, Info: Reason = OCSP application verification failure.
 Host=Self CN=RSA_Tertiary_CA Serial=1006 AuthKey=B3B22CE3D30BCD71347AD9427E5EDA2426414C0F.
2022/11/11-18:33:07 (GMT), [SEC-3081], INFO, SECURITY, admin/admin/NONE/console/CLI,NA/Audit1/FID
 3, , Event: X509v3, Certificate Validation failed, Info: Reason = Invalid CA certificate Host=self
 CN=RSA_Intermediate_CA serial=1004 Authkey=B3B22CE3D30BCD71347AD9427E5EDA2426414C0F.
2022/11/11-18:34:42 (GMT), [SEC-3081], INFO, SECURITY, admin/admin/NONE/console/CLI,NA/Audit1/CHASSIS, ,
 Event: X509v3, Certificate Validation failed, Info: Reason = unable to get local issuer certificate.
 Host=Self CN=172.16.193.144 Serial=1001 AuthKey=074B83BC1325BC1B6DBCC6A4F389F8B683C39798.
2022/11/11-18:36:21 (GMT), [SEC-3081], INFO, SECURITY, NONE/root/NONE/none/CLI,NA/Audit1/CHASSIS, , Event:
 X509v3, Certificate Validation failed, Info: Reason = Hostname mismatch. Host=domain.englab.example.com
 CN=172.16.2.80, OU Serial=1014 AuthKey=9B2AC7CF394520953BA07BA7C2D40C610C13B87D.
2022/11/11-18:36:21 (GMT), [SEC-3081], INFO, SECURITY, NONE/root/NONE/none/CLI,NA/Audit1/
CHASSIS, , Event: X509v3, Certificate Validation failed, Info: Reason = unspecified
 certificate verification error. Host=domain.englab.example.com CN=172.16.2.80 Serial=1014
 AuthKey=9B2AC7CF394520953BA07BA7C2D40C610C13B87D.
2022/11/11-18:36:21 (GMT), [SEC-3077], INFO, SECURITY, NONE/root/NONE/none/CLI,NA/Audit1/CHASSIS, , Event:
 TLS SESSION, TLS handshake failed, Info: unsupported elliptic curve. Host=domain.englab.example.com.
2022/11/11-18:38:11 (GMT), [SEC-3081], INFO, SECURITY, NONE/NONE/172.16.255.24/none/
CLI,NA/Audit1/CHASSIS, , Event: X509v3, Certificate Validation failed, Info: Reason = IP
 address mismatch. Host=2620:100:4:f800:56d:b8a9:7a6d:3bf4 CN=WinAAA2016Auto.example.com
 Serial=7C0000000D2F05F7731A67DC9200000000000D AuthKey=E6ECA4CE4187C3398CC7915057EFF7F20A7D654D.
2022/11/11-19:28:07 (GMT), [SEC-3077], INFO, SECURITY, NONE/NONE/172.16.255.24/none/CLI,NA/Audit1/
CHASSIS, , Event: TLS SESSION, TLS handshake failed, Info: certificate verify failed. Host=3844openldap-
user4.example.com. CN=007@ewsexample.com, CN Serial=1003 AuthKey=DF43BBE0E8FE7AB858C2FC9127C601B8C6CB6AF3.
2022/11/11-19:38:13 (GMT), [SEC-3081], INFO, SECURITY, NONE/NONE/172.16.255.24/none/CLI,NA/Audit1/
CHASSIS, , Event: X509v3, Certificate Validation failed, Info: Reason = self signed certificate
 in certificate chain. Host=openldapuser1.example.com CN=bsnidcta1 Serial=8A6FC5F2ABEB262F
 AuthKey=9651AA0F260028A7FA3E58DC58B923CD6435B1DA.
2022/11/11-19:39:50 (GMT), [SEC-3081], INFO, SECURITY, NONE/NONE/172.16.255.24/none/CLI,NA/Audit1/
CHASSIS, , Event: X509v3, Certificate Validation failed, Info: Reason = unsupported certificate purpose.
 Host=Self CN=172.16.194.130 Serial=E3C2 AuthKey=.
2022/11/11-19:50:06 (GMT), [SEC-3081], INFO, SECURITY, NONE/NONE/172.16.255.24/none/CLI,NA/Audit1/
CHASSIS, , X509v3, Certificate Validation failed, Info: Reason = path length constraint exceeded. Host=Self
 CN=RSA_Intermediate_CA Serial=1011 AuthKey=1328F7583579E35E3157CC407D4C4EAB74613F27.
2022/11/11-19:58:44 (GMT), [SEC-3081], INFO, SECURITY, NONE/NONE/172.16.255.24/none/CLI,NA/Audit1/
CHASSIS, , Event: X509v3, Certificate Validation failed, Info: Reason = unable to find OCSP responder url.
 Host=Self CN=172.16.194.130 Serial=E3C3 AuthKey=C5E19B695C7981264EE0B098774BE6F90B95980D.
2022/10/19-12:26:43 (GMT), [SEC-3081], 71813, WWN 10:00:c4:f5:7c:01:ad:30 | CHASSIS, INFO, swd77,
 Event: X509v3, Certificate Validation failed, Info: Reason = invalid CA certificate: basic
 constraints absent for CA. Host=172.16.194.130 CN=subsubca-no-basic-constraints-rsa Serial=49
 AuthKey=95C9C9D83E68B52A21DC91A4C165FDF0B09AC162.
2022/10/19-12:27:34 (GMT), [SEC-3081], 71827, WWN 10:00:c4:f5:7c:01:ad:30 | CHASSIS, INFO,
 swd77, Event: X509v3, Certificate Validation failed, Info: Reason = invalid CA certificate:
 basic constraints false for CA. Host=172.16.194.130 CN=subsubca-ca-flag-false-rsa Serial=2B
 AuthKey=95C9C9D83E68B52A21DC91A4C165FDF0B09AC162.
2023/01/16-13:45:48 (GMT), [SEC-3081], INFO, SECURITY, admin/admin/172.16.194.130/ssh/CLI,NA/G720/FID 128,
 9.1.1b_bldo3, , , , , , Event: X509v3, Certificate Validation failed Info: Reason = EC explicit curve not
 allowed Host=self CN=subca-rsa serial=018C Authkey=95C9C9D83E68B52A21DC91A4C165FDF0B09AC162.
```

```
2023/01/16-13:21:36 (GMT), [SEC-3081], INFO, SECURITY, NONE/root/NONE/none/CLI,NA/swd77/
CHASSIS, 9.1.1b_bld03, , , , , , , Event: X509v3, Certificate Validation failed, Info: Reason
 = certificate is revoked to OCSP. Host=172.16.194.130 CN=tl27-16b.example.com Serial=D1
 AuthKey=0B41B4F80FB7ADC1A9653D6AD06F7527823E04FE.
2023/01/16-12:49:14 (GMT), [SEC-3081], INFO, SECURITY, NONE/root/NONE/none/CLI,NA/swd77/
CHASSIS, 9.1.1b_bld03, , , , , , , Event: X509v3, Certificate Validation failed, Info:
 Reason = certificate has expired. Host=1172.16.194.130 CN=tl27-16b.example.com Serial=87
 AuthKey=0B41B4F80FB7ADC1A9653D6AD06F7527823E04FE.
```

- TLS session errors:

```
2022/07/27-15:20:54 (GMT), [SEC-3077], 110, CHASSIS, INFO, 7810_BRM_Security3D2----------, Event: TLS
 SESSION, TLS handshake failed, Info: version too low. Host=172.16.37.177.
2023/01/16-15:20:54 (GMT), [SEC-3077], INFO, SECURITY, NONE/root/NONE/none/CLI,NA/G8000/CHASSIS,
 9.1.1b_bld03, , , , , , , Event: TLS SESSION, TLS handshake failed, Info: unsupported protocol.
 Host=tl27-16b.example.com.
2022/07/27-15:20:55 (GMT), [SEC-3077], 117, CHASSIS, INFO, 7810_BRM_Security3D2----------, Event: TLS
 SESSION, TLS handshake failed, Info: no shared cipher. Host=172.16.37.177.
2022/07/27-15:22:24 (GMT), [SEC-3077], 123, CHASSIS, INFO, 7810_BRM_Security3D2----------, Event: TLS
 SESSION, TLS handshake failed, Info: required cipher missing. Host=172.16.37.177.
2023/01/16-15:22:28 (GMT), [SEC-3077], 8906, WWN 10:00:c4:f5:7c:02:47:48 | CHASSIS, INFO, G8000, Event: TLS
 SESSION, TLS handshake failed, Info: sslv3 alert bad record mac. Host=tl27-16b.example.com.
2022/07/27-15:22:31 (GMT), [SEC-3077], 136, CHASSIS, INFO, 7810_BRM_Security3D2----------, Event: TLS
 SESSION, TLS handshake failed, Info: no suitable key share. Host=172.16.37.177.
2022/07/27-15:31:56 (GMT), [SEC-3077], 153, CHASSIS, INFO, 7810_BRM_Security3D2----------, Event: TLS
 SESSION, TLS handshake failed, Info: inappropriate fallback. Host=172.16.37.177.
2022/07/27-15:44:59 (GMT), [SEC-3077], 159, CHASSIS, INFO, 7810_BRM_Security3D2----------, Event: TLS
 SESSION, TLS handshake failed, Info: unexpected record. Host=172.16.37.177.
2022/07/27-15:45:02 (GMT), [SEC-3077], 172, CHASSIS, INFO, 7810_BRM_Security3D2----------, Event: TLS
 SESSION, TLS handshake failed, Info: block cipher pad is wrong. Host=172.16.37.177.
2023/01/16-10:46:50 (GMT), [SEC-3077], INFO, SECURITY, NONE/root/NONE/none/CLI,NA/swd77/CHASSIS,
 9.1.1b_bld03, , , , , , , Event: TLS SESSION, TLS handshake failed, Info: wrong certificate type.
 Host=tl27-16b.example.com.
2023/01/17-13:06:22 (GMT), [SEC-3077], INFO, SECURITY, NONE/root/NONE/none/CLI,NA/G8000/CHASSIS,
 9.1.1b_bld03, , , , , , , Event: TLS SESSION, TLS handshake failed, Info: unknown cipher returned.
 Host=tl27-16b.example.com.
2023/01/17-13:08:28 (GMT), [SEC-3077], 8903, WWN 10:00:c4:f5:7c:02:47:48 | CHASSIS, INFO, G8000, Event: TLS
 SESSION, TLS handshake failed, Info: bad signature. Host=tl27-16b.example.com.
2023/01/17-13:09:05 (GMT), [SEC-3077], 8904, WWN 10:00:c4:f5:7c:02:47:48 | CHASSIS, INFO, G8000, Event: TLS
 SESSION, TLS handshake failed, Info: digest check failed. Host=tl27-16b.example.com.
```

- TLS handshake initiation and termination:

```
2022/07/27-16:34:56 (GMT), [SEC-3078], INFO, SECURITY, NONE/admin/NONE/none/CLI,NA/sw0/CHASSIS, , Event:
 TLS SESSION, TLS handshake , Info: Establishing TLS connection. Host=172.16.73.62.
2022/07/27-16:34:56 (GMT), [SEC-3078], INFO, SECURITY, NONE/admin/NONE/none/CLI,NA/sw0/CHASSIS, , Event:
 TLS SESSION, TLS handshake , Info: Terminating TLS connection. Host=172.16.73.62.
```

- SSH connection errors:

```
2022/11/11-18:59:03 (GMT), [SEC-3076], INFO, SECURITY, NONE/NONE/NONE/none/CLI,NA/Audit1/CHASSIS, , Event:
 SSH, Status: failed, Info: SSH Session establishment failed. Reason: Unable to negotiate a key exchange
 method, IP Addr: 172.16.38.39.
2022/11/11-19:00:14 (GMT), [SEC-3076], INFO, SECURITY, NONE/NONE/NONE/none/CLI,NA/Audit1/CHASSIS, , Event:
 SSH, Status: failed, Info: SSH Session establishment failed. Reason: no matching cipher found, IP Addr:
 2001:db8:ffff:ffff:ffff:ffff:ffff:ffff:18.
```

```
2023/01/16-13:03:29 (GMT), [SEC-3073], WARNING, SECURITY, admin/admin/172.16.38.39/ssh/CLI,NA/swd77/
CHASSIS, 9.1.1b_bld03, , , , , , , Event: sshd, Status: failure, Info: SSH server received corrupt/big
 packet.
2023/01/16-15:44:11 (GMT), [SEC-3076], INFO, SECURITY, NONE/NONE/NONE/none/CLI,NA/swd77/CHASSIS,
 9.1.1b_bld03, , , , , , , Event: SSH, Status: failed, Info: SSH Session establishment failed. Reason: no
 matching hostkey algorithm found, IP Addr: 172.16.38.39.
2023/01/16-11:26:33 (GMT), [SEC-3076], INFO, SECURITY, NONE/NONE/NONE/none/CLI,NA/swd77/CHASSIS,
 9.1.1b_bld03, , , , , , , Event: SSH, Status: failed, Info: SSH Session establishment failed. Reason: no
 matching mac found, IP Addr: 172.16.38.39.
2023/01/16-12:56:42 (GMT), [SEC-3076], INFO, SECURITY, NONE/NONE/NONE/none/CLI,NA/swd77/CHASSIS,
 9.1.1b_bld03, , , , , , , Event: SSH, Status: failed, Info: SSH Session establishment failed. Reason:
 Unable to negotiate a key exchange method, IP Addr: 172.16.38.39.
```

- Login and Logout:

```
2022/11/11-19:09:12 (GMT), [SEC-3020], INFO, SECURITY, admin/admin/172.16.73.62/ssh/CLI,NA/switch_70/FID
 128, , Event: login, Status: success, Info: Successful login attempt via REMOTE, IP Addr: 172.16.73.62.
2022/11/11-19:09:12 (GMT), [SEC-3022], INFO, SECURITY, admin/admin/172.16.73.62/ssh/CLI,NA/Audit1/FID 3, ,
 Event: logout, Status: success, Info: Successful logout by user [admin].
2023/01/16-13:58:53 (GMT), [SEC-3020], INFO, SECURITY, admin/admin/NONE/console/CLI,NA/G720/FID 128,
 9.1.1b_bld03, , , , , , , Event: login, Status: success, Info: Successful login attempt via SERIAL.
2023/01/16-10:07:14 (GMT), [SEC-3021], INFO, SECURITY, admin/None/NONE/console/CLI,NA/G720/FID 128,
 9.1.1b_bld03, , , , , , , Event: login, Status: failed, Info: Failed login attempt via SERIAL.
```

- Failed logins:

```
2022/11/11-19:11:52 (GMT), [SEC-3021], INFO, SECURITY, r128/None/bsn1-2dot0.ndclab.example.com/ssh/
CLI,NA/Audit1/FID 3, , Event: login, Status: failed, Info: Failed login attempt via REMOTE, IP Addr:
 bsn1-2dot0.ndc.example.com.
2022/09/28-12:28:44:094498 (GMT), [SEC-5075], INFO, SECURITY, admin/None/10.210.211.141/ssh/CLI,NA/sw0/FID
 128, , Event: login, Status: failed, Info: Failed pubkey login attempt via REMOTE, IP Addr: 172.2.2.2.
2023/01/14-08:10:18 (GMT), [SEC-3023], INFO, SECURITY, NONE/NONE/tl27-16b.example.com/none/CLI,NA/G720/FID
 128, 9.1.1b_bld03, , , , , , , Event: login, Status: failed, Info: Account [FOSTestUser] locked, failed
 password attempts exceeded.
```

- Rekeying SSH session:

```
2022/11/11-05:09:13 (GMT), [SEC-3072], INFO, SECURITY, admin1/admin/172.16.255.25/ssh/CLI,NA/G730_num2/
CHASSIS, , Event: sshd, Status: success, Info: Rekeying for session for 172.16.255.25:37458.
```

- The following audit message indicates a successful Domain ID change via CLI:

```
2022/07/27-16:59:02 (GMT), [CONF-1042], INFO, CONFIGURATION, admin1/admin/NONE/console/CLI,NA/7810-brm-
bsnlab/FID 128, , Fabric Configuration Parameter Domain changed to 3.
```

- Successful firmware migration:

```
2023/01/04-17:07:22 (GMT), [SULB-1001], WARNING, FIRMWARE, admin/admin1/NONE/console/CLI,NA/G730_2/
CHASSIS, , Firmwaredownload command has started. (From v9.1.1b_bld02 To v9.1.1b_bld03).
2023/01/04-17:15:04 (GMT), [SULB-1039], INFO, FIRMWARE, NONE/root/NONE/none/CLI,NA/G730_2/CHASSIS, , CP has
 completed relocating the internal firmware image.
2023/01/04-17:17:10 (GMT), [SULB-1003], INFO, FIRMWARE, NONE/root/NONE/none/CLI,NA/G730_2/CHASSIS, ,
 Firmwarecommit has started.
2023/01/04-17:21:16 (GMT), [SULB-1004], INFO, FIRMWARE, NONE/root/NONE/none/CLI,NA/G730_2/CHASSIS, ,
 Firmwarecommit has completed.
2023/01/04-17:21:16 (GMT), [SULB-1002], INFO, FIRMWARE, NONE/root/NONE/none/CLI,NA/G730_2/CHASSIS, ,
 Firmwaredownload command has completed successfully.
```

- Failed firmware migration:

```
2022/11/11-16:47:09 (GMT), [SULB-1001], WARNING, FIRMWARE, admin/root/NONE/console/CLI,NA/Audit1/CHASSIS, ,
 Firmwaredownload command has started. (From v9.1.1b_bld02 To v9.1.1b_bld03).
```

```
2022/11/11-16:47:24 (GMT), [RAS-3009], INFO, CLI, admin/root/NONE/console/CLI,NA/Audit1/CHASSIS, , The
 command Firmwaredownload exits with return code: -62. Message: Firmware signature validation failed.
2022/11/11-16:47:28 (GMT), [RAS-3005], INFO, CLI, admin/root/NONE/console/CLI,NA/Audit1/CHASSIS, , CLI:
 firmwaredownload
```

- Error presented on console if the build does not support the platform:

```
Cannot download the requested firmware because the firmware doesn't support this platform. Please enter
 another firmware path.
```

- Generic error presented if firmware is not present, login failed, or SSH keys are wrong:

```
2022/07/27-18:23:01 (GMT), [SULB-1036], 56, CHASSIS, INFO, G720_2-----, Failed to access scp://
root:@172.16.38.39//root/builds/v9.1.1b_bld02/release.plist.

The server is inaccessible or firmware path is invalid. Please make sure the server name/IP address and the
 firmware path are valid, the protocol and authentication are supported. It is also possible that the RSA
 host key could have been changed and please contact the System Administrator for adding the correct host
 key.
```

- Error presented on console if the firmware key has been tampered with:

```
Firmwaredownload failed because the signature for the firmware could not be validated.
```

- IP filter allowing or disallowing ports:

```
2022/11/11-19:20:06 (GMT), [SEC-3075], INFO, SECURITY, admin/admin/NONE/console/CLI,NA/G720_1/FID 44, ,
 Event: ipfilter, HTTPS PORT STATE: DROP, Info: Activated ipfilter policy IP_v4 has blocked HTTPS port..
2022/11/11-19:20:21 (GMT), [SEC-3037], INFO, SECURITY, admin/admin/NONE/console/CLI,NA/G720_1/FID 44, ,
 Event: ipfilter, Status: success, Info: default_ipv4 ipfilter policy activated.
2022/11/11-19:20:21 (GMT), [SEC-3075], INFO, SECURITY, admin/admin/NONE/console/CLI,NA/G720_1/FID 44, ,
 Event: ipfilter, HTTP PORT STATE: ACTIVE, Info: Activated ipfilter policy default_ipv4 has activated HTTP
 port..
2022/11/11-19:20:21 (GMT), [SEC-3075], INFO, SECURITY, admin/admin/NONE/console/CLI,NA/G720_1/FID 44, ,
 Event: ipfilter, TELNET PORT STATE: ACTIVE, Info: Activated ipfilter policy default_ipv4 has activated
 Telnet port.
```

- Other admin actions:

```
2023/01/13-08:34:24 (GMT), [RAS-2013], 79113, WWN 10:00:c4:f5:7c:01:ad:30 | CHASSIS, INFO, swd77, syslog
 facility level has been changed from 7 to 6.
2023/01/13-08:51:11 (GMT), [SEC-3083], INFO, SECURITY, admin/admin/tl27-16b.example.com/ssh/CLI,NA/G720/FID
 128, 9.1.1b_bld03, , , , , , , Switch banner has been updated.
2023/01/13-08:49:08 (GMT), [RAS-3005], INFO, CLI, admin/admin/tl27-16b.example.com/ssh/CLI,NA/swd77/
CHASSIS, 9.1.1b_bld03, , , , , , , CLI: timeout 60
2023/01/13-11:04:16 (GMT), [SEC-1312], 79132, WWN 10:00:c4:f5:7c:01:ad:30 | FID 128, INFO, G720, passwdcfg
 params changed as (lockoutthreshold:10->3) .
2023/01/13-08:59:36 (GMT), [RAS-2006], INFO, SECURITY, admin/admin/tl27-16b.example.com/ssh/CLI,NA/swd77/
CHASSIS, 9.1.1b_bld03, , , , , , , Syslog server IP address tl27-16b.example.com added.
2023/01/13-09:57:26 (GMT), [SEC-3050], INFO, SECURITY, admin/admin/tl27-16b.example.com/ssh/CLI,NA/G720/
FID 128, 9.1.1b_bld03, , , , , , , Event: sshutil, Status: success, Info: Generated keypair for outgoing
 connection
2023/01/13-09:57:26 (GMT), [SEC-3050], 79118, WWN 10:00:c4:f5:7c:01:ad:30 | FID 128, INFO, G720, Event:
 sshutil, Status: success, Info: Generated keypair for outgoing connection
2023/01/13-10:21:37 (GMT), [SEC-3069], INFO, SECUR
ITY, admin/admin/NONE/console/CLI,NA/G720/FID 128, 9.1.1b_bld03, , , , , , , Event: seccrypt
ocfg, Status: success, Info: Applied security template, default_cc.
2023/01/16-17:03:18 (GMT), [RAS-3005], INFO, CLI, admin/admin/tl27-16b.example.com/ssh/CLI,NA/swd77/
CHASSIS, 9.1.1b_bld03, , , , , , , CLI: seccertmgmt delete -ca -client syslog
```

```
2023/01/16-17:03:18 (GMT), [SEC-3030], INFO, SECURITY, admin/admin/tl27-16b.example.com/ssh/CLI,NA/G720/
FID 128, 9.1.1b_bld03, , , , , , , Event: secCertMgmt, Status: success, Info: Deleted syslog switch ca
 certificate  - Clntca.pem.
```

Revision History

The revision history provides a list of the important changes made in each version of the document.

FOS-91x-CC-UG100; January 19, 2023

- Initial document version.

Documentation Legal Notice

This notice provides copyright and trademark information as well as legal disclaimers.

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.

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, to view the licensing terms applicable to the open source software, and to obtain a copy of the programming source code, please download the open source disclosure documents in the Broadcom Customer Support Portal (CSP). If you do not have a CSP account or are unable to log in, please contact your support provider for this information.


BROADCOM®