BROCADE
A Broadcom Company

Brocade® Fabric OS® Security Considerations

User Guide

Table of Contents

Chapter 1: Introduction

1.1 Overview

Broadcom provides this document to guide Brocade® SAN users when evaluating the security options specific to Brocade platforms. Select and align security settings on your Brocade SAN infrastructure in accordance with your organization's security policies.

Brocade Fabric OS® firmware, SANnav™ software, and hardware platforms have the specified ability to restrict and protect from malicious intent. All Brocade FOS SAN equipment should have the additional protection of network firewalls, intrusion detection systems, intrusion protection systems, application security, layer 2 design security, layer 3 design security, and layer 1 access security.

1.2 Applicability

The capabilities, content, and references in this document are based on features and functionality available with Brocade Fabric OS 9.2.x. If using a different version of Fabric OS (FOS), please reference the appropriate admin guide for configuration details.

See the Revision History section for details on which FOS version was the latest at the time of writing.

1.3 Document References

The following documents are referenced in this User Guide:

- *Brocade Fabric OS Administration Guide* (referred to in this document as FOS Administration Guide)
- *Brocade Fabric OS Command Reference Manual*
- *Brocade Fabric OS Web Tools User Guide*
- *Brocade Fabric OS REST API Reference Manual*
- *Brocade Fabric OS Extension User Guide*
- *Brocade Fabric OS Features and Standards Support Matrix*
- *Brocade Fabric OS Message Reference Manual*
- *Brocade Fabric OS MAPS User Guide*
- *Brocade Fabric OS Software Licensing User Guide*
- *Brocade Fabric OS Software Upgrade User Guide*
- *Brocade Fabric OS Access Gateway User Guide*
- *Brocade Fabric OS MIB Reference Manual*
- *Brocade Fabric OS FCoE User Guide*
- *Brocade SANnav Management Portal User Guide*

Chapter 2: Fabric OS Default Secure Configuration

Prior to FOS v9.2.0, the default FOS configuration set protocols and ciphers that lead to platforms not adhering to security best practices, which may result in them being flagged during a network security scan.

Switches shipping with FOS v9.2.0 from the factory are set with the Default Secure configuration.

Switches upgraded to FOS v9.2.0 can be set with the Default Secure configuration using a CLI command. Seamless migration between FOS levels is supported.

Default Secure configuration includes the following features and settings:

- Disable SNMPv1 and SNMPv2
- Block Telnet, HTTP and FTP
- Default strong cryptographic profile (ciphers and protocols)
- Support for SSH stronger key sizes
- Support for a new range of TLS protocols
- New Default IPv4 and IPv6 IP filter policies
  - Support option for resetting IP filter policies

There are potential disruptions when setting the Default Secure configuration:

- SSH
  - SSH fails on mismatch (unsupported) of any cipher suite between client and server.
  - Public key login fails for already setup users.
- TLS
  - Connections fail if there is mismatch in the supported and configured ciphers or protocol versions.
- LDAP, RADIUS PEAP-MSCHAP, Syslog, HTTPS
  - Existing certificates are deleted and need to be regenerated and resigned.
- IPfilter
  - Telnet and HTTP are denied by default in the new policy. If any port is explicitly in the permit state via an active policy IPfilter rule and in use, it will be blocked after the `securitydefault` operation.
  - For example: HTTP based applications on port 80, telnet on port 23, and any other ports permitted via custom IPfilter policies.

Chapter 3: Brocade Platform Access

Access to Brocade platforms can be initiated by either users or applications. All access is validated with Authentication; communications can be secure or plaintext. Secure communications are encrypted using private keys.

A variety of applications commonly access FOS via the management interface:

- Serial client
- SSH client
- Brocade SANnav
- Brocade Fabric OS Web Tools
- Active Support Connectivity Gateway (ASC-G)
- Automation applications via REST API
- SNMP

TLS is a secure protocol designed to provide secure communications over a network. Many protocols use TLS to secure their communications. Listed below are some of the protocols secured by TLS. TLS was based on SSL 3.0, which was subsequently deprecated in 2015. Brocade FOS supports various levels of TLS up to TLS v1.3, which is the current version at the time this document was updated.

Not all protocols use TLS, although TLS is the most common way to secure a protocol's network communications.

The port numbers in the table below are commonly used for these services; however, the port numbers could be customized to the environment. For example, Brocade SANnav servers configure SSH on port 123 because port 22 is used by the application. SSH might not be on port 22, depending on the environment.

Table 1: Secure Protocols

Secure Protocol	Security Protocol	Port
SSH	SSH	TCP 22
SFTP	SSH	TCP 22
SCP	SSH	TCP 22
HTTPS	TLS	TCP 443
LDAPS	TLS	TCP 389 and 636
Secure SMTP	TLS	TCP 587
Secure Syslog	TLS	TCP 6514
SNMPv3	SHA and AES	UDP 161 and 162
RADIUS	EAP-TLS, PEAP-MSCHAPv2	UDP 1812 and 1813

Table 2: Not Secure Protocols

Not Secure Protocol	Port
Telnet	TCP 23
SNMPv1	UDP 161 (polling) and 162 (traps)
SNMPv2	UDP 161 (polling) and 162 (traps)
HTTP	TCP 80
FTP	TCP 20 and TCP 21
RADIUS (EAP-TTLS/PAP)	UDP 1812 and 1813
syslog	UDP 514

3.1 FOS CLI Access

The FOS CLI can be accessed through the serial console or through the management interface (Ethernet). The section below describes each method and the steps recommended to secure access.

3.1.1 Serial Console

The serial console does not provide secure transmission across the wire; there is no serial data encryption. All serial communications are in the clear. The Brocade SAN platform credentials can be compromised using password recovery techniques if physical access to the platform is permitted.

Reference	Action
Security Best Practice	■ Place Brocade platforms in a secure and physical access restricted data center. ■ Ensure access to the serial console port is behind a locked cabinet door. ■ Enact a strict change control policy such that any unbeknownst changes are quickly discovered through the FOS audit functions. ■ Securely mount Brocade platforms in a data center cabinet, with redundant and secure cooling and power.
FOS Administration Guide	■ Work with your organization's security officer to best meet security objectives for your SAN infrastructure and operations. ■ Brocade does not provide an Admin Guide for data center access and physical platform security. ■ Review the following section: Console Sessions Using the Serial Port

3.1.2 IPv4 and IPv6 via Ethernet

Commonly IPv4 is the protocol used on the management network in data center environments, unless the organization has transitioned to IPv6, in which case IPv4 is not used.

The maximum number of console, SSH, and telnet sessions for locally authenticated admin and maintenance users is 12; this limit is not applicable to AAA authenticated users.

Reference	Action
Security Best Practice	■ If IPv4 is not used, do not configure an IPv4 IP address. ■ If IPv6 is not used, the IPv6 link-local remains accessible even without an IPv6 address (auto-configuration is disabled). ■ IPv6 can be secured by creating an IPfilter for IPv6 with a single deny rule. At least one rule has to be configured to activate a policy. Create a rule: Rule 1, the source IP = any, protocol = TCP (or UDP, does not matter), dest port = 22 (could be anything), action = deny. Effectively, this single deny rule plus the following implicit deny all creates a deny all IPv6 condition.
FOS Administration Guide	■ Review the following section: Brocade FOS IP Filter Policy.

3.1.3 FOS IPfilter

The management port is protected from unauthorized and malicious incoming IP traffic. IPfilter performs packet filtering, gaining essential protection against network-based attacks. By limiting ingress access to the management port, FOS IPfilter establishes the first line of defense.

The IPfilter default is to permit “any” source IP address for communication; however, to enhance security, only specific source IP addresses or subnets should be permitted. This requires modifying the IPfilter policies. Access rules are grouped into separate IP version (IPv4 and IPv6) policies. Every rule designates the protocol (UDP or TCP), the destination port, and the source IP address or subnet. If traffic does not match any rule and falls to the bottom, the result is an implicit deny all.

IPfilter only considers traffic that is coming into the management interface. No other interfaces are monitored with IPfilter. A TCP connection that FOS initiates does not need a rule for the returning traffic from that same connection; IPfilter recognizes the originated connection and permits the traffic.

The following applications are permitted by the default IPfilter policy:

Application	Protocol and Port	Action
SSH	TCP 22	Allow
Telnet	TCP 23	Allow (Default Secure Configuration is Deny)
HTTP	TCP 80	Allow (Default Secure Configuration is Deny)
HTTPS	TCP 443	Allow
SNMP (receiving requests)	UDP 161	Allow
NTP	UDP 123	Allow
Ephemeral	TCP 600-1023	Allow
Ephemeral	UDP 600-1023	Allow

Reference	Action
Security Best Practice	Update the default IPv4 and IPv6 IPfilter policies for enhanced security. Below is a list of recommended changes: ■ For FOS v9.2.0, the default secure configuration is with telnet (23) and HTTP (80) denied. When switches upgrade from FOS v9.1.1+, update their policies or use the default reset option. ■ For v9.1.1+, you cannot change the default IPv4 and IPv6 policies. New policies need to be cloned or created, and those policies used instead of the default. Depending on the FOS version, remove the rules allowing unsecure protocols, such as telnet (23) and HTTP (80). If traffic does not match a rule, and falls through to the bottom, the result is an implicit deny all. ■ SNMPv3 is more secure when you specify the source IP addresses (or subnet) for the devices making the SNMP request. Additionally, refer to the SNMPv3 section of this document for more security details for SNMP. ■ NTP is more secure when you specify the source IP addresses (or subnet) for the devices providing the NTP service. Additionally, refer to the NTP section of this document for more security details for NTP. ■ FOS uses ephemeral TCP and UDP ports 600-1023 for various external communications, and, therefore should remain open; however, the IPfilter source IP can be restricted to the Brocade platforms’ management IP addresses. ■ Ensure management access to the Brocade platforms originates from known administrative devices or platforms on a determined IP subnet. Change the SSH source IP address from “any” to the management IP address or subnet used to access the Brocade platforms. All other source IP addresses will be denied access. In the case of DHCP for laptops or VPNs, it is best to specify the subnets.
FOS Administration Guide	■ Review the following section: Brocade FOS AG IPfilter Policy. ■ Review the following section: Brocade FOS command `ipfilter`.

3.1.4 FOS CLI: Telnet

The FOS CLI shell can be accessed using Telnet over TCP/IP. Telnet is not secure because the username, password, and all data transmission are sent in the clear. From the perspective of SAN operations, a number of untrusted users can have access to the data center's management network; therefore, usernames and passwords can be compromised.

Telnet transmissions are vulnerable to masquerade, eavesdropping, replay, and man-in-the-middle attacks. Potentially, telnet can expose Brocade platforms to breach, resulting in critical systems losing access to volumes, going offline, and data loss.

Reference	Action
Security Best Practice	■ Use IPfilter to block telnet prohibiting access to TCP port 23.
FOS Administration Guide	■ Review the following section: Brocade FOS Blocking Telnet.

3.1.5 FOS CLI: SSH

The FOS CLI can be accessed using SSH over TCP/IP. Secure access to FOS must use a protocol, such as SSH (TCP port 22 by default). A secure protocol means the user is authenticated, and the transmissions are encrypted. SSH is secure because the username, password, and all data transmissions remain private over the data center's management network; confidential data cannot be easily compromised. SSH transmissions are not vulnerable to masquerade, eavesdropping, replay, and man-in-the-middle attacks.

- Safe SSH encryption algorithms include: AES256-CTR, ECDH-SHA2-NISTP521
- Unsafe SSH encryption algorithms include: 3DES, MD5

Reference	Action
Security Best Practice	■ Use SSH to remotely access the FOS CLI. ■ Newer versions of FOS support the following SSH client settings: – Encryption: AES256-CTR – Kex: ECDH-SHA2-NISTP521 – Mac: HMAC-SHA2-512 ■ FOS IPfilter by default permits SSH connections. ■ If not already denied, remove the IPfilter telnet rule (TCP port 23).
FOS Administration Guide	■ Review the following section: Brocade FOS Secure Shell Protocol.

3.1.6 FOS sshutil Command

The FOS `sshutil` command provides management to SSH keys, which can be imported, exported, generated, deleted, and listed.

OpenSSH 7.0 deprecated DSA keys in 2017. Remove the SSH DSA key and use the RSA or ECDSA keys instead.

Reference	Action
Security Best Practice	■ Depending on the version of FOS, delete the SSH DSA key from FOS. It has already been removed in newer versions of FOS. ■ Use only the RSA or ECDSA keys for SSH, which are enabled by default.
FOS Administration Guide	■ Review the following section: FOS command `sshutil`.

3.1.7 Idle Session Timeout and Idle Shell Timeout

There is a reduced chance of a CLI session hijacking when an appropriate inactivity timeout exists. Users may mistakenly leave a CLI session open and unattended; the session poses a severe security vulnerability. CLI session inactivity will timeout and automatically close an open session, forcing the user to log in again.

The default FOS CLI idle session timeout is 10 minutes while shell timeout per default is not configured.

Reference	Action
Security Best Practice	■ Set the CLI session timeout to 10 minutes or less. ■ Set the CLI shell timeout accordingly.
FOS Administration Guide	■ Review the following section: FOS timeout.

3.1.8 Login Banners

The security banner does not provide true physical or virtual protection for a system. However, it can provide legal protection if an unauthorized user violates access restrictions, such as Terms of Use, and accesses the system anyway.

Warning banners should be implemented at a device access point if an organization seeks to discipline an employee or prosecute an unauthorized user. By providing a clear and strong message, the warning banner essentially dissolves any excuse of a user not knowing what they did was wrong.

Brocade FOS provides both a pre and post-login banner for CLI access.

Reference	Action
Security Best Practice	■ Set a pre-login security banner with the verbiage per your organization’s SAN device login policies and Terms of Use.
FOS Administration Guide	■ Review the following section: FOS command `motd`. ■ Review the following section: FOS command `bannerset`.

3.1.9 FOS fosexec Command

The `fosexec` command allows you to run FOS commands on a single remote platform or all platforms in a fabric. The local and remote switches must be configured to send and receive remote command execution. There is no need to log in to the remote switch. The command outputs are displayed on the local switch. The commands run using fosexec are captured in the remote switch's CLI history and audit logs. Fosexec runs inline over the FC ISLs.

The fosexec feature is disabled by default. Fosexec execution is allowed based on remote RBAC permissions. Unless there is a need to run FOS CLI commands from one platform on another or all platforms in a fabric, for greater security, fosexec should remain disabled.

Reference	Action
Security Best Practice	■ Maintain fosexec in a disabled state.
FOS Administration Guide	■ Review the following section: FOS `fosexec`.

3.2 Accounts and Authentication

Brocade Fabric OS can accommodate a variety of methods for user account management. FOS, by default, has two enabled generic user accounts: admin and user. External authentication servers (AAA) or the FOS internal user database can be used for authentication. Every user that logs into a Brocade platform should have their own account, as this generates meaningful audits and enforces access management. Every user account has a designated role, which assigns privileges and restricts an account to the user's function. FOS RBAC is used to define roles, and FOS has various existing roles pre-configured.

3.2.1 Digital Certificates

Per the CAB forum, public TLS certificates will no longer have an Organization Unit (OU). OU is ignored in requests and there is no longer a prompt for OU during CSR generation. OU is not included in self-signed, new, renewed, and reissued public TLS certificates. There are no hard-coded values for OU. The unit-name leaf has been deprecated from REST configuration. A warning message occurs when importing a certificate with an OU field.

Reference	Action
Security Best Practice	■ When a TLS certificate needs to be reissued (self-signed, enterprise, or public CA), do not submit the OU.
FOS Administration Guide	■ Review the following section: FOS SecCryptoCfg.

3.2.2 FOS SecCryptoCfg Templates

SecCryptoCfg templates use predefined standardized values for FOS platform cipher configurations. A template can be easily loaded onto a platform to meet specific security requirements.

FOS supports templates for TLS, SSH, and FIPS configurations. Templates consist of key-value pairs for configuring minimum encryption levels, key exchange methods, hash functions, application-specific ciphers, protocol versions, certificate validation mode, and FIPS-specific configurations.

A template can be specific to a certification's requirements or be based on the definition of security configurations for various security levels. For example, a high-security configuration template can enforce high-security strengths that are not FIPS-approved. You cannot overwrite the default templates, but you can customize templates and create new templates based on the default templates. FOS supports a maximum of eight templates, including the default templates.

The following default templates are provided. Refer to the FOS Admin Guide for detailed specifications for the templates.

- Default configuration (default_generic)
- Secured configuration (default_strong)
- FIPS configuration (default_fips)
- Common criteria configuration (default_cc)

Reference	Action
Security Best Practice	■ Apply the FOS default_strong crypto template. **NOTE:** This is default on platforms shipping with FOS v9.2.0 and later, as part of Default Secure settings
FOS Administration Guide	■ Review the following section: FOS SecCryptoCfg.

3.2.3 User Accounts

User account access can be validated locally within FOS or by an authentication server called authentication, authorization, and accounting (AAA). Brocade FOS audit functions provide no benefit unless every user has their own account. Further, if a user needs to be denied access, for example if the user has left the organization, the user's account can be easily managed without affecting other users.

A best practice is to use AAA authentication with groups for Brocade platform access and designating roles. RBAC defines roles with specific privileges based on assigned functional responsibility.

Command access is denied if the command is not listed in RBAC for the role. Based on the user's role, if the command is not approved for the user or listed in the RBAC database, then following error is displayed: RBAC permission denied.

Reference	Action
Security Best Practice	■ No sharing of user accounts. ■ Every user logging into a Brocade platform must have their own account. ■ Every user account is assigned a role that appropriately fits their operational tasks.
FOS Administration Guide	■ Review the following section: FOS v9 Managing User Accounts. ■ Review the following section: FOS v9 `roleconfig`. ■ Review the following section: FOS v9 `userconfig`.

3.2.4 Authentication Servers

User accounts and associated roles can be centrally managed from an enterprise's AAA server. When an AAA server is configured on FOS, the Brocade platform's local authentication database is preempted; however, the local database can continue to be used as a backup if no AAA server responds. If the local Brocade FOS authentication database is used as a backup, it must be maintained and updated independently of the AAA servers.

NOTE: From FOS v9.2.1, federated authentication is supported for access to FOS. The federated IdP can apply multi-factor authentication prior to issuing an access token for the authorized user or application, such as SANnav, ASC-G, or a server executing scripts.

Every user that logs into a Brocade platform must have their own account; otherwise, auditing becomes useless and disabling a specific user's access becomes difficult. RBAC is equally important; evaluate the tasks performed by every user and assign the most appropriate role. Users should not have more access than is minimally required to perform their functions and assigned tasks. For example, Operations users do not need authorization to configure the Brocade platforms, whereas SAN administrators are authorized.

Table 3: Supported AAA Servers

Authentication Server Type	Ports
FOS Local Authentication	—
LDAPS (TLS)	TCP 636
LDAP (STARTTLS)	TCP 389
Global Catalog LDAPS (TLS)	TCP 3269
RADIUS (EAP-TLS)	UDP 1812 and 1813
TACACS+	TCP 49

User account creation and user management are managed on the AAA server, and on the Brocade platforms if the local database is used as a backup. FOS can map an existing AAA group to a role. Every type of server configures its users and group or role designations uniquely, which is not in this document's scope. Only one external AAA server type (LDAPS, RADIUS, or TACACS+) can be configured simultaneously. For redundancy, up to five authentication servers of the same type can be configured.

Brocade FOS has no secure communication protocol with TACACS+.

Reference	Action
Security Best Practice	■ Secure AAA communications, for example by using TLS. ■ Configure multiple AAA servers for redundancy. ■ Maintain key administrator accounts on the Brocade platforms for backup. ■ Every user logging into a Brocade platform must use their own account. ■ RBAC roles and AAA groups are narrowly defined based on user function and assigned tasks.
FOS Administration Guide	■ Review the following section: FOS Appendix A: Setting Up the AAA Server Configuration. ■ Review the following section: FOS `ldapcfg`. ■ Review the following section: FOS `aaaconfig`. ■ Review the following section: FOS `roleconfig`. ■ Review the following section: FOS `userconfig`.

3.2.5 The Root Account

Every user allowed to log in is an additional security weakness. By disabling root, one weakness is removed. When you disallow root to log in, the perpetrator must first guess the username and then the associated password.

For example, a list of plausible passwords has N entries, and a list of plausible usernames has M entries. The perpetrator has N*M entries to test, which is more difficult than already knowing the username root and trying a significantly reduced set of possibilities.

Another reason to disallow root is that root can undoubtedly do more damage to FOS than admin can, although admin privileges are sufficient to disrupt critical SAN operations.

Reference	Action
Security Best Practice	■ Upgrade to FOS v9.1.1 or later. ■ In FOS v9.1.1 and later, there is no longer an accessible root account. ■ In FOS versions with a root account, root is disabled by default. ■ In FOS versions with a root account, root access via CLI is disabled by default. Access is available via serial connection only. ■ If the root account exists, enable the account, change the default password, and disable the account again. ■ Contact your support organization for more information concerning securing root.

3.2.6 FOS Passwords

Every FOS user account is required to have a password. Preexisting accounts such as admin and user require that their default password be changed upon the first login. A best security practice is not to use preexisting FOS user accounts. Every user should have their own account for auditing and managing individual access.

Brocade products have comprehensive password policy settings. Modify the password policy to correspond with your organization's security policies, including the maximum number of invalid login attempts before being locked out.

From FOS v9.2.2, as part of Default Secure the password policy is set to require complex passwords.

3.2.6.1 Default Passwords

As of FOS v9.x and later, default passwords must be changed upon first login. Default passwords are well-known and easily referenced in public documentation. The default passwords must be changed to provide security and reduce the chances of a breach. Log into all accounts at least once and change the default passwords, even if the accounts will not be used.

For FOS versions prior to 9.x, there is no enforcement of changing default passwords; however, it is strongly recommended that all default passwords be changed, even if the accounts associated with the default passwords will not be used.

Reference	Action
Security Best Practice	■ Change the default passwords, even if the accounts associated with the default passwords will not be used. ■ Enable the account, change the password, and disable the account again.
FOS Administration Guide	■ Review the following section: FOS `userconfig`. ■ Review the following section: FOS `passwd`.

3.2.6.2 Password Policy

The password policy enforces password creation to conform to specific rules. Ensure replacement passwords adhere to your organization's security policy. The password policy can be modified to require a minimum length; the inclusion of uppercase, lowercase, numeric, and special characters; minimization of repeat and sequential characters; and monitoring password history to prevent all or parts of previous passwords.

Reference	Action
Security Best Practice	■ Modify the FOS password policy to be congruent with your organization's minimum password requirements. **NOTE:** ● For the FOS password policy to be effective, the policy must be modified before creating user passwords. ● From FOS v9.2.0, the Default Secure policy includes a more restrictive password policy. ● From FOS v9.2.2, the Default Secure policy includes a complex password policy.
FOS Administration Guide	■ Review the following section: FOS Password Strength Policy. ■ Review the following section: FOS `passwdcfg`.

3.2.6.3 Account Lockout Threshold

The lockout threshold is the number of permitted invalid password entries for a user before the user's account is locked. Set account lockout thresholds in accordance with your company's policy. Ideally, users should be able to mistype their password a few times without running into accidental account lockouts.

If the lockout value is set too low, in theory, an attacker could quickly lock many accounts leading to a Denial of Service (DoS).

Account lockout is enabled by default and the lockout threshold is set to 3. Admin lockout console access is enabled by default. Only another admin can unlock a locked-out admin account; therefore, there must be more than one account with the admin role in the event that an admin account becomes locked. Do not set account lockout until after creating more than one account with the admin role.

Reference	Action
Security Best Practice	■ Set the account lockout threshold to 5 attempts.
FOS Administration Guide	■ Review the following section: FOS Account Lockout Policy. ■ Review the following section: FOS `passwdcfg`.

3.2.6.4 Passwordless Credentials

Passwordless credentials for accessing FOS SSH can be achieved by importing a public key from a client and associating that key to a specific user. `sshutil` is used to generate a public key and export it to the client. The client and Brocade platforms have each other's public keys; the user can access the platforms without the client having to prompt for credentials.

Reference	Action
Security Best Practice	■ Passwordless credentials offer a greater level of security than username and password. ■ Logging into Brocade platforms is simplified without needing a username and password. ■ Access is restricted to known hosts that have the valid keys installed.
FOS Administration Guide	■ Review the following section: FOS SSH Public Key Authentication. ■ Review the following section: FOS `sshutil`

3.2.6.5 Password Recovery

Password recovery requires serial console access on Brocade platforms. Brocade Gen6 and Gen7 platforms have Secure-Boot enabled, which means there is no access to the Boot PROM or a Boot PROM recovery password. From FOS v9.1.x onwards, `sboot fospasswdreset` can be used for password recovery via console connection.

Reference	Action
Security Best Practice	■ Upgrade to FOS v9.1.x or later. ■ Secure physical access to the platform and its serial port. ■ No configuration tasks are needed on Gen6 and Gen7 platforms that have Secure-Boot enabled.
FOS Administration Guide	■ Review the following section: FOS sboot.

Contact your support organization for information and guidance in performing a password recovery.

3.2.7 CyberArk PSM

FOS v9.2 supports and integrates with CyberArk Privileged Session Manager (PSM) for outgoing connections, session management, and outbound access to Supportsave, License, Firmwaredownload, Firmwarecleaninstall, Configdownload, Configupload, Seccertmgmt, SecCryptoCfg.

3.3 FOS Access by Applications

Not all access to a FOS platform is through a user. Various applications, such as SANnav, SNMP, Web Tools, and Automation often access FOS. The section below describes the most common applications and recommends security actions.

3.3.1 REST API

Secure a communication channel with TLS:

1. The client authenticates the switch via an x.509 certificate. Although Brocade supports self-signed certificates, the best authentication security comes from pre-loading the CA certificate and associated leaf certificates. The client authenticates the switch by first using the root certificate to validate the switch certificate and then performing a challenge-response exchange. Most large enterprises operate their own CA and have their own root and intermediate certificates. Brocade FOS supports public CAs as well.

2. The switch authenticates the client by using credentials that the client sends in the encrypted tunnel after the session establishment. The password is base64-encoded to allow for unusual characters. The user name is cleartext; the user name and base64-encoded password are secure because of the encrypted tunnel.
3. Once the switch has authenticated the client and the client has authenticated the switch, the switch sends an API token that remains active until either the client logs out or the session times out. This API token is included in the header of all client API calls until the session context is terminated. The client's responsibility is to keep the token secure The token is only sent once by the switch. It can't be recovered if the client loses it, so the client has to re-establish another logical session.

This process looks like the regular security for a CLI SSH session; with the exception of the token and URI interface, it is the same. REST's nature is session-less, and the use of a token establishes client flow context. Multiple clients with the same credentials can have simultaneous non-interfering sessions in progress, the same as having various CLI SSH sessions from the same user.

Reference	Action
Security Best Practice	■ Automation and other applications accessing Brocade FOS via REST should use HTTPS. ■ HTTPS certificates can be self-signed or CA signed. ■ Disable HTTP.
FOS Administration Guide	■ Review the following section: FOS v9 REST API. ■ Review the following section: FOS Yang. ■ Review the following section: FOS Secure Sockets Layer Protocol. ■ Review the following section: FOS `mgmtapp`. ■ Review the following section: FOS `seccertmgmt`.

3.3.2 Web Tools

Web Tools can be accessed using HTTP or HTTPS. HTTP is not secure because the username, password, and all data transmission are sent in the clear. From the perspective of SAN operations, a number of untrusted knowledgeable users may have access to the data center management network; therefore, usernames and passwords can be compromised.

HTTP transmissions are vulnerable to masquerade, eavesdropping, replay, and man-in-the-middle attacks. HTTP exposes platforms to breach, potentially resulting in critical systems losing access to volumes, going offline, and data loss. A best practice is to allow only secure protocols for switch access. HTTP is not a secure protocol and should be disabled; use HTTPS instead. Complete a review and confirm that HTTPS keepalive and authmode are enabled.

NOTE: By default, FOS ships with HTTPS self-signed certificates for boot strapping. Use CA or Enterprise certificates.

HTTPS uses TLS, which is a certificate-based protocol. Certificates enable strong identity verification and data privacy (encryption). Certificates come from three entities: self-signed, Enterprise CA, and Public CA. Brocade FOS can create self-signed certificates for HTTPS. Self-signed certificates have a couple of caveats:

1. Self-signed certificates cannot be revoked, which might allow an attacker to spoof an identity after a private key is compromised. CAs can revoke a compromised certificate, which prevents further use. CA-signed certificates are, therefore, safer to use in production environments.
2. Brocade self-signed certificates expire in 2 years. In a production environment, self-signed certificates are open to eventual security breaches, compounded by the fact that self-signed certificates cannot be revoked.

A self-signed certificate is both a personal certificate and a root CA certificate. A user with a self-signed personal certificate might be able to use it to sign other personal certificates. In general, this is not true of personal certificates issued by a CA and represents significant exposure.

Some enterprises have their own Public Key Infrastructure (PKI) and can create signed certificates, referred to as an Enterprise CA. Trusted Public Certificate Authorities (CA) sign certificates. Enterprise and Public certificates can be revoked and have expiration dates. When changing to a new CA or when using self-signed certificates, the certificates must be deleted and regenerated on every Brocade platform to invalidate the prior certificates.

Reference	Action
Security Best Practice	■ Self-signed certificates are intended for boot-strapping deployment of platforms, Replace the self-signed certificates with CA or Enterprise certificates. ■ If HTTPS is not already enabled, enable it by adding the appropriate certificates. ■ Use Web Tools with HTTPS. ■ Disable HTTP.
FOS Administration Guide	■ Review the following section: FOS Secure Sockets Layer Protocol. ■ Review the following section: FOS `seccertmgmt`.

NOTE: From FOS v9.2.2, federated authentication is supported with Web Tools.

3.3.3 SANnav Access to FOS

SANnav communicates with Brocade SAN platforms to perform a variety of operational functions, and several protocols are used. Some protocols require TLS to be set up by adding the appropriate certificates, for example: Secure Syslog, Secure Kafka, Secure LDAP, and Secure SMTP. SANnav requires TLS-protected Secure Kafka communication with Brocade platforms.

Reference	Action
Security Best Practice	■ Use secure protocols such as SSH, HTTPS, SCP, SFTP, SNMPv3, Secure Syslog, Secure Kafka, Secure LDAP, and Secure SMTP, between SANnav and FOS.
SANnav Management Portal User Guide	■ Review the following section: Security.

NOTE: From SANnav v3.2.2, federated authentication is supported for access to FOS. FOS v9.2.1 and later supports federated authentication.

3.3.4 Brocade Support Link and Active Support Connectivity Gateway

Brocade Support Link (BSL) and Active Support Connectivity Gateway (ASC-G) are advanced support mechanisms for expediting the data collection process to open and quickly resolve support cases. BSL provides security assessments and best practice configuration validation.

In smaller environments, BSL can communicate directly with Broadcom support services. In larger environments, Brocade platforms communicate with ASC-G and ASC-G communicates with Broadcom support services. While customer FC data has no pathway from the FC ports to the platform management port, it is still essential that all BSL and ASC-G communications are secure; therefore safe certificate-based communications, such as SSH, HTTPS, SNMPv3, SCP, SFTP, Secure LDAP, and Secure Syslog, are used.

ASC-G does not support telnet or HTTP in any way. Unsecure protocols send confidential information in the clear, which can easily be recorded by devices on the management network. These unsecure protocols could be exploited, resulting in the compromise of SAN platforms or ASC-G. A compromised SAN could result in data loss and a disruptive unplanned outage of critical operations.

NOTE: By default, FOS ships with HTTPS self-signed certificates already installed.

Reference	Action
Security Best Practice	■ Do not send confidential data in the clear. ■ Implement secure protocols (SSH, HTTPS, SNMPv3, SCP, SFTP, Secure LDAP, and Secure Syslog) between FOS, ASC-G, and the external Broadcom support servers.
FOS Administration Guide	■ Review the following section: FOS command `supportlink`. ■ Review the following section: FOS `seccertmgmt`. ■ Review the following section: FOS `sshutil`. ■ Review the following section: FOS `ldapcfg`. ■ Review the following section: FOS `snmpconfig`.

NOTE: From ASC-G v3.1.0, federated authentication is supported for access to FOS. FOS v9.2.1 and later supports federated authentication.

3.3.5 SNMP

SNMPv1 is not a secure protocol, it sends data in the clear and there is no authentication. By default, FOS has SNMPv1 disabled and it should remain disabled.

SNMPv3 can be configured to use no authentication and no privacy; however, this is not the recommended configuration. SNMPv3 should be configured to use authentication (SHA or MD5) and encryption (DES or AES). Authentication and encryption settings may be limited by the matching capabilities on the Brocade platforms and SNMP servers. By default FOS has SNMPv3 enabled, but not configured.

Reference	Action
Security Best Practice	■ Disable SNMPv1. ■ Use SNMPv3 with the strongest algorithms available on the platform, for example, authentication (SHA512) and encryption (AES256), if possible.
FOS Administration Guide	■ Review the following section: FOS Simple Network Management Protocol. ■ Review the following section: FOS `snmpconfig`.

3.3.6 SMTP

Email (SMTP) is a Monitoring Alerting Policy Suite (MAPS) action. When a MAPS rule is triggered and its action includes email, an email is generated and forwarded to the server designated by the `relayconfig` command. There are no security options for MAPS emails. The email is communicated from the Brocade platform to the IP address designated in the `relayconfig` command.

Reference	Action
Security Best Practice	■ No action required.
FOS Administration Guide	■ Review the following section: FOS `mapsconfig`. ■ Review the following section: FOS `relayconfig`.

3.3.7 Syslog

If Syslog servers do not perform authentication of received messages, attackers can leveraged them to perform cyber attacks:

- Create a DoS (denial-of-service condition) by sending large amounts of data to the syslog service, which can consume all the file system space.
- Once the disk is full, logs can no longer be saved; any attack that would leave a trail within the logs would go unnoticed.
- Sending large amounts of specially crafted messages, an attacker can cause chaos if logs are monitored by intrusion detection systems or other systems that create alerts.

Brocade FOS syslog can use TLS (TCP port 6514) as its transport, which leverages authentication and encryption. TLS uses certificates that are self-signed, Enterprise CA-signed, or Public CA-signed. Secure syslog messages are only accepted from known entities and confidential information is encrypted across the management network.

Reference	Action
Security Best Practice	■ Implement secure syslog using certificates.
FOS Administration Guide	■ Review the following section: FOS Configuring Remote Syslog Servers. ■ Review the following section: FOS `syslogadmin`. ■ Review the following section: FOS `seccertmgmt`.

3.3.8 NTP

Brocade FOS NTP implements symmetric authentication to secure NTP from unauthorized servers. A typical NTP attack is an amplification attack or a reflection attack resulting in Denial of Service (DoS). The attacker exploits unsecured NTP servers by sending forged requests spoofed as the victim, and the replies overwhelm the victim with UDP traffic. By implementing secret keys for authentication, a third party cannot submit NTP requests on behalf of a potential victim. The most secure keys to prevent hijacking NTP use the HMAC-SHA256.

Brocade FOS NTP implements Restrictive Time Adjustment (RTA); time beyond ±7 days cannot be changed.

Reference	Action
Security Best Practice	■ Configure NTP symmetric authentication on the FOS platforms (NTP clients) and the enterprise NTP server.
FOS Administration Guide	■ Review the following section: FOS `tsclockserver`. ■ Review the following section: FOS `tstimezone`.

Chapter 4: Fabric Security

FOS offers fabric security features for restricting connectivity to authorized devices, device authentication, ISL encryption, limiting configuration from specific platforms, and default zoning requirements.

4.1 FOS Security Policies

FOS has various security policies to protect the integrity of the fabric, authenticate users, and protect IP access to the management port. Policies are stored in a local FOS database. The database contains the policies for FCS, DCC, SCC, passwords, authentication, and IPfilter. Policies can be in one of two states: active or defined. A policy can be defined but not activated. Passwords and IPfilter are databases at the chassis scope. Every Virtual Fabrics Logical Switch (VF-LS) has its own set of defined and active policies for FCS, DCC, SCC, and authentication.

In the following sections, references are provided to the related CLI commands and documentation in the *Brocade Fabric OS Administration Guide*.

In addition, security policies can be configured using REST and SANnav. A subset of security configurations can also be performed with Web Tools. Consult the respective guides for more details.

- REST, refer to the *Brocade FOS REST API Reference Manual.*
- Web Tools, refer to the *Brocade FOS Web Tools User Guide.*
- SANnav, refer to the *SANnav Management Portal User Guide.*

4.1.1 Fabric Configuration Server

Fabric Configuration Server (FCS) controls fabric-wide management operations. One or more switches can act as the trusted switches in charge of zoning changes and other security-related operations. These trusted switches are identified by their WWNs. Physical and remote access to FCS switches should be restricted. FOS permits the FCS policy definition to define a list of FCS switches. Once enabled, only the primary switch can propagate fabric-wide management changes. An FCS policy does not exist by default.

There are several FCS-exclusive activities:

- Zone, alias, and cfg changes
- Security policy (DCC, SCC, FCS) changes
- Password policy changes
- Distribute command

Reference	Action
Security Best Practice	■ Create a FCS policy on the switch you desire to be the primary FCS platform. ■ Add a second, and perhaps a third, Brocade platform as FCS backups for redundancy. ■ Activate and distribute the FCS policy fabric-wide for consistency.
FOS Administration Guide	■ Review the following section: FOS Configuring Security Policies. ■ Review the following section: FOS `secpolicycreate`. ■ Review the following section: FOS `secpolicyadd`. ■ Review the following section: FOS `secpolicysave`.

4.1.2 Switch Connection Control

The integrity of a fabric can be compromised if a malicious unauthorized switch were to join, or if an accidental merging of production fabrics were to occur by way of cross-connecting cables. Either of these instanced could cause a critical, unexpected outage. Use Switch Connection Control (SCC) to enhance security.

SCC authorizes known switches to join the fabric. An SCC policy is not created or updated automatically. Before the fabrics can merge, the new switch chassis WWN must be manually added to the SCC policy and activated.

SCC is frequently required in mainframe environments and is useful in merging SAN islands.

A mutual authentication process between switches is initiated when the following criteria are met:

- There is an active SCC policy.
- An E_Port to E_Port connection is made.
- The fabric is initialized or reinitialized.

The authentication process uses the Switch Link Authentication Protocol (SLAP) to authenticate every switch attempting to join the fabric. When a new switch is connected to a secure fabric, the two switches must be mutually authenticated. The new switch must be on the existing authorized list before it is allowed to join the fabric.

SCC occurs at the following levels:

- Before FCAP will permit a switch to join the fabric, the Brocade platforms require certificates for FCAP, which are based on the identity of the switch.
- The SCC policy contains the switches permitted to join the fabric.

Reference	Action
Security Best Practice	■ Create a SCC policy. ■ Add the wwn to the policy. ■ Activate the SCC policy.
FOS Administration Guide	■ Review the following section: FOS Configuring Security Policies. ■ Review the following section: FOS `secpolicycreate`. ■ Review the following section: FOS `secpolicyadd`. ■ Review the following section: FOS `secpolicyactivate`. ■ Review the following section: FOS `secpolicysave`.

4.1.3 Device Connection Control

Device Connection Control (DCC) controls the end devices that can connect to specific F_Ports (fabric ports). DCC minimizes the risk of an unauthorized device being attached to the fabric by thwarting unauthorized access. DCC allows an N_Port (end device port) to be bound to one or more F_Ports. DCC policies allow for the specification of binding rules for a device's ports to a specific domain's F_Ports.

If DCC policies are in effect, one or more DCC policies are active. When a device performs a FLOGI, the specified pWWN is validated to ensure an authorized device is logged in to an F_Port. If validation fails, the FLOGI is rejected and the port is denied access to the fabric. A pWWN specified in a DCC policy only gains fabric access if connected to the specified F_Port.

Port WWNs not specified in an active DCC policy are permitted to connect to the fabric on F_Ports not defined in an active DCC policy. F_Ports and pWWNs may exist in multiple DCC policies.

Reference	Action
Security Best Practice	■ Create a DCC policy and add all F_Ports to the policy. ■ Associate an end-device port by means of pWWN/number to specific F_Ports in the policy. ■ Save, activate, and distribute the policy fabric-wide.
FOS Administration Guide	■ Review the following section: FOS Configuring Security Policies. ■ Review the following section: FOS `secpolicycreate`. ■ Review the following section: FOS `secpolicyadd`. ■ Review the following section: FOS `secpolicyactivate`. ■ Review the following section: FOS `secpolicysave`.

4.1.4 FOS fddcfg and distribute Commands

It is an important part of security to maintain consistent configurations across the fabric. FOS can distribute security databases fabric-wide for consistency. Every platform can be configured to accept or reject a particular database that is distributed fabric-wide. Some databases are automatically distributed and some require manual distribution. For consistency, every database listed below should be strictly distributed fabric-wide.

`fddcfg` distributes the following security policy databases:

- FCS Policy
- SCC Policy
- DCC Policy
- Password Policy
- Fabric Authentication Policy
- IPfilter Policy

Reference	Action
Security Best Practice	■ Use the primary FCS to update and maintain the security databases. ■ Every database should be strictly distributed. ■ Distribute every security database fabric-wide for consistency.
FOS Administration Guide	■ Review the following section: FOS Policy Database Distribution. ■ Review the following section: FOS Distributing the Local User Database.

4.2 ISL Encryption

The Brocade FOS ISL Encryption (AES-256) feature allows FC frames to be encrypted at the egress and decrypted at the ingress. When delivered to an end device, frames are already decrypted. The encryption is port-based, and in-flight encryption can be enabled for E_Ports and EX_Ports on a per-port basis. By default, encryption is disabled for all ports. There are port ranges that allow encryption depending on the switch type; not all ports can perform encryption.

Encryption is often enabled in susceptible environments and across long-distance ISLs. Any time data leaves the secure confines of a data center, the data should be encrypted.

Reference	Action
Security Best Practice	■ When data leaves the confines of a secure data center, such as long-distance ISLs over DWDM, configure ISL encryption. ■ In environments with sensitive data, configure ISL encryption within the data center between Brocade platforms.
FOS Administration Guide	■ Review the following section: FOS ISL Encryption. ■ Review the following section: FOS `portcfgencrypt`.

4.3 Default FC Port Configuration

By leaving SAN ports in an enabled state, a serious security vulnerability exists. A FC-based device or another switch can be connected to the exposed port, thereby, giving access to the SAN. This can, in severe cases, result in data loss, data modification, data breach, or critical outage.

Disable unused ports and enable them only before connecting a device or ISL. Additionally, disallow E_Port mode on all ports other than those used for ISLs.

Reference	Action
Security Best Practice	■ Disable all unused FC ports. ■ Disable E_Port capability on all ports except those that will be used as E_Ports, even if the ports are disabled.
FOS Administration Guide	■ Review the following section: FOS `portcfgpersistentdisable`. ■ Review the following section: FOS `portcfgpersistentenable`. ■ Review the following section: FOS `portcfgeport`.

4.4 Default Zoning

Default zoning is used when a device port is connected to the fabric and no zone exists for the port or the pWWN. The default zone mode applies to the entire fabric. There are two options:

- All Access: All devices within the fabric can communicate with all other devices. All Access is not secure because it allows a device plugged into the fabric to access any other device.
- No Access: Devices in the fabric cannot access any other device in the fabric. No Access is the default configuration and prevents a rogue device plugged into the fabric to access any other device without explicitly being configured to do so through zoning.

All devices in a fabric should belong to a zone, typically single initiator-single target zones.

Reference	Action
Security Best Practice	■ Set the default zone to noaccess.
FOS Administration Guide	■ Review the following section: FOS `defzone`.

4.5 Repository for Brocade FOS Related Files

File repository refers to the storage of Brocade platform-related files that are external to the FOS platforms. There are four types of files of concern:

- SupportSaves
- ConfigUploads
- FOS Firmware
- FOS Licenses

When these files are uploaded, whatever device and operating system they are uploaded to must be restricted to authorized administrators and authenticate those users. Access, creation, changes, and deletion of files and directories should be audited. The location for protecting such files often uses the same LDAP authentication as users use to access the Brocade platforms.

Often, files are loaded onto a USB drive for transport to or from Brocade platforms. A USB drive requires a heightened level of care to prevent the files from being compromised. The files should be transferred to a secure repository and the USB erased using a non-data-recoverable formatting technique.

Brocade, in good faith, attempts to scrub passwords from ConfigUploads and SupportSaves; however, it is prudent to maintain restricted access to such files. SupportSaves and ConfigUploads have other information that could be useful in a targeted attack, for example, management and Extension IP addresses.

FOS firmware could potentially be altered, which could result in a data breach, opening a vulnerability, or a critical operations disruption. Altered firmware is allowed to boot; a message is entered into the fos_bootup_log indicating the failed validation.

If you suspect that the FOS firmware may have been altered, use the FOS command `firmwarecheck` to verify the checksum of the currently loaded FOS on the platform.

Reference	Action
Security Best Practice	■ Maintain externally stored Brocade platform-related files in a restricted, secure, audited location ■ Using SANnav Management Portal, SupportSaves can be stored with file password protection.
FOS Administration Guide	■ Refer to your organization's security protocols for storing and accessing restricted and sensitive data.

4.6 Authentication Policy for Fabric Elements

Brocade FOS supports Fibre Channel Authentication Protocols (FCAP) and Diffie-Hellman Challenge Handshake Authentication Protocols (DH-CHAP) for authentication on E_Ports and F_Ports. Authentication protocols provide additional security during link initialization by assuring that only the desired device connects to a given port. These protocols use shared secrets and digital certificates based on switch WWN and PKI technology. Upon a switch or port state change, authentication is initiated. A state change can be due to a switch reboot, switch or port disable and enable, or the activation of a policy.

Authentication is enforced based on the policy settings of every logical switch.

Reference	Action
Security Best Practice	■ In environments requiring authentication of attached Brocade platforms, hosts, or storage, use FCAP, DH-CHAP, or both for authentication.
FOS Administration Guide	■ Review the following section: FOS Authentication Policy for Fabric Elements. ■ Review the following section: FOS `authutil`. ■ Review the following section: FOS `secauthsecret`. ■ Review the following section: FOS `seccertmgmt`.

Chapter 5: Platform Decommissioning

In preparation for decommissioning of a Brocade switch platform, the end user can, after removing the switch from the fabric, use the switch decommission feature to remove all identifiable data and override the internal storage in the switch.In order to execute the decommission function, an authorization code must first be obtained by contacting Brocade Technical Support. Once decommissioning has been performed the switch will no longer be able to boot and is non-recoverable. For more information, refer to the *Brocade Fabric OS Administration Guide*.

Appendix A: Supported Brocade Platforms

The following hardware platforms are supported by Brocade Fabric OS 9.2.x:

- Brocade Gen 7 (64G) Fixed-Port Switches
  - Brocade G710 Switch
  - Brocade G720 Switch
  - Brocade G730 Switch
- Brocade Gen 7 (64G) Directors
  - Brocade X7-4 Director
  - Brocade X7-8 Director
- Brocade Gen 7 (64G) Extension
  - Brocade 7850 Extension Switch
- Brocade Gen 6 (32G) Fixed-Port Switches
  - Brocade G610 Switch
  - Brocade G620 Switch
  - Brocade G630 Switch
  - Brocade G648 Blade Server SAN I/O Module
- Brocade Gen 6 (32G) Directors
  - Brocade X6-4 Director
  - Brocade X6-8 Director
- Brocade Gen 6 (32G) Extension
  - Brocade 7810 Extension Switch

Appendix B: Supported Cipher Suites

B.1 FOS v9.2.x Default Secure Ciphers

- OpenSSL 3.0.7
- TLSv1.3

Protocol	Cipher				
HTTPS CIPHER	ECDSA:	AES:	!DHEPSK:	!ARIAGCM:	!SSLv3:
	ECDH:	!3DES:	!PSK:	!CAMELLIA:	!TLSv1:
	RSA:	!RSAPSK:	!DSS:	!CHACHA20:	!AESCCM
HTTPS TLS1.3 CIPHER	TLS_AES_256_GCM_SHA384:		TLS_AES_128_CCM_8_SHA256:		
	TLS_AES_128_GCM_SHA256:		TLS_AES_128_CCM_SHA256		
HTTPS PROTOCOL	TLSv1.3				
RADIUS CIPHER	ECDSA:	AES:	!DHEPSK:	!ARIAGCM:	!SSLv3:
	ECDH:	!3DES:	!PSK:	!CAMELLIA:	!TLSv1:
	RSA:	!RSAPSK:	!DSS:	!CHACHA20:	!AESCCM
RADIUS PROTOCOL	TLSv1.2				
LDAP CIPHER	ECDSA:	AES:	!DHEPSK:	!ARIAGCM:	!SSLv3:
	ECDH:	!3DES:	!PSK:	!CAMELLIA:	!TLSv1:
	RSA:	!RSAPSK:	!DSS:	!CHACHA20:	!AESCCM
LDAP PROTOCOL	TLSv1.2				
SYSLOG CIPHER	ECDSA:	AES:	!DHEPSK:	!ARIAGCM:	!SSLv3:
	ECDH:	!3DES:	!PSK:	!CAMELLIA:	!TLSv1:
	RSA:	!RSAPSK:	!DSS:	!CHACHA20:	!AESCCM
SYSLOG PROTOCOL	TLSv1.2				
SSH CIPHER	AES128-CTR	AES192-CTR	AES256-CTR		
SSH KEX	ECDH-SHA2-NISTP256		DIFFIE-HELLMAN-GROUP16-SHA512		
	ECDH-SHA2-NISTP384		DIFFIE-HELLMAN-GROUP18-SHA512		
	ECDH-SHA2-NISTP521		DIFFIE-HELLMAN-GROUP-EXCHANGE-SHA256		
	DIFFIE-HELLMAN-GROUP14-SHA256		CURVE25519-SHA256		
SSH MAC	HMAC-SHA2-256		HMAC-SHA2-512		
X509 VALIDATION	Basic				

Table 4: Brocade Cipher Suites Supported in Fabric OS 9.2.x

Supported Ciphers		
TLS_AES_256_GCM_SHA384	ECDHE-ECDSA-AES256-SHA384	ECDHE-RSA-RC4-SHA
TLS_CHACHA20_POLY1305_SHA256	ECDHE-RSA-AES256-SHA384	ECDHE-ECDSA-DES-CBC3-SHA
TLS_AES_128_GCM_SHA256	DHE-RSA-AES256-SHA256	ECDHE-RSA-DES-CBC3-SHA
ECDHE-ECDSA-AES256-GCM-SHA384	DHE-DSS-AES256-SHA256	DHE-RSA-DES-CBC3-SHA
ECDHE-RSA-AES256-GCM-SHA384	ECDHE-ECDSA-CAMELLIA256-SHA384	DHE-DSS-DES-CBC3-SHA
DHE-DSS-AES256-GCM-SHA384	ECDHE-RSA-CAMELLIA256-SHA384	RSA-PSK-AES256-GCM-SHA384
DHE-RSA-AES256-GCM-SHA384	DHE-RSA-CAMELLIA256-SHA256	DHE-PSK-AES256-GCM-SHA384
ECDHE-ECDSA-CHACHA20-POLY1305	DHE-DSS-CAMELLIA256-SHA256	RSA-PSK-CHACHA20-POLY1305

Table 4: Brocade Cipher Suites Supported in Fabric OS 9.2.x

Supported Ciphers		
ECDHE-RSA-CHACHA20-POLY1305	ECDHE-ECDSA-AES128-SHA256	DHE-PSK-CHACHA20-POLY1305
DHE-RSA-CHACHA20-POLY1305	ECDHE-RSA-AES128-SHA256	ECDHE-PSK-CHACHA20-POLY1305
ECDHE-ECDSA-AES256-CCM8	DHE-RSA-AES128-SHA256	DHE-PSK-AES256-CCM8
ECDHE-ECDSA-AES256-CCM	DHE-DSS-AES128-SHA256	DHE-PSK-AES256-CCM
DHE-RSA-AES256-CCM8	ECDHE-ECDSA-CAMELLIA128-SHA256	RSA-PSK-ARIA256-GCM-SHA384
DHE-RSA-AES256-CCM	ECDHE-RSA-CAMELLIA128-SHA256	DHE-PSK-ARIA256-GCM-SHA384
ECDHE-ECDSA-ARIA256-GCM-SHA384	DHE-RSA-CAMELLIA128-SHA256	AES256-GCM-SHA384
ECDHE-ARIA256-GCM-SHA384	DHE-DSS-CAMELLIA128-SHA256	AES256-CCM8
DHE-DSS-ARIA256-GCM-SHA384	ECDHE-ECDSA-AES256-SHA	AES256-CCM
DHE-RSA-ARIA256-GCM-SHA384	ECDHE-RSA-AES256-SHA	ARIA256-GCM-SHA384
ECDHE-ECDSA-AES128-GCM-SHA256	DHE-RSA-AES256-SHA	PSK-AES256-GCM-SHA384
ECDHE-RSA-AES128-GCM-SHA256	DHE-DSS-AES256-SHA	PSK-CHACHA20-POLY1305
DHE-DSS-AES128-GCM-SHA256	DHE-RSA-CAMELLIA256-SHA	PSK-AES256-CCM8
DHE-RSA-AES128-GCM-SHA256	DHE-DSS-CAMELLIA256-SHA	PSK-AES256-CCM
ECDHE-ECDSA-AES128-CCM8	ECDHE-ECDSA-AES128-SHA	PSK-ARIA256-GCM-SHA384
ECDHE-ECDSA-AES128-CCM	ECDHE-RSA-AES128-SHA	RSA-PSK-AES128-GCM-SHA256
DHE-RSA-AES128-CCM8	DHE-RSA-AES128-SHA	DHE-PSK-AES128-GCM-SHA256
DHE-RSA-AES128-CCM	DHE-DSS-AES128-SHA	DHE-PSK-AES128-CCM8
ECDHE-ECDSA-ARIA128-GCM-SHA256	DHE-RSA-SEED-SHA	DHE-PSK-AES128-CCM
ECDHE-ARIA128-GCM-SHA256	DHE-DSS-SEED-SHA	RSA-PSK-ARIA128-GCM-SHA256
DHE-DSS-ARIA128-GCM-SHA256	DHE-RSA-CAMELLIA128-SHA	DHE-PSK-ARIA128-GCM-SHA256
DHE-RSA-ARIA128-GCM-SHA256	DHE-DSS-CAMELLIA128-SHA	AES128-GCM-SHA256
AES128-CCM	ECDHE-ECDSA-RC4-SHA	PSK-AES128-CBC-SHA256
ARIA128-GCM-SHA256	CAMELLIA256-SHA	PSK-AES128-CBC-SHA
PSK-AES128-GCM-SHA256	PSK-AES256-CBC-SHA384	PSK-CAMELLIA128-SHA256
PSK-AES128-CCM8	PSK-AES256-CBC-SHA	ECDHE-PSK-RC4-SHA
PSK-AES128-CCM	PSK-CAMELLIA256-SHA384	RSA-PSK-RC4-SHA
PSK-ARIA128-GCM-SHA256	ECDHE-PSK-AES128-CBC-SHA256	DHE-PSK-RC4-SHA
AES256-SHA256	ECDHE-PSK-AES128-CBC-SHA	RC4-SHA
CAMELLIA256-SHA256	RSA-PSK-AES128-CBC-SHA256	RC4-MD5
AES128-SHA256	DHE-PSK-AES128-CBC-SHA256	PSK-RC4-SHA
CAMELLIA128-SHA256	RSA-PSK-AES128-CBC-SHA	ECDHE-PSK-3DES-EDE-CBC-SHA
ECDHE-PSK-AES256-CBC-SHA384	DHE-PSK-AES128-CBC-SHA	RSA-PSK-3DES-EDE-CBC-SHA
ECDHE-PSK-AES256-CBC-SHA	ECDHE-PSK-CAMELLIA128-SHA256	DHE-PSK-3DES-EDE-CBC-SHA
RSA-PSK-AES256-CBC-SHA384	RSA-PSK-CAMELLIA128-SHA256	DES-CBC3-SHA
DHE-PSK-AES256-CBC-SHA384	DHE-PSK-CAMELLIA128-SHA256	PSK-3DES-EDE-CBC-SHA
RSA-PSK-AES256-CBC-SHA	AES128-SHA	RSA-PSK-CAMELLIA256-SHA384
DHE-PSK-AES256-CBC-SHA	SEED-SHA	AES256-SHA
ECDHE-PSK-CAMELLIA256-SHA384	CAMELLIA128-SHA	AES128-CCM8
DHE-PSK-CAMELLIA256-SHA384		

Table 5: KEX Suites Supported in Fabric OS 9.x

Fabric OS 9.0.x KEX
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521
diffie-hellman-group-exchange-sha256
diffie-hellman-group-exchange-sha1
diffie-hellman-group14-sha1
diffie-hellman-group1-sha1
curve25519-sha256
diffie-hellman-group16-sha512
diffie-hellman-group18-sha512
diffie-hellman-group14-sha256

Appendix C: FAQ

SSH MaxStartups must be set to "10:30:100" or less. (OpenSSH default setting)

– The MaxStartups default value is already supported in FOS and are not configurable.

SSH MaxSessions must be set to 10 or less. (OpenSSH default is 10)

– The MaxSessions default is already supported, but not configurable in FOS.

Authentication by password must be disabled for SSH.

– Password authentication is a supported mechanisms in FOS; customers can use passwordless login to avoid this. There is not a configuration option to disable username/password authentication. Username/password is industry standard.

SSH configuration files and private portions of SSH keying material must be protected with masking of 0600 (owner has full read and write access, while no other user can access the file) or more restrictive. Public keys must have a masking of 0644 or more restrictive.

– Permission of 0600 is already set for ssh files including: sshd_config, host private key, host public key, and known hosts.

If RSA keys are used, they must have a key size of 3072 bits

– FOS supports 2048, 4096, and 8192 key sizes.

The system must protect itself against access overload situations.

– With the max sessions count, MaxStartups and MaxSessions configuration, FOS is protecting itself against overload.

Packets with IPv4 options have to be ignored.

– This is not available in FOS today.

The maximum number of ICMPv4 and v6 response packets per second must be limited.

– This is not available in FOS today.

Privileged user accounts must be protected with two factor authentication from different factors, or better.

– FOS supports two factor authentication with RADIUS and Federated Authentication (from FOS v9.2.1), which can be used for privileged user accounts.

If passwords are used as an authentication feature, protection against online attacks such as dictionary and brute force attacks must be in place to make password guessing difficult.

– Supported. Existing configuration command `passwdcfg` options (check of repeat, capitals, seq, alphanum) can be used to protect against such attacks.

If passwords are used as an authentication feature, they must be stored using a password hashing method that is recognized as sufficiently secure, in order to make attacks such as dictionary and brute force attacks difficult.

– Brocade FOS supports strong password hashing. Passwords can be secured using the command `passwdcfg --hash`

SSH moduli smaller than 2048 must not be used. Diffie-Hellman groups with a module of 2048 bits may be used in stock configurations until the end of the year 2025. These stock configurations are to be replaced by methods based on elliptic curves.

– Brocade FOS supports moduli greater than 2048. The command `seccryptocfg` is used to configure DH groups 14(2048 bits), 16(4096 bits), 18(8192 bits), etc. FOS also supports ECDH algorithms such as ecdh-sha2-nistp256 and ecdh-sha2-nistp384.

Glossary

Acronym	Description
TLS	Transport Layer Security
API	application programing interface
BSL	Brocade Support Link
ASC-G	Active Support Connectivity Gateway
PKI	public-key infrastructure
LDAPS	Lightweight Directory Access Protocol Secure
CA	certificate authority
SAN	subject alternate name, storage area network
CSR	certificate signing request
CLI	command line interface
TELNET	Telnet terminal connection
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
FOS	Brocade's Fabric Operating System
FTP	File Transfer Protocol
RAR	Risk Assessment Report
SFTP	Secure File Transfer Protocol
SCP	Secure Copy Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
NTP	Network Time Protocol
REST	Representational State Transfer
AES256	Advanced Encryption Standard (256-bit)
SMTP	Simple Mail Transfer Protocol

Revision History

FOS-Security-UG101; October 15, 2024

- Updated with the release of FOS v9.2.2 and SANnav v2.3.2.

FOS-Security-UG100; August 15, 2023

- Initial release.