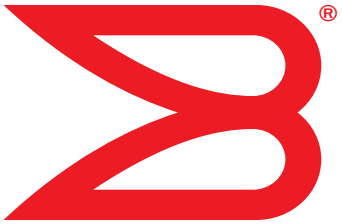
53-1003196-01
December 2014



Network OS

FIPS Configuration Guide

Supporting Network OS v4.1.1

BROCADE

Brocade Communications Systems, Incorporated

Corporate and Latin American Headquarters
Brocade Communications Systems, Inc.
130 Holger Way
San Jose, CA 95134
Tel: 1-408-333-8000
Fax: 1-408-333-8101
E-mail: info@brocade.com

European Headquarters
Brocade Communications Switzerland Sàrl
Centre Swissair
Tour B - 4ème étage
29, Route de l'Aéroport
Case Postale 105
CH-1215 Genève 15
Switzerland
Tel: +41 22 799 5640
Fax: +41 22 799 5641
E-mail: emea-info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems China HK, Ltd.
No. 1 Guanghua Road
Chao Yang District
Units 2718 and 2818
Beijing 100020, China
Tel: +8610 6588 8888
Fax: +8610 6588 9999
E-mail: china-info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems Co., Ltd. (Shenzhen WFOE)
Citic Plaza
No. 233 Tian He Road North
Unit 1308 – 13th Floor
Guangzhou, China
Tel: +8620 3891 2000
Fax +8620 3891 2111
E-mail: china-info@brocade.com

Document History

Title	Publication number	Summary of changes	Date
Network OS FIPS Configuration Guide	53-1003196-01	New document	December 2014

Contents

About This Document

In this chapter

How this document is organized

This document contains FIPS configuration and support information for Network OS version 4.1.1.

Supported hardware and software

This document includes information specific to Network OS v4.1.1. The following hardware platforms are supported in this release:

- Brocade VDX 6710-54
- Brocade VDX 6720
  - Brocade VDX 6720-24
  - Brocade VDX 6720-60
- Brocade VDX 6730
  - Brocade VDX 6730-32
  - Brocade VDX 6730-76
- Brocade VDX 6740, 6740T, and 6740T-1G
- Brocade VDX 8770
  - Brocade VDX 8770-4
  - Brocade VDX 8770-8

Although many different software and hardware configurations are tested and supported by Brocade Communications Systems, Inc. for Network OS v4.1.1, documenting all possible configurations and scenarios is beyond the scope of this document.

To obtain information about an OS version other than Network OS v4.1.1, refer to the documentation specific to that OS version.

What's new in this document

This is a new document.

Document conventions

This section describes text formatting conventions and important notice formats used in this document.

Text formatting

The narrative-text formatting conventions that are used are as follows:

bold text	Identifies command names Identifies the names of user-manipulated GUI elements Identifies keywords and operands Identifies text to enter at the GUI or CLI
italic text	Provides emphasis Identifies variables Identifies paths and Internet addresses Identifies document titles
code text	Identifies CLI output Identifies command syntax examples

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

Command syntax conventions

Command syntax in this manual follows these conventions:

command	Commands are printed in bold.
--**option, option**	Command options are printed in bold.
-**argument,** arg	Arguments.
[ ]	Optional element.
variable	Variables are printed in italics. In the help pages, values are underlined or enclosed in angled brackets < >.

...	Repeat the previous element, for example “member[;member...]”
value	Fixed values following arguments are printed in plain font. For example, **--show** WWN
|	Boolean. Elements are exclusive. Example: **--show -mode** egress | ingress

Notes, cautions, and warnings

The following notices and statements are used in this manual. They are listed below in order of increasing severity of potential hazards.

NOTE
A note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION
An Attention statement indicates potential damage to hardware or data.

CAUTION
A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER
A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Key terms

For definitions specific to Brocade and Fibre Channel, see the technical glossaries on MyBrocade. See “Brocade resources” on page viii for instructions on accessing MyBrocade.

For definitions of SAN-specific terms, visit the Storage Networking Industry Association online dictionary at:

http://www.snia.org/education/dictionary

Notice to the reader

This document may contain references to the trademarks of the following corporations. These trademarks are the properties of their respective companies and corporations.

These references are made for informational purposes only.

Corporation	Referenced Trademarks and Products
Microsoft Corporation	Windows, Windows NT, Internet Explorer
Oracle Corporation	Oracle, Java
Red Hat, Inc.	Red Hat, Red Hat Network, Maximum RPM, Linux Undercover
IBM	BladeCenter Advanced Management Module Protect Mode

Additional information

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

Brocade resources

To get up-to-the-minute information, go to *http://my.brocade.com* and register at no cost for a user ID and password.

White papers, online demonstrations, and data sheets are available through the Brocade website at:

http://www.brocade.com/products-solutions/products/index.page

For additional Brocade documentation, visit the Brocade website:

http://www.brocade.com

Release notes are available on the MyBrocade website and are also bundled with the Network OS firmware.

Other industry resources

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

http://www.t11.org

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

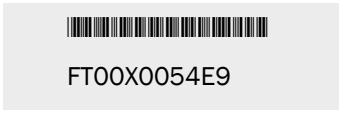
http://www.fibrechannel.org

Getting technical help

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

1. General Information
    - Switch model
    - Switch operating system version
    - Software name and software version, if applicable
    - Error numbers and messages received
    - **supportSave** command output
    - Detailed description of the problem, including the switch or fabric behavior immediately following the problem, and specific questions
    - Description of any troubleshooting steps already performed and the results
    - Serial console and Telnet session logs
    - syslog message logs
2. Switch Serial Number

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

    The serial number label is located as follows:

    - *Brocade VDX 6720*—On the switch ID pull-out tab located on the bottom of the port side of the switch
3. World Wide Name (WWN)

    Use the **show system** command to display the WWN of the chassis.

    If you cannot use the **show system** command because the switch is inoperable, you can get the WWN from the same place as the serial number, except for the Brocade DCX. For the Brocade DCX, access the numbers on the WWN cards by removing the Brocade logo plate at the top of the nonport side of the chassis.

Document feedback

Quality is our first concern at Brocade and we have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission, or you think that a topic needs further development, we want to hear from you. Forward your feedback to:

documentation@brocade.com

Provide the title and version number of the document and as much detail as possible about your comment, including the topic heading and page number and your suggestions for improvement.

Chapter

1

FIPS Support

In this chapter

FIPS overview

Federal Information Processing Standards (FIPS) specify the security standards to be satisfied by a cryptographic module utilized in Network OS v4.1.1 to protect sensitive information in the switch. As part of FIPS 140-2 level 2 compliance passwords, shared secrets, and the private keys used in SSL, TLS, and system login must be cleared out or *zeroized*.

Before enabling the FIPS-compliant state, a power-on self-test (POST) is executed when the switch is powered on to check for the consistency of the algorithms implemented in the switch. Known-answer tests (KATs) are used to exercise various features of the algorithm, and their results are displayed on the console for your reference. Conditional tests are performed whenever an RSA key pair is generated. These tests verify the randomness of the deterministic random number generator (DRNG) and nondeterministic random-number generator (non-DRNG). They also verify the consistency of RSA keys with regard to signing and verification and encryption and decryption. These conditional tests also verify that the downloaded firmware is signed.

ATTENTION
Once enabled, the FIPS-compliant state cannot be disabled.

FIPS compliance can be applied to switches in standalone and fabric cluster mode. To support FIPS compliance, the CA certificate of the Active Directory server's certificate should be installed on the switch, and FIPS-compliant TLS ciphers for Lightweight Directory Access Protocol (LDAP) should be used.

The Network OS v4.1.1 firmware is signed by means of both SHA1 1024-bit and SHA256 2048-bit keys. Firmware signatures are automatically validated during firmware download.

When upgrading or downgrading between Network OS v4.1.1 and a firmware version earlier than Network OS v4.1.1, firmware download uses the SHA256 and 2048-bit key for firmware signature validation.

Zeroization functions

Explicit zeroization can be done at the discretion of the security administrator. These functions clear the passwords and the shared secrets. Table 1 lists the various keys used in the system that will be zeroized in a FIPS-compliant Network OS switch.

TABLE 1 Zeroization behavior

Keys	Zeroization CLI	Description
FCSP CHAP secrets	fips zeroize	Automatically zeroized on session termination. All the SFTP sessions gets terminated on zeroization.
Passwords	fips zeroize	The **fips zeroize** command removes user-defined accounts in addition to default passwords for the root, factory, admin, and user default accounts. Only the admin role has permissions for this command which, in addition to removing user accounts and resetting passwords, performs the complete zeroization of the system, and reboots the switch.
RADIUS secret	**no radius-server host** *host*	The **radius-server host** *host* command configures the radius server. The **no radius-server host** *host* command zeroizes the secret and deletes a configured server.
RNG seed key	No command required	/dev/urandom is used as the initial source of seed for RNG. The RNG seed key is zeroized on every random number generation.
SFTP session keys	No command required	Automatically zeroized on session termination. All SFTP sessions are terminated on zeroization.
SSH DH private keys	No command required	Keys will be zeroized within code before they are released from memory.
SSH host keys	**fips zeroize***	Zeroized and deletes the existing host. A new RSA host key of size 2048 is generated.
SSH session key	No command required	This key is generated for each SSH session that is established with the host. It automatically zeroizes on session termination. All SSH sessions terminate on zeroization.
TLS authentication key	No command required	Automatically zeroized on session termination.
TLS pre-master secret	No command required	Automatically zeroized on session termination.
TLS private keys	**fips zeroize***	Only RSA keys of size 2048 are allowed.
TLS session key	No command required	Automatically zeroized on session termination.

*It is recommended that **fips zeroize** is executed with the administrator having physical control of the switch, rather than through remote connections.

Power-on self-tests

A power-on self-test (POST) is invoked by powering on the switch in the FIPS-compliant state. It does not require any operator intervention. If any KATs fail, the switch goes into a FIPS Error state, which reboots the system to start the test again. If the switch continues to fail the FIPS POST, you will need to return your switch to your switch service provider for repair.

Conditional tests

The conditional tests are for the random number generators and are executed to verify the randomness of the random number generators. The conditional tests are executed each time before using the random number provided by the random number generator.

The results of the POST and conditional tests are recorded in the system log or are displayed on the local console. This action includes logging both passing and failing results.

FIPS-compliant state configuration

By default, the switch comes up in the non-FIPS-compliant state. You can bring up the switch in the FIPS-compliant state by enabling the KATs and conditional tests and then rebooting the switch, but you must configure the switch first. The set of prerequisites shown in Table 2 must be satisfied for the system to enter the FIPS-compliant state.

To be FIPS compliant, the switch must be rebooted. KATs are run on the reboot. If the KATs are successful, the switch enters the FIPS-compliant state. If the KATs fail, then the switch reboots until the KATs succeed. If the switch cannot enter the FIPS-compliant state and continues to reboot, you must return the switch to your switch service provider.

When the switch successfully reboots in the FIPS-compliant state, you must follow the restrictions listed in Table 2 to be FIPS compliant. This table lists the Network OS features and their behaviors in the FIPS-compliant and non-FIPS-compliant states.

TABLE 2 FIPS-compliant state restrictions

Features	FIPS-compliant state	Non-FIPS-compliant state
autoupload of FFDC and trace support data	Not supported	Supported (FTP)
Configupload/ download/ supportsave/ firmwaredownload	SCP only	FTP and SCP
LDAP CA	CA certificate must be available. Cipher suites: AES256-SHA, AES128-SHA, DES-CBC3-SHA	CA certificate is optional.
Outbound SSH and telnet client	Not supported	Supported
RADIUS authentication protocols	PEAP-MSCHAPv2	CHAP, PAP, PEAP-MSCHAPv2
Root account	Disabled	Enabled
Signed firmware download	Mandatory firmware signature validation. Signed with 2048 key and SHA256.	Mandatory firmware signature validation. Signed with 1024/2048 key and SHA1/SHA256.
SSH algorithms	HMAC-SHA1 (MAC)	No restrictions
SSH public keys	RSA 2048 Bits Keys	RSA 1024/2048 bits Keys
TACACS+ authentication	Not supported	CHAP and PAP

TABLE 2 FIPS-compliant state restrictions (Continued)

Features	FIPS-compliant state	Non-FIPS-compliant state
Telnet/SSH access	Only SSH (RSA key size of 2048 and SHA 256 will only be allowed)	Telnet and SSH
vCenter	Not supported	Supported

NOTE
Although SNMP is not considered to be FIPS compliant, it is not blocked. SNMP is considered to have a plain text interface without any cryptographic content. The few write operations that are supported do not affect the security of the switch. OSPF is considered a plain text interface, and no protection is claimed for protocol data exchange.

Preparing the switch for FIPS

It is important to prepare the switch for the following restrictions that exist in the FIPS-compliant state:

- The root account and all root-only functions are not available.
- Access to the Boot PROM is not available.
- HTTP, HTTPS, Telnet, and SNMP must be disabled. Once these ports are blocked, you cannot use them to read or write data from and to the switch.
- For USB interfaces, an authorized operator is required to maintain the physical possession (at all times) of the USB token and shall not provide access to unauthorized individuals or entities.

See Table 2 on page 13 for a complete list of restrictions between the FIPS-compliant and non-FIPS-compliant states.

ATTENTION
You need the admin role permissions to prepare the switch for the FIPS-compliant state.

Preparing a switch for FIPS-compliant state operation removes all critical security parameters from the switch. As a consequence, some parameters needed to operate the switch must be applied after enabling the FIPS-compliant state, including the following parameters:

- IP ACL rules used to block HTTP, HTTPS, and Telnet access
- CA certificates used in LDAP authentication

These parameters must be reconfigured after each zeroization of the switch.

FIPS preparation overview

1. Disable Boot PROM access.
2. *Optional:* Configure an LDAP server for authentication and configure FIPS-compliant ciphers for LDAP.
3. *Optional:* Configure a RADIUS server for authentication and configure FIPS-compliant ciphers for RADIUS.
4. Configure FIPS-compliant ciphers and hash for SSH.

5. Disable root access.
6. Remove configurations of unsupported features vCenter and TACACS+, and disable Dot1x authentication.
7. If any FC-SP authentication policy attributes have been configured, configure all DH-group configuration to group 4.
8. Disable auto-upload.
9. Enable the KATs and the conditional tests.
10. Zeroize and reboot the switch into the FIPS-compliant state.
11. Disable the Telnet server.
12. Configure IP ACLS to block HTTP, HTTPS, and Telnet ports.
13. For authentication by a Microsoft Active Directory server, import and install the LDCAP CA certificate for LDAP authentication.

Enabling the FIPS-compliant state

1. Log in to the switch by using an account with the admin role.
2. To enable in standalone mode, enter the **no vcs enable** command in privileged EXEC mode.

   In VCS mode, use **vcs** *[rbridge-id rbridge-id] [vcsId ID] [enable ID]* command to configure the node.
3. Enter the **unhide** command to provide access to hidden commands. To execute this command, you must enter the password "**fibranne**".

   This step is necessary to gain access to the **prom-access**, **fips root disable**, **fips selftests**, and **fips zeroize** commands.

   ```
   switch# unhide fips
   Password: *****
   ```

CAUTION

Once access to the Boot PROM has been disabled, you cannot re-enable it.

4. Check the status of prom-access by executing these commands.

   ```
   switch# unhide built-in-self-test
   Password: ********
   switch#
   switch# show prom-access
   PROM access Disabled
   ```

   If prom-access is enabled, disable it by running following command, proceed to step 5.
5. Enter the **prom-access disable** command to disable access to the Boot PROM.

   ```
   switch# prom-access disable
   You are disabling PROM access. Do you want to continue? [yes/no] (no): yes
   PROM access Disabled
   ```
6. If LDAP will be used for authentication:

a. Configure FIPS-compliant LDAP ciphers (AES256-SHA, AES128-SHA, DES-CBC3-SHA):

```
switch# cipherset ldap
LDAP cipher list configured successfully.
```

b. Delete any LDAP DSA or RSA 1024 CA certificate that already exists on the switch:

```
switch# no certutil ldapca
Do you want to delete LDAP CA certificate? [y/n]:y
```

NOTE
In the FIPS-compliant state, only RSA 2048 CA certificates are supported. This command deletes all existing LDAP CA certificates on the switch.

For more details about configuring LDAP and the FIPS-compliant LDAP ciphers, refer to *"Setting up LDAP for the FIPS-compliant state"* on page 22.

7. If RADIUS will be used for authentication: Configure FIPS-compliant RADIUS ciphers (AES256-SHA, AES128-SHA, DES-CBC3-SHA):

```
switch# cipherset radius
RADIUS cipher list configured successfully.
```

8. Enter the **cipherset ssh** command to configure the FIPS-compliant ciphers for SSH (HMAC-SHA1 (mac), AES128-CBC, AES256-CBC).

```
switch# cipherset ssh
ssh cipher list configured successfully
switch# show cipherset
LDAP Cipher List    : !DH:HIGH:-MD5
SSH Cipher List     : aes128-cbc,aes256-cbc
```

9. Enter the **cipherset ssh sha256** command to configure ssh hash to SHA256.

   Once cipherset ssh sha256 is executed, connection to the switch will be accepted only from clients that support sha256 hash as part of RSA signature in OpenSSH. To allow other clients to connect, enter the "no cipherset ssh sha256" command to configure hash back to default(sha1).

```
switch# cipherset ssh sha256
```

NOTE
For Dual MM chassis, execute the above command both in Active and Standby MM's.

CAUTION
Once you have disabled root account access, you cannot re-enable it. To re-enable root account access, you must return your switch to your service provider.

10. Enter the **fips root disable** command and enter **yes** at the subsequent prompt to disable access from the root account.

```
switch# fips root disable
This operation disables root account. Do you want to continue? [yes,NO] yes

Network OS (switch)
switch console login: 2011/09/08-17:28:34, [SEC-1197], 19073,, INFO, switch,
Changed account root.
```

NOTE
The **fips root disable** command was exposed by the **unhide** command in step 3. It is normally a hidden command.

11. Enter the **show fips** command to confirm the status of fips.

```
switch# show fips
FIPS Selftests: Enabled
Root account: Disabled
```

12. Delete the TACACS+ configuration from the switch by using the following commands.

    a. Enter the **show running-config tacacs-server** command to list the existing TACACS+ configuration.

    b. For each TACACS+ server listed in step a, enter the **no tacacs-server host** command and the IP address or host name to delete the TACACS+ server configuration.

```
switch# show running-config tacacs-server host ?
Description: Configure a TACACS+ Server for AAA
Possible completions:
 10.20.57.13  INETADDRESS;;Domain name or IP Address of this TACACS+
server
 |       Output modifiers
 <cr>
Possible match completions:
 port    TCP Port for Authentication (default=49)
 protocol  Authentication protocol to be used (default=CHAP)
 key    Secret shared with this server (default='sharedsecret')
 retries  Number of retries for this server connection (default=5)
 timeout  Wait time for this server to respond (default=5 sec)
switch# configure terminal
Entering configuration mode terminal
switch(config)# no tacacs-server host 10.10.20.57.13
```

13. Enter the **no dot1x enable** command to disable 802.1x globally.

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# no dot1x enable
switch(config)# exit
```

14. If vCenter is configured, remove the configuration using the following CLI:

```
switch(config)# no vcenter <name>
```

15. DH group 0-3 is not supported in the fips compliance state of the switch. If DH group 0-3 or '*' is configured, execute the following to configure dh group to 4 (key size 2048 bits).

```
switch(config)# fcsp auth group 4
```

16. Configure DH policy to ACTIVE/ON to make sure DH-CHAP authentication will be initiated on E-Ex port formation by executing the following CLI:

```
switch(config)#fcsp auth policy switch <on/active>
```

17. Configure hash as SHA1 by executing the following CLI.

```
switch(config)#fcsp auth hash sha1
```

18. If autoupload is enabled, disable it.

```
switch# autoupload disable
```

CAUTION

Once FIPS self-tests are enabled, you cannot disable them. These tests will run on the next reboot and, if successful, will place the switch into the FIPS-compliant state.

19. Enter the **fips selftests** command to enable the FIPS KAT and conditional tests.

    To ensure FIPS-compliance, the Kex algorithm diffie-hellman-group-exchange-sha256 is enforced once the **fips selftests** command is run.

    Clients that support diffie-hellman-group-exchange-sha256 are only able to connect to the switch and switch can upload config and support files only to servers that support diffie-hellman-group-exchange-sha256.

```
switch# fips selftests
self tests enabled
```

NOTE

The **fips selftests** command was exposed by the **unhide** command in step 3. It is normally a hidden command.

20. Enter the **fips zeroize** command and enter **yes** at the subsequent prompt to clear all passwords and secrets.

    The switch reboots and comes up in the FIPS-compliant state.

```
switch# fips zeroize
This operation erases all passwords, shared secrets, private keys etc. on the
switch . Do you want to continue? [yes,NO] yes
```

NOTE

The **fips zeroize** command was exposed by the **unhide** command in step 3. It is normally a hidden command. When the switch reboots, the FIPS commands will be hidden again. Zeroization should only be performed by a local operator that has physical control of the cryptographic module, with all network connections physically disconnected

On reboot, the switch performs the KATs and conditional tests enabled in step 19. The following sample output indicates successful completion of these tests, after which the switch comes up in the FIPS-compliant state, as shown below:

```
FIPS-mode test application
1. Non-Approved cryptographic operation test...
        a. Excluded algorithm (MD5)...successful
        b. Included algorithm (D-H)...successful
2. Automatic power-up self test...
        2.a. FIPS RNG selftest...successful
        2.b. FIPS Rand method set...successful
3. AES-128,192,256 CBC  encryption/decryption...successful
4. RSA key generation and encryption/decryption...successful
4.1. RSA 2048 with 'SHA256' testing...successful
5. TDES-CBC encryption/decryption...successful
6a. SHA-1 hash...successful
6b. SHA-256 hash...successful
6c. SHA-512 hash...successful
6d. HMAC-SHA-1 hash...successful
6e. HMAC-SHA-224 hash...successful
6f. HMAC-SHA-256 hash...successful
```

```
6g. HMAC-SHA-384 hash...successful
6h. HMAC-SHA-512 hash...successful
7. Non-Approved cryptographic operation test...
        a. Excluded algorithm (MD5)...Not executed
        b. Included algorithm (D-H)...successful as expected
8. Zero-ization...Successful
9. TLS 1. 0 KDF...successful
10. SSH KDF …. Successful

All tests completed with 0 errors
```

NOTE
If the output shows errors, the switch reboots. If the errors persist, you must return the switch to your service provider for repair.

21. Use IP ACLs to block the HTTP, HTTPS, Telnet, and Brocade internal ports. Enter the following commands for IPv4 and IPv6.

    a. Enter the **ip access-list extended** command and a name for the IP ACL.

    b. Enter a **seq deny** command to create a rule for blocking the HTTP port (80).

    c. Enter a **seq deny** command to create a rule for blocking the HTTPS port (443).

    d. Enter a **seq deny** command to create a rule for blocking the Telnet port (23).

    e. Enter **seq deny** commands to create rules for blocking the Brocade internal server ports 3016, 4565, 5016, 7013, 7110, 7710, 9013, 9110, 9710, and 9910 through 10110.

    f. If SSH access is required, enter seq permit commands to allow access on ports 22 and 830.

    g. If remote access is required, such as through SCP or LDAP, enter seq permit commands to allow UDP and TCP traffic on ports 1024 through 65535.Enter the **interface management** *rbridge-id/port* command to enter the interface management subconfiguration mode.

    h. Enter the **ip access-group** command with the ACL name created in step a to apply the ACL to the management interface.

    These commands also disable the non-FIPS-compliant vCenter feature.

    For IPv4:

```
switch(conf-ip-ext)# seq 1 deny tcp any any eq www
switch(conf-ip-ext)# seq 2 deny tcp any any eq 443
switch(conf-ip-ext)# seq 3 deny tcp any any eq telnet
switch(conf-ip-ext)# seq 4 deny tcp any any eq 2301
switch(conf-ip-ext)# seq 5 deny tcp any any eq 2401
switch(conf-ip-ext)# seq 6 deny tcp any any eq 3016
switch(conf-ip-ext)# seq 7 deny tcp any any eq 3516
switch(conf-ip-ext)# seq 8 deny tcp any any eq 4516
switch(conf-ip-ext)# seq 9 deny tcp any any eq 5016
switch(conf-ip-ext)# seq 10 deny tcp any any eq 7013
switch(conf-ip-ext)# seq 11 deny tcp any any eq 7110
switch(conf-ip-ext)# seq 12 deny tcp any any eq 7710
switch(conf-ip-ext)# seq 13 deny tcp any any eq 9013
switch(conf-ip-ext)# seq 14 deny tcp any any eq 9110
switch(conf-ip-ext)# seq 15 deny tcp any any eq 9710
switch(conf-ip-ext)# seq 16 deny tcp any any range 9910 10110
switch(conf-ip-ext)# seq 17 deny udp any any eq 33351
switch(conf-ip-ext)# seq 18 deny udp any any eq 36851
switch(conf-ip-ext)# seq 19 deny udp any any eq 37731
switch(conf-ip-ext)# seq 20 deny udp any any eq 50690
```

```
switch(conf-ip-ext)# seq 21 permit tcp any any range 1024 65535
switch(conf-ip-ext)# seq 22 permit udp any any range 1024 65534
switch(conf-ip-ext)# seq 23 permit udp any any eq 65535
switch(conf-ip-ext)# seq 100 permit tcp any any eq 22
switch(conf-ip-ext)# seq 101 permit tcp any any eq 830
switch(conf-ip-ext)# exit
switch(config)#
```

For IPv6:

```
switch(conf-ip-ext)# seq 1 deny tcp any any eq 80
switch(conf-ip-ext)# seq 2 deny tcp any any eq 443
switch(conf-ip-ext)# seq 3 deny tcp any any eq 23
switch(conf-ip-ext)# seq 4 deny tcp any any eq 2301
switch(conf-ip-ext)# seq 5 deny tcp any any eq 2401
switch(conf-ip-ext)# seq 6 deny tcp any any eq 3016
switch(conf-ip-ext)# seq 7 deny tcp any any eq 3516
switch(conf-ip-ext)# seq 8 deny tcp any any eq 4516
switch(conf-ip-ext)# seq 9 deny tcp any any eq 5016
switch(conf-ip-ext)# seq 10 deny tcp any any eq 7013
switch(conf-ip-ext)# seq 11 deny tcp any any eq 7110
switch(conf-ip-ext)# seq 12 deny tcp any any eq 7710
switch(conf-ip-ext)# seq 13 deny tcp any any eq 9013
switch(conf-ip-ext)# seq 14 deny tcp any any eq 9110
switch(conf-ip-ext)# seq 15 deny tcp any any eq 9710
switch(conf-ip-ext)# seq 16 deny tcp any any range 9910 10110
switch(conf-ip-ext)# seq 17 deny udp any any eq 33351
switch(conf-ip-ext)# seq 18 deny udp any any eq 36851
switch(conf-ip-ext)# seq 19 deny udp any any eq 37731
switch(conf-ip-ext)# seq 20 deny udp any any eq 50690
switch(conf-ip-ext)# seq 21 permit tcp any any range 1024 65535
switch(conf-ip-ext)# seq 22 permit udp any any range 1024 65534
switch(conf-ip-ext)# seq 23 permit udp any any eq 65535
switch(conf-ip-ext)# seq 100 permit tcp any any eq 22
switch(conf-ip-ext)# seq 101 permit tcp any any eq 830
switch(conf-ip-ext)# exit
switch(config)#
```

For inband management IPv4 ports, use the following rules:

```
switch(conf-ip-ext)# seq 5 hard-drop tcp any any eq 80
switch(conf-ip-ext)# seq 10 hard-drop tcp any any eq 443
switch(conf-ip-ext)# seq 15 hard-drop tcp any any eq 23
switch(conf-ip-ext)# seq 20 hard-drop tcp any any eq 2301
switch(conf-ip-ext)# seq 25 hard-drop tcp any any eq 2401
switch(conf-ip-ext)# seq 30 hard-drop tcp any any eq 3016
switch(conf-ip-ext)# seq 35 hard-drop tcp any any eq 3516
switch(conf-ip-ext)# seq 40 hard-drop tcp any any eq 4516
switch(conf-ip-ext)# seq 45 hard-drop tcp any any eq 5016
switch(conf-ip-ext)# seq 50 hard-drop tcp any any eq 7013
switch(conf-ip-ext)# seq 55 hard-drop tcp any any eq 7110
switch(conf-ip-ext)# seq 60 hard-drop tcp any any eq 7710
switch(conf-ip-ext)# seq 65 hard-drop tcp any any eq 9013
switch(conf-ip-ext)# seq 70 hard-drop tcp any any eq 9110
switch(conf-ip-ext)# seq 75 hard-drop tcp any any eq 9710
switch(conf-ip-ext)# seq 80 hard-drop tcp any any range 9910 10110
switch(conf-ip-ext)# seq 85 hard-drop udp any any eq 33351
switch(conf-ip-ext)# seq 90 hard-drop udp any any eq 36851
switch(conf-ip-ext)# seq 95 hard-drop udp any any eq 37731
switch(conf-ip-ext)# seq 100 hard-drop udp any any eq 50690
switch(conf-ip-ext)# seq 105 permit tcp any any range 1024 65535
```

```
switch(conf-ip-ext)# seq 110 permit udp any any range 1024 65534
switch(conf-ip-ext)# seq 115 permit udp any any eq 65535
switch(conf-ip-ext)# seq 120 permit tcp any any eq 22
switch(conf-ip-ext)# seq 125 permit tcp any any eq 830
switch(conf-ip-ext)# exit
switch(config)#
```

NOTE
For the switch to remain FIPS compliant, the HTTP, HTTPS, Telnet, and Brocade internal server ports (80, 443, 23, 2301, 2401, 3016, 3516, 4516, 5016, 7013, 7110, 7710, 9013, 9110, 9710, 9910 through 10110, 33351, 36851, 37731, and 50690) must be blocked after every zeroization operation.

22. Disable the Telnet server.

```
switch(config)# telnet server shutdown
switch(config)#
```

23. If RADIUS authentication is required, execute the following CLI in config mode to configure Radius server to use only PEAP-MSCHAPv2. Radius server with PAP and CHAP is not allowed in FIPS compliant state.

```
switch(config)#radius-server host <host> protocol peap-mschapv2
```

24. If LDAP authentication is required, in global configuration mode, enter the following command syntax to import the LDAP CA certificate:

certutil import ldapca directory *ca-certificate-directory* **file** *filename* **protocol** {**FTP**|**SCP**} **host** *remote-ip-address* **user** *user-account* **password** *password*

NOTE
The ca certificate imported must be RSA2048 with SHA256 encrypted.

Specify SCP for the protocol.

```
switch# certutil import ldapca directory /usr/ldapcacert file cacert.pem
    protocol SCP host 10.23.24.56 user jane password ******
```

25. Enter the **copy running-config startup-config** command to save all settings to the startup configuration file.

```
switch# copy running-config startup-config
```

NOTE
After the switch is in the FIPS-compliant state, do not use any non-FIPS-compliant algorithms such as FTP, DHCHAP, MD5. With regards to SCP client on the switch, the remote SCP server must employ RSA host keys with a minimum length of 1024 bits.

Zeroizing for FIPS

1. Log in to the switch using an account with admin role permissions.
2. In privileged EXEC mode, enter the **fips zeroize** command.

   The switch reboots automatically. If the KATs and conditional tests are enabled, then the switch will reboot in the FIPS-compliant state. If the tests are not enabled, the switch comes up in the non-FIPS-compliant state.

NOTE
For the switch to remain FIPS compliant, the HTTP, HTTPS, telnet, and Brocade internal server ports (3016, 4565, 5016, 7013, 7110, 7710, 9013, 9110, 9710, and 9910 through 10110 inclusive) must be blocked after every zeroization operation.

LDAP in the FIPS-compliant state

You can configure your Microsoft Active Directory server to use the Lightweight Directory Access Protocol (LDAP) while in the FIPS-compliant state.

Table 3 lists the differences between the FIPS-compliant and non-FIPS-compliant states of operation.

TABLE 3 FIPS-compliant and non-FIPS-compliant states of operation

FIPS-compliant state	non-FIPS-compliant state
The certificate for the CA that issued the Microsoft Active Directory server certificate must be installed on the switch.	There is no mandatory CA certificate installation on the switch.
Configure FIPS-compliant TLS ciphers [TDES-168, SHA256, and RSA-2048] on the Microsoft Active Directory server. The host needs a reboot for the changes to take effect.	On the Microsoft Active Directory server, there is no configuration of the FIPS-compliant TLS ciphers.
The switch uses FIPS-compliant ciphers regardless of the Microsoft Active Directory server configuration. If the Microsoft Active Directory server is not configured for FIPS ciphers, authentication will still succeed.	The Microsoft Active Directory server certificate is validated if the CA certificate is found on the switch.
The Microsoft Active Directory server certificate is validated by the LDAP client. If the CA certificate is not present on the switch then user authentication will fail.	If the Microsoft Active Directory server is configured for FIPS ciphers and the switch is in the non-FIPS-compliant state, then user authentication will succeed.

When setting up an LDAP server for FIPS, you will need to perform the following tasks:

- Add a DNS server.
- Configure a Microsoft Active Directory server as the authentication device.
- Import the RSA 2048 LDAP CA certificate from the Microsoft Active Directory server to the switch.

Configuring the DNS server and the Microsoft Active Directory server should be performed before bringing up the switch in the FIPS-compliant state. Any DSA CA certificates must be deleted from the switch.

Setting up LDAP for the FIPS-compliant state

1. Log in to the switch by using an account with admin role permissions.
2. In privileged EXEC mode, enter the **configureterminal** command to enter global configuration mode.
3. Enter the **ip dns domain-name** and **ip dns name-server** commands to configure DNS on the switch.

Specify the DNS IP address in either IPv4 or IPv6 format. This address is needed for the switch to resolve the domain name to the IP address, because LDAP initiates a TCP session to connect to your Microsoft Active Directory server. A Fully Qualified Domain Name (FQDN) is needed to validate the server identity as mentioned in the common name of the server certificate.

```
switch# configure
Entering configuration mode terminal
switch(config)# ip dns domain-name sec.brocade.com
switch(config)# ip dns name-server 10.70.20.1
```

4. Enter the **aaa authentication login ldap** command to set the switch authentication mode for LDAP.

```
switch(config)# aaa authentication login ldap local
```

5. Enter the **ldap-server host** command to add your LDAP server. Provide the FQDN of the Microsoft Active Directory server for the host name parameter while configuring LDAP. The maximum supported length for the host name is 40 characters.

```
switch(config)# ldap-server host GEOFF5.ADLDAP.LOCAL basedn sec.brocade.com
port 389 retries 3
switch(config-ldap-server-GEOFF5.ADLAP.LOCAL)# exit
switch (config) exit
switch# show running-config ldap-server host GEOFF5.ADLDAP.LOCAL
ldap-server host GEOFF5.ADLDAP.LOCAL
 port        389
 domain      security.brocade.com
 retries     3
!
switch#
```

6. Enter the **cipherset ldap** command to configure the FIPS-compliant ciphers for LDAP operation.

```
switch# cipherset ldap
ldap cipher list configured successfully
```

7. Set up LDAP according to the instructions in the “External Server Authentication” chapter of the *Network OS Administrator’s Guide*, then perform the following additional Microsoft Active Directory settings.

   a. To support FIPS-compliant TLS cipher suites on the Microsoft Active Directory server, allow the SCHANNEL settings listed in Table 4.

TABLE 4 Active Directory keys to modify

Key	Sub-key
Ciphers	3DES
Hashes	SHA256
Key exchange algorithm	PKCS
Protocols	TLSv1.0

   b. Enable the FIPS algorithm policy on the Microsoft Active Directory.

1 LDAP in the FIPS-compliant state