

53-1003191-01
22 January 2014



FastIron

FIPS Configuration Guide

Supporting FastIron Software Release 07.4.00a

BROCADE

© 2014, Brocade Communications Systems, Inc. All Rights Reserved.

Brocade, the B-wing symbol, Brocade Assurance, ADX, AnyIO, DCX, Fabric OS, FastIron, HyperEdge, ICX, MLX, MyBrocade, NetIron, OpenScript, VCS, VDX, and Vyatta are registered trademarks, and The Effortless Network and the On-Demand Data Center are trademarks of Brocade Communications Systems, Inc., in the United States and in other countries. Other brands and product names mentioned may be trademarks of others.

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

The authors and Brocade Communications Systems, Inc. assume no liability or responsibility to any person or entity with respect to the accuracy of this document or any loss, cost, liability, or damages arising from the information contained herein or the computer programs that accompany it.

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

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

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

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 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
<i>FIPS Configuration Guide for FastIron Devices</i>	53-1003191-01	Generic version for all releases and products.	22 January 2014

Contents

About This Guide

Introduction	v
Supported Hardware	v
Audience	v
Document conventions	v
Text formatting	v
Command syntax conventions	vi
Notes, cautions, and danger notices	vi
Related publications	vi
Getting technical help	vii

Chapter 1

Federal Information Processing Standards

Overview	1
User roles in FIPS mode	2
Commands disabled in FIPS mode	2
Hidden files in FIPS mode	3
Cryptographic algorithms in FIPS mode	3
Protocol changes in FIPS mode	4
System reset and boot in FIPS mode	11
Placing the device in FIPS mode	11
General steps to place the device in FIPS mode	12
Copying the signature files	12
Enabling FIPS mode	12
Perform a FIPS self-test	14
Modifying the FIPS policy	15
Zeroizing shared secrets and host keys	16
Saving the configuration	17
Reloading the device	17
Running FIPS self-test	18
Disabling FIPS mode	18
Troubleshooting a failed software image installation in FIPS mode	19

About This Guide

Introduction

This guide describes how to configure Brocade FastIron platforms that support Federal Information Processing Standard (FIPS) mode as detailed in FIPS Publication 140-2. This guide includes procedures for configuring the software. The software procedures show how to perform tasks using the CLI. This guide also describes how to monitor Brocade products using statistics and summary screens.

Supported Hardware

This guide supports the Brocade ICX 6450 Series (ICX 6450) product family.

Audience

This document is designed for system administrators with a working knowledge of Layer 2 and Layer 3 switching and routing.

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
	Identifies text to enter at the GUI or CLI
<i>italic text</i>	Provides emphasis
	Identifies variables
	Identifies document titles
<code>code text</code>	Identifies CLI output

For readability, command names in the narrative portions of this guide are presented in bold: for example, **show version**.

Command syntax conventions

Command syntax in this manual follows these conventions:

command and parameters	Commands and parameters are printed in bold.
[]	Optional parameter.
<i>variable</i>	Variables are printed in italics enclosed in angled brackets < >.
...	Repeat the previous element, for example “member[:member...]”
	Choose from one of the parameters.

Notes, cautions, and danger notices

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.



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.

Related publications

The following Brocade documents supplement the information in this guide:

- IronWare Software Release Notes
- FIPS Security Seal Procedures applicable for your devices
- Hardware Installation Guides applicable for your devices

The latest version of these guides are posted at <http://www.brocade.com/ethernetproducts>.

If you find errors in the guides, send an email to documentation@brocade.com

Getting technical help

To contact Technical Support, go to <http://www.brocade.com/services-support/index.page> for the latest e-mail and telephone contact information.

Federal Information Processing Standards

This chapter contains steps for configuring FIPS mode on the Brocade device in compliance with standards established by the United States government and the National Institute of Standards and Technology (NIST). The sections in this chapter describe FIPS mode, how to enable and disable FIPS mode on the device, and the behavior of the device in FIPS mode.

Overview

FIPS are security standards developed by the United States government and NIST for use by all non-military government agencies and by government contractors. Due to their importance within the security industry, these standards form a baseline for many security requirements.

The FIPS Publication 140-2 is a technical standard and worldwide de-facto standard for the implementation of cryptographic modules.

You can configure the Brocade device to run in FIPS mode to ensure that the device is operating according to the standards stated in FIPS Publication 140-2.

For details on how to place the tamper seals, see the platform-specific FIPS Seal Procedure manual available at the [myBrocade](#) website.

A Brocade device is FIPS 140-2-compliant when the following requirements have been met:

- Tamper-resistant labels are applied to the device according to the instructions included in the tamper-resistant accessory kit. The accessory kit is purchased separately.
- The device software is placed in FIPS mode with the FIPS security policy applied.

You place a device in FIPS mode by entering the **fips enable** CLI command on the management station while the station is connected to the device console port with a serial cable. After you enter the **fips enable** command, the device is administratively in FIPS mode and by default runs in strict FIPS-compliant mode upon reload.

The default FIPS policy is for the system to run in a strict mode that fully supports FIPS 140-2 specifications. However, the device allows you the flexibility to configure a modified FIPS policy according to your network requirements. A FIPS policy that varies from the default policy weakens the intent of the FIPS 140-2 specifications; when implemented, the device is not operating in full compliance with these specifications. Refer to [“Modifying the FIPS policy”](#) on page 15.

The default FIPS policy enforces the following actions for strict FIPS compliance:

- Disables TFTP access
- Disables monitor access to memory access commands
- Returns 0 or null for SNMP MIBs for passwords or keys
- Zeroizes shared secrets and passwords

The device performs the following functions automatically during reboot after the **fips enable** command is entered:

- Disables Telnet
- Enables SCP access
- Disables the HTTP server
- HTTPS server:
 - Disables SSL 3.0 and uses only TLS version 1.0 and greater
 - Disables the RC4 cipher
 - Removes the **web-management allow-no-password** command from the configuration
- Disables SNMP access to Critical Security Parameter (CSP) MIB objects
- Disables AAA authentication for the console

After defining the FIPS policy, save the configuration, and reboot the device. While the device is booting, several tests are run to ensure the device is FIPS compliant. After these tests are completed successfully, the device reloads and is operationally in FIPS mode.

All the optional FIPS policy commands are provided to perform various FIPS non-approved operations when FIPS is enabled. It should be noted that if this any of these policy commands are configured, the module is not operating in the approved FIPS mode.

User roles in FIPS mode

A Brocade device in FIPS mode supports three user roles:

- **Crypto Officer Role:** The Crypto Officer Role on the device in FIPS mode is equivalent to the administrator role, or the super-user, in non-FIPS mode.
- **Port Configuration Administrator Role:** The Port Configuration Administrator on the device in FIPS mode is equivalent to the port configuration user in non-FIPS mode and has write access to the interface configuration mode only.
- **User Role:** The User Role on the device in FIPS mode has read-only privileges and no configuration mode access.

Note that strict password enforcement is not supported when the device is in FIPS mode. The password must be at least eight characters long. Also, if a password has only one character from a character class (uppercase, lowercase, numeric and ASCII non-alphanumeric characters), then it should not be the first or last character in the password.

Concurrent operators are supported but no limit is enforced. The number of concurrent users is only limited by the system resources.

Commands disabled in FIPS mode

The device in FIPS mode does not support the following commands:

- **enable password-display**
- **enable strict-password-enforcement**
- **web-management allow-no-password**
- **enable aaa console**
- **telnet server**
- **ip ssh scp disable**
- **ip ssh aes-only**

- **ip ssh key-authentication** no | yes
- **ip ssh permit-empty-password** no | yes
- **web-management** http

A device in FIPS mode does not support TFTP commands, including:

- **copy tftp flash** <ip>
- **boot system tftp** <ip> <file>
- **ip ssh pub-key-file tftp** <ip> <file> | pubkey>
- **ip ssl certificate-data-file tftp** <ip> <file>
- **ip ssl private-key file tftp** <tftp> <file>

Hidden files in FIPS mode

Hidden files are not displayed when the device is in FIPS mode. Hidden files are displayed only when the device is in non-FIPS mode.

Cryptographic algorithms in FIPS mode

The device in FIPS mode supports the following FIPS 140-2 approved cryptographic algorithms:

- Advanced Encryption Algorithm (AES)
- Triple Data Encryption Algorithm (Triple-DES)
- Secure Hash Algorithm (this includes all SHA variants the module supports: SHA-1, SHA-256, SHA-384, and SHA-512)
- Keyed-Hash Message Authentication code (HMAC)
- Deterministic Random Bit Generator (DRBG)
- Digital Signature Algorithm (DSA)
- Rivest, Shamir, and Adleman public key encryption Algorithm (RSA))
- Elliptic curve Digital Signature Algorithm (ECDSA)

Allowed exceptions include:

- RSA Key Wrapping
- Diffie-Hellman (DH)
- SNMPv3
- Message Digest 5 (MD5) as used in TLSv1.0
- Hashed Message Authentication codes - Message Digest 5 (HMAC-MD5) as used in RADIUS and TACACS+
- Non-Deterministic Random Number Generator (NDRNG)
- SSHv2Key Derivation Function (KDF)

The device in FIPS mode does not support the following cryptographic algorithms:

- RC4
- DES

Protocol changes in FIPS mode

[Table 1](#) lists the protocols that undergo changes while the device is in FIPS mode with the default policy applied.

TABLE 1 Protocol changes

Protocols/ Algorithms	Supported in FIPS mode	Supported in Non-FIPS mode	For more information on individual protocol changes, refer to the following sections:
BGP	Yes	Yes	“BGP” on page 4
HTTP	No	Yes	“HTTP” on page 5
HTTPS	Yes, with limitations	Yes	“HTTPS” on page 5
IPsec	Yes, with limitations	Yes	“IPsec” on page 6
MD5 password encryption	Yes, with limitations. MD5 password encryption is supported for SNTP, VRRP, and VRRP-E	Yes	
OSPFv3	Yes	Yes	“OSPFv2” on page 6
Proprietary 2-way encryption algorithms	No	Yes	“Proprietary 2-way encryption algorithms” on page 6
RADIUS	Yes, with limitations	Yes	“RADIUS” on page 6
SCP	Yes	Yes	“SCP” on page 7
SNMP	Yes, with limitations	Yes	“SNMP” on page 8
SSHv2	Yes, with limitations	Yes	“SSHv2” on page 10
TACACS+	Yes, with limitations	Yes	“TACACS+” on page 10
Telnet	No	Yes	“Telnet” on page 10
TFTP	No	Yes	“TFTP” on page 10
Web Authentication	No	Yes	“Web Authentication” on page 11

BGP

Border Gateway Protocol (BGP) allows peer-to-peer authentication or client-to-server authentication. To authorize an authentication, use a command such as the following to configure shared secret keys for BGP:

```
Brocade(config-bgp-router)# neighbor 192.168.1.2 password P@$w0rd
```

Syntax: `[no] neighbor <ip-addr> | <peer-group-name> password <string>`

For more information on BGP authentication commands, refer to FastIron Configuration Guide.

HTTP

HTTP is not supported on the device in FIPS mode.

The **web-management http** command is disabled if it is included in the device's configuration. When the HTTP server is enabled because the **web-management http** command has been configured, the system removes the command from the configuration and the device displays the following messages:

```
FIPS Compliance: HTTP service will been disabled
```

HTTPS continues to be enabled in FIPS mode and the configuration changes the **web-management http** command to the **web-management https** command.

HTTPS

The following HTTPS configurations are affected in FIPS mode:

- The **web-management https** command is maintained and offers equivalent functionality to the disabled **web-management http** command. Note that in addition to port 443, port 280 is also open for access by HP ProCurve Manager. You can disable this port using the **no web-management hp-top-tools** command.
- The **web-management allow-no-password** command is disabled.
- The AAA authentication method **none** option is not allowed in FIPS mode. For example, the **aaa authentication enable none** command (the **none** option designated as the authentication method) is disabled. In addition, you cannot enable FIPS when AAA authentication method **none** option is used. You must disable the **none** option before you can enable FIPS on the device.
- The **ip ssl certificate-data-file tftp** command is disabled when TFTP operation is disabled in FIPS mode. SCP supports this command's functionality. Refer to "[SCP](#)" on page 7.
- The **ip ssl private-key-file tftp** command is disabled when TFTP operation is disabled in FIPS mode. SCP supports the functionality of this command. Refer to "[SCP](#)" on page 7.
- The **crypto-ssl certificate zeroize** command zeroes out the RSA key pair and removes the digital certificate.
- SSL version 3 and earlier versions are disabled and TLS 1.0 or later versions are enabled.
- RC4 in TLS is disabled.
- HP

The FIPS 140-2 cipher suites consist of the following algorithms:

- Triple-DES (FIPS 46-3) or AES (FIPS 197) for symmetric key encryption and decryption.
- Secure Hash Standard (SHA-1, SHA-256, SHA-384, and SHA-512) (FIPS 180-2) for hashing.
- HMAC (FIPS 198) for keyed hash.
- Random number generator Hash DRBG (NIST SP800-90).
- Diffie-Hellman, EC Diffie-Hellman, or Key Wrapping using RSA keys for key establishment.
- DSA (FIPS 186-2 with Change Notice 1), RSA (PKCS #1 v2.1), or ECDSA (ANSI X9.62) for signature generation and verification.

The following cipher suites are allowed in FIPS mode:

- TLS_RSA_WITH_AES_128_CBC_SHA

- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA

The cipher suite TLS_RSA_WITH_AES_256 is the default cipher suite.

IPsec

FIPS 140-2 does not allow null encryption.

OSPFv2

The OSPFv2 protocol uses IPsec with IP ESP and HMAC-SHA-196, and is allowed in FIPS mode.

OSPF allows peer-to-peer authentication or client-to-server authentication. To authorize an authentication, use commands such as the following to configure shared secret keys for OSPF:

```
Brocade(config-if-e1000-1/1)# ip ospf authentication-key P@$w0rd
```

Syntax: `ip ospf authentication-key <string>`

```
Brocade(config-if-e1000-1/2)# ip ospf md5-authentication key-id 1 key P@$w0rd
```

Syntax: `ip ospf md5-authentication key-id <num> key <string>`

```
Brocade(config-ospf-router)# area 2 virtual-link 2.3.4.5 md5-authentication
key-id 2 key P@$w0rd
```

Syntax: `[no] area <ip-addr> | <num> virtual-link <router-id> [authentication-key <string> | md5-authentication key-id <num> key [0|1] <string>]`

```
Brocade(config-if-e1000-1/1)#ipv6 ospf authentication ipsec spi 256 esp sha1
1234567890123456789012345678901234567890
```

Syntax: `[no] ipv6 ospf authentication ipsec spi <spinum> esp sha1 [no-encrypt] <key>`

Proprietary 2-way encryption algorithms

The routing protocols OSPFv2, BGP, and the management protocol SNMP save authentications parameters using one of the following two proprietary algorithms:

- Global encoding scheme
- Base 64 encoding scheme

These proprietary algorithms are not supported in FIPS mode. When the default FIPS policy is applied, these authentication parameters are zeroized.

RADIUS

HMAC-MD5 authentication used in RADIUS is allowed in FIPS mode.

RADIUS allows peer-to-peer authentication or client-to-server authentication. To authorize an authentication, use commands such as the following to configure shared secret keys for RADIUS:

```
Brocade(config)# radius-server host 1.2.3.4 auth-port 1812 acct-port 1813 default
key 1 Example01
```

Syntax: [no] radius-server host <ip-addr> | <server-name> [auth-port <number> acct-port <number>][authentication-only accounting-only default] [key [0 1 2] <string> [dot1x]]]

```
Brocade(config)# radius-server key 1 Example01
```

Syntax: [no] radius-server key [0 | 1] <string>

SCP

Table 2 lists the Secure Copy (SCP) commands that are available to compensate for equivalent existing functionality of TFTP commands disabled in FIPS mode.

TABLE 2 Corresponding TFTP and SCP commands

Command functionality	TFTP commands not allowed in FIPS mode	SCP commands with corresponding functionality in FIPS mode
Import a digital certificate	ip ssl certificate-data-file tftp <ip-address> <certificate-filename>	scp <certificate-filename> <user>@<ip-address>:sslCert
Import an RSA private key from a client	ip ssl private-key-file tftp <ip-address> <key-filename>	scp <key-filename> <user>@<ip-address>: sslPrivKey
Load a DSA public key file from a client	ip ssh pub-key-file tftp <ip-address> <key-filename>	scp <key-filename> <user>@<ip-address>: sshPubKey

Importing a digital certificate

To import a digital certificate using SCP, enter a command such as the following one:

```
C:> scp certfile user@192.168.89.210:sslCert
```

Syntax: scp <certificate-filename> <user>@<ip-address>:sslCert

The <ip-address> variable is the IP address of the server from which the digital certificate file is downloaded.

The <certificate-filename> variable is the file name of the digital certificate that you are importing to the device.

The functionality of the **scp** command is equivalent to that of the disabled **ip ssl certificate-data-file tftp** command.

For more information on the **scp** command, refer to FastIron Configuration Guide.

Importing an RSA private key from a client

To import an RSA private key from a client using SCP, enter a command such as the following one:

```
C:> scp keyfile user@192.168.9.210:sslPrivKey
```

Syntax: scp <key-filename> <user>@<ip-address>: sslPrivKey

The `<ip-address>` variable is the IP address of the server that contains the private key file.

The `<key-filename>` variable is the file name of the private key that you want to import into the device.

The functionality of the **scp** command is equivalent to that of the disabled **ip ssl private-key-file tftp** command.

For more information on the **scp** command, refer to FastIron Configuration Guide.

Loading a DSA public key file from a client

To load a DSA public key file from a client using SCP, enter a command such as the following one:

```
C:> scp pkeys.txt user@192.168.1.234:sshPubKey
```

Syntax: **scp** `<key-filename>` `<user>@<ip-address>:sshPubKey`

The `<ip-address>` variable is the IP address of the server that contains the public key file.

The `<key-filename>` variable is the name of the DSA public key file that you want to import into the device.

The functionality of the **scp** command is equivalent to the disabled **ip ssh pub-key-file tftp** command.

For more information on the **scp** command, refer to FastIron Configuration Guide.

SNMP

In the FIPS mode of operation, the device uses the existing SNMP configuration. However, MIB objects related to keys and passwords output NULL or a 0 value. Refer to “[SNMP CSP objects](#)” on page 9.

SNMP allows peer-to-peer authentication or client-to-server authentication. To authorize an authentication, use commands such as the following to configure shared secret keys for SNMP:

```
Brocade(config)# snmp-server community brocadeSNMP ro
```

Syntax: **[no] snmp-server community** `<string>` **[ro | rw]**

```
Brocade(config)# snmp-server host 10.1.53.181 version v2c 1 $Si2^=d
```

Syntax: **[no] snmp-server host** `<ip-addr>` `<string>` **[port** `<value>`**]**

```
Brocade(config)# snmp-server group admingrp v3 priv read all write all notify all
```

Syntax: **[no]snmp-server group** `<groupname>` **v1| v2| v3** **auth | noauth | priv** **[access** `<standard-ACL-id>`**]** **[read** `<viewstring>` **| write** `<viewstring>` **| notify** `<viewstring>`**]**

```
Brocade(config)# snmp-server user adminuser admingrp v3 encrypted auth md5
c1c510d4f3c6bec15ff14f9c0f3ec120 priv encrypted aes
b0c4c6c05cded8cfe3a335299347c71b
```

Syntax: **[no] snmp-server user** `<name>` `<groupname>` **v3** **[[access** `<standard-ACL-id>`**]** **[[encrypted] [auth** `<md5-password>` **| sha** `<sha-password>`**]** **[priv** **[encrypted] des** `<des-password-key>` **| aes** `<aes-password-key>`**]]]**

SNMP CSP objects

The following SNMP MIB objects represent the Critical Security Parameter (CSP) entities that are restricted in FIPS mode:

Enterprise MIB objects:

- snRadiusKey
- snRadiusServerRowKey
- snTacacsKey
- snTacacsServerRowKey
- snVrrplfAuthPassword
- snAgGblPassword
- snAgGblReadOnlyCommunity
- snAgGblReadWriteCommunity
- snAgGblTelnetPassword
- snAgentUserAccntPassword
- fdryRadiusServerRowKey
- fdryTacacsServerRowKey
- snOspfIfAuthKey
- snOspfIfMd5AuthKey
- snOspfIf2AuthKey
- snOspfIf2Md5authKey
- snOspfVirtIfAuthKey
- snOspfVirtIfMd5AuthKey
- snOspfIfStatusAuthKey
- snOspfIfStatusMd5AuthKey
- snOspfVirtIfStatusAuthKey
- snOspfVirtIfStatusMd5AuthKey
- snBgp4NeighGenCfgPass
- snVrrplf2AuthPassword
- snVsrplfAuthPassword

Standard MIB objects:

- rip2IfConfAuthKey
- vrrpOperAuthKey
- dvmpInterfaceKey

SSHv2

Secure Shell version 2 (SSHv2) is allowed in FIPS mode.

The following SSH configurations are affected when the Brocade device is in FIPS mode:

- The **ssh server** command enables the SSH server. The SSH server is always enabled; however, to start it, use the **crypto key generate** command to create host keys.
- The **ip ssh aes-only** command is disabled.
- The **ip ssh key-authentication** command is disabled.
- The **ip ssh permit-empty-password** command is disabled.
- The **ip ssh pub-key-file tftp** command is disabled.
- The **ip ssh scp** command ensures that SCP is enabled to run in FIPS mode. SCP is needed for file communication and the **ip ssh scp disable** command is disabled in FIPS mode and displays the following message:

```
FIPS Compliance: SCP needs to be enabled
```

- The **crypto key zeroize** command removes configured SSH keys.

Use the command **show ip ssh config** to display SSH configuration information. For more information on the **show ip ssh config** command, refer to FastIron Configuration Guide.

SSH key generation time is affected by the increased security of authentication and encryption algorithms both in and out of FIPS mode.

TACACS+

HMAC-MD5 packet encryption used in TACACS+ is allowed in FIPS mode.

TACACS+ allows peer-to-peer authentication or client-to-server authentication. To authorize an authentication, use commands such as the following to configure shared secret keys for TACACS+:

```
Brocade(config)# tacacs-server host 172.16.114.63 auth-port 49 accounting-only
key P@$$w0rd
```

Syntax: **[no] tacacs-server host** <ip-addr> | <server-name> **[auth-port** <number> **accounting-only** **]** **[key** <string> **]**

```
Brocade(config)# tacacs-server key P@$$w0rd
```

Syntax: **[no] tacacs-server key** [0 | 1] <string>

For more information on TACACS+ authentication commands, refer to FastIron Configuration Guide.

Telnet

Telnet is disabled in FIPS mode as part of the default FIPS policy on the device. Attempts to start the Telnet server fail in FIPS mode.

TFTP

The following TFTP commands are disabled and return an error when TFTP operation is not allowed on the device in FIPS mode:

- All **copy tftp** commands
- The command **boot system tftp <ip-address> <filename>**

The following TFTP commands are disabled. Use SCP commands with equivalent functionality instead. Refer to [“SCP”](#) on page 7.

- **ip ssl certificate-data-file tftp <ip-address> <certificate-filename>**
- **ip ssl private-key-file tftp <ip-address> <key-filename>**
- **ip ssh pub-key-file tftp <ip-address> <key-filename>**

Web Authentication

Web Authentication is not supported when FIPS mode is enabled on the device.

System reset and boot in FIPS mode

Firmware digital signature verification and POST testing takes place as the device progresses through the boot sequence.

The following actions and limitations take effect when the device is operationally in FIPS mode according to the FIPS default policy:

- Boot from TFTP is disabled.
- Monitor mode memory access command set is disabled. Configure an alternative FIPS policy to the default policy to access the command set. Refer to [“Modifying the FIPS policy”](#) on page 15.
- Access to memory test mode is disabled.
- Debug commands are disabled from the application prompt in FIPS mode.

Placing the device in FIPS mode

Placing the device in FIPS mode is a multiple part process that begins with enabling FIPS mode on the device. This places the device administratively in FIPS mode. To operate the device in FIPS mode, save the configuration, and reboot the device. Always back-up the desired configuration to ensure it is saved in the event of a system reset.



CAUTION

After enabling the FIPS mode on your device, you cannot disable it without losing the device configuration. For disabling the FIPS mode, it is recommended that you contact Brocade Technical Support and perform the procedure under qualified guidance.

General steps to place the device in FIPS mode

NOTE

Run the **show version** command to ensure that you are running the FastIron 07.4.00a software version on your device. For upgrade procedure to software version 07.4.00a, see the FastIron 07.4.00a Release Note.

1. Disable the AAA authentication method **none** option if used in the device configuration.
2. Copy the needed signature files. Refer to [“Copying the signature files”](#) on page 12.
3. Perform a FIPS self test to verify the right signature files were copied. Refer to [“Perform a FIPS self-test”](#) on page 14.
4. Enable FIPS mode. Refer to [“Enabling FIPS mode”](#) on page 12.
5. Optionally, modify the default FIPS policy. Refer to [“Modifying the FIPS policy”](#) on page 15.
6. Optionally, zeroize shared secrets and host keys. Refer to [“Zeroizing shared secrets and host keys”](#) on page 16.
7. Save the configuration. Refer to [“Saving the configuration”](#) on page 17.
8. Reload the device. Refer to [“Reloading the device”](#) on page 17.

Copying the signature files

Refer to the release notes for the required signature file information.

1. Place the needed signature files on an accessible SCP or TFTP server.
2. Copy the signature file from the SCP or TFTP server into flash memory by entering the following commands:

Using TFTP:

```
Brocade# copy tftp flash 10.20.90.5 FCXR07300.sig fips-primary-sig
```

Syntax: `copy tftp flash <ip-address> <filename.sig> <fips-primary-sig | fips-secondary-sig>`

Using SCP:

```
c:\>scp FCXR07300.sig fastiron@10.20.91.7:file:primary.sig
```

Syntax: `scp <signaturefilename> username@ipaddress:file:<primary.sig | secondary.sig>`

Enabling FIPS mode

1. Attach a management station (PC or terminal) to the management module serial (console) port using a serial cable.

When the device is not in a console session, FIPS-related commands return errors.

2. Verify that the device is in non-FIPS mode using the following command:

```
Brocade(config)#fips show
```

Syntax: `fips show`

The **fips show** command lists the current configuration of the device and can be run in both FIPS and non-FIPS modes to establish whether the device is truly in FIPS mode.

The output of the **fips show** command confirms that the device is in FIPS mode and identifies the device as either administratively or operationally in FIPS mode.

The following example shows the output of the **fips show** command before the **fips enable** command is entered, and administrative status is off and operational status is off:

```
Brocade(config)#fips show
FIPS mode: Administrative Status: OFF, Operational Status: OFF
```

If the device is already in administrative FIPS mode, you can modify the FIPS policy. Refer to [“Modifying the FIPS policy”](#) on page 15.

3. Use the following command to place the device administratively in FIPS mode:

```
Brocade(config)# fips enable
```

Syntax: [no] fips enable

The following example shows the output of the **fips enable** command on a FastIron device:

```
Brocade(config)# fips enable
This device is now running in FIPS administrative mode.
At this time you can alter this system's FIPS default security policy
and then enter FIPS operational mode.
```

Note: Making changes to the default FIPS security policy weakens the security of the device and makes the device non-compliant with FIPS 140 Level 2. The default security policy defined in the FIPS Security Policy Document ensures that the device complies with all FIPS 140-2 specifications. Commands to alter the default security policy are available to the crypto-officer; however, Brocade does not recommend making changes to the default security policy at any time.

=====

To enter FIPS mode, complete the following steps:

1. Install the signature file now if not already done. Failure to install signature or wrong signature file can cause continuous resets
Also Optionally, configure FIPS policy commands that meets your network requirements. You must explicitly configure the following services if you want to use them when the device is operational in FIPS mode:
 - Allow TFTP access.
Current status: Disabled
 - Allow SNMP Access to the Critical Security Parameter (CSP) MIB objects.
Current status : Disabled
 - Allow access to all commands within the monitor mode.
Current status: Disabled
 - Retention of shared secret keys for all protocols and the host passwords.
Current status: Clear
 - Retention of SSH DSA host keys.
Current status: Clear
 - Retention the SSH RSA host keys and HTTPS certificate.
Current status: Clear

2. Enter the "fips zeroize all" command, which zeroes out the shared secrets

Placing the device in FIPS mode

used by various networking protocols, including the host access passwords, SSH and HTTPS host-keys with the digital signature based on the configured FIPS Security Policy.

3. Save the running configuration.
4. Reload the device.
5. Enter the "fips show" command to verify that the device entered FIPS operational mode.

=====

The system will disable the following services or commands after reload:

1. Telnet server will be disabled. The "telnet server" command will be removed.
2. AAA authentication for the console will be disabled to allow console access after reload in FIPS mode. The "enable aaa console" command will be removed.
3. SCP will be enabled. The "ip ssh scp disable" command will be removed.
4. HTTP server will be disabled. The "web-management http" command will be removed.
5. HTTPS server will change as follows:
 - SSL 3.0 will be disabled.
 - TLS version 1.0 and greater will be used.
 - RC4 cipher will be disabled.
 - Passwords will be required; the "web-management allow-no-password" command will be removed.

Please see FIPS config guide for complete details.

4. You can verify the status of the device as administratively in FIPS mode by using the **fips show** command.

The following example shows the output of the **fips show** command on a FastIron device after the **fips enable** command is entered and administrative status is on and operational status is off:

```
Brocade# fips show
FIPS mode: Administrative status ON: Operational status OFF
Some shared secrets inherited from non-fips mode may
not be fips compliant and has to be zeroized
(output truncated)
```

5. You can use the **no web-management hp-top-tools** command to disable the TCP port 280 that allows access to the device by HP ProCurve Manager. See FastIron Configuration Guide for more details.

Perform a FIPS self-test

Use FIPS self-test to verify the sanity of FIPS software. For more information on the FIPS self-test, refer to ["Running FIPS self-test"](#) on page 18.

1. From Privileged EXEC level of the CLI on the console, execute fips self-test to verify that the FIPS Software and Firmware Integrity Test passes:

Syntax: fips self-tests

2. If the test fails, make sure that the correct signature file was copied for the correct image file and version, and recopy as needed.

The following examples shows the FIPS Software and Firmware Integrity Test as passed:

```
Brocade#fips self-tests
```

```
Running FIPS Power on Self Tests.....PASSED
....
....
....
```

NOTE

This check must pass before saving the configuration and reloading the device.

Modifying the FIPS policy

After the device is administratively in FIPS mode, you can modify the default FIPS policy.

NOTE

Making changes to the default FIPS policy on the device is not recommended and weakens the security of the device. Any modification of the default FIPS policy places the device in a state that is not in compliance with FIPS 140-2.

The output of the **fips enable** command displays which protocols that constitute the FIPS policy are set in compliance with FIPS standards by default and can be adjusted to set a more flexible policy. The remaining protocols that constitute the FIPS policy are set to the appropriate status automatically during reload due to the **fips enable** command. The default FIPS policy is detailed in this chapter's overview. Refer to [“Overview”](#) on page 1.

When you make no changes to the FIPS policy, the default FIPS policy is applied on the device and the device operates in strict FIPS mode upon reload, in full compliance with FIPS 140-2 specifications.

To set a more flexible FIPS policy on the Brocade device, use the following commands as desired to modify the default FIPS policy.

- Allow TFTP access:

```
Brocade(config)# fips policy allow tftp-access
```

Syntax: **[no] fips policy allow tftp-access**

- Allow SNMP access to the Critical Security Parameter (CSP) MIB objects:

```
Brocade(config)# fips policy allow snmp-csp-access
```

Syntax: **[no] fips policy allow snmp-csp-access**

- Allow access to monitor mode for debugging both from application and from boot prompts:

```
Brocade(config)# fips policy allow monitor-full-access
```

Syntax: **[no] fips policy allow monitor-full-access**

- Retain the shared secret keys for all protocols and the host passwords:

```
Brocade(config)# fips policy retain shared-secrets
```

Syntax: **[no] fips policy retain shared-secrets**

- Retain the SSH DSA host keys:

```
Brocade(config)# fips policy retain dsa-host-keys
```

Syntax: **[no] fips policy retain dsa-host-keys**

- Retain the HTTPS RSA host keys and the HTTPS Server digital certificate:

```
Brocade(config)# fips policy retain rsa-host-keys
```

Syntax: [no] fips policy retain rsa-host-keys

Zeroizing shared secrets and host keys

After you have reviewed the FIPS policy, use the following command to zeroize the shared secrets and host keys used by various networking protocols.

```
Brocade# fips zeroize all
```

Syntax: [no] fips zeroize all | shared-secret | host-keys

The **all** option zeroizes all shared secrets and host keys. The **shared-secret** option zeroizes shared secret keys only. The **host-keys** option zeroizes host keys only.

For example, entering the **fips zeroize shared-secret** zeroizes only the shared secret keys of various networking protocols and host access passwords.

NOTE

This command may cause operational failure within networking protocols using shared secrets and should be used with careful consideration.

The default FIPS policy calls for the zeroization of all keys using the **fips zeroize all** command option. When you apply a less strict FIPS policy than the default, zeroize at your discretion.

NOTE

The **fips zeroize all** option zeroizes all keys irrespective of the configured FIPS policy.

[Table 3](#) lists the various keys used in the system that are zeroized in compliance with FIPS.

TABLE 3 Key zeroization

Keys used	Command option handling
DH Private Keys	Host-keys
FCSP Challenge Handshake Authentication Protocol (CHAP) Secret	Host-keys
SSH Session Key	Host-keys
SSH RSA Private Key	Host-keys
RNG Seed key	N/A
Passwords	Shared-secret
TLS Private Key	Host-keys
TLS pre-master secret	Host-keys
TLS session key	Host-keys
TLS authentication key	Host-keys

TABLE 3 Key zeroization

Keys used	Command option handling
RADIUS, TACACS+ secret	Shared-secret
Authentication passwords for various networking protocols	Shared-secret

Saving the configuration

After zeroizing, use the **write memory** command to save the configuration.

```
Brocade(config)# write memory
```

Syntax: **write memory**

NOTE

Keep a backup copy of the startup configuration in the event of system reset.

Reloading the device

NOTE

Before upgrading to a new image in FIPS mode, ensure that the corresponding signature file is available in the flash.

After you have saved the configuration, reload the device using the **reload** command:

```
Brocade# reload
```

Syntax: **reload**

Various tests, including Power-On Self Tests (POSTs) and Known Answer Tests (KATs), are run by the Brocade device during reload, during the transition between non-FIPS and FIPS mode.

POSTs check for the consistency of the FIPS approved algorithms implemented on the device.

KATs are used to exercise various features of FIPS-approved algorithms.

All interfaces on the device are down until the tests are completed successfully.

Possible POST failure messages indicating that the tests did not pass successfully include:

```
Crypto module initialization and KNown Answer Test (KAT) failed with reason:(Error Code 0x80000000)'CKR_VENDOR_DEFINED'
```

```
FIPS: Primary image verification failed
```

```
FIPS: Secondary image verification failed
```

After all tests are completed successfully, the device reloads in FIPS mode and FIPS mode is successfully enabled and operational on the Brocade device.

NOTE

Due to FIPS functionality, the device has changed to more secure both in and out of FIPS mode. As a result, boot time is slower upon reload for all FastIron devices release 7.2.01a and later.

You can verify the status of the device as operationally in FIPS mode by using the **fips show** command.

```
Brocade(config)# fips show
```

Syntax: fips show

The following is the output of the **fips show** command after the device reloads successfully in the default strict FIPS mode and administrative status is on and operational status is on:

```
Brocade(config)# fips show
FIPS mode: Administrative Status: ON, Operational Status: ON
System Specific:
OS monitor mode access: enabled

Management Protocol Specific:
Telnet server: disabled
TFTP Client: disabled
HTTPS SSL 3.0: disabled
SNMP Access to security objects: enabled

Critical Security Parameter Updates across FIPS Boundary:
Protocol shared secret and host passwords: clear
SSH DSA Host Keys: clear
HTTPS RSA Host Keys and Signature: Clear
```

Running FIPS self-test

Use the following command either in FIPS or non-FIPS mode to run the Known Answer Tests (KATs) and conditional tests on demand in both FIPS and non-FIPS mode:

```
Brocade(config)# fips self-test
```

Syntax: fips self-test

The following log message is only outputted to the console terminal and no trap messages are generated as the system is not fully operational when this event happens:

```
"Crypto module initialization and Known Answer Test (KAT) passed".
```

Disabling FIPS mode



CAUTION

After enabling the FIPS mode on your device, you cannot disable it without losing the device configuration. For disabling the FIPS mode, it is recommended that you contact Brocade Technical Support and perform the procedure under qualified guidance.

While a FIPS-supported image is running on the device, at any given time, the image can be running in FIPS or non-FIPS operational mode. When changing between modes, the SSH host-keys is lost because the FIPS-supported image saves the host keys in the flash as a file, but the downgraded non-FIPS image stores host keys in the backplane EEPROM. Also, in addition to SSH host-keys, moving from FIPS mode to non-FIPS mode clears all shared-secret passwords (including any MD5 passwords).

To place a device in non-FIPS mode and then use TFTP or SCP to download and initialize an older image, perform the following steps:

1. Logon to the device by entering your user name and password.
2. Disable FIPS by entering the **no fips enable** command at the prompt.
3. To copy the desired non-FIPS binary image into flash, enter the following command:

Syntax: copy tftp image <ip-address> <image-name>

NOTE

The device will perform a checksum validation on the newly downloaded image because the currently running image does not support FIPS and does not require a signature file.

4. Run the **Reload** command to reload the device.

Troubleshooting a failed software image installation in FIPS mode

In FIPS mode, firmware verification for a specified signature occurs during system initialization. If the verification fails, the following actions occur:

1. The system fails to initialize.
2. A log message appears on the console.
3. The device begins a self-reload.

You can interrupt a reload to recover and install another image from the TFTP server at the boot loader prompt.

NOTE

You cannot copy a signature file from the boot loader prompt. Before attempting recovery through boot loader prompt, you must ensure that the correct signature file is already loaded.

1. Reboot the device and press 'b' to enter the boot loader prompt.
2. Do the following to configure the network setting in boot loader:

```
Brocade-boot>> setenv ipaddr A.B.C.D
Brocade-boot>> setenv gatewayip W.X.Y.Z
Brocade-boot>> setenv netmask E.F.G.H
Brocade-boot>> saveenv
```

NOTE

The IP address A.B.C.D must be different from the management IP address of the switch.

3. Configure FastIron image name and upgrade primary or secondary image:

```
Brocade-boot>> setenv image_name <path/filename>
Brocade-boot>> saveenv
```

Troubleshooting a failed software image installation in FIPS mode

```
Brocade-boot>> update_primary  
OR  
Brocade-boot>> update_secondary
```