Brocade® FCX 624/648, ICX™ 6610, ICX 6450, ICX 6650 and SX 800/1600 Series with IronWare R08.0.01 Firmware

FIPS 140-2 Non-Proprietary Security Policy

Level 2 with Design Assurance Level 3 Validation

Document Version 1.0

June 27, 2014

Revision History

Revision Date	Revision	Summary of Changes
6/27/2014	1.0	Initial draft

1 Introduction

The Brocade FastIron SX and Brocade FCX switches are part of Brocade's FastIron L2/L3 switch family. They are designed for medium to large enterprise backbones. The FastIron SX series chassis devices are modular switches that provide the enterprise network with a complete end-to-end Enterprise LAN solution, ranging from the wiring closet to the LAN backbone. The FCX series is an access layer Gigabit Ethernet switch designed from the ground up for the enterprise data center environment. When these switches are stacked, they appear as one switch, reducing management up to 8 times.

Brocade ICX 6610 series stackable switches are part of Brocade's ICX 6610 product family. They are designed for medium to large enterprise backbones. The ICX 6610 series is an access layer Gigabit Ethernet switch designed from the ground up for the enterprise data center environment.

Brocade ICX 6450 switches provide enterprise-class stackable LAN switching solutions to meet the growing demands of campus networks. Designed for small to medium-size enterprises, branch offices, and distributed campuses, these intelligent, scalable edge switches deliver enterprise-class functionality without compromising performance and reliability.

The Brocade ICX 6650 Switch is a compact Ethernet switch that delivers industry-leading 10/40 GbE density, unmatched price/performance, and seamless scalability for the ultimate investment protection. Designed for demanding data center Top-of-Rack (ToR) environments and campus LAN aggregation deployments requiring cost-effective connectivity, the Brocade ICX 6650 offers flexible Ports on Demand (PoD) licensing for non-disruptive pay-as-you-grow scalability.

2 Overview

The FIPS 140-2 validation includes the thirty-eight (38) hardware devices running the firmware version presented in Table 1, Table 2, Table 5, Table 6, and Table 7. Table 8 lists the devices included in this validation.

Table 2 lists the six (6) Brocade FCX 624 series and FCX 648 series devices, referred collectively for the remainder of this document as FCX 624/648 device (cryptographic module, or simply the module). Each FCX 624/648 device is a fixed-port switch, which is a multi-chip standalone cryptographic module. The power supplies, fan tray assemblies and 2X10G Ethernet uplink module (FCX-2XG) are part of the cryptographic boundary and can be replaced in the field. An unpopulated FCX-2XG slot is covered by an opaque bezel which is part of the cryptographic boundary. For each module to operate in a FIPS Approved mode of operation, the tamper evident seals, supplied in FIPS Kit (Part Number: Brocade XBR-000195) must be installed, as defined in Appendix A.

Table 5 lists the ten (10) Brocade ICX 6610 series devices, referred collectively for the remainder of this document as ICX 6610 device (cryptographic module, or simply the module). Each ICX 6610 device is a fixed-port switch, which is a multi-chip standalone cryptographic module. The installed fans either use a push or pull configuration to move the air between the back and front of the device. Each model is orderable with either fan trays or power supply side intake (-I) or power supply side exhaust (-E) airflow, therefore two SKUs per module is listed in Table 5. The power supplies and fan tray assemblies are part of the cryptographic boundary and can be replaced in the field. Unpopulated power supplies and fan trays are covered by opaque bezels, which are part of the cryptographic boundary when the secondary redundant power supplies and/or fans trays are not used. The cryptographic boundary for each ICX 6610 device is represented by the opaque enclosure (including the power supply, fan tray and bezels) with removable cover. For each module to operate in a FIPS approved mode of operation, the tamper evident seals, supplied in FIPS Kit (Part Number: Brocade XBR-000195) must be installed, as defined in Appendix A.

Table 6 lists the five (5) Brocade ICX 6450 series devices, referred collectively for the remainder of this document as ICX 6450 device (cryptographic module, or simply the module). Each ICX 6450 device is a fixed-port switch, which is a multi-chip standalone cryptographic module. The power supplies and fan tray assemblies are part of the cryptographic boundary and cannot be replaced in the field. The cryptographic boundary for each ICX 6450 device is represented by the opaque enclosure (including the power supply, fan tray and bezels) with removable cover. For each module to operate in a FIPS Approved mode of operation, the tamper evident seals, supplied in FIPS Kit (Part Number: Brocade XBR-000195) must be installed, as defined in Appendix A.

Table 7 lists the ten (10) Brocade ICX 6650 series devices, referred collectively for the remainder of this document as ICX 6650 device (cryptographic module, or simply the module). Each ICX 6650 device is a fixed-port switch, which is a multi-chip standalone cryptographic module. The installed fans either use a push or pull configuration to move the air between the back and front of the device. Each model is orderable with either fan trays or power supply side intake (-I) or power supply side exhaust (-E) airflow, therefore two SKUs per module is listed in Table 7. The power supplies and fan tray assemblies are part of the cryptographic boundary and can be replaced in the field. Unpopulated power supplies and fan trays are covered by opaque bezels, which are part of the cryptographic boundary when the secondary redundant power supplies and/or fans trays are not used. The cryptographic boundary for each ICX 6650 device is represented by the opaque enclosure (including the power supply, fan tray and bezels) with removable cover. For each module to operate in a FIPS approved mode of operation, the tamper evident seals, supplied in FIPS Kit (Part Number: Brocade XBR-000195) must be installed, as defined in Appendix A.

Table 8 lists the IronWare SX800 and two (2) SX1600 series devices, referred collectively for the remainder of this document as SX800/1600 device (cryptographic module, or simply the module). Each SX800/1600 device is a chassis based switch, which is a multi-chip standalone cryptographic module. The field replaceable power supplies are not part of the cryptographic boundary. The fan tray assemblies are part of the cryptographic boundary and can be replaced in the field. Unpopulated management module, switch fabric module and port blade modules slots are covered by opaque bezels. The cryptographic boundary for each SX800/1600 device is represented by the opaque enclosure (including the management modules, switch fabric modules, fan trays and bezels) with a removable cover. For each module to operate in a FIPS approved mode of operation, the tamper evident seals, supplied in FIPS Kit (Part Number: Brocade XBR-000195) must be installed, as defined in Appendix A.

3 IronWare Firmware

The ICX 6610 series (listed in Table 5 ICX 6610 Switch Family Part Numbers) run the same firmware version that includes the cryptographic functionality described on page 24. The “–I” and “–E” designations in Table 2 define the airflow direction as either intake or exhaust. The “-24” and “-48” designations in Table 2 define the port count, and the designator “P” following the port count indicate PoE+ ports; the designator “F” indicate Small Form-Factor Pluggable (SFP) ports, per Table 16 ICX 6610 Series Physical Ports. Otherwise, devices with similar SKUs are identical.

Table 1 Firmware Version

Firmware Version
IronWare R08.0.01

4 Brocade FCX 624 and FCX 648 Series

Table 2 FCX Part Numbers

SKU	MFG Part Number	Brief Description
FCX624S	80-1002388-08	24-Port 1GbE, 2X16G stackable switch
FCX624S-HPOE-ADV	80-1002715-08	24-Port 1GbE, HPOE, 2X16G stackable, ADV L3 switch
FCX624S-F-ADV	80-1002727-07	24-Port, FE/GE SFP, 2X16G stackable, ADV L3 switch
FCX648S	80-1002392-08	48-Port 1GbE, 2X16 stackable switch
FCX648S-HPOE	80-1002391-10	48-Port 1GbE, HPOE, 2x16G stackable switch
FCX648S-HPOE-ADV	80-1002716-10	48-Port 1GbE, HPOE, 2x16G stackable, ADV L3 switch
XBR-000195	N/A	FIPS Kit containing tamper evident labels to be affixed to the module per Appendix A: Tamper Label Application in this document. All SKUs listed above utilize this kit to satisfy the physical security requirements

Table 3 FCX 624 and FCX 628 Optional Component Part Numbers

SKU	MFG Part Number	Brief Description
FCX-2XG	80-1002399-01	XFP Module,Uplink,2X10G,FCX

Table 4 Validated FCX624 and FCX648 Series Configurations*

Module	Configuration 1, SKUs (Count)	Configuration 2, SKUs (Count)
FCX 624S	Base: FCX624S** Interface module: None License: None	Base: FCX624S Interface module: FCX-2XG (1) License: None
FCX 624S-HPOE-ADV	Base: FCX624S-HPOE-ADV** Interface module: None License: Advanced L3 license	Base: FCX624S-HPOE-ADV Interface module: FCX-2XG (1) License: Advanced L3 license
FCX 624S-F-ADV	Base: FCX624S-F-ADV** Interface module: None License: Advanced L3 license	Base: FCX624S-F-ADV Interface module: FCX-2XG (1) License: Advanced L3 license
FCX 648S	Base: FCX648S** Interface module: None License: None	Base: FCX624S-F-ADV Interface module: FCX-2XG (1) License: None
FCX 648S-HPOE	Base: FCX648S-HPOE** Interface module: None License: None	Base: FCX648S-HPOE Interface module: FCX-2XG (1) License: None
FCX 648S-HPOE-ADV	Base: FCX648S-HPOE-ADV** Interface module: None License: Advanced L3 license	Base: FCX648S-HPOE-ADV V Interface module: FCX-2XG (1) License: Advanced L3 license

**Note: see table 2 for MFG part numbers.

Figure 1 illustrates the FCX 624S cryptographic module.

Figure 1 FCX624S cryptographic module

Figure 2 illustrates the FCX 624S-HPOE-ADV cryptographic module.

Figure 2 FCX 624S-HPOE-ADV cryptographic module

Figure 3 illustrates the FCX 648S cryptographic module.

Figure 3 FCX 648S cryptographic module

Figure 4 illustrates the FCX 648S-HPOE and FCX 648S-HPOE-ADV cryptographic module.

Figure 4 FCX 648S-HPOE and FCX 648-HPOE-ADV cryptographic module

Figure 5 illustrates the FCX 624S-F-ADV cryptographic module.

Figure 5 FCX 624S-F-ADV cryptographic module

***Note:** The following SKUs are physically equivalent to the FCX 624S, FCX 624S-F, and the FCX 648S:
FCX 624S-HPOE-ADV
FCX 624S-F-ADV
FCX 648S-HPOE
FCX 648S-HPOE-ADV

5 ICX6610 Series

Table 5 ICX 6610 Switch Family Part Numbers of Validated Cryptographic Modules

SKU	MFG Part Number	Brief Description
ICX 6610-24F-I	80-1005350-04	Stackable switch with 24 100/1000 Mbps Small Form-Factor Pluggable (SFP) ports, power supply side intake airflow ("-I" in the SKU)
ICX 6610-24F-E	80-1005345-04	Stackable switch with 24 100/1000 Mbps Small Form-Factor Pluggable (SFP) ports, power supply side exhaust airflow ("-E" in the SKU)
ICX 6610-24-I	80-1005348-05	Stackable switch with 24 10/100/1000 Mbps RJ-45 ports, power supply side intake airflow ("-I" in the SKU)
ICX 6610-24-E	80-1005343-05	Stackable switch with 24 10/100/1000 Mbps RJ-45 ports, power supply side exhaust airflow ("-E" in the SKU)
ICX 6610-24P-I	80-1005349-06	Stackable switch with 24 10/100/1000 Mbps RJ-45 PoE+ ports, power supply side intake airflow ("-I" in the SKU)
ICX 6610-24P-E	80-1005344-06	Stackable switch with 24 10/100/1000 Mbps RJ-45 PoE+ ports, power supply side exhaust airflow ("-E" in the SKU)
ICX 6610-48-I	80-1005351-05	Stackable switch with 48 10/100/1000 Mbps RJ-45 ports, power supply side intake airflow ("-I" in the SKU)
ICX 6610-48-E	80-1005346-05	Stackable switch with 48 10/100/1000 Mbps RJ-45 ports, power supply side exhaust airflow ("-E" in the SKU)
ICX 6610-48P-I	80-1005352-06	Stackable switch with 24 10/100/1000 Mbps RJ-45 PoE+ ports, power supply side intake airflow ("-I" in the SKU)
ICX 6610-48P-E	80-1005347-06	Stackable switch with 24 10/100/1000 Mbps RJ-45 PoE+ ports, power supply side exhaust airflow ("-E" in the SKU)
XBR-000195	N/A	FIPS Kit containing tamper evident labels to be affixed to the module per Appendix A: Tamper Label Application in this document. All SKUs listed above utilize this kit to satisfy the physical security requirements

Figure 6 illustrates the ICX 6610-24 and ICX 6610-24P cryptographic modules (See Table 5 ICX 6610 Switch Family Part Numbers).

Figure 6 ICX 6610-24 and ICX 6610-24P cryptographic modules

modules (See Table 5 ICX 6610 Switch Family Part Numbers).

Figure 7 illustrates the ICX 6610-48 and ICX 6610-48P cryptographic modules (See Table 5 ICX 6610 Switch Family Part Numbers).

Figure 7 ICX 6610-48 and ICX 6610-48P cryptographic modules

Figure 8 illustrates the ICX 6610-24F cryptographic modules (See Table 5 ICX 6610 Switch Family Part Numbers).

Figure 8 ICX 6610-24F cryptographic module

6 ICX 6450 Series

Table 6 ICX 6450 Switch Family Part Numbers of Validated Cryptographic Modules

SKU	MFG Part Number	Brief Description
ICX 6450-24	80-1005997-03	24-port 1G Switch, 2x1G SFP+ (upgradable to 10G) & 2x1G/10G SFP+ Uplink/Stacking Ports
ICX 6450-24P	80-1005996-04	24-port 1G Switch PoE+ 390W, 2x1G SFP+ (upgradable to 10G) & 2x1G/10G SFP+ Uplink/Stacking Ports
ICX 6450-48	80-1005999-04	48-port 1G Switch, 2x1G SFP+ (upgradable to 10G) & 2x1G/10G SFP+ Uplink/Stacking Ports
ICX 6450-48P	80-1005998-04	48-port 1G Switch PoE+ 780W, 2x1G SFP+ (upgradable to 10G) & 2x1G/10G SFP+ Uplink/Stacking Ports
ICX 6450-C12-PD	80-1007578-01	12-port 1G Compact Switch (4 PoE+), 2X100M/1G SFP, 2X100M/1G Copper Uplinks, Fanless, Layer 3
XBR-000195	N/A	FIPS Kit containing tamper evident labels to be affixed to the module per Appendix A: Tamper Label Application in this document. All SKUs listed above utilize this kit to satisfy the physical security requirements

Figure 9 illustrates the ICX 6450-24 and ICX 6450-24P cryptographic module (See Table 5 ICX 6610 Switch Family Part Numbers)

Figure 9 ICX 6450-24 and ICX 6450-24P cryptographic modules

Figure 10 illustrates the ICX 6450-48 and ICX 6450-48P cryptographic modules (See Table 5 ICX 6610 Switch Family Part Numbers).

Figure 10 ICX 6450-48 and ICX 6450-48P cryptographic modules

Figure 11 ICX 6450-C12-PD cryptographic modules

7 ICX 6650 Series

Table 7 ICX 6650 Switch Family Part Numbers of Validated Cryptographic Modules

SKU	MFG Part Number	Brief Description
ICX6650-32-E-ADV	80-1007115-02	Brocade ICX6650 with 32 10GbE SFP+ ports enabled. Includes two 250W AC power supplies and two fan units with exhaust airflow.
ICX6650-32-I-ADV	80-1007116-02	Brocade ICX6650 with 32 10GbE SFP+ ports enabled. Includes two 250W AC power supplies and two fan units with intake airflow.
ICX6650-40-E-ADV	80-1007179-03	Brocade ICX6650 with 32 10GbE SFP+ ports enabled and POD license for 8 10GbE SFP+ ports. Includes two 250W AC power supplies and two fan units with exhaust airflow.
ICX6650-40-I-ADV	80-1007181-03	Brocade ICX6650 with 32 10GbE SFP+ ports enabled and POD license for 8 10GbE SFP+ ports. Includes two 250W AC power supplies and two fan units with intake airflow.
ICX6650-48-E-ADV	80-1007180-03	Brocade ICX6650 with 32 10GbE SFP+ ports enabled and POD license for 16 10GbE SFP+ ports. Includes two 250W AC power supplies and two fan units with exhaust airflow.
ICX6650-48-I-ADV	80-1007182-03	Brocade ICX6650 with 32 10GbE SFP+ ports enabled and POD license for 16 10GbE SFP+ ports. Includes two 250W AC power supplies and two fan units with intake airflow.
ICX6650-56-E-ADV	80-1007117-03	Brocade ICX6650 with 32 10GbE SFP+ ports enabled and POD license for 24 10GbE SFP+ ports. Includes two 250W AC power supplies and two fan units with exhaust airflow.
ICX6650-56-I-ADV	80-1007118-03	Brocade ICX6650 with 32 10GbE SFP+ ports enabled and POD license for 24 10GbE SFP+ ports. Includes two 250W AC power supplies and two fan units with intake airflow.
ICX6650-80-E-ADV	80-1007119-03	Brocade ICX6650 with 32 10GbE SFP+ ports enabled, POD licenses for 24 10GbE SFP+ ports, and for 6 QSPF+ ports (24x10GbE, and 4 x40GbE). Includes two 250W AC power supplies and two fan units with exhaust airflow.
ICX6650-80-I-ADV	80-1007120-03	Brocade ICX6650 with 32 10GbE SFP+ ports enabled, POD licenses for 24 10GbE SFP+ ports, and for 6 QSPF+ ports (24x10GbE, and 4 x40GbE). Includes two 250W AC power supplies and two fan units with intake airflow.
XBR-000195	N/A	FIPS Kit containing tamper evident labels to be affixed to the module per Appendix A: Tamper Label Application in this document. All SKUs listed above utilize this kit to satisfy the physical security requirements.

Figure 12 illustrates the ICX 6650 cryptographic modules (See Table 7 ICX 6650 Switch Family Part Numbers).

Figure 12 ICX 6650 cryptographic module

8 SX 800 and SX 1600 Series

Each FI-SX800-S, FI-SX1600-AC and FI-SX1600-DC device validated within this implementation includes the following SX components: SX-FISF and SX-FIZMR-XL or SX-Fi-ZMR-XL-PREM6

Table 8 FastIron SX Part Numbers

SKU	MFG Part Number	Brief Description
FI-SX800-S	80-1003050-03, 80-1007143-03	FastIron SX800 CHASSIS
FI-SX1600-AC	80-1002764-02, 80-1007137-02	FastIron SX1600, 16 slot, 2 SX-FISF, 2 AC Power Supplies
FI-SX1600-DC	80-1003005-02, 80-1007138-02	FastIron SX1600, 16 slot, 2 SX-FISF, 2 DC Power Supplies

Table 9 Components of the SX 800 and SX 1600

SKU	MFG Part Number	Brief Description
SX-FISF	80-1002957-03	Switch Fabric module for the FI SX800 & FI SX1600
SX-FI-ZMR-XL	80-1006486-02	FastIron SX XL management module, No 10G ports
SX-FI-ZMR-XL-PREM6	80-1007350-02	FastIron SX XL management module, No 10G ports, support for IPv4 and IPv6 routing, SW-SX-FIL3U-6-IPV6 license
SX-ACPWR-SYS	80-1003883-02	FSX AC 90-240 VAC SYSTEM POWER SUPPLY
SX-DCPWR-SYS	80-1003886-02	FSX DC SYSTEM POWER SUPPLY

Table 10 Validated SX800 Series Configurations

Module	Configuration 1, SKUs (Count)	Configuration 2, SKUs (Count)
SX 800 (with AC power)	Base: FI-SX800-S* Management module: SX-FI-ZMR-XL (2) Switch Fabric: SX-FISF (2) License: None Power Supply: SX-ACPWR-SYS (1)	Base: FI-SX800-S Management module: SX-FI-ZMR-XL-PREM6 (2) Switch Fabric: SX-FISF (2) License: SW-SX-FIL3U-6-IPV6 Power Supply: SX-ACPWR-SYS (1)
SX 800 (with DC power)	Base: FI-SX800-S* Management module: SX-FI-ZMR-XL (2) Switch Fabric: SX-FISF (2) License: None Power Supply: SX-DCPWR-SYS (1)	Base: FI-SX800-S Management module: SX-FI-ZMR-XL-PREM6 (2) Switch Fabric: SX-FISF (2) License: SW-SX-FIL3U-6-IPV6 Power Supply: SX-DCPWR-SYS (1)

*Note: See Table 8 for MFG Part Numbers

Table 11 Validated SX1600 Series Configurations

Model	Configuration 1, SKUs (Count)	Configuration 2, SKUs (Count)
SX 1600 (with AC power)	Base: FI-SX1600-AC* Management module: SX-FI-ZMR-XL (2) Switch Fabric: SX-FISF (2) License: None Power Supply: SX-ACPWR-SYS (2)	Base: FI-SX1600-AC Management module: SX-FI-ZMR-XL-PREM6 (2) Switch Fabric: SX-FISF (2) License: SW-SX-FIL3U-6-IPV6 Power Supply: SX-ACPWR-SYS (2)
SX 1600 (with DC power)	Base: FI-SX1600-DC* Management module: SX-FI-ZMR-XL (2) Switch Fabric: SX-FISF (2) License: None Power Supply: SX-DCPWR-SYS (2)	Base: FI-SX1600-DC Management module: SX-FI-ZMR-XL-PREM6 (2) Switch Fabric: SX-FISF (2) License: SW-SX-FIL3U-6-IPV6 Power Supply: SX-DCPWR-SYS (2)

*Note: See Table 8 for MFG Part Numbers.

Figure 13 illustrates the FI-SX800 cryptographic module.

Figure 14 illustrates the FI-SX1600 cryptographic module.

9 Ports and Interfaces

9.1 FCX 624 and FCX 648 Series

Each FCX 624/648 device provides network ports, management connectors, and status LED. This section describes the physical ports and the interfaces that provide for Data Input, Data Output, Control Input, and Status Output.

While not part of this validation, the FCX 624/648 devices provide a range of physical network ports. The series supports both copper and fiber connectors with some models supporting combination ports. All models within the scope of this evaluation support 10G uplink ports for stacking devices. All models have an out-of-band management port and a console management port (Gigabit Ethernet RJ-45 connector and serial connector, respectively).

Table 12 summarizes the physical ports provided by FCX 624/648 devices. Table 13 shows the correspondence between the physical interfaces of a FCX 624/648 device and the logical interfaces defined in FIPS 140-2.

Table 12 FCX 624/648 Port mapping to logical interface

Physical Port	Logical Interface
SFP ports	Data input/Data output, Status output
10/100/1000 Mbps RJ-45 ports	Data input/Data output, Status output
AC socket	Power
Out of band management port	Control input, Status output
Console Port	Control input, Status output
Reset	Control input
LED	Status output

Table 13 FCX 624/648 Series Physical Port LED Status

LED	Condition	Status
Ethernet Ports 24-port and 48-port models	On (Flashing Green)	The port has established a valid link at 1000 Mbps. Flashing indicates the port is transmitting and receiving user packets.
	On (Flashing Amber)	The port has established a valid link at 10 or 100 Mbps. Flashing indicates the port is transmitting and receiving user packets.
	Off	A link is not established with a remote port.
HPOE 24-port and 48-port models	On (Green)	The port is providing HPOE power to a connected device.
	Off	The port is not providing HPOE power.
SFP (Link LED)	On (Flashing Green)	The SFP port has established a valid link. Flashing indicates that the port is transmitting and receiving user packets.
	Off	A link is not established with a remote port.
SFP (Speed LED)	On (Green)	The SFP port is operating at 1000 Mbps.
	On (Amber)	The SFP port is operating at 100 Mbps.
		A link is not established with a remote port.

Table 14 FCX 624/648 Series System LED Status

LED	Condition	Status
PS1	On (Green)	Power supply is operating normally.
	On (Amber)	Power supply fault detected.
	Off	Power supply is off or experience a system failure.
PS2	On (Green)	Power supply is operating normally.
	On (Amber)	Power supply fault detected.
	Off	Power supply is off or experience a system failure.
Diag (Diagnostic)	On (Flashing Green)	System self-diagnostic test is in progress.
	On (Green)	System self-diagnostic test successfully completed.
	On (Amber)	System self-diagnostic test detected a fault.
A (Active)	On (Green)	The device is the active controller.
	On (Amber)	The device is the standby controller.
	Off	The device is operating as a stack member or is in standalone mode.
S (Standby)	On (Green)	The device is the active controller.
	On (Amber)	The device is the standby controller.
	Off	The device is operating as a stack member or is in standalone mode.
Up link	On (Green)	Up link is operating properly.
	Off	Up link has failed or there is no link.
Down Link	On (Green)	Down link is operating properly.
	Off	Down link has failed or there is no link.
Stack ID (1-8)	On (Green)	Indicates the device stack ID.

Table 15 FCX 624/648 Series Power Module LED Status

LED	Condition	Status
DC OK	On (Green)	DC output OK.
	On (Red)	DC output failure.
AC OK	On (Green)	AC input OK.
	On (Red)	AC input failure.

9.2 ICX 6610 Series

Each ICX 6610 device provides network ports, management connectors, and status LED. This section describes the physical ports and the interfaces that provide for Data Input, Data Output, Control Input, and Status Output.

Though not part of this validation, the ICX 6610 devices provide a range of physical network ports. The series supports both copper and fiber connectors with some models supporting combination ports. Some models support uplink ports for stacking devices. Most models have an out-of-band management port and a console management port (Gigabit Ethernet RJ-45 connector and serial connector, respectively).

Table 16 and Table 17 summarize the network ports provided by each ICX 6610 model. Table 17 shows the correspondence between the physical interfaces of ICX 6610 devices and the logical interfaces defined in FIPS 140-2.

Table 16 ICX 6610 Series Physical Ports

Model	Dual-mode 1 GbE/10 GbE SFP/SFP+ ports	10/100/1000 Mbps RJ-45 ports	1 GbE SFP ports	40 Gbps high-performance QSFP stacking ports1	AC inlet2	Reset	Out of band management ports	LEDs												
								Ethernet		PoE+		SFP/SFP+	System Status							
								Speed	Status	Speed	Status		PSU1	PSU2	DIAG	XL1	XL6	MS	XL2-XL5	XL7-XL10	Stack ID3
ICX 6610-24F-I, ICX 6610-24F-E	8	N/A	24	4	2	1	2	NA	NA	NA	NA	40	1	1	1	1	1	1	1	1	10
ICX 6610-24-I, ICX 6610-24-E	8	24	NA	4	2	1	2	24	24	NA	NA	8	1	1	1	1	1	1	1	1	10
ICX 6610-24P-I, ICX 6610-24P-E	8	24	NA	4	2	1	2	NA	NA	24	24	8	1	1	1	1	1	1	1	1	10
ICX 6610-48-I, ICX 6610-48-E	8	48	NA	4	2	1	2	48	48	NA	NA	8	1	1	1	1	1	1	1	1	10
ICX 6610-48P-I, ICX 6610-48P-E	8	48	NA	4	2	1	2	NA	NA	48	48	8	1	1	1	1	1	1	1	1	10

Table 17 ICX 6610 Port mapping to logical interface

Physical Port	Logical Interface
Dual-mode 1 GbE/10 GbE SFP/SFP+ ports	Data input/Data output, Status output
10/100/1000 Mbps RJ-45 ports	Data input/Data output, Status output
1 GbE SFP ports	Data input/Data output, Status output
40 Gbps high-performance QSFP stacking ports	Data input/Data output, Status output
AC inlet	Power
Out of band management ports	Control input, Status output
Reset	Control input
LED	Status output

9.3 ICX 6450 Series

Each ICX 6450 device provides network ports, management connectors, and status LED. This section describes the physical ports and the interfaces that provide for Data Input, Data Output, Control Input, and Status Output.

While not part of this validation, the ICX 6450 devices provide a range of physical network ports. The series supports both copper and fiber connectors with some models supporting combination ports. Some models support uplink ports for stacking devices. Most models have an out-of-band management port and a console management port (Gigabit Ethernet RJ-45 connector and serial connector, respectively).

Table 18 ICX 6450 Port mapping to logical interface

Physical Port	Logical Interface
SFP/SFP+ ports	Data input/Data output, Status output
10/100/1000 Mbps RJ-45 ports	Data input/Data output, Status output
AC socket	Power
External power supply connector (EPS) (The ICX 6450-24, ICX 6450-24P and ICX 6450-48 have one EPS connector. The ICX 6450-48P has two EPS connectors)	Power
Out of band management port	Control input, Status output
Console Port	Control input, Status output
Reset	Control input
LED	Status output

Table 19 ICX 6450 Series Physical Port LED Status

LED	Condition	Status
Ethernet Ports 24-port and 48-port models	On/Flashing Green	The port has established a valid link at 10, 100 or 1000 Mbps. Flashing indicates the port is transmitting and receiving user packets.
	Off	A link is not established with a remote port.
PoE/PoE+ 24-port and 48-port models	On/Green	The port is providing PoE or PoE+ power to a connected device.
	Off	The port is not providing PoE or PoE+ power.
SFP/SFP+ (X1 - X4) for ICX 6450 devices	On/Flashing Green	The SFP port is operating at 10 Gbps. Flashing indicates the port is transmitting and receiving user packets at 10 Gbps.
	On/Flashing Yellow	The SFP port is operating at 1 Gbps. Flashing indicates the port is transmitting and receiving user packets at 1 Gbps.
	Off	A link is not established with a remote port.
Out-of-band management port (2 LEDs)	Off (both LEDs)	Offline.
	On/Flashing (left side)	Link-up. Flashing indicates the port is transmitting and receiving user packets.
	On/Green (right side)	1 Gbps Link-up.
	Right LED off, left LED on or flashing	10/100 Mbps Link-up. Flashing indicates the port is transmitting and receiving user packets.

Table 20 ICX 6450 System LED Status

LED	Condition	Status
EPS1 and EPS2 (External Power Supply status for ICX 6450-48P devices only)	Green	EPS1 and EPS2 power supplies are operating normally.
	Yellow	EPS1 and EPS2 power supply fault.

LED	Condition	Status
	Off	EPS1 and EPS2 off or not present.
PWR (Power)	Green	Power supply is operating normally.
	Yellow	Power supply fault.
	Off	Power supply off.
Diag (Diagnostic)	Flashing Green	System self-diagnostic test in progress. System reloads automatically.
	Steady Yellow	System self-diagnostic test has detected a fault (Fan, thermal, or any interface fault). The user must reload the system.
MS (Stacking configuration)	Green	The device is the Active controller. Flashing indicates the system is initializing.
	Yellow	Indicates the device is the Standby controller. Flashing indicates the system is in Master arbitration or selection state.
	Off	Device is operating as a stack member, or is in standalone mode.
Uplink (X1 and X2 stacking port status)	Green	Uplink port is operating normally.
	Off	Uplink failed or there is not link.
Downlink (X3 and X4, stacking port status)	Green	Downlink port is operating normally.
	Off	Downlink failed or there is not link.
1-8 (Switch ID in the stack)	Green	Indicates the switch ID in the stack. For ICX 6450 devices, 1 - 8 indicates the switch ID in the stack.

9.4 ICX 6650 Series

An ICX 6650 device provides network ports, management connectors, and status LED. This section describes the physical ports and the interfaces that provide for Data Input, Data Output, Control Input, and Status Output.

While not part of this validation, the ICX 6650 devices provide a range of physical network ports. The series supports both copper and fiber connectors. The ICX 6650 device has an out-of-band management port that utilizes an RJ-45 connector. The ICX 6650 device has console port that utilizes a mini-USB connector.

Table 22 summarizes the physical ports provided by ICX 6650 devices. Table 21 shows the correspondence between the physical interfaces of an ICX 6650 device and the logical interfaces defined in FIPS 140-2.

Table 21 ICX 6650 Port mapping to logical interface

Physical Port	Logical Interface
SFP ports	Data input/Data output, Status output
QSFP ports	Data input/Data output, Status output
10/100/1000 Mbps RJ-45 ports	Data input/Data output, Status output
AC socket	Power
External power supply connector	Power
Console Port	Control input, Status output
Out of band management port	Control input, Status output
Reset	Control input
LED	Status output

Table 22 ICX 6650 Series Physical Port LED Status

LED	Condition	Status
Management Port	Flashing	There is traffic and packets are being transmitted and received.
	Steady	No traffic is being transmitted, but the link is active.
	Off	External cable is not present.
1/10 GbE Port	Steady Green	Link is up in 10 GbE mode.
	Flashing Green	There is 10 GbE activity (traffic) and packets are being transmitted or received.
	Steady Amber	Link is up in 1 GbE mode.
	Flashing Amber	There is 1 GbE activity (traffic) and packets are being transmitted or received.
40 GbE (rear port) front port LED	Off	Disabled.
	Steady Blue	Link is up in 40 GbE mode.
	Flashing Blue	Active traffic. Packets are being transmitted or received.
4x10 GbE (rear port) front port LED	Off	Disabled
	Steady Green	Link is up in 10 GbE mode.
	Flashing Green	Active traffic. Packets are being transmitted or received.

Table 23 ICX 6650 System LED Status

LED	Condition	Status
PSU1 and PSU2	Green	PSU is on and operating normally.
	Amber	PSU power supply fault.
	Off	PSU is off or not present.
Diag (Diagnostic)	Flashing Green	System self-diagnostic test in progress. System reloads automatically.
	Steady Amber	System self-diagnostic test has detected a fault.
	Steady Green	System self-diagnostic test completed successfully. Device reboots and turns the LED off.
	Off	Diagnostic is off.

9.5 SX 800 and SX 1600 Series

Each FastIron device provides network ports, management connectors, and status LED. This section describes the physical ports and the interfaces that provide for Data Input, Data Output, Control Input, and Status Output.

Though not part of this validation, the Brocade FastIron devices provide a range of physical network ports. The family supports both copper and fiber connectors with some models supporting combination ports. Some models support uplink ports for stacking devices. Most models have an out-of-band management port and a console management port (Gigabit Ethernet RJ-45 connector and serial connector, respectively).

Table 24 summarizes the physical ports provided by the SX-FI-ZMR-XL and SX-FI-ZMR-PREM6 management modules. Table 25 shows the correspondence between the physical interfaces of an SX-FI-ZMR-XL and SX-FI-ZMR-PREM6 management modules and the logical interfaces defined in FIPS 140-2. Table 26 shows the

correspondence between the physical interfaces of an SX-FISF switch fabric module and the logical interfaces defined in FIPS 140-2.

Table 24 SX-FI-ZMR-XL and SX-FI-ZMR-PREM6 Port mapping to logical interface

Physical Port	Logical Interface
10/100/1000 Mbps Ethernet Port	Data input/Data output, Status output
Console Port	Control input, Status output
USB Port	Data input/Data output
Reset	Control input
LED	Status output

Table 25 SX-FI-ZMR-XL and SX-FI-ZMR-PREM6 LED Status

LED	Condition	Status
PWR (Power)	On (Green)	Module is receiving power.
	Off	Module is not receiving power.
Active	On (Green)	The module is the active management module.
	Off	The module is not the active management module.
MGMT-Link (Right-most Ethernet port LED)	On (Green)	10/100/1000.
	Blinking	The port is transmitting and receiving traffic.
	Off	No port connection exists.
Sync-Link (Left-most Ethernet port LED)	On (Green)	Two management modules are present.
	Blinking	Active and Standby modules are syncing.
	Off	No port connection exists.

Table 26 SX-FISF Switch Fabric LED Status

LED	Condition	Status
PWR	On (Green)	Module is receiving power.
	Off	Module is not receiving power.
Active	On (Green)	The module is functioning properly.
	Off	The module is not functioning properly.

10 Modes of Operation

FCX 624/648 devices, ICX 6610 devices, ICX 6450 devices, ICX 6650 devices and SX800/1600 devices (aka Brocade cryptographic modules) have two modes of operation: FIPS Approved mode and non-Approved mode. Section 10.3 describes services and cryptographic algorithms available in FIPS Approved mode. In non-FIPS Approved mode, the module runs without these FIPS policy rules applied. Section 13.1 FIPS Approved Mode describes how to invoke FIPS Approved mode.

10.1 Module Validation Level

The module meets an overall FIPS 140-2 compliance of Security Level 2 with Design Assurance Level 3.

Table 27 ICX 6610 Security Levels

Security Requirements Section	Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)	2
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A

10.2 Roles

In FIPS Approved mode, Brocade cryptographic modules support three roles: Crypto Officer, Port Configuration Administrator, and User:

1. Crypto Officer Role (Super User): The Crypto Officer role on the device in FIPS Approved mode is equivalent to the administrator role super-user in non-FIPS mode. The Crypto Officer role has complete access to the system.
2. Port Configuration Administrator Role (Port Configuration): The Port Configuration Administrator role on the device in FIPS Approved mode is equivalent to the port-config, a port configuration user in non-FIPS Approved mode. Hence, the Port Configuration Administrator role has read-and-write access for specific ports but not for global (system-wide) parameters.
3. User Role (Read Only): The User role on the device in FIPS Approved mode has read-only privileges and no configuration mode access (user).

The User role has read-only access to the cryptographic module while the Crypto Officer role has access to all device commands. Brocade cryptographic modules do not have a maintenance interface or maintenance role.

Section 11.2 Authentication describes the authentication policy for user roles.

10.3 Services

The services available to an operator depend on the operator's role. Unauthenticated operators may view externally visible status LED. LED signals indicate status that allows operators to determine if the network connections are functioning properly. Unauthenticated operators can also perform self-tests via a power-cycle. They can also view the module status via "fips show".

For all other services, an operator must authenticate to the device as described in section 11.2 Authentication.

The following subsections describe services available to operators based on role. Each description includes lists of cryptographic functions and critical security parameters (CSP) associated with the service. "Table 28 FIPS Approved Cryptographic Functions" summarizes the available FIPS-Approved cryptographic functions. Table 29 lists cryptographic functions that are not FIPS-Approved and only allowed in non-FIPS Approved mode of operation.

Table 28 FIPS Approved Cryptographic Functions

Label	Cryptographic Function
DSA	Digital Signature Algorithm
SHS	Secure Hash Standard

Table 29 Non-Approved Cryptographic Functions only allowed in non-FIPS Approved Mode

Label	Cryptographic Functions
KW	RSA (key wrapping; key establishment methodology provides 80 bits of encryption strength; non-compliant)
DH	Diffie-Hellman (key agreement; key establishment methodology provides 80 bits of encryption strength; non-compliant)
SNMP	SNMPv3 KDF (considered as plaintext)
MD5	Message-Digest algorithm (not exposed to the operator; internal to TLS v1.0, TACACS+ and RADIUS)
KDF	SSHv2 Key Derivation Function (non-compliant) & TLSv1.0 Key Derivation Function (non-compliant)
HWRNG	Generation of seeds for DRBG
HMAC-MD5	Used to support RADIUS authentication
AES	Advanced Encryption Algorithm (non-compliant)
Triple-DES	Triple Data Encryption Algorithm (non-compliant)
HMAC	Keyed-Hash Message Authentication code (non-compliant)
DRBG	Deterministic Random Bit Generator (non-compliant)
RSA	Rivest Shamir Adleman Algorithm (non-compliant)
DSA	Digital signature generation (non-compliant)
SHA-256	SHA-256 (non-compliant)
SHA-384	SHA-384 (non-compliant)
SHA-512	SHA-512 (non-compliant)

Table 30 Non-Approved Cryptographic Functions and Protocols only allowed in non-FIPS Approved Mode

Label/Protocol	Cryptographic Functions
HTTPS Cipher Suites	RSA_WithDES_CBC_SHA (non-compliant) RSA_With3DES_EDE_CBC_SHA (non-compliant) DHE_DSSWithDES_CBC_SHA (non-compliant) DHE_DSSWith3DES_EDE_CBC_SHA (non-compliant) DHE_RSAWithDES_CBC_SHA (non-compliant) DHE_RSAWith3DES_EDE_CBC_SHA (non-compliant) RSA_Export1024WithDES_CBC_SHA (non-compliant) RSA_WithAES_128_CBC_SHA (non-compliant) RSA_WithAES_256_CBC_SHA (non-compliant) DHE_DSS_WITH_AES_128_CBC_SHA (non-compliant) DHE_RSA_WITH_AES_128_CBC_SHA (non-compliant) DHE_DSS_WITH_AES_256_CBC_SHA (non-compliant) DHE_RSA_WITH_AES_256_CBC_SHA (non-compliant)
DES	Data Encryption Standard
MD2	Message Digest 2
RC2	Ron's Cipher 2
RC4	Ron's Cipher 4
HTTP	None
SNMP (Simple Network Management Protocol v1 and v2)	None
TACACS+	HMAC-MD5
TFTP (Trivial File Transfer Protocol)	None
"Two way encryption"	None; Base64
MD5	Message Digest 5
Syslog	None
OSPF-IPSEC	IPSEC Authentication only; None
VSRP	None
VRRP/VRRP-E	None

MPLS RSVP	None
MPLS-LDP	None
MSTP	None
SNTP	None
NTP	None
FCSP	None
BGP	None
SSH	None

10.4 User Role Services

10.4.1 Console

Console connection occurs via a directly connected RS-232 serial cable. Once authenticated as the User, the module provides console commands to display information about a Brocade cryptographic module and perform basic tasks (such as pings). The User role has read-only privileges and no configuration mode access.

10.5 Port Configuration Administrator Role Services

10.5.1 Console

This service is described in Section 10.4.1 above. Console access as the Port Configuration Administrator provides an operator with the same capabilities as User Console commands plus configuration commands associated with a network port on the device. EXEC commands.

10.6 Crypto Officer Role Services

10.6.1 Console

Logging in through the CLI service is described in Section 10.4.1 above. Console commands provide an authenticated Crypto Officer complete access to all the commands within the Brocade cryptographic module. This operator can enable, disable and perform status checks. This operator can also enable any service by configuring the corresponding command.

11 Policies

11.1 Security Rules

The Brocade cryptographic module's design corresponds to the cryptographic module's security rules. This section documents the security rules enforced by the cryptographic module to implement the FIPS 140-2 Level 2 security requirements. After configuring a FastIron device to operate in FIPS Approved mode, the Crypto Officer must execute the "fips self-tests" command to validate the integrity of the firmware installed on the device. If an error is detected during the self-test, the error must be corrected prior to rebooting the device.

1) The cryptographic module provides role-based authentication.
2) Until the module is placed in a valid role, the operator does not have access to any Critical Security Parameters (CSP).
3) The cryptographic module performs the following tests:
   a) Power up Self-Tests:
      i) Cryptographic Known Answer Tests (KAT):
      (1) DSA 1024 SHA-1 KAT (Signature Verification)
      (2) SHA-1 KAT (Hashing)

      ii) Firmware Integrity Test (DSA 1024 SHA-1 Signature Verification)
      iii) If the module does not detect an error during the Power on Self-Test (POST), at the conclusion of the test, the console displays the message shown below.

      Crypto module initialization and Known Answer Test (KAT) Passed.

      iv) If the module detects an error during the POST, at the conclusion of the test, the console displays the message shown below. After displaying the failure message, the module reboots.

      Crypto Module Failed <Reason String>

   b) Conditional Self-Tests:
      i) Continuous Random Number Generator (RNG) test – N/A
      ii) Pairwise Consistency Tests - N/A
      iii) Bypass Test – N/A
      iv) Manual Key Entry Test – N/A
      v) Firmware Load Test – DSA 1024 SHA-1 (Signature Verification)

4) At any time the cryptographic module is in an idle state, the operator can command the module to perform the power-up self-test by executing the “fips self-tests” command.
5) Data output to services defined in Section 10.3 Services is inhibited during self-tests, zeroization, and error states.
6) Status information does not contain CSPs or sensitive data that if used could compromise the module.

11.1.1 FIPS Fatal Cryptographic Module Failure.

When POST is successful, the following messages will be displayed on the console:

Running fips Power on Self tests and Software/Firmware Integrity Test

fips Power on Self tests and Software/Firmware Integrity tests successful

Running continuous drbg check

Running continuous drbg check successful

Running Pairwise consistency check

RSA key pair generation succeeded

Pairwise consistency check successful

Crypto module initialization and Known Answer Test (KAT) Passed.

In order to operate a Brocade cryptographic module securely, an operator should be aware of the following rules for FIPS Approved mode of operation:

External communication channels / ports shall not be available before initialization of a Brocade cryptographic module.

11.2 Authentication

Brocade cryptographic modules support role-based authentication.

1. Line password authentication

11.2.1 Line Authentication Method

The line method uses the Telnet password to authenticate an operator.

To use line authentication, a Crypto Officer must set the Telnet password.

11.2.2 Strength of Authentication

Brocade cryptographic modules minimize the likelihood that a random authentication attempt will succeed. The module supports minimum 7 character passwords selected from the following character set: digits (Qty. 10), lowercase (Qty. 26) and uppercase (26) letters, and punctuation marks (18) in passwords. Therefore the probability of a random attempted is 1/ 80^7 which is less than 1/1,000,000.

The module enforces a one second delay for each attempted password verification, therefore maximum of 60 attempts per minute, thus the probability of multiple consecutive attempts within a one minute period is 60/80^7 which is less than 1/100,000.

Table 31 Access Control Policy and CSP access summarizes the access operators in each role have to critical security parameters. The table entries have the following meanings:

1. r – operator can read the value of the item,
2. w – operator can write a new value for the item,
3. x – operator can use the value of the item without direct access and
4. d – operator can delete the value of the item by issuing the command *fips zeroize all*.

Table 31 Access Control Policy and CSP access

	User	Port Configuration Administrator	Crypto Officer
Services	Console	Console	Console
User Password	x		xrwd
Port Configuration Administrator Password		x	xrwd
Crypto Officer Password			xrwd
Firmware Integrity / Firmware Load DSA Public Key			xrwd

12 Physical Security

In order for a FCX 624/648 device, ICX 6610 device, ICX 6450 device, ICX 6650 device or SX800/1600 device to meet FIPS 140-2 Level 2 Physical Security requirements the Crypto Officer must install tamper evident seals. Tamper evident seals are available for order from Brocade under FIPS Kit (Part Number: Brocade XBR-000195). The Crypto Officer shall follow the Brocade FIPS Security Seal application procedures defined in Appendix A of this document prior to operating the module in FIPS mode.

The Crypto Officer is responsible for storing and controlling the inventory of any unused seals. The unused seals shall be stored in plastic bags in a cool, dry environment between 60° and 70° F (15° to 20° C) and less than 50% relative humidity. Rolls should be stored flat on a slit edge or suspended by the core.

The Crypto Officer shall maintain a serial number inventory of all used and unused tamper evident seals. The Crypto Officer shall periodically monitor the state of all applied seals for evidence of tampering. A seal serial number mismatch, a seal placement change, a checkerboard destruct pattern that appears in peeled film and adhesive residue on the substrate are evidence of tampering. The security officer shall periodically view each applied seal under a UV light to verify the presence of a UV wallpaper pattern. The lack of a wallpaper pattern is evidence of tampering. The Crypto Officer is responsible for returning a module to a FIPS approved state after any intentional or unintentional reconfiguration of the physical security measures.

Please refer to Appendix A of this Security Policy document for specific tamper evident seal application instructions.

13 Mode Status

FIPS Approved Mode

This section describes FIPS Approved mode of operation and the sequence of actions that place a Brocade cryptographic module in FIPS Approved mode. The module may be configured for FIPS mode by the Crypto Officer being physically present at the boundary, and by following the steps described below. Failure to adhere to the following guidance is an explicit violation of the Security Policy and as such deems the cryptographic module fully non-compliant and unfit for service in an Approved mode of operation. The module is put in FIPS Approved mode of operation by following the procedure below:

To configure the cryptographic module for FIPS Approved mode, perform the following procedures:

1. Log in as Crypto Officer.
2. Enable FIPS.
3. Perform zeroize service.
4. Disable AAA authentication.
5. Disable HTTPS.
6. Disable TLS.
7. Disable SNMP.
8. Disable SSH and SCP.
9. Do not use port 280.
10. Do not use HTTPS SSL 3.0 access Command web-management.
11. Disable HTTP.
12. Enable TFTP.
13. Do not use monitor mode.
14. Inspect the physical security of the module, including placement of tamper evident labels according to Appendix A.
15. Power cycle the module.

Table 32 Algorithm Certificates for Devices

Device	Algorithm	Supports	Certificate
FCX 624 / 648 Devices	Digital Signature Algorithm (DSA)	1024-bit Keys	#668
FCX 624 / 648 Devices	Secure Hash Standard (SHS)	SHA-1	#2227
ICX 6650 Devices	Digital Signature Algorithm (DSA)	1024-bit Keys	#801
ICX 6650 Devices	Secure Hash Standard (SHS)	SHA-1	#2224
SX800 / 1600 Devices	Digital Signature Algorithm (DSA)	1024-bit Keys	#802
SX800 / 1600 Devices	Secure Hash Standard (SHS)	SHA-1	#2225
ICX 6450 and ICX 6450-12-CP Devices	Digital Signature Algorithm (DSA)	1024-bit Keys	#803
ICX 6450 and ICX 6450-12-CP Devices	Secure Hash Standard (SHS)	SHA-1	#2226
ICX 6610 Devices	Digital Signature Algorithm (DSA)	1024-bit Key	#668
ICX 6610 Devices	Secure Hash Standard (SHS)	SHA-1	#2227

Users should reference the transition tables that will be available at the CMVP Web site (http://csrc.nist.gov/groups/STM/cmvp/). The data in the tables will inform users of the risks associated with using a particular algorithm and a given key length.

NOTICE: This cryptographic module is impacted by SP800-131A transition rules effective January 1,2014
In FIPS mode the only FIPS Approved algorithm is DSA 1024-SHA1 signature verification (Certs. #668, #801, #802 and #803).

14 Glossary

Term/Acronym	Description
AES	Advanced Encryption Standard
CBC	Cipher-Block Chaining
CLI	Command Line Interface
CSP	Critical Security Parameter
DES	Data Encryption Standard
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
ECB	Electronic Codebook mode
FI	FastIron
GbE	Gigabit Ethernet
HMAC	Keyed-Hash Message Authentication Code
KDF	Key Derivation Function
LED	Light-Emitting Diode
LP	Line Processor
Mbps	Megabits per second
MP	Management Processor
NDRNG	Non-Deterministic Random Number Generator
NI	NetIron
OC	Optical Carrier
POE	Power over Ethernet
POE+	High Power over Ethernet
PRF	Pseudo-random function
RADIUS	Remote Authentication Dial in User Service
RSA	Rivest Shamir Adleman
SCP	Secure Copy
SFM	Switch Fabric Module
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SSH	Secure Shell
TACACS+	Terminal Access Control Access-Control System
TDEA	Triple-DES Encryption Algorithm
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security

15 References

[FIPS 186-2+] Federal Information Processing Standards Publication 186-2 (+Change Notice), Digital Signature Standard (DSS), 27 January 2000

[RSA PKCS #1] PKCS #1: RSA Cryptography Specifications Version 2.1

[SP800-90] National Institute of Standards and Technology Special Publication 800-90, Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised), March 2007

Appendix A: Tamper Label Application

The FIPS Kit (Part Number: Brocade XBR-000195) contains the following items:

1. Tamper Evident Security Seals
    a. Count 120
    b. Checkerboard destruct pattern with ultraviolet visible “Secure” image

Use 99% isopropyl or ethyl alcohol to clean the surface area at each tamper evident seal placement location. Cleaning alcohol is not provided in the kit. However, cleaning alcohol is readily available for purchase from a chemical supply company. Prior to applying a new seal to an area, that shows seal residue, use consumer strength adhesive remove to remove the seal residue. Then use additional alcohol to clean off any residual adhesive remover before applying a new seal.

The Crypto Officer is responsible for securing and having control of any unused seals at all times

ICX 6610-24F Devices

Use the figures in this section as a guide for security seal placement on a FIPS-compliant Brocade ICX 6610-24F device. Each device requires the placement of eighteen (18) seals:

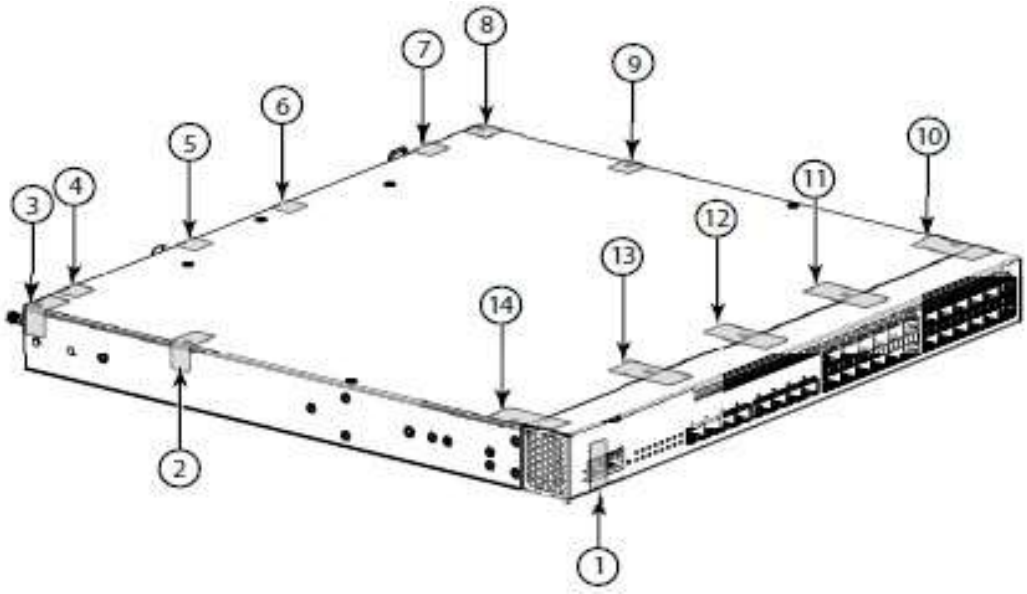
Front: Affix one seal (1) over the console port on the left side of the front panel. The seal should be centered on port and adhere to the front panel above and below the port. See Figure 15 and Figure 16 for correct seal orientation and positioning.

Top: Affix five seals between the top of the front panel and the top removable metal cover of the device. Apply each seal flat over the seam between the top cover and front panel so that part of the seal is on the metal cover and other part is affixed to the front panel as shown. See Figure 16 for correct seal orientation and positioning.

Right and left sides: Affix two seals to each side of the device. Place the seals in a 90 degree bend, so that part of the seal is affixed to the side of the device and the other part is affixed to the removable top cover as shown. The orientation and placement of seals on the left side of the device mirrors the orientation and placement of seals on the right side of the device. Refer to Figure 16 for correct seal orientation and positioning on the side of the device.

Figure 15 Front view of a Brocade ICX 6610-24F device with security seals

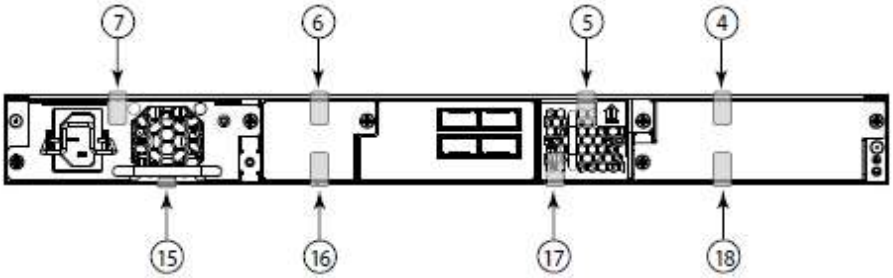
Figure 16 Top, front, and right side view of a Brocade ICX 6610-24F device with security seals



Rear: Affix eight seals to the backside of the device. Place four seals between the top removable cover and the rear panel and 4 between the bottom of the chassis and the rear panel. Place the seals in a 90 degree bend, so that part of the seal is affixed to the rear panel of the device and the other part is affixed to the top cover or chassis bottom. Refer to Figure 17 for correct seal orientation and positioning.

Note the placement of the seal (15) below the power supply handle.

Figure 17 Rear view of a Brocade ICX 6610-24F device with security seals



ICX 6610-24 and ICX 6610-24P Devices

Use the figures in this section as a guide for security seal placement on a FIPS-compliant Brocade ICX 6610-24 and ICX 6610-24P devices. Each device requires the placement of eighteen (18) seals:

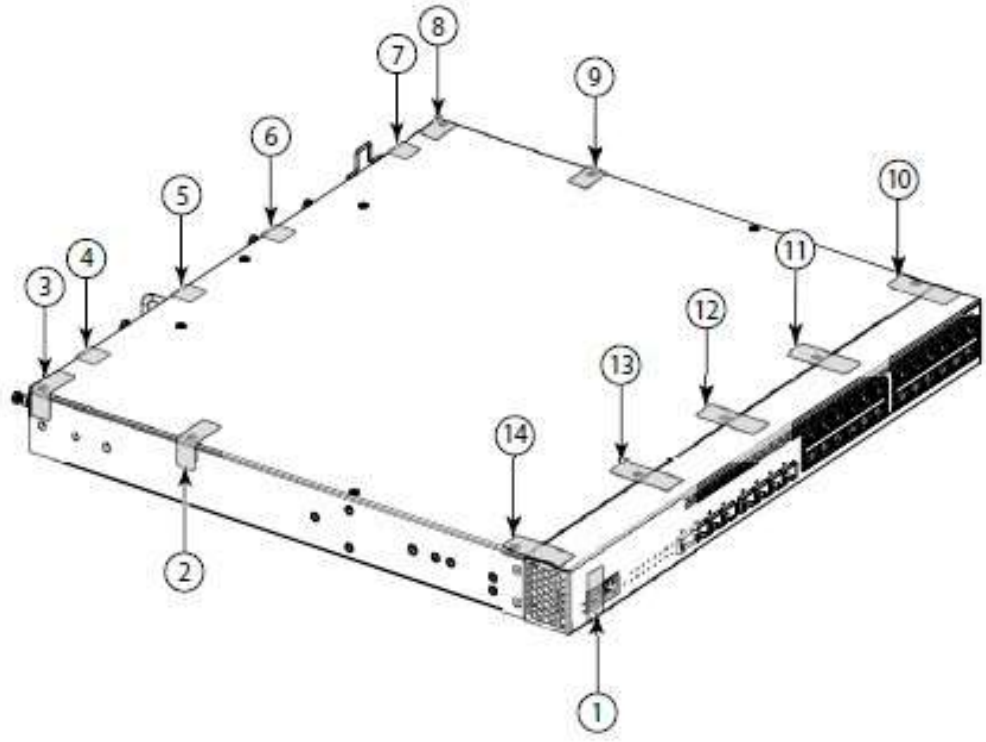
Front: Affix one seal (1) over the console port on the left side of the front panel. The seal should be centered on port and adhere to the front panel above and below the port. See Figure 18 and Figure 19 for correct seal orientation and positioning.

Top: Affix five seals between the top of the front panel and the top removable metal cover of the device. Apply each seal flat over the seam between the top cover and front panel so that part of the seal is on the metal cover and other part is affixed to the front panel as shown. See Figure 19 for correct seal orientation and positioning.

Right and left sides: Affix two seals to each side of the device. Place the seals in a 90 degree bend, so that part of the seal is affixed to the side of the device and the other part is affixed to the removable top cover as shown. The orientation and placement of seals on the left side of the device mirrors the orientation and placement of seals on the right side of the device. Refer to Figure 19 for correct seal orientation and positioning on the side of the device.

Figure 18 Front view of Brocade ICX 6610-24 and ICX 6610-24P devices with security seals

Figure 19 Front, top, and left side view of Brocade ICX 6610-24 and ICX 6610-24P devices with security seals

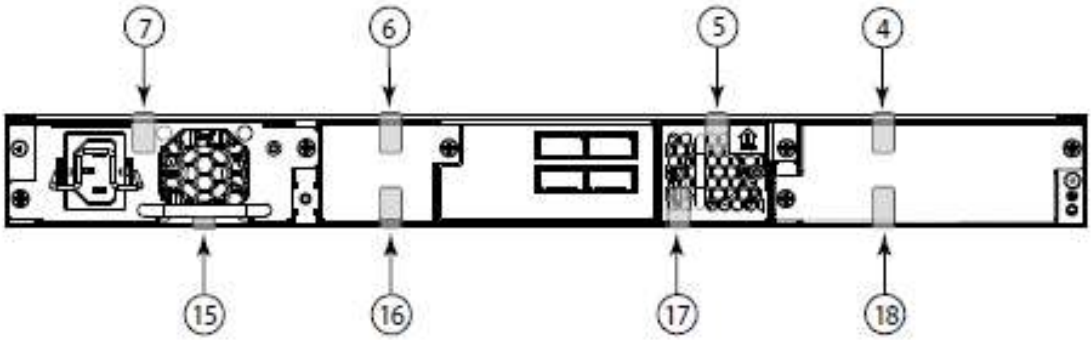


Rear: Affix eight seals to the rear of the device. Place four seals between the top removable cover and the rear panel and four between the bottom of the chassis and the rear panel. Place the seals in a 90-degree

bend, so that part the seal is affixed to the rear panel of the device and part is affixed to the top cover or chassis bottom as shown. Refer to Figure 20 for correct seal orientation and positioning.

Note the placement of the seal (15) below the power supply handle.

Figure 20 Rear view of Brocade ICX 6610-24 and ICX 6610-24P devices with security seals



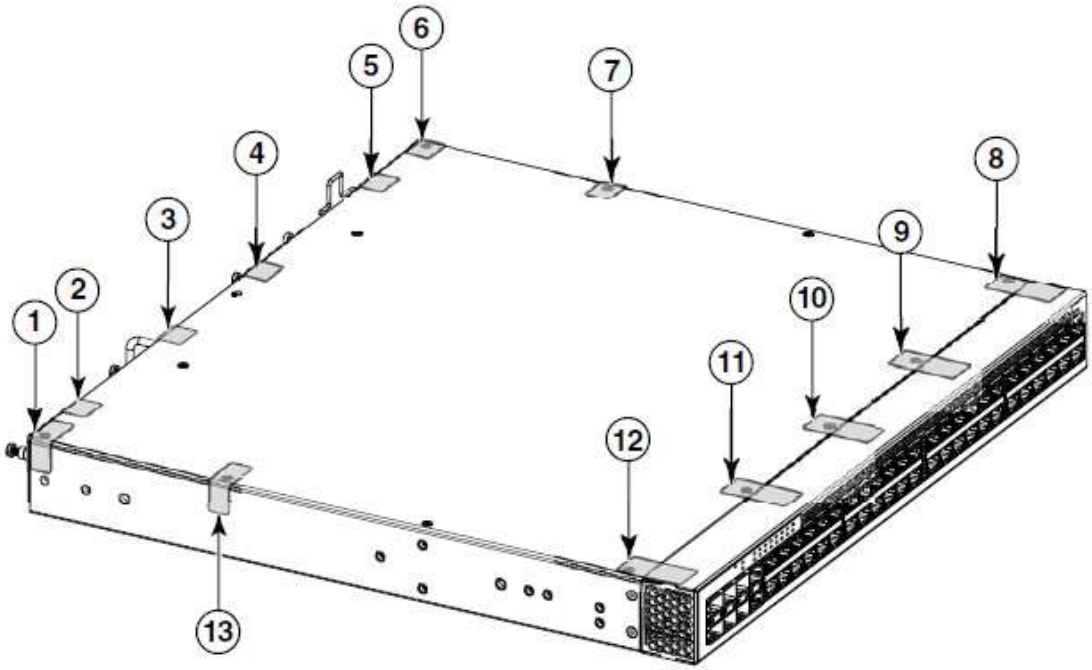
ICX 6610-48 and ICX 6610-48P Devices

Use the figures in this section as a guide for security seal placement on a FIPS-compliant Brocade ICX 6610-48 and ICX 6610-48P devices. Each device requires the placement of eighteen (18) seals.

Top: Affix five seals between the top of the front panel and the top removable metal cover of the device. Apply each seal flat over the seam between the top cover and front panel so that part of the seal is on the metal cover and other part is affixed to the front panel as shown. See Figure 21 for correct seal orientation and positioning.

Right and left sides: Affix two seals to each side of the device. Place the seals in a 90-degree bend, so that part the seal is affixed to the side of the device and part is affixed to the removable top cover as shown. The orientation and placement of seals on the left side of the device mirrors the orientation and placement of seals on the right side of the device. Refer to Figure 21 for correct seal orientation and positioning on the side of the device.

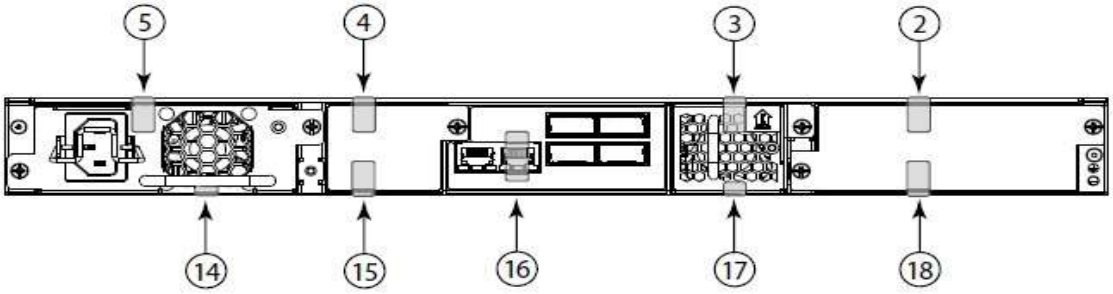
Figure 21 Front, top, and left side view of Brocade ICX 6610-48 and ICX 6610-48P devices with security seals



Rear: Affix nine seals to the rear of the device. Place four seals between the top removable cover and the rear panel and four between the bottom of the chassis and the rear panel. Place the seals in a 90-degree bend, so that part the seal is affixed to the rear panel of the device and part is affixed to the top cover or chassis bottom. Affix one seal (16) so that it covers the console port in the center of the rear panel and is oriented vertically. The seal should be centered on port and adhere to the rear panel above and below the port. Refer to Figure 22 for correct seal orientation and positioning.

Note the placement of the seal (14) below the power supply handle.

Figure 22 Rear view of Brocade ICX 6610-48 and ICX 6610-48P devices with security seals



FCX 624S-F-ADV, Brocade FCX 624S and Brocade FCX 624S-HPOE-ADV devices

Use the figures in this section as a guide for security seal placement on the following Brocade FastIron devices:

- Brocade FCX 624S-F-ADV
- Brocade FCX 624S
- Brocade FCX 624S-HPOE-ADV

Note: The following SKUs are physically equivalent to the FCX 624S, FCX 624S-F, and the FCX 648S:
FCX 624S-HPOE-ADV
FCX 624S-F-ADV
FCX 648S-HPOE
FCX 648S-HPOE-ADV

The connectors on the faceplates of your particular device might vary from the connectors shown on the figures, but the placement of the seals will be the same. Figure 23 and Figure 24 display a Brocade FCX 624S with seals as a model for the seal placement on the Brocade FCX 624S-F-ADV, FCX 624S and FCX 624S-HPOE-ADV. Each of these devices requires the placement of Fourteen (14) seals:

- **Top:** Affix 4 total seals to the top panel of the device. Affix two seals so that they cover the left and right front most screws on the top panel of the device. Affix two seals so that they cover the two screws adjacent to the front most screws on the top panel. See Figure 23 for correct seal orientation and positioning.
- **Right and left sides:** Affix 4 total seals to the left and right sides of the device--two seals on the right side and two seals on the left side. Each seal should cover two holes on either side of the first vent section. See Figure 23 for correct seal orientation and positioning on the right side of the device. The orientation and placement of seals on the left side mirrors the orientation and placement of seals on the right side of the device (visible in Figure 23).
- **Front:** Affix one seal horizontally aligned with half affixed to the front panel and half affixed to the bottom panel. You must bend this seal to place it correctly. See Figure 23 for correct seal orientation and positioning. Affix one seal over the console port covering it and adhering it on the left side. See Figure 23 and Figure 24 for correct seal orientation and positioning.
- **Rear:** Affix 4 total seals to the rear panel of the device. Affix one seal from the rear panel to the bottom panel and three seals from the rear panel to the top panel. You must bend these seals to place them correctly. See Figure 24 for correct seal orientation and positioning.

Figure 23 Front, top, and right side views of a Brocade FCX 624S-F-ADV, FCX 624S and FCX 624S-HPOE-ADV device with security seals

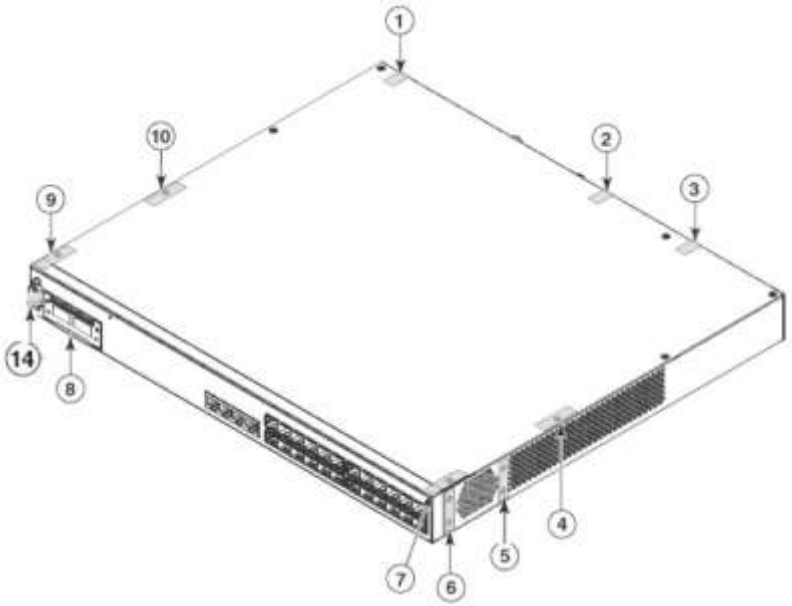
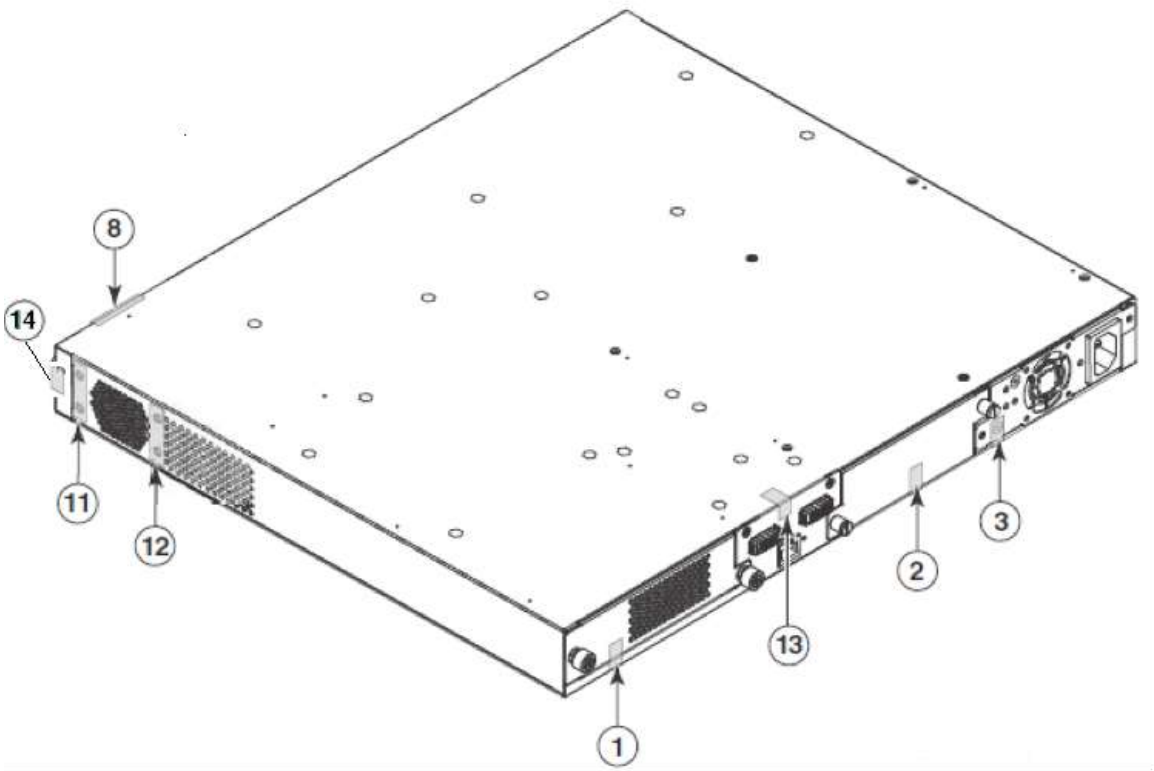


Figure 24 Rear, bottom, and left side views of a Brocade FCX 624S-F-ADV, FCX 624S and FCX 624S-HPOE-ADV device with security seals



FCX 648S, FCX 648S-HPOE and FCX 648S-HPOE-ADV devices

Use the figures in this section as a guide for security seal placement on the following Brocade FastIron devices:

- Brocade FCX 648S
- Brocade FCX 648S-HPOE
- Brocade FCX 648S-HPOE-ADV

Figure 25 and Figure 26 display a Brocade FCX 648S with seals as a model for the seal placement on the Brocade FCX 648S, FCX 648S-HPOE and FCX 648S-HPOE-ADV. Each of these devices requires the placement of fourteen (14) seals:

- **Top:** Affix 4 total seals to the top panel of the device. Affix two seals so that they cover the left and right front most screws on the top panel of the device. Affix two seals so that they cover the two screws adjacent to the front most screws on the top panel. See Figure 25 for correct seal orientation and positioning.
- **Right and left sides**: Affix 4 total seals to the left and right sides of the device–two seals on the right side and two seals on the left side. Each seal should cover two holes on either side of the first vent section. See Figure 25 for correct seal orientation and positioning on the right side of the device. The orientation and placement of seals on the left side mirrors the orientation and placement of seals on the right side of the device (visible in Figure 25).

- **Front:** Affix one seal horizontally aligned with half affixed to the front panel and half affixed to the bottom panel. You must bend this seal to place it correctly. See Figure 25 for correct seal orientation and positioning.

  Rear: Affix 4 total seals to the rear panel of the device. Affix one seal from the rear panel to the bottom panel and three seals from the rear panel to the top panel. You must bend these seals to place them correctly. See Figure 26 for correct seal orientation and positioning.

Figure 25 Front, top and right side views of a Brocade FCX 648S, FCX 648S-HPOE and FCX 648S-HPOE-ADV device with security seals

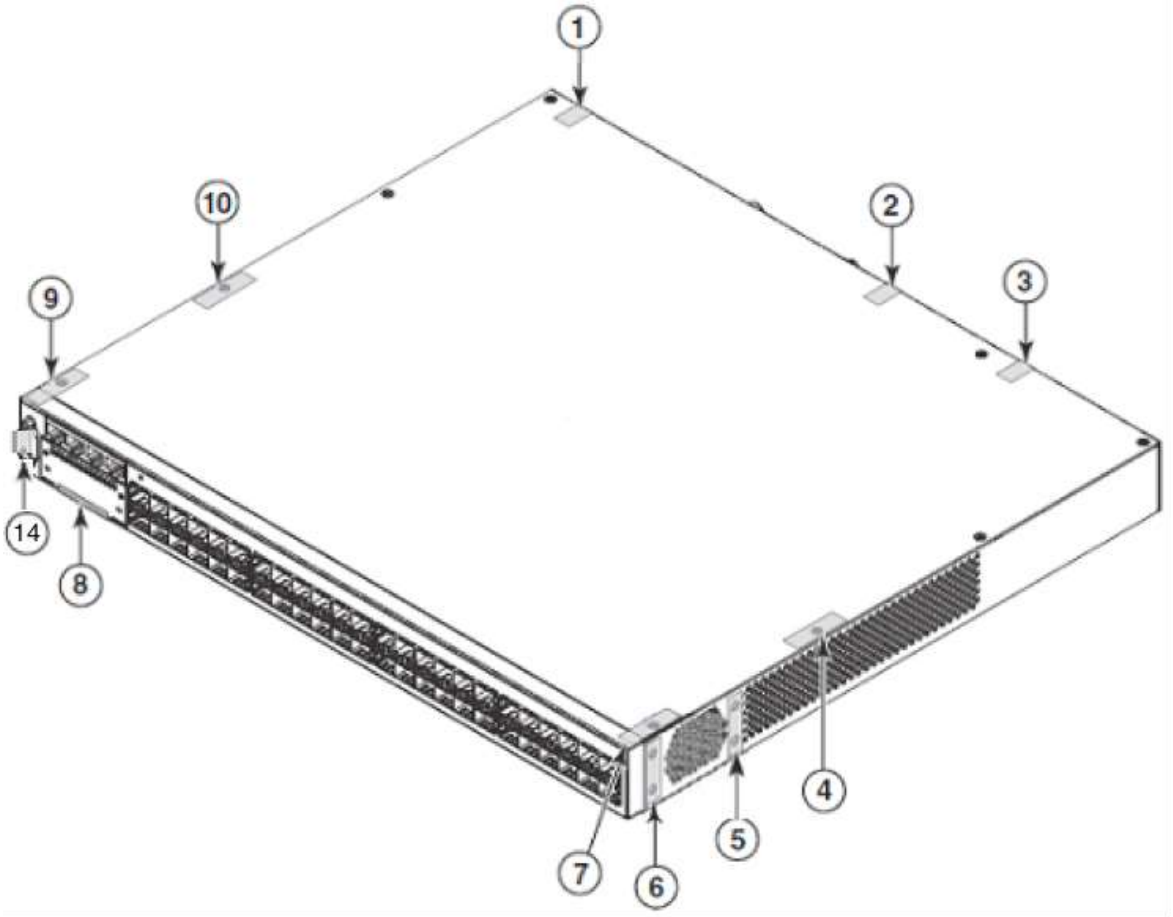
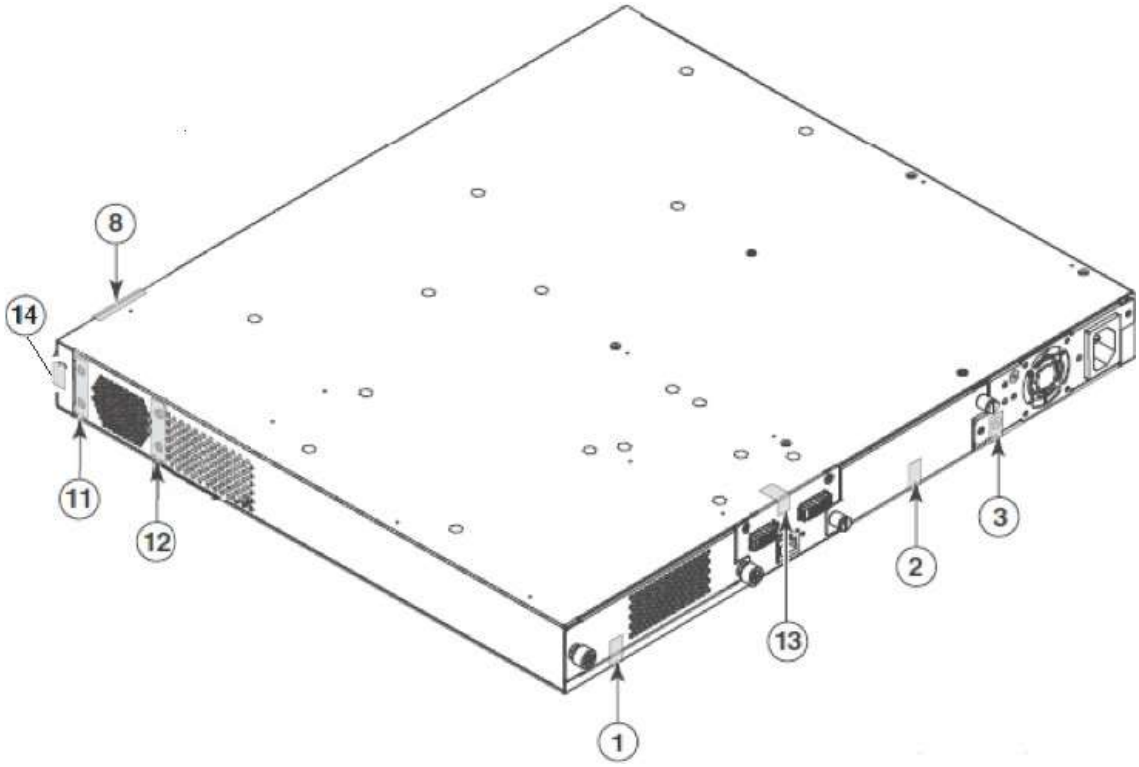


Figure 26 Rear, bottom, and left side views of a Brocade FCX 648S, FCX 648S-HPOE and FCX 648S-HPOE-ADV device with security seals



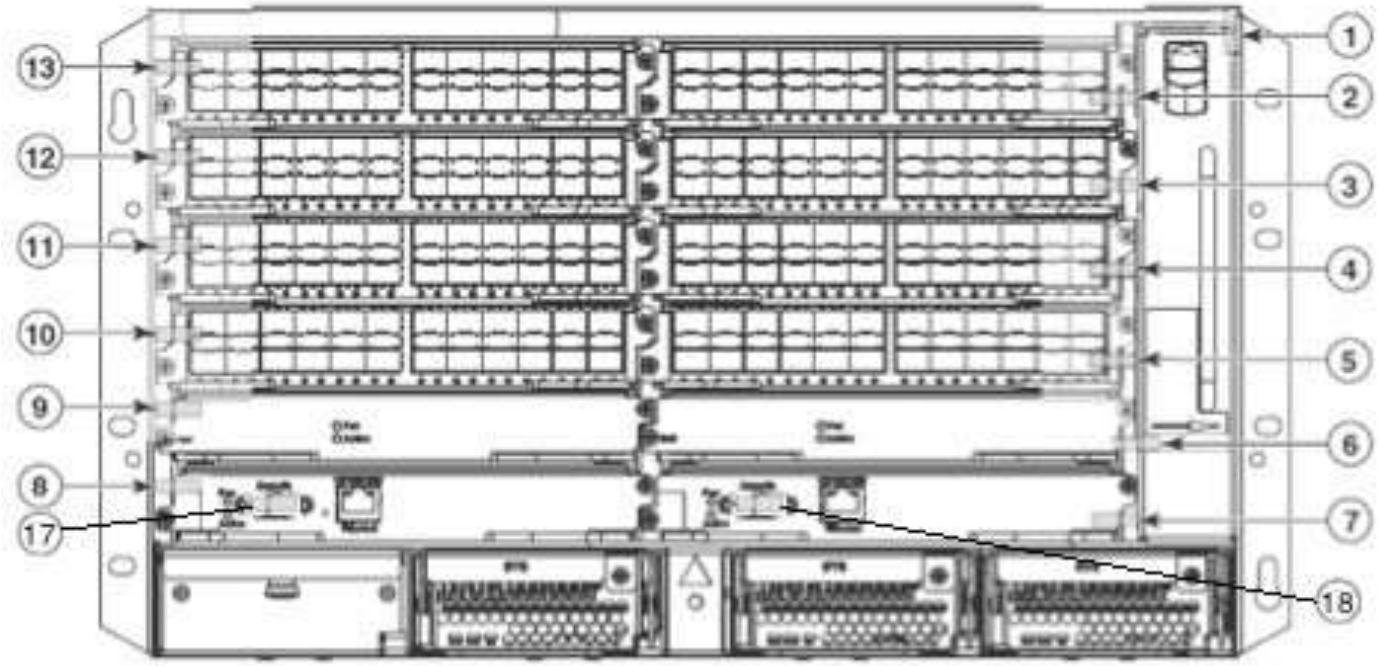
SX 800 devices

Use the figures in this section as a guide for security seal placement on a Brocade FastIron SX 800 device.

The connectors on the faceplates of a particular module might vary from the connectors shown on the figures, but the placement of the seals will be the same. There is no seal placement required on the side panels or solely on the top and bottom panels of Brocade FastIron SX 800 devices. Each Brocade FastIron SX 800 device requires the placement of eighteen (18) seals:

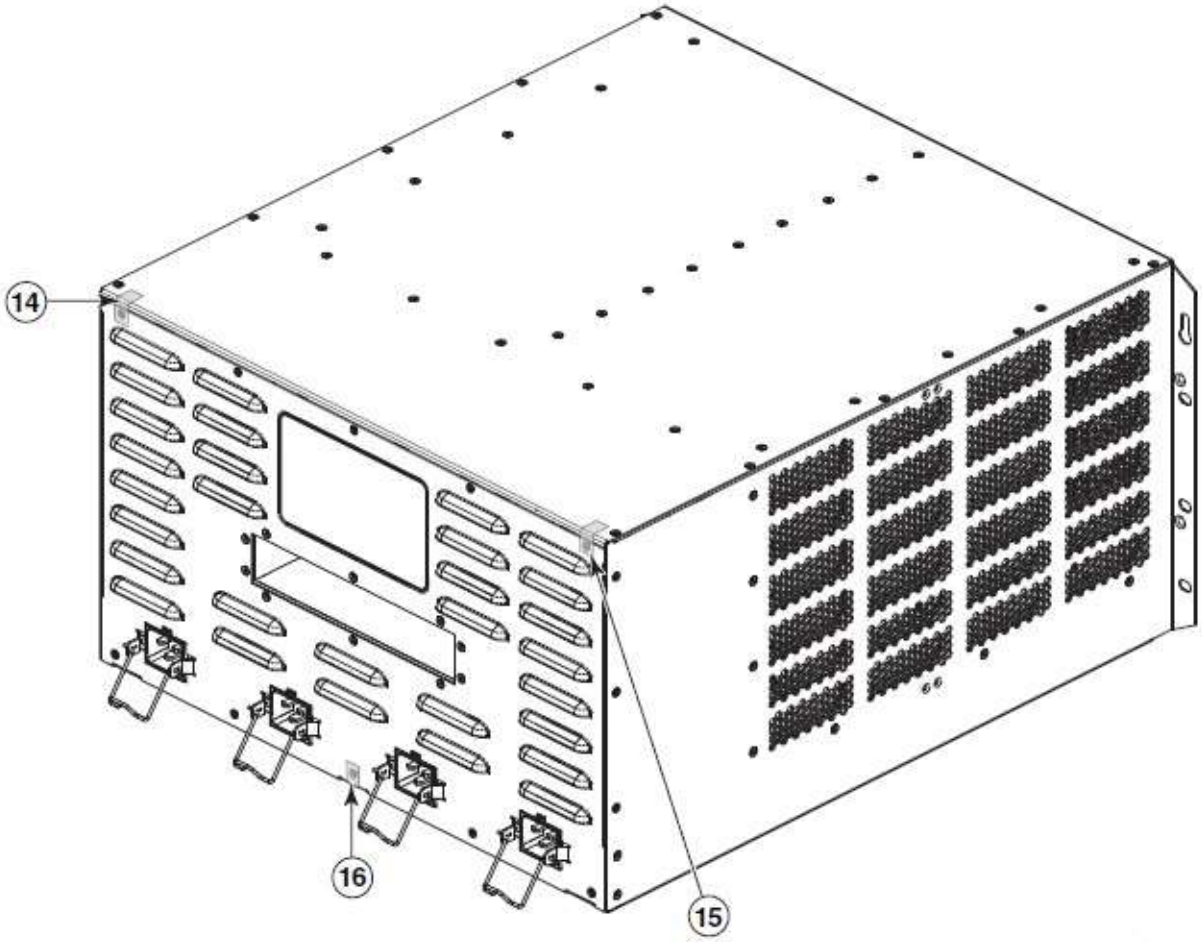
- **Front**: Affix 15 total seals to the front panel of the device. Affix one horizontally oriented seal to the left ear of each module installed in the left side of the chassis. As much as possible of the seal should be affixed to the module directly above the left screw for the left side modules. Affix one horizontally oriented seal to each of the modules installed in the right side of the chassis by affixing the seals directly under the screw to the right ear of each module and to the chassis. Affix one seal from the upper right corner of the fan tray to the chassis. Affix two seals horizontally over the console ports. All 15 of these seals should lie flat against the front of the device. See Figure 27 for correct seal orientation and positioning.

Figure 27 Front view of a Brocade FastIron SX 800 device with security seals



- **Rear**: Affix 3 total seals to the rear panel of the device. Affix two vertically-aligned seals at the upper right and left sides of the rear panel so that one half of the seal is affixed to the top panel of the device and the other half is affixed to the rear panel and covering the rightmost and leftmost screws. You must bend these seals to place them correctly. Affix one seal vertically aligned at the lower center of the rear panel so that one-half of the seal is affixed to the bottom panel of the device and the other half of the seal is affixed to the rear panel of the device, covering the middle screw. See Figure 28 for seal orientation and positioning.

Figure 28 Rear, top and left side panel views of a Brocade FastIron SX 800 device with security seals



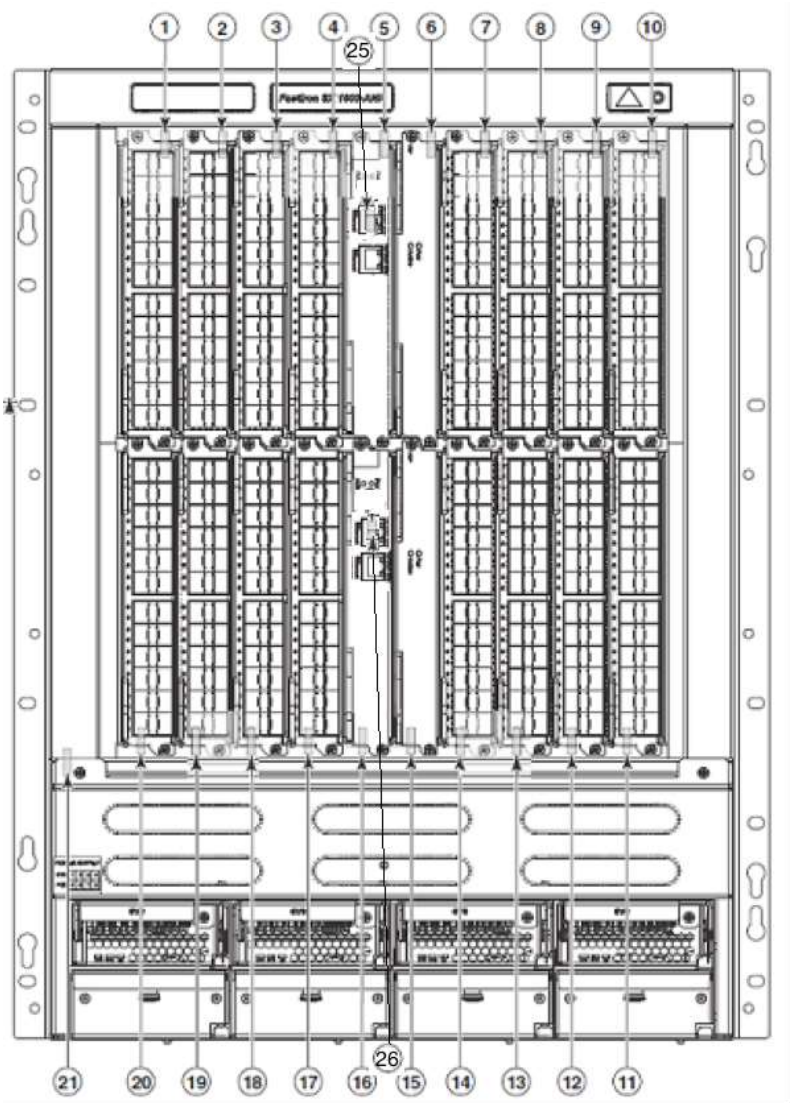
SX 1600 devices

Use the figures in this section as a guide for security seal placement on a Brocade FastIron SX 1600 device.

The connectors on the faceplates of a particular module might vary from the connectors shown on the figures, but the placement of the seals will be the same. There is no seal placement required on the top panel, bottom panel, or side panels of Brocade FastIron SX 1600 devices. Each Brocade FastIron SX 1600 device requires the placement of twenty-six (26) seals:

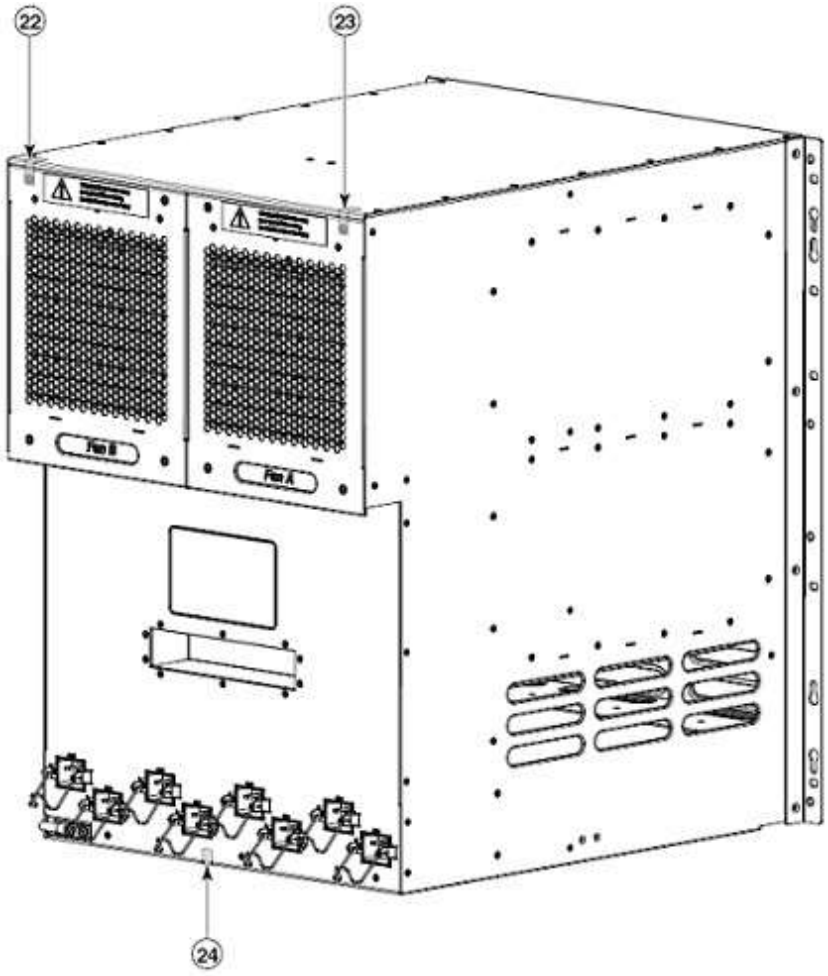
- **Front:** Affix 23 total seals to the front panel of the device. Affix one horizontally oriented seal to the upper ear of each module installed in the top row of the chassis as shown in Figure 29. As much as possible of the seal should be affixed to the module to the right of the screw that secures each module to the chassis. Affix one horizontally oriented seal to the lower ear of each module installed in the bottom row of the chassis as shown in Figure 29. As much as possible of the seal should be affixed to the module to the left of the screw that secures each module to the chassis. Affix one seal from the upper left corner of the fan tray to the chassis, as shown in Figure 29. Affix one seal over both console ports (2 seals total) as shown in Figure 29. All 23 of the seals should lie flat against the front panel of the device.

Figure 29 Front view of a Brocade FastIron SX 1600 device with security seals



- **Rear:** Affix 3 total seals to the rear panel of the device. Affix two vertically aligned seals to the right and left top edges of the chassis so that half of the seal is affixed to the top panel and half to the rear panel or, in the case of an ANR, to the bracket that attaches the ANR bracket to the rear panel of the chassis. Affix one seal vertically to the center bottom edge of the rear panel so that one-half of the seal is affixed to the rear panel of the device and one-half of the seal is affixed to the bottom panel. You must bend this seal to place it correctly. See Figure 30 for correct seal orientation and positioning.

Figure 30 Rear view of the FastIron SX 1600 device with security seals



ICX 6450-24 Devices

Use the figures in this section as a guide for security seal placement on a FIPS-compliant Brocade ICX 6450-24 device. Each device requires the placement of seven (7) seals:

- **Top:** Affix 3 seals between the top of the front panel and the top removable metal cover of the device. Apply each seal flat over the seam between the top cover and front panel so that part of the seal on the metal cover and the other part is affixed over the top of the front panel. See Figure 31 for correct seal orientation and positioning.
- **Rear:** Affix 3 seals to the rear of the device between bottom of the chassis and the rear removable cover. Place the seals in a 90 degree bend, so that part of the seal is affixed to the chassis bottom and the other part is affixed to the rear cover as shown. Refer to Figure 32 for correct seal orientation and positioning.
- **Console Port:** Affix 1 seal over the console port, as shown in Figure 39.

Figure 31 Top view of a Brocade ICX 6450-24 device with security seals

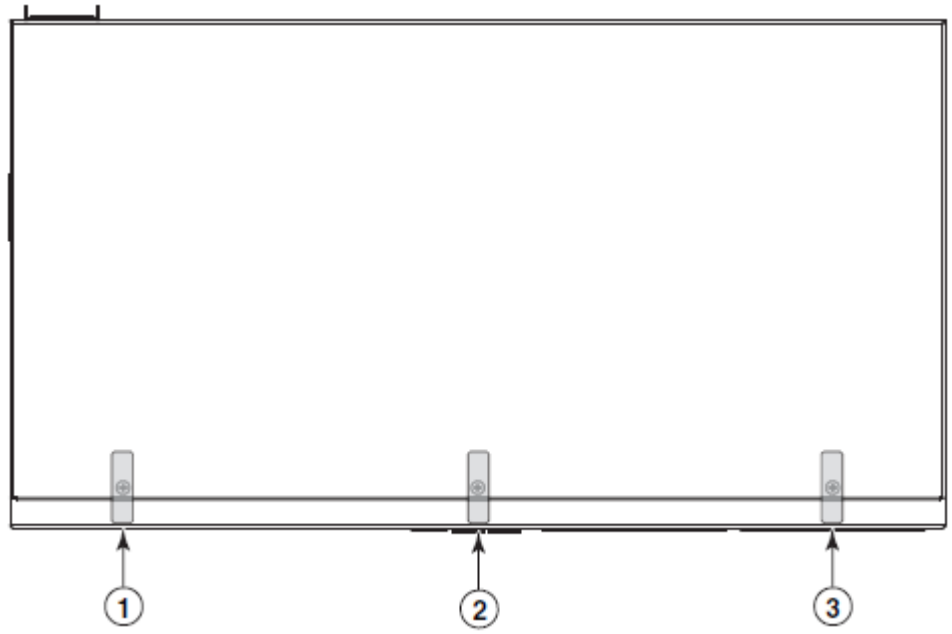
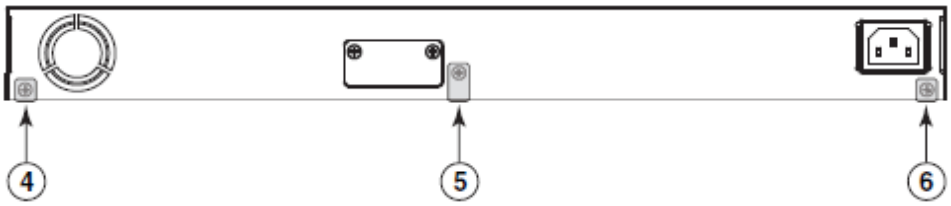


Figure 32 Rear view of a Brocade ICX 6450-24 device with security seals



ICX 6450-24P Devices

Use the figures in this section as a guide for security seal placement on a FIPS-compliant Brocade ICX 6450 - 24P device. Each device requires the placement of seven (7) seals:

- **Top:** Affix 3 seals between the top of the front panel and the top removable metal cover of the device. Apply each seal flat over the seam between the top cover and front panel so that part of the seal is on the metal cover and the other part is affixed over the top of the front panel as shown. See Figure 33 for correct seal orientation and portioning.
- **Rear:** Affix 3 seals to the back side of the device between bottom of the chassis and the rear removable cover. Place the seals in a 90 degree bend, so that part of the seal is affixed to the chassis bottom and the other part is affixed to the rear cover as shown. Refer to Figure 34 for correct seal orientation and positioning.
- **Console Port:** Affix 1 seal over the console port, as shown in Figure 39.

Figure 33 Top view of a Brocade ICX 6450-24P device with security seals

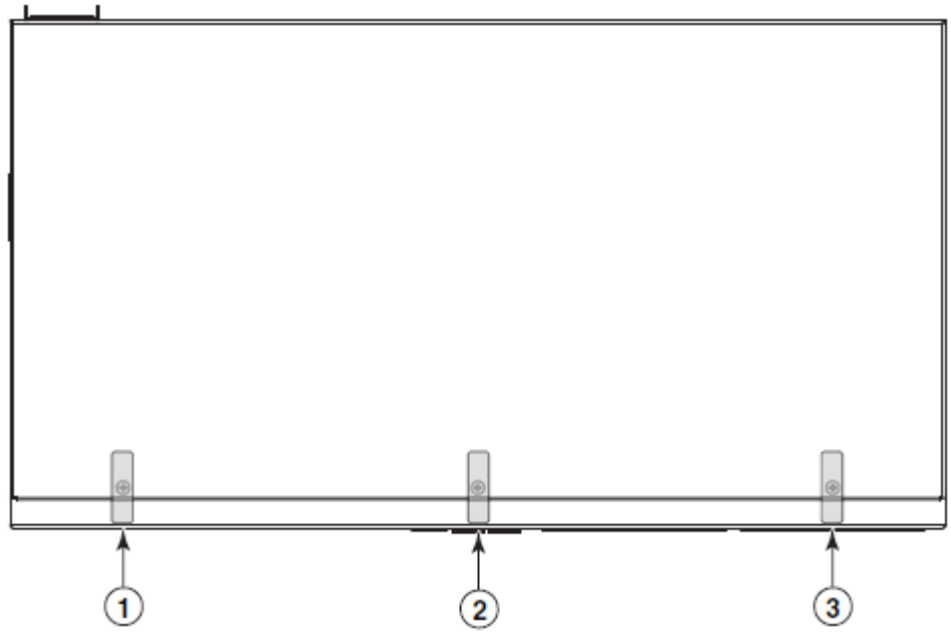
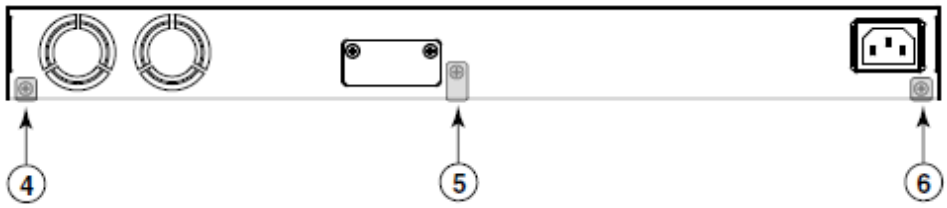


Figure 34 Rear view of a Brocade ICX 6450-24P device with security seals



ICX 6450-48 Devices

Use the figures in this section as a guide for security seal placement on a FIPS-compliant Brocade ICX 6450 - 48 device. Each device requires the placement of seven (7) seals:

- **Top:** Affix 3 seals between the top of the front panel and the top removable metal cover of the device. Apply each seal flat over the seam between the top cover and front panel so that part of the seal is on the metal cover and the other part is affixed over the top of the front panel. See Figure 35 for correct seal orientation and positioning.
- **Rear:** Affix 3 seals to the rear of the device between bottom of the chassis and the rear removable cover. Place the seals in a 90 degree bend, so that part of the seal is affixed to the chassis bottom and the other part is affixed to the rear cover as shown. Refer to Figure 36 for correct seal orientation and positioning.
- **Console Port:** Affix 1 seal over the console port, as shown in Figure 40 and Figure 41. Place the seal so that part of the seal entirely covers the console port while the remainder of the seal wraps around the side of the chassis as shown.

Figure 35 Top view of a Brocade ICX 6450-48 device with security seals

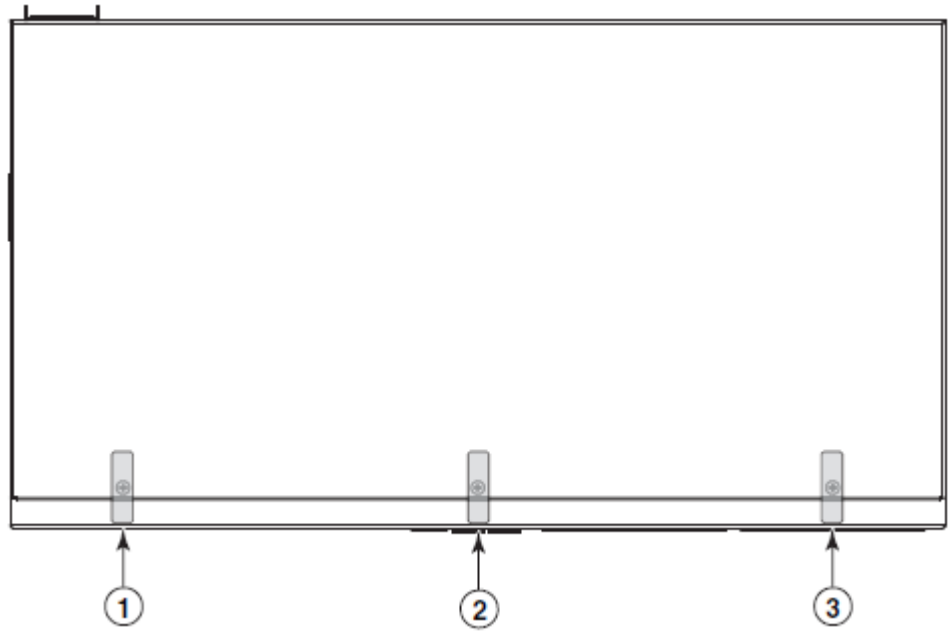
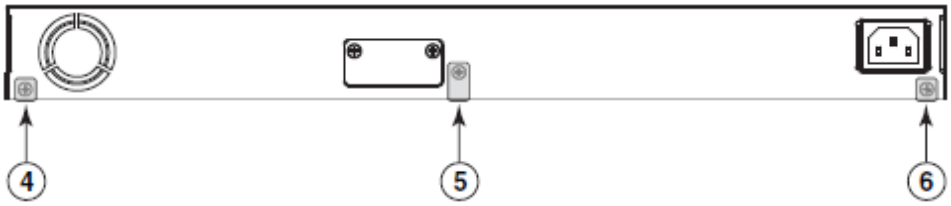


Figure 36 Rear view of a Brocade ICX 6450-48 device with security seals



ICX 6450-48P Devices

Use the figures in this section as a guide for security seal placement on a FIPS-compliant Brocade ICX 6450 - 48P device. Each device requires the placement of seven (7) seals:

- **Top:** Affix 3 seals between the top of the front panel and the top removable metal cover of the device. Apply each seal flat over the seam between the top cover and front panel so that part of the seal is on the metal cover and the other part is affixed over the top of the front panel as shown. See Figure 37 for correct seal orientation and portioning.
- **Rear:** Affix 3 seals to the back side of the device between bottom of the chassis and the rear removable cover. Place the seals in a 90 degree bend, so that part of the seal is affixed to the chassis bottom and the other part is affixed to the rear cover as shown. Refer to Figure 38 for correct seal orientation and positioning.
- **Console Port:** Affix 1 seal over the console port, as shown in Figure 40 and Figure 41. Place the seal so that part of the seal entirely covers the console port while the remainder of the seal wraps around the side of the chassis as shown.

Figure 37 Top view of a Brocade ICX 6450-48P device with security seals

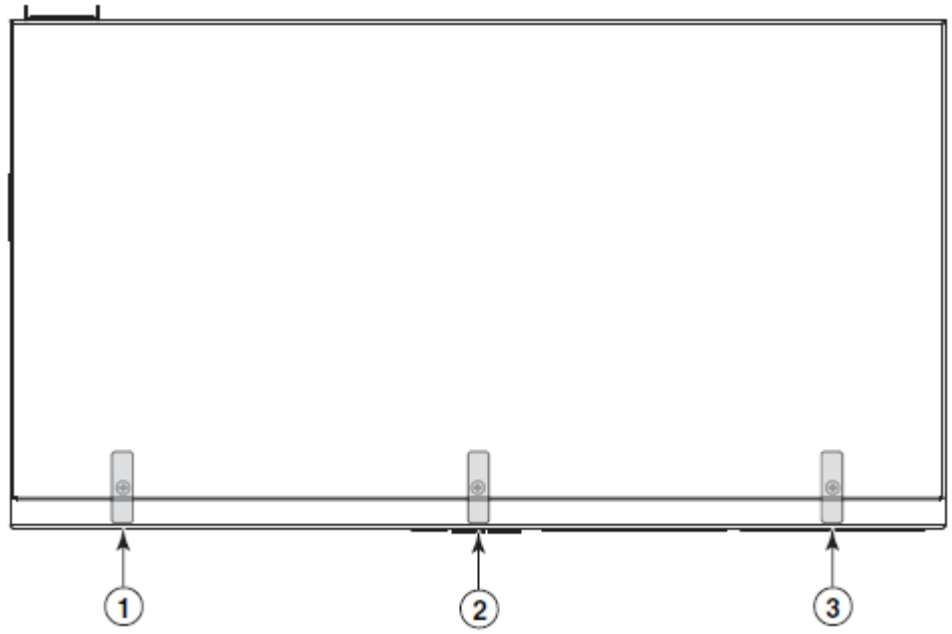


Figure 38 Rear view of a Brocade ICX 6450-48P device with security seals

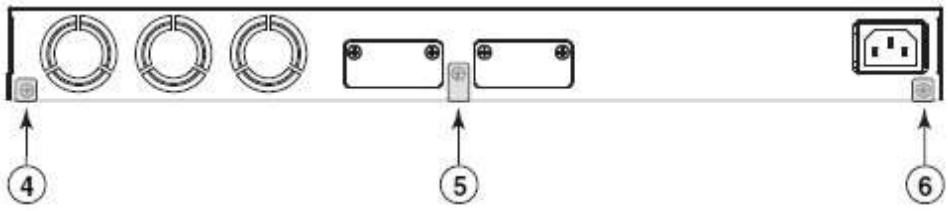


Figure 39 Security Seal over the console port on the Brocade ICX 6450-24 and ICX 6450-24P devices

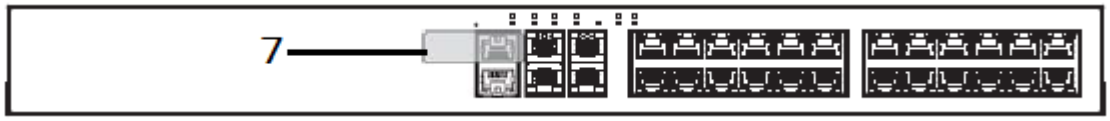


Figure 40 Security Seal over the console port on the Brocade ICX 6450-48 and ICX 6450-48P devices

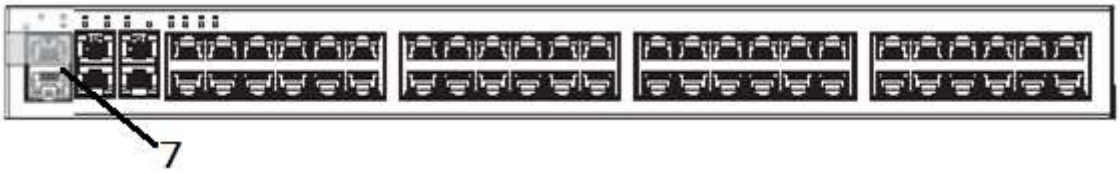
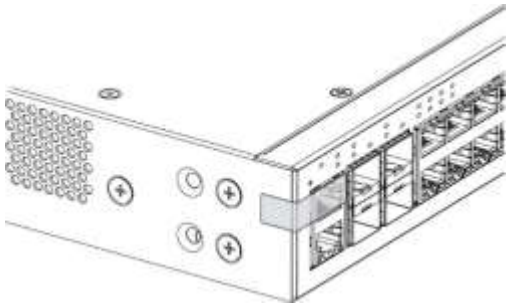


Figure 41 Side View of Security Seal over the console port on the Brocade ICX 6450-48 and ICX 6450-48P devices



ICX 6450-C12-PD Devices

Use the figures in this section as a guide for security seal placement on a FIPS-compliant Brocade ICX 6450- C12-PD device. Each device requires the placement of sixteen (16) seals:

- **Front:** Affix a seal, at seal locations 1 and 2, which wraps from the front panel to the side panel on the left and right side, respectively. Each seal must bridge the seam between the front panel and the side panel. See Figure 42 and Figure 43 for the correct seal orientation and portioning. Affix one seal over the console port. Three (3) seals are required to complete this step of the procedure.
- **Right:** Affix a seal at locations 10, 11, and 12 on the right side of the module, as seen in Figure 43.
- **Left:** Affix a seal at locations 14, 15, and 16 on the left side of the module, as seen in Figure 44A
- **Back:** Affix a seal at location 13, as seen in Figure 44A
- **Bottom:** Affix a seal, at seal locations 3 through 8, which covers the screws that attach the bottom panel to the chassis to chassis cover. Each seal must bridge the seam between the bottom panel and the chassis cover. See Figure 44 for the correct seal orientation and positioning. Six (6) seals are required to complete this step of the procedure.

Figure 42 Front view of a Brocade ICX 6450-C12-PD device with security seals

Figure 43 Front right side view of a Brocade ICX 6450-C12-PD device with security seals

Figure 44 Bottom side view of a Brocade ICX 6450-C12-PD device with security seals

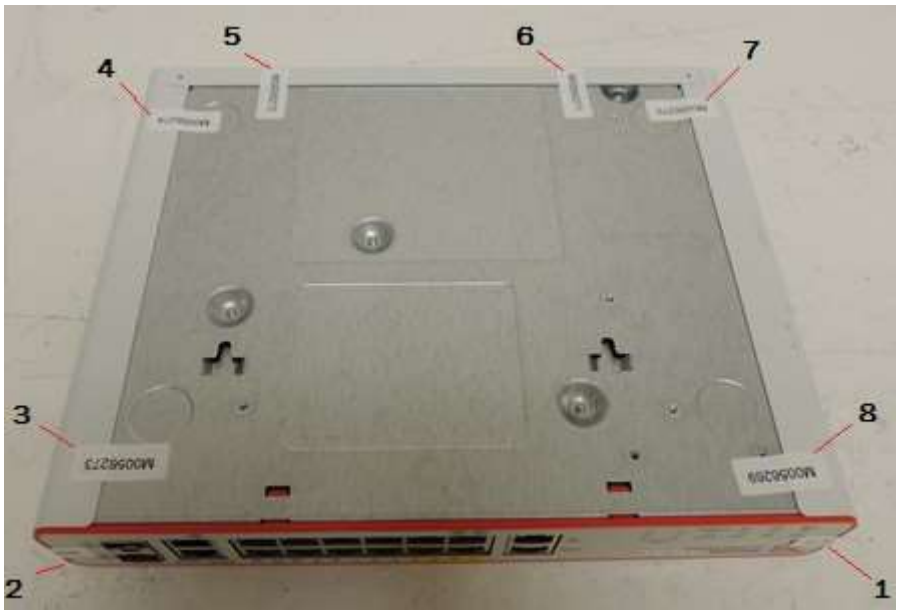


Figure 44A Back left side view of a Brocade ICX 6450-C12-PD device with security seals

ICX 6650 Device

Use the figures in this section as a guide for security seal placement on a FIPS-compliant Brocade ICX 6650 device. Each device requires the placement of seventeen (17) seals.

Top Front: Affix a seal, at seal locations 1, 2 and 3, which covers the screw that attaches the top cover to the front panel and bridges the seam between the top of the front panel and the removable metal cover of the device. See Figure 45 for correct seal orientation and positioning. Three (3) tamper evident seals are required to complete this step of the procedure.

Top right side: Affix a seal, at seal locations 4, 5, 6 and 7, which covers the screw that attaches the top cover to the right side panel and wraps around the 90 degree angle formed by the side panel and the removable metal cover of the device. See Figure 45 and Figure 46 for correct seal orientation and positioning. Four (4) tamper evident seals are required to complete this step of the procedure.

Top left side: Affix a seal, at seal locations 13, 14, 15 and 16, which covers the screw that attaches the top cover to the left side panel and wraps around the 90 degree angle formed by the side panel and the removable metal cover of the device. See Figure 45 and Figure 46 for correct seal orientation and positioning. Four (4) tamper evident seals are required to complete this step of the procedure.

Rear: Affix a seal, at seal locations 8, 9, 10, 11 and 12, which covers the screw that attaches the top cover to the rear panel and wraps around the 90 degree angle formed by the rear panel and the removable metal cover of the device. Place a seal at location 17 to cover the console port. See Figure 47 for correct seal orientation and positioning. Six (6) tamper evident seals are required to complete this step of the procedure.

Figure 45 Front top view of Brocade ICX 6650 device with security seals

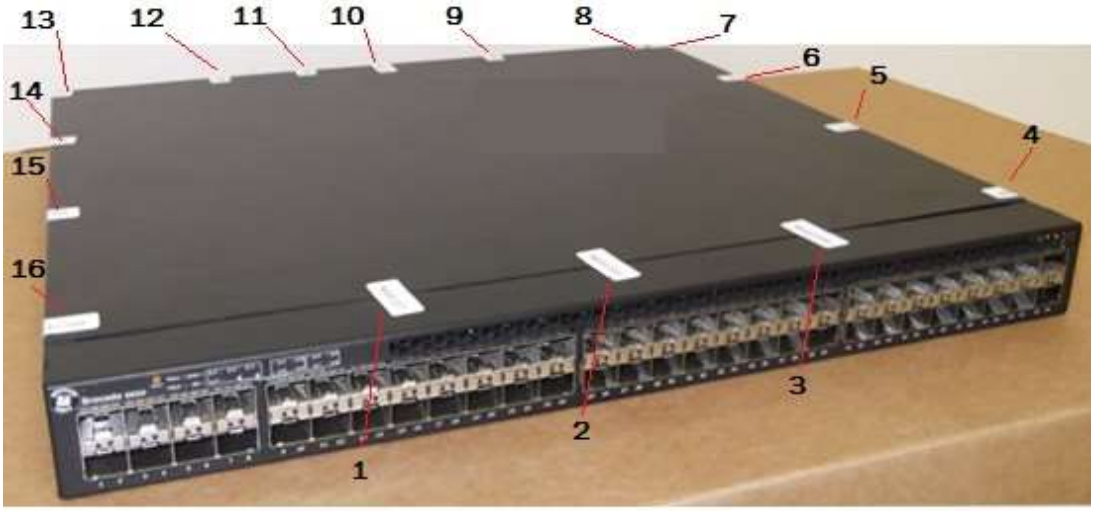


Figure 46 Right and left side view of Brocade ICX 6650 device with security seals

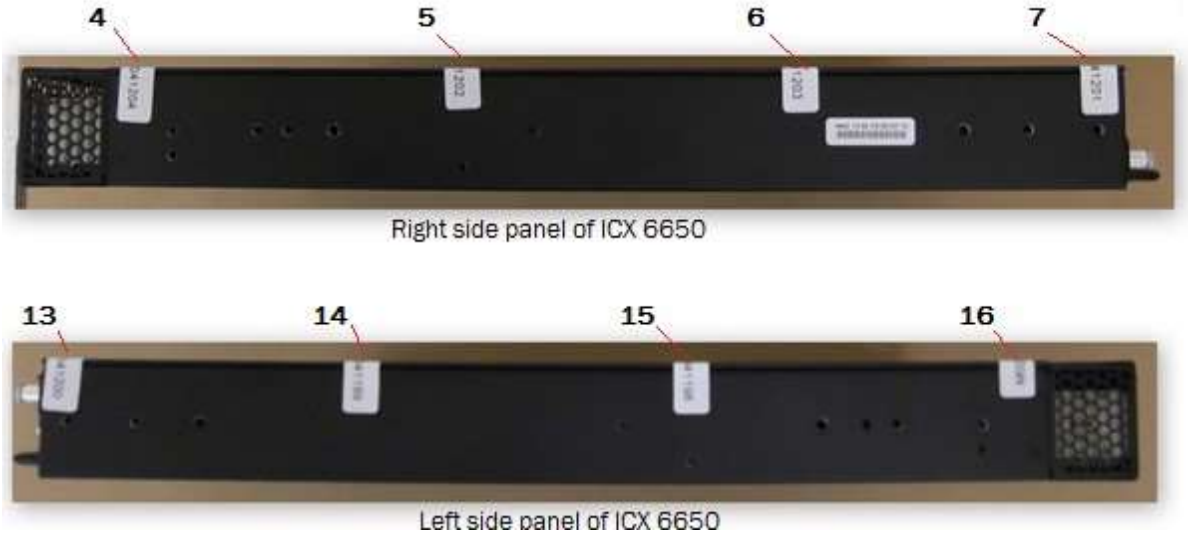


Figure 47 Rear top view of Brocade ICX 6650 device with security seals