

FIPS 140-2 Security Level 2 Policy
LX-4000T Series Console Servers



MRV Communications Inc.
300 Apollo Dr.
Chelmsford, MA. 01824
USA

Document ID 445-RD-43
July 1, 2016
Version 1.16

LX-4000T Series FIPS 140-2 Non-Proprietary Security Policy



Disclaimer

MRV provides this document without any warranty of any kind, whether expressed or implied, including but not limited to the implied warranties of merchantability or fitness for a particular purpose.

The user is advised to exercise due discretion in the use of the contents of this document since the user bears the sole responsibility.

Trademarks

All trademarks are the property of their respective owners.

Encryption Technologies Notice

This product may contain encryption technology. The use, import or export of encryption technology may be subject to country regulations.

Copyright © 2016 by MRV

All rights reserved. This document may be freely reproduced and distributed whole and intact including this copyright notice.

LX-4000T Series FIPS 140-2 Non-Proprietary Security Policy

1	SCOPE	5
2	LX-4000T SERIES CONSOLE SERVERS INTRODUCTION	5
3	PURPOSE	5
3.1	Models and Model Versions	6
3.2	Detailed Model Descriptions	7
3.3	Interfaces	8
3.4	LX-4000T Series Product Views	8
3.5	Module Validation Level	10
4	ROLES, SERVICES, AND AUTHENTICATION	11
4.1	Roles	11
4.1.1	PPCIBOOT User Role	11
4.1.2	Crypto-Officer Role	12
4.1.3	User Role	13
4.1.4	Unauthenticated Users/Services	14
4.1.5	Authentication Actions	14
4.1.6	Authentication Data Protection	14
4.2	Authentication Mechanisms	15
4.3	Non-Allowed Services in FIPS 140-2 Mode of Operation	16
5	CRYPTOGRAPHIC ALGORITHMS	18
5.1	LX-Series Algorithm Core	18
5.2	LX-Series Algorithm IPsec Core	18
5.3	Non-FIPS Approved But Allowed Function	19
5.4	Non-FIPS Allowed Algorithms	19
6	SETTING FIPS 140-2 MODE	20
6.1	Prerequisites	20
6.2	Notes and Restrictions	20
6.3	Applying Tamper Evident Labels	20
6.3.1	Operator Required Actions	22
6.4	Enabling FIPS 140-2 Mode of Operation	22
6.5	Changing the Default PPCiboot Password	23
6.6	Confirming Your Firmware is FIPS 140-2 Validated	24
6.7	Confirming FIPS 140-2 Mode of Operation	26
6.8	Changing the Default Subscriber Password	27
6.9	Changing the Default Superuser Password	27
6.10	FIPS 140-2 Mode Console Access	28
6.11	Upgrading Firmware	28
7	CRYPTOGRAPHIC KEY MANAGEMENT	29
7.1	Zeroization Methods Key	30
7.2	Critical Security Parameter Actions	30
7.3	Key Generation	30
7.3.1	DRBG Used	30

LX-4000T Series FIPS 140-2 Non-Proprietary Security Policy

7.3.2	Intermediate Key Generation Values.....	30
7.3.3	Key Generation Methods.....	30
8	SELF-TESTS.....	31
8.1	Firmware Function Power On Self-Tests	31
8.1.1	LX-Series Algorithm Core Algorithm Implementation POSTs.....	31
8.1.2	LX-Series Algorithm IPSEC Core Algorithm Implementation POSTs 31	
8.2	Conditional Tests	32
9	DESIGN ASSURANCE	32
10	MITIGATION OF OTHER ATTACKS	32

Tables

Table 1	LX Series User Documentation.....	5
Table 2	Current Models and Revisions Validated	6
Table 3	Logical Interface / Module Mapping	10
Table 4	Module Validation Levels	10
Table 5	PPCiboot User Services.....	12
Table 6	Crypto-Officer Services.....	13
Table 7	User Role Services	14
Table 8	Non-Allowed Services, Applications, Protocols and Features.....	17
Table 9	FIPS Validated Cryptographic Functions – Algorithm Core.....	18
Table 10	FIPS Validated Cryptographic Algorithms - IPSEC Core	18
Table 11	Non-FIPS Validated But Allowed Function.....	19
Table 12	Inspection / Testing of Physical Security Mechanisms.....	22
Table 13	Cryptographic Keys, CSPs and SRDIs	29

Figures

Figure 1	LX-4000T Series Typical Front Panel View (48 Port)	8
Figure 2	LX-4000T Series Typical Dual AC Rear Panel View (48 Port).....	9
Figure 3	LX-4000T Series Typical Dual DC Rear Panel View (48 Port).....	9
Figure 4	Tamper Evident Label Recommended Placement.....	21
Figure 5	Boot Selection Screen	23
Figure 6	Show Version Screen	25
Figure 7	Determining FIPS Mode status	26

1 Scope

The following describes the non-proprietary FIPS 140-2 Security Level 2 policy for the MRV LX-4000T Series Console Servers. “LX-4000T Series”, “LX Series”, and “LX” all refer to the MRV LX-4000T Series Console Servers. The term “User” and “Subscriber” are synonymous for the purposes of this Security Policy. The term “Superuser” and “Crypto-Officer” are synonymous for the purposes of this policy.

2 LX-4000T Series Console Servers Introduction

MRV’s Out-of-Band Network solutions, of which the LX-4000T Series Console Servers are a key offering, provide secure remote service port access and remote power control for devices deployed in an organization’s network. The product capability eliminates the need for physical presence at a device to correct problems or manage its everyday operation. The MRV Out-of-Band Network solution set includes console servers, terminal servers, device servers, power control and management systems. These capabilities combined with FIPS 140-2 security make the LX-4000T Series multi-chip standalone cryptographic modules an ideal choice for providing secure remote access in a variety of environments.

3 Purpose

This document defines FIPS 140-2 validated operation of the LX-4000T Series products. This includes initialization, role and responsibilities definition required to operate the product in a secure, FIPS 140-2 validated manner. Supporting this guidance is detailed product information that can be found in the following references:

Document Title	Part Number
Getting Started With the LX-4000T Series	451-0339
LX-4000T Series Quick Start Guide	451-0340
Installing the LX-4000T Series	451-0342
FIPS Configuration Guide	451-0364
Commands Reference Guide	451-0310
LX-Series Configuration Guide	451-0311
Release Notes	450-0172

Table 1 LX Series User Documentation

LX-4000T Series FIPS 140-2 Non-Proprietary Security Policy

3.1 Models and Model Versions

The module operational environment consists of a physical enclosure and two required firmware images, LinuxITO and PPCiboot. For the currently validated solution the following versions are required:

LinuxITO Version: 6.1.0

PPCiboot Version: 5.3.9

For the LX-4000T Series there are twenty-four hardware configurations as described in Table 2.

Model	Top Level	Rev	B/L	Rev
LX-4008T-001ACF	600-R3265	E	400-R0029	D
LX-4008T-002ACF	600-R3266	E	400-R0029	D
LX-4008T-012DCF	600-R3267	E	400-R0030	D
LX-4008T-101ACF	600-R3268	E	400-R0029	D
LX-4008T-102ACF	600-R3269	E	400-R0029	D
LX-4008T-112DCF	600-R3270	E	400-R0030	D
LX-4016T-001ACF	600-R3271	E	400-R0031	D
LX-4016T-002ACF	600-R3272	E	400-R0031	D
LX-4016T-012DCF	600-R3273	E	400-R0032	D
LX-4016T-101ACF	600-R3274	E	400-R0031	D
LX-4016T-102ACF	600-R3275	E	400-R0031	D
LX-4016T-112DCF	600-R3276	E	400-R0032	D
LX-4032T-001ACF	600-R3277	E	400-R0033	D
LX-4032T-002ACF	600-R3278	E	400-R0033	D
LX-4032T-012DCF	600-R3279	E	400-R0034	D
LX-4032T-101ACF	600-R3280	E	400-R0033	D
LX-4032T-102ACF	600-R3281	E	400-R0033	D
LX-4032T-112DCF	600-R3282	E	400-R0034	D
LX-4048T-001ACF	600-R3283	E	400-R0027	D
LX-4048T-002ACF	600-R3284	E	400-R0027	D
LX-4048T-012DCF	600-R3285	E	400-R0028	D
LX-4048T-101ACF	600-R3286	E	400-R0027	D
LX-4048T-102ACF	600-R3287	E	400-R0027	D
LX-4048T-112DCF	600-R3288	E	400-R0028	D

Table 2 Current Models and Revisions Validated

Prior production revisions including 600-R3265 Rev B through 600-R3288 Rev B (inclusive), 600-R3265 Rev C through 600-R3288 Rev C (inclusive), 600-R3265 Rev D through 600-R3288 Rev D (inclusive) and the models listed above can be updated with the latest LinuxITO and PPCiboot firmware to be considered FIPS 140-2 SL2 validated.

3.2 *Detailed Model Descriptions*

- **LX-4008T-001ACF** : LX-4000T with (8) RS232 RJ45 ports, & single AC power
- **LX-4008T-002ACF** : LX-4000T with (8) RS232 RJ45 ports, & dual AC power
- **LX-4008T-012DCF** : LX-4000T with (8) RS232 RJ45 ports, & dual DC (36-72V) power
- **LX-4008T-101ACF** : LX-4000T with (8) RS232 RJ45 ports, & single AC power & internal V.90 modem
- **LX-4008T-102ACF**: LX-4000T with (8) RS232 RJ45 ports, & dual AC power & internal V.90 modem
- **LX-4008T-112DCF** : LX-4000T with (8) RS232 RJ45 ports, & dual DC (36-72V) power & internal modem V.90
- **LX-40016T-001ACF**: LX-4000T with (16) RS232 RJ45 ports, & single AC power
- **LX-40016T-002ACF** : LX-4000T with (16) RS232 RJ45 ports, & dual AC power
- **LX-40016T-012DCF**: LX-4000T with (16) RS232 RJ45 ports, & dual DC (36-72V) power
- **LX-40016T-101ACF** : LX-4000T with (16) RS232 RJ45 ports, & single AC power & internal V.90 modem
- **LX-40016T-102ACF**: LX-4000T with (16) RS232 RJ45 ports, & dual AC power & internal V.90 modem
- **LX-40016T-112DCF**: LX-4000T with (16) RS232 RJ45 ports, & dual DC (36-72V) power & internal modem V.90
- **LX-40032T-001ACF**: LX-4000T with (32) RS232 RJ45 ports, & single AC power
- **LX-40032T-002ACF**: LX-4000T with (32) RS232 RJ45 ports, & dual AC power
- **LX-40032T-012DCF**: LX-4000T with (32) RS232 RJ45 ports, & dual DC (36-72V) power
- **LX-40032T-101ACF** : LX-4000T with (32) RS232 RJ45 ports, & single AC power & internal V.90 modem
- **LX-40032T-102ACF**: LX-4000T with (32) RS232 RJ45 ports, & dual AC power & internal V.90 modem

LX-4000T Series FIPS 140-2 Non-Proprietary Security Policy

- **LX-40032T-112DCF:** LX-4000T with (32) RS232 RJ45 ports, & dual DC (36-72V) power & internal modem V.90
- **LX-40048T-001ACF:** LX-4000T with (48) RS232 RJ45 ports, & single AC power
- **LX-40048T-002ACF:** LX-4000T with (48) RS232 RJ45 ports, & dual AC power
- **LX-40048T-012DCF:** LX-4000T with (48) RS232 RJ45 ports, & dual DC (36-72V) power
- **LX-40048T-101ACF:** LX-4000T with (48) RS232 RJ45 ports, & single AC power & internal V.90 modem
- **LX-40048T-102ACF:** LX-4000T with (48) RS232 RJ45 ports, & dual AC power & internal V.90 modem
- **LX-4048T-112DCF:** LX-4000T with (48) RS232 RJ45 ports, & dual DC (36-72V) power & internal modem V.90

3.3 Interfaces

The LX-4000T Series solutions are considered multi-chip standalone cryptographic modules. The cryptographic boundary of the module is defined by the outer case of module.

3.4 LX-4000T Series Product Views

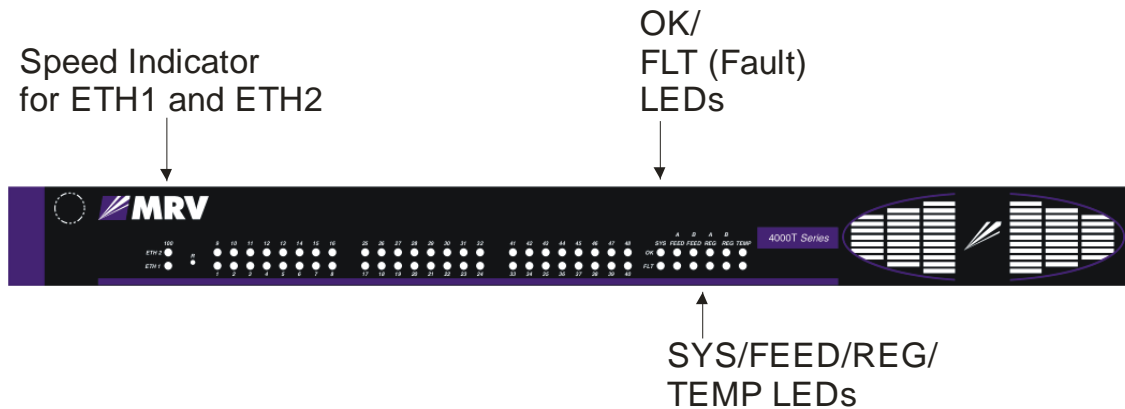


Figure 1 LX-4000T Series Typical Front Panel View (48 Port)

LX-4000T Series FIPS 140-2 Non-Proprietary Security Policy

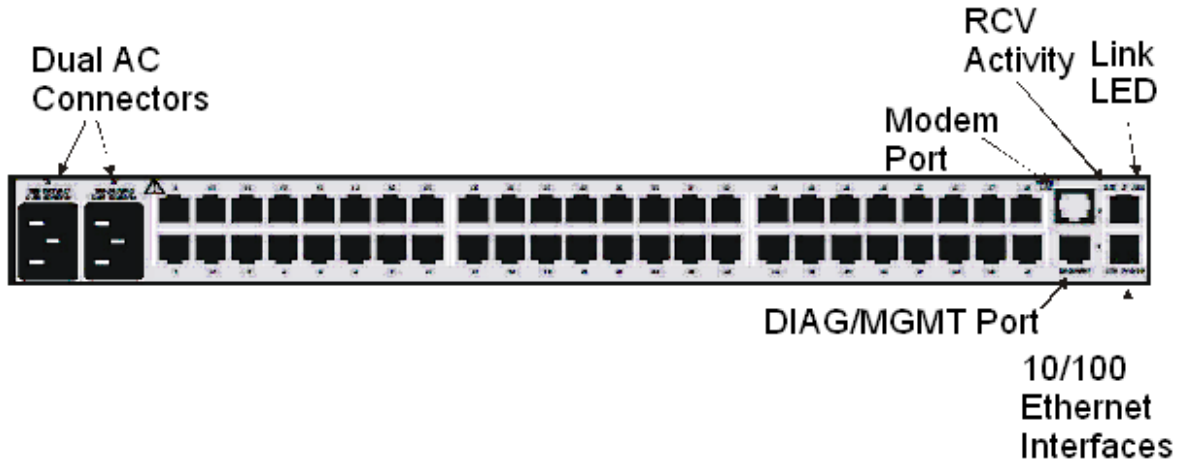


Figure 2 LX-4000T Series Typical Dual AC Rear Panel View (48 Port)

Dual DC Connectors



Figure 3 LX-4000T Series Typical Dual DC Rear Panel View (48 Port)

AC and DC power is fed through the identified power interface ports. The LX-4000T Series solution does not supply power to other devices. Other than the power input, all other ports are identical between AC and DC solutions.

LX-4000T Series FIPS 140-2 Non-Proprietary Security Policy

The logical interfaces and module mapping are described in the following table:

Logical Interface	Physical Interface Mapping
Data Input Interface	2 10/100 BASE-TX Ports 8 RS232 RJ45 Ports / 16 RS232 RJ45 Ports 32 RS232 RJ45 Ports / 48 RS232 RJ45 Ports RS232 RJ45 Diagnostic Management Port RS232 Modem Port
Data Output Interface	2 10/100 BASE-TX Ports 8 RS232 RJ45 Ports / 16 RS232 RJ45 Ports 32 RS232 RJ45 Ports / 48 RS232 RJ45 Ports RS232 RJ45 Diagnostic Management Port RS232 Modem Port
Control Input Interface	Reset Button 2 10/100 BASE-TX Ports 8 RS232 RJ45 Ports / 16 RS232 RJ45 Ports 32 RS232 RJ45 Ports / 48 RS232 RJ45 Ports RS232 RJ45 Diagnostic Management Port RS232 Modem Port
Status Output Interface	LEDs 2 10/100 BASE-TX Ports 8 RS232 RJ45 Ports / 16 RS232 RJ45 Ports 32 RS232 RJ45 Ports / 48 RS232 RJ45 Ports RS232 RJ45 Diagnostic Management Port RS232 Modem Port
Power Interface	Dual AC Power Input / Dual DC Power Input

Table 3 Logical Interface / Module Mapping

3.5 Module Validation Level

The following table lists the validation level for each FIPS PUB 140-2 focus area.

Focus Area	Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	2
Finite State Model	2
Physical Security – Multi-chip standalone cryptographic module	2
Operational Environment	N/A
Cryptographic Key Management	2
Electromagnetic Interface/Electromagnetic Compatibility	2
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A
Overall Module Validation Level	2

Table 4 Module Validation Levels

4 Roles, Services, and Authentication

The LX-4000T Series supports three authorized roles and a set of services specific to each of the roles. The module provides role-based authentication for all operators. The module authenticates an operator by password verification. Each role will then be explicitly assigned based on this authentication. The module implements a permission mechanism depending on the defined security level.

In addition, the module can also authenticate Crypto-Officer or User operators through the use of an authentication server mechanism such as LDAP, Kerberos, RADIUS, TACACS+, and RSA SecurID while in non-FIPS mode.

4.1 Roles

The roles of the module include a PPCIBOOT User role, Crypto-Officer role, and User Role. Services that are available are summarized below.

4.1.1 PPCIBOOT User Role

The PPCIBOOT User has limited responsibilities for configuring the boot loader. The following PPCiboot services are provided:

- Boot Loader Session Establishment
- Boot Parameters Configuration
- PPCiboot Password Update
- FIPS 140-2 mode enable
- FIPS 140-2 mode disable

With the exception of the password update capability, no Key/CSPs can be accessed while in the PPCiboot user role as depicted in Table 5 PPCiboot User Services.

SRDI/Role/Service Access Policy	Security Relevant Data Item	PPCiboot User password	Crypto-Officer password	User password	DSA public key for firmware load	ECDSA public/private Key Pair	Approved SP800-90A DRBG
Boot Loader Session Establishment		X					

LX-4000T Series FIPS 140-2 Non-Proprietary Security Policy

Boot Parameters Configuration							
PPCiboot Password Update	X						
FIPS 140-2 mode enable	Z	Z	Z	Z	Z	Z	na
FIPS 140-2 mode disable	Z	Z	Z	Z	Z	Z	na

Table 5 PPCiboot User Services

The above matrix uses the following convention:

- x: Security Relevant Data Items (SRDI) of the indicated type are used/generated by the service using its associated protocol messages
- z: SRDI of the indicated type that are stored in flash are zeroized by the service at FIPS mode transitions while executing PPCiboot User Role

4.1.2 Crypto-Officer Role

The Crypto-Officer, as the module administrator, establishes the security configuration. The term Superuser and Crypto-Officer are synonymous for the purposes of this policy. The Crypto-Officer is responsible for:

- Subscriber (User) permission levels
- Module service configuration, control, and status
- Serial device connection configuration, control, and status
- Sensor and power management configuration, control, and status

Refer to Table 6 Crypto-Officer Services for an overview of services that are provided.

Please see *LX-Series Commands Reference Guide* for the complete list of corresponding command-line (CLI) services. Please see *LX-Series Configuration Guide* for the complete description of corresponding Console CLI services.

SRDI/Role/Service Access Policy	Security Relevant Data Item	PPCiboot User password	Crypto-Officer password	User password	DSA public key for firmware load	ECDSA public/private Key Pair	Approved SP800-90A DRBG
Role/Service							

LX-4000T Series FIPS 140-2 Non-Proprietary Security Policy

Subscriber (User) Permission levels			p	p			
Module service configuration, control and status							
Additional detail: "reload" initiates self-tests "show" and LEDS provide status "update ppciboot" and "update software" firmware load from the operational environment					X	X	X
Serial device connection configuration, control, and status							
Sensor and power management configuration, control, and status							

Table 6 Crypto-Officer Services

The matrix uses the following convention:

- x: All Security Relevant Data Items (SRDI) of the indicated type are used/generated by the service using its associated protocol messages
- p: Only SRDI of the indicated type that are stored in flash are used by the service

4.1.3 User Role

The term User and Subscriber are synonymous for the purposes of this Security Policy. The User Role has access to a limited set of services as granted by the Crypto-Officer to retrieve information and status as well as limited configuration abilities.

The following services can be provided at Crypto-Officer discretion:

- User password update
- Limited module service configuration, control and status
- Serial device connection, configuration, control and status
- Sensor and power management configuration, control, and status

Please refer to Table 7 User Role Services for an overview of services that are provided:

LX-4000T Series FIPS 140-2 Non-Proprietary Security Policy

SRDI/Role/Service Access Policy	Security Relevant Data Item	PPCiboot User password	Crypto-Officer password	User password	DSA public key for firmware load	ECDSA public/private Key Pair	Approved SP800-90A DRBG
Role/Service							
User password update				X			
Limited module service configuration, control and status							
Serial device connection configuration, control, and status							
Sensor and power management configuration, control, and status							

Table 7 User Role Services

The matrix uses the following convention:

- x: All Security Relevant Data Items (SRDI) of the indicated type are used/generated by the service using its associated protocol messages

4.1.4 Unauthenticated Users/Services

The module provides the following unauthenticated services, which are available regardless of role:

- System status – module LEDs
- Reboot module by removing / replacing power
- Self-test and initialization at power-on

4.1.5 Authentication Actions

Authentication results are stored in the SDRAM and all SDRAM is cleared when the module is powered off or restarted via a reset. The results of all authenticated sessions are cleared. Thus, all operator roles must re-authenticate again to access any services.

4.1.6 Authentication Data Protection

LX-4000T Series FIPS 140-2 Non-Proprietary Security Policy

Only an authenticated Crypto-Officer can access Subscriber (User) and PPCiboot User accounts to protect against unauthorized disclosure, modification and substitution.

By design it is not possible to access the module until the module is initialized.

All authentication data (passwords) are echoed as asterisks during entry to obscure the entry.

Failed log-on attempts are echoed as "Login Incorrect".

4.2 Authentication Mechanisms

Acceptance rate predictions of false and/or random accesses for each authentication method:

PPCIBOOT Authentication Mechanism

Role: PPCIBOOT User

Authentication Type: password based authentication

Authentication Data: PPCiboot User password

The module enforces a 6 character password minimum chosen from the 94 human readable ASCII characters. The probability of a successful random attempt is $1/94^6$ which is less than one in 1,000,000.

The module can process a maximum of 60 attempts in a minute. The probability of a successful authentication attempt within multiple authentication attempts in a one minute period is $60/94^6$ which is less than one in 100,000

Crypto-Officer Authentication Mechanism

Role: Crypto-Officer

Authentication Type: password based authentication

Authentication Data: Crypto-Officer password

The module enforces a 6 character password minimum chosen from the 94 human readable ASCII characters. The probability of a successful random attempt is $1/94^6$ which is less than one in 1,000,000.

The module can process a maximum of 30,720 attempts in a minute. The probability of a successful authentication attempt within multiple authentication attempts in a one minute period is $30,720/94^6$ which is less than one in 100,000.

User Authentication Mechanism

LX-4000T Series FIPS 140-2 Non-Proprietary Security Policy

Role: User

Authentication Type: password based authentication

Authentication Data: User password

The module enforces a 6 character password minimum chosen from the 94 human readable ASCII characters. The probability of a successful random attempt is $1/94^6$ which is less than one in 1,000,000.

The module can process a maximum of 30,720 attempts in a minute. The probability of a successful authentication attempt within multiple authentication attempts in a one minute period is $30,720/94^6$ which is less than one in 100,000.

4.3 Non-Allowed Services in FIPS 140-2 Mode of Operation

Table 8 lists Non-Approved and disabled/dis-allowed services, applications, protocols and features for this release.

Feature	Default Status	Reason	Action / Role
Telnet client/server	Disabled	Connection data can be unencrypted. Lacks authentication services.	Not validated in FIPS 140-2 mode.
rlogin Client	Disabled	All information, including passwords is transmitted unencrypted.	Not validated in FIPS 140-2 mode.
LDAP	Disabled	Passwords are passed in plaintext. Lacks a validated RSA KeyGen method.	Not validated in FIPS 140-2 mode.
RSA SecurID	Disabled	Key exchange and session encryption not FIPS 140-2 validated.	Not validated in FIPS 140-2 mode.
TACACS+	Disabled	Proprietary protocol not FIPS 140-2 validated.	Not validated in FIPS 140-2 mode.
RADIUS	Disabled	Proprietary protocol not FIPS 140-2 validated.	Not validated in FIPS 140-2 mode.
Kerberos V5	Disabled	Proprietary protocol not FIPS 140-2 validated.	Not validated in FIPS 140-2 mode.
SNMP v1 & v2	Disabled	Community strings are passed in plaintext.	Not supported in FIPS 140-2 mode.
SNMP v3	Disabled	Lacks validated KDF tests.	Not validated in FIPS 140-2 mode.
SSHv1 Client / Server	Disabled	Insufficient data integrity protection.	Not supported in FIPS 140-2 mode.
SSHv2 Client / Server (SSH/SFTP/SCP)	Disabled	Lacks validated KDF tests.	Not validated in FIPS 140-2 mode.
Passwords/ Secrets less than 6 characters	Disabled	Due to FIPS 140-2 max authentication fail attempts	6 or greater enforced by software. CO role.
Linux shell access	Restricted	Possible access to secret and private keys	Functionality limited to CO prevent access to CSPs.
Boot firmware image from network	Disabled	Non-validated runtime images could be downloaded.	Boot only allowed from FLASH.

LX-4000T Series FIPS 140-2 Non-Proprietary Security Policy

Updating ppciboot.img from PPCiboot menu	Disabled	Non-validated runtime images could be downloaded.	Update only allowed from validated runtime image. CO.
Updating linuxito.img from PPCiboot menu	Disabled	Non-validated runtime images could be downloaded	Update only allowed from validated runtime image. CO.
Login mode shell	Disabled	Possible access to secret and private keys	Not supported in FIPS 140-2 mode.
Broadcast Groups	Disabled	Multiple connections to and from multiple systems which may or may not be FIPS 140-2 validated.	Not validated in FIPS 140-2 mode.
Fingerd	Disabled	Allows anyone to see who is logged in.	Not supported in FIPS 140-2 mode.
Load CONFIG from network	Disabled	Configuration information, while signed is stored in clear text.	Not validated in FIPS 140-2 mode.
Save CONFIG to network	Disabled	Configuration information, while signed is stored in clear text.	Not validated in FIPS 140-2 mode.
Remote SYSLOG	Disabled	Configuration information is clear text	Not validated in FIPS 140-2 mode.
No Authentication for local or interface access	Disabled	Unencrypted connections not allowed in FIPS 140-2 operation.	Not validated in FIPS 140-2 mode.
No Authentication for remote access or dynamic access ports (when accessed remotely)	Disabled	Bypasses port authentication	Not validated in FIPS 140-2 mode.
Dedicated Services	Disabled	Passwords are passed in plaintext.	Not validated in FIPS 140-2 mode.
DHCP	Disabled	PPCiboot network load disallowed in FIPS mode.	Use appropriate command from LinuxlTO. CO.
BOOTP	Disabled	PPCiboot network load disallowed in FIPS mode.	Use appropriate command from LinuxlTO. CO.
RARP	Disabled	PPCiboot network load disallowed in FIPS mode.	Use appropriate command from LinuxlTO. CO
NTP	Disabled	N/A	Crypto-Officer choice.
PPP (None/PAP/CHAP)	Disabled	N/A	Crypto-Officer choice.
Timed	Disabled	N/A	Crypto-Officer choice.
Fallback	Disabled	N/A	Crypto-Officer choice.
TCP Pipe	Disabled	TCP Pipe lacks user authentication.	Not validated in FIPS 140-2 mode.
IPSEC / IKE v2	Disabled	IPSEC / IKE V2 not FIPS 140-2 validated.	Not validated in FIPS 140-2 mode.
IPSEC / IKE v1	Disabled	Lacks validated KDF tests.	Not validated in FIPS 140-2 mode.
WEB GUI Services using TLS v1.1	Disabled	Lacks validated KDF tests.	Not validated in FIPS 140-2 mode.
WEB GUI Services using TLS v1.2	Disabled	Lacks validated KDF Tests	Not validated in FIPS 140-2 mode.
Cluster Configuration and Control (CCC)	Disabled	Lacks validated KDF tests	Not validated in FIPS 140-2 mode.
EXPECT Scripting	Disabled	Considered untrusted software	Not supported in FIPS 140-2 mode.

Table 8 Non-Allowed Services, Applications, Protocols and Features

5 Cryptographic Algorithms

The LX-4000T Series Cryptographic Module supports many cryptographic algorithms. Only FIPS validated algorithms are used while in the FIPS operational mode.

5.1 LX-Series Algorithm Core

Type	Algorithm	Modes	Key Size	Cert #
Symmetric Block Cipher	AES	ECB, CBC, OFB, CFB8, CFB128, CTR	128/192/256	#3765
Symmetric Block Cipher	Triple-DES	TECB, TCBC	192	#2093
Hash	SHA-1/SHA-2 (224, 256, 384,512)	-	-	#3134
Message Authentication	HMAC SHA-1 HMAC SHA-256	-	-	#2464
Asymmetric Key Cipher	ECDSA	PKG, PKV, SigGen, SigVer	P-256/P-384/P-521	#808
Asymmetric Key Cipher	DSA	PQG(gen), PQG(ver), Key Pair Gen, Sig(gen), Sig(ver)	2048/3072 with all SHA-2 sizes	#1046
DRBG	SP800-90A	CTR DRBG (AES-256)	-	#1035

Table 9 FIPS Validated Cryptographic Functions – Algorithm Core

Note: The module implements the power-up self-test service to each algorithm listed in Table 9. However, the module doesn't use Triple-DES Cert. #2093, HMAC Cert. #2464 and ECDSA Cert. #808 algorithms and DSA2048 in other security services while in FIPS mode at this time.

5.2 LX-Series Algorithm IPsec Core

Type	Algorithm	Modes	Key Size	Cert #
Symmetric Block Cipher	AES	CBC	128/192/256	#3764
Symmetric Block Cipher	Triple-DES	CBC	192	#2092
Hash	SHA-1, 256	-	-	#3133
Message Authentication	HMAC SHA-1, 256	-	-	#2463

Table 10 FIPS Validated Cryptographic Algorithms - IPSEC Core

Note: The module implements the power-up self-test service to each algorithm listed in Table 10. However, the module doesn't use AES Cert #3764, Triple-DES

LX-4000T Series FIPS 140-2 Non-Proprietary Security Policy

Cert. #2092, SHA Cert. #3133 and HMAC Cert. #2463 algorithms in other security services while in FIPS mode at this time.

5.3 Non-FIPS Approved But Allowed Function

Type	Algorithm	Modes	Key Size
Non-Approved RNG (NDRNG)	-	-	-

Table 11 Non-FIPS Validated But Allowed Function

Note:

- The Non-approved RNG is allowed in FIPS mode to seed the approved SP800-90A DRBG.

5.4 Non-FIPS Allowed Algorithms

The module implements the following algorithms which are non-Approved per the SP800-131A transition. These algorithms shall not be used when operating in the FIPS approved mode of operation.

- DES
 - Optional selection for RSA SecurID encryption in non-FIPS mode
 - Optional selection for SNMP in non-FIPS mode
- RSA (non-compliant)
 - Optional selection for SSH/SFTP/SCP key in non-FIPS mode
 - LDAP key in non-FIPS mode
 - Encrypt, Decrypt, KeyGen, Key Wrapping
 - 2048/3072/4096 w SHA-2 Keys
- MD5
 - Optional selection for SNMP V3 in non-FIPS mode
 - Used in Radius authentication in non-FIPS mode
 - Used in TACACS+ in non-FIPS mode
- HMAC-MD5
 - Optional selection for IPSEC/IKE in non-FIPS mode
- EC Diffie-Hellman
 - Used in TLS V1.2 and SSH services in non-FIPS mode
 - All NIST defined B, K and P Curves
- Non-compliant KDFs (Not tested through the NIST CAVP):
 - IKEv1 KDF
 - IKEv2 KDF
 - SNMP KDF
 - SSH KDF
 - TLS KDF

6 Setting FIPS 140-2 Mode

The following sections guide the Crypto-Officer through the installation and configuration of the LX-4000T Series cryptographic module to meet the requirements for FIPS 140-2 validated operation. Please see the user documentation *Installing the LX-4000T Series* for additional detail about how to install the module.

6.1 Prerequisites

The following requirements must be met to use the product in a FIPS 140-2 SL2 validated configuration:

- You must be running the firmware on the FIPS 140-2 tested LX-Series platform.
- You must place the provided Tamper Evident Labels (TEL) in the proper locations. See Section 6.3.
- You must use the FIPS 140-2 validated versions of the LX-Series LinuxITO and PPCiboot firmware. *Only specific versions of the LX-Series firmware are tested by an accredited cryptographic module test lab.*
- FIPS 140-2 mode must be enabled on the LX-Series FIPS 140-2 validated unit(s). See Section 6.4 Enabling FIPS 140-2 Mode of Operation.

6.2 Notes and Restrictions

- The default subscriber (user), named *InReach*, password must be changed.
- The default PPCiboot password must be changed.
- The default system password must be changed.
- Passwords must be greater than or equal to 6 characters in length. In some applications, greater minimums are enforced. Refer to Table 13 Cryptographic Keys, CSPs and SRDIs.

6.3 Applying Tamper Evident Labels

NOTE: The Tamper Evident Labels shall be installed by the CO for the module to operate in a FIPS approved mode of operation.

LX-4000T Series FIPS 140-2 Non-Proprietary Security Policy

Once the LX has been configured in FIPS 140-2 mode, the cover cannot be removed without signs of tampering. Applying Tamper Evident Labels to the LX-4000T Series unit will prevent anyone from opening the unit without your knowledge.

To seal the cover of the LX, the CO must apply the (4) Tamper Evident Labels as follows:

1. Clean the LX surface of any grease or dirt before you apply the Tamper Evident Labels.
2. Apply two labels each to the bottom left and right sides of the unit, as shown in Figure 4 Tamper Evident Label Recommended Placement.

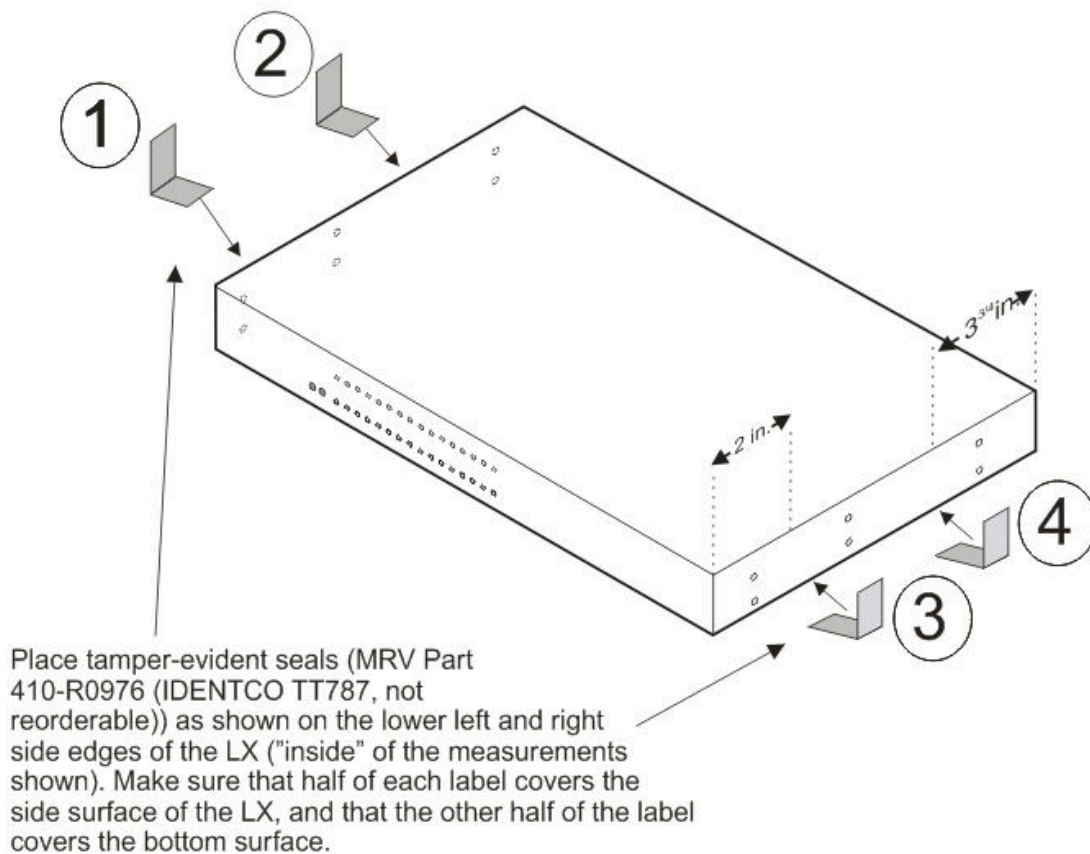


Figure 4 Tamper Evident Label Recommended Placement

3. Record the serial numbers of the labels you attached to the LX-4000T Series unit.
4. Allow 24 hours for the adhesive in the tamper-evident labels to cure.

LX-4000T Series FIPS 140-2 Non-Proprietary Security Policy

6.3.1 Operator Required Actions

The CO is required to inspect the Tamper Evident Labels periodically per Table 12 Inspection / Testing of Physical Security Mechanisms.

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection / Test Guidance
Tamper Evident Labels	12 months	Reference Section 6.3

Table 12 Inspection / Testing of Physical Security Mechanisms

The inspection should insure the labels continue to be securely attached and have not been tampered with. If evidence of tampering is found with the Tamper Evident Labels, the module must immediately be powered down and all administrators must be made aware of a physical security breach.

NOTE: Any unused TELs must be securely stored, accounted for, and maintained by the CO in a protected location.

NOTE: There are no user serviceable parts in the unit. TELs are not re-orderable.

6.4 Enabling FIPS 140-2 Mode of Operation

IMPORTANT!

If you want to configure your unit to run FIPS 140-2 Mode of Operation, you must do so **before** you attempt to configure the unit over and above the default settings. The act of enabling FIPS 140-2 mode will default the unit's configuration.

When FIPS 140-2 is enabled, the configuration file is returned to defaults. Therefore, if you had previously fully configured your unit and then turned on FIPS 140-2, your configuration will return to factory defaults. FIPS 140-2 mandates this to ensure that any passwords with fewer than six characters are purged, and that all unsupported applications are disabled.

NOTE:

When FIPS 140-2 Security is enabled via the PPCiboot Option [7] (See Figure 5 Boot Selection Screen), Option [1] Boot from Network is set to *Flash only* automatically. You can only update the images from operational environment while FIPS 140-2 is enabled. Option [4] *Update PPCiboot Firmware* is disabled when FIPS 140-2 is enabled.

LX-4000T Series FIPS 140-2 Non-Proprietary Security Policy

The FIPS 140-2 Security option lets you enable or disable FIPS 140-2 mode of operation.

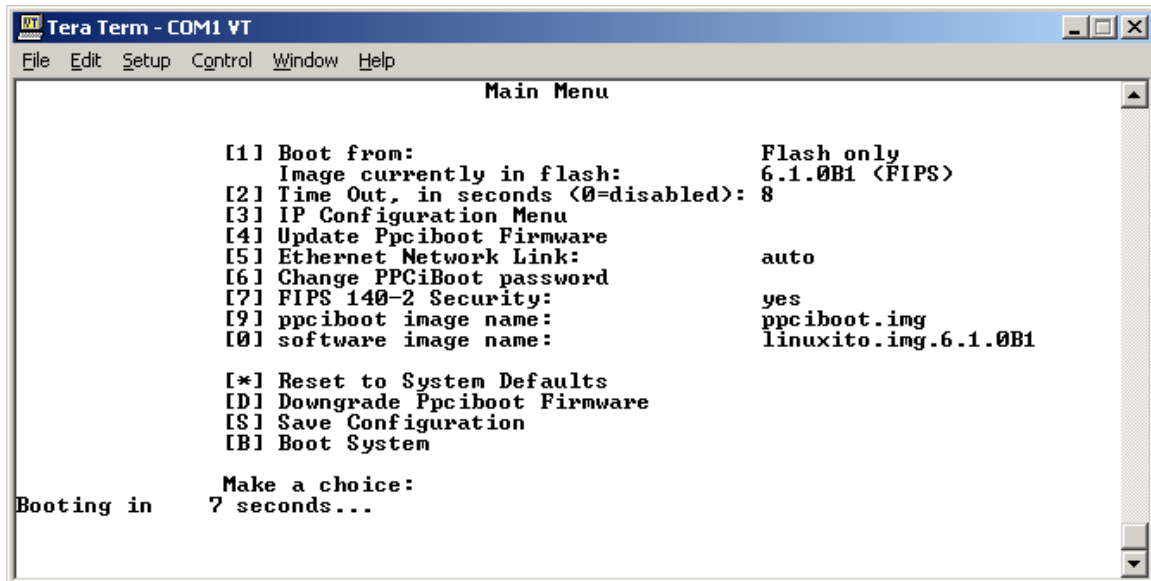


Figure 5 Boot Selection Screen

To enable or disable FIPS 140-2 Security Mode:

1. Enter the number 7 (FIPS 140-2 Security). The following prompt appears:
Enabling FIPS security will reset run-time configuration to defaults. Are you sure? (y/n):
2. If you select y (this defaults the flash immediately), a *Resetting Linux Configuration* message appears, and the Main Menu reappears after a few seconds. If you select n, the Main Menu reappears immediately.
3. If FIPS 140-2 is already enabled and you want to disable it, press 7 (FIPS 140-2 Security) from the Main Menu.
4. Update the PPCiboot password while at this screen per Section 6.5 Changing the Default PPCiboot Password

6.5 Changing the Default PPCiboot Password

After enabling the FIPS 140-2 Mode, you must enter a new PPCiboot password of minimum of six characters.

The *Change PPCiboot Password* option lets you change the PPCiboot password for the unit. To change the PPCiboot password:

1. Referring to Figure 5, select the number 6 (Change PPCiboot Password). The following prompt is displayed:

LX-4000T Series FIPS 140-2 Non-Proprietary Security Policy

Enter current password:

Enter the current PPCiboot password at the above prompt. After you have entered the current PPCiboot password, the following prompt is displayed:

Enter a new password (max. length is 32 char):

2. Enter the new PPCiboot password at the above prompt. The password must be a minimum of six characters.

After you have entered the new PPCiboot password, the following prompt is displayed:

Enter a new password again:

Re-enter the new PPCiboot password at the above prompt. A confirmation message is displayed.

3. Configure all other required PPCiboot options.
4. Save the configuration.
5. Press B to Boot the system

6.6 Confirming Your Firmware is FIPS 140-2 Validated

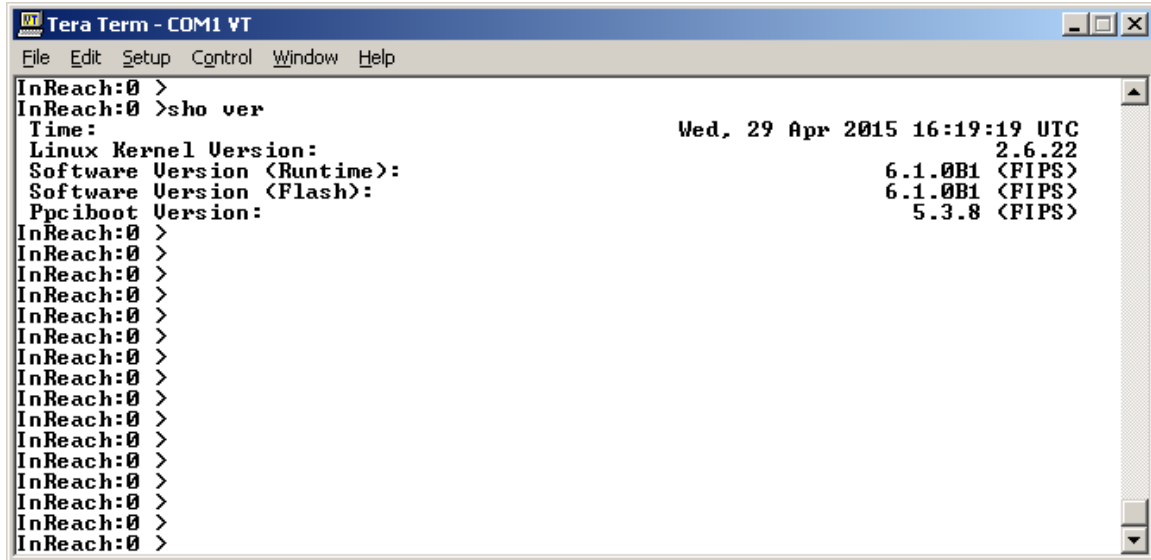
Do the following to determine if the firmware image you are running is FIPS 140-2 Validated:

1. Log into the CLI.
2. Enter the show version command at the **InReach:0 >** prompt; for example:

InReach:0 > show version

The Show Version screen appears (Figure 6), with the relevant fields highlighted:

LX-4000T Series FIPS 140-2 Non-Proprietary Security Policy



```
Tera Term - COM1 VT
File Edit Setup Control Window Help
InReach:0 >
InReach:0 >sho ver
Time: Wed. 29 Apr 2015 16:19:19 UTC
Linux Kernel Version: 2.6.22
Software Version (Runtime): 6.1.0B1 <FIPS>
Software Version (Flash): 6.1.0B1 <FIPS>
Ppciboot Version: 5.3.8 <FIPS>
InReach:0 >
InReach:0 >
InReach:0 >
InReach:0 >
InReach:0 >
InReach:0 >
InReach:0 >
InReach:0 >
InReach:0 >
InReach:0 >
InReach:0 >
InReach:0 >
InReach:0 >
InReach:0 >
InReach:0 >
InReach:0 >
InReach:0 >
```

Figure 6 Show Version Screen

If the firmware you are running has been FIPS 140-2 validated, the word <FIPS> appears to the right of the Software Version number and the PPCiboot Version number. If <FIPS> does not appear, your firmware has not been validated.

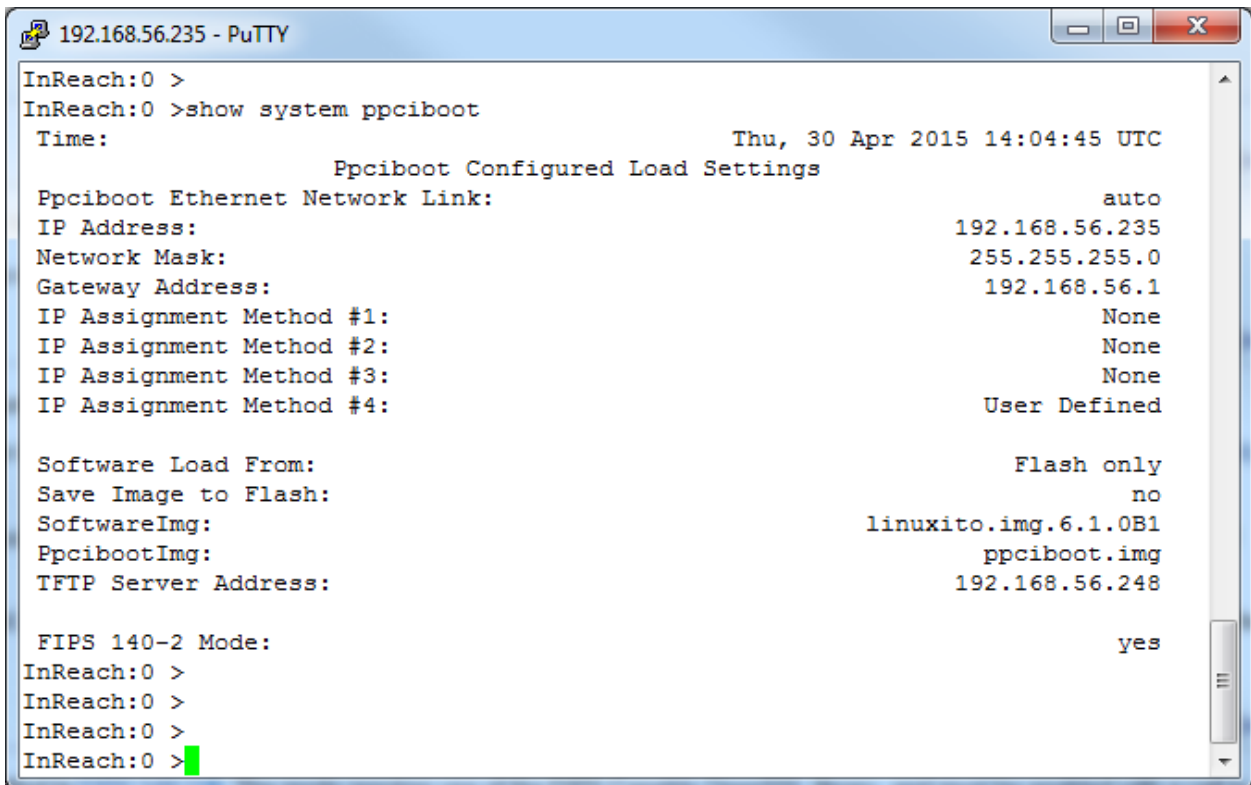
LX-4000T Series FIPS 140-2 Non-Proprietary Security Policy

6.7 Confirming FIPS 140-2 Mode of Operation

While running the LinuxITO, issue the following command:

```
InReach:0 > show system ppciboot
```

The following is displayed:



```
InReach:0 >
InReach:0 >show system ppciboot
Time:                               Thu, 30 Apr 2015 14:04:45 UTC
                                Ppciboot Configured Load Settings
Ppciboot Ethernet Network Link:      auto
IP Address:                          192.168.56.235
Network Mask:                        255.255.255.0
Gateway Address:                     192.168.56.1
IP Assignment Method #1:             None
IP Assignment Method #2:             None
IP Assignment Method #3:             None
IP Assignment Method #4:             User Defined

Software Load From:                  Flash only
Save Image to Flash:                 no
SoftwareImg:                         linuxito.img.6.1.0B1
PpcibootImg:                         ppciboot.img
TFTP Server Address:                 192.168.56.248

FIPS 140-2 Mode:                     yes
InReach:0 >
InReach:0 >
InReach:0 >
InReach:0 >
```

Figure 7 Determining FIPS Mode status

Note the line **FIPS 140-2 Mode**. **Yes** indicates it is enabled, **No** indicates it has not yet been enabled via the PPCiboot menu selection.

6.8 Changing the Default Subscriber Password

It is widely known that the default password for the **InReach** user is **access**. If an unauthorized user knew this username/password combination, he/she could log on to your LX-4000T Series unit. For this reason, you must change the InReach user's password to something other than **access**. The password must be at least six characters long.

Do the following to change the User-level password of the **InReach** User:

1. Access the Configuration Command Mode.
2. Access the Subscriber Command Mode for the **InReach** subscriber. You do this by entering the subscriber command with **InReach** as the command argument; for example:

```
Config:0 >> subscriber InReach
```

3. Enter the password command at the **Subs_InReach >>** prompt; for example:

```
Subs_InReach:0 >> password
```

4. Enter a new User password at the **Enter your NEW password:** prompt. The password will be displayed as asterisks, as in the following example:

```
Enter your NEW password:*****
```

5. Re-enter the new User password at the **Re-Enter your NEW password:** prompt. The password will be displayed as asterisks, as in the following example:

```
Re-Enter your NEW password:*****
```

6.9 Changing the Default Superuser Password

It is also widely known that the default Superuser password is **system**. To reduce the risk of an unauthorized user gaining access to the Superuser Command Mode, you must change this password to something other than **system**. The password must be at least six characters long.

To change the Superuser password for the LX-4000T Series unit, do the following:

1. Access the Superuser configuration command Mode.
2. Enter the password command at the **Config:0 >>** prompt; for example:

```
Config:0 >>password
```

LX-4000T Series FIPS 140-2 Non-Proprietary Security Policy

3. Enter a new Superuser password at the **Enter your NEW password:** prompt. The password will be displayed as asterisks, as in the following example:

Enter your NEW password:*****

4. Re-enter the new Superuser password at the **Re-Enter your NEW password:** prompt. The password will be displayed as asterisks, as in the following example:

Re-Enter your NEW password: *****

6.10 FIPS 140-2 Mode Console Access

You must use the console port to gain access to the module.

6.11 Upgrading Firmware

The ppciboot.img.sign and linuxito.img.sign digital signature files are used to authenticate firmware images during updating. Place these files along with the image files on the SFTP file server. Crypto Officer initiated *software update* commands from the Superuser operational environment will validate downloaded images using the sign file automatically.

Refer to “How to Upgrade the Software” in the *LX-Series Configuration Guide* for more information on upgrading the firmware.

7 Cryptographic Key Management

This section specifies the Security Relevant Data Items (SRDI), Critical Security Parameters (CSP) and Cryptographic Key Management when operating in a FIPS 140-2 Security Level 2 validated manner.

Security Relevant Data Item	Algorithm / Size	SRDI Description	Storage	Zeroization (see Method Definition below)
User Password	Password	6+ Char Minimum Password for User role authentication. Zeroization of these passwords reset them to product defaults.	FLASH	Methods 1 - 3
Crypto-Officer Password	Password	6+ Char Minimum Password for CO role authentication. Zeroization of these passwords reset them to product defaults.	FLASH	Methods 1 - 3
PPCiboot Password	Password	6+ Char Minimum Password for PPCiboot user role authentication. Zeroization of these passwords reset them to product defaults.	FLASH	Methods 1 - 3
Signature Sign/Verify				
Host public key	ECDSA P-256	ECDSA public key used for signature verification operation. It is generated by calling SP800-90A CTR_DRBG	FLASH	Methods 1 - 3
Host private key	ECDSA P-256	ECDSA private key used for signature sign operation. It is generated by calling SP800-90A CTR_DRBG.	FLASH	Methods 1 - 3
DSA public key	3072 bits w SHA-512	DSA public key used for signature verification operation when loading firmware. It is generated by calling SP800-90A CTR_DRBG.	FLASH	Methods 1 - 3
Approved SP800-90A DRBG				
DRBG Entropy Input	256 bits	Entropy inputs to DRBG function used to construct the DRBG seed.	SDRAM	Methods 4 - 5
DRBG Seed	384 bits	Input to the DRBG that determines the internal state of the DRBG. Generated using DRBG derivation function that includes the entropy input from the entropy source.	SDRAM	Methods 4 - 5
DRBG V	128 bits	Internal value derived as part of the DRBG operation.	SDRAM	Methods 4 - 5
DRBG Key	256 bits	Internal value derived as part of DRBG initialization	SDRAM	Methods 4 - 5

Table 13 Cryptographic Keys, CSPs and SRDIs

LX-4000T Series FIPS 140-2 Non-Proprietary Security Policy

7.1 Zeroization Methods Key

Method 1: Enter FIPS Mode from a non-FIPS operational status

Method 2: Exit FIPS Mode

Method 3: From the LinuxITO operational environment, under Superuser/CO role, issue the command:

```
InReach:0>> config default config
```

Method 4: Power Cycle or Hardware Reset of the Unit

Method 5: Under Superuser/CO role, issue:

```
InReach:0 >> reload
```

7.2 Critical Security Parameter Actions

Two independent actions are required to view the CSPs

1. The Operator must authenticate as a user or as the Crypto-Officer
2. The authenticated operator must execute the “show config” command

7.3 Key Generation

7.3.1 DRBG Used

The module implements a DRBG per the NIST SP800-90A, January 2012 recommendations. All key generation functions when in FIPS 140-2 operation mode call the approved DRBG implementation.

7.3.2 Intermediate Key Generation Values

Intermediate Key Generation Values are not output.

7.3.3 Key Generation Methods

The module generates all cryptographic keys compliant with the requirements defined in “Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program”, January 11, 2016 Section 7.8.

8 Self-Tests

8.1 Firmware Function Power On Self-Tests

Note all Power On Self-Tests (POSTs) are run on all start-up or restarts regardless of FIPS mode status. POST failures will result in a module restart.

8.1.1 LX-Series Algorithm Core Algorithm Implementation POSTs

- PPCiboot integrity test (CRC32)
- LinuxITO firmware integrity test (CRC32)
- AES (encrypt and decrypt) Known Answer Test (KATs)
- RSA (sign and verify) KATs¹
- RSA(encrypt and decrypt) KATs¹
- Triple-DES (encrypt and decrypt) KATs¹
- DSA signature sign and verify Pairwise Consistency Test (PWCT)
- ECDSA signature sign and verify PWCT¹
- SHA-1 KAT¹
- HMAC-SHA1 KAT¹
- HMAC-SHA224, -SHA256, -SHA384 and -SHA512 KAT^{1 2}
- SP800-90A DRBG KAT (Instantiate function KAT, Generate function KAT and Reseed function KAT)

Notes:

1. The module performs the indicated tests during the power on self-test. However, the module doesn't use those algorithms while in the FIPS mode.
2. Per IG 9.1, this testing covers SHA POST requirements

8.1.2 LX-Series Algorithm IPSEC Core Algorithm Implementation POSTs

- AES (encrypt and decrypt) KATs¹
- Triple-DES (encrypt and decrypt) KATs¹
- SHA-1 KAT¹
- HMAC-SHA1 KAT¹
- HMAC-SHA256 KAT^{1 2}

Notes:

1. The module performs the indicated tests during the power on self-test. However, the module doesn't use those algorithms while in the FIPS mode.

LX-4000T Series FIPS 140-2 Non-Proprietary Security Policy

2. Per IG 9.1, this testing covers SHA POST requirements.

8.2 Conditional Tests

LX-4000T Series products execute the following tests conditionally as applications require crypto services:

- Continuous Random Number Generator Test (CRNGT) for the FIPS approved SP800-90a CTR_DRBG.¹
- Continuous Random Number Generator Test to NDRNG.¹
- DSA Pairwise consistency test²
- ECDSA Pairwise consistency test²
- LinuxITO firmware load verification test³
 - 3072 bits DSA with SHA-512 Public Key
- PPCiboot firmware load verification test³
 - 3072 bits DSA with SHA-512 Public Key

Notes:

1. CRNGT test failures will result in a module panic and restart
2. PCT test failures result in a user message that the requested key generation failed.
3. Firmware load verification test failures result in a “Verification Failed” user message and the image is not updated.

9 Design Assurance

The module firmware images are pre-installed in the flash in a secure manufacturing facility. All shipping occurs via a reputable courier service. The administrator should inspect the shipment to make sure the boxes have not been tampered with or damaged upon receiving the modules. Damaged goods could indicate a security compromise.

10 Mitigation of Other Attacks

Additional design features were not employed to prevent attack scenarios described in the FIPS PUB 140-2. This section is not applicable.