FIPS 140-2 Non-Proprietary Security Policy

Uplogix LM80, LM83X, 500, and 5000

Lantronix, Inc.
48 Discovery, Suite 250
Irvine, CA 92618
USA

May 11, 2023

Document Version 3.0

Table of Contents

Table of Figures

Table of Tables

FIPS 140-2 Non-Proprietary Security Policy
Uplogix LM80, LM83X, 500, and 5000

1. Introduction

This document describes the Non-Proprietary FIPS 140-2 Security Policy for the Uplogix LM80, LM83X, 500, and 5000 modules.

The Uplogix Local Manager is a network independent management platform that is located with - and directly connected to - managed devices. It can stand alone or augment your existing centralized management tools providing the configuration, performance, and security management automation functions that are best performed locally.

The benefits are reduced operational costs, faster resolution when issues arise, and improved security and compliance versus centralized management. An enhanced focus on network devices readies your management systems for the transition to the production use of more network sensitive cloud and virtual infrastructure technologies.

The Uplogix LM80, LM83X, 500, and 5000 modules, also known as Local Managers (LM), are powered by the Uplogix firmware, also known as the Local Management Software (LMS), to automate hundreds of routine system maintenance, configuration, fault diagnosis, and recovery operations. These capabilities combined with FIPS 140-2 security enable the Uplogix platform to provide secure remote access and control in a variety of environments.

In this document the Uplogix LM80, LM83X, 500, and 5000 modules are also referred to as "Uplogix LM", "LM", "Local Manager", or "the module".

1.1. Purpose

This document covers the secure operation of the Uplogix LM80, LM83X, 500, and 5000 Local Managers including the initialization, roles, and responsibilities of operating the product in a secure, FIPS-compliant manner. This document applies to LMS firmware version 6.1.1.39602g which runs on the product.

Any firmware [software] loaded into this module that is not shown on the module certificate is out of the scope of this validation and requires a separate FIPS 140-2 validation.

1.2. Models Tested

Table 1: Models Tested under FIPS certificate #

Model	Firmware Version	Hardware Version
Uplogix FIPS LM80 Local Manager, 8 Serial Ports + 3 Ethernet Ports	6.1.1.39602g	80-8S-NNN-YAA
Uplogix FIPS LM83X Local Manager, 8 Serial Ports + 3 Ethernet Ports	6.1.1.39602g	83X-8S-000-YAA
Uplogix FIPS 500 Local Manager, 6 Serial Ports	6.1.1.39602g	61-5050-33
Uplogix FIPS 5000 Local Manager, 6 Serial Ports + 2 Expansion Bays	6.1.1.39602g	61-5500-33
Tamper Evident Labels	N/A	61-0001-00

Note: All are available with a V.92 modem, a cellular modem, a DB9 connection for a modem, an Ethernet SFP cage, or a blank over the mezzanine option slot.

The 5000 has two option slots on the front for connecting I/O modules. The LM83X has three option slots. I/O modules are available as an 8-port serial card, a 16-port serial card, and an 8-port Ethernet card.

1.3. Security Level

The table below identifies the level of validation for each of the sections in FIPS 140-2.

Table 2: FIPS Section Validation Levels

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

1.4. Glossary

Table 3: Glossary of Terms

Term/Acronym	Description
AC	Alternating Current
ACL	Access Control List
AES	Advanced Encryption Standard
CA	Certificate Authority
CBC	Cipher-Block Chaining

Term/Acronym	Description
CKG	Cryptographic Key Generation
CSP	Critical Security Parameter
CSR	Certificate Signature Request
DH	Diffie-Hellman
DHE	Diffie-Hellman Ephemeral
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ENT (NP)	Entropy (non-physical)
FFC	Finite Field Cryptography
FIPS	Federal Information Processing Standard
GMAC	Galois Message Authentication Code
HMAC	Hash-based Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure which uses TLS
I/O	Input/Output
IKE	Internet Key Exchange
IPMI	Intelligent Platform Management Interface
IPsec	Internet Protocol Security
KAS	Key Agreement Scheme
KDA	Key Derivation Algorithm
KDF	Key Derivation Function
LCD	Liquid Crystal Display
LM	Local Manager
LMS	Local Management Software
LRNG	Linux Random Number Generator written by Stephan Mueller to replace the Linux /dev/random implementation
MAC	Message Authentication Code
MD5	Message-Digest algorithm 5
NSS	Network Security Services
Non-IID	Not Independent and Identically Distributed
PBKDF2	Password-Based Key Derivation Function 2
PPP	Point-to-Point Protocol

Term/Acronym	Description
PPTP	Point-to-Point Tunneling Protocol
RADIUS	Remote Authentication Dial in User Service
RNG	Random Number Generator
RSA	Rivest, Shamir, and Adleman
SHA	Secure Hash Algorithm
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SMTPS	SMTP secured with TLS
SNMP	Simple Network Management Protocol
SRDI	Security Relevant Data Items
SSC	Shared Secret Computation
SSH	Secure Shell
TACACS+	Terminal Access Controller Access-Control System Plus
TEL	Tamper Evident Label
TLS	Transport Layer Security
Uplogix LM80 Local Manager	Comprehensive functionality in a fixed 8-port LM designed for enterprises needing to monitor, manage and control 8 or fewer devices and their power supplies at any distributed location.
Uplogix LM83X Local Manager	Uplogix Local Manager, available in 8 to 56 port models, delivers advanced remote management capabilities for data centers, branch offices, and remote locations.
Uplogix 500 Local Manager	Comprehensive functionality in a fixed 6-port LM designed for enterprises needing to monitor, manage and control six or fewer devices and their power supplies at any distributed location.
Uplogix 5000 Local Manager	Uplogix Local Manager, available in 6 to 38 port models, delivers advanced remote management capabilities for data centers, branch offices, and remote locations.
UCC	Uplogix Control Center is the web-based, centralized point of control for all Uplogix Local Managers and managed devices throughout your environment.
USB	Universal Serial Bus
VPN	Virtual Private Network

2. Physical Characteristics of Product Family

The Uplogix LM80, LM83X, 500, and 5000 are individually considered multi-chip standalone modules, and the cryptographic boundary of the modules is defined by the outer case of the modules. All components of the module are made of production-grade materials.

2.1. Uplogix LM80

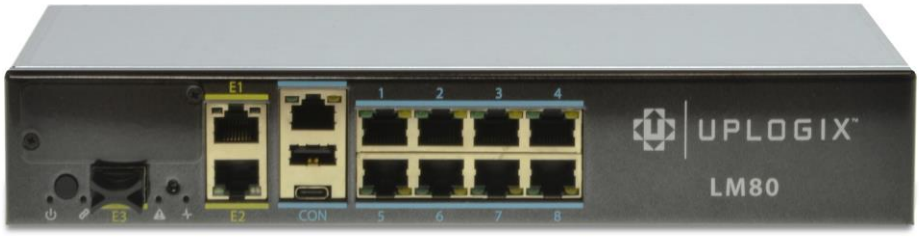

Figure 1: Uplogix LM80 Front Side

Figure 2: Uplogix LM80 Back Side

Table 4: Uplogix LM80 Logical Interfaces and their Behavior

Logical Interface	Logical Interface Behavior
Primary Ethernet	Data In and Out, Control In, Status Out
Secondary Ethernet	Data In and Out, Control In, Status Out
USB-A port	Data In and Out, Control In, Status Out, Power Out
USB-C port	Data In and Out, Control In, Status Out, Power Out
Console	Data In and Out, Control In, Status Out
Mezzanine Option Slot	Data In and Out, Control In, Status Out
SFP cage	Data In and Out, Control In, Status Out
Eight (8) Serial Ports*	Data In and Out
LEDs	Status Out
Reset Button	Control In
Power Button	Control In

* The Uplogix LM80 serial ports are used by the Local Manager to connect to devices being managed.

2.2. Uplogix LM83X

Figure 3: Uplogix LM83X Front Side

Figure 4: Uplogix LM83X Back Side

Table 5: Uplogix LM83X Logical Interfaces and their Behavior

Logical Interface	Logical Interface Behavior
Primary Ethernet	Data In and Out, Control In, Status Out
Secondary Ethernet	Data In and Out, Control In, Status Out
USB-A port	Data In and Out, Control In, Status Out, Power Out
USB-C port	Data In and Out, Control In, Status Out, Power Out
Console	Data In and Out, Control In, Status Out
Mezzanine Option Slot	Data In and Out, Control In, Status Out
SFP cage	Data In and Out, Control In, Status Out
Eight (8) Serial Ports*	Data In and Out
LEDs	Status Out
Reset Button	Control In
Power Button	Control In

* The Uplogix LM83X serial ports are used by the Local Manager to connect to devices being managed.

2.3. Uplogix 500

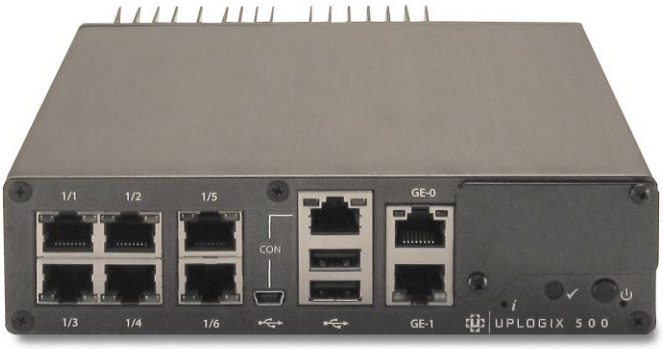

Figure 5: Uplogix 500 Front Side

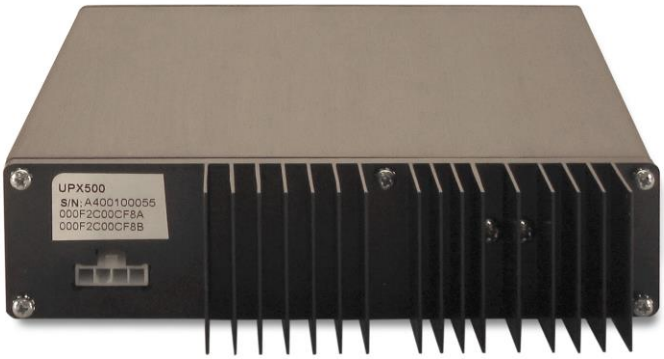

Figure 6: Uplogix 500 Back Side

Table 6: Uplogix 500 Logical Interfaces and their Behavior

Logical Interface	Logical Interface Behavior
Primary Ethernet	Data In and Out, Control In, Status Out
Secondary Ethernet	Data In and Out, Control In, Status Out
Two (2) USB ports	Data In and Out, Control In, Status Out, Power Out
Mezzanine Option Slot	Data In and Out, Control In, Status Out
Six (6) Serial Ports*	Data In and Out
LEDs	Status Out
Console	Data In and Out, Control In, Status Out
USB Console	Data In and Out, Control In, Status Out
Multipurpose Button	Control In
Power Button	Control In

* The Uplogix 500 serial ports are used by the Local Manager to connect to devices being managed.

2.4. Uplogix 5000

Figure 7: Uplogix 5000 Front Side

Figure 8: Uplogix 5000 Back Side

Table 7: Uplogix 5000 Logical Interfaces and their Behavior

Logical Interface	Logical Interface Behavior
Primary Ethernet	Data In and Out, Control In, Status Out
Secondary Ethernet	Data In and Out, Control In, Status Out
Two (2) USB ports	Data In and Out, Control In, Status Out, Power Out
Mezzanine Option Slot	Data In and Out, Control In, Status Out
Six (6) Serial Ports*	Data In and Out
LCD	Data Out and Status Out
Keypad	Control In and Data In
LEDs	Status Out
Console	Data In and Out, Control In, Status Out
USB Console	Data In and Out, Control In, Status Out

* The Uplogix 5000 serial ports are used by the Local Manager to connect to devices being managed.

3. Roles, Services, and Authentication

The Uplogix LM provides a flexible framework for defining roles. A role is a list of allow permissions and a list of deny permissions. Uplogix ACLs are of the form <principal> <resource> <role> where a principal is a user or group, and a resource is a port name (ex. port 1/1), modem, system (LM), or server (UCC). With the UCC, labels can be added to ports; these same labels can then be used as a resource name for ACLs.

3.1. Roles and Services

The module allows concurrent users. The module also allows any number of roles to be defined. The module ships with the Admin and Guest Roles. During FIPS initialization a third role is created to allow operators the ability to zeroize the system. A Crypto Officer is an operator that is assigned the Admin and Factory Reset Role. For a complete listing of privileges for each role, refer to Appendix A: Roles and Their Privileges on Resources. The default Guest role on the module corresponds to the FIPS 140-2 User role.

A user granted the appropriate permissions may use "show dashboard", "show version", or "show system fips" to determine whether the LM is in FIPS mode. A user granted "restart" may reboot the system at any time to force power-on self-tests to run.

3.1.1. Admin Role

The Admin Role, provided by default in the module, has all but two permissions: “config reinstall” (factory reset) and “use system auth”. The Admin Role can show and configure settings or issue software updates. It also allows the user to login via SSH or the console port where a user may initiate SSH or TLS interactions from the LM to the UCC[1] or other servers. The Admin Role is also responsible for managing the module via the UCC over a TLS session. For a complete listing of Admin Role privileges, refer to Appendix A.

3.1.2. Guest Role

The Guest Role, provided by default in the module, has access to a limited number of Uplogix commands. The Guest Role can log into the LM and run various show commands. The complete list of Guest Role commands is available in Appendix A.

[1] UCC refers to the Uplogix Control Center, which is a separate Uplogix appliance, outside the module’s cryptographic boundary. The UCC can be used to manage multiple Uplogix LMs over a TLS session. When an Uplogix LM is managed by a UCC, many of its SRDIs are accessible and configurable via the UCC: TLS or SSH private keys are notable exceptions.

3.1.3. Factory Reset Role

The Factory Reset role is created during the initialization of the LM in FIPS mode. The Factory Reset Role includes one privilege: the ability to factory reset ("config reinstall") the Uplogix Local Manager. The Factory Reset role is included in privilege listings in Appendix A.

3.2. Authentication Mechanisms

The module supports identity-based authentication of its operators. Operators may be authenticated by supplying a username and password or by using public key authentication. Username and password authentication is accessible to operators over the console, SSH, or HTTPS interfaces. Public key authentication may only be used when an operator establishes an SSH session or for authenticating SSH or TLS servers. Operators can also use remote authentication servers (RADIUS and TACACS+) for authenticating over SSH to the module.

3.3. Strength of Authentication Mechanisms

Uplogix LM requires a minimum 7-character password and a minimum 7-character shared secret for remote authentication. Thus, for password authentication over the console, SSH, and UCC's web UI (HTTPS), the probability of successfully guessing the password is at least 1 in 26^7 (if only lowercase letters are used).

When the Uplogix LM attempts to connect to an SSH server, it validates that the SSH host key for the server is an RSA key of 2048-bits or greater in length. All SSH public keys used to authenticate users to the LM must also be RSA keys of 2048-bits or greater in length. When the Uplogix LM attempts to connect to any TLS server, it requires the server's TLS certificate to be an RSA key of 2048-bits or greater.

A 2048-bit RSA key has an encryption strength of 2^112 bits. Thus, for public key authentication the probability is 1 in 2^112 of a randomly generated key pair to match.

Thus, for every possible authentication method, the probability of a random attempt to be successful is less than 1 in 1,000,000.

No more than 10,000 login attempts may be made over SSH in 1 minute. With password-based authentication that changes the probability to 1:803k, which is less than 1:100k. With public key authentication, the 10k login attempts changes the probability to approximately 1:2^98.

No more than 500 login attempts may be made via secure dial in or over the console in 1 minute. The probability of a successful password authentication login attempt over the console is then 500:26^7, or 1:16M.

Under normal operations, at most 10 web service requests (HTTPS) would be issued from the LM to the UCC per minute. No more than 100,000 TLS or SSH requests/minute can be attempted from the LM to any server. Given that a 2048-bit RSA key provides 2^112 bits of encryption strength, the likelihood of breaking the key in a minute with this strategy is 100,000 in 2^112 attempts or 1 in 2^95.

Thus, for every possible authentication method, the probability of a successful random attempt during a one-minute period is less than one in 100,000.

4. Secure Operation and Security Rules

In order to operate an Uplogix LM securely, the user should be aware of the security rules enforced by the module and should adhere to the required physical security rules and the required secure operation rules.

4.1. Security Rules

The security rules derived from FIPS 140-2 include both the security rules configured by the Crypto Officer and those imposed by the Uplogix LM.

4.1.1. Uplogix Security Rules enforced by the Crypto Officer

The following are security rules that result from the security requirements of FIPS 140-2. The Crypto Officer shall follow these rules to conform to FIPS 140-2.

1. During initialization and setup of the Uplogix LM, the admin password must be changed from the standard credentials.
2. Tamper evident labels (TELs) shipped with the LM must be properly applied while engaging the LM in FIPS mode.
3. The Crypto Officer will have the Uplogix LM generate its own unique TLS key pairs. The private key will never be exposed to any UI or exported from the LM. The public key and appropriate certificate signing requests may be exported via the UI for configuration purposes.
4. An Uplogix LM in FIPS mode will not communicate with a UCC that is not in FIPS mode. The UCC's certificate must be imported into the Uplogix LM.
5. If a UCC is managing the LMs in the deployment, the Crypto Officer will ensure that the UCC address is correctly entered when defining the management server for Uplogix LMs.
6. The mezzanine option (modem) slot must be populated in the LM for opacity reasons.
7. For the 500, the power cord must be plugged in on the LM for opacity reasons.
8. For the 5000 and LM83X, the I/O card slots must be populated in the LM for opacity reasons.
9. All data transferred over PPTP or IPsec (IKEv1 or IKEv2) is considered plain text unless protected by an SSH or TLS session.
10. All data transferred over SNMP is considered plain text.
11. All data transferred over TACACS+ and RADIUS is considered plaintext. To prevent leaking operator passwords, they must only be used with one-time password technologies that prevent replay.
12. If email servers are configured on the Uplogix LM with user authentication (config system email), then TLS must also be enabled for those servers by enabling "Prefer SSL for in-band (or out-of-band) email?" on the Local Manager. Additionally, the LM can either be configured to use SMTPS (SMTP over TLS) on port 465 of the

email server or the email server must be configured to require STARTTLS before authentication.

4.1.2. Uplogix Security Rules enforced by the Uplogix LM

The following are security rules that result from the security requirements of FIPS 140-2. The module enforces these requirements when initialized into FIPS mode.

1. When initialized to operate in FIPS mode, the Uplogix LM shall only use FIPS-approved cryptographic algorithms.
2. The Uplogix LM shall employ a SP800-90A DRBG to provide entropy for the application DRBG.
3. The Uplogix LM shall employ the FIPS-approved SP800-90A DRBG whenever generating cryptographic keys.
4. The Uplogix LM shall provide identity-based authentication of operators by verifying the operator's username and password or SSH public key.
5. The Uplogix LM software will disable the following services in FIPS mode: Telnet, Telnet pass-through, service access (except for `service_access off`), editing of the boot menu, update via LCD, and configuration import via FTP.
6. The Uplogix LM will allow dial in to be configured only with TLS encryption required.
7. All TLS transactions will require trusted public keys.
8. The Uplogix LM generates its own unique SSH key pairs. The public key may be transmitted to an accompanying UCC.
9. The Uplogix LM enforces minimum shared secret length of at least seven (7) characters when using TACACS+ or RADIUS.
10. The Uplogix LM will enforce user password restrictions (at minimum 7 characters).
11. The `config reinstall` command provides a Crypto Officer with the ability to zeroize keys and all other configuration data. Zeroization is the only way to switch the module from FIPS mode to non-FIPS mode.
12. On every boot of the LM the FIPS self-tests run.

4.2. Supported Algorithms

The Uplogix LMs provide many different cryptographic algorithms to ensure compatibility with today's marketplace. Specifically, the Uplogix LM provides the following algorithms:

Table 8: Cryptographic Algorithm Sizing

CAVP Cert.	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli
Digital Signature Services				
A1967	ECDSA	FIPS 186-4	KeyGen, KeyVer	P-256, P-384, P-521
A1967	ECDSA	FIPS 186-4	SigGen	SHA2-224, SHA2-256, SHA2-384, SHA2-512
A1967	ECDSA	FIPS 186-4	SigVer	SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512
A1967	RSA	FIPS 186-4	KeyGen, KeyVer	2048, 3072, 4096 bits
A1967	RSA	FIPS 186-4	SigGen, SigVer PKCS 1.5, PKCSPSS	2048, 3072, and 4096 bits; SHA2-224, SHA2-256, SHA2-384, SHA2-512
Encryption, Decryption				
A1967	AES	FIPS 197, SP 800-38A	CBC, CTR, ECB	128, 192, 256 bits
A1967	AES	FIPS 197, SP 800-38D	GCM (External IV 8.2.1)	128, 192, 256 bits
Entropy for HMAC-DRBG				
	ENT (NP)	SP 800-90B	Non-IID	The entropy source provides at least 1 bit of entropy per 8 bits of raw noise data. A minimum of 256 bits of entropy is used to initialize the HMAC-DRBG.
Hashing				
A1966, A1967, A1970	SHS	FIPS 180-4	SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	byte only

CAVP Cert.	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli
Key Agreement, Key Establishment				
	KAS	SP 800-56Ar3	DH with TLS-KDF and SSH-KDF	KAS-FFC-SSC Cert. #A1967, CVL Certs. #A1967, #A1968, and #A1969
A1967	KAS-SSC	SP 800-56Ar3	ECC-SSC	P-256, P-384, P-521
	KAS	SP 800-56Ar3	ECDH with TLS-KDF and SSH-KDF	KAS-ECC-SSC Cert. #A1967, CVL Certs. #A1967, #A1968, and #A1969
A1967	KAS-SSC	SP 800-56Ar3	FFC-SSC	ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, MODP-2048
Key Derivation Function				
A1967	KDA	SP 800-56Cr2	HKDF	SHA2-224, SHA2-256, SHA2-384, SHA2-512
CVL A1968, CVL A1969	KDF	SP 800-135	SSH	AES-128, AES-192, AES-256; SHA-1, SHA2-256, SHA2-384, SHA2-512
CVL A1967	KDF	SP 800-135	TLS 1.0/1.1	HMAC-SHA1, HMAC-MD5
CVL A1967	KDF	SP 800-135	TLS 1.2	HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512

CAVP Cert.	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli
Key Generation				
Vendor affirmed	CKG	SP 800-133	Symmetric keys and asymmetric seeds are the unmodified output of an SP 800-90A DRBG (Hash-DRBG with SHA2-256).	
A1967	Safe Primes Key Generation	SP 800-56Ar3	KeyGen	ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, MODP-2048
Key Transport				
A1697	KTS	SP 800-38F	AES with HMAC	key establishment methodology provides between 128 and 256 bits of encryption strength
A1697	KTS	SP 800-38F	AES	key establishment methodology provides 128 or 256 bits of encryption strength
MAC Generation				
A1967	HMAC	FIPS 198-1	HMAC-SHA-1, HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512	byte only, key size < block size, key size = block size, key size > block size
A1966, A1970	HMAC	FIPS 198-1	HMAC-SHA2-512	byte only, key size < block size, key size = block size, key size > block size
Random Bit Generation				
A1967	DRBG	SP 800-90A	Hash-DRBG (SHA2-256)	256 bits of entropy input
A1966, A1970	DRBG	SP 800-90A	HMAC-DRBG (SHA2-512)	256 bits of entropy input

All algorithm testing was performed using ACVP protocol version 1.0.

In compliance with IG 7.14, the module generates cryptographic keys whose strengths are modified by available entropy.

Table 9: Non-Approved Security Functions

Algorithm	How the Algorithm is Used
ChaCha20	LRNG initialization
PBKDF2-SHA-256 (no security claimed)	Password Authentication

4.2.1. SSH and TLS

The Local Manager supports SSH version 2.0 and TLS versions 1.0 through 1.3. No parts of these protocols, other than the SSH-KDF, TLS-KDF, and HKDF, have been tested by the CAVP and CMVP.

Only the following TLS 1.0 to 1.2 cipher suites are enabled in FIPS mode:

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC0, 0x13)
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xC0, 0x2F)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC0, 0x14)
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xC0, 0x30)

Only the following TLS 1.3 cipher suites are enabled in FIPS mode:

- TLS_AES_128_GCM_SHA256 (0x13, 0x01)
- TLS_AES_256_GCM_SHA384 (0x13, 0x02)

The Local Manager's TLS implementation aborts connections after 24,159,191,040 (0x5a << 28) records are processed to prevent too much data being processed by the same key. This limit (approximately 2^34.5) is well under the 2^64 limit required to prevent nonce wraparound with AES-GCM ciphers.

4.3. Secure Operation Initialization Rules

FIPS 140-2 prohibits the use of non-FIPS approved algorithms while operating in a FIPS compliant manner. The Crypto Officer should follow the following rules to initialize a new Uplogix LM to ensure FIPS level 2 compliance.

1. Power-up the Uplogix LM. The default credentials for the LM are username: admin and password: password.
2. Create the Factory Reset role by entering the command `config role FactoryReset`. Assign the factory reset privilege to the role by entering `allow config reinstall`. Exit the role creation wizard by typing `exit`.
3. Create a new user <username> using the command `config user <username>`.
    a. Select `y` to create this user.
    b. Add roles to this user by entering `system admin` to assign the admin role and `system FactoryReset` to assign the Factory Reset role.
    c. Type `exit` to complete the user creation and role assignment.
    d. Add a password for use in FIPS mode using the command `config password <username>`. The password should follow the FIPS restrictions and be at least seven characters long.
4. Use the `enable <username>` command to log out as admin and log in as <username>.
5. Disable the admin account via the `config user admin` command.
    a. Type `disabled` to disable the admin account.
    b. Type `no password` to remove the password.
    c. Type `authorized keys` to enter the SSH public keys menu.
    d. Type `exit` to erase all keys associated with the admin user.
    e. Type `no all admin` to remove privileges.
    f. Verify there are no privileges for the admin account via the command `show`. If any privileges show, remove them individually via the command `no <resource> <role>`.
    g. Type `exit` to complete the user creation and role assignment.
6. The Crypto Officer will delete all users currently present in the module except admin and the username created in step 3. The `show user *` will show all users currently present on the module. The `config user no <username>` should then be repeated for all usernames except for the username created in the above step.
7. Turn off Service Access by entering the command `service_access off` at the system level.
8. Enter the command `config sys fips enable`; this will reboot the system.
9. Log into the system as the user created in step 3.
10. If the LM is managed by a UCC, complete the following steps; otherwise, skip to step 12:
    a. Run `config sys crypto csr`
    b. Obtain a signed certificate from your CA for the CSR you generated.
    c. Run `config sys crypto certificate client` to import the signed certificate.
    d. Ensure that the CA that signed your certificate is accepted by your UCC installation.

e. Run `config sys crypto certificate management` to import the UCC's heartbeat certificate.

11. Run `config sys management` to point the LM at the UCC.
12. The tamper evident labels shall be installed for the module to operate in a FIPS Approved mode of operation. The surface of the LM should be cleaned prior to application or reapplication of TELs. Place tamper labels on the LM as indicated in Figure 9: Tamper Evident Label Placement on the LM80 and LM83X or Figure 10: Tamper Evident Label Placement on the 500 and 500. Additional TELs may be ordered from Lantronix using part number (61-0001-00).
    a. Once applied, the Crypto Officer shall not remove or replace the labels unless the module has shown signs of tampering
    b. The Crypto Officer should regularly inspect the tamper evident labels for damage or signs of tampering
    c. If damage or tampering is suspected, the Crypto Officer shall reimage the module and follow the procedure to place the module in FIPS mode.

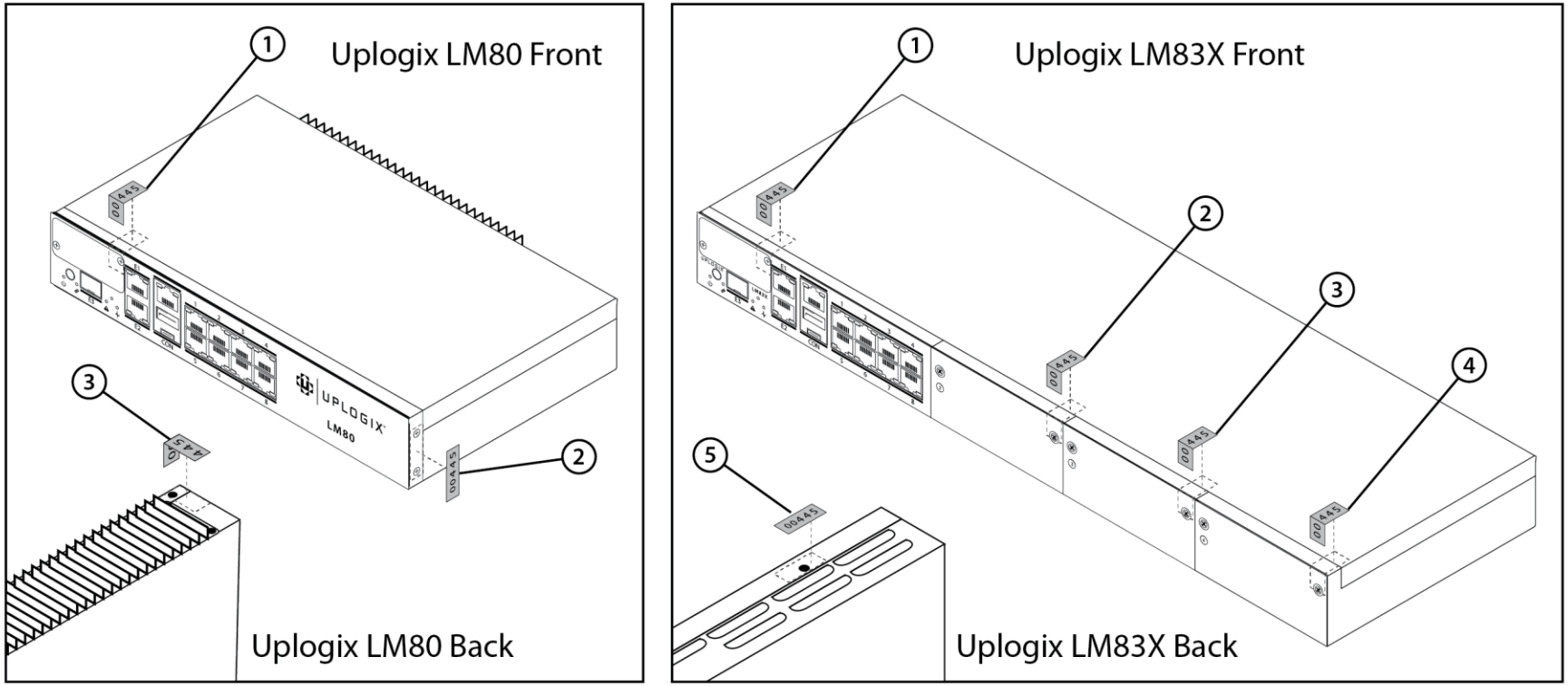

Figure 9: Tamper Label Placement on the LM80 and LM83X

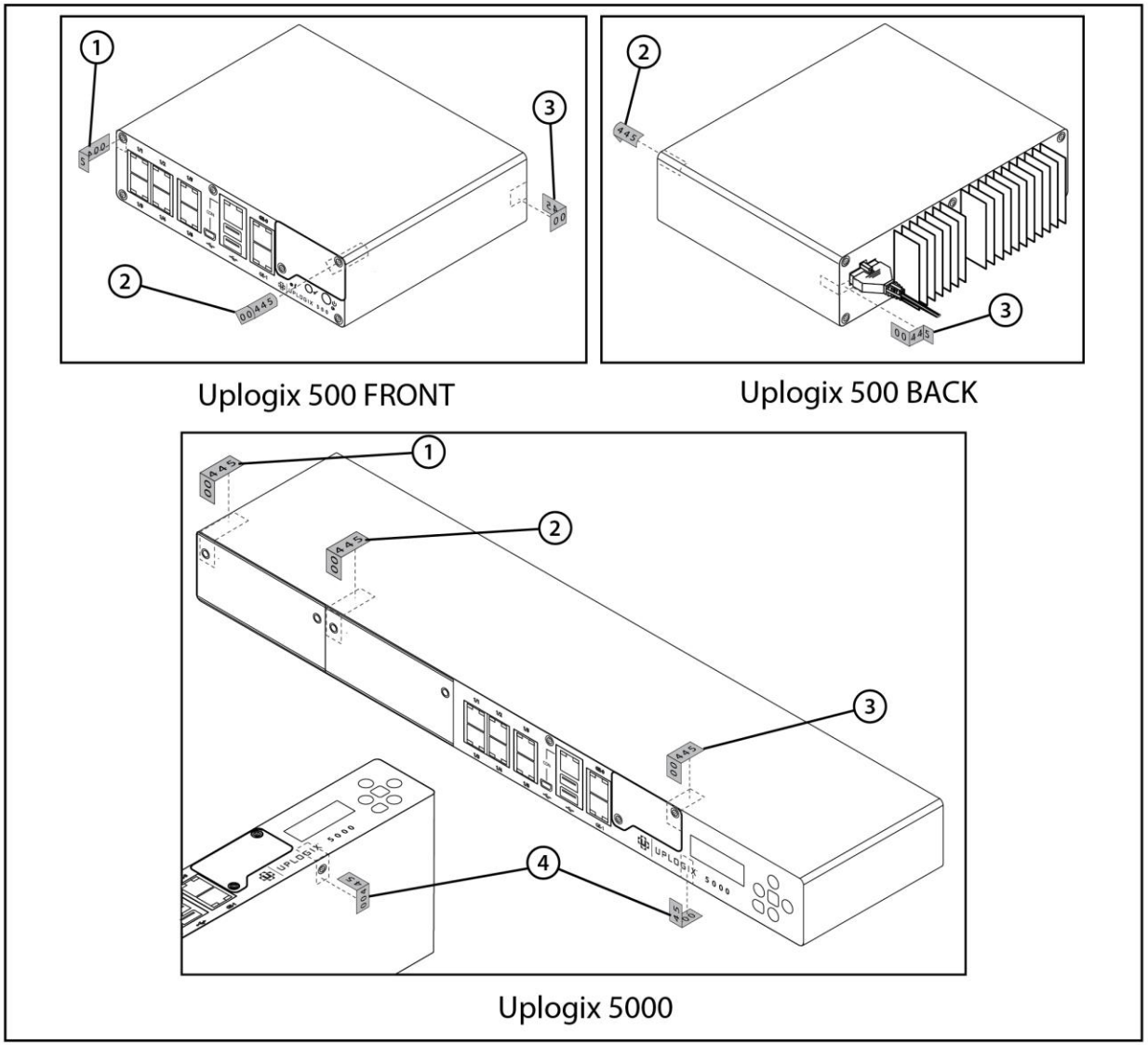

Figure 10: Tamper Label Placement on the 500 and 5000

4.4. Physical Security Rules

As part of enable FIPS-mode, the Crypto Officer is responsible for applying the tamper-evident labels on the modules, as shown in the Figure 9: Tamper label placement on the LM80 and LM83X or Figure 10: Tamper Label Placement on the 500 and 5000. The LM80 and 500 require three tamper-evident labels. The 5000 requires four, and the LM83X requires five.

The Crypto Officer must periodically inspect the physical case of the LM to ensure that no attacker has attempted to tamper with the LM. Signs of tampering include deformation, scratches, or scrape marks in tamper labels covering the LM.

The Crypto Officer is also responsible for securing and having control at all times of any unused tamper-evident labels, and for the direct control and observation of any changes to the module such as reconfigurations where the tamper evident labels may be removed or re-installed to ensure the security of the module is maintained during such changes and the module is returned to the FIPS-Approved state.

4.5. FIPS Operation Modes

This section describes FIPS operation modes.

4.5.1. FIPS Running Mode

Run the command `show sys fips`. If the LM is correctly placed into FIPS mode, the response will be “FIPS 140-2 mode is enabled.”

4.5.2. FIPS Failure Modes

With the exception of a software load failure, this mode is entered when the module fails a non-kernel conditional or start up self-test. If a software load test failure occurs, the module rejects the invalid binary file. The module will not perform the software load and will continue normal operations.

A. LM80 and LM83X – The warning and status LEDs will alternate between red and off.

B. LM83X and 5000 – The LCD will read “FIPS Failure”.

C. 500 – The power LED alternates between amber and green while the status LED blinks (in sync).

D. Any external USB LCD will read “FIPS Failure”.

4.5.3. Firmware Verify Mode

When an update is run from the CLI, LCD, or the UCC, a firmware image is first copied to the appliance. After the firmware is successfully copied, the Local Manager enters the firmware verify mode to validate the signature matches the 2048-bit Uplogix firmware

certificate. If the firmware verify mode successfully verifies the image, the image is then staged for a firmware upgrade and the Local Manager reboots.

5. Definition of SRDIs Modes of Access

This section specifies the Uplogix' Security Relevant Data Items as well as the access control policy enforced by the Uplogix LMs.

5.1. Cryptographic Keys, CSPs, and SRDIs

While operating in a level 2 FIPS compliant manner, the Uplogix LM contains the following security relevant data items:

Table 10: Security Relevant Data Items

Security Relevant Data Item	Key generation method	Key size	Input into module	Output from module	Storage	SRDI Description
Device Passwords	user entered	N/A	non-echoed clear text*, UCC**	clear text, UCC**	Disk	Passwords used to authenticate the LM with devices it manages.
Email Passwords	user entered	N/A	non-echoed clear text*, UCC**	SMTP, UCC**	Disk	Passwords used to authenticate the LM with SMTP servers.
Export Password	user entered	N/A	non-echoed clear text*, UCC**	SCP, FTP, UCC**	Disk	Password used to authenticate the LM with an SCP/FTP server receiving periodic stats via the export process.
LRNG DRBG Entropy Input	ENT (NP)	256 bits	no	no	RAM	Used for the SP 800-90A DRBG using HMAC-SHA2-512
LRNG DRBG Seed	ENT (NP)	256 bits	no	no	RAM	Used for the SP 800-90A DRBG using HMAC-SHA2-512
LRNG DRBG Key	HMAC-SHA2-512	512 bits	no	no	RAM	Used for the SP 800-90A DRBG using HMAC-SHA2-512
LRNG DRBG V Value	HMAC-SHA2-512	512 bits	no	no	RAM	Used for the SP 800-90A DRBG using HMAC-SHA2-512

Security Relevant Data Item	Key generation method	Key size	Input into module	Output from module	Storage	SRDI Description
NSS DRBG Entropy Input	LRNG DRBG	256 bits	no	no	RAM	Used for the SP 800-90A DRBG using SHA2-256
NSS DRBG Seed	SP 800-90A Hash_df	256 bits	no	no	RAM	Used for the SP 800-90A DRBG using SHA2-256
NSS DRBG V Value	SP 800-90A Hash_df	256 bits	no	no	RAM	Used for the SP 800-90A DRBG using SHA2-256
NSS DRBG C Value	SP 800-90A Hash_df	256 bits	no	no	RAM	Used for the SP 800-90A DRBG using SHA2-256
Operator Passwords	user entered	N/A	non-echoed clear text*, UCC**	UCC**	Disk	Used for user authentication via SSH, the console port, or with the UCC.
Operator Public Keys	user entered RSA	2048+ bits	clear text*, UCC**	clear text*	Disk	Alternative mechanism for user authentication via SSH.
Reverse-SSH RSA private key for LM	RSA	2048 bits	no	no	Disk	2048-bit RSA SSH private key used to authenticate to the Reverse-SSH server running on the UCC.
Reverse-SSH RSA public key for LM	RSA	2048 bits	no	clear text*, UCC**	Disk	2048-bit RSA SSH public key used to authenticate to the Reverse-SSH server running on the UCC.
Reverse-SSH RSA public key for UCC	RSA	2048 bits	UCC**	clear text*	Disk	RSA SSH public key of a server used to confirm the LM is talking to the intended reverse-SSH server.
SMS Key	AES	128-bit	no	UCC**	Disk	The SMS key is a 128-bit AES CBC key generated on the Uplogix LM and transmitted to the UCC via TLS web services. Its only purpose is to decrypt messages sent by the UCC to the LM over SMS.

Security Relevant Data Item	Key generation method	Key size	Input into module	Output from module	Storage	SRDI Description
SSH ECDHE/DHE Key Pair	ECDHE/DHE	ECDHE: 256, 384, or 521 bits; DHE: 2048 bit	no	no	RAM	Used to transmit keying information for SSH session keys.
SSH HMAC Integrity Keys	SSH-KDF	160, 256, or 512 bits	no	no	RAM	Used to verify SSH transport data. Algorithms: HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512.
SSH RSA 2048 Private Key	RSA	2048 bits	no	no	Disk	Unique RSA private key used to sign SSH key exchange data.
SSH RSA 2048 Public Key	RSA	2048 bits	no	clear text, UCC**	Disk	Unique RSA public key used to identify the LM to SSH clients. It is used to verify data signed by the RSA private key.
SSH Session Keys	SSH-KDF	128, 192, or 256 bits	no	no	RAM	Used to encrypt the SSH transport. Algorithms: AES-128-CBC, AES-192-CBC, AES-256-CBC, AES-128-CTR, AES-192-CTR, AES-256-CTR.
TLS CA Certificates	user entered	2048+ bits	clear text*, UCC**	clear text*, UCC**	Disk	Used to verify a server certificate used with generic HTTPS and SMTPS functionality. 2048-bit or larger RSA keys.
TLS ECDHE/DHE Key Pair	ECDHE/DHE	ECDHE: 256, 384, or 521 bits; DHE: 2048+ bits	no	no	RAM	Used with TLS cipher suites.
TLS MAC Integrity Keys	TLS-KDF	160, 256, or 384 bits	no	no	RAM	Used to verify TLS data. Algorithm: HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384.
TLS Pre-master Secret	TLS-KDF	48 bytes	no	no	RAM	48-byte key used to derive the TLS Master Secret in TLS 1.0 - 1.2.

Security Relevant Data Item	Key generation method	Key size	Input into module	Output from module	Storage	SRDI Description
TLS Master Secret	TLS-KDF, HKDF	48 bytes	no	no	RAM	Shared secret used to generate session keys, IVs, and MAC keys.
TLS RSA 2048-bit Certificate for Dial In	RSA	2048 bits	no	clear text*, UCC**	Disk	Unique 2048-bit RSA certificate that identifies the LM and is used with encrypted dial in.
TLS RSA 2048-bit Private Key for Dial In	RSA	2048 bits	no	no	Disk	Corresponding private key used to establish TLS-encrypted modem sessions.
TLS RSA Certificate for LM	user entered	2048+ bits	clear text*	clear text*, UCC**	Disk	Unique to the LM. Used to authenticate and differentiate itself with the UCC web services. 2048, 3072, or 4096-bit.
TLS RSA Certificate for UCC	user entered	2048+ bits	clear text*	clear text*	Disk	Used to authenticate the UCC to the LM for web services.
TLS RSA Private Key for LM	RSA	2048+ bits	no	no	Disk	Corresponding private key used to sign client key exchange messages.
TLS Resumption Master Secret	HKDF	48 bytes	no	no	RAM	Used to generate resumption tickets in TLS 1.3.
TLS Server Certificates	user entered	2048+ bits	clear text*, UCC**	clear text*, UCC**	Disk	Used to verify a server certificate for generic HTTPS and SMTPS functionality. 2048-bit or larger RSA keys.
TLS Session Keys	TLS-KDF, HKDF	128 or 256 bits	no	no	RAM	Used to encrypt the TLS transport. Algorithms: AES-128-CBC, AES-256-CBC, AES-128-GCM, AES-256-GCM.
Uplogix Firmware Certificate	RSA	2048 bits	no	no	Disk	2048-bit RSA key used to verify the signature of Uplogix firmware images for the LM.

Security Relevant Data Item	Key generation method	Key size	Input into module	Output from module	Storage	SRDI Description
Virtual-Port SSH RSA private key for LM	RSA	2048 bits	no	no	Disk	2048-bit RSA private key used to authenticate to virtual-port servers.
Virtual-Port SSH RSA public key for LM	RSA	2048 bits	no	clear text*, UCC**	Disk	2048-bit RSA public key used to authenticate to virtual-port servers.
Virtual-Port SSH RSA public key for server	user entered	2048+ bits	clear text*, UCC**	clear text*, UCC**	Disk	RSA SSH public key of a server used to confirm the LM is talking to the intended server.

Notes: * The data is either input or output to the user via plaintext on the CLI. The CLI is available via SSH, USB console, or serial console. Contents are only encrypted over SSH.

** The LM synchronizes its configuration information with the UCC via HTTPS.

Except for the Uplogix Firmware certificate, all SRDIs that are stored on disk are zeroized when a factory reset is performed on the LM. There are multiple ways to perform a factory reset.

5.2. Access Control Policy

The terminal allows controlled access to the SRDIs contained within it. The following table defines the access that an operator or application has to each SRDI while operating the LM in a given role performing a specific command. The permissions are categorized as a set of four separate permissions: read, write, delete, and zeroize. If no permission is listed, then an operator has no access to the SRDI.

Table 11: Access Control Policy

Uplogix LM SRDI/Role/Service Access Policy (r = read, w = write, d = delete, z = zeroize)	Roles/Service	Admin Role	Show Functions	Configuration Functions	config sys fips enable	Encrypted Dial in Mode	Other TLS functions	SSH	SMS Monitor	Update Functions	Guest Role	Configuration Functions	Encrypted Dial in	SSH	Show Functions	Factory Reset Role	Factory Reset (implicitly disables FIPS Mode)	Uplogix Control Center	Web Services
Security Relevant Data Item																			
Device Passwords				w													zw		r w d
Email Passwords				w													zw		r w d
Export Password				w													zw		r w d
LRNG DRBG Entropy Input																			
LRNG DRBG Seed																			
LRNG DRBG Key																			
LRNG DRBG V Value																			
NSS DRBG Entropy Input				r	r	r	r	r	r	r			r	r					
NSS DRBG Seed				r	r	r	r	r	r	r			r	r					
NSS DRBG V Value				r	r	r	r	r	r	r			r	r					
NSS DRBG C Value				r	r	r	r	r	r	r			r	r					
Operator Passwords				w d	r			r w				w		r w			zw		r w d
Operator Public Keys			r	w d	r d			r						r	r		zw		r w d
Reverse-SSH RSA private key for LM				w	d			r									zw		
Reverse-SSH RSA public key for LM			r	r w	d			r									zw		r
Reverse-SSH RSA public key for UCC			r	r w				r									zw		r w d
SMS Key				w	d				r								zw		r
SSH ECDHE/DHE Key Pair								r w						r w					

Uplogix LM SRDI/Role/Service Access Policy (r = read, w = write, d = delete, z = zeroize)	Roles/Service	Admin Role	Show Functions	Configuration Functions	config sys fips enable	Encrypted Dial in Mode	Other TLS functions	SSH	SMS Monitor	Update Functions	Guest Role	Configuration Functions	Encrypted Dial in	SSH	Show Functions	Factory Reset Role	Factory Reset (implicitly disables FIPS Mode)	Uplogix Control Center	Web Services
Security Relevant Data Item																			
SSH HMAC Integrity Keys								r w						r w					
SSH RSA 2048 Private Key Pair				w	d			r						r			zw		
SSH RSA 2048 Public Key Pair				w	d			r						r			zw		r
SSH Session Keys								r w						r w					
TLS CA Certificates			r	w d			r										zw		r w d
TLS ECDHE/DHE Key Pair						rw	r w						rw						r w
TLS MAC Integrity Keys						rw							rw						r w
TLS Pre-master Secret						rw	r w						rw						r w
TLS Master Secret						rw	r w						rw						r w
TLS RSA 2048-bit Certificate for Dial In			r	rd	d	r							r				d		r
TLS RSA 2048-bit Private Key for Dial In				d	d	r							r				d		
TLS RSA Certificate for LM			r	w	d												zw		r
TLS RSA Certificate for UCC			r	w	d												zw		r
TLS RSA Private Key for LM				w	d												zw		
TLS Resumption Master Secret						rw	r w						rw						rw
TLS Server Certificates			r	w d			r										zw		r w d
TLS Session Keys							r w												r w
Uplogix Firmware Certificate										r									
Virtual-Port SSH RSA private key for LM				w	d			r									zw		

Uplogix LM SRDI/Role/Service Access Policy (r = read, w = write, d = delete, z = zeroize)	Roles/Service	Admin Role	Show Functions	Configuration Functions	config sys fips enable	Encrypted Dial in Mode	Other TLS functions	SSH	SMS Monitor	Update Functions	Guest Role	Configuration Functions	Encrypted Dial in	SSH	Show Functions	Factory Reset Role	Factory Reset (implicitly disables FIPS Mode)	Uplogix Control Center	Web Services
Security Relevant Data Item																			
Virtual-Port SSH RSA public key for LM			r	r w	d			r									zw		r
Virtual-Port SSH RSA public key for server			r	r w				r									zw		r w d

Notes: On `config sys fips enable`, the SMS key, the TLS RSA LM key pair and certificate, the TLS RSA certificate for UCC, dial in key pair and certificate, the reverse-SSH LM key pair, the SSH RSA and DSA key pairs, and the virtual-port LM key pair are deleted. When the system next boots, the SMS key, RSA SSH host and virtual-port keys, and the dial in key pair and certificate are created automatically. The TLS certificates are manually created/configured. The Reverse-SSH LM key pair is only regenerated if reverse-SSH is enabled. DSA SSH key pairs are no longer created or used on the LM.

A user with only the guest role (`config password`, but not `config user`) is only able to see and edit his own SSH public keys. Likewise, a user with the guest role can only change his own password.

6. Self-Tests

6.1. Power-up Self-Tests

On boot, the following Linux kernel and LRNG self-tests are run.

- SHA-1 KAT
- ChaCha20 DRNG KAT
- SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 KAT
- HMAC-SHA-256, HMAC-SHA-512 KAT
- SP800-90A HMAC DRBG with SHA-256 KAT

If any of these kernel self-tests fail, the kernel panics and the system reboots.

Following kernel initialization, the system performs a firmware integrity test using SHA2-256; if this fails, the system goes into FIPS Failure.

After confirming integrity, the system performs the following self-tests.

- SP 800-90A Hash DRBG with SHA-256 KAT
- SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512 KAT

- AES (128, 192, 256) KAT encryption with ECB, CBC, and GCM
- AES (128, 192, 256) KAT decryption with ECB, CBC, and GCM
- HMAC KAT with SHA-1, SHA-224, SHA256, SHA-384, and SHA-512
- TLS 1.0/1.1 KDF KAT
- TLS 1.2 KDF KAT using SHA-256
- RSA 2048-bit KAT for public key encryption and private key decryption
- RSA 2048-bit KAT for PKCS#1 v1.5 sign and verify with SHA-256, SHA-384, SHA-512
- ECDSA (NIST P-256) KAT for sign and verify with SHA-256
- ECDH (NIST P-256) KAT for derive with SHA-256
- DH (2048-bit) KAT derive with SHA-256
- HKDF KAT (TLS 1.3) with HMAC-SHA-256

If any of these self-tests fail, the system goes into FIPS Failure.

Finally, during application startup, an SSH-KDF KAT is performed. If it fails, the system goes into FIPS Failure.

6.2. Conditional Self-Tests

LRNG runs the following continuous health tests.

- stuck test
- repetition count test
- adaptive proportion test

If a stuck test fails, the single entropy data point is discarded, and the repetition count is incremented. If the repetition count test or adaptive proportion test fails, the LRNG's internal state is reset, self-tests are re-run, and LRNG will not return new data until its entropy pool has been replenished.

Pair-wise consistency checks are performed on any RSA, ECDSA, ECDH, or DH key pairs that are generated. If any of these checks fail, the system goes into FIPS Failure.

NSS also runs a continuous check on its entropy input, such that if one block matches the previous block, the system goes into FIPS Failure.

The module performs a firmware load test on upgrade. It validates a 2048-bit RSA signature using SHA-512 matches the Uplogix firmware certificate. If the test fails, the upgrade is aborted, and the downloaded code is deleted.

7. Electromagnetic Interference and Compatibility (EMI/EMC)

The cryptographic module conforms to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A.

8. Mitigation of Other Attacks

Lantronix does not wish to claim that the module mitigates any other attacks.

Appendix A: Roles and Their Permissions on Resources

Table 12: Capabilities of Unauthenticated Users

Model	Mode	Resource	Permission	Modes
Uplogix LM80, LM83X, 500, and 5000	SNMP	system	show system properties	FIPS, non-FIPS
Uplogix LM80, LM83X, 500, and 5000	SNMP	system	show version	FIPS, non-FIPS
Uplogix LM80, LM83X, 500, and 5000	Visual Inspection	port, system, modem	Monitoring physical ports activity using the ports LEDs for all models	FIPS, non-FIPS
Uplogix LM80, LM83X, 500, and 5000	Console	system	show system fips	FIPS, non-FIPS
Uplogix LM80, LM83X, 500, and 5000	Console	system	show version	FIPS, non-FIPS
Uplogix LM80, LM83X, 500, and 5000	LCD/Keypad or USB LCD/Keypad	system	config reinstall	FIPS, non-FIPS
Uplogix LM80, LM83X, 500, and 5000	LCD/Keypad or USB LCD/Keypad	system	config system ip	FIPS, non-FIPS
Uplogix LM80, LM83X, 500, and 5000	LCD/Keypad or USB LCD/Keypad	system	config system management	FIPS, non-FIPS
Uplogix LM80, LM83X, 500, and 5000	LCD/Keypad or USB LCD/Keypad	system	config system pulse	FIPS, non-FIPS
Uplogix LM80, LM83X, 500, and 5000	LCD/Keypad or USB LCD/Keypad	system	config system serial	FIPS, non-FIPS
Uplogix LM80, LM83X, 500, and 5000	LCD/Keypad or USB LCD/Keypad	system	config update	Non-FIPS
Uplogix LM80, LM83X, 500, and 5000	LCD/Keypad or USB LCD/Keypad	system	restart	FIPS, non-FIPS
Uplogix LM80, LM83X, 500, and 5000	LCD/Keypad or USB LCD/Keypad	system	show alarms	FIPS, non-FIPS
Uplogix LM80, LM83X, 500, and 5000	LCD/Keypad or USB LCD/Keypad	port, system	show info	FIPS, non-FIPS
Uplogix LM80, LM83X, 500, and 5000	LCD/Keypad or USB LCD/Keypad	modem, system	show status	FIPS, non-FIPS
Uplogix LM80, LM83X, 500, and 5000	LCD/Keypad or USB LCD/Keypad	system	show sys ipv6	FIPS, non-FIPS
Uplogix LM80, LM83X, 500, and 5000	LCD/Keypad or USB LCD/Keypad	system	show system ip	FIPS, non-FIPS
Uplogix LM80, LM83X, 500, and 5000	LCD/Keypad or USB LCD/Keypad	system	show system management	FIPS, non-FIPS

Model	Mode	Resource	Permission	Modes
Uplogix LM80, LM83X, 500, and 5000	LCD/Keypad or USB LCD/Keypad	system	show system pulse	FIPS, non-FIPS
Uplogix LM80, LM83X, 500, and 5000	LCD/Keypad or USB LCD/Keypad	system	show system serial	FIPS, non-FIPS
Uplogix LM80, LM83X, 500, and 5000	LCD/Keypad or USB LCD/Keypad	system	shutdown	FIPS, non-FIPS
Uplogix LM80 and LM83X	Power Button	system	shutdown	FIPS, non-FIPS
Uplogix LM80 and LM83X	Reset Button	system	config reinstall	FIPS, non-FIPS
Uplogix LM80 and LM83X	Warning and Status LEDs	system	Shows the state of the Local Manager	FIPS, non-FIPS
Uplogix 500	Power Button	system	shutdown	FIPS, non-FIPS
Uplogix 500	Multipurpose Button	system	config reinstall	FIPS, non-FIPS
Uplogix 500	Multipurpose Button	system	Application Health Check (causes status button to blink five times if the application is running)	FIPS, non-FIPS
Uplogix 500	Status LED	system	Shows the state of the Local Manager	FIPS, non-FIPS
Uplogix 500	Power LED	system	Monitoring power status	FIPS, non-FIPS

Notes: The 5000 has a built-in LCD/keypad. The LM83X can have an LCD/keypad option card module installed. All LMs can have a separate USB connected LCD/keypad.

LM80, LM83X, 500, and 5000 console prompt displays the OS version while prompting for username and password. Additionally, the console port outputs the FIPS Failure status message every second when the module is in FIPS Failure/Error State, this message can be seen by any unauthenticated operator.

Admin Access:

The Admin Role is a standard role provided by LMS and thus is the same on all versions of the module.

Table 13: Permissions Granted to the Admin Role

Resource	Permission	Modes
port	assimilate	FIPS, non-FIPS
port	autorecovery	FIPS, non-FIPS

Resource	Permission	Modes
port	capture	FIPS, non-FIPS
port	certify	FIPS, non-FIPS
port	clear counters	FIPS, non-FIPS
port	clear log	FIPS, non-FIPS
port	clear password	FIPS, non-FIPS
port	clear service-module	FIPS, non-FIPS
server	config aaa***	FIPS, non-FIPS
modem	config answer	FIPS, non-FIPS
port	config authentication	FIPS, non-FIPS
system	config date	FIPS, non-FIPS
port	config device logging	FIPS, non-FIPS
system	config environment	FIPS, non-FIPS
system	config export	FIPS, non-FIPS
server	config filter***	FIPS, non-FIPS
system	config group	FIPS, non-FIPS
server	config hierarchy***	FIPS, non-FIPS
system	config import	FIPS, non-FIPS
port	config info	FIPS, non-FIPS
port	config init	FIPS, non-FIPS
server	config inventory***	FIPS, non-FIPS
server	config label***	FIPS, non-FIPS
server	config license***	FIPS, non-FIPS
port, system	config log rule	FIPS, non-FIPS
port, system	config monitors	FIPS, non-FIPS
port	config outlets	FIPS, non-FIPS
system	config password	FIPS, non-FIPS
modem	config ppp	FIPS, non-FIPS
port	config properties	FIPS, non-FIPS
port	config protocols forward	FIPS, non-FIPS
port	config protocols pass-through	FIPS, non-FIPS
port	config protocols shadow	FIPS, non-FIPS
port, system	config removejob	FIPS, non-FIPS
server	config report***	FIPS, non-FIPS
system	config restrict	FIPS, non-FIPS
system	config role	FIPS, non-FIPS
system	config rule	FIPS, non-FIPS
system	config ruleset	FIPS, non-FIPS
port, system	config schedule	FIPS, non-FIPS

Resource	Permission	Modes
port	config serial	FIPS, non-FIPS
port	config service-processor	FIPS, non-FIPS
port	config settings	FIPS, non-FIPS
system	config slv	FIPS, non-FIPS
system	config system applet	FIPS, non-FIPS
system	config system archive	FIPS, non-FIPS
system	config system authentication	FIPS, non-FIPS
system	config system banner	FIPS, non-FIPS
system	config system clear alarms	FIPS, non-FIPS
system	config system clear archive	FIPS, non-FIPS
system	config system clear export	FIPS, non-FIPS
system	config system clear port	FIPS, non-FIPS
system	config system clear securid	FIPS, non-FIPS
system	config system clear slot	FIPS, non-FIPS
system	config system crypto certificate client	FIPS
system	config system crypto certificate management	FIPS
system	config system crypto certificate other*	FIPS, non-FIPS
system	config system crypto certificate dialin	FIPS, non-FIPS
system	config system crypto regenerate**	FIPS, non-FIPS
system	config system email	FIPS, non-FIPS
system	config system export	FIPS, non-FIPS
system	config system fips	FIPS, non-FIPS
system	config system ip	FIPS, non-FIPS
system	config system ipt	FIPS, non-FIPS
system	config system keypad	FIPS, non-FIPS
system	config system management	FIPS, non-FIPS
system	config system ntp	FIPS, non-FIPS
system	config system os policy***	FIPS, non-FIPS
system	config system page-length	FIPS, non-FIPS
system	config system properties	FIPS, non-FIPS
system	config system protocols dhcp	FIPS, non-FIPS
system	config system protocols filter	FIPS, non-FIPS
system	config system protocols ssh	FIPS, non-FIPS
system	config system protocols telnet	Non-FIPS
system	config system pulse	FIPS, non-FIPS
system	config system reverse-ssh	FIPS, non-FIPS
system	config system serial	FIPS, non-FIPS
system	config system slot	FIPS, non-FIPS

Resource	Permission	Modes
system	config system snmp	FIPS, non-FIPS
system	config system subinterface	FIPS, non-FIPS
system	config system syslog-options	FIPS, non-FIPS
system	config system timeout	FIPS, non-FIPS
system	config update	FIPS, non-FIPS
system	config user	FIPS, non-FIPS
system	config user certificate	FIPS, non-FIPS
modem	config vpn	FIPS, non-FIPS
system	connect	FIPS, non-FIPS
port	copy	FIPS, non-FIPS
port	delete	FIPS, non-FIPS
port	device execute	FIPS, non-FIPS
port	device ping	FIPS, non-FIPS
port	edit running-config	FIPS, non-FIPS
system	export	FIPS, non-FIPS
port	forward	FIPS, non-FIPS
port	interface	FIPS, non-FIPS
system	login	FIPS, non-FIPS
port	name	FIPS, non-FIPS
port	off	FIPS, non-FIPS
port	on	FIPS, non-FIPS
system, port	ping	FIPS, non-FIPS
port	power	FIPS, non-FIPS
modem	ppp off	FIPS, non-FIPS
modem	ppp on	FIPS, non-FIPS
port	pull os	FIPS, non-FIPS
port	pull running-config	FIPS, non-FIPS
port	pull startup-config	FIPS, non-FIPS
port	pull tech	FIPS, non-FIPS
port	pull tftp	FIPS, non-FIPS
port	push os	FIPS, non-FIPS
port	push running-config	FIPS, non-FIPS
port	push startup-config	FIPS, non-FIPS
port	push tftp	FIPS, non-FIPS
port	reboot	FIPS, non-FIPS
port	recover configuration	FIPS, non-FIPS
system	restart	FIPS, non-FIPS
port	restore	FIPS, non-FIPS

Resource	Permission	Modes
port	rollback assimilate	FIPS, non-FIPS
port	rollback authentication	FIPS, non-FIPS
port	rollback config	FIPS, non-FIPS
server	run report***	FIPS, non-FIPS
system	service access	Non-FIPS
port	service-processor exec	FIPS, non-FIPS
server	show aaa***	FIPS, non-FIPS
port, system	show alarms	FIPS, non-FIPS
system	show all	FIPS, non-FIPS
modem	show answer	FIPS, non-FIPS
system	show archive	FIPS, non-FIPS
port	show authentication	FIPS, non-FIPS
port	show buffer	FIPS, non-FIPS
system	show capture	FIPS, non-FIPS
port	show chassis	FIPS, non-FIPS
port	show circuit	FIPS, non-FIPS
port	show config	FIPS, non-FIPS
system	show date	FIPS, non-FIPS
port	show device change	FIPS, non-FIPS
port	show device changes	FIPS, non-FIPS
port	show device logging	FIPS, non-FIPS
port	show device syslog	FIPS, non-FIPS
port	show diff	FIPS, non-FIPS
port	show directory	FIPS, non-FIPS
system	show environment	FIPS, non-FIPS
port, system	show events	FIPS, non-FIPS
port	show faults	FIPS, non-FIPS
server	show filter***	FIPS, non-FIPS
port	show gps events	FIPS, non-FIPS
port	show gps position	FIPS, non-FIPS
system	show group	FIPS, non-FIPS
port	show info	FIPS, non-FIPS
system	show install-history	FIPS, non-FIPS
port	show interface	FIPS, non-FIPS
server	show inventory***	FIPS, non-FIPS
port	show label	FIPS, non-FIPS
server	show license***	FIPS, non-FIPS
port, system	show log	FIPS, non-FIPS

Resource	Permission	Modes
port, system	show monitors	FIPS, non-FIPS
port	show outlets	FIPS, non-FIPS
port	show pingstats	FIPS, non-FIPS
system	show ports	FIPS, non-FIPS
port	show post	FIPS, non-FIPS
modem	show ppp	FIPS, non-FIPS
system	show privileges	FIPS, non-FIPS
port	show properties	FIPS, non-FIPS
port	show protocols forward	FIPS, non-FIPS
port	show protocols pass-through	FIPS, non-FIPS
port	show protocols shadow	FIPS, non-FIPS
port	show remotestate	FIPS, non-FIPS
server	show report	FIPS, non-FIPS
system	show restrict	FIPS, non-FIPS
system	show role	FIPS, non-FIPS
port	show rollback-config	FIPS, non-FIPS
system	show rule	FIPS, non-FIPS
system	show ruleset	FIPS, non-FIPS
port	show running-config	FIPS, non-FIPS
port, system	show schedules	FIPS, non-FIPS
port	show serial	FIPS, non-FIPS
port	show service-module	FIPS, non-FIPS
port	show service-processor	FIPS, non-FIPS
system	show session	FIPS, non-FIPS
system	show sessions	FIPS, non-FIPS
port	show settings	FIPS, non-FIPS
system	show slv stats	FIPS, non-FIPS
system	show slv test	FIPS, non-FIPS
port	show startup-config	FIPS, non-FIPS
port	show status	FIPS, non-FIPS
system	show system applet	FIPS, non-FIPS
system	show system archive	FIPS, non-FIPS
system	show system authentication	FIPS, non-FIPS
system	show system banner	FIPS, non-FIPS
system	show system crypto certificate client	FIPS
system	show system crypto certificate dialin	FIPS, non-FIPS
system	show system crypto certificate management	FIPS
system	show system crypto certificate other	FIPS, non-FIPS

Resource	Permission	Modes
system	show system email	FIPS, non-FIPS
system	show system export	FIPS, non-FIPS
system	show system fips	FIPS, non-FIPS
system	show system ip	FIPS, non-FIPS
system	show system ipt	FIPS, non-FIPS
system	show system keypad	FIPS, non-FIPS
system	show system management	FIPS, non-FIPS
system	show system ntp	FIPS, non-FIPS
system	show system os policy***	FIPS, non-FIPS
system	show system page-length	FIPS, non-FIPS
system	show system properties	FIPS, non-FIPS
system	show system protocols	FIPS, non-FIPS
system	show system pulse	FIPS, non-FIPS
system	show system reverse-ssh	FIPS, non-FIPS
system	show system serial	FIPS, non-FIPS
system	show system slot	FIPS, non-FIPS
system	show system snmp	FIPS, non-FIPS
system	show system subinterface	FIPS, non-FIPS
system	show system syslog-options	FIPS, non-FIPS
system	show system timeout	FIPS, non-FIPS
port	show tech	FIPS, non-FIPS
system	show user	FIPS, non-FIPS
system	show version	FIPS, non-FIPS
modem	show vpn	FIPS, non-FIPS
system	show who	FIPS, non-FIPS
system	shutdown	FIPS, non-FIPS
port	squeeze	FIPS, non-FIPS
port, system	suspend	FIPS, non-FIPS
port	terminal	FIPS, non-FIPS
port	terminal break	FIPS, non-FIPS
port	terminal force	FIPS, non-FIPS
port	terminal lock	FIPS, non-FIPS
port	terminal shadow	FIPS, non-FIPS
server	upload archive***	FIPS, non-FIPS
port	use system auth	FIPS, non-FIPS
port	xbrowser	Non-FIPS
port	config xbrowser	Non-FIPS
port	show xbrowser	Non-FIPS

Resource	Permission	Modes
port	clear xbrowser	Non-FIPS
port	unlock xbrowser	Non-FIPS

Notes:
* provides `config system crypto certificate ca`, `config system crypto certificate server`, `config system crypto ipsec csr`, and `config system crypto ipsec client`
** provides `config system crypto regenerate dialin`, `config system crypto regenerate reverse-ssh`, `config system crypto regenerate sms`, `config system crypto regenerate ssh`, and `config system crypto regenerate virtual`
*** This permission is only available on the Uplogix Control Center.
All privileges in the table above with a port resource are also available on the modem.

Guest Access:

The Guest Role is a standard role provided by LMS and thus is the same on all versions of the module.

Table 14: Permissions Granted to the Guest Role

Resource	Permission	Modes
system	config password	FIPS, non-FIPS
system	login	FIPS, non-FIPS
system, port	ping	FIPS, non-FIPS
system, port	show alarms	FIPS, non-FIPS
port	show buffer	FIPS, non-FIPS
system	show date	FIPS, non-FIPS
port	show directory	FIPS, non-FIPS
system	show environment	FIPS, non-FIPS
system	show session	FIPS, non-FIPS
port	show status	FIPS, non-FIPS
system	show version	FIPS, non-FIPS
system	show who	FIPS, non-FIPS

Factory Reset Access:

The Factory Reset Role is created by the Crypto Officer.

Table 15: Permissions Granted to the FactoryReset Role

Resource	Permission	Modes
system	config reinstall	FIPS, non-FIPS