FIPS 140-2 Security Policy

Uplogix 430 and 3200

Uplogix, Inc.
7600 N Capital of Texas Highway, Suite 220
Austin, Texas 78731
USA

December 21, 2011

Document Version 1.1

Table of Contents

Table of Figures

Table of Tables

FIPS 140-2 Security Policy
Uplogix 430 and 3200

1. Introduction

This document describes the Non-Proprietary FIPS 140-2 Security Policy for the Uplogix 430 and 3200 modules.

Uplogix 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 vs. centralized only 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 430 and 3200 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.

1.1. Purpose

This document covers the secure operation of the Uplogix 430 and 3200 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 4.3.5.19979 which runs on the product.

1.2. Models Tested

Table 1: Models Tested

Model	Firmware Version	Hardware Version
Uplogix 430, FIPS, HD	4.3.5.19979	43-1002-50
Uplogix 430, FIPS, CF	4.3.5.19979	43-1102-50
Uplogix 3200, FIPS-03, SSD	4.3.5.19979	37-0326-03
Uplogix 3200, FIPS-04, SSD	4.3.5.19979	37-0326-04

Note: Both 430 models are available with either a V.92 modem, DB9 connection for modem or a blank over the modem slot. Both 3200 models have two option slots on the front of the equipment for connecting I/O modules. I/O modules are available in two forms: a 16 serial

card and an 8 serial by 8 Ethernet card. Additionally, Both 3200 models are available with either a V.92 modem or DB9 connection for modem in the modem slot.

1.3. Glossary

Table 2: Glossary of Terms

Term/Acronym	Description
2TDEA	2-key Triple-DES
3TDEA	3-key Triple-DES
AC	Alternating Current
ACL	Access Control List
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
CA	Certificate Authority
CBC	Cipher-Block Chaining
CFB	Cipher Feedback
CSP	Critical Security Parameter
CSR	Certificate Signature Request
DES	Data Encryption Standard
DH	Diffie-Hellman
DHE	Diffie-Hellman key Exchange
DRAC	Dell Remote Access Controller
DRBG	Deterministic Random Bit Generator
DSA	Digital Security Algorithm
ECB	Electronic Code Book
FIPS	Federal Information Processing Standard
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure which uses TLS or SSL
HMAC-MD5	Hash-based Message Authentication Code – Message-Digest algorithm 5
HMAC-MD5-96	Hash-based Message Authentication Code – Message-Digest algorithm 5 truncated to 96 bits
HMAC-SHA1	Hash-based Message Authentication Code – Secure Hash Algorithm 1
HMAC-SHA-96	Hash-based Message Authentication Code – Secure Hash Algorithm 1 truncated to 96 bits
IKE	Internet Key Exchange
IPMI	Intelligent Platform Management Interface
IPSec	Internet Protocol Security
LCD	Liquid Crystal Display
LM	Local Manager
LMS	Local Management Software
MD5	Message-Digest algorithm 5
NSS	Network Security Services
PPP	Point-to-Point Protocol

PPTP	Point-to-Point Tunneling Protocol
RADIUS	Remote Authentication Dial in User Service
RC4	Rivest Cipher 4
RNG	Random Number Generator
RSA	Rivest, Shamir and Adleman
SHA1	Secure Hash Algorithm 1
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SMTPS	SMTP secured with TLS or SSL
SNMP	Simple Network Management Protocol
SOCKS	Proxy protocol for TCP and UDP data
SRDI	Security Relevant Data Items
SSH	Secure Shell
SSL	Secure Sockets Layer
TACACS+	Terminal Access Controller Access-Control System Plus
TEL	Tamper Evident Label
TLS	Transport Layer Security
Triple-DES	Triple Data Encryption Algorithm
Uplogix 430 Local Manager	Comprehensive functionality in a fixed 4-port LM designed for enterprises needing to monitor, manage and control four or fewer devices and their power supply at any distributed location.
3200 Local Manager	Uplogix Local Manager, available in 8-, 16-, 24-, or 32-port models, that delivers advanced remote management capabilities for data centers, branch offices and remote locations.
UCC	Uplogix Control Center; 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
XAuth	Extended authentication for IPSec

2. Physical Characteristics of Product Family

The Uplogix 430 and 3200 are individually considered as multi-chip standalone modules, and the cryptographic boundary of the modules is defined by the outer case of the modules.

2.1. Uplogix 430

Figure 1: Uplogix 430 Front Side

Figure 2: Uplogix 430 Back Side

Table 3: Uplogix 430 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, Power Out
Modem Slot	Data In and Out, Control In, Status Out
Power Controller	Data In and Out
Four (4) Serial Ports**	Data In and Out

LEDs	Status Out
Reset Button	Control In

* The console port of the Uplogix 430 is covered with a Tamper Evident Label (TEL) while operating in FIPS-approved mode and thus the console port is unusable in FIPS mode.
** The Uplogix 430 serial ports are used by the Local Manager to connect to devices being managed.

2.2. Uplogix 3200

Figure 3: Uplogix 3200 Front Side

Figure 4: Uplogix 3200 Back Side

Table 4: Uplogix 3200 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, Power Out
Modem Slot	Data In and Out, Control In, Status Out
Power Controllers	Data In and Out
LCD	Status Out

Keypad	Control In
LEDs	Status Out
Proprietary Temperature/ Humidity Adapter	Data In
Console	Data In and Out, Control In, Status Out
Removable Power Supply	Power Port

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, powercontrol, 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 default 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 User role.

3.1.1. Admin Role

The Admin Role, provided by default in the module, has the ability to perform all actions on various resources with the exception of factory reset of the local manager. The Admin Role can show and configure settings or issue software updates and allows the user to login via SSH or the console port, initiate the out-of-band sequence which utilizes IPSec VPNs, and may force web service interactions with the UCC[1]. 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 login to the local manager and run various show commands. The complete list of Guest Role commands is available in Appendix A.

3.1.3. Factory Reset Role

The Factory Reset role is created during the initialization of the Uplogix Local Manager in FIPS mode. The Factory Reset Role includes one privilege: the ability to

[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, most of its SRDIs are accessible and configurable via the UCC.

factory reset 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 the UCC.

Operators can also use remote authentication servers RADIUS and TACACS+ for authenticating over SSH to the module. Uplogix LM requires the operators to establish the shared secret of a minimum 7 characters long (as also listed in the 'Security Rules' section of this document).

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 TLS web GUI, the probability of successfully guessing the password is at least 1 in 26^7.

Both the Uplogix LM and UCC RSA certificates used for SSH and HTTPS web services traffic must be at least 2048-bits in length. This provides 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 1:2^2034.

No more than 500 login attempts may be made 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 would be issued from the LM to the UCC per minute. No more than 4000 requests/minute can be attempted for connection attempts from LM to UCC. Given that a 2048-bit RSA key provides 2^112

bits of encryption strength, the likeliness of breaking the key in a minute with this strategy is 4000 in 2^112 attempts or 1 in 2^100.

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 set up of the Uplogix LM, the admin password must be changed from the standard credentials.
2. Tamper labels shipped with the LM must be properly applied while engaging the LM in FIPS mode.
3. If TACACS+ or RADIUS is used, ensure the shared secret is at least 7 characters long.
4. The IPSec shared key and IPSec X Auth user password must be at least 7 characters long.
5. 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.
6. 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.
7. For the 3200, the power supply and I/O cards must be installed in the LM for opacity reasons.
8. For the 430, the modem slot must be populated in the LM for opacity reasons.
9. 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.

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 the FIPS-approved pseudo random number generators ANSI X9.31 RNG and the SP800-90 DRBG whenever generating keys.
3. The Uplogix LM shall provide identity-based authentication of operators by verifying the operator's username and password or SSH public key.
4. The Uplogix LM software will disable the following services in FIPS mode: Telnet, Telnet pass-through, dial-in, xbrowser, service access (with the exception of `service_access off`), login via the power controller, editing of the boot menu, update via LCD, and configuration import via FTP.
5. All TLS transactions will require trusted public keys.
6. The Uplogix LM generates its own unique SSH key pairs. The public key may be transmitted to an accompanying UCC.
7. The Uplogix LM will enforce user password restrictions (at minimum 7 characters).
8. The `config reinstall` command provides a Crypto Officer the ability to zeroize keys and all other configuration data.
9. On every boot of the LM the FIPS self-tests run.
10. All data transferred over PPTP is considered plain text unless protected by an SSH or TLS session.
11. All data transferred over SNMP is considered plain text.

4.2. Secure Operation Initialization Rules

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

Table 5: Uplogix Cryptographic Algorithm Sizing

Algorithm	Sizing / Use	Compliant?	NSS Certificate #	Libgcrypt Certificate #
Asymmetric Algorithms				
DSA	1024 bit	Yes	515	517
RSA	1024 to 4096 bit	Yes	812	815
Symmetric Algorithms				
AES	128, 192, and 256	Yes	1644	1647
Triple-DES	2TDEA, 3TDEA	Yes	1074	1076
Hashing Algorithms				
SHA1	160, 224, 256, 384 and 512 bit variants	Yes	1445	1448
HMAC-SHA1	160, 224, 256, 384 and 512 bit variants	Yes	966	968
Random Number Generators				
ANSI X9.31	AES 128-bit	Yes		881
DBRG 800-90	SHA-256	Yes	90	

Key Exchange				
RSA (key wrapping; key establishment methodology provides between 112 and 150 bits of encryption strength)	TLS Pre-Master Secret	No*		
Diffie-Hellman (key agreement; key establishment methodology provides between 80 and 112 bits of encryption strength)	TLS Pre-Master Secret	No*		
Diffie-Hellman (key agreement; key establishment methodology provides between 112 and 192 bits of encryption strength)	IKE Session Key	No*		
Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength)	SSH Session Key	No*		

*This algorithm is not FIPS-approved, but it is allowed for this use in FIPS mode.

Table 6: Other Uplogix Cryptographic Algorithm Uses

Algorithm	How the Algorithm is Used	FIPS-approved
DES	SNMPv3	No
AES/CFB *	SNMPv3	No
HMAC-MD5-96	SNMPv3	No
HMAC-SHA-96	SNMPv3	No
MD5	TACACS+ and RADIUS	No
RC4	PPTP	No

* SNMP v3 uses a non-FIPS validated implementation of AES.

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 user name: 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 of minimum seven characters.
4. Use the `enable <username>` command to log out as admin and log in as <username>.
5. Once the new user has been created, 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 in to the system as the user created in step 3.
10. If the LM will be 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` 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 4: Tamper Evident Label Placement on the 430 and 3200. Additional TELs may be ordered from Uplogix using part number (61-0001-00).

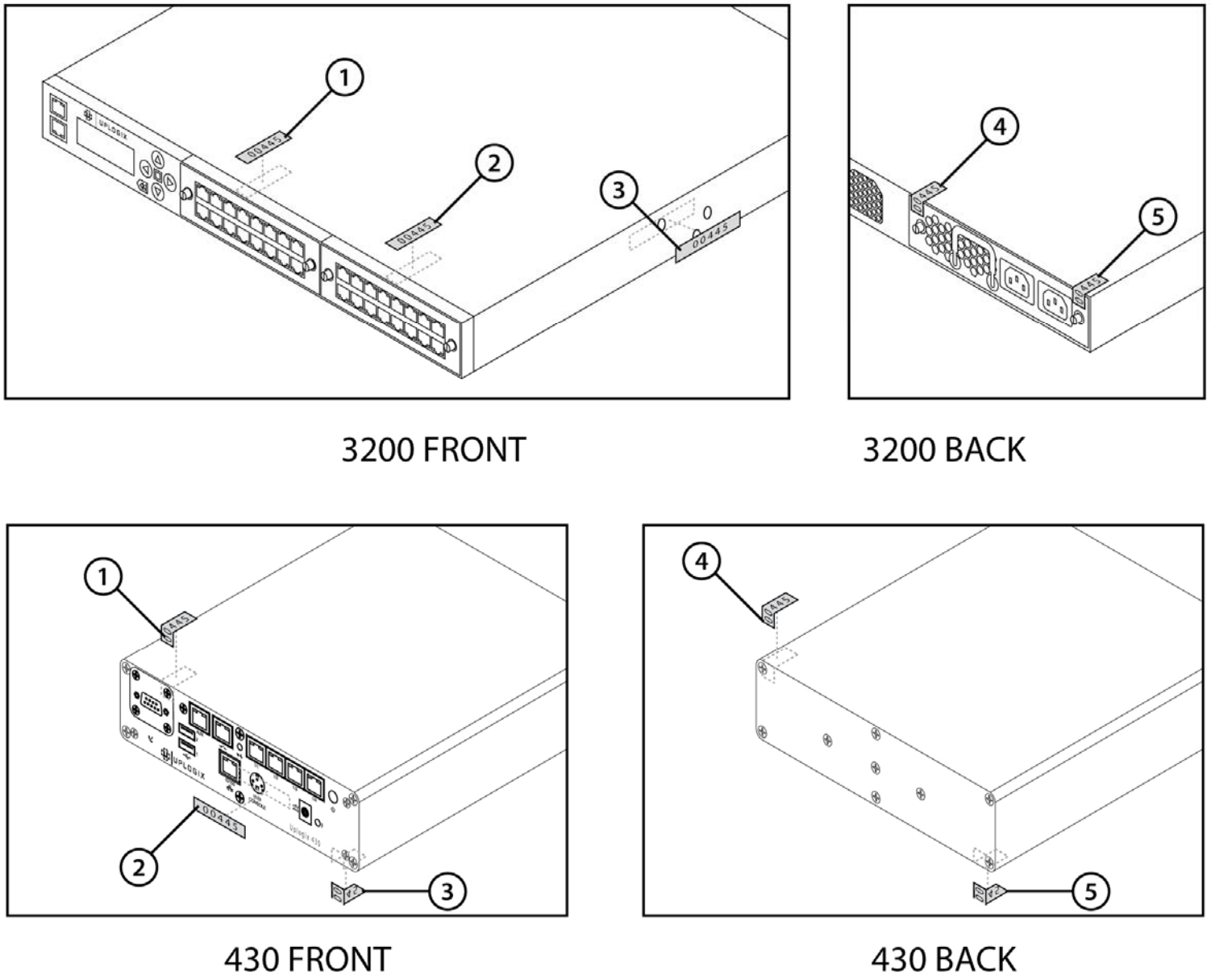

Figure 5: Tamper Label Placement on the 430 and 3200

4.3. Physical Security Rules

As part of the FIPS-mode enabling procedure, the Crypto-Officer is responsible for applying the tamper-evident labels on the modules, as shown in the Figure 4: Tamper label placement on the 430 and 3200. Each 430 and the 3200 module versions require a total of five tamper-evident labels.

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.

4.4. FIPS Operation Modes

This section describes FIPS operation modes.

4.4.1. 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.”

4.4.2. FIPS Failure Modes

This mode is entered when the module fails conditional or start up self-tests with the exception of a software load failure. 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. 430 – The heartbeat LED will blink S.O.S using Morse Code

B. 3200 – The LCD will read “FIPS Failure”

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 7: Uplogix Security Relevant Data Items

Security Relevant Data Item	Storage	SRDI Description
NSS RNG Seed	RAM	Used for the SP 800-90 DRBG using SHA-256
Libgcrypt RNG Seed	RAM	Used for ANSI X9.31 RNG using 128-bit AES.
Libgcrypt RNG Seed Key	RAM	Used for ANSI X9.31 RNG using 128-bit AES.
Operator Passwords	Disk	Used for user authentication via SSH, the console port, or with the UCC.
Operator Public Keys	Disk	Alternative mechanism for user authentication via SSH.
SSH RSA 2048 Public Key	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 RSA 2048 Private Key	Disk	Unique RSA private key used to sign SSH key exchange data.
SSH DH Key Pair	RAM	Used to transmit keying information for SSH session keys.
SSH HMAC Integrity Keys	RAM	Used to verify SSH transport data. Algorithm: HMAC-SHA1.
SSH Session Keys	RAM	Used to encrypt the SSH transport. Algorithms: Triple-DES CBC, AES 128 CBC, AES 192 CBC, AES 256 CBC.
TLS RSA Certificate for LM	Disk	Unique to the LM. Used to authenticate and differentiate itself with the UCC web services. 2048, 3072, or 4096-bit.
TLS RSA Private Key for LM	Disk	Corresponding private key to decrypt messages created with the certificate/public key.
TLS RSA Certificate for UCC	Disk	Used to authenticate the UCC to the LM for web services.
TLS CA Certificates	Disk	Used to verify a server certificate used with generic HTTPS and SMTPS functionality. 1024-4096 RSA or 1024 DSA keys.
TLS Server Certificates	Disk	Used to verify a server certificate used with generic HTTPS and SMTPS functionality. 1024-4096 RSA or DSA keys.
TLS DH Key Pair	RAM	Used with the DHE_RSA/DHE_DSS TLS cipher suites.
TLS Pre-master Secret	RAM	48-bytes key used to generate session keys for TLS.
TLS HMAC Integrity Keys	RAM	Used to verify TLS data. Algorithm: HMAC-SHA1.
TLS Session Keys	RAM	Used to encrypt the TLS transport. Algorithms: Triple-DES CBC, AES 128 CBC, AES 256 CBC.
IKE Pre-Shared Key	Disk	Used to authenticate the LM with a VPN server during

		phase 1 aggressive mode of IPSec.
IPSec XAuth user Password	Disk	Secondary authentication for the LM with the VPN server using the XAuth extension after phase 1 aggressive mode.
IKE DH Key Pair	RAM	Used during phase 1 aggressive mode to negotiate the IKE Session key.
IKE HMAC Integrity Keys	RAM	Used to verify IKE data. Algorithm HMAC-SHA1.
IKE Session Key	RAM	Used to encrypt XAuth and phase 2 quick mode interactions. Algorithms: Triple-DES CBC, AES 128 CBC, AES 192 CBC, AES 256 CBC.
IPSec HMAC Integrity Keys	RAM	Used to verify IPSec data. Algorithm: HMAC-SHA1.
IPSec Session Keys	RAM	Used to encrypt the IPSec transported data. Algorithms: Triple-DES CBC, AES 128 CBC, AES 192 CBC, AES 256 CBC.
IPSec PFS DH Key Pair	RAM	Used during phase 2 quick mode to negotiate the IPSec Session keys.
Uplogix Firmware Certificate	Disk	2048-bit RSA key used to verify the signature of Uplogix firmware images for the LM.
RADIUS Shared Key	Disk	Shared secret used with RADIUS authentication server.
TACACS+ Shared Key	Disk	Shared secret used with TACACS+ authentication server.
SMS Key	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.
PPP Shared Key	Disk	Shared secret used with PPP server.
PPTP Shared Key	Disk	Shared secret used with PPTP server.
Email Passwords	Disk	Passwords used to authenticate LM with SMTP servers.
Device Passwords	Disk	Passwords used to authenticate LM with devices it manages.
IPMI Passwords	Disk	Passwords used to authenticate LM with device service processors (ex. Dell DRAC).
Export Password	Disk	Password used to authenticate LM with SCP/FTP server receiving periodic stats via export process.
SOCKS Proxy Password	Disk	Password used by UCC applet to authenticate with SOCKS server which proxies access to the LM. This is not used on the LM, but it is transmitted from the UCC to the LM during the heartbeat web (TLS) service.
SNMPv3 Auth Password	Disk	Optional password used by SNMPv3 clients to retrieve very limited system information.
SNMPv3 Priv Password	Disk	Optional password used by SNMPv3 clients to retrieve very limited system information.

With the exception of 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 five separate permissions: read, write, execute, delete, and zeroize. If no permission is listed, then an operator has no access to the SRDI.

Table 8: Uplogix 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	SSH	Other TLS functions	IPSec	SMS Monitor	Update Functions	Guest Role	SSH	Show Functions	Configuration Functions	Factory Reset Role	Factory Reset (implicitly disables FIPS Mode)	Uplogix Control Center	Web Services
Security Relevant Data Item																		
NSS RNG Seed				r	r	r	r		r	r		r						
libgcrypt RNG Seed								r										
libgcrypt RNG Seed Key								r										
Operator Passwords				w d	r	r w						r w		w		z w		r w d
Operator Public Keys			r	w d		r						r	r			z w		r w d
SSH RSA 2048 Public Key Pair				w	d	r						r				z w		r
SSH RSA 2048 Private Key Pair				w	d	r						r				z w		
SSH DH Key Pair						r w						r w						
SSH HMAC Integrity Keys						r w						r w						
SSH Session Keys						r w						r w						
TLS RSA Certificate for LM			r	w	d											z w		r
TLS RSA Private Key for LM				w	d											z w		
TLS RSA Certificate for UCC			r	w	d											z w		r
TLS CA Certificates			r	w d			r									z w		r w d
TLS Server Certificates			r	w d			r									z w		r w d
TLS DH Key Pair							r w											r w
TLS Pre-master Secret							r w											r w
TLS HMAC Integrity																		r w

Keys																	
TLS Session Keys							r w										r w
IKE Pre-Shared Key				w				r							z w		r w d
IPSec XAuth User Password				w				r							z w		r w d
IKE DH Key Pair								r w									
IKE HMAC Integrity Keys								r w									
IKE Session Key								r w									
IPSec HMAC Integrity Keys								r w									
IPSec Session Keys								r w									
IPSec PFS DH Key Pair								r w									
Uplogix Firmware Certificate										r							
RADIUS Shared Key				w		r					r				z w		r w d
TACACS+ Shared Key				w		r					r				z w		r w d
SMS Key				w	d				r						z w		r
PPP Shared Key				w											z w		r w d
PPTP Shared Key				w											z w		r w d
Email Passwords				w											z w		r w d
Device Passwords				w											z w		r w d
IPMI Passwords				w											z w		r w d
Export Password				w											z w		r w d
SOCKS Proxy Password															z w		w d
SNMPv3 Auth Password				w											z w		r w d
SNMPv3 Priv Password				w											z w		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, and the SSH RSA and DSA key pairs are deleted. When the system next boots, SMS and SSH keys are created automatically. The TLS certificates are manually created/configured.

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. Mitigation of Other Attacks

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

Appendix A: Roles and Their Permissions on Resources

Unauthenticated Access:

Model	Mode	Resource	Permission
Uplogix 3200	LCD/Keypad	system	config reinstall
Uplogix 3200	LCD/Keypad	system	config system ip
Uplogix 3200	LCD/Keypad	system	config system management
Uplogix 3200	LCD/Keypad	system	config system pulse
Uplogix 3200	LCD/Keypad	system	config system serial
Uplogix 3200	LCD/Keypad	system	restart
Uplogix 3200	LCD/Keypad	system	show alarms
Uplogix 3200	LCD/Keypad	port, system	show info
Uplogix 3200	LCD/Keypad	modem, system	show status
Uplogix 3200	LCD/Keypad	system	show sys ipv6
Uplogix 3200	LCD/Keypad	system	show system ip
Uplogix 3200	LCD/Keypad	system	show system management
Uplogix 3200	LCD/Keypad	system	show system pulse
Uplogix 3200	LCD/Keypad	system	show system serial
Uplogix 3200	LCD/Keypad	system	shutdown
Uplogix 3200	Console	system	show system fips
Uplogix 3200	Console	system	show version
Uplogix 430 and 3200	SNMP	system	show system properties
Uplogix 430 and 3200	SNMP	system	show version
Uplogix 430	430 button	system	restart
Uplogix 430	430 button	system	config reinstall
Uplogix 430 and 3200	Visual Inspection	N/A	Monitoring physical ports activity using the ports LEDs for both 430 and 3200
Uplogix 430	Visual Inspection	N/A	Monitoring FIPS-mode status using the Heartbeat LED
Uplogix 430 and 3200	Visual Inspection	N/A	Monitoring power status on both 430 and 3200 using the power LEDs

Note: 3200 console prompt displays the OS version while prompting for username and password. Additionally, the 3200 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.

Resource	Permission
port	assimilate
port	autorecovery
port	capture
port	certify
port	clear counters
port	clear log
port	clear password
port	clear service-module
server	config aaa
modem	config answer
port	config authentication
system	config date
port	config device logging
system	config environment
system	config export
server	config filter
system	config group
server	config hierarchy
system	config import
port	config info
port	config init
server	config inventory
server	config label
server	config license
port	config log rule
port, system	config monitors
powercontrol	config outlets
system	config password
modem	config ppp
port	config properties

port	config protocols forward
port	config protocols pass-through
port	config protocols shadow
port, system	config removejob
server	config report
system	config restrict
system	config role
system	config rule
system	config ruleset
port, system	config schedule
port	config serial
port	config service-processor
port	config settings
system	config slv
system	config system applet
system	config system archive
system	config system authentication
system	config system banner
system	config system clear archive
system	config system clear export
system	config system clear port
system	config system clear securid
system	config system clear slot
system	config system crypto certificate client
system	config system crypto certificate management
system	config system crypto certificate other*
system	config system crypto regenerate**
system	config system email
system	config system export
system	config system fips
system	config system ip
system	config system ipt
system	config system keypad
system	config system management
system	config system ntp
system	config system page-length
system	config system properties

system	config system protocols dhcp
system	config system protocols filter
system	config system protocols ssh
system	config system protocols telnet
system	config system pulse
system	config system serial
system	config system snmp
system	config system syslog-options
system	config system timeout
system	config update
system	config user
system	config user certificate
modem	config vpn
system	connect
port	copy
port	delete
port	device execute
port	device ping
port	edit running-config
system	export
port	forward
port	interface
system	login
port	name
powercontrol	off
powercontrol	on
system, port	ping
port	power
modem	ppp off
modem	ppp on
port	pull os
port	pull running-config
port	pull startup-config
port	pull tech
port	push os
port	push running-config
port	push startup-config

port	reboot
port	recover configuration
system	restart
port	restore
port	rollback assimilate
port	rollback authentication
port	rollback config
server	run report
system	service access
port	service-processor exec
server	show aaa
port, system	show alarms
system	show all
modem	show answer
system	show archive
port	show authentication
port	show buffer
system	show capture
port	show chassis
powercontrol	show circuit
port	show config
system	show date
port	show device change
port	show device changes
port	show device logging
port	show device syslog
port	show diff
port	show directory
system	show environment
port, system	show events
port	show faults
server	show filter
port	show gps events
port	show gps position
system	show group
port	show info
system	show install-history

port	show interface
server	show inventory
port	show label
server	show license
port, system	show log
port, system	show monitors
powercontrol	show outlets
port	show pingstats
system	show ports
port	show post
modem	show ppp
system	show privileges
port	show properties
port	show protocols forward
port	show protocols pass-through
port	show protocols shadow
port	show remotestate
server	show report
system	show restrict
system	show role
port	show rollback-config
system	show rule
system	show ruleset
port	show running-config
port, system	show schedules
port	show serial
port	show service-module
port	show service-processor
system	show session
system	show sessions
port	show settings
system	show slv stats
system	show slv test
port	show startup-config
port	show status
system	show system applet
system	show system archive

system	show system authentication
system	show system banner
system	show system crypto certificate client
system	show system crypto certificate management
system	show system crypto certificate other
system	show system email
system	show system export
system	show system fips
system	show system ip
system	show system ipt
system	show system keypad
system	show system management
system	show system ntp
system	show system page-length
system	show system properties
system	show system protocols
system	show system pulse
system	show system serial
system	show system snmp
system	show system syslog-options
system	show system timeout
port	show tech
system	show user
system	show version
modem	show vpn
system	show who
system	shutdown
port	squeeze
port, system	suspend
port	terminal
port	terminal break
port	terminal force
port	terminal lock
port	terminal shadow
server	upload archive
port	use system auth

Notes:

* provides `config system crypto certificate ca` and `config system crypto certificate server`
** provides `config system crypto regenerate sms` and `config system crypto regenerate ssh`
All privileges in the table above with a port resource are also available on the power controller and modem.

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

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

Factory Reset Access:
The Factory Reset Role is created by the Crypto Officer.

Resource	Permission
system	config reinstall