FIPS 140-2 Security Policy

Uplogix 430, 3200, 500 and 5000

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

May 5, 2014

Document Version 2.4

Table of Contents

Table of Figures

Table of Tables

FIPS 140-2 Security Policy
Uplogix 430, 3200, 500 and 5000

1. Introduction

This document describes the Non-Proprietary FIPS 140-2 Security Policy for the Uplogix 430, 3200, 500 and 5000 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, 3200, 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.

1.1. Purpose

This document covers the secure operation of the Uplogix 430, 3200, 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 4.6.4.24340g which runs on the product.

1.2. Models Tested

Table 1: Models Tested under FIPS certificate #2140

Model	Firmware Version	Hardware Version
Uplogix 430, FIPS, CF	4.6.4.22900g	43-1102-50
Uplogix 3200, FIPS-05, SSD	4.6.4.22900g	37-0326-04
Uplogix 500 Local Manager, 5 Serial Ports, Government	4.6.4.22900g	61-5050-33
Uplogix 5000 Local Manager, 5 Serial Ports + 2 Expansion Bays, Government	4.6.4.22900g	61-5500-33

Note: The 430 model is available with a V.92 modem, DB9 connection for modem or a blank over the modem slot. The 500 and 5000 models are available with a V.92 modem, cellular modem, a DB9 connection for a modem, or a blank over the mezzanine option slot.

Additionally, the 3200 model is available with either a V.92 modem or DB9 connection for modem in the modem slot.

The 3200 model and the 5000 have two option slots on the front of the equipment for connecting I/O modules. I/O modules are available in two forms on the 3200: a 16 serial card and an 8 serial by 8 Ethernet card. I/O modules are also available in two forms on the 5000: an 8 serial card and an 8 Ethernet card.

Subsequent to receipt of FIPS certificate #2140 for models tested in table 1, non-security relevant changes were identified in the firmware of the models. These changes include modifications to the certificate process for heartbeat when in non-FIPS mode and bug fixes that do not impact security relevant items. Code with these changes is identified with a different firmware version number for the models tested. These models are listed below.

Table 2: Models tested with code revisions

Model	Firmware Version	Hardware Version
Uplogix 500 Local Manager, 5 Serial Ports, Government	4.6.4.24340g	61-5050-33
Uplogix 5000 Local Manager, 5 Serial Ports + 2 Expansion Bays, Government	4.6.4.24340g	61-5500-33

1.3. Security Level

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

Table 3: 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 2
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 4: 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
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
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-SHA	Hash-based Message Authentication Code – Secure Hash Algorithm
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
PBKDF2	Password-Based Key Derivation Function 2
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

SHA	Secure Hash Algorithm
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.
Uplogix 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.
Uplogix 500 Local Manager	Comprehensive functionality in a fixed 5-port LM designed for enterprises needing to monitor, manage and control five or fewer devices and their power supply at any distributed location.
Uplogix 5000 Local Manager	Uplogix Local Manager, available in 5-,13-, or 21-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, 3200, 500 and 5000 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 5: 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 6: 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

2.3. Uplogix 500

Figure 5: Uplogix 500 Front Side

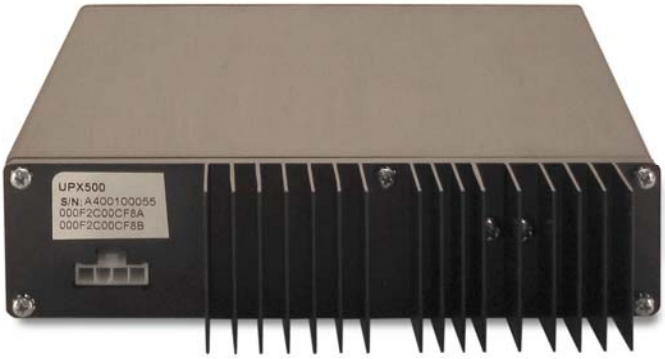

Figure 6: Uplogix 500 Back Side

Table 7: 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, Power Out
Mezzanine Option Slot	Data In and Out, Control In, Status Out
Five (5) Serial Ports*	Data In and Out
Power Controllers	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 8: 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, Power Out
Mezzanine Option Slot	Data In and Out, Control In, Status Out
Five (5) Serial Ports*	Data In and Out
Power Controllers	Data In and Out
LCD	Status Out
Keypad	Control 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, 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.

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 the ability to perform all actions on various resources with the exception of factory reset of the LM. 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 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, most of its SRDIs are accessible and configurable via the UCC.

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 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.

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 1:2^98.

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 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 likelihood 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 setup 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. 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. For the 430, the modem slot must be populated in the LM for opacity reasons.
7. For the 3200, the power supply must be installed and I/O card slots must be populated in the LM for opacity reasons.
8. For the 500, the mezzanine option slot must be populated and the power cord plugged in on the LM for opacity reasons.
9. For the 5000, the I/O card slots and the mezzanine option slot must be populated in the LM for opacity reasons.

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, 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. The Uplogix LM will allow dial in to be configured only with TLS encryption required.
6. All TLS transactions will require trusted public keys.
7. The Uplogix LM generates its own unique SSH key pairs. The public key may be transmitted to an accompanying UCC.
8. The Uplogix LM enforces minimum shared secret length of at least seven (7) characters when using TACACS+ or RADIUS.
9. The Uplogix LM will enforce user password restrictions (at minimum 7 characters).
10. The `config reinstall` command provides a Crypto Officer the ability to zeroize keys and all other configuration data.
11. On every boot of the LM the FIPS self-tests run.
12. All data transferred over PPTP or IPsec is considered plain text unless protected by an SSH or TLS session.
13. 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 9: Uplogix Cryptographic Algorithm Sizing

Algorithm	Sizing / Use	Compliant?	NSS Certificate #
Asymmetric Algorithms			
DSA*	1024 bit	Yes	719
RSA**	1024 to 4096 bit	Yes	1181
Symmetric Algorithms			
AES	128, 192, and 256	Yes	2293
Triple-DES	2TDEA, 3TDEA	Yes	1442
Hashing Algorithms			
SHA	160, 224, 256, 384 and 512 bit variants	Yes	1976

HMAC-SHA	160, 224, 256, 384 and 512 bit variants	Yes	1409
Random Number Generator			
DBRG 800-90	SHA-256	Yes	285
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 112 bits of encryption strength; non-compliant less than 112 bits)	TLS Pre-Master Secret	No***	
Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength)	SSH Session Key	No***	

*DSA certificate #719; non-compliant with the functions from the CAVP Historical DSA list
**RSA certificate #1181; non-compliant with the functions from the CAVP Historical RSA list
***This algorithm is not FIPS-approved, but it is allowed for this use in FIPS mode

Table 10: Key Defining Functions

Key Defining Functions	Algorithm	Certificate Numbers		
		SSH Client	SSH Server	NSS
SSH KDF	DH14 and SHA-1	48	47	--
TLS 1.0	SHA-1 and MD5	--	--	46

Additionally, algorithms used by the Uplogix' IPsec implementation are non-approved because the ANSI X9.31 RNG is not guaranteed to have sufficient entropy. Therefore, all data transferred over IPsec is considered plain text unless protected by an SSH or TLS session.

Table 11: Uplogix IPsec Algorithm Sizing (Non-Approved)

Algorithm	Sizing / Use
Asymmetric Algorithm	
DSA	1024 bit
Symmetric Algorithms	
AES	128, 192, and 256
Triple-DES	2TDEA, 3TDEA
Hashing Algorithms	
SHA	160, 224, 256, 384 and 512 bit variants
HMAC-SHA	160, 224, 256, 384 and 512 bit variants
Random Number Generator	
ANSI X9.31	AES 128-bit

Key Exchange	
Diffie-Hellman (key agreement; key establishment methodology provides up to 192 bits of encryption strength)	IKE Session Key
Key Defining Function	
IKEv1	Legacy implementation; HMAC-SHA1, HMAC-SHA-256, DH5, DH14-18

Table 12: Other Uplogix Cryptographic Algorithm Uses (Non-Approved)

Algorithm	How the Algorithm is Used
DES	SNMPv3, TACACS+, and RADIUS
AES/CFB *	SNMPv3
HMAC-MD5-96	SNMPv3
HMAC-SHA-96	SNMPv3
MD5	Password Authentication
PBKDF2-SHA-256	Password Authentication
RC4	PPTP

* 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 into 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 9: Tamper Evident Label Placement on the 430 and 3200 or Figure 10: Tamper Evident Label Placement on the 500 and 500. Additional TELs may be ordered from Uplogix 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.

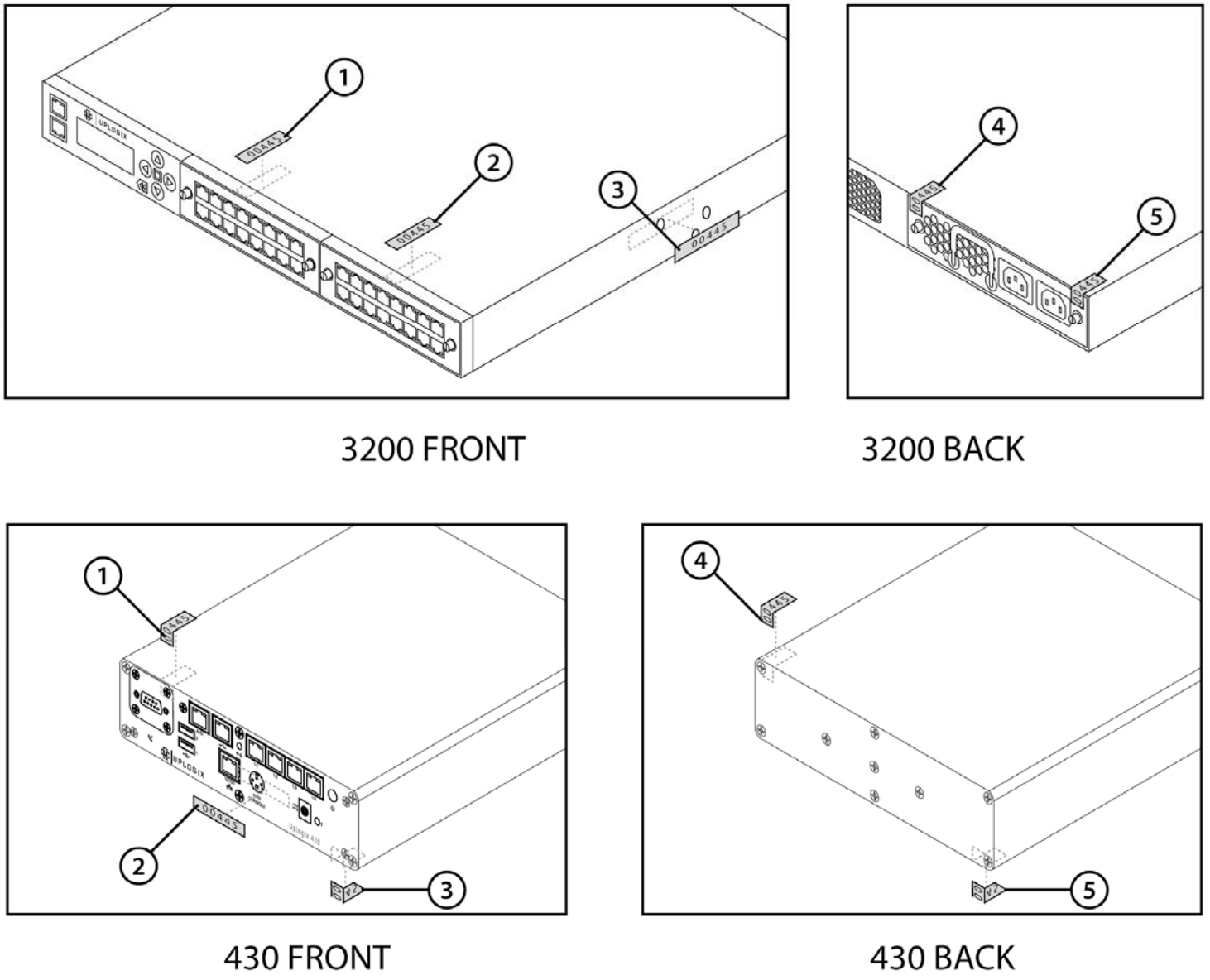

Figure 9: Tamper Label Placement on the 430 and 3200

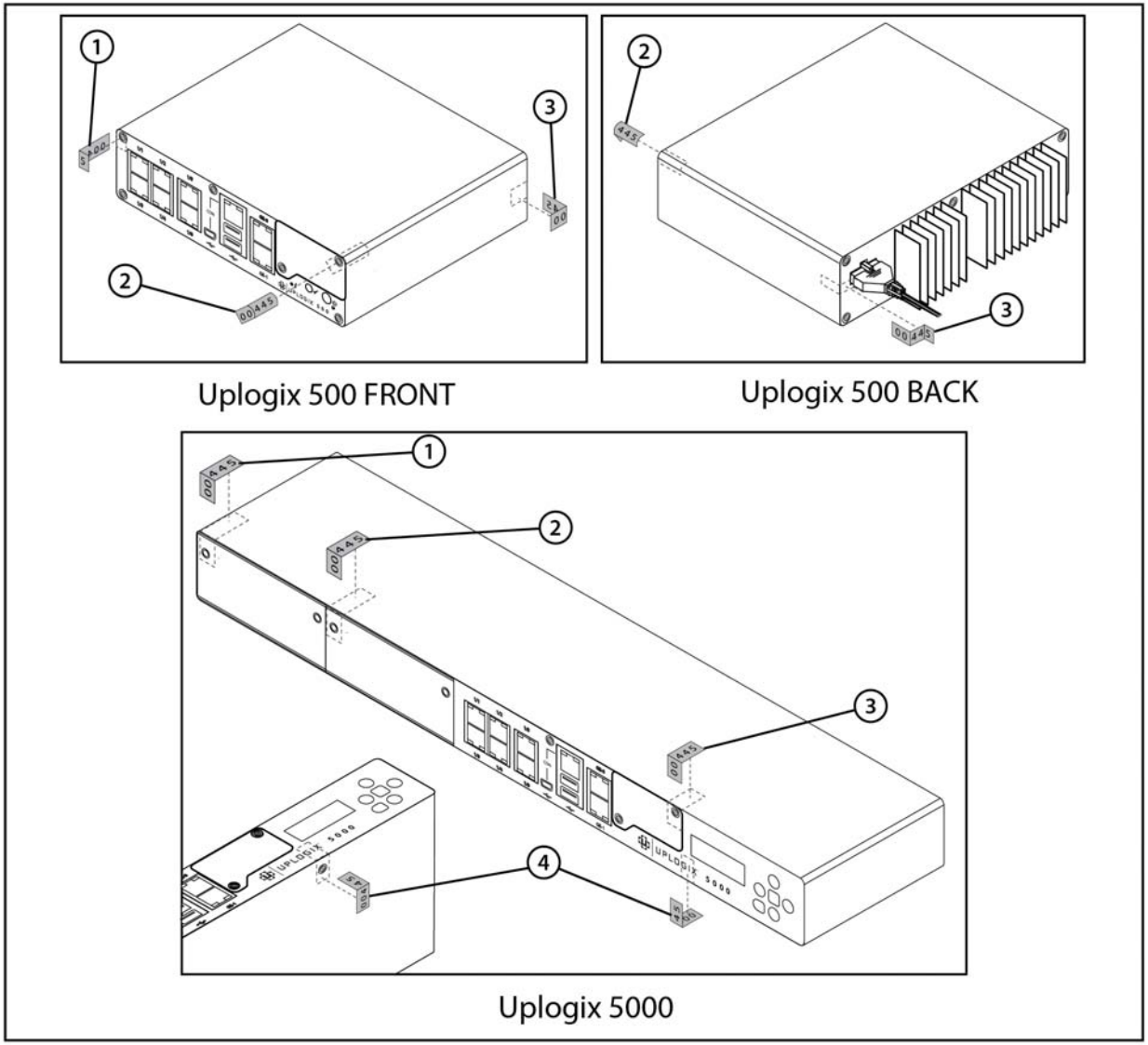

Figure 10: Tamper Label Placement on the 500 and 5000

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 9: Tamper label placement on the 430 and 3200 or Figure 10: Tamper Label Placement on the 500 and 5000. The 430 and the 3200 module versions require a total of five tamper-evident labels while the 500 module requires 3 and the 5000 module requires 4.

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 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)

4.4.3. 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 13: Uplogix Security Relevant Data Items

Security Relevant Data Item	Storage	SRDI Description
Device Passwords	Disk	Passwords used to authenticate LM with devices it manages.
Email Passwords	Disk	Passwords used to authenticate LM with SMTP servers.
Export Password	Disk	Password used to authenticate LM with SCP/FTP server receiving periodic stats via export process.
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 or HMAC-SHA-256.
IKE Pre-Shared Key	Disk	Used to authenticate the LM with a VPN server during phase 1 aggressive mode of IPsec.
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.
IPMI Passwords	Disk	Passwords used to authenticate LM with device service processors (ex. Dell DRAC).
IPsec HMAC Integrity Keys*	RAM	Used to verify IPsec data. Algorithm: HMAC-SHA1 or HMAC-SHA-256.
IPsec PFS DH Key Pair*	RAM	Used during phase 2 quick mode to negotiate the IPsec Session keys.
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 XAuth user Password	Disk	Secondary authentication for the LM with the VPN server using the XAuth extension after phase 1 aggressive mode.
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.
NSS DRBG Entropy Input	RAM	Used for the SP 800-90 DRBG using SHA-256
NSS DRBG Seed	RAM	Used for the SP 800-90 DRBG using SHA-256
NSS DRBG V Value	RAM	Used for the SP 800-90 DRBG using SHA-256
NSS DRBG C Value	RAM	Used for the SP 800-90 DRBG using SHA-256
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.
PPP Shared Key	Disk	Shared secret used with PPP server.
PPTP Shared Key	Disk	Shared secret used with PPTP server.
RADIUS Shared Key	Disk	Shared secret used with RADIUS 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.
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.
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.
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 RSA 2048 Private Key	Disk	Unique RSA private key used to sign SSH key exchange data.
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 Session Keys	RAM	Used to encrypt the SSH transport. Algorithms: Triple-DES CBC, AES 128 CBC, AES 192 CBC, AES 256 CBC.
TACACS+ Shared Key	Disk	Shared secret used with TACACS+ authentication server.
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 DH Key Pair	RAM	Used with the DHE_RSA/DHE_DSS TLS cipher suites.
TLS HMAC Integrity Keys	RAM	Used to verify TLS data. Algorithm: HMAC-SHA1.
TLS Pre-master Secret	RAM	48-bytes key used to generate session keys for TLS.
TLS RSA 2048-bit Certificate for Dial In	Disk	Unique 2048-bit RSA certificate that identifies the LM, and is used when the Uplogix dial in applet attempts to use an encrypted modem session.
TLS RSA 2048-bit Private Key for Dial In	Disk	Corresponding private key used to establish TLS-encrypted modem sessions.
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 Certificate for UCC	Disk	Used to authenticate the UCC to the LM for web services.
TLS RSA Private Key for LM	Disk	Corresponding private key to decrypt messages created with the certificate/public key.
TLS Server Certificates	Disk	Used to verify a server certificate used with generic HTTPS

		and SMTPS functionality. 1024-4096 RSA or DSA keys.
TLS Session Keys	RAM	Used to encrypt the TLS transport. Algorithms: Triple-DES CBC, AES 128 CBC, AES 256 CBC.
Uplogix Firmware Certificate	Disk	2048-bit RSA key used to verify the signature of Uplogix firmware images for the LM.

Notes:

* The Libgcrypt RNG is only used to generate secrets for IKE and IPsec. While the Libgcrypt RNG is often seeded with sufficient entropy, Uplogix cannot guarantee that the Libgcrypt RNG is always seeded with the 80 bits of entropy required to generate sufficiently random keys. Therefore, all data transferred over IPsec is considered plain text unless protected by an SSH or TLS session.

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 four separate permissions: read, write, delete, and zeroize. If no permission is listed, then an operator has no access to the SRDI.

Table 14: 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	Encrypted Dial in Mode	IPsec	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
IKE DH Key Pair							r w													
IKE HMAC Integrity Keys							r w													
IKE Pre-Shared Key				w			r											zw		r w d
IKE Session Key							r w													
IPMI Passwords				w														zw		r w d

IPsec HMAC Integrity Keys							r w											
IPsec PFS DH Key Pair							r w											
IPsec Session Keys							r w											
IPsec XAuth User Password				w			r										zw	r w d
libgcrypt RNG Seed							r											
libgcrypt RNG Seed Key							r											
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					r	r		zw	r w d
PPP Shared Key				w													zw	r w d
PPTP Shared Key				w													zw	r w d
RADIUS Shared Key				w					r					r			zw	r w d
SMS Key				w	d					r							zw	r
SNMPv3 Auth Password				w													zw	r w d
SNMPv3 Priv Password				w													zw	r w d
SOCKS Proxy Password																	zw	w d
SSH DH Key Pair									r w					r w				
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				
TACACS+ Shared Key				w					r					r			zw	r w d
TLS CA Certificates			r	w d				r									zw	r w d
TLS DH Key Pair						rw		r w					rw					r w
TLS HMAC Integrity Keys						rw							rw					r w

TLS Pre-master Secret						rw		r w						rw					r w
TLS RSA 2048-bit Certificate for Dial In			r	rd	d	r								r				d	d
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 Server Certificates			r	w d				r										zw	r w d
TLS Session Keys								r w											r w
Uplogix Firmware Certificate											r								

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, and the SSH RSA and DSA key pairs are deleted. When the system next boots, SMS and SSH keys and the dial in key pair and certificate 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	Modes
Uplogix 430, 3200, 500 and 5000	SNMP	system	show system properties	FIPS, non-FIPS
Uplogix 430, 3200, 500 and 5000	SNMP	system	show version	FIPS, non-FIPS
Uplogix 430, 3200, 500 and 5000	Visual Inspection	N/A	Monitoring physical ports activity using the ports LEDs for all models	FIPS, non-FIPS
Uplogix 430, 3200, 500 and 5000	Visual Inspection	N/A	Monitoring power status on all models using the power LEDs	FIPS, non-FIPS
Uplogix 3200, 500 and 5000	Console	system	show system fips	FIPS, non-FIPS
Uplogix 3200, 500 and 5000	Console	system	show version	FIPS, non-FIPS
Uplogix 3200 and 5000	LCD/Keypad	system	config reinstall	FIPS, non-FIPS
Uplogix 3200 and 5000	LCD/Keypad	system	config system ip	FIPS, non-FIPS
Uplogix 3200 and 5000	LCD/Keypad	system	config system management	FIPS, non-FIPS
Uplogix 3200 and 5000	LCD/Keypad	system	config system pulse	FIPS, non-FIPS
Uplogix 3200 and 5000	LCD/Keypad	system	config system serial	FIPS, non-FIPS
Uplogix 3200 and 5000	LCD/Keypad	system	config update	Non-FIPS
Uplogix 3200 and 5000	LCD/Keypad	system	restart	FIPS, non-FIPS
Uplogix 3200 and 5000	LCD/Keypad	system	show alarms	FIPS, non-FIPS
Uplogix 3200 and 5000	LCD/Keypad	port, system	show info	FIPS, non-FIPS
Uplogix 3200 and 5000	LCD/Keypad	modem, system	show status	FIPS, non-FIPS
Uplogix 3200 and 5000	LCD/Keypad	system	show sys ipv6	FIPS, non-FIPS
Uplogix 3200 and 5000	LCD/Keypad	system	show system ip	FIPS, non-FIPS

Uplogix 3200 and 5000	LCD/Keypad	system	show system management	FIPS, non-FIPS
Uplogix 3200 and 5000	LCD/Keypad	system	show system pulse	FIPS, non-FIPS
Uplogix 3200 and 5000	LCD/Keypad	system	show system serial	FIPS, non-FIPS
Uplogix 3200 and 5000	LCD/Keypad	system	shutdown	FIPS, non-FIPS
Uplogix 430	430 Button	system	restart	FIPS, non-FIPS
Uplogix 430	430 Button	system	config reinstall	FIPS, non-FIPS
Uplogix 430	Visual Inspection	N/A	Monitoring FIPS-mode status using the Heartbeat LED	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 and Status Buttons	system	FIPS mode status	FIPS, non-FIPS

Note: 3200, 500 and 5000 console prompt displays the OS version while prompting for username and password. Additionally, the 3200, 500 and 5000 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	Modes
port	assimilate	FIPS, non-FIPS
port	autorecovery	FIPS, non-FIPS
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
powercontrol	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
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 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
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 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 serial****	FIPS, non-FIPS
system	config system slot	FIPS, non-FIPS
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
powercontrol	off	FIPS, non-FIPS
powercontrol	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
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
powercontrol	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
port, system	show monitors	FIPS, non-FIPS
powercontrol	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
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 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 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
port	clear xbrowser	Non-FIPS
port	unlock xbrowser	Non-FIPS

Notes:
* provides `config system crypto certificate ca` and `config system crypto certificate server`
** provides `config system crypto regenerate dialin`, `config system crypto regenerate sms` and `config system crypto regenerate ssh`
*** This permission is only available on the Uplogix Control Center.
**** This permission is only available on the Uplogix 3200.
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	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.

Resource	Permission	Modes
system	config reinstall	FIPS, non-FIPS