User Guide

for Local Managers

Version 5.1

December 2014

uplogix.com

Information in this document is subject to change without notice.

Uplogix, Inc.

7600-B North Capital of Texas Highway

Suite 220

Austin, Texas 78731

USA

Contents

About this guide

This guide describes configuration, management, and advanced features of the Local Manager. Refer to the *Installation Guide for Uplogix Local Managers* to install and initially configure the Local Manager.

The information in this guide applies to all models of the Local Manager except where otherwise noted.

> For best results, the Local Manager and a Control Center that manages it must use the same minor version of software (e.g., 5.1). Patch releases may differ (e.g., 5.1.1).

Information in this document is subject to change without notice. Please visit support.uplogix.com for the latest updates to Uplogix product documents.

Target audience

This guide is for trained, qualified network support technicians responsible for installing the Local Manager.

Typographical conventions

The following conventions are used in this guide.

Sample text from the Uplogix command line interface is presented in `this font`. Text that you enter is presented in **`this font`**. For example:

```
[admin@UplogixLM]# show who
admin ssh Mar 22 13:38 (203.0.113.6)
```

Keyboard characters are enclosed in angle brackets. For example, press <Enter>.

Navigation paths to command equivalents on a Control Center are shown in **`this font`**. For example:

```
Administration > Server Settings
```

Safety summary

Following all cautions and warnings will ensure your own safety and protect the Local Manager from potential damage or loss of data.

Caution: Read the installation instructions before connecting the Local Manager to a power source.

Read and understand the following instructions before using the Local Manager:

- Use three wire electrical extension cords with a current rating equal to or greater than the Local Manager’s current rating.
- Always disconnect the Local Manager from power before cleaning and servicing.
- Do not spray liquids directly onto the Local Manager when cleaning. Always apply the liquid first to a static free cloth.
- Do not immerse the Local Manager in any liquid or place any liquids on it.
- Do not disassemble the Local Manager. Hazardous voltages are present inside the Uplogix 5000 system and can result in injury or death. To reduce the risk of shock and to maintain the warranty on the device, a qualified technician must perform service or repair work.
- Connect the Local Manager to a grounded outlet.
- Only connect the Local Manager to surge-protected power outlets.

SAVE THESE INSTRUCTIONS.

Uplogix Glossary

Term	Definition
Archive	Local Managers send bulk data, such as: session logs, change logs, and all other non-urgent statistical data to the Control Center every 60 minutes (default) using an encrypted HTTPS proprietary data communication protocol on port 8443.
Heartbeat	Local Managers communicate with the Control Center every 30 seconds (default) using a secure HTTPS proprietary communication protocol on TCP port 8443. Device state, alarms, events and configuration parameters are sent during a heartbeat.
Local Manager (LM)	A Local Management device that is directly connected to managed network devices and servers.
Pulse	Used by the Local Manager to determine network connectivity by sending data to an echo server on TCP port 7 (echo) every 30 seconds. Up to three may be defined to determine failure.
Uplogix 500	Uplogix 500 Local Manager appliance is a compact, fixed 6-port model that can be used to manage 5 devices and one switched power controller.
Uplogix 5000	Uplogix 5000 Local Manager appliance is a modular chassis model with higher port density that can scale to manage 21 directly connected devices and one switched power controller.
Control Center (UCC)	Centralized element manager for all Local Managers and their managed devices deployed throughout the network. The web-based graphical user interface (GUI) enables IT administrators to easily view, manage, configure and control all network devices and servers connected to Local Managers and supplies access to real time data from these devices. The Control Center is also the integration point for all remotely collected data and diagnostics for upstream delivery to NMS tools such as Solarwinds, HP OpenView, CA Spectrum and Tivoli Netcool.

Introduction to the Local Manager

The Local Manager is a management device that connects directly to managed network devices and servers. The Local Manager runs a proprietary operating system. Utilizing the Local Manager, network device chassis and interface statistics, configuration and event logs are retrieved directly from managed devices using the console command line interface to determine functionality and availability. Maintenance operations can be bundled together as automated procedures, to efficiently perform complex tasks such as OS and configuration upgrades, interface cycles, and password recovery. Automated recovery procedures include configuration rollback and recovery, boot loader (such as ROMmon for Cisco devices) monitoring and recovery, and hung console detection. The Local Manager provides extensive auditing functionality through device and user activity logging at all times, even when the network is down.

This chapter provides information about the physical features of the Local Manager. It also provides information about using the command line interface (CLI). Topics include:

- Chassis views and indicator lights — locations of connectors, indicator lights, and other features
- Working with the keypad
- Working with the front panel
- Working with the command line — structure, command shortcuts, and help

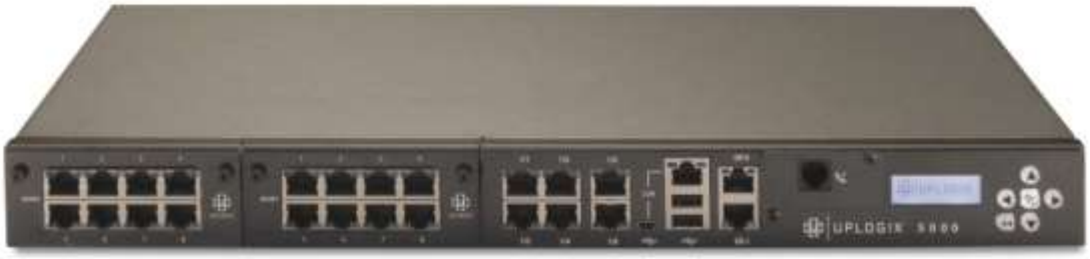
Chassis views and indicator lights

This section identifies the main physical features of the Local Manager.

The Local Manager uses lights to communicate operational status. The Ethernet and serial connectors on the Local Manager have link and activity indicator lights.

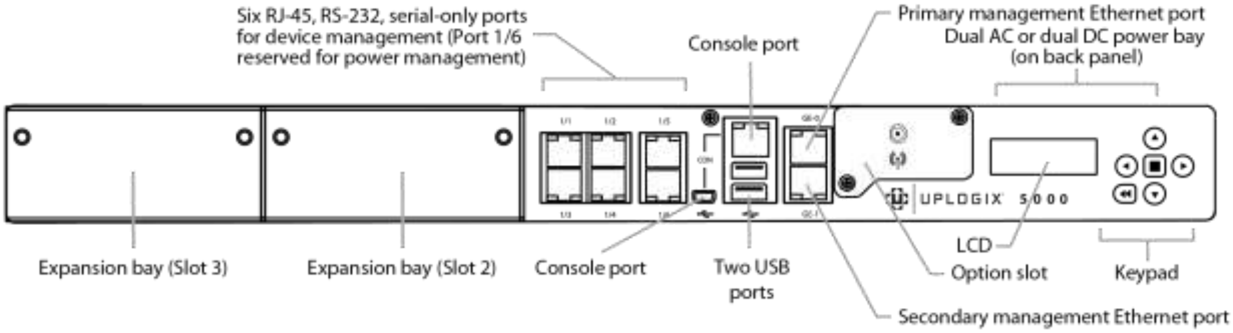
Uplogix 5000

The Uplogix 5000 may be customized by adding additional ports through the two modular expansion bays.



Installing an expansion card

The leftmost bay in the 5000 is designated slot 3 in the system and the rightmost bay as slot 2. Each expansion bay can be used to add either 4, 8 or 16 serial ports or 8 dedicated Ethernet ports. Dedicated Ethernet ports are paired with serial ports to enhance management capabilities for some devices.


Six RJ-45, RS-232, serial-only ports for device management (Port 1/6 reserved for power management)
Console port
Primary management Ethernet port
Dual AC or dual DC power bay (on back panel)
UPLOGIX 5000
Expansion bay (Slot 3)
Expansion bay (Slot 2)
Console port
Two USB ports
LCD
Option slot
Keypad
Secondary management Ethernet port

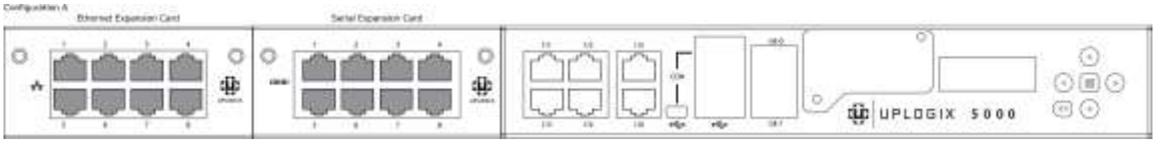
Port Pairings when using Expansion Cards

The Local Manager can use Ethernet to move configuration and software image files back and forth between it and its managed devices.

Dedicated Ethernet ports are used to make a direct Ethernet connection between the Local Manager and managed devices. Dedicated Ethernet ports are always paired with serial ports in the system. The placement of an Ethernet expansion card in the system will determine which serial ports map to its Ethernet ports.

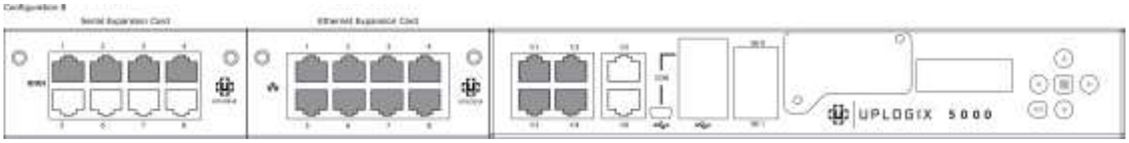
Configuration A: One Ethernet expansion card, one serial expansion card

When an 8 or 16 port serial expansion card is installed in the right expansion bay (slot 2) and an 8 port Ethernet expansion card is installed in the left expansion bay (slot 3), the 8 dedicated Ethernet ports in slot 3 are paired with the first 8 serial ports (ports 2/1 to 2/8) in slot 2.



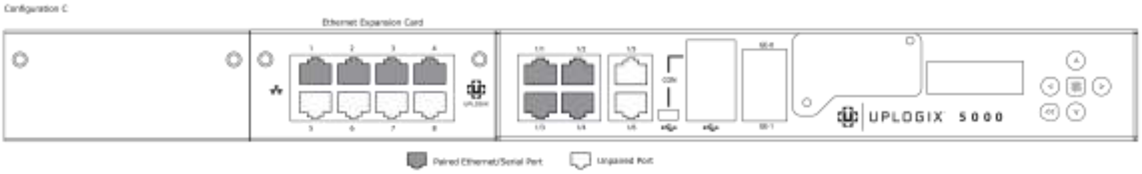
Configuration B One serial port expansion card, one Ethernet expansion card

When an 8 port Ethernet expansion card is installed in the right expansion bay (slot 2) and an 8 or 16 port serial expansion card is installed in the left expansion bay (slot 3), the first four dedicated Ethernet ports are paired with the first four fixed serial ports (ports 1/1 thru 1/4). The remaining Ethernet ports (ports 5-8) are paired with the first four serial ports on the serial port expansion card (ports 3/1 to 3/4).



Configuration C: One Ethernet expansion card, no serial expansion card

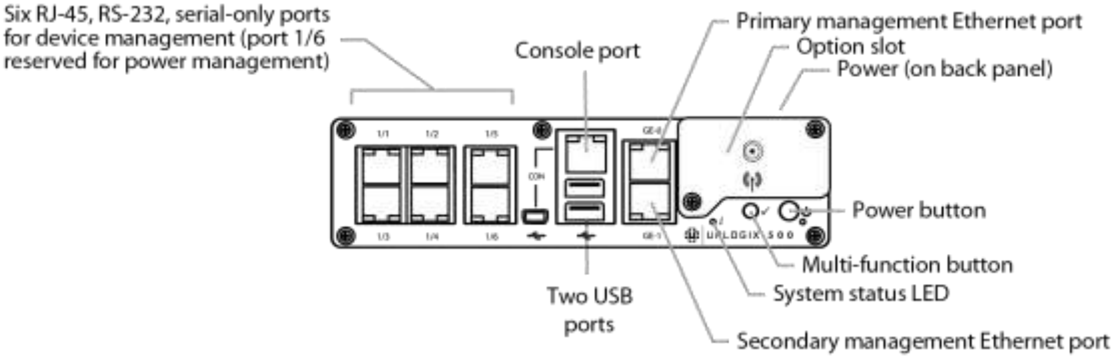
When an eight-port Ethernet expansion card is installed in the right expansion bay (slot 2), the first four Ethernet ports are paired with the first four fixed serial ports (ports 1/1 to 1/4). The remaining fixed serial port (port 1/5) is not paired with a dedicated Ethernet port.



Uplogix 500

The Uplogix 500 is a small form factor Local Manager offering a fixed set of console ports for connection to managed devices.

There are six serial ports that can be connected to managed devices including an intelligent power controller.

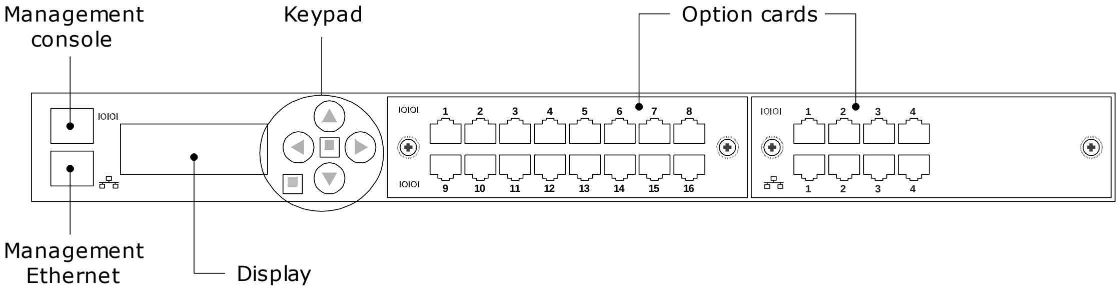

Six RJ-45, RS-232, serial-only ports for device management (port 1/6 reserved for power management)
Console port
Primary management Ethernet port
Option slot
Power (on back panel)
Power button
Multi-function button
System status LED
Secondary management Ethernet port
Two USB ports
1/1
1/2
1/5
1/3
1/4
1/6
CON
GE-0
GE-1
UPLOGIX 500

Uplogix 3200

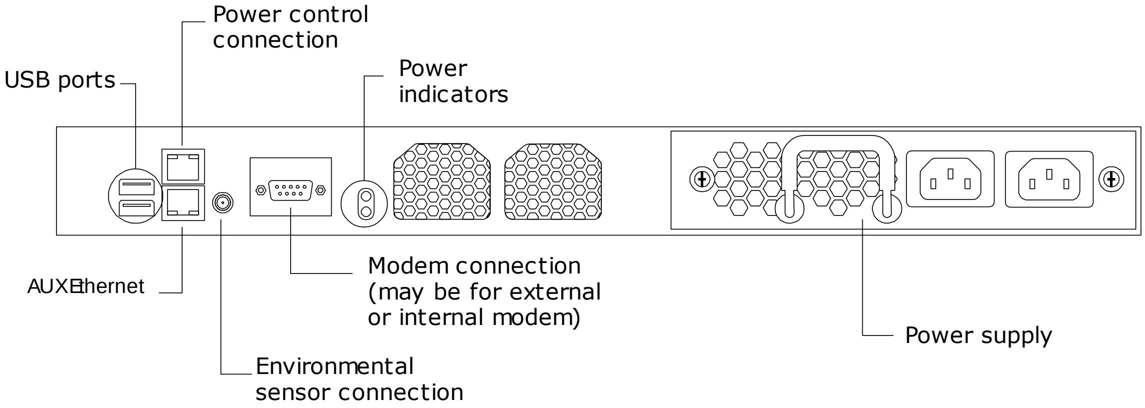
The Uplogix 3200 may be customized by adding additional ports through the two modular expansion bays.

Front panel

The leftmost bay in the 3200 is designated slot 1 in the system and the rightmost bay as slot 2. Each expansion bay can be used to add either four, eight or sixteen serial ports or four, eight or sixteen dedicated Ethernet ports. Dedicated Ethernet ports are paired with serial ports to enhance management capabilities for some devices by providing direct Ethernet connections between the Local Manager and the managed devices.

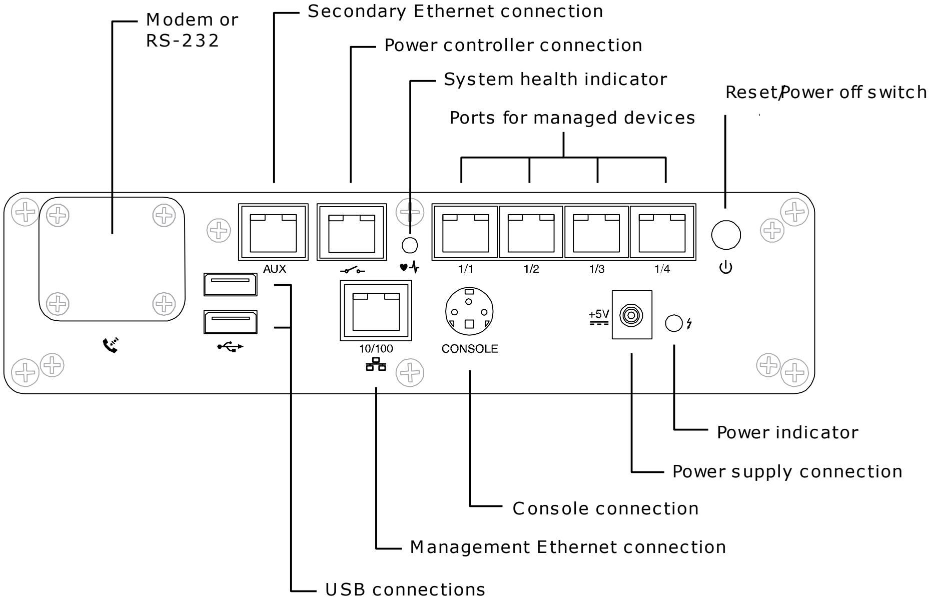


Back panel


Power control connection
USB ports
Power indicators
AUXEthernet
Modem connection (may be for external or internal modem)
Power supply
Environmental sensor connection

Uplogix 430

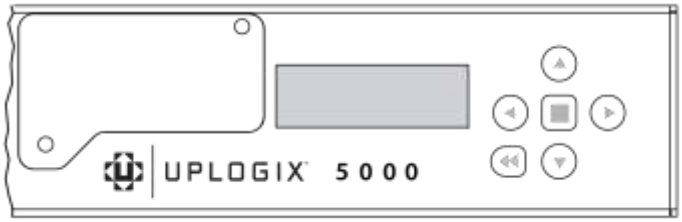
The Uplogix 430 is a small form factor Local Manager offering a fixed set of console ports for connection to managed devices.



There are five serial ports that can be connected to managed devices, where one port is dedicated for connection to an intelligent power controller.

Working with the keypad

The keypad appears on the Uplogix 3200 and 5000 Local Managers.



The keypad located on the front panel provides up, down, left, and right keys (labeled with arrows) as well as enter/power (i.e., the middle key) and back keys. The left and right arrow keys move the cursor left and right, respectively. The up and down arrow keys change numerical values.

Press the Enter/Power key in the center of the keypad to power the Local Manager on when it is powered off. When the Local Manager is powered on, press the Enter/Power key in the center of the keypad to display the menu. The menu functions include:

- Configure — Covers the steps needed to work with the Local Manager via an SSH session. Refer to the *Installation Guide for Local Managers* for more information.
    - Equivalent to the following commands: `config system ip, config system management` and the `config system pulse`
- Restart — Reboots the Local Manager.
    - Equivalent to the `restart` command

- Shutdown — Powers off the Local Manager.
    - Equivalent to the `shutdown` command
- Update — Upgrade the software from the USB flash drive. This option is available only if a USB flash drive is connected to the Local Manager.
    - Equivalent to the `config update usb` command
- Factory reset — Restores the Local Manager to its initial state. For more information, refer to Factory Reset.

Press the Back key below the left arrow key to exit the menu and resume scrolling status information.

Working with the front panel

In most cases the command line provides the functionality needed to work with the Local Manager. The front panel allows basic configuration, power, and reset operations.

Power and reset operations

Uplogix 500 Power and Restart Operations

To do this:	Check to be sure that:	Take this action:	The process is complete when:
Power on	All lights are off	Plug in the power supply and then press the power button on the front panel.	The system status light will slowly blink while the Local Manager boots and will become solid green when the boot process completes.
	The system status light is off and the power supply light is on (amber)	Press the power button on the front panel.	
Restart	The system health light is on and not blinking	A restart is only supported from the CLI or UCC for this platform. To manually restart this platform, follow the instructions in this table to power off and then power on the Local Manager.	
Power off	The system status light is on and not blinking	Press and release power button to initiate a graceful shutdown of the system. The system status light will blink as the unit shuts itself down.	The system status light is off and the power indicator is amber.

Uplogix 5000 Power and Restart Operations

To do this:	Check to be sure that:	Take this action:	The process is complete when:
Power on	All lights are off	Plug in one or both power supplies. A dimly lit keypad and dark LCD indicates power is applied but that the LM is powered down. Next, press the center button on the keypad to power the LM on.	The LCD is scrolling Local Manager information and device status
	Keypad is dimly lit but the LCD is dark/off.	Press the center button on the keypad to power the LM on.	The LCD is scrolling Local Manager information and device status
Restart	The LCD is scrolling Local Manager information and device status	Press the center button on the keypad. Press the down arrow button to navigate to the Restart menu item. Press the center button to select Restart.	The LCD is scrolling Local Manager information and device status
Power off	The LCD is scrolling Local Manager information and device status	Press the center button on the keypad. Press the down arrow button to navigate to the Shutdown menu item. Press the center button to select Shutdown.	The keypad is dimly lit and the LCD is dark/off.

Uplogix 3200 Power and Restart Operations

To do this:	Check to be sure that:	Take this action:	The process is complete when:
Power on	All lights are off	Plug in the power supplies	The LCD is scrolling Local Manager information and device status
Restart	The LCD is scrolling Local Manager information and device status	Press the center button on the keypad. Press the down arrow button to navigate to the Restart menu item. Press the center button to select Restart.	The LCD is scrolling Local Manager information and device status
Power off	The LCD is scrolling Local Manager information and device status	Press the center button on the keypad. Press the down arrow button to navigate to the Shutdown menu item. Press the center button to select Shutdown.	The LCD and keypad are no longer lit.

Uplogix 430 Power and Restart Operations

To do this:	Check to be sure that:	Take this action:	The process is complete when:
Power on	All lights are off	Plug in the power supply	The system health light is on and not blinking
	The system health light is off and the power supply light is on	Disconnect the power supply, then plug it in again	
Restart	The system health light is on and not blinking	Press and hold the reset/power off switch for 1 to 2 seconds	The system health light is on and not blinking
Power off	The system health light is on and not blinking	Press and hold the reset/power off switch until the system health light begins blinking slowly	The system health light is off

Working with the command line

The Local Manager uses a command line interface (CLI). Where commands differ among models, the differences are noted.

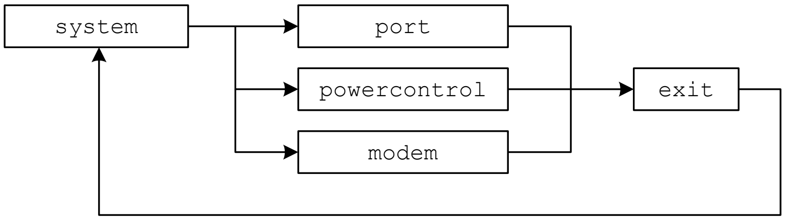
The command line is accessible from the onboard console port or via the network using SSH. Terminal access (TTY) is available via dial-in modem and Telnet, but both are disabled by default for security reasons.

This section covers the following topics:

- Structure of the command line
- Opening and closing a CLI session
- Command types
- Command shortcuts
- Redirecting command output to a file
- Viewing context-sensitive help
- Viewing the command history

Structure of the CLI

The command line employs a hierarchy for organizing the Local Manager, ports, power controllers, and modems. These are called resources. The system resource is the root resource.



To return to the system resource from another resource, use the `exit` command.

Resource	Description	Command
`system`	The root resource. All Local Manager configuration and user management functions are accessed from this resource.	`exit` (return from another resource)
`port`	Use to configure and manage a device connected to a device port on the Local Manager.	`port <slot/number>` (from any resource)
`powercontrol`	Use to configure and manage an external power controller and map its outlets to devices managed by the Local Manager.	`powercontrol` (from the system resource)
`modem`	Use to configure embedded and external modems and related settings.	`modem` (from the system resource)

Opening and closing a CLI session

Before beginning, the Local Manager must be installed and the initial configuration must be complete. Refer to the *Installation Guide for Local Managers* for information on completing these tasks.

Supported terminal clients

To use the command line from a workstation connected to the management console port, open a terminal session using one of the supported terminal clients:

- Windows HyperTerminal
- ZTerm (Macintosh OS X)
- Minicom (Unix/Linux)
- PuTTy

The default console connection settings are 9600 baud, 8 data bits, 1 stop bit, no parity, and no flow control. For best results, set the terminal emulator to use ANSI encoding.

> By default, Windows HyperTerminal uses hardware flow control. The Uplogix 430 Local Manager does not use flow control. If using HyperTerminal with the Uplogix 430 Local Manager, flow control must be disabled when configuring the session.

Supported SSH clients

Local Manager uses Secure Shell (SSH) v2 software to provide secured remote access. The remote client application must also support SSH v2.

To use the command line from a console workstation via SSH, open a Secure Shell connection using one of the supported Secure Shell clients:

- Control Center CLI Applet
- PuTTY
- SSH® Tectia™
- VanDyke® SecureCRT®
- SSHTerm for Windows
- iTerm for Macintosh OS X
- UNIX’s built-in ssh command

For example, in a UNIX command line, type **`ssh admin@198.51.100.254`**

Substitute the IP address of the Local Manager.

Logging in

After connecting to the Local Manager, you are prompted for a username and password. The default username is `admin` and the default password is `password`.

> Usernames and passwords are case-sensitive.

Closing the session

To exit the command line, use the **`logout`** command.

Command types

Many commands are executed without dialog. Some, such as `ping`, require command arguments; others, like `logout` and `shutdown`, do not take command arguments.

Interactive commands prompt for new information and may display current settings. For example:

```
[admin@UplogixLM]# config date
Displayed time is 12/30/2014 10:33:16 CST
System time is    12/30/2014 16:33:16 UTC
Change these? (y/n) [n]: y
Current system time (MM/dd/yyyy HH:mm:ss):12/30/2014 16:36:00
Displayed time is 12/30/2014 10:36:02 CST

System time is    12/30/2014 16:36:02 UTC
```

In this example, the current date and time is displayed (both UTC and local time zone). A prompt asks whether you wish to change the settings. If you answer **y**, the Local Manager prompts for the new date and time. After entering this information, the Local Manager displays the new date and time and returns to the system prompt.

Some interactive commands present default or current settings, which can be accepted by pressing the Enter key.

Some commands open **editors** in which you can issue subcommands in any order. To save changes and return to the main command line from an editor, use the `exit` command.

Command shortcuts

The command line provides several ways to reduce the amount of typing required in the command line.

Repeating commands

Repeat the most recent command—and go back to earlier commands in reverse sequence—by pressing the up arrow key and then the Enter key.

Abbreviating commands

As with many command line interfaces, the Uplogix command line allows you to abbreviate commands to the shortest string that uniquely identifies the command.

For example, shorten the `ping` command to `pi`. Similarly, shorten `show dashboard` to `sh das`.

An error results if the `ping` command is shortened to `p`. This is because `p` matches all other commands beginning with the letter `p`. Similarly, an error results if `show dashboard` is shortened to `sh da` because this string matches `show date`.

The exception is `shutdown`. To minimize the potential for accidental shutdown, this command is not accepted if it is abbreviated.

Using wild card characters

The command line allows the `*` character as a wildcard. For example, issue the command `show rule cpu*` to view all rules that have names starting with `cpu`.

Paging through command feedback

Some commands return large amounts of information. When reviewing long displays of command feedback, type `<` to return to the beginning of the display or `>` to go to the end.

Canceling out of interactive commands

Use the `<Ctrl>+c` command to exit interactive commands without saving changes.

Redirecting command output to a file

Some show commands return more information than is practical to view in the command line window. For example, the show role command may produce several screens of output and the show buffer command will typically produce several hundred screens. In these cases it may be preferable to copy the output to a file that can be examined later.

Use the pipe character | to redirect the output of a command via FTP or SCP. The syntax is:

```
<command> | <ftp | scp | mailto username@host:path/to/file
```

For example, to use SCP to redirect the output of the show config command to another computer:

```
show config | scp username@host:path/to/file
```

where username@host:path/to/file specifies the destination for the data.

Need help using the pipe redirect? Enter | ? in the command line.

Redirecting command output to Email

Some show commands return more information than is practical to view in the command line window. For example, the show role command may produce several screens of output and the show buffer command will typically produce several hundred screens. In these cases it may be preferable to copy the output to an email that can be examined later. This functionality requires the Local Manager Email server settings to be properly configured (config system email command).

Use the pipe character | to redirect the output of a command as a file attachment in an email to the specified email address. The syntax is:

```
<command> | mailto username@host:<filename>
```

For example, to use SCP to redirect the output of the show config command to another computer:

```
show config | scp username@host:path/to/file
```

where username@host:path/to/file specifies the destination for the data.

Need help using the pipe redirect? Enter | ? in the command line.

For example, to send the contents of a port buffer to the support@uplogix.com email address as a file named “buffer.log”, use the following syntax:

```
[admin@UplogixLM] (port1/1)# show buffer | mailto support@uplogix.com:buffer.log
```

Parsing Output

Using the pipe character, you can redirect the output of a command to grep for parsing. The syntax is:

```
<command> | grep “keywords”
```

For example, you can parse the output of show user * to pull out email addresses:

```
[admin@UplogixLM]# show user * | grep email
email support@uplogix.com
email tjones@uplogix.com
```

Viewing context-sensitive help

To show command usage notes, type the command and then ?.

```
[admin@UplogixLM]# port ?
usage: port <slot number>/<port number>
[admin@UplogixLM]# config export ?
usage: export <method> <target>
              methods: ftp, scp, usb

Export via FTP
ex. config export ftp <userId@host:fileName>
Export via SCP
ex. config export scp <userId@host:fileName>
Export via USB
ex. config export usb <fileName>
```

To view a list of available commands from any resource within the command line, type ?. The commands listed will be limited to the allowed actions for your role in the current resource.

For example, if you navigate to the modem resource and type ? on a line by itself, the Local Manager returns the following help text:

```
[admin@UplogixLM (modem)]# ?
Uplogix LMS v5.1 26966

config                   Edit settings
copy                     Copy file to another port or from an external location
exit                     Exit modem menu
history                  Display command history
logout                   Logout
modem                    Commands specific to modem
outband                  Interact with outband
port                     Commands specific to port
power                    Control power of external modem on console
powercontrol             Commands specific to powercontrol
ppp                      Interact with PPP
show                     Display settings and status
suspend                  Suspend automated or recovery processes
terminal                 Terminal access
```

Usage notes allow you to drill down into a command:

```
[admin@UplogixLM (modem)]# show ?
Uplogix LMS v5.1.0.26966

alarms                   Display alarms for this device
all                      Display all device configuration data
answer                   Show dialing options
buffer                   Display buffer of device output
dashboard                Brief display of the system and its managed devices
directory                Display files for this device
events                   Shows events
info                     Display device information
```

```
labels                   Display device labels
log                      Display logs
monitors                 Display list of current monitors
ppp                      Display PPP configuration
properties               Display properties for device
protocols                Display protocol settings
schedules                Display currently scheduled processes
serial                   Display serial configuration for device
settings                 Display settings
status                   Display ppp and pptp status
vpn                      Display VPN configuration

[admin@UplogixLM (modem)]# show alarms ?
usage: alarms [options]

--- options ---

  -all        Current and cleared alarms
  -cleared    Cleared alarms
  -n <count>  Maximum number of alarms
  -v          Use multiple lines
```

Viewing the command history

The `history` command displays up to the last 20 commands (if available) from the current resource.

```
[admin@UplogixLM]# history
modem
config init
show ?
show alarms
history
```

To execute a listed command, enter `!` followed by the command number.

```
[admin@UplogixLM]# !5
show alarms
There are no alarms right now.
```

Configuring the Local Manager

Before beginning the tasks in this section, ensure that the procedures in the *Installation Guide for Uplogix Local Managers* have been completed.

Most of the configuration settings in this chapter are available through the `config system` commands. To view configurable settings, enter `config system ?`. For more detailed information about the commands in this chapter, refer to the *Command Reference Guide for Uplogix Local Managers*.

This chapter covers:

- Configuring communication settings — management IP and serial settings, out-of-band behavior, management by Control Center element management system
- Exporting Local Manager configuration — for environments in which no Control Center is used
- Configuring CLI behavior — banners, CLI window scrolling, session idle timeout
- Configuring reporting information — originating address for emailed alerts, date and time, environmental thresholds, properties, SNMP settings

Configuring communication settings

This section covers the following topics:

- Configuring IP settings
- Configuring the management console port
- Configuring the Local Manager to be managed by a Control Center
- Configuring archiving

Configuring IP settings

The Local Manager is initially configured to use DHCP. Change this and any related settings for the management Ethernet interface using the interactive `config system ip` command. On some models of the Local Manager, this can be performed from the front panel keypad.

```
[admin@A405100070]# config system ip
--- Existing Values ---
Use DHCP: Yes
Management IP: 192.0.2.102
Host Name: UplogixLM
Subnet Mask: 255.255.255.0
Broadcast Address: 192.0.2.255
Default Route: 192.0.2.254
Speed/duplex: auto:100full
MAC Address: 00:0F:2C:00:CA:98
DNS Server 1:
DNS Server 2:
```

```
Bonding Link: yes
Primary Ethernet Link: yes (primary)
Auxiliary Ethernet Link: yes (outband)
Change these? (y/n) [n]: n
```

If the Local Manager has a DNS server configured, it uses domain name resolution for the commands that support it. Most functions do not use DNS.

Configuring the management console port

The default management console connection settings for the Local Manager are 9600 baud, 8 data bits, 1 stop bit, no parity, and no flow control.

By default, Windows HyperTerminal uses hardware flow control. The Uplogix 430 Local Manager does not use flow control. If using HyperTerminal with the Uplogix 430 Local Manager, flow control must be disabled when configuring the session.

The mini-USB console ports on the 500/5000 platforms are enabled in this software release for the Windows operating system (Windows 7).

The console ports for the Local Managers accept standard RS-232 serial cables with RJ-45 connectors configured as DCE unless otherwise labeled or configured. The Uplogix 400 and 3200 can be configured to use null modem cables by rolling the TX/RX connections in hardware.

The Uplogix 430 Local Manager is shipped with its own console cable.

To use a null modem cable with an Uplogix 400 or 3200, use the interactive `config system serial` command and enable the null modem setting, if it was not enabled during initial configuration when the Local Manager was installed.

```
[admin@A200101303]# config system serial
--- Existing Values ---
Null modem: no
Change these? (y/n) [n]: y
Enable null modem? (y/n) [n]: y
Do you want to commit these changes? (y/n): y
```

If the Local Manager is managed by a Control Center, null modem can be configured through the Uplogix web interface.

For a single Local Manager: `Inventory > Local Manager page > Configuration menu > Serial`

For a group of Local Managers: `Inventory > group page > Configuration menu > Serial`

Configuring the Local Manager to be managed by a Control Center

Local Managers can be managed by a Control Center, a centralized web-based interface element manager for managing multiple Local Managers. Once integrated, the Control Center becomes the vehicle for scheduling tasks across the enterprise, archiving data, events and device information, and integrating with other enterprise network management systems.

The Local Manager communicates with a Control Center server via an SSL-encrypted proprietary protocol – the messages initiated by the Local Manager to the UCC are called heartbeats. The heartbeat interval is configurable with the default being 30 seconds.

To configure the Local Manager to communicate with a Control Center, use the interactive `config system management` command.

```
[admin@UplogixLM]# config system management
--- Existing Values ---
Use Management Server: false
Hostname or IP: 127.0.0.1
Port: 8443
Heartbeat interval (seconds): 30
Heartbeat band: all
Always use minimal heartbeat: false
Last successful heartbeat:  (not yet contacted)
Change these? (y/n) [n]: y
--- Enter New Values ---
Use Management Server (y/n) [n]: y
Hostname or IP [127.0.0.1]: 203.0.113.100
Port [8443]:
Heartbeat interval (seconds) [30]:
Heartbeat during [all]:
Do you want to commit these changes? (y/n): y
```

The default port and heartbeat interval can be changed with this command. When the heartbeat occurs can also be specified: during all operations, only during in-band operation, or only during out-of-band operation

To enable server hostname resolution, use the interactive `config system ip` command and set a DNS IP address. Refer to Configuring IP settings for more information.

After the Local Manager contacts the server, you can modify archiving to alter the defaults.

> When the Local Manager is managed by a Control Center, changes made via the command line will show up on the Uplogix web interface after the next heartbeat. Similarly, changes made to the Local Manager using the Control Center web interface will be available on the Local Manager after the next heartbeat.

Configuring archiving

If the Local Manager is managed by a Control Center, it uploads device statistics, user sessions, device files, and other data to the Control Center at regular intervals. Archiving uses high data compression to reduce network impact. Archiving is suspended by default when the Local Manager is operating out-of-band, but the Local Manager can be configured to archive data when out-of-band.

Archiving occurs over port 8443, and is configured automatically when configuring the Local Manager for use with a Control Center. To see the current archive settings for the Local Manager, use the `show system archive` command.

Archive settings can be edited using the `config system archive` command.

```
[admin@UplogixLM]# config system archive
--- Existing  Values ---
Time Between Archivals (seconds): 3,600
Maximum Archives Stored Locally: 100
Enable While Out of Band: false
Change these? (y/n) [n]:
```

If the Local Manager is not managed by a Control Center, you can export configuration data manually.

Archiving can be configured through the Uplogix web interface.

For a single Local Manager: `Inventory > expanded Local Manager page > Configuration menu > Archive`

For a group of Local Managers: `Inventory > group page > Local Manager Configuration menu > Archive`

Exporting Local Manager Configuration

Use this feature to back up Local Manager configuration data to an external source.

The `config export` command uses FTP, SCP or USB to export the Local Manager configuration as an XML file to a specified location. The XML file can be loaded back onto the Local Manager using the `config import` command. Use the `show config` command to view the data that will be exported.

An XML file should only be loaded onto a Local Manager running the same software version or a higher software version as the Local Manager from which the file was exported.

Configuring CLI behavior

This section covers the following topics:

- Setting and clearing banners
- Setting CLI page length
- Setting session timeout

Setting and clearing banners

The Local Manager can display two banners:

- Welcome banner — displayed prior to login
- Login banner — displayed after successful authentication

By default, no banners are defined.

Setting banners

Define banners to display any required legal information or operational notes with the `config system banner` editor command. The `login` parameter allows you to edit the banner that is displayed before login. The `welcome` parameter allows you to edit the banner that is displayed after login. Enter the desired text; more than one line may be used. When finished, use the `exit` command to leave the editor and return to the main CLI.

```
[admin@UplogixLM]# config system banner welcome
Type 'exit' on a line by itself to exit
[config system banner welcome]# You are now logged in to UplogixLM.
[config system banner welcome]# exit
```

Do not use non-printing characters in banners. Spaces are considered printing characters.

Some SSH clients do not support the login banner.

Verify the current banners with the `show system banner` command:

```
[admin@UplogixLM]# show system banner
Welcome Banner:
You are now logged in to UplogixLM.
Login Banner:
No login banner set.
```

In this example, there is no login banner set.

Clearing banners

To clear a banner, use the `config system banner` command with either the `login` or the `welcome` parameter. Type `exit` without entering any other text.

Use the `show system banner` command to verify that you have cleared the banner.

```
[admin@UplogixLM]# config system banner welcome
Type 'exit' on a line by itself to exit
[config system banner welcome]# exit

[admin@UplogixLM]# show system banner
Welcome Banner:
No welcome banner set.

Login Banner:
No login banner set.
```

If the Local Manager is managed by a Control Center, banners can be configured through the Uplogix web interface.

For a single Local Manager: `Inventory > Local Manager page > Configuration menu > Banners`

For a group of Local Managers: `Inventory > group page > Local Manager Configuration menu > Banners`

Setting CLI page length

By default, the Local Manager automatically tries to determine the appropriate number of lines to display in the CLI window before providing a scroll prompt. If the appropriate page length cannot be determined, the CLI displays 24 lines before presenting a scroll prompt.

To change the number of lines displayed, use the `config system page-length` command:

```
[admin@UplogixLM]# config system page-length
Page length preference is auto.
Change this? (y/n) [n]: y
Page length preference (2 or more lines or auto):50
```

In this example, the command line will display 50 lines before prompting you to press a key to scroll the display.

Setting session timeout

Local Managers disconnect users after a specified number of minutes of inactivity. The default timeout is five minutes. Use the `config system timeout` command to change this interval.

```
[admin@UplogixLM]# config system timeout
Current session timeout is 5 minutes.
Change these? (y/n) [n]: y
Timeout (5 to 120 minutes): [5]: 10
```

This example changes the inactivity timeout to 10 minutes.

If the Local Manager is managed by a Control Center, timeout can be configured through the Uplogix web interface.

For a single Local Manager: `Inventory > Local Manager page > Configuration menu > Timeout`

For a group of Local Managers: `Inventory > group page > Configuration menu > Timeout`

Configuring reporting information

This section covers the following topics:

- Setting originating email address and SMTP server for alerts
- Setting date and time
- Setting environmental thresholds
- Configuring properties
- Configuring syslog forwarding
- Configuring SNMP settings

Setting originating email address and SMTP server for alerts

Local Managers can be configured to notify administrators of certain situations by email.

The Local Manager’s mail system supports separate email servers for use in and out-of-band. IP addresses are used in place of hostnames to minimize dependence on DNS servers. SSL connections and SMTP authentication are both supported.

Configure email settings with the interactive `config system email` command:

```
[admin@UplogixLM]# config system email
--- Existing Values ---
In band SMTP Server: 127.0.0.1
In band from address: system@127.0.0.1
In band SMTP Port: 25
Use user authentication in band: no
Prefer SSL for in band email: no
Out of band SMTP Server: 127.0.0.1
Out of band from address: system@127.0.0.1
Out of band SMTP Port: 25
Use user authentication out of band: no
Prefer SSL for out of band email: no
Change these? (y/n) [n]:y

[admin@UplogixLM]# config system email
--- Existing Values ---
In band hostname or IP [127.0.0.1]: 198.51.100.250
In band from address [system@127.0.0.1]: UplogixLM@uplogix.com
In band SMTP Port [25]: 587
Use user authentication for in band email? (y/n) [n]: y
In band username: UplogixLM
In band password: ********
Confirm password: ********
Prefer SSL for in band email? (y/n) [n]:
Out of band hostname or IP [203.0.113.4]:
Out of band from address [system@127.0.0.1]:
Out of band SMTP Port [25]:
Use user authentication for out of band email? (y/n) [n]:
Prefer SSL for out of band email? (y/n) [n]:
Do you want to commit these changes? (y/n):y
```

If the Local Manager is managed by a Control Center, the originating email address can be configured through the Uplogix web interface.

For a single Local Manager: `Inventory > Local Manager page > Configuration menu > Email`

For a group of Local Managers: `Inventory > group page > Configuration menu > Email`

For information about setting up monitoring and defining the behavior for alerts, refer to the *Guide to Rules and Monitors*.

Setting date and time

In most cases, you will not need to set the date and time. To ensure accurate reporting and to coordinate activities across multiple time zones, Local Managers use Coordinated Universal Time (UTC) with the time set at the factory.

If the Local Manager is configured to work with a Control Center, by default it uses the date and time from the Control Center's NTP (Network Time Protocol) server. If NTP is not approved or unavailable, the Local Manager can use the time configuration from the Control Center in the heartbeat. The time provided using this option may be less accurate than time provided by an NTP server.

The date and time settings can be adjusted manually or the Local Manager can be configured to use a separate NTP server.

Setting date and time manually

To set the date and time manually, use the interactive `config date` command. Convert your local time to UTC before changing the time on the Local Manager.

```
[admin@UplogixLM]# config date
Displayed time is 08/13/2012 14:56:49 UTC
System time is 08/13/2013 14:56:49 UTC
Change these? (y/n) [n]:
```

Setting the Local Manager to use an NTP server

To override time and date settings from the Control Center by using NTP, use the interactive `config system ntp` command to set the NTP server's IP address and optionally add a secondary server in case the primary server fails.

```
[admin@UplogixLM]# config system ntp
--- Existing Values ---
Use NTP: no
Change these? (y/n) [n]: y
--- Enter New Values ---
Use NTP:  (y/n) [n]: y
NTP Primary Server Hostname or IP [127.0.0.1]: 203.0.113.253
NTP Secondary Server Hostname or IP: 192.0.2.253
Do you want to commit these changes? (y/n): y
```

To confirm NTP settings, use the `show system ntp` command.

If the Local Manager is managed by a Control Center, it can be configured to use an NTP server through the Uplogix web interface.

For a single Local Manager: `Inventory > Local Manager page > Configuration menu > NTP`

For a group of Local Managers: `Inventory > group page > Configuration menu > NTP`

Setting environmental thresholds

All models of the Local Manager, except the 430, can measure temperature and humidity, providing constant and reliable environmental monitoring. The 500, 3200 and the 5000 require an optional temperature and humidity probe.

The default temperature limit for Local Managers with sensing capability is 95° F (35° C), and the default humidity limit is 85%. If the temperature or humidity exceeds the defined threshold, an alarm is triggered. Alarms are not triggered if the relevant data is unavailable—for example, if no sensor is installed.

In addition to temperature and humidity, the environment settings allow you to specify which hardware resources are connected so that the Local Manager can report a failure/alarm when one exists. This includes indicators for all Ethernet interfaces and an indicator to alarm on power supply failure (for example, when both power supplies are connected on the Uplogix 5000).

All of these settings can be changed using the `config environment` command as shown below.

```
[admin@UplogixLM]# config environment
--- Existing  Values ---
Humidity Threshold: 85.0
Temperature Threshold: 95.0
Use Celsius: false
Alarm on power supply failure: false
Alarm on primary Ethernet link failure: false
Alarm on secondary Ethernet link failure: false
Alarm on tertiary Ethernet link failure: false
```

```
Change these? (y/n) [n]: y
--- Enter New Values ---
Humidity Threshold [85.0]:
Temperature Threshold [95.0]: 40
Use Celsius (y/n) [n]: y
Alarm on power supply failure (y/n) [n]: y
Alarm on primary Ethernet link failure (y/n) [n]: y
Alarm on secondary Ethernet link failure (y/n) [n]:
Alarm on tertiary Ethernet link failure (y/n) [n]:
Do you want to commit these changes? (y/n): y
```

Configuring properties

The `config system properties` editor command allows you to set arbitrary pairs of data for use in reports generated by the Control Center. For example:

```
[admin@UplogixLM]# config system properties
[config system properties]# installDate 07/10/13
[config system properties]# rack 7
[config system properties]# exit
```

This would allow you to generate a report showing the rack number and install date of each Local Manager.

When you configure SNMP settings, use this command to set the values for `sysContact.0` and `sysLocation.0`.

If the Local Manager is managed by a Control Center, properties can be configured through the Uplogix web interface.

`Inventory > Local Manager page > Properties`

Configuring syslog forwarding

The interactive command `config system syslog` allows you to configure the Local Manager to send its alarms and events to a syslog server. Specify the server IP address and port number, and select the syslog facility to write to (e.g., local1, local2, etc.).

```
[admin@UplogixLM]# config system syslog
--- Existing Values ---
Syslog enabled: no
Syslog server IP:
Syslog port number: 514
Syslog facility: local1
Change these? (y/n) [n]:
```

If the Local Manager is managed by a Control Center, syslog settings can be configured through the Uplogix web interface.

For a single Local Manager: `Inventory > Local Manager page > Configuration menu > Syslog`

For a group of Local Managers: `Inventory > group page > Configuration menu > Syslog`

Configuring SNMP settings

Local Managers can respond to SNMP Version 3 queries from a network management system. SNMP Version 1 and 2 as well as SNMP “Walks” are not supported.

By default, SNMP is disabled. Enable SNMP on the Local Manager with the `config system snmp` command:

```
[admin@UplogixLM]# config system snmp
--- Existing Values ---
SNMP is disabled.
Change these? (y/n) [n]: y
--- Enter New Values ---
Security Level (authPriv,authNoPriv,noAuthNoPriv,disabled): [authPriv]: authPriv
Port: [161]:
Username: snmpuser
Auth Protocol: [SHA]:
Auth Password [*********]: ********
Confirm Auth Password: ********
Priv Protocol: [AES256]:
Priv Password [*********]: ********
Confirm Priv Password: ********
Do you want to commit these changes? (y/n): y
```

Security level

Set the security level to `disabled` to completely turn off SNMP.

The `noAuthNoPriv` level requires that the user connects with the SNMP username, but no message validation or encryption is performed.

The `authNoPriv` level requires that the user connect with the SNMP username and makes sure that the message is valid by using the specified auth password.

The `authPriv` level requires that the user connect with the SNMP username, requires that it has been signed with the Auth password, and that it has been encrypted with the Priv password.

Uplogix recommends that you protect the Local Manager with the `authPriv` security level.

Security level designations are case-sensitive.

Port

You can change the SNMP port from the default of 161.

Username and passwords

Set a username and the passwords that will be required to execute SNMP requests.

Auth and Priv protocols

For `Auth Protocol`, enter `SHA` or `MD5`.

For `Priv Protocol`, enter `AES256, AES192, AES128`, or `DES`.

Further setup

You can change the values for `sysContact.0` and `sysLocation.0` by running `config system properties` and setting appropriate values:

```
[admin@UplogixLM]# config system properties
[config properties]# sysLocation.0 Austin, TX
[config properties]# sysContact.0 S.Jones
[config properties]# exit
```

If the Local Manager is managed by a Control Center, SNMP settings can be configured through the Uplogix web interface.

For a single Local Manager: `Inventory > Local Manager page > Configuration menu > SNMP`

For a group of Local Managers: `Inventory > group page > Configuration menu > SNMP`

Configuring Out-of-Band Communication

The Local Manager uses the Pulse feature to test in-band network connectivity by sending 15 bytes of data on TCP port 7 (echo) every 30 seconds to up to three echo servers. You can configure the Local Manager to respond to a loss of connectivity — defined as no response for four consecutive pulses — by initiating an out-of-band connection over a modem or the secondary Ethernet management port through an alternate network such as the internet back into your network. The following sections detail how to configure PPP and optional VPN (IPSec and PPTP) settings when necessary.

During out-of-band operation, the Local Manager continues sending echo requests to the Pulse server through the in-band connection. When it receives five consecutive echoes, the out-of-band connection is dropped and normal operation resumes. If users are logged in to the Local Manager over the out-of-band connection via SSH, the out-of-band session will persist until all SSH sessions are closed.

Because of the limited bandwidth of dial-up connections, bandwidth-intensive operations such as archive and export are suspended by default until in-band connectivity is restored. Archive and export functions can however be configured to operate over the out-of-band connection. Complete archives will be cached and will resume once the in-band network has been restored. SLV tests are also suspended by default during out-of-band operation.

The Local Manager can be configured to use separate mail servers for in-band and out-of-band operation. This allows it to bypass the internal network to send alerts and notifications to subscribed users' out-of-band email addresses.

This chapter covers:

- Configuring Pulse settings
- Configuring the modem
- Configuring PPP
- Configuring VPN settings
- Configuring remote locations to be contacted by the Control Center
- PPP Cycle
- Secondary Ethernet

Configuring Pulse settings

To determine when to initiate an out-of-band connection, the Local Manager sends a TCP echo packet to a Pulse server every 30 seconds. The echo packets are 15 bytes to limit impact on the network. If the Pulse server does not receive echo packets for four consecutive attempts, the Local Manager can be configured to automatically initiate an out-of-band connection or enable the modem for dial-in access. The echo is expected to return the exact data sent.

> To optionally use the modem's TTY dial-in access feature for out-of-band connectivity, it can be configured to answer only on Pulse failure using the `config answer` command. Refer to Configuring the modem for more information.

To configure the Pulse process, select up to three hosts in your network to be Pulse servers. The hosts should be a reliable indicator of good network connectivity. A Control Center can be used as a Pulse server; however, it should be given a secondary IP address for that purpose to provide heartbeat communications over the out-of-band network when the network is down. If the Local Manager cannot communicate with the server, it cannot deliver network data or receive configuration updates. Other common devices that can be used as pulse servers are Cisco routers using the TCP-small-servers service or Windows or Unix systems configured with the echo process enabled.

By default, the Local Manager uses TCP port 7 for the Pulse process and is configurable. Up to three pulse servers can be configured, enabling pulse server redundancy.

Use the `config system pulse` command to enter the settings.

```
[admin@UplogixLM]# config system pulse
--- Existing Values ---
Use Pulse: false
Pulse Server IP 1: 127.0.0.1
Pulse Server Port: 7
Enable Outband on Pulse Failure: no
Change these? (y/n) [n]: y
--- Enter New Values ---
Use Pulse (y/n) [n]: y
Pulse IP 1: [127.0.0.1]: 203.0.113.225
Pulse Port 1: [7]:
Pulse IP 2: [127.0.0.1]: 203.0.113.226
Pulse Port 2: [7]:
Pulse IP 3: [127.0.0.1]: 198.51.100.225
Pulse Port 3: [7]:
Enable Outband on Pulse Failure (y/n) [n]: y
Do you want to commit these changes? (y/n): y
```

If you do NOT want the Local Manager to automatically initiate an out-of-band connection on pulse failure, be sure to answer **`n`** to the `Enable Outband on Pulse Failure (y/n)` question.

The Pulse server's echo application should comply with RFC 862 such as those provided with Microsoft Windows 2000 Server or Red Hat Linux 7.3.

If the Local Manager is managed by a Control Center, Pulse can be configured through the Uplogix web interface.

For a single Local Manager: `Inventory > expanded Local Manager page > Configuration menu > Pulse`

For a group of Local Managers: `Inventory > group page > Configuration menu > Pulse`

Configuring the modem

By default, the modem ignores incoming calls. This capability must be enabled in order to use it.

The Local Manager can be configured to accept dial-in calls during out-of-band operation (dial-in requires a modem with circuit switched service, such as a V.92 modem or an Iridium modem). This presents an ANSI terminal interface similar to the onboard console port, providing only TTY access to the command line. Advanced features such as file transfer are unavailable, as this is not an IP connection.

The Local Manager is available with an internal modem. An external modem may be used but must be initialized.

Enabling dial-in and setting answering behavior

To prevent unauthorized access, the modem's default behavior is to ignore incoming calls. When the modem is enabled to accept incoming communication, default security settings are applied. These include a phone number filter. By default, the filter includes no phone numbers, so all calls are refused until the modem is configured to allow calls from some or all phone numbers.

Use the `config answer` editor command to enable the modem and configure additional settings:

- `show` — Display the current answering behaviors.
- `enable` — Enable the dial-in feature.

> If the `pulse` subcommand is used to enable the modem to answer on Pulse failure, the modem will do so regardless of whether the `enable` subcommand is applied.

- `disable` — Disable the dial-in feature.
- `init "" ATZ <modem init string>` — Set a modem init string.

> Ensure the double quotes are in the `init` string. One of the most common causes of modem issues is the omission of these quotes.

- `[no] allow <phone number>` — Specify a phone number or a range of phone numbers allowed to call in to the modem. For example, in the USA, `allow 512` will permit access from any number in the 512 area code. To specify the range of numbers assigned to your organization, use `allow 5128577`.
- `[no] deny <phone number>` — Specify a phone number or range of phone numbers that will be refused.
- `[no] number <phone number>` and `[no] domain <SMS domain name>` — To allow a Control Center to establish contact with the Local Manager in a remote location via Iridium modem, set `number` as the Local Manager's phone number and `domain` as the service provider's SMS domain name. The Control Center uses these parameters to construct a valid SMS email address, to which it can send the `ppp on` message to establish contact. This capability is available for Iridium modems.
- `[no] rings <number>` — Specify the number of rings before the modem answers. The default value is 3.
- `[no] ringback` — When ringback is enabled, the Local Manager ignores an incoming call until it hangs up. If the user calls back within a specified amount of time, the Local Manager answers the call.
- `[no] pulse` — Specify whether the modem answers after a Pulse failure initiates out-of-band operation, applying all other defined restrictions. Setting `pulse` overrides the `enable` and `disable` subcommands.
- `[no] suspend` — Disable SLV tests when PPP is enabled. This is the default behavior.

If the Local Manager is managed by a Control Center, the modem can be configured through the Uplogix web interface.

For a single Local Manager: `Inventory > Local Manager page > Configuration menu > Modem`

For a group of Local Managers: `Inventory > group page > Configuration menu > Modem`

Modem troubleshooting

Issue the `pull tech` command followed by the `show tech` command to display information about the modem that can be helpful when troubleshooting modem problems. Here is an example of the information collected from an internal GPRS cellular modem:

```
[admin@A400100063 (modem)]# pull tech
Checking IMEI / Modem Serial Number
Checking Modem Firmware Version
Checking Modem Functionality Mode
Checking Network Registration State
Checking Signal Strength
Checking ICCID / SIM Card Number
Checking Network Operator Name
Checking International Mobile Subscriber Identity
Checking Mobile Directory Number
Checking PDP Context
Pull tech completed and saved as current.

[admin@A400100063 (modem)]# show tech
IMEI / Modem Serial Number (AT+CGSN):
    011998000336851

Modem Firmware Version (AT+CGMR):
    R7.45.1.201105250600.WMP50 2203572 052511 06:00

Modem Functionality Mode (AT+CFUN?):
    Mobile full functions with power saving disabled. (1)

Network Registration State (AT+CREG?):
    Registered, home network. (0,1)

Signal Strength (AT+CSQ):
    (-67) dBm.

ICCID / SIM Card Number (AT+CCID):
    "89014104212409549491"

Network Operator Name (AT+CPHS=2,5):
    AT&T

Mobile Country Code (AT+CIMI):
    310

Mobile Network Code (AT+CIMI):
    410

Mobile Subscriber Identification Number (AT+CIMI):
    240954949

Mobile Directory Number (AT+CNUM):
    15128675309

PDP Context (AT+CGDCONT?):
    1,"IP","ccspbdd000.acfes.org",,0,0
```

Optional: Specifying an external modem

To configure an external modem, navigate to the modem resource and use the `config init` command. When configuring the modem resource, the make you enter will depend on the type of external modem being managed. The GenericModem make can be used with an external V.92 modem. The Local Manager will automatically recognize a USB-connected MultiTech iCell modem – for this case, the MultiTech option will be available during configuration and should be used. If you connect a MultiTech iCell modem to the Local Manager using a DB-9 serial connection, select the cellular make. The example below demonstrates how to configure the modem resource when it is connected to an external Iridium modem.

```
[admin@UplogixLM]# modem
 embedded

[admin@UplogixLM (modem)]# config init
This device has already been initialized.
Would you like to reinitialize it? (y/n): y
--- Enter New Values ---
description: []: Iridium 9522B
make: [embedded]: Iridium
serial bit rate [38400]: 19200
serial data bit [8]:
serial parity [none]:
serial stop bit [1]:
serial flow control [none]:
Do you want to commit these changes? (y/n):y
Testing login will take a few moments...
Login successful; credentials are valid.
```

To change the configuration of a modem that has already been configured, use the `config info` and `config serial` commands.

```
[admin@UplogixLM (modem)]# config info
Hostname:
Description: Iridium 9522B
Make: Iridium
Model:
OS:
OS Version:
Management IP:
Change these? (y/n) [n]: y


[admin@UplogixLM (modem)]# config serial
Serial Bit Rate: 19,200
Serial Data Bit: 8
Serial Parity: none
Serial Stop Bit: 1
Serial Flow Control: none
DSR: false
CTS: false
RX : 0
TX : 0
Frame Errors: 0
Overrun Errors: 0
Parity Errors: 0
Breaks: 0
Change these? (y/n) [n]: y
```

Optional: Specifying a virtual modem

The Local Manager can be configured to connect to an external modem over Ethernet – this is achieved by configuring a virtual modem (supported on the 500 and 5000 platforms only). A virtual modem will override an embedded modem when configured. Use the `config system slot modem` command to configure a virtual modem. A virtual modem is a virtual port that connects to a modem – see the virtual port section for more details on virtual port configuration.

```
[admin@UplogixLM]# config sys slot modem
[config system slot modem]# port 1 203.0.113.6 7002 ssh
Port 1 added.
Username: admin
The authenticity of host ‘203.0.113.6’  cannot be established.
Fingerprint: ef:74:9a:3f:27:ed:ec:82:c3:d2:13:19:58:e6:55:7b
    SHA-256: 3b3f.2899.5deb.f5a9.587a.e192.d5e0.f9e8
             5256.e013.fd84.69d2.2fc9.e71a.7a11.6642

Are you sure you want to continue connecting (y/n): y
Auth failed for user admin
Password: ********
Confirm Password: ********
Successfully connected using password.
[config system slot modem]#
```

Configuring PPP

To enable out-of-band communication with the Local Manager, use the `config ppp` command in the modem resource to configure PPP settings.

```
[admin@UplogixLM (modem)]# config ppp
--- Existing Values ---
Phone Number:
User Name:
Password: ********
Use Static IP Address: false
Change these? (y/n) [n]: y
--- Enter New Values ---
Phone Number: []: 5121234567
User Name: []: uplogix
```

```
Password []: *****
Confirm Password: *****
Use Static IP Address: (y/n): n
Do you want to commit these changes? (y/n): y
```

- `Phone Number` – The phone number of the remote access server that will terminate the PPP connection.
- `Username and password` – Used to authenticate the PPP connection with the dial-up service provider / remote access server.

If you have configured the Local Manager to use an Iridium modem, answer `y` to the prompt `Use static IP address` to assign an IP address to the modem that is within the range of IP addresses assigned to you by Iridium.

If the Local Manager is managed by a Control Center, PPP can be configured through the Uplogix web interface.

For a single Local Manager: `Inventory > Local Manager page > Configuration menu > PPP`

For a group of Local Managers: `Inventory > group page > Configuration menu > PPP`

Configuring VPN settings

To configure the Local Manager to use a VPN server while operating out-of-band, use the interactive `config vpn` command in the `modem` resource to configure IPsec or PPTP settings.

To configure IPsec, the command presents this dialog:

```
[admin@UplogixLM]# modem
 embedded
[admin@UplogixLM (modem)]# config vpn
--- Existing  Values ---
VPN type: none
Change these? (y/n) [n]: y
--- Enter New Values ---
VPN type [none]: ipsec
Vendor [cisco]:
IPsec Server Hostname or IP: 203.0.113.1
IKE DH Group [dh2]:
Perfect Forward Secrecy [server]:
NAT Traversal Mode [none]:
Allow Single DES (y/n) [n]:
Deny MD5 (y/n) [n]:
Group ID:
Shared key:
User Name:
Password:
Do you want to commit these changes? (y/n):
```

To configure PPTP, the command presents this dialog:

```
[admin@UplogixLM (modem)]# config vpn
--- Existing  Values ---
VPN type: none
Change these? (y/n) [n]: y
```

```
--- Enter New Values ---
VPN type [none]: pptp
PPTP Server Hostname or IP: 198.51.100.105
User Name:
Password:
Do you want to commit these changes? (y/n):
```

If the Local Manager is managed by a Control Center, the modem can be configured through the Uplogix web interface.

For a single Local Manager: `Inventory > Local Manager page > Configuration menu > VPN`

For a group of Local Managers: `Inventory > group page > Configuration menu > VPN`

Configuring remote locations to be contacted by the Control Center

In environments where Local Managers contact the Control Center as needed via satellite modem, initiate contact from the Control Center by sending an SMS message instructing an Local Manager to start PPP.

Requirements for using this capability are:

- The Local Manager uses a GSM cellular modem or an Iridium modem.
- The Local Manager has been configured with a phone number and SMS domain name. These are configured with the `config answer` command.
- An SMS modem monitor has been configured on the modem with the *smsPppOn* rule that tells the Local Manager to initiate the PPP connection when a validate SMS message is received.

Using the `config answer` editor, set the Local Manager's phone number with the `number` subcommand, and use the `domain` subcommand to set the service provider's SMS domain name. Use the `config monitor` command to configure the SMS modem monitor. The Control Center uses these parameters to construct a valid SMS email address, to which it can send the `ppp on` message to establish contact.

For more information about the `config answer` command, refer to Configuring the modem.

PPP Cycle

The PPP Cycle feature allows the Local Manager to bring up its out-of-band connection for a specified duration. When called from a scheduled job, this feature can regularly validate the Local Manager’s out-of-band capability (modem, PPP and VPN functionality). For devices in remote locations, the PPP Cycle command can be used to test the end-to-end out-of-band connection by establishing the connection long enough to communicate briefly with the Control Center, and then tearing it down.

Required Privileges

- `config ppp` — Configures the PPP settings for the device
- `config vpn` — Required for VPN establishment
- `ppp` — Runs the PPP command on demand
- `config schedule` — Used to schedule the `pppCycleDuration` and `pppCycleHeartbeat` jobs
- `config removejob` — Used to remove jobs and monitors

Other Requirements

Valid PPP settings (phone number, username, password, etc.) are required to use this feature. See Configuring PPP in this document for assistance with inputting PPP settings.

A Control Center is required to use the `ppp cycle heartbeat` feature. Also, the device must have a route back to the Control Center to heartbeat while out-of-band. See the Configuring the Local Manager to be managed by a Control Center section for assistance with setting up communication between the Local Manager and a Control Center.

Running PPP Cycle Duration

The `ppp cycle duration` command will complete the following actions:

- Turn PPP on
- Display the out-of-band IP address (will show PPP and VPN addresses)
- Wait one minute
- Turn PPP off

Use `ppp cycle duration` from the modem resource to execute a onetime PPP test. The device will remain out-of-band for one minute (default duration) before it disables PPP. Use the `–d` flag to change the duration in minutes.

```
[admin@UplogixLM (modem)]# ppp cycle duration
Secondary network Local Address is 192.0.2.225
Out of Band is turned on
Waiting 1 minutes
Waited 1 minutes; Out of Band is up
Done waiting
Out of Band is turned off
Out of Band Cycle: OK
```

Scheduling PPP Cycle Duration

To run `ppp cycle duration` as a job, use the `config schedule pppCycleDuration` command. The job will complete the following actions:

- Turn PPP on
- Display the out-of-band IP address
- Wait one minute
- Turn PPP off
- Wait a specified time and then run again

Use the `config schedule` command from the modem resource to schedule this job. Refer to the *Command Reference Guide for Uplogix Local Managers* for more information scheduling jobs. Note that the syntax differs because the `config schedule` command is being used. The `–d` flag is used to specify a delay between executions in seconds. To specify the PPP cycle duration, add a number after the job name.

For example:

`config schedule pppCycleDuration –d 86400` (executes every 24 hours with a default duration of 1 minute)

`config schedule pppCycleDuration 10 –d 86400` (executes every 24 hours with a duration of 10 minutes)

The following example uses the default duration.

```
[admin@UplogixLM (modem)]# config schedule pppCycleDuration -d 86400
```

```
Validate scheduled job(pppCycleDuration)?  (This will execute the job now.) (y/n): y
Secondary network Local Address is 198.51.100.25
Out of Band is turned on
Waiting 1 minutes
Waited 1 minutes; Out of Band is up
Done waiting
Out of Band is turned off
Out of Band Cycle: OK
Job 2 was scheduled.
```

Running PPP Cycle Heartbeat

The `ppp cycle heartbeat` command will complete the following actions:

- Turn PPP on
- Display the out-of-band IP address
- Send one heartbeat to the Control Center
- Display Control Center heartbeat version for verification
- Turn PPP off

Run `ppp cycle heartbeat` from the modem resource to execute a one-time PPP test. Use the `-m` flag to specify minimal heartbeat mode (for low-bandwidth OOB connections).

```
[admin@UplogixLM (modem)]# ppp cycle heartbeat
Secondary network Local Address is 192.0.2.100
Out of Band is turned on
Attempting heartbeat
Server heartbeat version: 4.7.24674
Heartbeat complete
Out of Band is turned off
Out of Band Cycle: OK
```

Scheduling PPP Cycle Heartbeat

The `ppp cycle heartbeat` command can also be run on a schedule. The `pppCycleHeartbeat` job will complete the following actions:

- Turn PPP on
- Display the out-of-band IP address
- Send one heartbeat to the Control Center
- Display Control Center heartbeat version for verification
- Turn PPP off
- Wait a specified time and then run again

Use the `config schedule pppCycleHeartbeat` command to schedule this job. The `-d` flag can be used to specify a delay between executions in seconds. The following example schedules a PPP cycle heartbeat test to happen every 24 hours.

```
[admin@UplogixLM (modem)]# config schedule pppCycleHeartbeat -d 86400
Validate scheduled job(pppCycleHeartbeat)?  (This will execute the job now.) (y/n): y
Secondary network Local Address is 192.0.2.100
Out of Band is turned on
Attempting heartbeat
Server heartbeat version: 4.7.24674
```

```
Heartbeat complete
Out of Band is turned off
Out of Band Cycle: OK
Job 1 was scheduled.
```

Error Handling

If a scheduled PPP cycle fails, a Scheduled Job Failed (`pppCycleDuration`) alarm will be created and logged. Use the `show alarms` command to view this information on the device.

```
[admin@UplogixLM (modem)]# show alarms


UTC     Elapsed  Device   Interface    Message
-----   -------  ------   ---------    -----------------------------
20:33   1:47     modem                 Unable to establish PPP session. (BUSY)
```

Out-of-Band Setup and Teardown Log

The Local Manager logs detailed dialer, PPP, IP, and VPN setup and teardown information when it attempts to bring up an out-of-band connection (either in the event of an in-band network failure or during an out-of-band network test via the `ppp cycle` command). This information can be helpful when troubleshooting out-of-band network configuration or infrastructure issues. Use the `show log outband` command on the Local Manager to view the log for the last successful or failed attempt to communicate out-of-band.

Secondary Ethernet

The Secondary Ethernet port can operate in one of four modes:

- `Bonded` — Use this default mode to join the Secondary Ethernet interface with the front management interface to form a single logical network interface. This mode is most useful for failover scenarios. `Capture` — Use this mode to enable the capture of network traffic for troubleshooting purposes.
- `DHCPServer` — Use this mode when connecting a modem over Ethernet to the Local Manager that will be configured as a virtual modem.
- `Outband` — Use this mode to configure a secondary management network to be used as an out-of-band channel.

Physical Connection

All Uplogix devices have a secondary Ethernet port. Connect the secondary Ethernet port on your Local Manager to your alternate/out-of-band network connection using this port. The following table identifies the secondary Ethernet port for each Local Manager platform:

Uplogix 500/5000	Use the GE-1 port located below Management Ethernet port GE-0.
Uplogix 3200	Use the AUX port located on the back of the device beneath the power controller port.
Uplogix 430	Use the AUX port located to the left of the power controller port.
Uplogix 400	Use the AUX 1 port located on the back of the device.

Bonded Mode

This mode is enabled by default, even if no physical connection is present. Both Ethernet interfaces are combined into a single logical bond0 Ethernet management interface. If a switch port, cable, or interface fails on the primary Ethernet port connection, the system will automatically fail over to the secondary Ethernet connection.

Usage Notes

- Both network interfaces need to be connected to the same VLAN.
- The bond0 interface will use the MAC address of the primary interface. The `show system secondary` command will not display a MAC address for the secondary Ethernet interface while in this mode.

Capture Mode

This mode allows the capture and review of network traffic via the secondary Ethernet interface. A switch can be configured to span/mirror traffic to a port that is connected to the secondary Ethernet port of the Local Manager, where the Local Manager can then capture, filter, display and export traffic captures.

Usage Notes

- The directly connected switch must be configured to send traffic to the Local Manager’s secondary Ethernet port.
- The maximum size of the capture file is 5MB. Traffic capture will automatically stop when this limit is reached.

System Configuration

To configure outband mode, run `config system secondary` from the system resource. When asked for type, specify `outband` and options will become available for DHCP, speed/duplex, and DNS. If not using DHCP, the device will prompt for IP address, subnet mask, and default route.

The following example uses DHCP.

```
[admin@UplogixLM]# config system secondary
--- Existing  Values ---
Type: bonded
Bonding Link: yes
Primary Ethernet Link: yes (bonded active)
Auxiliary Ethernet Link: no (bonded)
Change these? (y/n) [n]: y
--- Enter New Values ---
Type [bonded]: capture
speed/duplex [auto]:
Warning: Remote connections may be lost if you commit changes.
Do you want to commit these changes? (y/n): y
```

Capturing Packets (Basic)

To begin capturing packets, use the `capture` command from the system resource. Capture will continue until you press x, CTRL-C, or the 5MB capture limit is reached.

```
[admin@UplogixLM]# capture
Press 'x' or Ctrl+C to stop capturing packets.
4864 bytes
Capture stopped.
```

Capturing Packets (Advanced)

A variety of options for the capture command are available to filter captured packets.

IP Address	capture host 192.168.1.100
Network	capture net 192.168.1.0/24
Port	capture port 80
IP Address and Port	capture host 192.168.1.100 and port 80
Source	capture src 192.168.1.1
Destination	capture destination 192.168.1.253
Frame Size	capture greater 512, capture less 128
Bytes Per Frame	capture -size 1514

Viewing Captured Packets

To begin capturing packets, use the `capture` command from the system resource. Capture will continue until you press x, CTRL-C, or the 5MB capture limit is reached.

```
[admin@UplogixLM]# show capture
18:53:25.281292 CDPv2, ttl: 180s, Device-ID '333A'[|cdp]
18:53:25.284526 CDPv2, ttl: 180s, Device-ID '333A'[|cdp]
18:53:25.287029 CDPv2, ttl: 180s, Device-ID '333A'[|cdp]
18:53:25.926118 802.1d config TOP_CHANGE 8000.00:d0:ba:bf:62:cd.8022 root
2000.00:d0:01:c1:c4:34 pathcost 23 age 3 max 20 hello 2
fdelay 15
18:53:26.315752 IP6 :: > ff02::16: HBH ICMP6, multicast listener report v2, 1 group
record(s), length 28
18:53:26.391749 IP6 :: > ff02::1:ff00:1524: ICMP6, neighbor solicitation, who has
fe80::20f:2cff:fe00:1524, length 24
18:53:26.942055 802.1d config TOP_CHANGE 8000.00:d0:ba:bf:62:cd.8022 root
2000.00:d0:01:c1:c4:34 pathcost 23 age 2 max 20 hello 2
fdelay 15
18:53:27.391840 IP6 fe80::20f:2cff:fe00:1524 > ff02::2: ICMP6, router solicitation,
length 16
18:53:28.358245 802.1d config TOP_CHANGE 8000.00:d0:ba:bf:62:cd.8022 root
2000.00:d0:01:c1:c4:34 pathcost 23 age 2 max 20 hello 2
fdelay 15
```

To export the capture file in pcap format, use the `show capture -pcap` command and pipe it to SCP, FTP, or E-mail.

```
[admin@UplogixLM]# show capture -pcap | scp uplogix@203.0.113.5:u5000.cap1
uplogix@203.0.113.5's password:*******
..
File successfully sent to 203.0.113.5.
copy succeeded
```

To export via E-mail, use the following syntax:

```
[admin@UplogixLM]# show capture -pcap | mailto support@uplogix.com:u5000.cap1
..
File successfully sent to uplogix.com.
copy succeeded
```

In the above example, the capture file will be attached to the email with the filename u5000.cap1. You can then view this file in any third party application capable of reading pcap files like Wireshark, etc.

To export the capture file in plain text with SCP, FTP, or E-mail, simply omit the – `pcap` option.

DHCPServer Mode

This mode allows the secondary Ethernet interface to be configured for an Ethernet connection to a remote modem.

Usage Notes

- The remote modem should be configured to use DHCP in order to get an IP address from the Local Manager secondary Ethernet port.
- The modem MAC address prefix must be specified in the DHCP MAC address filter field when configuring the secondary Ethernet interface for DHCPServer mode – this prevents the Local Manager from becoming a generic DHCP server to other devices for the case where another device might attempt to DHCP an IP address.
- A virtual modem port must be configured to connect to the IP address that the secondary Ethernet port serves to the modem.

System Configuration

To configure DHCPServer mode, run `config system secondary` from the system resource. When asked for type, specify `dhcpserver` and options will become available for DHCP MAC filter and speed/duplex.

The following example uses DHCP.

```
[admin@UplogixLM]# config system secondary
--- Existing  Values ---
Type: bonded
Bonding Link: yes
Primary Ethernet Link: yes (bonded active)
Auxiliary Ethernet Link: no (bonded)
Change these? (y/n) [n]: y
--- Enter New Values ---
Type [bonded]: dhcpserver
DHCP MAC Address Filter [00:80:a3:]:
speed/duplex [auto]:
Warning: Remote connections may be lost if you commit changes.
Do you want to commit these changes? (y/n): y
```

Viewing Secondary Ethernet DHCPServer Configuration

To view the DHCPServer settings on the secondary Ethernet interface, use the `show system secondary` command from the system resource. Note that the device IP shown below is the IP address given to the modem.

```
[admin@UplogixLM]# show system secondary
Type: dhcpserver
DHCP MAC Address Filter: 00:80:a3:
```

```
Device IP: 169.254.100.254
Port IP: 169.254.100.253
Subnet: 255.255.255.252
Speed/duplex: auto (no link)
MAC Address: 00:0F:2C:00:CF:07
```

Outband Mode

This mode allows the secondary Ethernet interface to be configured as an out-of-band channel for use during primary network outages.

Usage Notes

- The secondary IP subnet must not conflict with the primary and dedicated IP subnets of the Local Manager.
- The secondary Ethernet interface is disabled during in-band operation. The interface will not respond to IP traffic until the out-of-band connection is enabled.
- If you want the Local Manager to establish a VPN over this secondary Ethernet connection, be sure to configure the VPN settings. Use the `config vpn` command from the modem resource to configure VPN settings.
- Dial-in access via the modem is available through the `config answer` command. PPP dial-up via the modem is disabled in this mode.

System Configuration

To configure outband mode, run `config system secondary` from the system resource. When asked for type, specify `outband` and options will become available for DHCP, speed/duplex, and DNS. If not using DHCP, the device will prompt for IP address, subnet mask, and default route.

The following example uses DHCP.

```
[admin@UplogixLM]# config system secondary
>> output removed <<
Change these? (y/n) [n]: y
Type: [bonded]: outband
Use DHCP: (y/n) [n]: y
speed/duplex: [auto]:
DNS Server IP: []:
Do you want to commit these changes? (y/n): y
```

To specify the out-of-band IP address, run `config system secondary` again and set DHCP to no.

```
[admin@UplogixLM]# config system secondary
>> output removed <<
Change these? (y/n) [n]: y
Type: [outband]: outband
Use DHCP: (y/n) [y]: n
Management IP: [0.0.0.0]: 203.0.113.250
Default Route: [0.0.0.0]: 203.0.113.254
Subnet Mask: [0.0.0.0]: 255.255.255.0
speed/duplex: [auto]:
DNS Server IP: []:
Do you want to commit these changes? (y/n): y
```

Usage

Outband mode can be activated both manually and automatically.

`Manual Activation` — To bring up the out-of-band interface, use the `outband on` command from the modem resource.

```
[admin@UplogixLM (modem)]# outband on
Secondary Ethernet Adapter is down.
Secondary network Local Address is 203.0.113.250
Out of Band is turned on.
```

`Secondary Ethernet Adapter is down` — Refers to the adapter's status prior to running outband on. If PPP is already up, the following message will be displayed.

```
[admin@UplogixLM (modem)]# outband on
Secondary Ethernet Adapter is up.
```

To turn off the outband connection, use the `outband off` command.

```
[admin@UplogixLM (modem)]# outband off
Out of Band is turned off
```

`Automatic Activation` — The outband connection can be activated from built-in features like Pulse and through the rules engine.

```
[admin@UplogixLM]# config system pulse
>> output removed <<
Change these? (y/n) [n]: y
--- Enter New Values ---
Use Pulse (y/n) [y]: y
Pulse IP 1 [192.0.2.03]: 203.0.223.225
Pulse Port 1 [7]:
Pulse IP 2 [127.0.0.1]: 203.0.223.226
Pulse Port 2 [7]:
Pulse IP 3 [127.0.0.1]: 198.51.100.225
Pulse Port 3 [7]:
Enable Outband on Pulse Failure (y/n) [n]: y
Do you want to commit these changes? (y/n): y
```

If Pulse fails, the device will automatically enable the outband connection.

```
[admin@uUplogixLM]# show alarms
UTC     Elapsed  Device   Interface    Message
-----   -------  ------   ---------    -----------------------------
14:09   0:40                           Failed to connect to pulse server.
20:33   1:47     modem                 Unable to establish PPP session. (BUSY)
```

```
[admin@UplogixLM]# show event
UTC     Context      Message
-----   -------      -----------------------------
12:56                PPP is up. (203.0.113.200)
```

A rule can also be used to activate PPP. The following is a simplified example that turns PPP on upon scheduling.

```
[admin@UplogixLM]# config rule outbandAlwaysOn
[config rule pppAlwaysOn]# action pppOn
[config rule pppAlwaysOn]# action alarm -a "Enabling Secondary Ethernet OOB"
[config rule pppAlwaysOn]# conditions
[config rule pppAlwaysOn conditions]# true
[config rule pppAlwaysOn conditions]# exit
[config rule pppAlwaysOn]# exit
[admin@UplogixLM]# config monitor system outbandAlwaysOn
Validate scheduled monitor(system)?  (This will execute the job now.) (y/n): y
Job was scheduled 4: [Interval: 00:00:30 Mask: * * * * *] rulesMonitor system
outbandAlwaysOn
[admin@u3200]# show alarms


UTC     Elapsed  Device   Interface    Message
-----   -------  ------   ---------    -----------------------------
14:38   0:24                           Enabling Secondary Ethernet OOB
```

Use the `show status` command from the modem resource to view out-of-band information.

```
[admin@UplogixLM (modem)]# show status
Outband: Secondary Ethernet
Inactive
[admin@UplogixLM (modem)]# show status
Outband: Secondary Ethernet
Active: address 192.0.2.100, duration 10 minutes
```

Configuring Managed Devices and Power Control

The device ports for the Local Manager are initially configured to the native. When a supported device is connected, the port must be initialized for the specific device being managed. Once the initial configuration is complete, minor device changes may be recommended to facilitate the timely and efficient collection of data from the device, such as increased console port speed and optimized logging.

This chapter covers:

- Initializing ports — setting up a port to manage a device
- Configuring port settings for managed devices — alter port settings at the device or group level to optimize device management
- Fine-tuning the device's configuration — manually alter logging options by device
- Uplogix file system — files and types stored locally, creating named files
- Scheduling jobs and monitors — schedule discrete tasks to collect information about the device it is managing
- Changing device configuration after initial set-up — making changes after initial configuration
- Customizing the device hostname — edit the hostname
- Configuring the Local Manager to assign DHCP addresses to connected devices — DHCP setup
- Using dedicated Ethernet ports on switches — Ethernet setup
- Enhanced native mode — setting up a port to manage a device without an advanced driver
- Pull/Push SFTP and TFTP — enable manual and automatic transfer of configuration and OS files
- Clearing a previously configured port or slot — removing port or slot information from the Local Manager
- Configuring virtual ports — setting up virtual ports and slots
- Configuring power control — setting up power control

Initializing ports

The Local Manager uses the default serial settings of `9600, 8, n, 1` when operating in native mode.

When connecting a device, the next step is to initialize the Local Manager port to use the appropriate driver and to enable active monitoring and control of the managed device. Uplogix recommends logging into the device to verify serial communication settings and passwords prior to port initialization. Then navigate to the appropriate `port` resource and use the `config init` command to set up the port. This must be performed even if the native settings are appropriate for the device; otherwise, the device information is not displayed when using the `show dashboard` command.

The settings presented vary by device make and model. Refer to the device’s documentation for configuration settings. In addition, Ethernet-related settings are not presented if using an Uplogix 430 or 500 Local Manager, or an Uplogix 3200 or 5000 Local Manager without dedicated Ethernet modules.

```
[admin@UplogixLM (port1/1)]# config init
--- Enter New Values ---
description: Quest 32/HFGS/012345/NW
make [native]: cisco
model:
os: ios
os version:
management IP: 192.0.2.220
Configure dedicated ethernet port? (y/n) [n]:
console username: bob
console password: *******
confirm password: *******
enable username:
enable password: *****
confirm password: *****
secondary console username:
secondary console password:
secondary enable username:
secondary enable password:
Serial Bit Rate [9600]: 115200
Serial Data Bit [8]:
Serial Parity [none]:
Serial Stop Bit [1]:
Serial Flow Control [none]:
Do you want to commit these changes? (y/n): y
Testing login will take a few moments...
Login successful; credentials are valid.
Retrieving device information directly from device...
Hostname     : Quest-HSGS1
Serial Number: FHK1310F1Z3
Make         : cisco
Model        : CISCO2921/K9
OS Type      : IOS
OS Version   : 15.1(4)M
Uptime       : 4 days, 19 hours, 21 minutes
Updating model.
Updating OS version.
Assimilating the device will set buffered logging on the console.
Proceed? (y/n): y
Retrieving running-config from device ...
- Output removed -
```

Description (optional free text field up to 255 characters) – Optionally, enter information about the device attached to the port. If left blank the device hostname will automatically be used. This field will be displayed as part of the information that normally scrolls on the Local Manager front panel display.

Some symbol characters, such as the ~ and \ are not shown correctly on the front panel display.

Make (required) – The available settings for make are:

- 3Com
- Alcatel
- Brocade
- Cisco
- Comtech
- enchanced
- Foundry
- Garmin
- GE
- Gilat
- HP
- IBM
- iDirect
- Juniper
- native
- ND SatCom
- Netscreen
- Nortel
- PPP
- Sea Tel
- server
- SpaceTrack
- Sun
- Tasman
- Tippingpoint
- TracStar

Use the native setting for devices that are not explicitly supported.

Detailed configuration information for supported devices is available at support.uplogix.com.

A device configured as native can be controlled by a serial connection and by the power control unit, but can only monitor chassis statistics gathered externally such as Ethernet link beat and serial CTS/DSR/TX/RX.

Model (automatic free text field of up to 255 characters) — Information entered in this field is replaced by what the Local Manager detects on this port, unless the device is configured as native.

Operating system (required) — Available settings depend on the specified `make`. For example, BayRS for Nortel; IOS/IOS-XE, NX-OS, ASA, Pix or CatOS for Cisco; JunOS for Juniper; TOS for TippingPoint; and TiOS for Tasman.

Operating system version (automatic free text field of up to 255 characters) — Information entered in this field is replaced by what the Local Manager detects on this port, unless the device is configured as `native`.

Management IP address (optional) — This field is for the management IP address of the managed device. For the case of a Cisco router, it is best to use the lowest numbered interface on the router (GigabitEthernet0/0, for example), as this address and interface are used by default with the TFTPDNLD functionality during ROMmon recovery and when sourcing SNMP traps sent on behalf of the device.

Dedicated Ethernet port (optional) — The dedicated Ethernet port is used to create a reliable, direct Ethernet connection between the Local Manager and the managed device. If configured, the Local Manager will use this connection to move OS and configuration files back and forth between the managed device and the Local Manager using such file transfer protocols like FTP, SFTP/SCP and TFTP. If the port is configured, a non-overlapping IP subnet must be used for the dedicated link. Non-routable private (RFC 1918) addresses such as 169.254.x.x are recommended. To configure a dedicated Ethernet port, enter **y**.

If you configure a dedicated Ethernet port on a switch, please read Using dedicated Ethernet ports on switches.

Use DHCP (available if you opt to configure a dedicated Ethernet port) — Configures the Local Manager to provide the managed device dedicated Ethernet interface with an IP address via DHCP. When using DHCP, be sure to configure the managed device dedicated Ethernet port to use DHCP to get its IP address.

To use this feature, you must also configure the Local Manager to assign DHCP addresses. Refer to Configuring the Local Manager to assign DHCP addresses to connected devices.

Dedicated device IP (required if using static addressing for the dedicated Ethernet port) — The IP address on the managed device. This IP address is not used in SYSLOG/SNMP messages for this device, but can be used in device recovery to communicate directly to the managed device and move files.

Dedicated port IP (required if using dedicated Ethernet port) — The dedicated Ethernet link IP address for the Local Manager.

Dedicated Ethernet subnet mask (required if using dedicated Ethernet port) — The subnet mask for the dedicated Ethernet link. Since this is a point-to-point Ethernet connection all that is required is a 255.255.255.252 mask.

The dedicated network of each device must be on its own IP subnet.

Port speed (optional) — The speed used by the device’s Ethernet port. Speed can be set for better performance or to overcome auto-negotiation problems. Available settings are 10half, 10full, 100half, 100full, 1000full and auto (default).

Console username (optional free text field) — Enter the username to be used to access the managed device for the case where a username is required to access the device.

Console password (optional free text field, usually required) — Enter the password to be used to access the managed device for the case where a username/password or just a password is required to access the device.

Enable username (optional free text field) — If there is no privileged super user account this field is not necessary. Leave this field blank for the case where there is only an enable password to enter privileged mode.

Enable password (optional free text field, usually required) — This password is used to enter privileged mode on a Cisco device or as the root password for Juniper devices.

Secondary Console username (optional free text field) — For use in situations that require the device to utilize an alternate authentication scheme – for example, you may want to failover to using a locally defined user account when AAA servers are unreachable.

Secondary Console password (optional free text field) — For use in situations that require the device to utilize an alternate authentication scheme – for example, you may want to failover to using a locally defined user account when AAA servers are unreachable.

Secondary Enable username (optional free text field) — For use in situations that require the device to utilize an alternate authentication scheme. Leave this field blank for the case where there is only an enable password to enter privileged mode.

Secondary Enable password (ptional free text field) — For use in situations that require the device to utilize an alternate authentication scheme. This is usually the same enable password as is used for the other/primary login credentials.

Serial bit rate (optional) — The bit rate used by the managed device. Available settings are 1200, 2400, 4800, 9600, 19200, 38400, 57600, and 115200.

Serial data bit (optional) — The number of data bits (7 or 8) used by the managed device.

Serial parity (optional) — The parity setting (none, even, or odd) used by the managed device.

Serial stop bit (optional) — The number of stop bits (1 or 2) used by the managed device.

Null modem (400 and 3200 Local Manager only— optional) — If a rolled cable is used, enter y.

Commit changes (required) — You must commit changes before they are implemented.

When changes are committed, the Local Manager queries the device based on the information entered. Model and OS version may be replaced with specific information collected from the device.

Configuring port settings for managed devices

Each port has a set of parameters that control interactions with the device it manages. You can define file transfer methods and priorities, configure file save method, wait time during device reboots, and so forth. These are the settings applied during the assimilation process, which fine-tunes the device settings for optimum performance.

The factory default settings for the Local Manager represent common industry practices, but your environment may require customized settings.

To access port settings, use the interactive `config settings` command. Each entry in the settings list is accessed by entering the number associated with that entry.

```
[admin@UplogixLM (port2/2)]# config settings
--- Settings Menu ---
1 Assimilated terminal speed: 19200
2 Modify terminal serial speed on assimilation: false
3 Device configuration pull method: console
4 Device configuration push method: xmodem
```

```
5 Alternative device configuration push method: tftp
6 Device configuration push retries: 3
7 Automatic configuration rollback: [disabled/manual/automatic] automatic
8 Count delay before automatic configuration rollback: 75
9 Issue 'write memory' after configuration rollback: true
10 Verify OS upgrade: true
11 Use manual boot during upgrade, if applicable: true
12 OS image push method: tftp
13 Alternative OS image push method: xmodem
14 Attempt to use XModem-1K (first attempt only): true
15 Save Configuration on change before reboot? true
16 Reset console and telnet on auth. change? true
17 Previous OS image not found, continue? true
18 Maximum OS image push retry attempts: 3
19 Device reboot timeout (seconds): 300
20 Force the device to reboot immediately after pushing the OS: true
21 Device pass through timeout(seconds): 300
22 Enable local echo: false
23 Leave old OS if space permits during OS upgrade: true
24 Done
Select setting to edit or 24 to end: 21
Device pass through timeout (seconds): 300 [300]:600
```

After the setting is modified, the full list of settings is displayed again, with your change.

If the Local Manager is managed by a Control Center, you can configure settings from the Uplogix web interface.

For a single Local Manager: `Inventory > Local Manager page > port detail > Port Settings`

For a group of Local Managers: `Inventory > group page > default port settings` (allows you to configure settings for categories of devices)

Item	Setting	Detail
1	Assimilated terminal speed	Define the assimilated terminal speed. Options: 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600 or 115200
2	Modify terminal serial speed on assimilation	Allows the Local Manager to change the terminal speed of the managed device during assimilation. Options: True or False
3	Device configuration pull method	Defines the method the Local Manager will use to pull configuration information from the managed device. Options: TFTP, console, or FTP
4	Device configuration push method	Defines the method the Local Manager will use to push configuration information to the managed device. Options: TFTP, console, xmodem, or FTP
5	Alternative device configuration push method	Defines a secondary method the Local Manager will use to push configuration information to the managed device if the primary method fails. Options: TFTP, console, xmodem, or FTP

6	Device configuration push retries	Number of retry attempts the Local Manager will make to push a configuration to a managed device. Options: Integer value
7	Automatic configuration rollback	Enable, disable or change SurgicalRollback™ settings. Options: manual, disabled, or automatic
8	Count delay before automatic configuration rollback	Set the delay (in seconds) the Local Manager will wait before initiating SurgicalRollback™ if that feature has been set to run automatically. Options: Integer value
9	Issue 'write memory' after configuration rollback	Define if the Local Manager will perform a ‘write memory’ on a device after a configuration has been rolled back. Options: True or False
10	Verify OS upgrade	Define if the Local Manager will verify the managed device successfully upgraded. Options: True or False
11	Use manual boot during upgrade, if applicable	Define if the Local Manager will manually boot the managed device during the course of a scheduled upgrade. Options: True or False
12	OS image push method	Defines the method the Local Manager will use to push an OS image to the managed device. Options: TFTP, ymodem, xmodem, or FTP
13	Alternative OS image push method	Defines a secondary method the Local Manager will use to push an OS image to the managed device if the primary method fails. Options: TFTP, ymodem, xmodem, or FTP
14	Attempt to use XModem-1K (first attempt only)	Defines if XModem-1K will be used in the first attempt of a pull or push activity. Options: True or False
15	Save Configuration on change before reboot?	Defines if a managed device configuration will be saved if there is a change and the user has issued a reboot. Options: True or False
16	Reset console and telnet on auth. change?	Not used. This setting has been deprecated and will be removed in a future version of LMS.
17	Previous OS image not found, continue?	Defines if the Local Manager will push a new OS image if a previous version is not stored locally. Options: True or False
18	Maximum OS image push retry attempts	Defines the number of attempts the Local Manager will retry a push OS operation after it has initially failed. Options: Integer value

19	Device reboot timeout (seconds)	Defines wait time during a managed device reboot. Options: Integer value
20	Force the device to reboot immediately after pushing the OS	Defines if the Local Manager will reboot the managed device after an OS is pushed to it. Options: True or False
21	Device pass through timeout (seconds)	Defines the inactivity timeout of a terminal session on the managed device. Options: Integer value
22	Enable local echo	Enables or disables local echo on a managed device. Options: True or False
23	Leave old OS if space permits during OS upgrade	Determines what the Local Manager will do with the old OS file(s) on a managed device during an OS upgrade
24	Done	Saves changes made and exits the port settings wizard

Fine-tuning the device's configuration

The assimilation process sets synchronous logging on the managed device console port and configures buffered logging. When you initialize the port, the `config init` dialog prompts you to assimilate the device. If you do not choose to assimilate the device as a part of the initialization, this fine-tuning step can be performed later, either automatically or manually.

Changing the device configuration manually

If you choose not to assimilate the device when initializing the Local Manager port to manage the device, you can do so manually as shown below.

Synchronous logging (Cisco only)

Enabling synchronous logging is done so that device-originated console output is displayed after console output originated by the user or by the Local Manager. For example, if the Local Manager requests a display of the device's running configuration and the device generates console-bound system log messages while the configuration display is in progress, the entire configuration is displayed first, and the system log message is displayed afterward. By default, synchronous logging is used on Cisco devices. Use the `config device logging` command to change this.

```
[admin@UplogixLM (port1/1)]# config device logging
--- Existing Values ---
Set the console to use synchronous logging: yes
Set the console to use logging buffered: yes
Logging level for buffered logging (PIX only): 3
Device buffer polling interval: 30
Clear device log buffer on poll: yes
Port syslog forwarding enabled: no
Change these? (y/n) [n]: y
```

Buffered logging

To minimize the load on the network device, turn on buffered logging so the Local Manager can refer to the buffered list of messages. This batch approach operates more efficiently because it requires fewer resources on the device. Use the `config device logging` command to change this.

> Some devices do not support buffered logging. The Local Manager defaults to collecting console log data as it streams to the console.

Optimizing the device configuration automatically

The assimilation process is available outside of the `config init` process with the `assimilate` command.

To change the settings used in the assimilation process, use the `config settings` command as described in Configuring default settings for managed devices.

```
[admin@UplogixLM (port1/1)]# assimilate
Retrieving running-config from device ...
Complete. running-config pulled.
Setting buffered logging.
Setting logging synchronous.
Setting configured speed to 115200.
```

Assimilation can be undone by issuing the `rollback assimilate` command.

Uplogix file system

Each port resource on the Local Manager comes with its own file system for storing configuration files, OS images, output from Power On Self Tests (POST), and the output from a `show tech` command on a managed device. Categories in the file system include:

- Config – Running
- Config – Startup
- OS
- Post
- Tech

The file system names files using a built-in naming system.

- Versions
  - Candidate: Used for staging a new configuration or OS prior to update or upgrade
  - Current: The current version of file running on the managed device
  - Previous: The previous version running on the managed device before it was replaced by Current
  - Archive #: Previous versions that were running on the managed device. The file system will store up to 20 archived versions
  - Named: user-defined version names. The file system will store up to 5 named configuration versions and 6 named OS versions

The built-in version names will continue to cycle as new running configurations are detected.

Viewing files

Use the `show directory -v` command to view the files in the Uplogix file system for a managed device.

```
[admin@UplogixLM (port2/2)]# show dir -v
All times shown in UTC.

Type     Version    Size        Date          Name
-------  ---------  ----------  ------------  ------------
Config
    Running
         current    4112        Nov  4 22:10  running-config
         previous   4095        Oct 15 15:32  running-config
         archive 1  4099        Oct 15 15:30  running-config
         archive 2  4146        Oct  8 20:59  running-config

    Startup
         current    4148        Oct 15 20:59  startup-config
         previous   4152        Oct 15 15:30  startup-config
         vlandata   780         Oct 15 20:59  vlan.dat
         archive 1  4132        Oct  8 20:59  startup-config

OS
         current    70542428    Oct  8 21:00  c2900-universalk9-mz.SPA.151-4.M.bin

Tech
         current    417818      Oct 15 15:22  showTech

Post
         current    4621        Oct 15 15:25  readPost

[admin@UplogixLM (port2/2)]#
```

User-defined file version names

The user-defined version names feature allows users to assign unique names to files stored in the Uplogix file system for managed devices, and to use those named files for the push, pull, copy, and delete file operations. The named file will remain untouched until it is deleted or overwritten. Up to five configuration files of each type may be named and up to six named OS files may be stored in the local file system. File names are limited to nine characters in length.

There are a few situations where the Local Manager automatically creates a named configuration and OS file. The advanced Cisco IOS driver will back up that VLAN database from a switch and store it as a named startup-config file called “vlandata”. The OS Policy feature will store a standard OS file that is referenced for the given make and model in an OS Policy on the Control Center as a named OS file with the name “standard”.

A user must have a role with the following permissions in order to complete the operations described for this feature:

- `show directory` — Displays stored files on a port resource
- `copy` — Copies a stored file
- `delete` — Deletes a stored file

Copying and Naming Files

Use the `copy` command to rename a file or to move it. The syntax for the `copy` command is:

```
copy [options] {source} {destination}
Where each parameter is made up of the following choices:
Type = <os | running-config | startup-config | tech | post>
Version = <candidate | current | previous | <user ver> | archive #>
User versions can include A-Z, a-z, 0-9, and _,  1 to 9 characters.
Port = port #/#


Example of copying the current running-config to a user-named running-config with the
name “golden”:
[admin@UplogixLM (port1/3)]# copy running-config current golden
copy succeeded
[admin@UplogixLM (port1/3)]# show directory
Type        Version      Size         Date             Name
------- ----------       ------       ------------     ------------
Config
Running
Current     7592          17 Feb 12:52     running-config
golden      7592          17 Feb 12:51     running-config
```

Deleting files

Use the `delete` command to remove a named file from the Uplogix file system.

Note: Built-in versions cannot be deleted.

The syntax for the `delete` command is:

```
delete <Type> <user-defined version>
```

An example of deleting a named file from the file system:

```
[admin@UplogixLM (port1/3)]# delete running-config golden
Really delete runningConfig, "golden"? (y/n): y
```

Scheduling Jobs and Monitors

Schedule a Job

Jobs are discrete tasks that the Local Manager uses to collect information about the device it is managing. Jobs can include the collection of device info or the pull or push of a configuration or OS. Many jobs on the Local Manager are scheduled automatically during the initial `config init` process, but it is also possible to schedule additional jobs at any time. To schedule a job, use the `config schedule` command:

```
config schedule <crontab> <job [job args]>
```

Command parameter definitions:

- `Crontab:` Set the timing of when the job will run. The job can run once, run at a specific time and repeat with a delay, or run during an interval of time. The following formats are used:
    - `One time`: Schedule a job to run one time with the –o flag: `<-o execution time>`
    - `Cron schedule`: Schedule a job to run at a specific time and repeat at a specific interval. Define the start time and interval time with the following flags: `<[-m 0-59] [-h 0-23] [-D 1-31] [-M 1-12] [-W 0-6]> [-d delay]`
    - `Interval schedule`: Schedule a job to run during a period of time with a specific delay between repetitions. Define the interval and delay with the following flags: `[-s startTime] [-e endTime] <-d delay>`

    ```
    All times are MM/dd/yy-HH:mm:ss format
      -M <month>       month range (1 - 12)
      -h <hour>        hour range (0 - 23)
      -D <day>         day range (1 - 31)
      -m <minute>      minute range (0 - 59)
      -W <week>        week day (0 - 6)
      -d <delay>       delay between 2 consecutive executions of the job in
      seconds
      -e <end time>    end time after which the job is removed from the scheduler
      -o <one time>    the one time at which the job should run
      -s <start time>  start time for the job
    ```

- `job [job args]`: The job the Local Manager will run on the defined schedule. Jobs available for use with this command include:
    - `clearCounters`: Clears all interface counters
    - `clearServiceModule`: Clears service module
    - `deviceInfo`: Collects Serial#/Make/Model/OS information
    - `interfaceCycle`: Cycles the interface specified
    - `interfaceOff`: Turns off the interface specified
    - `interfaceOn`: Turns on the interface specified
    - `powerCycle`: Cycle device power
    - `powerOff`: Turn device power off
    - `powerOn`: Turn device power on
    - `pullOS`: Copies an OS image from the device
    - `pullRunningConfig`: Pull a running config from a device
    - `pullSftp`: Pull a file using SFTP/SCP
    - `pullStartupConfig`: Pull a startup config from a device
    - `pullTftp`: Pull a file using TFTP
    - `pullVlanConfig`: Pull a VLAN database from a device
    - `pushOS`: Push an OS Image to a device
    - `pushRunningConfig`: Push a running config to a device
    - `pushSftp`: Push a file using SFTP/SCP
    - `pushStartupConfig`: Push a startup config to a device
    - `pushTftp`: Push a file using TFTP
    - `reboot`: Reboot the device connected to this port
    - `showTech`: Retrieve tech-support info from a device

Schedule Job Examples

Here are some examples of job schedules:

`config schedule -s 01/03/14-10:30:00 -e 02/03/14-10:29:59 -d 30 deviceInfo`	Executes the deviceInfo job every 30 seconds between Jan 3 and Feb 3, 2014
`config schedule -o 01/03/14-10:30:00 deviceInfo`	Executes the deviceInfo job once on Jan 3, 2014
`config schedule -M 3 -m 30 deviceInfo`	Executes the deviceInfo job every half hour in March

Issue the `show schedule` command at the managed device port to see the scheduled job.

```
[admin@UplogixLM (port1/1)]# show schedule
Listing currently scheduled jobs for device: port1/1  All times shown in UTC.
6: [Interval: 03:00:00 Mask: * * * * *] pullRunningConfig
8: [Interval: 336:00:00 Mask: * * * * *] pullOS
3: [Interval: 00:05:00 Mask: * * * * *] deviceInfo
```

Delete a Scheduled Job

Use the `show schedule` and `config removejob {job ID}` commands to find the scheduled job number and then remove that job from port. Note that the `pullTftp` job number in the `show schedule` example above is `job 55`. To delete this scheduled job from the Local Manager port, issue the following command:

```
[admin@UplogixLM (port1/1)]# config removejob 3
Job 3 has been removed from the scheduler queue.
```

Schedule a Monitor

A monitor is a set of instructions to collect data at regular intervals. The Local Manager can collect certain data from any supported device. The available data depends on the device.

By default, monitors run every 30 seconds. When you create a monitor, you can specify how frequently the monitor runs. Many monitors may be scheduled automatically during the config init process. Monitors may include rules that specify how to evaluate the collected data. Rules give the monitor the ability to respond to changes or trends.

To schedule a monitor, use the `config monitor` command.

```
config monitor <monitor> <ruleList> <:[delay seconds>
```

Command Parameters:

- `monitor:` The type of monitor. Options include: chassis, consoleLog, interface, ping or terminal
- `rulelist:` The list of rules or rulesets that define when to alarm and what actions to take based on the data collected. The list of rules and rulesets are separated by a comma or bar.
- `delay:` Delay time in seconds between monitor executions.

Schedule Monitor Examples

Here are some examples of simple monitor schedules:

`config monitor interface Ethernet0/0 interfaceBasic :30`	Schedules an interface monitor on Ethernet 0/0 applying the interfaceBasic ruleset with a delay of 30 seconds.
`config monitor ping 203.0.113.225 OOB-ping 30`	Schedules a monitor to ping `203.0.113.225` applying the OOB-ping rule with a delay of 30 seconds.
`config monitor chassis :30`	Schedules a chassis monitor with a delay of 30 seconds.

Changing device configuration after initial setup

The settings configured with the `config init` command can be updated at any time after you set up the port (refer to Initializing ports) through the use of additional commands.

`config authentication`	Change authentication settings for the device, including Console/Enable usernames and passwords.
`config device logging`	Configures logging settings for the port.
`config info`	Configures description, make, model, OS, OS version, management IP address and dedicated Ethernet IP address.
`config serial`	Configures serial settings.

Customizing device hostname

The hostname of each port device is used in the dashboard view that is displayed when logging in or when using the `show dashboard` command. If no hostname is available, the description is used.

The front panel display on the Uplogix 3200 and 5000 Local Managers also provide information including the hostname and status for each port device. The hostname may be what the Local Manager retrieves from the device or what you set as the description.

To change the device description, set the description field using the `config init` or `config info` command. This only changes the dashboard display if the Local Manager cannot retrieve a hostname from the device.

Configuring the Local Manager to assign DHCP addresses to connected devices

When connecting managed devices to the dedicated Ethernet ports of the Local Manager, configure their dedicated Ethernet connections to use static IP addresses or acquire DHCP addresses from the Local Manager.

Dedicated Ethernet is not available for the Uplogix 430 and 500 Local Manager platforms, as they provide serial device ports only.

When setting the Local Manager to assign DHCP addresses to devices, the DHCP pool must not overlap with other pools or subnets:

- the base address must not overlap the system's management IP address
- the base address must not overlap existing static assignments on ports

Caution: If these requirements are not met, the Local Manager will not assign addresses properly and Ethernet-related features will be unavailable.

Use the `config system protocols dhcp` command to set the base DHCP address that will be used in generating addresses.

The syntax for this command is: `config system protocols dhcp <nnn.nnn.nnn>` where `<nnn.nnn.nnn>` is the base address to be used. The default base address is `169.254.100`.

The devices connected to individual ports must also be configured to use DHCP. When configuring a device on a port using the `config init` command, the dialog asks whether to configure a dedicated Ethernet port. If you respond with `y`, the next prompt asks whether to use DHCP.

```
Configure dedicated ethernet port? (y/n) [n]: y
Use DHCP? (y/n) [n]: y
```

If the device is configured to use DHCP, it is not accessible until it requests a DHCP address.

Changes to the `config system protocols dhcp` setting take effect after restarting the Local Manager.

If the Local Manager is managed by a Control Center, the DHCP server settings can be configured through the Uplogix web interface.

For a single Local Manager: `Inventory > Local Manager page > Configuration menu > Protocols Settings > DHCP Server Settings`

For a group of Local Managers: `Inventory > group page > Configuration menu > Protocols Settings > DHCP Server Settings`

Using dedicated Ethernet ports on switches

> For a switch configured to use a dedicated Ethernet port with a static IP address, the Local Manager turns off the interface except when it is needed. When the Local Manager turns on the dedicated Ethernet port, it can take 30-50 seconds for the switch to start forwarding traffic if the Spanning Tree Protocol (STP) is running on the switch port. Uplogix recommends using a feature like Cisco's portfast STP feature when connecting a switch port to a Local Manager dedicated Ethernet port.

Sometimes, actions that result in a pull OS operation (such as using the `copy` command) may return messages that FTP has failed, because the pull operation starts before the interface is ready. The pull operation then succeeds when the pull is attempted using its secondary transfer method. *This issue is unique to switches using dedicated Ethernet ports with static IP addresses where the Spanning Tree Protocol is running on the switch port.*

If the dedicated Ethernet port uses DHCP, the interface remains up during normal operation.

There are two ways to prevent the problem:

- Configure the dedicated Ethernet connection to use DHCP (not available for Uplogix 430 or 500 Local Managers)

OR

- Enable the portfast feature on Cisco switch ports – see following configuration example:

```
interface FastEthernet1/0/1
description dedicated Ethernet to Local Manager
switchport access vlan 2
spanning-tree portfast
```

Enhanced native mode

Enhanced native mode allows the Local Manager to automate basic commands for devices for which no advanced driver exists. Using regular expressions, the Local Manager can log in, log out, and recognize the command prompt. Coupled with rules, monitors and the ability to pull and push files using SFTP/SCP/TFTP, the enhanced native driver provides a very significant amount of automated functionality to bridge the gap between native mode and an advanced driver. Enhanced native mode allows users to configure a port such that it will:

- Automatically authenticate with the device when the user runs the `terminal` command.
- Automatically exit the device command line when exiting a terminal session, when the idle timeout is reached, or if the user's session is lost unexpectedly.
- Schedule monitors with custom rules for device monitoring/testing.

Enhanced native settings become available after running `config init` and selecting enhanced as the device make. Enhanced-specific options are:

Option	Default Value	Description
command prompt	`[#>]`	A regular expression representing the command prompt of the managed device. By default, matches all command prompts that end in # or >.
login prompt	`sername:\s`	A regular expression representing the username prompt. For example, the default value of **`sername:`** followed by a whitespace (\s) would match all the prompts below: Username: Username: Enter Username:
password prompt	`ssword:\s`	A regular expression representing the password prompt. For example, the default value of **`ssword:`** followed by whitespace (\s) would match all the prompts below: Password: Password: Enter Password:
logout command	`exit`	The command used to exit the managed device's command line interface. Other examples include `logout` or `quit`.
wakeup command	`\r`	The command used to wake up the managed device. In other words, cause the device to present a login prompt when the default line feed will not result in a prompt. For example, if the user must enter `CTRL+C` key sequence to get a login prompt, then the wakeup command should be `\c`.

The default values will not work with all devices. Before running `config init, terminal` into your device (in native mode or with a workstation) and take note of the various command prompts as well as the login/password prompt. Some trial and error may be necessary before finding the most robust prompt definition for your device.

Regular Expressions

Regular expressions are used to specify the command, username, and password prompts for the managed device. Please contact support.uplogix.com for assistance creating regular expressions for your specific device. Below are basic operations:

[ ]	Brackets: Matches any of the characters within the brackets. Example 1: [#>!] matches a prompt that ends with #, >, or ! Example 2: [~!]# matches a prompt that ends with ~# or !#
|	Pipe: Separates alternative strings. Example: router>|router# matches a prompt ending in router> or router#
()	Parentheses: Provides order of operation when evaluating expressions. Example: router(>|#) matches router first, then either > or # at the end of it. Without the parenthesis, router>|# would match router> and #.
*	Asterisk: Describes a possibility for zero or more instances of the character preceding it. Example: pas*word matches paword (zero instances of s), pasword (1 instance), password and passsword (multiple instances).
\s	Represents any form of whitespace, including tab, newline, space, carriage return, form-feed, etc.

Examples

Device Configuration	**Local Manager Configuration**
command prompts: `hostname>`	command prompt: `>`
login prompts: `login:`	login prompt: `ogin:\s`
password prompts: `password:`	password prompt: `ssword:\s`
logout command: `exit`	logout command: `exit`

command prompts:
`hostname>`
`hostname#`
`hostname!`
	command prompt: `[>#!]`

login prompts `Username:`	login prompt: `sername:\s`
password prompts: `User Secret:`	password prompt: `ecret:\s`
logout command: `quit`	logout command: `quit`

Device Configuration	**Local Manager Configuration**

command prompts:
`user name$`
`group name!`
`group name=`
`group name!=`
	command prompt: `[$!=]\s`

login prompts
`User Email:`
`Group Email:`
`User Number`
`Group Number`
	login prompt: `(mail|umber):\s`

password prompts:
`User Password:`
`Group password:`
	password prompt: `ssword:\s`

logout command: close	logout command: close

Configuring a port in enhanced native mode

To configure a port for enhanced native mode, follow these steps. Log in to the Local Manager via SSH or the console management port. Navigate to the port using the `port <slot>/<number>` command and run `config init`. When prompted for make, enter `enhanced`**.**

```
[admin@UplogixLM (port1/2)]# config init
--- Enter New Values ---
description: Extreme 150
make [native]: enhanced
model:
os:
os version:
management IP: 192.0.2.111
command prompt [[#>]]:
login prompt [sername:\s]: login:\s
password prompt [ssword:\s]:
logout command [exit\r]:
wakeup command [\r]:
console username: admin
console password:
Serial Bit Rate [9600]:
Serial Data Bit [8]:
Serial Parity [none]:
Serial Stop Bit [1]:
Serial Flow Control [none]:
Do you want to commit these changes? (y/n): y
```

Timeout Configuration

By default, the enhanced native driver waits up to 5 seconds for the managed device to respond (i.e. to present login and password prompts as well as the CLI prompt after issuing a command). Some devices may not respond to the driver quick enough, causing the driver to fail to login or detect the state of the managed device. A port property named `Enhanced_TimeoutSeconds` can be specified with a timeout value (in seconds) to override the default value – the timeout value can be extended or shortened using this mechanism. For example, to configure this value to 8 seconds, login to the Local Manager, navigate to the enhanced native port, and issue the `config properties` command as follows:

```
[admin@UplogixLM]# port 1/1
enhanced
[admin@UplogixLM (port1/1)]# config properties
[config properties]# Enhanced_TimeoutSeconds 8
[config properties]# exit
```

To view enhanced native property settings, issue the `show properties` command at the Local Manager port:

```
[admin@xyzcoAuz (port1/1)]# show properties
Enhanced_CommandPrompt: [#>]
Enhanced_LoginPrompt: login:\s
Enhanced_LogoutCommand: exit\r
Enhanced_PasswordPrompt: ssword:\s
Enhanced_TimeoutSeconds: 8
Enhanced_WakeupCommand: \r
```

Configuration and OS File Backup and Restoration

If the managed device supports SFTP, SCP or TFTP and supports commands to back up its configuration and OS files to a SFTP/SCP/TFTP server, our Pull/Push SFTP and TFTP command functionality can be used to create automatic file backups for example. See the following section for details on how to configure this.

Pull/Push SFTP and TFTP

Local Manager device drivers have functionality that enables manual and automatic transfer of configuration and OS files between the Local Manager and the managed device using Secure File Transfer Protocol (SFTP) or Trivial File Transfer Protocol (TFTP).

The `pull SFTP` and `pull TFTP` features are used to transfer files from the managed device to the Local Manager. The `push SFTP` and `push TFTP` features are used to transfer files from the Local Manager to the managed device. These features can be initiated as a CLI command, a scheduled job, or an action in a rule.

The SFTP command generates a temporary unique password to authenticate the SFTP transfer. Remember to allow outbound SSH connections from the device’s console port since it is the underlying transport for SFTP. For example on a Cisco device you should include the configuration:

```
line con 0
transport output ssh
```

There are several instances when it would be appropriate to apply the pull/push SFTP or TFTP feature, such as:

- Schedule `pull SFTP` and `pull TFTP` jobs for a device configured with the Enhanced Native device driver to regularly backup startup and running configuration files to the Local Manager file system for that device.
- Backup OS image files from the managed device to the Local Manager.
- Backup any file from a managed device to the Local Manager.
- Automatically restore a golden configuration file to the managed device when certain conditions are met on the managed device using a monitor and the rules engine.
- Locally stage and download managed device OS files from the Local Manager.

In order to utilize pull and push SFTP or TFTP, a user must have the following privileges:

- `pull file` – The define and initiate command to copy a file from the managed device to the Local Manager.
- `push file` – The define and initiate command to copy a file to the managed device from the Local Manager.

Pull TFTP or SFTP Usage

Use the following command at the Local Manager port prompt to transfer a file from a managed device to the Local Manager:

```
pull tftp [dedicated] <“remote command”> <xferFileName> <type> [version]

pull sftp [options]   "<remote command>"              <type> [version]
```

Command parameter definitions:

- `dedicated`: An optional parameter that can be added to specify the use of a dedicated Ethernet connection between the Local Manager and managed device for the file transfer.
- `remote command`: The copy command that should be issued at the CLI of the managed device to copy a file over to the Local Manager from the managed device. This command string can also include embedded escape sequences such as \r, which are helpful when the managed device command involves a command dialogue rather than a single command.
- `xferFileName`: The name of the file being pulled/transferred from the managed device to the Local Manager.

The transfer filename must be unique across all ports in the Local Manager. For example, if there are two enhanced native ports managing the same kind of device, the transfer filename must be different for each port.

- `type`: Indicates the Local Manager file system file type. Valid file types are `running-config`, `startup-config`, `OS`, and `show-tech`.
- `version`: An optional file type version parameter that designates the version in which the file shall be saved. The default is `current`. Valid versions are `candidate`, `current`, `previous`, and `customVersion` (a user-named version).
- `prompt`: Available for SFTP only, this is the password prompt presented by the device to send a password.

For SFTP transfers, additional variable information is required. The SFTP variables are used in the device’s syntax to place macros instead of hard coding names and addresses. Uplogix will replace these at runtime with appropriate substitutes:

- ${user}: The macro to insert the port username into the device’s file transfer command.
- ${pass}: The macro to insert the temporary password available for file transfer to that port.
- ${path}: Temporary file name for transfer to the Local Manager.
- ${ip}: IP address on Uplogix to transfer the file to. Could be subinterface, dedicated or management.

TFTP Example

The first example demonstrates pulling the startup-config from the Extreme switch. Note the use of the `\x22` escape sequence in the command that is used to put the VR-Mgmt parameter in double quotes. Note that `192.0.2.151` is the IP address of the Local Manager.

```
[admin@UplogixLM (port1/1)]# pull tftp "upload log 192.0.2.151 vr \x22VR-Mgmt\x22
Extreme150Log chronological" Extreme150Log show-tech
Pull showTech/current ...
TFTP server at 192.0.2.151:69
Executing: upload log 192.0.2.151 vr \"VR-Mgmt\" Extreme150Log chronological
Received Extreme150Log (47,156 bytes)
MD5: cd607a15b7472c37ea9c8d968ca626a4
```

The next example below demonstrates pulling the running-config from the Extreme switch:

```
[admin@UplogixLM (port1/1)]# pull tftp "upload configuration 192.0.2.151
x150RunningConfig" x150RunningConfig running-config current
Pull runningConfig/current ...
TFTP server at 192.0.2.151:69
Executing: upload configuration 192.0.2.151 x150RunningConfig
Received x150RunningConfig (11,770 bytes)
MD5: dcd44a8490522671addebcd84fc0fdfa
```

The second example demonstrates chaining two commands together with the `\r escape` sequence (for a carriage return) between the commands in order to issue a `show tech` on the Extreme switch and then copy the resulting file to the Local Manager as the current Tech file.

```
[admin@UplogixLM (port1/1)]# pull tftp "show tech all logto file \r tftp put 192.0.2.151
internal-memory show_tech.log.gz" show_tech.log.gz show-tech current
Pull showTech/current ...
TFTP server at 192.0.2.151:69
Executing: show tech all logto file \r tftp put 192.0.2.151 internal-memory
show_tech.log.gz
Received show_tech.log.gz (16,786 bytes)
MD5: 8c36d5aeacf34b9cdb4a75d0467048c2
```

Issue the `show directory` command to see files pulled from the managed device.

```
[admin@UplogixLM (port1/1)]# show directory
Type        Version                     Name
------- ----------            ------------
Config
       Running
          Current                 x150RunningConfig
       Startup
          Current                 x150StartupConfig
OS
          Candidate           summitX-12.4.5.3.xos
Tech*
          Current                 Extreme150Log
          Previous                show_tech.log.gz
* Additional archived versions are available. Execute show dir -v
```

SFTP Example

This example demonstrates pulling the self-signed certificate from a Cisco router using SFTP. Note the use of the `variables` to populate the router's parameters with the Local Manager's information. Since the router needs a carriage return to execute, it is represented with a '\r' at the end of the remote command. We will place the certificate in a named OS object "Cert" since it is a binary file.

```
[admin@UplogixLM (port1/1)]# pull sftp -file IOS-Self-Sig#3737.cer "copy nvram:IOS-Self-Sig#3737.cer scp:\pr${ip}\r${user}\r${path}\r${pass}\r" os  Cert

Pull os/custom ...
SFTP/SCP service at 192.0.2.220:22
Executing: copy nvram:IOS-Self-Sig#3737.cer scp:\r${ip}\r${user}\r${path}\r${pass}\r
Responding to password prompt
SFTP/SCP started
SFTP/SCP done
Transfer complete
```

The next example demonstrates pulling a text file from the router's flash that maintains DHCP address information:

```
[admin@UplogixLM (port1/1)]# pull sftp -file dhcp "copy flash:dhcp-bindings.txt scp:\r${ip}\r${user}\r${path}\r${pass}\r" startup-config dhcp
Waiting for another job to complete
Pull startupConfig/custom ...
SFTP/SCP service at 203.0.1130.100:22
Executing: copy flash:dhcp-bindings.txt scp:\r${ip}\r${user}\r${path}\r${pass}\r
Waiting for SFTP/SCP to start ....Responding to password prompt
SFTP/SCP started
SFTP/SCP done
Transfer complete
```

Issue the `show directory` command to see files pulled from the managed device.

```
[admin@UplogixLM (port1/1)]# show directory
Type     Version               Name
-------  ----------            ------------
Config
      Running
          Current              x150RunningConfig
      Startup
          Current              x150StartupConfig
          dhcp                 dhcp
OS
      Candidate           summitX-12.4.5.3.xos
      Cert                IOS-Self-Sig#3737.cer
Tech*
      Current             Extreme150Log
      Previous                 show_tech.log.gz
```

Issue the `show startup dhcp` command to see content of text files:

```
[admin@UplogixLM (port1/1)]# show startup dhcp
*time* Dec 30 2013 04:17 PM
*version* 4
!IP address     Type  Hardware address   Lease expiration       VRF
203.0.113.169    id    0124.ab81.e070.73  Dec 31 2013 04:03 PM
203.0.113.170    id    0144.4c0c.c049.2e  Dec 31 2013 01:05 PM
203.0.113.171    id    0100.f4b9.6098.c2  Dec 31 2013 03:54 PM
203.0.113.172    id    0130.10e4.84fc.a7  Dec 31 2013 11:02 AM
203.0.113.173    1     fe7b.6609.2770     Dec 31 2013 10:58 AM
```

Push TFTP or SFTP Usage

Use the following command at the Local Manager port prompt to transfer a file from the Local Manager file system to a managed device:

```
push tftp [dedicated] <“remote command”> <transfer filename> <type> [version]

pull sftp [options]   "<remote command>"                     <type> [version]
```

Command parameter definitions:

- `Dedicated`(-dedicated for SFTP) An optional parameter — include this information when you want to move files over a dedicated Ethernet link between the Local Manager and managed device rather than using the management Ethernet interface (i.e. moving files over the LAN).
- `remote command`: The copy command that is issued at the CLI of the managed device to copy a file from the Local Manager to the managed device. This command string can also include embedded escape sequences such as `\r`, which are helpful when the managed device command involves a command dialogue rather than a single command. Refer to the ASCII Escape Sequences section below for more information about escape sequences.
- `transfer filename`(-file for SFTP) The name of the file being pushed/transferred from the Local Manager to the managed device.
- `type`: Indicates the Local Manager file system file type. Valid file types are `running-config`, `startup-config`, `OS`, and `show-tech`.
- `version`: An optional file type version parameter designates the version in which the file shall be pushed/transferred. The default is `current`. Valid versions are `candidate`, `current`, `previous`, and `customVersion` (a user-named version).
- `prompt`: Available for SFTP only, this is the password prompt presented by the device to send a password.

For SFTP transfers, additional variable information is required. The SFTP variables are used in the device’s syntax to place macros instead of hard coding names and addresses. Uplogix will replace these at runtime with appropriate substitutes:

- ${user}: The macro to insert the port username into the device’s file transfer command.
- ${pass}: The macro to insert the temporary password available for file transfer to that port.
- ${path}: Temporary file name for transfer to the Local Manager.
- ${ip}: IP address on Uplogix to transfer the file to. Could be subinterface, dedicated or management.

TFTP Example

The first example chains two commands together (with the `\r escape` sequence for a carriage return between the commands) in order to push a golden running-config file from the Local Manager file system to an Extreme switch and then load it to the running configuration.

Note that `192.0.2.151` is the IP address of the Local Manager.

```
[admin@UplogixLM (port1/1)]# push tftp "tftp get 192.0.2.151 x150RunningConfig.xsf \r
load script x150RunningConfig.xsf" x150RunningConfig.xsf running-config Golden
Push runningConfig/custom ...
TFTP server at 192.0.2.151:69
Executing: tftp get 192.0.2.151 x150RunningConfig.xsf \r load script
x150RunningConfig.xsf
Transfered x150RunningConfig.xsf
```

The second example demonstrates pushing a candidate OS file to an Extreme switch:

```
[admin@UplogixLM (port1/1)]# push tftp "download image 192.0.2.151 summitX-12.4.5.3.xos
secondary \rn\r" summitX-12.4.5.3.xos os candidate
Push os/candidate ...
TFTP server at 192.0.2.151:69
Executing: download image 192.0.2.151 summitX-12.4.5.3.xos secondary \rn\r
Transfered summitX-12.4.5.3.xos
```

SFTP Example

This SFTP example demonstrates pushing a stored firewall configuration to a Linux system:

```
[admin@UplogixLM (port1/5)]# push sftp -dedicated "scp ${user}@${ip}:${path}
/etc/sysconfig/iptables" startup-config iptables
Push startupConfig/custom ...
SFTP/SCP service at 169.254.100.14:22
Executing: scp ${user}@${ip}:${path} /etc/sysconfig/iptables
Responding to password prompt
SFTP/SCP started
SFTP/SCP done
Transfer complete
```

ASCII Escape Sequences

Control characters and special characters that might be necessary as part of a command (or chain of commands) on a managed device can be embedded in the command string the driver executes on the managed device. Any command that requires double quotes must be escaped, as the Uplogix CLI uses double quotes to enclose the command that is to be issued on the managed device. Here are a few useful escape sequences:

Sequence/Characters	Meaning
`\xhh`	ASCII character with hexadecimal value 0x*hh*
`\cX`	Control character corresponding to *X*
`\r`	Carriage return
`\n`	New line
`\t`	Tab character
`\\`	Backslash character

Clearing a previously configured port or slot

When you disconnect a device from a port, the Local Manager retains the device's configuration data. You can clear this data and return the port to its factory default configuration using the `config system clear port` command.

```
[admin@UplogixLM]# port 2/1
 tasman 6300 tios
 tasman
[admin@UplogixLM] (port2/1)]# exit
[admin@UplogixLM]# config system clear port 2/1
Clearing port 2/1 will delete all associated data.
Continue? (y/n): y
port2/1 cleared
```

Navigate to the port to verify that it has been reset to factory defaults:

```
[admin@UplogixLM]# port 2/1
native
```

Use the wildcard character * to clear all ports on the option card. This automatically assumes there are 16 ports on the card, instead of detecting the hardware in use.

```
[admin@UplogixLM]# config system clear port 1/*
Clearing port 1/* will delete all associated data.
Continue? (y/n): y
port1/1 cleared
port1/2 cleared
port1/3 cleared
port1/4 cleared
port1/5 cleared
port1/6 cleared
port1/7 cleared
port1/8 cleared
port1/9 cleared
port1/10 cleared
port1/11 cleared
port1/12 cleared
port1/13 cleared
port1/14 cleared
port1/15 cleared
port1/16 cleared
```

If removing an option card or virtual slot, use the `config system clear slot` command to ensure that the hardware is completely cleared from the database.

```
[admin@UplogixLM]# config system clear slot 4
Slot 4 is about to be cleared.
Do you want to commit these changes? (y/n): y
```

For more on virtual ports and slots, see the Configuring Virtual Ports section.

Configuring virtual ports

There are a variety of cases where typical console device management may be impractical or impossible. For these deployments the Local Manager can be configured to use virtual device management ports. These virtual ports mimic the functionality of the physical serial interfaces on the front of your Local Manager. Some cases where virtual ports are applicable include:

- Manage devices where the distance between the Local Manager and the managed device is too far for a RS 232 serial connection or where there is an inability to run additional cables.
- Manage devices already connected to a console server.
- Manage devices whose serial ports are being used for other purposes.
- Manage devices with IP connectivity but no serial connectivity.
- Manage devices using an Local Manager virtual machine (VM) running on a VMware ESXi server.

This feature requires the purchase of a virtual port license for each virtual port from Uplogix. Licenses are installed on the Control Center. All virtual ports are limited to virtual slot 4 on Uplogix hardware platforms. The maximum number of allowable virtual ports varies on a platform basis as follows:

Uplogix 400	8 virtual ports supported
Uplogix 430	4 virtual ports supported
Uplogix 3200	16 virtual ports supported
Uplogix 500	16 virtual ports supported
Uplogix 5000	16 virtual ports supported

To assure adequate performance on richly configured systems, Uplogix recommends that the sum of configured physical ports and virtual ports not exceed the total number of physical ports supported by the Uplogix platform. It is possible to exceed the recommended maximum port count and not experience degradation in performance – performance will vary based on the amount of monitoring, automation and SLV tests that are configured, and based on the frequency of the monitors and the Local Manager's communication with the Control Center.

While all advanced drivers are configurable on virtual ports that terminate at a console server, Uplogix officially supports only the native, enhanced native, and Cisco IOS device drivers for virtual ports that terminate on the managed device (i.e., VTY/IP connection where no console server is involved).

Virtual ports that terminate on the managed device (i.e., VTY/IP connection where no console server is involved) do not support all of the functionality supported for managed devices that are directly or indirectly connected to the local manager via a serial console port connection. The following driver functionality is not available in this case:

- LAN independence
- Bare metal restore
- ROMmon recovery
- Password/Configuration recovery where boot loader configuration is required
- Power On Self Test (POST) data collection
- Automatic Rollback
- xmodem and ymodem file transfers

The following privileges are required to configure virtual ports:

- `config system slot` – Configure a virtual slot and virtual ports.
- `show system slot` – View virtual slot/port configuration.
- `config system clear slot` – Clear virtual slot configuration.
- `config system clear port` – Clear port/virtual port data from the database.

Configure a virtual port

Use the `config system slot {slot_number}` command to enter the virtual slot configuration editor. Slot 4 is the only virtual slot allowed for Local Manager hardware.

```
[admin@UplogixLM]# config system slot 4
```

Once in the editor, use the `?` command to view a list of possible configuration options.

```
[config system slot 4]# ?
Allowable arguments are:
show
[no] port <number|range> <IP> <TCP port> <ssh|telnet> [-noroute]
config port <number>  (to configure SSH virtual credentials)
or exit to quit config mode
? (to display this help)

Maximum virtual ports supported: <number>

* Note: specify -noroute if the virtual port connection should route over an out-of-band
connection when it is up

Examples:
========
Adding virtual ports:
port 1 192.168.100.20 22 ssh
port 3-8 172.30.100.2 6003 telnet
* Note that additional prompts will appear if the port type is SSH.

Removing virtual ports:
no port 1
no port 3-8
* Note that in some cases, re-configuration of a removed port may require exit and re-entry of
virtual port slot configuration.

Editing SSH virtual port credentials:
config port 2
* You must remove and recreate the SSH virtual port if you want to clear any parameter
* You do not need to enter a password if you are using SSH public key authentication to the
remote device. When using public key authentication, be sure to place the Local Manager public
key in the appropriate location on the managed device prior to configuring the virtual port here.
Use the show system crypto certificate virtual command to display the Local Manager public
key.
[config system slot 4]#
```

Command definitions:

- `show`: Display the current virtual slot/port configuration.
- `[no] port <number | range> <IP> <TCP port> <ssh | telnet> [-noroute]`: Define virtual ports. Use the SSH option to use secure virtual ports. Only add the `–noroute` parameter if the virtual port traffic should be routed over the Local Manager's out-of-band network connection during an in-band network connectivity failure (not typically used, as most use cases call for always routing virtual port traffic over the LAN/in-band network connection on the Local Manager). Use the no option to remove virtual port(s) from the virtual slot.
- config port <number>: Configure SSH authentication credentials for a secure virtual port.
- `Exit`: Exit the configuration editor.

Once the virtual slot has been configured on the Local Manager, create virtual ports for managed devices. Below are a few examples of how to create and map virtual ports to managed devices:

Map virtual port 1 to TCP port 6001 of a console server with an IP address of 192.0.2.101:

```
port 1 192.0.2.101 6001 telnet
```

Map virtual port 2 to SSH TCP port 22 on a managed device with IP address 192.0.2.100:

```
port 2 192.0.2.100 22 ssh
```

Map virtual ports 3 and 4 to TCP ports 6002 and 6003 of a console server with IP address 192.0.2.101 using the range command (assumes contiguous TCP ports).

```
port 3-4 192.0.2.101 6002 telnet
```

To view the virtual slot configuration editor, use the `show system slot {slot_number}` command. Slot 4 is the only virtual slot allowed for Local Manager hardware.

```
[admin@UplogixLM]# show system slot 4
1 192.0.2.101 6001 Telnet
2 192.0.2.100 22 SSH
3 192.0.2.101 6002 Telnet
4 192.0.2.101 6003 Telnet
```

Delete a virtual port

Use the `config system slot {slot_number}` command to enter the virtual slot configuration editor and and the `no port {port_number}` command to delete a particular virtual port.

This example deletes virtual port 2 from virtual slot 4:

```
[admin@UplogixLM]# config system slot 4
[config system slot 4]# show
1 192.0.2.101 6001 Telnet
2 192.0.2.100 22 SSH
3 192.0.2.101 6002 Telnet
4 192.0.2.101 6003 Telnet
[config system slot 4]# no port 2
[config system slot 4]# show
1 192.0.2.101 6001 Telnet
3 192.0.2.101 6002 Telnet
4 192.0.2.101 6003 Telnet
```

```
[config system slot 4]# exit
```

Once a virtual port is deleted, it is necessary to clear the database and dashboard of information associated with the deleted virtual port by using the `config system clear port {port_number}` command as described in the Clearing a previously configured port or slot section.

Configuring power control

Local Managers can use an external power controller in the management and recovery of network devices. To access the `powercontrol` resource, use the `powercontrol` command. If the power controller has not been configured, it must be initialized.

The initialization process is similar to initializing a port. Only the `make` and `OS` are required. The following `makes` are currently supported:

- APC
- Avocent
- BayTech
- Lantronix
- ServerTech

Refer to your power controller’s documentation for OS version and authentication settings.

The Local Manager uses mapped power outlets to cycle power to devices.

```
[admin@UplogixLM]# powercontrol

admin@UplogixLM (powercontrol)]# config init
--- Enter New Values ---
description: Austin Rack 123 Power
make: servertech
model:
os: sentryipt
os version:
console username: admn
console password: ****
confirm password: ****
Serial Bit Rate [9600]:
Serial Data Bit [8]:
Serial Parity [none]:
Serial Stop Bit [1]:
Serial Flow Control [none]:
Do you want to commit these changes? (y/n): y
Testing login will take a few moments...
Login successful; credentials are valid.
Retrieving outlet names.  Please wait...
Outlet names retrieved.
Would you like to add a new mapping? (y/n) [n]: y
Outlet: A1
Interface: port1/1
Would you like to add a new mapping? (y/n) [n]: y
Outlet: A2
```

```
Interface: port1/2
Would you like to add a new mapping? (y/n) [n]: n
Scheduling default jobs
Testing job rulesMonitor
Job rulesMonitor was successful
Job rulesMonitor was scheduled
```

After you configure the outlet mappings, the Local Manager tests its initialization settings. After initialization, you can return to the `powercontrol` resource and edit the power controller's settings:

`config authentication`: Configure the information that the Local Manager uses to login to the power controller.

`config outlets`: Specify the outlets to which managed devices are connected. This enables you to cycle power to a specific device if necessary.

`config serial`: Specify the serial settings for the power controller.

`config info`: Modify information about the power controller such as make, model, OS, and management IP address.

Each of these `config` commands has a corresponding `show` command to view what is currently configured.

Power cycling devices from the port level

Once the outlets have been mapped on a power controller, there are two methods to power on, off or cycle a managed device from the Local Manager. From the port level, use the `power` command:

```
power <on | off | cycle [secondsToWait]>
```

Command Parameters:

- `on`: Power on a managed device
- `off`: Power off a managed device
- `cycle [secondsToWait]`: Power cycle a device with a delay in an integer number of seconds

The second method also uses the `power` command, but is issued from the system level and includes a parameter for the port.

```
power <port #/#> <on | off | cycle [secondsToWait]>
```

Command Parameters:

- `port #/#`: The slot and port number of the managed device where the power event will occur
- `on`: Power on a managed device
- `off`: Power off a managed device
- `cycle [secondsToWait]`: Power cycle a device with a delay in an integer number of seconds

Managing Accounts and Security

This chapter describes how to control access to the Local Manager and covers:

- Managing access and communication — configuring SSH and Telnet protocols; filtering inbound communication by IP address or phone number; locking the front panel keypad to prevent unauthorized changes to the Local Manager
- Managing user and group accounts — creating, updating, disabling, and deleting accounts; setting up alerting
- Managing authentication settings and passwords — setting requirements for passwords; using certificates; using hardware authentication; changing passwords
- Managing roles and privileges — setting user privileges using default roles; tailoring privileges to your requirements

Managing access and communication

This section gives information about the communication protocols that the Local Manager uses, ways to limit incoming communication, and preventing changes from the front panel keypad.

Topics in this section:

- About inbound communication
- About outbound communication
- Configuring SSH security
- Allowing Telnet connections
- Configuring IP address filtering
- Configuring phone number filtering
- Locking the keypad

About inbound communication

By default, only Secure Shell version 2 connections are allowed to communicate with the Local Manager. File servers using TFTP, FTP and SFTP are available for serving files to network devices, but only within specific file transfer operations such as `push OS`, and in many cases that communication is directly limited to a specific IP address or dedicated network connection.

SSH version 2

Secure Shell version 2 is the default user method of communicating with the Local Manager. Users may authenticate using passwords, certificates, or a combination of both. Local Managers recognize both DSA and RSA encryption methods with key length up to 2048 bytes. Encryption is configurable. The default secure shell port (TCP 22) may be changed to any port between 1024 and 10000.

Client SSH applications can be used to access the Local Manager directly. Supported clients include:

- PuTTY
- SSH® Tectia™

- VanDyke® SecureCRT®
- SSHTerm for Windows
- OpenSSH

Secure Copy

The Local Manager can use Secure Copy (SCP) to copy files to and from a server. Based on the Secure Shell framework, SCP can be used via the `copy`, `update`, `export`, and `backup` commands.

FTP

The Local Manager’s FTP client is used by the copy command, export, archive, and backup. FTP is much less secure than SCP and should be used only in completely trusted networks.

The Local Manager’s FTP server is used to transfer files to network devices that support it. The Local Manager limits connections to specific IP addresses documented as device management IP addresses. The FTP server is only available during automated file transfer operations or if manually initiated during terminal pass-through. The server process is automatically terminated to limit possible security exposure.

TFTP

Like the FTP server, the Local Manager’s TFTP server is available only during automated file transfers between network devices and the Local Manager and on manual instantiation. It is not limited to IP addresses; it limits possible security exposure by specifically naming files.

SFTP

Like the FTP server, the Local Manager’s SFTP server is available only during automated file transfers between network devices and the Local Manager and on manual instantiation. It is not limited to IP addresses.

Telnet access

Telnet access to the Local Manager may be enabled, allowing clear-text clients to access the CLI. Port 23 is used by default. After enabling Telnet access, a reboot of the Local Manager is required.

Modem access

Optional modem teletype (TTY) access is available if configured to provide single user dial-in access to the command line with support for encryption. Uplogix recommends using the Local Manager’s outbound PPP/VPN service to reduce the security risks associated with dial-in modems. Refer to Configuring Out-of-Band Communication for more details.

By default, the modem does not answer incoming calls. To enable the dial-in capability, refer to Enabling dial-in and setting answering behavior.

Console access

An on-board RS-232 and mini USB console port is available for local access to the command line. Refer to Chassis views and indicator lights for the connector location.

The connect command

When logged in to one Local Manager, use the `connect` command to connect to another Local Manager’s command line interface. While the protocol uses SSH, this command limits connectivity to only Local Managers, reducing overall security risk. Like all commands, this feature is limited to users authorized to execute it.

```
[admin@UplogixLM]# connect 198.51.100.254
Connecting to 198.51.100.254
```

```
admin's password: ********
Uplogix LMS v4.7.0 24442 -- Powering Business Uptime
-------------------------------------------------------------------------------
Port         Hostname     Status       Con Eth Uptime    Processor    Last
                                                       Utilization    Alarm
---- ------------------ ------------------ --- --- ------- ----------- -------

[output removed]
```

About outbound communication

Most of the Local Manager’s communication is designed to be initiated by the Local Manager, reducing the number of potential security vulnerabilities. These operations are discussed in detail below.

Archiving and exporting

If the Local Manager is managed by a Control Center, the Local Manager periodically archives device statistics, user session log files, device files, and other data automatically to the Control Center using HTTPS over port 8443. Archiving uses high data compression to reduce the impact to the network. When operating out-of-band, archiving is suspended by default until the Local Manager returns to in-band communication. This functionality can be enabled to work when the Local Manager is communicating over its out-of-band connection.

If the Local Manager is not managed by a Control Center, use the `config export` command to create an XML file of the Local Manager's configuration and send it to the IP address of your choice using SCP or FTP. Use the `config system export` command to archive collected device statistics to an external server using FTP or SCP.

Pulse

The Pulse client uses the ECHO protocol (TCP port 7) to determine network availability. TCP ECHO packets are sent every 30 seconds from the management Ethernet port to one or more pulse servers (usually in the Network Operation Center or on the other side of the WAN). The in-band/production network is deemed down after four consecutive ECHO failures from all defined pulse servers, after which the Local Manager can automatically initiate an out-of-band connection over the modem or secondary Ethernet port to reestablish connectivity to the remote site. While out-of-band, the Local Manager routes all traffic over the out-of-band connection except for ECHOs destined for the pulse server and for local traffic as defined by the user with the `config system route` CLI command. The Local Manager will automatically tear down the out-of-band connection and communicate over the in-band/management Ethernet connection when it sees that the in-band network is operational again (determined by five consecutive successful `echo requests`).

Heartbeat

The Local Manager communicates with the Control Center using a proprietary TLS-encrypted protocol that uses TCP port 8443 to provide regular updates that include current device status information, status of scheduled jobs, alarms, events and configuration changes on the Local Manager. The message that is sent by the Local Manger to the Control Center and that is acknowledged by the Control Center is called the heartbeat. The heartbeat contains compressed data to reduce the load on the network and has a 30 second interval by default.

You can change the heartbeat interval and TCP port from the command line using the `config system management` command, or you can change it from the Uplogix web interface on the Server Settings page under Administration.

Network Time Protocol

If this feature is enabled, the Local Manager will synchronize time with a Network Time Protocol (NTP) server using UDP port 123. If the Local Manager is used with the Control Center, it will sync its time over the heartbeat with the Control Center by default. The Local Manager can be configured to sync its time with an NTP server instead of the Control Center using the `config system ntp` command. For information on using an NTP server, refer to Setting date and time.

Configuring SSH security

The Local Manager allows you specify the SSH port, encryption, compression, and key exchange information for SSH sessions using the `config system protocols ssh` command.

```
[admin@UplogixLM]# config system protocols ssh
--- Existing Values ---
sshPort: 22
Preferred Encryption Cipher:3des-cbc
Allow: aes128-cbc
Allow: aes128-ctr
Allow: aes192-cbc
Allow: aes192-ctr
Allow: aes256-cbc
Allow: aes256-ctr
Allow: blowfish-cbc
Allow: cast128-cbc
Allow: twofish128-cbc
Allow: twofish192-cbc
Allow: twofish256-cbc
Preferred HMAC:hmac-sha1
Allow: hmac-md5
Preferred Compression:none
Allow: zlib
Preferred Key Exchange Algorithm:diffie-hellman-group1-sha1
Allow: diffie-hellman-group14-sha1
Change these? (y/n) [n]:
```

Changes to the `config system protocols ssh` settings take effect after you `restart` the Local Manager.

The preferred settings must be specified. During negotiation, the client's preferred settings are given a greater weight then the server's. For example, if you configure your Local Manager with a preferred encryption cipher of 3des-cbc but also allow aes128-cbc, and a client attempts to connect to the Local Manager with a preferred cipher of aes128-cbc, the server will permit the use of the client's preferred cipher — aes-128-cbc — for the SSH session.

The Local Manager's default SSH port can be changed to a non-standard TCP port for enhanced security or for interoperability with your network's firewall by using the `config system protocols ssh` command.

SSH configuration changes affect both the server and client SSH configuration for the Local Manager. These include server processes running on the Local Manager such as sshd daemon and commands such as `connect` and `config import`.

If the Local Manager is managed by a Control Center, SSH protocol can be configured through the Uplogix web interface.

For a single Local Manager: `Inventory > Local Manager page > Configuration menu > Protocols`

For a group of Local Managers: `Inventory > group page > Configuration menu > Protocols`

Allowing Telnet connections

By default, the Local Manager allows users to connect via SSH to TCP port 22 only. The Local Manager can be configured to also allow Telnet connections.

To allow the Local Manager to respond to Telnet requests on TCP port 23, use the `config system protocols telnet enable` command.

> This command takes effect after you `restart` the Local Manager.

If the Local Manager is managed by a Control Center, Telnet protocol can be configured through the Uplogix web interface.

For a single Local Manager: `Inventory > expanded Local Manager page > Configuration menu > Protocols`

For a group of Local Managers: `Inventory > group page > Configuration menu > Protocols`

Configuring IP address filtering

By default, the Local Manager allows access from any IP address; however, access can be restricted to certain IP addresses or networks by using the `config system protocols filter` command. This command opens an editor that allows you to explicitly permit and deny access to source IP addresses and networks.

For example, specify your management subnet or your own computer and then use the `deny all` subcommand to block any IP address not explicitly allowed. This blocks all new communication with the Local Manager that is not sourced from the permitted IP address or network.

The filter automatically adds defined services such as the Control Center, TACACS, RADIUS, and NTP servers, as well as each device's specified management or dedicated IP address to the list of allowed IP addresses.

Filters are applied during both in-band and out-of-band communications.

Use the `allow` and `deny` subcommands to specify networks. Use the `no` modifier to remove previously configured behavior.

```
[admin@UplogixLM]# config system protocols filter
[config system protocols filter]# deny 192.0.2.1
[config system protocols filter]# deny 198.51.100.0/24
[config system protocols filter]# deny 203.2.0.0/16
[config system protocols filter]# deny 203.0.0.0/8
[config system protocols filter]# allow 198.51.100.254
[config system protocols filter]# no allow 198.51.100.254
```

Filtering subtracts the sum of the deny statements from the sum of allow statements.

Filtering only applies to new connections. If you `deny` an IP address while a user at that address has a CLI session open, the connection will not be affected. However, the user will not be able to open a new session.

Filters are applied after you `exit` the editor.

If the Local Manager is managed by a Control Center, IP filtering can be configured through the Uplogix web interface.

For a single Local Manager: `Inventory > Local Manager page > Configuration menu > Protocols`

For a group of Local Managers: `Inventory > group page > Configuration menu > Protocols`

Configuring phone number filtering

By default, the modem refuses all incoming calls. Dial-in capability must be enabled from the command line before use. Refer to Enabling dial-in and setting answering behavior for more information. Use the `config answer` command to specify phone numbers from which the modem will accept calls.

If Caller ID is available, you can allow or deny calls from specific phone numbers. Prefix masking can be used, which allows the following:

- permit or deny all of a given area code, such as 512
- permit or deny numbers beginning with a given string, such as 512555
- permit or deny specific numbers such as 5125551212

```
[config answer]# deny 512
[config answer]# allow 512555
[config answer]# deny 5125551212
```

You may need to configure the modem initialization string to turn on caller ID delivery.

Do not use dashes or dots between numbers.

To remove previously configured behavior, the `no` modifier can be used with most commands.

```
[config answer]# no deny 5125551212
```

The Local Manager relies on Caller ID information to identify incoming calls. If Caller ID is not available, use the `allow all` subcommand to override the default deny.

```
[config answer]# allow all
```

Locking the keypad

After completing basic configuration, you may choose to disable the front panel keypad on the Uplogix 3200 or 5000 using the `config system keypad` command. This prevents configuration changes from the keypad. The restart, shutdown, and factory reset functions remain available from the keypad at all times.

If the Local Manager is managed by a Control Center, the keypad can be locked or unlocked through the Uplogix web interface.

For a single Local Manager: `Inventory > Local Manager page > Configuration menu > LCD`

For a group of Local Managers: `Inventory > group page > Configuration menu > LCD`

Managing user and group accounts

If the Local Manager is not managed by a Control Center the `config user` and `config group` commands allow you to create accounts unique to that Local Manager.

If the Local Manager is managed by a Control Center, the Control Center web interface must be used for the tasks in this section. The `config user` and `config group` commands cannot be used when the Local Manager is under management.

This section covers:

- Viewing user account details
- Viewing groups
- Creating and editing user accounts
- Creating and editing group accounts
- Configuring an account to receive alerts
- Disabling a user's account
- Reactivating a disabled account
- Deleting an account

The `show user` and `show group` commands present account details for individual user accounts and groups, respectively.

Viewing user account details

The `show user` command returns user account details. To view a single user account, specify the username. You can view all user accounts with the `show user *` command.

```
[admin@UplogixLM]# show user ajones
ajones
created 07/15/2011 16:41:34 UTC
password ********
alert eligible * * * * *
timezone US/Central dst
email ajones@xyzco.com
powercontrol - admin
modem - admin
system - admin
port1/1 - guest
port1/2 - guest
```

```
port1/3 - guest
port1/4 - guest
subscribe powercontrol
subscribe modem
subscribe system
subscribe port 1/1
subscribe port 1/2
subscribe port 1/3
subscribe port 1/4
```

If the Local Manager is managed by a Control Center, user accounts can be viewed through the Uplogix web interface:

`Administration > Users`

Viewing groups

To display all groups, use the `show group` command. To view a specific group, use `show group <groupname>`.

```
[admin@UplogixLM]# show group southwestOps
southwestOps
created 07/10/2007 18:01:16 UTC
description southwest region ajoness
email southwest_ops@xyzco
start 20-07-15 00:00:00.0
expire 2009-12-31 23:59:59.0
Group is currently INACTIVE
user  amarvin
user  ajones
user  lprosser
user  fchurch
powercontrol - guest
modem - guest
system - guest
port1/1 - guest
port1/2 - guest
port1/3 - guest
port1/4 - guest
```

If the Uplogix system is managed by a Control Center, group accounts can be viewed through the Uplogix web interface:

`Administration > Groups`

Creating and editing user accounts

The `config user` command opens an editor that allows you to create and edit user accounts. Information in the user's account may include password, account start and end dates, permissions, alert subscriptions and allowable times to receive alerts, and email address for receiving alerts.

> If the Local Manager is managed by a Control Center, user accounts must be managed through the Control Center web interface. `Administration > Users` provides access to user account management functions. Refer to the *User's Guide for the Uplogix Control Center*.

To edit a user account, use the `config user <username>` command. If the specified username does not exist, the Local Manager prompts you to create it.

User and group names must be unique. For example, if there is a group account called `sysadmin` on the Local Manager, you cannot create a user account called `sysadmin`.

In the examples in this section, we create and configure a user account called `ajones`.

```
[admin@UplogixLM]# config user ajones
User ajones does not exist. Create (y/n): y
[config user ajones]#
```

Usernames are case-sensitive.

Type `?` to see a list of configurable settings. Type `show` to view the user's current settings.

```
[config user ajones]# ?
Allowable arguments are:
alert eligible
alert frequency
alert threshold
show
[no] description
[no] disabled
[no] email
[no] system
[no] expire
[no] password
[no] all
[no] label <label name>
[no] modem
[no] port #/#
[no] powercontrol
[no] authorized keys
[no] start
[no] subscribe
[no] timezone
or 'exit' to quit config mode
```

Password

To log in, users need either passwords or SSH certificates. You can set a password within the `config user` editor with the `password` subcommand:

```
[config user ajones]# password pass02
```

Passwords are case-sensitive.

> If another user views your session using the `show session` command, the `config user` interaction will be displayed exactly as it appears to you, including any password that you set. In no other case is the password ever displayed in clear text. For security purposes, set or change the password using the `config password` command after you exit the `config user` editor.

Users can change their own passwords with the `config password` command. Refer to Changing an account password for more information.

> Do not create a password that ends with the space character. When you attempt to log in using a password that ends with a space, the Local Manager strips the space character and the login fails.

Authorized keys

SSH certificates may be used instead of passwords. They are also used in place of locally cached passwords if remote authentication servers are unavailable.

Multiple certificates may be added to the authorized keys field of a user’s account, but each must be pasted in a single contiguous line.

```
[config user ajones]# authorized keys
Each key must be on its own line. Type 'exit' on a line by itself to exit
[config user ajones authorized keys]# ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAm4lEK0c73bkTgKMw46P0K2gf08ahRc4LfmmLQW8bhOm8wa0XKNAQYVvhrI0zY
ojcM8dKETaOvgMvrdK7kNWMOmcFbNJbRfxlw8mO0NF0Btnf5qZA7oLOtBieNj2Sxeg/lCZCNym9GYMPVmBoZlxHIp
baCacLjMCxMZpMxE7mQUM= ajones
[config user ajones authorized keys]#
[config user ajones authorized keys]# exit
[config user ajones]#
```

Both RSA and DSA certificates can be used.

Certificate format varies widely among SSH clients. Each vendor’s documentation should be consulted to determine which key formats and encryption algorithms are available.

Disabled

To suspend a user's account without deleting the account information, use the `disabled` subcommand. For more information on disabling and reactivating accounts, refer to Disabling a user's account and Reactivating a disabled account for more information.

Alert eligibility and frequency

The eligibility setting is used to restrict alert messages to specified times. The Local Manager determines who will receive alert emails based on the eligibility setting as well as frequency and subscription settings. The setting uses a CRON formatted string. For example, this command:

```
[config user ajones]# alert eligible 0 22-08 * * 1-5
```

would send alert emails to user `ajones` between 10:00 p.m. UTC to 8:00 a.m. UTC, Monday through Friday.

When the Local Manager has an alert email to send, it will check the alert frequency settings of eligible users. If the user has been alerted within the time set as the alert frequency, the message will not be sent. This setting represents a time frame in which the Local Manager will not send more than one alert.

For example, to limit alerts to no more than one every 10 minutes, use the `alert frequency` subcommand:

```
[config user ajones]# alert frequency 10
```

Time zone

Time and date reporting can be customized for each user. The `timezone` subcommand takes a single argument that represents the user's time offset from UTC. The additional parameter `no dst` can be added if the user's location does not observe daylight savings time.

```
[config user ajones]# timezone -6
```

Email

To receive alert messages, a user must have a valid email address set.

```
[config user ajones]# email ajones@xyzco.com
```

You can set more than one email address and you can specify when the Local Manager uses an address — only when the Local Manager is operating in-band or only when it is out-of-band. If you do not specify `in-band` or `out-of-band`, the Local Manager uses the address in both situations.

```
[config user ajones]# email ajones@xyzco.com in-band
[config user ajones]# email alerts@xyzco.com out-of-band
```

For more information about alerting, refer to Configuring an account to receive alerts.

Description

You can set a description for the user by using the `description` command.

```
[config user ajones]# description A. Jones- Network Analyst
```

Roles and resources

By default, users have no privileges on any resource. Privileges are defined by roles, which are tables of permitted commands. Privileges are granted by assigning appropriate roles on the desired resources to define what the user can do on each resource.

The `config user` command allows user privileges to be customized. The first argument is the resource, followed by a role. The `no` modifier can precede the command to remove privileges.

```
[config user ajones]# system guest
[config user ajones]# port 1/1 guest
[config user ajones]# port 1/2 admin
[config user ajones]# port 1/3 guest
[config user ajones]# no port 1/4
[config user ajones]# powercontrol guest
[config user ajones]# modem guest
```

> The admin role (separate from the admin user account) has access to every available command except the config reinstall command that is used to factory reset the Local Manager. To manage the Local Manager, at least one user account must be assigned the admin role unless the Local Manager is being managed by a Control Center.

For more information about using roles, refer to Assigning roles.

Subscriptions

An alert is an alarm that is emailed to subscribed users. Subscriptions allow you to direct alerts to the appropriate personnel.

To receive alerts, users must subscribe to resources they are interested in. To receive all alerts from the Local Manager, use the subscribe all command. Users can subscribe to individual resources as well as interfaces on managed devices.

```
[config user ajones]# subscribe port 1/1
[config user ajones]# subscribe system
[config user ajones]# subscribe port 1/3 chassis
[config user ajones]# subscribe port 1/4 interface Serial0/0
[config user ajones]# subscribe port 1/4 interface Serial0/1
```

For more information about alerting, refer to Configuring an account to receive alerts.

Start and expire dates

By default, user accounts are valid indefinitely; however, they can be set up to begin and end at predefined dates and times. The start and expire subcommands are used to define the date range. Accounts are active only during the defined period. The account must be active for the user to log in or execute commands. The Local Manager can be configured to send an alert to the user when the account expires.

The start and expire commands take date and time as an argument in MMDDYYYYHHMMSS format.

```
[config user ajones]# start 06212012000000
[config user ajones]# expire 12312014235959
```

This example activates the account on June 21, 2012. The account expires at the end of 2014. Note that start and expire dates use UTC time; if this user is in the Central time zone in the USA, the account will expire at 6 p.m. local time on December 31, 2014.

Start and expire settings can be removed with the no modifier.

```
[config user ajones]# no start
[config user ajones]# no expire
```

Review a user account after making changes

To verify a user account's configuration, use the show subcommand while in the user editor. For this example, we have set this user's role to analyst on all resources.

```
[config user ajones]# show
ajones
created 06/18/2013 22:17:52 UTC
description A. Jones- Network analyst
start 06/21/2013 00:00:00 UTC
User is currently INACTIVE
password ***********************
alert frequency 10m
alert eligible 0 22-08 * * 1-5
```

```
timezone US/Central dst
email ajones@xyzco.com
powercontrol - analyst
modem - analyst
system - analyst
port1/1 - analyst
port1/2 - analyst
port1/3 - analyst
port1/4 - analyst
subscribe powercontrol
subscribe modem
subscribe system
[output removed]
```

If the Local Manager is managed by a Control Center, user accounts can be viewed through the Uplogix web interface:

`Administration > Users`

Creating and editing group accounts

Groups are made up of a combination of applied roles, users, and effective times. They can be used to manage authority for a number of users at the same time.

> If the Local Manager is managed by a Control Center, group accounts must be managed through the Uplogix web interface. `Administration > Groups` provides access to group account management functions. Refer to the *User's Guide for the Control Center*.

To create a group, use the interactive `config group <groupname>` command. This opens an editor that allows set up of the group's attributes.

```
[admin@UplogixLM]# config group AustinNOC
Group AustinNOC does not exist. Create (y/n): y
[config group AustinNOC]# ?
Allowable arguments are:
show
[no] description
[no] email
[no] system
[no] expire
[no] group
[no] modem
[no] port #/#
[no] powercontrol
[no] start
[no] subscribe
[no] user or 'exit' to quit config mode
```

Account names must be unique. For example, if there is a user account called `sysadmin` on the Local Manager, you cannot create a group account called `sysadmin`.

If the Local Manager is managed by a Control Center, group accounts can be edited through the Uplogix web interface:

`Administration > Users`

Description

To set a description for the group, use the `description` subcommand.

```
[config group AustinNOC]# description The NOC Group in Austin
```

Email

To set a group email address, use the `email` subcommand.

```
[config group AustinNOC]# email AustinNOC@xyzco.com
```

Roles and resources

By default, groups have no privileges on any resource. Privileges are defined by roles, which are tables of permitted commands. Privileges are granted by assigning appropriate roles on the desired resources to define what the group can do on each resource. Users in a group inherit the group's assigned privileges.

The `config group` command allows group privileges to be customized. The first argument is the resource, followed by a role. The `no` modifier can precede the command to remove privileges.

```
[config group AustinNOC]# port 1/1 guest
[config group AustinNOC]# no port 1/4 guest
[config group AustinNOC]# port 1/2 guest
[config group AustinNOC]# port 1/2 admin
[config group AustinNOC]# system admin
```

For more information about using roles, refer to Assigning roles.

Start and expire dates

Group accounts may have effective dates, just like user accounts. The `start` and `expire` subcommands take date and time as an argument in `MMDDYYYYHHMMSS` format.

```
[config group AustinNOC]# start 01012012000000
[config group AustinNOC]# expire 12312013235959
```

Start and expire settings can be removed with the `no` modifier.

```
[config group AustinNOC]# no start
[config group AustinNOC]# no expire
```

Adding and removing users

To add users to a group, use the `user <username>` subcommand.

```
[config group AustinNOC]# user dsmith
```

To remove users from a group, use the `no` modifier with the `user <username>` subcommand.

```
[config group AustinNOC]# no user dsmith
```

Configuring an account to receive alerts

An alert is an alarm that is emailed to subscribed users. To receive alerts:

- The Local Manager must be configured to use a mail server, refer to Setting originating email address and SMTP server for alerts.
- You must have a user account.
- Your user account must include at least one email address.
- You must be subscribed to the alerts you wish to receive.

Use the `config user` editor to define subscriptions using the `subscribe` command. This allows you to direct alerts to the appropriate personnel.

To subscribe a user to alerts from all resources, use the `subscribe all` subcommand.

In the following example, D. Smith will receive all alerts.

```
[config user dsmith]# subscribe all
```

In the following example, D. Smith will receive alerts from port 1/2, the port 1/3 chassis, the power controller, and the Local Manager.

```
[config user dsmith]# subscribe port 1/2
[config user dsmith]# subscribe port 1/3 chassis
[config user dsmith]# subscribe powercontroller
[config user dsmith]# subscribe system
```

D. Smith may choose to limit alerts to specific interfaces that are being monitored on a managed device as follows:

```
[config user dsmith]# subscribe port 1/4 interface Serial0/0
[config user dsmith]# subscribe port 1/4 interface Serial0/1
```

The account can be configured to receive alerts at separate email addresses during in-band and out-of-band operation. Use the `config user` command to set the user's email addresses with either the `in-band` or `out-of-band` parameter:

```
[config user dsmith]# email dsmith@xyzco.com in-band
[config user dsmith]# email alerts@xyzco.com out-of-band
```

Setting up different in-band and out-of-band email addresses provides an indication of whether the Local Manager is operating out-of-band, and can allow you to receive alerts through a different email account if your work email account is unavailable because of a network outage.

> The Local Manager does not email alerts if a session is in progress. If alarms occur, they are only emailed after all users have logged out or their sessions have timed out.

The Local Manager aggregates alarms and sends alerts by SMTP-based email every two minutes during an outage. Data from each alarm is included in CSV format.

For more information on using the subscribe command to receive alerts, refer to the *Reference Guide for Uplogix Local Managers*.

Although you do not receive alerts while you are logged into the Local Manager, alarms continue to be logged on the Local Manager and to stream to a syslog server if one is configured. If the Local Manager is managed by a Control Center, alarms continue to be updated there as well.

If you log out while there are current alarms, the Local Manager displays the current alarms and prompts you whether to delay alerts or restart them immediately. You may specify a time to delay alerts in hours or minutes. The delay may be up to two hours.

If the Local Manager is managed by a Control Center, you can set up subscriptions to alerts through the Uplogix web interface:

```
Administration > Users > {User Name} > Alert Subscriptions
```

Disabling a user's account

To disable a user's account without deleting it, open the user account editor with the `config user` command. The subcommand `disabled` preserves the account information while rejecting attempts to log in with that user's credentials.

```
[admin@UplogixLM]# config user ajones
[config user ajones]# disabled
[config user ajones]# exit
```

To verify that the account has been suspended, execute the `show user` command:

```
[admin@UplogixLM]# show user ajones
ajones
created 06/15/2007 16:41:34 UTC
User is currently INACTIVE
password *********************
alert eligible * * * * *
timezone US/Central dst
email ajones@company.com
[Output removed]
```

The account is shown as INACTIVE.

If the Local Manager is managed by a Control Center, user accounts must be managed through the Uplogix web interface:

```
Administration > Users {User Name} > Disabled checkbox
```

Reactivating a disabled account

To reactivate an account that has been disabled, open the user account editor with the `config user` command. The subcommand `no disabled` reactivates the account. However, the user account is still subject to its start and expire dates.

```
[admin@UplogixLM]# config user ajones
[config user ajones]# no disabled
[config user ajones]# exit
```

The `show user` command lets you verify that the account is no longer inactive.

```
[admin@UplogixLM]# show user ajones
ajones
created 06/15/2007 16:41:34 UTC
password *******************
alert eligible * * * * *
timezone US/Central dst
email ajones@company.com
```

If the Local Manager is managed by a Control Center, user accounts must be managed through the Uplogix web interface:

```
Administration > Users > {User Name} > Disabled checkbox
```

Deleting an account

When you remove an account, all the account information is deleted. An alternative for user accounts is to disable the account, which allows you to prevent access while preserving the account information.

To delete user account information, use the `no` modifier with the `config user` command.

```
[admin@UplogixLM]# config user no ksmith
```

To delete a group, use the `no` modifier with the `config group` command.

```
[admin@UplogixLM]# config group no DallasNOC
Group DallasNOC deleted from Uplogix
```

If the Local Manager is managed by a Control Center, user and group accounts must be managed through the Uplogix web interface.

To delete a user account:

`Administration > Users`

To delete a group account:

`Administration > Groups`

Managing authentication settings and passwords

This section provides information about user passwords, SSH certificates, and hardware authentication. Topics include:

- Configuring authentication and account settings
- Using TACACS/RADIUS to manage privileges
- About SSH certificates
- Changing an account password
- Changing the admin account's password

Configuring authentication and accounting settings

For security, individual users should be assigned unique usernames, passwords, and authority. Accounting and user authentication may be managed locally on the Local Manager, centrally on the Control Center, or remotely on an external RADIUS or TACACS server.

The settings in this section are presented in the interactive `config system authentication` command.

With the exception of the admin user, all local users are deleted when an Local Manager is placed under management of a Control Center. Maintain the admin user's local modifications, if any exist, using the AAA settings on the server. Users and groups on the server are globally unique and are applied to all Local Managers. Refer to the *User's Guide for the Uplogix Control Center*.

TACACS and RADIUS servers can be used for authentication, authorization and accounting. For more information about how to use TACACS for authorization, refer to Using TACACS/RADIUS to manage privileges.

If the Local Manager is managed by a Control Center, authentication settings can be configured through the Uplogix web interface:

```
Administration > AAA Settings
```

Authentication type

Available options are `local`, `tacacs`, and `radius`. These are case-sensitive. Some of the command prompts depend on the authentication type you specify.

Limit maximum concurrent sessions

Sessions can be limited to one per login or to any number you specify.

Authentication method

This option is displayed if the authentication type is set as `tacacs` or `radius`. Supported authentication methods include `PAP`, `CHAP`, and `MS-CHAP`.

Accounting type

This option is displayed if the authentication type is set as `tacacs` or `radius`. The auditing feature can send executed commands to an accounting server. Choose `start-stop` to send audits before and after each command, `stop-only` to send audits only after commands, or `none` for no auditing.

RADIUS accounting can only be used with RADIUS authentication and TACACS accounting can only be used with TACACS authentication.

Use RADIUS/TACACS authorization

This option is displayed if the authentication type is set as `radius` or `tacacs`. The local permission scheme can be overridden by using RADIUS or TACACS as an authorization source respectively.

Create users

This option is displayed if the authentication type is set as `tacacs` or `radius`. If a user successfully authenticates with an external authentication source, but does not exist on the Local Manager, a user account can be automatically created. This option is disabled by default.

Cache passwords

This option is displayed if the authentication type is set as `tacacs` or `radius`. The Local Manager can be configured to save passwords if the user authenticates successfully with an external server. The password is written to their user account and synchronized throughout the deployment.

This feature can be used in conjunction with “If server is down, use local authentication” to provide failover protection in case of a network outage.

If server is down, use local authentication

This option is displayed if the authentication type is set as `tacacs` or `radius`. The Local Manager can fall back to local authentication if it cannot contact the authentication server. If `Cache Passwords` is enabled, users will be able to log in with their TACACS or RADIUS passwords, provided their passwords were cached during a previous login. If `Cache Passwords` is not enabled, a local, secondary password can be added to user accounts for use during a network outage.

Authentication host IP, accounting host IP

These options are displayed if the authentication type is set as `tacacs` or `radius`. Enter the IP addresses of the authentication and accounting servers as prompted.

Up to four authentication servers and four accounting servers can be specified for redundancy.

Successful authentication requires an affirmative response from one of the configured servers. If a server fails to respond, the next server is queried. An unresponsive server is not treated as a failed authentication; however, if a server responds and fails the authentication, the user will be denied access.

Shared secret

This option is displayed if the authentication type is set as `tacacs` or `radius`. Enter and confirm the shared secret for each server to enable communication with the server.

Authentication and accounting ports

This option is displayed if the authentication type is set as `tacacs` or `radius`. Specify the port number of each authentication and accounting server to which the Local Manager should connect. The default port for TACACS is 49, while the default port for RADIUS is 1812.

Use strong password

To enhance security, you can require users to choose strong passwords based on restrictions you specify:

```
 Use strong passwords: (y/n) [n]: y
Require mixed case: (y/n) [n]:
Require numbers and punctuation: (y/n) [n]:
Reject variation of login id: (y/n) [n]:
Reject word in dictionary: (y/n) [n]: y
    Reject standard substitutions (@ for a, 3 for e, etc): (y/n) [n]:
Reject sequences in numbers or letters (qwerty): (y/n) [n]: y
Reject previous password: (y/n) [n]: y
    Number of previous passwords to check [1 to 20]: [6]: 6
Reject single character difference from previous password: (y/n) [n]: y
Enforce minimum password length: (y/n) [n]: y
    Minimum password length: [6]: 8
```

`Require mixed case` — password must have both capital and lowercase characters. Valid password example: `PassWord`

`Require numbers and punctuation` — password must include at least one numeral and at least one symbol. Valid password example: `P@ssW0rd`

`Reject variation of login id` — password must not be a simple variation of the login id

`Reject word in dictionary and reject standard substitutions (@ for a, 3 for e, etc.)` — if both are selected, users may not set passwords such as p@$$w0rd. Valid password example: `P&ssW*r#`

`Reject sequences in numbers or letters` — users may not set passwords that consist of all the letters or numbers on one row of the keyboard, in sequence either from left to right or right to left, or a character string that contains such a sequence. Broken sequences such as `abc!defg` or `qwerty12` may be used.

`Reject previous password and number of previous passwords to check` — obvious variations on the previous password will be rejected. The following examples assume that the previous password was `P@ssW0rd`.

- change of case only; `p@SSw0rD` will be rejected

- reversed character sequence; `dr0Wss@P` will be rejected
- doubled sequence; `P@ssW0rdP@ssW0rd` will be rejected
- string containing the earlier password; `myP@ssW0rd!` will be rejected

`Reject single character difference from previous password` — when changing a password, at least two characters must be changed.

Once strong passwords are implemented, failed login attempts will extend the time between retries to defer dictionary attacks.

Expire password

You can specify a time limit for passwords and have them expire automatically. If a user logs in using an expired password, the Local Manager allows the login and immediately prompts the user to set a new password.

Number of invalid attempts before lockout

Enable lockout by specifying the maximum number of times a user can attempt authentication before the Local Manager refuses further attempts. Setting lockout to `0` disables lockout protection. If lockout is enabled, the Local Manager prompts to specify the number of minutes the user will be locked out. The default lockout time is 30 minutes.

Using TACACS/RADIUS to manage privileges

Setting up the Local Manager to delegate group membership to a TACACS ACL or RADIUS Group allows the server to manage Uplogix authorization. Groups are assigned permissions to resources and group members are added when the attributed is sent in the TACACS or RADIUS authentication response. To use this feature, set up the group on the Local Manager and on the TACACS server.

These steps are described in detail below.

If AAA functions are delegated to an external server, create a user with the `admin` role on the Local Manager and add that account on the external server beforehand. If no user has the `admin` role on the Local Manager, the administration functions are not accessible.

Set up TACACS authorization

Configure authorization using the `config system authentication` command. Make the following changes:

- Set authentication type as `tacacs`.
- For authentication method, enter `pap`, `chap`, or `ms-chap`, as appropriate.
- Answer `y` to the `Use TACACS Authorization` prompt.
- Usernames and attributes created on the Local Manager or UCC will be added to the specific groups for the user’s session duration. If users are not defined in the Local Manager beforehand a successful authentication can create the account. Answer `y` to the `Create users` prompt.
- Optionally, answer `y` to the `Cache Passwords` prompt to persist TACACS created usernames and group membership. This will ensure that users will still receive the correct privileges if the TACACS server is offline during the next authentication/authorization.
- Enter the IP address, port, and shared secret for each TACACS server. You may specify up to four servers.

```
[admin@UplogixLM]# config system authentication
--- Existing Values ---
(output removed)
--- Enter New Values ---
Authentication type: [local]: tacacs
Authentication method: [pap]:
Accounting type: [none]:
Use RADIUS/TACACS Authorization: (y/n) [n]: y
Create users: (y/n) [n]: y
Cache passwords: (y/n) [n]: y
If server is down, should the system use local authentication: (y/n) [n]: y
(output removed)
```

Set up RADIUS authorization

Configure authorization using the `config system authentication` command. Make the following changes:

- Set authentication type as `radius`.
- For authentication method, enter `pap`, `chap`, or `ms-chap`, as appropriate.
- Answer `y` to the `Use RADIUS Authorization` prompt.
- Usernames and attributes created on the Local Manager or UCC will be added to the specific groups for the user’s session duration. If users are not defined in the Local Manager beforehand a successful authentication can create the account. Answer `y` to the `Create users` prompt.
- Optionally, answer `y` to the `Cache passwords` prompt to persist RADIUS created usernames and group membership. This will ensure that users will still receive the correct privileges if the RADIUS server is offline during the next authentication/authorization.
- Enter the IP address, port, and shared secret for each RADIUS server. You may specify up to four servers.

```
[admin@UplogixLM]# config system authentication
--- Existing Values ---
(output removed)
--- Enter New Values ---
Authentication type: [local]: radius
Authentication method: [pap]:
Accounting type: [none]:
Use RADIUS/TACACS Authorization: (y/n) [n]: y
Create users: (y/n) [n]: y
Cache passwords: (y/n) [n]: y
If server is down, should the system use local authentication: (y/n) [n]: y
(output removed)
```

Create a role to apply the desired privileges

If necessary, use the `config role` command to edit or create a role with the privileges that you want to assign. Depending on your organization's needs, you may be able to use an existing role. For more about roles, refer to Managing roles and privileges.

Create a group

If necessary, use the `config group` command to create a group.

Use the `system`, `port`, `modem`, and `powercontrol` subcommands as needed to apply the role containing the desired set of permissions.

Users will be added to the group each time a successful authentication occurs.

Associate the ACL to users on the TACACS Server

The examples below demonstrates how to create new users or add the ACL to existing users. Refer to your TACACS administrator's guide for more specific examples of configuration required for this functionality.

Creating a TACAS User

To create TACACS users:

- On the TACACS server, create users.
- For each user, specify the ACL with the name of the group created on the Local Manager.

Enabling Authorization on a TACACS User

To enable authorization on an existing TACACS user:

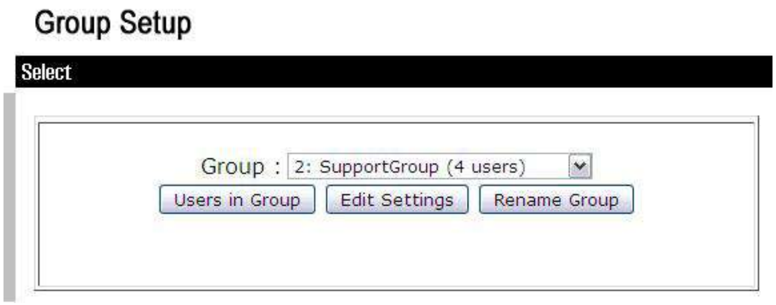
- Once the user is created and is able to authenticate to the Local Manager, add authorization by adding an ACL under the Exec service in your user or group.
- In most Unix TACACS deployments, you can edit the users file and add the following lines to either the group or the user:

```
service = exec {
acl = <acl name set for the group(s)>
}
```

Enabling Authorization on a TACACS User with Cisco ACS

To enable authorization on an existing TACACS user with Cisco ACS:

- On your ACS, create a group for your users and then edit it by clicking Edit Settings.

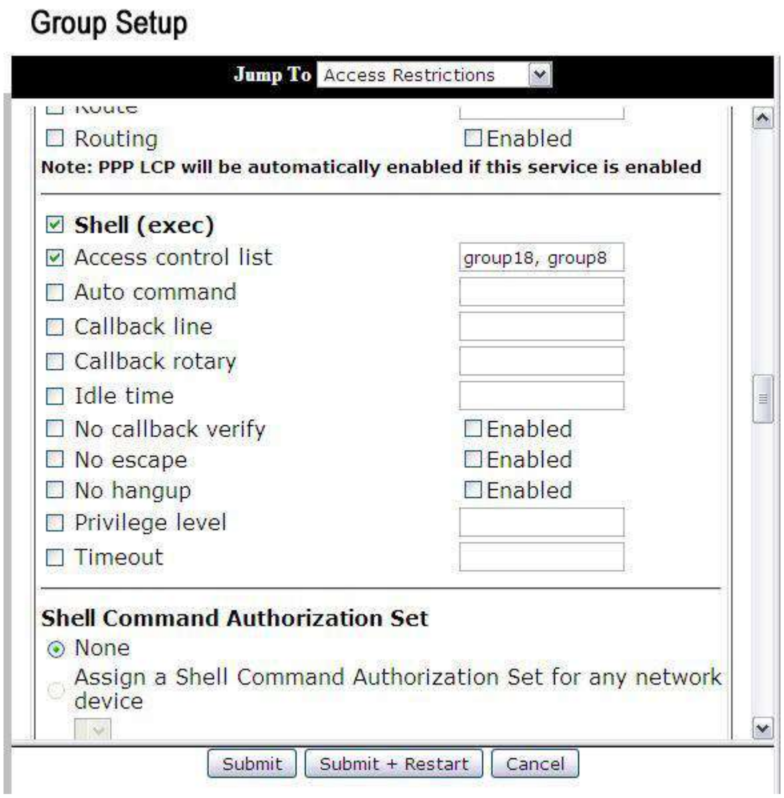


Group Setup

Select

Group : 2: SupportGroup (4 users)

- Then edit that group to include the following options: Shell (exec) and Access control list.



□ Route

□ Routing □Enabled

Note: PPP LCP will be automatically enabled if this service is enabled

☑ **Shell (exec)**

☑ Access control list group18, group8

□ Auto command

□ Callback line

□ Callback rotary

□ Idle time

□ No callback verify □Enabled

□ No escape □Enabled

□ No hangup □Enabled

□ Privilege level

□ Timeout

Shell Command Authorization Set

● None

○ Assign a Shell Command Authorization Set for any network device

- Add a list of groups that you wish your users to be a part of, and then click Submit + Restart.

Associate Uplogix Groups with users on the RADIUS Server

Create new users or add the ACL to existing users.

- The RADIUS Vendor specific attribute (VSA) "Uplogix-Version" is used to configure information specific to Uplogix.
- A new field called "Uplogix-User-Groups" in the VSA to hold a user's group information should be created.
  - The field can contain a single group name or comma-separated list of groups.
  - The group names must be established and configured on the Uplogix system separately from the RADIUS configuration.
  - On successful login on RADIUS, the VSA for Uplogix will be returned with the RADIUS response to the Uplogix device.

These steps are described in detail below.

- The Radius Dictionary contains these fields and is also available from the Uplogix support site.

```
Uplogix          10243
BEGIN VENDOR     Uplogix
ATTRIBUTE        Uplogix Version        1    string
ATTRIBUTE        Uplogix User Groups    3    string
ATTRIBUTE        Uplogix CLI Command    4    string
ATTRIBUTE        Uplogix Envoy Serial   5    string
ATTRIBUTE        Uplogix Task ID        6    string
END VENDOR       Uplogix
```

About SSH certificates

SSH certificates may be used instead of passwords. When configured, they override TACACS and RADIUS authentication. Local authorization must be configured since there is no TACACS or RADIUS query to determine privileges. Both RSA and DSA certificates can be used.

Certificate format varies widely among SSH clients; refer to the vendor's documentation to determine which key formats and encryption algorithms are available.

A combination of certificates and passwords are provided by requiring a password to use a certificate. This password is managed by the certificate store, not by the Local Manager.

To configure an account to use SSH certificates, specify `authorized keys` in the `config user` editor. Refer to Creating and editing user accounts for more information.

If the Local Manager is managed by a Control Center, SSH certificates can be configured through the Uplogix web interface:

```
Administration > Users
```

Changing an account password

To change your own password, use the `config password` command. The CLI prompts you to enter and then confirm your new password. Depending on your role, you may be prompted for your old password.

```
[ajones@UplogixLM]# config password
Old Password: ********
New Password [********]: *********
Confirm Password: *********
Password changed.
```

Do not create a password that ends with a space character. When you attempt to log in using a password that ends with a space, the Local Manager strips the space character and the login fails.

If you have the `admin` or another role that allows use of the `config password` command on the system resource, you can use the `config password` command to change another user's password. In this example, the user `dsmith` changes the password for user `ajones`.

```
[dsmith@UplogixLM]# config password ajones
New Password: ********
Confirm Password: ********
Password changed.
```

The `config user` editor allows you to change a user's password also. This is not recommended, as the password is set using a subcommand in the editor that does not mask the password. If a user reviews your session using the `show session` command, the password set using this method displays in clear text.

If the Local Manager is managed by a Control Center, user accounts (including passwords) must be managed through the Control Center web interface:

```
Administration > Users
```

The exception is that when a user logs into the Local Manager with an expired password, the Local Manager prompts for a new password regardless of whether it is managed by a Control Center.

Changing the admin account's password

To ensure system security, change the admin user's password after logging in for the first time. The admin user cannot be deleted and has access to all commands, unless explicitly managed from the Control Center.

To change the admin user's password, use the `config password` command.

If the Local Manager is managed by a Control Center, the admin user can be managed through the Uplogix web interface:

`Administration > AAA Settings > Manage ‘admin’ user checkbox`

Managing roles and privileges

Local Managers allow you to control exactly which commands a user can run on each resource. This section discusses how to manage user privileges.

Topics in this section include:

- Using roles to limit user activities
- Predefined roles
- Creating and editing roles

Using roles to limit user activities

The Local Manager restricts access to features based on user privileges. All aspects of working with the Local Manager and the equipment it manages are affected by account privileges.

By default, user and group accounts have no privileges. When you create an account, you must explicitly assign roles on the resources on which the user or group needs access. Refer to Assigning roles.

If the Local Manager is managed by a Control Center, you can manage roles through the Uplogix web interface.

For a single Local Manager: `Inventory > Local Manager page > Configuration menu > Roles`

For a group of Local Managers: `Inventory > group page > Configuration menu > Roles`

Definitions

Permissions, roles, and privileges are defined as follows:

- `permission` — ability to use a specific command; can be allowed or denied
- `role` — a named set of permissions, such as `admin`
- `privilege` — a role assigned to a group or specific user account for a specific resource, such as `system admin` or `port 1/2 guest`

If your privileges on a specific resource do not allow you to use a specific command, the Local Manager will return a message stating the command was not found.

If you have no privileges on a specific resource, you will be unable to navigate to that resource. The example below shows the result when a user with no privileges on port 1/1 tries to navigate to port 1/1.

```
[ajones@UplogixLM]# port 1/1
port 1/1 is not available.
```

Predefined roles

The following predefined roles are available:

- `admin` — all command permissions available on the resource to which the role is applied; this role cannot be edited or deleted
- `guest` — view some basic information, such as alarms, status, and version

By default, the admin user account has the admin role on all resources.

Examples

The example below shows how roles affect what users can do. First, the admin user issues the `config system ip` command. Since the admin user has the admin role on the system resource, this command is permitted.

```
[admin@UplogixLM]# config system ip
--- Existing Values ---
Use DHCP: Yes
Management IP: 192.0.2.109
Host Name: UplogixLM
Subnet Mask: 255.255.255.0
Broadcast Address: 192.0.2.255
Default Route: 192.0.2.254
Speed/duplex: auto:100full
DNS Server:
MAC Address: 00:0F:2C:00:02:BF
Change these? (y/n) [n]: y
```

User `cclark` has the guest role on the system resource. This role does not include the `config system ip` permission.

```
[cclark@UplogixLM]# config system ip
Command 'system' not found.  Type ? for help.

[cclark@UplogixLM]# config system ?
Command 'system' not found.  Type ? for help.
```

User `cclark` cannot execute the `config system ip` command, or any other `config system` subcommand, so the command line responds as if the command did not exist and it is not displayed.

Use the `config role` command to create custom roles that give users exactly the permissions you want. Refer to Creating and editing roles for more information.

Assigning roles

To define what a user or group can do, specific roles must be assigned on specific resources using the `config user` or `config group` command. Assign any role that has been defined. In this example, we assign user `dsmith` the admin role on the system resource, and the guest role on several other resources.

```
[admin@UplogixLM]# config user dsmith
[config user dsmith]# system admin
[config user dsmith]# modem guest
[config user dsmith]# powercontrol guest
[config user dsmith]# port 1/1 guest
[config user dsmith]# port 1/2 guest
[config user dsmith]# exit
```

As with other editors, use the no modifier to remove existing settings. For example, to remove user dsmith's guest role on port 1/2:

```
[config user dsmith]# port 1/2 no guest
```

Users who are members of group accounts will inherit the permissions associated with the group account in addition to the permissions associated with their own user accounts.

A user can be assigned more than one role on a given resource. The user will be able to execute any command allowed by any of the user's roles on the resource unless denied by one of the roles. For example, if assigned the allow shutdown and deny shutdown roles, the deny shutdown role always takes precedence.

> The admin role (separate from the admin user account) has access to every available command except the config reinstall command that is used to factory reset the Local Manager. To manage the Local Manager, at least one user account must be assigned the admin role unless the Local Manager is being managed by a Control Center.

Creating and editing roles

If the predefined roles do not meet your organization's needs, use the config role command to create custom roles that give users the exact permissions you want them to have.

In this example, we create a role called newRole.

```
[admin@UplogixLM]# config role newRole
Role newRole does not exist. Create (y/n): y
```

Type ? to see a list of configurable settings.

```
[config role newRole]# ?
Allowable arguments are:
show
[no] description
[no] allow
[no] deny
[no] start
[no] expire
or 'exit' to quit config mode
Use ? with allow or deny to list permissions

[config role newRole]# description this is an example role
[config role newRole]# allow login
[config role newRole]# allow show user
[config role newRole]# allow show role
[config role newRole]# allow config password
```

> Roles assigned at the system level must include the login permission to give the user access to the Local Manager. To access port, modem, and powercontrol resources, the role must include a permission that allows the user to view the resource, such as the show status permission.

Type show to view the current settings for the role.

```
[config role newRole]# show
newRole - this is an example role
```

```
        allow config password
        allow login
        allow show role
        allow show user
```

To remove a permission that has already been set, use the no modifier.

```
[config role newRole]# no allow show role
[config role newRole]# show
newRole - this is an example role
        allow config password
        allow login
        allow show user
[config role newRole]# exit
```

Description

Use the optional description subcommand to provide information about the role. This is a free text field of 255 characters.

Syntax:

```
description <“text”>
```

Allow and deny

These subcommands specify commands that accounts with this role may and may not execute. Use * as a wildcard character and use ? to show a list of commands that can be allowed or denied.

Syntax:

```
allow <command | ?>
deny <command | ?>
```

Specifically denied commands are filtered from those specifically allowed. The all keyword is overridden by any specific allow or deny statement. For example, if the deny show * command is issued after allowing the show user command, the role allows show user but no other show commands.

Start and expire

Optionally, set the month and day of the current year that the role becomes valid and the month and day of the current year after which the role is no longer valid.

Syntax:

```
start <MMDD>
expire <MMDD>
```

By default, roles do not have start or expire dates.

Reviewing the role settings

Use the show subcommand to display the current settings for the role.

```
[config role newRole]# show
newRole - example role
        allow login
        allow show role
        allow show user
```

Removing settings

Use the no modifier to remove settings. For example, no expire removes a previously set expire date.

Deleting a role

To delete a role, use the no modifier with the config role command. For example, to delete a role called temporary_role:

```
[admin@UplogixLM]# config role no temporary_role
[admin@UplogixLM]# show role temporary_role
Could not find role 'temporary_role'
```

If the Local Manager is managed by a Control Center, roles must be managed through the Uplogix web interface.

To create or modify a global role: Administration > Roles > Create/Edit role

Example: Granting terminal access only, on one port only

Sometimes a user needs only minimal access. In this example, we create a user who can only login to one Local Manager and only execute the terminal command on port 1/1. The steps to complete this are:

- Create a custom role
- Create a user account that will have this role
- Apply the role to the appropriate resources

Creating the role

Use the config role command to create a custom role called terminalOnly.

```
[admin@UplogixLM]# config role terminalOnly
Role terminalOnly does not exist. Create (y/n): y
```

The user can only execute commands while logged in to the Local Manager, so the role must also allow login:

```
[config role terminalOnly]# allow login
```

The user will need to navigate to the appropriate port. There is no port permission. Instead we will use the show status permission. When applied to a port, this permission allows the user to navigate to the port.

```
[config role terminalOnly]# allow show status
```

This role must allow the user to execute the terminal command:

```
[config role terminalOnly]# allow terminal
```

The terminalOnly role now includes all the permissions required to allow the user to login to the Local Manager, navigate to a port, and open a terminal session. Use the exit subcommand to close the role editor.

```
[config role terminalOnly]# exit
```

Creating the user account

Use the config user command to create a user and assign the terminalOnly permission.

```
[admin@UplogixLM]# config user termOnlyUser
User termOnlyUser does not exist. Create (y/n): y
```

Although the `config user` editor allows you to assign a password, this is not a secure way to do so. Instead, use the `config password` command after creating the user account.

The `config user` editor allows roles to be assigned, the next step.

Applying the role to create permissions

The role we created, `terminalOnly`, includes Local Manager-level commands (`login` and `show status`) and port-level commands (`show status` and `terminal`). To log into the Local Manager, the user account will need the `login` permission at the Local Manager level. Use the `config user` editor to apply the `terminalOnly` permission at the Local Manager level:

```
[config user termOnlyUser]# system terminalOnly
```

This user will need access to port 1/1 to be able to open terminal sessions. Port access and terminal permissions are part of the `terminalOnly` role, so we can apply this role to the port where the user will need access:

```
[config user termOnlyUser]# port 1/1 terminalOnly
```

The `termOnlyUser` account will not need any other permissions, as we only want this account holder to be able to open terminal sessions on port 1/1. Use the `exit` subcommand to close the `config user` editor.

```
[config user termOnlyUser]# exit
```

Completing the account setup

Use the `config password` command to securely set a password for the `termOnlyUser` account.

```
[admin@UplogixLM]# config password termOnlyUser
New Password: *********
Confirm Password: ********
Password changed.
```

The `termOnlyUser` account is now ready to use.

Managing Devices

This chapter covers:

- Terminal sessions — Work directly with managed devices
- Working with service processors — Automate server management using service processors
- Upgrading a device operating system
- Managing device configurations — Push a configuration to a device
- Rolling back configuration changes — Automatic fail-safe rollback and manual rollback
- Forcing a configuration recovery — Cisco devices only
- Recovering a device from boot loader state

Terminal sessions

The Local Manager allows terminal sessions to devices.

When you initialize a port with the `config init` command, the Local Manager stores console and enable credentials. The credentials allow the Local Manager to authenticate to the manage device for automated operations. Terminal pass-through allows users with the admin role (or a custom role with the `use system auth` privilege) on a given port to use these stored `credentials` when starting a terminal session. In all other cases, the Local Manager logs out of the device when a user issues the `terminal` command; the user must log in manually using his/her own credentials.

If the Local Manager is managed by a Control Center, the device CLI can also be accessed through the Uplogix web interface:

```
Inventory > Local Manager page > port detail > Device CLI
```

Starting a terminal session

To start a terminal session with a device, navigate to the appropriate port and issue the `terminal` command. You may be prompted to log into the device. Terminal commands available are role-based and port-specific.

Terminal commands

Commands available in terminal sessions:

~a - Authentication wizard

~b - Send break signal

~c - Incremental commit

~e - Turn on local echo (on by default for ComTech devices)

~f - Start or stop the FTP server

~g - Enable/disable SFTP/SCP service

~h - Show this help menu

~l - Lock this port - other users and jobs will be ignored. The user who locks the port can term back in unhindered; the session resumes where the user left off. A user with the `terminal force` permission can term in to a locked port.

~n - Append newlines to carriage returns (on by default for ComTech devices)

~p - Power on/off/cycle this device

~q - Send Solaris alternate break signal

~r - Rollback wizard

~s - Serial connection settings wizard

~t - TFTP server wizard

~x - Xmodem wizard

~y - Ymodem wizard

Locking a terminal session

If your role on the port includes the `terminal lock` permission, you can issue the `~l` command to lock the terminal during long processes. Other users who try to initiate terminal sessions to the device will be notified that a terminal lock is in effect. Users with the `terminal force` permission on the device can override the lock. The terminal lock is removed the next time you start a terminal session to the device.

Ending a terminal session

End a terminal session by typing `~ <Enter>` on a line by itself.

When you end your session, you will be prompted to enter a comment describing the reason for your changes if changes are detected.

Using the Local Manager's credentials for terminal sessions

When you configure a device on one of the Local Manager's ports using the `config init` command, the Local Manager prompts you to enter console and enable login credentials.

Depending on the privileges allowed by your role on the device, the Local Manager may send the console and enable usernames and passwords for the device, so that you are logged in automatically. To use this capability, you must have a role on the port that includes the `use system auth` permission, such as the `admin` role.

Using terminal pass-through

If terminal pass-through is enabled on the device, an SSH or Telnet session can be opened directly to the Local Manager while retaining the rollback capabilities, session logging, and authorization checking of the Local Manager. Refer to Configuring SSH or Telnet terminal pass-through protocol for information on configuring terminal pass-through.

```
Depending on your permissions, you may need to login to the device.
dsmith@central:~$ ssh -p 2001 admin@203.0.113.1
admin@203.0.113.1's password:
Permission granted for pass-through
Press ~[ENTER] to exit
Connecting ...
```

Working with service processors

When a connected device is initialized as `hp`, `sun`, or `server` using the `config init` command, the service processor commands become available to help automate server management.

Configuring the service processor

Use the `config service-processor` command to configure communication with the service processor.

```
[admin@UplogixLM (port1/2)]# config service-processor
Service processor enabled: false
Change these? (y/n) [n]: y
--- Enter New Values ---
Enable service processor (y/n) [n]: y
Service processor use dedicated (y/n) [n]: y
Service processor IPMI port [623]:
Service processor username []: solar2
Service processor password: *******
Confirm Password: *******
Service processor connection type: [auto]:
Do you want to commit these changes? (y/n): y
```

Viewing service processor information

Use the `show service-processor` commands to view information about the service processor:

`show service-processor config` — Lists the current configuration of the service processor.

`show service-processor events` — Displays the service processor log.

`show service-processor info` — Displays information about the service processor.

`show service-processor power` — States whether the service processor is powered on.

`show service-processor sensor` — Displays information from the service processor's sensors to give a low-level view of the server's health.

Working with the service processor using IPMI

Use the `service-processor execute` command to work directly with the service processor. Command syntax is: `service-processor execute <command>`

`<command>` may be any of these:

`Channel`	Configure Management Controller channels
`Chassis`	Get chassis status and set power state

`Event`	Send pre-defined events to Management Controller
`Fru`	Print built-in FRU and scan SDR for FRU locators
`Fwum`	Update IPMC using Kontron OEM Firmware Update Manager
`i2c`	Send an I2C Master Write-Read command and print response
`isol`	Configure IPMIv1.5 Serial-over-LAN
`kontronoem`	OEM commands for Kontron devices
`lan`	Configure LAN channels
`mc`	Management Controller status and global enables
`pef`	Configure Platform Event Filtering (PEF)
`picmg`	Run a PICMG/ATCA extended command
`power`	Shortcut to chassis power commands
`raw`	Send a RAW IPMI request and print response
`sdr`	Display Sensor Data Repository entries and readings
`sel`	Display System Event Log (SEL)
`sensor`	Display detailed sensor information
`session`	Display session information
`sunoem`	OEM commands for Sun servers
`user`	Configure Management Controller users

Controlling power to the service processor

Use the `service-processor power` command to control power to the service processor. Command parameters are `on`, `off`, and `cycle`.

Upgrading a device operating system

Before you start, obtain the appropriate OS image from the manufacturer of the device to be upgraded.

To transfer the file using FTP, TFTP, or SFTP, Ethernet connectivity to the managed device is required; xmodem or ymodem may be used with serial connections when supported by the managed device.

To transfer an OS image to the Local Manager, navigate to the port that is connected to the managed device and execute the `copy` command:

```
copy [scp|ftp] "username@server:fileName" os [candidate|current]
```

For example, to copy a new Cisco switch OS from a server to the Local Manager using the SCP protocol:

```
[admin@UplogixLM (port1/1)]# copy scp dsmith@203.0.113.11:c3560-12.3t.bin os candidate
```

Enter the `show settings` command to determine the current file transfer preference settings for this port. To change the current settings, use the `config settings` command.

After configuring OS upgrade settings, the upgrade can be performed. The image previously downloaded to the Local Manager has been assigned to the candidate slot, which means it has not yet been successfully deployed to your specific device.

To begin the upgrade, enter or schedule the `push os candidate` command from the appropriate port resource. The Local Manager first attempts to transfer the image using the primary method. If that fails, the alternative method is used. When the transfer is complete, the device may automatically reboot if the Local Manager port settings are configured to include this behavior. The Local Manager monitors and saves the Power On Self Test (POST) log messages and reports if the upgrade is successful. You may manually schedule a reboot for later, but in this case the automated validation will not be performed.

```
[admin@UplogixLM (port2/1)]# push os candidate
System image file is "flash0:/c2951-universalk9-mz.SPA.151-4.M.bin"
6 interfaces and 1 types found.
Information logged Before Upgrade
There are no outlet mappings for this device.
Hostname     : Aus3-router
Serial Number: FT2TX19AKZR
Make         : cisco
Model        : CISCO2951/K9
OS Type      : IOS
OS Version   : 15.1(4)M
Uptime       : 2 weeks, 2 days, 4 hours, 58 minutes
Device Image Verified.
Initiating file transfer
Sending c2951-universalk9-mz.SPA.151-3.T1.bin to 192.0.2.2:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
TFTP download of c2951-universalk9-mz.SPA.151-3.T1.bin succeeded.
Verified: flash0:c2951-universalk9-mz.SPA.151-3.T1.bin
Retrieving running-config from device ...
Complete. running-config pulled.
Retrieving running-config from device ...
Complete. running-config pulled.
Issuing 'reload'
Reading post
Bootstrap posted
CISCO2951/K9 platform with 2621440 Kbytes of main memory
.Image decompressing
Image decompressed

Device loaded

Post complete.
Hostname     : Aus3-router
Serial Number: FT2TX19AKZR
Make         : cisco
Model        : CISCO2951/K9
OS Type      : IOS
OS Version   : 15.1(3)T1
Uptime       : 0 minutes
6 interfaces and 1 types found.
Push OS succeeded.
```

Managing device configurations

Use the `push` commands to write a saved configuration to a device.

Whether you write the entire configuration or make incremental changes, the procedure is:

1. Pull the current running configuration from the device by logging into the device with the `terminal` command.
2. Verify that the configuration file you intend to push is the correct file.
3. Push the file using either the `push startup-config` or the `push running-config` command. The Local Manager will pull the configuration before and after the push operation, so the change can be undone if necessary.

Use `push startup-config` to write the entire configuration (e.g., replacing a device). For the case of a device with a VLAN database, also use `push vlan` to restore the VLAN database (vlan.dat) file.

Use the `push running-config` command to make incremental changes. In the example below, the running-config candidate file contains only one line; when this running-config file is pushed to the device, only its hostname will be changed.

First, log into the device with the `terminal` command. The Local Manager automatically pulls the current running-config so it can track changes made during the terminal session, which are required for the rollback feature and device change logging.

```
[dsmith@UplogixLM (port 1/1)]# terminal

Press ~[ENTER] to exit
Connecting ...
Retrieving running-config from device ...
Complete. running-config pulled.
running-config saved to archive as current.

Console session started.
```

The `show running-config` command displays the device's current configuration. Some information has been removed from the command output.

```
XYZ-CORE# show run
Building configuration...

Current configuration : 750 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service tcp-small-servers
!
hostname XYZ-CORE
!
logging buffered 4096 debugging
no logging console

[output removed]
```

```
XYZ-CORE#
Console session ended.

Disconnecting ...

Logging out of device...
Retrieving running-config from device ...
Complete. running-config pulled.
running-config saved to archive as current.
```

The Local Manager pulls the running configuration again as the terminal session ends.

Using the `show running-config candidate` command, view the running configuration file that you will push to the device.

```
[dsmith@UplogixLM (port1/1)]# show running-config candidate
hostname foo
```

This running configuration file will only change the device hostname. To push this configuration to the device, use the `push running-config candidate` command.

```
[dsmith@UplogixLM (port1/1)]# push running-config candidate
Retrieving running-config from device ...
Complete. running-config pulled.

Copying running-config to device.

Transferring via XModem. (Attempt 1)
Initiating file transfer
Transferring file ...

Sent running-config at 133 B/s.

File running-config was transferred to the device successfully via XModem.
Retrieving running-config from device ...
Complete. running-config pulled.
running-config saved to archive as current.
runningConfig downloaded to device.
Retrieving running-config from device ...
Complete. running-config pulled.
running-config saved to archive as current.
```

When the file transfer is complete, view the new running configuration using the `show running-config current` command. Some information has been removed from the command output.

```
[dsmith@UplogixLM (port1/1)]# show running-config current
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
```

```
no service password-encryption
service tcp-small-servers
!
hostname foo
!
logging buffered 4096 debugging
no logging console
[output removed]
```

Rolling back configuration changes

Some manual configuration changes to an operational device can cause it to drop the command line connection. You can undo the changes from a terminal session without reapplying the entire running configuration, either with the automatic SurgicalRollback™ feature or with a manually initiated rollback.

Both rollback features return the device to the state immediately before the changes, reducing time to recovery as well as the time needed for contingency planning.

When using the `terminal` command or a terminal pass-through session to access a device, the Local Manager retrieves the device's running configuration. After exiting the terminal session and returning to the command line, the Local Manager retrieves another copy of the running configuration. The Local Manager compares the two running configurations and creates a difference file. Both rollback methods undo the changes in the difference file without reapplying the entire running configuration or rebooting the managed device.

The `config settings` command specifies rollback transfer methods (XMODEM, TFTP, FTP).

The rollback capability is only available when using a terminal session from the Local Manager to access the device (note: changes made to a device via a SSH session to the managed device that bypasses the Local Manager cannot be rolled back). This feature can only roll back changes from the most recent terminal session. Entering and exiting the device via the `terminal` command constitutes a session. For example, if you access the device using the `terminal` command, change the hostname, and exit the terminal session; then `terminal` in again, issue a `show version` command and exit, you will not be able to use either automatic SurgicalRollback™ or manually initiated rollback to undo the hostname change, as it was not done during the most recent session.

Scheduled tasks and monitors do not affect rollback.

Undoing changes automatically with SurgicalRollback™

SurgicalRollback™ is the default behavior when ending a terminal session. If the Local Manager notes configuration changes during a terminal session, it displays the changes along with a message warning that your changes will be rolled back if you don’t commit the changes. The Local Manager prompts you to commit your changes, postpone rollback, or roll back the changes immediately. If you do not respond within 75 seconds, the rollback takes place by default. During the countdown to rollback, the Local Manager sends the ASCII bell character each time it refreshes the countdown display, to provide an audio cue that rollback is about to start.

If you need more time to review the list of changes, you can delay SurgicalRollback™ by typing `p` to postpone the process for the number of seconds that you specify.

The following example shows a configuration change and the difference document that the Local Manager creates.

```
[admin@UplogixLM (port1/1)]# terminal
```

```
Press "~[ENTER]" to exit
Connecting ...
Retrieving running-config from device ...
Complete. running-config pulled.
Cisco7206#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Cisco7206(config)#hostname Demo7206
Demo7206(config)#access-list 101 permit pim any 192.0.2.0 0.0.0.255 tos min-delay
Demo7206(config)#exit
~<enter>
Disconnecting ...
Retrieving running-config from device ...
Complete. running-config pulled.
Changes made in current terminal session:
+hostname Demo7206
-hostname Cisco7206
+access-list 101 permit pim any 192.0.2.0 0.0.0.255 tos min-delay

Warning: Automatic rollback in effect.
Any changes to the device's running-config will be restored in 75 seconds.
70 seconds remaining. ([C]ommit/[P]ostpone/[R]ollback immediately):
```

In the example above, after return to the command line, the Local Manager identifies configuration changes listed and begins a countdown to automated configuration rollback.

Lines that are removed are prefixed with the – character.

Lines that are added are prefixed with a + character.

Undoing changes with a manually initiated rollback

If you commit the changes from a terminal session but then decide they should be rolled back, start a rollback procedure manually. To see the list of changes that will be made, use the `show rollback-config` command. For example, if you completed the terminal session shown above and committed the changes, the following would display:

```
[admin@UplogixLM (port1/1)]# show rollback-config
!
no hostname Demo7206
no access-list 101 permit pim any 192.0.2.0 0.0.0.255 tos min-delay
hostname Cisco7206
!
```

To make the changes listed, use the `rollback config` command.

This capability is available for some but not all types of managed devices. For more information on the `show rollback-config` and `rollback config` commands, refer to the *Reference Guide for Local Managers*.

Forcing a configuration recovery — Cisco devices only

The Local Manager can restore the configuration of a Cisco router or switch that it cannot access because of an authentication or an improperly pushed configuration file. Configuration recovery can recover a password by restoring a previously stored password, along with that configuration.

This feature is available for Cisco routers running IOS and Cisco switches running CatOS.

The following conditions must be met before the Local Manager can force the configuration recovery:

- A valid device startup configuration must be stored on the Local Manager. One can be manually obtained using the `pull config startup` command.
- The device must be plugged into a power controller that is managed by and appropriately configured on the Local Manager.

The configuration recovery consists of replacing the startup-config on the device with a startup-config stored on the Local Manager.

```
[admin@UplogixLM (port1/4)]# recover configuration
This process can take about 5 minutes.
Attempting to revert startup configuration to current from 10 Jun 21:57
Powering off outlet(s) [1, 2]
DSR was active.
CTS was active.
CTS is still active.
Powering on outlet(s) [1, 2]
Serial link is active.
Attempting to break into ROMmon mode.
Break into ROMmon successful.
Reading post
Image decompressing
Image decompressed
Post complete.
recoverPassword on port1/4 succeeded
```

Recovering a device from its boot loader state

Local Managers can recover devices that have entered a boot loader state such as Cisco's ROMmon state. While the process varies among vendors and models, the Local Manager delivers standardized operations that require low-level boot loader and operating system configuration recovery steps in an efficient, rapid manner.

The recovery process is automatic and does not require any immediate user attention to initiate or complete.

You must have copies of the device OS and startup configuration files in order to recover from ROMmon.

The `config init` command schedules periodic collection of these files. The OS files are transferred using the FTP and TFTP protocols, so you must have a working network connection from the Local Manager's management Ethernet interface to an Ethernet interface on the device in question.

If the device's operating system does not offer this ability, the files can be obtained from the vendor and stored on the Local Manager in the event they are needed.

After the `pull os` command is successful, the Local Manager will have a copy of the device's OS image stored locally. The stored image is relevant only for the device connected to the Local Manager's console port. If you prefer to use a previously collected OS file from one port for another port, reference the `copy` command.

The following is a `pull os` command example:

```
[admin@UplogixLM]# port 2/2
AustinR1-SRE cisco CISCO2921/K9 IOS 15.1(4)M
             Cisco2921

[admin@UplogixLM (port2/2)]# pull os
Starting pull of Cisco IOS Image
System image file is "flash:/c2900-universalk9-mz.SPA.151-4.M.bin"
Backing up os file: flash:c2900-universalk9-mz.SPA.151-4.M.bin
Transferring file via FTP

Writing scratch/temp.file
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!
70542428 bytes copied in 29.516 secs (2389972 bytes/sec)

AustinR1-SRE#
FTP Transfer complete

[admin@UplogixLM (port2/2)]# show directory
Type     Version    Name
-------  ---------  ------------
Config
    Running
         current    running-config

    Startup
         current    startup-config

OS
         current    c2900-universalk9-mz.SPA.151-4.M.bin
```

In this example, if the Local Manager later detects that the Cisco 2921 is in ROMmon mode, it immediately attempts a recovery. If it finds a bad or missing OS image, the Local Manager will use the stored current OS image as part of its recovery process.

The configuration file used to cold-start a network device will also be necessary.

Retrieve the startup configuration using the `pull startup-config` command to maintain a copy locally for these and other operational recovery procedures. As above, you can also schedule the Local Manager to automatically gather this information as often as is practical.

These files are automatically scheduled when using the `config init` command in setting up a new supported device.

Advanced Local Manager Applications

This chapter covers additional features and how they may be applied to help manage your network:

- Cisco recovery from ROMmon customization
- Configuring SSH or Telnet terminal pass-through protocol
- Serial Port Forwarding
- SSH Port Forwarding
- Subinterfaces
- Capture Mode
- Setting up frozen console monitoring and recovery

Cisco recovery from ROMmon customization

This section describes how to tailor Cisco NVRAM variables used by the Uplogix Cisco advanced driver when it needs to recover the OS image from ROMmon. More specifically, this allows you the ability to customize the variable settings used by the TFTPDNLD command when the Local Manager finds a router or switch in ROMmon and determines that the OS image needs to be recovered on the Cisco device.

You can customize the following ROMmon variable settings relevant to TFTPDNLD: IP address, subnet mask, default gateway, Ethernet interface, Ethernet interface speed, and duplex settings that override derived and default settings used by the Uplogix driver. For more information on Cisco's ROM Monitor and recovering a system image using TFTPDNLD, refer to Cisco's *Troubleshooting and Maintenance: Using the ROM Monitor* documentation for the 1800/2800/3800 Series Integrated Services Routers or the 1900/2900/3900 Series Integrated Services Routers.

Usage Notes

Customizing ROMmon variable settings adds value in the following situations:

- TFTPDNLD must take place over an Ethernet interface that is not the lowest numbered interface on the device.
- TFTPDNLD uses an interface that is not in the same subnet as the Local Manager Ethernet management interface and which is not a dedicated Ethernet connection to the Local Manager.
- TFTPDNLD uses an Ethernet interface that requires a specific speed and duplex setting in order to work properly from ROMmon.

Feature Limitations

- This feature is limited to Cisco routers and the switches that support the TFTPDNLD command in ROMmon
- This feature may not work on all Cisco routers and versions of IOS. Check the Cisco website to validate support for these ROMmon variables.

Required Privileges

- `config properties` — Configure properties on an Local Manager port.
- `show properties` — View properties on an Local Manager port.

Usage

Configuring ROMmon Variable Settings

The Uplogix advanced driver recovery from ROMmon functionality only works on Cisco devices that support the TFTPDNLD feature to download an OS image while in ROMmon. This feature utilizes Local Manager port properties to allow defining ROMmon variable settings that should be set by the Uplogix advanced Cisco IOS driver when it attempts to transfer an OS image to the router that is in ROMmon. Any user-defined ROMmon variable settings will override default settings used by the Uplogix LM.

The following ROMmon variables apply to all routers:

1. `IP_ADDRESS` — IP address of the router
2. `IP_SUBNET_MASK` — subnet mask of the router
3. `DEFAULT_GATEWAY` — default gateway of the router

For routers with Fast Ethernet interfaces, the following ROMmon variables should be available to indicate which Fast Ethernet port should be used, as well as the speed and duplex setting for that interface:

1. `FE_PORT` = [0 | 1]
   - 0 indicates FastEthernet0/0
   - 1 indicates FastEthernet0/1
2. `FE_SPEED_MODE` = [0 | 1 |2 | 3 | 4]
   - 0 indicates 10 Mbps, half-duplex
   - 1 indicates 10 Mbps, full-duplex
   - 2 indicates 100 Mbps, half-duplex
   - 3 indicates 100 Mbps, full-duplex
   - 4 indicates Automatic selection (default)

For routers with Gigabit Ethernet interfaces, the following ROMmon variables should be available to indicate which Gigabit Ethernet port should be used, as well as the speed and duplex setting for that interface:

1. `GE_PORT` = [0 | 1 | 2]
   - 0 indicates GigabitEthernet0/0
   - 1 indicates GigabitEthernet0/1
   - 2 indicates GigabitEthernet0/2
2. `GE_SPEED_MODE` = [0 | 1 |2 | 3 | 4 | 5]
   - 0 indicates 10 Mbps, half-duplex
   - 1 indicates 10 Mbps, full-duplex
   - 2 indicates 100 Mbps, half-duplex
   - 3 indicates 100 Mbps, full-duplex
   - 4 indicates 1 Gbps, full-duplex
   - 5 indicates Automatic selection (default)

All user-defined ROMmon variable settings in the port properties must be the actual ROMmon variable name prepended with _rommon_. For example, to set the default gateway, configure the following property on the Local Manager port that is managing the router:

```
_rommon_DEFAULT_GATEWAY 192.0.2.254
```

Use the config properties command at the port level in the Local Manager to enter the port properties configuration editor.

```
[admin@UplogixLM (port1/4)]# config properties
[config properties]#
```

Once in the editor, you can use the ? command to view a list of possible configuration options.

```
[config properties]# ?
Allowable arguments are:
show
<propertyName> <propertyValue>
no <propertyName>
or 'exit' to save current values and quit config mode
[config properties]#
```

show	Display configured properties.
[no] {property name} {property value}	Define property names. The no prefix will remove the property from the port. Example: Instruct the Uplogix LM to transfer an image to the router, where auto negotiation should be used for interface GigiabitEthernet0/2, with an IP address of 192.0.2.142, a subnet of 255.255.255.0 and a default gateway of 192.0.2.254: _rommon_IP_ADDRESS 192.0.2.142 _rommon_IP_SUBNET_MASK 255.255.255.0 _rommon_DEFAULT_GATEWAY 192.0.2.254 _rommon_GE_PORT 2 _rommon_GE_SPEED_MODE 5
Exit	Exit the configuration editor.

Display Properties

Use the show properties command to view the properties on the Local Manager port:

```
[admin@Uplogix (port1/4)]# show properties
_rommon_DEFAULT_GATEWAY: 192.0.2.254
_rommon_GE_PORT: 2
_rommon_GE_SPEED_MODE: 5
_rommon_IP_ADDRESS: 192.0.2.142
_rommon_IP_SUBNET_MASK: 255.255.255.0
```

Configuring SSH or Telnet terminal pass-through protocol

Terminal pass-through is available on the `port`, `modem`, and `powercontrol` resources and is enabled on a device-by-device basis. This feature allows an SSH session to be opened directly to the device, passing through the Local Manager, while retaining the Local Manager's rollback capabilities, session logging, and authorization checking.

To configure terminal pass-through, navigate to the desired resource and use the `config protocols pass-through` command to specify either SSH or Telnet and optionally, the TCP port number. Command syntax is:

```
config protocols pass-through <enable | disable> <telnet | ssh> [“port number”]

admin@UplogixLM (port1/1)]# config protocols pass-through enable ssh
Pass-through port will be 2001.
SSH port change will take place after the next Uplogix restart.
```

By default, device ports map to TCP ports starting at 2001. Alternate TCP ports (1023 – 9999) may be specified if desired.

This setting takes effect after you `restart` the Local Manager.

Once configured, instead of logging in to the Local Manager, navigating to the port, and issuing the terminal command, you can open an SSH session directly to the device using the pass-through port number assigned.

```
xyzcouser@central:~$ ssh -p 2001 admin@198.51.100.254
admin@198.51.100.254's password: *******
Permission granted for pass-through
Press ~[ENTER] to exit
```

If the Local Manager is managed by a Control Center, then SSH and Telnet pass-through can also be configured through the Uplogix web interface. A restart of the Local Manager is still required.

For a single Local Manager: `Inventory > Local Manager page > Configuration menu > Protocols`

For a group of Local Managers: `Inventory > group page > Configuration menu > Protocols`

Serial Port Forwarding

Use the Serial Port Forwarding feature to make the console port of the managed device available on a local workstation via reverse SSH tunnel. In order to utilize this feature, a user must have the `terminal` privilege.

An SSH client with reverse tunnel capabilities is required to use this feature. Supported clients include PuTTY and the CLI Applet on the Control Center.

Prior to setting up serial port forwarding, initialize the Local Manager port with the appropriate device driver via the `config init` command. Refer to the appropriate device configuration guide for information.

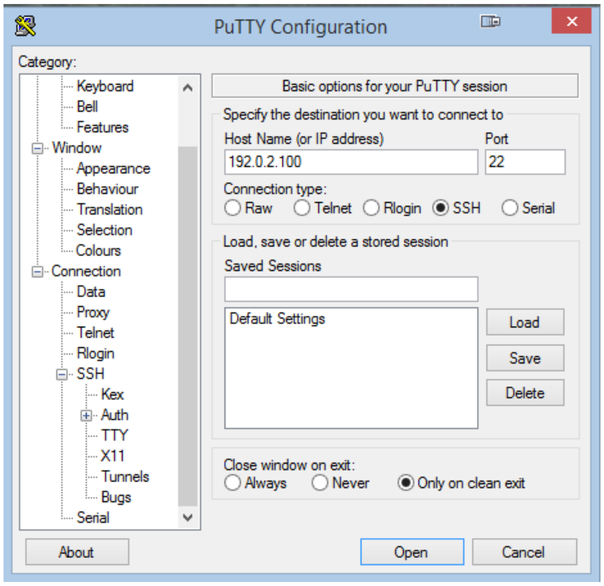
Serial port forwarding connection information:

- Only one telnet connection is allowed per forwarded port. Subsequent connections will fail until the first connection is exited.
- The telnet connection can be terminated by quitting the telnet command, exiting the terminal session on the original SSH session, or by closing the SSH client.
- Accessing a forwarded port via telnet bypasses authentication and authorization. These are handled by the original SSH session.
- Connections to forwarded ports are subject to the same idle timeouts as normal terminal sessions. The idle counter is reset if data is passed over the telnet connection.

Below is an example using PuTTY, for an example using the CLI Applet in the Control Center, refer to the *Control Center User Guide*.

To set up serial port forward using PuTTY:

1. Open PuTTY to display the configuration window.
2. Enter the IP address of the Uplogix device.



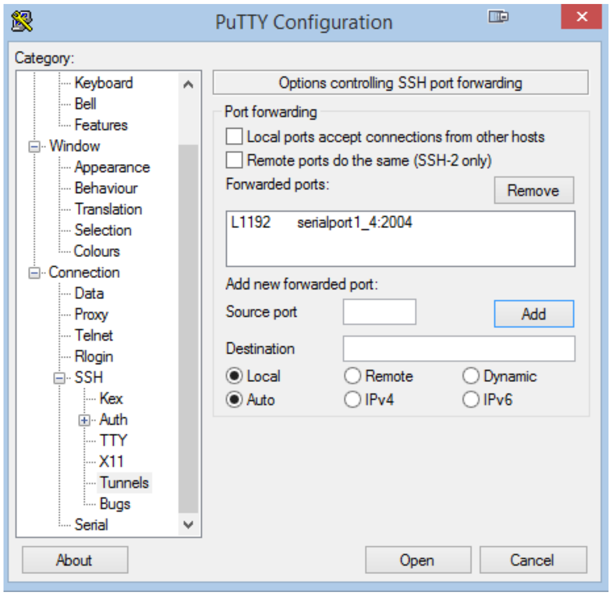
Host Name (or IP address): 192.0.2.100 Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Saved Sessions: Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

3. Under Category, expand the SSH group and select `Tunnels`.
4. For `Source Port`, enter the local port to forward the console connection to.
5. For `Destination`, enter `serialportX_Y:Z` where X is the slot number, Y is the port number, and Z is an arbitrary port number.
6. Leave all other options as default and click `Add`.



Port forwarding

□ Local ports accept connections from other hosts

□ Remote ports do the same (SSH-2 only)

Forwarded ports:

```
L1192     serialport1_4:2004
```

Add new forwarded port:

Source port

Destination

● Local ○ Remote ○ Dynamic

● Auto ○ IPv4 ○ IPv6

7. Click `Open` to begin the SSH session.
8. Enter your `username/password` and navigate to the port you wish to forward.
9. Use the `terminal forward` command to begin a forwarded session.

```
[admin@UplogixLM]# port 1/4
DAL-CORE cisco 7604 IOS 12.2
[admin@u3200 (port1/4)]# terminal forward
Press ~[ENTER] to exit
Connecting ...
Retrieving running-config from device ...
Complete. running-config pulled.
running-config saved to archive as current.
Console session forwarded.
DAL-CORE#
```

10. The console port of the managed device is now available locally. Telnet to 127.0.0.1 (localhost) on the port specified in step 4.

```
# telnet 127.0.0.1 1192
Connecting to 127.0.0.1 1192…

DAL-CORE#sh controllers T1 | include 0/0/0
T1 0/0/0 is up.
```

11. Anything typed in the telnet session will be visible on the original SSH session.

```
running-config saved to archive as current.
Console session forwarded.
DAL-CORE#sh controllers T1 | include 0/0/0
T1 0/0/0 is up.
```

SSH Port Forwarding

This feature enables access to network services running on the dedicated or management IP addresses of a managed device. Multiple users on multiple workstations can use SSH Port Forwarding concurrently.

Certain privileges are required to edit or view a port’s forward configuration.

- `show protocols forward` — Views the forwarding settings.
- `config protocols forward` — Configures the forwarding settings.
- `forward` — Allows the user to open an SSH session with a tunnel to the forwarded port.

The Uplogix device will attempt to forward incoming TCP traffic regardless of whether the destination is configured properly or not. Ensure the managed device is configured to listen on the port specified.

Complete the following steps to configure SSH port forwarding for your managed device.

Configure IP Addresses

The managed device’s management or dedicated IP address must be configured on the Uplogix device. This can be configured using `config init` or `config info`.

```
[admin@UplogixLM (port1/1)]# config init
--- Enter New Values ---
description: []:
////
management IP: []: 192.0.2.200
Configure dedicated ethernet port? (y/n) [y]:
Use DHCP? (y/n) [n]:
dedicated device IP []: 192.0.2.2
dedicated port IP []: 192.0.2.1
dedicated netmask: []: 255.255.255.252
speed/duplex: [auto]:
////
Do you want to commit these changes? (y/n): y
```

Configure Port Forwarding

Use the `config protocols forward` command to open the port forwarding configuration editor.

```
[admin@UplogixLM (port1/1)]# config protocols forward
[forward]#
```

Once in the editor, you can use the `?` command to view a list of possible options.

```
[forward]# ?
Forward options are:
[no] management {port}
[no] dedicated {port}
[no] events
show
exit
```

`[no] management {port}`	Enables forwarding to the management IP address and the port specified. The no prefix will remove the forward. Example: To enable traffic forwarding to port 80 on the managed device's management IP address, use `management 80`.
`[no] dedicated {port}`	Enables forwarding to the dedicated IP address and the port specified. The no prefix will remove the forward. Example: To enable traffic forwarding to port 80 on the managed device's dedicated IP address, use `dedicated 80`.
`[no] events`	Turns on event logging for traffic forwarding. The no prefix will turn off event logging.
`show`	Displays the current configuration.
`exit`	Exits the configuration editor.

Note that the port specified should match the listening port on the managed device. If the managed device is running an SSH server on its management IP address, forwarding should be configured as `management 22`.

Creating a Tunnel

When connecting with an SSH client, you can specify an IP address or hostname and a port to create a tunnel. With forwarding enabled, the Uplogix device will allowing incoming users to establish a tunnel for which they have the `forward` privilege.

Hostnames will take the form of `portx_y`. For example, "port1/1" will specified as "port1_1" when creating the tunnel. This hostname will point to whichever IP address is configured for forwarding, either management or dedicated. If both addresses are configured for forwarding, an IP address should be used to avoid ambiguity.

SSH Client Examples

Below are examples of how to set up this feature using OpenSSH and PuTTY. For an example of this feature using the Control Center CLI Applet, refer to the *Uplogix Control Center Users Guide*.

OpenSSH (Linux/Unix)

The `ssh` command on most Linux platforms provides for port forwarding with the `-L option`. For example, if port 1/3 is forwarding port 80 on its dedicated IP address and you want to map it locally to port 1080, use the following command:

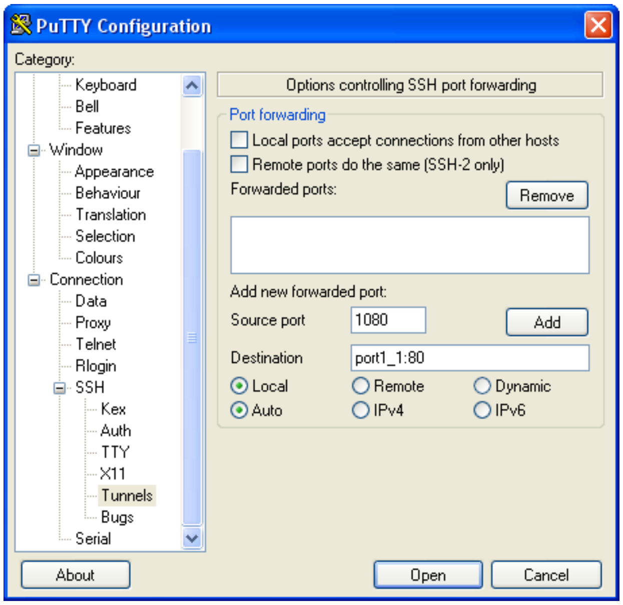
```
# ssh -L 1080:port1_3:80 username@uplogixlocalmanager
```

An IP address can also be used:

```
# ssh -L 1080:192.0.2.40:80 username@uplogixlocalmanager
```

PuTTY

To use PuTTY with SSH Port Forwarding, run the program and view the PuTTY Configuration window. On the left side of the window, select the Tunnels section under Connection -> SSH.



Options controlling SSH port forwarding

Port forwarding

☐ Local ports accept connections from other hosts

☐ Remote ports do the same (SSH-2 only)

Forwarded ports:

Add new forwarded port:

Source port: 1080

Destination: port1_1:80

● Local ○ Remote ○ Dynamic

● Auto ○ IPv4 ○ IPv6

Configure port forwarding with the following options:

- Source Port: A local port on the user's workstation to forward the remote port to. For example, to make the remote port 80 appear locally as 1080, use `1080` as the source port.
- Destination: A combination of the destination hostname (or IP address) and the remote port. For example, to create a tunnel to port 80 on port 1/1, use `port1_1:80`. If you would like to specify the IP address, use `192.0.2.1:80` (where 192.x.x.x is the management or dedicated IP address of the managed device).
- The default options of Local and Auto will be sufficient for creating the tunnel.

Click Add to save the configuration for use with the next SSH connection. Once you click `Open` and establish a session, the tunnel will be created.

In this example, you would then be able to open a web browser to `http://127.0.0.1:1080`. Your request will be forwarded through the tunnel to the managed device on port 1/1.

Notes

- Access to forwarded ports is secured by mapping the requested hostname or IP address to a managed device on the Local Manager. If forwarding is enabled for two ports that have the same management or dedicated IP addresses, it may be possible for a user to access the forwarded port of a device that they do not have explicit permission for.
- Any tunnels created with an SSH session will be torn down if the session times out or is exited. To regain access to the tunnel, initiate another SSH session.

Subinterfaces

Through the application of subinterfaces, the Local Manager enables:

- SLV traffic to be directed to specific VLANs on the Local Manager Ethernet management interface (i.e. subinterfaces), enabling synthetic SLV traffic to follow the same path through the network as the real traffic being simulated/measured.
- Multiple network interfaces to be defined on the Local Manager (i.e. interfaces on different VLANs), allowing users to login to the Local Manager from non-management VLANs.

- Some networks local to the Local Manager may not be reachable through the out-of-band network. Static routes can now be created on the management interface to force traffic on the Local Manager destined for these local networks to use the in-band Ethernet interface when routing to these specific local networks that would not be reachable over the out-of-band network.

In order to apply this feature, a user must have the following privileges:

- `config system subinterface` — Configures a subinterface.
- `show system subinterface` — View system subinterfaces.
- `config system route` — Configure static routes for the management interface.
- `show system route` — View system routing table.
- `config system ipt` — Configure IP Telephony settings to use a subinterface.
- `show system ipt` — View IP Telephony settings.

Additionally, the application of the subinterface feature requires the Ethernet management interface connection for the Local Manager to be an 802.1Q trunk with the native VLAN (untagged) used for the `config system ip` management address.

Use the `config system subinterface {subinterface_name}` command to open the subinterface configuration editor.

```
[admin@UplogixLM]# config system subinterface voice
Subinterface voice does not exist. Create (y/n): y
Warning: Remote connections may be lost if you commit changes.
[config subint voice]#
```

Once in the editor, you can use the `?` command to view a list of possible configuration options.

```
[config subint voice]# ?
Allowable arguments are:
show
description
vlan
[no] ip
[no] ipv6
[no] route
[no] gateway
or 'exit' to quit config mode
```

`show`	Display the current subinterface configuration.
`description`	Describe the purpose of the subinterface. Example: `description Voice VLAN for SLV IPT traffic`
`vlan {vlan_number}`	Define the VLAN associated with the subinterface. Example: To associate the subinterface with VLAN=51, use `vlan 51.`
`[no] ip {dhcp | IPv4_address/netmask_bits}`	Set the IPv4 address for the subinterface. The `no` prefix will remove the IP address from the subinterface. Example: To set to a class C IPv4 address of 192.0.1.2, use `ip 192.0.2.2/24`. To set the subinterface to DHCP an IP address, use `ip dhcp.`
`[no] ipv6 {IPv6_address/netmask_bits}`	Set the IPv6 address for the subinterface. The `no` prefix will remove the IP address from the subinterface. Example: To set the IPv6 address to 2001:DB8:b951:600:1293:e8f1:fe0b:4932 with a prefix length of 64, use `ipv6 2001:DB8:b951:600:1293:e8f1:fe0b:4932/64`.
`[no] route {IPv4_address/netmask_bits | IPv6_address/netmask_bits }`	Set an IPv4 or IPv6 static route to be associated with this subinterface. The `no` prefix will remove the static route from the subinterface. Example: To route all outgoing traffic headed to the 203.0.113/24 network over this subinterface, use `route 203.0.113.0/24`. To route all outgoing traffic headed for 2001:DB8:4870:0/32, use `route 2001:DB8:4870:0/32`.
`[no] gateway {IPv4_address | IPv6_address}`	Set the IPv4 or IPv6 gateway for this subinterface. The `no` prefix will remove the gateway address from the interface. Example: To set the IPv4 gateway to 192.0.2.254, use `gateway 192.0.2.254`. To set the IPv6 gateway to 2001:DB8:b951:600:1222:ab71:fe01:2386, use `gateway 2001:DB8:b951:600:1222:ab71:fe01:2386`
`exit`	Exit the configuration editor.

Display a Subinterface

Use the `show system subinterface {subinterface_name}` command to view the subinterface configuration for a particular subinterface, or use `show system subinterface *` to display the configuration for all subinterfaces on the Local Manager.

```
[admin@UplogixLM]# show system subinterface voice
name voice
vlan 51
description Voice VLAN for SLV IPT traffic
ip 192.0.2.2/24
gateway 192.0.2.254
ipv6 2001:DB8:b951:600:1293:e8f1:fe0b:4932/64
gateway 2001:DB8:b951:600:1222:ab71:fe01:2386
route 203.0.113.0/24
route 2001:DB8:4870:0:0:0:0:0/32
```

Delete a Subinterface

Use the `config system subinterface no {subinterface_name}` command to delete specified subinterface. Here is an example that deletes a subinterface named 'voice.'

```
[admin@UplogixLM]# config system subinterface no voice
```

Update IP Telephony Settings for VoIP Subinterface

The system IPT (IP Telephony) settings must be configured if a voice subinterface is implemented for IPT service level validation (SLV). Use the `config system ipt` command to open the IPT configuration editor.

```
[admin@UplogixLM]# config system ipt
[config system ipt]#
```

Once in the editor, you can use the `?` command to view a list of possible configuration options.

```
[config system ipt]# ?
Allowable arguments are:
show
[no] subinterface

duration
endpoints
[no] listen

payload
[no] allow
[no] deny
or 'exit' to quit config mode
```

Use the `subinterface {subinterface_name}` command in this editor to configure the Local Manager to listen for IP Telephony traffic on the voice VLAN subinterface (substituting the name of the voice subinterface for subinterface_name). The following example configures the Local manager to listen for IPT traffic on the subinterface named 'voice,' displays the IPT settings and then exits the IPT editor.

```
[config system ipt]# subinterface voice
[config system ipt]# show
subinterface voice
duration 30
```

```
endpoints 10
listen true
payload harvardfemale

[config system ipt]# exit
```

Configure a Static Route for the Management Interface

For the case where a trunk is used to connect the Local Manager to the network, the main management interface uses the trunk native VLAN (usually VLAN=1, unless otherwise specified in the switch port configuration), which is configured using the `config system ip` command. Use the `config system route` command to enter the route editor.

```
[admin@UplogixLM]# config system route
Warning: Remote connections may be lost if you commit changes.
[config route]#
```

Once in the editor, you can use the `?` command to view a list of possible configuration options.

```
[config route]# ?
Allowable arguments are:
show
[no] route
or 'exit' to quit config mode
```

`show`	Display the current static routes for the management interface.
`[no] route {IPv4_address/netmask_bits | IPv6_address/netmask_bits }`	Set an IPv4 or IPv6 static route to be associated with the management interface. The no prefix will remove the static route from the management interface. Example: To route all outgoing traffic headed to the 192.0.2.0/24 network over the in-band management Ethernet interface, use `route 192.0.2.0/24`. To route all outgoing traffic headed for 2001:DB8::0/32, use `route 2001:DB8::0/32`.
`exit`	Exit the configuration editor.

It is important to note two things here:

1. Connectivity to the Local Manager will be temporarily lost while the route(s) are applied to the management interface.
2. IPv6 static routes can only be added to the management interface for the case where a static IPv6 address was assigned to the management interface using the config system ipv6 command (i.e. static IPv6 routes are not allowed if IPv6 auto configuration is enabled for the Local Manager).

Display System Routes

Use the `show system route` command to view the Local Manager routing table, which includes user defined static routes on the management interface and subinterfaces.

```
[admin@UplogixLM]# show system route
Destination                   Gateway                       Interface
Default                       192.0.2.254                 Management
203.0.113.0/24                   192.0.2.254                 voice
192.0.2.0/24                                              Management
198.51.100.0/24                                              voice
192.0.2.1/32               192.0.2.254                 Management
192.0.2.0/24                192.0.2.254                 Management


Default                       fe80::20a:41ff:fe7c:8d20      Management
Default                       2001:DB8:b951:600:1222:ab71:fe01:2386 voice
2001:DB8::/32                 2001:DB8:b951:600:1222:ab71:fe01:2386 voice
2001:DB8:b951:600::/64                                      voice
2001:DB8:b851:10::/64                                       Management
```

Capture Mode

This mode allows the capture and review of network traffic via the Secondary Ethernet interface.

- The maximum size of the capture file is 5MB. Collection will automatically stop when this limit is reached.
- Traffic can be captured from a switch port in port monitor mode if the switch is configured correctly.

Device Configuration

To enable capture mode, run the `config system secondary` command from the system resource and specify capture as the type.

```
[admin@UplogixLM]# config system secondary
>> output removed <<
Change these? (y/n) [n]: y
Type: [outband]: capture
speed/duplex: [auto]:
Do you want to commit these changes? (y/n): y
```

Capturing Packets (Basic)

To begin capturing packets, use the capture command from the system resource. Capture will continue until you press x, CTRL+C, or the 5MB capture limit is reached.

```
[admin@UplogixLM]# capture
Press 'x' or Ctrl+C to stop capturing packets.
4864 bytes
Capture stopped.
```

Capturing Packets (Advanced)

A variety of options are available to filter captured packets.

IP Address	`capture host 192.0.2.100`
Network	`capture net 192.0.2.0/24`
Port	`capture port 80`
IP Address & Port	`capture host 192.0.2.100 and port 80`
Source	`capture src 192.0.2.1`
Destination	`capture destination 192.0.2.253`
Frame Size	`capture greater 512, capture less 128`
Bytes Per Frame	`capture -size 32`

Viewing Captured Packets

To view the capture file in plain text, use the `show capture` command.

```
[admin@UplogixLM]# show capture
18:53:25.281292 CDPv2, ttl: 180s, Device-ID '333A'[|cdp]
18:53:25.284526 CDPv2, ttl: 180s, Device-ID '333A'[|cdp]
18:53:25.287029 CDPv2, ttl: 180s, Device-ID '333A'[|cdp]
18:53:25.926118 802.1d config TOP_CHANGE 8000.00:d0:ba:bf:62:cd.8022 root
2000.00:d0:01:c1:c4:34 pathcost 23 age 3 max 20 hello 2
fdelay 15
18:53:26.315752 IP6 :: > ff02::16: HBH ICMP6, multicast listener report v2, 1 group
record(s), length 28
18:53:26.391749 IP6 :: > ff02::1:ff00:1524: ICMP6, neighbor solicitation, who has
fe80::20f:2cff:fe00:1524, length 24
18:53:26.942055 802.1d config TOP_CHANGE 8000.00:d0:ba:bf:62:cd.8022 root
2000.00:d0:01:c1:c4:34 pathcost 23 age 2 max 20 hello 2
fdelay 15
18:53:27.391840 IP6 fe80::20f:2cff:fe00:1524 > ff02::2: ICMP6, router solicitation,
length
16
18:53:28.358245 802.1d config TOP_CHANGE 8000.00:d0:ba:bf:62:cd.8022 root
2000.00:d0:01:c1:c4:34 pathcost 23 age 2 max 20 hello 2
fdelay 15
```

To export the capture file in pcap format, use the `show capture -pcap` command and pipe it to SCP, FTP, or Email.

To export via SCP, use the following syntax:

```
[admin@UplogixLM]# show capture -pcap | scp uplogix@192.0.2.226:uplogixlm.cap1
uplogix@192.0.2.226's password:*******
..
File successfully sent to 192.0.2.226.
copy succeeded
```

To export via Email, use the following syntax:

```
[admin@UplogixLM]# show capture -pcap | mailto support@uplogix.com:uplogixlm.cap1
..
File successfully sent to uplogix.com.
copy succeeded
```

In the above example, the capture file will be attached to the email with the filename *uplogixlm.cap1*. The file can then be viewed in any third party application capable of reading pcap files (Wireshark, etc.).

To export the capture file in plain text with SCP, FTP, or Email, simply omit the `–pcap` option.

Setting up frozen console monitoring and recovery

A common issue with network devices is that they become unresponsive. A device console is considered unresponsive when the following three conditions have occurred:

- The device is powered up.
- The cable is connected and the serial console is active (i.e., serial handshaking is still occurring).
- The Local Manager detects that the device’s console has been operating for at least four intervals but is no longer responding to requests.

Often the fastest way to recover an unresponsive device is to cycle power.

When used with a supported power controller, the Local Manager can power cycle the device to recover from this state.

> A device (i.e., a router) may stop responding to the console but otherwise remain fully operational. In this situation, power cycling the device may cause unnecessary disruption.

The frozen console recovery feature allows you to set a monitor to check for this condition. The criteria described above, coupled with previously successful polls of the device, trigger a power cycle.

> The Local Manager only power cycles the device once to avoid continuously rebooting the device if the hardware has been damaged.

The device must have a power mapping assigned to it.

To set up autorecovery, navigate to the port of the device to monitor.

```
[admin@UplogixLM]# port 1/2
Quest-HSGS cisco CISCO2911/K9 IOS 15.2(3)T
```

Use the autorecovery command to begin the autorecovery monitor.

```
[admin@UplogixLM (port1/2)]# autorecovery 120
Job was scheduled 13: [Interval: 00:02:00] intelligentReboot
The device is now monitored for frozen console.
```

Maintenance and Troubleshooting

Automated device maintenance and recovery operations include:

- Upgrading the Local Manager software
- Reviewing user sessions

Upgrading the Local Manager software

Log on to support.uplogix.com and navigate to the software download page.

Locate and download the appropriate file. If you are not certain which version to use, contact Technical Support at support@uplogix.com.

Choose one of the following procedures.

Upgrading from your workstation

Log into the Local Manager.

Enter the `config update` command, specifying the connection type and the location of the file. For example:

```
config update scp user@198.51.100.172:lms4.7.bin
```

or

```
config update ftp user@198.51.100.172:lms4.7.bin
```

or

```
config update http http://198.51.100.172/lms4.7.bin
```

If the Local Manager is managed by a Control Center, you can upload the upgrade file to the Control Center's file archive under a suitable file category. You can then upgrade from the Local Manager's command line using the syntax `config update ems category/file` — for example:

```
config update ems uplogixUpdates/lms4.7.bin
```

Upgrading from a USB flash drive

Connect a USB flash drive to your computer and copy these files to a USB flash drive:

```
upgrade.mnf
```

```
UplogixOS-<version>.i386.bin
```

1. Connect the USB flash drive to the Local Manager.
2. Perform one of the following:
   - On the front panel keypad, press the `Enter` key and select `Update` from the menu.

     OR
   - From your workstation, log into the Local Manager and enter the command `config update usb`. By default, the Local Manager attempts to install the `UplogixOS-[version].i386.bin` file. You can specify another file in the command; for

example, `config update usb 4.7/UplogixOS-[version].i386.bin` allows you to specify both the file and its location.

Uplogix recommends using a 1 GB FAT16 formatted USB flash drive. Upgrading the Local Manager from a FAT32 formatted flash drive may be unsuccessful.

Upgrading from Control Center

1. Login to the Control Center and go to `Administration > File Archive`.
2. Choose Upload File**.**
3. Browse to the file just downloaded from the support site, and click Upload.
4. Open the Inventory tab and navigate to the Local Manager.
5. Ensure that the Local Manager has been moved out of the Unassigned group.
6. Open and expand the detail page for the Local Manager.
7. From the list of tasks that can be scheduled, select Update and click Schedule.
8. From the list of Update parameters, select the file just uploaded and click next.
9. On the Update - Frequency page, select the date and time to start the update, and select Runs Once as the frequency. The upgrade starts immediately if you accept the defaults. Click schedule to schedule or start the upgrade.

To avoid degrading the Control Center's performance, upgrade no more than 100 Local Managers at the same time.

Reviewing user sessions

The Local Manager stores the session histories of all users. To view a list of current and previous sessions, use the `show sessions` command.

```
[admin@UplogixLM]# show sessions
Id  user         ip address       logged in            logged out
--  -----        --------------   ----------------     -----------
3       dsmith       192.0.2.24        Jul 18 16:58 UTC
2       admin        2001:DB8:3:100::150   Jul 18 12:26 UTC
1       admin        198.51.100.110    Jul 17 12:15 UTC      Jul 17 12:25 UTC
```

Use the `session id` number to view a specific session. The session is displayed page by page. The `show session` command shows a transcript of what was visible in the CLI window; for example, if the user changed a password using the `config password` command, the password is not displayed.

Type `q` at any time to quit viewing the display.

```
[admin@UplogixLM]# show session 3
------------------------------------------------------------
User: dsmith
From: 192.0.2.24
Logged In: Dec 18 16:58:54 UTC 2013
Logged Out: Still logged in
------------------------------------------------------------
> Uplogix LMS v4.7.1  -- Powering Business Uptime
```

```
>
> ------------------------------------------------------------------------------
> Port     Hostname            Status        Con Eth Uptime   Processor   Last
>                                                            Utilization  Alarm
> ---- ------------------ ------------------ --- --- ------- ----------- -------
>  1/1
>  1/2
>  1/3
>  1/4
>  PWR
>  MDM embedded                               *
>  SYS 505100099         OK                  *   *           20/21/07   43s
> ------------------------------------------------------------------------------
> Con(sole) or Eth(ernet) link status indicated with '*'
> Processor Utilization displayed as last collected, 1 and 5 minute averages
> Last Alarm displays time since last Alarm matched.
>                   d=day, h=hour, m=minute, s=second
>
> [dsmith@505100099]# show version
> Uplogix
> Serial Number: 505100099
>
>LMS version: 4.7.0.24381
>LMS build: 20131202:040331
>FIPS 140-2 mode: disabled
>Slot 2 serial number: V63070891-0

>Secondary Ethernet: supported
>Uptime: 14d 4h
>Last boot: 12/16/13-15:37:05
>Last incremental restart: 12/16/13-15:38:32
>
> [dsmith@505100099]# conf user ajones
> User ajones does not exist. Create (y/n): y
> [config user ajones]# password password
> [config user ajones]# exit
>
> [dsmith@505100099]# logout
------------------------------------------------------------
--DONE–
```

If the Local Manager is managed by a Control Center, user sessions can be viewed through the Uplogix web interface: `Inventory > Local Manager page > Session Logs`

Port Buffer Log

In some cases you may wish to review the contents of a port buffer. Navigate to the desired port and use the `show buffer` command.

Syntax:

```
show buffer [-raw | -previous]
```

The command `show buffer` displays the most recent 1 MB of data. Use the optional `-previous` parameter to view the "previous" buffer.

Use the optional `-raw` parameter to display the buffer contents without additional formatting.

You may wish to redirect the command output to a file using the pipe character.

Outband Log

The Local Manager logs detailed dialer, PPP, IP, and VPN setup and teardown information when it attempts to bring up an out-of-band connection (either in the event of an in-band network failure or during an out-of-band network test via the `ppp cycle` command). This information can be very helpful when troubleshooting out-of-band network configuration or infrastructure issues. Use the `show log outband` command on the Local Manager to view the log for the last successful or failed attempt to communicate out-of-band.

Embedded Modem Troubleshooting

You can issue the `pull tech` command followed by the `show tech` command at the modem resource to display information about the modem that can be helpful when troubleshooting modem problems. This command collects information about line voltage and loop current for V.92 modems as well as network registration state, signal strength and modem functionality mode for cellular modems.

Factory reset

In some situations, you may wish to clear all configuration information, logs, and other data stored on the Local Manager. Factory reset completes the following:

- shuts down all services
- reformats the hard drive
- reinstalls the software

No data is retained. Following a factory reset, the Local Manager is in its initial state, just as it was when it was shipped. However, it will remain on its current software revision if it has been upgraded since its purchase.

To set an individual port back to its initial state, use the `config system clear port` command. Refer to Clearing a previously configured port for more information.

Caution: Do not power off or cycle power during the factory reset process.

If the Local Manager is managed by a Control Center, delete it from the inventory before starting the factory reset.

Following a factory reset, the initial configuration steps described in the *Installation Guide for Local Managers* must be completed. Then all applicable configuration procedures in Configuring the Local Manager must be completed.

Factory Resetting a Local Manager via the CLI

Local Managers can be factory reset using the `config reinstall` command. To protect against accidental usage, this command is not included in any of the default roles. It must be added to the role of the user. In this example, we will create a new role and assign it to the admin user.

1. Create a role called reinstall.

```
[admin@UplogixLM]# config role reinstall
Role reinstall does not exist. Create (y/n): y
```

2. Add the config reinstall permission to the role.

```
[config role reinstall]# allow config reinstall
[config role reinstall]# exit
```

3. Edit the admin user and assign the reinstall role on the system resource.

```
[admin@UplogixLM]# config user admin
[config user admin]# system reinstall
[config user admin]# exit
```

4. Admin can now run the config reinstall command.

```
[admin@UplogixLM]# config reinstall
** Issuing this command will completely reset the system. **
** All data will be lost. IP connectivity will be lost. **
Proceed? (y/n): y
```

Factory Resetting an Uplogix 400, 3200 or 5000 via the Keypad

A factory reset can be initiated on one of these Local Manager platforms if you have physical access to the Local Manager keypad. To do so:

1. Press then Center button on the keypad to enter the menu.
2. Scroll down to Factory Reset, press the Center button to select it. You will have to scroll down past two blank lines.
3. Confirm your decision to Factory Reset.

By default, the Local Manager will try to acquire an IP address via DHCP, so you will have to re-address the device once it finishes.

Factory Resetting an Uplogix 500 Local Manager

1. Shut down the device, either using the `shutdown` command or by pressing and releasing the power cycle button.
2. Press and **`HOLD`** the Multi-function Button (the button with a checkmark next to it). At the same time press and release the **`Power`** button.
3. The Status LED will change from `OFF -> SLOW BLINK -> FAST BLINK`.
4. Once the Status LED changes to `FAST BLINK` you may release the Multi-Function button and the Factory Reset will begin.
5. During the Factory Reset, the Status LED will change to `SLOW BLINK` and remain in that state until the Factory Reset is complete.

You can connect to the console port of the Uplogix 500 and watch the Factory Reset process.

Factory Resetting an Uplogix 430 Local Manager

Read through the instructions completely before attempting to factory reset your device.

1. Shut down the device, either using the `shutdown` command or by pressing the power cycle button and holding it for five seconds.
2. Disconnect the power cable.
3. Press and HOLD the power button.
4. Connect the power cable.
5. The system health light will change from `OFF -> SLOW BLINK -> FAST BLINK` as the device boots up.
6. When the system health light changes to `FAST BLINK`, release the power button.
7. Immediately press and **`HOLD`** the power button again until the system health light turns off.

Release the `power` button when the system health light turns off.

You can connect to the console port of the Uplogix 430 and watch the factory reset process.

If you do not complete the sequence of button presses, the device will boot normally.

Reference

Local Manager custom device properties

The following custom device properties are available for configuration on the Local Managers.

Property	Description
`sysContact.0`	When SNMP is enabled on the Local Manager, defines the system contact.
`sysLocation.0`	When SNMP is enabled on the Local Manager, defines the system location. Useful if the Local Manager is behind a firewall or NAT.
`sshPort`	This property overrides the default port 22 for SSH connections. Useful if the Local Manger is behind a router with port forwarding capabilities.
`sshIp`	This property overrides the reported IP address when initiating an SSH connection with the CLI applet.
`sshIpv6`	Specifies an alternate IPv6 address to be used instead of the address reported by the Local Manager.
`sshPortOob`	This property overrides the default port 22 for SSH connections while the Local Manager is operating out-of-band.
`sshIpOob`	This property overrides the reported out-of-band IP address. Useful if the Local Manager is behind a firewall or NAT when it brings up its out of band connection.

Property	**Description**
`sshIpv6Oob`	Specifies an alternate IPv6 addressed to be used when the Local Manager is operating out-of-band.
`_csr_OU`	For use when placing the Local Manager in FIPS mode, the property defines the Organization Unit required when generating a certificate.
`_csr_CN`	For use when placing the Local Manager in FIPS mode, the property defines the Common Name required when generating a certificate.
`_csr_O`	For use when placing the Local Manager in FIPS mode, the property defines the Organization required when generating a certificate.
`_csr_L`	For use when placing the Local Manager in FIPS mode, the property defines the Location required when generating a certificate.
`_csr_ST`	For use when placing the Local Manager in FIPS mode, the property defines the State required when generating a certificate.
`_csr_C`	For use when placing the Local Manager in FIPS mode, the property defines the Country required when generating a certificate.
`_csr_E`	For use when placing the Local Manager in FIPS mode, the property defines the Email Address required when generating a certificate.
`_csr_other`	For use when placing the Local Manager in FIPS mode, the property defines other elements that the user may wish to include when generating a certificate.
`forwardIpAddress`	Set IP address for forwarding inbound UDP packets.

Property	Description
readCommunity	Configuration information specific to ND SatCom.
writeCommunity	Configuration information specific to ND SatCom.
Enhanced_CommandPrompt	Define an enhanced driver’s command prompt.
Enhanced_PasswordPrompt	Define an enhanced driver’s password prompt.
Enhanced_LoginPrompt	Define an enhanced driver’s login prompt.
Enhanced_LogoutCommand	Define an enhanced driver’s logout command.
Enhanced_TimeoutSeconds	Define an enhanced driver’s timeout duration in seconds.
Enhanced_WakeupCommand	Define an enhanced driver’s command to wake up a managed device.
safedelay	Define a delay period for use after a command is run.
safeDebug	For use on Sea Tel devices, define for extra log messages on the console during Push OS.
_powerOnValidationTimeout	Defines a time in milliseconds for the system to wait before checking CTS and DSR during a power on or power cycle operation.
debug	For RFC-2217 "TCP" connections and/or virtual ports set property for extra log messages on the console.

Property	Description
`_keepalive`	For use with virtual ports on Cisco devices, configure a message or character to be sent to maintain the connection.
`_ROMMON_*`	During a ROMmon recovery, ROMmon variables defined in this property will be passed to the Cisco device.
`remoteHostOrIpAddress`	For use when connecting to an IP address or port via the management Ethernet on the Local Manager, this property defines that destination host or IP Address.
`tcpPort`	For use when connecting to an IP address or port via the management Ethernet on the Local Manager, this property defines that destination port.
`_applet_failover_ssh_ip`	Set the failover SSH IP address when configuring the CLI applet to failover directly to a managed device.
`_applet_failover_ssh_port`	Set the failover SSH port when configuring the CLI applet to failover directly to a managed device.
`_applet_failover_ssh_fingerprint`	Set the SSH fingerprint when configuring the CLI applet to failover directly to a managed device.
`_lcp_echo_interval`	Define the value in seconds between LCP echo requests. Set property to 0 to disable LCP echo.
`_lcp_echo_failure`	Define the number of subsequent failures before a PPP link goes down.
`_modem_monitor_init`	This property overrides the modem initialization string on the modem monitor.
`_modem_monitor_test`	This property provides a test dial string on the modem monitor.

Property	**Description**
`_snmp_1.3.6.1.4.1.10243.10.1.5.5`	Set to "enable" if customer has a GPS attached to their Local Manager and would like the statistics to show up in SNMP.
`_snmp_.1.3.6.1.4.1.2021.10.1`	Set to "enable" to get SNMP Load Average (UCD-SNMP-MIB).
`_snmp_.1.3.6.1.2.1.25.2.3.1.1.1`	Set to "enable" to get SNMP Memory Info (HOST-RESOURCES-MIB).
`_snmp_.1.3.6.1.2.1.25.2.3.1.1.31`	Set to "enable" to get SNMP Disk Info (HOST-RESOURCES-MIB).

Support and Regulatory information

Getting technical support

The Uplogix technical support web site allows you to open and review support requests, browse the knowledge base and download software updates. You must have a user account to view this site.

Requesting an account

To create an account, send an email to support@uplogix.com with the subject line “create account”. Include this information:

- organization name
- account user’s email address
- user’s general contact information

Requesting support

Uplogix provides 24x7x365 support. If you need to contact Uplogix customer support, please provide this information:

- Product model
- Serial number and software version (use the `show version` command from the command line or use the arrow keys on the front panel to scroll through the information on the display)

Phone: 512-857-7070

Fax: 512-857-7002

URL: support.uplogix.com

Providing comments about this guide

Did you find the information you needed?

Was it accurate?

Did it help you?

Please contact our publications staff at support@uplogix.com to notify us of any issues with this guide's accuracy, completeness, or clarity.

We want you to be successful using our products. If you find a problem with this material, we will do our best to fix it.

Regulatory notices

The following section provides regulatory agency approvals for safety, electromagnetic Interference (EMI) and electromagnetic compliance (EMC).

Safety notices

Uplogix 500 and 5000: UL60950-1, CAN/CSA C22.2, NO. 60950-1, EN 60950-1:2006 +A11. Tested using IEC 60950-1:2005 (2nd Edition); Am 1:2009.

Uplogix 430: FCC Part 15, Canadian ICES-003, CISPR 22:2005, EN 55022:2006 Class A ITE Radio Disturbance Characteristics standards and the European Union EMC Directive 2004/108/EC.

Uplogix 3200 (Envoy NRM): IEC 60950-1:2001 and/or EN 60950-1:2001+A11:2004, First Edition.

EMC notices

Federal Communications Commission (FCC) Class A Sub Part B

United States Federal Communications Commission notices

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy; and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

Modifications to this product not authorized by Uplogix could void the FCC approval and negate your authority to operate the product.

RoHS compliance

The new Envoy NRM and Control Center products are in full compliance with the Directive 2002/95/EC of the European Parliament and of the Council of 27 January 2003 on the restriction of the use of certain hazardous substances in electrical and electronic equipment.

Declaration of Conformity

A full copy of the Declaration of Conformity can be obtained from:

Uplogix, Inc.
7600-B North Capitol of Texas Highway, Suite 220
Austin, Texas 78731
USA

Declaration of Conformity: This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

Déclaration de Conformité: Cet appareil est conforme aux conditions essentielles et à toute autre modalité pertinente de la Directive 1999/5/CE.

Declaración de Conformidad: Este equipo cumple los requisitos esenciales y otras cláusulas importantes de la directiva 1999/5/CE.

Konformitätserklärung: Dieses Gerät erfüllt die grundlegenden Anforderungen und sonstige maßgebliche Bestimmungen der Richtlinie 1999/5/EG.

Konformitätserklärung: Dette utstyret er i overensstemmelse med de grundlæggende krav og de relevante punkter i direktiv 1999/5/EF.