User's Guide

for Uplogix Secure Remote Management Appliances

Version 3.5

August 2008

UP500028 Rev A

www.uplogix.com

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 Uplogix appliances. Consult the ***Installation Guide for Uplogix Secure Remote Management Appliances*** to install and initially configure the appliance.

The information in this guide applies to all Uplogix secure remote management appliances except where otherwise noted.

Note: Uplogix appliances must use the same version of software as the Uplogix Control Center element management system (EMS) that manages them, though they do not need to use the same patch release.

Examples:
An Uplogix Control Center running version 3.4 software cannot manage Uplogix appliances that have been upgraded to version 3.5 software; nor can an Uplogix Control Center running version 3.5 software manage Uplogix appliances that are still using version 3.4 software.

An Uplogix Control Center EMS running any version 3.5.x software can manage Uplogix appliances running any 3.5.x software.

Information in this document is subject to change without notice.

Please visit www.uplogix.com/support for the latest updates to Uplogix product documents.

Target audience

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

Typographical conventions

The following conventions are used in this guide.

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

```
[admin@A101100303]# show who
admin ssh Mar 22 13:38 (172.30.235.126)
```

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

Navigation paths to command equivalents on the Uplogix Control Center EMS are shown in this font. For example:

Administration > Server Settings

Safety summary

Follow all cautions and warnings to protect the appliance from potential damage or loss of data, and to ensure your own safety.

Read and understand the following instructions before using the appliance:

- Follow all cautions and warnings to protect the appliance from potential damage or loss of data, and to ensure your own safety.
- Only use electrical extension cords with a current rating at least equal to that of the appliance.
- Always disconnect the appliance from power before cleaning and servicing.
- Do not spray liquids directly onto the appliance when cleaning. Always apply the liquid first to a static free cloth.
- Do not immerse the appliance in any liquid or place any liquids on it.
- Do not disassemble this appliance. To reduce the risk of shock and to maintain the warranty on the appliance, a qualified technician must perform service or repair work.
- Connect this appliance to a grounded outlet.
- Only connect the appliance to surge-protected power outlets.
- Keep ventilation openings free of any obstructions.

SAVE THESE INSTRUCTIONS.

What's new in this guide

The following items have changed in version 3.5.

New product

With version 3.5, Uplogix introduces the new Uplogix 430 secure remote management appliance - a compact 4-port appliance for smaller deployments. Where this product differs from other models, the differences are noted.

New features

The **`config system protocols ssh`** command now provides configurable encryption settings. See Configuring SSH security on page 55.

The new xbrowser feature provides remote web access to managed devices with browser-based user interfaces. See Using xbrowser on page 100.

Other changes

The products' operating system is now called RMOS.

The management server is now called the Uplogix Control Center element management system (EMS).

Some chapters in this manual have been reorganized.

Introduction to Uplogix appliances

Uplogix secure remote management appliances provide a unique platform for managing network devices from the device's perspective. The appliance's capabilities represent industry best practice networking policies.

Maintenance operations can be bundled together as automated procedures to efficiently perform complex tasks such as OS upgrades, interface cycles, and password recovery. Automated recovery procedures such as configuration rollback and recovery, boot ROM monitoring and recovery, and hung console detection are part of the appliance's integrated recovery operations. The appliance provides extensive auditing functionality through device and user activity logging, whether the network is up or down.

Uplogix appliances are designed and tested to ensure that they do not send unexpected hardware breaks to connected equipment. Uplogix products are Sun Solaris™ break-safe.

This chapter provides information about the physical features of Uplogix appliances. It also provides information about using the RMOS 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 Uplogix 430 appliance's front panel
- Working with the command line - structure, command shortcuts, and help

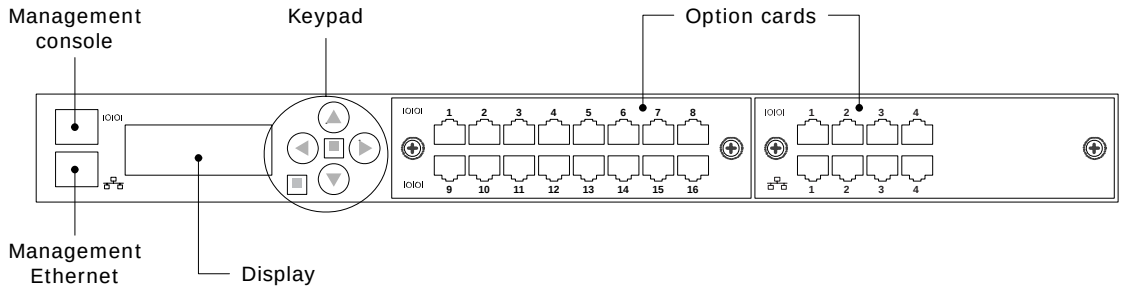
Chassis views and indicator lights

This section identifies the main physical features of Uplogix secure remote management appliances.

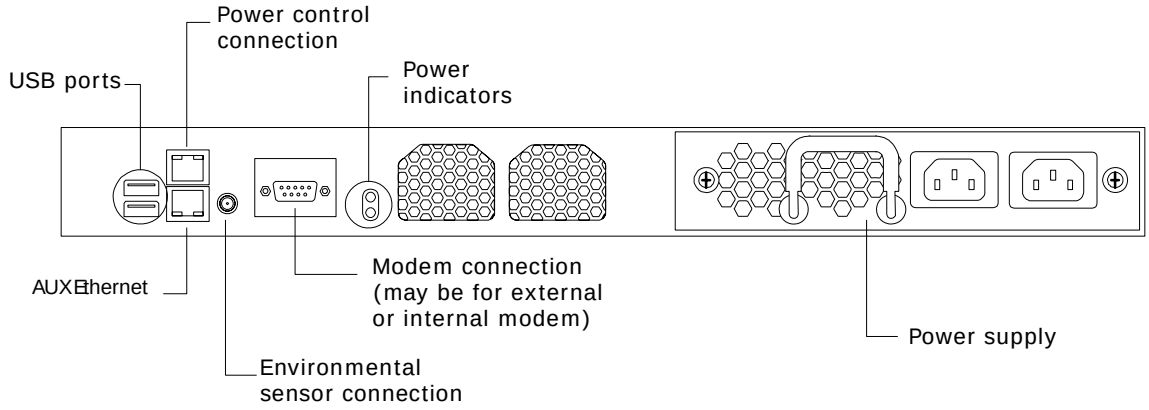
Uplogix appliances use lights to provide some basic indications of operational status. The Ethernet and serial connectors on Uplogix appliances have link and activity indicator lights. These are not present on the expansion modules for the older 4-port appliance. One of the lights (usually the green one, on the left) on the RJ-45 connector will glow when low-level connectivity is established. The other light (usually the yellow one, on the right) shows activity on the connection.

32-port Uplogix appliance

Front panel



Back panel

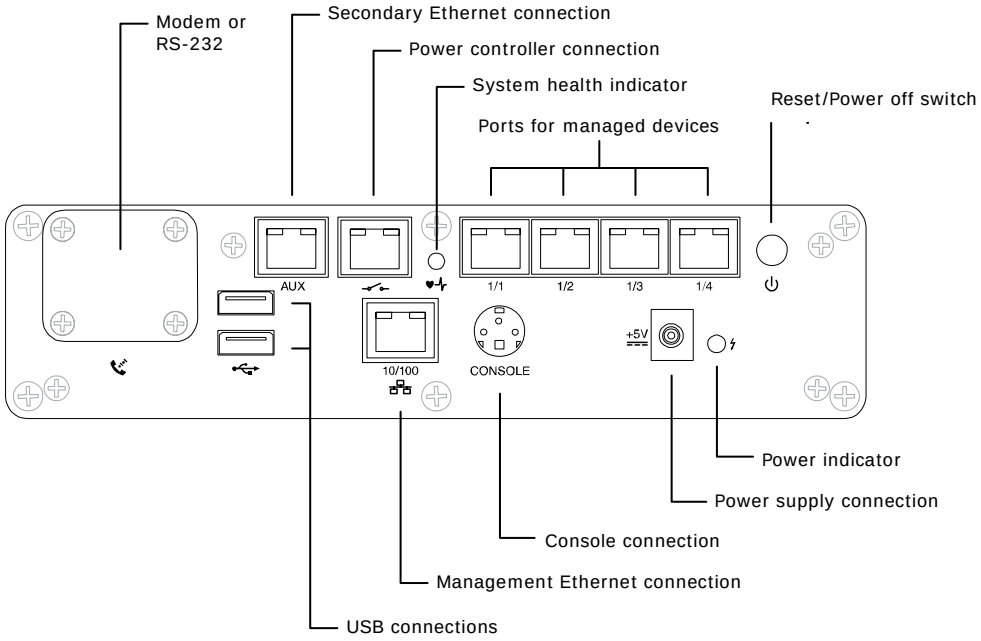


Keypad - Illuminated when the appliance is powered on; provides power and reset functionality and basic configuration capabilities.

Front panel display - Illuminated when the appliance is powered on; presents status messages and selections for power, reset, and basic configuration options.

Power indicators on the back of the chassis - Two LEDs show the status of the power supply. The lower LED indicates whether there is power to the primary power supply; this is the plug on the right.

Uplogix 430 appliance



Power indicator - Illuminates to show that power is connected.

Reset/power off switch - Allows you to restart or shut down the appliance.

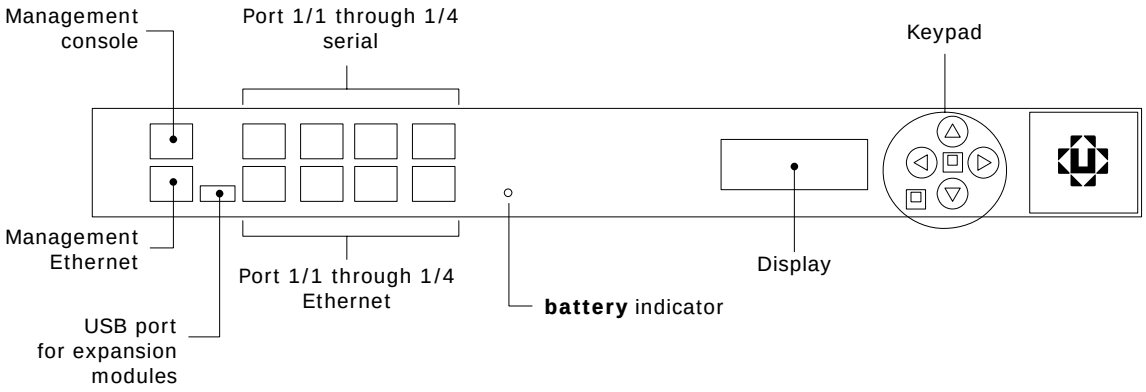
Note: After the appliance is powered off, to power on the appliance you will need to physically disconnect and then reconnect the power cable.

System health indicator - Illuminates to show that the appliance is operational. Blinks to show that an upgrade, reset, or power off operation is in progress.

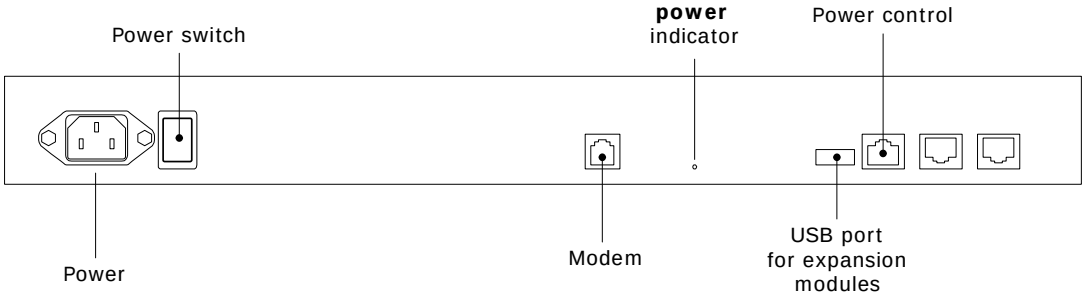
Link integrity and activity indicators on RJ-45 connectors - The Ethernet and serial connectors have link and activity indicator lights. One of the lights on the RJ-45 connector illuminates when low-level connectivity is established. The other light shows activity on the connection.

Older 4-port Uplogix appliance

Front panel



Back panel



Battery indicator (front) - Green when operating on external AC power, red when operating on battery power.

Keypad - Provides power and reset functionality and basic configuration capabilities.

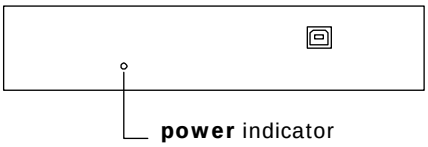
Front panel display - Illuminated when the appliance is powered on; presents status messages and selections for power, reset, and basic configuration options.

Power indicator (back) - Green when the appliance is powered on.

Expansion modules

These provide additional capacity for the older 4-port appliance. The power indicator on the back provides this information:

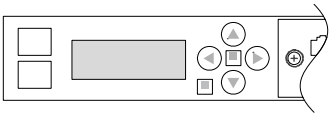
- Green: Serial ports are successfully set up and module is operating normally
- Amber: Activity on a serial port.
- Blinking amber: Installation in progress.
- Red: Loss of USB communication with the host. If the light is red but the physical connection has not been lost, you may need to reinstall the expansion module.
- Blinking red: Reconnecting to host, or installation in progress.

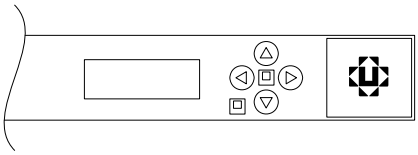


Note: Expansion modules cannot be used with other Uplogix products.

Working with the keypad

The keyboard and display are not present on the Uplogix 430 appliance.





During normal operation, the display scrolls information about the appliance. You can use the arrow keys to browse through this information rather than waiting for it to be displayed.

Press the Enter button in the center of the keypad to display the menu, which includes these functions:

- `Configure` - Covers the steps needed to allow you to work with the appliance via an SSH session. This is equivalent to the config system ip command. This function is discussed in the Installation Guide for Uplogix Secure Remote Management Appliances.
- `Restart` - Reboots the appliance and logs the event. This is equivalent to the restart command.
- `Shutdown` - Powers off the appliance. This is equivalent to the shutdown command.
- `Update` - Allows you to upgrade the software from the USB flash drive. This is equivalent to the config update usb command. This option is available only if a USB flash drive is connected to the appliance.
- `Factory reset` - Restores the appliance to its initial state. For more information, see Factory Reset on page 122.

To exit the menu and resume scrolling status information, press the Back button below the left arrow.

Working with the Uplogix 430 appliance's front panel

In most cases the RMOS command line provides the functionality you need to work with the Uplogix 430 appliance. The front panel allows basic power and reset operations.

Viewing system status messages

Progress messages that would be displayed on other Uplogix appliances' front panel displays are available via the management console connection on the Uplogix 430.

Progress messages that would be displayed on the front panel display in the case of the 32-port RC Manager are available via the management console connection on the 4-port model.

For a list of supported terminal clients, see Supported terminal clients on page 11.

Power and reset 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

Note: The connectivity indicators on the appliance's management Ethernet connector still has power when the appliance is powered down. Verify system status with the system health light.

Note: After the appliance is powered off, to power on the appliance you will need to physically disconnect and then reconnect the power cable.

Working with the command line

Uplogix appliances use the RMOS command line interface (CLI). Where commands differ among models, the differences are noted.

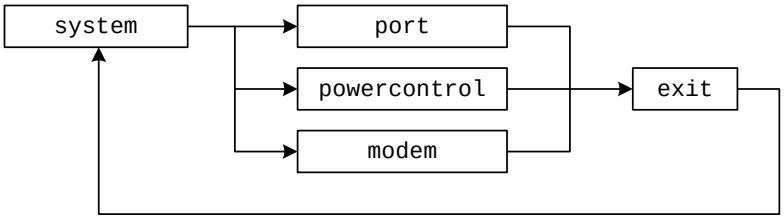
The command line is accessible from the onboard console port or via the network using SSH. Terminal access (TTY) is available via dial-in modem and Telnet, but both are disabled by default for security reasons.

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 RMOS command line employs a hierarchy for organizing the appliance, 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`	This is the root resource. All appliance configuration and user management functions are accessed from this resource.	**`exit`** (return from another resource)
`port`	Allows you to configure and manage a device connected to a device port on the appliance.	**`port <slot/number>`** (from any resource)
`powercontrol`	Allows you to configure and manage an external power controller and map its outlets to devices managed by the appliance.	**`powercontrol`** (from the `system` resource)
`modem`	Allows you to configure embedded and external modems and related settings.	**`modem`** (from the `system` resource)

Opening and closing a CLI session

Before you start, the Uplogix appliance must be installed and the initial configuration must be complete. Refer to the ***Installation Guide for Uplogix Secure Remote Management Appliances*** for information on completing these tasks.

Supported terminal clients

To use the RMOS 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)

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

Note: By default, Windows HyperTerminal uses hardware flow control. The Uplogix 430 appliance does not use flow control. If you use HyperTerminal with the Uplogix 430 appliance, you must disable flow control when configuring the session.

Supported SSH clients

Uplogix appliances use Secure Shell (SSH) v2 software to provide secured remote access. Your remote client application must also support SSH v2.

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

- 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@192.168.1.35`

Substitute the IP address of your appliance.

Logging in

After you connect to the appliance, you will be prompted for a username and password. The default username is **`admin`** and the default password is **`password`**.

Note: Usernames and passwords are case-sensitive.

Closing the session

To exit the RMOS 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@A101100303]# config date
Displayed time is 07/24/2008 15:30:45 UTC
Uplogix time is     07/24/2008 20:30:45 UTC
Change these? (y/n) [n]: y
Current system time (MM/dd/yyyy HH:mm:ss):07/24/2008 20:33:00
Displayed time is 07/24/2008 15:33:01 UTC
Uplogix time is     07/24/2008 20:33:01 UTC
```

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

In some cases, changes are saved automatically as you make them. In other cases, however, the RMOS command line prompts you to commit the changes you have made; these changes are not made if you do not commit them.

Some interactive commands present default or current settings, which you can accept by pressing the <Enter> key.

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

Command shortcuts

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

Repeating commands

You can 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 RMOS command line allows you to abbreviate commands to the shortest string that uniquely identifies the command.

For example, you can shorten the **ping** command to **pi**. Similarly, you can shorten **show dashboard** to **sh das**.

You cannot shorten the **ping** command to **p**; this results in an error because it also matches all other commands beginning with the letter p. Similarly, you cannot shorten **show dashboard** to **sh da** because this string also 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 RMOS command line allows you to use the ***** character as a wildcard. For example, you can 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, you can 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 you may prefer to copy the output to a file that you can examine later.

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

<"command"> | <ftp | scp> username@host:/filepath/

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

show config | scp username@host:/filepath/

where **username@host:/filepath/** specifies the destination for the data.

You can get help on using the pipe redirect by entering **| ?** in the command line.

Viewing context-sensitive help

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

```
[admin@A101100303]# port ?
usage: port <slot number>/<port number>

[admin@A101100303]# config export ?
usage: export <scp | ftp> userId@IP:fileName
```

To view a list of available commands from any resource within the RMOS 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 appliance returns something like this:

```
[admin@A101100303 (modem)]# ?
Uplogix RMOS v3.5
config                  Edit settings
exit                    Exit modem menu
history                 Display command history
logout                  Exit Uplogix
port                    Commands specific to port
power                   Control power of external modem on console
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@A101100303 (modem)]# show ?
Uplogix RMOS v3.5
alarms                    Display alarms for this device
all                       Display all device configuration data
answer                    Show dialin options
buffer                    Display buffer of device output
dashboard                 Brief display of Uplogix and managed devices
events                    Shows events
info                      Display device information
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
status                    Display ppp and pptp status
vpn                       Display VPN configuration

[admin@A101100303 (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@A101100303]# history
1. config system ntp
2. modem
3. config init
4. show ?
5. show alarms
6. history
```

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

```
[admin@A101100303]# !5
show alarms
There are no alarms right now.
```

Configuring the Uplogix appliance

Before you start the tasks in this section, the procedures in the ***Installation Guide for Uplogix Secure Remote Management Appliances*** should all have been completed.

Most of the configuration settings in this chapter are available through the **config system** commands. You can enter **config system ?** to view configurable settings. For more detailed information about the commands in this chapter, consult the ***Reference Guide for Uplogix Secure Remote Management Appliances***.

This chapter covers:

- Configuring communication settings - management IP and serial settings, out-of-band behavior, management by Uplogix Control Center element management system (EMS)
- Exporting appliance configuration - for environments in which no Uplogix 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 appliance to be managed by an Uplogix Control Center
- Configuring archiving

Configuring IP settings

The Uplogix appliance is initially configured to use DHCP. You can change this and related settings for the management Ethernet interface using the interactive **config system ip** command. On some appliances, you can also do this from the front panel keypad.

```
[admin@A101100303]# config system ip
--- Existing Values ---
Use DHCP: No
Management IP: 172.30.238.102
Host Name: xyzcoAus01
Subnet Mask: 255.255.255.0
Broadcast Address: 172.30.238.255
Default Route: 172.30.238.254
Speed/duplex: auto:100full
DNS Server:
MAC Address: 00:0F:2C:00:02:BF
Change these? (y/n) [n]: y
```

Note: If the appliance is licensed for Service Level Verification (SLV), it automatically uses domain name resolution for the SLV tests that require it. Most commands do not use DNS.

Configuring the management console port

The appliance's default management console connection settings are 9600 baud, 8 data bits, 1 stop bit, no parity, and no flow control.

Note: By default, Windows HyperTerminal uses hardware flow control. The Uplogix 430 appliance does not use flow control. If you use HyperTerminal with the Uplogix 430 appliance, you must disable flow control when configuring the session.

Uplogix 32-port and older 4-port appliances' console ports accept standard RS-232 serial cables with RJ-45 connectors, but can be configured to use null modem cables instead.

The Uplogix 430 appliance is shipped with its own console cable. You do not need to enable null modem on the Uplogix 430 appliance.

To use a null modem cable, use the interactive **config system serial** command and enable the null modem setting, if it was not enabled during initial configuration when the appliance was installed.

```
[admin@A101100303]# 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 Uplogix appliance is managed by an Uplogix Control Center EMS, null modem can be configured through the Uplogix web interface.

For a single appliance: **Inventory > expanded appliance page > Configuration** tab **> Serial**

For a group of appliances: **Inventory > group page > appliance configuration** button **> Serial**

Configuring the appliance to be managed by an Uplogix Control Center

Uplogix appliances can be managed by an Uplogix Control Center element management system (EMS), a centralized web-based interface for managing multiple appliances in an enterprise. Once integrated, the Uplogix 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.

Uplogix appliances communicate with the Uplogix Control Center server via a heartbeat function. The interval is configurable; the default is 30 seconds.

To configure the appliance to communicate with an Uplogix Control Center EMS, use the interactive **config system management** command.

```
[admin@xyzcoAus01]# config system management
--- Existing  Values ---
Use EMS: false
EMS Server Hostname or IP: 127.0.0.1
EMS Server Port: 8443
Heartbeat interval (seconds): 30
Heartbeat band: all
Last successful heartbeat:  (not yet contacted)
Change these? (y/n) [n]: y
--- Enter New Values ---
Use EMS: (y/n) [n]: y
EMS Server IP: [127.0.0.1]: 172.30.51.20
Set ntp location to 172.30.50.20: (y/n) [y]:
EMS Server Port: [8443]:
Heartbeat interval (seconds): [30]:
Heartbeat during: [all]:
Do you want to commit these changes? (y/n): y
```

Note that you can change the default port and heartbeat interval with this command. You can also specify that heartbeat occurs during all operation, 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. See Configuring IP settings on page 17.

After the appliance contacts the server, you can configure archiving if you did not do so in the **config system ip** interaction.

Note: When the appliance is managed by an Uplogix Control Center EMS, changes that you make via the RMOS command line will show up on the Uplogix web interface after the next heartbeat. Similarly, changes that you make to the appliance using the Uplogix web interface will be available on the appliance after the next heartbeat.

Configuring archiving

If the Uplogix appliance is managed by an Uplogix Control Center EMS, it uploads device statistics, user sessions, device files, and other data to the EMS at regular intervals. Archiving uses high data compression to reduce network impact. It is disabled when operating out of band.

Archiving occurs over port 8443, and is configured automatically when you configure the appliance to use EMS. To see the appliance's current archive settings, use the **show system archive** command.

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

```
[admin@xyzcoAus01]# config system archive
--- Existing  Values ---
Time Between Archivals: 3,600
Maximum Archives Stored Locally: 100
Change these? (y/n) [n]:
```

If the Uplogix appliance is not managed by an Uplogix Control Center EMS, export the appliance configuration to archive data from the appliance.

Archiving can be configured through the Uplogix web interface.

For a single appliance: **Inventory > expanded appliance page > Configuration** tab **> Archive**

For a group of appliances: **Inventory > group page > appliance configuration** button **> Archive**

Exporting appliance configuration

Use this feature to back up appliance configuration data if the Uplogix appliance is not managed by an Uplogix Control Center EMS.

The **config export** command uses FTP or SCP to export the appliance configuration as an XML file to a location that you specify. The XML file can be loaded back onto the appliance using the **config import** command. You can use the **show config** command view the data that will be exported.

This feature is not available if the appliance is managed by an Uplogix Control Center EMS. Instead, the EMS automatically archives appliance information hourly.

Configuring CLI behavior

This section covers the following topics:

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

Setting and clearing banners

Uplogix appliances can display two banners:

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

By default, no banners are defined.

Setting banners

You can 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, which may use more than one line. When you are finished, use the **exit** command to leave the editor and return to the main CLI.

```
[admin@xyzcoAus01]# config system banner welcome
Type 'exit' on a line by itself to exit
[config system banner welcome]# You are now logged in to xyzcoAus01.
[config system banner welcome]# exit
```

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

Note: Some SSH clients do not support the login banner.

You can verify the current banners with the **show system banner** command:

```
[admin@xyzcoAus01]# show system banner
Welcome Banner:
You are now logged in to xyzcoAus01.
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@xyzcoAus01]# config system banner welcome
Type 'exit' on a line by itself to exit
[config system banner welcome]# exit
[admin@xyzcoAus01]# show system banner
Welcome Banner:

Login Banner:
No login banner set.
```

If the Uplogix appliance is managed by an Uplogix Control Center EMS, banners can be configured through the Uplogix web interface.

For a single appliance: **Inventory > expanded appliance page > Configuration** tab **> Banners**

For a group of appliances: **Inventory > group page > appliance configuration** button **> Banners**

Setting CLI page length

By default, Uplogix appliances automatically try 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@xyzcoAus01]# config system page-length
Page length preference is auto.
Change this? (y/n) [n]: y
Page length preference (2 or more lines or auto):15
```

In this example, the command line will display 15 lines before prompting you to press a key to scroll the display.

Setting session timeout

Uplogix appliances 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@xyzcoAus01]# config system timeout
Current session timeout is 5 minutes.
Change these? (y/n) [n]: y
Timeout (5 to 120 minutes): [15]: 10
```

This example changes the inactivity timeout to 10 minutes.

If the Uplogix appliance is managed by an Uplogix Control Center EMS, timeout can be configured through the Uplogix web interface.

For a single appliance: **Inventory > expanded appliance page > Configuration** tab **> Timeout**

For a group of appliances: **Inventory > group page > appliance configuration** button **> 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

Uplogix appliances can be configured to notify administrators of certain situations by email.

The appliance'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@xyzcoAus01]# config system email
--- Existing  Values ---
In band SMTP Server IP Address: 127.0.0.1
In band FROM address: system@127.0.0.1
In band SMTP Port: 25
Use user authentication in band: no
Out of band SMTP Server IP Address: 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
Change these? (y/n) [n]:
```

This example shows the default values.

If the Uplogix appliance is managed by an Uplogix Control Center EMS, the originating email address can be configured through the Uplogix web interface.

For a single appliance: **Inventory > expanded appliance page > Configuration** tab **> Email**

For a group of appliances: **Inventory > group page > appliance configuration** button **> 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, Uplogix appliances use Coordinated Universal Time (UTC); the time is set at the factory.

If the appliance is configured to work with an Uplogix Control Center element management system (EMS), by default it uses the date and time from the Uplogix Control Center.

The date and time settings can be adjusted manually, or the appliance can be configured to use a separate Network Time Protocol (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 appliance.

```
[admin@xyzcoAus01]# config date
Displayed time is 07/01/2008 14:56:49 UTC
System time is     07/01/2008 14:56:49 UTC
Change these? (y/n) [n]:
```

Setting the appliance to use an NTP server

To override time and date settings from the Uplogix Control Center, or to specify an NTP server of your own, 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@xyzcoAus01]# 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 IP: []: 172.30.51.20
NTP Secondary Server IP: []:
Do you want to commit these changes? (y/n):
```

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

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

For a single appliance: **Inventory > expanded appliance page > Configuration** tab **> NTP**

For a group of appliances: **Inventory > group page > appliance configuration** button **> NTP**

Setting environmental thresholds

The 32-port model uses an optional external probe to measure temperature, providing constant and reliable environmental monitoring. The older 4-port Envoy appliance uses an internal temperature/humidity sensor mounted at the air intake. The Uplogix 430 appliance does not have environmental sensing capabilities.

The default temperature limit for Uplogix appliances with sensing capability is 95° F (35° C), and the default humidity limit is 85%. If the temperature or humidity exceeds the defined threshold, this triggers an alarm.

Alarms are not triggered if the relevant data is unavailable – for example, if no sensor is installed.

Temperature and humidity thresholds can be changed using the **config environment** command. The appliance can use Celsius instead of Fahrenheit.

```
[admin@xyzcoAus01]# config environment
--- Existing  Values ---
Humidity Threshold: 85.0
Temperature Threshold: 95.0
Use Celsius: 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
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 Uplogix Control Center EMS. For example:

```
[admin@xyzcoAus01Leander]# config system properties
[config system properties]# installDate 07/10/08
[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 appliance.

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

If the Uplogix appliance is managed by an Uplogix Control Center EMS, properties can be configured through the Uplogix web interface:

Inventory > expanded appliance page > Status tab **> Properties**

Configuring syslog forwarding

The interactive command **config system syslog** allows you to enable syslog forwarding. Specify the server IP address and port number, and select the syslog facility to write to (such as local1, local2, etc).

```
[admin@A101100303]# config system syslog
--- Existing  Values ---
Syslog enabled: no
Syslog server IP:
Syslog port number: 514
Syslog facility:
Change these? (y/n) [n]:
```

If the Uplogix appliance is managed by an Uplogix Control Center EMS, syslog settings can be configured through the Uplogix web interface.

For a single appliance: **Inventory > expanded appliance page > Configuration** tab **> Syslog**

For a group of appliances: **Inventory > group page > appliance configuration** button **> Syslog**

Configuring SNMP settings

Uplogix appliances can report back SNMP information to snmp-get or snmp-walk requests. By default, SNMP is disabled. You can enable SNMP on the appliance with the **config system snmp** command:

```
[admin@xyzcoAus01]# 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 turn off SNMP completely.

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

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, and 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 appliance with the authPriv security level.

Note: 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@A101100569]# config system properties
[config properties]# sysLocation.0 Austin, TX
[config properties]# sysContact.0 T.McMillan
[config properties]# exit
```

If the Uplogix appliance is managed by an Uplogix Control Center EMS, SNMP settings can be configured through the Uplogix web interface.

For a single appliance: **Inventory > expanded appliance page > Configuration** tab **> SNMP**

For a group of appliances: **Inventory > group page > appliance configuration** button **> SNMP**

Configuring out-of-band communication

The appliance determines network connectivity by sending a pulse to a Pulse server on TCP port 7 (echo) every 30 seconds. You can configure the appliance to respond to a loss of connectivity - defined as no echo for four consecutive pulses - by initiating an out-of-band connection to a point-to-point protocol (PPP) server or enabling the modem for dial-in. Point-to-point tunneling protocol (PPTP) or virtual private network (VPN) clients allow you to use the Internet as an out-of-band provider.

During out-of-band operation, the appliance 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 appliance over the out-of-band connection via SSH, the dial-up 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 will be disabled until normal connectivity is restored. However, complete archives will be cached and will resume once the in-band network has been restored. SLV tests are also suspended during out-of-band operation.

The appliance 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 Uplogix Control Center

Configuring pulse settings

To determine when to initiate an out-of-band connection, the Uplogix appliance sends a TCP echo packet to a pulse host every 30 seconds. The echo packets are under 64 bytes to limit impact on the network. If the pulse server does not echo packets for four consecutive attempts, the appliance triggers a PPP connection or enables the modem for dial-in access. The echo is expected to return the exact data sent.

Note: To use the modem's dial-in access feature for out-of-band connectivity, you must configure it to answer on pulse failure using the **`config answer`** command. See Configuring the modem (next section) for more information.

To configure the pulse process, select a host in your network to be the pulse server. The host should be a reliable indicator of good network connectivity. The Uplogix Control Center can be used as a pulse server; however, it should be given a secondary IP address to prevent routing issues when the network is down. If the appliance cannot communicate with the server, it cannot deliver network data or receive configuration updates. For more information, contact support@uplogix.com.

By default, the appliance uses TCP port 7 for the pulse process; this is configurable.

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

```
[admin@xyzcoAus01]# config system pulse
--- Existing  Values ---
Use Pulse: false
Pulse Server IP: 127.0.0.1
Pulse Server Port: 7
Dial Out when pulse fails: no
Change these? (y/n) [n]: y
--- Enter New Values ---
Enable ppp to dial out on pulse failure: (y/n) [n]: y
Use Pulse: (y/n) [n]: y
Pulse IP: [127.0.0.1]: 172.30.237.18
Pulse Port: [7]:
Do you want to commit these changes? (y/n): y
```

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

If the Uplogix appliance is managed by an Uplogix Control Center EMS, pulse can be configured through the Uplogix web interface.

For a single appliance: **Inventory > expanded appliance page > Configuration** tab **> Pulse**

For a group of appliances: **Inventory > group page > appliance configuration** button **> Pulse**

Configuring the modem

By default, the modem refuses incoming calls. You must enable this capability in order to use it.

The Uplogix appliance can be configured to accept dial-in calls during out-of-band operation. 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.

The appliance is available with an internal modem; or you may use an external modem. If you use an external modem, you must initialize it first.

Enabling dial-in and setting answering behavior

To prevent unauthorized access, the modem's default behavior is to ignore incoming calls. When you enable the modem 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 you configure the modem 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.

Note: If you use the **pulse** subcommand to enable the modem to answer on Pulse failure, the modem will do so whether you have applied the **enable** subcommand or not.

disable - Disable the dial-in feature.

init "" ATZ <modem init string> - Set the modem init string.

Note: Be sure to include the double quotes in the **init** string. This is one of the commonest causes of modem issues.

[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, you could **allow 512** to permit access from any number in the 512 area code. You may wish to specify the range of numbers assigned to your organization, for example **allow 5128577**.

[no] deny <phone number> - Specify a phone number or range of phone numbers that will be refused.

[no] number <envoy phone number> and **[no] domain <SMS domain name>** - To allow an Uplogix Control Center EMS to establish contact with an Uplogix appliance in a remote location via Iridium modem, set **number** as the appliance's phone number and **domain** as the service provider's SMS domain name. The Uplogix 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 appliance ignores an incoming call until it hangs up. If the user calls back within a specified amount of time, the appliance 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 **no enable** and **disable** subcommands.

[no] suspend - Disable SLV tests when PPP is enabled. This is the default behavior.

If the Uplogix appliance is managed by an Uplogix Control Center EMS, the modem can be configured through the Uplogix web interface.

For a single appliance: **Inventory > expanded appliance page > Configuration** tab **> Modem**

For a group of appliances: **Inventory > group page > appliance configuration** button **> Modem**

Optional: Specifying an external modem

To configure an external modem, navigate to the modem resource and use the **config init** command.

```
[admin@xyzcoAus01]# modem
 embedded

[admin@xyzcoAus01 (modem)]# config init
This device has already been initialized.
Would you like to reinitialize it? (y/n): y
--- Enter New Values ---
description: []: Iridium 9522A
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):
```

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

```
[admin@xyzcoAus01 (modem)]# config info
Hostname:
Description: Iridium 9522A
Make: Iridium
Model:
OS:
OS Version:
Management IP:
Change these? (y/n) [n]:

[admin@xyzcoAus01 (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
Overrun Errors: 0
Change these? (y/n) [n]:
```

Configuring PPP

To enable out-of-band communication with the Uplogix appliance, use the **config ppp** command in the modem resource to configure PPP settings.

```
[admin@xyzcoAus01]# modem
 embedded
[admin@xyzcoAus01 (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: []: 5125550001
User Name: []: xyzcoaus01
Password []: *****
Confirm Password: *****
Use Static IP Address: (y/n): n
Do you want to commit these changes? (y/n): y
```

Phone Number is the phone number of the line in to your modem.

The username and password are used for authenticating with the dial-up service provider.

If you have configured the appliance to use an Iridium modem, answer **y** to the prompt Use static IP address to assign an IP address to the modem.

If the Uplogix appliance is managed by an Uplogix Control Center EMS, PPP can be configured through the Uplogix web interface.

For a single appliance: **Inventory > expanded appliance page > Configuration** tab **> PPP**

For a group of appliances: **Inventory > group page > appliance configuration** buttons **> PPP**

Configuring VPN settings

To configure the Uplogix appliance 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@xyzcoAus01]# modem
 embedded
[admin@xyzcoAus01 (modem)]# config vpn
--- Existing  Values ---
VPN type: none
Change these? (y/n) [n]: y
--- Enter New Values ---
VPN type: [none]: ipsec
IPsec Server IP: []:
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@xyzcoAus01 (modem)]# config vpn
--- Existing  Values ---
VPN type: none
Change these? (y/n) [n]: y
--- Enter New Values ---
VPN type: [none]: pptp
PPTP Server IP: []:
User Name: []:
Password []:
Do you want to use encryption for pptp: (y/n):
Do you want to use mppe: (y/n) [n]:
Do you want to refuse 40 bit encryption: (y/n) [n]:
Do you want to refuse 128 bit encryption: (y/n) [n]:
Do you want to refuse stateless encryption: (y/n) [n]:
Do you want to commit these changes? (y/n):
```

If the Uplogix appliance is managed by an Uplogix Control Center EMS, the modem can be configured through the Uplogix web interface.

For a single appliance: **Inventory > appliance page > Configuration** tab **> VPN**

For a group of appliances: **Inventory > group page > appliance configuration** button **> VPN**

Configuring remote locations to be contacted by the Uplogix Control Center

In environments where appliances contact the Uplogix Control Center EMS as needed via satellite modem, you can initiate contact from the Uplogix Control Center by sending an SMS message instructing an Uplogix appliance to start PPP.

Requirements for using this capability are:

- The appliance uses an Iridium modem.
- The appliance has been configured with a phone number and SMS domain name. These are configured with the **config answer** command.

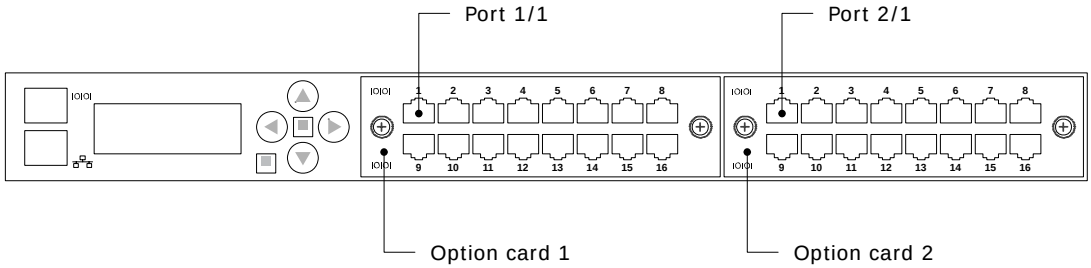
Using the **config answer** editor, set the appliance's phone number with the **number** subcommand, and use the **domain** subcommand to set the service provider's SMS domain name. The Uplogix Control Center uses these parameters to construct a valid SMS email address, to which it can send the ppp on message to establish contact.

For more information about the **config answer** command, see Configuring the modem on page 31.

Configuring managed devices and power control

The Uplogix appliance's device ports are initially configured to the "native" settings used for devices not explicitly supported. When you connect a supported device, you will need to initialize the port for the specific device being managed. Once the initial configuration is complete, minor device changes may be recommended to facilitate timely and efficient collection of data from the device, such as increased console port speed and optimized logging.

On the 32-port appliance, ports are designated by slot and port number, starting with port 1/1 on the first option card and port 2/1 on the second option card.



The Uplogix 430 appliance provides device ports 1/1 through 1/4 only.

For a list of supported devices, see the ***Reference Guide for Uplogix Secure Remote Management Appliances***.

This chapter covers:

- Configuring the appliance to assign DHCP addresses to connected devices
- Initializing the port
- Configuring default settings for managed devices
- Fine-tuning the device's configuration
- Changing device configuration after initial set-up
- Configuring SSH or Telnet pass-through protocol
- Customizing device hostname and status messages
- Clearing a previously configured port
- Configuring power control

Configuring the appliance to assign DHCP addresses to connected devices

When you connect devices to the Uplogix appliance's device ports, you can configure their dedicated Ethernet connections to use static IP addresses, or to acquire DHCP addresses from the appliance. This capability is available whether the appliance itself uses a static IP address or a DHCP address.

Note: This capability is not available for the Uplogix 430 appliance, as it provides serial device ports only.

When setting the appliance 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 you do not ensure all of these requirements are met, the appliance 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.

You must restart the appliance for this change to take effect.

You will also need to configure the devices connected to individual ports to use DHCP. When you configure a device on a port using the **config init** command, the dialog asks if you wish to configure a dedicated Ethernet port. When you respond **y**, the next prompt asks whether you wish to use DHCP.

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

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

Note: Changes to the **config system protocols dhcp** setting take effect after you **restart** the Uplogix appliance.

Initializing ports

By default, the Uplogix appliance's device ports are configured to the native setting: 9600, 8, n, 1. This replaces the generic setting in previous releases.

When you connect a device, the next step is to initialize the device port to use the appropriate driver and to enable active monitoring and control of the device. Navigate to the appropriate **port** resource and use the **config init** command to set up the port. You will need to do this even if the native settings are appropriate for the device; otherwise, the device information is not displayed when you use the **show dashboard** command.

The settings presented vary by device make and model. Consult the device's documentation for configuration settings. In addition, Ethernet-related settings are not presented if you are using an Uplogix 430 appliance.

```
[admin@xyzcoAus01 (port1/1)]# config init
--- Enter New Values ---
description: []: tasman6300
make: [native]: tasman
model: []: 6300
os: []: tios
os version: []:
management IP: []:
configure dedicated ethernet port? (y/n) [n]:
console username: []: tasman
console password []: *********
confirm password: *********
enable username: []:
enable password []:
serial bit rate [9600]:
serial data bit [8]:
serial parity [none]:
serial stop bit [1]:
serial flow control [none]:
use null modem (rolled cable to device)? (y/n) [n]:
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     : TASMAN-6300
Serial Number: 63000AISD0510009
Make         : tasman
Model        : 6300
OS Type      : TiOS
OS Version   : r6
Uptime       : 121:11:35
Updating OS version.
Assimilating the device will set buffered logging on the console.
Proceed? (y/n): y
Retrieving running-config from device via console...
Done.
- Output removed -
```

You may wish to skip the assimilation process for now, and modify the device settings separately. See Configuring default settings for managed devices on page 43 and Fine-tuning the device's configuration on page 44.

Description (optional free text field up to 255 characters) - For information about the device attached to the port. This will be used as the device hostname, and will be displayed as part of the information that normally scrolls on the appliance's front panel display.

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

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

- 3Com
- Alcatel
- Cisco
- Comtech
- Garmin
- HP
- iDirect
- Juniper
- ND SatCom
- Netscreen
- Nortel
- Sun
- Tasman
- TippingPoint
- server
- ppp
- native

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

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 you enter here will be replaced by what is actually detected by the appliance 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, 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 you enter here will be replaced by what the appliance detects on this port, unless the device is configured as `native`.

Management IP address (optional) - This field is for the IP address of the lowest numbered interface on the device (Ethernet0, for example). This address is used 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 maintain Ethernet heartbeat with the device (link integrity) as well as the default file transfer conduit between the Uplogix appliance and the device. 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**.

Note: If you configure a dedicated Ethernet port on a switch, please read About using dedicated Ethernet ports on switches (next section).

Use DHCP (available if you opt to configure a dedicated Ethernet port) - Configures the device to request an IP address from the appliance.

Note: To use this feature, you must also configure the appliance to assign DHCP addresses. See Configuring the appliance to assign DHCP addresses to connected devices on page 38.

Dedicated device IP (required if using dedicated Ethernet port) - This is the IP on the managed device. This IP is not used when reporting for SYSLOG/SNMP, 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) - This is the IP address that the appliance uses to communicate with the device.

Dedicated Ethernet subnet mask (required if using dedicated Ethernet port) - This is the subnet mask of the device.

Note: Each device's dedicated network must be on its own subnet.

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

Console username (optional free text field)

Console password (optional free text field, usually required)

Enable username (optional free text field) - not necessary if there is no distinguished super user account.

Enable password (optional free text field, usually required) - This field is also used as the root password for Juniper devices.

Secondary Console username (Cisco only - optional free text field) - for use in situations that require the device to use an alternate authentication scheme, such as TACACS/RADIUS failure.

Secondary Console password (Cisco only - optional free text field) - for use in situations that require the device to use an alternate authentication scheme.

Secondary Enable username (Cisco only - optional free text field) - for use in situations that require the device to use an alternate authentication scheme.

Secondary Enable password (Cisco only - optional free text field) - for use in situations that require the device to use an alternate authentication scheme.

Serial bit rate (optional) - The bit rate that the managed device uses. Available settings are 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200.

Serial data bit (optional) – The number of data bits (7 or 8) that the managed device uses.

Serial parity (optional) – The parity setting (none, even, or odd) that the managed device uses.

Serial stop bit (optional) – The number of stop bits (1 or 2) that the managed device uses.

Null modem (optional) - If a rolled cable is used, enter **y**.

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

When you commit the changes, the Uplogix appliance queries the device based on the information that you enter. Model and OS version may be replaced with specific information collected from the device.

About using dedicated Ethernet ports on switches

Note: For a switch configured to use a dedicated Ethernet port with a static IP address, the appliance turns off the interface except when it is needed. When the appliance turns on the dedicated Ethernet port, it takes about 30 seconds to become active.

Because of this, 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.*

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

There are two ways to prevent the problem:

- Configure the dedicated Ethernet connection to use DHCP (not available for Uplogix 430 appliances),
  OR
- Enable portfast on the switch port:

```
interface FastEthernet1/0/1
description dedicated ethernet to envoy
switchport access vlan 2
spanning-tree portfast
```

Configuring default 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 Uplogix appliance's factory default settings 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@xyzcoAus01 (port1/1)]# config settings
--- Settings Menu ---
1 Assimilated terminal speed: 19,200
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 Done
Select setting to edit or 22 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 Uplogix appliance is managed by an Uplogix Control Center EMS, you can configure settings from the Uplogix web interface.

For a single device: **Inventory > appliance page > port detail > Port Settings**

For devices on a single appliance: **Inventory > expanded appliance page > Status** tab **> Default Port Settings**

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

Fine-tuning the device's configuration

The assimilation process optimizes the device's configuration using predefined settings as described in the previous section, Configuring default settings for managed devices. 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, you can do this fine-tuning step later, either automatically or manually.

Changing the device configuration manually

If you do not assimilate the device, you may need to make these changes manually.

Device console baud rate

When device baud rate is defined during the initialization process, the Uplogix appliance assumes that the device is also using that rate. If the baud rate definitions are synchronized for the appliance and the device, the initialization process takes place. After it completes successfully, the assimilation process begins. During assimilation, the appliance sets the baud rate based on the settings defined for that type of device using the **config settings** command.

To specify the device's post-initialization/assimilation baud rate, use the **config settings** command to change the first and second options. By default, the second option prevents the assimilation process from changing the device's baud rate. To change this, change the first option to specify the baud rate the device should use, and change the second to allow this to be set during assimilation.

Used together, these allow you to set the assimilated terminal speed as desired:

```
[admin@A101100303 (port1/1)]# config settings
--- Settings Menu ---
1 Assimilated terminal speed: 19,200
2 Modify terminal serial speed on assimilation: false

[output removed]

Select setting to edit or 22 to end: 1
Assimilated terminal speed: 19,200 [19200]: 38400

[output removed]

Select setting to edit or 22 to end:2
Modify terminal serial speed on assimilation: false [false]: true
```

Then use the **assimilate** command to start the assimilation process.

Synchronous logging (Cisco only)

Enabling logging synchronous is done so that device-originated console output is displayed after console output originated by the user or by the Uplogix appliance. For example, if the appliance 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 if you need to change this.

```
[admin@A101100303 (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]:
```

Buffered logging

To minimize the load on the network device, turn on buffered logging so the appliance can refer recurrently 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 if you need to change this.

Note: Some devices do not support buffered logging. The Uplogix appliance 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 on page 43.

```
[admin@xyzcoAus01 (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.

If the Uplogix appliance is managed by an Uplogix Control Center EMS, the device changes can be made through the Uplogix web interface:

Inventory > appliance page> port detail > Port Settings

Changing device configuration after initial set-up

The settings configured with the **config init** command can be updated at any time after you set up the port (see Initializing ports on page 39) through the use of additional commands.

config authentication	Allows you to change authentication settings for the device, including Console/Enable usernames and passwords.
config device logging	Configures logging settings for the port.
config info	Configures hostname, make, OS, and related fields.
config serial	Configures serial settings.

If the Uplogix appliance is managed by an Uplogix Control Center EMS, device configuration can be changed through the Uplogix web interface:

Inventory > appliance page > port detail

Configuring SSH or Telnet terminal pass-through protocol

Terminal pass-through is available on the `port`, `modem`, and `powercontrol` resources. It is enabled on a device-by-device basis. This feature allows you to open an SSH session directly to the device while retaining the appliance'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@xyzcoAus01 (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.

Note: This setting takes effect after you **restart** the Uplogix appliance.

Now, instead of logging in to the appliance, 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.

```
tmcmillan@central:~$ ssh -p 2001 admin@172.30.151.100
admin@172.30.151.100's password: *******
Permission granted for pass-thru
Press ~[ENTER] to exit
```

If the Uplogix appliance is managed by an Uplogix Control Center EMS, SSH and Telnet pass-through can be configured through the Uplogix web interface.

For a single appliance: **Inventory > expanded appliance page > Configuration** tab **> Protocols**

For a group of appliances: **Inventory > group page > appliance configuration** button **> Protocols**

Customizing device hostname and status messages

Each port device's hostname is used in the dashboard view that is displayed when you log in or when you use the **show dashboard** command. If no hostname is available, the description is used.

The front panel displays present on the 32-port appliance and the older 4-port appliance also provide information including the hostname and status for each port device. The hostname may be what the appliance retrieves from the device, or it may be what you set as the description.

To change the device description, set the description field of the **config init** or **config info** command. This only changes the dashboard display if the appliance cannot retrieve a hostname from the device.

The appliance also displays the status of each device, both on the LCD panel (if present) and in the dashboard display. If the standard status messages do not meet your needs, you can create custom status messages.

To create a custom status message, use the **config rule** command to create a rule that allows you to monitor the device for the conditions of interest, and use the rule action **statusWrite** to define a brief status message. For information about creating rules, see the ***Guide to Rules and Monitors***.

If the Uplogix appliance is managed by an Uplogix Control Center EMS, rules to display custom messages can be set up through the Uplogix web interface:

Inventory > group page **> rules** button

Clearing a previously configured port

When you disconnect a device from a port, the Uplogix appliance 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@xyzcoAus01]# port 2/1
 tasman 6300 tios
 tasman
[admin@xyzcoAus01 (port2/1)]# exit
[admin@xyzcoAus01]# 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@xyzcoAus01]# port 2/1
native
```

You can use the wildcard character ***** to clear all ports on the option card. This will automatically assume that there are 16 ports on the card, rather than detecting the hardware in use.

```
[admin@xyzcoAus01]# 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
```

Note: If you are removing an option card or expansion unit, use the **config system clear slot** command also, to ensure that the hardware is completely cleared from the database.

Configuring power control

Uplogix appliances 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, you will need to initialize it.

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

- APC
- BayTech
- ServerTech

Consult your power controller's documentation for OS version and authentication settings.

The appliance uses mapped power outlets to cycle power to devices.

```
[admin@A101100303]# powercontrol

[admin@A101100303 (powercontrol)]# config init
--- Enter New Values ---
description: []: apcMS
make: []: apc
model: []: masterswitch
os: []: masterswitch vm
os version: []:
console username: []:
console password []:
serial bit rate [9600]:
serial data bit [8]:
serial parity [none]:
serial stop bit [1]:
serial flow control [none]:
use null modem (rolled cable to device)? (y/n) [n]:
Would you like to add a new mapping? (y/n) [n]: y
Outlet:1
Interface:port1/1
Would you like to add a new mapping? (y/n) [n]: y
Outlet:2
Interface:port1/2
Would you like to add a new mapping? (y/n) [n]: n
Do you want to commit these changes? (y/n): y
Testing login will take a few moments...
```

After you configure the outlet mappings, the appliance tests its initialization settings.

After initialization, you can return to the `powercontrol` resource and edit the power controller's settings:

`config authentication` allows you to configure the information that the appliance uses to log in to the power controller.

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

`config serial` allows you to specify the serial settings for the power controller.

`config info` allows you to 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 that allows you to see what is currently configured.

Note: The Uplogix appliance may report amps incorrectly for multi-bank or multi-phase PDUs.

Managing accounts and security

This chapter describes how to control access to the Uplogix appliance.

This chapter 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 appliance
- 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 Uplogix appliance 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 appliance. File servers using TFTP and FTP 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 appliance. Users may authenticate using passwords, certificates, or a combination of both. Uplogix appliances 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 appliance directly. Supported clients include:

- PuTTY
- SSH® Tectia™
- VanDyke® SecureCRT®
- SSHTerm for Windows
- iTerm for Macintosh OS X
- UNIX's built-in ssh command

Secure Copy

The appliance 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 appliance'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 secure networks.

The appliance's FTP server is used to transfer files to network devices that support it. The appliance 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 appliance's TFTP server is available only during automated file transfers between network devices and the appliance and on manual instantiation. It is not limited to IP addresses; it limits possible security exposure by specifically naming files.

Telnet access

Telnet access to the appliance is available if specifically enabled. Requiring a reboot of the appliance, it allows clear-text clients to access the CLI. Port 23 is used by default.

Modem access

Optional modem teletype (TTY) access is available if configured to provide single user dial-in access to the RMOS command line. Uplogix recommends using the appliance's outbound PPP/VPN service to reduce the security risks associated with dial-in modems. Refer to Chassis views and indicator lights on page 3 for the connector location.

By default, the modem does not answer incoming calls. To enable the dial-in capability, see Enabling dial-in and setting answering behavior on page 31.

Console access

An on-board console port is available for local access to the RMOS command line. Refer to Chassis views and indicator lights on page 3 for the connector location.

The connect command

When you are logged in to an Uplogix appliance, you can connect to another Uplogix appliance's command line interface using the **connect** command. While the protocol uses Secure Shell, this command limits connectivity to other appliances, reducing overall security risk. Like all RMOS commands, this feature is limited to users authorized to execute it.

```
[admin@xyzcoAus01]# connect 172.16.210.251
Connecting to 172.16.210.251
admin's password: ********
Uplogix RMOS v3.5  -- Powering Business Uptime

ssh client did not request X11 forwarding
--------------------------------------------------------------------------------
Port     Hostname            Status        Con Eth Uptime   Processor   Last
                                                            Utilization  Alarm
---- ----------------- ----------------- --- --- ------- ----------- -------

[output removed]
```

About outbound communication

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

Archiving and exporting appliance configuration

If the Uplogix appliance is managed by an Uplogix Control Center element management system (EMS), the EMS automatically archives device statistics, user sessions, device files and other data periodically using HTTPS over port 8443. Archiving uses high data compression to reduce the impact to the network. Archiving is automatically disabled when operating out-of-band.

If the appliance is not managed by an Uplogix Control Center, you can use the **`config export`** command to create an XML file of the appliance's configuration and send it to the IP address of your choice using SCP or FTP.

Pulse

The Pulse client uses the ECHO protocol (TCP 7) to determine network availability. TCP ECHO packets are sent every 30 seconds from the management Ethernet port; unsuccessful packets are counted, initiating a dial-backup connection after four consecutive failures. While the default route for the Uplogix appliance is directed to the out-of-band link, the ECHO packets continue to be sent via management Ethernet, automatically disconnecting the backup after five consecutive successful packets.

Heartbeat

The Uplogix appliance communicates to the Uplogix Control Center over a two-way HTTPS stream secured by SSL certificate, providing regular updates to current device status, status of scheduled jobs, alarm and event information, and other system status variables. Using TCP port 8443 by default on 30-second intervals, this data is compressed to reduce impact of the appliance's management traffic on the network.

You can change the heartbeat interval and TCP port from the RMOS 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 Uplogix appliance will synchronize time with a Network Time Protocol (NTP) server using UDP port 123. If the appliance is used with the Uplogix Control Center EMS, it is automatically set to use the EMS as its default time server. You can configure the appliance to use a different time server using the **`config system ntp`** command. If the Uplogix Control Center is used but NTP is disabled, the appliance will synchronize time using the heartbeat. For information on using an NTP server, see Setting date and time on page 23.

Configuring SSH security

Uplogix appliances allow you specify SSH port, encryption, compression, and key exchange for SSH sessions using the **config system protocols ssh** command.

```
[admin@xyzcoAus01]# 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]:
```

You must **restart** the appliance for your changes to take effect.

Note: Changes to the **config system protocols ssh** settings take effect after you **restart** the appliance.

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 appliance with a preferred encryption cipher of 3des-cbc but also allow aes128-cbc, and a client attempts to connect to the appliance 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 Uplogix appliance's default SSH port can be changed to a non-standard TCP port for enhanced security or for interoperability with your network's firewall. Use the **config system protocols ssh** command.

SSH configuration changes affect both the server and client SSH configuration for the appliance, which include server processes running on the appliance such as sshd daemon and commands such as **connect** and **config import**.

If the Uplogix appliance is managed by an Uplogix Control Center EMS, SSH protocol can be configured through the Uplogix web interface.

For a single appliance: **Inventory > expanded appliance page > Configuration** tab **> Protocols**

For a group of appliances: **Inventory > group page > appliance configuration** button **> Protocols**

Allowing Telnet connections

By default, the Uplogix appliance allows users to connect only via SSH to TCP port 22. You can configure the appliance to allow Telnet connections as well.

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

Note: This command takes effect after you **`restart`** the appliance.

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

For a single appliance: **Inventory > expanded appliance page > Configuration** tab **> Protocols**

For a group of appliances: **Inventory > group page > appliance configuration** button **> Protocols**

Configuring IP address filtering

By default, Uplogix appliances allow access from any IP address; however, you can use the **config system protocols filter** command to restrict access. This command opens an editor that allows you enter IP addresses to allow or block. Networks can be specified by IP address followed by an optional subnet mask.

For example, you could 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 appliance from the denied addresses, preventing any other computer from accessing the appliance.

The filter automatically adds defined services such as the Uplogix 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@xyzcoAus01]# config system protocols filter
[config system protocols filter]# deny 10.0.0.1
[config system protocols filter]# deny 10.10.1.0/24
[config system protocols filter]# deny 10.11.0.0/16
[config system protocols filter]# deny 11.0.0.0/8
[config system protocols filter]# allow 172.30.237.220
[config system protocols filter]# no allow 172.30.238.154
```

The 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. The user will not be able to open a new session, however.

Filters are applied after you **exit** the editor.

If the Uplogix appliance is managed by an Uplogix Control Center EMS, IP filtering can be configured through the Uplogix web interface.

For a single appliance: **Inventory > expanded appliance page > configuration** tab **> Protocols**

For a group of appliances: **Inventory > group page > appliance configuration** button **> Protocols**

Configuring phone number filtering

By default, the modem refuses all incoming calls. Dial-in capability must be enabled from the RMOS command line before use. (See Enabling dial-in and setting answering behavior on page 31.) 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 you to:

- 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.

Do not use dashes or dots between numbers.

```
[config answer]# deny 804
[config answer]# allow 512555
[config answer]# deny 5125551212
```

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

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

The appliance 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
```

Other optional security measures are:

Ring-back - When enabled, the appliance ignores an incoming call until it hangs up. If the user calls back within a specified amount of time, the appliance answers the call.

Answer only on pulse failure - Specifies that the modem ignores calls unless the pulse server fails to echo four consecutive pulses, which indicates a network outage and triggers out-of-band operation.

If the Uplogix appliance is managed by an Uplogix Control Center EMS, phone number filtering and other modem security measures can be configured through the Uplogix web interface.

For a single appliance: **Inventory > expanded appliance page > Configuration** tab **> Modem**

For a group of appliances: **Inventory > group page > appliance configuration** button **> Modem**

Locking the keypad

After completing basic configuration, you may choose to disable the front panel keypad 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 Uplogix appliance is managed by an Uplogix Control Center EMS, the keypad can be locked or unlocked through the Uplogix web interface.

For a single appliance: **Inventory > expanded appliance page > Configuration** tab **> Keypad**

For a group of appliances: **Inventory > group page > appliance configuration** button **> Keypad**

Managing user and group accounts

If the Uplogix appliance is not managed by an Uplogix Control Center element management system (EMS), the **config user** and **config group** commands allow you to create accounts unique to that appliance.

If the Uplogix appliance is managed by an Uplogix Control Center, you must use the Uplogix web interface for the tasks in this section. The **config user** and **config group** commands cannot be used when the appliance is under management.

This section covers:

- Viewing accounts
- 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@xyzcoAus01]# show user adent
adent
created 07/15/2008 16:41:34 UTC
password $sha1$WzcrBzDoNaVe$TTj7+4/2vytaVG0nXc9bFdFL+jQ=
alert eligible * * * * *
timezone US/Central dst
email adent@xyzco.us.com
powercontrol - security
modem - security
system - security
port1/1 - security
port1/2 - security
port1/3 - security
port1/4 - security
subscribe powercontrol
subscribe modem
subscribe system
subscribe port 1/1
subscribe port 1/2
subscribe port 1/3
subscribe port 1/4
```

If the Uplogix appliance is managed by an Uplogix Control Center EMS, user accounts can be viewed through the Uplogix web interface:

Administration > Users > Create/Edit user.

Viewing groups

To display all groups, use the **show group** command.

To view a specific group, use **show group <groupname>**.

```
[admin@xyzcoAus01]# show group southwestOps
southwestOps
created 07/10/2007 18:01:16 UTC
description southwest region operators
email southwest_ops@xyzco.us.com
start 2007-07-15 00:00:00.0
expire 2009-12-31 23:59:59.0
Group is currently INACTIVE
user  amarvin
user  adent
user  lprosser
user  fchurch
powercontrol - operator
modem - operator
system - operator
port1/1 - operator
port1/2 - operator
port1/3 - operator
port1/4 - operator
```

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

Administration > Groups> Create/Edit group

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.

Note: If the Uplogix appliance is managed by an Uplogix Control Center, user accounts must be managed through the Uplogix web interface. **Administration > Users** provides access to user account management functions. Refer to the ***User's Guide for the Uplogix Control Center Element Management System***.

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

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

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

```
[admin@xyzcoAus01]# config user adent
User adent does not exist. Create (y/n): y
[config user adent]#
```

Usernames are case-sensitive.

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

```
[config user adent]# ?
Allowable arguments are:
alert eligible
alert frequency
show
[no] description
[no] disabled
[no] email
[no] system
[no] expire
[no] password
[no] modem
[no] port #/#
[no] powercontrol
[no] authorized keys
[no] start
[no] subscribe
[no] tacacs
[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 adent]# password 2inf1nit9
```

Passwords are case-sensitive.

Caution: 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, 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. See Changing an account password on page 79 for more information.

Note: 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 Uplogix appliance 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 adent]# authorized keys
[config user adent]# authorized keys Each key must be on its own line. Type
'exit' on a line by itself to exit
[config user adent authorized keys]# ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAm4lEK0c73bkTgKMw46P0K2gf08ahRc4LfmmLQW8bhOm8wa0XKNA
QYVvhrI0zYojcM8dKETaOvgMvrdK7kNWMOmcFbNJbRfxlw8mO0NF0Btnf5qZA7oLOtBieNj2Sxeg/lC
ZCNym9GYMPVmBoZlxHIpbaCacLjMCxMZpMxE7mQUM= root@ems17.uplogix
[config user adent authorized keys]#
[config user adent authorized keys]# exit
[config user adent]#
```

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 format as well as which 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, see Disabling a user's account and Reactivating disabled user accounts on page 70.

Alert eligibility and frequency

The eligibility setting is used to restrict alert messages to specified times. The Uplogix appliance 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 adent]# alert eligible 0 22-08 * * 1-5
```

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

When the appliance 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 appliance 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 adent]# alert frequency 10
```

Time zone

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

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

Email

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

```
[config user adent]# email adent@xyzco.us.com
```

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

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

For more information about alerting, see Configuring an account to receive alerts on page 69.

Description

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

```
[config user adent]# description A. Dent - Network Analyst
```

TACACS

Specifies whether the user authenticates via an authentication server.

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 you to customize user privileges. The first argument is the resource, followed by a role. The **no** modifier can precede the command to remove privileges.

```
[config user adent]# system guest
[config user adent]# port 1/1 guest
[config user adent]# port 1/2 security
[config user adent]# port 1/3 operator
[config user adent]# no port 1/4
[config user adent]# powercontrol operator
[config user adent]# modem operator
```

Note: If you set up a user account with **no system**, the user is locked out of the system resource. The user may still have roles that allow access to other resources such as the device ports.

Note: The admin role (separate from the admin user account) has access to every available command. To manage the Uplogix appliance, at least one user account must be assigned the admin role unless the appliance is being managed by an Uplogix Control Center EMS.

For more information about using roles, see Assigning roles on page 83.

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 that they are interested in. To get all alerts from the Uplogix appliance, use the **subscribe all** command. Users can subscribe to individual resources as well as interfaces on managed devices.

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

For more information about alerting, see Configuring an account to receive alerts on page 69.

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 Uplogix appliance 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 adent]# start 06212008000000
[config user adent]# expire 12312009235959
```

This example activates the account on June 21, 2008. The account expires at the end of 2009. 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, 2009.

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

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

Review a user account after making changes

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

```
[config user adent]# show
adent
created 06/18/2007 22:17:52 UTC
description A. Dent - Network analyst
start 06/21/2007 00:00:00 UTC
User is currently INACTIVE
password $sha1$uydgA91B4HO7$NqX1pE0OhRp9kjwhWYitZeWBvnE=
alert frequency 10m
alert eligible 0 22-08 * * 1-5
timezone US/Central dst
email adent@xyzco.us.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 Uplogix appliance is managed by an Uplogix Control Center EMS, user accounts can be viewed through the Uplogix web interface:

Administration > Users > Create/Edit user

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.

Note: If the Uplogix appliance is managed by an Uplogix 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 Uplogix Control Center Element Management System***.

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

```
[admin@xyzcoAus01]# 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] tacacs
[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 appliance, you cannot create a group account called sysadmin.

If the Uplogix appliance is managed by an Uplogix Control Center EMS, group accounts can be edited through the Uplogix web interface:

Administration > Groups> Create/Edit group

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@yourcompany.com
```

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 group** command allows you to customize group privileges. 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 operator
[config group AustinNOC]# no port 1/4 guest
[config group AustinNOC]# port 1/2 operator
[config group AustinNOC]# port 1/2 security
[config group AustinNOC]# system analyst
```

For more information about using roles, see Assigning roles on page 83.

Start and expire dates

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

```
[config group AustinNOC]# start 01012008000000
[config group AustinNOC]# expire 12312009235959
```

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

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

TACACS

Use this command to specify a TACACS ACL if you are creating the group in order to use TACACS to manage privileges. For more information, see Using TACACS to manage privileges on page 76.

Adding and removing users

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

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

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

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

Configuring an account to receive alerts

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

- The Uplogix appliance must be configured to use a mail server (See Setting originating email address and SMTP server for alerts on page 23)
- 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. Jones will receive all alerts.

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

In the following example, D. Jones will receive alerts from port 1/2, the port 1/3 chassis, the power controller, and the Uplogix appliance.

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

D. Jones may choose to limit alerts to specific interfaces as follows:

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

You can configure the account to receive alerts at separate email addresses during in-band and out-of-band operation. To do this, use the **config user** command to set the user's email addresses with either the **in-band** or **out-of-band** parameter:

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

Setting up different in-band and out-of-band email addresses provides an indication of whether the appliance 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.

Note: The appliance 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 Uplogix appliance 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, consult the ***Reference Guide for Uplogix Secure Remote Management Appliances***.

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

If you log out while there are current alarms, the appliance 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 Uplogix appliance is managed by an Uplogix Control Center EMS, you can set up subscriptions to alerts through the Uplogix web interface:

Administration > Users > Create/Edit user - add report subscriptions button

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@xyzcoAus01]# config user adent
[config user adent]# disabled
[config user adent]# exit
```

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

```
[admin@xyzcoAus01]# sho user adent
adent
created 06/15/2007 16:41:34 UTC
User is currently INACTIVE
password $sha1$WzcrBzDoNaVe$TTj7+4/2vytaVG0nXc9bFdFL+jQ=
alert eligible * * * * *
timezone US/Central dst
email adent@xyzco.us.com
[Output removed]
```

The account is shown as INACTIVE.

If the Uplogix appliance is managed by an Uplogix Control Center EMS, user accounts must be managed through the Uplogix web interface:

Administration > Users > 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. The user account is still subject to its start and expire dates, however.

```
[admin@xyzcoAus01]# config user adent
[config user adent]# no disabled
[config user adent]# exit
```

The **show user** command lets you verify that the account is no longer inactive.

```
[admin@xyzcoAus01]# show user adent
adent
created 06/15/2007 16:41:34 UTC
password $sha1$WzcrBzDoNaVe$TTj7+4/2vytaVG0nXc9bFdFL+jQ=
alert eligible * * * * *
timezone US/Central dst
email adent@xyzco.us.com
```

If the Uplogix appliance is managed by an Uplogix Control Center EMS, user accounts must be managed through the Uplogix web interface:

Administration > Users > Disabled checkbox (clear)

Deleting an account

When you remove an account, all the account information is deleted. An alternative for user accounts is to disable the account (see previous page), 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@xyzcoAus01]# config user no ksmith
```

To delete a group, use the **no** modifier with the **config group** command.

```
[admin@xyzcoAus01]# config group no DallasNOC
Group DallasNOC deleted from Uplogix
```

If the Uplogix appliance is managed by an Uplogix Control Center EMS, user and group accounts must be managed through the Uplogix web interface.

To delete a user account:

Administration > Users > delete link associated with the account ID

To delete a group account:

Administration > Groups > delete link associated with the account ID

Managing authentication settings and passwords

This section provides information about user passwords, SSH certificates, and hardware authentication. Topics include:

- Configuring user authentication and security settings
- Using TACACS to manage authorization
- About SSH certificates
- Configuring hardware authentication
- 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 Uplogix appliance, centrally on the Uplogix Control Center EMS, or remotely on an external RADIUS or TACACS server, keeping user passwords synchronized throughout the enterprise while authorization is maintained on the appliance.

The settings in this section are presented in the interactive **`config system authentication`** command.

If the appliance is placed under management by an Uplogix Control Center, local users will be deleted, with the exception of the admin user. The AAA settings on the server allow you to maintain the admin user's local modifications (if any). Users and groups on the server are globally unique and are applied to all Uplogix appliances. Refer to the ***User's Guide for the Uplogix Control Center Element Management System***.

While either TACACS or RADIUS can be used for authentication and accounting, TACACS can also be used to manage user privileges. For more information about this capability, see Using TACACS to manage privileges on page 76.

If the Uplogix appliance is managed by an Uplogix Control Center EMS, 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 prompt is displayed if you set the authentication type as **`tacacs`** or **`radius`**. Supported authentication methods include **`pap`**, **`chap`**, and **`mschap`**.

Accounting type

This prompt is displayed if you set the authentication type 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.

Note: RADIUS accounting can only be used with RADIUS authentication and TACACS accounting can only be used with TACACS authentication.

Use TACACS authorization

This prompt is displayed if you set the authentication type as **tacacs**. The local permission scheme can be overridden by using TACACS as an authorization source.

Create users

This prompt is displayed if you set the authentication type as **tacacs**. If a user successfully authenticates with an external authentication source, but does not exist on the Uplogix appliance, a user account can be automatically created. This option is disabled by default.

Cache TACACS ACLs

This prompt is displayed if you set the authentication type as **tacacs**. If this option is enabled, the appliance will cache privileges to be used in case the authentication server cannot be reached, such as in the event of a network failure.

Cache passwords

This prompt is displayed if you set the authentication type as **tacacs** or **radius**. To configure the appliance to use local authentication when the authentication server is unavailable, answer **y** to this prompt. This allows the appliance to fall back to authenticating users with the passwords you assign from the appliance's command line (or from the Uplogix Control Center, if one is used) if the authentication server cannot be reached, such as in the event of a network failure.

Use this option and the next one ("If server is down, should Uplogix use local authentication?") together.

If server is down, use local authentication

This prompt is displayed if you set the authentication type as **tacacs** or **radius**. The appliance can fall back to local authentication if it cannot contact the authentication server. If you choose to use local authentication, be sure you have enabled the `Cache Passwords` option. If passwords are not cached, authentication will fail if the authentication server is not available.

Authentication host IP, accounting host IP

These prompts are displayed if you set the authentication type 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 to authenticate, the user will be denied access.

Shared secret

This prompt is displayed if you set the authentication type as **tacacs** or **radius**. Enter and confirm the shared secret for each server to enable communication with it.

Authentication and accounting ports

This prompt is displayed if you set the authentication type as **tacacs** or **radius**. Specify the port number of each authentication and accounting server to which the Uplogix appliance 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 – 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 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** – recently used passwords may not be reused.

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 appliance 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 appliance refuses further attempts. Setting lockout to **0** disables lockout protection. If you enable lockout, the appliance prompts you to specify the number of minutes the user will be locked out. The default lockout time is 30 minutes.

Using TACACS to manage privileges

Setting up an account to use a TACACS ACL allows the TACACS server to manage authorization. To use this feature, you will need to set up the account on the Uplogix appliance and on the TACACS server.

The general procedure is:

1. Configure the appliance to use TACACS.
2. Set up a group and give it a TACACS ACL.
3. Select or create a role with the desired set of permissions; assign it to the group on the appropriate resources.
4. Add users on the TACACS side and assign them the ACL you defined for the group.

These steps are described in detail below.

Note: If you delegate AAA functions to an external server, create a user with the `admin` role on the Uplogix appliance and add that account on the external server beforehand. If no user has the `admin` role on the appliance, the administration functions are not accessible.

Set up TACACS authorization

Configure authentication 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.
- Answer **`y`** to the `Create users` prompt.
- Optional: Answer **`y`** to the prompts for `Cache TACACS ACLs` and `Cache Passwords` to ensure that users will still receive the correct privileges if the TACACS server is off-line 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@xyzcoAus01]# config system authentication
--- Existing  Values ---

(output removed)
--- Enter New Values ---
Authentication type: [local]: tacacs
Limit maximum concurrent sessions: (y/n) [n]:
Authentication method: [pap]:
Accounting type: [none]:
Use TACACS Authorization: (y/n) [n]: y
Create users: (y/n) [n]: y
Cache TACACS ACLs: (y/n) [n]: y
Cache passwords: (y/n) [n]: y
If server is down, should Envoy 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, see Managing roles and privileges on page 81.

Create a group

Use the **config group** command to create a group that defines the TACACS ACL.

Use the **system**, **port**, **modem**, and **powercontrol** subcommands as needed to apply the role containing the desired set of permissions.

Use the **tacacs** subcommand to define the TACACS ACL - this is similar to a password. For example:

```
[config group centex]# tacacs longhorns
```

You do not need to add users to the group.

Associate the ACL to users

You can do this by creating new users or adding the ACL to existing users.

To create TACACS users:

On the TACACS server, create users.

For each user, specify the ACL you defined when you created the group on the Uplogix appliance. For example:

```
acl=longhorns
```

To enable authorization on an existing TACACS user:

Once the user is created and is able to authenticate to the Uplogix appliance, you can 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>
}
```

Your TACACS administrator’s guide should give more specific examples of configuration required for this functionality.

About SSH certificates

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

Certificate format varies widely among SSH clients; the vendor's documentation should be consulted to determine what key format as well as what 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 Uplogix appliance.

To configure an account to use SSH certificates, specify **authorized keys** in the **config user** editor. See Creating and editing user accounts on page 62 for more information.

If the Uplogix appliance is managed by an Uplogix Control Center EMS, SSH certificates can be configured through the Uplogix web interface:

Administration > Users > Create/Edit User

Configuring hardware authentication

To use a hardware authenticator, connect an RSA® SecurID® SID800 hardware authenticator to one of the USB connectors on the Uplogix appliance. Use the **config ppp** command and set the password as
[PIN]$(SECURID)

where **[PIN]** is an optional password of up to 8 characters and the rest is entered exactly as shown. The password is case-sensitive.

You can review PPP settings by using the **show ppp** command.

```
[admin@xyzcoAus01 (modem)]# show ppp
Phone Number: 5125550001
User Name: xyzcoAus01
Password: ********
```

If you remove the hardware authenticator while it is in use, the appliance generates an alarm. You can clear the alarm using the **config system clear securid** command.

If the Uplogix appliance is managed by an Uplogix Control Center EMS, you can configure this through the Uplogix web interface:

Inventory > expanded appliance page > Configuration tab **> Modem**

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.

```
[adent@xyzcoAus01]# config password
Old Password:********
New Password [********]: *********
Confirm Password: *********
Password changed.
```

Note: 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 Uplogix appliance strips the space character and the login fails.

If you have the **admin** or **security** role on the system resource, you can use the **config password** command to change another user's password. In this example, the user tmcmillan changes the password for user adent.

```
[tmcmillan@xyzcoAus01]# config password adent
New Password: ********
Confirm Password: ********
Password changed.
```

Note: The **config user** editor allows you change a user's password also. This is not recommended, as the password is set using a subcommand in the editor that does not hash the password. If a user reviews your session using the **show session** command, the password you set in this way will be displayed in clear text.

If the Uplogix appliance is managed by an Uplogix Control Center EMS, user accounts (including passwords) must be managed through the Uplogix web interface:

Administration > Users

The exception is that when a user logs in to an Uplogix appliance with an expired password, the appliance prompts for a new password regardless of whether it is managed by an Uplogix Control Center.

Changing the admin account's password

To ensure system security, change the admin user's password after you log in for the first time. The admin user cannot be deleted and has access to all commands, unless explicitly managed from the Uplogix Control Center.

To change the admin user's password, use the **config password** command.

```
[admin@xyzcoAus01]# config password
Old Password:********
New Password [********]: ********
Confirm Password: ********
Password changed.
```

Note: 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 Uplogix appliance strips the space character and the login fails.

If the Uplogix appliance is managed by an Uplogix Control Center EMS, the admin user can be managed through the Uplogix web interface:

Administration > AAA Settings - Manage 'admin' user checkbox under Authentication Settings.

Managing roles and privileges

Uplogix appliances 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 available
- Creating and editing roles
- Example: Granting terminal access only, on one port only

Using roles to limit user activities

Uplogix appliances restrict access to features based on users' privileges. All aspects of working with the Uplogix appliance 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. See Assigning roles on page 83.

If the Uplogix appliance is managed by an Uplogix Control Center EMS, you can manage roles through the Uplogix web interface.

For a single appliance: **Inventory > appliance page > Status** tab **> Roles**

For a group of appliances: **Inventory > group page > 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 specific account for a specific resource, such as **system admin** or **port 1/2 operator**.

If your privileges on a specific resource do not allow you to use a specific command, the appliance will return a message that the command is unavailable when you try to use it.

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.

```
[adent@xyzcoAus01]# port 1/1
port1/1 is not available.
usage: port <slot number>/<port number>
```

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.
- analyst - most command permissions available on the resource to which the role is applied; not permitted to work with rules, reporting functions, and certain security-related items.
- operator - configure CLI behavior, set up monitoring, manage devices, view information about Uplogix appliance configuration
- security - configure accounts, authentication, roles, and other security-related settings
- guest - view some basic information, such as alarms, status, and version.

For a command-by-command comparison of these roles, see Predefined roles available on page 84.

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@xyzcoAus01]# config system ip
--- Existing  Values ---
Use DHCP: Yes
Management IP: 172.30.151.109
Host Name: xyzcoAus01
Subnet Mask: 255.255.255.0
Broadcast Address: 172.30.151.255
Default Route: 172.30.151.254
Speed/duplex: auto:100full
DNS Server:
MAC Address: 00:0F:2C:00:02:BF
Change these? (y/n) [n]: y
```

User operatorbob has the operator role on the system resource. This role does not include the config system ip permission.

```
[operatorbob@xyzcoAus01]# config system ip
Command 'ip' not found.  Type ? for help.

[operatorbob@xyzcoAus01]# config system ?
Uplogix RMOS v3.5
page-length              Configure page length
timeout                  Sets session timeout
```

User operatorbob cannot execute the **config system ip** command, so the RMOS command line does not display it.

You can use the **config role** command to create custom roles that give users exactly the permissions you want. See Creating and editing roles on page 92 for more information.

Assigning roles

To define what a user or group can do, you must assign specific roles on specific resources using the **config user** or **config group** command. You can assign any role that has been defined. In this example, we assign user tmcmillan the admin role on the system resource, and the analyst role on several other resources.

```
[admin@xyzcoAus01]# config user tmcmillan
[config user tmcmillan]# system admin
[config user tmcmillan]# modem analyst
[config user tmcmillan]# powercontrol analyst
[config user tmcmillan]# port 1/1 analyst
[config user tmcmillan]# port 1/2 analyst
[config user tmcmillan]# exit
```

As with other editors, you can use the **no** modifier to remove existing settings. For example, to remove user tmcmillan's analyst role on port 1/2:

```
[config user tmcmillan]# port 1/2 no analyst
```

For a list of command permissions associated with each of the predefined roles, see Predefined roles available (next section). For information on creating custom roles, see Creating and editing roles on page 92.

Users who are members of group accounts will have the permissions associated with the group account in addition to the permissions associated with their own user accounts.

You can assign a user 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.

Note: The admin role (separate from the admin user account) has access to every available command. To manage the Uplogix appliance, at least one user account must be assigned the admin role unless the appliance is being managed by an Uplogix Control Center EMS.

Predefined roles available

The role assigned to you on a given resource determines which commands you can execute on that resource. The admin role gives you access to all commands.

To view the permissions associated with a role, use the **show role** command:

```
[admin@xyzcoAus01]# show role guest
guest
        allow config password
        allow login
        allow ping
        allow show alarms
        allow show date
        allow show directory
        allow show environment
        allow show session
        allow show status
        allow show version
        allow show who
```

The following table lists the permissions for each predefined role.

Note: Roles may contain permissions for commands that are not available on the appliance you are using.

Permission	admin	analyst	operator	security	guest
assimilate	yes	yes	no	no	no
autorecovery	yes	yes	no	no	no
certify	yes	yes	no	no	no
clear counters	yes	yes	yes	no	no
clear log	yes	yes	yes	no	no
clear password	yes	no	no	yes	no
clear service-module	yes	yes	yes	no	no
clear xbrowser	yes	no	no	no	no
config aaa (no CLI command)	yes	no	no	no	no
config answer	yes	yes	no	no	no
config authentication	yes	yes	no	yes	no
config backup	yes	yes	yes	no	no
config date	yes	yes	no	no	no
config device logging	yes	yes	no	no	no
config environment	yes	yes	yes	no	no
config export	yes	no	no	no	no

Permission	admin	analyst	operator	security	guest
config filter (no CLI command)	yes	no	no	no	no
config group	yes	yes	no	no	no
config hierarchy (no CLI command)	yes	no	no	no	no
config import	yes	no	no	no	no
config info	yes	yes	no	no	no
config init	yes	yes	no	no	no
config inventory (no CLI command)	yes	no	no	no	no
config label (no CLI command)	yes	no	no	no	no
config license (no CLI command)	yes	no	no	no	no
config log rule	yes	yes	no	no	no
config monitors	yes	yes	yes	no	no
config outlets	yes	yes	no	no	no
config password	yes	yes	yes	yes	yes
config ppp	yes	yes	no	no	no
config privileges (no CLI command)	yes	yes	no	yes	no
config properties	yes	yes	no	no	no
config protocols pass-through	yes	yes	no	no	no
config protocols shadow	yes	yes	no	no	no
config removejob	yes	yes	yes	no	no
config report (no CLI command)	yes	no	no	no	no
config restrict	yes	no	no	no	no
config role	yes	no	no	yes	no
config rule	yes	no	no	no	no
config ruleset	yes	no	no	no	no
config schedule	yes	yes	no	no	no
config serial	yes	yes	no	no	no
config service-processor	yes	no	no	no	no
config settings	yes	yes	no	no	no

Permission	admin	analyst	operator	security	guest
config slv	yes	yes	no	no	no
config system archive	yes	yes	no	no	no
config system authentication	yes	no	no	yes	no
config system banner	yes	no	no	yes	no
config system clear port	yes	yes	no	no	no
config system clear securid	yes	yes	no	no	no
config system clear slot	yes	yes	no	no	no
config system email	yes	yes	no	no	no
config system ip	yes	yes	no	no	no
config system ipt	yes	yes	no	no	no
config system keypad	yes	yes	no	no	no
config system management	yes	yes	no	no	no
config system ntp	yes	yes	no	no	no
config system page-length	yes	yes	yes	no	no
config system properties	yes	yes	no	no	no
config system protocols dhcp	yes	yes	no	no	no
config system protocols filter	yes	yes	no	no	no
config system protocols ssh	yes	yes	no	no	no
config system protocols telnet	yes	yes	no	no	no
config system pulse	yes	yes	no	no	no
config system serial	yes	yes	no	no	no
config system snmp	yes	yes	no	no	no
config system syslog-options	yes	yes	no	no	no
config system timeout	yes	yes	yes	no	no
config update	yes	yes	no	no	no
config user	yes	yes	no	yes	no
config user certificate	yes	yes	no	yes	no
config vpn	yes	yes	no	no	no

Permission	admin	analyst	operator	security	guest
config xbrowser	yes	no	no	no	no
connect	yes	yes	yes	no	no
copy	yes	yes	yes	no	no
device execute	yes	yes	no	no	no
device ping	yes	yes	yes	no	no
edit running-config	yes	yes	no	no	no
interface (no CLI command)	yes	yes	yes	no	no
login	yes	yes	yes	yes	yes
off	yes	yes	no	no	no
on	yes	yes	no	no	no
ping	yes	yes	yes	no	yes
power	yes	yes	yes	no	no
ppp off	yes	yes	yes	no	no
ppp on	yes	yes	yes	no	no
pull os	yes	yes	yes	no	no
pull running-config	yes	yes	yes	no	no
pull startup-config	yes	yes	yes	no	no
pull tech	yes	yes	yes	no	no
push os	yes	yes	no	no	no
push running-config	yes	yes	no	no	no
push startup-config	yes	yes	no	no	no
reboot	yes	yes	yes	no	no
recover configuration	yes	yes	no	no	no
restart	yes	yes	yes	no	no
restore	yes	yes	no	no	no
rollback assimilate	yes	yes	no	no	no
rollback authentication	yes	yes	no	no	no
rollback config	yes	yes	no	no	no

Permission	admin	analyst	operator	security	guest
run report (no CLI command)	yes	no	no	no	no
service access (no CLI command)	yes	yes	no	no	no
service-processor exec	yes	no	no	no	no
show aaa (no CLI command)	yes	no	no	no	no
show alarms	yes	yes	yes	no	yes
show all	yes	yes	yes	no	no
show answer	yes	yes	yes	no	no
show archive	yes	no	no	no	no
show authentication	yes	yes	no	no	no
show buffer	yes	yes	no	yes	no
show chassis	yes	yes	no	no	no
show circuit	yes	yes	yes	no	no
show config	yes	no	no	no	no
show date	yes	yes	yes	yes	yes
show device change	yes	yes	yes	no	no
show device changes	yes	yes	yes	no	no
show device logging	yes	yes	yes	no	no
show device syslog	yes	yes	yes	no	no
show diff	yes	yes	yes	no	no
show directory	yes	yes	yes	no	yes
show environment	yes	yes	yes	no	yes
show events	yes	yes	yes	no	no
show faults	yes	yes	no	no	no
show filter (no CLI command)	yes	no	no	no	no
show gps events	yes	no	no	no	no
show gps position	yes	no	no	no	no
show group	yes	yes	no	no	no
show info	yes	yes	yes	no	no

Permission	admin	analyst	operator	security	guest
show install-history	yes	yes	no	no	no
show interface	yes	yes	no	no	no
show label (no CLI command)	yes	no	no	no	no
show license (no CLI command)	yes	no	no	no	no
show log	yes	yes	yes	no	no
show monitors	yes	yes	yes	no	no
show outlets	yes	yes	no	no	no
show pingstats	yes	yes	yes	no	no
show ports	yes	yes	yes	no	no
show post	yes	yes	yes	no	no
show ppp	yes	yes	yes	no	no
show privileges	yes	yes	no	yes	no
show properties	yes	yes	yes	no	no
show protocols pass-through	yes	yes	no	no	no
show protocols shadow	yes	yes	yes	no	no
show remotestate	yes	yes	no	no	no
show report (no CLI command)	yes	no	no	no	no
show restrict	yes	no	no	no	no
show role	yes	yes	no	yes	no
show rollback-config	yes	yes	yes	no	no
show rule	yes	no	no	no	no
show ruleset	yes	no	no	no	no
show running-config	yes	yes	yes	no	no
show schedules	yes	yes	yes	no	no
show serial	yes	yes	no	no	no
show service-module	yes	yes	no	no	no
show service-processor	yes	no	no	no	no
show session	yes	yes	yes	no	yes

Permission	admin	analyst	operator	security	guest
show sessions	yes	yes	no	no	no
show settings	yes	yes	yes	no	no
show slv stats	yes	yes	no	no	no
show slv test	yes	yes	no	no	no
show startup-config	yes	yes	yes	no	no
show status	yes	yes	yes	no	yes
show system archive	yes	yes	no	no	no
show system authentication	yes	yes	no	no	no
show system banner	yes	yes	yes	yes	no
show system email	yes	yes	yes	no	no
show system ip	yes	yes	yes	no	no
show system ipt	yes	yes	no	no	no
show system keypad	yes	yes	yes	no	no
show system management	yes	yes	yes	no	no
show system ntp	yes	yes	no	no	no
show system page-length	yes	yes	yes	no	no
show system properties	yes	yes	yes	no	no
show system protocols	yes	yes	no	no	no
show system pulse	yes	yes	yes	no	no
show system serial	yes	yes	yes	no	no
show system snmp	yes	yes	yes	no	no
show system syslog-options	yes	yes	no	no	no
show system timeout	yes	yes	yes	no	no
show tech	yes	yes	yes	no	no
show user	yes	yes	no	yes	no
show version	yes	yes	yes	yes	yes
show vpn	yes	yes	yes	no	no
show who	yes	yes	yes	yes	yes

Permission	admin	analyst	operator	security	guest
show xbrowser	yes	no	no	no	no
shutdown	yes	yes	no	no	no
squeeze	yes	yes	no	no	no
suspend	yes	yes	yes	yes	no
terminal	yes	yes	yes	no	no
terminal break	yes	no	no	no	no
terminal force	yes	no	no	no	no
terminal lock	yes	no	no	no	no
terminal shadow	yes	yes	no	yes	no
upload archive (no CLI command)	yes	no	no	no	no
use system auth (no CLI command)	yes	yes	no	no	no
xbrowser	yes	no	no	no	no

The analyst, operator, security, and guest roles are editable. For information about editing these roles or creating custom roles, see Creating and editing roles (next section).

If the Uplogix appliance is managed by an Uplogix Control Center EMS, you can view roles through the Uplogix web interface:

Administration > Roles > Create/Edit role

Creating and editing roles

If the predefined roles do not meet your organization's needs, you can use the **config role** command to create custom roles that give users exactly the permissions you want them to have.

In this example, we create a role called newRole.

```
[admin@xyzcoAus01]# 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
```

Note: Roles assigned at the system level must include the **login** permission to give the user access to the appliance. 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 you have already 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

You can 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. You may use ***** as a wildcard character, and you may 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 you issue the **deny show *** command after allowing the **show user** command, the role allows **show user** but no other **show** commands.

Start and expire

Optional - 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, if you have created a role called `temporary_role` and you wish to delete it:

```
[admin@xyzcoAus01]# config role no temporary_role
[admin@xyzcoAus01]# show role temporary_role
Could not find role 'temporary_role'
```

If the Uplogix appliance is managed by an Uplogix Control Center EMS, roles must be managed through the Uplogix web interface.

To create or modify a global role: **Administration > Roles > Create/Edit role**

To create or modify a role applicable only to a specific inventory group: **Inventory > group page > Role**

Example: Granting terminal access only, on one port only

Sometimes a user needs only minimal access. In this example we will create a user who can only log in to one Uplogix appliance, and only execute the terminal command on port 1/1. To do this, we must:

- 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@A101100303]# config role terminalOnly
Role terminalOnly does not exist. Create (y/n): y
```

The user can only execute commands while logged in to the Uplogix appliance, 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 we apply it 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 log in to the Uplogix appliance, 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@A101100303]# config user termOnlyUser
User termOnlyUser does not exist. Create (y/n): y
```

Note: 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 you have created the user account.

The **config user** editor allows you to assign roles, the next step.

Applying the role to create permissions

The role we created, terminalOnly, includes appliance-level commands (**login** and **show status**) and port-level commands (**show status** and **terminal**). The user account will need the **login** permission at the appliance level, to log in to the Uplogix appliance. Use the **config user** editor to apply the terminalOnly permission at the appliance 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@A101100303]# 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
- Installing a device operating system upgrade
- 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
- Setting up frozen console monitoring and recovery
- Working with service processors - Automate server management using service processors
- Using xbrowser - Manage devices through their browser-based user interfaces
- Recovering a device from boot ROM

Terminal sessions

Uplogix appliances allow terminal sessions to devices.

When you initialize a port with the **`config init`** command, the Uplogix appliance stores console and enable credentials, which allow it to authenticate to the device for automated operations. Terminal pass-through allows users with the admin or analyst 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 Uplogix appliance logs out of the device when a user issues the terminal command; the user must log in manually.

If the Uplogix appliance is managed by an Uplogix Control Center EMS, the device CLI can also be accessed through the Uplogix web interface:

Inventory > appliance page> port detail > Device CLI

Starting a terminal session

To start a terminal session with a device, navigate to the appropriate port and use the **`terminal`** command. You may be prompted to log in to the device, and the commands available to you depend on the permissions your role provides on this port.

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

`~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

~ <Enter> – Exit Terminal

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 lifted the next time you start a terminal session to the device.

Ending a terminal session

You can end a terminal session by typing **~** on a line by itself.

When you end your session, you will be prompted to enter a comment describing the reason for your changes.

Using the appliance's credentials for terminal sessions

When you configure a device on one of the Uplogix appliance's ports using the **`config init`** command, the appliance prompts you to enter console and enable login credentials.

Depending on the privileges allowed by your role on the device, the appliance 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 admin or analyst.

Using terminal pass-through

If terminal pass-through is enabled on the device, you can open an SSH or Telnet session directly to the device while retaining the appliance's rollback capabilities, session logging, and authorization checking. See Configuring SSH or Telnet terminal pass-through protocol on page 46 for information on configuring terminal pass-through.

Depending on your permissions, you may need to log in to the device.

```
tmcmillan@central:~$ ssh -p 2001 admin@172.30.151.100 admin@172.30.151.100's
password:
Permission granted for pass-thru
Press ~[ENTER] to exit
Connecting ...
Currently running job: showLog
Press 'x' to exit, 'f' to force (use carefully), or 's' to shadow.
Currently running job: rulesMonitor
Press 'x' to exit, 'f' to force (use carefully), or 's' to shadow.
Console session started.
```

When you use terminal pass-through, you can end your session to the device using the **~ <Enter>** command.

Using xbrowser

Uplogix appliances provide xbrowser, a browser-based device management capability similar to KVM. Xbrowser is supported on Windows XP and Linux Desktop.

Prerequisites for using the xbrowser feature:

- The device that you manage via xbrowser must be configured with a dedicated Ethernet port.
- You must have an XServer installed on your computer. Supported XServers:
  - Cygwin (install X11 components)
  - Xming (required if using the SSH applet on the Uplogix Control Center)
  - X11 (X.Org version:1.3.0)
- You must use an SSH client that supports X11 display forwarding. Supported clients:
  - Cygwin
  - OpenSSH (OpenSSH 4.7p1, OpenSSL 0.9.8b 04 May 2006)
  - Uplogix Control Center's SSH applet
  - X-Windows
- Your SSH client must be configured for X11 display forwarding.
- Your SSH client must be configured so that xbrowser runs a trusted connection to the local XServer. This is the default for the Uplogix Control Center's SSH applet, but needs to be configured on some clients. For example, if you use Cygwin as your SSH client, configure it as follows:
  `export DISPLAY=:0.0`
  `xauth generate :0.0 . trusted`
  `ssh -Y 172.30.x.x`
  If it is not set up properly you will see the message "Warning: No xauth data; using fake authentication data for X11 forwarding."

Note: In some cases, the xbrowser feature requires the use of the -Y ssh flag (trusted X11 forwarding) rather than the preferred -X flag which subjects the connection to the X11 security extensions.

Note: PuTTY is not a supported client for xbrowser.

Configuring the device for xbrowser

To configure xbrowser on a device, go to the appropriate port and use the **`config xbrowser`** command to make any changes needed.

```
[tmcmillan@xyzcoAus01 (port1/1)]# config xbrowser
--- Existing Values ---
Browser port: 80
Browser protocol: http
Change these? (y/n) [n]:
```

Browser protocol may be **`http`** or **`https`**. You may wish to set the TCP port to 443 if you use `https`.

Viewing current xbrowser settings

Use the **show xbrowser** command to display current xbrowser settings:

```
[admin@A101100303 (port1/1)]# show xbrowser
Browser port: 80
Browser protocol: http
```

Opening an xbrowser session

When you start your SSH session to the appliance, use the appropriate syntax to enable X11 display forwarding. When you log in, the dashboard display includes a statement that X11 forwarding is enabled.

Navigate to the appropriate port, and use the **xbrowser** command to open the device's user interface in a browser window.

Note: In the case of the Sun ILOM KVM solution, your browser presents a warning that the site's certificate cannot be verified. Accept the certificate to continue to the xbrowser session. If you wait more than two minutes to accept the certificate, you will see an "unknown user" error. If this happens, close the browser window and issue the **xbrowser** command again.

Note: At present, xbrowser does not support service processor firmware upgrades.

Working with service processors

When you initialize a connected device as **hp**, **sun**, or **server** using the **config init** command, the service processor commands become available to help you automate server management.

Configuring the service processor

Use the **config service-processor** command to configure communication with the service processor.

```
[admin@A101100303 (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):
```

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. This operation is available from the Uplogix web interface: **Inventory > expanded appliance** page **> Status** tab **> SP 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**.

Installing a device operating system upgrade

Before you start, obtain the appropriate OS image from the manufacturer of the device to be upgraded.

To transfer the file using FTP or TFTP, you will need a connection to the device using Ethernet; to use XModem, you will need a serial connection.

To transfer this image to the Uplogix appliance, select the port to which the device is connected 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 UNIX host to the appliance:

```
[admin@xyzcoAus01 (port1/1)]# copy SCP djones@10.22.100.11:c3560-12.3t.bin os candidate
```

Enter the **show settings** command to determine the current file transfer settings for this port. To change the current settings, use the **config settings** command.

After configuring OS upgrade settings, you are ready to perform the upgrade. The image you previously downloaded to the Uplogix appliance 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 the **push os candidate** command from the appropriate port resource. The appliance 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 settings are configured to include this behavior. The appliance monitors the POST 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@xyzcoAus01 (port1/1)]# push os candidate
System image file is "flash:/c1700-y-mz.123-9.bin"
3 interfaces and 3 types found.
Information logged Before Upgrade
Serial Number: FOC08060NSX
Make : cisco
Model : 1760
OS Type : IOS
OS Version : 12.3(9)
Uptime : 14 hours, 22 minutes
Device Image Verified.
Sending c1700-y-mz.123-1a.bin to
10.10.10.1: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
TFTP download of c1700-y-mz.123-1a.bin succeeded.
Retrieving running-config from device ...
Complete. running-config pulled.
Retrieving running-config from device ...
Complete. running-config pulled.
Issuing 'reload'
98304C1700 platform with 65536 Kbytes of main memory
decompressing
Image decompressed
Image decompressing
Image decompressed
Device loaded
Post complete.
Serial Number: FOC08060NSX
Make : cisco
Model : 1760
```

```
OS Type : IOS
OS Version : 12.3(1a)
Uptime : 0 minutes
3 interfaces and 3 types found.
Push OS succeeded.
```

Managing device configurations

The **push** commands allow you to write a previously 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. You can do this by logging in to 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 appliance will pull the configuration before and after the push operation, so you will be able to undo the change if necessary.

Use **push startup-config** if you need to write the entire configuration; for example, if you are replacing a device. This can be a relatively time-consuming operation.

Use the **push running-config** command to make incremental changes. In the example below, the running-config candidate file contains one only line; when this running-config file is pushed to the device, only its hostname will be changed. Because it is a small change, it will not take much time.

First, log in to the device with the **terminal** command. The appliance automatically pulls the current running-config so that if any harmful changes are made during the terminal session, they can be rolled back.

```
[tmcmillan@xyzcoAus01 (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
!
boot system flash flash:flash:c2600-i-mz.122-26.bin
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 appliance pulls the running configuration again as the terminal session ends.

Using the **show running-config candidate** command, you can view the running configuration file that you will push to the device.

```
[tmcmillan@xyzcoAus01 (port1/1)]# show run 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.

```
[tmcmillan@xyzcoAus01 (port1/1)]# push run 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, you can view the new running configuration using the **show running-config current** command. Some information has been removed from the command output.

```
[tmcmillan@xyzcoAus01 (port1/1)]# show run 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
!
boot system flash flash:flash:c2600-i-mz.122-26.bin
logging buffered 4096 debugging
no logging console
[output removed]

[tmcmillan@xyzcoAus01 (port1/1)]# exit
```

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 these 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 you use terminal pass-through to access a device using the **terminal** command, the Uplogix appliance retrieves the device's running configuration. After you exit the terminal session and return to the RMOS command line, the appliance retrieves another copy of the running configuration. The appliance compares the two running configurations and creates a difference document. Both rollback methods undo the changes in the difference document without reapplying the entire running configuration.

The **config settings** command specifies rollback transfer methods (xmodem, tftp).

The rollback capability is only available when you use terminal pass-through to access the device. 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.

Note: Scheduled tasks and monitors do not affect rollback.

Undoing changes automatically with SurgicalRollback

SurgicalRollback™ is the default behavior when you end a terminal pass-through session. If the appliance notes configuration changes, it displays the difference document along with a message warns you that your changes will be rolled back. The appliance 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. During the countdown to rollback, the appliance 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 appliance creates.

```
[admin@xyzcoAus01 (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 Demo2610
Demo7206(config)#access-list 101 permit pim any 192.168.1.0 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 192.168.1.0 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 RMOS command line, the appliance 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, you can 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, you would see this:

```
[admin@xyzcoAus01 (port1/1)]# show rollback-config
!
no hostname Demo7206
no access-list 101 permit pim any 192.168.1.0 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 device. For more information on the **show rollback-config** and **rollback config** commands, consult the ***Reference Guide for Uplogix Secure Remote Management Appliances***.

Forcing a configuration recovery - Cisco devices only

The Uplogix appliance can restore the configuration of a router or switch that it cannot access because of an authentication or console port speed mismatch, or an improperly pushed configuration file. Configuration recovery can recover a password by restoring a previously stored password, along with that configuration.

Note: This feature is available for Cisco routers running IOS or CatOS, and Cisco switches running CatOS.

The following conditions must be met before the appliance can force the configuration recovery:

- A valid device startup configuration must be stored on the appliance. 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 appliance.

The configuration recovery consists of taking a stored configuration and forcing the replacement of the configuration on the device.

```
[admin@xyzcoAus01 (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
```

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 appliance 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 Uplogix appliance can power cycle the device to recover from this state.

Note: This is not always a desirable operation. A device (for example, 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.

Note: The Uplogix series appliance 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@xyzcoAus01]# port 1/2
cisco 2610 IOS 12.1(22b)
Use the autorecovery command to begin the autorecovery monitor.
[admin@xyzcoAus01 (port1/2)]# autorecovery 120
Job was scheduled 13: [Interval: 00:02:00] intelligentReboot
```

The device is now monitored for frozen console.

Recovering a device from boot ROM

Uplogix appliances can recover devices that have entered ROMmon state. While the process varies among vendors and models, the appliance delivers standardized operations that require low-level operating system and 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. If you choose not to assimilate the device, run the **pull os** and **pull startup-config** commands from within the port. You should always do this on an unassimilated device as soon as practical. The OS file is transferred using TFTP, so you must have a working network connection from the appliance'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 appliance in the event they are needed.

After the **pull os** command is successful, the appliance will have a copy of the device's OS image stored locally. The stored image is relevant only for the device connected to the appliance's console port. If you prefer to use a previously collected file from one port for another, reference the copy command.

The following is a **pull os** command example:

```
[admin@xyzcoAus01]# port 1/1
cisco 3640 IOS 12.2(23)
[admin@xyzcoAus01 (port1/1)]# pull os
Starting pull of Cisco IOS Image
System image file is "flash:/c3640-i-mz.122-23.bin"
Backing up os file: flash:/c3640-i-mz.122-23.bin
Transferring file ...
Receiving c3640-i-mz.122-23.bin to
10.16.90.34: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
TFTP upload of c3640-i-mz.122-23.bin succeeded.
[admin@xyzcoAus01 (port1)]# show dir
OS
Current c3640-i-mz.122-23.bin
```

In this example, if the appliance later detects that the Cisco 3640 is in ROMmon mode, it first determines why and attempts a recovery. If the reason was a bad or missing OS image, the appliance 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 config startup-config** command to maintain a copy locally for these and other operational recovery procedures. As above, you can also schedule the appliance to automatically gather this information as often as is practical.

These files are automatically scheduled when you use the **config init** command in setting up a new supported device.

Maintenance and troubleshooting

Automated device maintenance and recovery operations include:

- Reviewing user sessions on the appliance and on devices - Viewing a list of sessions or a transcript of the command line interactions within a session
- Upgrading the appliance software
- Factory reset
- Troubleshooting

Upgrading the appliance software

Log on to www.uplogix.com/support 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 these procedures:

Upgrading from your workstation

Log in to the Uplogix appliance.

Enter the **config update** command, specifying the connection type and the location of the file - for example:

config update scp envoyuser@172.30.28.172:UplogixOS-3.5.0.13567.i386.bin

or

config update ftp envoyuser@172.30.28.172:UplogixOS-3.5.0.13567.i386.bin

or

config update http http://172.30.28.172/UplogixOS-3.5.0.13567.i386.bin

If the appliance is managed by an Uplogix Control Center, you can upload the upgrade file to the Uplogix Control Center's file archive under a suitable file category. You can then upgrade from the appliance's command line using the syntax **config update ems category/file** - for example,

config update ems uplogixUpdates/UplogixOS-3.5.0.13567.i386.bin

Upgrading from a USB flash drive

1. Connect a USB flash drive to your computer and copy these files to a USB flash drive:
   `upgrade.mnf`
   `UplogixOS-<version>.i386.bin`
2. Connect the USB flash drive to the Uplogix appliance.
3. Choose one of these:
   - On the front panel keypad, press the Enter key and select Update from the menu,

     OR
   - From your workstation, log in to the Uplogix appliance and enter the command **`config update usb`**. By default the appliance attempts to install the `UplogixOS-[version].i386.bin` file. You can specify another file in the command; for example, **`config update usb 3.5/UplogixOS-[version].i386.bin`** allows you to specify both the file and its location.

Note: Uplogix recommends using a 1 GB FAT16 formatted USB flash drive. Upgrading the appliance from a FAT32 formatted flash drive may be unsuccessful.

Upgrading from Uplogix Control Center

1. Log in to the Uplogix Control Center EMS and go to **Administration > File Archive**.
2. Click upload file.
3. Browse to the file you just downloaded from the support site, and click **upload**.
4. Open the **Inventory** tab and navigate to the appliance.
5. Ensure that the appliance has been moved out of the Unassigned group.
6. Open and expand the detail page for the appliance.
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 you 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 either schedule or start the upgrade.

Note: To avoid degrading the Uplogix Control Center's performance, upgrade no more than 100 Uplogix appliances at the same time.

Reviewing user sessions

The Uplogix appliance stores the session histories of all users. To view a list of current and previous sessions, use the **show sessions** command.

```
[admin@xyzcoAus01]# show sessions
id     user      ip address         logged in          logged out
--     -----     --------------     ----------------   -----------
3      tmcmillan 172.30.5.24        Jul 18 16:58 UTC
2      admin     172.30.235.110     Jul 18 12:26 UTC
1      admin     172.30.235.110     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.

You can type **q** at any time to quit viewing the display.

```
[admin@xyzcoAus01]# show session 3
-------------------------------------------------------------
User: tmcmillan
From: 172.30.5.24
Logged In: Jul 18 16:58:54 UTC 2008
Logged Out: Still logged in
-------------------------------------------------------------
> Uplogix RMOS v3.5  -- Powering Business Uptime
>
> ------------------------------------------------------------------------------
-
> Port     Hostname            Status        Con Eth Uptime   Processor   Last
>                                                            Utilization  Alarm
> ---- ----------------- ----------------- --- --- ------- ----------- ------
-
>  1/1
>  1/2
>  1/3
>  1/4
>  PWR
>  MDM embedded                              *
>    E A101100303         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
>
> [tmcmillan@A101100303]# show version
> Uplogix
> Serial Number: A101100303
> RMOS version: 3.5.0.13272
> RMOS build: 20080624:2210
> Uplogix v3.5  build 20080206:2346
> Last boot: 07/14/08-09:20:41
> Last incremental restart: 07/14/08-09:21:59
>
> [tmcmillan@A101100303]# conf user adent
> User adent does not exist. Create (y/n): y
> [config user adent]# password password
```

```
> [config user adent]# exit
>
> [tmcmillan@A101100303]# logout
------------------------------------------------------------
--DONE--
```

If the Uplogix appliance is managed by an Uplogix Control Center EMS, user sessions can be viewed through the Uplogix web interface:

Inventory > expanded appliance page **> Status** tab **> Sessions**

Troubleshooting

The following table lists some common problems, their usual causes, and ways you can correct them.

If a problem persists after you take the appropriate actions, contact support@uplogix.com.

Problem	Possible cause	What to do
A user is unable to log in to the appliance.	This user account does not exist on this appliance.	Create the user account. Add the user to the appropriate group, or assign the user appropriate roles on the appropriate resources.
	This user account lacks the appropriate permissions to log in to this appliance.	Add the user to the appropriate group, or assign the user appropriate roles on the appropriate resources.
	An upgrade or factory reset is in progress.	Wait until the appliance returns to its operational state. This may take up to half an hour.
The user can log in to the appliance but is unable to connect to a device using the **`terminal`** command.	This user lacks the appropriate permissions to use the **`terminal`** command on this port.	Add the user to the appropriate group, or assign the user appropriate roles on the appropriate resources.
	There is a problem with the connection to the device.	Check the connection between the device and the appliance, and correct any problems that exist – bad/incorrect cable or adapter, cable not fully seated, etc.
	There is a problem with the device itself.	Check the device and correct any problems that exist.
Older 4-port appliances: Expansion modules are not working - a port or a range of ports is listed as UNAVAILABLE in the dashboard view.	An expansion module was removed but not cleared from the database.	Reinstall the expansion module or use the **`config system clear slot`** command to remove the expansion module from the database.
Older 4-port Envoy appliances: Devices connected to expansion modules do not show up on the expected ports. Expansion modules are swapped - port 2/x bank is on the right, port 3/x bank is on the left.	The module on the right was connected to the appliance first.	Label the modules or reposition them in the expansion module mounting shelf. Note that swapping the cables to the expansion modules will not change the port assignments. Port designations are associated with the serial number of the expansion module the first time it is connected to the appliance.

Problem	Possible cause	What to do
Option cards for the 32-port appliance are not working - a port or a range of ports is listed as UNAVAILABLE in the dashboard view.	The option card is not properly seated.	Shut down the appliance, remove and reseat the option card, tighten the captive screws, and then power on again.
	The option card was removed but not cleared from the database.	Use the **config system clear slot** command to remove the expansion module from the database.
A device's status is listed as UNKNOWN when you log in or use the **show dashboard** command.	The device is not connected to the port.	Connect the device to the port.
	The device's power is off.	Power on the device.
The external modem is not working.	The serial bit rate is set incorrectly.	Use the **config init** or **config serial** command to change the serial bit rate. If you are using an Iridium modem, try 9600 or 19200.
	The modem **init ""** string was entered incorrectly. The double quotes are required.	Use the **show answer** command to check the **init** string. If you need to correct it, use the **config answer** editor.
The modem can dial out but does not answer incoming calls.	Dial-in has not been enabled.	Use the **config answer** command to **enable** the dial-in feature.
The Uplogix appliance does not open an out-of-band connection to the Uplogix Control Center EMS when pulse fails.	The appliance and Uplogix Control Center are on the same subnet.	The connection from the appliance to the Uplogix Control Center needs to use the default route. If both are on the same subnet, the PPP connection will not route properly.
The system health light on the Uplogix 430 is blinking.	The appliance is powering off or on, restarting. An upgrade or factory reset is in progress.	Wait for the appliance to return to its operational state (light stops blinking and remains on).
The link integrity light on an RJ-45 connector does not light when connected, and there is no communication; OR The device status does not show up as connected when you use the **show dashboard** command.	The `null modem` setting is incorrect.	Use the **config init** or **config serial** command to change the `null modem` setting.
	The wrong type of cable is connected. Check using the **config serial** command; if receive/transmit data zero or not incrementing, or if DSR and CTS are false, this indicates a problem with the cable.	If a null-modem (rolled) cable is connected, try a straight-through cable instead. Serial only: If a straight-through cable is connected, try a null-modem cable.

Problem	Possible cause	What to do
	The cable pin-out is incorrect, or the cable adapter pin-out is incorrect.	Check the pin-outs of all cables and adapters between the device and the Uplogix appliance.
	The cable is bad.	Try another cable of the same type.
	The cable is not securely connected (for example, the latch tab on the RJ-45 connector is broken).	Reseat or replace the cable.
	The port is not working properly.	Test this by moving a known good connection to this port; contact Uplogix support for RMA if port is bad.
	The device connected to this port is not working properly.	Test this by moving the device connection to a known good port.
A device connected by Ethernet has no IP address.	The device is configured to use DHCP but the Uplogix appliance is not configured to assign DHCP addresses.	Use the config system protocols DHCP command to enable this capability. See Configuring the appliance to assign DHCP addresses to connected devices on page 38.
The link integrity light on an RJ-45 connector does not light when connected, but you can use the terminal command to access the device.	Serial only: CTS and/or DSR may not be present on the appropriate pins.	Check the pin-outs of all cables and adapters between the device and the Uplogix appliance.
The user can log in to the device using the **terminal** command, but cannot log in directly to the device.	Terminal pass-through is not enabled.	Use the **config protocols pass-through** command to enable SSH or Telnet pass-through, and restart the appliance.
	Terminal pass-through has been enabled but the appliance has not been restarted. The appliance must be restarted for the command to take effect.	Restart the appliance.
	The user does not have the appropriate permissions to use terminal pass-through.	Add the user to the appropriate group, or assign the user appropriate roles on the appropriate resources.

Problem	Possible cause	What to do
The appliance is performing poorly.	There is a speed/duplexing mismatch on the IP connection. If Autonegotiation is set on only one side, that side will default to 10/half.	Set both sides of the connection to use the same speed/duplexing setting, even if the setting is Autonegotiation.
	Archiving is in progress.	Wait a few minutes. Performance should return to normal when the appliance finishes archiving.
Device returns garbled text when you access it with the terminal command, OR When you access the device using the terminal command, no characters appear but the **`show serial`** command displays incrementing RX and TX.	Serial bit rate is set incorrectly.	Use the **`config serial`** command to change the port speed.
Pull or push operations to a switch fail by FTP but succeed by TFTP.	For a switch configured to use a dedicated Ethernet port with a static IP address, the appliance turns off the interface except when it is needed. When the appliance turns on the dedicated Ethernet port, it can take 30 seconds or more to become fully operational. This is long enough for the appliance to try the FTP transfer three times, and fail over to TFTP.	Configure the STP portfast feature on the layer 2 interface of the switch, or configure the switch to use DHCP for the dedicated Ethernet connection. See About using dedicated Ethernet ports on switches on page 42.
The display is illuminated but not scrolling status information. The display shows action selections instead.	The configuration menu is open.	Press the Back button (below the left arrow) to exit the configuration menu.
The `Configure` option is not available from the front panel (not applicable to Uplogix 430)	The keypad is disabled.	Use the **`config system keypad enable`** command.
An error message states that the appliance's time differs from the Uplogix Control Center's time.	The clocks do not match and the time difference is large enough to cause issues with reporting and logging functions.	Use the **`config system ntp`** command, and enter the Uplogix Control Center's IP address as the address of the NTP server.
Logs show UTC, not local time.	This is normal.	No action required.

Problem	Possible cause	What to do
Alert emails are not being sent.	At least one user is logged in to the appliance.	This is normal; alerts are emailed only if no sessions are open.

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.

Factory reset

In some situations, you may wish to clear all configuration, logs, and other data stored on the Uplogix appliance. Factory reset does these things:

- shuts down all services
- reformats the hard drive
- reinstalls the software

No data is retained. Following a factory reset, the appliance is in its initial state, just as it was when it was shipped.

The factory reset process takes roughly half an hour.

Note: To set an individual port back to its initial state, use the **`config system clear port`** command. See Clearing a previously configured port on page 48 for more information.

Caution: Do not power off or cycle power during the factory reset process.

Following a factory reset, you will need to do the initial configuration steps described in the ***Installation Guide for Uplogix Secure Remote Management Appliances***. Then do all applicable configuration procedures in Configuring the Uplogix appliance on page 17.

Resetting a 32-port Uplogix appliance or an older 4-port Uplogix appliance

If the appliance is managed by an Uplogix Control Center, delete it from the inventory before starting the factory reset.

For the 32-port Uplogix appliance and the older 4-port appliance, factory reset is available from the front panel keypad. Press the Enter key to scroll through the selections. The display shows several blank lines before displaying `Factory reset`. You will be prompted to answer `Yes` or `No` when you select `Factory reset`.

Resetting an Uplogix 430 appliance

To perform a factory reset on the Uplogix 430 appliance:

Step	System health light
Shut down the appliance, either using the shutdown command or by pressing the power cycle button and holding it for five seconds.	off
Disconnect the power cable.	off
Press and hold the power cycle button while reconnecting the power cable; continue to hold the power cycle button while the system health light blinks slowly.	off slow blink
When the system health light changes from blinking slowly to blinking fast, release the power cycle button.	fast blink
Immediately press and hold the power cycle button again. Continue to hold the power cycle button until the system health light turns off. The factory reset process is now starting. During the factory reset process, the system health light will begin blinking. When factory reset is complete, the system health light will stop blinking and stay illuminated.	fast blink off slow blink

Note: If you do not complete the sequence of button presses, the appliance powers on normally.

Support and regulatory information

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.

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

You may request up to 10 accounts.

Requesting 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 RMOS command line)

Phone: 512-857-7070

Fax: 512-857-7002

URL: www.uplogix.com/support

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 publications@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 compliance (EMC) and functional immunity that pertains to Uplogix systems.

Safety notices

USA: UL 60950-1

Canada: CSA C-22.2 No 60950-1-07

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.

Industry Canada (IC)

This Class [A] digital apparatus complies with Canadian ICES-003.

Cet appareil numerique de la Classe [A] est conforme à la norme NMB-003 du Canada.

RoHS compliance

The Uplogix Envoy NRM system and Uplogix 430 system 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.

CE Mark R & TTE directive

This equipment has been marked with the CE mark. This mark indicates compliance with EEC Directives 89/336/EC (electromagnetic compatibility), 73/23/EC (low voltage), and 92/59/EC (general product safety).

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.

Index