



User Guide

Uplogix Control Center

Version 4.6

December 2013

www.uplogix.com

Information in this document is subject to change without notice.

© 2013 Uplogix, Inc. All Rights Reserved. **Uplogix**, the **Uplogix logo**, and **SurgicalRollback** are trademarks of Uplogix, Inc. in the United States and other jurisdictions. All other marks referenced are those of their respective owners.

Uplogix, Inc.

7600-B North Capital of Texas Highway

Suite 220

Austin, Texas 78731

USA

Contents

About this guide	1
Target audience	1
Typographical conventions	1
Safety summary	2
Uplogix Glossary	3
Installation and configuration	4
Site requirements	4
Unpacking and installation	5
Unpacking the shipping box	5
Installing the server in a rack	5
Connecting power	5
Connecting the Ethernet port	5
Connecting the management console port	5
Provisioning	6
Completing access and security setup	7
Port communication	8
Working with the web interface	9
Logging in	9
Navigating the web interface	10
Information bar	10
Navigation bar	11
Contextual left navigation	11
Work area	11
Entering information	11
Printing	12
Managing the Uplogix Control Center	13
Install Information	14
Basic Settings	14
Setting the login banner	14
Setting the Web session timeout	15
Setting the time zone	15
Configuring Mail Settings	15
Configuring SNMP Settings	16
Send Logs	17
Managing the deployment	18
About inventory groups and inheritance	19
Viewing the inventory	20
Organizing inventory groups	21
About the Unassigned group	22
Editing an inventory group	23
Adding an inventory group	24
Reassigning an inventory group	25
Deleting an inventory group	26
Adding a Local Manager	27
Reassigning a Local Manager	31
Removing a Local Manager	32
Working with the dashboard	33

Managing licenses	34
Managing the equipment.....	36
Managing from the Local Manager Detail page.....	36
The summary view	37
Configuring a Local Manager	38
Configuration Options	39
Creating default Local Manager settings	42
Creating default port settings.....	43
Managing from the port detail pages.....	46
Creating categories for managing devices	47
Creating port labels	47
Assigning privileges by label	48
Setting up task filters using labels.....	49
Viewing reports by label	50
Managing scheduled tasks	50
Setting up filters and scheduling tasks.....	51
Tasks that can be scheduled	56
Scheduling tasks on a single Local Manager.....	59
Scheduling software upgrades on Uplogix Local Managers	60
Managing rules and monitors	63
Working with rules.....	63
Working with rule sets	66
Scheduling monitors	67
Applet Manual Out-of-Band modem connectivity via dial button	70
Managing accounts and security	72
Managing authentication	72
Setting authentication globally or within the inventory	73
Authentication, authorization, and accounting (AAA) settings	75
Setting requirements for strong passwords	78
Working with user and group accounts	80
Creating and editing user accounts	81
Creating and editing group accounts	83
Disabling user accounts.....	85
Deleting accounts.....	86
Managing privileges.....	86
Adding server privileges to accounts	86
Adding inventory privileges to accounts	87
Viewing and deleting user account privileges	90
Creating and customizing roles.....	91
Using Radius/TACACS to manage privileges.....	94
Example: Creating a superuser.....	96
Example: Limiting a user's access to one port on one system.....	97
Importing user, group, and privilege files	101
Logs, reports, and diagnostics.....	103
Setting up email, auditing, and subscriptions	104
Configuring an account to receive email from the Uplogix Control Center	104
Configuring the account to audit others and to be audited	105
Subscribing to alerts	105
Subscribing to reports.....	106
Specifying when and how often the subscriber receives alerts	107
Viewing alarms and events	109
Viewing reports	110
Inventory group reports	110
Local Manager reports.....	112
Reports by label	113
Report files.....	114
Report assignments	114

Viewing archive status information for a Local Manager	116
Viewing Local Manager Syslog Setting.....	117
Viewing session logs and auditing users	118
Local Manager session logs	118
Auditing user activities on the Uplogix Control Center	118
Sending logs to Technical Support	121
Replacing a Local Manager	122
Shutting down the Control Center.....	123
Advanced Control Center Functionality	124
SOCKS Proxy Support.....	124
Arguments	124
Usage	125
Serial Port Forwarding	126
About Connections.....	126
Usage	126
SSH Port Forwarding	129
Usage	130
Notes	132
SMS Outband (PPP on)	132
CLI Applet Failover to Managed Device	133
Device Properties	133
Usage	137
CLI Applet SSH Key Authentication	137
Arguments	137
Usage	141
Support and Regulatory information	142
Getting technical support	142
Requesting an account	142
Requesting support.....	142
Providing comments about this guide	142
Index	143

About this guide

This guide describes how to install and work with the Uplogix Control Center.



For best results, the Uplogix Local Manager and the Uplogix Control Center that manages it must use the same version of software.

Examples:

An Uplogix Control Center running version 4.5 or earlier, cannot manage Uplogix Local Managers that have been upgraded to version 4.6. An Uplogix Control Center running version 4.6 can provide limited management to Uplogix Local Managers that are using version 4.5 or earlier.

An Uplogix Control Center running any version 4.6.x software can manage Uplogix Local Managers running any 4.6.x software.

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

Target audience

This guide is intended for trained, qualified network support technicians responsible for installing and using the Uplogix Control Center.

Typographical conventions

The following conventions are used in this guide.

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

```
[admin@A505100303]# 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 are shown in **this font**. For example:

```
Administration > Server Settings
```

Safety summary

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



Caution: Follow all federal, state, and local regulations when disposing of this product.

Read and understand the following instructions before using the Uplogix Control Center:

- Use only electrical extension cords with a current rating equal to or greater than the Uplogix Control Center's current rating.
- Always disconnect the Uplogix Control Center from power before cleaning and servicing.
- Do not spray liquids directly onto the Uplogix Control Center when cleaning. Always apply the liquid first to a static free cloth.
- Do not immerse the Uplogix Control Center in any liquid or place any liquids on it.
- Connect the Uplogix Control Center to a grounded outlet.
- Only connect the Uplogix Control Center to surge-protected power outlets.
- Keep ventilation openings free of any obstructions.

SAVE THESE INSTRUCTIONS.

Uplogix Glossary

Term	Definition
Archive	Local Managers send bulk data, such as: session logs, device files, change logs, and all other non-urgent statistical data to the UCC every 60 minutes (default) using this encrypted HTTPS data communication protocol on port 8443.
Heartbeat	Uplogix Local Managers communicate with the UCC every 30 seconds (default) using this secure HTTPS communication method on TCP port 8443. Device state, alarms and configuration parameters are sent during a heartbeat.
Local Manager (LM)	A physical device or virtual machine directly connected to managed network devices and servers and that runs the Uplogix Local Management Software (LMS).
Uplogix 500	The Uplogix 500 Local Manager device is a fixed 5-port model that delivers advanced remote management capabilities for branch offices and remote locations on a robust platform. An additional (6th) port is available for power management connecting to a switched PDU (ServerTech/APC, etc.).
Uplogix 5000	The Uplogix 5000 Local Manager device is a modular chassis model with higher port density options that delivers advanced remote management capabilities for larger office and data center locations. The 5000 device has a power management port used to connect and manage switched PDUs (ServerTech/APC, etc.).
Uplogix Control Center (UCC)	Centralized point of control for all Uplogix Local Managers and managed devices deployed throughout the distributed IT environment. The web-based graphical user interface (GUI) enables IT administrators to easily manage, configure, and control all network devices and servers connected to Uplogix Local Managers. And access to real time data from these devices is supplied. The UCC is also the integration point for all remotely collected data and diagnostics for upstream delivery to NNM tools such as Solarwinds, HP OpenView, CA Spectrum, Tivoli, etc.

Installation and configuration

This chapter covers:

- [Site requirements](#)—power, temperature, air flow, and related safety information
- [Unpacking and installation](#)—physical connections
- [Provisioning the server](#)—configuration using the setup script
- [Completing access and security setup](#)—logging in to the server via SSH connection; changing the default password
- [Port communication](#)—inbound ports

Site requirements

Ensure that the power source:

- Provides the appropriate line voltage and frequency - 100 to 240 VAC, 50/60 Hz
- Provides overload protection
- Is connected to earth ground



Warning: The power source must meet all these requirements to ensure safe and reliable operation.

Ensure that the installation site meets these requirements:

- Ambient temperature does not exceed 95° F (35° C)
- The site provides at least 3 inches (8 cm) clearance beyond the Control Center's ventilation openings



Caution: The unit will overheat if the site does not meet these requirements.

Unpacking and installation

Before you begin the tasks in this section, verify your installation site meets all site requirements.

Unpacking the shipping box

Verify that you have received the following items:

- Uplogix Control Center
- Power cords
- Rack mount kit

Installing the server in a rack

The Uplogix Control Center is designed for installation in a 19-inch rack. Follow the instructions supplied with the mounting brackets.



Caution: Do not stack the chassis on other equipment. If the chassis falls, it can cause injury and equipment damage.

Connecting power

To power up the server, complete the following steps:

1. Connect the server to a suitable power source. The Uplogix Control Center uses dual power supplies for redundancy.
2. Connect both of the included power cords to the power receptacles located at the right rear of the server and to A/C power sources.



Caution: The plug-socket combination serves as the main disconnecting device and must be accessible at all times.

3. Press the power button on the front left to switch the system on.

Connecting the Ethernet port

Connect the lowest number Ethernet interface on the Uplogix Control Center to your LAN.

Connecting the management console port

To manage the server using the TTY console, connect a serial cable to your computer. The default speed setting is 9600, 8, N, 1.

Provisioning

Configure the Uplogix Control Center using one of these methods:

- Connect a standard VGA monitor, a keyboard and a mouse
- Configure using the console port by connecting your computer directly to the server using the DB-9 connector on the server's rear panel. Supported terminal clients include:
 - Windows HyperTerminal
 - ZTerm (Macintosh OS X)
 - Minicom (Unix/Linux)



Console default communication settings are 9600 baud, 8 data bits, 1 stop bit, no parity, and no flow control. Set your terminal emulator to use ANSI encoding for best results.

Log into the Uplogix Control Center using the `emsadmin` user account. The default password is password. To run the initial setup, use the `netSetup.sh` script located in `/uplogix/embassy/`.

```
ajones ~ $ ssh emsadmin@192.0.2.11
emsadmin@192.0.2.11's password:
[emsadmin@ems13 ~]$ /uplogix/embassy/netSetup.sh
Run Setup? (y/n) [y]
Install multi application servers? (y/n) [n]
Interface eth0 IP Address: 192.0.2.11
Interface eth0 Gateway: 198.0.2.1
Interface eth0 Netmask: 255.255.255.0
Configure eth1? (y/n) [n]
Disable eth1? (y/n) [n]
Configure hostname? (y/n) [n] y
Hostname: XYZCo_TX
Configure DNS? (y/n) [n] y
Primary DNS Server IP: 198.51.100.1
Secondary DNS Server IP: 198.51.100.2
Tertiary DNS Server IP:
Configure NTP? (y/n) [n] y
NTP Server: 198.51.100.112
Change emsadmin password? (y/n) [n]
Commit? (y/n) y
**** Editing /etc/sysconfig/network-scripts/ifcfg-eth0 ****
Gateway '198.51.100.1'
Netmask '255.255.255.0'
IP Address '192.0.2.11'
(output removed)
```

After committing your changes, the server displays messages as it updates the affected files.

Log out when you are returned to the command line prompt.

```
[emsadmin@ems13 ~]$ logout
```

If the server's hostname was set or changed, the change does not appear in the command prompt until your next session.

Completing access and security setup

The Uplogix Control Center uses Secure Shell (SSH) v2 software to provide secure remote access. Your remote client application must also support SSH v2. Use the SSH client to initiate a secure remote connection to the server.



The root account is not allowed to log in via SSH. Use the `emsadmin` account and supplied passwords.

Supported Secure Shell clients include:

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

For example, from a UNIX command line, type:

```
ssh emsadmin@192.0.2.0
```



The first time your SSH client connects to an SSH host following installation or upgrade, you may see an SSH key fingerprint message. This is normal. The client usually caches the key for subsequent use and warns if the host has changed, often indicating network eavesdropping.

To ensure security, change the `emsadmin` password after logging in for the first time. Use the UNIX `passwd` command:

```
[emsadmin@station]# passwd
Enter Old Password: *****
New Password [*****]: *****
Confirm Password: *****
```

The `emsadmin` user has super-user privileges with the `sudo` command. Review your security policy to determine if another user account should be created, though the account is limited to basic IP addressing of the server.

Port communication

The Control Center is designed to receive and respond to requests from Local Managers. The following inbound ports are used during normal operation.

Port	Usage Description
TCP 443	HTTP, provides access to the Control Center GUI
TCP 8443	Heartbeat, used for communication between Control Center and Local Managers
TCP 7	Echo, used by the Pulse feature
TCP 22	SSH, used to connect to the Control Center CLI
TCP 80	HTTP, provides access to the Control Center GUI, redirects to 443
UDP 123	NTP, provides NTP servers to managed devices



TCP 443 and TCP 8443 are required for normal UCC and LM interactions.

Working with the web interface

A web interface is provided with the Uplogix Control Center. Minimum requirements for the interface are Internet Explorer 7.0 and Firefox 3.6, with 128-bit encryption and the Java applet 1.5 plug-in. Recommended browsers include the latest stable release of Internet Explorer, Firefox, or Google Chrome.

This chapter covers basic information about the web interface:

- [Logging in](#)—start a session via a web browser
- [Navigating the web interface](#)—screen layout and navigational cues
- [Entering information](#)—things to know about typing in text fields
- [Printing](#)—capture the current view

Logging in

Direct a browser to **http://ipaddress**, where **ipaddress** is the address of the server. Requests made to port 80 (http) of the Uplogix Control Center are redirected to port 443 (https).



Your browser is likely to present a strong warning stating that the site's security certificate was issued for a different IP address. This is normal. The message will disappear once a recognized certificate is installed.

The browser displays the login screen.



Log in using your username and password. Both are case-sensitive. If setting up the Uplogix Control Center for the first time, log in using the default username and password as follows:

Username: **administrator**
Password: **password**



For security purposes, it is recommended that you immediately change the administrator's password. For information on setting passwords, see [Creating and editing user accounts](#).

Once successfully logged in, the Alarms page appears if there are active alarms. Otherwise, the Dashboard page is displayed.



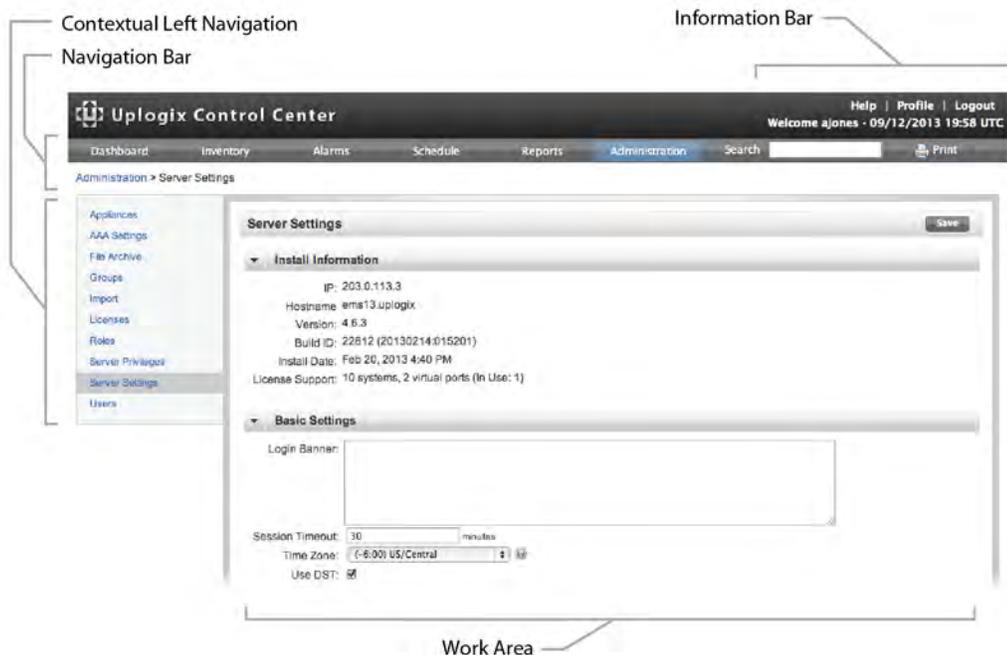
Last Occurrence	Duration	Appliance	Device	Context	Message
07/12/2013 11:53	67d 22h 31m	Pasadena	port4/1 (native)		TCP driver connection
07/12/2013 11:53	43d 14h 32m	Pasadena			NTP server invalid. (2
07/12/2013 11:53	43d 14h 32m	Pasadena			System and managem

3 items found, displaying all items.

Navigating the web interface

The Uplogix web interface presents four areas:

- The [information bar](#) shown at the top of the screen
- The [navigation bar](#) which displays the six main tabs
- The [contextual left navigation](#) which displays additional menu items
- The [work area](#) showing information or fields for input entry



Information bar

The information bar shown at the top of the screen displays the time and date as well as links to help, editing your user profile, and logging out of the UCC.

Navigation bar

The navigation bar displays six tabs provide access to a set of related tasks and information. The area you are working is indicated by the highlighted tab.

- [Dashboard](#)—Displays brief summary information, alarms, and events for user selected Local Managers.
- [Inventory](#)—Displays the organization of your Uplogix deployment, including inventory groups and individual Uplogix Local Managers.
- [Alarms](#)—Displays a summary of active alarms.
- [Schedule](#)—Use to define actions not triggered by rules.
- [Reports](#)—Provides access to create report assignments, view report files, and sort reports by label.
- [Administration](#)—Provides access to auditing, user administration, and configuration functions.

Contextual left navigation

The contextual left navigation displays additional menu items specific to the section of the user interface.



The controls available to you are based on the privileges assigned to your account. Unavailable items appear in gray. Mouse over a gray item to show a tooltip of the missing privilege.

Breadcrumb navigation

Breadcrumb navigation is provided at the top of the work area throughout the Uplogix Control Center. For example, when viewing the Detail page for an Uplogix Local Manager, the following navigation displays:

Inventory > XYZco_TX > Region 1 > A505100303

Each element is a link to another page, allowing you to move quickly between pages.

Some parts of the user interface are displayed in different ways depending on the browser you use.

Work area

The work area displays information and provides input fields to update or reconfigure the Uplogix Control Center or Local Manager.

Entering information

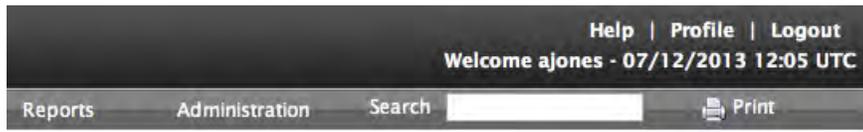
Some features require you to enter text - for example, when creating a user account you must enter a user name and may choose to enter a description.

Use only printing characters to complete text fields. Spaces may be used in descriptions, but not in naming accounts, roles, or other information that users may work with from an individual Local Manager's command line.

User names and passwords are case-sensitive. If you create a user account named ajones, the person will not be able to log in as Ajones. Some other information is case-sensitive as well.

Printing

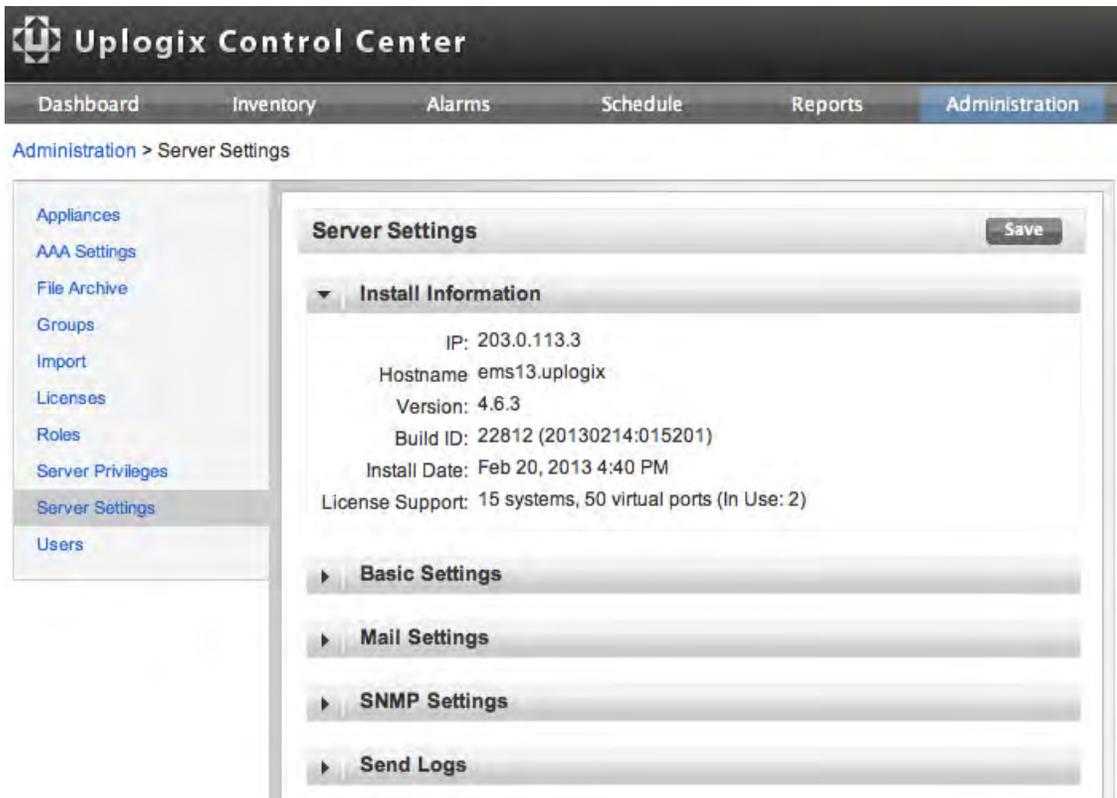
The Uplotix web interface provides a Print icon in the information bar.



Use Print to print the current contents of the work area. If a suitable PDF creator printer driver is installed, use the Print icon to save the current view as a PDF file.

Managing the Uplogix Control Center

This chapter describes the Administration > Server Settings selections.



This chapter covers:

- [Install information](#)—obtain the IP address, hostname, version, and build
- [Setting the login banner](#)—add a custom message on the login screen
- [Setting the Web session timeout](#)—change the default Web session timeout
- [Setting the time zone](#)—make adjustment for daylight saving time
- [Configuring mail settings](#)—specify a mail server and originating address for outgoing messages
- [Configuring SNMP settings](#)—specify an SNMP server

Install Information

Administration > Server settings > Install Information

The install information lists the IP address, hostname, version of software currently installed, software build, date of software installation, and the number of Local Manager licenses on the server.

Basic Settings

Administration > Server settings > Basic Settings

Use Basic Settings to set the:

- [Login Banner](#)—specify text to be displayed in the Uplogix Control Center login screen
- [Session Timeout](#)—set the Uplogix Control Center timeout
- [Time Zone](#)—set the system time zone

Setting the login banner

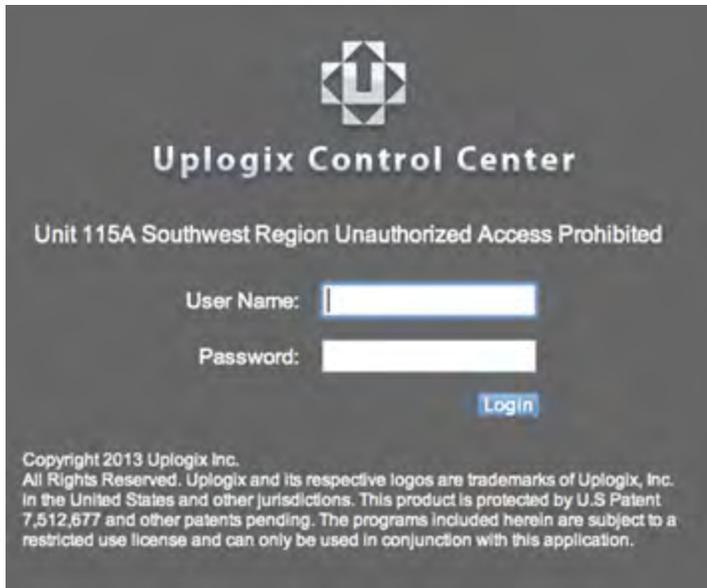
Specify the text to display in the Uplogix Control Center login screen. Line breaks entered in this text box are ignored.



Use only printing characters in the banner and other text fields. Spaces are considered printing characters.

A screenshot of the Uplogix Control Center web interface. The top navigation bar includes 'Dashboard', 'Inventory', 'Alarms', 'Schedule', 'Reports', 'Administration', and 'Search'. The 'Administration' menu is expanded to show 'Server Settings'. On the left, a sidebar lists various settings categories like 'Appliances', 'AAA Settings', 'File Archive', 'Groups', 'Import', 'Licenses', 'Roles', 'Server Privileges', 'Server Settings', and 'Users'. The main content area is titled 'Server Settings' and contains two sections: 'Install Information' and 'Basic Settings'. The 'Install Information' section shows details like IP (203.0.113.3), Hostname (ems13.uplogix), Version (4.6.3), Build ID (22812 (20130214:015201)), Install Date (Feb 20, 2013 4:40 PM), and License Support (15 systems, 50 virtual ports (In Use: 2)). The 'Basic Settings' section includes a 'Login Banner' text area containing the text 'Unit 115A', 'Southwest Region', and 'Unauthorized Access Prohibited'. Below this are fields for 'Session Timeout' (30 minutes), 'Time Zone' (set to (-6:00) US/Central), and a checked 'Use DST' checkbox. A 'Save' button is located in the top right corner of the settings panel.

Click **Save** and the new banner displays on the login screen.



Setting the Web session timeout

By default, Uplogix Control Center sessions time out after 30 minutes of inactivity. If this does not meet your organization's needs, change the value for Session timeout. You can set the timeout to any integer value from 5 to 1440 minutes (24 hours).

Once finished making changes, click **Save**.

The session timeout for Uplogix Local Managers is set separately. To set the Local Manager timeout across the inventory or within an inventory group, see [Creating default Local Manager settings](#). To set the timeout on individual Local Managers, see [Configuring a Local Manager](#).



If your session times out, you will be logged out but any operation in progress will not be affected. When you log in again, you are returned to the same page.

Setting the time zone

Correct UCC time is critical and should be provided by an NTP server. Set or change the IP address of the NTP server when running the setup script. See [Provisioning](#).

Daylight Saving Time adjustment

Although the Uplogix Control Center uses UTC in timestamps for alerts and events, it can be set to show local time in generated reports. Select **Use DST** if you desire to adjust Daylight Saving time in reporting.

Once finished making changes, click **Save**.

Configuring Mail Settings

Administration > Server settings > Mail Settings

The Uplogix Control Center can be configured to send alerts and reports by email. A mail server should be configured with a valid IP address and authentication settings. For more information, see [Setting up email, auditing, and subscriptions](#).

Mail Settings

Mail Server:

Mail Server Port:

Mail User:

Mail Password:

Confirm Mail Password:

From Address:

Prefer SSL for sending Email:

[Send a Test Email ▶](#)

To verify the email settings are configured correctly, click **Send a Test Email** to open the test email form. At a minimum, provide a valid email address where the test message should be received. Click **Send Test Email** to send the message.

[Send a Test Email ▼](#)

Recipient:

Subject:

Message:

Email successfully sent

Once finished making changes, click **Save**.

Configuring SNMP Settings

Administration > Server settings > SNMP Settings

During normal operation, the Uplogix Control Center receives Alarm and Event information from managed Uplogix Local Managers. If a third-party SNMP management tool has been set up to listen for SNMP traps, the Uplogix Control Center can be configured to forward any traps it receives. SNMP messages from Uplogix Local Managers source from the IP address of the managed Local Manager for system traps such as incorrect password attempts as well as for devices without Management IP addresses set. If a Management IP is specified the source address for the trap will reflect it.

SNMP Settings

Use SNMP:

Primary Host Name:

Primary Port:

Primary Read Community:

Secondary Host Name:

Secondary Port:

Secondary Read Community:

Once finished making changes, click **Save**.

Send Logs

Administration > Server settings > Send Logs

Users can send logs from the Uplogix Control Center by entering a valid email address and clicking the Send Logs button. These logs may be helpful to the Uplogix support team if they need to troubleshoot an issue with the Uplogix Control Center. To send logs to the Uplogix support team, enter the email address support@uplogix.com.

Managing the deployment

The Uplogix Control Center provides a central location for the configuration and monitoring of deployed Uplogix Local Managers. This chapter describes the organization scheme, CLI to GUI relationships, and Local Manager specific data display.

The groups mentioned in this chapter are inventory groups, not user groups.



For best results, Uplogix Local Managers and the Uplogix Control Center that manages them must use the same version of software.

Examples:

An Uplogix Control Center running version 4.5 or earlier, cannot manage Uplogix Local Managers that have been upgraded to version 4.6. An Uplogix Control Center running version 4.6 can provide limited management to Uplogix Local Managers that are using version 4.5 or earlier.

An Uplogix Control Center running any version 4.6.x software can manage Uplogix Local Managers running any 4.6.x software

This chapter covers:

- [Inventory groups and inheritance](#)—how changes propagate through the inventory
- [Viewing the inventory](#)—displaying only the information you need
- [Organizing inventory groups](#)—working with groups and moving Local Managers among them
- [Working with the dashboard](#)—keeping track of key information by groups of Local Managers
- [Managing licenses](#)—applying licenses you purchase



For most of the tasks described in this chapter, a role on the Uplogix Control Center that includes the config inventory privilege is required, such as the `admin` role. For more information, see [Adding server privileges to accounts](#) and [Adding inventory privileges to accounts](#).

About inventory groups and inheritance

Use the Uplogix Control Center to manage Uplogix Local Managers by group. Defining and applying user roles, rules, and tasks across large numbers of Local Managers in physically separate locations, reduces the need to repeat the same operations on each unit and the risk of introducing the variations that can occur during manual operations.

By grouping Uplogix Local Managers, all members of any inventory group can be treated the same while each inventory group can be treated differently. Many of the tasks that the Uplogix Control Center manages, such as assigning user roles and defining rules, can be performed at the root level or within any child group. All members of the inventory group and its child groups automatically inherit the newly created information.

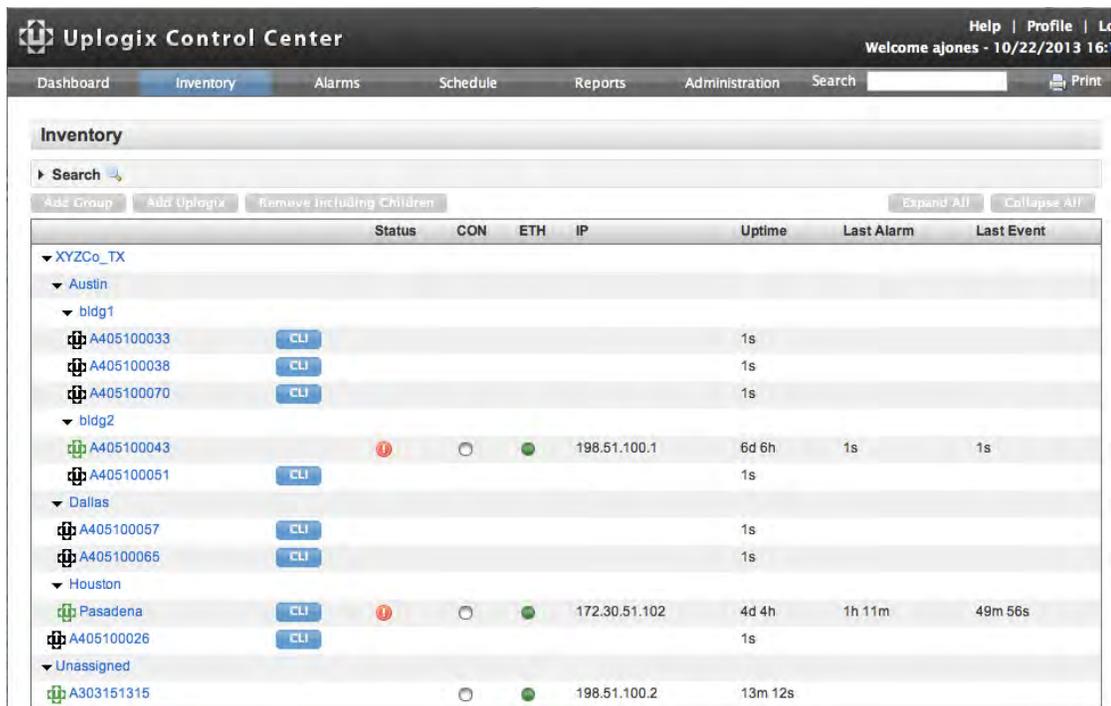
By default, the server provides the **Your Company** root group, which can be renamed, and the **Unassigned Group**, which is not editable. Neither of these can be deleted.

New inventory groups can be created within the root group. These child groups may also be nested. Groups may be based on any criteria that help organize your deployment. Uplogix Local Managers can be reassigned from one group to another at any time.

In this example, the root group has been renamed **XYZCo_TX** and contains three inventory groups: Austin, Dallas, and Houston. The Austin inventory group contains two child groups of its own: bldg1 and bldg2.

Uplogix Local Managers have been added to each of the inventory groups (Austin, Dallas, and Houston). In the case of the Austin inventory group, each Local Manager has been added to one of the two child groups within Austin. One Uplogix Local Manager, xyzsa01, has been assigned directly to the root group.

The Unassigned group contains an Uplogix Local Manager that has been configured to use this Uplogix Control Center, but has not yet been assigned to an inventory group.



The screenshot shows the Uplogix Control Center interface. The top navigation bar includes 'Dashboard', 'inventory', 'Alarms', 'Schedule', 'Reports', 'Administration', and 'Search'. The 'Inventory' section is active, displaying a search bar and buttons for 'Add Group', 'Add Uplogix', and 'Remove Including Children'. Below this is a table of inventory items with columns for 'Status', 'CON', 'ETH', 'IP', 'Uptime', 'Last Alarm', and 'Last Event'. The tree structure shows 'XYZCo_TX' expanded to 'Austin', which contains 'bldg1' and 'bldg2'. 'bldg1' has three units (A405100033, A405100038, A405100070) with 'CU' buttons. 'bldg2' has two units (A405100043, A405100051) with status indicators and 'CU' buttons. 'Dallas' has two units (A405100057, A405100065) with 'CU' buttons. 'Houston' has two units (Pasadena, A405100026) with status indicators and 'CU' buttons. 'Unassigned' has one unit (A303151315) with status indicators.

	Status	CON	ETH	IP	Uptime	Last Alarm	Last Event
XYZCo_TX							
Austin							
bldg1							
A405100033					1s		
A405100038					1s		
A405100070					1s		
bldg2							
A405100043	!	○	●	198.51.100.1	6d 6h	1s	1s
A405100051					1s		
Dallas							
A405100057					1s		
A405100065					1s		
Houston							
Pasadena	!	○	●	172.30.51.102	4d 4h	1h 11m	49m 56s
A405100026					1s		
Unassigned							
A303151315		○	●	198.51.100.2	13m 12s		

A collection of default port settings for Cisco model 3925 within the Austin inventory group of XYZCo_TX can be created. All Local Managers within the Austin inventory group and all child groups inherit these default port settings.

If a Local Manager is added to the bldg2 group, it inherits the Cisco 3925 default port settings from the Austin group. Similarly, if a child group is added to the bldg2 group, it also inherits the Cisco 3925 default port settings from its parent group.

If a child group, such as bldg1, already has Cisco 3925 default port settings before the Cisco 3911 settings are created in the Austin group, the child group retains its original Cisco 3925 default port settings by default. You can choose to overwrite existing settings in child groups.

Local Managers within the Unassigned group do not inherit any settings; they are outside the inventory's root group.



If default settings are deleted from a group, child groups retain the settings.

Viewing the inventory

Inventory

To view an expandable tree view of inventory, select the Inventory tab.

	Status	CON	ETH	IP	Uptime
▶ Your Company					
▶ Unassigned					

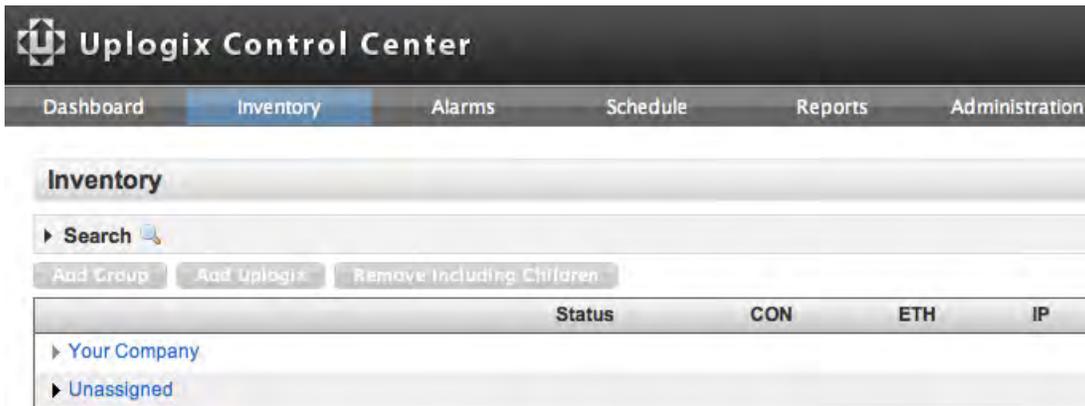
- The current organization of your deployment is shown, including inventory groups and individual Local Managers. Initially, the Inventory list shows only the two default groups, Your Company and Unassigned.
- The inventory is sorted alphabetically.
- To search for a specific Uplogix Local Manager, enter its hostname in the search box at the top of the inventory pane.
- To view the contents of an inventory group, click the expand icon ▶ to the left of the inventory group name.
- To view the group details, click the group name and the group detail page displays.
 - All functions concerning inventory groups can be accessed from the group detail page
 - A gray icon indicates the group is empty.

The icons beside each entry denote status or other information.

Icon	Description
	Inventory group is collapsed. <ul style="list-style-type: none"> Black arrow indicates the group contains at least one Local Manager or child group. Gray indicates the group is empty.
	Inventory group is expanded, listing the Local Managers and child groups.
	The Local Manager has communicated within the past four heartbeat intervals. The default interval is 30 seconds.
	No communication has been received from this Local Manager within the past four heartbeat intervals.
	This unit is communicating in minimal heartbeat mode. Commonly indicating local managers using an older version of LM software.
	This unit is communicating over the Outband (out-of-band) connection.
	The unit has been manually added to the inventory, but has not yet contacted the server.

Organizing inventory groups

Use the Inventory tab to organize and manage Local Managers by inventory group.



- Most management operations occur at the group level.
- To view the group details, click the group name and the group detail page displays.
 - All functions concerning inventory groups can be accessed from the group detail page
 - A gray icon indicates the group is empty.
- Inventory groups are always visible regardless of your privilege settings.

This section covers:

- [About the Unassigned group](#)
- [Editing an inventory group](#)
- [Adding an inventory group](#)
- [Reassigning an inventory group](#)
- [Deleting an inventory group](#)
- [Adding a Local Manager](#)
- [Reassigning a Local Manager](#)
- [Deleting a Local Manager](#)

About the Unassigned group

Executing the `config system management` command on an Uplogix Local Manager, places it under management by an Uplogix Control Center. The Local Manager is then placed in the Unassigned group on the Control Center, unless you have already created a placeholder for it in another group. See [Adding a Local Manager](#).



Unlike other inventory groups, the Unassigned group does not provide management capabilities. To manage an Uplogix Local Manager, it must be reassigned from Unassigned to another inventory group. See [Reassigning a Local Manager](#).

The Unassigned group cannot be deleted or edited and Local Managers cannot be reassigned to it.

To place an Uplogix Local Manager in the Unassigned group, delete it from another inventory group. At the next heartbeat, the Local Manager appears in the Unassigned group.

Editing an inventory group

Inventory > Group

The name and description of the root group and any inventory group you add can be edited. Changes to the name or description affect only the selected inventory group. Child groups or Uplogix Local Managers within the inventory group are not affected.

To edit an inventory group name:

1. Click **Edit** on the Group Detail page.



2. Edit the Name or Description as needed.
 - Name is required.
 - Description is optional.



3. Click **Save**.



Use only printing characters when completing text fields. Spaces are considered printing characters.

Adding an inventory group

Inventory > Group



Groups cannot be added to the Unassigned group.

To add an inventory group:

1. Navigate to the group in which a new child group is to be added.
2. Click **Add** in the Child Group area, the Create Group page displays.



3. Enter a Name and optionally, a Description of the new inventory group.
 - Name is required and must be unique within the entire inventory hierarchy.
 - Description is optional.





An inventory group name cannot be duplicated at a different level or within a different parent group.



Use only printing characters when completing text fields. Spaces are considered printing characters.

4. Click **Save**. The inventory list and detail is automatically refreshed. If the parent group was previously empty, its expand/collapse arrow changes from gray to black in the inventory tree view.



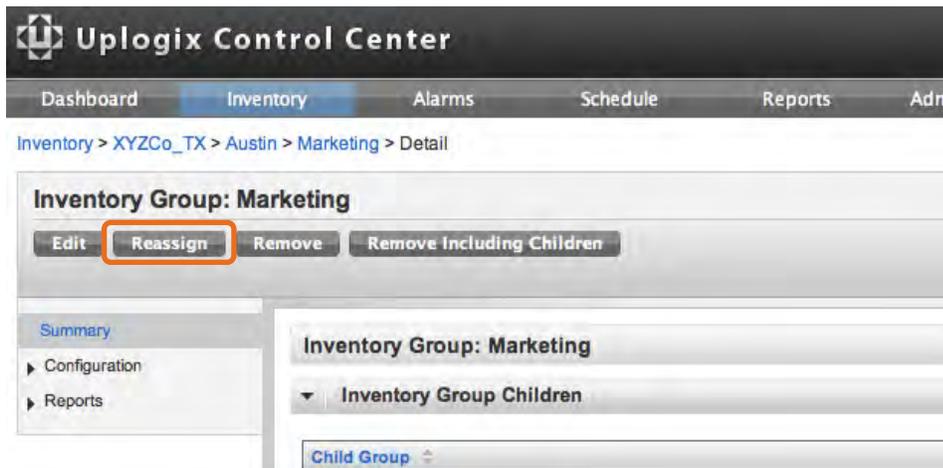
Reassigning an inventory group

Inventory > Group

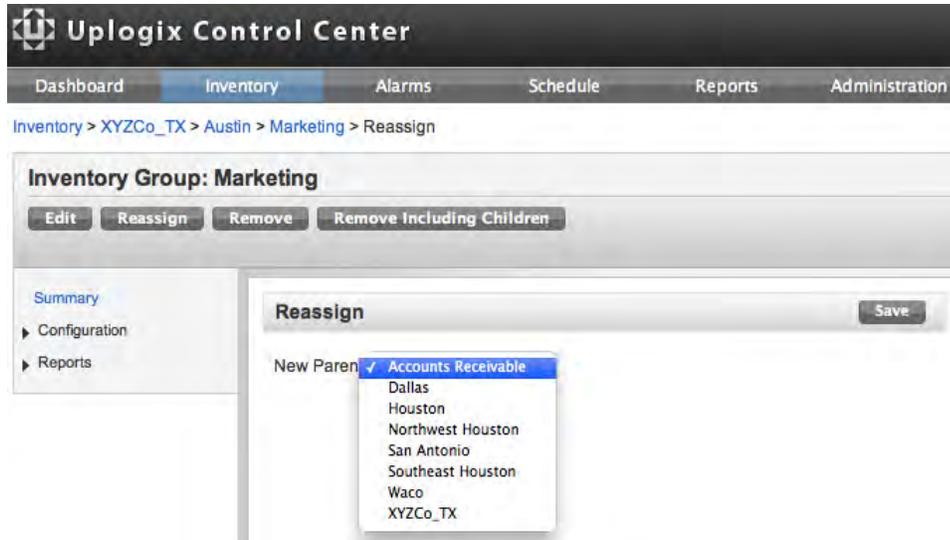
All groups, with the exception of the root and Unassigned groups, can be moved to another parent. Reassignment includes all of the child groups and Uplogix Local Managers assigned to the inventory group.

To reassign an inventory group:

1. Click **Reassign** on the Group Detail page, the Reassign page displays.



2. The **New Parent** list displays any available inventory groups. Only the current parent and Unassigned group are not shown. Select the new parent from the menu.



3. Click **Save**. The inventory list is automatically refreshed and displays the new location of the inventory group.

Deleting an inventory group

Inventory > Group

An inventory group can be deleted from the Uplogix Control Center using one of the following methods:

- Click **Remove** to move all the child groups and Local Managers into the parent group prior to deletion. For example, clicking Remove on the screen below would move all the members of the Marketing inventory group into the Austin group before Marketing would be deleted.



- Click **Remove Including Children** to delete the group and its child groups. For example, clicking Remove Including Children on the screen above would delete the Marketing inventory group, any child groups, and any Uplogix Local Managers assigned to the Marketing inventory group. Deleted Uplogix Local Managers return to the Unassigned group when they re-establish contact with the server at the next heartbeat.



Caution: There is no delete confirmation.

Adding a Local Manager

A management relationship must be established before the Uplogix Control Center can manage an Uplogix Local Manager.

A placeholder can be set up for the Local Manager beforehand, so the Local Manager is automatically added to the appropriate group when it contacts the server.



If user accounts have been created on the Uplogix Local Manager, they are deleted when the Uplogix Control Center adds the Local Manager to its inventory.

Creating a placeholder on the Uplogix Control Center (optional)

Inventory > Group

Create a placeholder in advance to add the Uplogix Local Manager directly to the inventory group of your choice. Users with the appropriate privileges within that group can manage the Local Manager as soon as it contacts the Uplogix Control Center. The Local Manager also inherits the configuration settings, privileges, roles, rules, preferences, and other defaults from that inventory group.

This step can be performed before the Uplogix Local Manager is physically installed.

To create a placeholder in advance:

1. Obtain the serial number of the Local Manager to be added. Find this number by issuing the `show version` command from the Local Manager's command line or by referencing the plate on the bottom of the 430 or 3200 Local Manager or the back of the 500 or 5000 Local Manager.
2. Select a group from the inventory list and the Group Detail page displays.

Uplogix Control Center

Dashboard Inventory Alarms Schedule Reports Administration

Inventory > XYZCo_TX > Austin > Building 1 > Detail

Inventory Group: Building 1

Edit Reassign Remove Remove Including Children

Summary

- Configuration
 - Applet
 - Archive
 - Authentication
 - Banners
 - Default Port Settings
 - DNS
 - Email
 - Export
 - LCD
 - Modem
 - NTP
 - Passwords
 - PPP
 - Privileges
 - Protocols

Inventory Group: Building 1

Inventory Group Children

Child Group Description

There are no child groups.

Add

Appliance Children

Appliance IP Hostname

There are no appliances in this group.

Add

3. Click **Add**.
4. Enter the serial number of the Uplogix Local Manager and optionally, a description.

Uplogix Control Center

Dashboard Inventory Alarms Schedule Reports

Inventory > XYZCo_TX > Austin > Building 1 > Create Uplogix

Inventory Group: Building 1

Edit Reassign Remove Remove Including Children

Summary

- Configuration
 - Applet
 - Archive
 - Authentication
 - Banners

Create Uplogix

Appliance Serial Number: A500100061

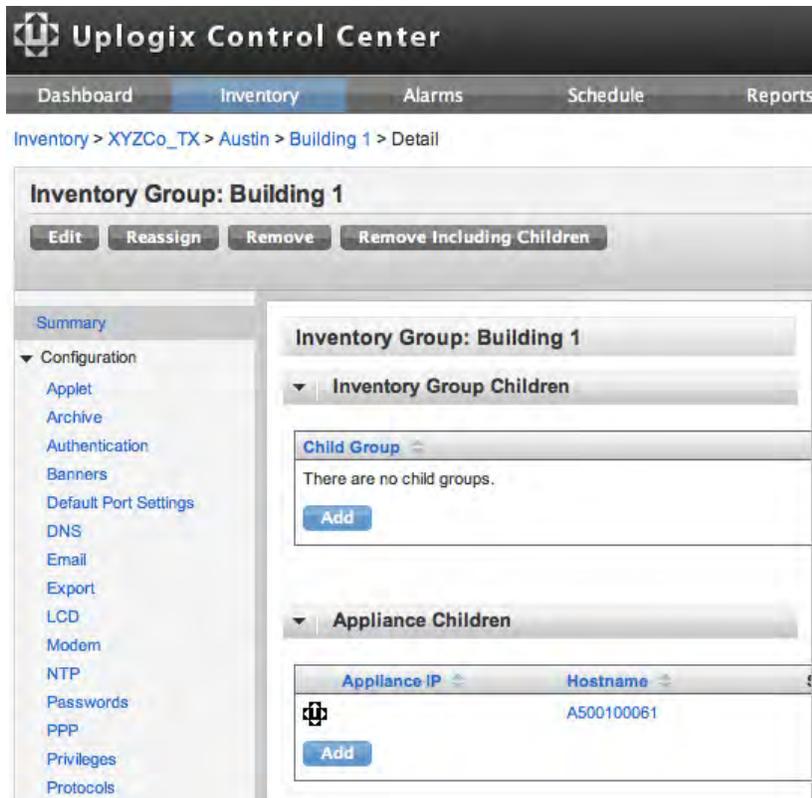
Description: Pasadena

Save

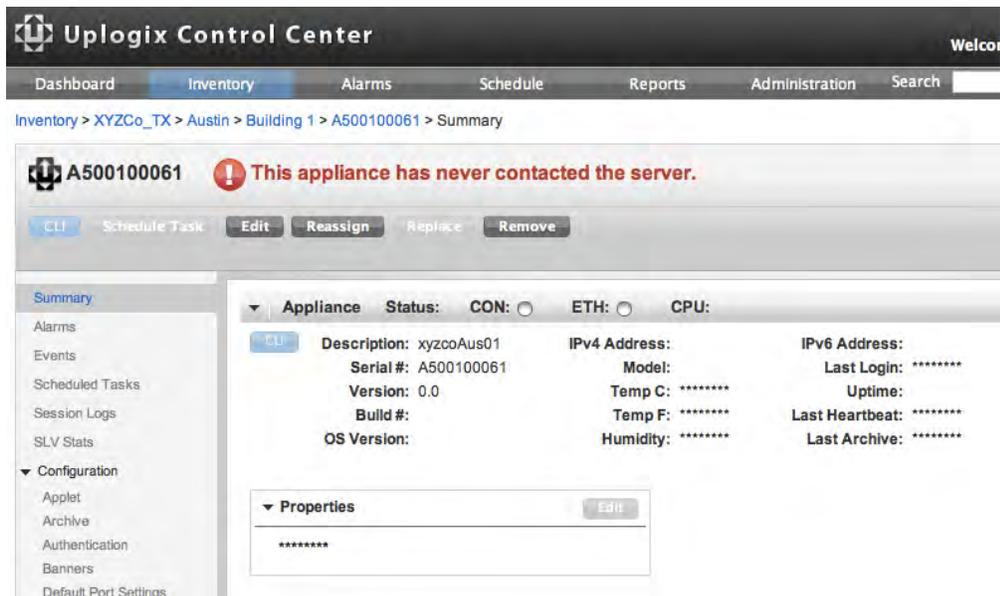


Use only printing characters when completing text fields. Spaces are considered printing characters.

5. Click **Save** to add a placeholder for the Local Manager. The Group detail page is automatically refreshed and displays the Local Manager



6. If the Local Manager is selected to view the detail page, its symbol appears in black. This is because there is no communication between the server and the Local Manager at this point.



Configure the Local Manager to use the Uplogix Control Center (required)

From the Uplogix Local Manager's command line interface, issue the `config system management` command. Use the IP address of your Uplogix Control Center in place of the IP address shown in the following example:

```
[admin@pasadena]# config system management
--- Existing Values ---
Use Management Server: false
Server Hostname or IP: 127.0.0.1
Server Port: 8443
Heartbeat interval (seconds): 30
Heartbeat Band: all
Always use minimal heartbeat: false (may only be configured on UCC)
Last successful heartbeat: (not yet contacted)
Change these? (y/n) [n]: y
--- Enter New Values ---
Use Management Server: (y/n) [n]: y
Server Hostname or IP: [127.0.0.1]: 192.0.2.11
Server Port: [8443]:
Set ntp location to 192.0.2.11: (y/n) [y]:
Heartbeat interval (seconds): [30]:
Heartbeat Band: all
Do you want to commit these changes? (y/n): y
Enabling NTP to point to 192.0.2.11
```

If a placeholder has already been set up in the inventory, once the LM executes a full Heartbeat the black icon for the placeholder turns green and the serial number is replaced by the hostname of the Local Manager (if one has been configured on the Local Manager). The default heartbeat interval is 30 seconds.



If a placeholder has not already been set up in the inventory, the Local Manager is placed in the Unassigned group.



The Local Manager cannot be managed while in the Unassigned group. It must first be reassigned to another inventory group. See [Reassigning a Local Manager](#).

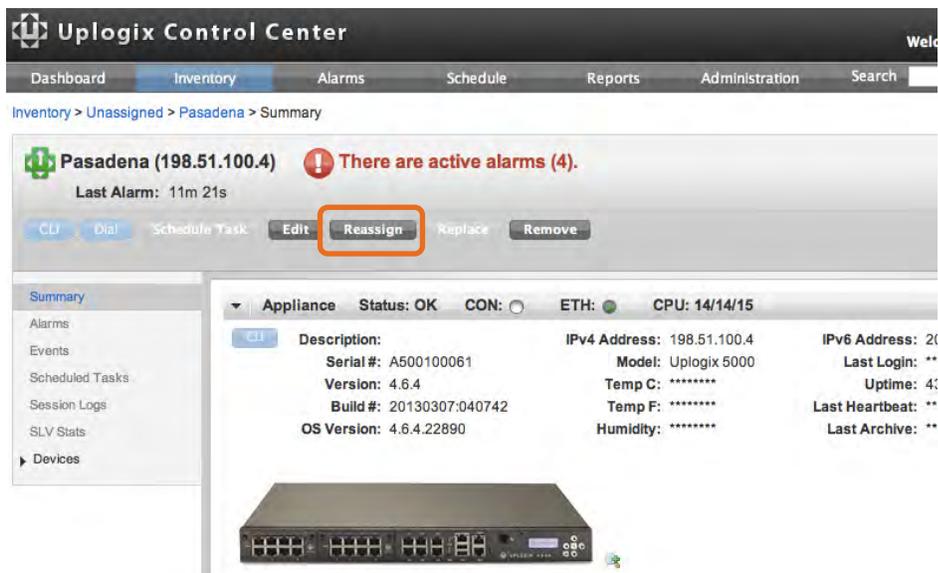
Reassigning a Local Manager

Inventory > Local Manager Page

An Uplogix Local Manager can be reassigned from the Unassigned group to another inventory group. Remember that a Local Manager in the Unassigned group cannot be managed.

To reassign a local manager:

1. Select the Local Manager from the inventory list.
2. Click **Reassign** from its detail page.



3. Available inventory groups are shown in the New Parent list. The only groups not shown are the current parent and the Unassigned group.

The screenshot shows the Uplogix Control Center interface. At the top, there is a navigation bar with tabs for Dashboard, Inventory, Alarms, Schedule, Reports, and Ad. Below this, a breadcrumb trail reads 'Inventory > Unassigned > Pasadena > Reassign'. The main content area displays 'Pasadena (198.51.100.4)' with a red warning icon and the text 'There are active alarms (4)'. Below this, it says 'Last Alarm: 11m 30s'. A row of buttons includes 'CLI', 'Dial', 'Schedule Task', 'Edit', 'Reassign', 'Replace', and 'Remove'. On the left, a sidebar menu lists 'Summary', 'Alarms', 'Events', 'Scheduled Tasks', 'Session Logs', 'SLV Stats', and 'Devices'. The 'Reassign' dialog is open, showing a 'New Parent' dropdown menu with a checkmark next to 'Accounts Receivable'. Other options in the dropdown include 'Austin', 'Building 1' (highlighted), 'Dallas', 'Houston', 'Marketing', 'Northwest Houston', 'San Antonio', 'Southeast Houston', 'Waco', and 'XYZCo_TX'. A 'Save' button is visible in the top right of the dialog.

4. Select the new parent group and click **Save**. The Uplogix Local Manager appears in the appropriate group of the inventory list.



While there is no function for moving an Uplogix Local Manager into the Unassigned group, this can be done by deleting the Local Manager. If it is still configured to use the Uplogix Control Center, it will reconnect on the next heartbeat and will then be placed in the Unassigned group.

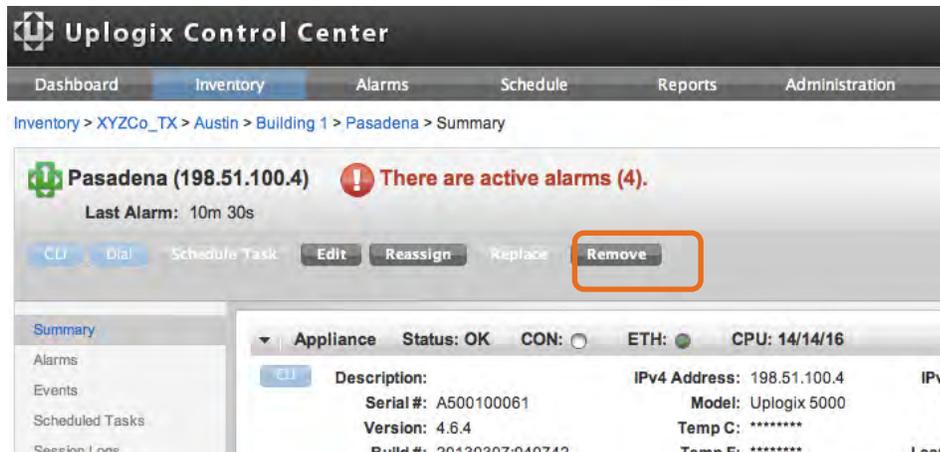
All inherited settings and user settings will be removed from the Local Manager

Removing a Local Manager

Inventory > Local Manager Page

An Uplogix Local Manager can be removed from the inventory. To remove a Local Manager from inventory:

1. Click **Remove** from the Local Manager page.



2. Most of the information about the Local Manager remains in the database. If the Local Manager subsequently contacts the server, it is placed in the Unassigned group. This happens if the Local Manager remains connected and configured to use the Uplogix Control Center.
3. To set the Local Manager to operate without management by the Uplogix Control Center, log into the Local Manager and issue the `config system management` command:

```
[admin@xyzcoAus01]# config system management
--- Existing Values ---
Use Management Server: true
Server Hostname or IP: 192.0.2.11
Server Port: 8443
Heartbeat interval (seconds): 30
Heartbeat Band: all
Last successful heartbeat: 07/03/2013 19:54:09 UTC (Full)
Change these? (y/n) [n]: y
--- Enter New Values ---
Use Management Server: (y/n) [y]: n
Disable NTP also? (y/n) [y]: y
Do you want to commit these changes? (y/n): y
```

4. You can also do this by selecting **Server** from the Configuration tab.

Working with the dashboard

Dashboard

The Dashboard helps keep track of key information for a selected group of Local Managers. The summary information of the selected Local Managers, as well as their ten most recent alarms and events, is displayed. The dashboard can also provide information to users with limited access to the Uplogix deployment.

To add a Local Manager to the dashboard, select the hostname from the dropdown menu and click **Add**.

Uplogix Control Center

Dashboard Inventory Alarms Schedule Reports Administration

Dashboard

✓ A101100558 Add Add All Remove
 A303151315
 Bammel
 Pasadena

You are currently tracking any appliances.

The Dashboard helps you track appliances you have permission to and care about. Try adding an appliance from the pulldown above to begin viewing summary information about it. The top 10 most recent alarms and events will be displayed. If you are not sure what appliances you want to follow, try clicking 'Add All'. If you don't have any appliances to choose from please contact your server administrator for assistance.

Alarms
There are no alarms.

Events
There are no events.



Available local managers are limited to ones you have permission to view. If no Local Managers appear in the selection menu, contact your server administrator for assistance.

Managing licenses

Administration > Licenses

Each Uplogix Control Center is initially configured to support a maximum of ten Uplogix Local Managers. By purchasing additional licenses, more management capability and advanced functionality can be added to the Uplogix Control Center.

Uplogix Control Center

Dashboard Inventory Alarms Schedule Reports Administration

Administration > Licenses

Appliances
 AAA Settings
 File Archive
 Groups
 Import
 Licenses

Licenses

By default the management server supports 10 systems.

Add Remove Choose System

Licenses

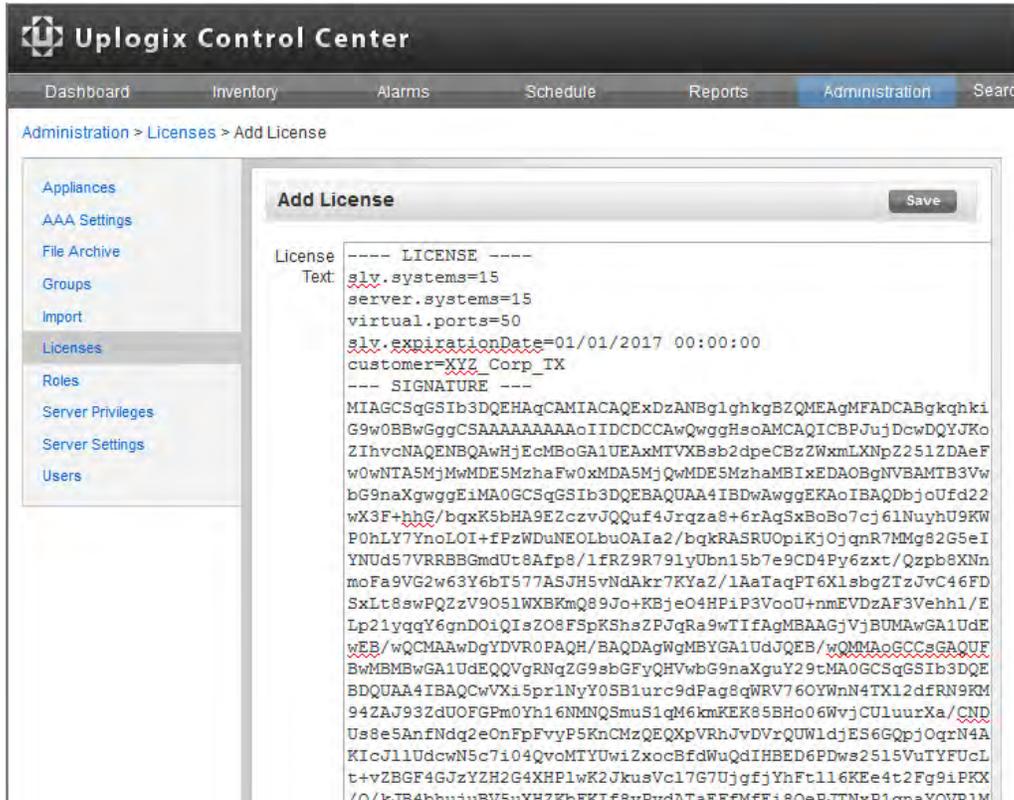
There are no licenses.

Uplogix Control Center licenses:

- specify the maximum number of managed Uplogix Local Managers which limits the number of units that can be moved from the Unassigned group.

- may include Service Level Verification (SLV) features which specify the number of Uplogix Local Managers on which SLV can be enabled.
- may include Virtual Port features which specify the number of Virtual Ports that can be created on Local Managers throughout the deployment.
- are not cumulative. The most recent license takes precedence if multiple licenses are present.

To apply a license, copy and paste the license text and click **Save**.



If the license includes SLV information, the **Choose Systems** link becomes active. Click the link to apply the SLV license to specific Uplogix Local Managers. SLV configuration options are available only for the specific Uplogix Local Managers to which the license is applied.



Managing the equipment

The Uplogix Control Center provides the ability to manage equipment at the group level. Individual Uplogix Local Managers and ports can also be managed.

This chapter covers:

- [Managing from the Local Manager detail page](#)—work with the dashboard view of an Uplogix Local Manager and the devices it manages
- [Configuring a Local Manager](#)—access the functionality offered by the `config` system commands
- [Creating default Local Manager settings](#)—automate configuration of newly added Local Managers
- [Creating default port settings](#)—automate configuration of devices on Uplogix Local Managers
- [Managing from the port detail pages](#)—detailed information about devices; access to the device CLI
- [Creating categories for managing devices](#)—creating and applying port labels
- [Managing scheduled tasks](#) – create filters to schedule tasks for specific Local Managers or managed devices
- [Managing rules and monitors](#)—automate performance assessment, diagnosis, and recovery
- [Establishing contact with a Local Manager via dial button](#)—contact remote Local Managers via dial button



To complete the tasks described in this chapter, a role with the appropriate permissions assigned at a suitable level within the inventory or a role on the Uplogix Control Center that includes the `config` inventory privilege (such as the `admin` role) is required. For more information, see [Adding server privileges to accounts](#) and [Adding inventory privileges to accounts](#).

Managing from the Local Manager Detail page

Inventory > Local Manager Page

From the Inventory list, or any screen where a given Local Manager is listed, click the hostname to view its detail screen. A quick view of the Local Manager and the devices connected to it appears. The equivalent Uplogix LMS CLI command is `show dashboard`. The Local Manager detail page displays the information being collected from the Uplogix Local Manager.



The Local Manager detail page shows or hides information based on your privileges. To see the name and details of a Local Manager listed in the Inventory hierarchy, your privileges must include login on that Local Manager or you must have the config hierarchy permission.

The summary view

The summary view is the default view for the Local Manager. The contextual left navigation provides options for viewing alarms, events, scheduled tasks, session logs, SLV statistics as well as configuration, reports and devices attached to the Local Manager. To display further configuration, reports and device options, click on the right arrow ▶ on the menu. The Local Manager's configuration information is listed in the work area, followed by information on the devices attached to the Local Manager. Initially, Local Manager and device information is expanded. Collapse these sections by clicking the down arrow ▼ icons to hide this information.

The screenshot displays the Uplogix Control Center interface. At the top, there is a navigation bar with tabs for Dashboard, Inventory, Alarms, Schedule, Reports, Administration, and Search. Below this, a breadcrumb trail shows the path: Inventory > XYZCo_TX > Austin > Building 1 > Pasadena > Summary.

The main content area features a header for "Pasadena (198.51.100.4)" with a red warning icon and the text "There are active alarms (3)". Below this, it indicates "Last Alarm: 10m 55s". A row of buttons includes CLI, Dial, Schedule Task, Edit, Reassign, Replace, and Remove.

A left-hand navigation menu is visible, listing options such as Summary, Alarms, Events, Scheduled Tasks, Session Logs, SLV Stats, Configuration (with a sub-menu), Applet, Archive, Authentication, Banners, Default Port Settings, DNS, Email, Export, IP, IPv6, and IPT.

The main content area is divided into sections. The "Appliance" section shows "Status: OK", "CON: ○", "ETH: ●", and "CPU: 14/14/15". Below this, a table lists details for the appliance:

CLI	Description:	IPv4 Address:	IPv6 Address:
	Serial #: A500100061	198.51.100.4	
	Model: Uplogix 5000		Last Log
	Version: 4.6.4	Temp C: N/A	Uptir
	Build #: 20130307:040742	Temp F: N/A	Last Heartbe
	OS Version: 4.6.4.22890	Humidity: N/A	Last Archi

Below the table, there is a "Properties" section with an "Edit" button and the text "No properties configured". To the right of this section is a photograph of the Uplogix 5000 appliance.

The "Devices" section is expanded, showing a list of devices. The first device is "port1/1 192.168.93.122" with a status of "○". The second device is "port4/1 UNAVAILABLE" with a status of "○" and a red warning icon.



The Local Manager detail page displays information based on your privileges. Scheduling functions are limited based on the config schedule command. Only users with access to this command on the system resource or port resource are able to schedule jobs on those resources from the Uplogix Control Center. Some elements in the left menu structure may be unavailable based on your privileges. SLV options are unavailable until the appropriate license is applied.

The Uplogix web interface provides a CLI applet used to access the Uplogix Local Manager's LMS command line using Secure Shell. The CLI applet requires Java to be installed on the workstation. Download the latest version of the Java Runtime Environment from <http://java.sun.com>.

The minimum and recommended system requirements for the CLI applet are:

Minimum	Recommended
Microsoft® Windows® XP, service pack 2	Microsoft® Windows® XP, service pack 3
Microsoft® Internet Explorer® 7	Latest stable releases of Microsoft® Internet Explorer®, Mozilla Firefox® or Google Chrome
Mozilla Firefox® 3.6	
Sun Java™ 1.5.0	Sun Java™ 1.6 or 1.7



Once launched, the CLI applet is independent of your session on the Uplogix Control Center. If you log out of the Uplogix Control Center while an active session is running in the CLI applet window, your CLI session remains open and active.

Use the CLI button  to access the built-in CLI applet to access the Uplogix Local Manager or devices.

Configuring a Local Manager

Inventory > Local Manager Page

The Uplogix Control Center provides a graphical interface for the configuration of managed Uplogix Local Managers. Use the Configuration menu to edit the Local Manager's configuration. The Configuration menu offers most of the same capabilities as the Uplogix LMS command line.

Click on the right arrow  on the menu to expand the Configuration menu.



Use only printing characters when completing text fields. Spaces are considered printing characters.

The configuration options mirror those of the Uplogix Local Manager. To change the Local Manager's configuration, select an option from the menu on the left. Enter the updated values and click **Save** to force the changes onto the Local Manager.

Some options may be unavailable, depending on your privileges. The IPT option is available only if the Local Manager has a Service Level Verification (SLV) license.

Configuration Options

Configuration option	Permission required	Purpose
Applet	show system applet	Configure authentication settings for Socks Proxy
Archive	config system archive	Configure archiving frequency from the Local Manager to the Uplogix Control Center
Authentication	config system authentication	Configure authentication settings for the Uplogix Local Manager
Banners	config system banner	Set banners on the Uplogix Local Manager
Default Port Settings	config settings	Edit or delete default port settings on the Uplogix Local Manager
DNS	config system ip	Specify the address of a DNS server (required only for SLV options)
Email	config system email	Configure outbound email from the Uplogix Control Center – for sending reports to subscribed users
Export	config system export	Configure settings for export of Uplogix Local Manager configuration
IP	config system ip	Configure the Uplogix Local Manager management Ethernet settings
IPv6	show system ip6	Configure the Uplogix Local Manager IPv6 address
IPT	config system ipt	Set up Local Manager to respond to SLV Voice testing VLANs and addresses.
LCD	config system keypad	Configure the Uplogix Local Manager LCD settings

Configuration option	Permission required	Purpose
Modem	<code>config answer (Modem resource)</code>	Configure modem behavior
NTP	<code>config system ntp</code>	Specify an NTP server By default, Local Managers use the Uplogix Control Center
Passwords	<code>config password</code>	Configure password settings
PPP	<code>config ppp (Modem resource)</code>	Configure dial-up information for establishing out-of-band connections
Privileges	<code>config privileges</code>	Configure access on the port associated with the Uplogix Local Manager
Properties	<code>config system properties</code>	Configure properties on the Uplogix Local Manager
Protocols	<code>config system protocols filter</code>	Configure IP filtering
	<code>config system protocols ssh</code>	Configure terminal pass-through using SSH
	<code>config system protocols telnet</code>	Configure terminal pass-through using Telnet
Pulse	<code>config system pulse</code>	Specify a pulse server for the Uplogix Local Manager
Roles	<code>config role</code>	Create or update roles on the Uplogix Local Manager
Rules	<code>config rules</code>	Create or update rules on the Uplogix Local Manager
Rule Sets	<code>config ruleset</code>	Create or update rule sets on the Uplogix Local Manager
Secondary Ethernet	<code>show system ip</code>	Configure the Uplogix Local Manager secondary Ethernet settings for bonded, capture or Outband

Configuration option	Permission required	Purpose
Serial	<code>config system serial</code>	Specify whether the Uplogix Local Manager is DCE for its serial management connection (400/3200 Only)
Server	<code>config system management</code>	Configure the Uplogix Local Manager to delegate to an Uplogix Control Center, the TCP port used, the heartbeat interval, and other related information
SLV Tests	<code>config slv</code>	Configure and view SLV tests being run on the Uplogix Local Manager
SNMP	<code>config system snmp</code>	Enable and configure the Uplogix Local Manager to respond to SNMP requests – Version 3 only
Syslog	<code>config system syslog-options</code>	Enable syslog and specify target syslog server
Subinterfaces	<code>config system subinterface</code>	Configure and view subinterfaces defined on the Uplogix Local Manager's Management Ethernet port
Timeout	<code>config system timeout</code>	Set the idle CLI session timeout for the Uplogix Local Manager
Virtual Slots	<code>config system slot</code>	Configure or remove virtual slots on the Uplogix Local Manager
VPN	<code>config vpn (Modem resource)</code>	Configure VPN type and setup

For configuration information, consult the *User Guide for Uplogix Local Managers*.

Configuration settings are also available on the Inventory Group level. However, some Local Manager-specific settings such as IP address cannot be applied to an inventory group.

Creating default Local Manager settings

Inventory > Group

Use the Uplogix Control Center to apply a standard configuration to all Uplogix Local Managers within a group.



To set up standard configurations, your role must have either Local Manager configuration permissions on the affected Local Managers or the config hierarchy permission. If your role includes the config hierarchy permission, only configurations for empty inventory groups can be set up. For more about roles and permissions, see [Managing privileges](#).

To create default Local Manager settings:

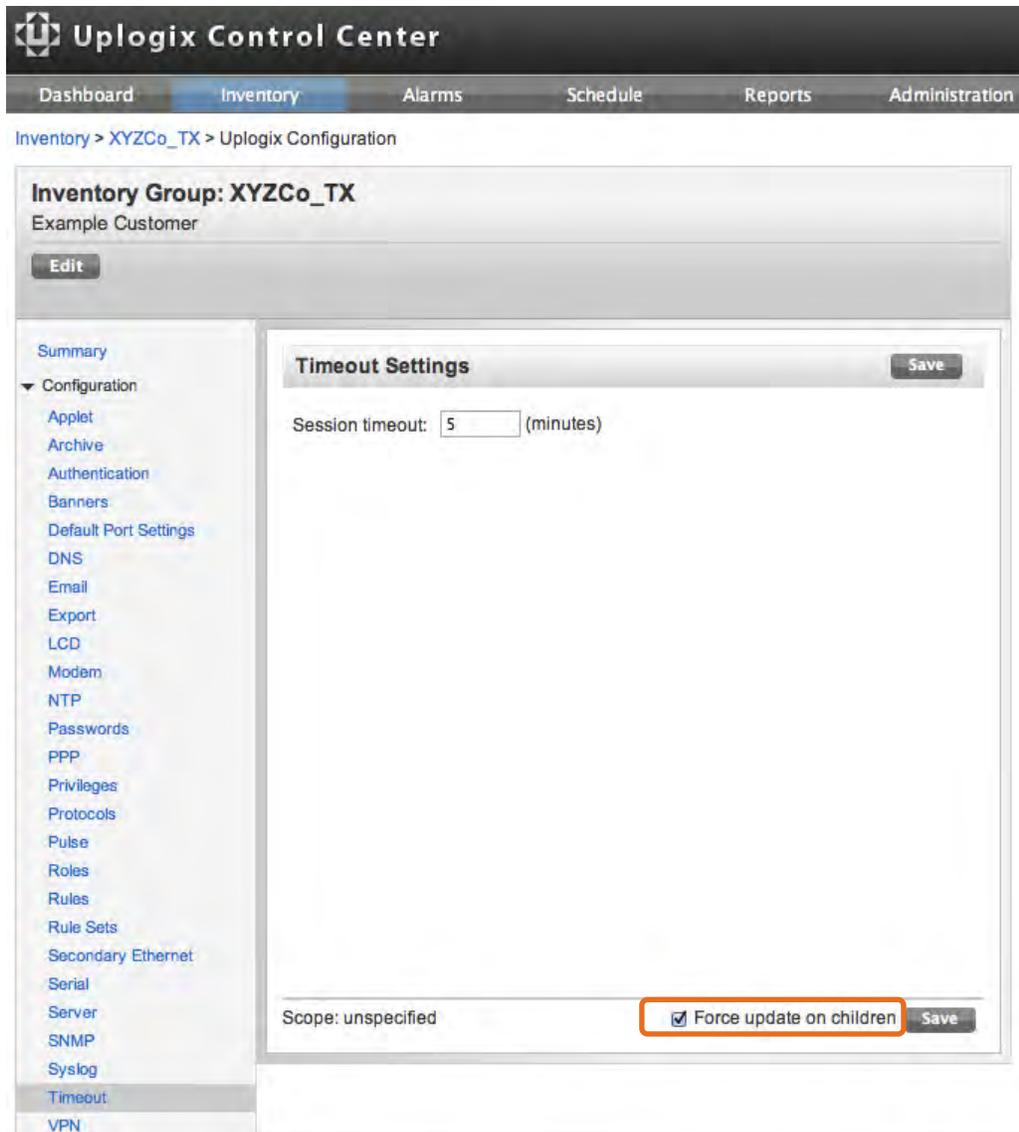
1. Expand the Configuration menu on the left to view the list of Configuration settings (i.e., Applet, Archive, Authentication, etc.).

The screenshot shows the Uplogix Control Center interface. At the top, there is a navigation bar with tabs for Dashboard, Inventory (selected), Alarms, Schedule, and Reports. Below the navigation bar, the breadcrumb path is 'Inventory > XYZCo_TX > Detail'. The main content area is titled 'Inventory Group: XYZCo_TX' and includes an 'Edit' button. On the left side, there is a 'Configuration' menu with various settings listed, including Applet, Archive, Authentication, Banners, Default Port Settings, DNS, Email, Export, LCD, Modem, NTP, Passwords, PPP, Privileges, Protocols, Pulse, Roles, Rule Sets, and Secondary Ethernet. The main content area is divided into two sections: 'Inventory Group Children' and 'Appliance Children'. The 'Inventory Group Children' section contains a table with columns 'Child Group' and 'Description'. The table lists four child groups: Dallas (Finance Group B), Houston (Operations Group), San Antonio (Marketing Group), and Waco (Accounting Group). There is an 'Add' button below the table. The 'Appliance Children' section contains a table with columns 'Appliance IP' and 'Hostname'. The table is empty, and there is a message 'There are no appliances in this group.' with an 'Add' button below it.

Child Group	Description
Dallas	Finance Group B
Houston	Operations Group
San Antonio	Marketing Group
Waco	Accounting Group

Appliance IP	Hostname
There are no appliances in this group.	

2. Click the setting name for each configuration setting to be defined.
3. Make any necessary changes.
4. To override settings locally defined to Uplogix Local Managers in the group, select **Force update on children**.



5. Click **Save**.

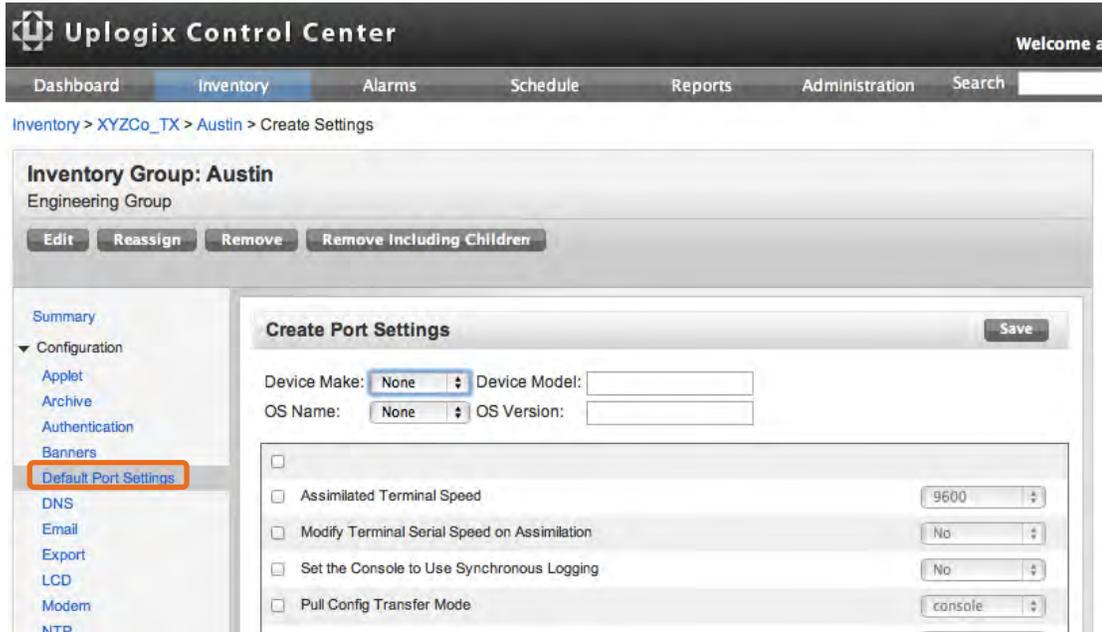
Creating default port settings

Inventory > Group

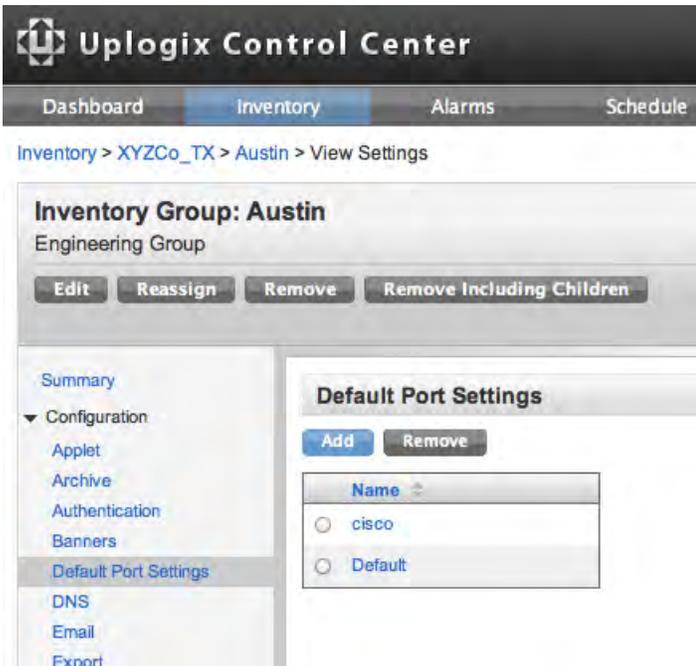
Use the `config settings` command on the Uplogix Local Manager to define how the Local Manager communicates with the device connected to a given port. On the Uplogix Control Center, these settings can be defined and applied to more than one port; they could apply to all devices of a specific make, model, or operating system. For example, define a default port settings profile for all Cisco devices to set the terminal speed to 19200 for any Cisco device.

Default port settings are inherited from inventory groups, so a setting profile defined at the root group is inherited by the entire deployment. Setting profiles defined in a child inventory group are only inherited by its child groups and the Uplogix Local Managers in those inventory groups. Therefore, it is possible to have default port settings for a Cisco 3925 that set the terminal speed to 9600 in Group 1, and identically named default port settings in Group 2 that set the speed to 19200. This type of situation can also occur when a child group already has default port settings stored under the same name as the settings you create in the parent group.

To access the Create Port Settings page, click **Default Port Settings** from within the Configuration menu for the group to which the settings apply.



Any default settings that have been created are listed. Use the View Settings page to edit, remove, or add default port setting profiles.





Removing a port setting profile does not affect the devices where the settings have already been applied. For example, referring to the screen above, if the Cisco settings are removed, the configuration of Cisco devices is not changed. If you then connect a Cisco device to an Uplogix Local Manager, the Cisco profile is no longer present and the port settings will manually need to be configured using the `config settings` command.



The Create Settings option is not available if the inventory group is empty. However, the Default profile can be edited. This default port settings profile can be changed but not deleted.

The Create Settings and Edit Settings page present the same choices as the `config settings` command in the Uplogix LMS CLI.

Specify as much or as little information as necessary when creating settings. The Uplogix Local Managers that inherit these settings will apply them to any port that matches all the information given. For example, specifying **cisco** will match all Cisco devices. Specifying **cisco** and **3925** will match only Cisco 3925 devices. If the desired device make is not listed, choose **native**.

Select the settings to change using the checkboxes on the left, and modify the values as needed.

The screenshot shows the Uplogix Control Center interface. At the top, there's a navigation bar with 'Dashboard', 'Inventory', 'Alarms', 'Schedule', 'Reports', 'Administration', and 'Search'. Below that, a breadcrumb trail reads 'Inventory > XYZCo_TX > Austin > Create Settings'. The main content area is titled 'Inventory Group: Austin' and 'Engineering Group'. There are buttons for 'Edit', 'Reassign', 'Remove', and 'Remove Including Children'. On the left, a sidebar menu lists various configuration options under 'Configuration', with 'Default Port Settings' selected. The main panel is 'Create Port Settings'. It features a 'Device Make' dropdown menu with 'cisco' selected. Below it, there's a list of device models with checkboxes: 'Assimilation', 'Modify T...', 'Set the C...', 'Pull Con...', 'Push Co...', 'Alternati...', 'Config T...', 'OS Imag...', 'Alternati...', 'Attempt...', 'Save Co...', and 'Reset C...'. To the right, there are input fields for 'Device Model' and 'Version', and a table of settings with checkboxes and buttons.

When editing existing default port settings, specify whether to force the update on any child groups within the affected inventory group. Otherwise, the settings are only updated in the current inventory group.

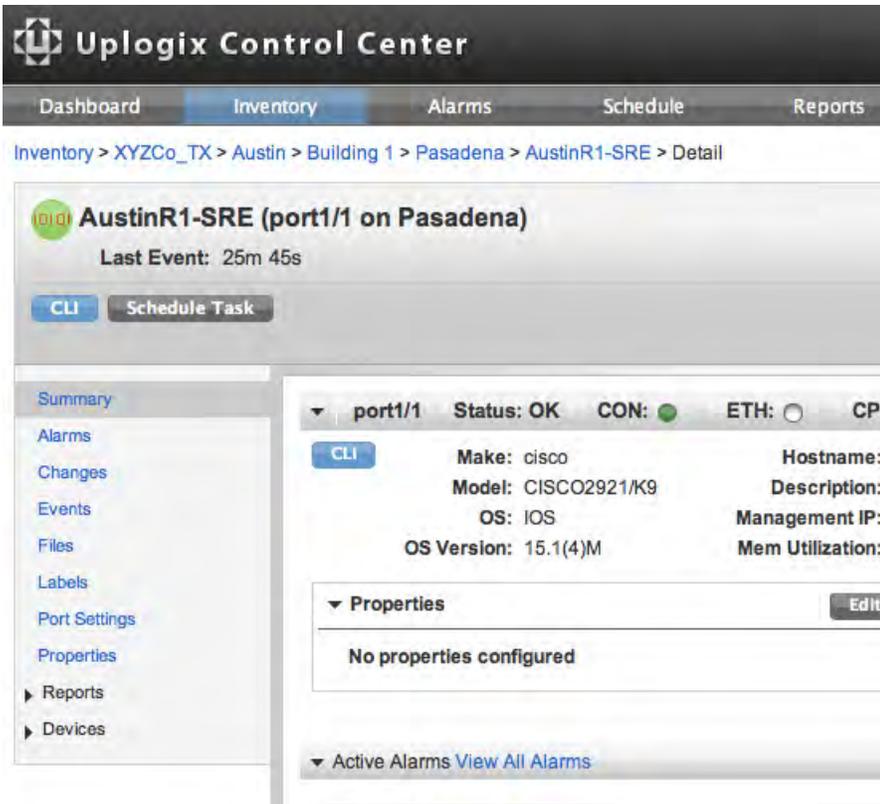


A screenshot of a web form for configuring port settings. It contains three rows of settings, each with a checkbox on the left and a value field on the right. The first row is 'manual boot' with a value of 'No'. The second row is 'Device pass through timeout' with a value of '300'. The third row is 'Enable local echo' with a value of 'No'. At the bottom right of the form, there is a checkbox labeled 'Force update on children' and a 'Save' button.

Managing from the port detail pages

Inventory > Local Manager Page > Port Page

From the Local Manager page, view the port details by clicking the individual port. The contextual left navigation provides access to features that correspond to CLI commands executed from the port resource.



A screenshot of the Uplogix Control Center interface showing the details for a port. The top navigation bar includes 'Dashboard', 'Inventory', 'Alarms', 'Schedule', and 'Reports'. The breadcrumb trail is 'Inventory > XYZCo_TX > Austin > Building 1 > Pasadena > AustinR1-SRE > Detail'. The main content area is titled 'AustinR1-SRE (port1/1 on Pasadena)' and shows 'Last Event: 25m 45s'. There are two buttons: 'CLI' and 'Schedule Task'. A left sidebar contains a navigation menu with items: Summary, Alarms, Changes, Events, Files, Labels, Port Settings, Properties, Reports, and Devices. The main content area shows the port name 'port1/1' with status 'OK', 'CON' (green dot), 'ETH' (grey circle), and 'CPU'. Below this, there is a 'CLI' button and a table of device information: 'Make: cisco', 'Model: CISCO2921/K9', 'OS: IOS', 'OS Version: 15.1(4)M', 'Hostname:', 'Description:', 'Management IP:', and 'Mem Utilization:'. A 'Properties' section is collapsed, showing 'No properties configured' and an 'Edit' button. At the bottom, there is an 'Active Alarms' section with a 'View All Alarms' link.

Creating categories for managing devices

There are several methods to manage your Uplogix deployment and managed devices. Use inventory groups to manage Uplogix Local Managers by logical groups such as location or business unit. Device information entered during port configuration of the Local Managers allows users to manage devices by make and model. Finally, users can assign labels to an Uplogix Local Manager's managed devices to group them in more flexible ways.

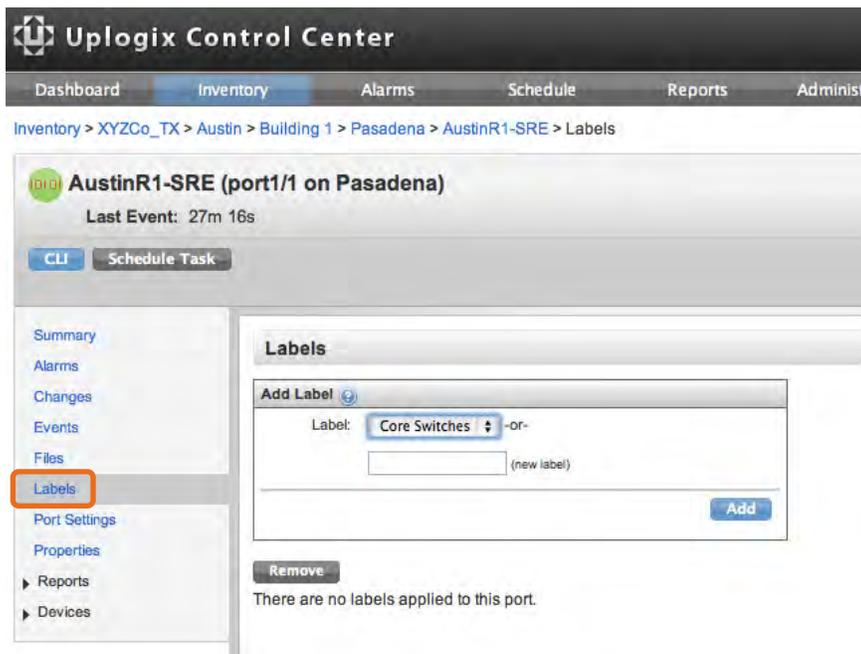
Labels can be used to group devices by other criterion such as maintenance windows, scheduling reports, or assigning privileges on all routers regardless of make. Another would be grouping managed devices by business unit in cases where several business units share an Uplogix Local Manager.

Labels are managed from the Uplogix Control Center and cannot be assigned from the Local Manager's LMS command line.

Creating port labels

Local Manager Page > Port Page

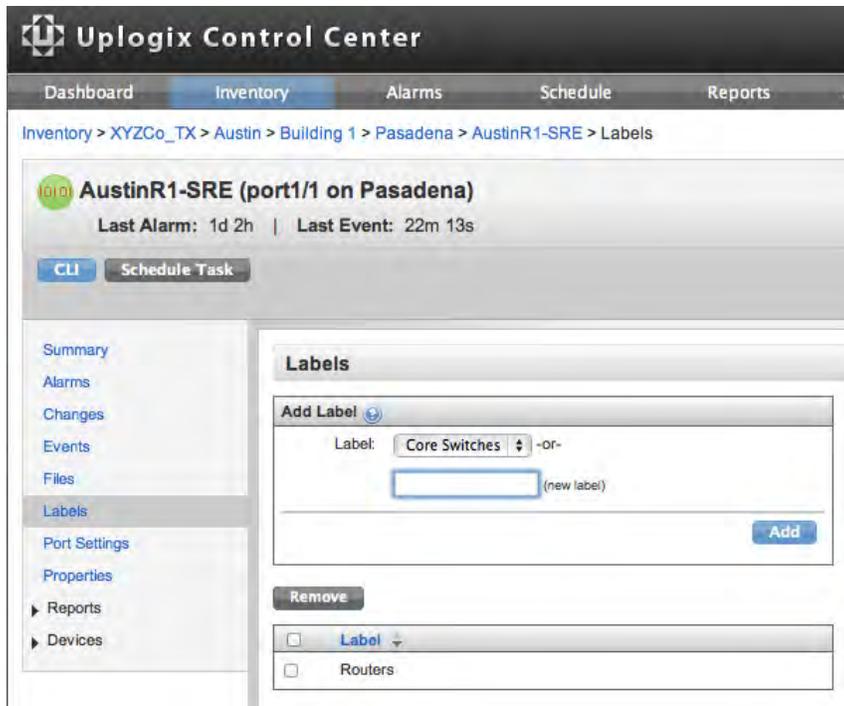
To assign a label to a port, open the detail page for the Uplogix Local Manager that manages it. Then expand the detail for the port to be labeled.



Click the **Labels** menu item to open the Labels page.

Create a new label for the port and then click **Add** to apply the label to this port. More than one label can be applied to a port.

For example, port 1/1 may be given a new label, **Core Switches**.

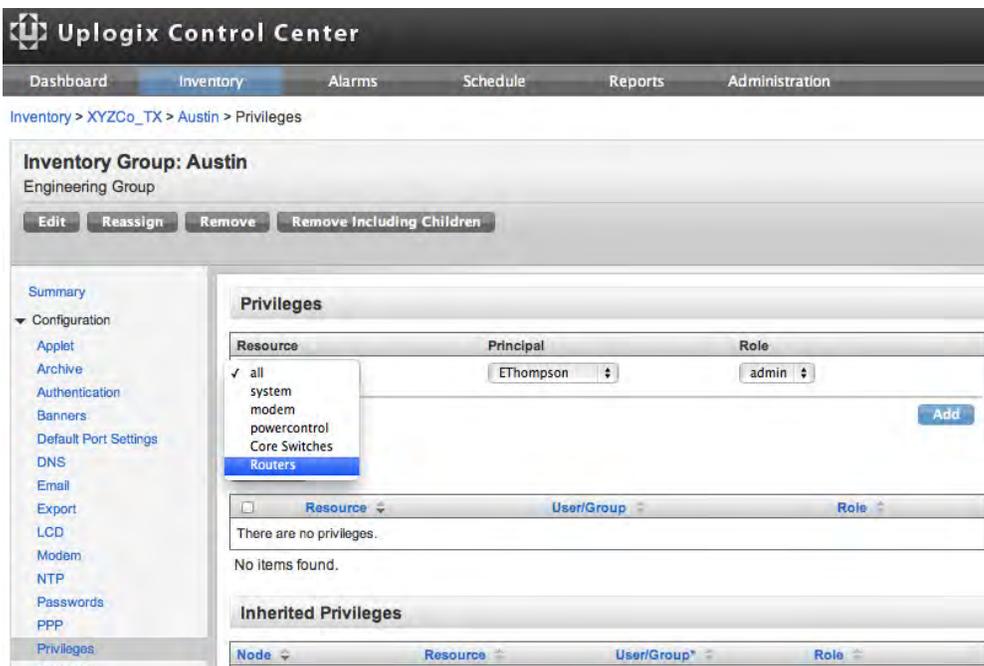


Assigning privileges by label

Inventory > Group > Configuration > Privileges

Privileges are created by assigning the user or user group a role (such as admin or guest) to a resource (such as port 1/2). The default resources within the inventory are the same resources found in the Uplogix LMS command line interface - system, modem, powercontrol, and the individual ports. If labels have been created, they are also considered resources.

The example below shows how to assign admin rights to a user on all routers. For more information about assigning privileges, see [Managing privileges](#).



Setting up task filters using labels

Schedule > Filters

Use Labels as a filtering criterion when setting up filters for scheduling tasks. View and edit these filters on the Schedule > Filters page. For more information about task filters, see [Setting up filters and scheduling tasks](#).

Schedule > Filters > Edit Filter

Scheduled Tasks

Filters

Edit Filter: RoutersAustin

Filter Information

Name: RoutersAustin
Description: All Routers in the Austin Group

Inventory Groups

Remove

Group Name ⇅

Austin

Building 1 ▾ **Add**

Appliances

Remove

Appliance Name ⇅

This filter contains no appliances.

select **Add**

Devices

Remove

Device ⇅

This filter contains no devices.

select **Add**

Device Criteria

Device Criteria ⇅

This filter contains no device criteria.

Device Make: **None** ▾ Device Model: **Add**

OS Name: **None** ▾ OS Version:

Labels

Remove

Label ⇅

This filter contains no labels.

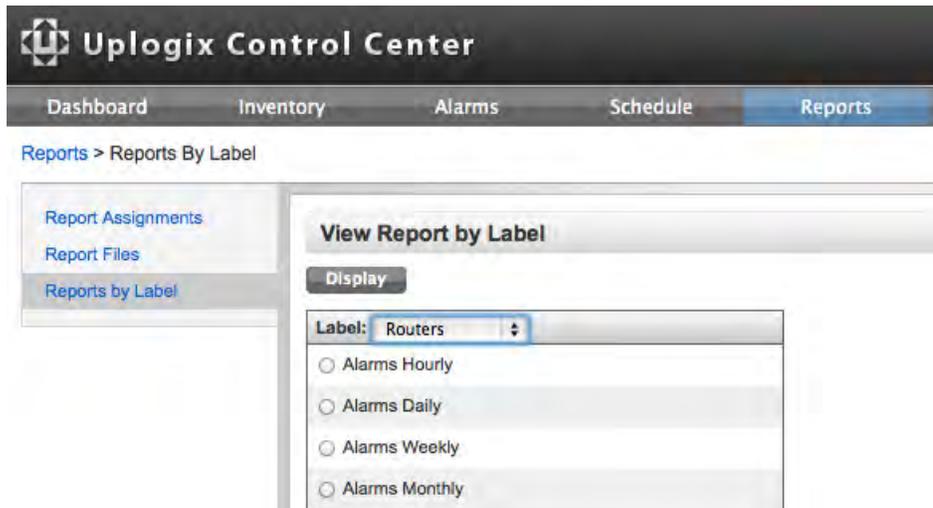
routers ▾ **Add**

routers

Viewing reports by label

Reports > Reports by Label

Once labels are assigned to port devices, the Uplogix Control Center automatically creates reports based on the labels. View these reports on the Reports > Reports by Label page. For more information about reports, see [Viewing reports](#).



Managing scheduled tasks

Schedule routine tasks to take place automatically. To schedule a task:

- Create a task filter or select an existing task filter
- Choose and schedule the task

A filter specifies the portion of the inventory that is affected by a scheduled task.

For example, to define a task that clears the counters on all Cisco devices within a specific inventory group periodically, a filter is needed which specifies all Cisco devices within that group. Use this filter to schedule the Clear counters task.

Filters and filter options are limited to Local Managers and ports to which you have config schedule access.

Some scheduled tasks are available from the expanded Local Manager detail pages. These tasks are scheduled only on the individual Local Manager; therefore a filter does not need to be selected.

This section covers:

- [Setting up filters and scheduling tasks](#)
- [Tasks that can be scheduled](#)
- [Scheduling tasks on a single Local Manager](#)
- [Scheduling software upgrades on Uplogix Local Managers](#)

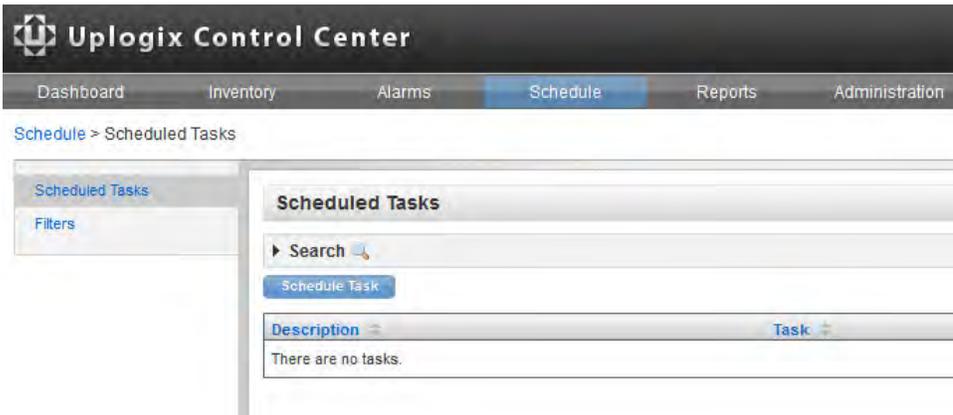
Setting up filters and scheduling tasks

Schedule

Use the Schedule tab to schedule tasks that will be performed across several devices or Uplogix Local Managers. Steps in this process are:

- Specify what equipment is affected by choosing or creating a filter
- Specify the type of task
- Provide the information required to complete the task
- Specify when the task is to be performed and, if applicable, how often it repeats

When the Schedule tab is clicked, the list of scheduled tasks opens. If no filters have been set up, then no tasks are listed and the schedule task button is not available.

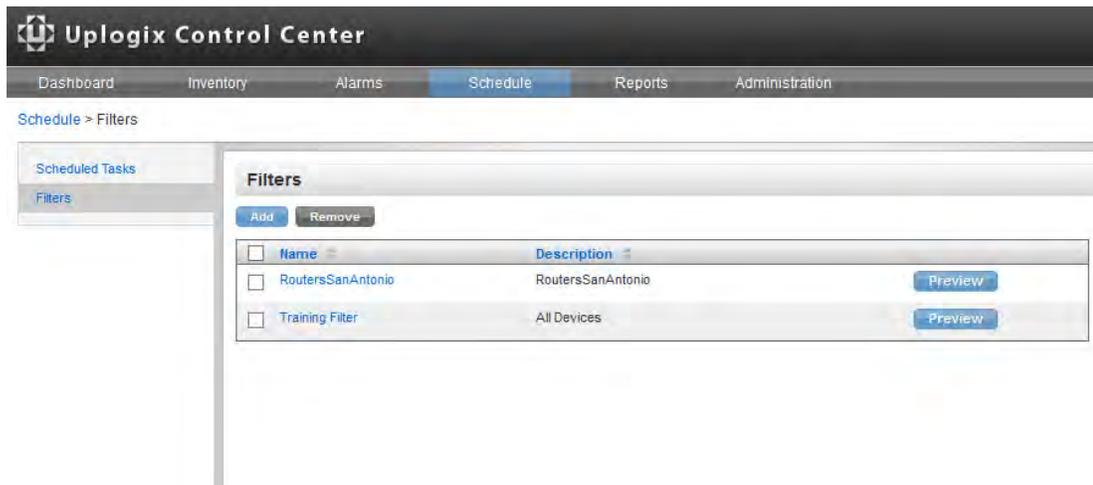


A filter must be created before a task can be scheduled.

Creating a filter

Schedule > Filters

To create a new filter, select **Filters** from the contextual left navigation on the Schedule tab.



To create a filter and filter criteria:

1. Enter a name and a description for the filter. The name of the filter cannot be changed once it is created, though the filter can be deleted and recreated under a new name.



Use only printing characters when completing text fields. Spaces are considered printing characters.

A screenshot of the Uplogix Control Center interface showing the 'Create Filter' form. The breadcrumb trail is 'Schedule > Filters > Create Filter'. The form has a 'Filter Information' section with two text input fields: 'Name' containing 'allSwitchesAustin' and 'Description' containing ':Austin inventory group'. There are 'Save' and 'Cancel' buttons at the top right of the form.

2. Click **Save**. If options have been defined, they display under each inventory group along with a hyperlink to remove them.

A screenshot of the Uplogix Control Center interface showing the 'Edit Filter' form for the filter named 'allSwitchesAustin'. The breadcrumb trail is 'Schedule > Filters > Edit Filter'. The form has a 'Filter Information' section showing the name and description. Below this are three sections: 'Inventory Groups', 'Appliances', and 'Devices'. Each section has a 'Remove' button, a checkbox, and a text field. The 'Inventory Groups' section shows a dropdown menu with 'Austin' selected and an 'Add' button. The 'Appliances' and 'Devices' sections also have 'select' and 'Add' buttons. At the bottom, there is a 'Device Criteria' section with a text field and an 'Add' button.

3. Add filter criteria as needed by choosing a criterion and then clicking **Add** to register your choice. Multiple criteria can be applied in each section.

Initially, each section of the filter editor displays a message indicating that nothing has been added to this section of the filter. Use the Label section to use the port labels that have been created, if any. For more information about creating port labels, see [Creating your own categories to manage devices](#).

Device makes, operating systems, group names, and labels are presented in drop-down lists. Uplogix Local Managers and devices are presented in the Hostname Picker dialog boxes.

4. Click **Preview** to see which Local Managers and devices are affected by the filter. When satisfied with the filter, click **Done** to save your changes. The Filter Manager page now lists the filter which can be previewed, edited, or deleted.



Scheduling a task

Schedule > Scheduled Tasks

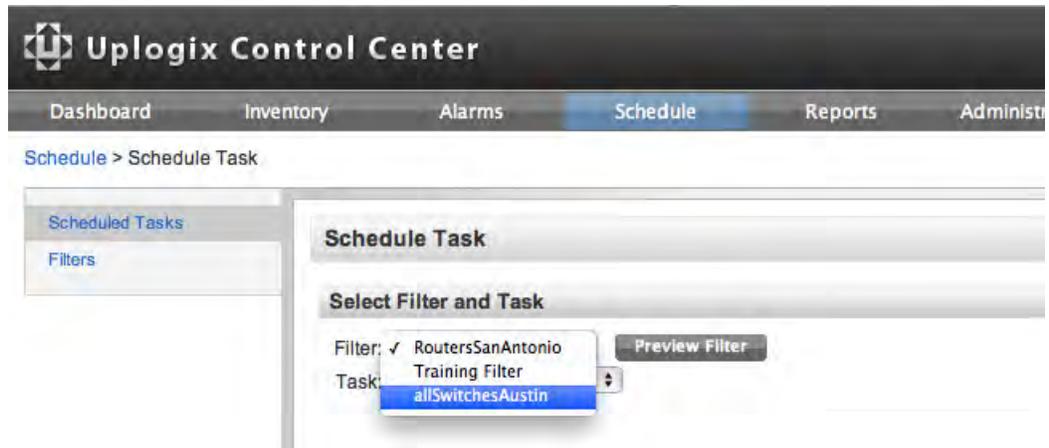
Once task filters have been defined, tasks can be scheduled from the Scheduled Tasks page.



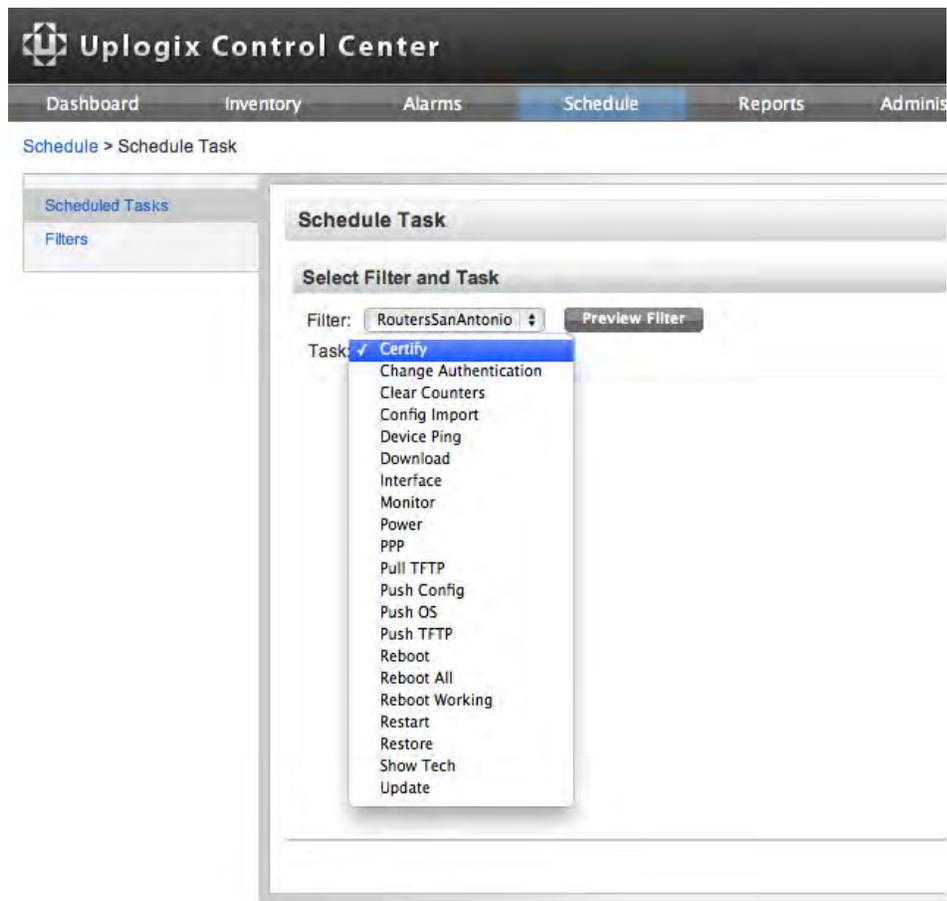
By default, the only tasks shown on the Scheduled Tasks List are tasks that have not yet been completed. To see all tasks, select **Show completed tasks**.



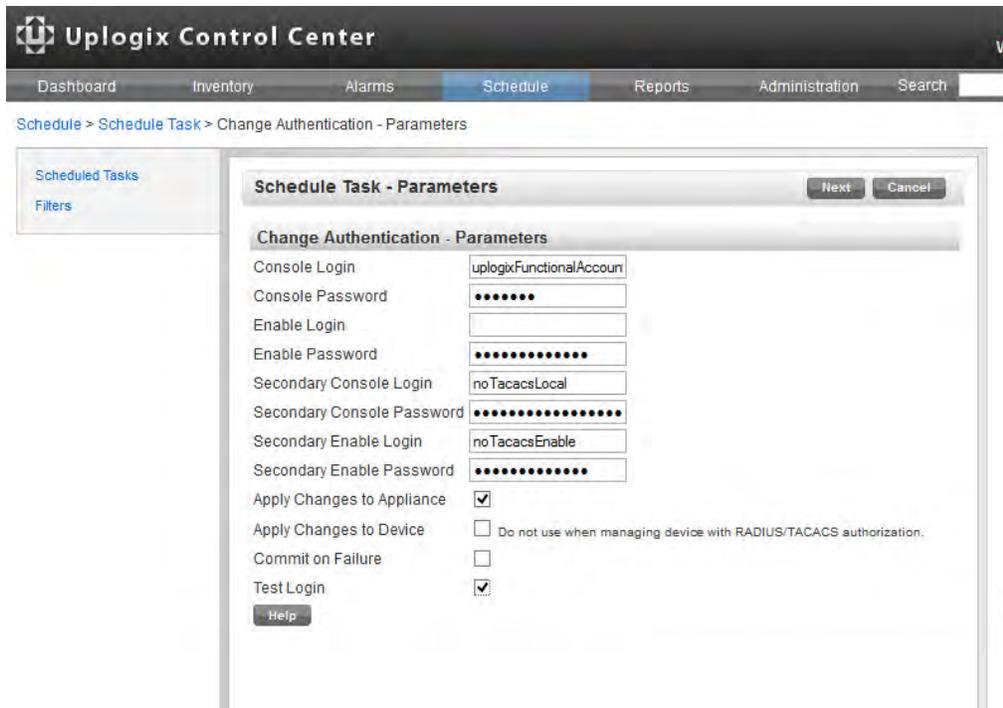
1. Select **Scheduled Tasks** from the contextual left navigation on the Schedule tab.
2. Available task filters are shown in the Filter list. Choose the appropriate filter from the list. If the filter is not listed, click **Cancel** and create a new filter (see the previous section).



3. There are several types of tasks that can be scheduled. The tasks available depend on the device platform. For example, the Clear Counters action is not available for servers.



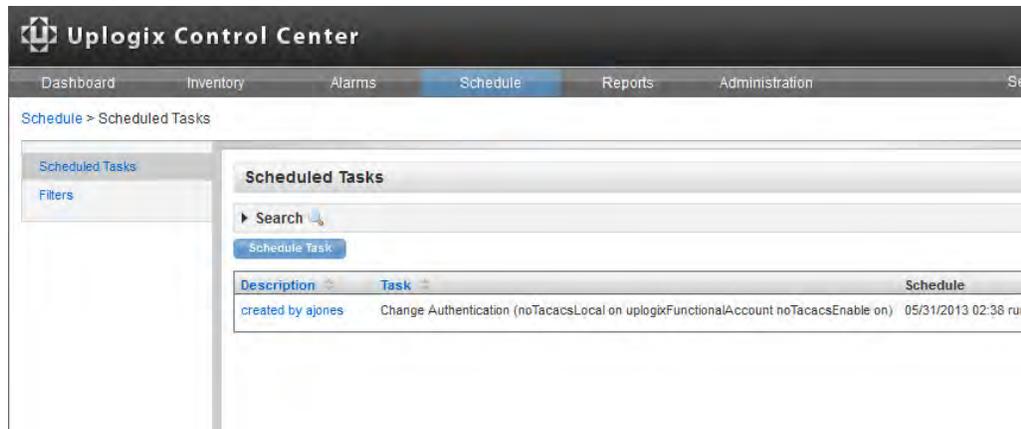
Some tasks, such as Change Authentication, take more than one step to schedule. Others, such as Clear Counters, present only a scheduling page.



- The default starting date and time is the current date and time. Change the date and time if the task is not to be executed immediately.
- Complete the required information on each page, and click **Schedule**.



- The Scheduled Tasks list shows the new task.



- Click **details** to view the equipment affected by the task.
- Click **hold** to postpone the task.
- Click **resume** when ready to allow the task to proceed.
- Click **cancel** if the task should not be executed.

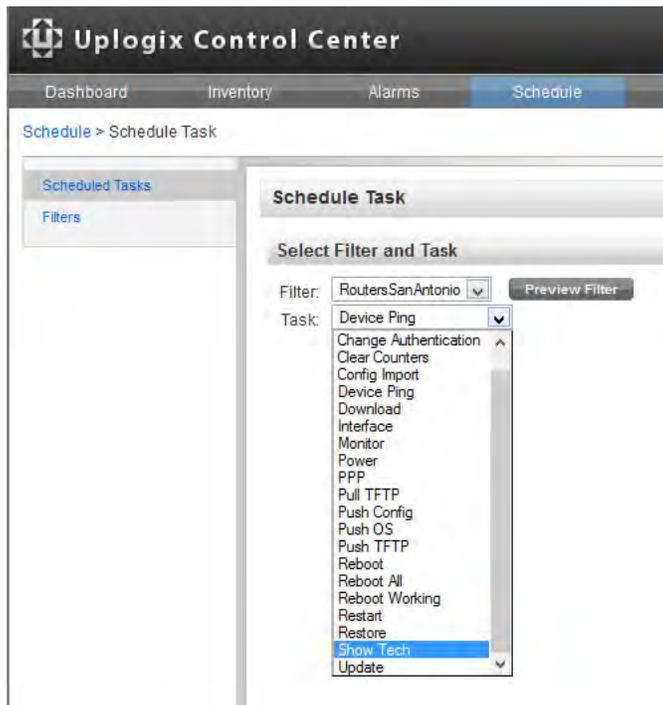


By default, tasks are hidden after they are completed or canceled. To see tasks that are no longer pending, select **Show completed tasks** at the top of the page.

Tasks that can be scheduled

Schedule > Schedule Tasks

The list of tasks available depends on the filter. If the filter specifies managed devices by make, some tasks are unavailable.



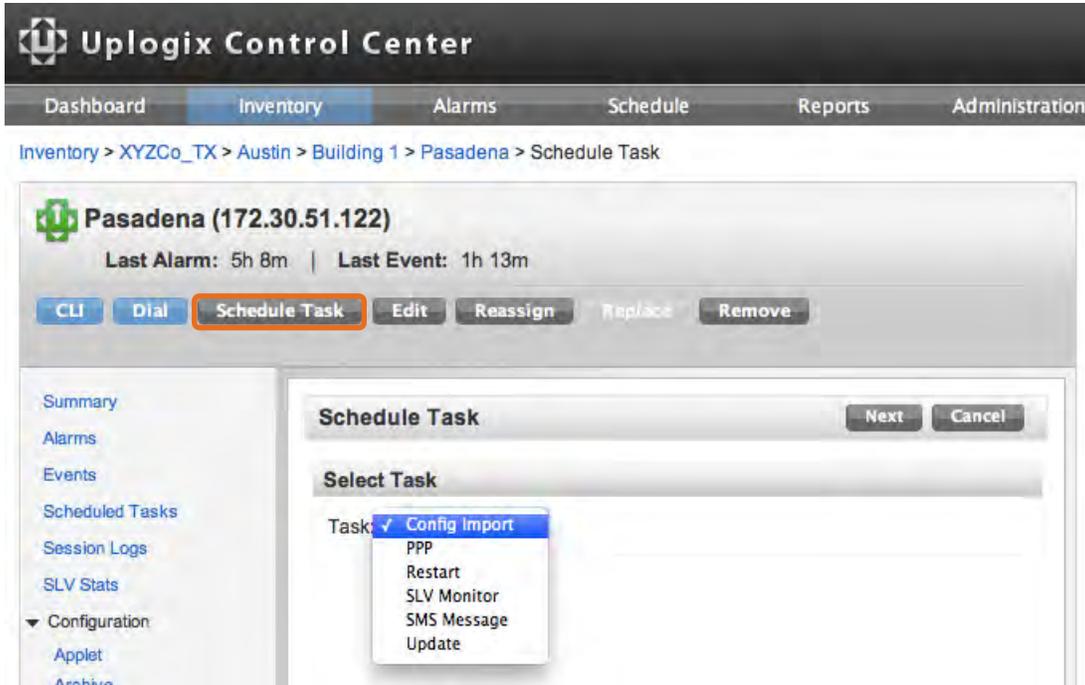
Task	Purpose
Certify	This is an Alcatel specific task that validates a configuration before deploying it.
Change Authentication	Schedule an authentication change for a device, with the option to change the console login and password, the enable login and password, and on some devices failover credentials used when centralized authentication systems are unavailable.
Clear Counters	Clear interface counters on a device. All interfaces counters are cleared.
Config Import	Import Local Manager configuration settings. The file to be imported must exist in the File Archive prior to scheduling. For more information, see Uploading files from your computer to the file archive .
Device Ping	Schedule a ping task from a device attached to the Uplogix Local Manager to a target destination.
Download	This task is a step in the process of applying a file to an Uplogix Local Manager or a managed device. To make the file available to the Local Manager, it must be downloaded from the Uplogix Control Center to the Local Manager. Before downloading files to Local Managers, they may need to be uploaded to the Uplogix Control Center. See Uploading files from your computer to the File Archive . To download a file from the Uplogix Control Center to Local Managers, choose the type of file and file status based on where the file should be saved. Then select a file to download from the File Archive.
Interface	Interfaces can be set on, off, or cycled at a specified time. Choose the desired action and enter the name of the interface.
Monitor	Schedule interface, ping, chassis, console, or log monitors to run, defaults to 30 seconds.

Task	Purpose
Power	Devices can be powered on, off, or power cycled at a specified time. Choose the desired action and if applicable, enter the delay between powering off and on.
PPP	Schedule the Local Manager to initiate Outband (out –of-band) communication.
Pull TFTP	Pull various files from device to Local Manager port file system.
Push Config	Push a new configuration onto a device by specifying the type of file and version. These options refer to files located on the Uplogix Local Manager, in the port's file archive. Also, specify whether the device should be rebooted after the new configuration is loaded.
Push OS	As with configurations, operating system images can be pushed onto a device.
Push TFTP	Push various files to device from Local Manager port file system.
Reboot	Schedule a device to reboot at a specified time.
Reboot All	This is an Alcatel specific task.
Reboot Working	This is an Alcatel specific task.
Restart	Restart the Uplogix Local Manager.
Restore	This is an Alcatel specific task.
Show Tech	Execute low-level debug collection command on the device and automatically save the output to the Uplogix Local Manager.
Update	Update the Uplogix Local Manager software. The new software image must exist in the File Archive prior to scheduling.

Scheduling tasks on a single Local Manager

Inventory > Local Manager Page

Schedule the following tasks for a specific Uplogix Local Manager from the Local Manager's detail page.



Task	Purpose
Config Import	Import a configuration file. The appropriate file must be present in the File Archive. See Uploading files from your computer to the File Archive .
PPP	Schedule an Outband on cycle or off action.
Restart	Restart the Local Manager.
SLV Monitor	Setup SLV monitors. This task is available only if your license includes Service Level Verification. In addition, the appropriate SLV tests and rules must be available. For detailed information about creating rules, refer to the <i>Guide to Rules and Monitors</i> .

Task	Purpose
SMS Message	Send an SMS message to an Uplogix Local Manager containing a command to execute. Only ppp on (Outband) is supported.
Update	Schedule a software update for the Uplogix Local Manager. The appropriate file must be present in the File Archive; otherwise the update cannot be scheduled.

Scheduling software upgrades on Uplogix Local Managers

Automate the process of upgrading Uplogix Local Managers.

The steps in the upgrade process are:

- Download the software upgrade to your computer
- Upload the software to the Uplogix Control Center
- Schedule the Update task

Downloading the software upgrade to your computer

To upgrade the Uplogix Local Managers that the Uplogix Control Center manages, download the software upgrade to your computer and then upload it to the Uplogix Control Center following these steps:

1. Point your browser to support.uplogix.com
2. Navigate to the software download page, locate the appropriate file and download it to your computer.

If you are not certain which file to use, contact Support at support@uplogix.com.

Uploading files from your computer to the File Archive

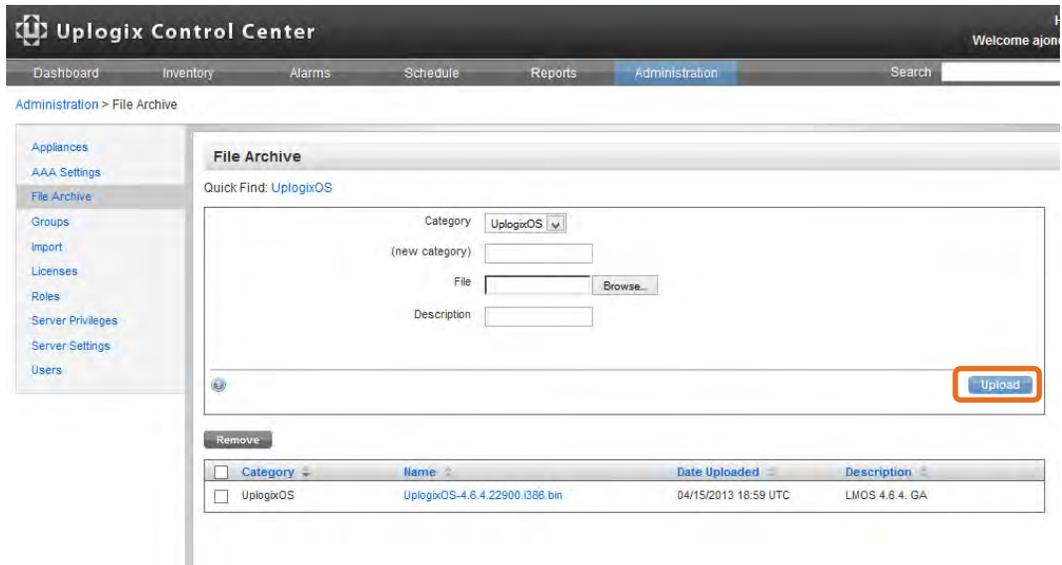
After downloading the desired file to your computer, follow these steps to upload the files to the File Archive:

1. Go to the Uplogix Control Center's **Administration > File Archive** page.
Any files present are displayed with category, filename, upload date, and description information.
2. Choose a category for the file being uploaded. If the selected category does not exist, it is automatically created.



Do not use spaces in the category name.

3. Browse to and select the file that is to be uploaded. If a file with the same name as a file currently in the selected category is uploaded, this new upload overwrites the existing file.
4. Optionally, enter a file description which can be helpful in identifying the file.



5. Click **upload** to copy the file to the Uplogix Control Center. When the upload is complete, the File Archives list displays the file.



Caution: When upgrading to a new release (for example, from 4.5 to 4.6), always upgrade the Uplogix Control Center first. Uplogix Local Managers cannot heartbeat properly to an Uplogix Control Center using an earlier release of software. This is not necessary for patch releases (for example, 4.6 to 4.6.x).

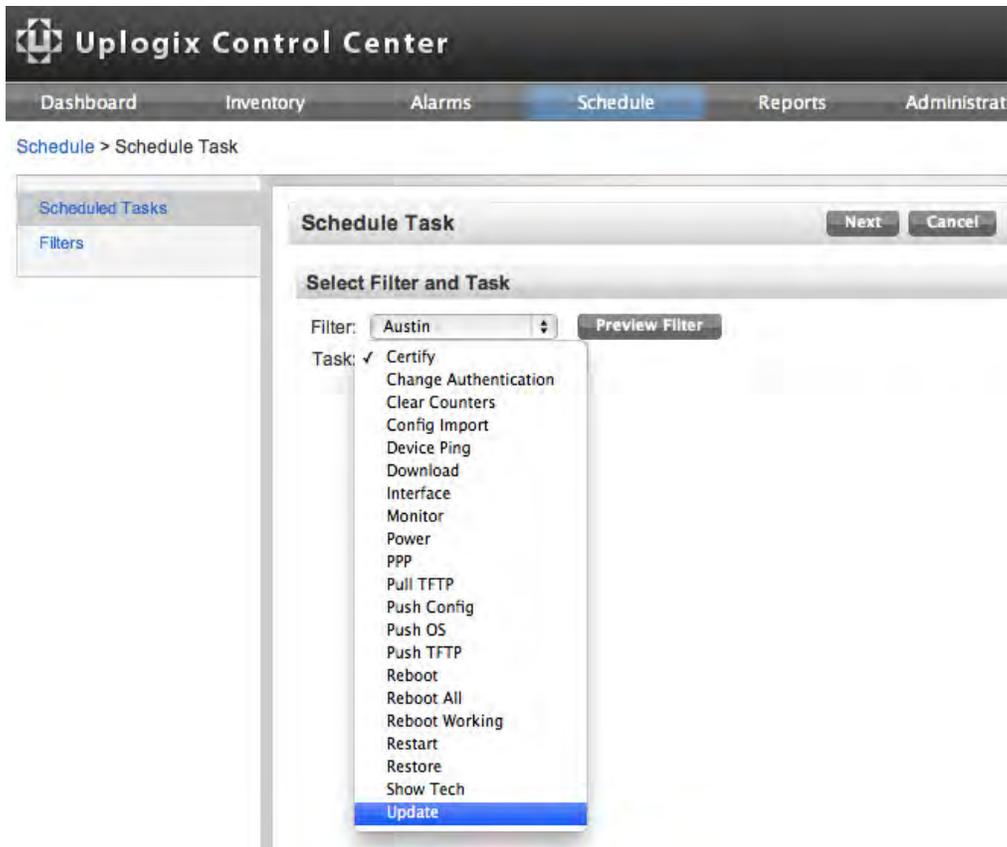
Scheduling the update task for more than one Local Manager

To schedule the update, there must be a task filter that specifies the Uplogix Local Managers to be upgraded. For information about creating filters, see [Setting up filters and scheduling tasks](#).

1. On the Schedule tab, click **Schedule Task** to open the Schedule Task page.
2. Choose the filter that specifies the Local Managers to be upgraded and then select the **Update** task.



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



3. Continue as for scheduling any task.

Scheduling the update task on a single Local Manager

In some cases, you may wish to upgrade only one Uplogix Local Manager.

1. Open the **Inventory** tab and navigate to the Local Manager.
2. Ensure that the Local Manager has been moved out of the Unassigned group.
3. Click **Schedule Task** and then select **Update** as the task type.
4. Click **Next** to open the Schedule Task Parameters page.
5. Select the file just uploaded and click **Next**.
6. Continue as for scheduling any task.

Managing rules and monitors

Monitors gather data, in some cases by running user-defined tests; and they may include rules to evaluate and respond to the data.

A rule specifies at least one condition to evaluate, and at least one action to take if the set of conditions evaluates true. Rules may also include a time element.

Rules can be grouped together into rule sets. This simplifies the process of creating monitors.

This section covers:

- [Working with rules](#)
- [Working with rule sets](#)
- [Scheduling monitors](#)

For a detailed discussion of rules and monitors, refer to the **Guide to Rules and Monitors**.

Working with rules

Inventory > Configuration > Rules

Rules can be centrally managed from the Uplogix Control Center. Like privileges and preferences, rules edited at the inventory group level are inherited by child groups and Uplogix Local Managers. Rules edited at the Local Manager level only apply to that Local Manager.

To access Rules, click **Rules** from the Configuration menu at a group detail or Local Manager detail page. New rules can be created and existing rules can be edited.

The screenshot shows the Uplogix Control Center interface. At the top, there's a navigation bar with tabs for Dashboard, Inventory, Alarms, Schedule, Reports, Administration, and Search. Below this, a breadcrumb trail reads 'Inventory > XYZCo_TX > Austin > Building 1 > Pasadena > View Rules'. The main content area is titled 'Pasadena (172.30.51.122)' and shows 'Last Alarm: 9h 7m' and 'Last Event: 2h 13m'. Below this are several action buttons: CLI, Dial, Schedule Task, Edit, Reassign, Replace, and Remove. On the left, there's a sidebar menu with categories like Summary, Alarms, Events, Scheduled Tasks, Session Logs, SLV Stats, and Configuration. Under Configuration, various settings are listed, including Applet, Archive, Authentication, Banners, Default Port Settings, DNS, Email, Export, IP, IPv6, IPT, LCD, and Modem. The main area displays a 'Rules' section with an 'Add' and 'Remove' button. Below this is a table with columns for 'Rule', 'Description', and 'Scope'. The table lists ten rules, each with a checkbox and a right-pointing arrow. The rules are: adminStatusDown (description: the interface has been turned off, scope: local), adminStatusIsDown (description: the interface has been turned off for a while, scope: local), adminStatusUP (description: the interface has been turned on, scope: local), aisAlarmIncrements (description: , scope: local), carrier (description: Serial Carrier Problems, scope: local), clearToSendIsDown (description: , scope: local), consoleHung (description: System cannot talk to the device, scope: local), cpuFiveMinuteAverageGreaterThan90 (description: CPU Five Minute Average Load Greater Than 90%, scope: local), cpuOneMinuteAverageGreaterThan90 (description: CPU One Minute Average Load Greater Than 90%, scope: local), and currentErroredSecondsIncrements (description: , scope: local). Below the table, it says '45 items found, displaying 1 to 10.' and provides navigation links: [First/Prev] 1, 2, 3, 4, 5 [Next/Last].

Click **Add** to create a new rule. This is equivalent to issuing the `config rule` command from the LMS command line.



Do not use spaces in the rule name.

The Edit Rule page contains drop-down menus and lists of the same options available from the rules editor within the LMS command line.

The screenshot displays the Uplogix Control Center interface for editing a rule on a device named 'Pasadena (172.30.51.122)'. The top navigation bar includes 'Dashboard', 'Inventory', 'Alarms', 'Schedule', 'Reports', 'Administration', and 'Search'. The breadcrumb trail is 'Inventory > XYZCo_TX > Austin > Building 1 > Pasadena > Edit Rule'. The main content area is titled 'Pasadena (172.30.51.122)' and shows 'Last Alarm: 9h 8m' and 'Last Event: 2h 13m'. A toolbar contains buttons for 'CLI', 'Dial', 'Schedule Task', 'Edit', 'Reassign', 'Replace', and 'Remove'. On the left, a configuration menu lists various settings like 'Applet', 'Archive', 'Authentication', etc., with 'Rules' highlighted. The main area is divided into 'Create Rule' (with a 'Save' button) and 'Rule Information' (with fields for Name, Description, Start, and End). Below is the 'Rule Conditions' section, which features a table with 'NOT' and 'Conditional Statement' columns. It includes several rows of condition builders with dropdown menus and buttons for adding different types of conditions: 'Add Compare-value Condition', 'Add Has-value Condition', 'Add Has-run Condition', and 'Add Static Condition'. A 'Conditions' text box is located at the bottom of this section.

Edit conditions manually in the Conditions text box or add a new condition using the drop-down menus shown below. Four different menu sets cover the condition types for rules. As each condition is added, the text changes to reflect the new conditions.

Alarms and events are defined using drop-down items and free text fields.

Tasks can be manually edited or specified with the selections on this page.

The screenshot shows a web-based configuration interface for creating a rule. It is divided into several sections:

- Alarm Section:** Contains a checkbox labeled "oid" (unchecked), a text input field, a checkbox labeled "no email" (checked), and an "Add Alarm" button.
- Event Section:** Contains a dropdown menu for "event type" set to "AIS_ALARM", a checkbox labeled "append message" (unchecked), a text input field, and an "Add Event" button.
- Tasks Section:** A large empty text area for defining tasks, with an "Add Action" button at the bottom right.
- Global Options:** At the bottom, there is a "Scope: local" label, a checkbox for "Force update on children" (unchecked), and a "Save" button.

Click **Save** at the bottom of the page to create the rule. Select **Force update on children** to force Uplogix Local Managers to update a previously inherited rule.

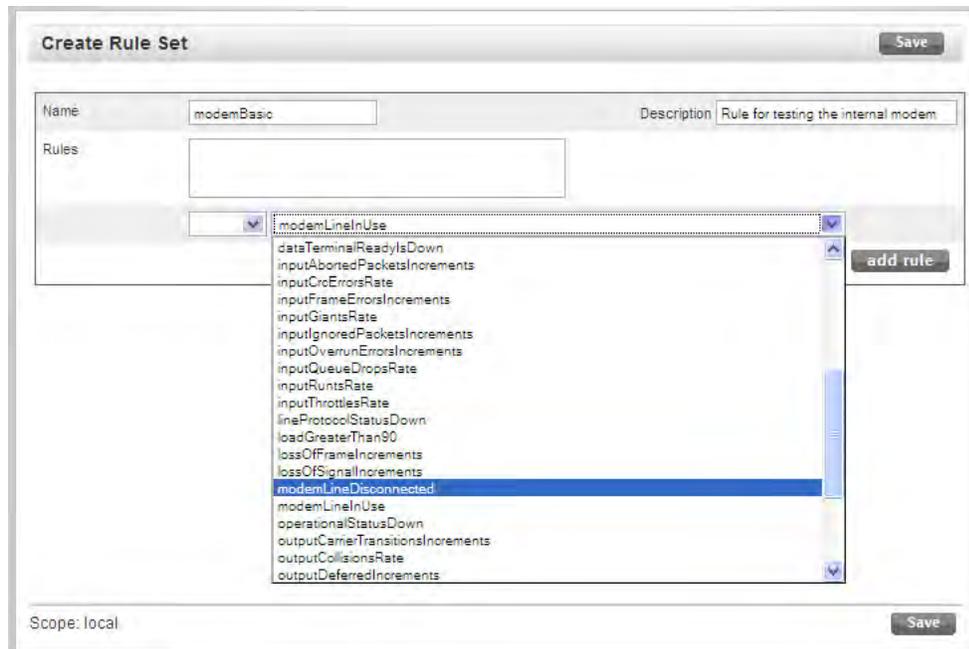
Consult the *Guide to Rules and Monitors* for more information on creating rules.

Reference information is available at support.uplogix.com and includes rule examples, default rules, and condition variables.

Working with rule sets

Some rules are often used together. Therefore, it may be convenient to group them into rule sets. When creating monitors, available rules and rule sets are presented together.

1. Click **Rule Sets** from the Configuration menu on a group detail or Local Manager detail page.
2. Existing rule sets are listed on the View Rule Sets page. To create a rule set, click **Add**.
3. In the Create Rule Set screen, provide a name and (optionally) a brief description for the rule set.



The screenshot shows the 'Create Rule Set' dialog box. The 'Name' field is 'modemBasic' and the 'Description' is 'Rule for testing the internal modem'. The 'Rules' field is empty. A list of available rules is shown, with 'modemLineInUse' selected. An 'add rule' button is visible to the right of the list. The 'Scope' is set to 'local'.

4. Select the first rule from the list of available rules, and click **add rule**.
5. Select the relationship (AND; OR) of the first rule to the second rule from the list to the left, then select the second rule.



The screenshot shows the 'Create Rule Set' dialog box. The 'Name' field is 'modemBasic' and the 'Description' is 'Rule for testing the internal modem'. The 'Rules' field contains 'modemLineInUse'. A dropdown menu is open, showing the relationship '(or)'. The second rule 'adminStatusDown (the interface has been turned off)' is selected. An 'add rule' button is visible to the right.

6. Continue until all the desired rules have been added to the rule set. Click **Save** to save the rule set. The new rule set is listed on the View Rule Sets page.

Rule Sets			
<input type="button" value="Add"/> <input type="button" value="Remove"/>			
<input type="checkbox"/> Rule Set	Description	Rules	Scope
<input type="checkbox"/> adminStatus	determines the state of the interface	adminStatusDown adminStatusUP, adminStatusisDown	local
<input type="checkbox"/> default	Rules designed to troubleshoot Serial Interfaces	carrier physical	local
<input type="checkbox"/> interfaceBasic	Individual alarms for interfaces	lossOfSignalIncrements lossOfFrameIncrements aisAlarmIncrements remoteAlarmIncrements currentLineCodeViolationsIncrements currentPathCodeViolationsIncrements currentFrameLossSecondsIncrements currentLineErrorSecondsIncrements currentErroredSecondsIncrements operationalStatusDown lineProtocolStatusDown loadGreaterThan90 reliabilityLessThan90 dataCarrierDetectIsDown dataSetReadyIsDown dataTerminalReadyIsDown requestToSendIsDown clearToSendIsDown outputQueueDropsRate inputQueueDropsRate inputRuntsRate inputGiantsRate inputThrottlesRate inputCrcErrorsRate inputFrameErrorsIncrements inputOverrunErrorsIncrements outputLateCollisionsIncrements inputIgnoredPacketsIncrements inputAbortedPacketsIncrements outputCollisionsRate outputInterfaceResetsIncrements outputDeferredIncrements outputNoCarrierIncrements outputCarrierTransitionsIncrements	local
<input type="checkbox"/> modemBasic	Rule for testing the internal modem	modemLineInUse modemLineInUse	local
<input type="checkbox"/> recoverConsole	recovering the device when it has become unusable	consoleHung, cpuFiveMinuteAverageGreaterThan90, cpuOneMinuteAverageGreaterThan90	local

5 items found, displaying all items.

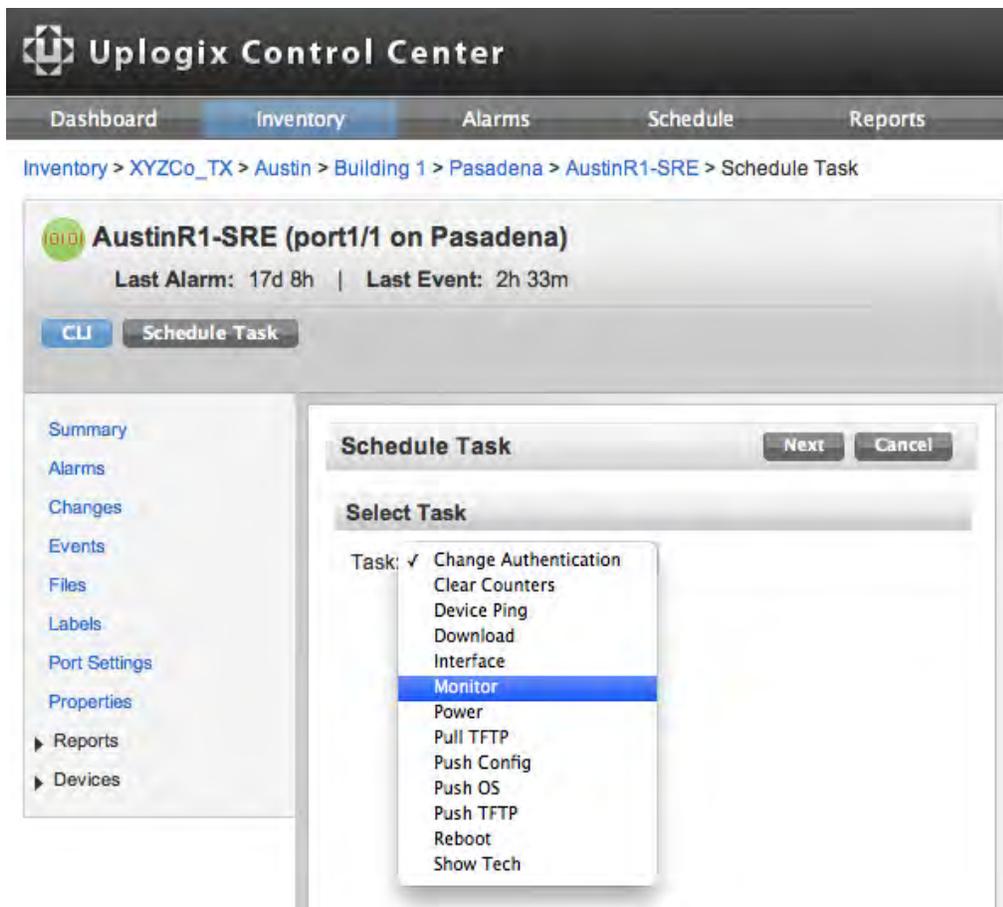
Scheduling monitors

Inventory > Local Manager > Port > Schedule Task

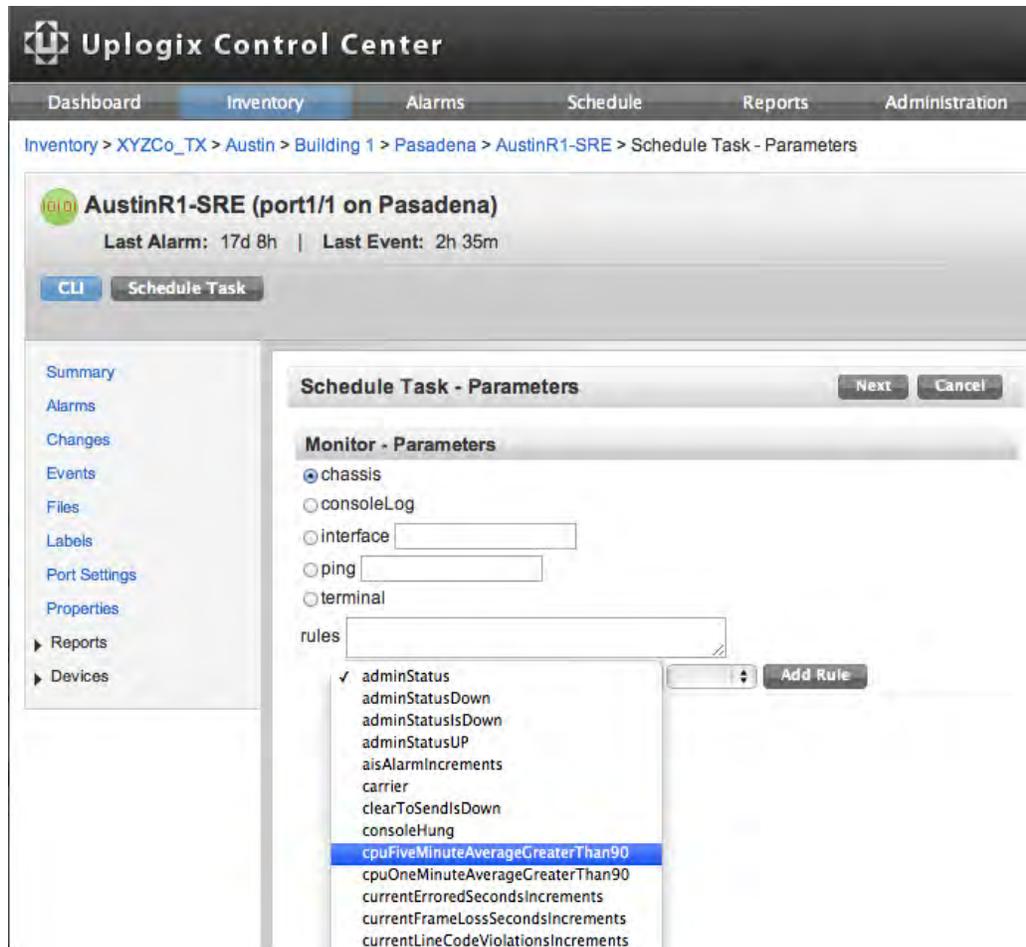
A monitor is a type of scheduled task. Monitors gather data and may apply rules to interpret and respond to the data. Monitors are created from the port pages on individual Local Managers.

To create a monitor:

1. Go to **Inventory > Local Manager > Port >** and click **Schedule Task** to open the Schedule Task page.
2. Select or create a filter to specify what equipment is monitored.
3. Select **Monitor** from the list of tasks and click **Next**.



4. On the Monitor - Parameters page, choose the type of monitor. If it is an interface monitor, specify the interface to be monitored - for example, Serial0.
5. The monitor can be set up without adding rules. The Local Manager gathers and stores the data without acting on it. To do this, click **Next** to go to the scheduling page.
6. To create a monitor that uses rules to interpret and respond to the data as it is gathered, select a rule from the list of available rules and click **Add Rule**.
7. To add another rule, select the rule and its relation to the rule already added. Then click **Add Rule**.



8. On the Monitor - Frequency page, specify the schedule for this monitor and optionally provide a brief description.
9. Click **Save**. The monitor runs as scheduled and appears on the Scheduled Tasks page.



The default interval for monitors is 30 seconds. However, this interval can be changed.

Canceling monitors

To cancel a monitor:

1. Go to the Scheduled tasks page.
2. Locate the monitor to be canceled and click the **cancel** link. The canceled monitor continued to be shown but is struck out on the Scheduled tasks list.

Applet Manual Out-of-Band modem connectivity via dial button

Inventory > Local Manager Page > Configuration > Modem

This functionality executes a Java applet on the user's workstation to connect asynchronously to a local managers modem.

If a circuit-switched TTY connection is available, a Pooled Modem server can be configured to dial from the UCC Java applet into the Local Manager to establish a TTY (teletype) session.

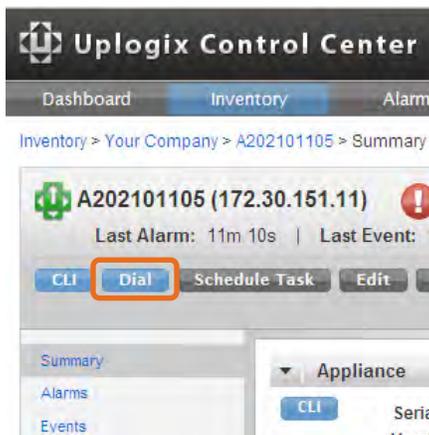
Requirements for using this capability are:

- The Local Manager uses a circuit switched modem such as V.92 or Iridium.
- The Local Manager has been configured to answer the call when dialed and from a specific source phone number, the calling number has been specifically granted. These settings are configured with the config answer command.

In the example below, Cisco router is configured to provide a pool of modems for the CLI Applet to connect to the Local Manager. From the Local Manager configuration menu, select **Modem** and enter the RAS information.

- Host: IP address or DNS Name of the host gateway. In the example below, the Iridium AS5350 gateway has been entered.
- Port Range: Port range assigned by host for remote access.
- Phone Number: Enter the command for dialing (ATDI/ATDT/ATD) and the phone number with no spaces.
- Init String: Enter an optional initialization string with no spaces.
- Local Port: Local port on the workstation to be used with Forward on Connect.
- Forward on Connect: Check this box to forward the terminal session upon connection.

Once the RAS information has been configured, a Dial button appears in the Control Center. Select the Dial button to connect to the Local Manager via out-of-band, circuit switched phone number.



The Control Center CLI applet connects to the modem server with the information pre-programmed RAS section of the Local Manager Modem configuration.

Managing accounts and security

The Uplogix Control Center manages accounts, privileges, and authentication in much the same way that the Uplogix Local Manager does. User and group accounts created on the server are inherited by managed Uplogix Local Managers. Managing users and account security from the Uplogix Control Center ensures consistency over your entire deployment.



Accounts created on the Uplogix Local Manager are deleted when it contacts the Uplogix Control Center.

In this chapter:

- [Working with user and group accounts](#)—create, edit, disable, and delete accounts
- [Managing privileges](#)—control what each user can do on the Uplogix Control Center and the Local Managers it manages
- [Importing user, group, and privilege files](#)—automate account and privilege setup
- [Managing authentication](#)—specify how users authenticate; set password requirements

Managing authentication

Administration > AAA Settings

Inventory > Local Manager Detail > Configuration > Authentication

The Uplogix Control Center and Uplogix Local Managers can handle authentication, authorization, and accounting (AAA) functions locally. However, these functions can be deferred to one or more third-party AAA servers.

This section covers the following topics:

- [Setting authentication requirements globally or within the inventory](#)
- [Authentication, authorization, and accounting \(AAA\) settings](#)
- [Setting requirements for strong passwords](#)

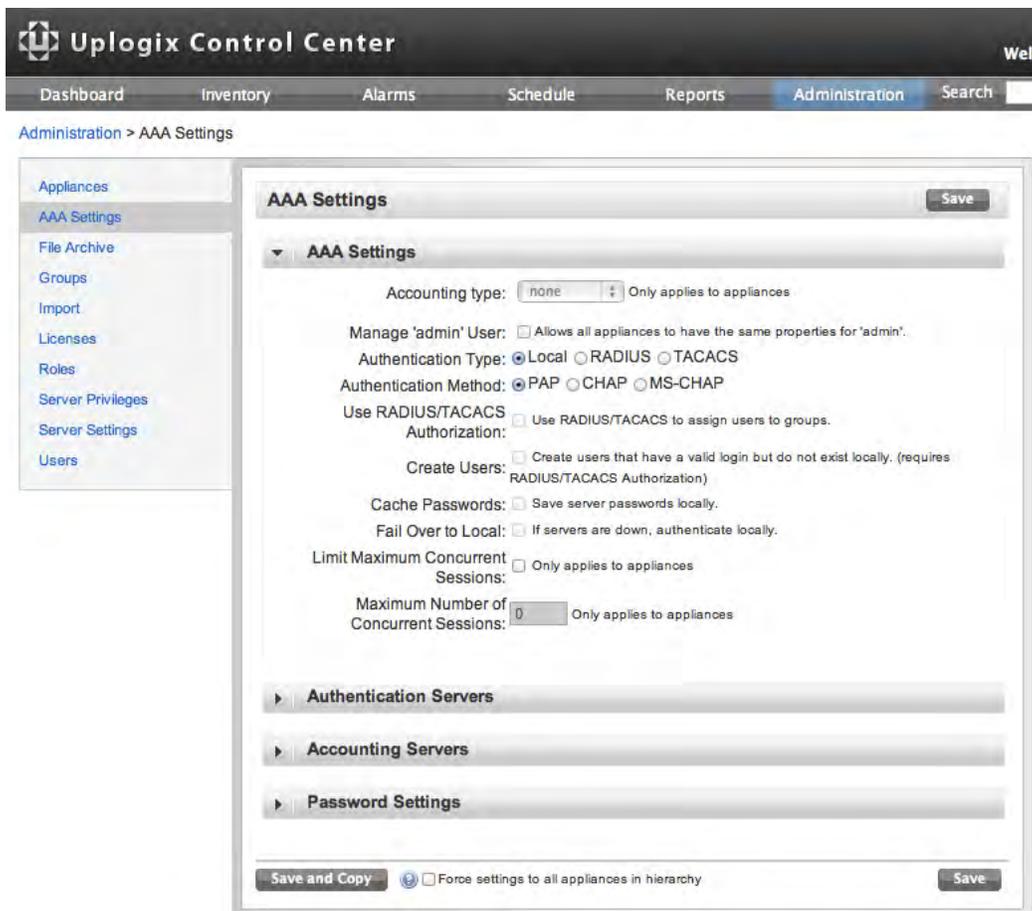
Setting authentication globally or within the inventory

Authentication/authorization/accounting settings can be managed globally from the AAA Settings page under the Administration tab. They can also be customized for specific portions of the deployment from the appropriate group within the inventory.

Setting authentication globally or on the Uplogix Control Center only

To configure AAA settings for the Uplogix Control Center, and optionally for the entire inventory, go to **AAA Settings** under the Administration tab.

This page also includes strong password settings and other password-related settings such as lockout after login failure.



The screenshot shows the Uplogix Control Center interface. The top navigation bar includes Dashboard, Inventory, Alarms, Schedule, Reports, Administration (selected), and Search. Below the navigation bar, the breadcrumb path is Administration > AAA Settings. On the left, a sidebar menu lists various settings: Appliances, AAA Settings (selected), File Archive, Groups, Import, Licenses, Roles, Server Privileges, Server Settings, and Users. The main content area is titled 'AAA Settings' and contains several configuration options:

- Accounting type: Only applies to appliances
- Manage 'admin' User: Allows all appliances to have the same properties for 'admin'.
- Authentication Type: Local RADIUS TACACS
- Authentication Method: PAP CHAP MS-CHAP
- Use RADIUS/TACACS Authorization: Use RADIUS/TACACS to assign users to groups.
- Create Users: Create users that have a valid login but do not exist locally. (requires RADIUS/TACACS Authorization)
- Cache Passwords: Save server passwords locally.
- Fail Over to Local: If servers are down, authenticate locally.
- Limit Maximum Concurrent Sessions: Only applies to appliances
- Maximum Number of Concurrent Sessions: Only applies to appliances

Below these settings are three expandable sections: Authentication Servers, Accounting Servers, and Password Settings. At the bottom, there are two buttons: 'Save and Copy' and 'Save'. A checkbox between them is labeled 'Force settings to all appliances in hierarchy'.

For information on configuring accounting and authentication, see [Authentication, authorization, and accounting \(AAA\) settings](#).

- To apply changes on this page to the Uplogix Control Center only, click **Save**.
- To copy the changes on this page to the root-level inventory group, click **Save and Copy**. Like other inventory settings, the authentication settings do not overwrite existing locally created settings unless you force them to do so. It will overwrite changes made in the top level of the hierarchy, but not those made in child groups.
- To force the changes on this page on all Uplogix Local Managers managed by this Uplogix Control Center, select **Force settings to all appliances in hierarchy** before clicking **Save and Copy**.

Setting authentication within an inventory group

To configure AAA settings for an inventory group, open the detail page for that group and click **Authentication** from the Configuration menu to open the **Authentication Settings** page.

The screenshot shows the Uplogix Control Center interface. The top navigation bar includes Dashboard, Inventory, Alarms, Schedule, Reports, Administration, and Search. The breadcrumb trail is Inventory > XYZCo_TX > Austin > Uplogix Configuration. The main content area is titled "Inventory Group: Austin" and "Engineering Group". Below this are buttons for Edit, Reassign, Remove, and Remove Including Children. A left sidebar menu lists various configuration options, with "Authentication" highlighted in a red box. The main content area displays the "Authentication Settings" page, which includes a "Save" button and a "AAA Settings" section. The AAA Settings section contains the following options:

- Accounting type: none
- Authentication Type: Local RADIUS TACACS
- Authentication Method: PAP CHAP MS-CHAP
- Use RADIUS/TACACS Authorization: Use RADIUS/TACACS to assign users to groups.
- Create Users: Create users that have a valid login but do not exist locally. (requires RADIUS/TACACS Authorization)
- Cache Passwords: Save server passwords locally.
- Fail Over to Local: If servers are down, authenticate locally.
- Limit Maximum Concurrent Sessions:
- Maximum Number of Concurrent Sessions: 0

Below the AAA Settings section are expandable sections for "Authentication Servers" and "Accounting Servers". At the bottom of the page, there is a "Scope: inherited" label and a checkbox for "Force update on children" with a "Save" button.

Settings available on the Uplogix Configuration page are inherited by all the members of this inventory group, except where they would overwrite existing settings. Select **Force update on children** to overwrite all existing settings.

For information on configuring accounting and authentication, see [Authentication, authorization, and accounting \(AAA\) settings](#).

Setting authentication for a single Local Manager

To configure AAA settings for a single Uplogix Local Manager, navigate to the Local Manager and select **Authentication** from the Configuration menu.

Authentication, authorization, and accounting (AAA) settings

Administration > AAA Settings

Inventory > Group Detail > Configuration > Authentication

Inventory > Local Manager > Configuration > Authentication

Authentication/authorization/accounting settings can be managed globally from the AAA Settings page under the Administration tab. They can also be customized for specific portions of the deployment from the appropriate group or Local Manager within the inventory. Navigate to the appropriate page to configure AAA settings.

Accounting settings

Accounting events can be sent to a configured TACACS or RADIUS server using the start-stop (before and after each command) or the stop-only (after each command) model. This setting is not available if local authentication is used. Accounting applies to Uplogix Local Managers only; however, you can set it for all Local Managers by navigating to Administration > AAA Settings.

The screenshot displays the Uplogix Control Center interface. At the top, there is a navigation bar with tabs for Dashboard, Inventory (selected), Alarms, Schedule, Reports, and Administration. Below the navigation bar, the breadcrumb trail reads: Inventory > XYZCo_TX > Austin > Uplogix Configuration. The main content area is titled "Inventory Group: Austin" and "Engineering Group". It features four buttons: Edit, Reassign, Remove, and Remove Including Children. On the left, there is a sidebar menu with options: Summary, Configuration (expanded), Applet, Archive, Authentication (selected), Banners, Default Port Settings, DNS, Email, Export, and LCD. The main content area shows the "Authentication Settings" section, which is expanded to show "AAA Settings". The "Accounting type" dropdown menu is open, showing options: none (selected), start-stop, and stop-only. Below this, the "Authentication Type" is set to RADIUS/TACACS. The "Authentication Method" is set to PAP. There are three checkboxes: "Use RADIUS/TACACS Authorization" (unchecked), "Create Users" (unchecked), and "Cache Passwords" (unchecked).

Managing the Local Managers' admin account

Administration > AAA Settings

For security, the default admin account that is part of every Uplogix Local Manager's factory configuration can be limited or disabled.

To make the admin account editable, select **Manage 'admin' user** from the Administration > AAA page. This adds admin to the list of users on the Administration > Users page, providing a simple way to change the admin password on all Uplogix Local Managers or otherwise modify this account. If this choice is not selected, the admin account is not listed on the Administration > Users page.

Authentication settings

Most authentication settings available through the Uplogix Control Center mirror those available through the `config system authentication` command in the Uplogix LMS command line. They include the ability to select the type of authentication, to specify the necessary configuration information for each type, and to limit the number of concurrent sessions per account.

All authentication settings available at the individual Local Manager level are also available at the inventory group level and globally. Some additional settings are available at the inventory group or global levels.

AAA Settings Save

AAA Settings

Accounting type: Only applies to appliances

Manage 'admin' User: Allows all appliances to have the same properties for 'admin'.

Authentication Type: Local RADIUS TACACS

Authentication Method: PAP CHAP MS-CHAP

Use RADIUS/TACACS Authorization: Use RADIUS/TACACS to assign users to groups.

Create Users: Create users that have a valid login but do not exist locally. (requires RADIUS/TACACS Authorization)

Cache Passwords: Save server passwords locally.

Fail Over to Local: If servers are down, authenticate locally.

Limit Maximum Concurrent Sessions: Only applies to appliances

Maximum Number of Concurrent Sessions: Only applies to appliances

Authentication Servers

Accounting Servers

Password Settings

Save and Copy Force settings to all appliances in hierarchy Save

Authentication Type and Method: Select the type of authentication to use. Local, RADIUS, and TACACS are available. If using TACACS or RADIUS, select the authentication method as well. PAP, CHAP, and MS-CHAP are available.



If the Uplogix Control Center is configured to use one or more authentication servers, or accounting servers, the managed Uplogix Local Managers can use the same servers, if desired. Optionally the Uplogix Control Center will maintain password synchronization with AAA servers and distribute changes to each local manager as they are updated.

Use Radius/TACACS Authorization: Some AAA servers support returning authorization keys that can be used by the Uplogix Control Center to assign privileges to users. For information on configuring this, see [Using Radius/TACACS to manage privileges](#).

Create Users: If users are managed on the authentication server, they are able to authenticate but not have accounts on the Uplogix Control Center or Uplogix Local Manager. If this setting is enabled, the user is created. If Radius/TACACS authorization is not used, users initially have no privileges - so they are not able to log in, as this requires the `login` privilege.

Cache Passwords: Enable this setting if the Uplogix Control Center is configured to use authentication server(s) and Fail Over to Local is selected. This allows users to use a previously saved password if no authentication server is available and the Uplogix Control Center fails over to local authentication.

Fail Over to Local: Enable this setting to allow the Uplogix Control Center to authenticate users locally when no configured authentication server is available. When using this setting, enable Cache Passwords to make the passwords available for local authentication.

Limit Maximum Concurrent Sessions and Maximum Number of Concurrent Sessions: These settings allow you to limit the number of open sessions that any user may have on any particular Uplogix Local Manager at a given time. Set the maximum number to 0 to allow unlimited concurrent sessions.

Authentication and accounting servers

If the Uplogix Control Center or Local Managers are configured within the inventory to use RADIUS or TACACS, at least one of the appropriate type of server must be configured. Up to four authentication servers and up to four accounting servers can be specified for redundancy. All must be of the same type, either RADIUS or TACACS. If an authentication server fails to respond, the next server is queried; the first response determines whether the authentication is successful.

For each server, enter the IP address and port; then enter and confirm the secret. For RADIUS servers, the default port is 1645 or 1812; for TACACS, the default port is 49.

To remove server information already configured, click **Clear** associated with that server.

The screenshot displays the configuration interface for AAA servers. It is divided into two main sections: Authentication Servers and Accounting Servers. Each section contains a list of servers with input fields for IP, Port, Secret, and Confirm Secret, along with a 'Clear' button for each server.

Authentication Servers

Server	IP	Secret	Port	Confirm Secret	Clear
Authentication Server 1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Clear"/>
Authentication Server 2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Clear"/>
Authentication Server 3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Clear"/>
Authentication Server 4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Clear"/>

Accounting Servers

Server	IP	Secret	Port	Confirm Secret	Clear
Accounting Server 1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Clear"/>
Accounting Server 2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Clear"/>

Choosing how to apply AAA changes

When making changes on the Administration > AAA page, apply them in three ways:

- Update AAA settings only on the Uplogix Control Center—click **Save**.
- Update AAA settings on the Uplogix Control Center and at the root level of the inventory without changing settings on Uplogix Local Managers currently in the inventory—click **Save and Copy**.
- Update AAA settings globally, overwriting existing settings on the Uplogix Control Center and all Uplogix Local Managers—select **Force settings to all appliances in hierarchy**, then click **Save and Copy**.

The screenshot shows the bottom of the configuration form. It features a 'Save and Copy' button, a checkbox labeled 'Force settings to all appliances in hierarchy', and a 'Save' button.

When making changes at the inventory group level from the Authentication page, apply them without changing settings on Local Managers currently in the group or overwrite the Local Managers' authentication settings.

- Update AAA settings for the group without changing settings on Uplogix Local Managers currently in the inventory—click **Save**.
- Update AAA settings for the group, overwriting existing settings on all Uplogix Local Managers in the group and its child groups—select **Force updates on children**, then click **Save**.

Scope: inherited Force update on children **Save**

Setting requirements for strong passwords

Configure strong passwords at any level within the inventory, on the Uplogix Control Center only, or globally. The password requirements can be tailored separately for different groups or Local Managers within the deployment. For a detailed description of how to apply settings globally or within a subset of the deployment, see [Setting authentication globally or within the inventory](#).

Global or Uplogix Control Center only: Administration > AAA Settings

Inventory group: Inventory > Group Detail > Configuration > Passwords

Single Local Manager: Inventory > Local Manager > Configuration > Passwords

For password restrictions to take effect, **Use Strong Passwords** must be selected. To remove strong password restrictions temporarily, clear **Use Strong Passwords** while leaving the restrictions configured.

Authentication Servers
 Accounting Servers
 Password Settings

Use strong passwords:
 Require mixed case:
 Require numbers and punctuation:
 Reject variation of login id:
 Reject word in dictionary:
 Reject standard substitutions: (@ for a, 3 for e, etc)
 Reject sequences in numbers or letters: (qwerty)
 Reject previous password:
 Number of previous passwords to check: 6
 Reject single character difference from previous password:
 Enforce minimum password length:
 Minimum password length: 6
 Expire password:
 Number of valid days: 30
 Number of invalid attempts before lockout: 0 Only applies to appliances
 Lockout duration in minutes: 0 Only applies to appliances

Save and Copy Force settings to all appliances in hierarchy **Save**

Restrictions include:

Setting	Description
Require mixed case	Password must have both capital and lowercase characters Valid password example: PassWord
Require numbers and punctuation	Password must include at least one numeral and at least one symbol. Valid password example: P@ssw0rd
Reject variation of Login ID	Password cannot be derived from the login ID Invalid Example: admin1
Reject variation of previous passwords	Obvious variations on the previous password will be rejected. The following examples assume that the previous password was P@ssw0rd <ul style="list-style-type: none"> - 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 Reject standard substitutions (@ for a, 3 for e, etc.)	If both options 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. Partial or broken sequences such as abc!defg or qwerty12 may be used.
Reject previous password 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
Enforce minimum password length Minimum password length	Keeps users from setting passwords short enough to be easily guessed.
Expire password Number of valid days	Forces users to change their passwords periodically.

Setting	Description
Number of invalid attempts before lockout	Specify the maximum number of times a user can attempt to log into a Local Manager before the Local Manager refuses further attempts, and the length of the lockout period. Set the number of attempts to 0 to disable lockout protection. The default lockout time is 30 minutes. These settings apply only to Uplogix Local Managers, not to the Uplogix Control Center.
Lockout duration in minutes	



Do not create a password that ends with a space character. When an attempt is made to log into an Uplogix Local Manager using a password that ends with a space, the Uplogix Local Manager strips the space character and the login fails.

Working with user and group accounts

Administration > Users

Use the Users and Groups pages under the Administration tab to manage accounts. The options on the Create/Edit User and Create/Edit Group pages are the same as those found in the LMS commands `config user` and `config group`.

Uplogix Control Center

Dashboard Inventory Alarms Schedule Reports Administration

Administration > Users

Users

Search

Add Remove

<input type="checkbox"/>	User ID	Email Address	Server Login	Disabled	Description
<input type="checkbox"/>	EThompson	ethompson@xyzco.com	no	yes	
<input type="checkbox"/>	Jason		no	no	
<input type="checkbox"/>	Jose		yes	no	
<input type="checkbox"/>	Paul		no	no	
<input type="checkbox"/>	administrator		yes	no	Server .
<input type="checkbox"/>	ajones		yes	no	
<input type="checkbox"/>	athompson		yes	no	
<input type="checkbox"/>	scott		yes	no	

8 items found, displaying all items.

Accounts that exist locally on an Uplogix Local Manager are deleted when the Local Manager makes contact and synchronizes with the Uplogix Control Center. Accounts cannot be managed locally through the LMS command line if the Local Manager is managed by an Uplogix Control Center.

There is an exception for users whose passwords expire. If you log into an Uplogix Local Manager with an expired password, the command line prompts for a new password. When you set the password, it is pushed up to the Uplogix Control Center.

User account management tasks include:

- [Creating and editing user accounts](#)
- [Creating and editing group accounts](#)
- [Disabling user accounts](#)
- [Deleting accounts](#)

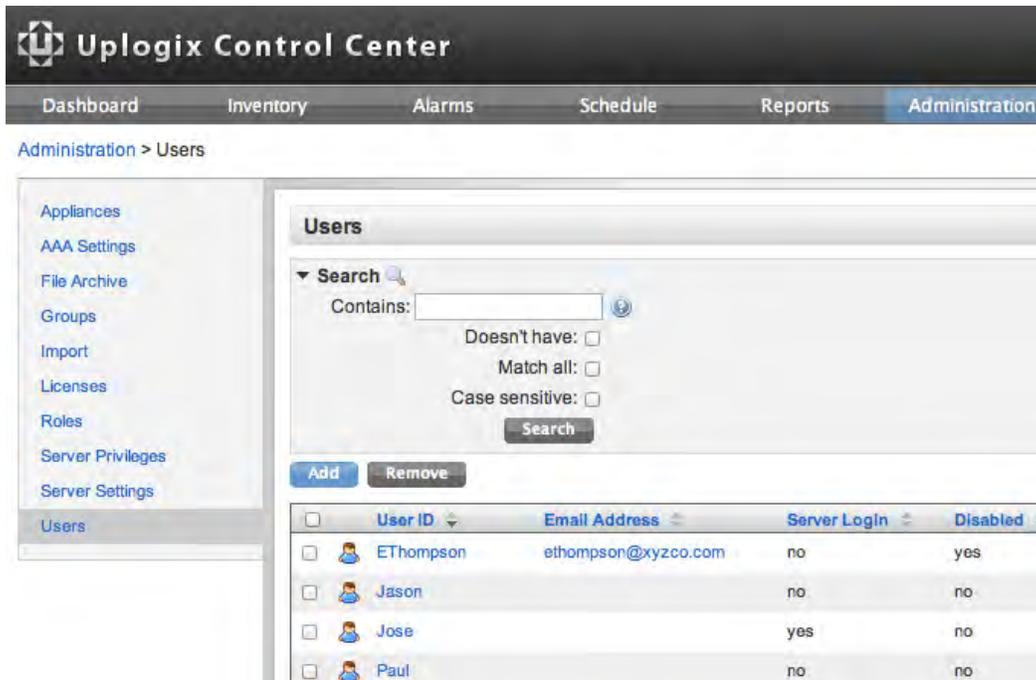
Creating and editing user accounts

Administration > Users

To add a new account, click **Add**.

To edit an existing user account, click the **User ID**. When an existing user is edited, the **Edit User** page displays a timestamp showing when the account was created. The account name cannot be edited.

Search the list of users by entering a text string in the search box, select the type of search, and click **Search**.



The screenshot shows the Uplogix Control Center interface. The top navigation bar includes Dashboard, Inventory, Alarms, Schedule, Reports, and Administration. The current page is Administration > Users. On the left is a sidebar menu with options like Appliances, AAA Settings, File Archive, Groups, Import, Licenses, Roles, Server Privileges, Server Settings, and Users. The main content area is titled 'Users' and features a search section with a search box, a search type dropdown (set to 'Contains'), and checkboxes for 'Doesn't have', 'Match all', and 'Case sensitive'. A 'Search' button is below these options. Underneath are 'Add' and 'Remove' buttons. A table lists the following users:

	User ID	Email Address	Server Login	Disabled
<input type="checkbox"/>	ETHompson	ethompson@xyzco.com	no	yes
<input type="checkbox"/>	Jason		no	no
<input type="checkbox"/>	Jose		yes	no
<input type="checkbox"/>	Paul		no	no

Complete the fields needed to create the account and set it up appropriately for your environment.



Account names must be unique. For example, if there is a group account called sysadmin, a user account called sysadmin cannot be created.



Use only printing characters when completing text fields. Spaces are considered printing characters, but may only be used in the description field.



Do not create a password that ends with a space character. When an attempt to log into an Uplogix Local Manager is made using a password that ends with a space, the Uplogix Local Manager strips the space character and the login fails.



If the Time Zone setting for a user account is changed while that user is logged in to an Uplogix Local Manager, the change does not take effect on that Local Manager until the user ends the session.

Click **Save** when finished setting up the account information.

Initially, user accounts have no privileges so the new user cannot log into the Uplogix Control Center or to the Uplogix Local Managers within the deployment. Privileges must be assigned to the new user account to allow the user to work with elements of your deployment. See [Managing privileges](#).

Some users may need to receive alerts, reports, or audit other accounts. For information about setting up these functions, see [Setting up email, auditing and report subscriptions](#).

Several users can be created at once by importing a user file. See [Importing user, group, and privilege files](#).

Creating and editing group accounts

Administration > Groups

Use the Uplogix Control Center to create and manage group accounts across multiple Uplogix Local Managers to ensure a consistent user group organization and privilege policy.

To create or edit a group account, select **Groups** from the left menu under the Administration tab. Existing groups are displayed in the Group box.



The screenshot shows the Uplogix Control Center interface. At the top, there's a navigation bar with tabs: Dashboard, Inventory, Alarms, Schedule, Reports, and Administration. Below this, a breadcrumb trail reads 'Administration > Groups > Create Group'. On the left, a sidebar menu lists 'Create Group', 'Privileges', 'Auditing', 'Alert Subscriptions', and 'Report Subscriptions'. The main content area is titled 'Create Group' and contains a 'Group Information' section with the following fields: '*Name:' (required), 'Description:', 'Start Date:', and 'Expiration Date:'. Each date field has a calendar icon. There are 'Save' buttons at the top right and bottom right of the form.

To create a new group, click **Add**. Specify a name for the group and optionally provide a description as well as a start and expiration date.

To edit an existing group, click the **Group ID**. This is equivalent to issuing the `config group` command from the Uplogix LMS command line. When an existing group is edited, the **Edit Group** page displays a timestamp showing when the account was created.



Account names must be unique. For example, if there is a user account called `sysadmin`, a group account called `sysadmin` cannot be created.



Use only printing characters when completing text fields. Spaces are considered printing characters, but may only be used in the **description** field.

Once the group is created, add users or other groups as members of this group. Members of the group inherit group-related settings such as privileges.

The screenshot shows the 'Edit Group: InstallTeam' interface. At the top, there's a navigation bar with 'Administration' selected. Below it, a breadcrumb trail reads 'Administration > Groups > InstallTeam'. On the left, a sidebar lists options: 'InstallTeam', 'Privileges', 'Auditing', 'Alert Subscriptions', and 'Report Subscriptions'. The main content area is titled 'Edit Group: InstallTeam' with a 'Save' button. It contains several sections:

- Group Information:** Fields for Name (pre-filled with 'InstallTeam'), Description, Start Date, and Expiration Date. An 'Add To Group' button is below.
- Email Addresses:** A section with a 'Count: 0'.
- Children: Users:** A section with a 'Count: 4'. It has 'Add' and 'Remove' buttons. Below is a list of users: 'User', 'ETompson', 'Jason', 'Paul', and 'ajones', each with a checkbox.
- Children: Groups:** A section with a 'Count: 0'. It has 'Add' and 'Remove' buttons. Below is a 'Group' section with a message: 'There are no child groups in group InstallTeam.'

 A 'Save' button is located at the bottom right of the main content area.

The Available Users and Available Groups list are populated with information from the Uplogix Control Center database. To add a new member to a group, the new user or group must first exist in the database. Click **Add** and select the user or group from the pop-up window as appropriate.

Click **Save** to save the group. Initially, User groups are automatically inherited by Uplogix Local Managers. Initially, group accounts have no privileges so members of the group have only the permissions assigned to their individual accounts. Group privileges must be assigned to the new user account to allow the user to work with elements of your deployment. See [Managing privileges](#).

The group may need to receive alerts, reports, or audit other accounts. For information about setting up these functions, see [Setting up email, auditing and report subscriptions](#).

Several groups can be created at once by importing a group file. See [Importing user, group, and privilege files](#).

Disabling user accounts

Administration > Users

To suspend access to a user account without deleting the account, go to **Administration > Users** and select the User ID for the account to be edited.

On the Edit User screen, select **Disabled** and click **Save**.

The screenshot shows the 'Edit User: ETHompson' interface. The user's status is 'Disabled', indicated by a checked checkbox. Other fields include Name (ETHompson), Password, Confirm, Description, Time Zone (set to (-6:00) US/Central), and Start/Expiration Dates. There are 'Add To Group' and 'Save' buttons.

The user is not able to log in while the account is disabled. The status of Disabled displays in the user list.

The screenshot shows the 'Users' list in the Uplogix Control Center. The user list includes columns for User ID, Email Address, Server Login, Disabled, and Desc. The 'Disabled' status for user ETHompson is highlighted in orange.

User ID	Email Address	Server Login	Disabled	Desc
ETHompson	ethompson@xyzco.com	no	yes	
Jason		no	no	
...

If the user is logged in when their account is disabled, the user is logged out immediately.

Deleting accounts

Administration > Users

Administration > Groups

To delete an account, click the check box associated with the User ID or Group ID and select Remove. This is equivalent to using the LMS commands `config user no [username]` and `config group no [groupname]` on a Local Manager not managed by an Uplogix Control Center.



Caution: There is no delete confirmation.

Managing privileges

Permissions, roles, and privileges are defined as follows:

- **Permission:** Ability to use a specific command or capability; can be allowed or denied in a role definition
- **Role:** A named set of permissions that a user is permitted to execute, such as `admin`
- **Privilege:** A role assigned to a specific account for a specific resource, such as "admin on system" or "guest on port 1/4"



Some permissions, such as `config hierarchy`, are not associated with specific commands but provide override ability and should be used sparingly.

The Uplogix Control Center restricts access to features based on a user's privileges. For example, if a user does not have a role that includes permission to use the `config system ip` command, the IP configuration link is unavailable for that user on the Local Manager detail Page.

All aspects of working with the Uplogix Control Center and the equipment it manages are affected by account privileges. By default, user and group accounts have no privileges.

The administrator account on the Uplogix Control Center has admin access to all features of the server, but no privileges on individual Uplogix Local Managers. So administrator cannot log into an Uplogix Local Manager. Conversely, the admin account on Uplogix Local Managers has no privileges on the Uplogix Control Center. However, the administrator account has the `config hierarchy` permission, which allows the administrator to manage individual Local Managers through the Uplogix Control Center.

In this section:

- [Adding server privileges to accounts](#)
- [Adding inventory privileges to accounts](#)
- [Viewing and deleting user account privileges](#)
- [Creating and customizing roles](#)
- [Using TACAS to manage privileges](#)
- [Creating a superuser](#)
- [Limiting a user's access to one port on one system](#)

Adding server privileges to accounts

Administration > Server Privileges

When a new user or group account is created, the account has no privileges. To log into the Uplogix Control Center and work with its web interface, users must have appropriate levels of server privileges.

Privileges on the Uplogix Control Center are assigned separately from privileges on the equipment in the inventory. Both are needed if a user is to use the Uplogix web interface to work with Uplogix Local Managers and to access Local Managers individually via SSH.

Privileges can be assigned to several users at once by importing a permissions file. See [Importing user, group, and privilege files](#).

To assign server privileges, go to the Server Privileges page on the Administration tab.

The screenshot shows the Uplogix Control Center Administration page. The top navigation bar includes Dashboard, Inventory, Alarms, Schedule, Reports, and Administration. The Administration tab is selected, and the breadcrumb path is Administration > Server Privileges. On the left is a sidebar menu with options: Appliances, AAA Settings, File Archive, Groups, Import, Licenses, Roles, Server Privileges (selected), Server Settings, and Users. The main content area is titled 'Server Privileges' and contains a form with two dropdown menus: 'Principal' (set to 'EThompson') and 'Role' (set to 'admin'). Below these is an 'Add' button and a 'Remove' button. A table lists existing assignments:

<input type="checkbox"/>	User/Group	Role
<input type="checkbox"/>	Jose	admin
<input type="checkbox"/>	administrator	admin
<input type="checkbox"/>	ajones	admin
<input type="checkbox"/>	athompson	admin
<input type="checkbox"/>	scott	admin

At the bottom of the table, it says '5 items found, displaying all items.'

Unlike inventory privileges, server privileges only apply to one resource - the Uplogix Control Center.

Select a user or group from the User/Group list, select a role, and click **Add**. Groups are listed first, followed by users. An * after the group name indicates a group.

As with Uplogix Local Manager privileges, more than one role can be assigned to an account to tailor that account's privileges.

Adding inventory privileges to accounts

Inventory > Group Detail > Configuration > Privileges

When a new user or group account is created, the account has no privileges. Set an account's privileges to apply to all Uplogix Local Managers in the inventory by assigning them at the root level or limit privileges to specific inventory groups.

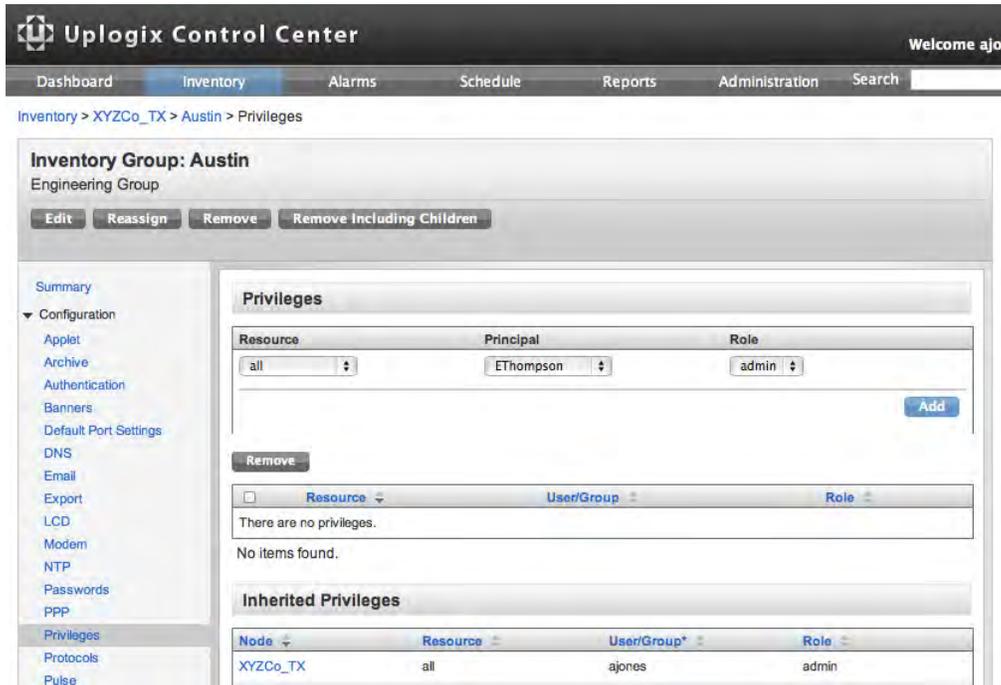


Inventory privileges are limited to Local Managers in the inventory, and the devices they control. Server privileges must be assigned separately. See [Adding server privileges to](#)

[accounts](#). To manage the inventory through the Upligix Control Center, users must have server privileges.

Privileges can be assigned to several users at once by importing a permissions file. See [Importing user, group, and privilege files](#).

To add inventory privileges, select the appropriate inventory group from the Inventory page and click **Privileges** under the Configuration menu.



Use the Privilege List page to assign privileges to accounts in the form of defined roles and to specify the resources where each role is applied – all, system, modem, or powercontrol. If labels have been created, these are available as resources also.

Select a user or group from the User/Group list, select a role, and click **Add**. Groups are listed first, followed by users. An * after the group name indicates a group.

More than one role can be assigned to an account and be given different roles on different resources.

The screenshot shows the Uplogix Control Center interface. At the top, there is a navigation bar with tabs for Dashboard, Inventory, Alarms, Schedule, Reports, Administration, and Search. Below this, the breadcrumb path is 'Inventory > XYZCo_TX > Austin > Privileges'. The main content area is titled 'Inventory Group: Austin' and 'Engineering Group'. It features buttons for 'Edit', 'Reassign', 'Remove', and 'Remove Including Children'. On the left, there is a 'Configuration' menu with various options like 'Applet', 'Archive', 'Authentication', etc., and 'Privileges' is selected. The main area contains a 'Privileges' table with columns for Resource, Principal, and Role. A dropdown menu is open over the 'Resource' column, showing options like 'all', 'system', 'modem', 'powercontrol', 'Core Switches', and 'Routers'. Below this, there is a section for 'Inherited Privileges' with a table listing nodes, resources, user groups, and roles.

Resource	Principal	Role
<input checked="" type="checkbox"/> all <input type="checkbox"/> system <input type="checkbox"/> modem <input type="checkbox"/> powercontrol <input type="checkbox"/> Core Switches <input checked="" type="checkbox"/> Routers	ETHompson	admin
<input type="checkbox"/> Resource	User/Group	Role

Node	Resource	User/Group*	Role
XYZCo_TX	all	ajones	admin
XYZCo_TX	all	athompson	admin

To remove privileges at the port level, select an Uplogix Local Manager from the inventory and select **Privileges** from Configuration menu.

Use the Local Manager's Privilege List to add or delete user roles by individual resource.

The screenshot shows the Uplogix Control Center interface. The top navigation bar includes Dashboard, Inventory, Alarms, Schedule, Reports, Administration, and Search. The breadcrumb trail is Inventory > XYZCo_TX > Austin > Building 1 > Pasadena > Privileges. The main content area is titled 'Pasadena (172.30.51.122)' and shows 'Last Alarm: 1d 5h' and 'Last Event: 1h 31m'. Below this are buttons for CLI, Dial, Schedule Task, Edit, Reassign, Replace, and Remove. A left sidebar menu lists various configuration options, with 'Privileges' selected. The main content area has a 'Privileges' section with a form to add a new privilege. The form has three dropdown menus: Resource (set to 'all'), Principal (set to 'EThompson'), and Role (set to 'admin'). Below the form is a 'Remove' button. A table below the form lists existing privileges:

Resource	User/Group	Role	Inherited
<input type="checkbox"/> all	admin	admin	
<input type="checkbox"/> all	ajones	admin	*
<input type="checkbox"/> all	athompson	admin	*
<input type="checkbox"/> all	scott	admin	*

Below the table, it says '4 items found, displaying all items.'

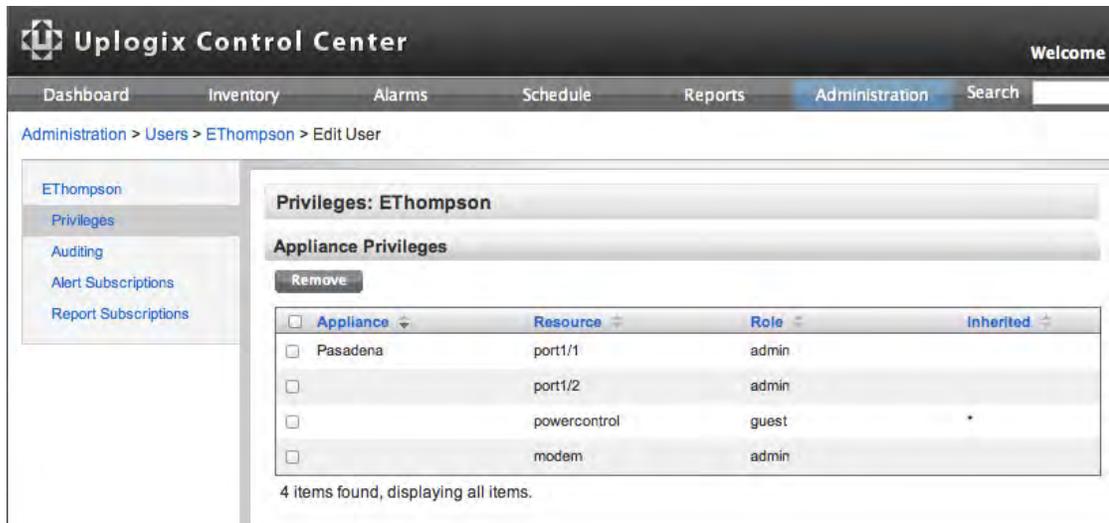
If the pre-configured standard roles do not meet your organization's needs, create roles to meet the specific requirements of your deployment. See [Creating and customizing roles](#).

Viewing and deleting user account privileges

Administration > Users

To view or edit a user's privileges, click the **user id** and then select **Privileges** from the left menu.

Use the user privileges detail to see and delete specific privileges. In the example below, the user EThompson has admin privileges assigned locally on Local Manager Pasadena, and inherited guest privileges that have been assigned at the inventory group level.



Creating and customizing roles

Inventory > Configuration > Roles

A role is a set of commands that a user is permitted to execute. When privileges are assigned to a user or group account, the account is associated with one or more roles on one or more resources. See [Adding inventory privileges to accounts](#).

The Uplogix Control Center provides the same predefined roles that are available in the Uplogix LMS CLI. In addition to these standard roles, custom roles can be defined to suit your deployment. Roles may be created at the root level to apply globally or they may be created within an inventory group to apply only to that group and its child groups.

To view a list of roles defined for any given inventory group, select the group from the inventory list and click **Roles** under the Configuration menu.

On the View Roles page, click **Add** to add a role or select the **Role ID** to edit an existing role. This is equivalent to issuing the `config role` command from the Uplogix LMS command line.

The screenshot shows the Uplogix Control Center interface. At the top, there is a navigation bar with the following items: Dashboard, Inventory (selected), Alarms, Schedule, Reports, Administration, and Search. Below the navigation bar, the breadcrumb path is "Inventory > XYZCo_TX > Roles". The main content area is titled "Inventory Group: XYZCo_TX" and "Example Customer". There is an "Edit" button. On the left side, there is a sidebar menu with the following items: Summary, Configuration (expanded), Applet, Archive, Authentication, Banners, Default Port Settings, DNS, Email, Export, LCD, Modem, NTP, Passwords, PPP, Privileges, Protocols, Pulse, Roles (selected), and Rules. The main content area shows the "Roles" configuration page. It has three buttons: "Add", "Remove", and "Import Role XML File". Below the buttons is a table with the following columns: "Role", "Description", "Active", and "Scope". The table contains two rows: "admin" and "guest". Both roles are active and have a local scope. Below the table, it says "2 items found, displaying all items."

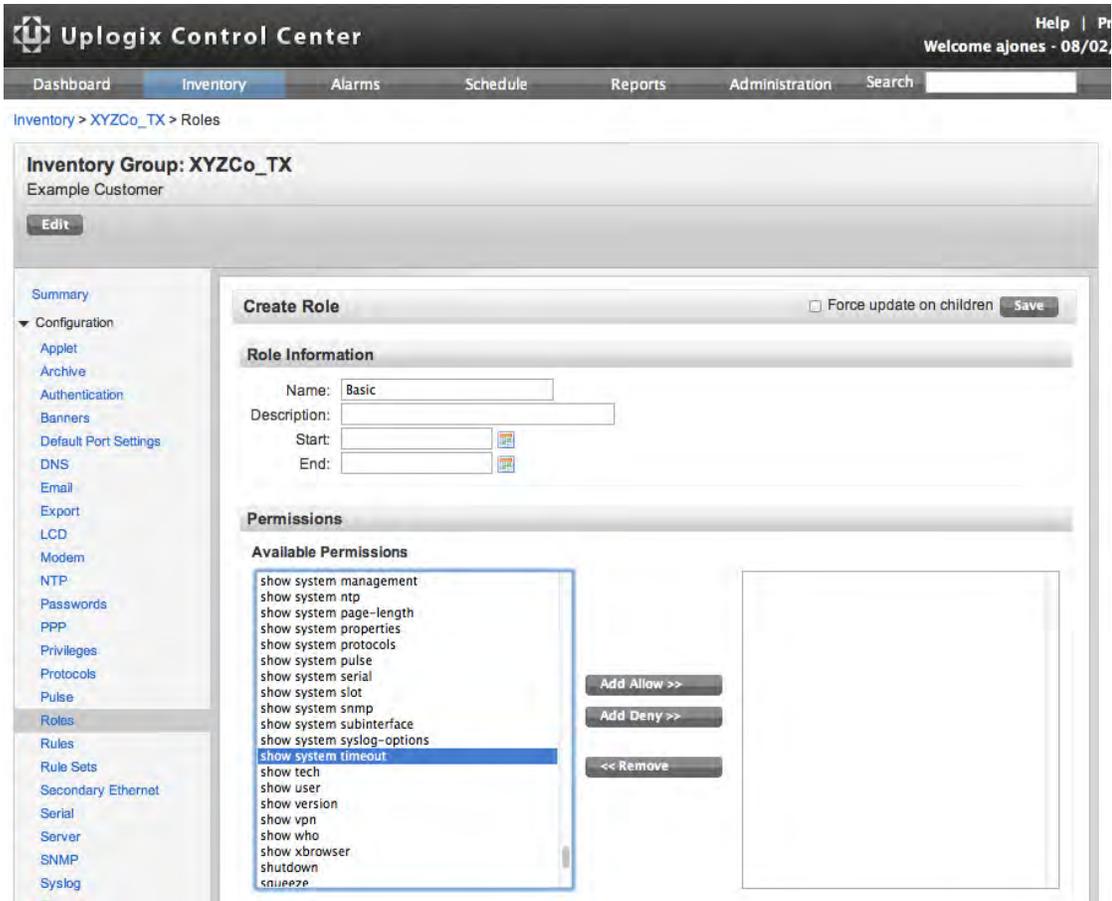
The role name is required when creating a new role.



Use only printing characters when completing text fields. Spaces are considered printing characters, but may only be used in the description field.

Specify the role permissions by selecting them from the Available Permissions list and using the **Add Allow** and **Add Deny** buttons.

To select more than one permission at a time, use shift-click on the first and last items in a range or use control-click to select permissions separately.



As with many other settings, when a role is created it is automatically inherited by any Uplogix Local Managers and child groups within the current inventory group. If a role with the same name already exists on an Uplogix Local Manager or child group within the current inventory group, select **Force update on children** to overwrite it.

Once the privileges for the role are defined, click **Save**.

Using Radius/TACACS to manage privileges

Setting up a user account to use a Radius or TACACS ACL allows the TACACS server to send group member information in the initial login transaction. To use this feature, the account must be set up on the TACACS server.

The general procedure is as follows:

1. Configure the Uplogix Control Center to use Radius or TACACS.
2. Set up a user group and associate a Radius or TACAS ACL to it.
3. Assign at least one role to give the group the desired set of permissions; create a suitable role if necessary.

These steps are described in detail below.



If AAA functions are delegated to an external server, create a user with the admin role on the Uplogix Control Center and add that account on the external server beforehand. If no user has the admin role on the Uplogix Control Center, the administration functions are not accessible.

Set up authentication

On the **Administration > AAA Settings** page, set up the Authentication Settings as follows:

1. Under Authentication Type, select RADIUS or TACACS.
2. Select the appropriate authentication method.
3. Select **Use RADIUS/TACACS Authorization**.
4. If you want to automatically create Uplogix user accounts for users defined in your AAA server, choose Select **Create Users**.
5. Enter the IP address and shared secret for each AAA server. Up to four servers may be specified.
6. Optionally, select **Cache Passwords** to ensure that user accounts, passwords and privileges will still be available if the AAA server is offline during a future login authentication/authorization.

The screenshot shows the 'AAA Settings' configuration page. At the top right is a 'Save' button. Below the title is a dropdown menu for 'AAA Settings'. The configuration options are as follows:

- Accounting type: none (dropdown menu) Only applies to appliances
- Manage 'admin' User: Allows all appliances to have the same properties for 'admin'.
- Authentication Type: Local RADIUS TACACS
- Authentication Method: PAP CHAP MS-CHAP
- Use RADIUS/TACACS Authorization: Use RADIUS/TACACS to assign users to groups.
- Create Users: Create users that have a valid login but do not exist locally. (requires RADIUS/TACACS Authorization)
- Cache Passwords: Save server passwords locally.
- Fail Over to Local: If servers are down, authenticate locally.
- Limit Maximum Concurrent Sessions: Only applies to appliances
- Maximum Number of Concurrent Sessions: (input field) Only applies to appliances

At the bottom of the page is a section for 'Authentication Servers' with a right-pointing arrow.

When a user logs in to the Upligix Control Center with Cache Passwords enabled, the Upligix Control Center verifies the password with the authentication server and then updates the user account (caching) on the Control Center. Since the account is updated, this change gets pushed down to all the Local Managers, changing the user's password on Local Managers throughout the inventory.

Using this method, the Upligix Control Center can be configured to use AAA, but the Local Managers don't have to. The Local Manager receives the user's new password via the Upligix Control Center and authenticates locally with the password received remotely. Although the user logs into the Local Manager with the account's TACACS password, the Local Manager is not really contacting the TACACS server.

In this scenario, if the user's password changes on TACACS, it is not updated on the Local Managers in the inventory until the user logs into the Upligix Control Center to cache the new password. At this time it is pushed to the Local Managers. Evaluate whether this is a suitable approach for your environment.



Upligix User passwords are encrypted on the Upligix Control Center and Local Manager using AES encrypted with a one-way SALT.

Create a group and assign a TACACS ACL

The group provides a means to associate roles to the TACACS ACL.

1. Under **Administration** > **Groups** create a group. Users do not need to be added to the group.
2. Enter a name or a number that means something to you in the in the TACACS ACL field.

A screenshot of the Upligix Control Center web interface. The top navigation bar includes 'Dashboard', 'Inventory', 'Alarms', 'Schedule', 'Reports', 'Administration', and 'Search'. The breadcrumb trail shows 'Administration > Groups > InstallTeam'. The main content area is titled 'Edit Group: InstallTeam' with a 'Save' button. It contains several sections: 'Group Information' with fields for Name (InstallTeam), Description (InstallersRock), Start Date, and Expiration Date; 'Email Addresses' with a count of 0; 'Children: Users' with a count of 4 and a list of users (EThompson, Jason, Paul, ajones) with checkboxes; and 'Children: Groups' with a count of 0.

3. Assign suitable roles to the group. See [Adding server privileges to accounts](#) and [Adding inventory privileges to accounts](#). Users are not able to authenticate until they have roles.

Enable authorization on an existing TACACS user

Once the user is created and is able to authenticate to the Uplogix Local Manager, authorization can be added by adding an ACL under the “Exec” service in your user or group. In most Unix TACACS deployments, the users file can be edited and the following lines can be added to either the group or the user:

```
service = exec {  
acl = <acl name/number from Uplogix Control Center group>  
}
```

Refer to your TACACS administrator guide for more specific examples of configuration required for this functionality.

Example: Creating a superuser

The Uplogix Control Center is a resource, just as Uplogix Local Managers and their ports, modems, and power controllers are resources. Users cannot log into the Uplogix Control Center until they have privileges.

The administrator account on the Uplogix Control Center has admin access to all features of the server, but no privileges on individual Uplogix Local Managers. Therefore, administrator cannot log into an Uplogix Local Manager. This account does have the `config` hierarchy permission which allows the administrator to manage individual Local Managers through the Uplogix Control Center.

Conversely, the admin account on Uplogix Local Managers has no privileges on the Uplogix Control Center.

Server privileges and Uplogix Local Manager privileges are separate and must both be explicitly assigned if a user is to work with equipment in the inventory as well as the Uplogix Control Center itself.

To create a user who can execute any operation on any resource, first create the user. See [Creating and editing user accounts](#).

1. Go to the **Server Privileges** page and assign the admin role to the user.

Principal	Role
✓ EThompson	admin
InstallTeam*	
Jason	
Jose	
Paul	
TrainingGroup*	
administrator	
ajones	admin
athompson	admin
scott	admin

5 items found, displaying all items.

2. Go to the **Inventory** tab. The detail page for the root group is displayed. Click **privileges**.

- Assign the user admin privileges on all resources.



- The user now has access to all commands and capabilities on the Uplogix Control Center and on all equipment at every level of the inventory.

Example: Limiting a user's access to one port on one system

Sometimes a user needs only minimal access. In this example a user is created who can only log into one Uplogix Local Manager, and after logging in, can only execute the terminal command on port 1/1. To do this, we must complete the following:

- [Create a custom role](#)
- [Create a user account that will have this role](#)
- [Apply the role to the appropriate resources](#)

Creating the role

On the **Administration > Roles** page, click **Add** to open the Create Role page. Use this page to create a role that is universally available.

If the role should only be available within a specific inventory group and child groups, access the Create Role page by clicking the **Roles** button on the appropriate inventory group detail page.

For this example, a role called `terminal0n1y` will be created that can be assigned at the system level and on the desired port. This role gives only the permissions required for a user to be able to open a terminal session to the device on port 1/1.

Users can only execute commands while logged in to the Uplogix Local Manager, so the user's permissions must include the `login` permission on the system.

The terminal command runs on the port resources only, so this user needs to navigate to the appropriate port in order to open terminal sessions. There is no "port" permission. Instead, use the `show status` permission. When applied to a port, this permission allows the user to navigate to the port.

When the user has navigated to the appropriate port, this role must allow the user to execute the terminal command, so the role must include the `terminal` permission.

Upligix Control Center

Help
Welcome aJones - 08

Dashboard Inventory Alarms Schedule Reports Administration Search

Administration > Roles > Create Role

Appliances
AAA Settings
File Archive
Groups
Import
Licenses
Roles
Server Privileges
Server Settings
Users

Create Role Force update on children **Save**

Role Information

Name: terminalOnly
Description:
Start:
End:

Permissions

Available Permissions

- show system properties
- show system protocols
- show system pulse
- show system serial
- show system slot
- show system snmp
- show system subinterface
- show system syslog-options
- show system timeout
- show tech
- show user
- show version
- show vpn
- show who
- show xbrowser
- shutdown
- squeeze
- suspend
- terminal
- terminal break

allow login
allow show status
allow terminal

Add Allow >>
Add Deny >>
<< Remove

Scope: local Force update on children **Save**

Once the required permissions have been added, click **Save** to save the terminalOnly role.

Creating the user account

On the Administration > Users page, click **Add** to open the Create User page.

For this example, a user account called termOnlyUser is created.

Upligix Control Center

Dashboard Inventory Alarms Schedule Reports Administration

Administration > Users > termOnlyUser

termOnlyUser
Privileges
Auditing
Alert Subscriptions
Report Subscriptions

Edit User: termOnlyUser **Save**
Created:08/02/2013 19:08:43

User Information

*Name: termOnlyUser
Password:
Confirm:
Description:
Disabled:
Time Zone: (-6:00) US/Central Use DST
Start Date:
Expiration Date:
Add To Group

Email Addresses Count: 0

Authorized Keys

Save

Applying the role to create permissions

This user account does not need access to the web interface; therefore no server privileges are assigned.

The account should only provide access to port 1/1 on a single system, so privileges from the Local Manager's expanded detail page are assigned.

Locate the appropriate system in the inventory. On the Configuration menu, click **Privileges** to open the Privilege list for the system.

Assign the `terminalOnly` role to `termOnlyUser` on the system resource. This allows `termOnlyUser` to use the system-level permissions (login and show status) in the `terminalOnly` role.

The screenshot shows the Uplogix Control Center interface. The breadcrumb trail is: Inventory > XYZCo_TX > Austin > Building 1 > Pasadena > Privileges. The main header for the system is "Pasadena (172.30.51.122)" with "Last Alarm: 1d 9h" and "Last Event: 2h 32m". Below this are buttons for CLI, Dial, Schedule Task, Edit, Reassign, Replace, and Remove. A left sidebar contains a navigation menu with items like Summary, Alarms, Events, Scheduled Tasks, Session Logs, SLV Stats, Configuration, Applet, Archive, Authentication, Banners, Default Port Settings, DNS, Email, Export, IP, IPv6, IPT, LCD, Modem, NTP, Passwords, PPP, Privileges, and Properties. The main content area is titled "Privileges" and contains a form with three dropdown menus: Resource (set to "system"), Principal (set to "termOnlyUser"), and Role (set to "terminalOnly"). An "Add" button is to the right of the Role dropdown. Below the form is a "Remove" button and a table listing existing privilege assignments. The table has columns for Resource, User/Group, Role, and Inherited. There are 8 items listed, with some marked as inherited with an asterisk icon.

Resource	Principal	Role
system	termOnlyUser	terminalOnly

Resource	User/Group	Role	Inherited
<input type="checkbox"/>	all	admin	
<input type="checkbox"/>	all	admin	*
<input type="checkbox"/>	all	admin	*
<input type="checkbox"/>	all	admin	*
<input type="checkbox"/>	modem	admin	
<input type="checkbox"/>	port1/1	admin	
<input type="checkbox"/>	port1/2	admin	
<input type="checkbox"/>	powercontrol	guest	*

8 items found, displaying all items.

Assign the `terminalOnly` role to `termOnlyUser` on the port 1/1 resource. This allows `termOnlyUser` to use the port-level permissions (show status and terminal) on this port only. The `show status` permission allows the user to navigate to the port; `terminal` allows the user to open terminal sessions.

Uplogix Control Center Welcome

Dashboard **Inventory** Alarms Schedule Reports Administration Search

Inventory > XYZCo_TX > Austin > Building ↑ > Pasadena > Privileges

Pasadena (172.30.51.122)
 Last Alarm: 1d 9h | Last Event: 2h 32m

CLI Dial Schedule Task Edit Reassign Replace Remove

Summary
 Alarms
 Events
 Scheduled Tasks
 Session Logs
 SLV Stats
 Configuration
 Applet
 Archive
 Authentication
 Banners
 Default Port Settings
 DNS
 Email
 Export
 IP
 IPv6
 IPT
 LCD
 Modem
 NTP
 Passwords
 PPP
Privileges
 Properties

Privileges

Resource: system | Principal: termOnlyUser | Role: terminalOnly

all
 system
port1/1
 port1/2
 port1/3
 port1/4
 port1/5
 port4/1

Resource	Principal	Role	
<input type="checkbox"/> system	termOnlyUser	terminalOnly	<input type="button" value="Add"/>
User/Group	Role	Inherited	
<input type="checkbox"/> admin	admin		
<input type="checkbox"/> ajones	admin	*	
<input type="checkbox"/> athompson	admin	*	
<input type="checkbox"/> scott	admin	*	
<input type="checkbox"/> ETThompson	admin		
<input type="checkbox"/> port1/1	ETThompson	admin	
<input type="checkbox"/> port1/2	ETThompson	admin	
<input type="checkbox"/> powercontrol	ETThompson	guest	*

8 items found, displaying all items.

The user termOnlyUser can now log into the Pasadena system and open a terminal session to the device on port 1/1.

Importing user, group, and privilege files

Administration > Import

The Uplogix Control Center can import preformatted lists of user accounts, group accounts, privileges, and group members. This feature is useful if managing accounts and privileges in a third-party application such as Microsoft Excel. The import functions accept comma-separated value (CSV) formats.

The screenshot displays the Uplogix Control Center interface. At the top, there is a navigation bar with tabs for Dashboard, Inventory, Alarms, Schedule, Reports, and Administration. Below this, the breadcrumb path 'Administration > Import' is shown. On the left side, there is a sidebar menu with options: Appliances, AAA Settings, File Archive, Groups, Import (highlighted), Licenses, Roles, Server Privileges, Server Settings, and Users. The main content area is titled 'Import' and contains four distinct sections, each for a different type of CSV import:

- Import Users CSV File:** Includes a 'Choose File' button (no file selected), an 'Action:' label with radio buttons for 'Add/Update' and 'Delete', and 'Import' and 'Help' buttons.
- Import Groups CSV File:** Includes a 'Choose File' button (no file selected), an 'Action:' label with radio buttons for 'Add/Update' and 'Delete', and 'Import' and 'Help' buttons.
- Import User Group Membership CSV File:** Includes a 'Choose File' button (no file selected), an 'Action:' label with radio buttons for 'Add/Update' and 'Delete', and 'Import' and 'Help' buttons.
- Import Privileges CSV File:** Includes a 'Choose File' button (no file selected), an 'Action:' label with radio buttons for 'Add/Update' and 'Delete', and 'Import' and 'Help' buttons.

For information on setting up the CSV file, click **Help** in the appropriate Import box.

Uplogix Control Center

Dashboard Administration > Import

- Appliances
- AAA Settings
- File Archive
- Groups
- Import**
- Licenses
- Roles
- Server Privileges
- Server Settings
- Users

User Import File Format

Field Summary:
username,description,timezone,dst,alertEligibility,alertFrequency,start,expire,password,email

Examples:
bob,desc,US/Central,TRUE,*****,,1/1/00,12/12/05,bob,bob@company.com,
bob,,,,,,,,,bob@uplogix.com,

- If username entry appears more than once in the import file, only the first record is processed.

Field Details	Required	Default	Notes
username	yes		
description	no		When updating, an empty value will clear the field.
timezone	no	US/Central	When updating, an empty field will leave existing value unchanged.
dst	no	TRUE	When updating, an empty field will leave existing value unchanged.
alertEligibility	no	*****	When updating, an empty field will leave existing value unchanged.
alertFrequency	no	2	When updating, an empty value will leave existing value unchanged.
start	no		When updating, an empty value will clear the field.
expire	no		When updating, an empty value will clear the field.
password	yes when adding		When updating, an empty value will leave existing value unchanged.
email	no		Always treated as In-Band unchecked, Out-of-Band unchecked, Terse unchecked. When updating, an empty value will leave existing entries unchanged. Populated value will add to existing email entires for the user, unless an exact match already exists.

Logs, reports, and diagnostics

The Uplogix Control Center captures several kinds of information about the Uplogix Local Managers it manages and the devices connected to each Local Manager, as well as user activity. This chapter describes how to access information about:

Events—major user actions such as login, logout, and changes to accounts; major automated actions

Alarms—records of changes that may trigger alerts or other actions

Logs—line-by-line records of all user activity

Reports—details on alarms, changes, events, or sessions

In this chapter:

- [Setting up email, auditing, and report subscriptions](#)—configure an account to receive reports and alerts from the Uplogix Control Center
- [Viewing alarms and events](#)—global, group, and Local Manager views
- [Viewing reports](#)—receiving, downloading, and viewing reports from the Uplogix Control Center
- [Viewing archive status information for a Local Manager](#)—time the last archive took place, whether it was successful, and related information
- [Viewing device syslogs](#)—current device syslogs
- [Viewing session logs and auditing users](#)—view transcripts and configure accounts to receive reports of activities
- [Sending logs to Technical Support](#)—how to send information to the support team for troubleshooting
- [Replacing a Local Manager](#)—replace a Local Manager with a new Local Manager and transfer all configurations and data from previous Local Manager
- [Shutting down the Control Center](#)—how to properly turn off the Control Center

Setting up email, auditing, and subscriptions

To provide subscribed information, alerts and reports, the Uplogix Control Center must be configured to send email. For more information, see [Configuring mail settings](#).

To receive alerts and reports, the account must be:

- configured with an email address where alerts and reports are received from the Uplogix Control Center
- subscribed to the desired alerts and reports

To audit other accounts, the account must be:

- configured with an email address where alerts and reports are received from the Uplogix Control Center
- configured to audit at least one other account
- subscribed to the appropriate session report (hourly, daily, weekly, or monthly) for the account to be audited

These can be configured on the Create/Edit User or Create/Edit Group pages. Click the right arrows ▶ to expand the collapsed sections of these pages.

Configuring an account to receive email from the Uplogix Control Center

For an account to receive alerts or reports by email, at least one email address where the user can receive alerts and reports (including user audits) must be entered.

The in-band and out-of-band settings only apply to information that Uplogix Local Managers email to you. By default, the address entered is used in both situations.

Select **Terse** to limit the message to a subject line only. Use the Terse setting for email directed to a pager or cell phone. Click **Add Email** when all the email information has been entered and then **Save** on the edit user details screen.

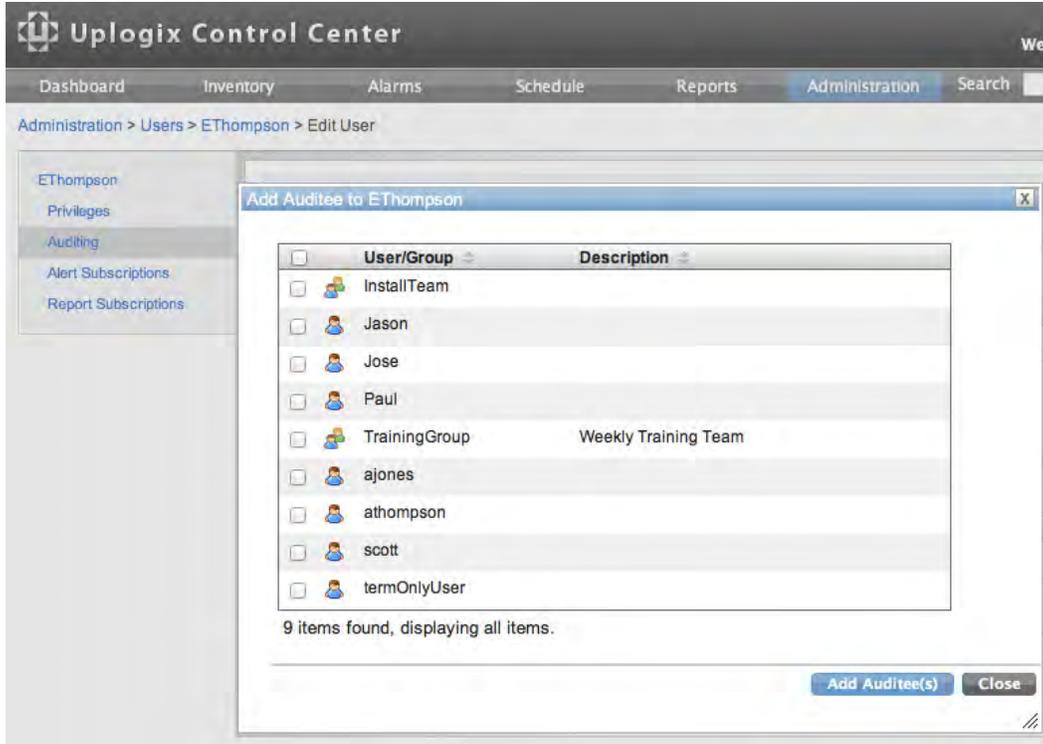


To remove an email address, use the **clear** button rather than manually clearing the address field.

The screenshot shows the 'Edit User: ETHompson' page in the Uplogix Control Center. The page is titled 'Edit User: ETHompson' and 'Created: 04/24/2013 19:21:17'. The 'User Information' section is expanded, showing fields for Name, Password, Confirm, Description, Disabled, Time Zone, Start Date, and Expiration Date. The 'Email Address' section is also expanded, showing a list of email addresses with 'Add Email' and 'Remove' buttons. The 'Add Email' button is highlighted. The 'Email Address' field contains 'ethompson@xyzco.com'. The 'In-band' and 'Out-of-band' checkboxes are checked, and the 'Terse' checkbox is unchecked. The 'Save' button is visible at the bottom right of the form.

Configuring the account to audit others and to be audited

To allow the user to audit others, select the user from the User menu under Administration by clicking on the **User ID**. Then from the left menu, select **Auditing**. In the auditing detail page, add auditees by clicking the **Add** button and selecting users from the checklist. Click **Add Auditee(s)**.



To allow another user to audit this user, open the Auditor Picker by clicking **Add**. Add auditors following the same steps as adding auditees.

To allow this user to audit others, the user must also be subscribed to session reports. See [Subscribing to reports](#).

Subscribing to alerts

Administration > Users > Edit

Individual user accounts may subscribe to alerts.

Subscribe the account to alerts on the desired resources.

- Subscription resources are individual ports, modem, powercontrol, system, or all.
- Sub-resources are interface, chassis, or all.

The screenshot shows the 'Alert Subscriptions' configuration page for user ETHompson. The page has a navigation bar with 'Administration' selected. A left sidebar lists options: ETHompson, Privileges, Auditing, Alert Subscriptions (selected), and Report Subscriptions. The main content area is titled 'Subscriptions: ETHompson' and includes a 'Save' button. Under 'Alert Subscriptions', there is a table with columns: Appliance (select), Resource (all), Sub-resource (all), Interface Name (empty), and Wait Time (min) (0). An 'Add' button is at the bottom right of this table. Below is a 'Remove' button and another table with columns: Appliance, Resource, Sub-resource, Interface Name, and Wait Time (min). A message states 'There are no alert subscriptions configured.' At the bottom, there is an 'Alert Options' section and another 'Save' button.

Click **Save** at the top or bottom of the page when finished setting up the account information.

Subscribing to reports

Administration > Users

Administration > Groups

To subscribe an account to reports, go to **Administration > Users** or **Administration > Groups** and select the User ID associated with the user. Then from the left menu, select **Report Subscriptions**. This link is only active if the account is configured with an email address.

The report subscription specifies how often the report is created and emailed.

The report subscriptions link takes you to the Report Subscriptions page.

Choose the Uplogix Local Manager inventory group or port from which to receive reports, and the file format for the report - CSV, HTML, or PDF. Click the Subscribe links to subscribe to the desired reports. Depending on the file format selected, the user may receive zipped files.

The screenshot shows the 'Report Subscriptions' configuration page for user mhoward. The page has a navigation bar with 'Administration' selected. A left sidebar lists options: mhoward, Privileges, Auditing, Alert Subscriptions, and Report Subscriptions (selected). The main content area is titled 'Report Subscriptions: mhoward' and includes a 'Remove' button. Below is a table with columns: Scope, Group, Name, Resource, and To Address. The table contains three rows:

Scope	Group	Name	Resource	To Address
<input type="checkbox"/>	Appliance	Alarms	Hourly	A101101100
<input type="checkbox"/>	Inventory Group	Logins	Daily	Austin
<input type="checkbox"/>	Inventory Group	Changes	Daily	Austin

 Below the table is a 'Label Reports' section and an 'Inventory Group Reports' section with a 'Subscribe' button. At the bottom, there are dropdown menus for 'Inventory Group: Austin', 'Email: mhoward@uplogix.com', and 'Export Type: PDF'. Below these is a table with columns: Group, Name, File, and Frequency.

Group	Name	File	Frequency
<input type="radio"/>	Alarms	Hourly	alarmsByNodeReport.jrxml
<input type="radio"/>	Alarms	Daily	alarmsByNodeReport.jrxml
<input type="radio"/>	Alarms	Weekly	alarmsByNodeReport.jrxml

Session reports are available in the Principal Reports area at the bottom of the page. You can only subscribe to session reports on accounts that are configured as auditees on your user account. For more information on this, see [Configuring the account to audit others and to be audited.](#)

Specifying when and how often the subscriber receives alerts

Administration > Users > User ID > Alert Subscriptions

By default, alerts are emailed to subscribed users every two minutes while they are active.

Limit the number of alerts that a user receives with the Alert Options settings on the Alert Subscriptions page.

The screenshot shows the Uplogix Control Center interface. The top navigation bar includes Dashboard, Inventory, Alarms, Schedule, Reports, Administration (selected), and Search. The breadcrumb trail is Administration > Users > ETHompson > Edit User. On the left, a sidebar lists options: ETHompson, Privileges, Auditing, Alert Subscriptions (selected), and Report Subscriptions. The main content area is titled 'Subscriptions: ETHompson' and contains two sections: 'Alert Subscriptions' and 'Alert Options'. The 'Alert Subscriptions' section has a table with columns: Appliance (select), Resource (all), Sub-resource (all), Interface Name, and Wait Time (min) (0). Below the table are 'Add' and 'Remove' buttons. The 'Alert Options' section is titled 'Specify when alerts should be received' and includes fields for: Days of the week (*), Months of the year (*), Days of the month (*), Hours (*), Minutes (*), Frequency (0 minutes), and Threshold (2). A 'Save' button is at the bottom right.

Alert Options specify the times, days, and frequency when alerts may be emailed to this user. The limit options are as follows. Leave the wildcard * character in the fields you do not wish to restrict.

Option	Description
Days of the week	Limit the receipt of alerts to certain days of the week. Specify the range of days numerically with 1 representing Monday. For example, if the user should only receive alerts from Friday through Monday, enter 5-1.

Option	Description
Months of the year	<p>Limit the receipt of alerts to certain months. Specify the beginning and ending month by number.</p> <p>For example, if the user should only receive alerts from September through May, enter 9-6.</p>
Days of the month	<p>Limit the receipt of alerts to certain days of the month. Specify which days by number.</p> <p>For example, if the user is on call only from the 16th to the end of the month, enter 16-31.</p>
Hours	<p>Hours are specified in UTC time.</p> <p>Limit the receipt of alerts to a specific time of day. Specify start and end time.</p> <p>For example, if the user is in the US central time zone (UTC -6:00) and needs to receive alerts generated between 5 p.m. and midnight, convert these times to UTC (00:00 to 06:00) and enter the hours as 23-6.</p>
Minutes	<p>Limit the receipt of alerts to a specific part of each hour. Specify the start and end minutes.</p> <p>For example, if the user should only receive alerts during the first 15 minutes of every hour, enter 00-15.</p>
Frequency	<p>Set how often the Uplogix Control Center sends alerts. Alerts can be sent as seldom as every 120 minutes or as often as every minute.</p>
Threshold	<p>If the user would like to receive alerts after a specific number of occurrences of the alert, set the number of occurrences as the threshold.</p>

Viewing alarms and events

Alarms and events are similar. Both are logged. An alarm differs from an event as follows:

- An alarm has a duration—it remains active as long as the triggering condition exists.
- An alarm has a state—current or cleared.

The Alarms page provides a quick overview of active alarms on any of the managed Uplogix Local Managers.

The alarm summary shows when an alarm was last generated, how long it has been active, which Local Manager it occurred on, and a message detailing the alarm. If the alarm involves a specific device and/or interface, that information is displayed as well. Alarms can be filtered by Local Manager, and by number of results. To quickly access the Local Manager reporting the alarm, click the hostname in the Local Manager column to bring up the Local Manager detail page. The Selecting the Alarms menu displays alarms respectively for the specific device.

Last Occurrence	Duration	Appliance	Device	Context	Message
08/05/2013 12:49		Pasadena	AustinR1-SRE		Envoy unable to commun

To view events on a Local Manager, navigate to the device and select Events from the menu. The Events page shows recent events for the selected Uplogix Local Manager. Each entry shows the time of the event, the device and interface on which it occurred (if available), the user, and a descriptive message.

Time	Context	User	Message
08/05/2013 12:47		ajones	User logged out of Envoy. (Envoy detected use
08/05/2013 12:44		ajones	User logged into Envoy.

Search the list of events by entering a text string in the search box, selecting the type of search, and clicking **Search**.

Alarm and event reports for inventory groups can also be viewed. Go to the appropriate group detail page and select the report that spans the time period of interest.

Uplogix Control Center Welcome

Dashboard **Inventory** Alarms Schedule Reports Administration Search

Inventory > XYZCo_TX > Austin > Report

Inventory Group: Austin
Engineering Group

Edit Reassign Remove Remove Including Children

Summary
 Configuration
 Reports
 Alarms
 Hourly
 Daily
Weekly
 Monthly
 Changes
 Hourly
 Daily
 Weekly
 Monthly
 Events
 Hourly
 Daily
 Weekly
 Monthly

View Report

View report containing 07/28/2013 00:00:00

Uplogix Control Center Start: 07/28/2013 00:00 UTC
Weekly Alarms Report End: 08/04/2013 00:00 UTC

Uplogix	Device	Flag	Start Time (UTC)	Duration
Pasadena	port4/1	CLEARED	05/05/13 13:22	86d 1h
Message:	TCP driver connection error. (Error reading 192.168.93.201:22 - No route to host)			
Pasadena		CLEARED	07/27/13 06:50	3d 7h
Message:	System and management server clocks are more than 20 seconds out of sync.			
Pasadena		CLEARED	07/27/13 06:50	3d 7h
Message:	NTP server invalid. ('203.0.113.3', server strata too high)			
Pasadena	port4/1	CLEARED	07/28/13 08:01	1m 46s
Message:	TCP driver connection error. (Error reading 192.168.93.201:22)			
Pasadena	port4/1	CLEARED	07/30/13 14:34	1s
Message:	TCP driver connection error. (Error writing 192.168.93.201:22 - No route to host)			

Viewing reports

The Uplogix Control Center regularly archives data received from Uplogix Local Managers. Reports can be generated from the inventory group and Local Manager level. A report from the inventory group level includes information from all Uplogix Local Managers within the inventory group, while the Local Manager level only includes the specific Local Manager.

Inventory group reports

Inventory > group detail > Reports

Access inventory group reports from the Group Detail page. Expand the Reports menu and click the link for the report of interest.

Uplogix Control Center

Dashboard **Inventory** Alarms Schedule Reports Administration

Inventory > XYZCo_TX > Austin > Detail

Inventory Group: Austin
Engineering Group

Edit Reassign Remove Remove Including Children

Summary

- Configuration
- Reports
 - Alarms
 - Hourly
 - Daily
 - Weekly
 - Monthly
 - Changes
 - Hourly
 - Daily
 - Weekly
 - Monthly
 - Events
 - Hourly
 - Daily
 - Weekly
 - Monthly
 - Logins
 - Hourly
 - Daily

Inventory Group: Austin

Inventory Group Children

Child Group	Description
Building 1	
Marketing	

Add

Appliance Children

Appliance IP	Hostname
There are no appliances in this group.	

Add

If necessary, specify the desired range of times.

Reports start at the beginning of the specified time span. For example, a weekly report begins on Sunday rather than showing the previous seven days; a monthly report begins on the first of the month rather than showing the previous 30 days.

View Report

View report containing **Display** **Download CSV** **Download PDF**

Uplogix Control Center Start: 07/14/2013 00:00
End: 07/21/2013 00:00

Weekly Logins Report

Uplogix	Username	Client IP	Conn Type	Occurred (UTC)
Basadara	sloner	2001:470:b851:500:9156:75fa:8ba3:70d7cch		07/17/13 15:03

Once the time period of interest is specified, click **Display**, **Download PDF** or **Download CSV** as appropriate.

Local Manager reports

Inventory > Local Manager > Reports

Access Local Manager specific reports from the reports menu on the Local Manager page.

Uplogix Control Center

Dashboard | **Inventory** | Alarms | Schedule | Reports | Administration

Inventory > XYZCo_TX > Austin > Building 1 > Pasadena > Summary

Pasadena (172.30.51.120)

Last Alarm: 1d 3h | Last Event: 1h 30m

[CLI](#) [Dial](#) [Schedule Task](#) [Edit](#) [Reassign](#) [Replace it](#) [Remove](#)

- Summary
- Alarms
- Events
- Scheduled Tasks
- Session Logs
- SLV Stats
- Configuration
- Reports
 - Alarms
 - Hourly
 - Daily
 - Weekly
 - Monthly
 - Changes
 - Hourly
 - Daily
 - Weekly
 - Monthly
 - Events
 - Hourly

Appliance Status: OK CON: ETH: CPU: 16/17/18

[CLI](#) Description: IPv4 Address: 172.30.51.120 IPv6 Address: 2001:4:
Serial #: A500100061 Model: Uplogix 5000 Last Login: 08/06/2
Version: 4.6.4 Temp C: N/A Uptime: 71d 14h
Build #: 20130307:040742 Temp F: N/A Last Heartbeat: 08/09/2
OS Version: 4.6.4.22890 Humidity: N/A Last Archive: 08/09/2

Properties [Edit](#)

No properties configured

Devices

Show: Sort by: Hide unconfigured devices

CLI	port1/1 AustinR1-SRE	OK	<input checked="" type="radio"/>	CLI	port4/1 UNAVAILABLE	<input type="radio"/>
CLI	port1/2 usausarc-sre3	OK	<input checked="" type="radio"/>			
CLI	port1/3 L1-SSG5-AAF	OK	<input checked="" type="radio"/>			

Reports by label

Reports > Reports by Label

Most reports are available on the Group Detail, Local Manager Detail, and Port Detail pages. However, reports can also be generated for custom labels. If labels have been created for managed devices (see [Creating categories for managing devices](#)), standard reports for each label are available on the Reports by Label page.

The screenshot shows the Uplogix Control Center interface. At the top, there is a navigation bar with the following tabs: Dashboard, Inventory, Alarms, Schedule, Reports (highlighted), and Administration. Below the navigation bar, the breadcrumb path is 'Reports > Reports By Label'. On the left side, there is a sidebar menu with three items: 'Report Assignments', 'Report Files', and 'Reports by Label' (highlighted). The main content area is titled 'View Report by Label' and contains a 'Display' button. Below the button, there is a dropdown menu for 'Label:' with 'Core Switches' selected. A list of report types is displayed, each with a radio button:

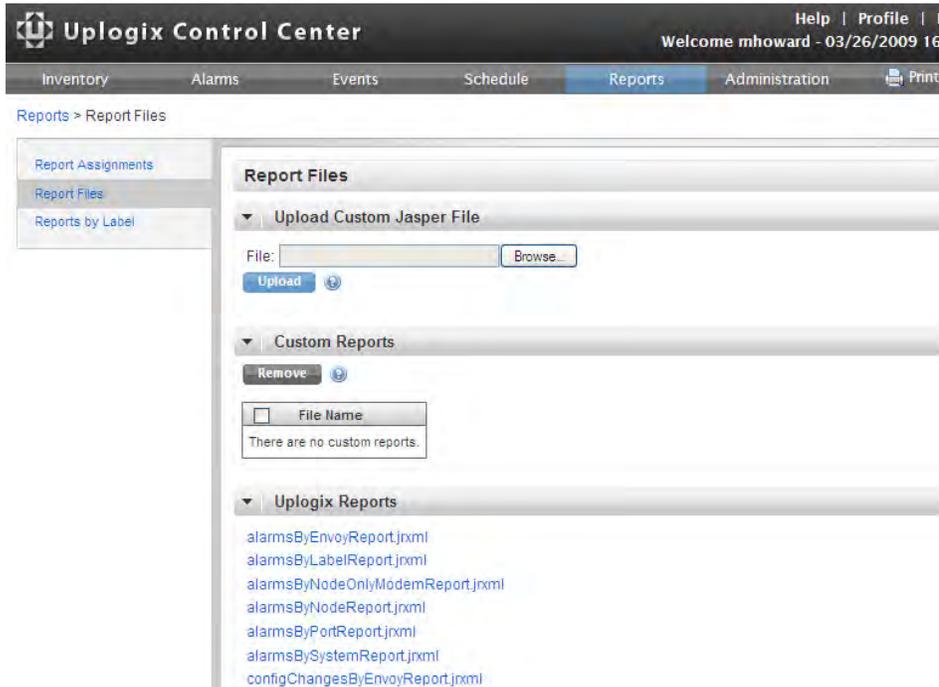
- Alarms Hourly
- Alarms Daily
- Alarms Weekly
- Alarms Monthly
- Changes Hourly
- Changes Daily
- Changes Weekly
- Changes Monthly
- Events Hourly
- Events Daily
- Events Weekly
- Events Monthly
- Privileges

Report files

Reports > Report Files

Reports are generated from Jasper XML files. Several are included with the Uplogix Control Center, but custom files can also be uploaded. Once uploaded, these files are available for use on the Report Assignments page.

After creating a custom Jasper file, browse to find it and click **upload**. The file is now available from the list of files on the Report Assignments page.



Please contact support@uplogix.com if you need assistance with this feature.

Report assignments

Reports > Report Assignments

The Uplogix Control Center can generate a wide range of reports on a variety of subjects. These correspond to the reports listing seen on the Group Detail, Local Manager Detail, and Port Detail pages.

Reports are generated in various formats and emailed to system users or groups

Use the Report Assignments page to schedule any of the existing reports.

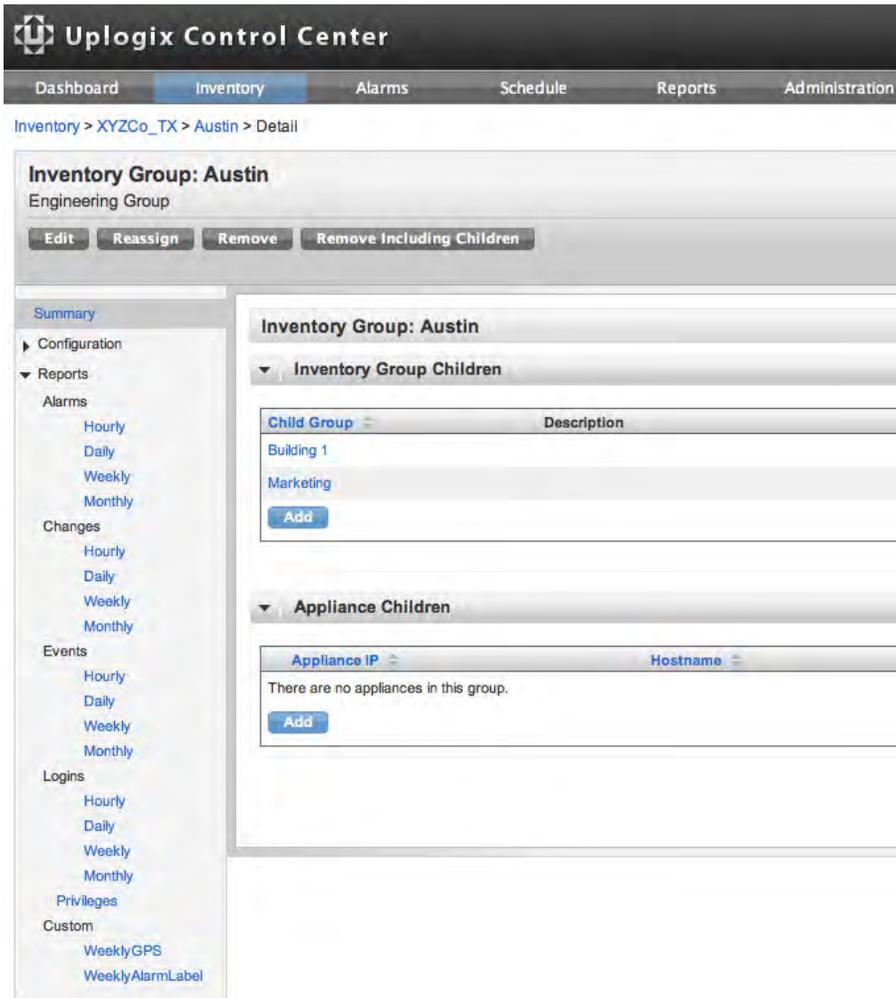
To create a new report assignment:

- Choose the **scope**—this may be label, inventory group, system, or port.
- Choose a **group**—this may be alarms, changes, events, logins, custom, or none.
- If there is at least one report in the group chosen within the selected scope (for example, alarm reports on inventory group pages), select the **offset**. This specifies the report's position in the list. An offset of 0 places the report first on the list.
- Name the report, select the appropriate jrxml format file, and choose the frequency of report generation.

In the following example, a weekly report of GPS events on managed devices is created. The report is available from inventory group pages under a custom report grouping.



Click **Assign** to create the report and assign it to the specified scope. In this example, the report is assigned to inventory group pages. The report is now available.



Although an existing report assignment cannot be edited, a new report assignment with the same name can be created. This overwrites the existing report assignment.

Viewing archive status information for a Local Manager

Inventory > Local Manager Summary

From the Local Manager summary page, clicking on the time of the last archive generates a pop-up showing information about the last data archive operation.

The screenshot shows the Uplogix Control Center interface. The top navigation bar includes Dashboard, Inventory, Alarms, Schedule, Reports, Administration, and Search. The breadcrumb trail is Inventory > XYZCo_TX > Austin > Building 1 > Pasadena > Summary. The main content area displays the summary for Pasadena (172.30.51.122), including status (OK), connection (CON: off), and CPU usage (13/15/17). A table of properties is shown, with the 'Last Archive' time highlighted in orange. A pop-up window titled 'Data Archive Information' is overlaid, displaying the following information:

Data is accurate as of 08/07/2013 18:56.	
Successfully finished processing data archive at 08/07/2013 18:57.	
Last Updated: 08/07/2013 18:57	Last Upload: 08/07/2013 18:56
Last Status: processed	In Queue: 0

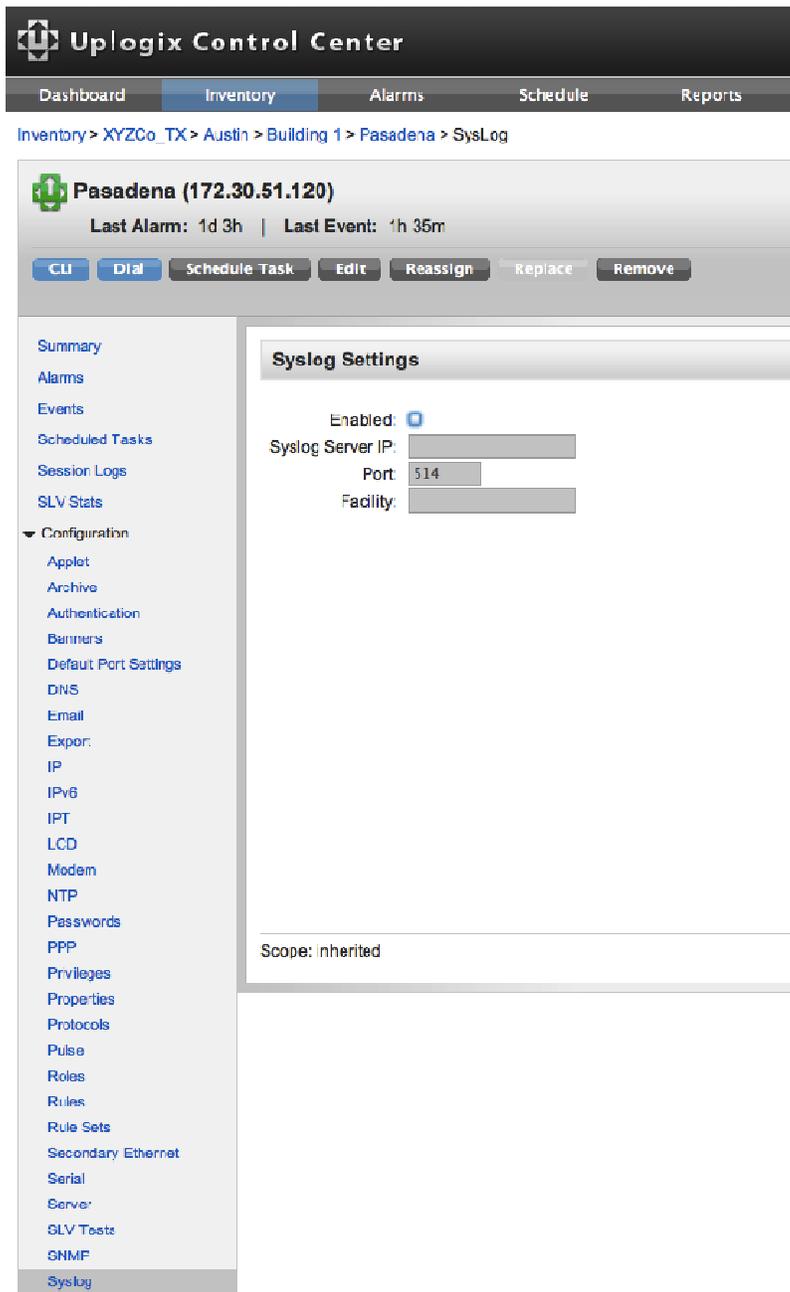
Viewing Local Manager Syslog Setting

Inventory > Local Manager Page > Configuration > Syslog

Syslog forwarding can be configured on the Configuration menu of the Local Manager page, or from the Uplogix command line with the `config system syslog-options` command.

In some advanced drivers, the console messages can be forwarded as syslog messages. This is configured from the port's config device logging command.

If device syslog forwarding is enabled, a connected device's console messages will be reformatted as syslog messages and forwarded to external syslog servers. The source IP address of the syslog message will be the Uplogix Local Manager's management IP, so multiple facilities should be used to classify the messages for various devices from the same Local Manager.



The screenshot displays the Uplogix Control Center interface. At the top, there is a navigation bar with tabs for Dashboard, Inventory, Alarms, Schedule, and Reports. Below this, the breadcrumb path is: Inventory > XYZCo_TX > Austin > Building 1 > Pasadena > SysLog. The main content area is titled "Pasadena (172.30.51.120)" and shows "Last Alarm: 1d 3h" and "Last Event: 1h 35m". A toolbar contains buttons for CLI, Dial, Schedule Task, Edit, Reassign, Replace, and Remove. On the left, a navigation menu lists various configuration options, with "Syslog" selected. The main content area displays the "Syslog Settings" configuration for the selected device. The settings include:

- Enabled:
- Syslog Server IP:
- Port:
- Facility:

At the bottom of the settings area, it indicates "Scope: inherited".

Viewing session logs and auditing users

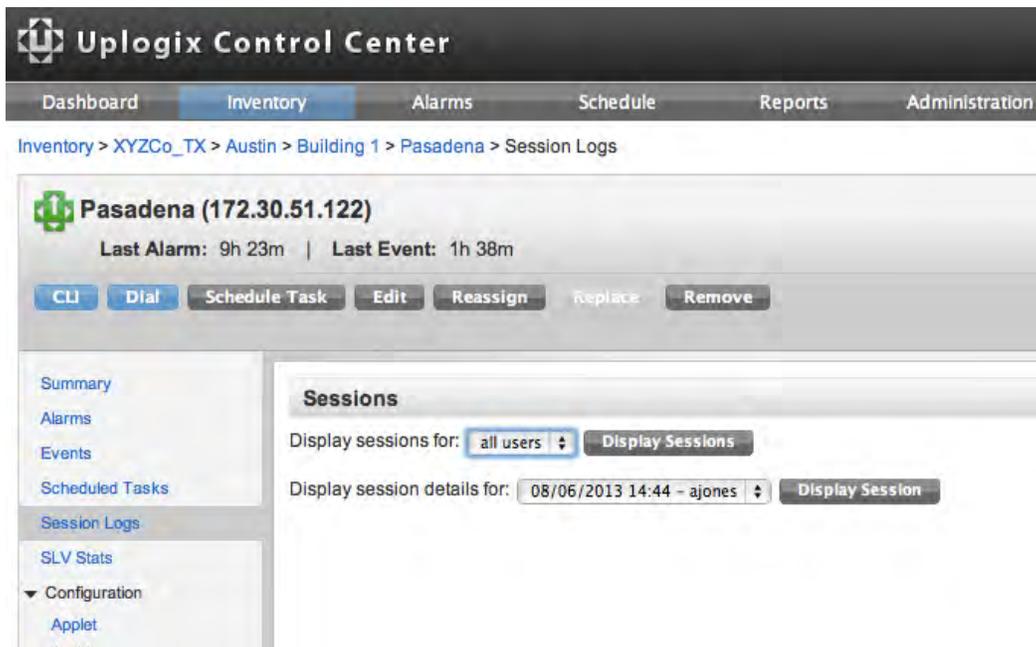
View transcripts of individual LMS command line sessions that have ended. And, configure accounts to receive reports of individual accounts' activities on the Uplogix Control Center.

Local Manager session logs

Inventory > Local Manager Page > Session Logs

Every command line interaction between a user and the Uplogix Local Manager is logged and subsequently archived on both the Local Manager and the Uplogix Control Center. To view archived sessions, click **Session Logs** from the left menu of the Local Manager page.

A list of archived sessions by user can be displayed, just as with the Uplogix LMS command line using the `show sessions` command. Select the user from the list and click **Display Sessions**. To view the details of a listed session, click **Display Session** to the right of the timestamp. This is equivalent to the `show session` command.



Session information is updated every 30 seconds on the Uplogix Local Manager, but the actual recorded transaction is transferred during the archive process.

Session details are not available for sessions in progress.

Auditing user activities on the Uplogix Control Center

Administration > Users > User Name > Auditing

To audit users, your account configuration must include:

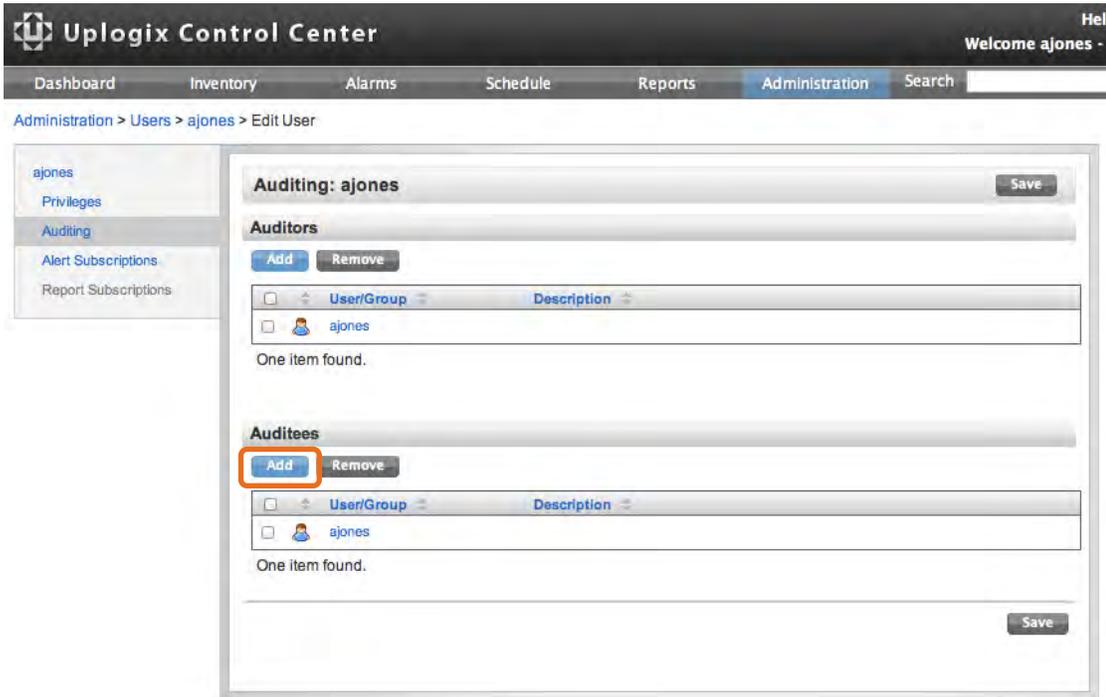
- A valid email address
- The permission to audit the user as one of your auditees
- A report subscription to the appropriate session report on each user to be audited. See [Setting up email, auditing, and subscriptions](#).

The reports are emailed as .pdf, .html, or .csv files.

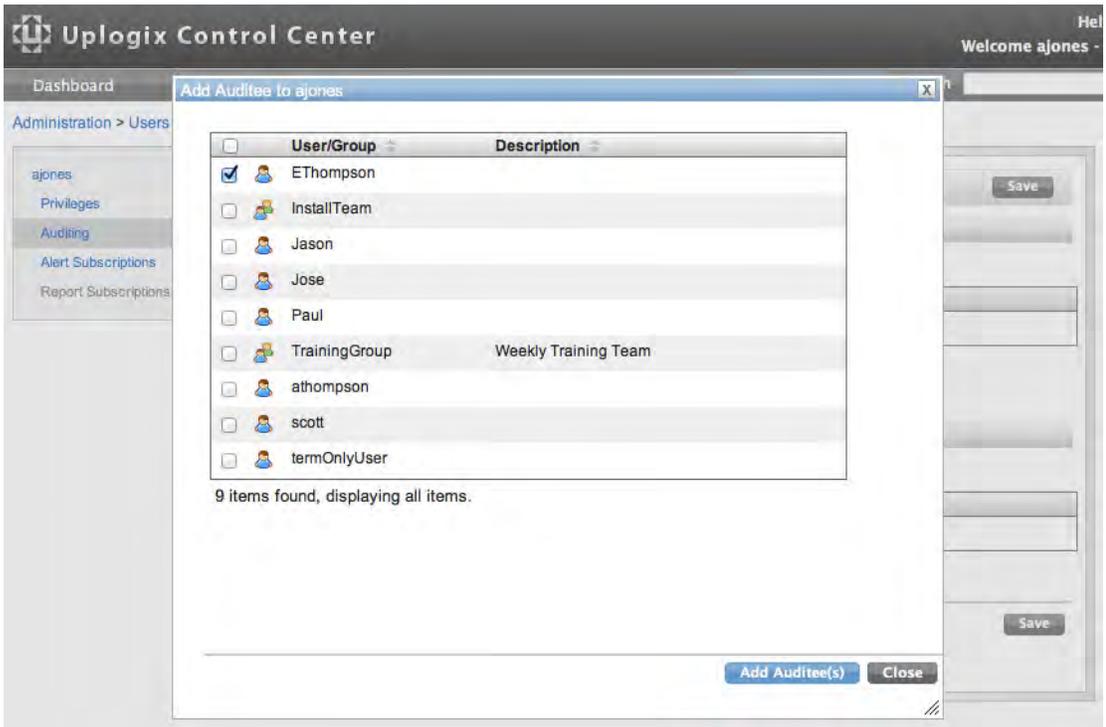
The following example shows how to configure a user to audit another user. In this example, the user `ajones` (who has the admin role on the Uplogix Control Center) will be configured to audit another user, `ethompson`.

Every user account is automatically able to audit itself. To audit others, auditees must be added to the auditor's user profile.

From the Auditing menu, click **Add** under Auditees.



From the pop-up, select the user to be audited, in this case, ethompson and click **Add Auditee(s)**. Click **Save** at the top or bottom of the page and the auditees are added to ajones auditee listing.



The ajones account has an email address, and the user ethompson is now among ajones' auditees, so ajones will be able to subscribe to reports on ethompson.

The next step is to subscribe to the desired reports. Click **Report Subscriptions** from the left menu to go to the Report Subscriptions page.

On the Report Subscriptions page, expand the **Principal Reports** section at the bottom of the Report Subscriptions page.

Select the Principal—the user to be audited. If your account is configured to audit many users, you may wish to enter a filter string to shorten the list of usernames.

Uplogix Control Center

Dashboard Inventory Alarms Schedule Reports Administration

Administration > Users > ajones > Edit User

Report Subscriptions: ajones

WARNING: No subscriptions will be sent until server mail settings are configured. [Server Settings](#)

There are no report subscriptions for ajones.

- ▶ Label Reports
- ▶ Inventory Group Reports
- ▶ Appliance Reports
- ▶ Port Reports
- ▼ Principal Reports

[Subscribe](#)

Principal: **select** Email: ajones@xyzco.com Export Type: PDF Send Blank:

Group	Principal Picker	Export Type	Frequency
<input type="radio"/> Activity	Filter String:	ort,jrxml	HOURLY
<input type="radio"/> Activity		ort,jrxml	DAILY
<input type="radio"/> Activity	EThompson	ort,jrxml	WEEKLY
<input type="radio"/> Activity	ajones	ort,jrxml	MONTHLY
<input type="radio"/> Change		ort,jrxml	HOURLY
<input type="radio"/> Change	Daily	sessionReport,jrxml	DAILY
<input type="radio"/> Change	Weekly	sessionReport,jrxml	WEEKLY
<input type="radio"/> Change	Monthly	sessionReport,jrxml	MONTHLY
<input type="radio"/> Full	Hourly	sessionReport,jrxml	HOURLY
<input type="radio"/> Full	Daily	sessionReport,jrxml	DAILY
<input type="radio"/> Full	Weekly	sessionReport,jrxml	WEEKLY
<input type="radio"/> Full	Monthly	sessionReport,jrxml	MONTHLY

Select the auditor's email address if more than one is available, and choose the file type that will be emailed - .pdf, .html, or .csv. Then **Subscribe** to the desired report.

- Activity reports—include all page views.
- Change reports—include all actions that resulted in changes on the Uplogix Control Center, any Uplogix Local Manager under management, or any device connected to a managed Local Manager.
- Full reports—include all information from both activity and change reports.

Use the radio buttons next to the reports to select which reports to receive and click on the **Subscribe** button. The new subscription is listed at the top of the Report Subscriptions page, and in the Report Subscriptions area of the Edit User page.

Report Subscriptions: ajones

WARNING: No subscriptions will be sent until server mail settings are configured. [Server Settings](#)

[Remove](#)

<input type="checkbox"/> Scope	Group	Name	Resource	To Address	Export	Send Blank
<input type="checkbox"/> Principal	Change	Weekly	ETHompson	ajones@xyzco.com	PDF	false

▶ **Label Reports**

▶ **Inventory Group Reports**

▶ **Appliance Reports**

▶ **Port Reports**

▼ **Principal Reports**

[Subscribe](#)

Principal: select	Email: ajones@xyzco.com	Export Type: PDF	Send Blank: <input type="checkbox"/>	
Group	Name	File	Frequency	
<input type="radio"/>	Activity	Hourly	sessionReport.jxml	HOURLY
<input type="radio"/>	Activity	Daily	sessionReport.jxml	DAILY

Sending logs to Technical Support

Administration > Server Settings

If you contact Uplogix Technical Support about an issue with the Uplogix Control Center, the technical support staff may ask you to send the logs. The Send Logs section at the bottom of the Server Settings page provides a convenient way to do this.

Uplogix Control Center

Dashboard Inventory Alarms Schedule Reports **Administration**

Administration > Server Settings

Server Settings [Save](#)

▶ **Install Information**

▶ **Basic Settings**

▶ **Mail Settings**

▶ **SNMP Settings**

▼ **Send Logs**

Send Logs To:

Verbose:

[Send Logs](#)

Follow the support technician's instructions to send the logs.

Replacing a Local Manager

Inventory > Local Manager Page

If an Uplogix Local Manager stops sending heartbeats, the Local Manager's icon in the inventory changes to gray after four consecutive failures. The default heartbeat interval is 30 seconds.

The detail page for an unresponsive system displays the Replace button.



Click **Replace** for a list of Local Managers that are available to replace the unresponsive Local Manager. To be listed, a Local Manager must be unassigned, running the same software version as the Uplogix Control Center, and communicating properly.

Select a replacement. The unresponsive Local Manager is replaced in the inventory list by the Local Manager selected. The Uplogix Control Center pushes the stored network device configuration from the replaced Local Manager to the replacement.

After the replacement Local Manager is updated, disconnect all devices from the replaced unit and connect them to the corresponding connectors on the replacement.



Local Managers must be replaced with an identical product. For example, an Uplogix 500 must be replaced with an Uplogix 500 for the replacement to work.



The software versions must also be the same. For example, replace 4.6.x with 4.6.x for replacement to work.

Shutting down the Control Center

The Control Center can be shut down or restarted from the CLI using Linux commands.



Caution: Do not remove power from the Control Center while it is running. Failure to shut down properly may result in the loss of data.

Open a console or SSH session with your Control Center and become root. To restart the Control Center, use the `shutdown -r now` command. To shut down the Control Center, use the `shutdown -h now` command.

Using the `shutdown` command ensures that all services exit cleanly before the reboot / shutdown.

Advanced Control Center Functionality

The Uplogix Control Center offers several advanced features to help manage your deployment.

In this chapter:

- [SOCKS Proxy Support](#)—set up and configuration of a SOCKS proxy for device access
- [Serial Port Forwarding Using the CLI Applet](#)—make the console port of the managed device available on a local workstation via reverse SSH tunnel
- [SSH Port Forwarding](#)—access to network services running on the dedicated or management IP addresses of a managed device
- [Manual Out-of-Band Modem](#)—contact remote Local Managers via SMS message to start PPP
- [CLI Applet Failover to Managed Device](#)— open SSH connections to Local Managers that pass through to the console port of a managed device via the CLI Applet
- [CLI Applet SSH Key Authentication](#)—open SSH connections with private key authentication to Local Managers and to managed devices via the CLI Applet

SOCKS Proxy Support

The Uplogix Control Center’s CLI applet supports the use of a SOCKS Proxy server when accessing Uplogix devices. Setting up a SOCKS Proxy allows users to access devices through a proxy to bypass routing and firewall limitations and configure proxy servers for groups and/or individual devices.



A properly configured SOCKS Proxy server is required to use this feature. Contact Uplogix support if you would like to configure a SOCKS Proxy on the Uplogix Control Center.

Arguments

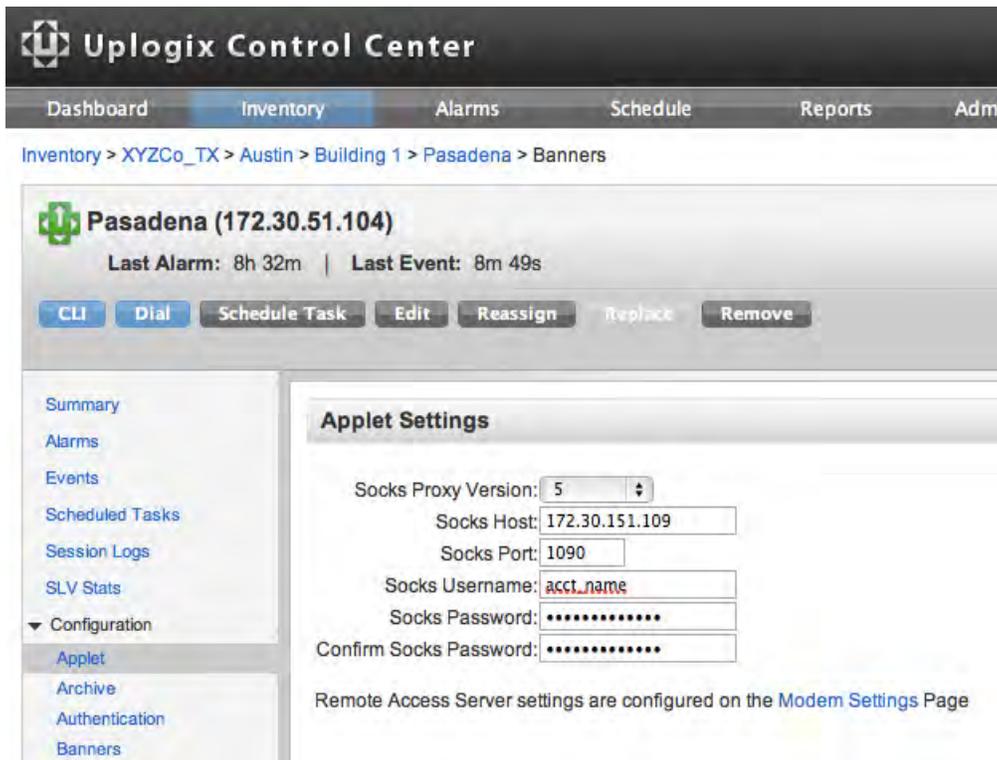
Socks Proxy Version	Both Socks Proxy Version 4 and 5 are supported.
Socks Host	The IP address of the Socks Proxy Server.
Socks Port	The listening port of the Socks Proxy Server. Typical default port is 1080.
Socks Username	Username to authenticate with the proxy server, if required.
Socks Password	Password to authenticate with the proxy server, if required.

Usage

Proxy settings can be configured at the global, group, or individual device level. First, connect to the web interface of the Control Center and navigate to the Inventory page. Select an Uplogix device from the Inventory tree to bring up its detail page. On the left, expand the Configuration menu and select **Applet**.

In this example, the Control Center will be configured to use a socks proxy server with the following configuration:

Version: 5
IP Address: 172.30.151.109
Port: 1080
Username: acct_name
Password: password27



When the Socks Proxy Version is set to disabled, the configuration options will be grayed out. To begin configuring settings, change the Socks Proxy Version to either 4 or 5.

- Version 4: Requires an IP address and a listening port. Since Version 4 does not support authentication, the password field is grayed out.
- Version 5: All configuration options are available with this version. Depending on the configuration of the proxy server, a username and password may be required.

Once you have configured necessary settings, click **Save**.

The Socks Proxy configuration will be transparent to the end user. To test your settings, select a previously inaccessible device from the inventory and launch the CLI applet. A connection to the device should succeed.

If the connection fails, verify that your settings are correct by examining the configuration of the proxy server or by testing with an SSH client such as Putty or SecureCRT.

Serial Port Forwarding

Use the Serial Port Forwarding feature to make the console port of the managed device available on a local workstation via reverse SSH tunnel. In order to utilize this feature, a user must have the `terminal` privilege.

An SSH client with reverse tunnel capabilities is required to use this feature. Supported clients include PuTTY and the CLI Applet on the Uplogix Control Center.

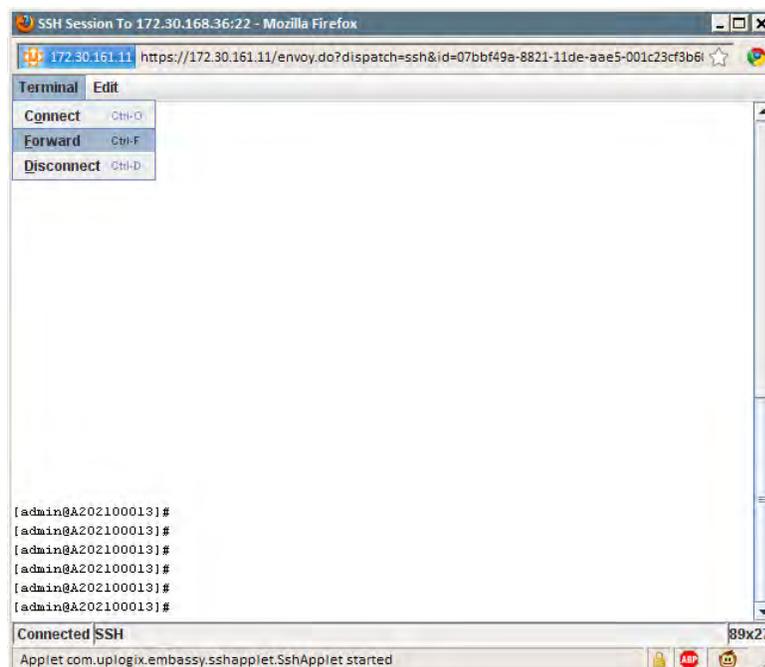
Prior to setting up serial port forwarding, initialize the Local Manager port with the appropriate device driver via the `config init` command. Refer to the appropriate device configuration guide for information.

About Connections

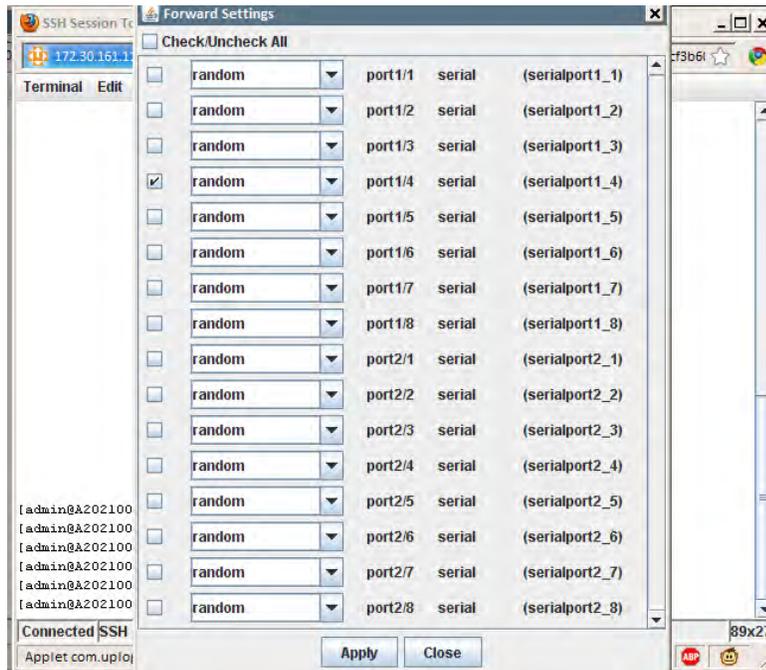
- Only one telnet connection is allowed per forwarded port. Subsequent connections will fail until the first connection is exited.
- The telnet connection can be terminated by quitting the telnet command, exiting the terminal session on the original SSH session, or by closing the SSH client.
- Accessing a forwarded port via telnet bypasses authentication and authorization. These are handled by the original SSH session.
- Connections to forwarded ports are subject to the same idle timeouts as normal terminal sessions. The idle counter is reset if data is passed over the telnet connection.

Usage

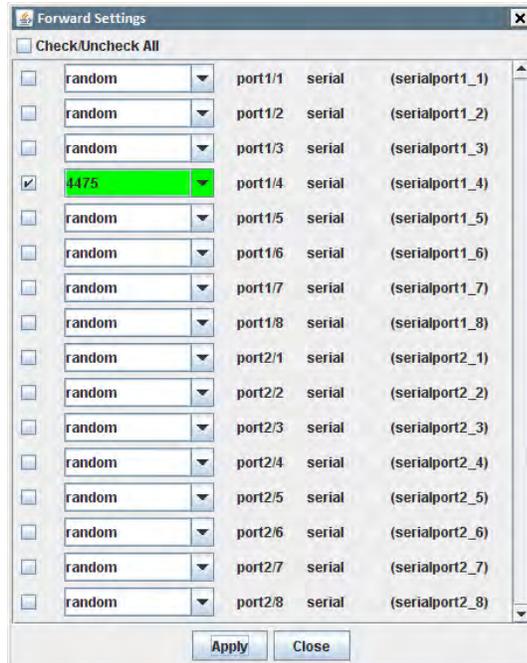
1. Start the CLI Applet by navigating to a device in the inventory tree and clicking on the **CLI** button. Once the applet loads, authenticate with the device and log in.
2. Click on **Terminal** in the CLI Applet menu bar and select **Forward**.



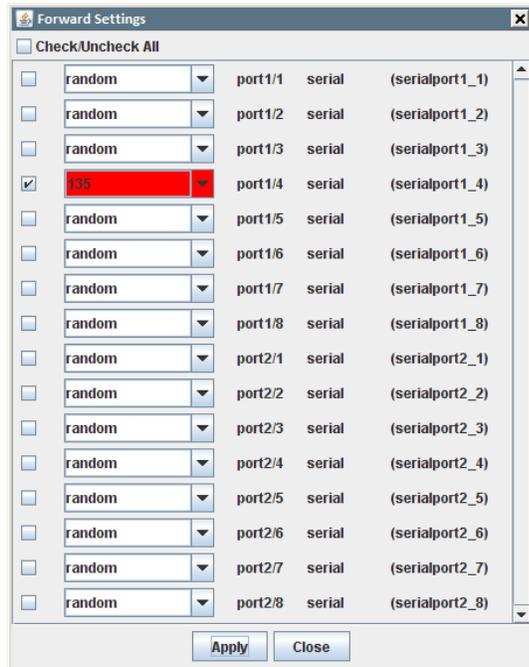
3. Mark the checkbox next to the port you wish to forward. By default, the applet will forward to a random local port. To specify a port, delete random and enter the desired port.



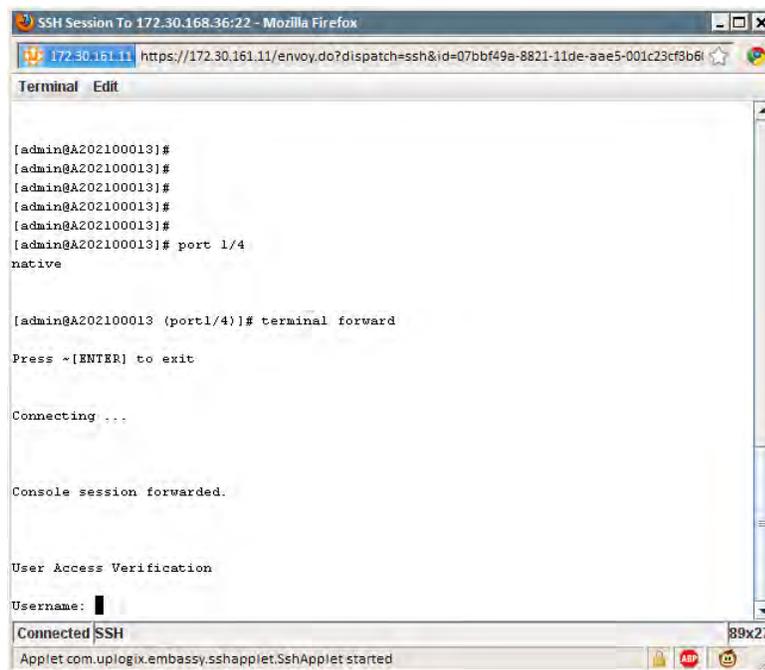
4. Click **Apply** to save your settings. If a random port was assigned, it will be displayed and highlighted in green.



- If you specified an invalid port (in use or conflicting), it will be highlighted in red.



- Click **Close** to return to your SSH session.
- Navigate to the desired port and use the `terminal forward` command to start forwarding.

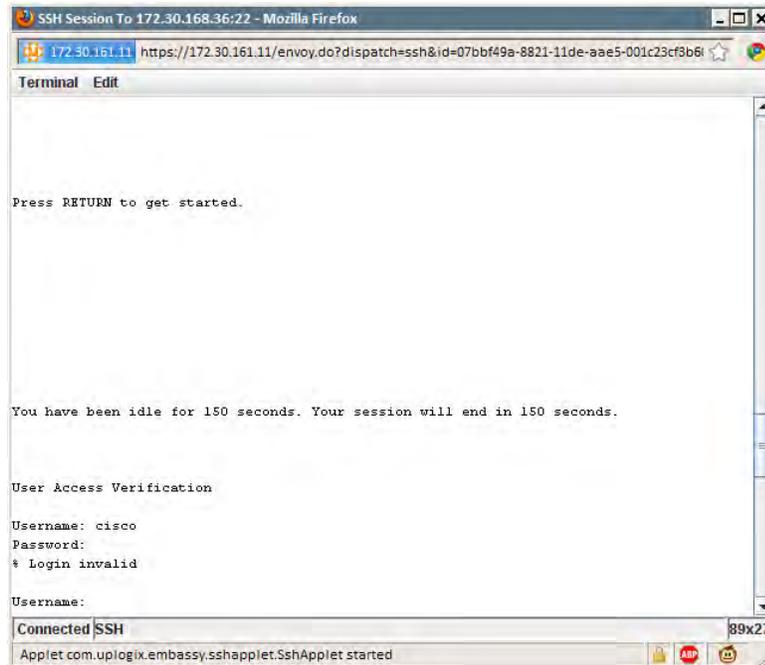


Once the message `Console session forwarded` displays, connect to the forwarded session on your local machine. Telnet to 127.0.0.1 (localhost) on the port specified in step 4 or 5.

```
# telnet 127.0.0.1 4475
Connecting to 127.0.0.1 4475...
```

```
Username: cisco
Password:
% Login invalid
```

8. Anything typed to the forwarded port will be displayed in the original terminal session.



See the *Uplogix Local Manager Guide* for information on how to forward a serial port using PuTTY.

SSH Port Forwarding

SSH port forwarding enables access to network services running on the dedicated or management IP addresses of a managed device. Multiple users on multiple workstations can use SSH Port Forwarding concurrently.

Certain privileges are required to edit or view a port's forward configuration:

- `show protocols forward`—Views the forwarding settings.
- `config protocols forward`—Configures the forwarding settings.
- `forward`—Allows the user to open an SSH session with a tunnel to the forwarded port.

The Uplogix device will attempt to forward incoming TCP traffic regardless of whether the destination is configured properly or not. Ensure the managed device is configured to listen on the port specified.

When using the CLI Applet on the Uplogix Control Center, a Java JRE must be installed on the user's workstation.

Usage

First, connect to the web interface of the Control Center and navigate to the Inventory page. Select an Uplogix device from the Inventory tree to bring up its detail page. Launch the UCC applet by clicking on the **CLI** button.

Configure IP Addresses

The managed device's management or dedicated IP address must be configured on the Uplogix device. This can be configured using `config init` or `config info`.

```
[admin@xyzcoAus (port1/1)]# config init
--- Enter New Values ---
description: []:
<output removed>
management IP: []: 10.10.5.200
Configure dedicated ethernet port? (y/n) [y]:
Use DHCP? (y/n) [n]:
dedicated device IP []: 192.168.1.2
dedicated port IP []: 192.168.1.1
dedicated netmask: []: 255.255.255.252
speed/duplex: [auto]:
<output removed>
Do you want to commit these changes? (y/n): y
```

Configure Port Forwarding

Use the `config protocols forward` command to open the port forwarding configuration editor.

```
[admin@xyzcoAus (port1/1)]# config protocols forward
[forward]#
```

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

```
[forward]# ?
Forward options are:
[no] management {port}
[no] dedicated {port}
[no] events
show
exit
```

[no] management {port}	Enables forwarding to the management IP address and the port specified. The no prefix will remove the forward. Example: To enable traffic forwarding to port 80 on the managed device's management IP address, use <code>management 80</code> .
[no] dedicated {port}	Enables forwarding to the dedicated IP address and the port specified. The no prefix will remove the forward. Example: To enable traffic forwarding to port 80 on the managed device's dedicated IP address, use <code>dedicated 80</code> .

[no] events	Turns on event logging for traffic forwarding. The no prefix will turn off event logging.
Show	Displays the current configuration.
Exit	Exits the configuration editor.

Note that the port specified should match the listening port on the managed device. If the managed device is running an SSH server on its management IP address, forwarding should be configured as management 22.

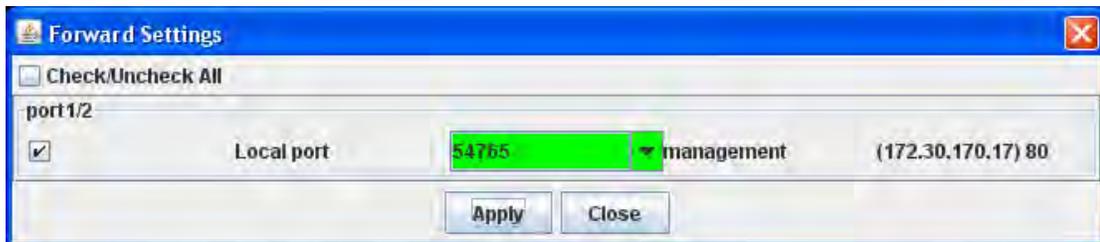
Creating a Tunnel

To use the CLI Applet on the Control Center, navigate to a device in the Inventory tree and click on the **CLI** button. Once the applet has loaded, click on Terminal in the menu bar and select Forward.



In this example, the Uplogix device has already been configured to forward traffic to port 80 at the management IP address for the device on port 1/2. The screen above allows you to select which tunnels to create. On a device with multiple forwards configured, the above list would be longer.

To create a tunnel, check the box next to the port forwards you wish to enable. Then, select a local port to use for forwarding. If random is selected, the applet will select a random port on the workstation. Click **Apply** to save your settings.



If the forward was successful, the drop down box will turn green. If a random port was requested, the port number will be displayed in the green box.

If the drop-down menu turns red, then the tunnel was not created. Double-check the forwarding settings on the target device. Ensure that forwarding is enabled and that the user has permission to forward to that port.

Notes

- Access to forwarded ports is secured by mapping the requested hostname or IP address to a managed device on the device. If forwarding is enabled for two ports that have the same management or dedicated IP addresses, it may be possible for a user to access the forwarded port of a device that they do not have explicit permission for.
- If port forwarding is enabled on the Uplogix device CLI, a full heartbeat must occur before the forward menu will be available in the CLI applet.
- Any tunnels created with an SSH session will be destroyed if the session times out or is exited. To regain access to the tunnel, initiate another SSH session.
- See the Uplogix Local Manager Guide for information on how to SSH port forward using PuTTY.

SMS Outband (PPP on)

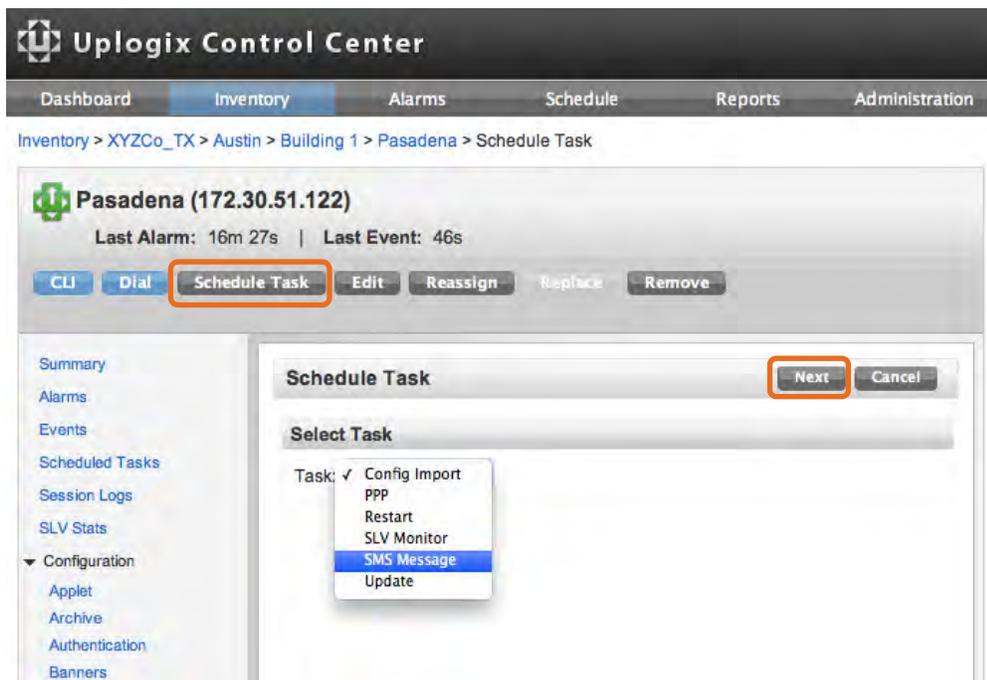
In environments where Local Managers contact the Uplogix Control Center as needed via wireless modem, contact can be initiated from the Uplogix Control Center by sending an SMS message instructing an Uplogix Local Manager to initiate Dial-in.

Requirements for using this capability are:

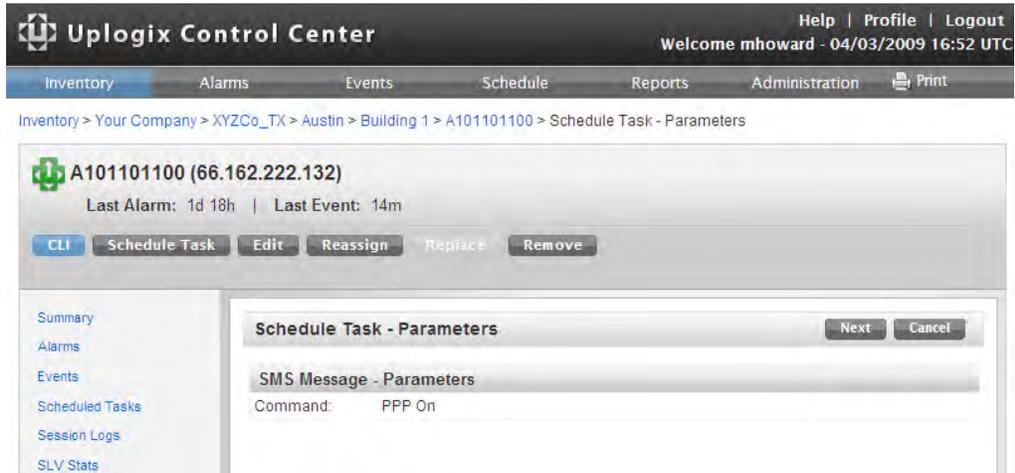
- The Local Manager uses a wireless modem (GPRS/CDMA/Iridium/Inmarsat) modem that supports SMS commands.
- The Local Manager has been configured with a phone number and SMS domain name that the Uplogix Control Center can use to construct a valid SMS email address. These are locally configured with the `config answer` command.

To initiate contact:

1. Select the Local Manager from the Inventory and expand the page to show the Local Manager detail.
2. From the list of tasks that may be scheduled, select **SMS Message** and click **Next**.



- The SMS Message – Parameters page opens. Click **Next** and the **ppp on** command is sent immediately by SMS message. It may take a few minutes before the Uplogix Local Manager receives the SMS message and activates PPP.



CLI Applet Failover to Managed Device

The Uplogix Control Center provides users with the ability to open SSH connections to Local Managers that pass through to the console port of a managed device via the CLI Applet. Under normal circumstances, the CLI Applet establishes an SSH connection to the Uplogix Local Manager. In the unusual event that the applet is unable to establish an SSH connection to the Uplogix Local Manager, the CLI Applet Failover feature allows configuration of the CLI Applet so that it fails over to establishing an SSH connection directly to the managed device.



Many of the valuable Uplogix features such as session logs, events, and configuration rollback become unavailable when the CLI Applet fails over to connecting directly to the managed device, as the Local Manager is out of the connection loop in this scenario.

Device Properties

This feature is activated by adding one or both of the following device properties to the Local Manager port for the managed device.

<p><code>_applet_failover_ssh_fingerprint</code></p>	<p>Defines the SSH fingerprint for the managed device.</p> <p>The CLI applet will only establish a failover SSH connection to the managed device if the fingerprint it receives from the managed device matches the fingerprint value stored in this device property.</p> <p>This property can be configured through the Local Manager CLI and via the Control Center.</p>
--	--

<p>_applet_failover_ssh_ip</p>	<p>Defines the IP address that the CLI applet should attempt to establish an SSH session to in the case where the applet fails to connect to the Local Manager.</p> <p>This property is only required if a management IP address is not defined for the managed device within the Uplogix Local Manager or Control Center.</p> <p>If a management IP address exists for the managed device and this property is not defined, then the CLI applet will attempt the failover SSH connection to the defined management IP address.</p> <p>If this property IS specified/defined, then the CLI applet failover feature will use the IP address contained in this property rather than the management IP address.</p> <p>This property can be configured through the Local Manager CLI and via the Control Center.</p>
--------------------------------	--

The following example walks through the process of configuring CLI Applet Failover to a Cisco 3925 router connected to port 1/2 of the Local Manager.

Determine the SSH Fingerprint for the Managed Device

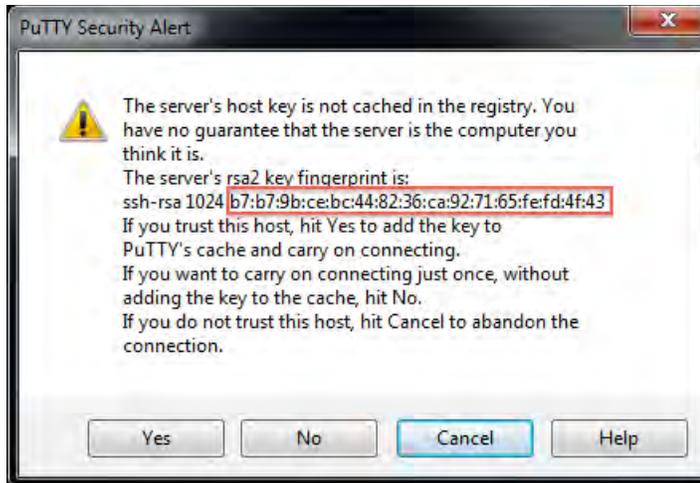
Part of enabling CLI applet failover to the managed device involves configuring the Uplogix Local Manager with the SSH fingerprint of the managed device. Initiate an SSH session to the managed device via a terminal session or application such as PuTTY. The managed device fingerprint will display with a question asking whether to continue connecting. This assumes the PC/workstation does not have the managed device's RSA key in its known host file. If the fingerprint is not presented with a question asking whether to continue, then edit the SSH known host file on your PC/workstation to remove the entry for the managed device. Here is an example using a Linux, Unix or Mac terminal session:

```

/Users/admin > ssh admin@192.0.2.100
The authenticity of host '192.0.2.100 (192.0.2.100)' can't be established.
RSA key fingerprint is b7:b7:9b:ce:bc:44:82:36:ca:92:71:65:fe:fd:4f:43.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.0.2.100' (RSA) to the list of known hosts.

```

An example of the fingerprint in a Putty popup window is shown below:



Copy the SSH fingerprint. It is a required device property that will be set up in the next step.

Configure Device Properties via the Local Manager CLI

Log into the Uplogix Local Manager and navigate to the port that is to be configured for CLI applet failover and enter the device property editor by issuing the following commands:

```
[admin@A400100052]# port 1/2
LRT-3925 cisco CISCO3925-CHASSIS IOS 15.1(4)M
3925
[admin@A400100052 (port1/2)]# config properties
[config properties]#
```

Now configure the `_applet_failover_ssh_fingerprint` device property for the managed device SSH fingerprint (determined in the previous step) with the following command (where there is a space between the property and the fingerprint value):

```
[config properties]# _applet_failover_ssh_fingerprint
b7:b7:9b:ce:bc:44:82:36:ca:92:71:65:fe:fd:4f:43
[config properties]# show
_applet_failover_ssh_fingerprint: b7:b7:9b:ce:bc:44:82:36:ca:92:71:65:fe:fd:4f:43
[config properties]#
```

If there is no management IP address for the managed device configured in the Local Manager, or if the failover IP address that should be used is different from the configured management IP address, then the `_applet_failover_ssh_ip` device property should be configured to specify the failover IP address for the managed device. The Uplogix `show info` CLI command can be used to determine the management IP address for a given device. The following example shows the managed device to have a management IP address of `192.0.2.100`:

```
[admin@A400100052 (port1/2)]# show info
Hostname: LRT-3925
Description: 3925
Make: cisco
```

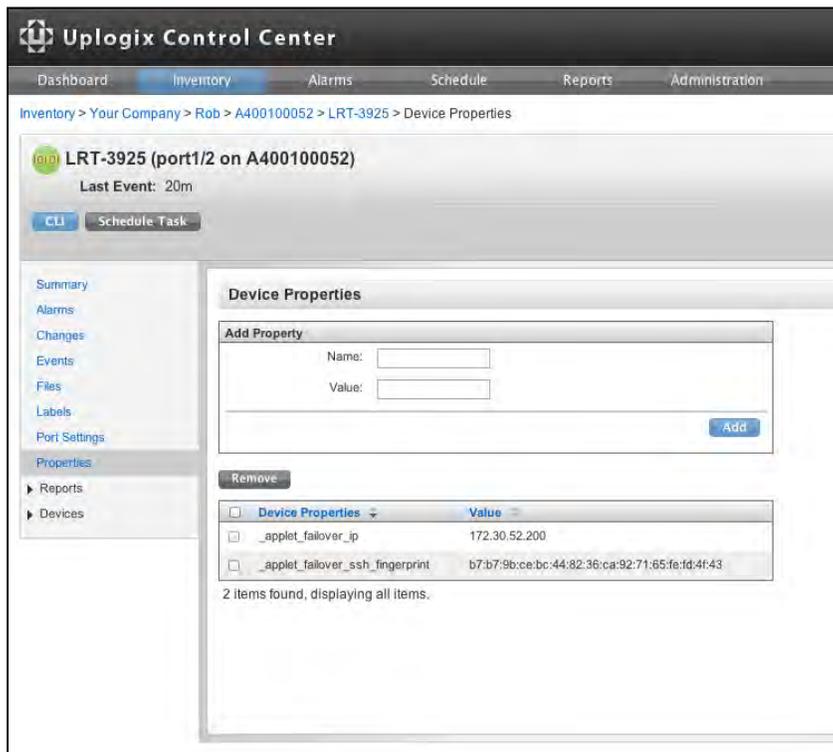
```
Model: CISCO3925-CHASSIS
OS: IOS
OS Version: 15.1(4)M
Management IP: 192.0.2.100
Current CPU Utilization: 0%
CPU Utilization (1 minute average): 1%
CPU Utilization (5 minute average): 1%
Total Memory: 762273884 bytes
Used Memory: 52811412 bytes
Free Memory: 709462472 bytes
```

To demonstrate how to set this device property, suppose that the CLI applet should failover to IP address 192.0.2.200 if a SSH session cannot be established to the Uplogix Local Manager. Issue the following commands to enter the device property configuration editor on the managed device port and set the applet failover IP address:

```
[admin@A400100052 (port1/2)]# config properties
[config properties]# _applet_failover_ssh_ip 192.0.2.200
[config properties]# show
_applet_failover_ssh_ip: 192.0.2.200
_applet_failover_ssh_fingerprint: b7:b7:9b:ce:bc:44:82:36:ca:92:71:65:fe:fd:4f:43
[config properties]# exit

[admin@A400100052 (port1/2)]#
```

Alternatively, device properties can be set via the UCC. Log into the UCC, navigate to the Uplogix Local Manager in the Inventory, click on the port for the managed device in the Device section of the Local Manager summary page, and click the Properties link in the left navigation bar. The following page appears so device properties can be added or deleted:



Usage

Once device properties are configured for a managed device as specified above, the CLI applet failover feature is configured and active. To use the CLI applet to access the console port of a managed device, connect to the web interface of the Control Center and navigate to the Inventory page. Select an Uplogix device from the Inventory tree to bring up its detail page. Launch the UCC applet by clicking on the **CLI** button. Should the CLI applet fail to establish an SSH session to the Local Manager, the applet will then attempt to establish an SSH session directly to the managed device.

CLI Applet SSH Key Authentication

The Uplogix Control Center provides the capability to open SSH connections to Local Managers and to managed devices via the CLI Applet.



Providing public keys to authenticate overrides TACACS/Radius authentication for that user.

Arguments

Authorized Keys	The SSH public key stored in the user profile in the UCC. This key is synchronized to Local Managers with user information.
SSH Private Key File	The path to the SSH private key file on the user's workstation. This path is stored in a cookie in the user's browser and is set via the CLI Applet Terminal->PrivateKey function.

This example walks through the process of configuring CLI applet SSH key authentication for user Norm.

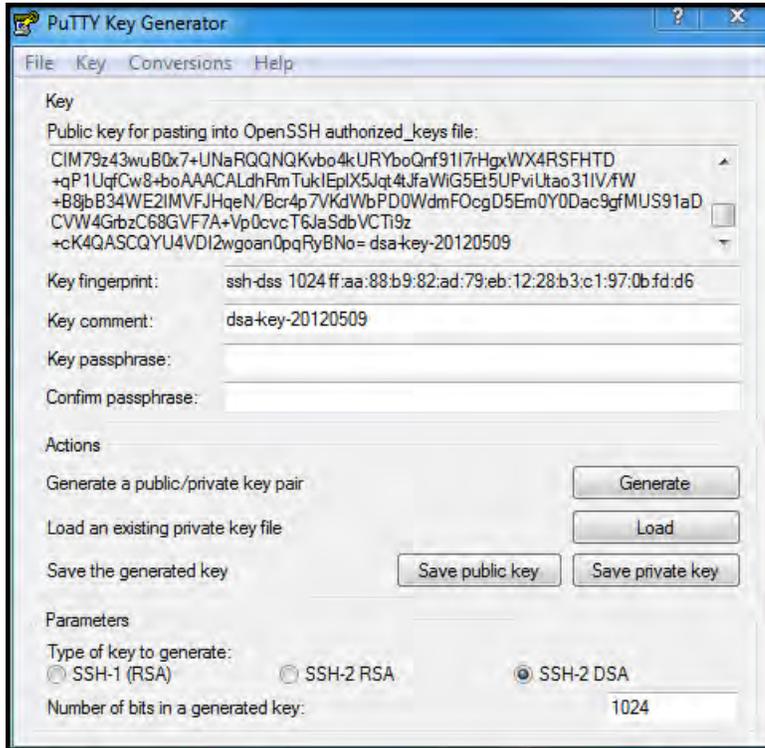
Generate SSH Key Pair on Client Workstation (If one has not been previously created)

If the client workstation (i.e., the workstation that will launch the CLI applet to connect to the Local Manager or managed devices) is running Linux, Unix, or Mac OSX (or is running Windows with a Linux-like environment application like Cygwin), issue the following command in a terminal window to generate the key pair: `ssh-keygen -t dsa`.

```
/Users/admin > ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/Users/admin/.ssh/id_dsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /Users/admin/.ssh/id_dsa.
Your public key has been saved in /Users/admin/.ssh/id_dsa.pub.
The key fingerprint is:
53:6d:4d:bd:5e:45:15:e1:16:45:ad:67:b9:1b:ed:d9 admin@lenovo-2444abfb.uplogix.local
```

If the Uplogix solution is running in FIPS mode, then a “rsa” key must be generated with at least 2048 bits – here is the command to generate this key pair: `ssh-keygen -t rsa -b 2048`.

If the client workstation is running a Windows operating system, the free [puTTYgen tool](#) can be downloaded and used to generate SSH key pairs. An example of this puTTYgen tool is shown below:

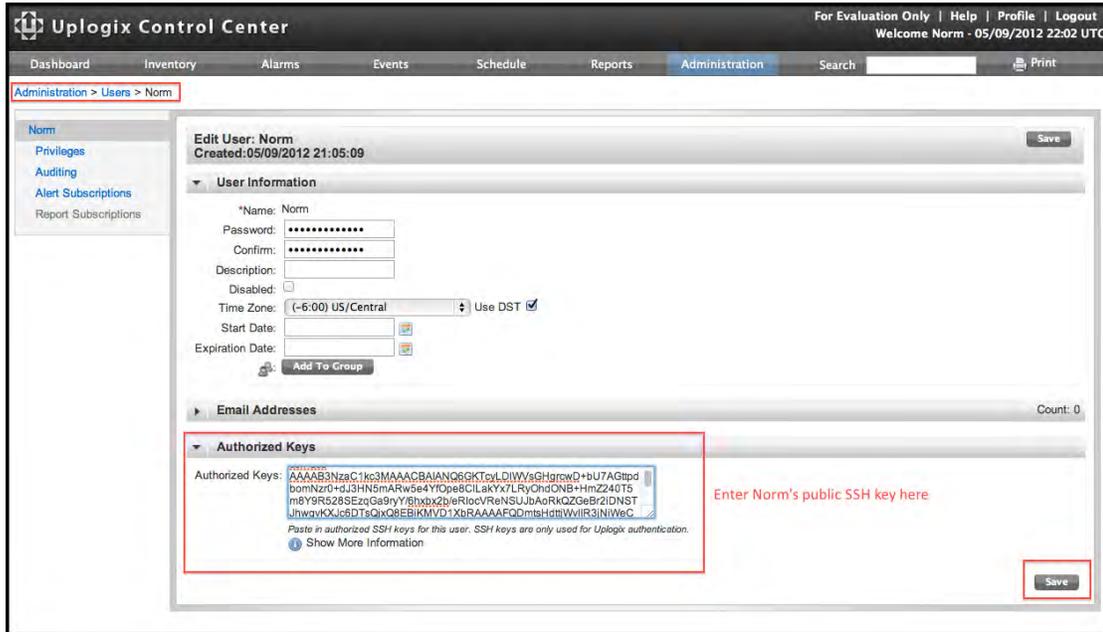


After installing and running the puTTYgen tool, perform the following:

1. In the Parameters section, choose **SSH-2 DSA**, leave the default number of bits set to **1024** and click the **Generate** button for the standard, non-FIPS Uplogix Local Management solution. In the case where the UCC is running in FIPS mode, choose **SSH-2 RSA**, set the number of bits in the generated key to **2048** and then click **Generate**.
2. Move the mouse in the small screen as instructed by the tool during key generation in order to add randomness to the key pair being generated.
3. Enter a key comment to identify the key pair. This is useful when using several SSH key pairs.
4. Do not enter a **Key passphrase** – leave it blank.
5. Click **Save private key** to save your private key. Give the key a filename and confirm that it should have a blank passphrase. Also, note the filename and path, as the location for this private key will be configured in a subsequent step.
6. Click **Save public key** to save the public key and give it a filename.

Add Public SSH key to User in Upligix Control Center

The contents of the SSH public key should be copied and provided to an Upligix Control Center admin if the user does not have privileges to edit their user profile. Next, the user or Upligix Control Center admin should login to the web interface, navigate to the Administration-Users page and then click on the user to be provisioned with the SSH public key. In the example below, the SSH public key for user Norm is pasted into the Authorized Keys text box. Be sure to click **Save** after pasting the SSH public key.

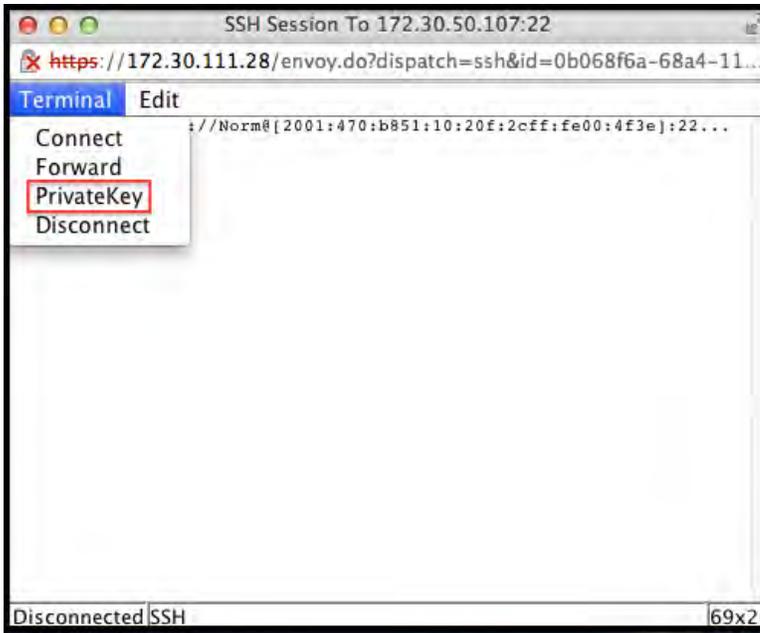


Set SSH Private Key Location in Browser

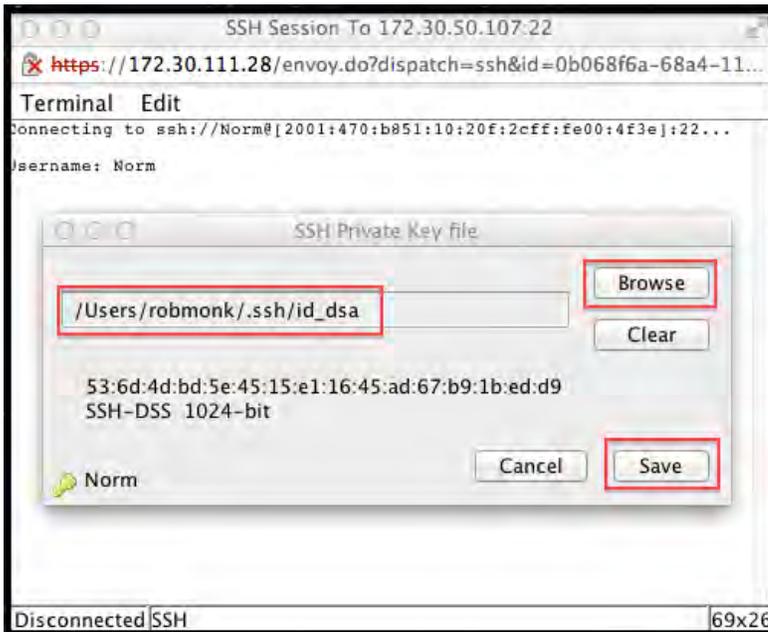
Log into the Upligix Control Center, navigate to a Local Manager, and click on a CLI applet button.

Upon clicking CLI and launching the CLI applet, you may be prompted with a couple windows asking for confirmation that you trust the Upligix Control Center certificate and to allow the CLI applet access to your workstation – you must trust the certificate and allow the applet access to your workstation in order to continue.

Once the applet finishes initializing, click the Terminal menu selection at the top of the screen and then click PrivateKey in the submenu as shown below.



Next, click **Browse** on the popup menu, browse to and select the private key file, then click **Open** to set the path as shown below. Finally, click **Save** to save the path to the private key in an Uplogix cookie in the browser. Close the applet window.



This completes configuration for user Norm – Norm’s public key is stored in the Uplogix Control Center and the path to the private key is stored as a cookie in Norm’s browser.

Usage

Once the private key has been configured as specified above, the CLI applet failover feature is configured and active. To use the CLI applet to access the console port of a managed device, connect to the web interface of the Control Center and navigate to the Inventory page. Select an Uplogix device from the Inventory tree to bring up its detail page. Launch the UCC applet by clicking on the **CLI** button. The applet should establish and authenticate the SSH session without the user having to enter a password.

Note: Alternatively, this failover may be created by configuring a public key in the user profile and a private key in the CLI Applet authenticates subsequent SSH sessions from the user workstation to Local Managers rather than requiring the user to provide a password in the applet window at each login.

Support and Regulatory information

Getting technical support

The Uplogix technical support web site allows you to open and review support requests, browse the knowledge base and download software updates. You must have a user account to view this site.

Requesting an account

To create an account, send an email to support@uplogix.com with the subject line "create account". Include this information:

- organization name
- account user's email address
- user's general contact information

Requesting support

Uplogix provides 24x7x365 support. If you need to contact Uplogix customer support, please provide this information:

- Product model
- Serial number and software version (use the `show version` command from the command line or use the arrow keys on the front panel to scroll through the information on the display)

Phone: 512-857-7070

Fax: 512-857-7002

URL: support.uplogix.com

Providing comments about this guide

Did you find the information you needed?

Was it accurate?

Did it help you?

Please contact our publications staff at support@uplogix.com to notify us of any issues with this guide's accuracy, completeness, or clarity.

We want you to be successful using our products. If you find a problem with this material, we will do our best to fix it.

Index

- A**
- AAA (authentication, authorization, accounting)
 - settings
 - accounting 75
 - authentication 75
 - authorization 94
 - for a single system 73
 - for an inventory node 73
 - global or Uplogix Control Center only 73
 - accounting settings 75
 - accounts
 - configuring to receive email 104
 - created on systems 80
 - deleting 86
 - group 83
 - importing 101
 - subscribing to reports and alerts 104
 - user, creating and editing 81
 - user, disabling 85
 - actions in rules 63
 - adding
 - inventory groups 24
 - systems 27
 - task filters 51
 - adjusting width of inventory display 20
 - admin role 96
 - air flow requirements 4
 - alarms
 - definition 103, 124
 - subscribing to 104
 - using rules to define 63
 - viewing 109
 - alerts, subscribing to 104
 - audit settings 81, 83, 104
 - authentication
 - admin account 75
 - administrator account 72
 - external 75
 - for a single system 73
 - for an inventory node 73
 - global or Uplogix Control Center only 73
 - local 75
 - servers, specifying 75
 - setting password requirements 78
 - TACACS or RADIUS 75
 - authorization keys 81
 - authorization using TACACS ACL 75, 94
- B**
- banner, login 14
- basic configuration 6
- browsers, recommended 9
- button
 - delete including children 26
 - force updates on children 43, 63, 91
 - print 12
 - unavailable 86
- C**
- caching passwords 75
- case sensitivity of logins 9, 11
- changing emsadmin password 7, 8
- child group (definition) 19
- collapsing information 36
- color codes in inventory display 20
- command
 - clear counters 56
 - config answer 38, 132
 - config authentication 56, 75
 - config group 80, 83, 94
 - config group no [username] 86
 - config import 56
 - config init (modem) 38
 - config ppp 38, 42, 56
 - config pptp 42
 - config role 91, 94
 - config rule 63
 - config schedule 36, 50, 51, 56
 - config settings 43
 - config system archive 38, 42
 - config system authentication .. 72, 75, 78, 94
 - config system banner 38, 42
 - config system email 38, 42
 - config system ip 38
 - config system ipt 38, 42
 - config system keypad 38, 42
 - config system management 27, 32, 38, 42
 - config system ntp 38, 42
 - config system protocols 38, 42
 - config system pulse 38
 - config system serial 38
 - config system snmp 38
 - config system syslog-options 38, 42, 117
 - config system timeout 38, 42
 - config user 80, 81, 87
 - config user no [username] 86
 - config vpn 38
 - off 56
 - on 56
 - power 56

push config	56	system chassis	59
push os	56	system dashboard	36
reboot	56	device labels	47
show alarms	109	device syslog	117
show dashboard	36	devices, managing	46
show session	118	disabling user accounts	85
show sessions	118	display	
show status	36	license support	13
show tech	56	software version and build	13
show version	142	DNS server, configuring	6
compatibility, system/management server		DST (daylight saving time)	15
software version	1, 18	E	
concurrent sessions, limiting	75	email address	
conditions in rules	63	to contact Uplogix technical support	142
connections		to receive alerts	81, 83, 104
Ethernet	5	user, deleting	81
management console	5	emsadmin user	6
power	5	Envoy privileges	87, 90, 91
contacting a remote appliance from Uplogix		events	
Control Center	132	definition	103, 124
conventions, typographical	1	using rules to define	63
creating		expanding chassis and port information	36
group accounts	83	expired passwords, resetting	80
inventory group	24	external authentication	75, 94
placeholders for systems	27	F	
roles	91	Failover	133, 134
rule sets	66	features of inventory group detail page	21
rules	63	files	
task filters	51	permission	86, 87
user accounts	81	system software upgrade	60
D		filter manager (scheduled tasks)	51
daylight saving time (DST)	15	filters, task	51
default console settings	6	force updates on children (button) ...	43, 63, 91
default login		G	
Uplogix Control Center CLI	6	gateway, Uplogix Control Center, configuring.	6
Uplogix web interface	9	group accounts	
default port settings	43	creating	83
default settings, system	42	deleting	86
definitions		importing	101
alarm	103, 124	naming	11
child group	19	subscribing to reports	104
event	103, 124	group, inventory	
inventory group	19	about	19
log	103, 124	adding	24
monitor	63	adding systems	27
permission	86	configuring systems	42
privilege	86	deleting	26
report	103, 124	detail page features	21
role	86	editing name and description	23
rule	63	naming requirements	24
rule set	63	reassigning (moving)	25
strong password	78	root, renaming	23
delete including children (button)	26	Unassigned	22
deleting		viewing	20
accounts	83, 86	grouping	19
inventory groups	26	groups of rules (rule sets)	66
systems	32	I	
detail view		icons in inventory display	20
port	46, 117	importing	

group accounts	101
privilege lists	101
user accounts	101
inactivity timeout	15
inheritance	43
initiating contact with a remote appliance	132
inventory	
icons and color codes	20
privileges	86, 87, 90, 91, 94, 96
structure	19
inventory group	
adding	24
adding systems	27
configuring systems	42
definition	19
deleting	26
detail page features	21
editing name and description	23
naming requirements	24
reassigning (moving)	25
root, renaming	23
Unassigned	22
viewing	20
IP address, Uplogix Control Center, configuring	6
L	
labels	47
license support	13
licenses	33, 34
limiting concurrent sessions	75
local accounts	80
local authentication	75
login banner	14
login, default	
Uplogix Control Center CLI	6
Uplogix web interface	9
logs	
definition	103, 124
device syslog, viewing	117
session, viewing	118
M	
managing devices	43, 46
managing inventory groups	42
modem, Iridium	132
monitors	
creating and scheduling	67
definition	63
mounting	5
moving a system	31
moving an inventory group	25
N	
naming requirements	
accounts, roles, and rules	11
inventory groups	24
netmask, Uplogix Control Center, configuring	6
NTP server, configuring	6
number of concurrent sessions, limiting	75
O	
organizing appliances by group	19

P	
packing list	5
parts of the web interface	10
passwords	
administrator, default	9
caching	75
emsadmin, changing	7, 8
expired, resetting on system CLI login	80
strong	78
user, setting	81
permission (defined)	86
placeholder for system	27
port detail	46, 117
port settings, default	43
port, TCP	
RADIUS	75
TACACS	75
ports, managing	43, 46
power	
connecting	5
requirements	4
precautions, safety	2
print button	12
privileges	
assigning	86, 87
by Envoy resource	87
by label	47
creating and editing	91
definition	86
deleting	87, 90
importing	101
inventory	96
managing with TACACS ACL	94
required for configuring systems	38
server	86
viewing	90
Q	
quick search	
inventory	20
username	81
R	
reassigning	
inventory groups	25
system	31
removing	
accounts	83, 86
inventory groups	26
systems	32
renaming the inventory root group	23
replacing a system	122, 123
reports	
by label	47
definition	103, 124
subscribing	104
requirements	
air flow	4
naming accounts, roles, and rules	11
naming inventory groups	24
power	4

temperature	4	reassigning (moving)	31
roles		replacing	122, 123
admin	96	scheduling tasks	59
assigning	86, 87	searching by hostname	20
by Envoy resource	87	upgrading software	60
by label	47	viewing summary	36
defined	86	system, configuring	38, 42
naming requirements	11	system/management server software version compatibility	1, 18
root inventory group, renaming	23	T	
rule sets		TACACS	
creating and editing	66	accounting settings	75
definition	63	ACL	94
rules		servers, specifying	75
creating and editing	63	task filters	51
definition	63	tasks, scheduling	50, 67
in monitors	67	TCP port	
naming requirements	11	RADIUS	75
S		TACACS	75
safety precautions	2	technical support email address	142
satellite modem	132	temperature requirements	4
scheduling		terminal clients (list)	6
monitors	67	timeout for inactive sessions	15
software upgrade, system	60	Timezone (setting)	15
tasks	50, 51, 59	typographical conventions	1
screen, login	14	U	
searching		Unassigned inventory group	22
inventory	20	unavailable features	86
list of users	81	upgrading system software	60
secure shell clients supported (list)	7, 8	use DST (setting)	15
serial settings, management console defaults	6	username	
server privileges	86, 90, 96	case sensitivity	9, 11
service clearance	4	naming requirements	11
service level verification (SLV) license	33, 34	users	
session timeout	15	auditing	81, 104
sessions	118	creating and editing	81
site requirements	4	deleting	86
SLV (service level verification) license	33, 34	disabling accounts	85
SMS message	59, 132	importing	101
software version compatibility,		subscribing to reports and alerts	104
system/management server	1, 18	V	
software version display	13	ventilation requirements	4
software, system, upgrading	60	version compatibility	18
space character	11	version display	13
SSH clients supported (list)	7, 8	viewing	
SSH Key Authentication	137	alarms	109
strong passwords	78	device syslog	117
structure of inventory	19	inventory groups	20
subnet mask, Uplogix Control Center,		license support	13
configuring	6	sessions	118
subscribing to reports and alerts	104	software version	13
superuser	96	W	
suspending user accounts	85	web browsers, recommended	9
syslog, viewing	117	web interface, page structure and navigation	10
system		width control, inventory display	20
adding	27	window, login	14
adding more than 10	33, 34	Y	
deleting	32	Your Company inventory group, renaming	23
port detail	46, 117		