User's Guide

for the Uplogix Control Center Element Management System

Version 4.0

March 2009

UP500030 Rev A

www.uplogix.com

Information in this document is subject to change without notice.
© 2009 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
What's new in this guide 3

Installation and configuration 5
Site requirements 5
Unpacking and installation 6
Unpacking the shipping box 6
Installing the server in a rack 6
Connecting power 6
Connecting the Ethernet port 6
Connecting the management console port 6
Provisioning 7
Completing access and security setup 8

Working with the web interface 9
Logging in 9
Navigating the web interface 10
Entering information 11
Printing 11
Getting help 12

Managing the Uplogix Control Center 13
Setting the time zone and session timeout 14
Daylight Saving Time adjustment 14
Web session timeout 14
Configuring email settings 15
Configuring SNMP settings 16

Managing the deployment 17
About inventory groups and inheritance 17
Viewing the inventory 19
Organizing inventory groups 19
About the Unassigned group 20
Editing an inventory group 22
Adding an inventory group 23
Reassigning an inventory group 24
Deleting an inventory group 25
Adding an appliance 26
Reassigning an appliance 31
Deleting an appliance 32
Managing licenses 33

Managing the equipment 35
Creating default appliance settings 36
Managing from the appliance detail page 37
The summary view 38
Configuring an appliance 39

Creating default port settings 41
Managing from the port detail pages 43
Creating your own categories for managing devices 45
Creating port labels 45
Assigning privileges by label 46
Setting up task filters using labels 48
Viewing reports by label 49
Reestablishing contact with an appliance that connects via Iridium modem 50
Managing scheduled tasks 51
Setting up filters and scheduling tasks 51
Tasks that can be scheduled 58
Scheduling tasks on a single appliance 60
Scheduling software upgrades on Uplogix appliances 61
Managing rules and monitors 65
Working with rules 65
Working with rule sets 69
Scheduling monitors 71
Canceling monitors 74

Managing accounts and security 75
Managing authentication 75
Setting authentication globally or within the inventory 76
Authentication, authorization, and accounting (AAA) settings 78
Setting requirements for strong passwords 82
Working with user and group accounts 84
Creating and editing user accounts 85
Creating and editing group accounts 87
Disabling user accounts 89
Deleting accounts 90
Managing privileges 91
Adding server privileges to accounts 92
Adding inventory privileges to accounts 92
Viewing and deleting user account privileges 96
Creating and customizing roles 96
Using TACACS to manage privileges 99
Example: Creating a superuser 102
Example: Limiting a user's access to one port on one system 104
Importing user, group, and privilege files 108

Logs, reports, and diagnostics 111
Setting up email, auditing, and subscriptions 112
Configuring an account to receive email from the Uplogix Control Center 112
Configuring the account to audit others and to be audited 114
Subscribing to alerts 114
Subscribing to reports 115
Specifying when and how often the subscriber receives alerts 116
Viewing alarms and events 118
Viewing reports 120
Inventory group reports 120
Appliance reports 121
Reports by label 123
Report files 123
Report assignments 124
Viewing archive status information for an appliance 126
Viewing temperature statistics 128
Viewing device syslogs 129
Viewing session logs and auditing users 130
Appliance session logs 130
Auditing user activities on the Uplogix Control Center 130

Troubleshooting 135
Sending logs to Technical Support 136
Replacing an appliance 136

Support and regulatory information 139
Getting technical support 139
Requesting support 139
Providing comments about this guide 139
Regulatory notices 139
Safety notices 139
EMC notices 140
RoHS compliance 140
CE Mark R & TTE directive 140

Index 141

About this guide

This guide describes how to install and work with the Uplogix Control Center element management system (EMS).

Additional documentation is available at www.uplogix.com/support.

Information in this document is subject to change without notice.

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

Examples:
An Uplogix Control Center running version 3.5 or earlier software cannot manage Uplogix appliances that have been upgraded to version 4.0 software; nor can an Uplogix Control Center running version 4.0 software manage Uplogix appliances that are still using version 3.5 or earlier software.

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

Target audience

This guide is 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 RMOS command line is presented in `this font`. Text that you enter is presented in **`this font`**. For example:

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

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

Safety summary

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

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

Read and understand the following instructions before using the appliance:

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

SAVE THESE INSTRUCTIONS.

What's new in this guide

This section summarizes the major changes in this manual for version 4.0.

With this release, Uplogix is pleased to introduce an improved user interface on the Uplogix Control Center for better navigation and increased scalability for up to 250 SRM appliances and 8,000 devices in typical configurations.

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

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 appliance's ventilation openings

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

Unpacking and installation

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

Unpacking the shipping box

Verify that you have received the following items:

- Uplogix Control Center enclosure
- Power cords
- Software pack

Installing the server in a rack

The Uplogix Control Center element management system is designed to be installed in a 19-inch rack. Follow the instructions supplied with the mounting brackets.

Warning: 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:

Connect the server to a suitable power source. The Uplogix Control Center uses dual power supplies for redundancy. 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.

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

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

Connecting the Ethernet port

Connect Ethernet port Gb2 of the Uplogix Control Center to your LAN. The Ethernet port supports up to gigabit speeds.

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, N, 8, 1.

Provisioning

Configure the Uplogix Control Center in one of these two ways:

- Connect a standard VGA monitor, a keyboard and a mouse
- Configure using the console port – Connect 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)

Note: 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 in to the Uplogix Control Center using the **emsadmin** user account. The default password is **password**. The server presents a prompt asking if you would like to run setup.

```
tmcmillan ~ $ ssh emsadmin@172.30.111.40
emsadmin@172.30.111.40's password:
Run Setup? (y/n) [y]
Install multi application servers? (y/n) [n]
Interface eth0 IP Address: 172.30.111.40
Interface eth0 Gateway: 172.30.111.254
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: 172.30.4.252
Secondary DNS Server IP: 172.30.4.253
Tertiary DNS Server IP:
Configure NTP? (y/n) [n] y
NTP Server: 172.30.235.254
Change emsadmin password? (y/n) [n]
Commit? (y/n) y
***** Editing /etc/sysconfig/network-scripts/ifcfg-eth0 *****
  Gateway '172.30.111.254'
  Netmask '255.255.255.0'
  IP Address '172.30.111.40'
(output removed)
```

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

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

```
[emsadmin@172.30.238.20 ~]$ logout
```

Note that if you set or changed the server's hostname, the change will not appear in the command prompt until your next session.

Completing access and security setup

The Uplogix Control Center uses Secure Shell (SSH) Version 2 software to provide secured remote access. Your remote client application must also support SSH v2. Use your SSH client to initiate a secure remote connection to the server.

Note: 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@10.20.234.1
```

Note: The first time your SSH client connects to an SSH host, 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 for the system, change the emsadmin password after you log in the first time. Use the UNIX **`passwd`** command:

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

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

Working with the web interface

The Uplogix Control Center element management system (EMS) provides a web interface. Recommended browsers include Internet Explorer 7.0 or later and Firefox 3.0 or later, with 128-bit encryption.

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
- Getting help - forms of help available

Logging in

The Uplogix Control Center provides a web interface. Recommended browsers include Internet Explorer 7.0 or later and Firefox 3.0 or later, with 128-bit encryption.

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

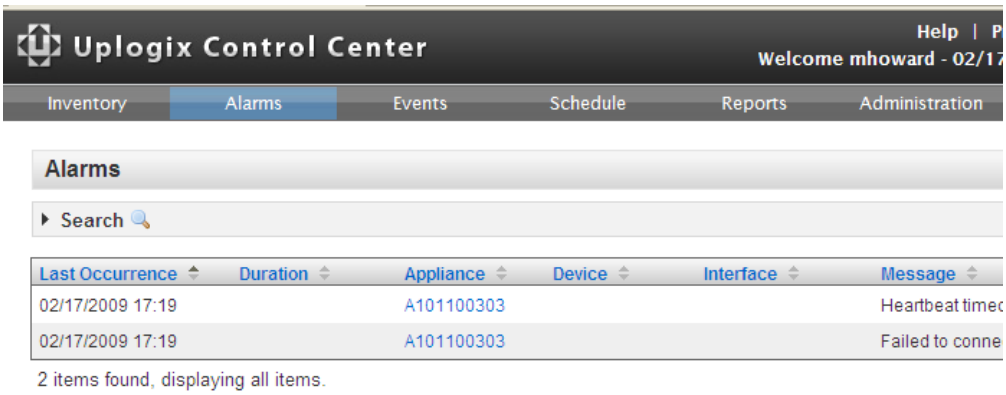
Note: Your browser is likely to present a strong warning stating that the site's security certificate was issued for a different IP address. This is normal.

The browser displays the login screen. Log in using your username and password. Both are case-sensitive. If you are setting up the Uplogix Control Center for the first time, log in using the default username and password:

User Name: **`administrator`**
Password: **`password`**

Note: For security, you should immediately change the administrator's password. For information on setting passwords, see Creating and editing user accounts on page 85.

You will see the Alarms page when you log in.



Navigating the web interface

The Uplogix web interface presents four areas – the **information bar** at the top of the window, navigation bar containing the six main tabs, contextual left navigation, and work area.

The **navigation bar** highlights the main area where you are working. Each of the tabs provides access to a set of related tasks and information:

- **Inventory** – Shows the organization of your Uplogix deployment, including inventory groups and individual Uplogix appliances.

- **Alarms** – Shows a summary of active alarms. **Events** – Shows recent events for all Uplogix appliances managed by the Uplogix Control Center.
- **Schedule** – Allows you to define actions that are 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 is displayed for the following tabs: Schedule, Reports, Administration, and Inventory (at all levels below the topmost inventory level). The **work area** shows the main or default page for the active tab.

Note: The privileges assigned to your account determine which controls are available to you. Unavailable items appear in gray. Tooltips informing you of the missing privilege will appear as you mouse over items in gray.

The Uplogix Control Center pages provide breadcrumb navigation at the top of the work area. For example, when you are viewing the Detail Page for an Uplogix appliance, you see a navigation display something like this:

Inventory > XYZco_TX> Region 1 > A101100303

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.

Entering information

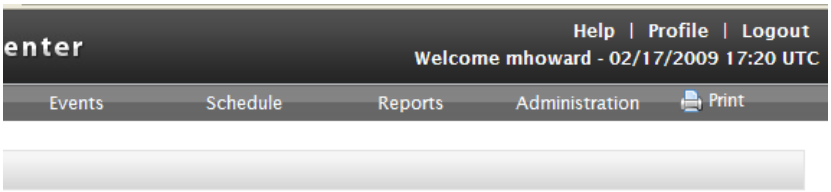
Some features require you to enter text - for example, when you create a user account, you must enter a user name and you may choose to enter a description.

Use only printing characters to complete text fields. You may use spaces in descriptions, but not in naming accounts, roles, or other information that users may work with from an individual appliance's command line.

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

Printing

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

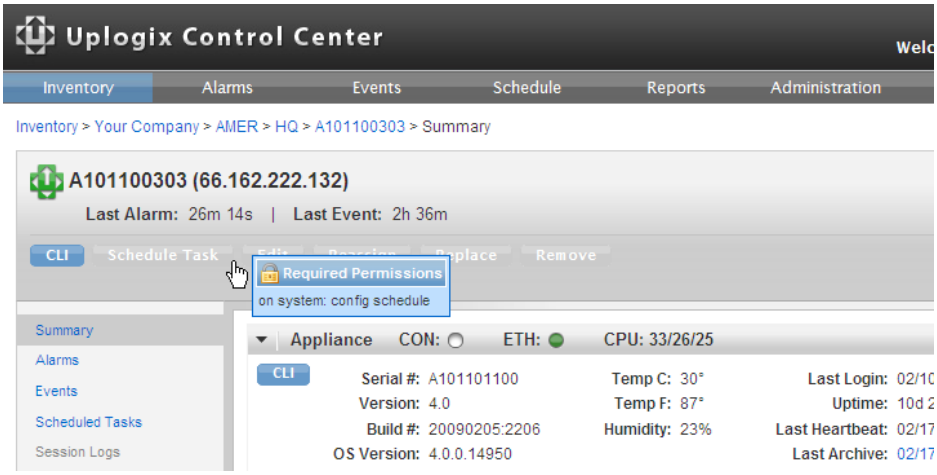


This allows you to print the current contents of the work area. If you have a suitable printer driver installed, you can use the Print icon to save the current view as a PDF file.

Getting help

Some features provide help. Move the cursor over the symbol to display more information.

Depending on your privileges, some controls and links may not be available. These appear in gray. Mouse over an unavailable item to see what commands your role would need to include to make this item available to you.



The Help link in the upper right corner of the window provides access to this guide.

Managing the Uplogix Control Center

This chapter describes the selections under Server Settings on the Administration menu.

The install information lists the version of software currently installed, the software build, date of software installation, and the number of appliance licenses on the server.

This chapter covers:

- Setting the time zone and server session timeout
- Setting the login banner - add a custom message on the login screen
- Configuring email settings - specify a mail server and originating address for outgoing messages
- Configuring SNMP settings - specify an SNMP server

Setting the time zone and session timeout

Administration > Server settings > Basic Settings

System time is normally provided by an NTP server. You can set or change the IP address of the NTP server when you run the setup script. See Provisioning on page 7.

Daylight Saving Time adjustment

Although the Uplogix Control Center element management system uses UTC in timestamps for alerts and events, you can set it to show local time in generated reports. Select **Use DST** if this location uses Daylight Saving time.

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 **Server session timeout**. You can set the timeout to any integer value from 5 to 1440 minutes (24 hours).

The session timeout for Uplogix appliances is set separately. To set the appliance timeout across the inventory or within an inventory group, see Creating default appliance settings on page 36. To set the timeout on individual appliances, see Configuring an appliance on page 39.

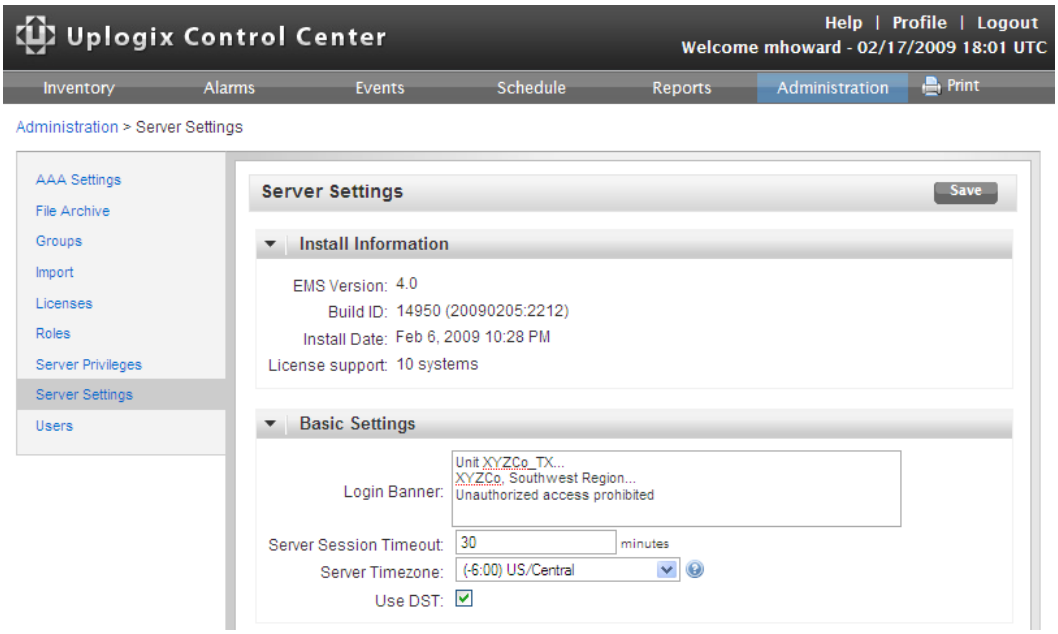
Note: If your session times out, you will be logged out but any operation in progress will not be affected. When you log in again, you are returned to the same page.

If you are finished making changes on this page, click **update** at the bottom of the page to save your changes. Setting the login banner

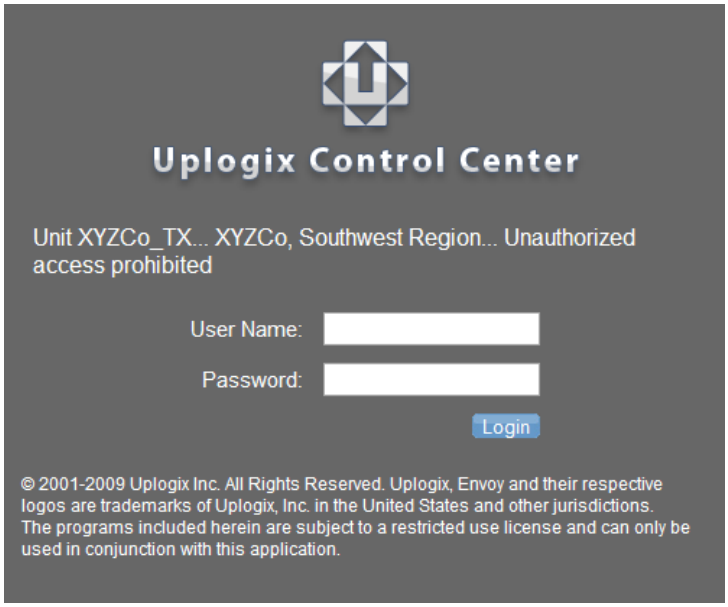
Administration > Server settings > Basic Settings

You can specify text to be displayed in the Uplogix Control Center login window. Line breaks that you enter in this text box will be ignored.

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



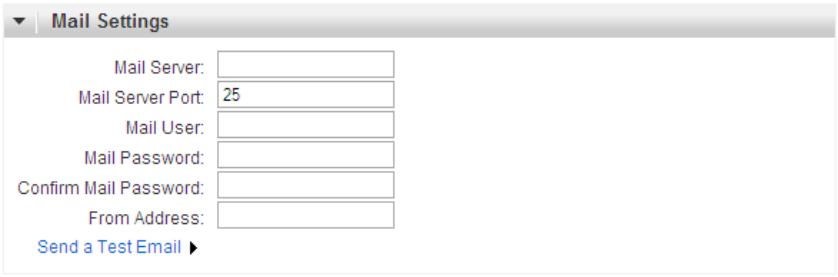
If you are finished making changes on this page, click **save** at the top or bottom of the page to save your changes. The new banner is displayed on the login screen.



Configuring email settings

Administration > Server settings > Mail Settings

To allow the Uplogix Control Center to send alerts and reports by email, configure a mail server with a valid IP address and authentication settings. For more information on using this capability, see Setting up email, auditing, and subscriptions on page 112.



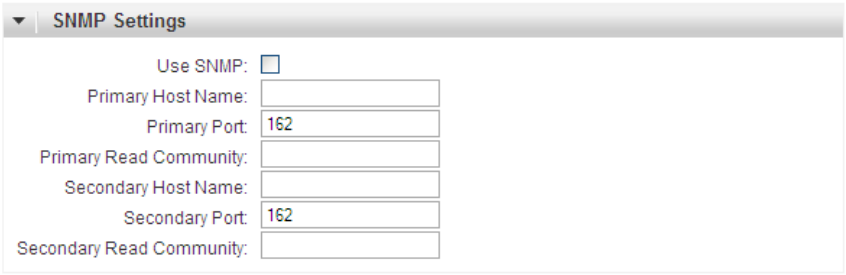
To verify that you have configured the email settings correctly, click **Send a Test Email** to open the test email form. At a minimum, provide a valid email address where the test message should be received. Click the **send test email** button to send the message.

If you are finished making changes on this page, click **save** at the bottom or top of the page to save your changes.

Configuring SNMP settings

Administration > Server settings > SNMP Settings

During normal operation, the Uplogix Control Center receives SNMP trap information from managed Uplogix appliances. If you have set up a third-party SNMP management tool to listen for SNMP traps, the Uplogix Control Center can be configured to forward any traps it receives. SNMP messages from Uplogix appliances will show the IP address of the managed appliance as their source.



If you are finished making changes on this page, click **save** at the bottom or top of the page to save your changes.

Managing the deployment

The Uplogix Control Center element management system provides a central location for the configuration and monitoring of deployed Uplogix appliances. This chapter describes the organization scheme, CLI to GUI relationships, and appliance-specific data display.

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

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

Examples:
An Uplogix Control Center running version 3.5 or earlier software cannot manage Uplogix appliances that have been upgraded to version 4.0software; nor can an Uplogix Control Center running version 4.0 software manage Uplogix appliances that are still using version 3.5 or earlier software.

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

This chapter covers:

- Organizing the deployment - the inventory tree
- 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 appliances among them
- Managing licenses - applying licenses you purchase

For most of the tasks described in this chapter, you will need a role on the Uplogix Control Center that includes the `config inventory` privilege, such as the `admin` role. For more information, see Adding server privileges to accounts on page 92 and Adding inventory privileges to accounts on page 92.

About inventory groups and inheritance

The Uplogix Control Center element management system allows you to manage Uplogix appliances by group, allowing you to define and apply user roles, rules, and tasks across large numbers of appliances in physically separate locations, without the need to repeat the same operations on each unit and without the risk of introducing the variations that can occur during manual operations.

Grouping Uplogix appliances allows you to treat all members of any inventory group in the same way, while allowing you to treat each inventory group differently. Many of the tasks that the Uplogix Control Center EMS manages – such as assigning user roles and defining rules – can be done 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.

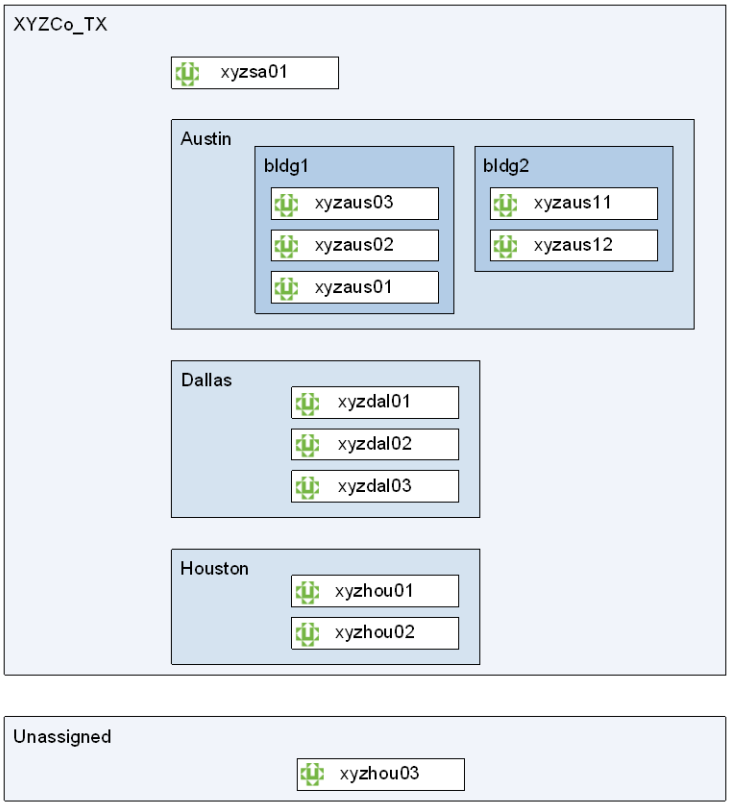
By default, the server provides the Your Company root group, which you may rename, and the Unassigned group, which is not editable. Neither of these can be deleted.

You can create new inventory groups within the root group. These child groups may also be nested. Groups may be based on any criteria that help to organize your deployment. You may reassign Uplogix appliances from one group to another at any time.

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

The inventory groups Austin, Dallas, and Houston have all had Uplogix appliances added. In the case of the Austin inventory group, each appliance have been added to one of the two child group within Austin. One Uplogix appliance, xyzsa01, has been assigned directly to the root group.

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



You can create a collection of default port settings for Cisco model 2610 within the **Austin** inventory group of **XYZCo_TX**. All appliances within the Austin inventory group and all child groups inherit these default port settings.

If you add an appliance to the **bldg2** group, it inherits the Cisco 2610 default port settings from the Austin group. Similarly, if you add a child group to the bldg2 group, it also inherits the Cisco 2610 default port settings from its parent group.

If a child group - for example, **bldg1** - already has Cisco 2610 default port settings before you create the Cisco 2610 settings in the **Austin** group, by default the child group retains its original Cisco 2610 default port settings. You can choose to overwrite existing settings in child groups.

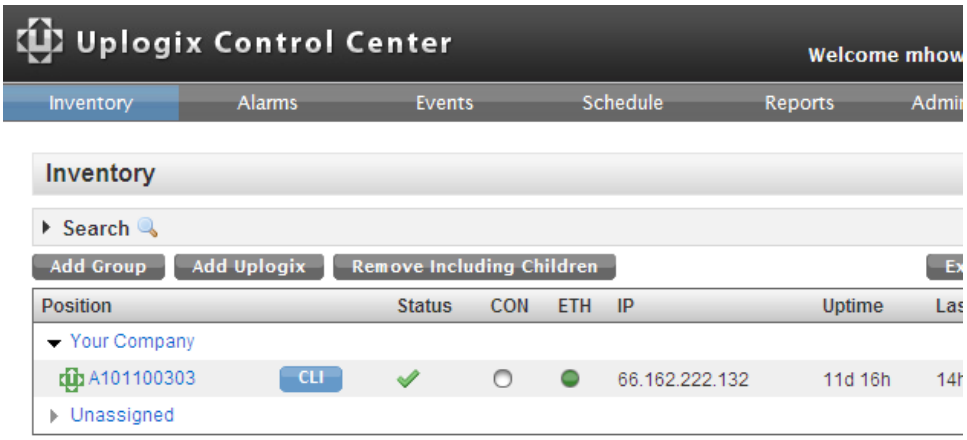
Appliances within the Unassigned group do not inherit any settings; they are outside the inventory's root group.

Note: If you delete default settings from a group, child groups retain the settings.

Viewing the inventory

Inventory

To view an expandable tree view of your inventory, select the inventory tab. This tree shows the current organization of your deployment, including inventory groups and individual appliances. Initially, the Inventory list shows only the two default groups, Your Company and Unassigned.



To view the contents of an inventory group, click the expand icon ▸ beside the inventory group name. To view details, click the group name to open the group detail page. If the group is empty, this icon is gray.

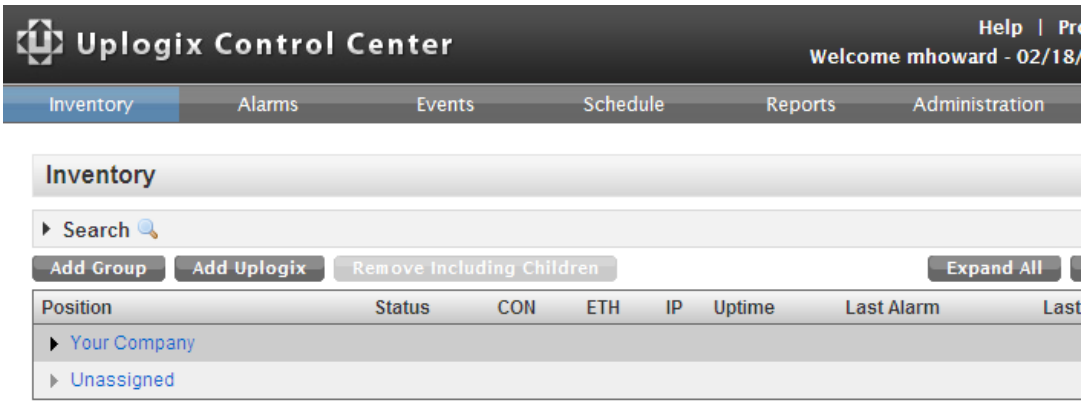
Icons beside each entry denote status or other information.

Icon	Description
▸	Inventory group is collapsed. The arrow is black if the group contains at least one appliance or child group, gray if it is empty.
▾	Inventory group is expanded, listing appliances and child groups.
	The appliance has communicated within the past four heartbeat intervals (default interval is 30 seconds).
	No communication has been received from this unit within the past four heartbeat intervals.
	This unit is communicating in minimal heartbeat mode.
	This unit is communicating over out-of-band connection.
	The unit has been manually added to the inventory, but has not yet contacted the server.

The inventory is sorted alphabetically. To search for a specific Uplogix appliance, enter its hostname in the search box at the top of the inventory pane.

Organizing inventory groups

The **Inventory** tab allows you to organize and manage appliances by inventory group. Most management operations occur at the group level.



Select the name of a group in the inventory list to bring up the Group Detail page. All functions concerning inventory groups can be accessed from this page.

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 an appliance
- Reassigning an appliance
- Deleting an appliance

About the Unassigned group

When you execute the **`config system management`** command on an Uplogix appliance to place it under management by a Uplogix Control Center element management system, it is placed in the Unassigned group on the Control Center unless you have already created a placeholder for it in another group. (For information on this, see Adding an appliance on page 26.)

Unlike other inventory groups, the Unassigned group does not provide management capabilities. To manage Uplogix appliances, you must reassign them from Unassigned to another inventory group. See Reassigning an appliance on page 31.

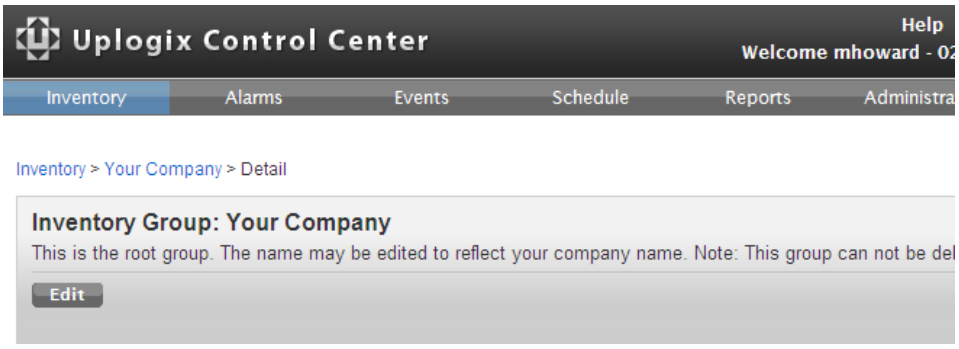
You cannot delete or edit the Unassigned group, nor can you reassign Uplogix appliances to it.

You can place an Uplogix appliance in the Unassigned group by deleting it from another inventory group. At the next heartbeat, the appliance appears in the Unassigned group.

Editing an inventory group

Inventory

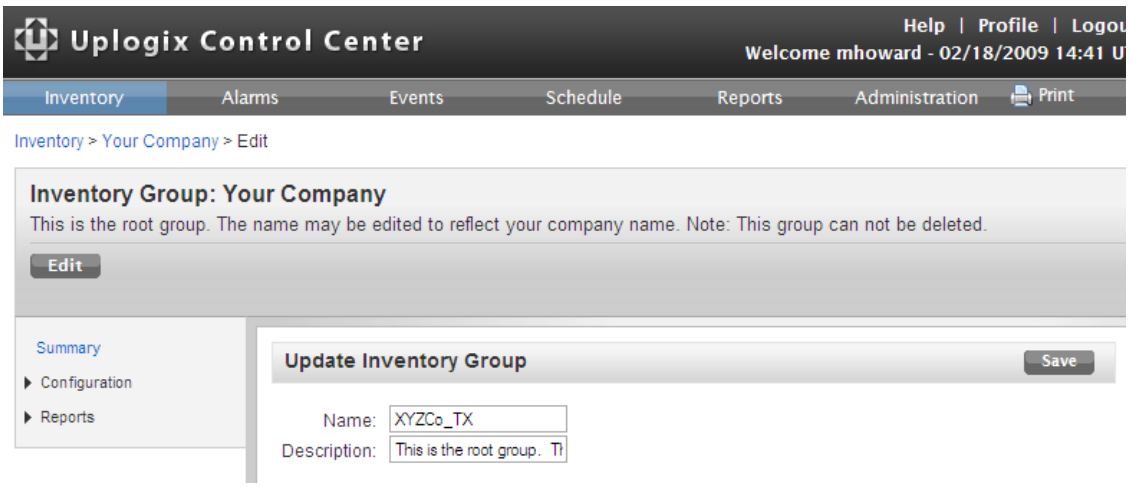
You can edit the name and description of the root group or of any inventory group that you add. From the Group Detail page, click **edit**. The group must have a name; the description field is provided for your convenience.



Edit the information in the text boxes and click save to save your changes. The Description field is for your convenience, and is not displayed except on this page.

Editing an inventory group only changes its name and description; it does not affect the child groups or Uplogix appliances within it.

Note: When completing text fields, use only printing characters. Spaces are considered printing characters.

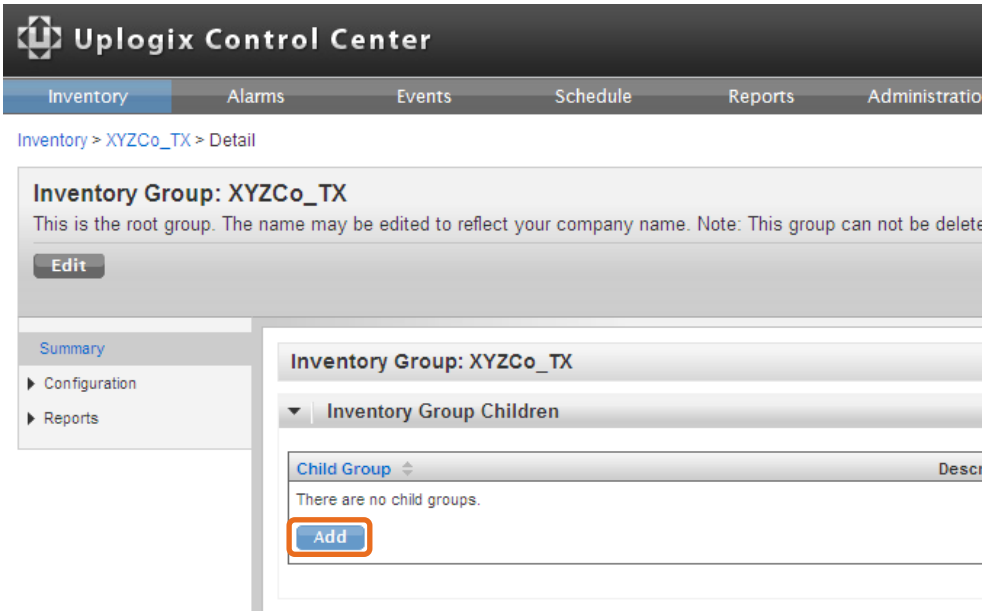


Adding an inventory group

Inventory

To add an inventory group, navigate to the group in which you want to create a new child group. You cannot create groups within the Unassigned group.

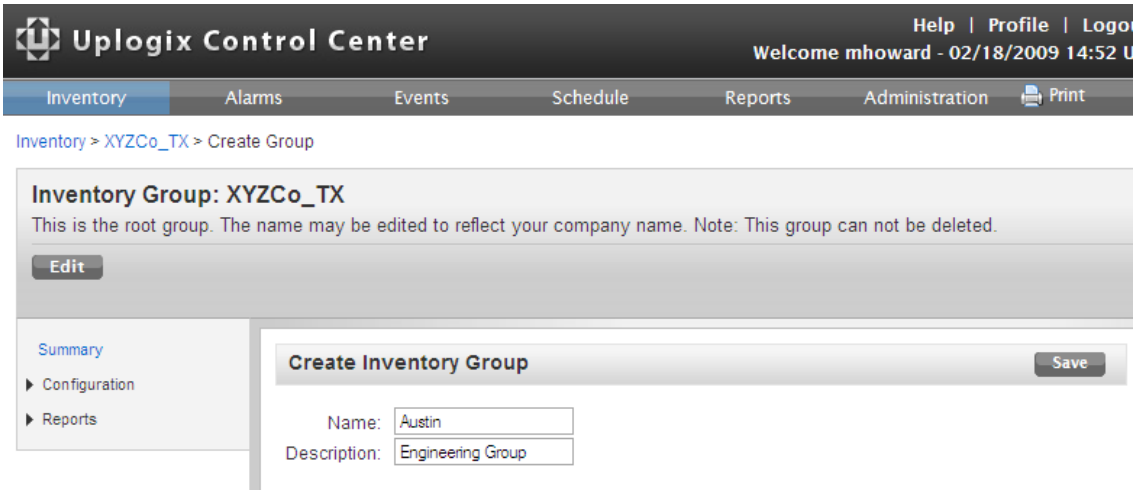
In the **Child Group** area of the group detail page, click **Add** to open the Create Group page.



Enter a name (required) and a description (optional). The name of the new inventory group must be unique within the entire inventory hierarchy. You may not create another inventory group of the same name at a different level or within a different parent group.

Note: When completing text fields, use only printing characters. Spaces are considered printing characters.

Click **save** to add the inventory group. The example below creates a new group called **Austin**.

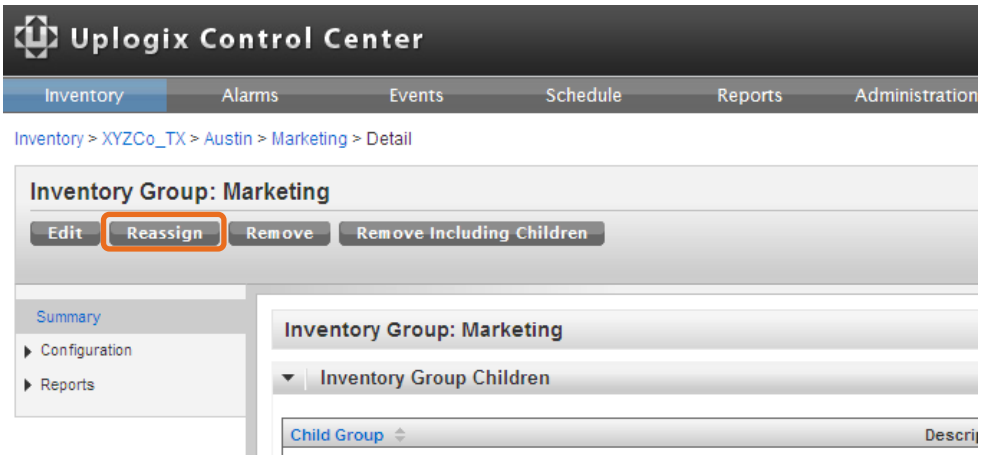


The inventory list and the information in the inventory detail automatically refreshes. If the parent group was previously empty, its expand/collapse arrow changes from gray to black in the inventory tree view.

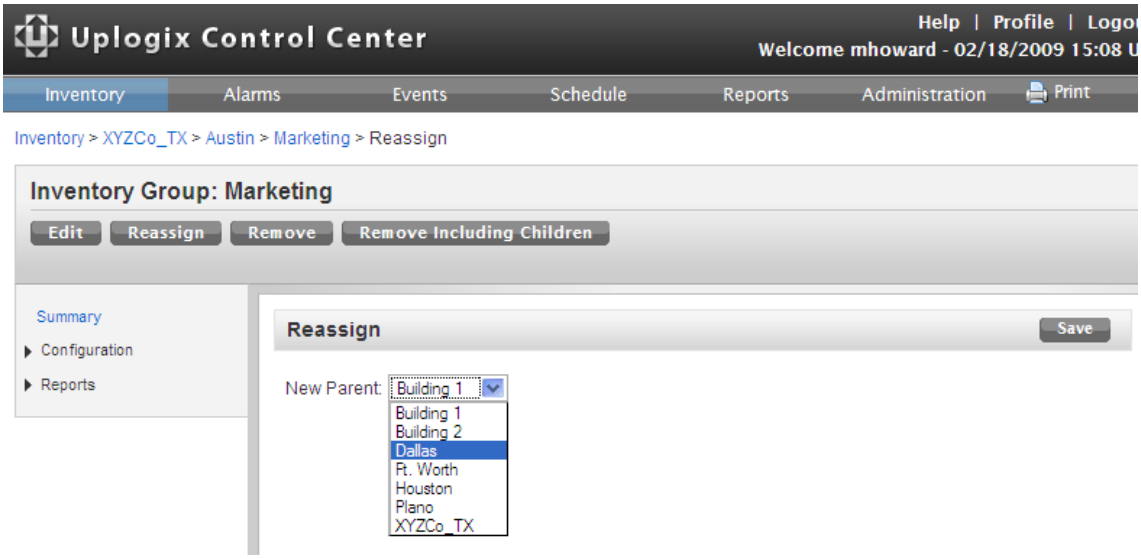
Reassigning an inventory group

Inventory

All groups except the root group and Unassigned can be moved to another parent. Reassignment includes all of the inventory group's child groups and Uplogix appliances. Click **reassign** on the Group Detail page to open the Reassign page.



The **New Parent** list shows available inventory groups. The only groups not shown are the current parent and the Unassigned group. Select the new parent from the menu and click **save**.



The inventory list automatically refreshes and displays the inventory group's new location.

Deleting an inventory group

Inventory

There are two ways to delete an inventory group from the Uplogix Control Center EMS.

Choose **delete** to move all the child groups and appliances into the parent group. For example, clicking **delete** on the screen shown below would move all the members of the **Marketing** inventory group into the **Dallas** group before deleting **Marketing**.

Choose **delete including children** to delete the group with its child groups. For example, clicking **delete including children** on the screen shown below would delete the **Marketing** inventory group, along with any child groups and Uplogix appliances assigned to **Marketing**. Deleted Uplogix appliances will return to the Unassigned group when they re-establish contact with the server at the next heartbeat.

Caution: There is no delete confirmation.

Adding an appliance

A management relationship must be established before the Uplogix Control Center EMS can manage an Uplogix appliance.

You can set up a placeholder for the appliance beforehand, so that the appliance is automatically added to the appropriate group when it contacts the server.

Note: If user accounts have been created on the Uplogix appliance, they will be deleted when the Uplogix Control Center adds the appliance to its inventory.

Create a placeholder on the Uplogix Control Center (optional)

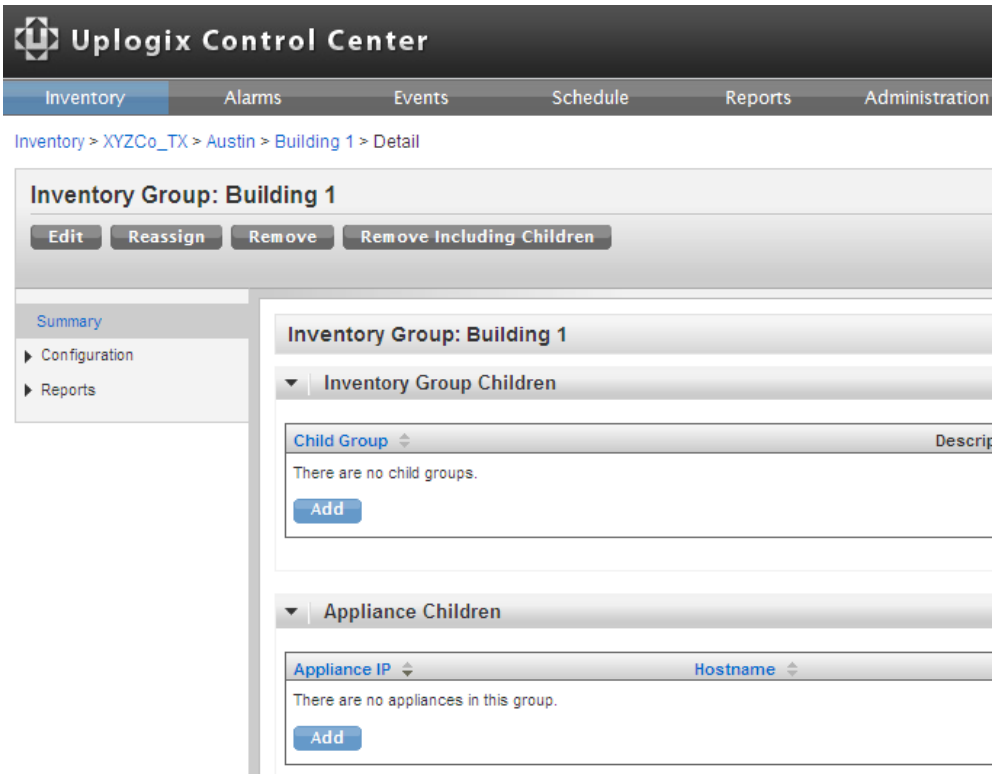
Inventory > Group

Creating a placeholder in advance allows you to add the Uplogix appliance directly to the inventory group of your choice, so that users with the appropriate privileges within that group can manage the appliance as soon as it contacts the Uplogix Control Center. The appliance will also inherit the configuration settings, privileges, roles, rules, preferences, and other defaults from that inventory group.

You can do this step before the Uplogix appliance is physically installed.

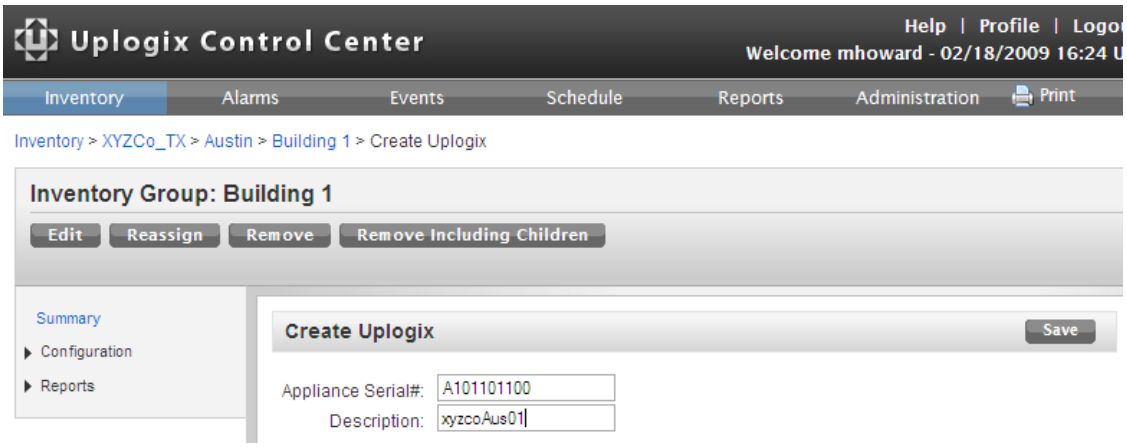
You will need the serial number of the appliance you wish to add. This number can be found by issuing the **`show version`** command from the appliance's command line or referencing the plate on the bottom of the appliance.

Select a group from the inventory list to bring up the Group Detail page, and click **add appliance** to open the Create Uplogix dialog box.



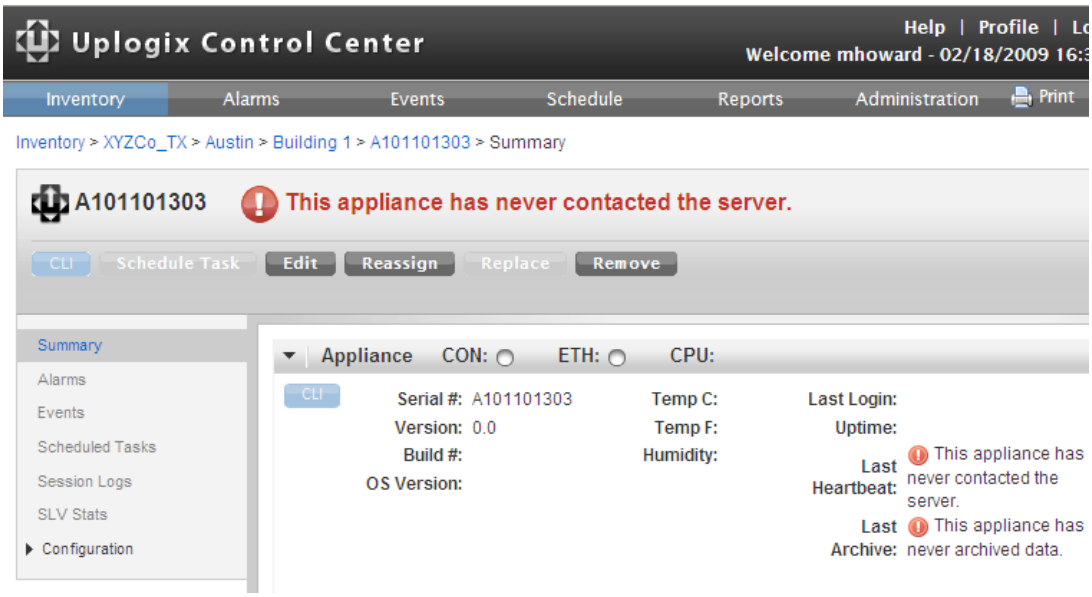
In the Create Uplogix dialog box, enter the serial number of the Uplogix appliance and an optional description. Click **create** to add the appliance.

Note: When completing text fields, use only printing characters. Spaces are considered printing characters.



The group detail page automatically refreshes and displays the appliance.

If you select the appliance to view the detail page, you will see its symbol appears in black because there is no communication between the server and the appliance at this point.

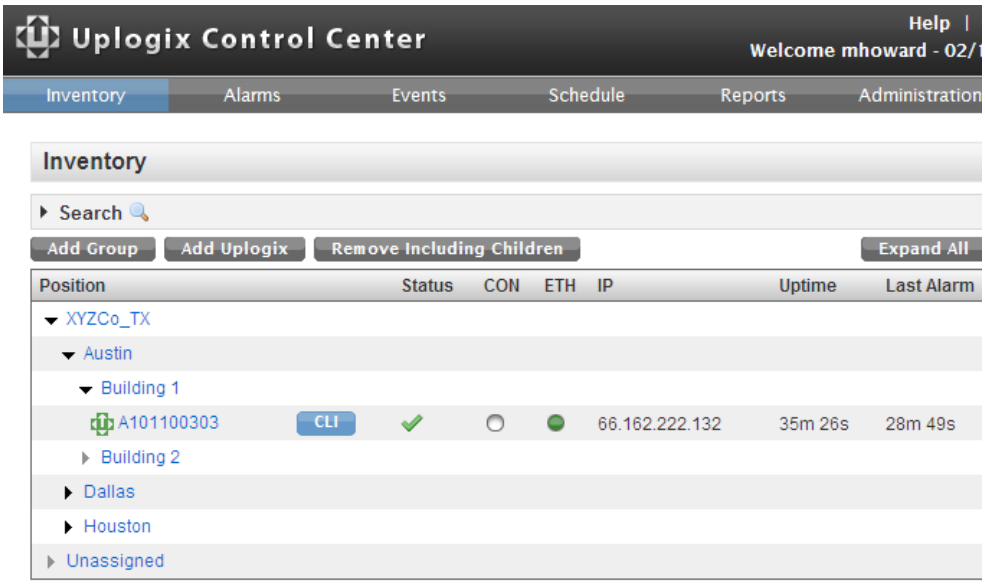


Configure the appliance to use the Uplogix Control Center (required)

From the Uplogix appliance's command line interface, issue the **`config system management`** command. Use your Uplogix Control Center's IP address in place of the IP address in this example:

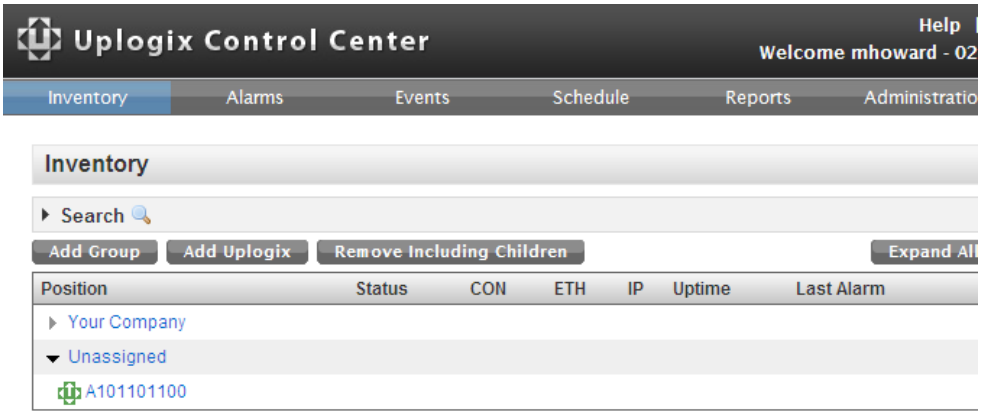
```
[admin@xyzcoAus01]# config system management
--- Existing  Values ---
Use EMS: false
EMS Server Hostname or IP: 127.0.0.1
EMS Server Port: 8443
Heartbeat interval (seconds): 30
Last successful heartbeat:  (not yet contacted)
Change these? (y/n) [n]: y
--- Enter New Values ---
Use EMS: (y/n) [n]: y
EMS Server Hostname or IP: [127.0.0.1]: 172.30.238.20
EMS Server Port: [8443]:
Set archive location to 172.30.238.20: (y/n) [y]:
Set ntp location to 172.30.238.20: (y/n) [y]:
Heartbeat interval (seconds): [30]:
Do you want to commit these changes? (y/n): y
Updating archive to point to 172.30.238.20
Enabling NTP to point to 172.30.238.20
```

If you set up a placeholder in the inventory before you do this, the black icon for the placeholder turns green and the serial number is replaced by the appliance's hostname (if one has been configured on the appliance) when the Uplogix Control Center has received a full heartbeat. The default heartbeat interval is 30 seconds.



If you did not create a placeholder on the Uplogix Control Center, the appliance will be placed in the **Unassigned** group.

Note: You will not be able to manage the appliance while it is in the **Unassigned** group. You will need to reassign it into another inventory group to manage it. See Reassigning an appliance on page 31.



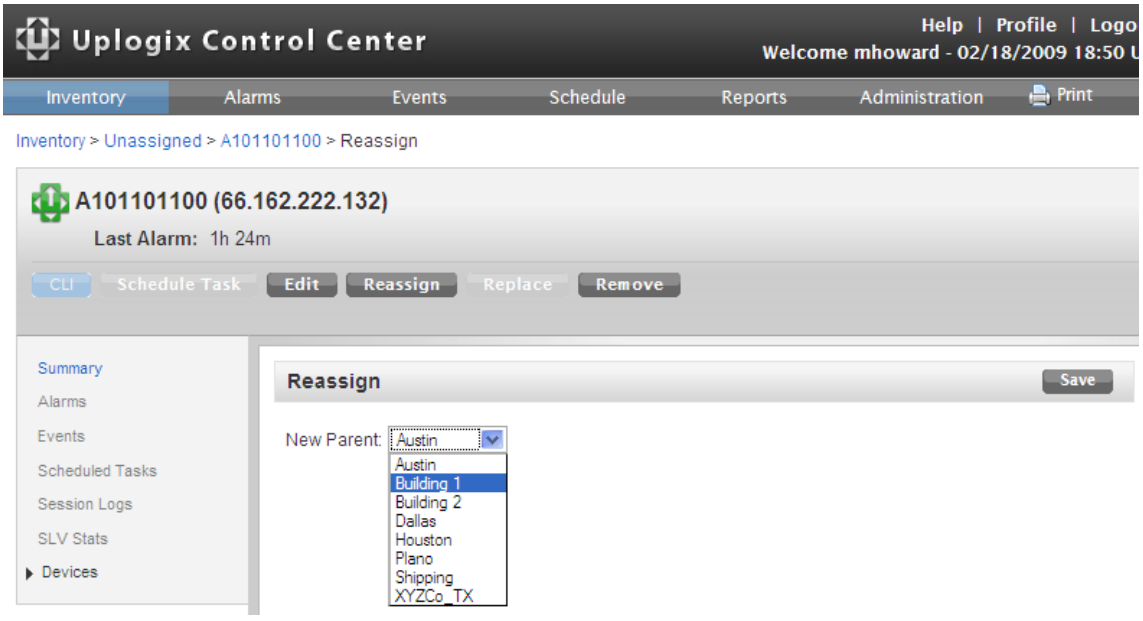
Reassigning an appliance

Inventory > Appliance Page

If an Uplogix appliance appears in the Unassigned group or if you want to move it, you can reassign it to another inventory group. You will need to reassign appliances that are in the Unassigned group before you can manage them.

Select the appliance from the inventory list and click **reassign** from its detail page.

The New Parent list shows available inventory groups. The only groups not shown are the current parent and the Unassigned group.



Select the new parent group and click **save** to finish.

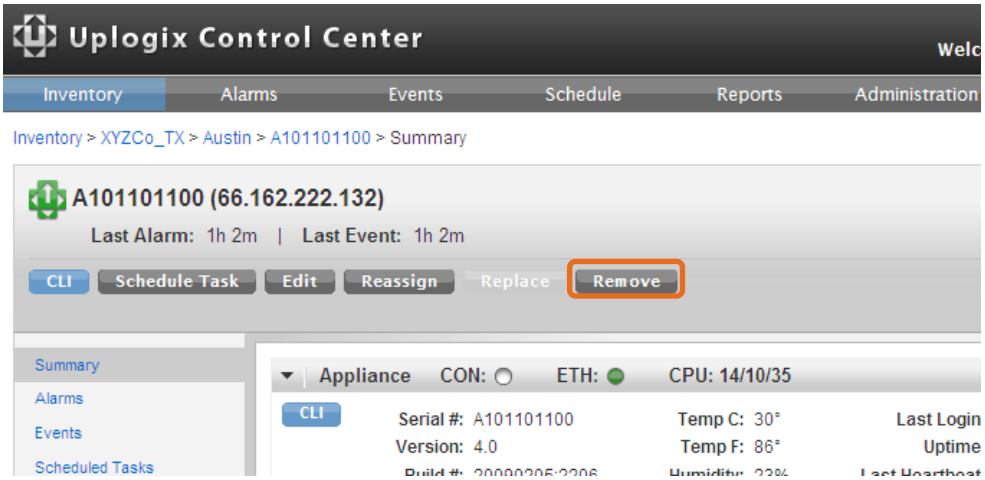
Note: While there is no function for moving an Uplogix appliance into the Unassigned group, you can do this by deleting the appliance. If it is still configured to use the Uplogix Control Center EMS, it will reconnect within a few seconds. It will then be placed in the Unassigned group.

The Uplogix appliance is now displayed in the appropriate group in the inventory list.

Deleting an appliance

Inventory > Appliance Page

You can remove an Uplogix appliance from the inventory by clicking the **remove** button from the appliance page.



Most of the information about the appliance remains in the database. If the appliance subsequently contacts the server, it will be placed in the Unassigned group. This happens if the appliance remains connected and configured to use the Uplogix Control Center.

To set the appliance to operate without management by the Uplogix Control Center, log in to the appliance and issue the **`config system management`** command:

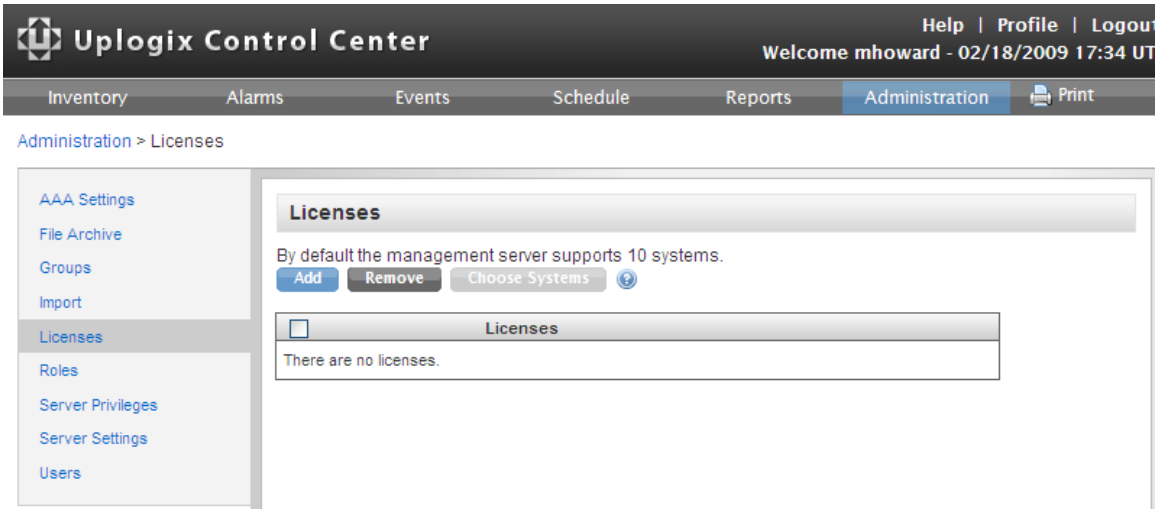
```
[admin@xyzcoAus01]# config system management
--- Existing  Values ---
Use EMS: true
EMS Server Hostname or IP: 172.30.238.20
EMS Server Port: 8443
Heartbeat interval (seconds): 30
Last successful heartbeat: 07/03/2007 19:54:09 UTC (Full)
Change these? (y/n) [n]: y
--- Enter New Values ---
Use EMS: (y/n) [y]: n
Do you want to commit these changes? (y/n): y
```

You can also do this by selecting **Server** from the **Configuration** tab of the expanded appliance page before you delete the appliance.

Managing licenses

Administration > Licenses

Each Uplogix Control Center EMS is initially configured to support up to 10 Uplogix appliances. By purchasing additional licenses, you can add more management capability and advanced functionality to the Uplogix Control Center.



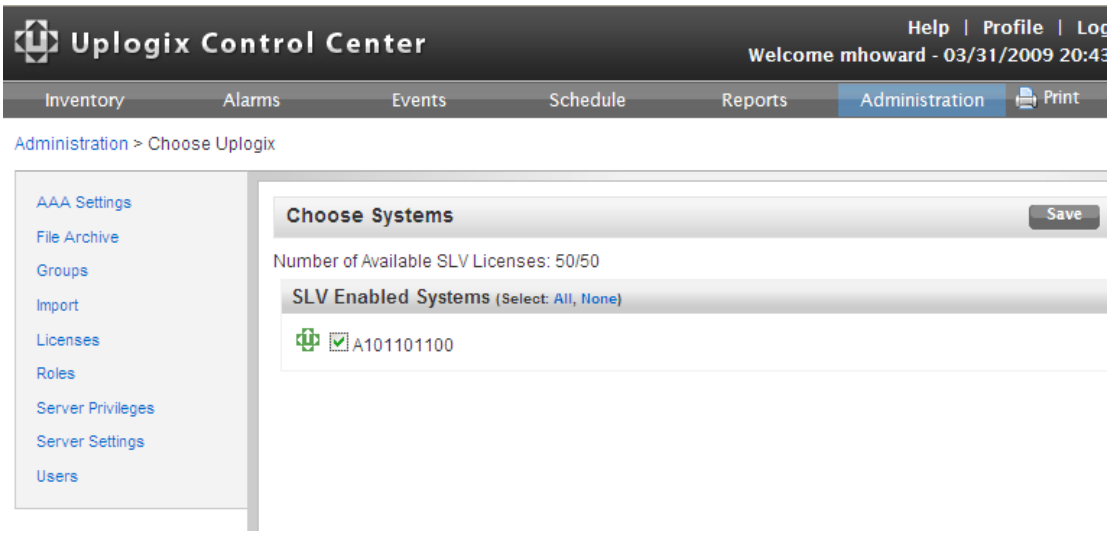
Uplogix Control Center licenses specify the maximum number of managed Uplogix appliances. This limits the number of units that can be moved from the Unassigned group.

Uplogix Control Center licenses may also include Service Level Verification (SLV) features. These specify the number of Uplogix appliances on which SLV can be enabled.

Licenses are not cumulative. The most recent license takes precedence if multiple licenses are present.

Copy and paste the license text and click **save** to apply the license.

If the license includes SLV information, the **choose systems** link becomes active. Click the link to apply the SLV license to specific Uplogix appliances. SLV configuration options are available only for the specific Uplogix appliances to which the license is applied.


Uplogix Control Center
Help | Profile | Log
Welcome mhoward - 03/31/2009 20:43
Inventory
Alarms
Events
Schedule
Reports
Administration
Print
Administration > Choose Uplogix
AAA Settings
File Archive
Groups
Import
Licenses
Roles
Server Privileges
Server Settings
Users
Choose Systems
Save
Number of Available SLV Licenses: 50/50
SLV Enabled Systems (Select: All, None)
A101101100

Managing the equipment

The Uplogix Control Center element management system allows you to manage at the group level; but it also allows you to manage individual Uplogix appliances - even individual ports.

This chapter covers:

- Creating default appliance settings - automate configuration of newly added appliances
- Managing from the appliance detail page - work with the dashboard view of an Uplogix appliance and the devices it manages
- Configuring an appliance - access the functionality offered by the config system RMOS commands
- Creating default port settings - automate configuration of devices on Uplogix appliances
- Managing from the port detail pages - detailed information about devices; access to the device CLI
- Creating your own categories to manage devices - creating and applying port labels
- Reestablishing contact with an appliance that connects via Iridium modem - contact remote appliances via SMS message to start PPP
- Managing scheduled tasks - automate maintenance
- Managing rules and monitors - automate performance assessment, diagnosis, and recovery

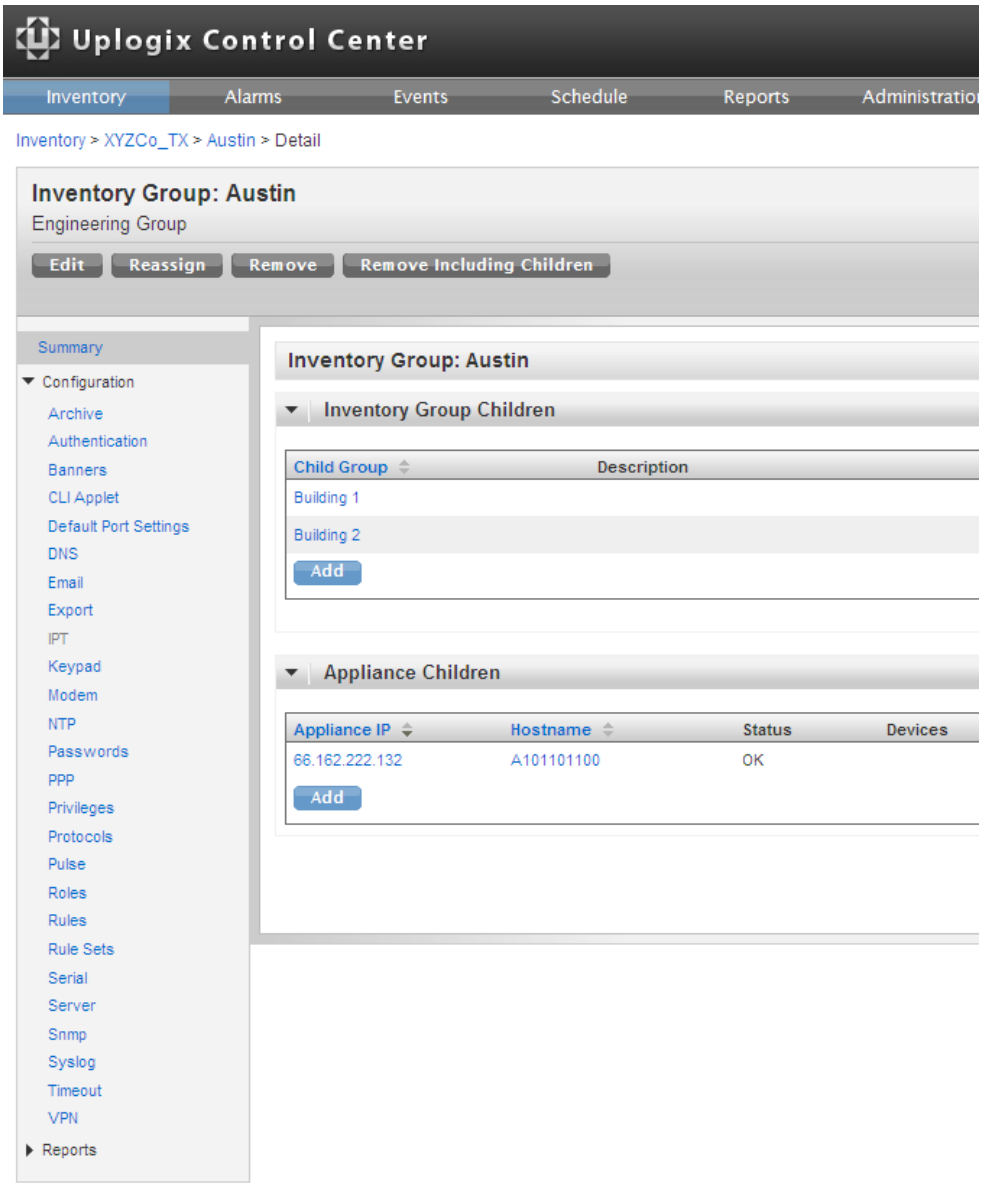
For the tasks described in this chapter, you will need either a role with the appropriate permissions assigned at a suitable level within the inventory, or you will need a role on the Uplogix Control Center that includes the `config hierarchy` privilege, such as the `admin` role. For more information, see Adding server privileges to accounts on page 92 and Adding inventory privileges to accounts on page on page 92.

Creating default appliance settings

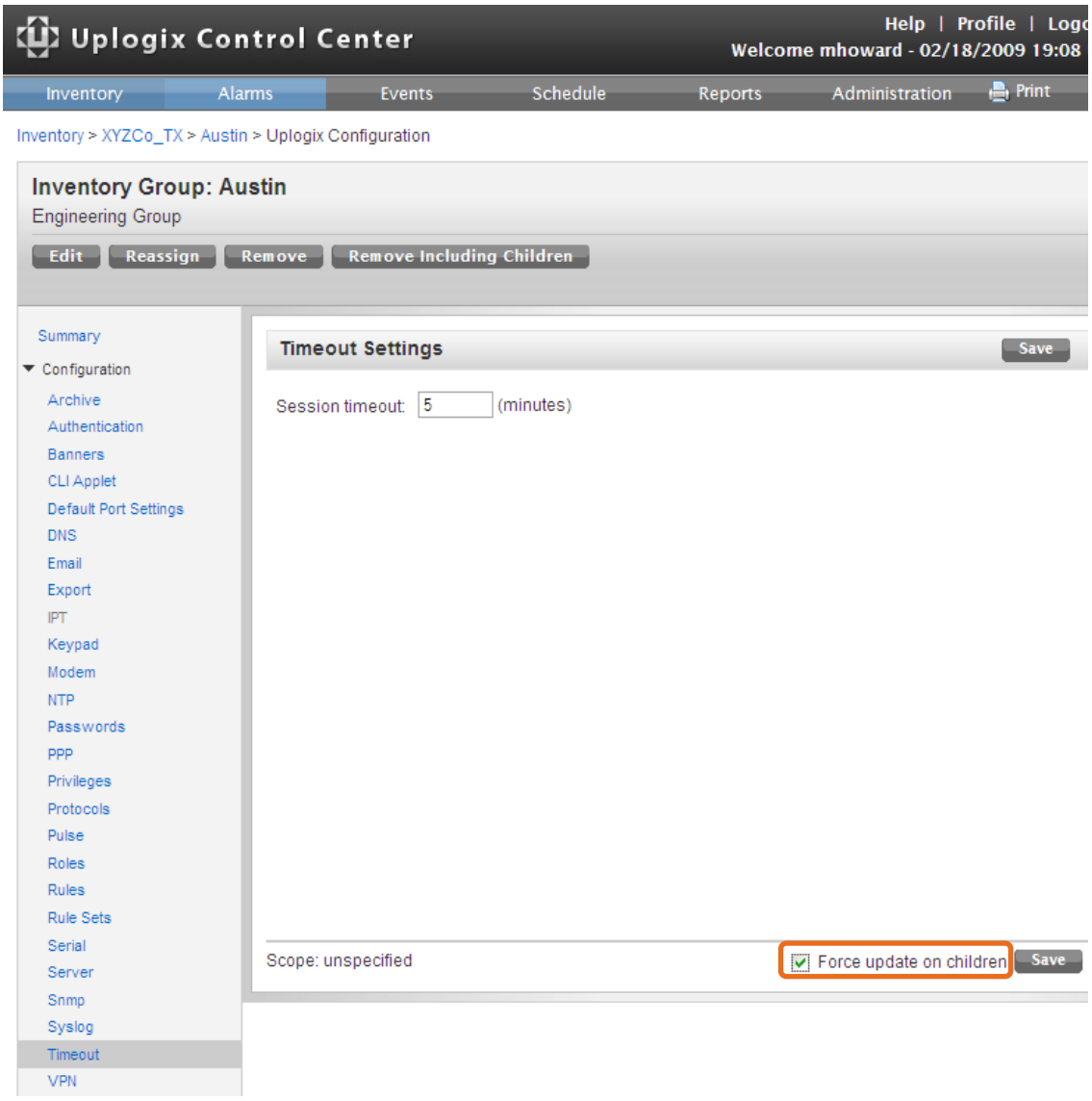
Inventory > Group

The Uplogix Control Center allows you to apply a standard configuration to all Uplogix appliances within a group.

Your role must have either appliance configuration permissions on the affected appliances or the **`config hierarchy`** permission in order for you to set up standard configurations. You can only set up configurations for empty inventory groups if your role includes the **`config hierarchy`** permission. For more about roles and permissions, see Managing privileges on page 91.



To begin, expand the **Configuration** menu. For each configuration setting you wish to define, click the setting name in the configuration list.



Make your changes. If you wish the setting to be propagated to Uplogix appliances already present in the group, select **Force update on children**.

Click **save** to save your changes.

Managing from the appliance detail page

Inventory > Appliance Page

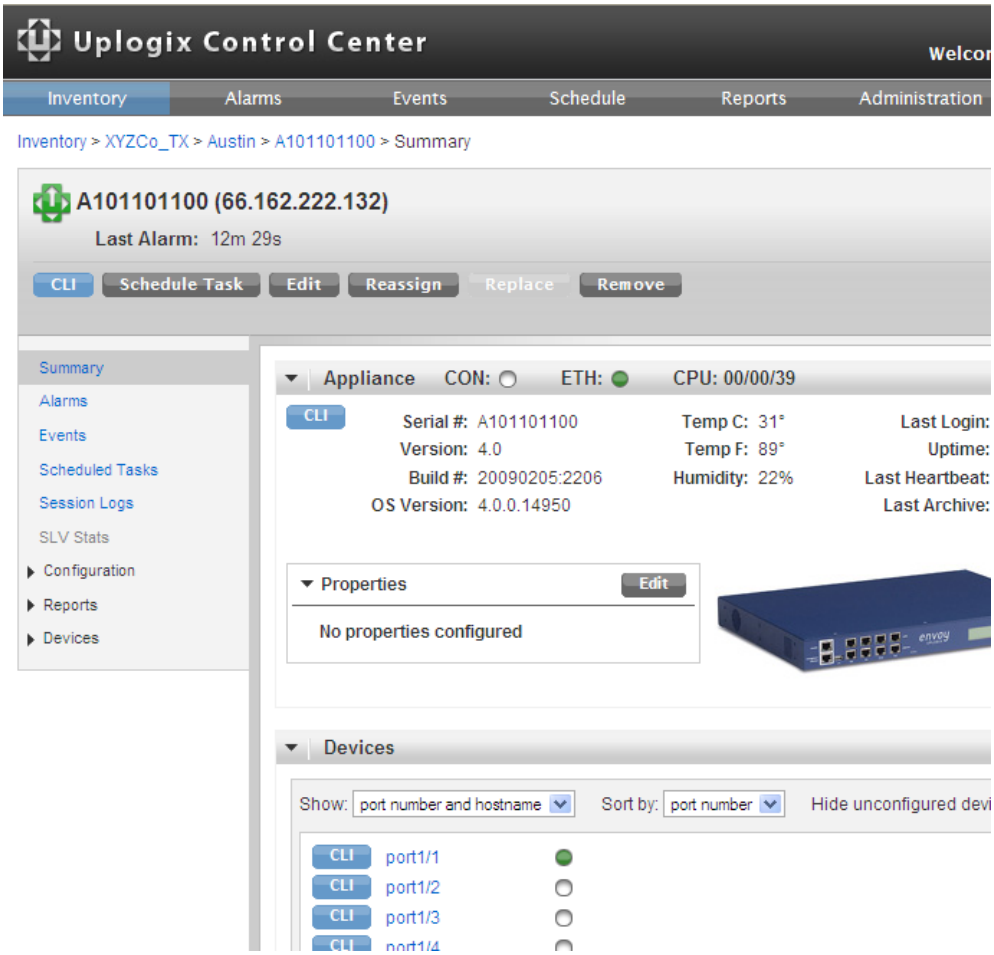
From the Inventory list, or from any other screen where a given appliance is listed, click its hostname to view its detail screen. This provides a quick look at the appliance and the devices connected to it. The equivalent Uplogix RMOS CLI command is **`show dashboard`**. The appliance detail page displays the information being collected from the Uplogix appliance.

The appliance detail page shows or hides information based on your privileges. To be able to see the name and details of an appliance listed in the Inventory hierarchy, your privileges must include `login` on that appliance, or you must have the **`config hierarchy`** permission.

Note: The appliance detail does not indicate whether the appliance is using an out-of-band connection.

The summary view

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



The appliance detail page shows or hides information based on your account's 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 will be 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 that you can use to access the Uplogix appliance's RMOS command line. The CLI applet requires Java to be installed on the workstation. You can download the latest version of the Java Runtime Environment from http://java.sun.com. Minimum and recommended system requirements for the CLI applet are:

Minimum	Recommended
Microsoft® Windows® XP, service pack 2 Microsoft ® Internet Explorer® 6 Sun Java™ 1.5.0	Microsoft® Windows ® XP, service pack 3 Microsoft ® Internet Explorer® 7 or later or Firefox 3 Sun Java™ 1.5.06

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

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

. Click the device name to view the device detail page.

Configuring an appliance

Inventory > Appliance Page

The Configuration menu allows you to edit the appliance's configuration through the graphical interface. It offers most of the same capabilities as the Uplogix RMOS command line.

The Uplogix Control Center provides a graphical interface for the configuration of managed Uplogix appliances. Use the right arrow ▸ Click expand the **Configuration** menu using the right arrow ▸.

Note: When completing text fields, use only printing characters. Spaces are considered printing characters.

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

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

Configuration option	Permission required	Purpose
Archive	`config system archive`	Configure archiving from the appliance to the Uplogix Control Center
Authentication	`config system authentication`	Configure authentication settings for the Uplogix appliance
Banners	`config system banner`	Set banners on the appliance
CLI Applet	`show system applet`	Configure authentication settings for Socks Proxy
Default Port Settings	`config settings`	Edit or delete default port settings on the Uplogix appliances

Configuration option	Permission required	Purpose
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 appliance configuration
IP	**config system ip**	Configure the appliance's management Ethernet settings
IPT	**config system ipt**	Set up IPT testing and IP filtering
Keypad	**config system keypad**	Enable or lock the appliance's keypad
Modem	**config answer** (Modem resource)	Configure modem behavior
NTP	**config system ntp**	Specify an NTP server (by default, appliances use the Uplogix Control Center)
Passwords	**config password**	Configure password settings
PPP	**config ppp** (Modem resource)	Configure dial-up information for establishing out-of-band connections
Privileges	**config privileges**	Configure access on the port associated with the Uplogix appliances
Properties	**config system properties**	Configure properties on the Uplogix appliance
Protocols	**config system protocols filter** **config system protocols ssh** **config system protocols telnet**	Configure IP filtering Configure terminal pass-through using SSH Configure terminal pass-through using Telnet
Pulse	**config system pulse**	Specify a pulse server for this appliance
Roles	**config role**	Create or update roles on the Uplogix appliance
Rules	**config rules**	Configure pulse server settings
Rule Sets	**config ruleset**	Rule sets allowed to set-up on the Uplogix appliance

Configuration option	Permission required	Purpose
Serial	**config system serial**	Specify whether the appliance uses a null modem cable for its serial management connection
Server	**config system management**	Change the appliance's management configuration - whether the appliance uses the Uplogix Control Center, TCP port used, heartbeat interval, and related information
SLV Tests	**config slv**	Configure and view SLV tests being run on the Uplogix appliance
Snmp	**config system snmp**	Enable and configure SNMP
Syslog	**config system syslog-options**	Enable syslog and specify syslog server
Timeout	**config system timeout**	Set the idle CLI session timeout for this appliance
VPN	**config vpn** (Modem resource)	Configure VPN type and setup

For configuration information, consult the ***User's Guide for Uplogix Secure Remote Management Appliances***.

Configuration settings are also available on the Inventory Group level. Some appliance-specific settings such as IP address cannot be applied to an inventory group.

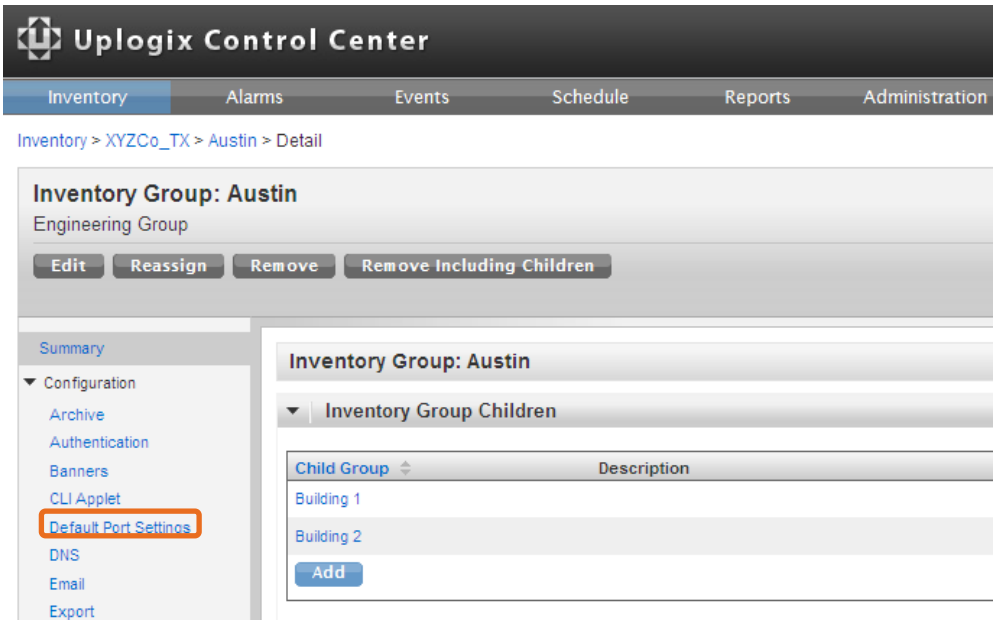
Creating default port settings

Inventory > Group

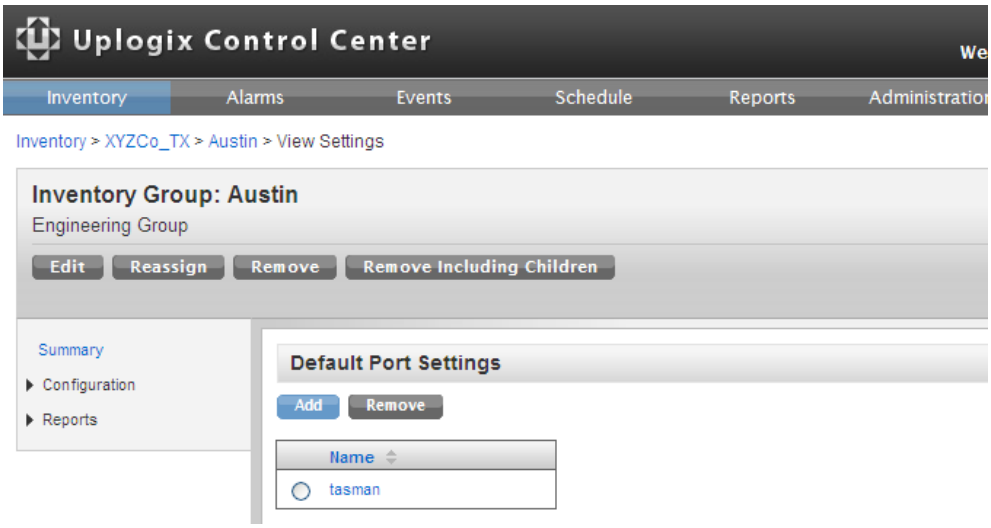
The **config settings** command on the Uplogix appliance allows you to define how the appliance communicates with the device connected to a given port. On the Uplogix Control Center, these settings can be defined and applied to more than just one port; they could apply to all devices of a specific make, model, or operating system. For example, you could 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 will be inherited by the entire deployment. Setting profiles defined in a child inventory group will only be inherited by its child groups and the Uplogix appliances in those inventory groups. Therefore, it is possible to have default port settings for a Cisco 2511 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 Settings page, click **default port settings** on the configuration menu for the group to which the settings will apply.



If any default settings have been created, they will be listed. The View Settings page allows you to edit, remove, or add default port setting profiles.



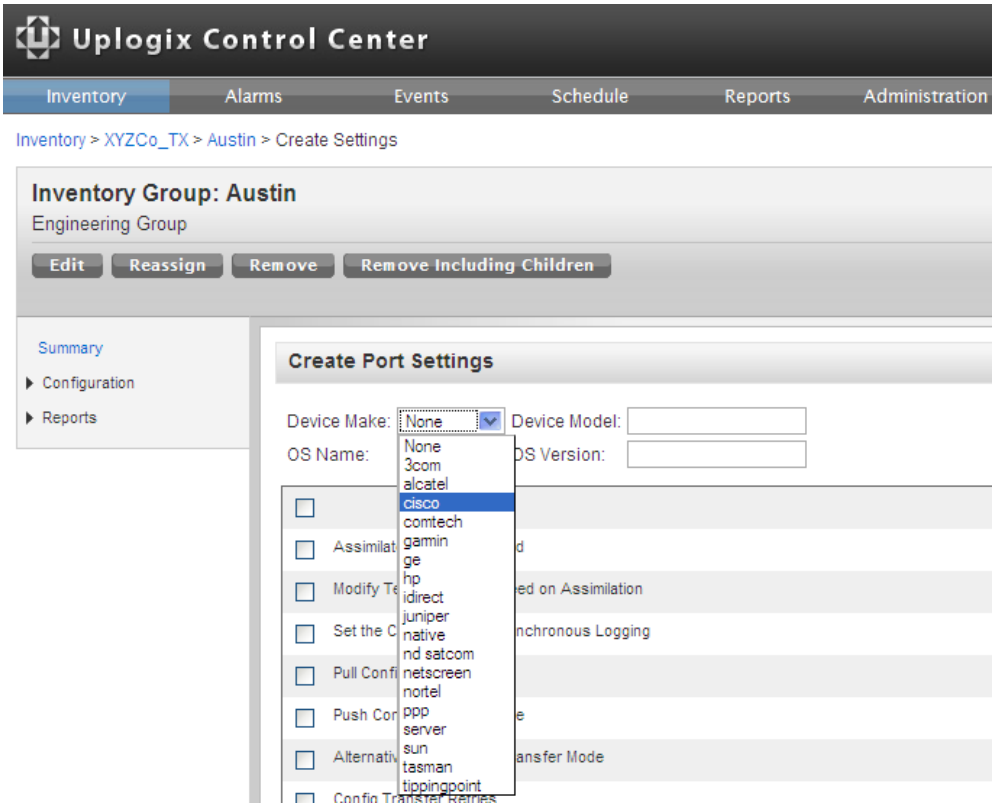
Note: Deleting a setting profile does not affect the devices where the settings have already been applied. For example, referring to the screen above, if you delete the **tasman** settings, it will not change the configuration of any Tasman devices. If you then connect a Tasman device to an Uplogix appliance, however, the **tasman** profile will no longer be present and you will need to configure the port manually using the **`config init`** command.

Note: The **create settings** option is not available if the inventory group is empty. You can, however, edit the **Default** profile. 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 RMOS CLI.

Specify as much or as little information as necessary when creating settings. The Uplogix appliances that inherit these settings will apply them to any port that matches all the information given. For example, simply specifying "cisco" will match all Cisco devices. Specifying "cisco" and "2511" will only match Cisco 2511 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.

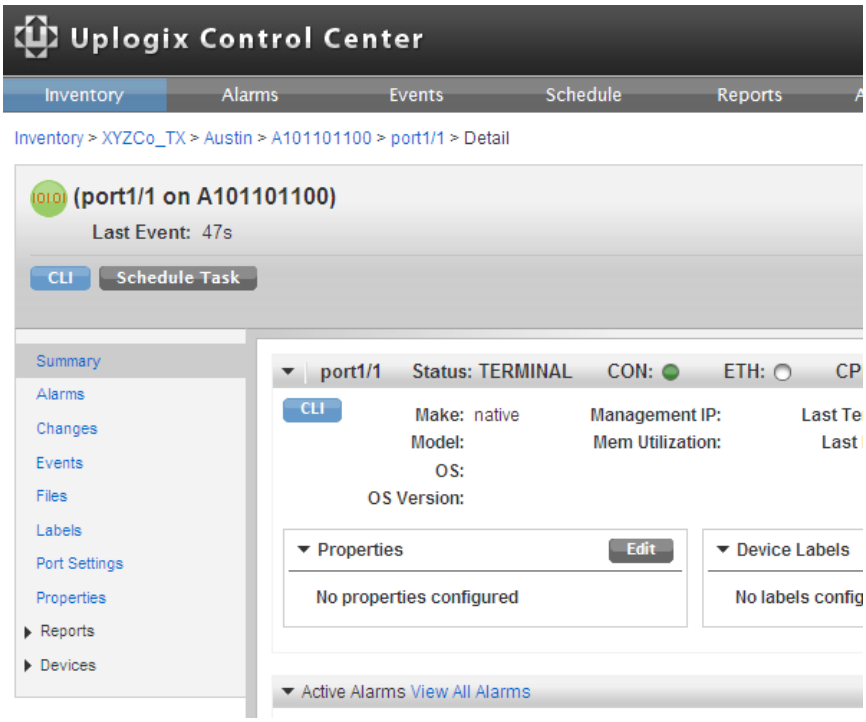


When you edit existing default port settings, you must specify whether to force the update on any child groups within the affected inventory group. Otherwise, the settings will only be updated in the current inventory group.

Managing from the port detail pages

Inventory > Appliance Page > Port Page

From the appliance page, you can 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.


Uplogix Control Center
Inventory
Alarms
Events
Schedule
Reports
Inventory > XYZCo_TX > Austin > A101101100 > port1/1 > Detail
(port1/1 on A101101100)
Last Event: 47s
CLI
Schedule Task
Summary
Alarms
Changes
Events
Files
Labels
Port Settings
Properties
Reports
Devices
port1/1
Status: TERMINAL
CON:
ETH:
CP
CLI
Make: native
Model:
OS:
OS Version:
Management IP:
Mem Utilization:
Last Te
Last
Properties
Edit
No properties configured
Device Labels
No labels config
Active Alarms View All Alarms

Creating your own categories for managing devices

Inventory groups provide a way to manage Uplogix appliances by location or business unit, and the information you enter when configuring ports allows you to manage devices by make and model.

In some cases you may wish to organize and manage devices by some other criterion - for example, you may wish to schedule maintenance on all servers, receive reports or assign privileges on all routers regardless of make, or group managed devices by business unit in cases where several business units share an Uplogix appliance.

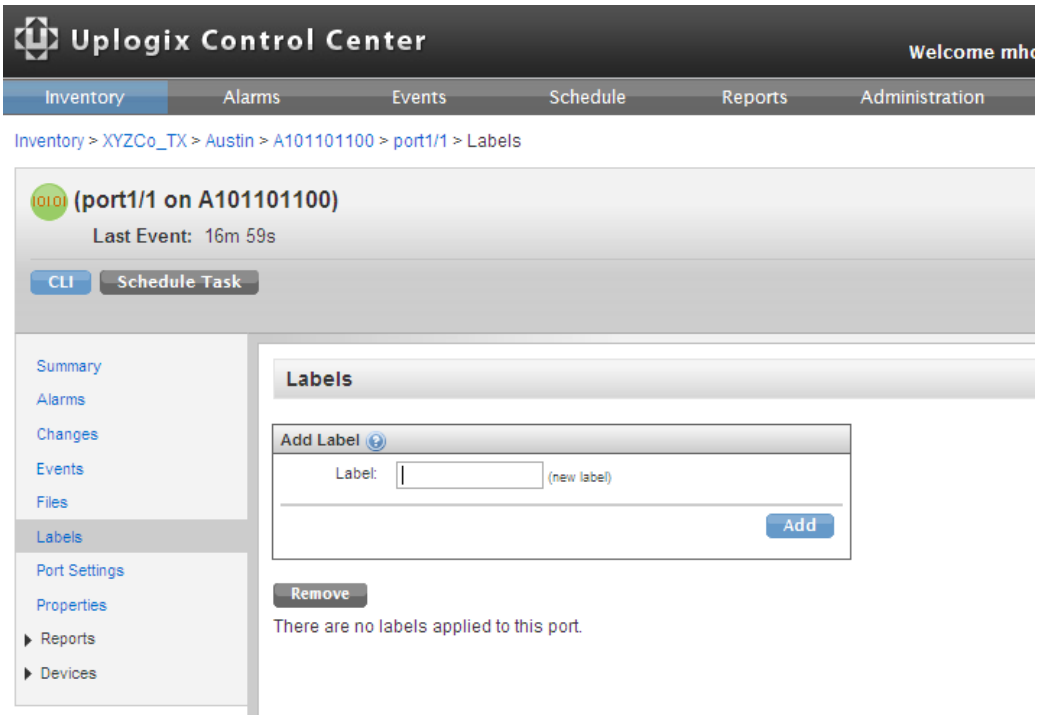
By assigning labels to an Uplogix appliance's managed devices, you can group them in more flexible ways.

Labels are managed from the Uplogix Control Center; they cannot be assigned from the appliance's RMOS command line.

Creating port labels

Appliance Page > Port Page

To assign a label to a port, open the detail page for the Uplogix appliance that manages it. Then expand the detail for the port you wish to label.



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. You can apply more than one label to a port.

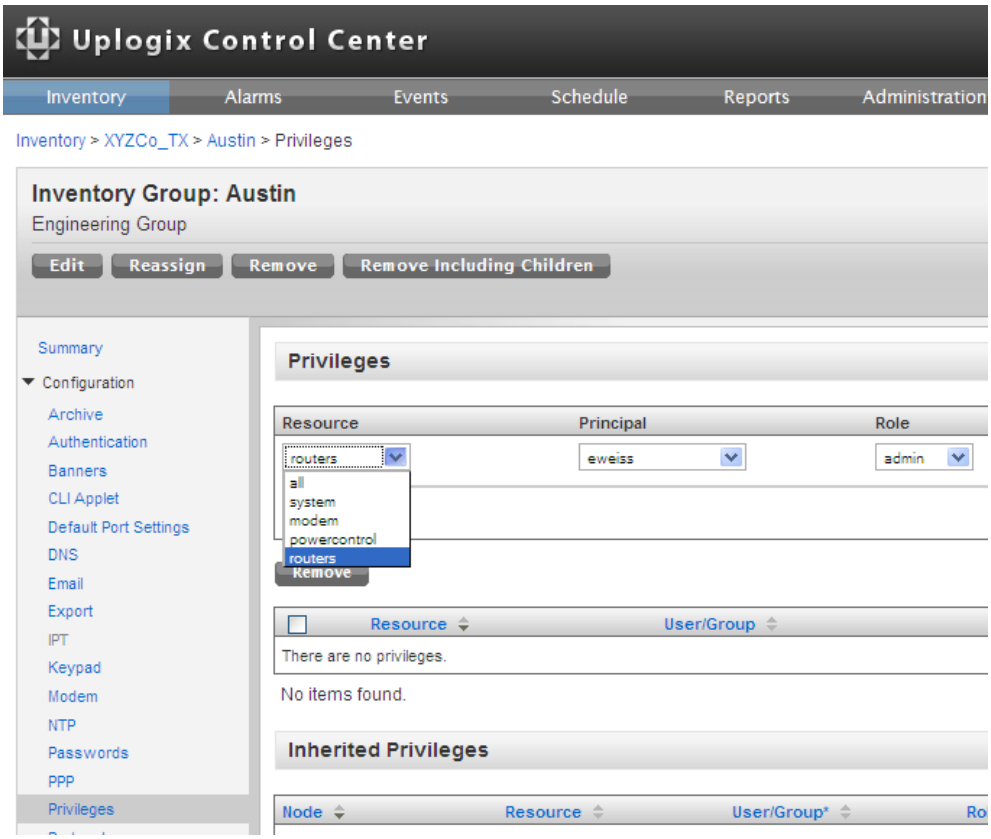
In this example, port 1/1 is given a new label, routers.

Assigning privileges by label

Inventory > Group > Configuration > Privileges

Account privileges are created by assigning the account a role (such as admin or guest) on a resource. The default resources within the inventory are the same resources you find in the Uplogix RMOS command line interface - system, modem, powercontrol, and the individual ports. If you have created labels, they are also considered resources.

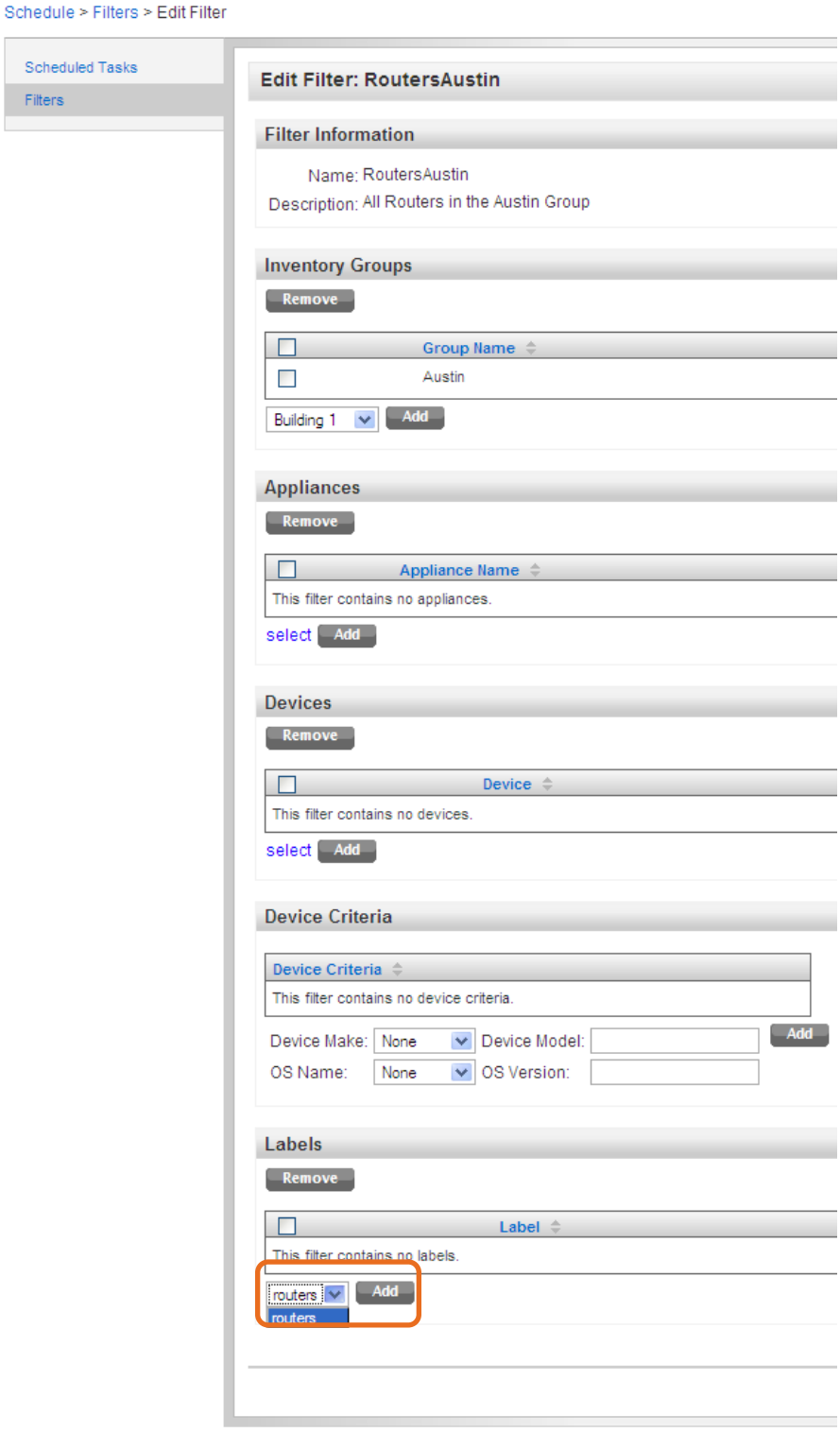
The example below shows how to give a user admin rights on all routers. For more information about assigning privileges, see Managing privileges on page 91.


Uplogix Control Center
Inventory
Alarms
Events
Schedule
Reports
Administration
Inventory > XYZCo_TX > Austin > Privileges
Inventory Group: Austin
Engineering Group
Edit
Reassign
Remove
Remove Including Children
Summary
Configuration
Archive
Authentication
Banners
CLI Applet
Default Port Settings
DNS
Email
Export
IPT
Keypad
Modem
NTP
Passwords
PPP
Privileges
Privileges
Resource
Principal
Role
routers
eweiss
admin
all
system
modem
powercontrol
routers
Remove
Resource
User/Group
There are no privileges.
No items found.
Inherited Privileges
Node
Resource
User/Group*
Ro

Setting up task filters using labels

Schedule > Filters

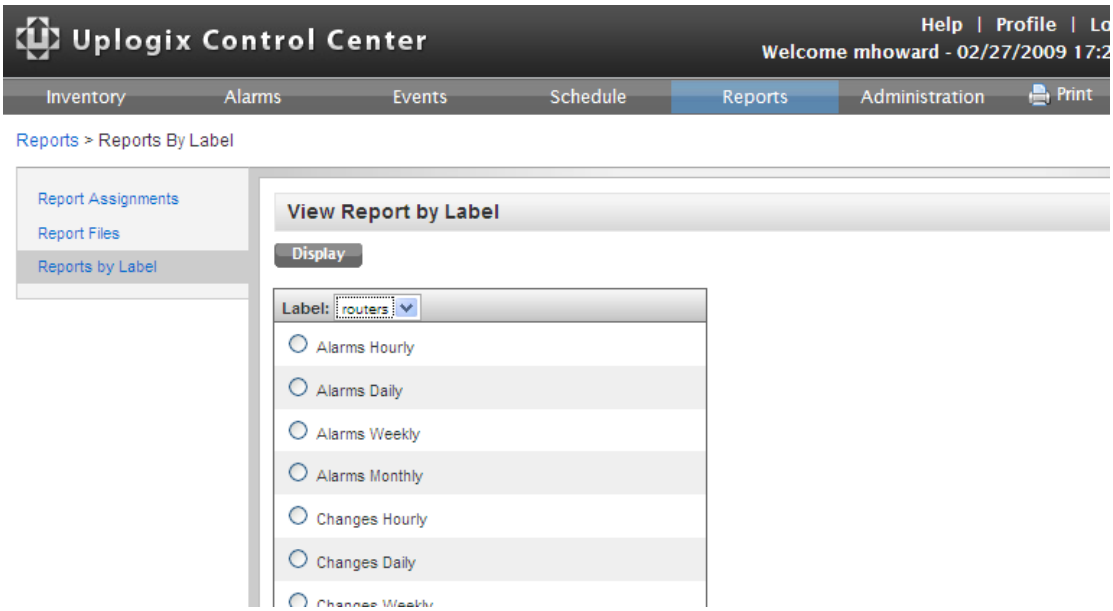
The Schedule > Filter page allows you to use labels as one of the filtering criteria when you set up filters for scheduling tasks. For more information about task filters, see Setting up filters and scheduling tasks on page 51.



Viewing reports by label

Reports > Reports by Label

When you have assigned labels to port devices, the Uplogix Control Center automatically creates reports based on the labels. You can view these reports on the **Reports > Reports by Label** page. For more information about reports, see Viewing reports on page 120.



Reestablishing contact with an appliance that connects via Iridium modem

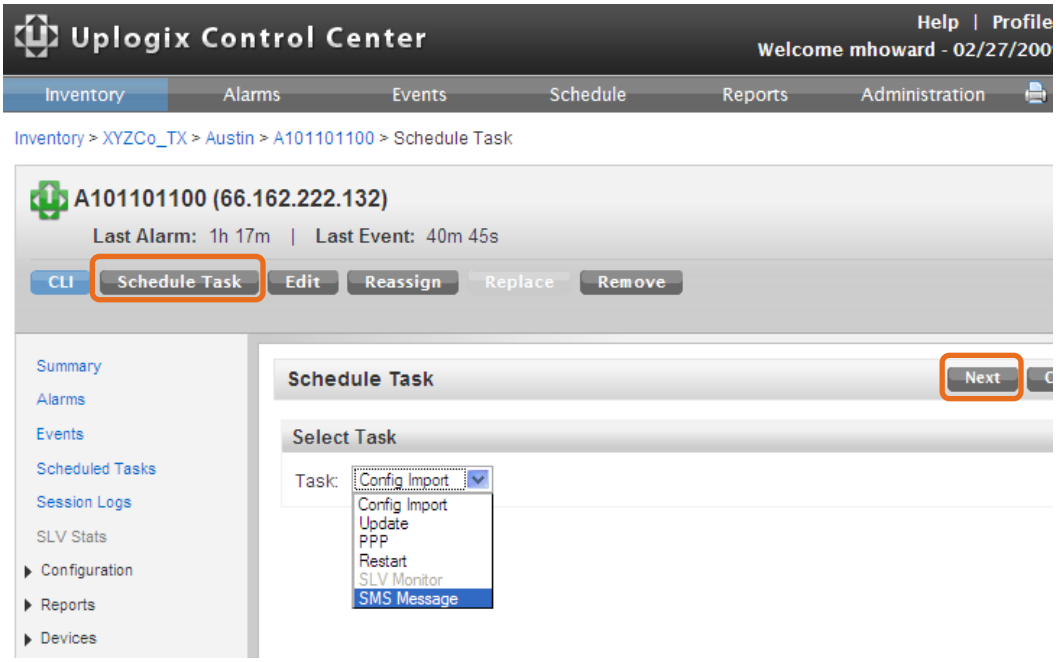
Inventory > Appliance Page

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

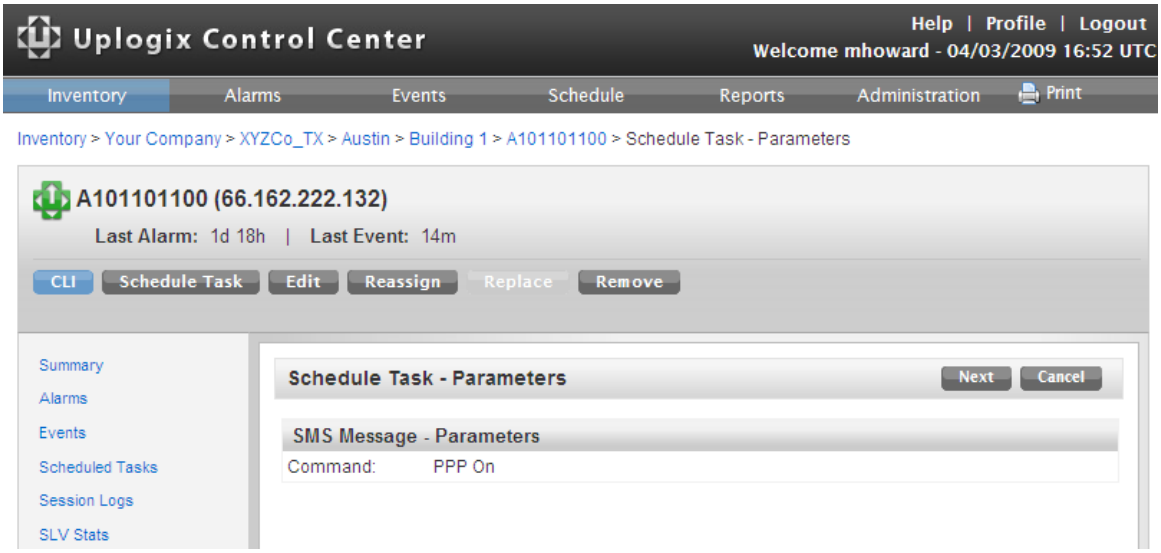
Requirements for using this capability are:

- The appliance uses an Iridium modem.
- The appliance has been configured with a phone number and SMS domain name that the Uplogix Control Center can use to construct a valid SMS email address. These are configured with the **`config answer`** command.

To initiate contact, select the appliance from the Inventory and expand the page to show the appliance detail. From the list of tasks that may be scheduled, select SMS Message and click **Next**.



The SMS Message Parameters page opens. Click **next**. The **`ppp on`** command will be sent immediately by SMS message.



A few heartbeats may elapse before the Uplogix appliance receives the message and activates PPP.

Managing scheduled tasks

You can schedule routine tasks to take place automatically. Steps in scheduling a task are:

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

A filter specifies the portion of the inventory that will be 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, you need a filter that specifies all Cisco devices within that group. Using this filter, you can schedule the Clear counters task.

Filters and filter options are limited to appliances and ports to which you have **`config schedule`** access.

Some scheduled tasks are available from the expanded appliance detail pages. These tasks are scheduled only on the individual appliance, so you do not need to select a filter.

This section covers:

- Setting up filters and scheduling tasks
- Tasks that can be scheduled
- Scheduling tasks on a single appliance
- Scheduling software upgrades on Uplogix appliances

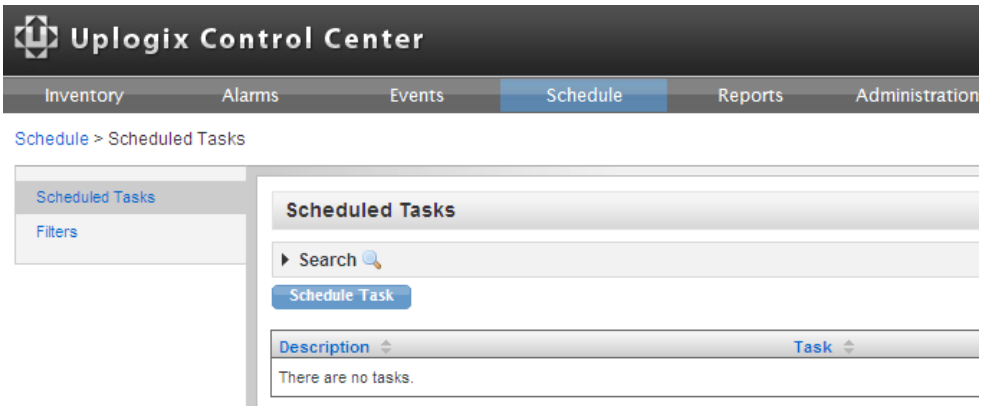
Setting up filters and scheduling tasks

Schedule

The Schedule tab allows you to schedule tasks that will be done across several devices or Uplogix appliances. Steps in this process are:

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

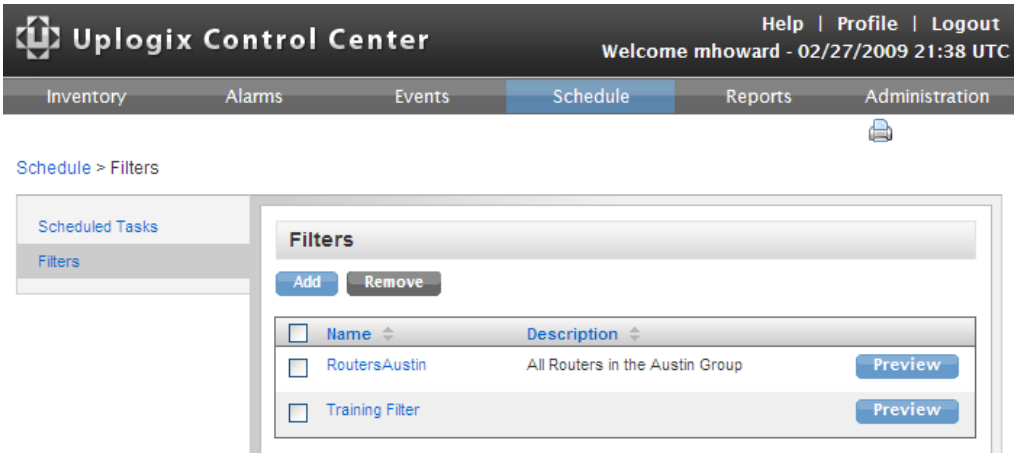
When you click the Schedule tab, the list of scheduled tasks opens. If you have not set up any filters yet, no tasks are listed and the schedule task button is not available.



You must create a filter before you can schedule a task.

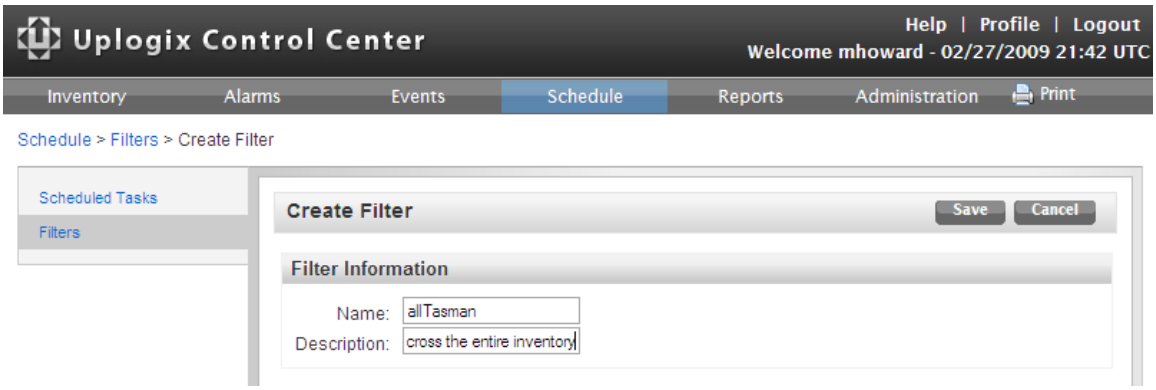
Creating a filter

To create a new filter, go to the Filter page, available from the contextual left navigation on the Schedule tab.



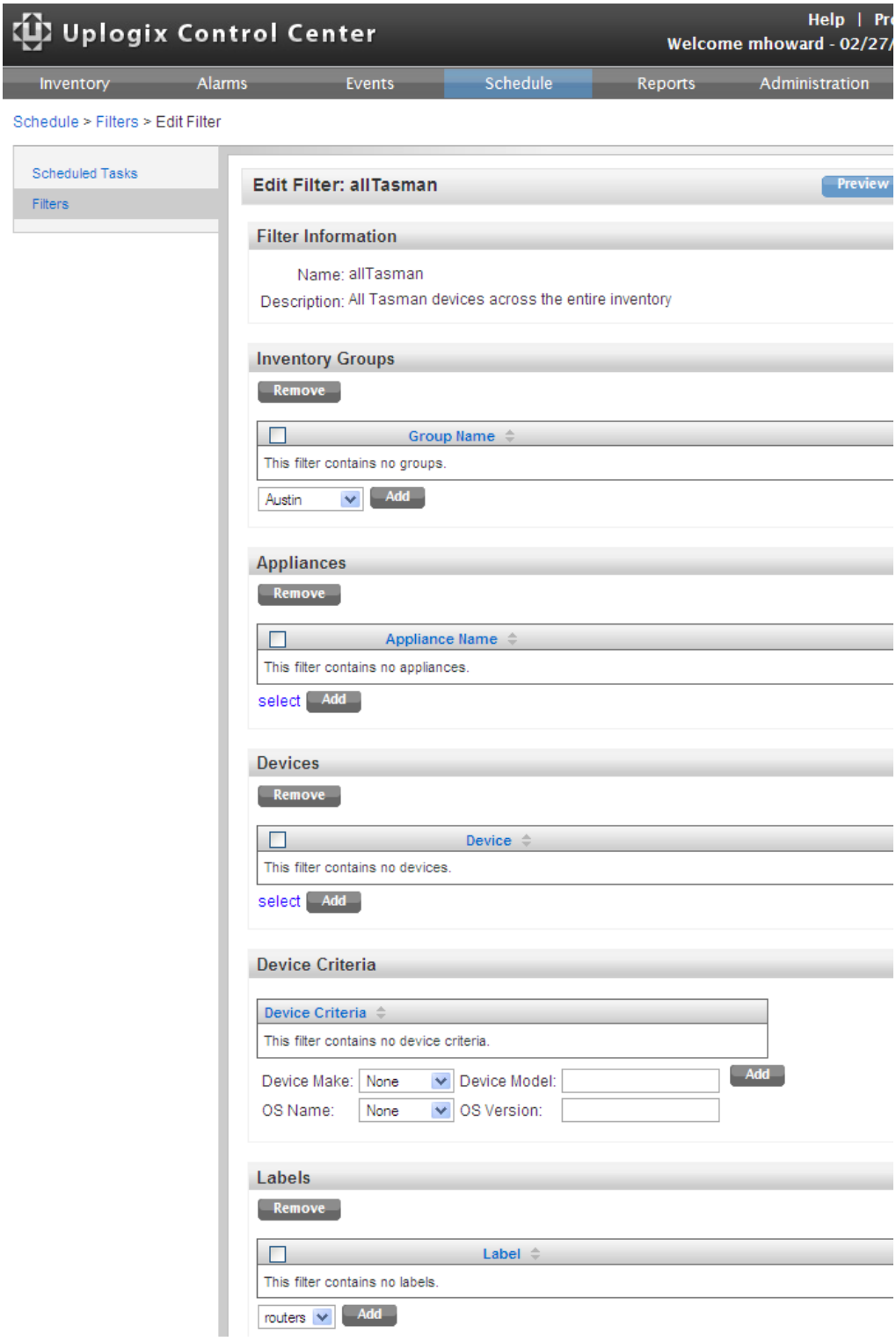
Filters are created in two steps. First, enter a name and a description for the filter. The name of the filter cannot be changed once it is created, though the filter can be deleted and recreated under a new name.

Note: When completing text fields, use only printing characters. Spaces are considered printing characters.



Click **save** to advance to the Edit Filter page.

The Edit Filter page allows you to add and delete filter criteria. If there are already options defined, they are displayed under each inventory group along with a hyperlink to remove them.



Adding filter criteria requires two steps - choosing a criterion, and clicking **add** to register your choice.

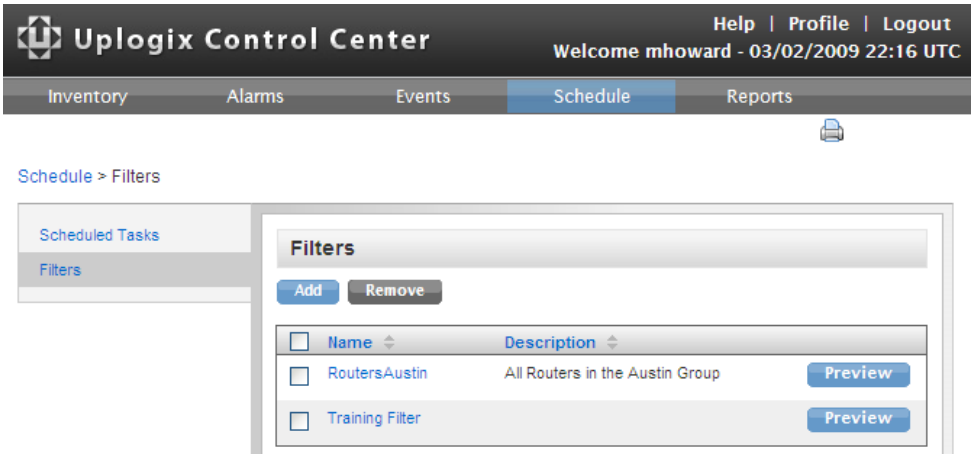
Initially, each section of the filter editor displays a message indicating that you have not added anything to this section of the filter. The Label section lets you use the port labels you have created, if any. For more information about creating port labels, see Creating your own categories to manage devices on page 45.

Device makes and operating systems, group names, and labels are presented in drop-down lists. Uplogix appliances and devices are presented in Hostname Picker dialog boxes. Click **add** after selecting any filter criterion; otherwise your selection is not saved.

Multiple criteria can be applied in each section.

Click **preview** to see which appliances and devices are affected by the filter. When you are satisfied with the way you have defined the filter, click **done** to save your changes.

The Filter Manager page now lists the filter. From this page, you can preview, edit, or delete filters.

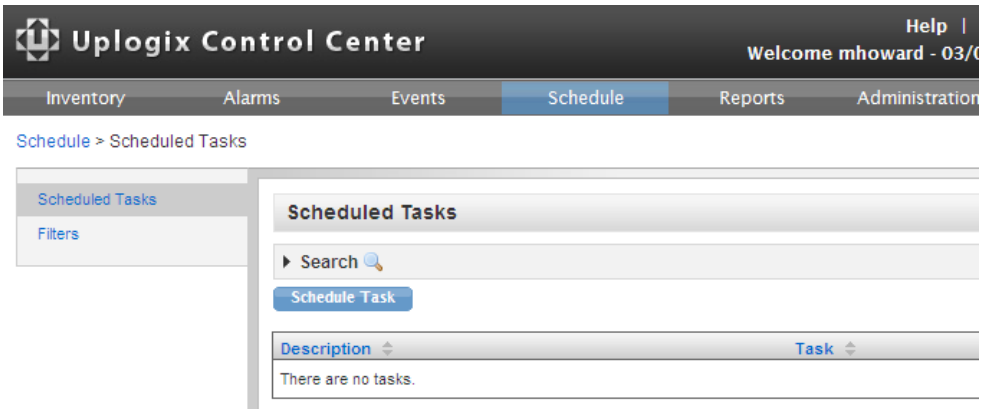


Caution: There is no delete confirmation.

Scheduling a task

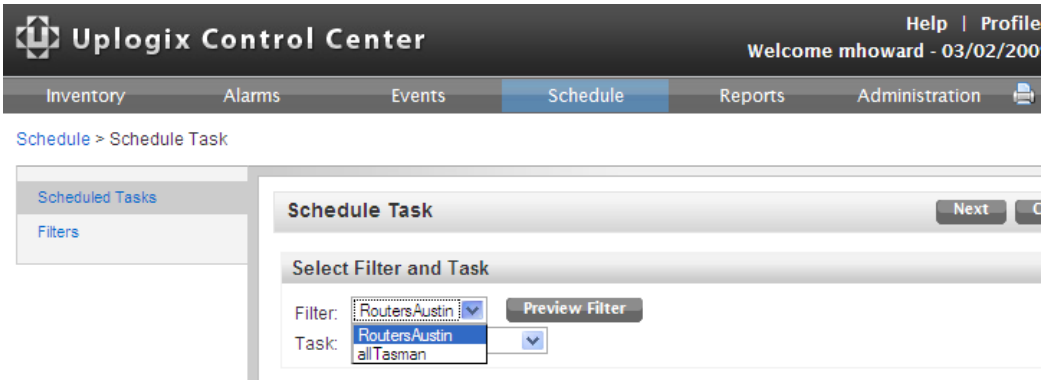
If task filters have been defined, you can schedule tasks from the Scheduled Tasks page.

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

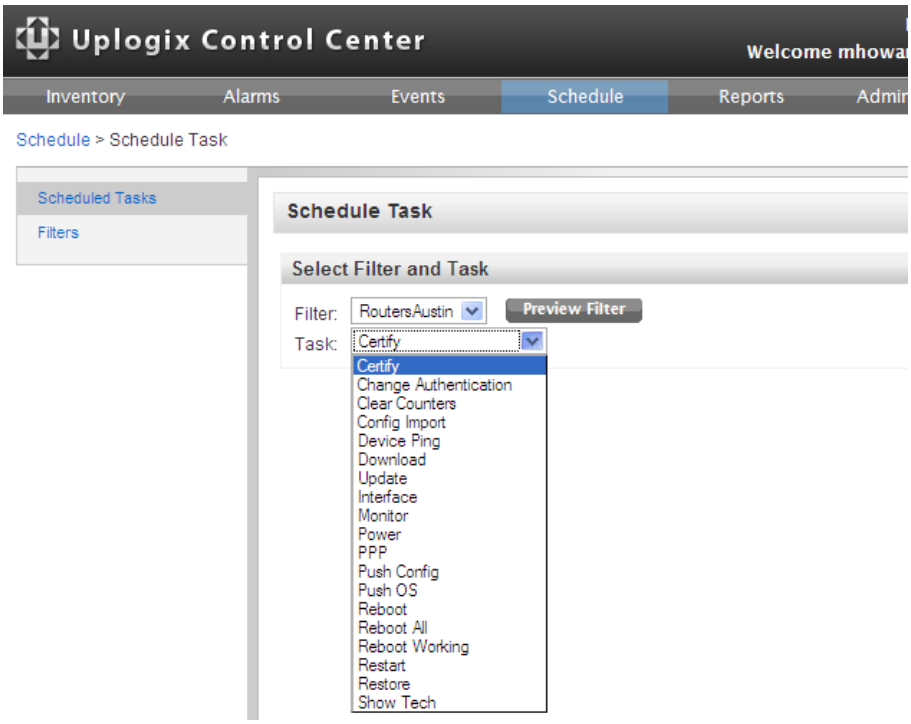


Click the **scheduled tasks** menu item in the contextual left menu to go to the Scheduled Task page.

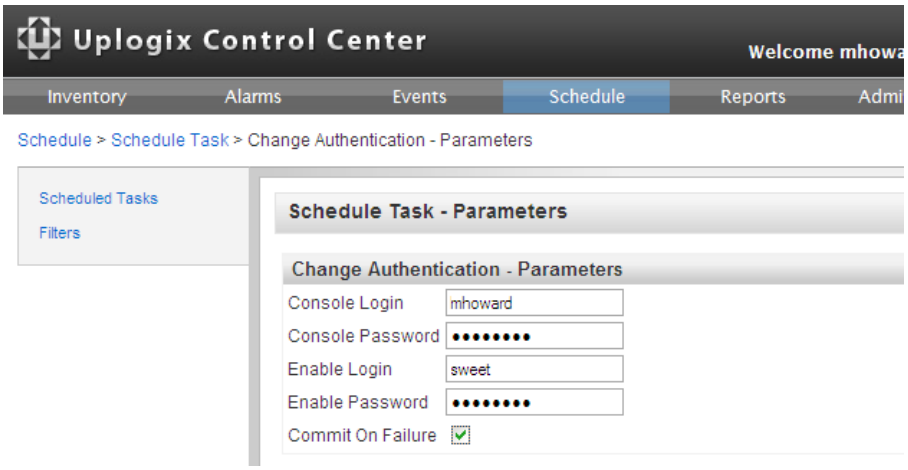
On the Scheduled Tasks page, the **Filter** list shows available task filters. Choose the appropriate filter from the list. If the filter you need is not listed, click **cancel** and create a new filter (see previous section).



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

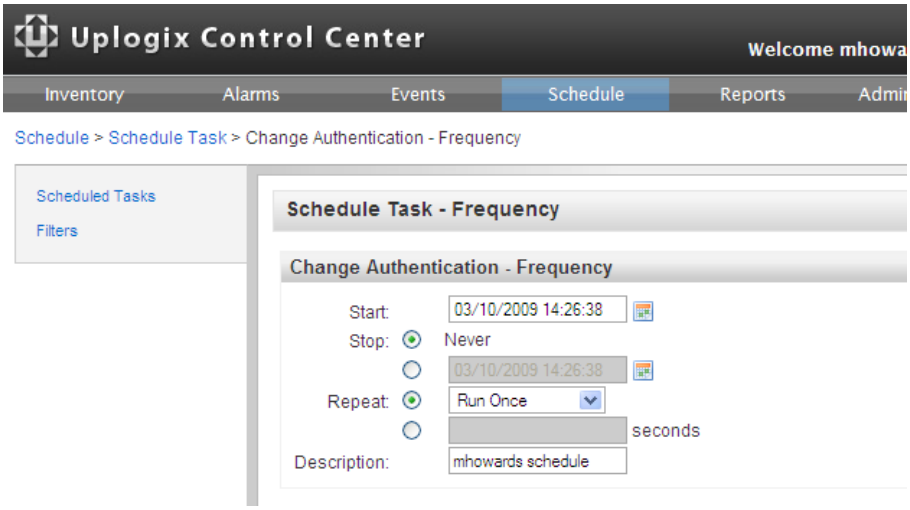


Some tasks - like Change Authentication - take more than one step to schedule; others, such as Clear Counters, present only a scheduling page.

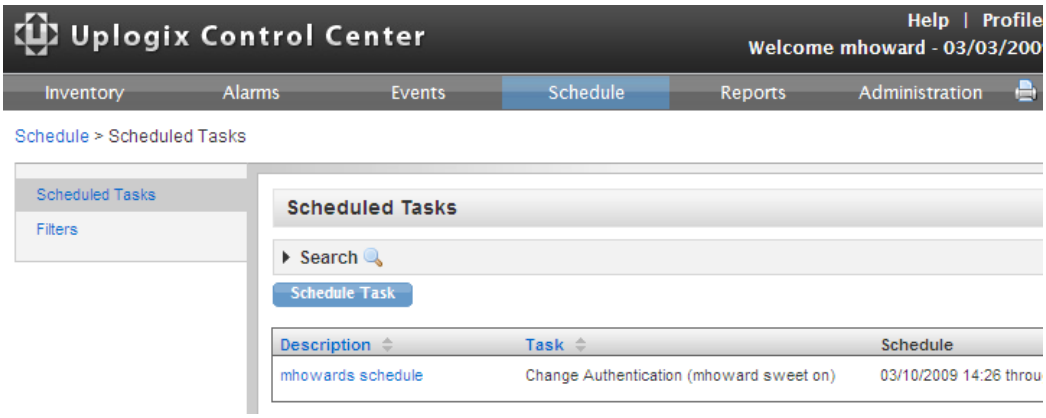


Note that the default starting date and time is the current date and time. Change the date and time if you do not want to execute the task immediately.

Complete the required information on each page, and click **schedule**.



The Scheduled Tasks list shows the new task.

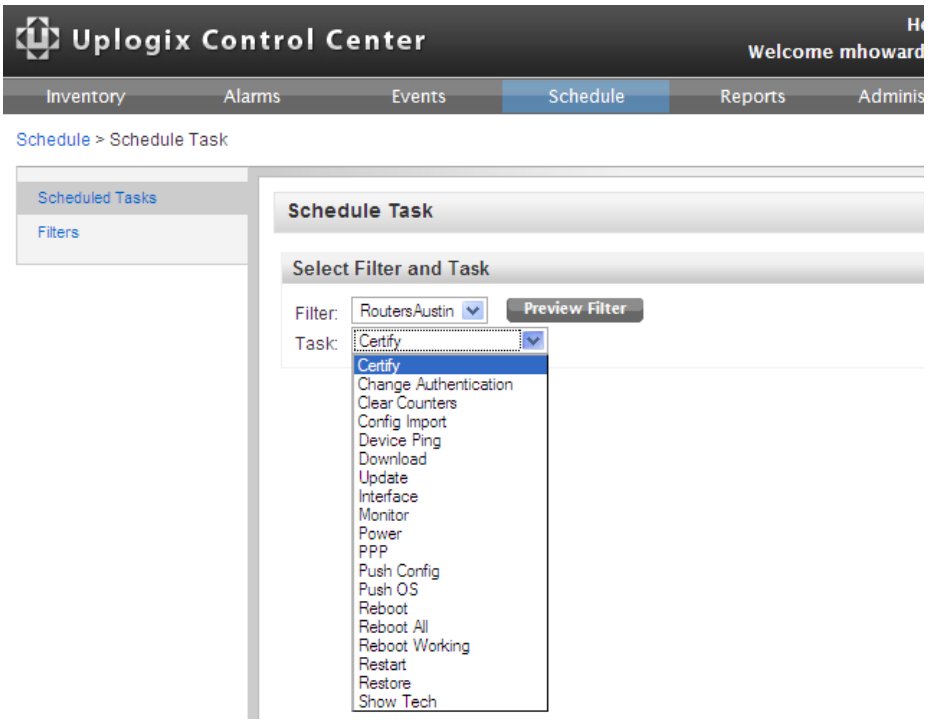


The Scheduled Tasks list provides **details**, **hold** and **cancel** controls. Click **details** to view the equipment affected by the task. To postpone the task, click **hold**; when you are ready to allow the task to proceed, click **resume**. If you do not want the task to execute, **cancel** it.

Note: 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

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



Certify – This is a Alcatel specific task.

Change Authentication - This option allows you to schedule an authentication change for a device, with the option to change the console login and password, the enable login and password, or both.

Some devices do not require usernames for console and enable access. Leave these boxes blank when scheduling for such a device.

Caution: A blank password box will clear the password and will not retain the previous password.

Note: If your browser is set to save passwords, the browser displays a dialog box asking you to confirm the password change, and presents a list of usernames that are not related to the Uplogix Control Center. Close the dialog box by clicking Cancel.

Clear Counters - This option allows you to clear interface counters on a device. All interfaces counters will be cleared. To aid in troubleshooting, this should be done regularly.

Config Import - You can automatically import appliance configuration settings by selecting this option. 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 on page 61.

Device Ping – This option allows you to schedule a ping task from a device attached to the Uplogix appliance to a target destination.

Download - This task is a step in the process of applying a file to an Uplogix appliance or a managed device - to make it available to the appliance, you must download it from the Uplogix Control Center to the appliance. Before you can download files to appliances, you may need to upload them to the Uplogix Control Center. See Uploading files from your computer to the File Archive on page 61. To download a file from the Uplogix Control Center to appliances, choose the type of file and file status based on where you would like the file saved. Then select a file to download from the File Archive.

Update - This option updates the Uplogix appliance software. The new software image must exist in the File Archive prior to scheduling.

Interface - Interfaces can be set on, off, or be cycled at a specified time. Choose the desired action and enter the name of the interface.

Monitor - Monitors can be scheduled to run at specified times.

Power - Devices can be powered on or off, or be power cycled at a specified time. Choose the desired action and if applicable, enter the delay between powering off and on.

PPP - Allows you to set PPP on or off.

Push Config - You can push a new configuration onto a device by specifying the type of file and version. These options refer to files located on the Uplogix appliance, in the port's file archive. You can also specify whether the device should be rebooted after the new configuration is loaded.

Push OS - Like configurations, operating system images can be pushed onto a device.

Reboot - You can schedule a device to reboot at a specified time.

Reboot All - This is a Alcatel specific task.

Reboot Working - This is a Alcatel specific task.

Restart - This task restarts the Uplogix Appliance.

Restore - This is a Alcatel specific task.

Show Tech - This option allows you to schedule a **`show tech`** command on the device and automatically save the output to the Uplogix appliance.

Scheduling tasks on a single appliance

Inventory > Appliance Page

You can schedule the following tasks for a specific Uplogix appliance from the appliance's detail page:

Config Import - Allows you to import a configuration file. The appropriate file must be present in the File Archive. See Uploading files from your computer to the File Archive on page 61.

Update - Allows you to schedule a software update for the appliance. The appropriate file must be present in the File Archive already; otherwise you will not be able to schedule the update.

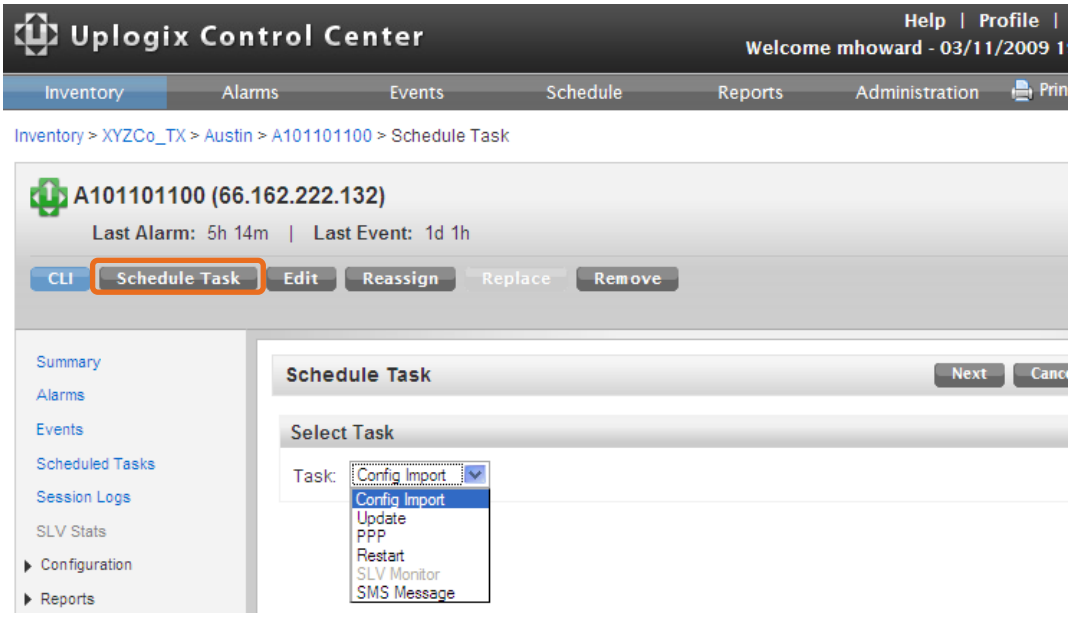
PPP - Allows you to schedule a PPP on or PPP off action.

Restart - Allows you to restart the appliance.

SLV Monitor - Allows you to set up SLV monitors. This task is only available 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 ***Guide to Rules and Monitors***.

SMS Message - Allows you to send the `ppp on` command to reestablish contact with an Uplogix appliance connected to an Iridium satellite modem. This task is not scheduled; it occurs immediately.



Scheduling software upgrades on Uplogix appliances

You can automate the process of upgrading your Uplogix appliances.

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 appliances that the Uplogix Control Center manages, you will need to download the software upgrade to your computer and then upload it to the Uplogix Control Center.

Point your browser to www.uplogix.com/support. 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 Technical Support at support@uplogix.com.

Uploading files from your computer to the File Archive

After you have downloaded the desired file to your computer, go to the Uplogix Control Center's **Administration > File Archive** page.

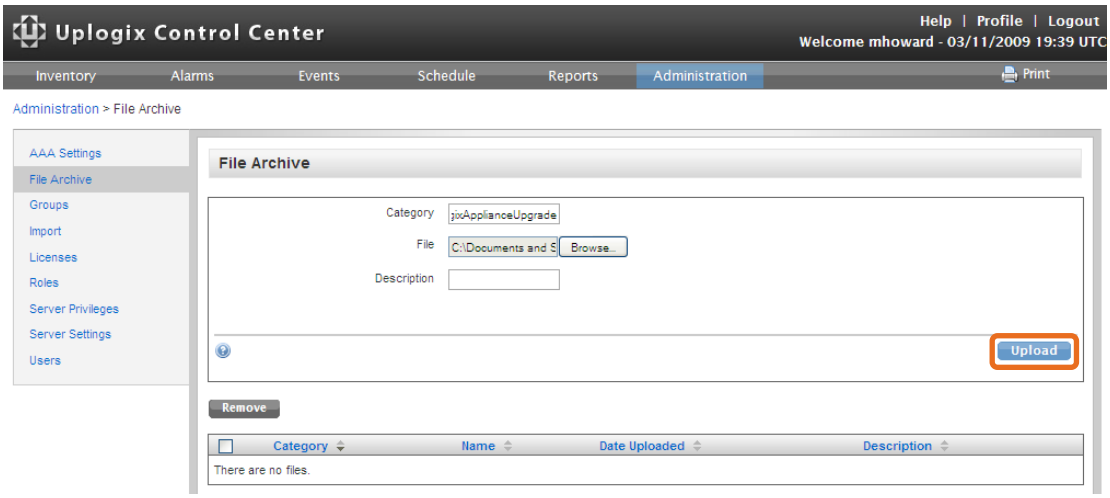
Any files present are displayed with category, filename, upload date, and description information.

Choose a category for the file being uploaded. If the category you enter does not exist, it will be automatically created.

Note: Do not use spaces in the category name.

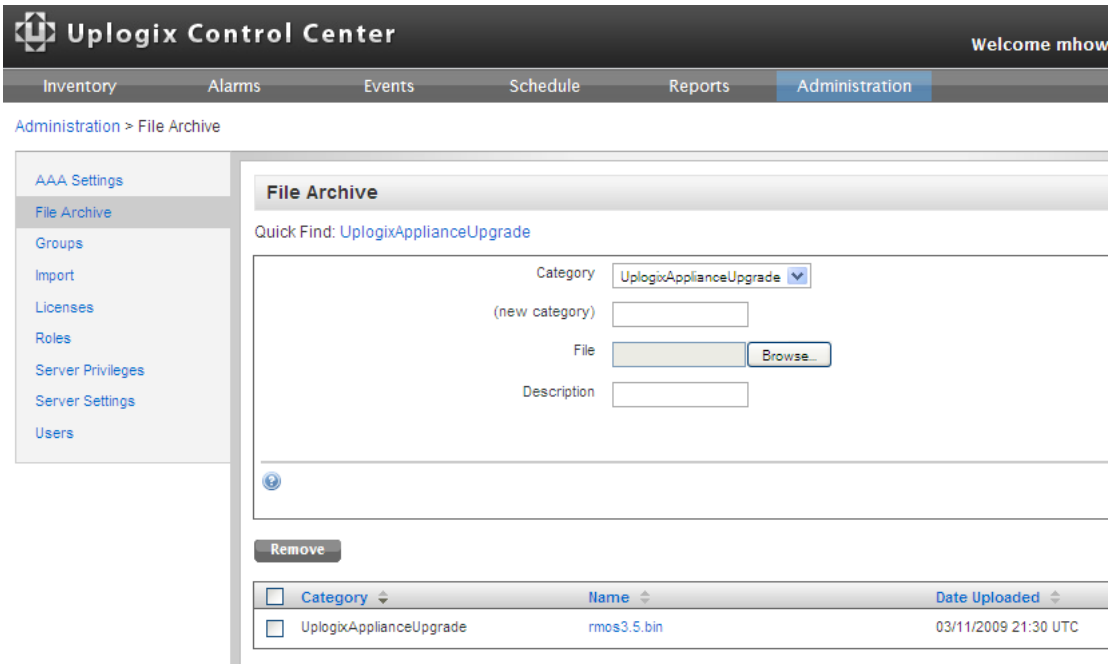
Browse to the file that is to be uploaded, and select it. If you upload a file with the same name as a file currently in the selected category, your upload will overwrite the existing file.

The file description is optional, but can be helpful in identifying the file.



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 3.4 to 3.5), always upgrade the Uplogix Control Center first. Uplogix appliances cannot heartbeat properly to an Uplogix Control Center using an earlier release of software. This is not necessary for patch releases (for example, 3.5 to 3.5.x).

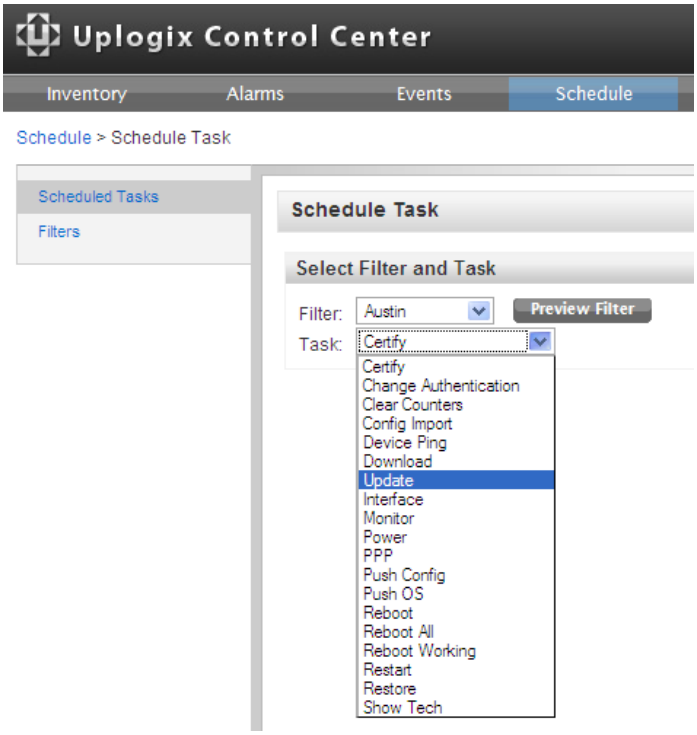
Scheduling the update task for more than one appliance

To schedule the update, there must be a task filter that specifies the Uplogix appliances to be upgraded. For information about creating filters, see Setting up filters and scheduling tasks on page 51.

On the **Schedule** tab, click **schedule task** to open the Schedule Task window.

Choose the filter that specifies the appliances to be upgraded. Then select the **Update** task.

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



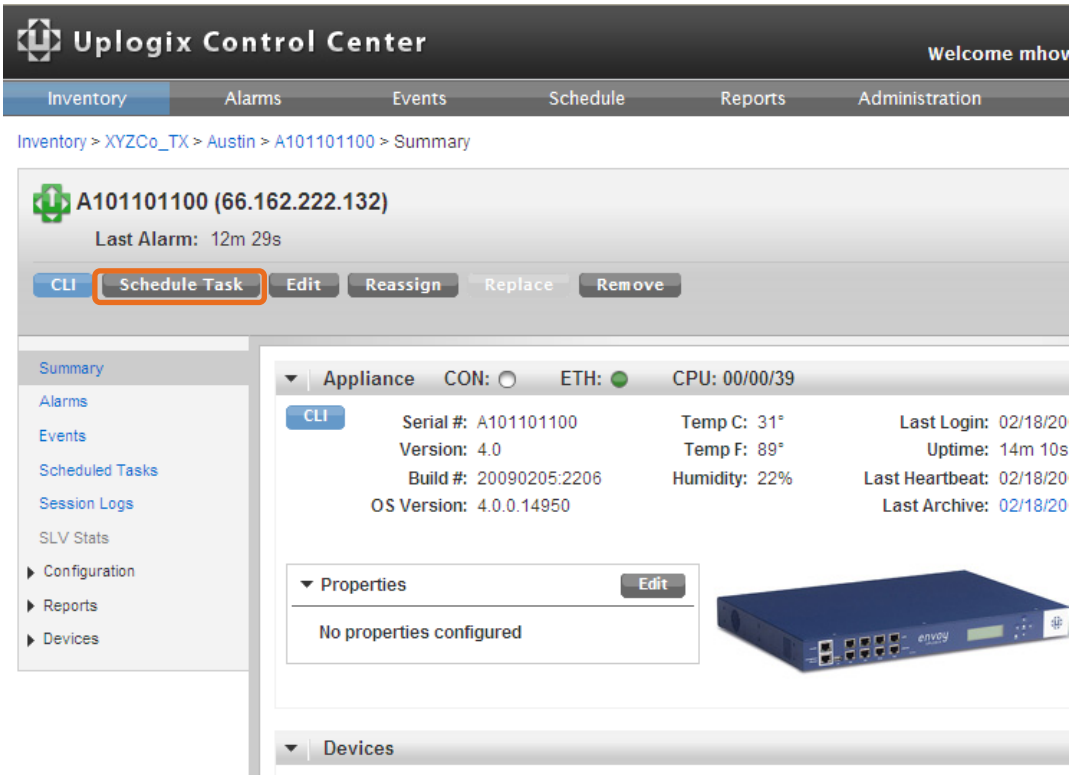
Continue as for scheduling any task.

Scheduling the update task on a single appliance

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

Open the **Inventory** tab and navigate to the appliance.

Ensure that the appliance has been moved out of the Unassigned group.



Click the **Schedule Task** button then select **Update** as the task type and click **next** to open the Schedule Task Parameters page.

From the list of Schedule Task Parameters page, select the file you just uploaded and click **next**.

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 in 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***.

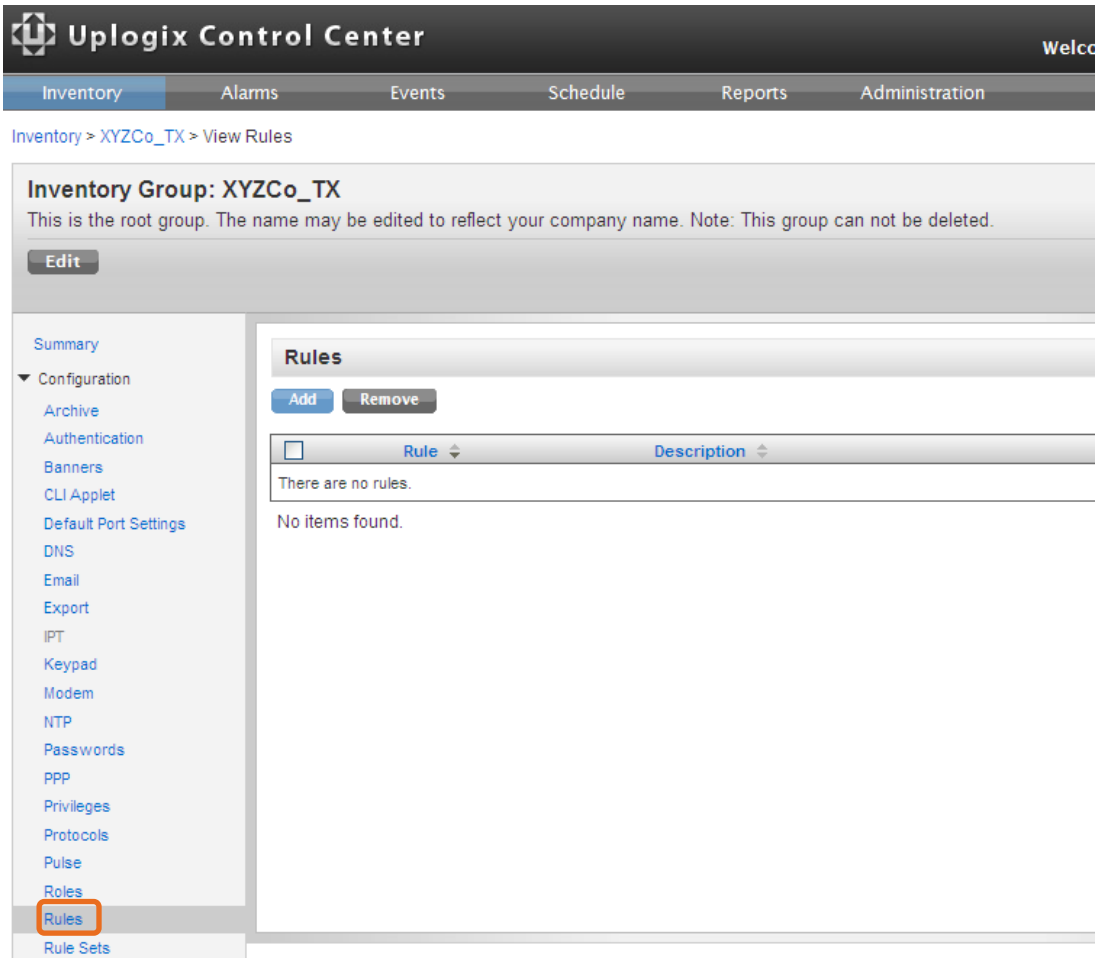
Working with rules

Inventory > Configuration > Rules

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

Access the Rules screen by clicking **rules** from the Configuration menu at a group detail or appliance detail page.

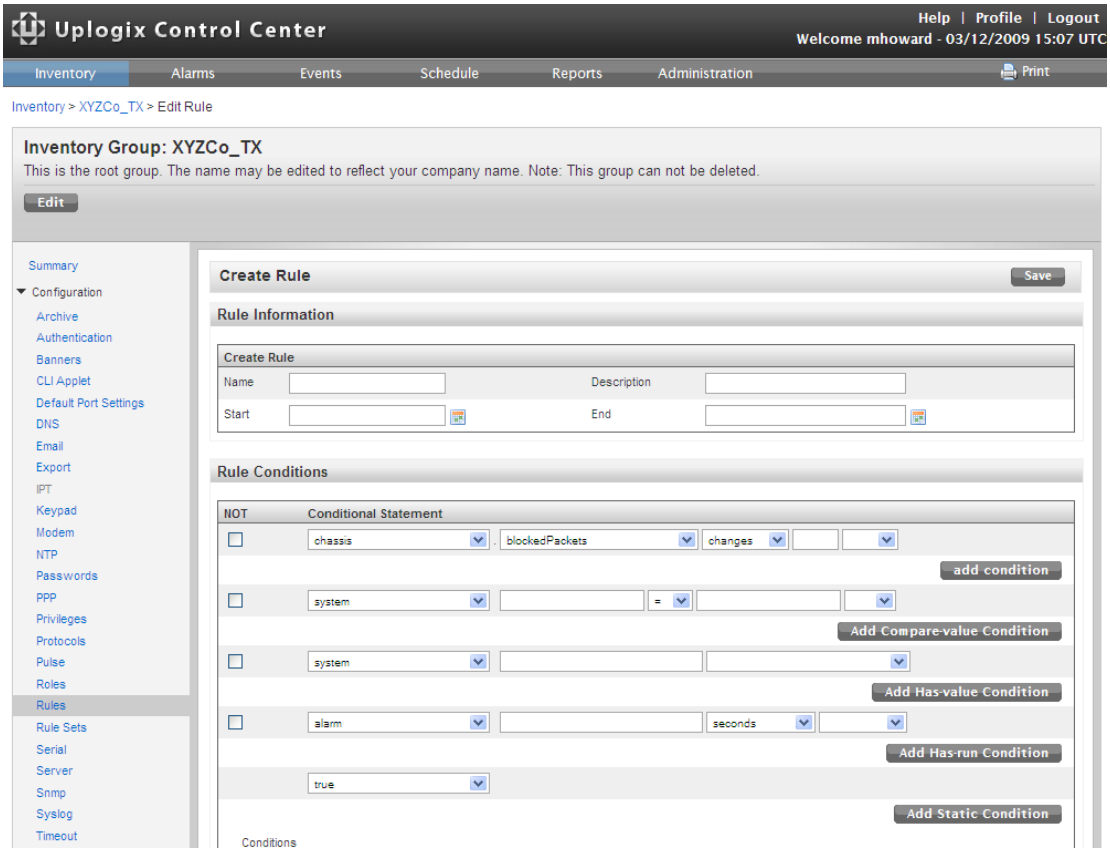
From the View Rules page, you can edit existing rules or create new ones.



Click **create rule** on the View Rules page to start a new rule. This is equivalent to issuing the **`config rule`** command from the RMOS command line.

Note: Do not use spaces in the rule name.

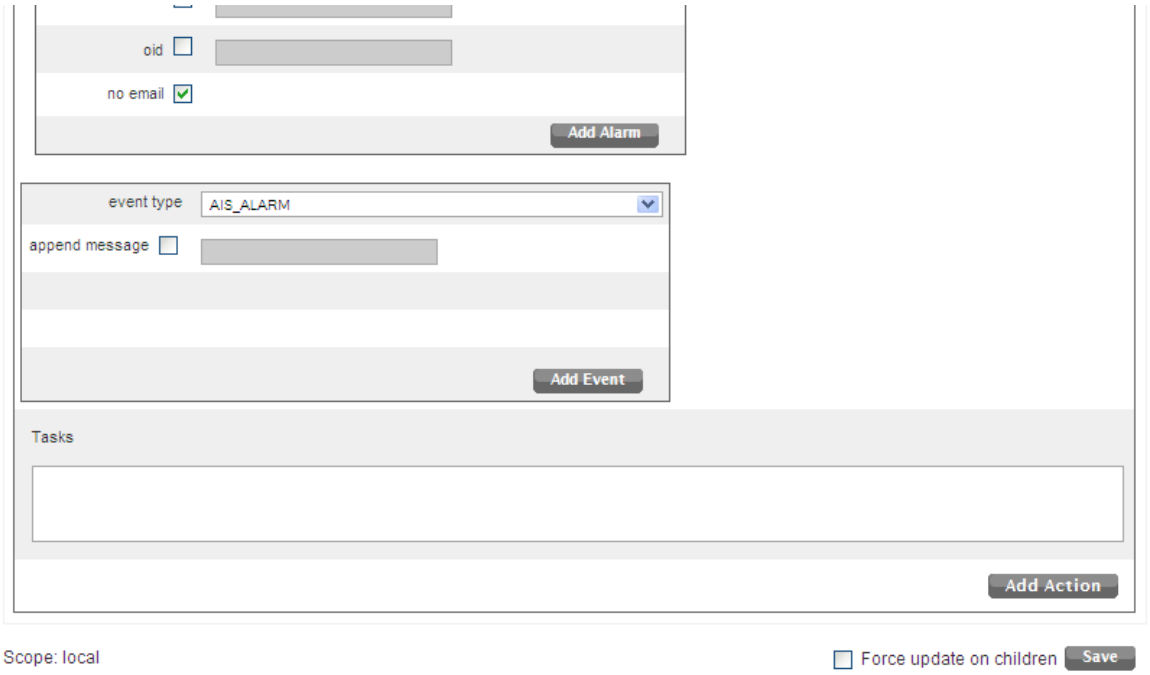
The Edit Rule page contains drop-down menus and lists of the same options available from the rules editor within the RMOS command line.



Conditions can be edited manually in the Conditions text box or added with the drop-down menus below it. 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.



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

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

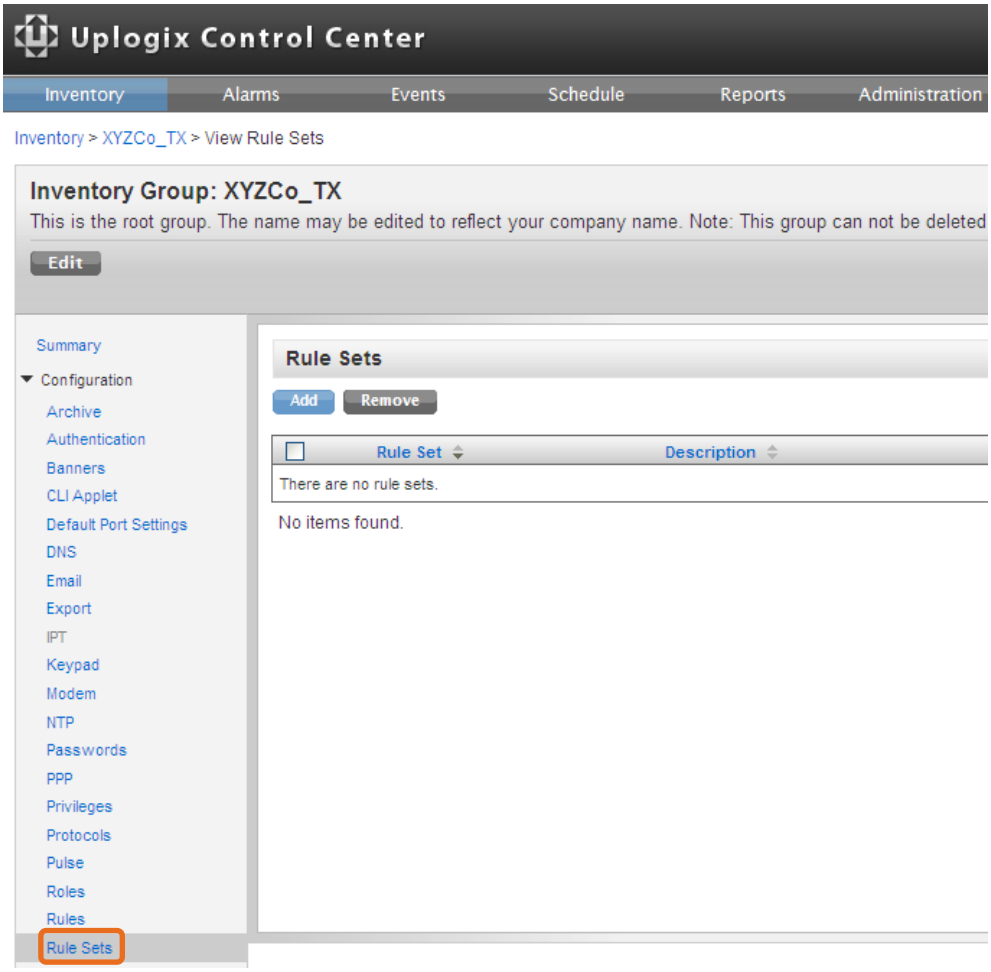
Reference information is available at www.uplogix.com/support and includes rule examples, default rules, and condition variables.

Working with rule sets

Some rules are often used together. You may find it convenient to group them into rule sets. When you create monitors, available rules and rule sets are presented together.

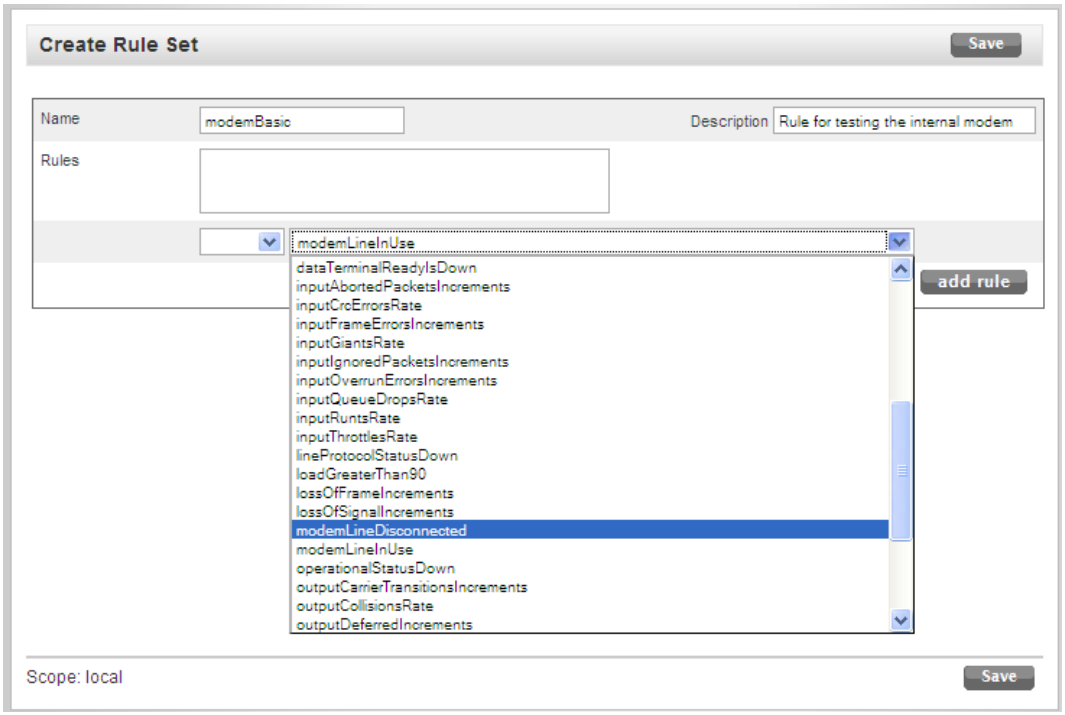
Access the Rule sets screen by clicking **rule sets** from the Configuration menu on a group detail or appliance detail page.

Any rule sets that exist are listed on the View Rule Sets page.



To create a rule set, click **add**.

In the Create Rule Set window, provide a name and (optionally) a brief description for the rule set.

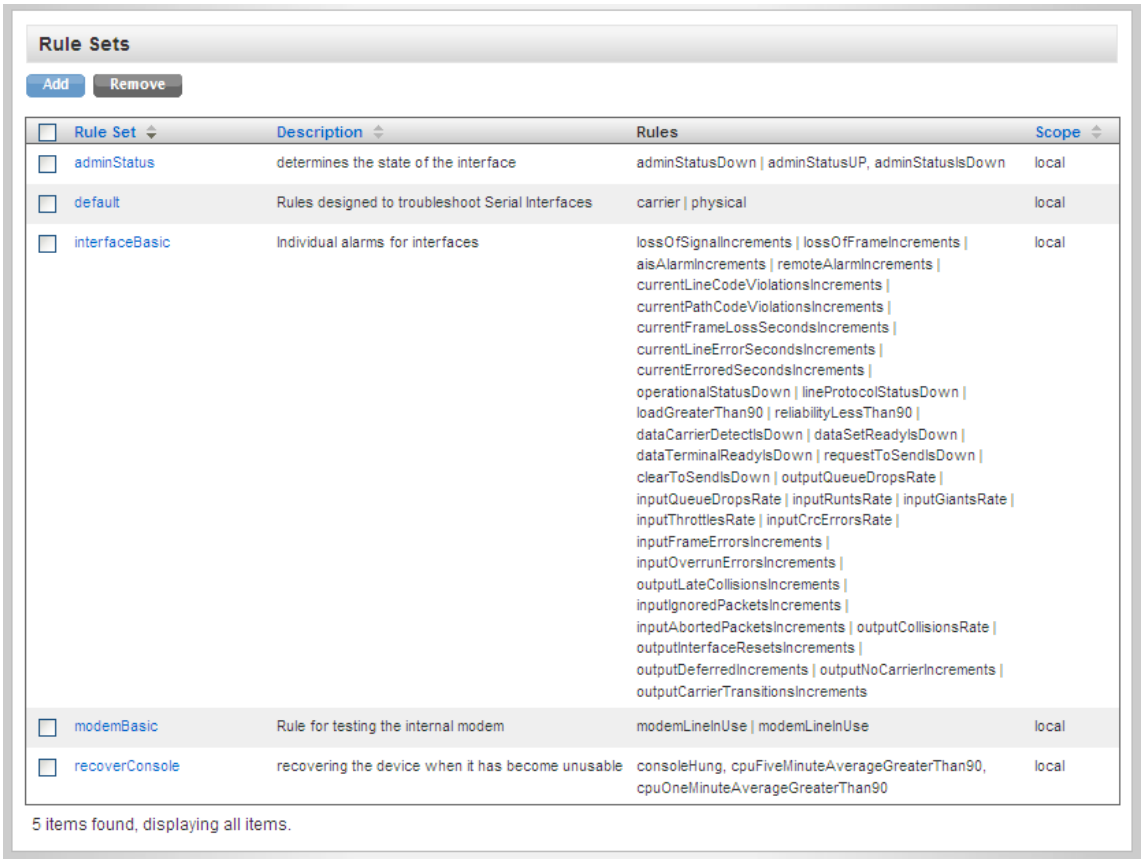


Select the first rule from the list of available rules, and click **add rule**.

Select the relationship (AND; OR) of the first rule to the second from the list to the left of the rules, then select the second rule.

Continue until you have added all the desired rules to the rule set. Click **save** to save the rule set.

The new rule set is listed on the View Rule Sets page.

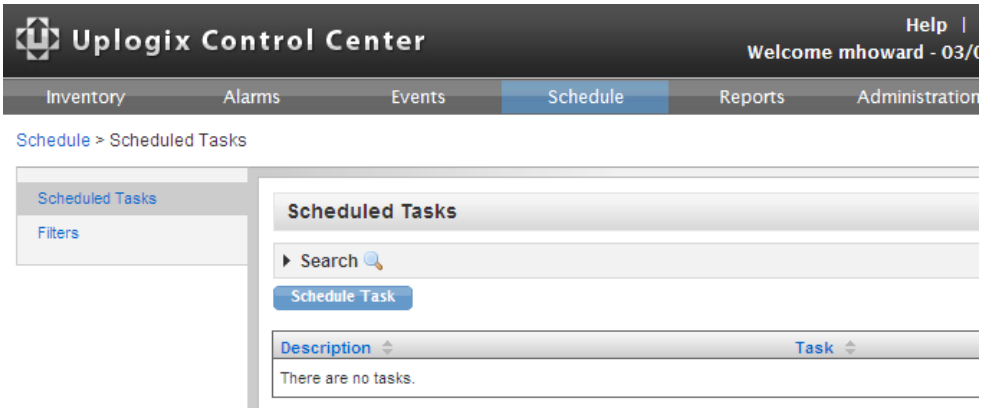


Scheduling monitors

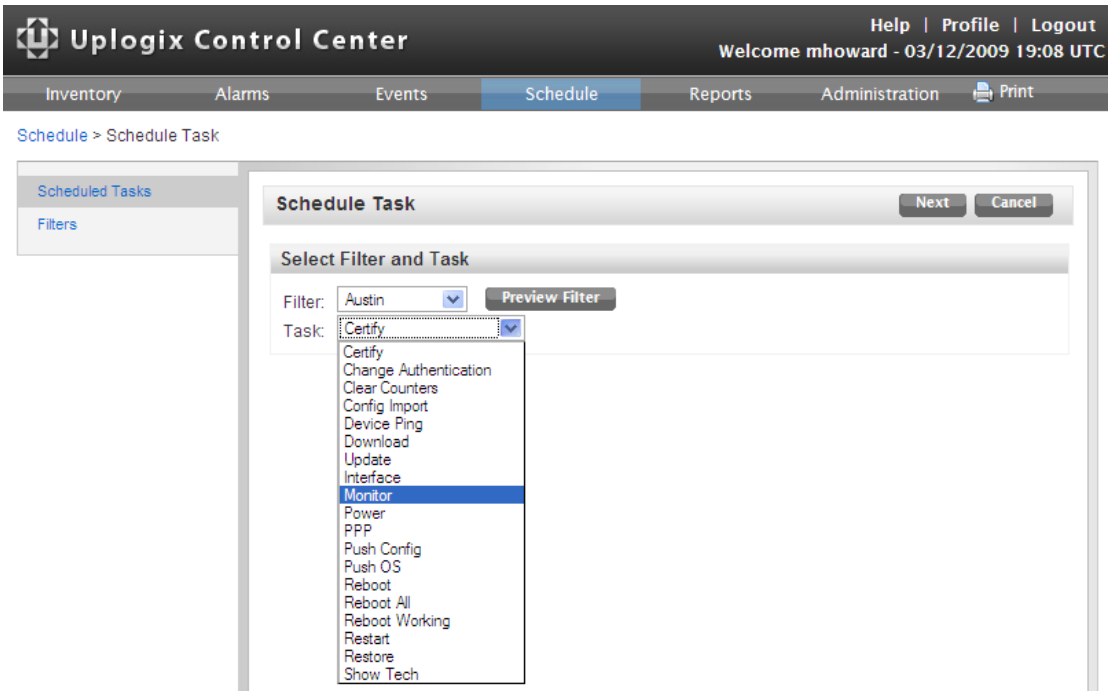
Inventory > Appliance > Port > Schedule Task

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 appliances.

To create a monitor, go to **Inventory > Appliance > Port >** and click **schedule task** to open the Schedule Task page.



On the Schedule Task page, select or create a filter to specify what equipment will be monitored. Then select **Monitor** from the list of tasks, and click **next**.

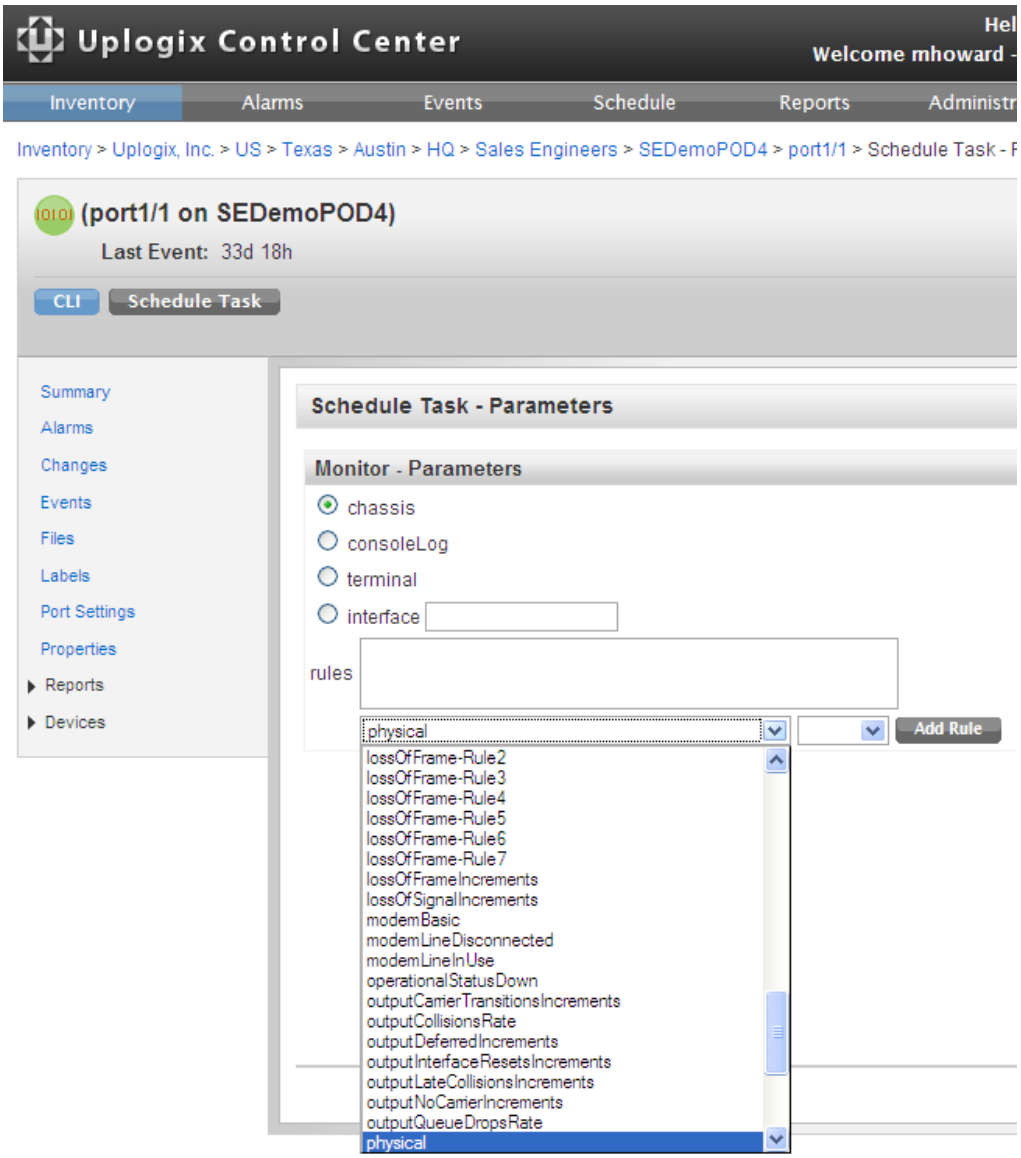


On the **Monitor - Parameters** page, choose the type of monitor. If it is an interface monitor, specify the interface to be monitored - for example, Serial0.

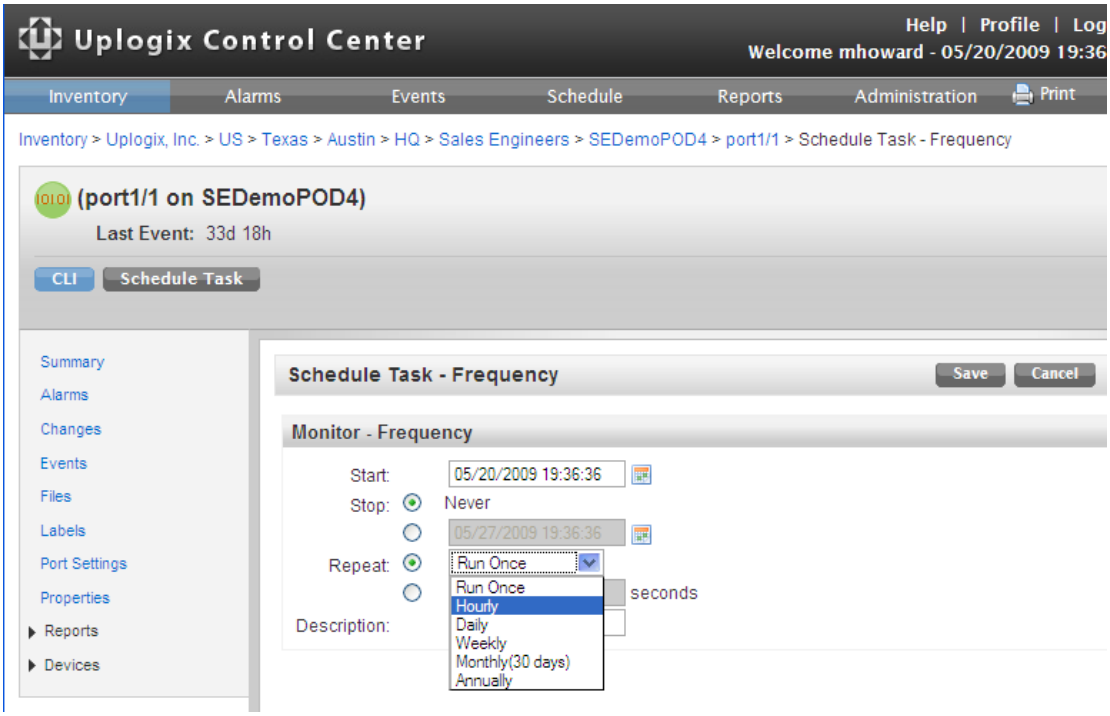
You can set up the monitor without adding rules. The appliance will gather and store the data without acting on it. To do this, click **next** to go to the scheduling window.

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**.

To add another rule, select the rule and its relation to the rule you already added. Then click **add rule**.


Uplogix Control Center
Welcome mhoward -
Inventory
Alarms
Events
Schedule
Reports
Administr
Inventory > Uplogix, Inc. > US > Texas > Austin > HQ > Sales Engineers > SEDemoPOD4 > port1/1 > Schedule Task - F
(port1/1 on SEDemoPOD4)
Last Event: 33d 18h
CLI
Schedule Task
Summary
Alarms
Changes
Events
Files
Labels
Port Settings
Properties
Reports
Devices
Schedule Task - Parameters
Monitor - Parameters
chassis
consoleLog
terminal
interface
rules
physical
Add Rule
lossOfFrame-Rule2
lossOfFrame-Rule3
lossOfFrame-Rule4
lossOfFrame-Rule5
lossOfFrame-Rule6
lossOfFrame-Rule7
lossOfFrameIncrements
lossOfSignalIncrements
modemBasic
modemLineDisconnected
modemLineInUse
operationalStatusDown
outputCarrierTransitionsIncrements
outputCollisionsRate
outputDeferredIncrements
outputInterfaceResetsIncrements
outputLateCollisionsIncrements
outputNoCarrierIncrements
outputQueueDropsRate
physical

On the **Monitor - Frequency** page, specify the schedule for this monitor and optionally give it a brief description. Then click **save**. The monitor will run as scheduled, and will appear on the Scheduled Tasks page.



Although the default interval for monitors is 30 seconds, you can change this.

Canceling monitors

To cancel a monitor, go to the Scheduled tasks page. Locate the monitor to be canceled and click the cancel link. The canceled monitor is still shown but struck out on the Scheduled tasks list.

Managing accounts and security

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

Note: Accounts created on the Uplogix appliance 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 appliances 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 > Appliance detail > Configuration > Authentication

The Uplogix Control Center and Uplogix appliances 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

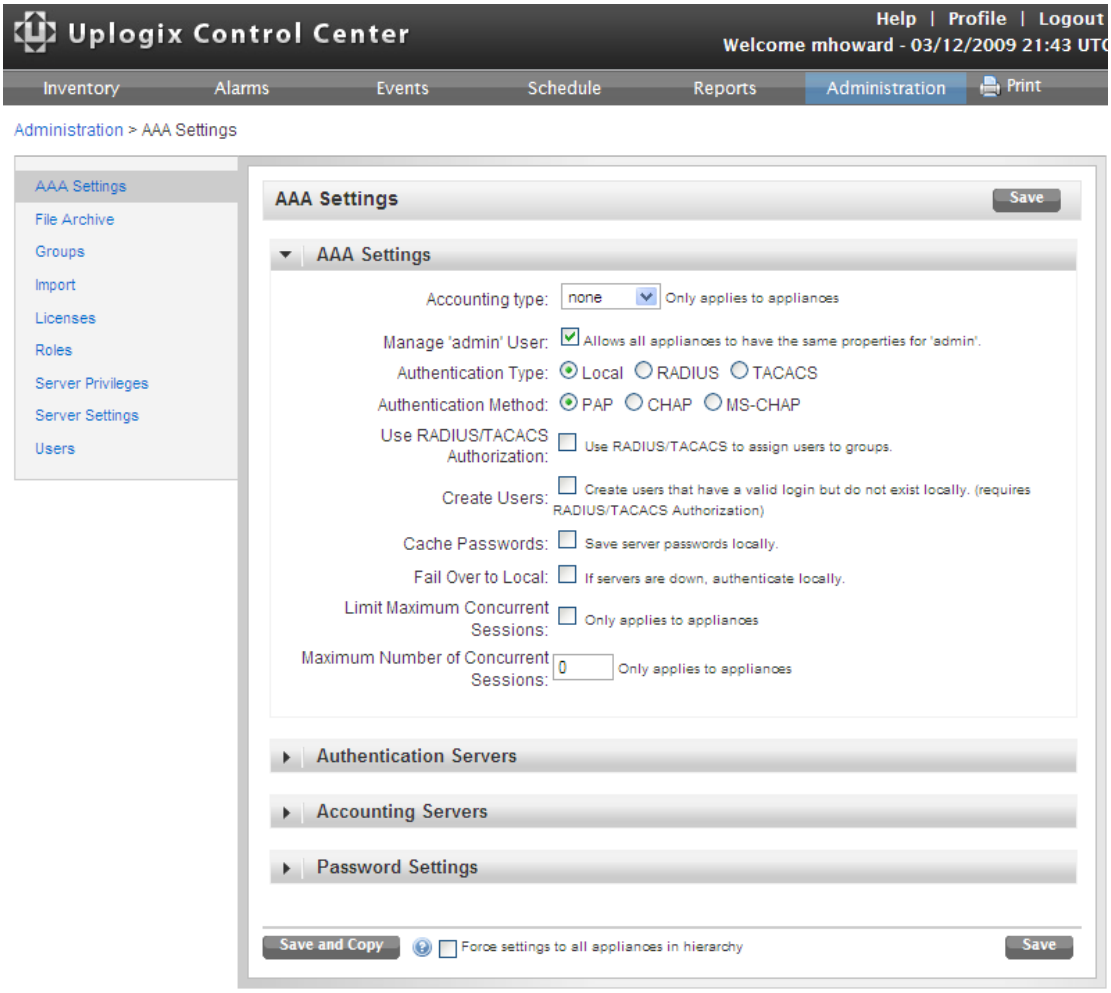
Setting authentication globally or within the inventory

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.



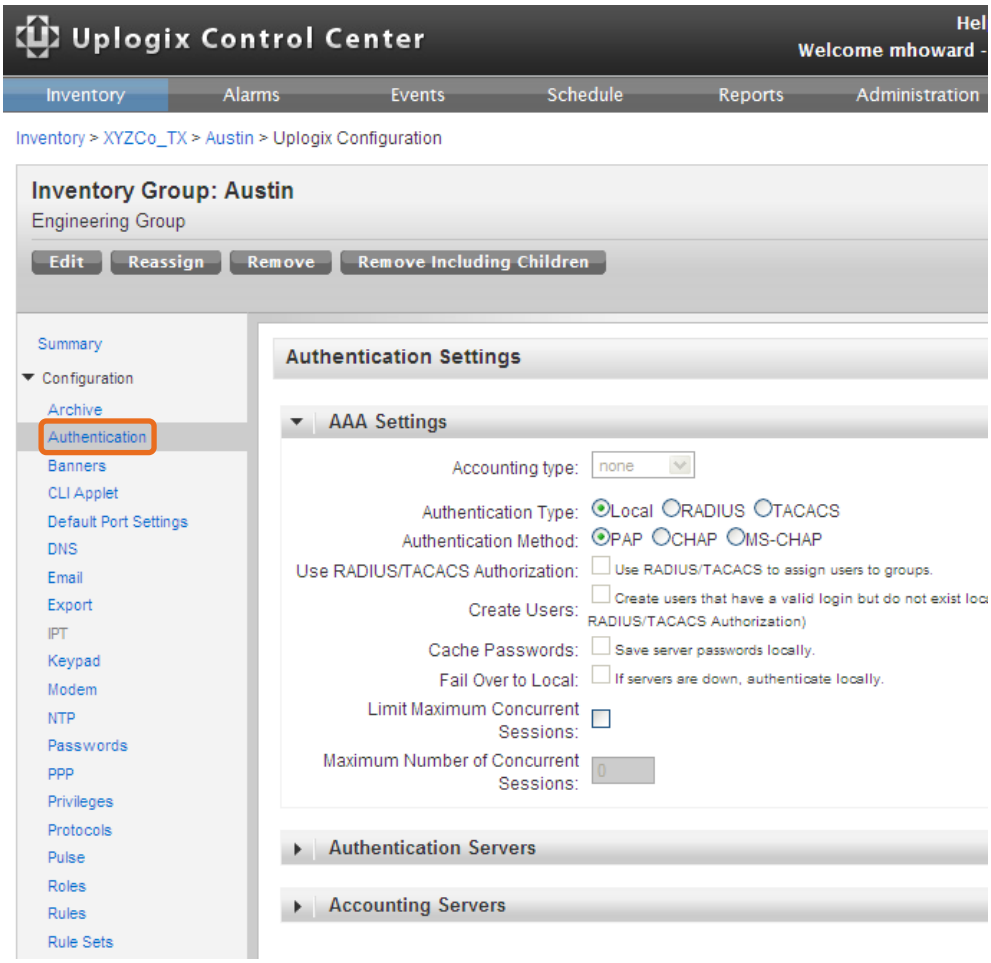
For information on configuring accounting and authentication, see Authentication, authorization, and accounting (AAA) settings on page 78.

- To apply changes on this page to the Uplogix Control Center only, click the **save** button at the bottom of the page.
- To copy the changes on this page to the root-level inventory group, click the **save and copy** button. Like other inventory settings, the authentication settings will 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 appliances managed by this Uplogix Control Center, select **Force settings to all appliances in hierarchy** before you click the **save and copy** button.

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.



Settings available on the Uplogix Configuration page are inherited by all the members of this inventory group, except where they would overwrite existing settings. The **Force update on children** option beside the **save** button allows you to overwrite all existing settings.

For information on configuring accounting and authentication, see Authentication, authorization, and accounting (AAA) settings (next page).

Setting authentication for a single appliance

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

Authentication, authorization, and accounting (AAA) settings

Administration > AAA Settings

Inventory > Group Detail > Configuration > Authentication

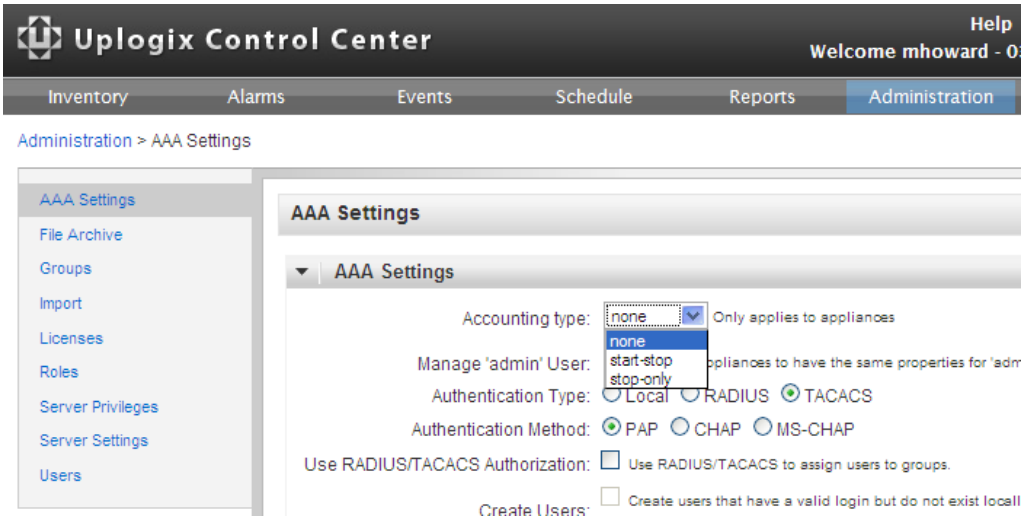
Inventory > Appliance > Configuration > Authentication

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 appliance within the inventory. Navigate to the appropriate page to configure AAA settings.

While either TACACS or RADIUS can be used for authentication and accounting, TACACS can also be used to manage user privileges. For more information about this capability, see Using TACACS to manage privileges on page 99.

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 appliances only; however, you can set it for all appliances by navigating to **Administration > AAA Settings**.



Managing the appliances' admin account

Administration > AAA Settings

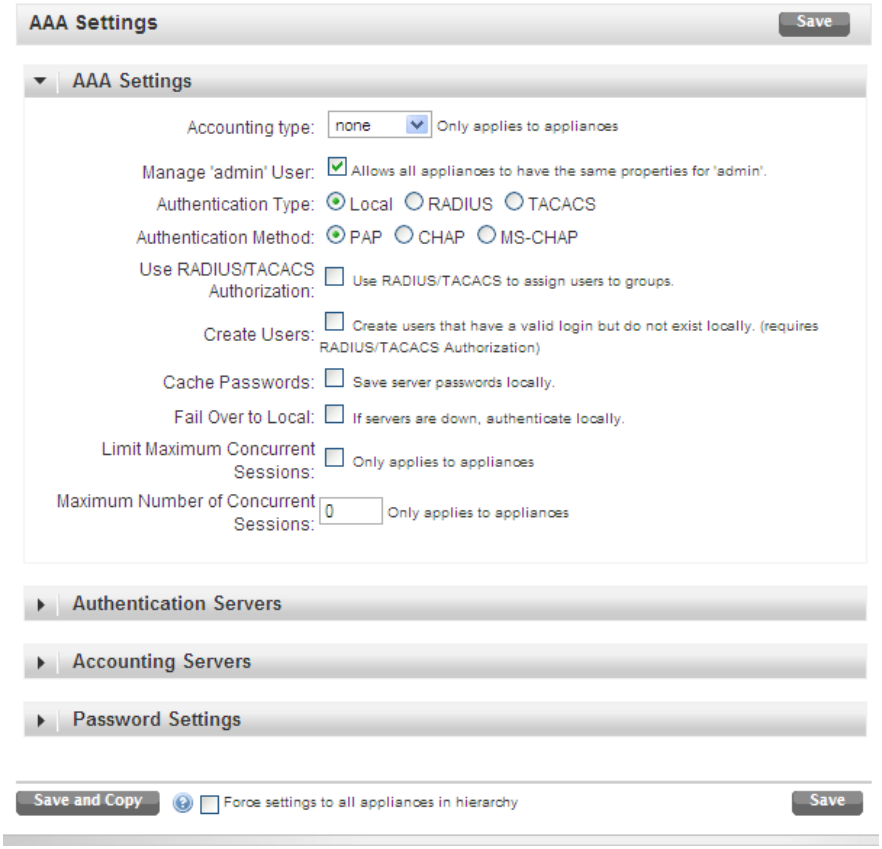
For security, you may wish to limit or disable the default `admin` account that is part of every Uplogix appliance's factory configuration.

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 appliances or otherwise modify this account. If this choice is not selected, the `admin` account will not be 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 RMOS 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 appliance level are also available at the inventory group level and globally. Some additional settings are available at the inventory group or global levels.



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.

Note: If the Uplogix Control Center is configured to use one or more authentication servers, or accounting servers, the managed Uplogix appliances should use the same servers.

Use TACACS Authorization - Some TACACS 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 TACACS to manage privileges on page 99.

Create Users - If users are managed on the authentication server, they will be able to authenticate but will not have accounts on the Uplogix Control Center or Uplogix appliance. If this setting is enabled, the user will be created. If TACACS authorization is not used, users will initially have no privileges - so they will not be 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 log in 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. If you use this setting, enable **Cache Passwords** to make the passwords available for local authentication.

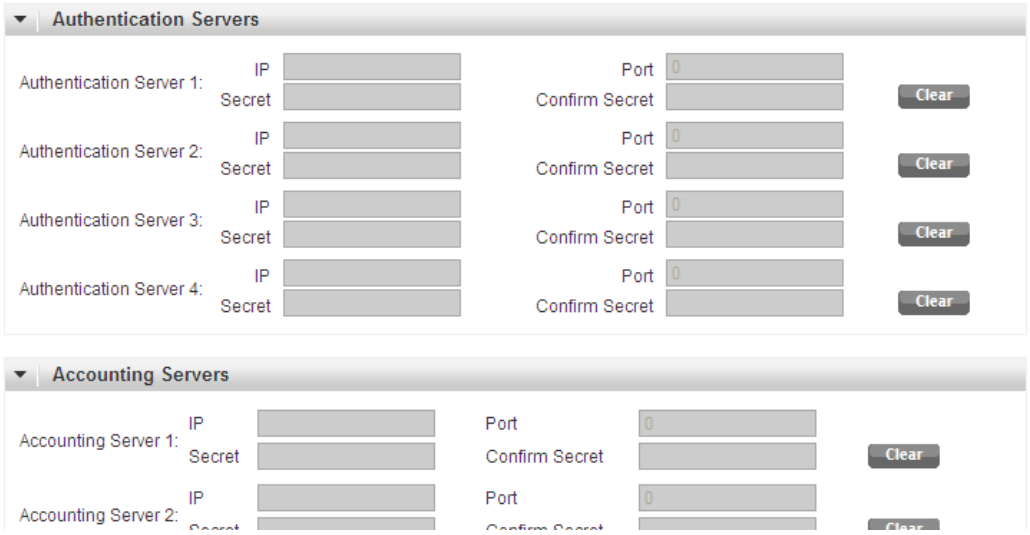
Limit Maximum Concurrent Sessions and **Maximum Number of Concurrent Sessions** - These settings allow you to limit the number of open sessions that any user may have on any particular Uplogix appliance at a given time. Set the maximum number to 0 to allow unlimited concurrent sessions.

Authentication and accounting servers

If you configure the Uplogix Control Center or appliances within the inventory to use RADIUS or TACACS, you must configure at least one of the appropriate type of server. 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 1812; for TACACS, the default port is 49.

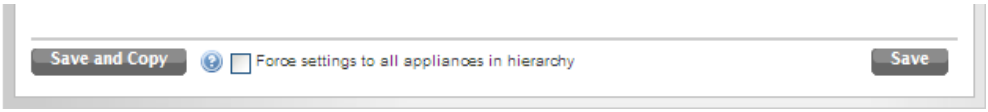
To remove server information that you have already configured, use the **clear** button associated with that server.



Choosing how to apply AAA changes

When you make changes on the **Administration > AAA** page, you can 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 appliances currently in the inventory - click **save and copy**.
- Update AAA settings globally, overwriting existing settings on the Uplogix Control Center and all Uplogix appliances - select **Force settings to all appliances in hierarchy**, then click **save and copy**.



When you make changes at the inventory group level from the Authentication page, you can apply them without changing settings on appliances currently in the group, or you can overwrite the appliances' authentication settings.

- Update AAA settings for the group without changing settings on Uplogix appliances currently in the inventory - click **save**.

- Update AAA settings for the group, overwriting existing settings on all Uplogix appliances in the group and its child groups - select **Force updates on children**, then click **save**.

Setting requirements for strong passwords

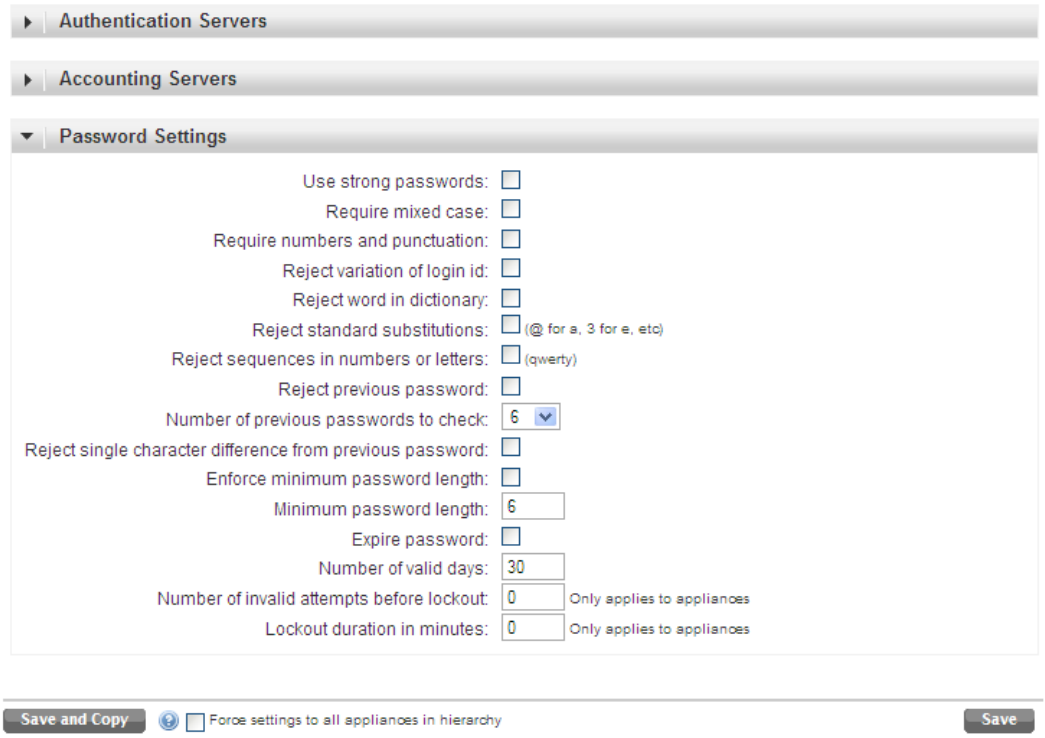
You can configure strong passwords at any level within the inventory, on the Uplogix Control Center only, or globally. You can also tailor the password requirements separately for different groups or appliances within the deployment. For a detailed description of how to apply settings globally or within a subset of the deployment, see Setting authentication globally or within the inventory on page 76.

Global or Uplogix Control Center only: **Administration > AAA Settings**

Inventory group: **Inventory > Group Detail > Configuration > Passwords**

Single appliance: **Inventory > Appliance> Configuration > Passwords**

You must select **Use Strong Passwords** for your password restrictions to take effect. If you need to remove strong password restrictions temporarily, you can clear **Use Strong Passwords** while leaving the restrictions configured.



Restrictions include:

Require mixed case – Password must have both capital and lowercase characters. Valid password example: **`PassWord`**

Require numbers and punctuation – password must include at least one numeral and at least one symbol. Valid password example: **`P@ssW0rd`**

Reject variation of login id – obvious variations on the previous password will be rejected. The following examples assume that the previous password was `P@ssW0rd`.

- change of case only; **`p@SSw0rD`** will be rejected
- reversed character sequence; **`dr0Wss@P`** will be rejected
- doubled sequence; **`P@ssW0rdP@ssW0rd`** will be rejected
- string containing the earlier password; **`myP@ssW0rd!`** will be rejected

Reject word in dictionary and **Reject standard substitutions (@ for a, 3 for e, etc.)** – if both are selected, users may not set passwords such as p@$$w0rd. Valid password example: **`P&ssW*r#`**

Reject sequences in numbers or letters – users may not set passwords that consist of all the letters or numbers on one row of the keyboard, in sequence either from left to right or right to left, or a character string that contains such a sequence. Partial or broken sequences such as **`abc!defg`** or **`qwerty12`** may be used.

Reject previous password and **Number of previous passwords to check** – recently used passwords may not be reused.

Reject single character difference from previous password – when changing a password, at least two characters must be changed.

Enforce minimum password length and **Minimum password length** - keep users from setting passwords short enough to be easily guessed.

Expire password and **Number of valid days** - force users to change their passwords periodically.

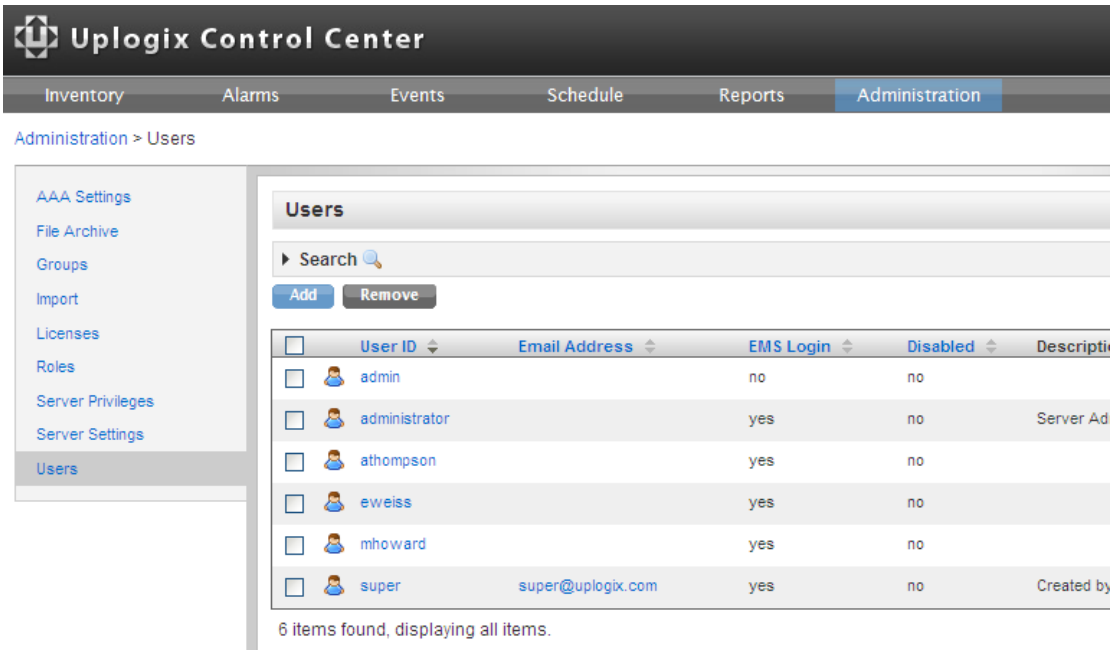
Number of invalid attempts before lockout and **Lockout duration in minutes** - specify the maximum number of times a user can attempt to log in to an appliance before the appliance refuses further attempts, and the length of the lockout period. Set the number of attempts to 0 to disable lockout protection. The default lockout time is 30 minutes. These settings apply only to Uplogix appliances, not to the Uplogix Control Center.

Note: Do not create a password that ends with a space character. When you attempt to log in to an Uplogix appliance using a password that ends with a space, the Uplogix appliance strips the space character and the login fails.

Working with user and group accounts

Administration > Users

The **Users** and **Groups** pages under the **Administration** tab allow you to manage accounts. The options contained on the Create/Edit User and Create/Edit Group pages are the same ones found in the RMOS commands **`config user`** and **`config group`**.



Accounts that exist locally on an Uplogix appliance are deleted when the appliance makes contact and synchronizes with the Uplogix Control Center. You cannot manage accounts locally through the RMOS command line if the appliance is managed by an Uplogix Control Center.

There is an exception for users whose passwords expire. If you log in to an Uplogix appliance with an expired password, the command line prompts you 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 user 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.

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

To create a new account, click **add**. To edit an existing user, click the user ID.

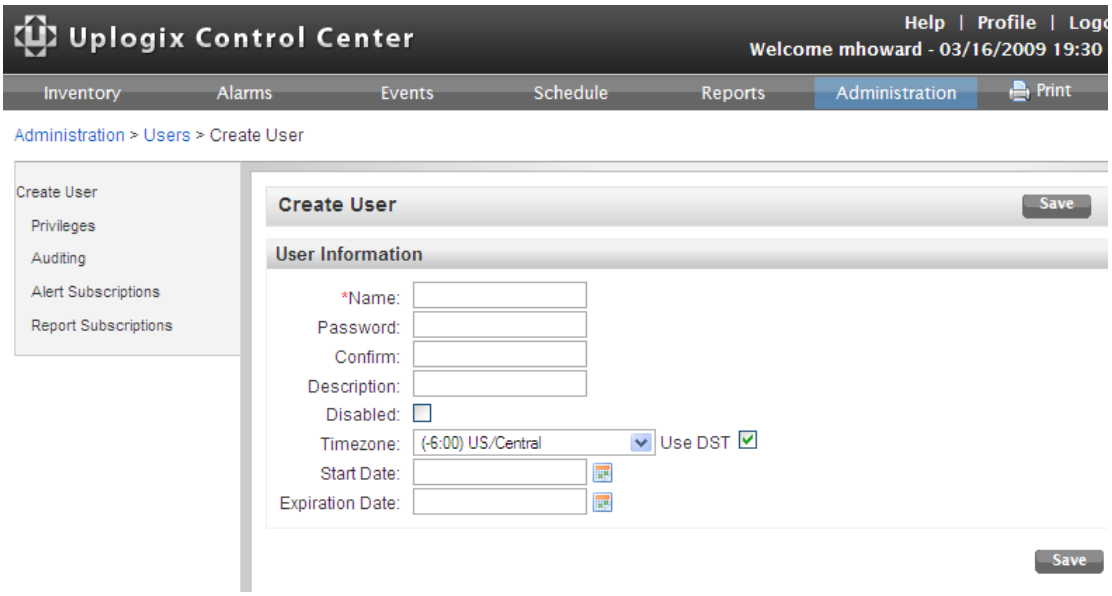
When you edit an existing user, the **Edit User** page displays a timestamp showing when the account was created. You cannot edit the account name.

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

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

Note: When completing text fields, use only printing characters. Spaces are considered printing characters, but may only be used in the **description** field.

Note: Do not create a password that ends with a space character. When you attempt to log in to an Uplogix appliance using a password that ends with a space, the Uplogix appliance strips the space character and the login fails.



Note: If you change the **Timezone** setting for a user account while that user is logged in to an Uplogix appliance, the change does not take effect on that appliance until the user ends the session.

Click the **save** button at the top or bottom of the page when you finish setting up the account information.

User accounts have no privileges initially, so the new user cannot log in to the Uplogix Control Center or to the Uplogix appliances within the deployment. You must assign privileges to the new user account to allow the user to work with elements of your deployment. See Managing privileges on page 91.

Some users may need to receive alerts or reports, or audit other accounts. For information about setting up these functions, see Setting up email, auditing and report subscriptions on page 112.

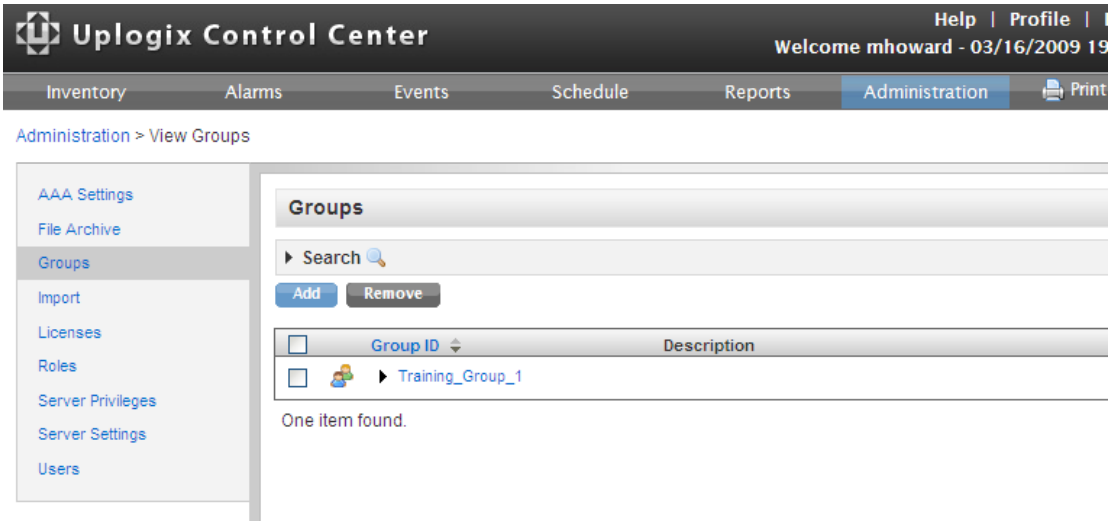
You can create several users at once by importing a user file. See Importing user, group, and privilege files on page 108.

Creating and editing group accounts

Administration > Groups

The Uplogix Control Center allows you to create and manage group accounts across multiple Uplogix appliances 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.



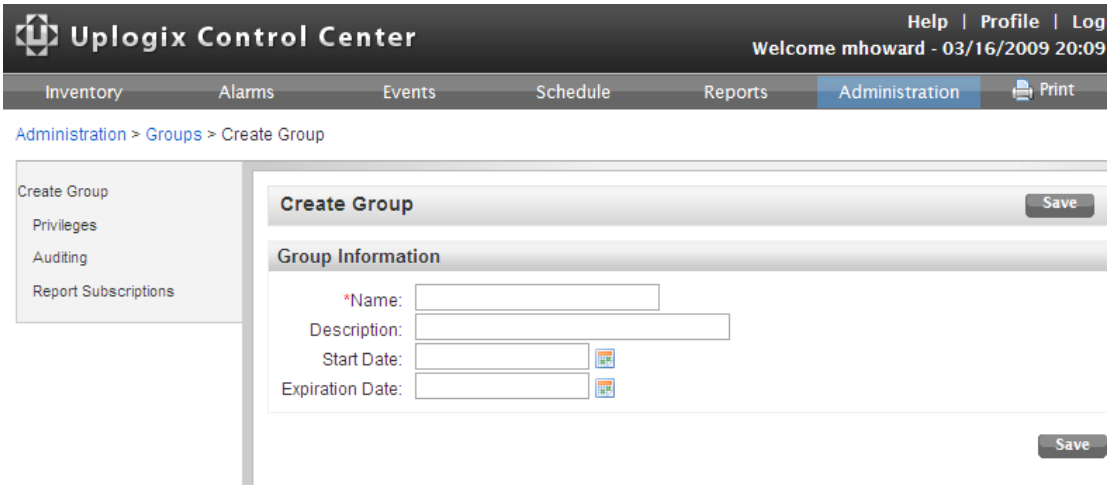
To create a new account, click **add**. To edit an existing group, click the **group id** This is equivalent to issuing the **`config group`** command from the Uplogix RMOS command line.

Note that when you edit an existing group, the **Edit Group** page displays a timestamp showing when the account was created.

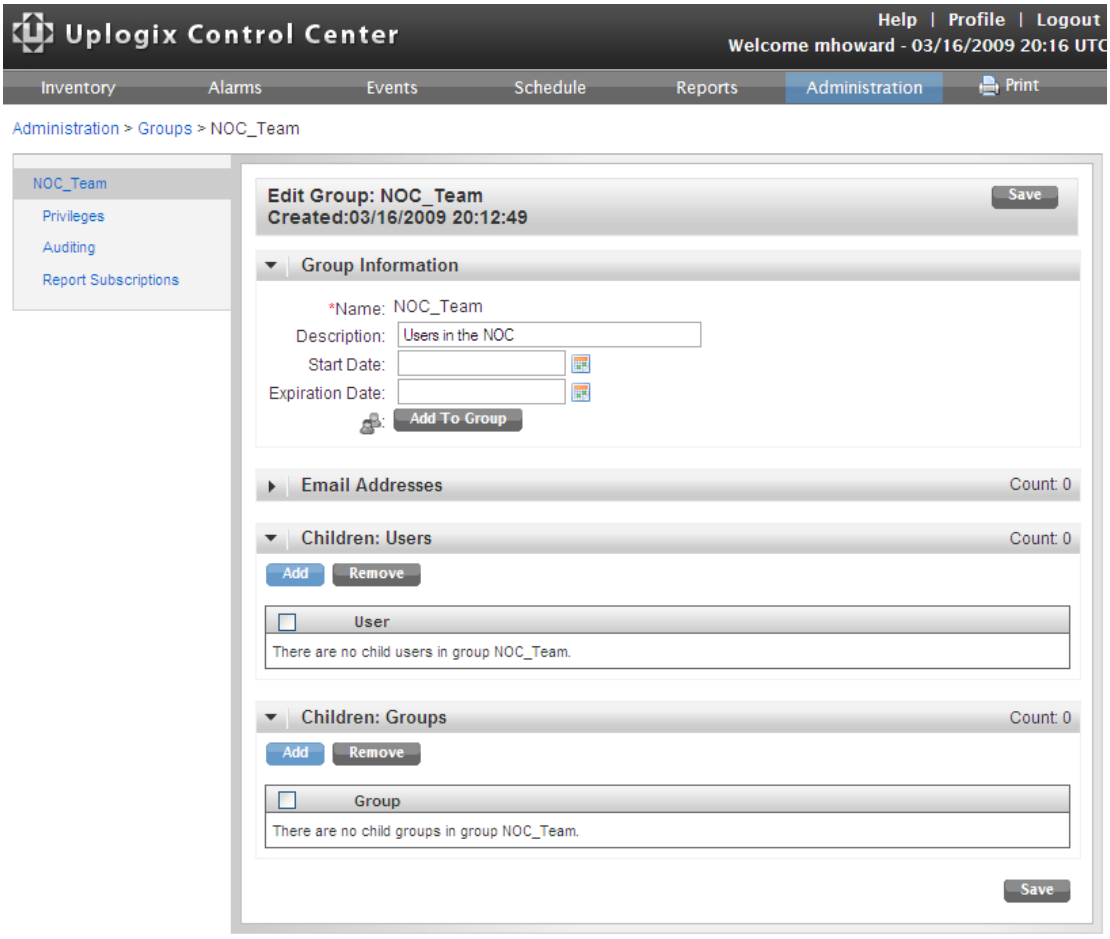
Note: When completing text fields, use only printing characters. Spaces are considered printing characters, but may only be used in the **description** field.

If you are creating a group account, specify a name for it. Optionally, provide a description and start and expiration dates.

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



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



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** or **add**, and select the user or group from the pop-up window as appropriate.

Click **save** to save the group. User groups are automatically inherited by Uplogix appliances.Group accounts have no privileges initially, so members of the group have only the permissions assigned to their individual accounts. You can assign group privileges to the new user account to allow the user to work with elements of your deployment. See Managing privileges on page 91.

The group may need to receive alerts or reports, or audit other accounts. For information about setting up these functions, see Setting up email, auditing and report subscriptions on page 112.

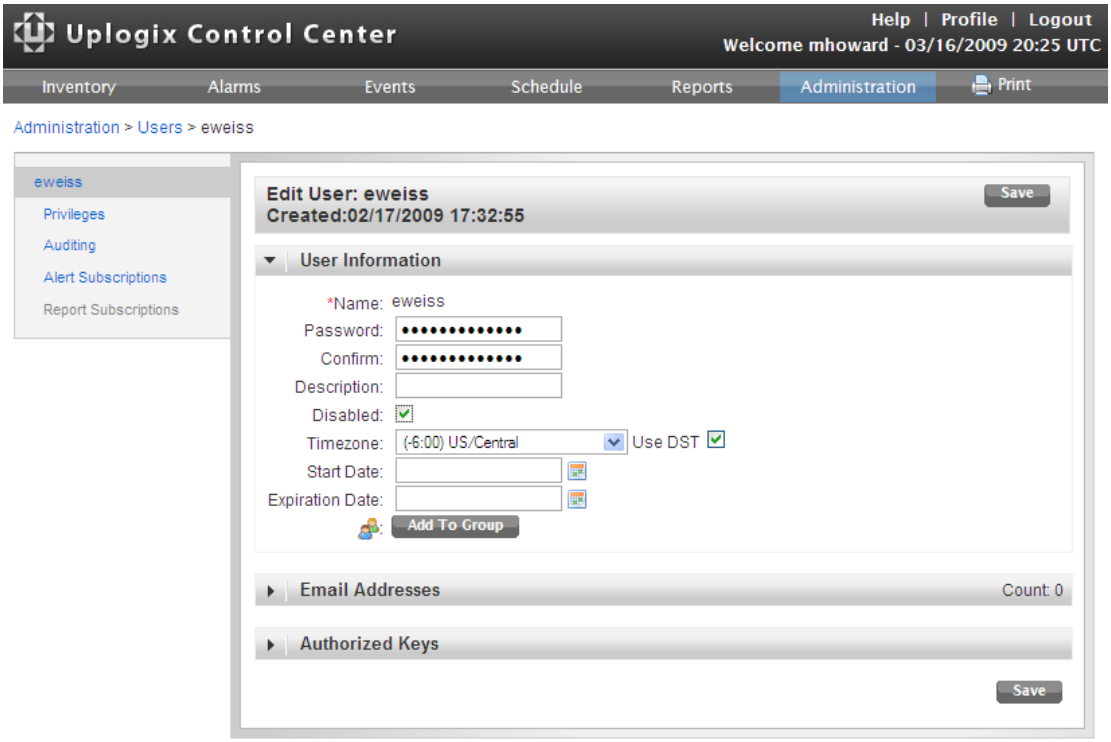
You can create several groups at once by importing a group file. See Importing user, group, and privilege files on page 108.

Disabling user accounts

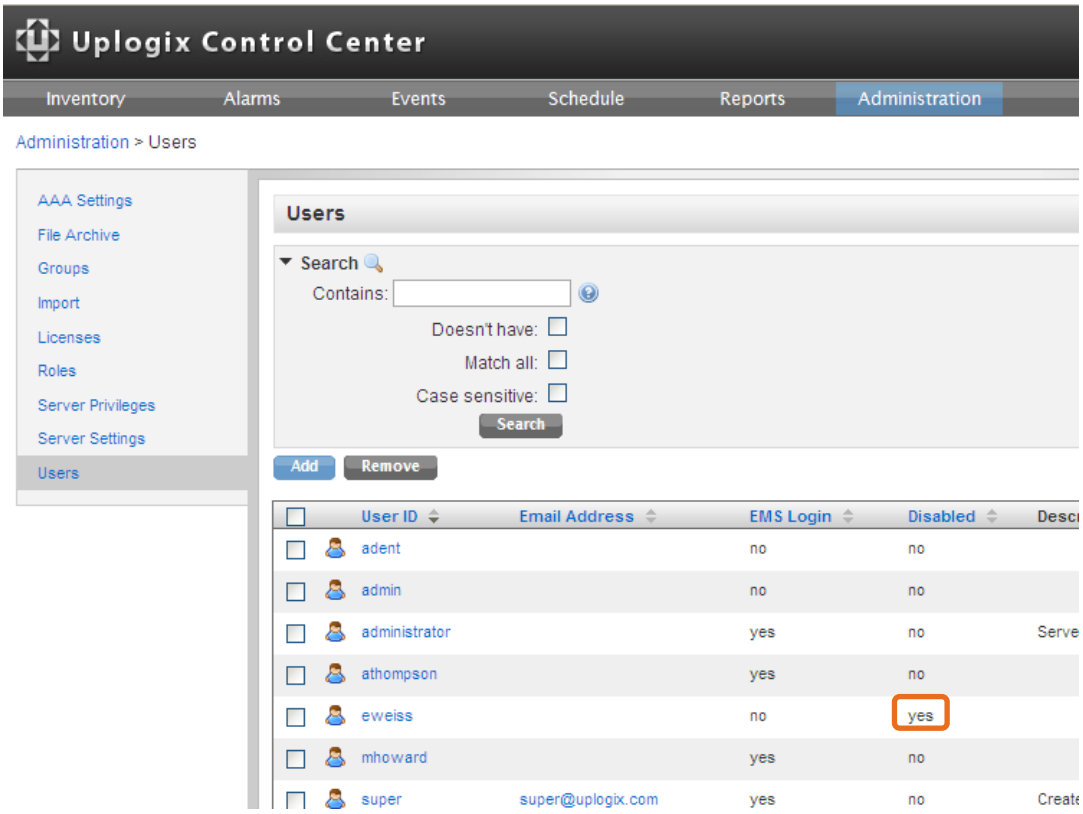
Administration > Users

To suspend access to a user account without deleting the account, go to **Administration > Users** and select the user id for the account you wish to edit.

On the **Edit user** screen, select **Disabled** and click **save**.



The user will not be able to log in while the account is disabled, and the disabled status will be displayed in the user list. If the user is logged in when you disable the account, the user will be logged out immediately.



Deleting accounts

Administration > Users

Administration > Groups

To delete an account, click the check box next to theassociated with the User ID or Group ID and select **Remove**. This is equivalent to using the RMOS commands **`config user no [username]`** and **`config group no [groupname]`** on an appliance not managed by an Uplogix Control Center EMS.

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, such as admin
- **privilege** - a role assigned to a specific account for a specific resource, such as "admin on server" or "guest on port 1/4"

Note: Some permissions, such as `config hierarchy`, are not associated with specific commands.

The Uplogix Control Center restricts access to features based on users' 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 will be unavailable for that user on the appliance 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 itself, but no privileges on individual Uplogix appliances - so **administrator** cannot log in to an Uplogix appliance. Conversely, the **admin** account on Uplogix appliances has no privileges on the Uplogix Control Center. The **administrator** account has the `config hierarchy` permission, however, which allows the administrator to manage individual appliances through the Uplogix Control Center.

In this section:

- Adding server privileges to accounts
- Adding inventory privileges to accounts
- Viewing and deleting user privileges
- Creating a superuser
- Creating and customizing roles

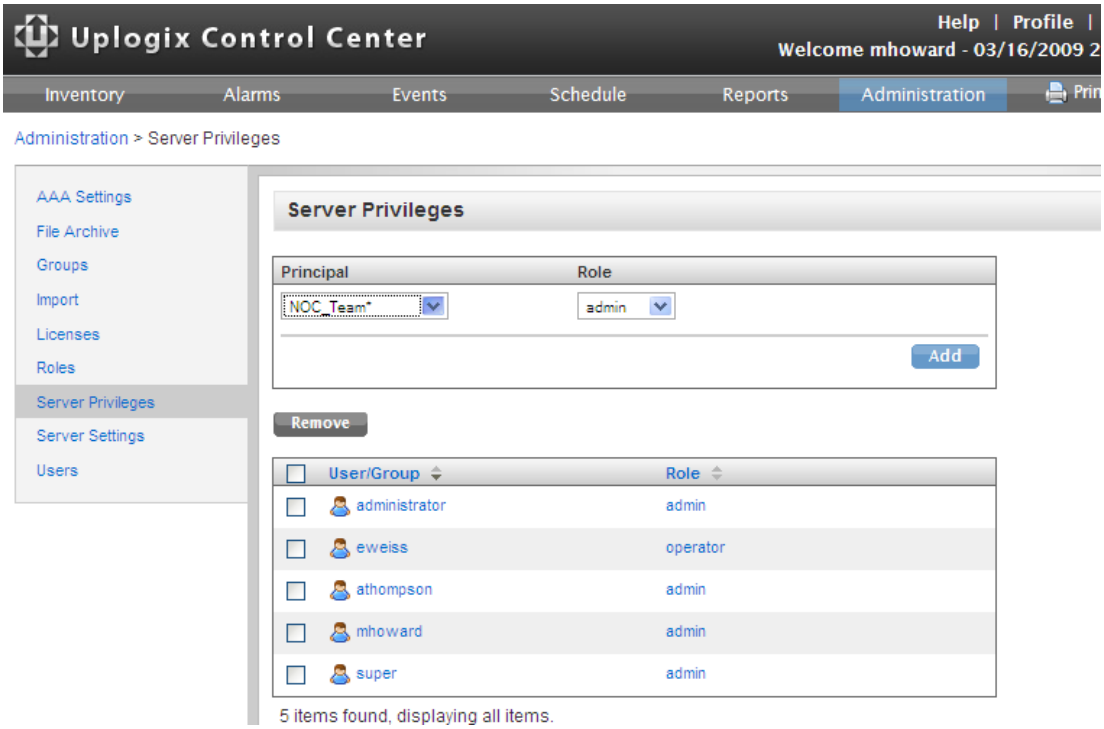
Adding server privileges to accounts

Administration > Server Privileges

When you create a new user or group account, the account initially has no privileges. To log in to 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. Users need both if they are to use the Uplogix web interface to work with Uplogix appliances, and to access appliances individually via SSH.

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



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 before users, and are marked with a * after the group name.

As with Uplogix appliance privileges, you can assign more than one role to an account to tailor that account's privileges.

You can assign privileges to several users at once by importing a permissions file. See Importing user, group, and privilege files on page 108.

Adding inventory privileges to accounts

Inventory > Group Getail > Configuration > Privileges

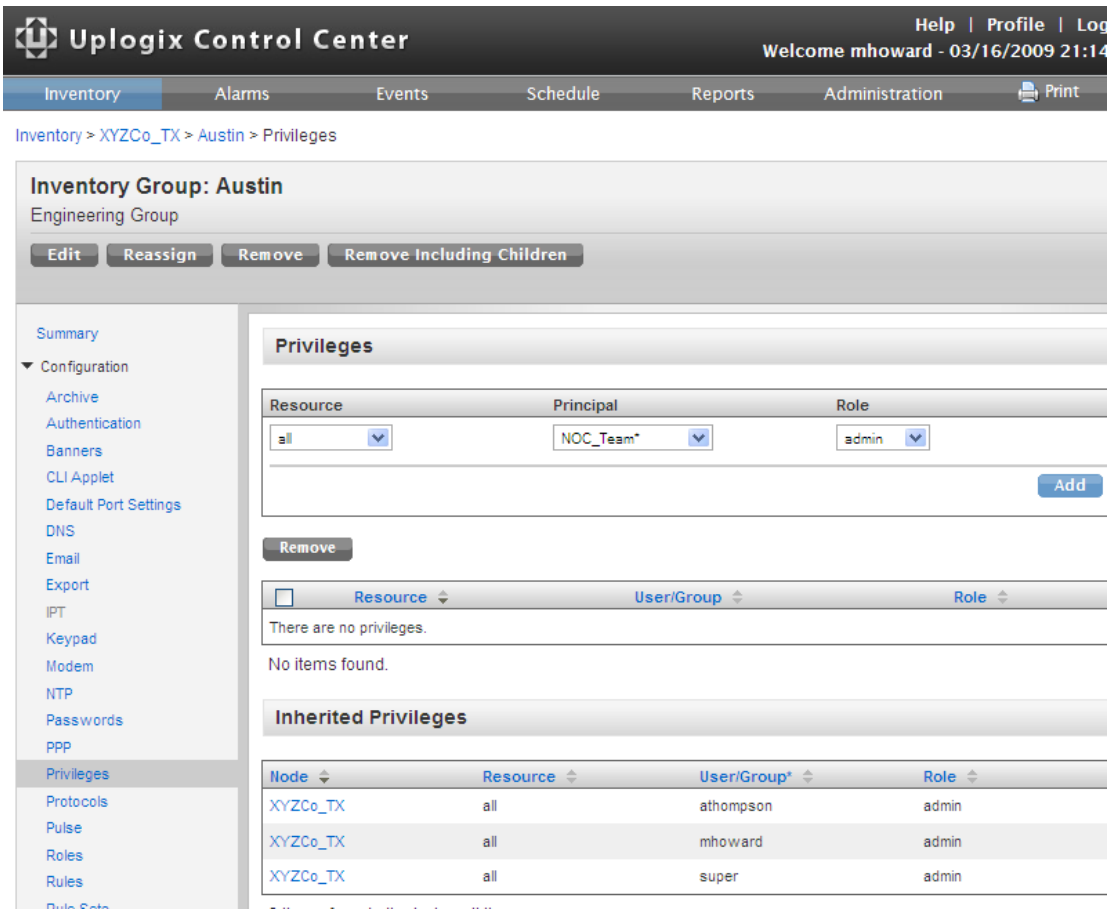
When you create a new user or group account, the account initially has no privileges. You can set an account’s privileges to apply to all Uplogix appliances in the inventory by assigning them at the root level, or you can limit privileges to specific inventory groups.

Note: Inventory privileges are limited to appliances in the inventory, and the devices they control. Server privileges must be assigned separately (see the previous section, Adding

server privileges to accounts). To manage the inventory through the Uplogix Control Center, users must have server privileges.

You can assign privileges to several users at once by importing a permissions file. See Importing user, group, and privilege files on page 108.

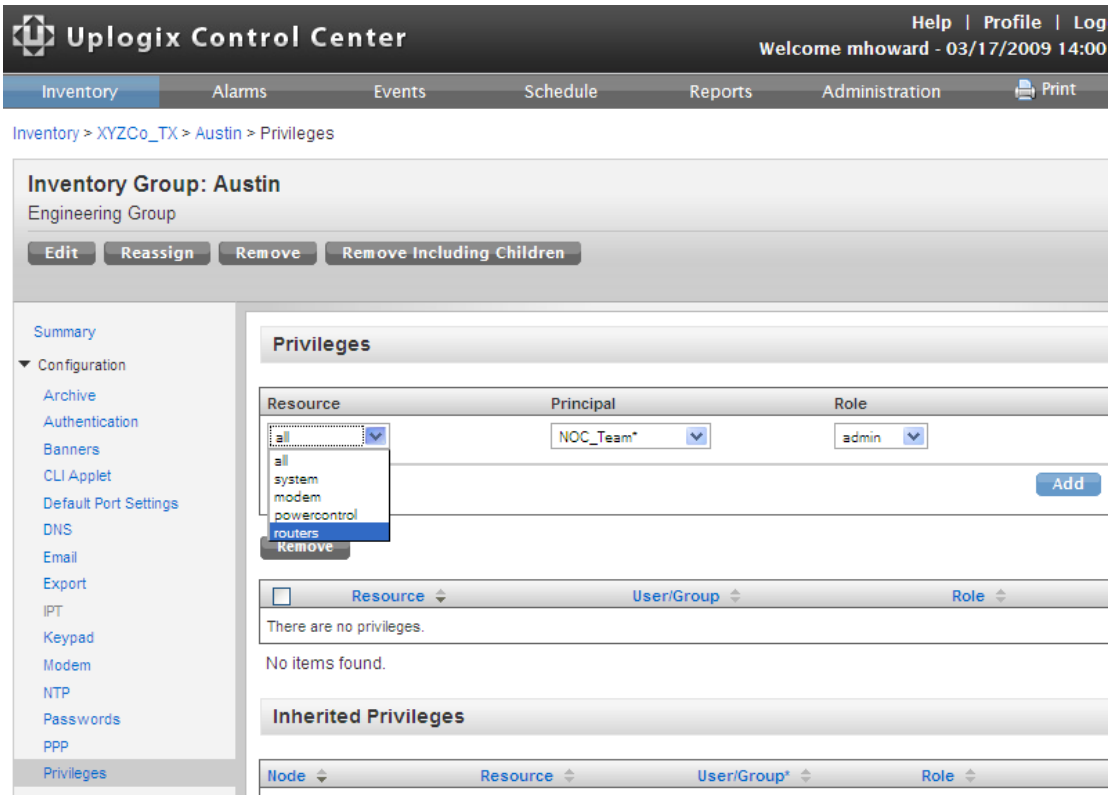
To add inventory privileges, select the appropriate inventory group from the Inventory page and click **privileges** under the Configuration menu.



The Privilege List page allows you 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.

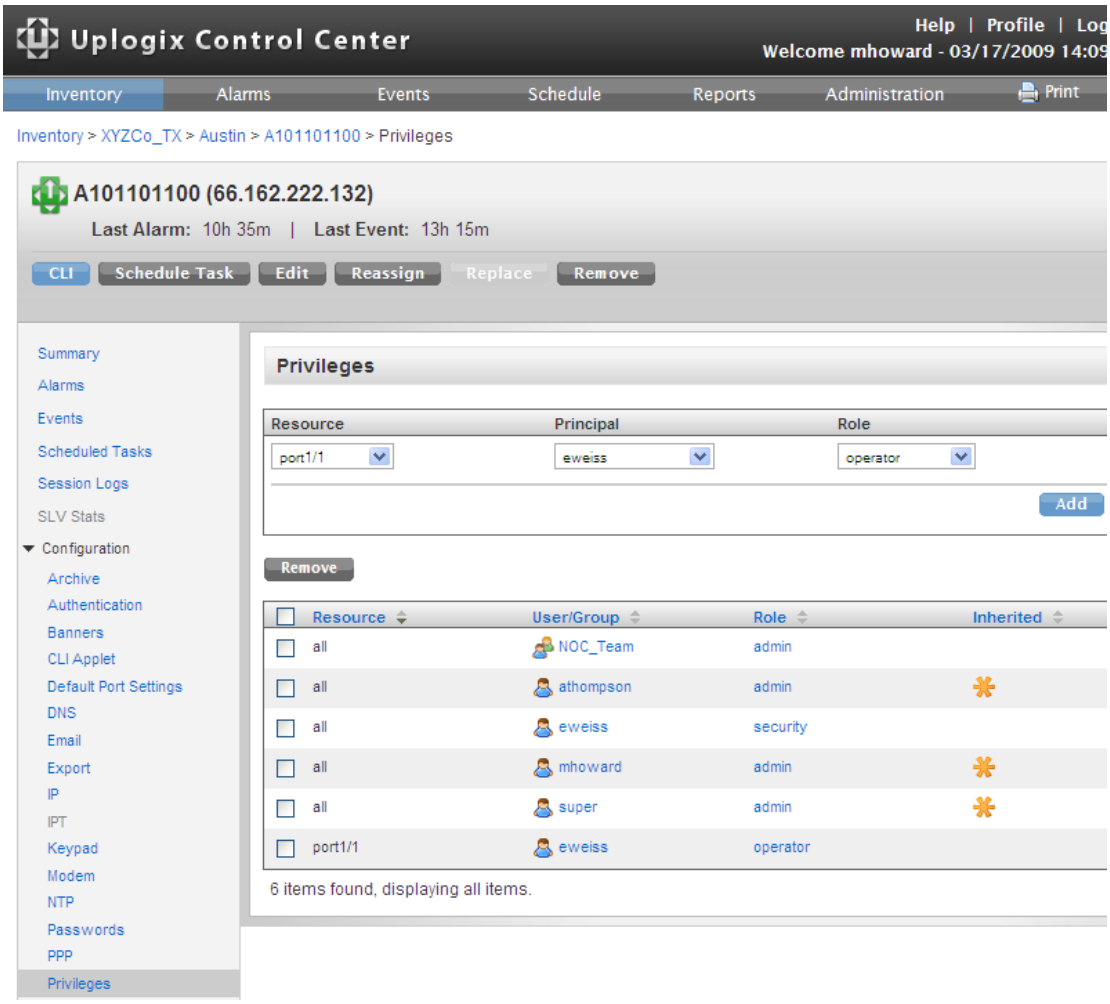
Select a user or group from the User/Group list, select a role, and click **add**. Groups are listed before users, and are marked with a * after the group name.

You may assign more than one role to the account, and you may give the account different roles on different resources.



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

The appliance's Privilege List allows you to add or delete user roles by individual resource.



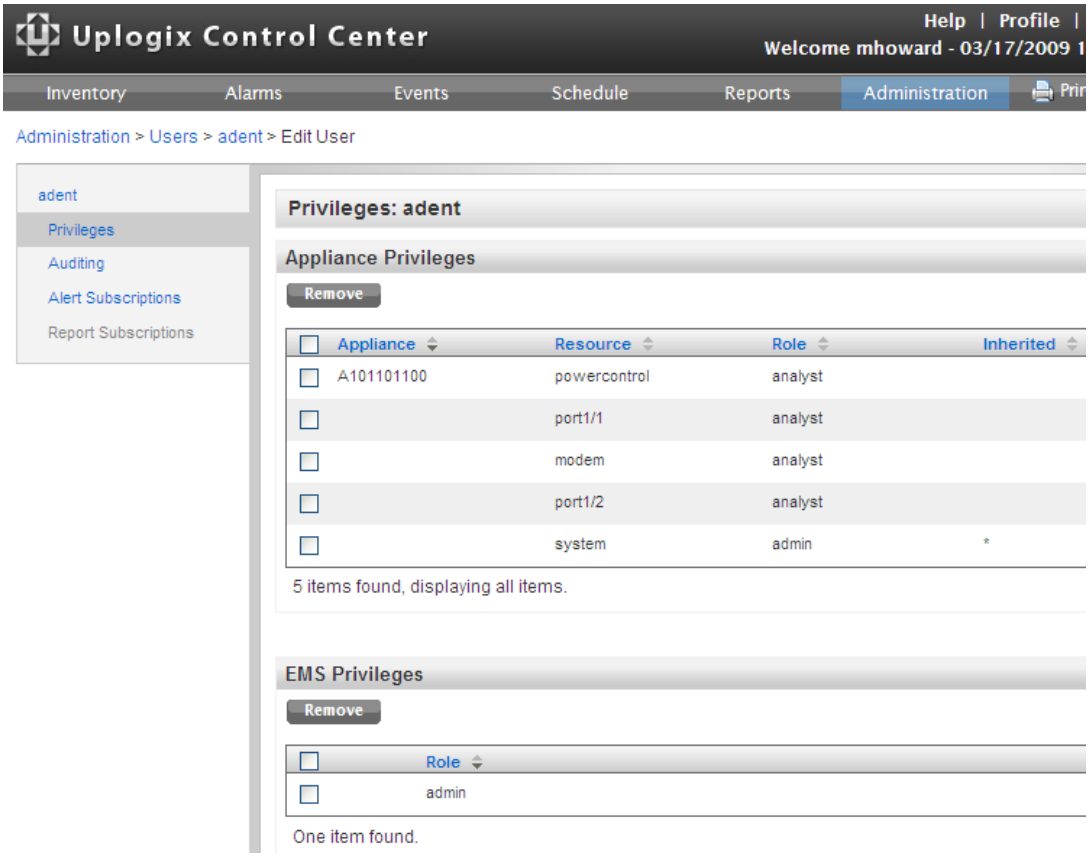
If the pre-configured standard roles do not meet your organization's needs, you can create roles to meet the specific requirements of your deployment. See Creating and customizing roles on page 96.

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.

The user privileges detail allows you to see and delete specific privileges. In the example below, the user `adent` has `analyst` privileges assigned locally on appliance A101101100, and inherited `admin` privileges that have been assigned at the inventory group level.



Creating and customizing roles

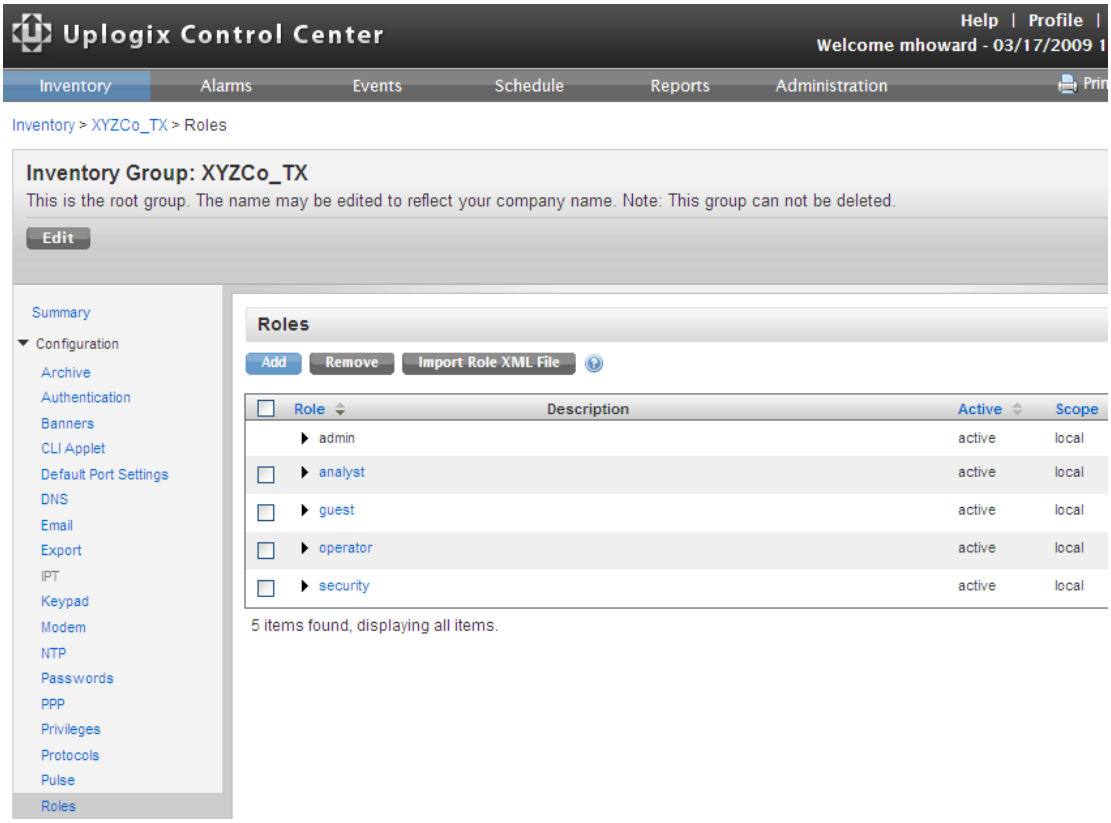
Inventory > Configuration > Roles

A role is a set of commands that a user is permitted to execute. When you assign privileges to a user or group account, you associate the account with one or more roles on one or more resources. See Adding inventory privileges to accounts on page 92.

The Uplogix Control Center provides the same predefined roles that are available in the Uplogix RMOS CLI. In addition to these standard roles, you can define custom roles 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, select the role id to edit an existing role. This is equivalent to issuing the **`config role`** command from the Uplogix RMOS command line.

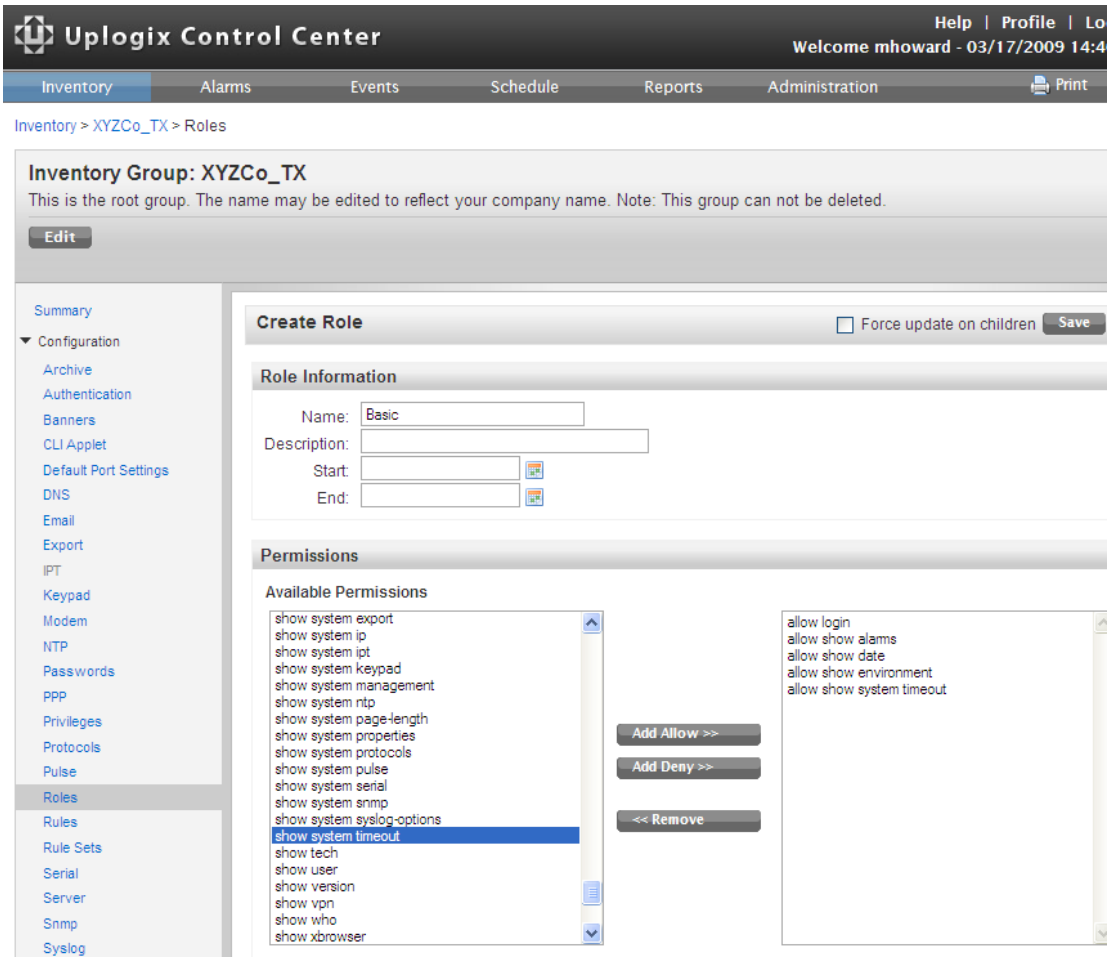


If you are creating a new role, you must enter the role name.

Note: When completing text fields, use only printing characters. 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.

You can select more than one permission at a time by Shift-clicking the first and last items in a range, or by Control-clicking to select permissions separately.



As with many other settings, roles that you create are automatically inherited by any Uplogix appliances and child groups within the current inventory group. If a role with the same name already exists on an Uplogix appliance or child group within the current inventory group, select **Force update on children** to overwrite it.

When you have defined the privileges for the role, click **save**.

Using TACACS to manage privileges

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

The general procedure is:

1. Configure the Uplogix Control Center to use TACACS
2. Set up a group so that you can define a TACACS ACL and associate it with users
3. Assign at least one role to give the group the desired set of permissions; create a suitable role if necessary.

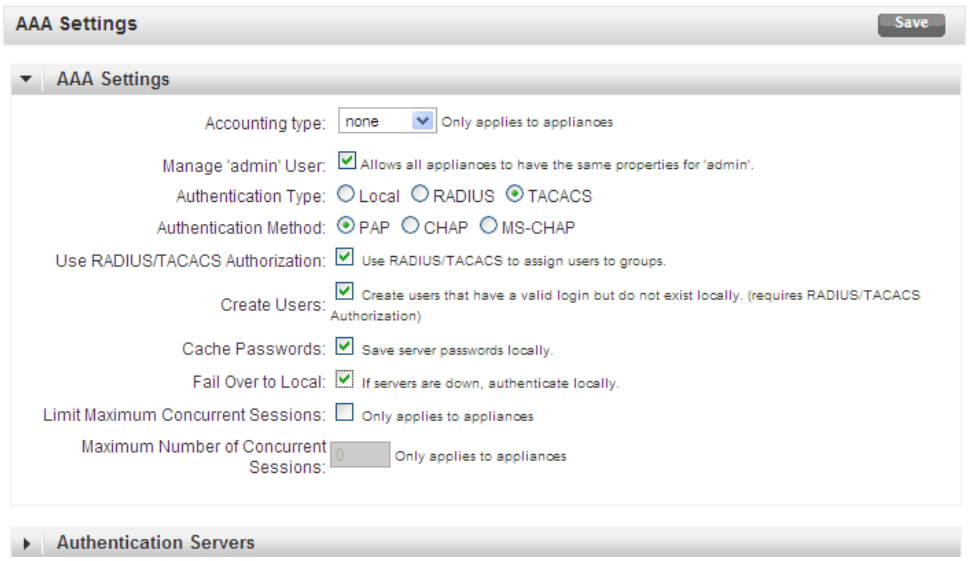
These steps are described in detail below.

Note: If you delegate AAA functions 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 TACACS.
2. Select the appropriate authentication method.
3. Select Use TACACS Authorization.
4. Select Create Users. This allows the Uplogix Control Center to create accounts for users who already exist on the TACACS server.
5. Enter the IP address and shared secret for each TACACS server. You may specify up to four servers.
6. Optional: Select Persist TACACS ACL and Cache Passwords to ensure that users will still receive the correct privileges if the TACACS server is off-line during the next authentication/authorization.



When a user logs in to the Uplogix Control Center with Cache Passwords enabled, the Uplogix Control Center asks the authentication server for the account's password and then updates the user account (caching). Since the account is updated, this change gets pushed down to all the appliances, changing the user's password throughout the inventory when it changes on the authentication server.

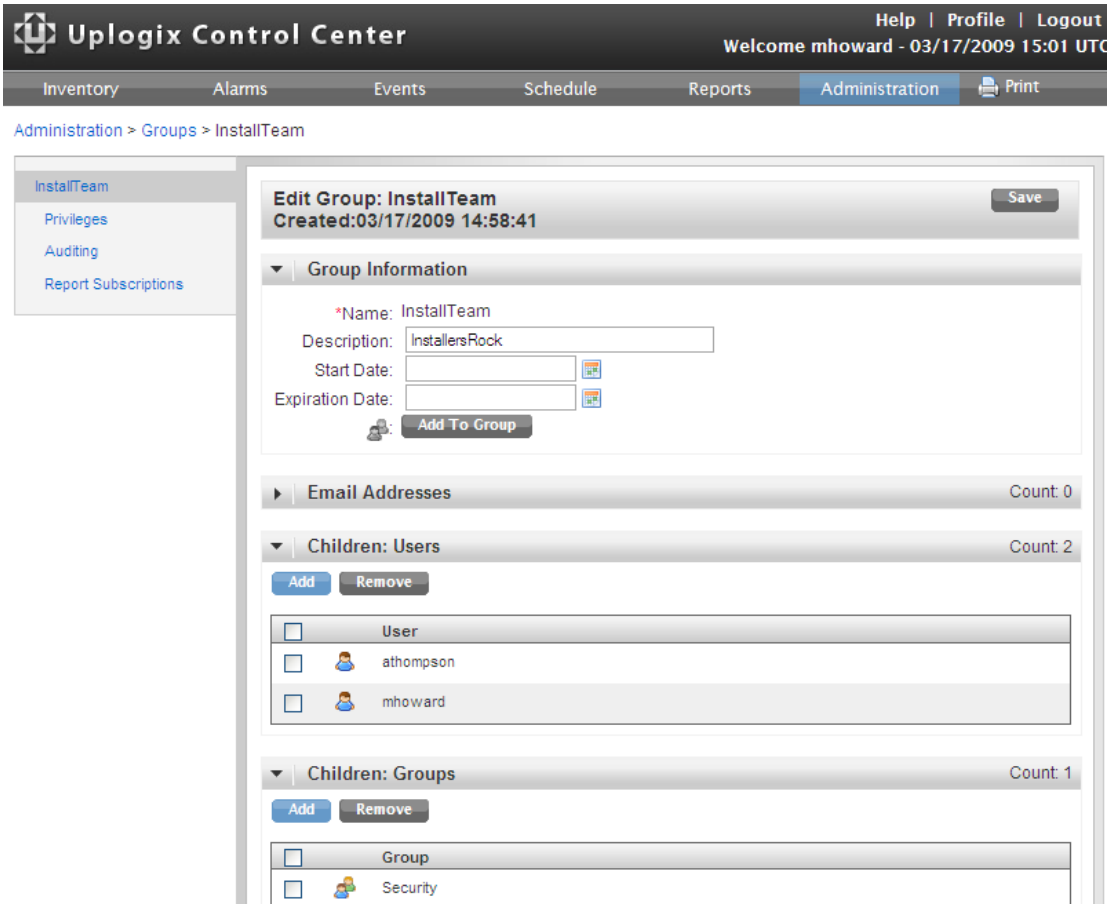
In this way, you can configure Uplogix Control Center to use TACACS, but the appliances don't have to. The appliance receives the user's new password via the Uplogix Control Center and authenticates locally with the password received remotely. Although the user logs into the appliance with the account's TACACS password, the appliance is not really contacting the TACACS server.

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

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. You do not need to add users to the group.
2. Enter a name or a number that means something to you in the in the TACACS ACL field.



3. Assign suitable roles to the group. See Adding server privileges to accounts on page 92 and Adding inventory privileges to accounts on page 92. Users will not be 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 appliance, you can add authorization by adding an ACL under the "Exec" service in your user or group. In most Unix TACACS deployments, you can edit the `users` file and add the following lines to either the group or the user:

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

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

Example: Creating a superuser

The Uplogix Control Center is a resource, just as Uplogix appliances and their ports, modems, and power controllers are resources. Users cannot log in to the Uplogix Control Center until they have privileges on it.

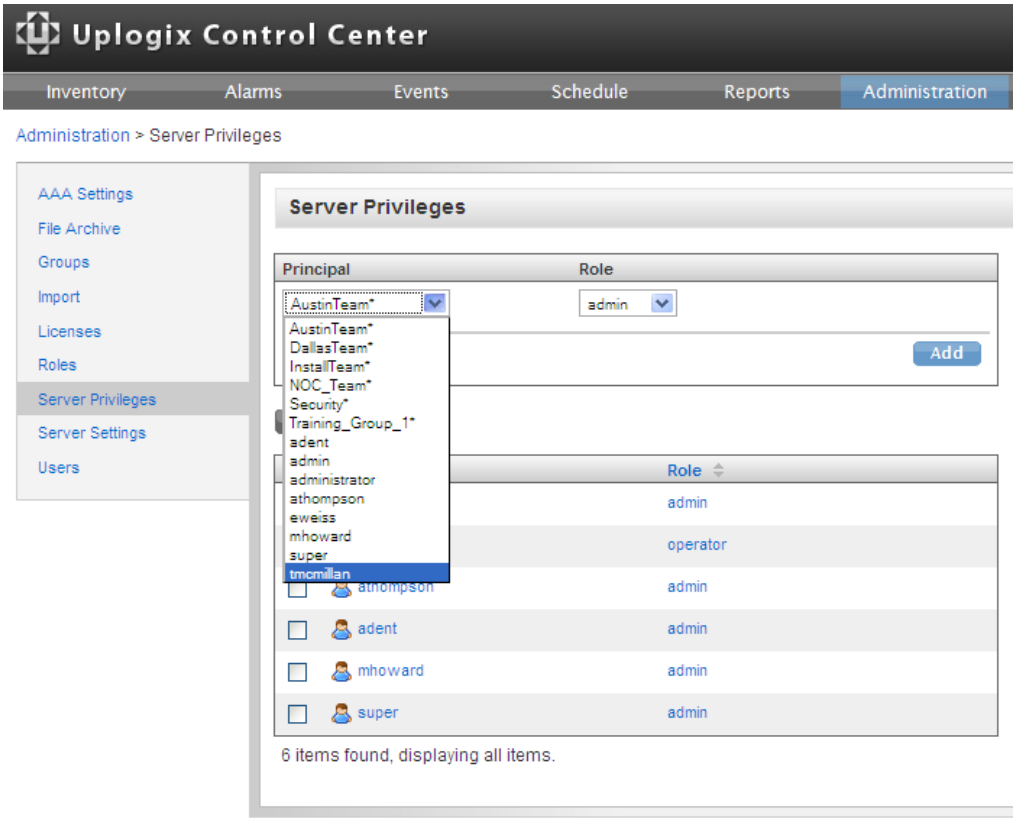
The **administrator** account on the Uplogix Control Center has `admin` access to all features of the server itself, but no privileges on individual Uplogix appliances - so **administrator** cannot log in to an Uplogix appliance. This account has the `config hierarchy` permission, however, which allows the administrator to manage individual appliances through the Uplogix Control Center.

Conversely, the **admin** account on Uplogix appliances has no privileges on the Uplogix Control Center.

Server privileges and Uplogix appliance 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.

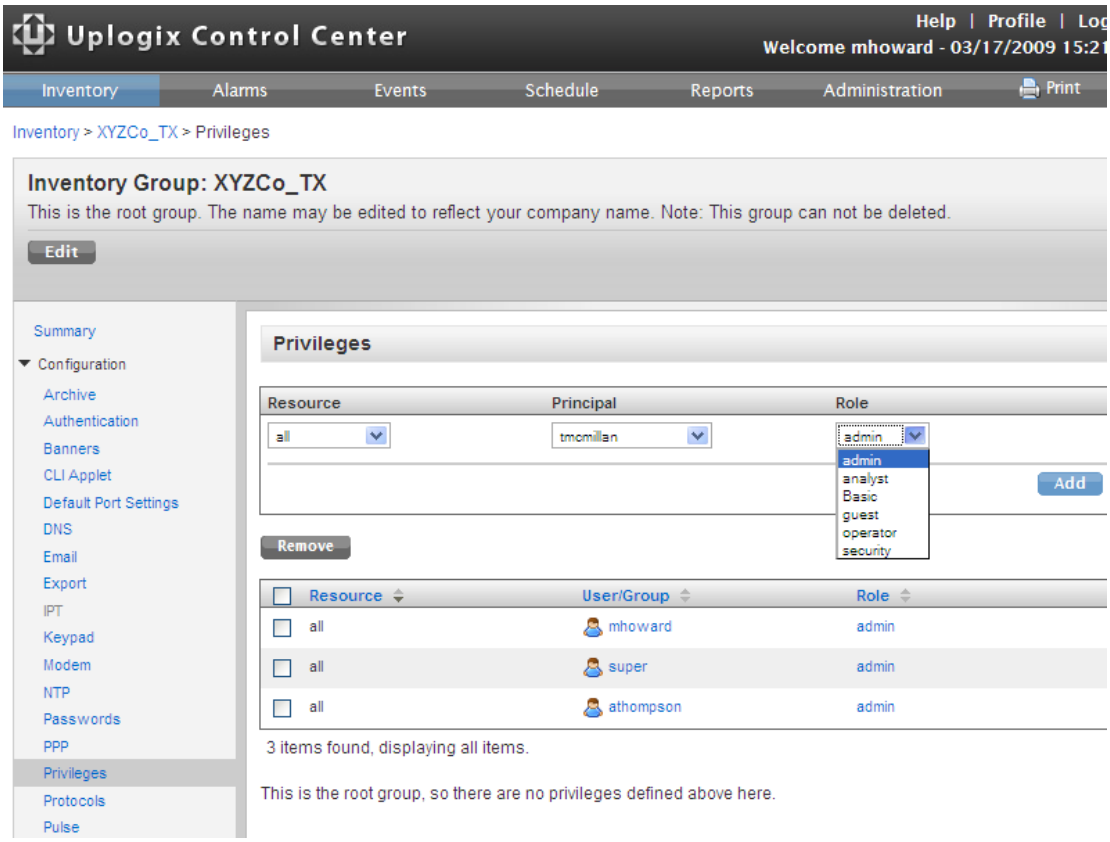
To create a user who can execute any operation on any resource, first create the user. (See Creating and editing user accounts on page 85.)

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



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 we will create a user who can only log in to one Uplogix appliance, and after logging in, can only execute the terminal command on port 1/1. To do this, we must:

- Create a custom role
- Create a user account that will have this role
- Apply the role to the appropriate resources

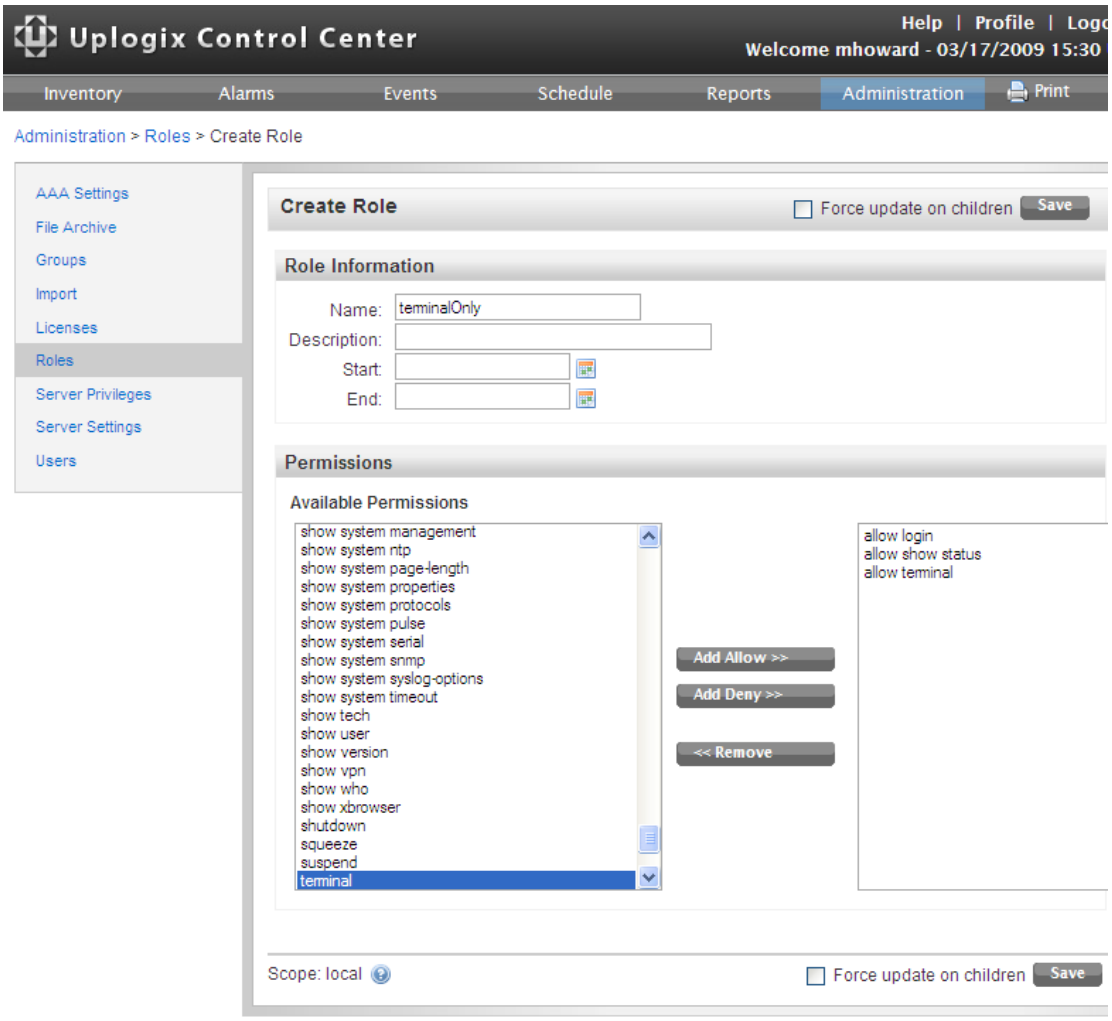
Creating the role

On the **Administration > Roles** page, click **add** to open the Create Role page. This allows you to create a role that is universally available.

You can also access the Create Role page by clicking the **roles** button on the appropriate inventory group detail page, if you only want the role to be available within that inventory group and any child groups.

For this example, we will create a role called `terminalOnly` that we can assign at the system level and on the desired port. This role will give 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 appliance, 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 will need to navigate to the appropriate port in order to open terminal sessions. There is no "port" permission. Instead we will use the `show status` permission. When we apply it to a port, this permission allows the user to navigate to the port.
- 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.

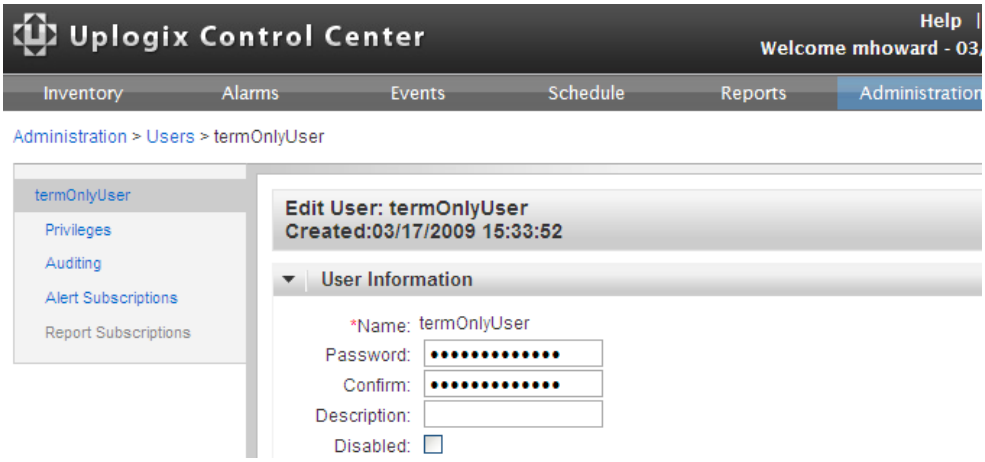


When you have added the required permissions, click **save** to save the terminalOnly role.

Creating the user account

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

For this example, we will create a user account called termOnlyUser.



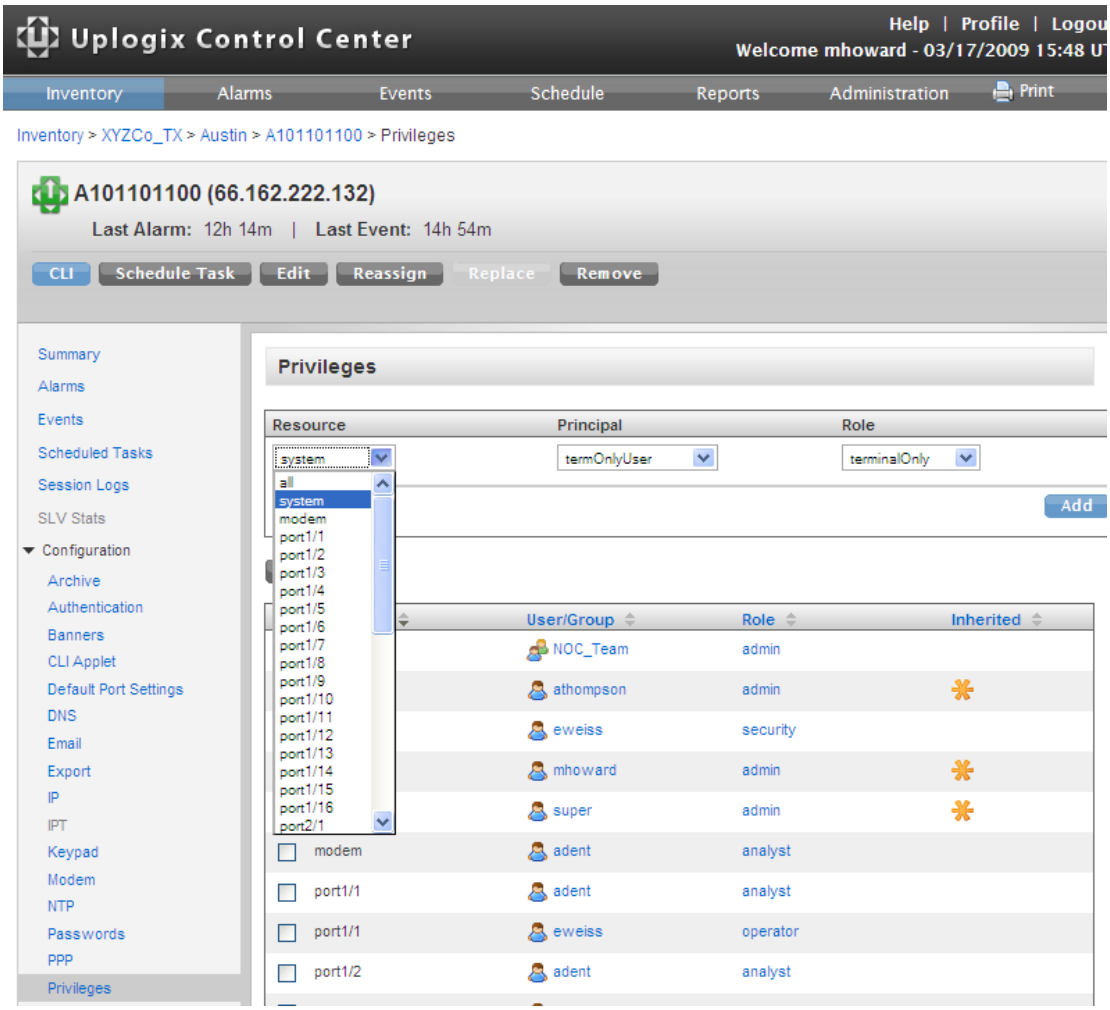
Applying the role to create permissions

This user account will not need access to the web interface, so we will not assign server privileges.

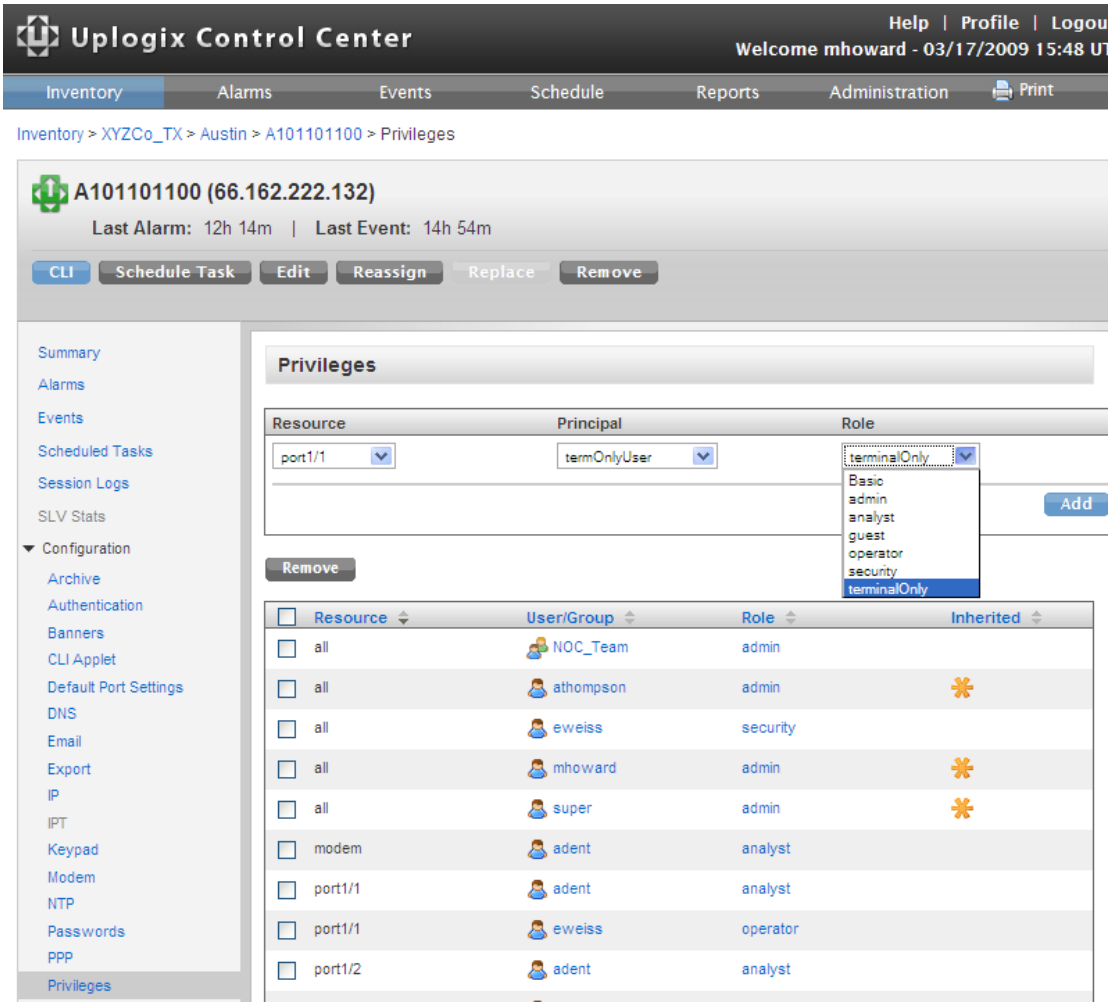
The account should only provide access to port 1/1 on a single system, so we will assign privileges from the appliance's expanded detail page.

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.



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.

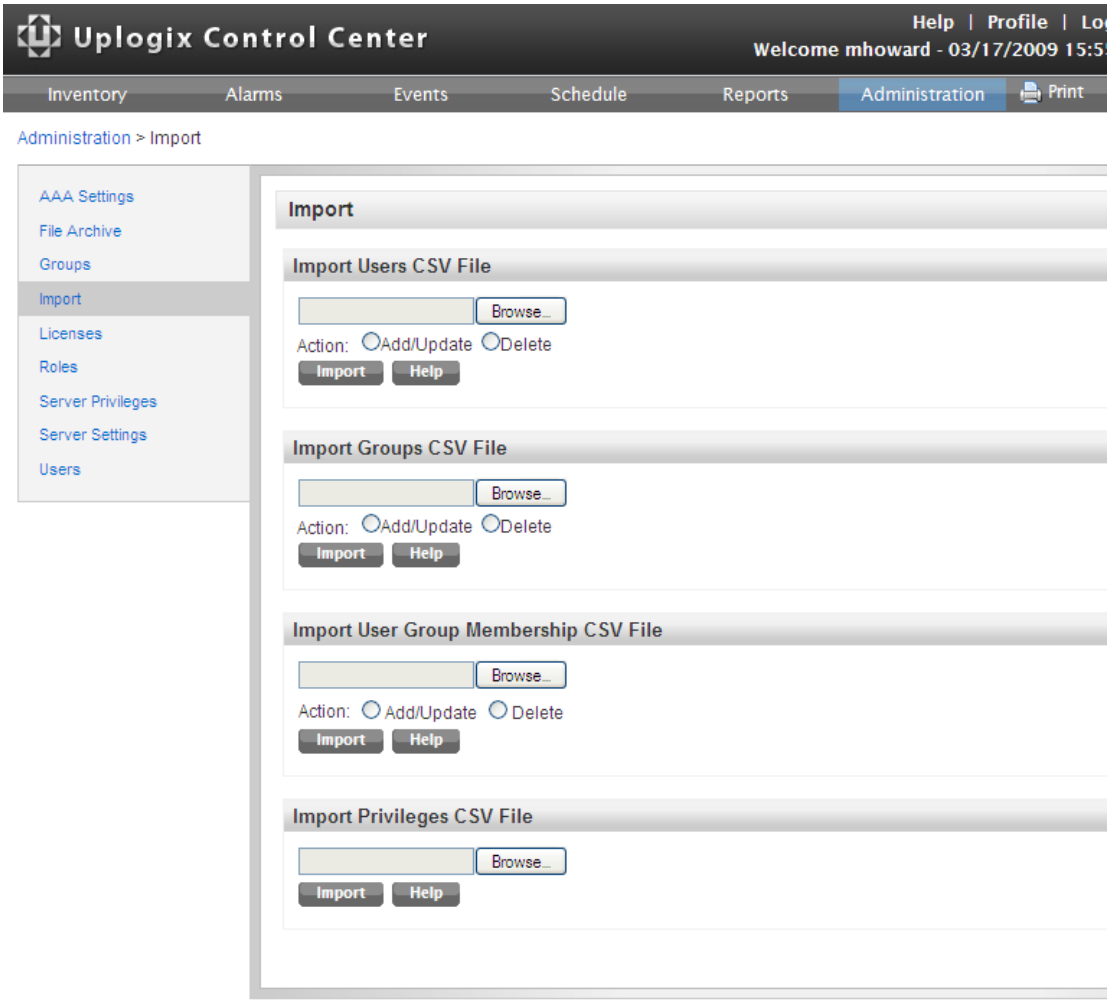


The user `termOnlyUser` can now log in to the xyzcoAus01 system and open a terminal session to the device on port 1/1.

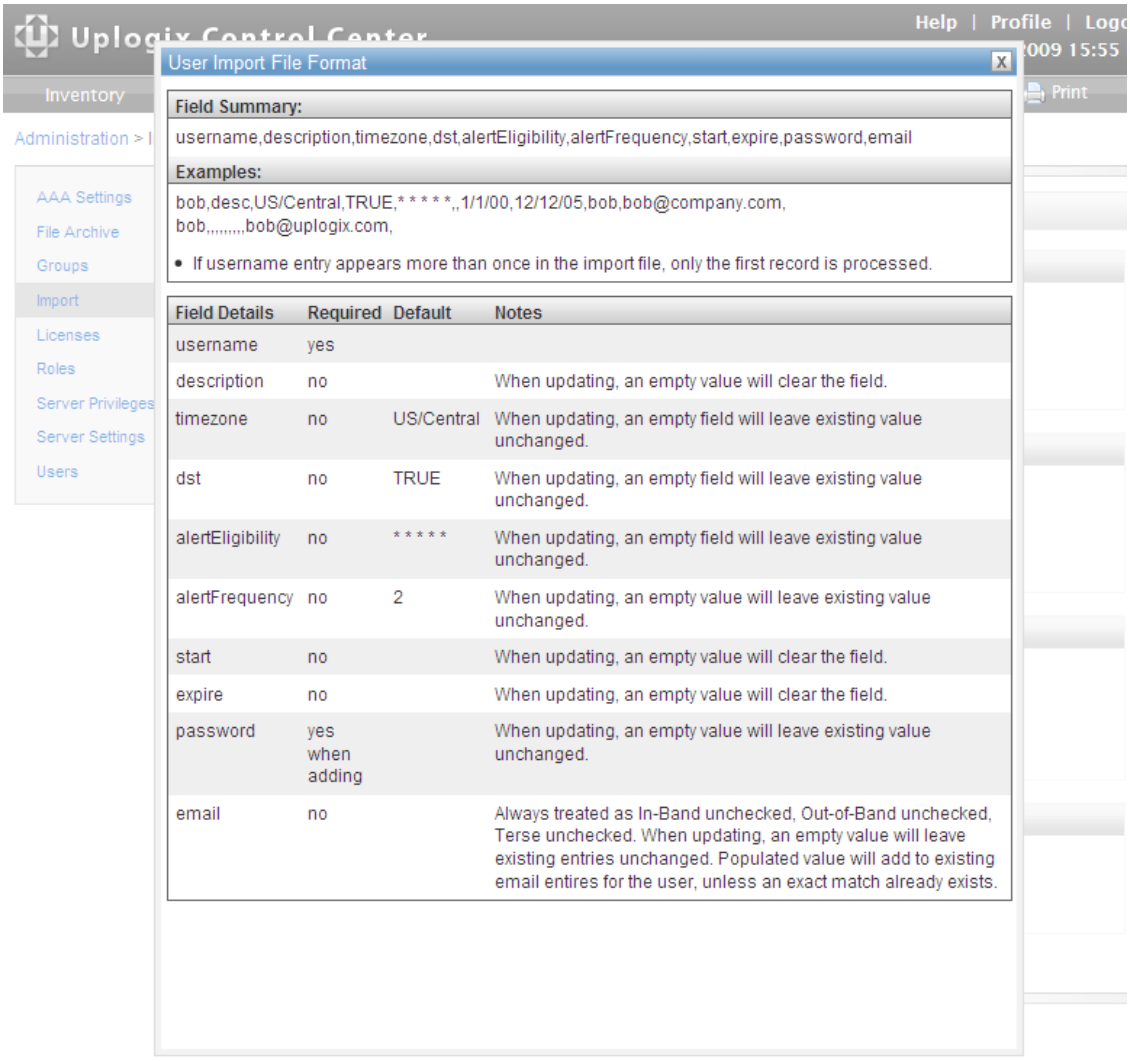
Importing user, group, and privilege files

Administration > Import

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



For information about how to set up the CSV file, click the **Help** button in the appropriate Import box.



Logs, reports, and diagnostics

The Uplogix Control Center element management system captures several kinds of information about the Uplogix appliances it manages and the devices connected to each, and about 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 appliance views
- Viewing reports - receiving, downloading, and viewing reports from the Uplogix Control Center
- Viewing archive status information for an appliance - time that the last archive took place, whether it was successful, related information.
- Viewing temperature statistics - current, recent, and historical data
- Viewing device syslogs
- Viewing session logs and auditing users
- Troubleshooting
- Sending logs to Technical Support
- Replacing an appliance

Setting up email, auditing, and subscriptions

To provide subscribed information - alerts and reports - the Uplogix Control Center must be configured to send email. For information on this, see Configuring email settings on page 15.

To receive alerts and reports, your account must be:

- configured with an email address where you will receive alerts and reports from the Uplogix Control Center
- subscribed to the desired alerts and reports
- To audit other accounts, your account must be:
- configured with an email address where you will receive alerts and reports 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.

You can click the right arrows ▸ to expand the collapsed sections of these pages.

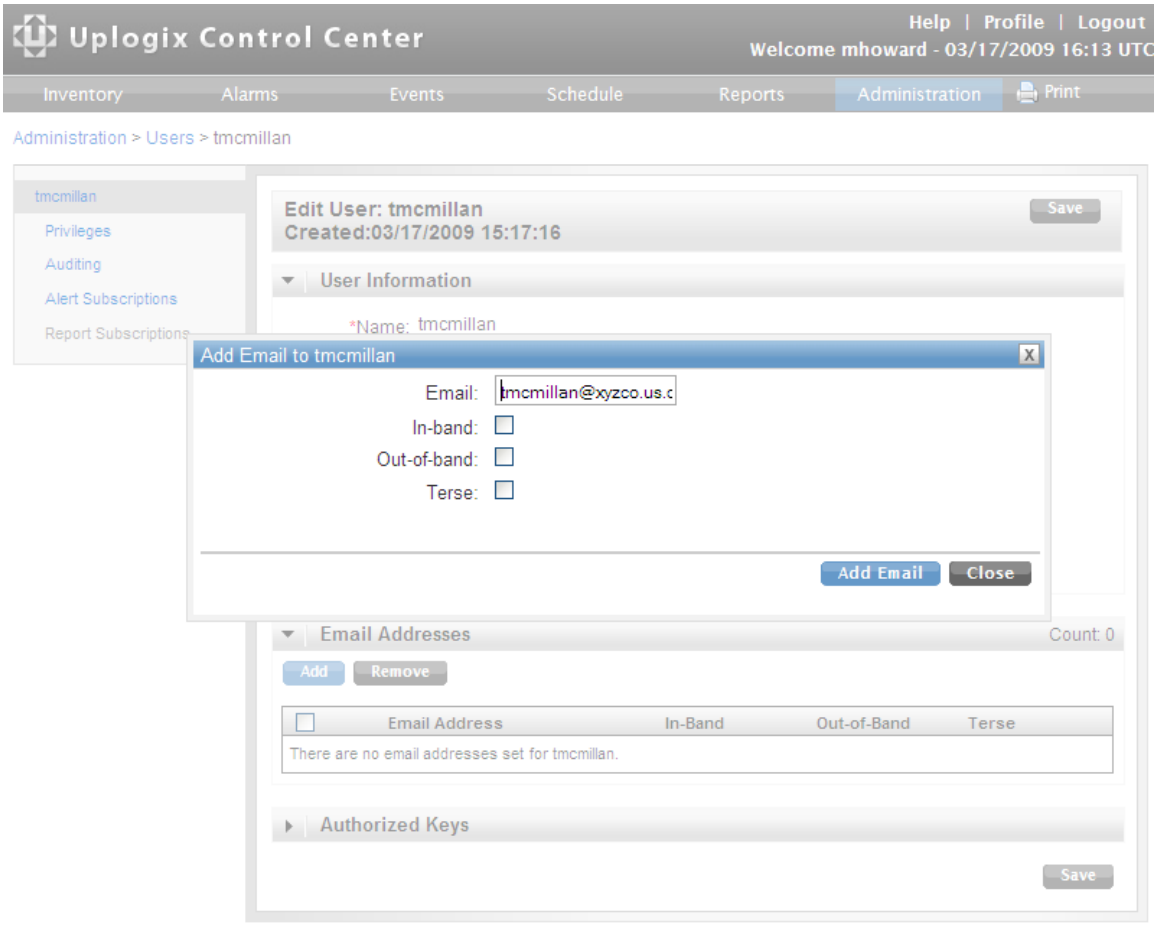
Configuring an account to receive email from the Uplogix Control Center

To allow an account to receive alerts or reports by email, enter at least one email address where the user can receive alerts and reports (including user audits).

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

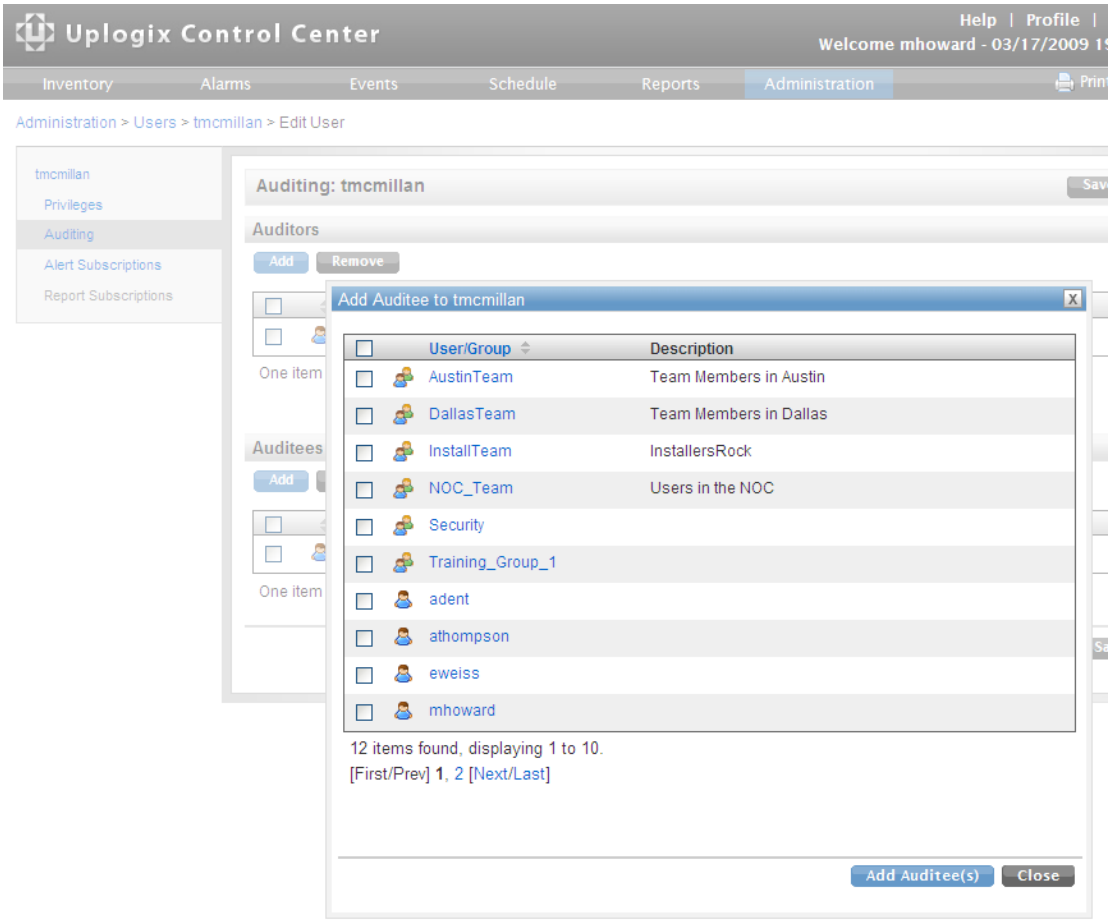
Select **Terse** to limit the message to a subject line only. You may want to use the Terse setting for email directed to a pager or cell phone. Click **add email** when you have entered all the email information and then save on the edit user details screen

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


Uplogix Control Center
Help | Profile | Logout
Welcome mhoward - 03/17/2009 16:13 UTC
Inventory
Alarms
Events
Schedule
Reports
Administration
Print
Administration > Users > tmcmillan
tmcmillan
Privileges
Auditing
Alert Subscriptions
Report Subscriptions
Edit User: tmcmillan
Created:03/17/2009 15:17:16
Save
User Information
*Name: tmcmillan
Add Email to tmcmillan
Email: tmcmillan@xyzco.us.c
In-band:
Out-of-band:
Terse:
Add Email
Close
Email Addresses
Count: 0
Add
Remove
Email Address
In-Band
Out-of-Band
Terse
There are no email addresses set for tmcmillan.
Authorized Keys
Save

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 check list and clicking on the **Add Auditee(s)** button.



To allow another user to audit this user, open the Auditor Picker by clicking the **add** button. Add auditors the same way you added auditees.

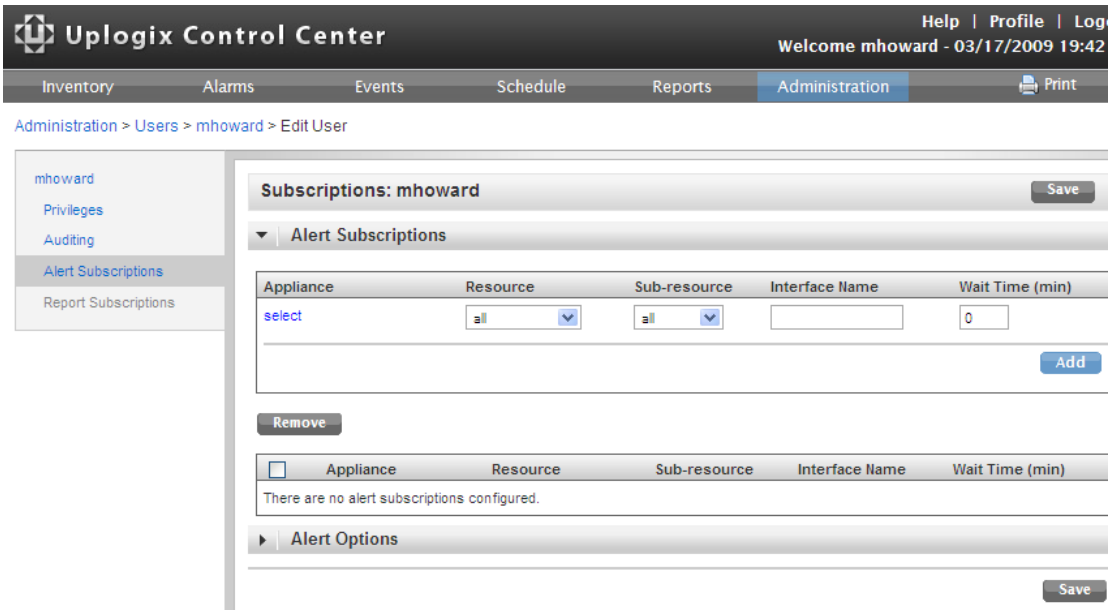
To allow this user to audit others, you will also need to subscribe the user to session reports. See Subscribing to reports on page 115 for instructions.

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.



Click the **save** button at the top or bottom of the page when you finish setting up the account information.

Subscribing to reports

Administration > Users

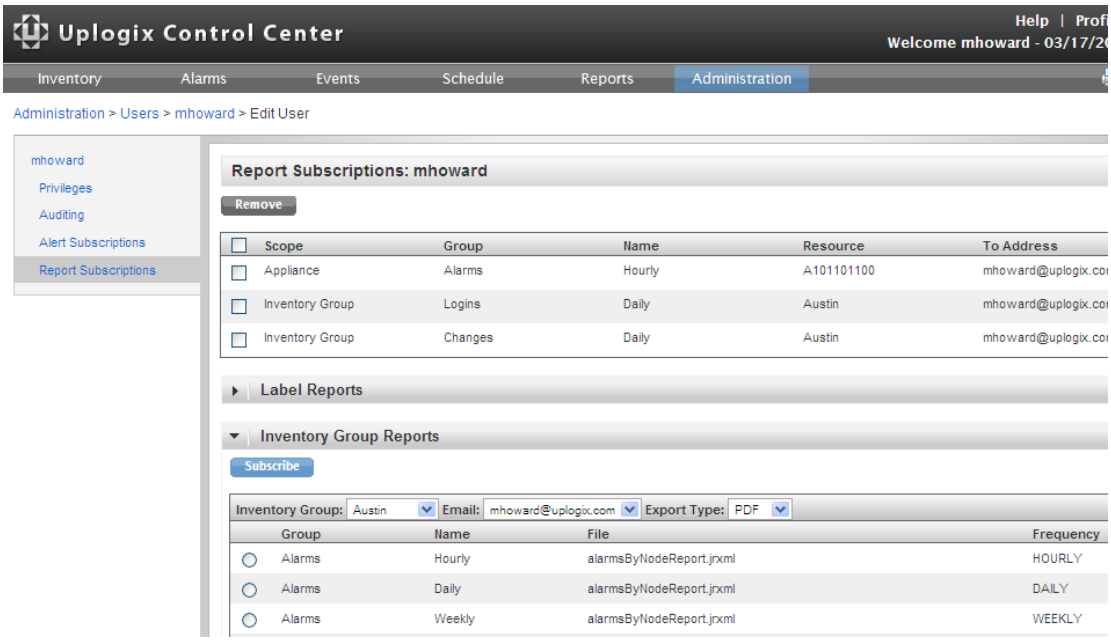
Administration > Groups

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 inventory group, Uplogix appliance, 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.



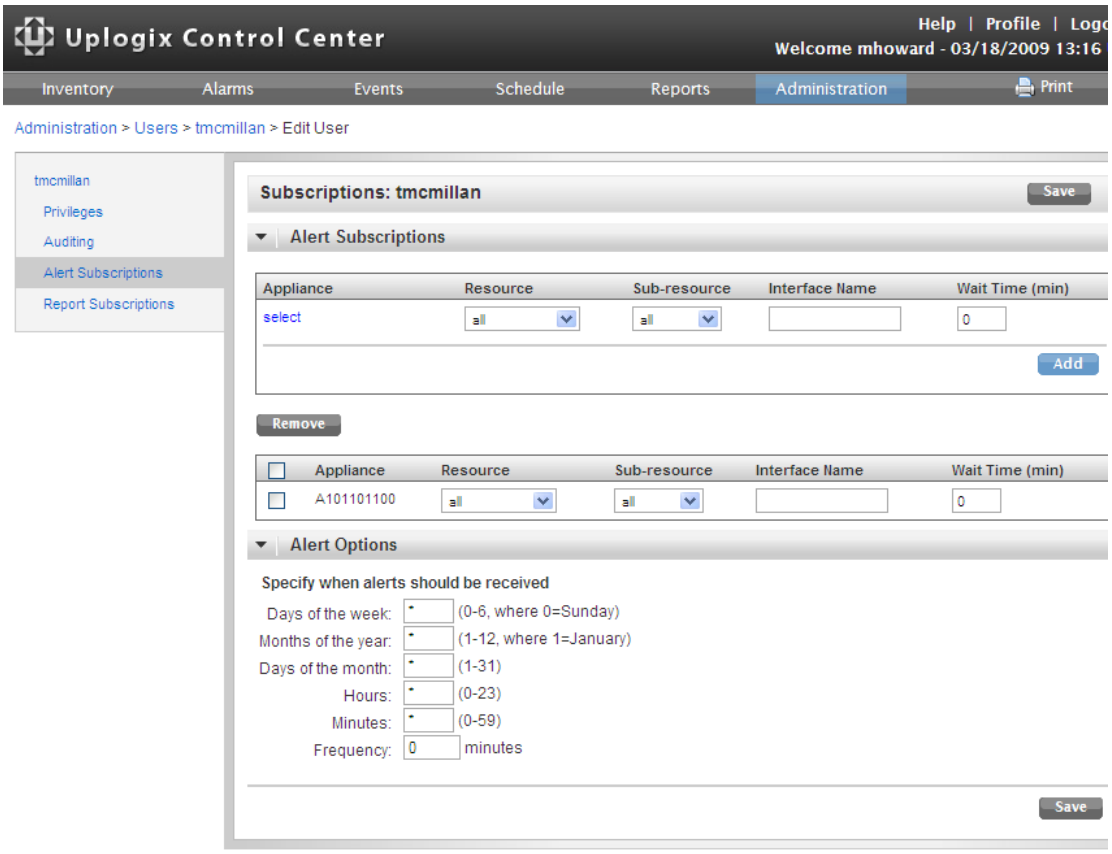
Session reports are available in the Principal Reports area at the bottom of the page. You can only subscribe to session reports on accounts that are configured as auditees on your user account. For more information on this, see Configuring the account to audit others and to be audited on page 114.

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.

You can limit the number of alerts that a user receives with the **Alert Options** settings on the Alert Subscriptions page.



Alert Options specifies times, days, and frequency when alerts may be emailed to this user. You may limit:

Days of the week - If this user should receive alerts only on 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.

Months of the year - If this user should only receive alerts during certain months, specify the beginning and ending month by number. For example, if the user should only receive alerts from September through May, enter 9-6.

Days of the month – If this user should receive alerts only during certain days of the month, specify which days here. For example, if the user is on call only from the 16th to the end of the month, enter 16-31.

Hours – Hours are specified in UTC time. To limit alerts to a specific time of day, specify start and end. For example, if a user in the US central time zone (UTC -6:00) needs to receive alerts that are generated between 5 p.m. and midnight, convert these times to UTC (00:00 to 06:00) and enter the hours as 23-6.

Minutes - To limit alerts to a specific part of each hour, specify the start and end - for example, 00-15.

Frequency - To change how often the Uplogix Control Center sends alerts. You may set the Uplogix Control Center to send alerts as seldom as every 120 minutes or as often as every minute.

Leave the wildcard * character in the fields you do not wish to restrict.

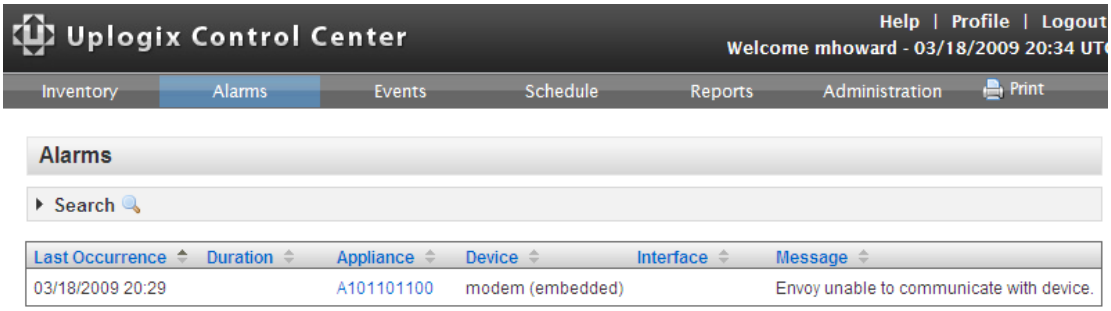
Viewing alarms and events

Alarms and events are similar. Both are logged. An alarm differs from an event in these ways:

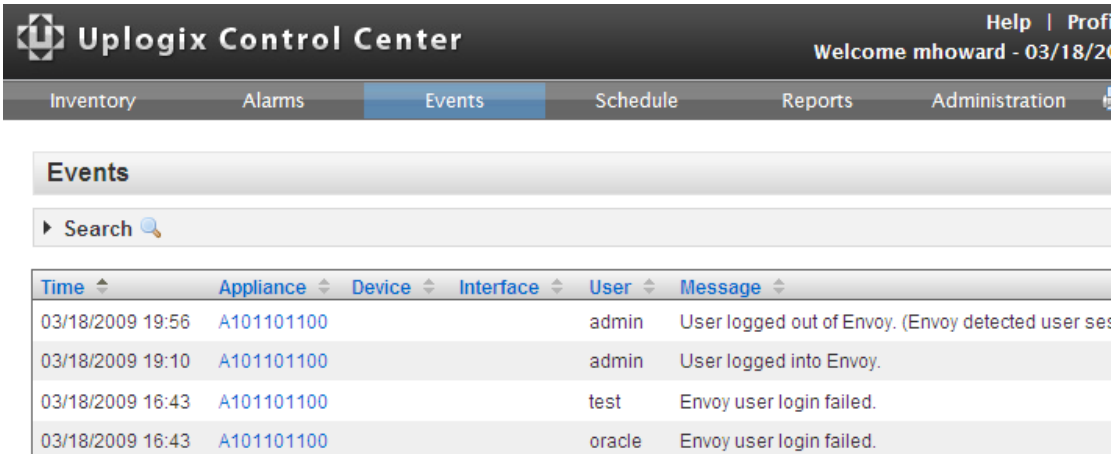
- An alarm has a duration; it remains active as long as the triggering condition exists.
- An alarm has a state: active or silenced.

The Alarms page provides a quick overview of active alarms on any of the managed Uplogix appliances. If there are any alarms when you log in, this is the screen you will see first.

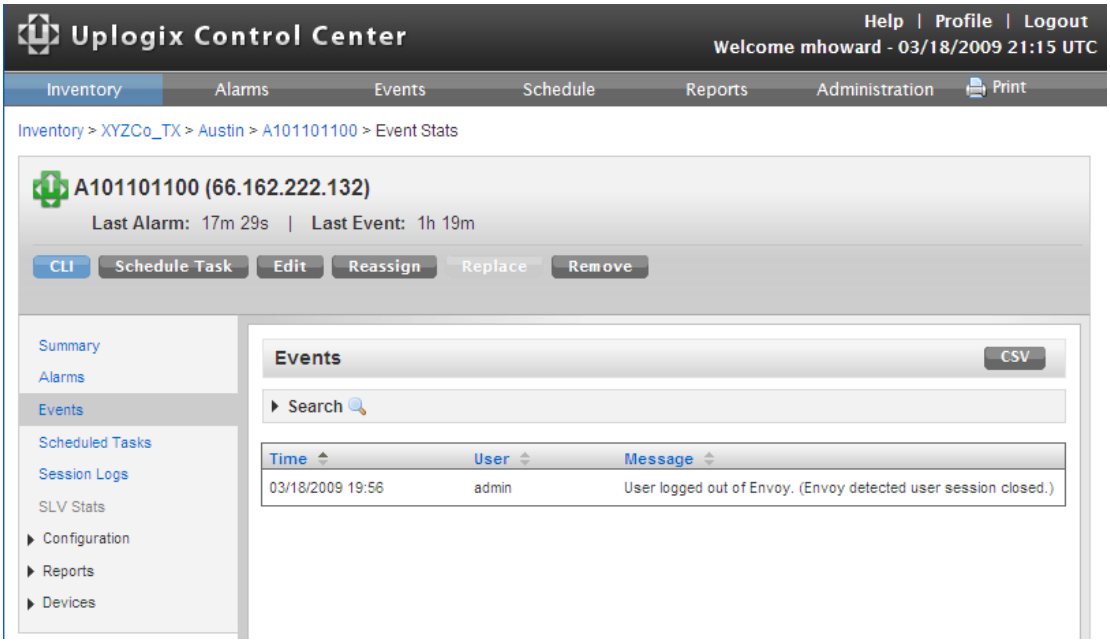
The alarm summary shows when an alarm was last generated, how long it has been active, which appliance it occurred on, and a message detailing the alarm. If the alarm involves a specific device and/or interface, that information is displayed as well.



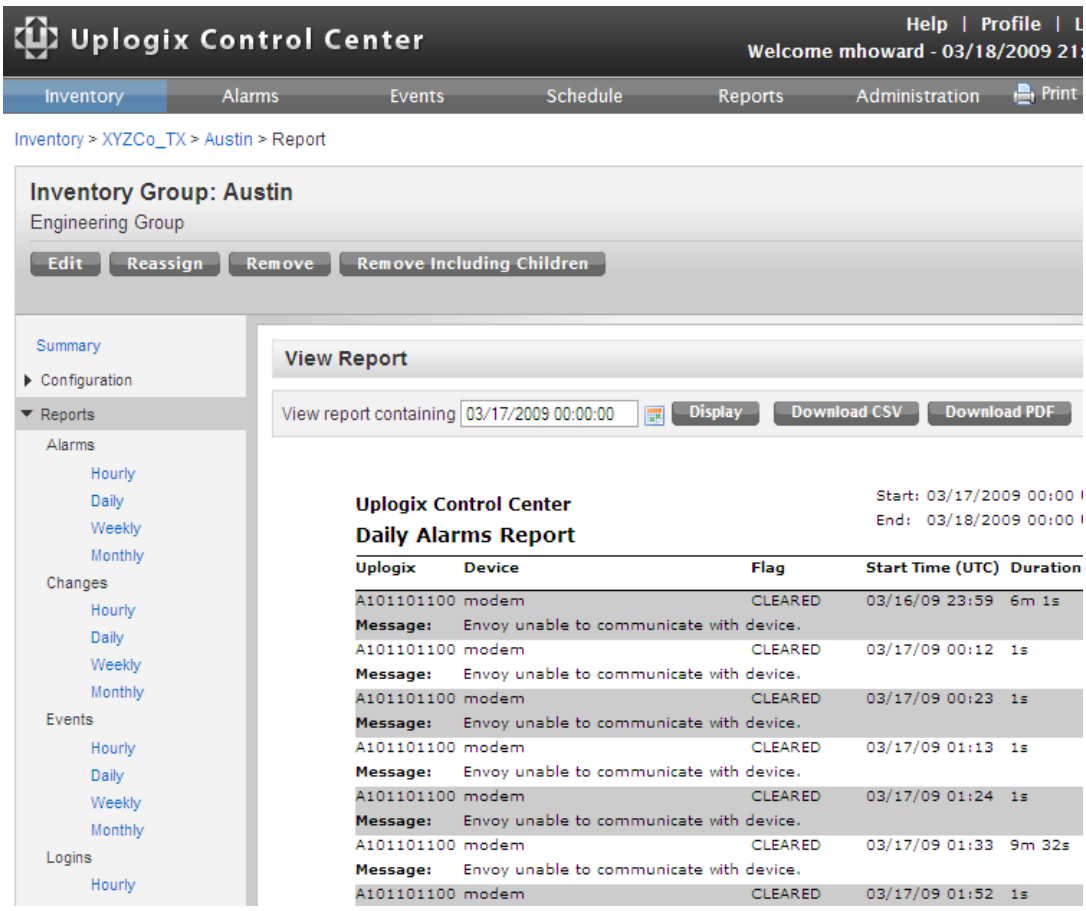
The Events page shows recent events for all managed Uplogix appliances. It is organized similarly to the Alarms page. Each entry shows the time of the event, the Uplogix appliance on which it occurred, the device and interface on which it occurred (if available), the user, and a descriptive message.



Alarms and events can be filtered by appliance, and by number of results. You can search the list of events by entering a text string in the search box, selecting the type of search and clicking **Search** To quickly access the appliance reporting the alarm or event, click the hostname in the Appliance column to bring up the appliance detail page. The Selecting the Alarms or Events menu will display alarms or events respectively for the specific device.



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



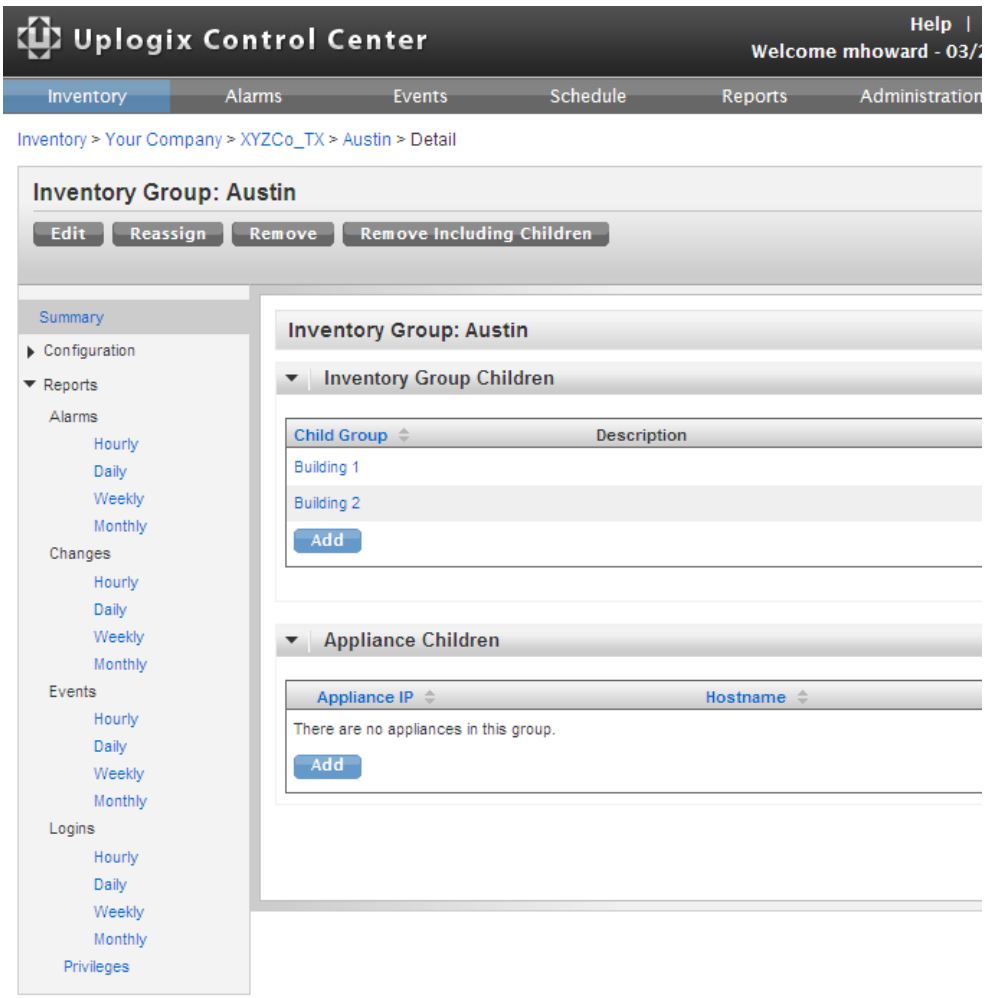
Viewing reports

The Uplogix Control Center regularly archives data received from Uplogix appliances. You can download the information in .jrxml files. Reports can be generated from inventory group and appliance levels. A report from the inventory group level will include information from all Uplogix appliances within the inventory group, while the appliance level will only include the specific appliance.

Inventory group reports

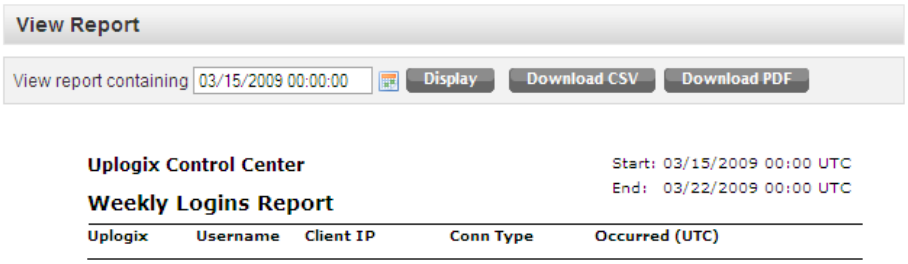
Inventory > group detail > Reports

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

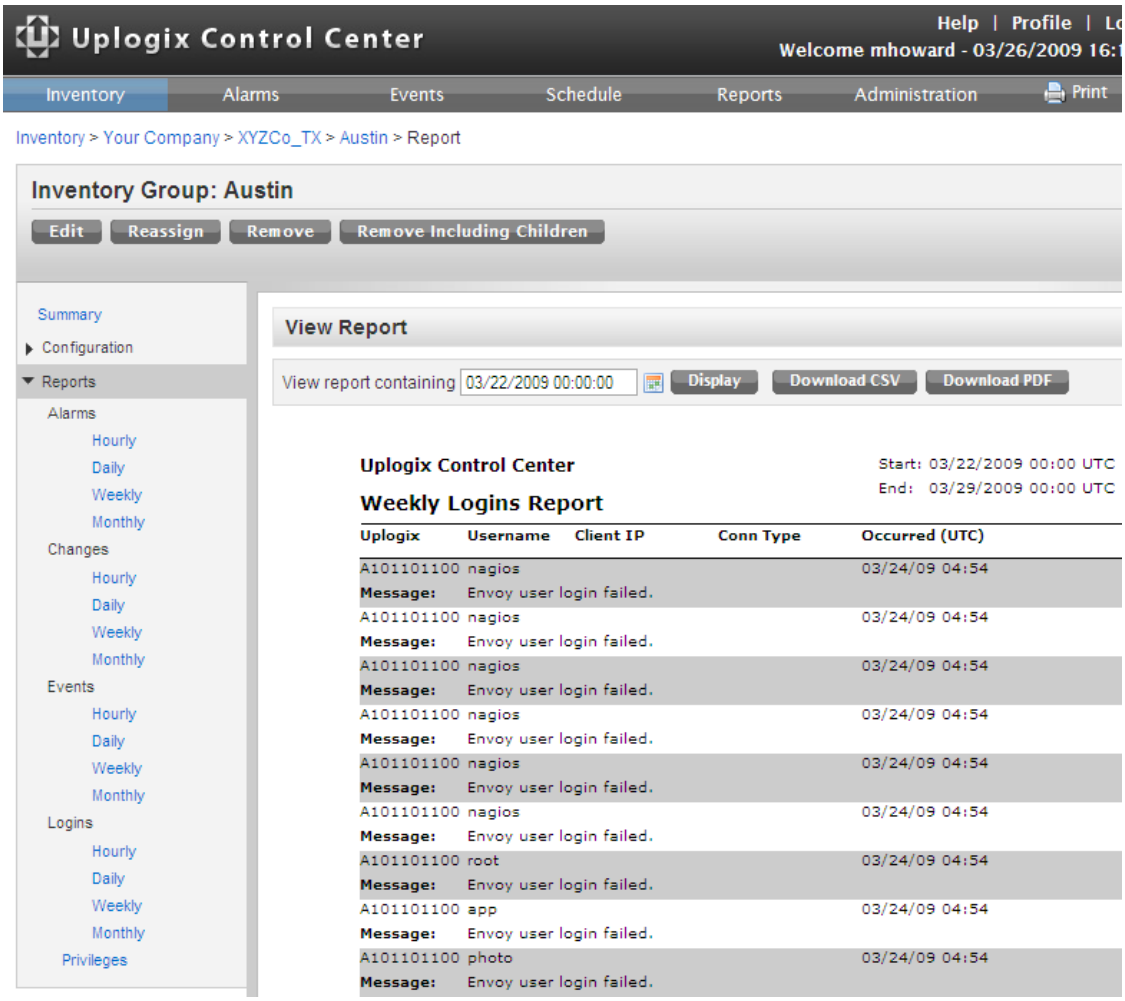


You may need to specify the desired range of times.

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.



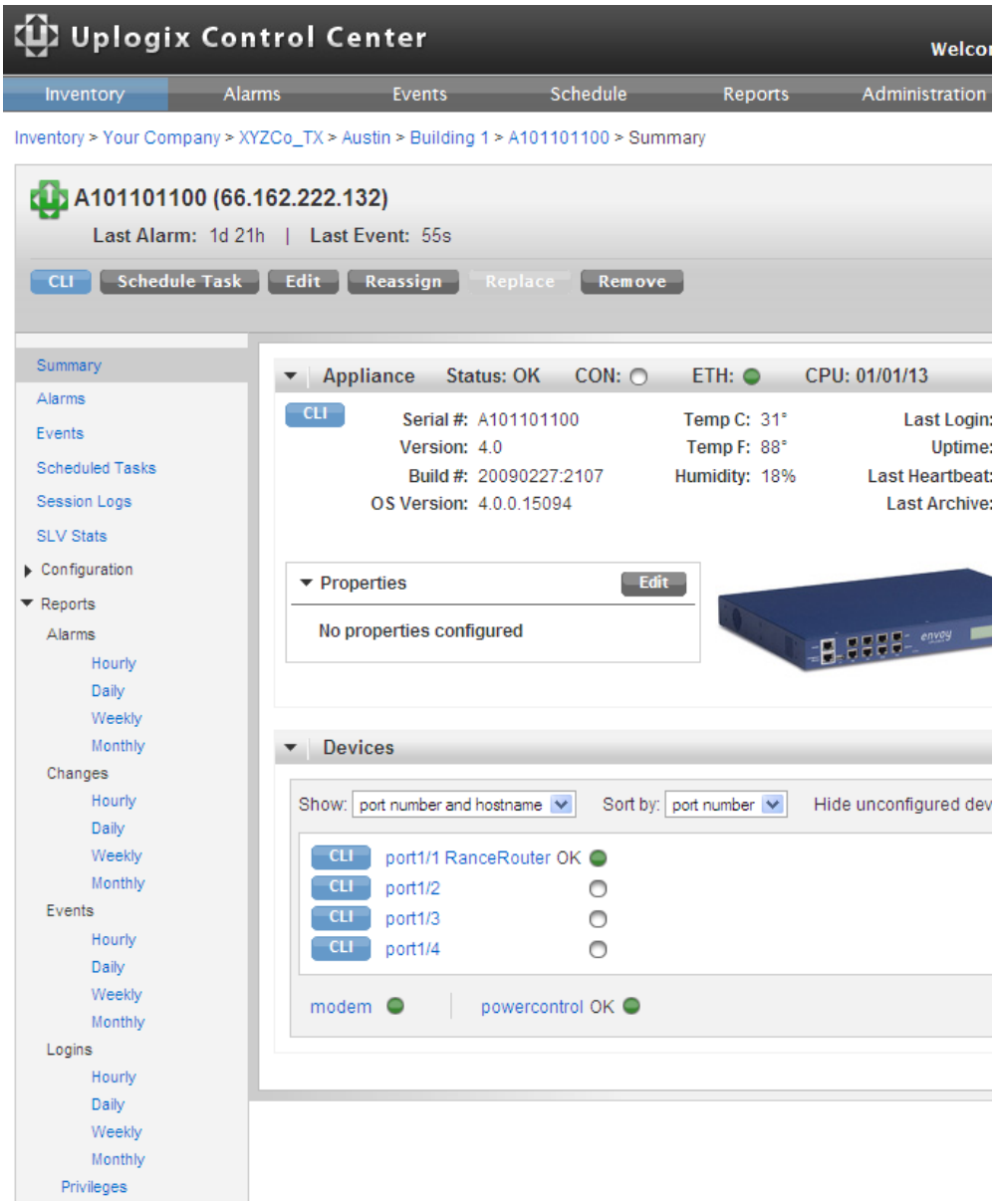
When you have specified the time period of interest, click **display**, **download PDF**, or **download CSV** as appropriate.



Appliance reports

Inventory > Appliance > Reports

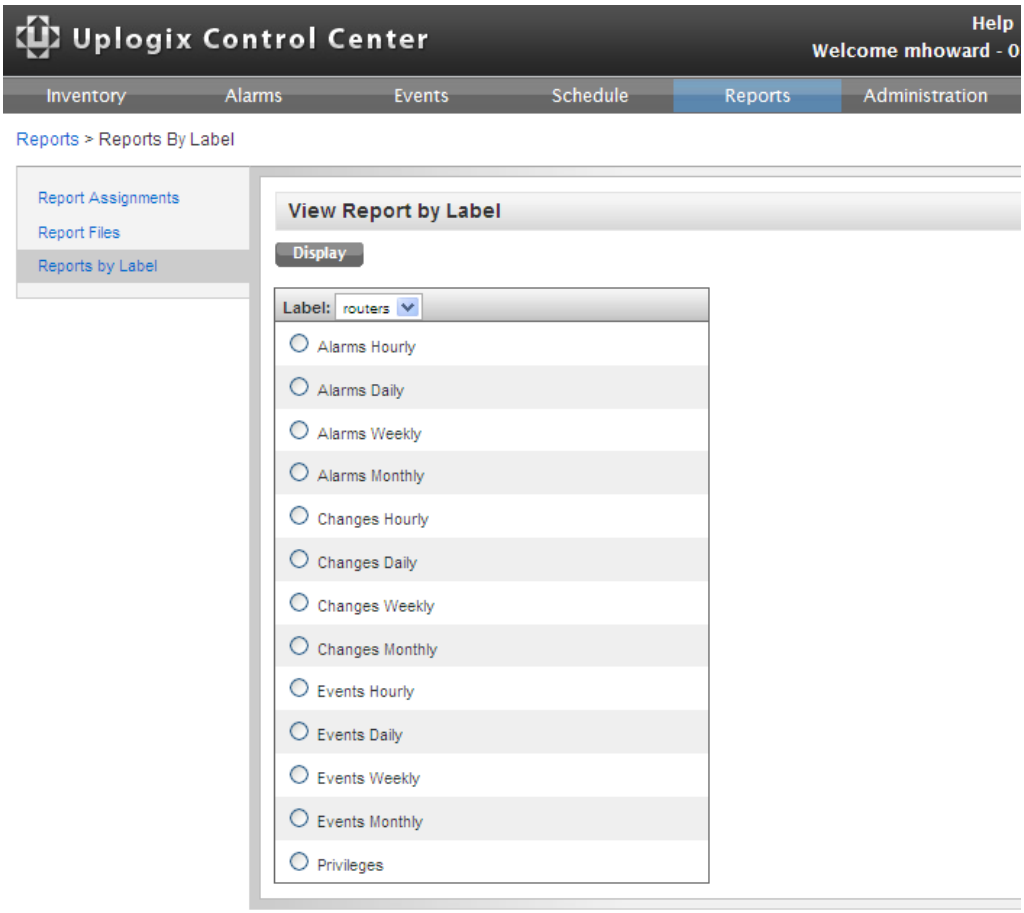
You can access appliance-specific reports from the reports menu of the appliance's page.


Uplogix Control Center
Welcor
Inventory
Alarms
Events
Schedule
Reports
Administration
Inventory > Your Company > XYZCo_TX > Austin > Building 1 > A101101100 > Summary
A101101100 (66.162.222.132)
Last Alarm: 1d 21h | Last Event: 55s
CLI
Schedule Task
Edit
Reassign
Replace
Remove
Summary
Alarms
Events
Scheduled Tasks
Session Logs
SLV Stats
Configuration
Reports
Alarms
Hourly
Daily
Weekly
Monthly
Changes
Hourly
Daily
Weekly
Monthly
Events
Hourly
Daily
Weekly
Monthly
Logins
Hourly
Daily
Weekly
Monthly
Privileges
Appliance Status: OK CON: ETH: CPU: 01/01/13
CLI
Serial #: A101101100
Version: 4.0
Build #: 20090227:2107
OS Version: 4.0.0.15094
Temp C: 31°
Temp F: 88°
Humidity: 18%
Last Login:
Uptime:
Last Heartbeat:
Last Archive:
Properties
Edit
No properties configured
Devices
Show: port number and hostname
Sort by: port number
Hide unconfigured dev
CLI port1/1 RanceRouter OK
CLI port1/2
CLI port1/3
CLI port1/4
modem
powercontrol OK

Reports by label

Reports > Reports by Label

Most reports are available on Group Detail, appliance detail, and port detail pages. However, reports can also be generated for custom labels. If you have created labels for managed devices (see Creating your own categories to manage devices on page 45), standard reports for each label are available on the Reports by Label page.

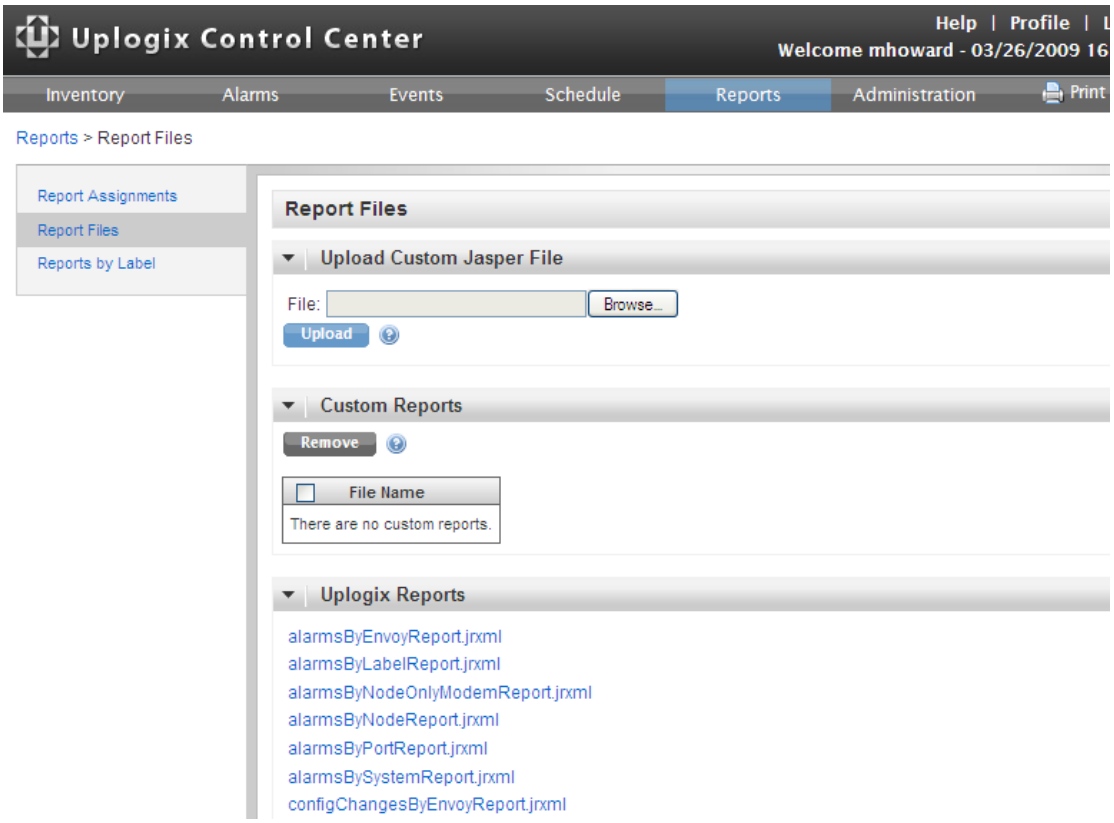


Report files

Reports > Report Files

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

After you have created a custom Jasper file, browse to 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 group detail, appliance detail, and port detail pages.

The Report Assignments page allows you to create custom reports to supplement any of the existing reports.

This feature creates reports as Jasper XML files. Please contact support@uplogix.com if you need help with this feature.

To create a new report assignment:

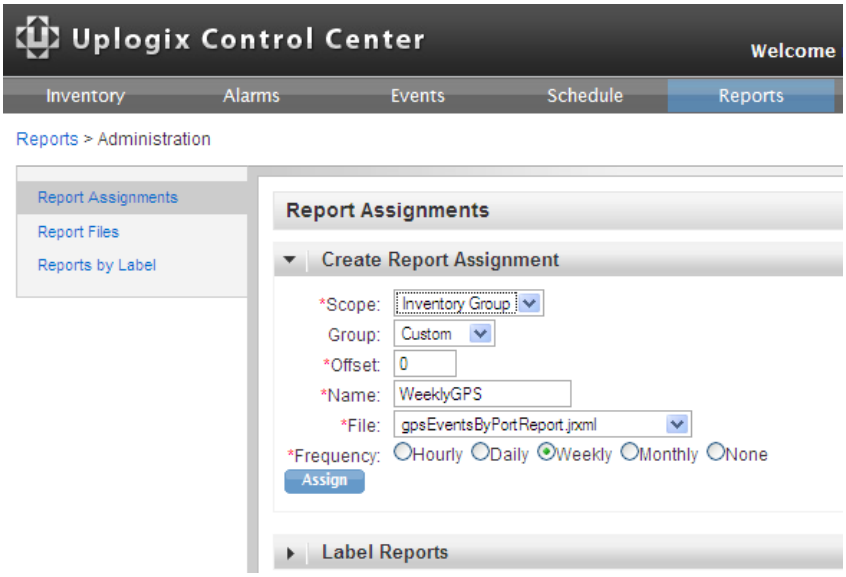
Choose the **scope** - this may be label, inventory group, system, or port.

Choose a **group** - this may be alarms, changes, events, logins, custom, or none.

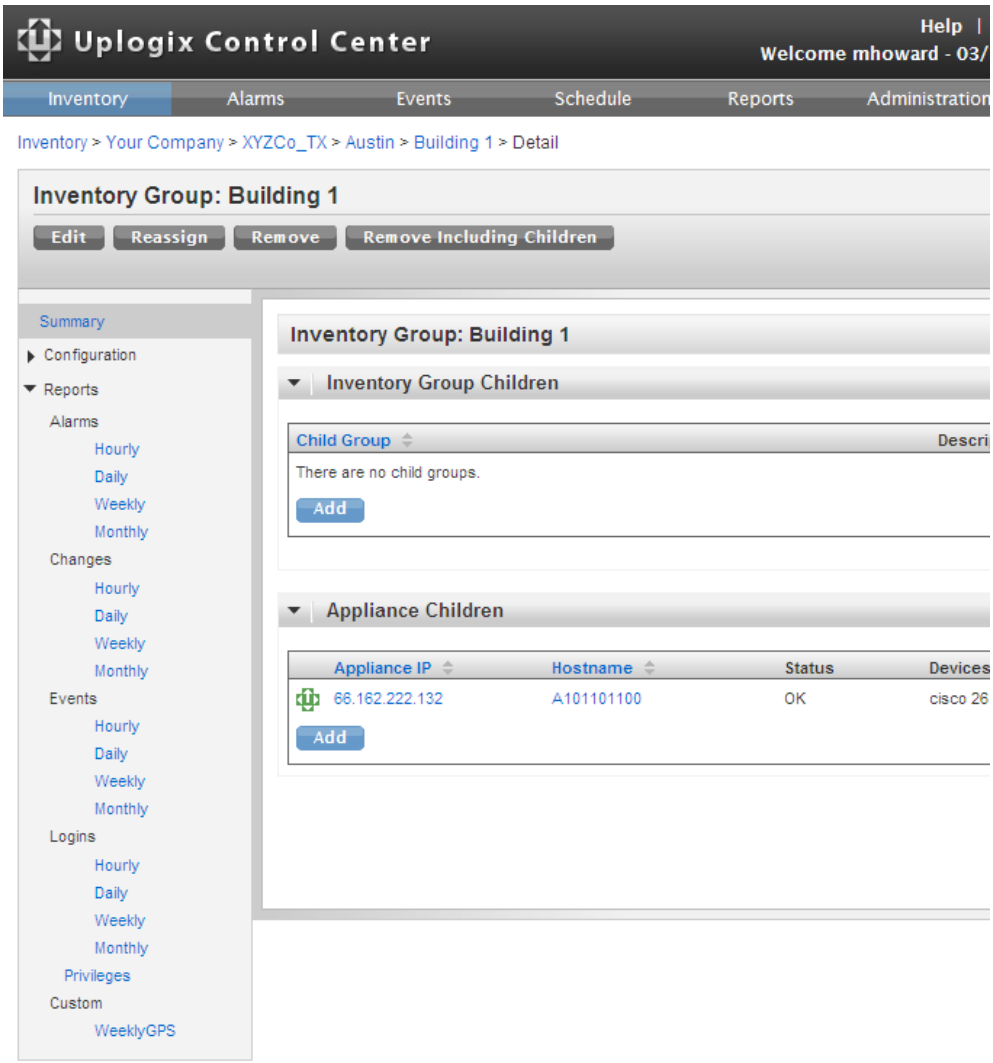
If there is already at least one report in the group that you choose within the selected scope (for example, alarm reports on inventory group pages), select the **offset**. This specifies the report's position in the list. An offset of 0 places the report first on the list.

Name the report, select the appropriate .jrxml file, and choose the frequency of report generation.

In the example shown here, we create a weekly report of GPS events on managed devices. The report will be available from inventory group pages under a custom report grouping.



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

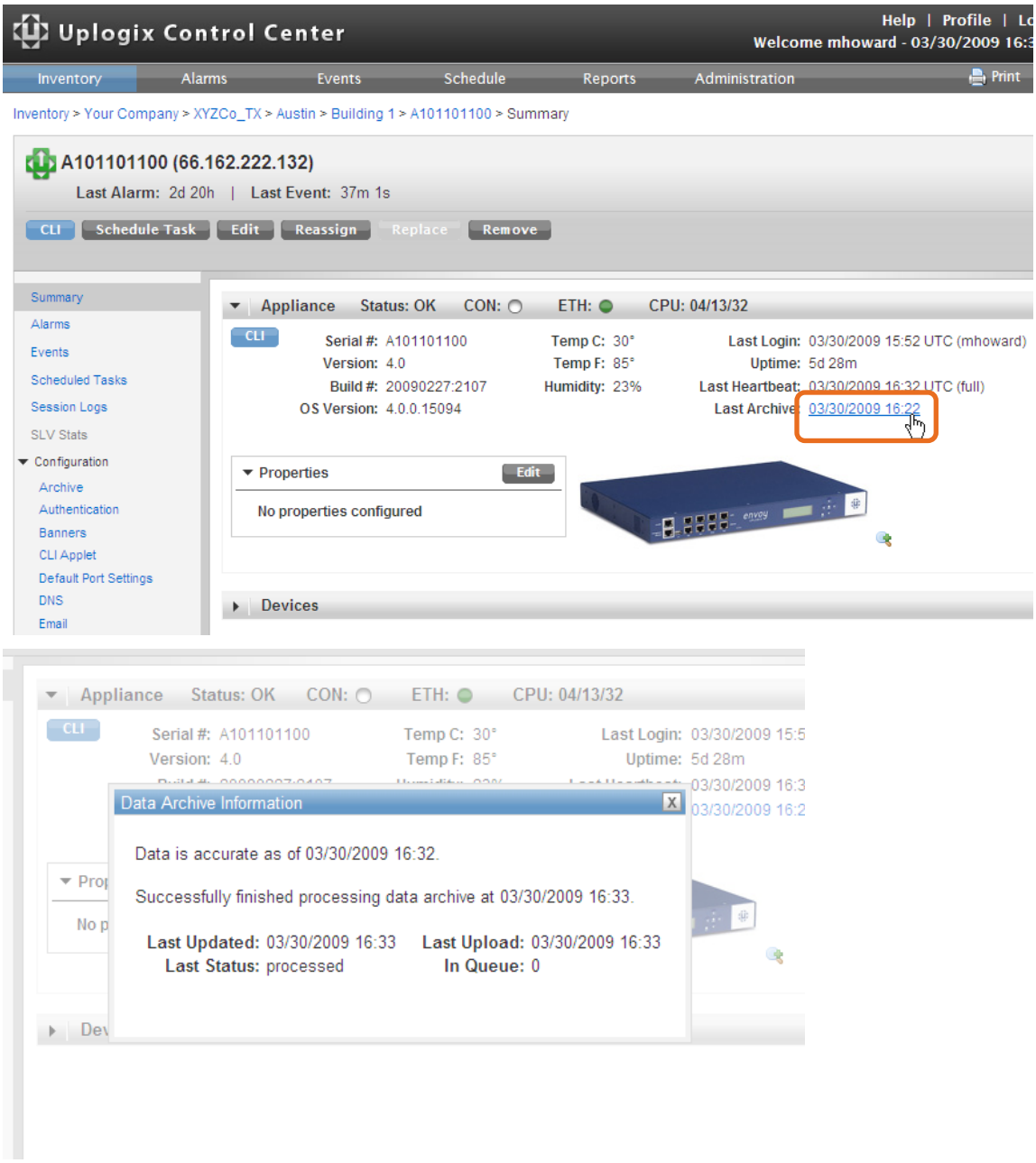


Although you cannot edit an existing report assignment, you can create a new report assignment with the same name. This overwrites the existing report assignment.

Viewing archive status information for an appliance

Inventory > Appliance Summary

The appliance summary page, clicking on the time of the last archive will generate a pop up that shows information about the last data archive operation.

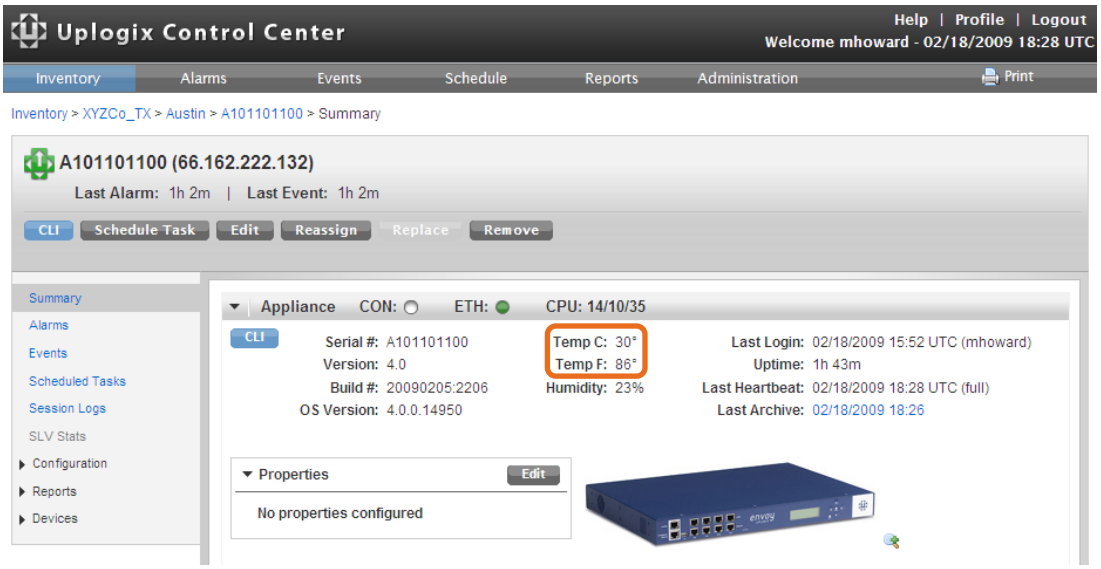

Uplogix Control Center
Help | Profile | Lo
Welcome mhoward - 03/30/2009 16:3
Inventory
Alarms
Events
Schedule
Reports
Administration
Print
Inventory > Your Company > XYZCo_TX > Austin > Building 1 > A101101100 > Summary
A101101100 (66.162.222.132)
Last Alarm: 2d 20h | Last Event: 37m 1s
CLI
Schedule Task
Edit
Reassign
Replace
Remove
Summary
Alarms
Events
Scheduled Tasks
Session Logs
SLV Stats
Configuration
Archive
Authentication
Banners
CLI Applet
Default Port Settings
DNS
Email
Appliance Status: OK CON: ETH: CPU: 04/13/32
CLI
Serial #: A101101100
Version: 4.0
Build #: 20090227:2107
OS Version: 4.0.0.15094
Temp C: 30°
Temp F: 85°
Humidity: 23%
Last Login: 03/30/2009 15:52 UTC (mhoward)
Uptime: 5d 28m
Last Heartbeat: 03/30/2009 16:32 UTC (full)
Last Archive: 03/30/2009 16:22
Properties
Edit
No properties configured
Devices

Appliance Status: OK CON: ETH: CPU: 04/13/32
CLI
Serial #: A101101100
Version: 4.0
Temp C: 30°
Temp F: 85°
Last Login: 03/30/2009 15:5
Uptime: 5d 28m
Data Archive Information
Data is accurate as of 03/30/2009 16:32.
Successfully finished processing data archive at 03/30/2009 16:33.
Last Updated: 03/30/2009 16:33
Last Upload: 03/30/2009 16:33
Last Status: processed
In Queue: 0

Viewing temperature statistics

Inventory > Appliance Summary

The appliance summary shows temperature reading (if available) from the last update.

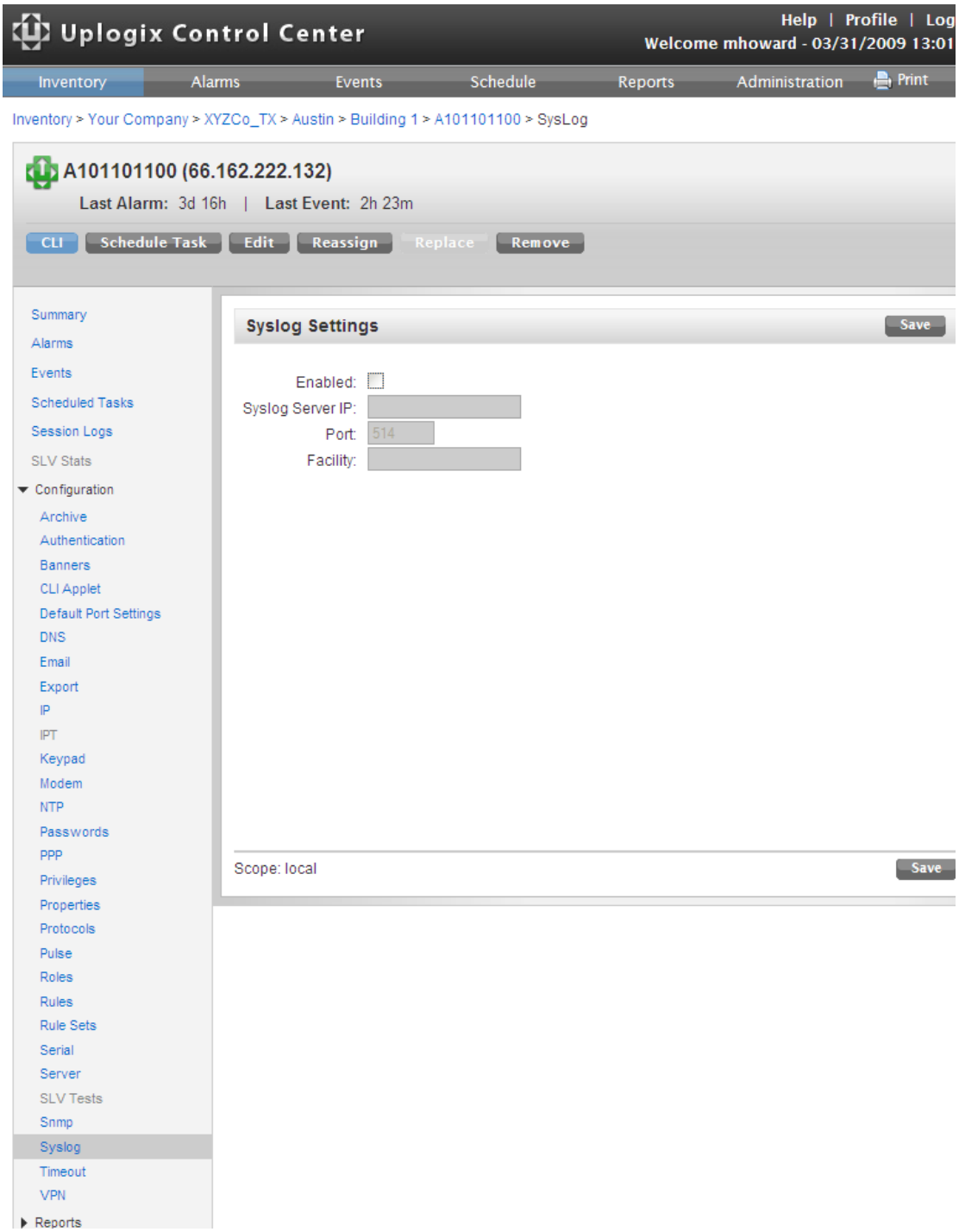


Viewing device syslogs

Inventory > Appliance Page > Configuration > Syslog

If syslog forwarding is enabled, you can review a connected device's syslogs from the **Configuration** menu on the appliance page.

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



Viewing session logs and auditing users

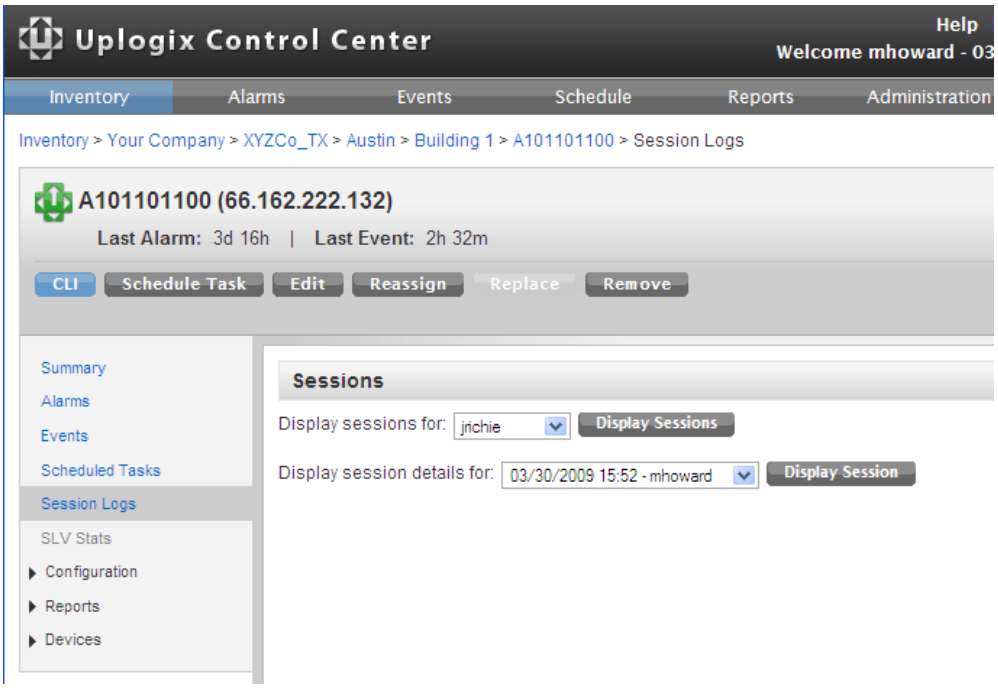
You can view transcripts of individual RMOS command line sessions that have ended, and you can configure accounts to receive reports of individual accounts' activities on the Uplogix Control Center.

Appliance session logs

Inventory > Appliance Page > Session Logs

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

You can display a list of archived sessions by user, as you can do through the Uplogix RMOS command line using the `show sessions` command. To do this, select the user from the list and click **display sessions**. To view the details of a listed session, click the **display session** button to the right of the timestamp. This is equivalent to the `show session` command.



Session information is updated every 30 seconds on the Uplogix appliance, 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:

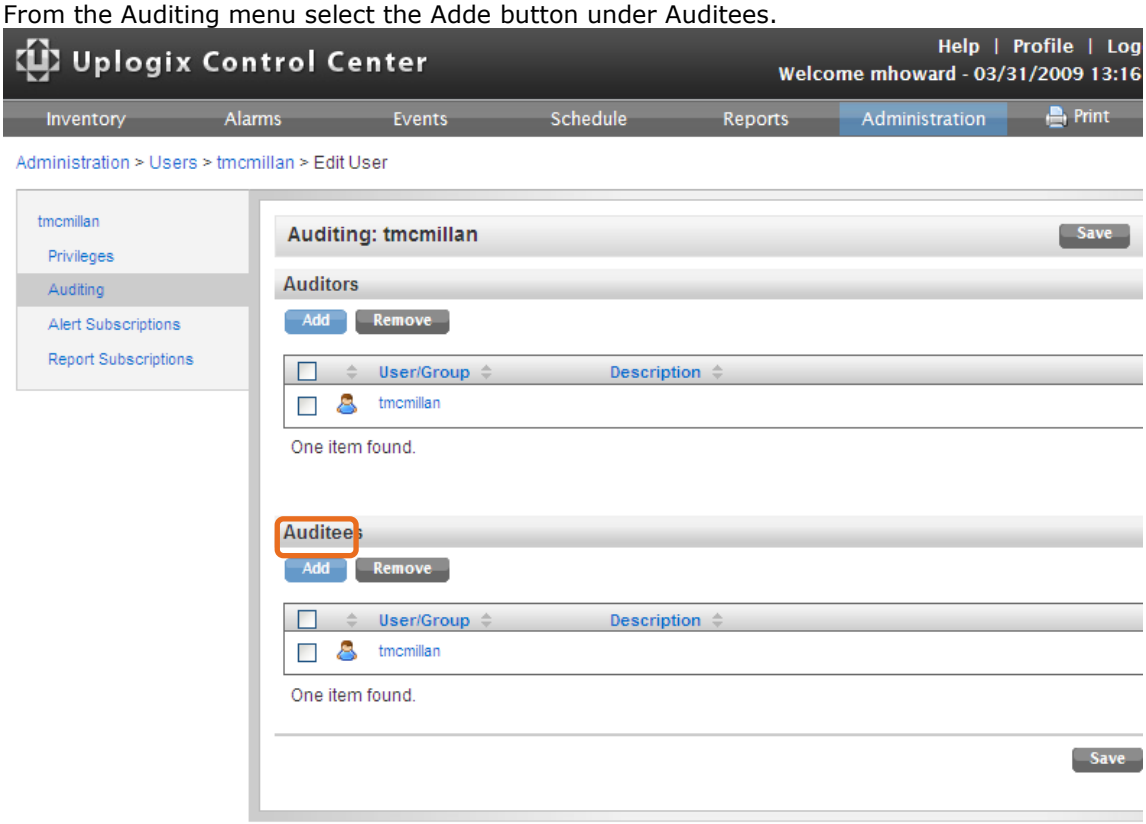
- A valid email address
- The users as auditees
- A report subscription to the appropriate session report on each user to be audited (See Setting up email, auditing, and subscriptions on page 112)

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

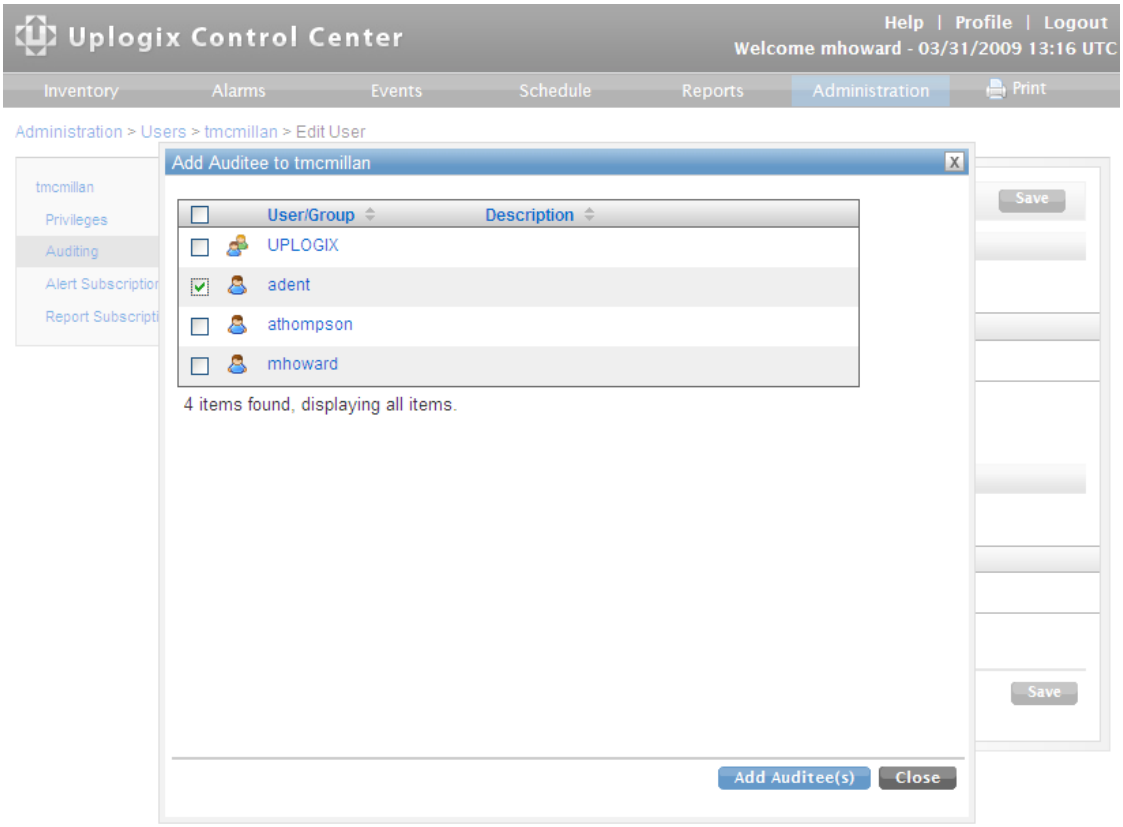
The following example shows how to configure a user to audit another user. In this example, the user **tmcmillan** (who has the admin role on the Uplogix Control Center) will be configured to audit another user, **adent**.

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 select the Adde button under Auditees.



From the pop up select the user to be audited, in this case, **adent** and click on the **Add Auditee(s)** button. The auditees will be added to tmcmillan's auditee listing, then click the **Save** button at the top or bottom of the page.

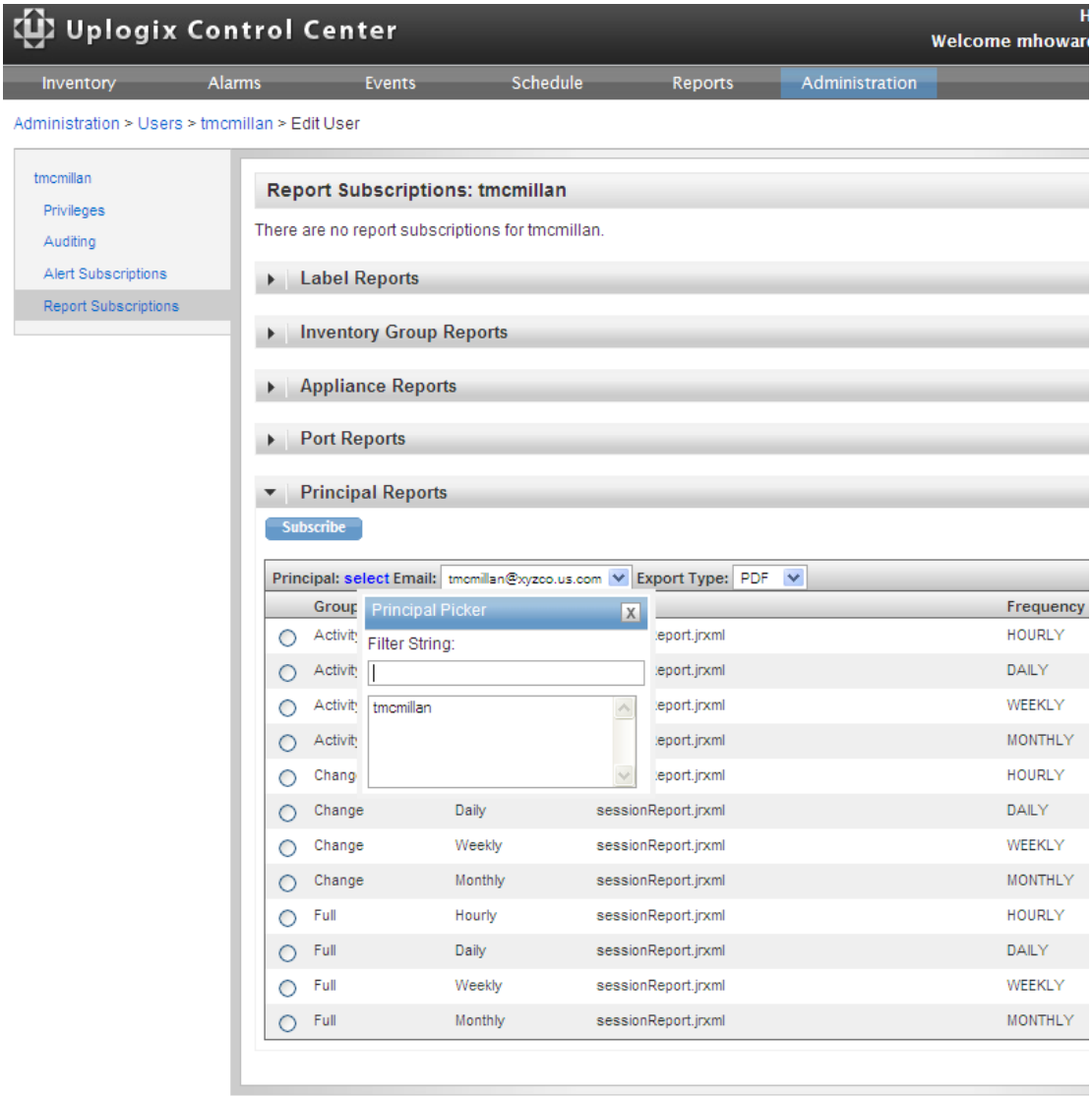


The tmcmillan account has an email address, and the user **adent** is now among **tmcmillan's** auditees, so **tmcmillan** will be able to subscribe to reports on **adent**.

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.

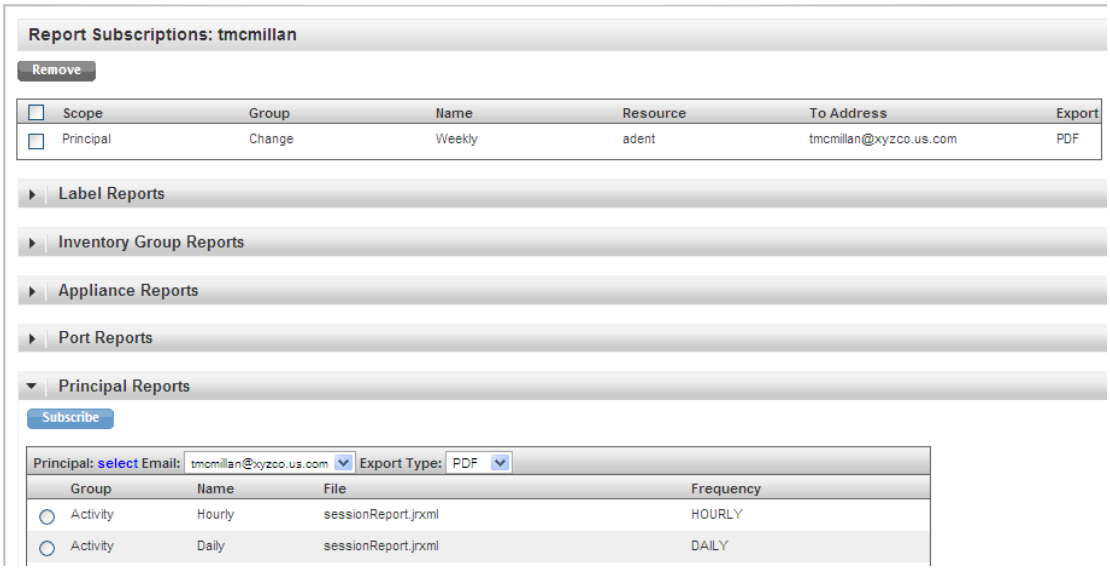
Select the **Principal** - the user to be audited. If your account is configured to audit many users, you may wish to enter a filter string to shorten the list of usernames.



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 appliance under management, or any device connected to a managed appliance.
- Full reports include all information from both activity and change reports.

Use the radio buttons next to the reports to select which reports you would like 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: tmcmillan
Remove
Scope
Group
Name
Resource
To Address
Export
Principal
Change
Weekly
adent
tmcmillan@xyzco.us.com
PDF
Label Reports
Inventory Group Reports
Appliance Reports
Port Reports
Principal Reports
Subscribe
Principal: select Email: tmcmillan@xyzco.us.com Export Type: PDF
Group
Name
File
Frequency
Activity
Hourly
sessionReport.jrxml
HOURLY
Activity
Daily
sessionReport.jrxml
DAILY

Troubleshooting

The following table lists some common problems, their usual causes, and ways you can correct them. More detailed troubleshooting information is available from the Uplogix Support knowledge base at www.uplogix.com/support/kb.

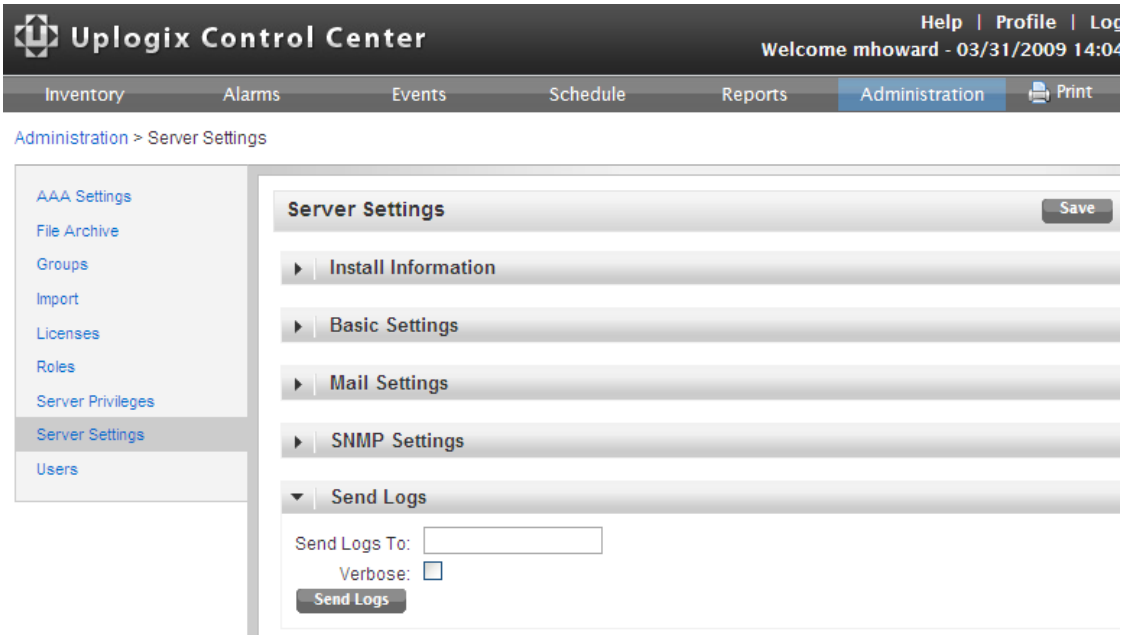
If a problem persists after you take the appropriate action(s), contact support@uplogix.com.

Problem	Possible cause	What to do
An error message indicates that an appliance's clock differs from the Uplogix Control Center's clock.	The appliance is not using the Uplogix Control Center as its clock source.	Log in to the appliance and use the `config system ntp` command to enable NTP. Specify the Uplogix Control Center's IP address as the NTP server.
An Uplogix appliance in the inventory did not inherit everything it should from Uplogix Control Center.	This is a known issue with certain versions of software.	Upgrade to version 4.0. Delete the appliance from the inventory tree, wait for it to show up in the Unassigned group, and then assign it back to the appropriate node in the inventory tree.
An Uplogix appliance shows up in the inventory as **permission denied**.	The appliance and the Uplogix Control Center are using different versions of software.	Upgrade whichever is using the earlier version, so that both the appliance and the Uplogix Control Center are using the same version.
A change report shows that a device configuration change was made and then reversed during an automated operation.	There is a communication issue between the appliance and the managed device.	Set the baud rate to a higher speed or open the firewall, if applicable, so that a TFTP connection can be enabled between the Envoy and the device.
A user is unexpectedly denied access to an Uplogix appliance via SSH; the SSH client gives a fatal error message rather than completing the login sequence.	The user does not have login privileges on this appliance, or the user's privileges need to be reset.	On the Inventory tab, select the Uplogix appliance's parent group. Click **privileges** to view the users and groups with privileges to appliances in this group. If the user is not listed, create the user's privileges. If the user is listed, select the radio button next to the user's name and click the **Remove** button and create the user's privileges again.

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 for you to do this.



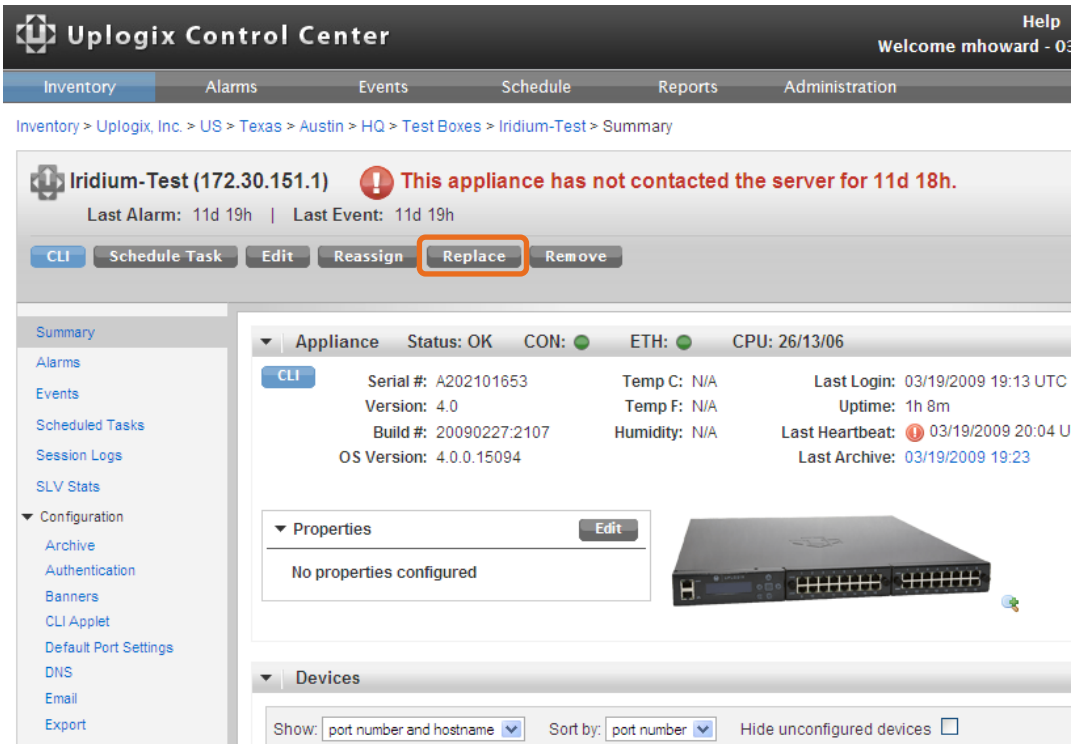
Follow the support technician's instructions to send the logs.

Replacing an appliance

Inventory > Appliance Page

If an Uplogix appliance stops sending heartbeats, the appliance'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 the **replace** button for a list of appliances that are available to replace the unresponsive appliance. To be listed, an appliance must be unassigned, running the same software version as the Uplogix Control Center, and communicating properly.

Select a replacement. The unresponsive appliance is replaced in the inventory list by the appliance you select. The Uplogix Control Center pushes the stored network device configuration from the replaced appliance to the replacement.

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

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.

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

- Organization name
- Account user's email address
- User's general contact information

You may request up to 10 accounts.

Requesting support

If you need to contact Uplogix customer support, please provide this information:

- Product model
- Serial number and software version (use the **`show version`** command from the RMOS command line)

Phone: 512-857-7070

Fax: 512-857-7002

URL: www.uplogix.com/support

Providing comments about this guide

Did you find the information you needed?

Was it accurate?

Did it help you?

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

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

Regulatory notices

The following section provides regulatory agency approvals for safety, electromagnetic compliance (EMC) and functional immunity that pertains to the Envoy NRM system.

Safety notices

UL 1950 - CSA 950 (US/Canada)

EMC notices

Federal Communications Commission (FCC) Class A Sub Part B

United States Federal Communications Commission notices

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy; and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

Modifications to this product not authorized by Uplogix could void the FCC approval and negate your authority to operate the product.

Industry Canada (IC)

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

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

RoHS compliance

The new Envoy NRM and Uplogix Control Center products are in full compliance with the Directive 2002/95/EC of the European Parliament and of the Council of 27 January 2003 on the restriction of the use of certain hazardous substances in electrical and electronic equipment.

CE Mark R & TTE directive

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

A full copy of the Declaration of Conformity can be obtained from:

Uplogix, Inc.
7600-B North Capitol of Texas Highway, Suite 220
Austin, Texas 78731
USA

Declaration of Conformity: This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

Déclaration de Conformité: Cet appareil est conforme aux conditions essentielles et à toute autre modalité pertinente de la Directive 1999/5/CE.

Declaración de Conformidad: Este equipo cumple los requisitos esenciales y otras cláusulas importantes de la directiva 1999/5/CE.

Konformitätserklärung: Dieses Gerät erfüllt die grundlegenden Anforderungen und sonstige maßgebliche Bestimmungen der Richtlinie 1999/5/EG.

Konformitätserklärung: Dette utstyret er i overensstemmelse med de grundlæggende krav og de relevante punkter i direktiv 1999/5/EF.

Index

?

? button 12

A

AAA (authentication, authorization, accounting) settings
- accounting 78
- authentication 78
- authorization 99
- for a single system 76
- for an inventory node 76
- global or Uplogix Control Center only 76

accounting settings 78

accounts
- configuring to receive email 112
- created on systems 84
- deleting 90
- group 87
- importing 108
- subscribing to reports and alerts 112
- user, creating and editing 85
- user, disabling 89

actions in rules 65

adding
- inventory groups 23
- systems 26
- task filters 51

adjusting width of inventory display 19

admin role 102

air flow requirements 5

alarms
- definition 111
- subscribing to 112
- using rules to define 65
- viewing 118

alerts, subscribing to 112

audit settings 85, 87, 112

authentication
- admin account 78
- administrator account 75
- external 78
- for a single system 76
- for an inventory node 76
- global or Uplogix Control Center only 76
- local 78
- servers, specifying 78
- setting password requirements 82
- TACACS or RADIUS 78

authorization keys 85

authorization using TACACS ACL 78, 99

B

banner, login 14

basic configuration 7

browsers, recommended 9

button
- ? (help) 12
- delete including children 25
- force updates on children 41, 65, 96
- print 11

buttons, unavailable 12, 91

C

caching passwords 78

case sensitivity of logins 9, 11

changing emsadmin password 8

child group (definition) 17

collapsing information 37

color codes in inventory display 19

command
- clear counters 58
- config answer 39, 50
- config authentication 58, 78
- config group 84, 87, 99
- config group no [username] 90
- config import 58
- config init (modem) 39
- config ppp 36, 39, 58
- config pptp 36
- config role 96, 99
- config rule 65
- config schedule 37, 51, 58
- config settings 41
- config system archive 36, 39
- config system authentication 75, 78, 82, 99
- config system banner 36, 39
- config system email 36, 39
- config system ip 39
- config system ipt 36, 39
- config system keypad 36, 39
- config system management 26, 32, 36, 39
- config system ntp 36, 39
- config system protocols 36, 39
- config system pulse 39
- config system serial 39
- config system snmp 39
- config system syslog-options 36, 39, 129
- config system timeout 36, 39
- config user 84, 85, 92
- config user no [username] 90
- config vpn 39

off 58
on 58
power 58
push config 58
push os 58
reboot 58
show alarms 118
show dashboard 37
show environment 128
show session 130
show sessions 130
show status 37
show tech 58
compatibility, system/management server
software version 1, 17
concurrent sessions, limiting 78
conditions in rules 65
connections
Ethernet 6
management console 6
power 6
contacting a remote appliance from Uplogix Control Center 50
conventions, typographical 1
creating
group accounts 87
inventory group 23
placeholders for systems 26
roles 96
rule sets 69
rules 65
task filters 51
user accounts 85
D
daylight saving time (DST) 14
default console settings 7
default login
Uplogix Control Center CLI 7
Uplogix web interface 9
default port settings 41
default settings, system 36
definitions
alarm 111
child group 17
event 111
inventory group 17
log 111
monitor 65
permission 91
privilege 91
report 111
role 91
rule 65
rule set 65
strong password 82
delete including children (button) 25
deleting
accounts 87, 90
inventory groups 25
systems 32
detail view
port 43, 129
system chassis 60
system dashboard 37
device labels 45
device syslog 129
devices, managing 43
dimmed features 12
disabling user accounts 89
display
license support 13
software version and build 13
display 13
DNS server, configuring 7
DST (daylight saving time) 14
E
email address
originating, for sending alerts 15
to contact Uplogix technical support 140
to receive alerts 85, 87, 112
user, deleting 85
email settings 15
emsadmin user 7
Envoy privileges 92, 96
events
definition 111
using rules to define 65
expanding chassis and port information 37
expired passwords, resetting 84
external authentication 78, 99
F
features of inventory group detail page 19
files
permission 92
system software upgrade 61
filter manager (scheduled tasks) 51
filters, task 51
force updates on children (button) .. 41, 65, 96
G
gateway, Uplogix Control Center, configuring. 7
grayed-out features 12
group accounts
deleting 90
importing 108
naming 11
subscribing to reports 112
group, inventory
adding 23
adding systems 26
configuring systems 36
deleting 25
detail page features 19
editing name and description 22
naming requirements 23
reassigning (moving) 24
root, renaming 22
Unassigned 20
viewing 19

grouping 17
groups of rules (rule sets) 69
H
help button 12
help link 12
I
icons in inventory display 19
importing
  group accounts 108
  privilege lists 108
  user accounts 108
importing 108
inactivity timeout 14
inheritance 41
initiating contact with a remote appliance 50
inventory
  icons and color codes 19
  privileges 91, 92, 96, 99, 102
  structure 17
inventory group
  adding 23
  adding systems 26
  configuring systems 36
  definition 17
  deleting 25
  detail page features 19
  editing name and description 22
  naming requirements 23
  reassigning (moving) 24
  root, renaming 22
  Unassigned 20
  viewing 19
IP address, Uplogix Control Center, configuring 7
L
labels 45
license support 13
licenses 33
limiting concurrent sessions 78
link, help 12
local accounts 84
local authentication 78
login banner 14
login, default
  Uplogix Control Center CLI 7
  Uplogix web interface 9
logs
  definition 111
  device syslog, viewing 129
  session, viewing 130
M
mail settings 15
managing devices 41, 43
managing inventory groups 36
modem, Iridium 50
monitors
  creating and scheduling 71
  definition 65
moving a system 31
moving an inventory group 24
N
naming requirements
  accounts, roles, and rules 11
  inventory groups 23
netmask, Uplogix Control Center, configuring 7
NTP server, configuring 7
number of concurrent sessions, limiting 78
O
organizing appliances by group 17
P
packing list 6
parts of the web interface 10
passwords
  administrator, default 9
  caching 78
  emsadmin, changing 8
  expired, resetting on system CLI login 84
  mail 15
  strong 82
  user, setting 85
permission (defined) 91
placeholder for system 26
port detail 43, 129
port settings, default 41
port, TCP
  mail server 15
  RADIUS 78
  SNMP 16
  TACACS 78
ports, managing 41, 43
power
  connecting 6
  requirements 5
precautions, safety 2
print button 11
privileges
  assigning 92
  by Envoy resource 92
  by label 45
  creating and editing 96
  definition 91
  deleting 92, 96
  importing 108
  managing with TACACS ACL 99
  required for configuring systems 39
  server 92
  viewing 96
problems, solving 135
Q
quick search
  inventory 19
  username 85
R
reassigning
  inventory groups 24
  system 31

removing
accounts 87, 90
inventory groups 25
systems 32
renaming the inventory root group 22
replacing a system 136
reports
by label 45
definition 111
subscribing 112
requirements
air flow 5
naming accounts, roles, and rules 11
naming inventory groups 23
power 5
temperature 5
roles
admin 102
assigning 92
by Envoy resource 92
by label 45
defined 91
naming requirements 11
root inventory group, renaming 22
rule sets
creating and editing 69
definition 65
rules
creating and editing 65
definition 65
in monitors 71
naming requirements 11
S
safety precautions 2
satellite modem 50
scheduling
monitors 71
software upgrade, system 61
tasks 51, 60
screen, login 14
searching
inventory 19
list of users 85
secure shell clients supported (list) 8
serial settings, management console defaults 7
server privileges 91, 92, 96, 102
service clearance 5
service level verification (SLV) license 33
session timeout 14
sessions 130
site requirements 5
SLV (service level verification) license 33
SMS message 50, 60
SNMP settings 16
software version compatibility 1, 17
software version display 13
software, system, upgrading 61
solving problems 135
space character 11
SSH clients supported (list) 8
statistics, system temperature 128
strong passwords 82
structure of inventory 17
subnet mask, Uplogix Control Center, configuring 7
subscribing to reports and alerts 112
superuser 102
suspending user accounts 89
syslog, viewing 129
system
adding 26
adding more than 10 33
deleting 32
port detail 43, 129
reassigning (moving) 31
replacing 136
scheduling tasks 60
searching by hostname 19
temperature statistics 128
upgrading software 61
viewing summary 37
system, configuring 36, 39
system/management server software version compatibility 1, 17
T
TACACS
accounting settings 78
ACL 99
servers, specifying 78
task filters 51
tasks, scheduling 51, 71
TCP port
mail server 15
RADIUS 78
SNMP 16
TACACS 78
temperature requirements 5
terminal clients (list) 7
timeout for inactive sessions 14
Timezone (setting) 14
troubleshooting 135
typographical conventions 1
U
Unassigned inventory group 20
unavailable features 12, 91
upgrading system software 61
use DST (setting) 14
Use SNMP (setting) 16
username
case sensitivity 9, 11
naming requirements 11
users
auditing 85, 112
creating and editing 85
deleting 90
disabling accounts 89
importing 108
subscribing to reports and alerts 112

V
ventilation requirements 5
version compatibility 17
version display 13
viewing
  alarms 118
  device syslog 129
  inventory groups 19
  license support 13
  sessions 130
  software version 13
W
web browsers, recommended 9
web interface, page structure and navigation 10
width control, inventory display 19
window, login 14
Y
Your Company inventory group, renaming 22