



RACK POWER MANAGER

INSTALLER/USER GUIDE 





Rack Power Manager

Installer/User Guide

Emerson, Emerson Network Power and the Emerson Network Power logo are trademarks or service marks of Emerson Electric Co. Avocent, the Avocent logo, AlterPath, Cyclades, DSR and DSView are trademarks or service marks of Avocent Corporation or its affiliates in the U.S. and other countries. All other marks are the property of their respective owners. This document may contain confidential and/or proprietary information of Avocent Corporation, and its receipt or possession does not convey any right to reproduce, disclose its contents, or to manufacture or sell anything that it may describe. Reproduction, disclosure, or use without specific authorization from Avocent Corporation is strictly prohibited. ©2013 Avocent Corporation. All rights reserved.

TABLE OF CONTENTS

Product Overview	1
<i>System Components</i>	<i>1</i>
<i>Third party products</i>	<i>2</i>
<i>Supported Units</i>	<i>2</i>
<i>Power devices</i>	<i>3</i>
Installation	5
<i>About Installation</i>	<i>5</i>
<i>Minimum requirements for the Rack Power Manager software</i>	<i>5</i>
<i>Before installing and configuring the Rack Power Manager software</i>	<i>6</i>
<i>Installing the Rack Power Manager Software</i>	<i>6</i>
<i>Configuring the Rack Power Manager Software</i>	<i>8</i>
<i>Running the Rack Power Manager Software</i>	<i>9</i>
<i>Minimum client requirements</i>	<i>10</i>
<i>Opening a client session</i>	<i>10</i>
<i>Uninstalling the Rack Power Manager Software</i>	<i>11</i>
<i>Java Installation</i>	<i>12</i>
Transition	15
<i>DSView™ 3 Software and Power Manager Plug-in to RPM software</i>	<i>15</i>
<i>Data Replication</i>	<i>15</i>
<i>Back up the DSView 3 Software</i>	<i>16</i>
<i>Backup the Power Management database</i>	<i>17</i>
<i>Install Rack Power Manager Hub Server</i>	<i>18</i>
<i>Migration Utility</i>	<i>19</i>
<i>Exporting the Data</i>	<i>19</i>
<i>Importing the Data</i>	<i>20</i>
<i>Configure RPM Hub and Spoke servers</i>	<i>22</i>
<i>DSView software to RPM software</i>	<i>22</i>
<i>Data Replication</i>	<i>22</i>
<i>Back up the DSView Software</i>	<i>23</i>
<i>Extract the PostgreSQL data file</i>	<i>24</i>

<i>Install Rack Power Manager Hub Server</i>	24
<i>Importing the Data</i>	25
<i>Configure RPM Hub and Spoke server</i>	26
Rack Power Manager Explorer Windows	27
<i>Using the Side Navigation Bar</i>	28
<i>Using Windows</i>	29
<i>Sorting information in a window</i>	29
<i>Filtering information in a window</i>	29
<i>Using the Customize link in windows</i>	30
<i>Displaying pages</i>	32
<i>Printing a window</i>	32
<i>Refreshing a window</i>	32
<i>Using keyboard commands</i>	33
Basic Operations	35
<i>Rack Power Manager Help</i>	35
<i>Configuring the Rack Power Manager help location</i>	35
<i>Installing Rack Power Manager help on a local server</i>	36
<i>Global System Properties</i>	36
<i>Legal Notice</i>	37
<i>PCI Compliance Configuration</i>	37
<i>Power Settings</i>	38
<i>Profiles</i>	39
<i>Changing user options</i>	39
<i>Changing the color scheme</i>	40
<i>Changing your password</i>	40
<i>Choosing the serial session application</i>	41
<i>Specifying a user certificate</i>	41
<i>Specifying an SSH key</i>	42
<i>Enabling user credential caching</i>	43
<i>Built-in User Groups</i>	43

<i>Internet Explorer Considerations</i>	45
<i>Managing ActiveX® controls</i>	45
<i>Security zones</i>	46
<i>Advanced Internet options</i>	48
<i>Certificates</i>	49
<i>System certificate policy and trust store</i>	50
<i>Integrated Windows Authentication</i>	52
<i>Firewalls</i>	53
<i>VPNs</i>	54
<i>NAT Devices</i>	56
<i>Licenses</i>	58
<i>Adding a new license key</i>	60
<i>System Information</i>	60
Rack Power Manager Servers	61
<i>Server Properties</i>	61
<i>Server certificates</i>	63
<i>Server trap destinations</i>	68
<i>Client session information</i>	69
<i>Email</i>	70
<i>Unit status polling</i>	70
<i>Backing up and Restoring Hub Servers Manually</i>	71
<i>Spoke Servers</i>	74
<i>Replication</i>	78
Authentication Services	81
<i>Supported Authentication Services</i>	81
<i>Rack Power Manager software internal authentication service</i>	82
<i>Active Directory external authentication service</i>	84
<i>Windows NT external authentication service</i>	91
<i>LDAP external authentication service</i>	93
<i>RADIUS external authentication service</i>	99

<i>TACACS+ external authentication service</i>	101
<i>RSA SecurID external authentication service</i>	105
<i>User Authentication Services Window</i>	107
Units View Windows	109
<i>Types of Units View windows</i>	109
<i>Topology view</i>	110
<i>Accessing Units View windows</i>	111
<i>Showing and hiding units</i>	112
<i>Units View windows fields</i>	113
<i>Multiple unit operations from a Units View window</i>	115
<i>Unit Overview Windows</i>	116
<i>Unit Status Window</i>	117
Adding and Deleting Units	119
<i>Adding Units</i>	119
<i>Wizards that add units</i>	120
<i>Adding a single managed appliance</i>	120
<i>Adding managed appliances from a range or list of IP addresses</i>	122
<i>Adding a generic appliance</i>	123
<i>Deleting Units</i>	124
<i>Automatically deleting attached units</i>	124
Synchronizing the Rack Power Manager Software Database	125
<i>Name Synchronization</i>	125
<i>Automatic name push</i>	125
<i>Automatic name pull</i>	126
<i>Manual name push</i>	128
<i>Manual name pull</i>	128
<i>Topology Synchronization</i>	129
<i>Automatic topology synchronization</i>	129
<i>Topology synchronization options in the Add Unit Wizard</i>	130
<i>Topology synchronization options in the Resync Wizard</i>	130

<i>Automatic Inheritance for Group Memberships and Properties</i>	131
Managing Units	133
<i>Appliance Configuration Templates</i>	133
<i>Saving appliance configuration templates</i>	133
<i>Modifying appliance configuration template properties</i>	134
<i>Applying appliance configuration templates</i>	135
<i>Unit Properties</i>	136
<i>Unit Overview Settings</i>	140
<i>About Access Rights</i>	143
<i>How access rights can be assigned</i>	144
<i>Unit Access Rights</i>	144
<i>Managed Appliance Settings</i>	145
<i>Managed Appliance SNMP Settings</i>	147
<i>Bulk Configuration of Individual settings</i>	148
<i>Infrastructure View</i>	149
<i>Asset and Usage Reports</i>	150
<i>Unit Reports</i>	151
<i>Asset</i>	152
<i>Usage</i>	152
<i>Scheduled Reports</i>	153
<i>Segregated Temperature Readings</i>	154
<i>Tiered Energy Cost Setting</i>	155
Power Devices and Power Device Sockets	157
<i>Power Devices</i>	157
<i>Power Device Input Feed</i>	159
<i>Power Device Sockets</i>	160
<i>Power Control of Devices Attached to Power Devices</i>	162
<i>Power Operations</i>	163
Unit Sessions and Connections	165
<i>Managed Appliance Session Settings</i>	165

<i>Customizing the Appliance Sessions window</i>	165
<i>Connections to Units</i>	166
SSH Passthrough Sessions	167
<i>Configuring SSH Passthrough</i>	167
<i>Enabling SSH Passthrough</i>	167
<i>SSH port sharing</i>	168
<i>SSH Passthrough Sessions</i>	169
<i>Establishing an SSH Passthrough connection to a unit</i>	170
<i>Escape key sequence</i>	172
<i>Break sequences</i>	173
<i>Transferring read/write access</i>	174
<i>Disconnecting a session</i>	175
<i>Displaying session output</i>	175
Grouping Units	177
<i>Site, Department and Location Groups</i>	177
<i>Custom Fields</i>	180
<i>Unit Groups</i>	183
<i>Unit group hierarchy</i>	185
<i>Adding or deleting a unit group</i>	188
<i>Changing the unit group properties</i>	189
<i>Custom Groups</i>	192
<i>Adding or deleting a custom group query</i>	192
<i>Changing the custom group properties</i>	193
<i>Changing the custom group rights</i>	193
<i>Custom Group Reports and Scheduled Tasks</i>	194
DS Zones	197
<i>Managing and Accessing Zones</i>	197
<i>Enabling DS Zones</i>	197
<i>Creating zones</i>	197
<i>Accessing zones</i>	198

<i>Transferring units to a zone</i>	199
<i>Managing zone properties</i>	200
<i>Using Zones</i>	202
<i>Units actions in a zone</i>	202
Managing User Accounts	209
<i>User Accounts Windows</i>	209
<i>Adding User Accounts</i>	211
<i>Deleting User Accounts</i>	214
<i>Unlocking User Accounts</i>	214
<i>Resetting a User Account Password</i>	214
<i>Changing User Account Properties</i>	215
<i>Username</i>	215
<i>User certificates</i>	216
<i>User SSH key</i>	216
<i>User password</i>	217
<i>User account restrictions and expiration settings</i>	217
<i>User group membership</i>	218
<i>Address</i>	219
<i>Phone contact</i>	219
<i>Email contact</i>	219
<i>User notes</i>	220
<i>Custom field properties</i>	220
<i>User Access Rights</i>	220
User Groups	223
<i>Adding User-defined User Groups</i>	224
<i>Deleting User-defined User Groups</i>	227
<i>User Group Properties</i>	227
<i>Changing User Group Members</i>	228
<i>User Group Access Rights</i>	229
Using the Telnet Viewer	231

<i>About the Telnet Viewer</i>	231
<i>Telnet Viewer Window Features</i>	232
<i>Telnet Viewer window toolbar</i>	233
<i>Security Property</i>	234
<i>Opening a Session</i>	235
<i>Customizing the Telnet Viewer</i>	235
<i>Customizing Session Properties</i>	236
<i>Login scripts</i>	239
<i>Reviewing Session Data</i>	240
<i>Macros</i>	241
<i>Macro groups</i>	243
<i>Logging</i>	245
<i>Copying, Pasting and Printing Session Data</i>	248
<i>Power Control of Devices Attached to Power Devices</i>	249
<i>Closing a Telnet Viewer Session</i>	250
Using Tools	251
<i>Using Unit Tools</i>	251
<i>Exporting units</i>	251
<i>Exporting access rights</i>	253
<i>Importing data</i>	254
<i>Using the Managed Appliance Tools</i>	255
<i>Rebooting</i>	255
<i>Upgrading firmware</i>	256
<i>Resynchronizing units</i>	257
<i>Saving a managed appliance configuration</i>	258
<i>Restoring a managed appliance configuration</i>	259
<i>Saving a managed appliance user database</i>	259
<i>Restoring a managed appliance user database</i>	260
Using Tasks	261
<i>Using the Tasks Window</i>	261

<i>Adding tasks</i>	262
<i>Specifying when to run tasks</i>	262
<i>Adding Tasks Using the Add Task Wizard</i>	265
<i>Task: Backup Rack Power Manager software database and system files</i>	265
<i>Task: Configure SNMP trap settings on a managed appliance</i>	266
<i>Task: Exporting an event log .csv file</i>	267
<i>Task: Exporting an Asset Report to a .csv file</i>	269
<i>Task: Exporting a Usage Report to a .csv file</i>	270
<i>Task: Updating the firmware of an appliance type</i>	271
<i>Task: Validating user accounts on an external authentication server</i>	272
<i>Task: Pull names from selected units</i>	272
<i>Task: Update topology for selected units</i>	273
<i>Running tasks manually</i>	274
<i>Displaying task results</i>	275
<i>Deleting tasks</i>	275
<i>Changing tasks</i>	276
<i>Firmware Management</i>	276
Events and Event Logs	279
<i>Event Severity and Categories</i>	279
<i>Event severity</i>	279
<i>Event categories</i>	280
<i>Email Notifications</i>	280
<i>Enabling and Disabling Event Logging</i>	283
<i>Displaying the Event Log</i>	284
<i>Event states</i>	286
<i>Using the date filter</i>	287
<i>Changing the Event Log Retention Period</i>	287
<i>Creating an Event Log .csv File</i>	288
Plug-ins	291
<i>Recommended Sequence for Adding/Upgrading Plug-ins</i>	291

<i>Adding Plug-ins</i>	292
<i>Displaying Plug-in Information</i>	293
<i>Managing Plug-ins</i>	295
<i>Upgrading a plug-in</i>	295
<i>Disabling and activating a plug-in</i>	295
Appendix A: Technical Support	297
Appendix B: Terminal Emulation	298
Appendix C: Regaining Access to the Rack Power Manager Software	316

Product Overview

Rack Power Manager software is a stand-alone web browser-based, centralized Rack PDU Management solution. It provides all centralized management capabilities related to Rack PDU devices, ability to perform power control actions as well as run power consumption reports for outlets, PDU's, racks, rows etc. as well as for all custom groups of equipment.

NOTE: Unless otherwise specified, all references to DSView™ software refer to DSView software version 4 or higher.

System Components

The Rack Power Manager software system contains the following components.

Rack Power Manager management software

The Rack Power Manager software resides on the Rack Power Manager server (host or hub computer) and provides a web gateway and services for managing rack PDUs using a web browser.

Users may connect to the Rack Power Manager server from Rack Power Manager software clients and use the Rack Power Manager Explorer windows to communicate with the system.

Rack Power Manager server

The Rack Power Manager server contains the Rack Power Manager management software. The server provides a centralized database for storing configuration, user, unit and system information. It also provides services for authentication, access control, logging events, monitoring and license management.

You may configure one or more spoke (backup) servers in addition to the hub server. The hub server is responsible for maintaining the master copy of the database in a Rack Power Manager software system. Only one server in a Rack Power Manager software system may be configured as the hub server.

Spoke servers are primarily used for redundancy of all PDU management and to have improved scalability. They perform database replication with the hub server. The hub server acts as the coordinator for database replication between itself and all of the other spoke servers in a Rack Power Manager software system. A hub server and a spoke server both offer the same Rack Power Manager software functionality to a user. The distinction of hub or spoke refers only to the database replication role that the server plays and not with the functionality that the server provides. Adding one or more spoke servers to a Rack Power Manager software system provides redundancy and the ability to distribute Rack Power Manager software functionality across multiple sites. Power consumption data is not replicated to all spokes, however, when a report is created it spans across all servers to gather the data.

After the hub server and optional spoke server(s) are configured, you may create and configure the type of access levels for users within your network environment. You may also set up event logs to record full details of user access and other events.

Rack Power Manager software client

A Rack Power Manager software client is a computer with a web browser that can access the Rack Power Manager management software installed on the Rack Power Manager server.

Third party products

Third party products are not a part of the Rack Power Manager software, but are supported for use with it.

- External authentication servers - An external authentication server enables the Rack Power Manager server to broker authentication requests from users requesting access to the Rack Power Manager software system.
- SNMP managers - The SNMP (Simple Network Management Protocol) manager monitors the managed appliances and receives SNMP traps from the Rack Power Manager software on the server. An example of an SNMP manager is the HP OpenView product.
- Third party Telnet viewers - A third party Telnet viewer may be used for serial sessions instead of the Rack Power Manager software Telnet Viewer.

Supported Units

For management functions, the Rack Power Manager software client uses HTTPS (Hypertext Transfer Protocol with SSL encryption) to send a request to the Rack Power Manager server, which then sends a command to the managed appliance. The appliance then performs the requested function.

The Rack Power Manager software supports the managed appliances listed in this section. Other appliances may be supported by plug-ins; see the Avocent web site, www.avocent.com, for a list of plug-ins that may currently ship with the Rack Power Manager software and/or that can be added to the Rack Power Manager software. See *Plug-ins* on page 291 for information about adding and managing plug-ins in the Rack Power Manager software system.

Power devices

The Rack Power Manager software supports the following power devices:

- Avocent SPC power control devices
- Server Technologies Sentry Switched CDU CW-8H1, CW-8H2, CW-16V1, CW-16V2, CW-24V2, CW-24V3, CW-32VD1 and CW-32VD2 (supported models may change; contact Avocent Technical Support for current information)
- Cyclades™ Intelligent Power Distribution Unit (AlterPath™ manager)
- Avocent Power Management Distribution Unit (PM PDU) PM 1000/2000/3000 PDUs
- Liebert MPH/MPX units
- APC 78xx/79xx PDUs

All of the above power devices are supported on DSR™ KVM over IP switches that contain one or more SPC ports. Server Technologies power devices are also supported when connected through Avocent appliances.

Avocent models are supported when connected serially or through an Avocent appliance or directly over the network. Liebert and APC models are supported only when connected directly through the network.

CHAPTER

2

Installation

This chapter describes the installation sequence for the Rack Power Manager software:

- What you should do before installing the software
- How to install the software
- Configuring the software, plus considerations when upgrading
- Starting a client session

Final sections describe how to change your password, uninstall the software, end a Rack Power Manager software session and install Java.

About Installation

When the Rack Power Manager software is installed, the RPM software database is installed on the dedicated server.

Rebooting the dedicated server is not required prior to using the Rack Power Manager software.

Once the Rack Power Manager software is installed and you have configured the hub server, users may log in as a Rack Power Manager software client, using a supported web browser.

You may also install the Rack Power Manager software on additional computers and configure them as spoke servers. See *Spoke Servers* on page 74

NOTE: A license key permits the operation of the Rack Power Manager software on the dedicated server. The license key also specifies the number of clients that may use the software.

Minimum requirements for the Rack Power Manager software

Visit <http://www.avocent.com/software-requirements> for the minimum requirements for installing the Rack Power Manager software on a dedicated hub or spoke server.

NOTE: Rack Power Manager

Before installing and configuring the Rack Power Manager software

Before installing the Rack Power Manager software, install the managed appliance hardware.

If the computer will be a hub server, you will need the license key obtained from Emerson and provide a username and password to use for initial log in.

If the computer will be a spoke server, you will need to identify the associated hub server and provide the name/password of the hub server's Rack Power Manager software administrator.

Installing the Rack Power Manager Software

The Rack Power Manager software can be installed on a physical server or VM and the installation instructions described in this section apply to both scenarios. The Rack Power Manager management software may be installed using the Rack Power Manager software DVD or by downloading the software in a self-extracting .zip file from the Avocent web site.

To install the Rack Power Manager software:

1. Log on to the dedicated server as Administrator or root.
2. To install from a DVD:
 - a. Insert the Rack Power Manager software DVD. An autorun file opens a menu of installation options.
 - b. Click *Install Rack Power Manager Software*.

-or-

For Windows, if autorun is not enabled, type **<drive:>\RPM\win32\setup.exe**, where **<drive:>** is the letter of your DVD drive.

A dialog box will indicate that the server will be verified to ensure it meets the minimum requirements for installing the Rack Power Manager software.

For Linux, issue the following command to mount the DVD volume: **mount <device> <mount point>**, where **<device>** and **<mount point>** are the names of your server's DVD Linux device and mount point directory, respectively.

For example, to mount the first IDE cdrom on /media/cdrom, enter the command: **mount /dev/cdrom /media/cdrom**

3. To install from a downloaded file:
 - a. Using your web browser, download the Rack Power Manager software from the Avocent web site. Go to www.avocent.com and click the *Support* link. On the Technical Support page, click the *Product Upgrades* link, then select *RPM Software Upgrades*.

- b. Double-click on the downloaded installation package (setup.exe). A dialog box will indicate that the server will be verified to ensure it meets the minimum requirements for installing the Rack Power Manager software.
- c. For Linux, enter the following command to access the readme file: **less /<mount point>/RPM/readme**. For example, the following command accesses the readme file on the /media/cdrom mount point.

less /media/cdrom/Rack Power Manager/readme

4. If the current version of the Rack Power Manager software is already installed, the Installed Product Found: Same Version message box will appear. Click *OK* to reinstall the Rack Power Manager software or *Cancel* to exit setup.
5. The Check for an UPDATED version window will open. (If the Rack Power Manager software is already installed on the dedicated server, a message box will display. Click *OK* to close the box.)
 - a. Click *Next* to reinstall the software, or click *Cancel* to stop the reinstallation.
 - b. Click *Check for UPDATES* and then click *Next* to check the Avocent web site for the most recent Rack Power Manager software installation package. Go to step 5.

-or-

Click *Next* to install the DVD or downloaded version of the Rack Power Manager software. Go to step 6.
6. If a newer version of the Rack Power Manager software is found, an Update Available message appears.
 - a. Click *OK* to download the latest Rack Power Manager software installation package. The installation will be cancelled and the server's default web browser will launch and open in the Product Upgrades and Options page of the Avocent web site.

-or-

Click *Cancel* to resume installation of the older version of the Rack Power Manager software. Go to step 6.

 - b. Type your email address and password, and then click *Submit* to log in to the web site.
 - c. Download the Rack Power Manager software installation package, log out and close the web browser. Return to step 2.
7. The Introduction window will open. Follow the on screen instructions.
8. For a new database installation, click *Next* to install a new PostgreSQL database.
 - a. Choose a location to install the database.

- b. Enter the port number.
 - c. Enter the password.
 - d. Click Install.
9. For an existing database installation, click the checkbox to Use Existing Database.
10. Click Next.
 - a. Enter the database IP address, listening port number and the database username and password.
 - b. On the Installation Settings Confirmation screen, click Install.
11. The Installation Complete window will open.
 - To begin configuration of the Rack Power Manager software, click *Done*; see *Configuring the Rack Power Manager Software* on page 8. A Security Alert dialog box will appear containing certificate information and a warning that the generator of the certificate is not trusted. This occurs because the Rack Power Manager server certificate created when the server is installed is a self-signed certificate. You may either import the certificate into the Rack Power Manager software client web browser (choosing to trust the certificate) or obtain a server certificate from a Certificate Authority (CA) trusted by the web browser.
 - To configure the Rack Power Manager software at a later time, click *X* (Cancel) in the top right corner of the window.

Configuring the Rack Power Manager Software

After the Rack Power Manager software has been installed, it must be configured using a web browser.

During configuration, you specify whether the computer will be a hub server or a spoke server. If this is your first Rack Power Manager server installation, *hub* should be selected in the Select RPM Server Role window. The hub server should be installed before any spoke servers are added.

To configure the Rack Power Manager software:

1. If you are configuring the Rack Power Manager software during the installation process, you have already clicked *Done* in the Launch Default Browser window.

If you quit after installing the Rack Power Manager software installation process (by closing the window), select *Start - Programs - Emerson Rack Power Manager - RPM Software*.

2. A security alert box will appear containing certificate information. See *Certificates* on page 49.
3. The Select RPM Server Role window opens.
 - Click *Hub* to assign the dedicated server as the hub server, then click *Next*. Go to step 4.
 - Click *Spoke* to assign the dedicated server as a spoke server, then click *Next*. Go to step 8.
4. Follow the on screen instructions.
5. Click *Finish*.
6. The User Login window will open in the Rack Power Manager Explorer.

You may now log in using the username and password specified during configuration. If you chose to configure the server as a spoke server in the Select RPM Server Role window or if you entered a duplicate software license key in the Type in Master License Key window, continue with the following steps.
7. The Type in Hub Server Address and Port window will open. Type the address of the Rack Power Manager software hub server using standard dot notation (xxx.xxx.xxx.xxx) or type the DNS name in the Address field. Click *Next*.
8. The Accept Rack Power Manager Server Certificate window will open. Click *Next* to accept the certificate.
9. The Type in Hub Administrator Credentials window will open. Type a valid username and password for a user with Rack Power Manager software administrator privileges on the Rack Power Manager software hub server. Click *Next*.
10. The Registering Spoke Server window will open with the message *Request In Progress Please Wait*. The configuration of the spoke server will be saved to the database of the hub server and the spoke server's certificates will be installed on the hub server.
11. The Completed Successful window will open when the spoke server has been added. Click *Finish*.

Running the Rack Power Manager Software

Rack Power Manager software clients access the Rack Power Manager software host using a supported web browser. Any software required by the client, such as applets and the Java Runtime Environment (JRE), will be automatically installed by the Rack Power Manager server host.

The Rack Power Manager software uses Secure Sockets Layers (SSL) encryption to send data between the Rack Power Manager software host and the web browser on the client to ensure data integrity and privacy. When a user attempts to log in to a Rack Power Manager software client session, the authentication service configured in the Rack Power Manager software by the Rack Power Manager software administrator verifies the credentials of the user. Security alerts related to the certificates on the Rack Power Manager software host may appear. See *Certificates* on page 49.

Minimum client requirements

Visit <http://www.avocent.com/software-requirements> for minimum client requirements.

Opening a client session

Before opening a client session

- Enable cookies and JavaScript on the client's web browser.
- Configure the web browser. If you are using Internet Explorer, see *Internet Explorer Considerations* on page 45.

To open a client session:

NOTE: If Rack Power Manager Software Client Certificate Authentication or Rack Power Manager Software Client Integrated Windows Authentication is being used, the user will not be required to log in. See *Certificates* on page 49.

1. From the Rack Power Manager software client web browser, enter the URL of the server host in the address bar in the format:

https://<servername>/RPM

In this case, <servername> is the DNS name of the host system, or the IP address in standard dot notation (xxx.xxx.xxx.xxx).

NOTE: To avoid multiple security warnings, enter the DNS name.

-or-

If you are opening the session on the Rack Power Manager server, you may select *Start - Programs - Emerson Rack Power Manager - RPM Software*.

2. Accept all security alerts that may appear as the client computer connects to the Rack Power Manager server. The Rack Power Manager Explorer User Login window will open.

If an RSA SecurID external authentication service has been added to the Rack Power Manager software, see *RSA SecurID login* on page 11 below for the login procedure.

3. Type a valid username and password in the fields provided.

Depending on the settings specified by the administrator, you may be required to change your password before being allowed to complete the login process. See *Adding User Accounts* on page 211.

4. Click *Login*. The window that appears depends on the rights assigned to the Rack Power Manager user that is logging in.

If the client machine uses an onboard video controller and experiences video problems, be sure the BIOS is updated to the latest version.

RSA SecurID login

When an RSA SecurID external authentication service has been added to the Rack Power Manager software, the login credentials include a username and a passcode. The passcode includes a PIN and an RSA SecurID tokencode. The login request is sent to the RSA Authentication Manager. Depending on the user configuration and state on the RSA Authentication Manager, the user may be prompted for a second successive tokencode.

The user configuration also specifies how the four to six digit PIN will be generated:

- User defined - the user must enter a PIN
- System generated - the user cannot enter a PIN; it must be generated by the RSA server
- User selectable - the user may choose to enter a PIN or allow the RSA server to generate it

If a PIN has not yet been assigned to the user or if security policy requires a PIN change, the user will be prompted accordingly. If the RSA server generates the PIN, the user will be given a brief interval to memorize it.

Uninstalling the Rack Power Manager Software

To uninstall the Rack Power Manager software on a supported Windows system:

1. Select *Start - Settings - Control Panel*. The Control Panel will appear.
2. From the Control Panel, click *Add/Remove Programs*. The Add/Remove Programs dialog box will appear.
3. Select *Emerson Rack Power Manager* and then click *Change/Remove*. The Uninstall Avocent RPM window will open.
4. Click *Uninstall*.

To uninstall the Rack Power Manager software on a supported Linux system:

1. Log in to the server as root.

2. Insert the Rack Power Manager software DVD into your DVD drive. If AutoMount is supported and enabled, open a command window and continue with step 3.

-or-

If your system does not support AutoMount, issue the following command to mount the DVD volume: **mount <device> <mount point>**, where <device> and <mount point> are the names of your server's DVD Linux device and mount point directory, respectively.

For example, to mount a DVD which is the second IDE unit on /media/cdrom, enter the command:

mount /dev/cdrom /media/cdrom

3. Enter the following command to access the readme file.

less /media/cdrom/RPM/readme

Follow the instructions in the readme file.

To close a Rack Power Manager software session:

From the Rack Power Manager Explorer, click *LOGOUT* or the logout icon.

Java Installation

On non-Windows clients, Telnet requires Java version 1.5. The Telnet/SSH applet may work with other versions.

On Windows clients, Java is required to run the Emerson Telnet/SSH Viewer. If the Win32 PuTTY Telnet/SSH Viewer is selected in the user's profile, then Java is not required on the client. On a Windows client, it is recommended that the JRE (Java Runtime Environment) be installed in the C:\Program Files\ location.

To configure Java to find the JRE:

1. Access the Java Control Panel.
2. Select the *Java* tab.
3. In the Java Application Runtime Settings panel, click *View*.
4. Change the path to the installed JRE.
5. Click *OK*.

For Windows and Linux operating systems, the Rack Power Manager software client automatically downloads and installs the JRE the first time it is needed. For Macintosh

operating systems, you must update Java and install the JRE using the Macintosh software updates. Refer to the Macintosh operating system documentation for more information.

To install the JRE on a Windows client:

1. In a Rack Power Manager software Units View window (see *Accessing Units View windows* on page 111), click an Action link.
2. A window will open, containing a link for downloading the JRE installer. Download the JRE installer, then close all browser windows.
3. Click on the JRE icon to launch the installer.
4. Restart the browser, and click an Action link.

To install the JRE on a Linux client:

NOTE: Only one version of the JRE can be installed in the browser for Rack Power Manager software support. Depending on your system's configuration, you may have to log in as the root user to install the JRE. Contact your system administrator if you need help with installing software as the root user.

1. In a Rack Power Manager software Units View window (see *Accessing Units View windows* on page 111), click an Action link.
2. A window will open, containing a link for downloading the JRE installer. Download the JRE installer, then close all browser windows.
3. Run the installer.
4. Restart the browser, and click an Action link.

Transition

This chapter describes the steps for transitioning to Rack Power Manager software.

- Transitioning from DSView 3 management software and DSView 3 Power Manager Plug-in to Rack Power Manager software
- Transitioning from DSView software version 4 or higher to the Rack Power Manager software

DSView™ 3 Software and Power Manager Plug-in to RPM software

NOTE: In this document, DSView 3 software refers to DSView software versions 3.7.2.x or 3.7.3.x.

NOTE: In order to safely upgrade to the RPM software, and to provide a roll-back path in case of upgrade failures, perform each of the following steps. If your DSView 3 configuration does not include spoke servers, skip the steps that refer to spoke servers.

Before you begin, ensure that you budget sufficient time to transition the hub and spoke servers concurrently.

Data Replication

Perform a replication of all DSView 3 software spoke servers. In order to ensure that the entire system has fully replicated, run the replication task twice to ensure that all spokes are in sync with the hub server.

To initiate an immediate replication on a spoke server:

1. On the spoke server, click the *System* tab.
2. Click *Tasks* in the top navigation bar. The Tasks window will open.
3. Check the checkbox to the left of the Database Replication task and then click *Run Now*.

Back up the DSView 3 Software

Using the DSView 3 software backup and restore utility or the command line, back up the hub and each spoke server. The backup includes the database, plug-ins, firmware, appliance templates and system properties. You may manually create a backup of your hub server. Two methods are available:

- From a command line in an MS-DOS window. This method may be used for DSView 3 software hub servers on supported Windows® systems.
- Use the Backup and Restore system task located in the DSView 3 software WebUI. The backup is saved as a .zip file containing the files needed to restore the DSView 3 management software. This method may be used for DSView 3 software hub servers on supported Windows® systems only.

Client sessions will be temporarily disconnected during a manual backup. The sessions will be automatically reconnected when the backup is completed.

Manual backup and restore procedures require DSView 3 software administrator privileges.

To manually back up a hub server using a command line on a supported Windows system:

1. In the Start menu on your desktop, select *Start - Programs - Accessories - Command Prompt*. A command prompt window will open.
2. Change directories to the directory in which the DSView 3 software is installed (typically C:\Program Files\Avocent DSView 3\bin).
3. Enter **DSViewBackupRestore** to display the DSView 3 Backup and Restore Utility dialog box.
4. To back up the DSView 3 software hub server, enter **DSViewBackupRestore -backup -archive "<archive name>" -passwd <password>**.

For example, entering the following in a command prompt window will create a backup named db.zip with the password test.

DSViewBackupRestore.exe -backup -archive "db.zip" -passwd test

To manually back up a hub server using a command line on a supported Linux system:

1. Access the command prompt on your system.
2. Change directories to the directory where the DSView 3 software is installed, which is typically /usr/local/dsviewserver/bin.

3. To backup the DSView 3 software hub server, enter **DSViewBackupRestore.sh -backup -archive <archive name> -passwd <password> -overwrite**.

For example, entering the following in a command prompt window will create a backup named dbasebackup.zip with the password test1.

DSViewBackupRestore.sh backup -archive dbasebackup.zip -passwd test1

To manually back up a hub server using the Backup and Restore Utility dialog box on a supported Windows system:

1. In the Start menu on your desktop, select *Start - Programs - Avocent DSView 3- Backup and Restore Utility*. The DSView 3 Backup/Restore Utility dialog box will appear.
2. Click *Backup Database to a file*.
3. To password-protect the backup file, click *Enabled* and type a password in the Password field.
4. Click *Browse* and use the Save As dialog box to specify a directory and name for the backup file. Click *Save* when you are finished.
5. Click *Backup*. The DSView 3 software system backup files are saved.
6. Click *Close* to close the DSView 3 Backup/Restore Utility dialog box.

Backup the Power Management database

This task creates a folder containing a backup of the Power Manager database. The backup folder is named dsviewPluginBackup;<SYSTEM NAME> by default, but you may also append the date and time to the end of the backup folder. Run this task on each of the hub and spoke servers.

To configure the PMP backup:

1. Click the *System* tab.
2. Click *Tasks* in the top navigation bar. The Tasks window will open.
3. Click *Add*. The Add Task Wizard will appear.
4. Select *Backup Power Manager database* from the drop-down menu. Type a 1-64 character name for the task.
5. Select a time to run the task, then click *Next*.
6. The Specify Power Manager Database Backup Properties window will open.
 - a. Type the directory location in which to create the backup file, which may be a physical local drive on the DSView 3 server or a shared network location specified by

a UNC (Universal Naming Convention) path. The Location field cannot be set to a mapped network drive. The directory name must be entered in case sensitive text if your operating system supports case sensitive filenames.

- b. If the specified directory location is a network path that requires a login, enable the *Login required to access shared drive location* checkbox. Then type the username and password and confirm the password of a user account that has read/write access to the network share location.
- c. To append the date and time (in military time) to the end of the system backup folder, enable the *Use date and time for folder naming* checkbox. For example, if you are creating the backup folder on October 1, 2005 at 10:04 pm, the folder created will be named dsviewBackup1001052204;<Machine Name>.

If a backup folder already exists in the specified directory and the *Use date and time for folder naming* option is not enabled, the existing backup folder will be overwritten when the new backup folder is created.

7. Click *Finish*.
8. Navigate to the etc folder of this backup folder. Compress the etc folder into a zip file manually. Use the zip of etc folder in all subsequent steps that require the backup of a Power Management database.

Install Rack Power Manager Hub Server

To Install RPM Software:

1. Download the latest version of RPM software to the server.
2. Run the installation file.
3. Click *Next* to continue with the installation.
4. Accept the terms of the License Agreement, click *Next*.
5. Click *Next* on the Installation Settings screen.
6. Choose the RPM software installation location and click *Next*.
7. Review the default RPM software TCP Port Settings tab, make any changes needed and click *Next*.
8. On the PostgreSQL Installation screen, check the box to Use Existing Database if connecting to an existing and click *Next*.

-or-

Click *Next* to install a new instance.

9. For an existing PostgreSQL server, enter the IP address, port, username and password and click *Next*.

-or-

For a new instance, enter the install folder, port, and password and click *Next*. Click *Install* on the confirmation screen.

10. Click *Ok* on the Service Startup message.
11. Click *Done*.

Migration Utility

Exporting the Data

The DSView data migration utility was installed with the RPM software. It will allow you to convert from the embedded DSView PMP database to PostgreSQL data format.

To export the DSView 3 backup data into PostgreSQL format from a Windows operating system:

1. To launch the migration utility, from the Windows server, click *Start - All Programs - Emerson - RPM1.0 - DSViewDataMigrationUtility*.
2. On the Export tab, select the Server Type from the drop-down menu.
 - a. Choose *Hub*, if you are exporting data from the hub.
 - b. Choose *Spoke* if you are exporting data from the spoke.
3. Select *DSView* for the Database Type from the drop-down menu when you are specifying a DSView Software backup.

-or-

Select *PMP* for the Database Type from the drop-down menu when you are specifying backup of the Power Management database. If you have both DSView Software backup and Power Management database backup, you will have to run the utility twice to select both the options.

4. In the field Data Backup File Path, enter the path or browse to the location of the DSView Software backup or PMP database backup file. If using a PMP database backup file, this is the zip file of the etc folder that was created previously.
5. In the Migration File Path field, enter or browse to the location that you will save the exported file.
6. Click on *Export*.

To export the DSView 3 software data from a Linux® operating system:

1. Navigate to the DSViewDataMigrationUtility folder, By default this folder is located at /usr/local/Emerson/RackPowerManager/DSViewDataMigrationUtility. To launch the migration utility, enter **./DataMig.sh** from the command line.
2. Choose option number two to export the data.
3. From the menu, enter the server type.
 - a. Choose *Hub*, if you are exporting data from the hub.
 - b. Choose *Spoke* if you are exporting data from the spoke.
4. Select *DSView* for the Database Type when you are specifying a DSView software backup.
-or-
Select *PMP* for the Database Type when you are specifying backup of the Power Management database. If you have both DSView software backup and Power Management database backup, you will have to run the utility twice to select both the options.
5. Input the location of the DSView Software backup or PMP database backup file. If using a PMP database backup file, this is the zip file of the etc folder that was created previously.
6. Input the location to save the Migration File.
7. Verify the settings and enter **Y** to continue with the export.

Importing the Data

The RPM data migration utility migrates the exported data you get from the previous steps into the RPM database.

To Import DSView or DSView + PMP database from a Windows Operating System:

1. To launch the migration utility, from the Windows server, click *Start - All Programs - Emerson - RPM1.0 - RPMDDataMigrationUtility*.
2. Click *Next* to continue.
3. Select *DSView3+PMP to RPM 1.0* and click *Next*.
4. Enter the server IP address of the RPM software hub server.
5. Enter the listening port for your hub database server in the DB Server Port field.
6. Enter the database username in the Username field.
7. Enter the password for the database in the Password field.

8. Enter the database name in the DB Name field.
9. Click *Next*.
10. In the DSView Hub Database field, enter or browse to the location that you saved the DSView 3 software export file.
11. In the PMP Database field, enter the path or browse to the location of the exported PMP database file.
12. Click *Next*.
13. Assign the data from servers on your DSView System to your RPM System and click *Next*.
14. Confirm the server assignments and click *Next*.
15. In case you have assigned data to RPM spoke server, you will be prompted for the DB server port, user name and password of the spoke DB server. Enter these details and click *Next*.
16. Click *Finish*.

To Import PMP Database from a Linux Operating System:

1. Navigate to the RPMDDataMigrationUtility folder. By default this folder is located at /usr/local/Emerson/RackPowerManager/RPMDDataMigrationUtility. To launch the migration utility, enter **.DBMigration.sh** from the command line.
2. Click *Next* to continue.
3. Select *DSView3+PMP to RPM 1.0* and click *Next*.
4. Enter the server IP address of the RPM software hub server.
5. Enter the listening port for your hub database server in the DB Server Port field.
6. Enter the database username in the Username field.
7. Enter the password for the database in the Password field.
8. Enter the database name in the DB Name field.
9. Click *Next*.
10. In the DSView Hub Database field, enter or browse to the location that you saved the DSView 3 software export file.
11. In the PMP Database field, enter the path or browse to the location of the exported PMP database file.
12. Click *Next*.

13. Assign the data from servers on your DSView System to your RPM System and click *Next*.
14. Confirm the server assignments and click *Next*.
15. In case you have assigned data to RPM spoke server, you will be prompted for the DB server port, user name and password of the spoke DB server. Enter these details and click *Next*.
16. Click *Finish*.

Configure RPM Hub and Spoke servers

To configure the hub server:

1. Stop the RPM service on the hub server.
2. Copy the backed up firmware, appliance templates and system properties over to the corresponding folders on the hub server.
3. Restart the hub server.

To configure the spoke server(s):

1. Stop the RPM service on the spoke service.
2. Copy the backed up firmware, appliance templates and system properties over to the corresponding folders on the spoke server.
3. Restart the spoke server.
4. Run data replication on each spoke server.

DSView software to RPM software

The section describes how to transition to RPM software from DSView software version 4 or higher. Before you begin, ensure that you budget sufficient time to transition the hub and spoke servers concurrently.

Data Replication

Perform a replication of all DSView software spoke servers. In order to ensure that the entire system has fully replicated, run the replication task twice to ensure that all spokes are in sync with the hub server.

To initiate an immediate replication on a spoke server:

1. On the spoke server, click the *System* tab.
2. Click *Tasks* in the top navigation bar. The Tasks window will open.

3. Check the checkbox to the left of the Database Replication task and then click *Run Now*.

Back up the DSView Software

Using the DSView software backup and restore utility or the command line, back up the hub and each spoke server. The backup includes the database, plug-ins, appliance templates and system properties. You may manually create a backup of your hub server. Two methods are available:

- From a command line in an MS-DOS window. This method may be used for DSView software hub servers on supported Windows® systems.
- Use the Backup and Restore system task located in the DSView software WebUI. The backup is saved as a .zip file containing the files needed to restore the DSView software. This method may be used for DSView software hub servers on supported Windows® systems only.

Client sessions will be temporarily disconnected during a manual backup. The sessions will be automatically reconnected when the backup is completed.

Manual backup and restore procedures require DSView software administrator privileges.

To manually back up a hub server using a command line on a supported Linux system:

1. Access the command prompt on your system.
2. Change directories to the directory where the DSView software is installed, which is typically `/usr/local/dsviewserver/bin`.
3. To backup the DSView software hub server, enter **DSViewBackupRestore.sh -backup -archive <archive name> -passwd <password> -overwrite**.

For example, entering the following in a command prompt window will create a backup named `dbasebackup.zip` with the password `test1`.

```
DSViewBackupRestore.sh backup -archive dbasebackup.zip -passwd test1
```

To manually back up a hub server using the Backup and Restore Utility dialog box on a supported Windows system:

1. In the Start menu on your desktop, select *Start - Programs - Avocent DSView - Backup and Restore Utility*. The DSView Backup/Restore Utility dialog box will appear.
2. Click *Backup Database to a file*.
3. To password-protect the backup file, click *Enabled* and type a password in the Password field.

4. Click *Browse* and use the Save As dialog box to specify a directory and name for the backup file. Click *Save* when you are finished.
5. Click *Backup*. The DSView software system backup files are saved.
6. Click *Close* to close the DSView Backup/Restore Utility dialog box.

Extract the PostgreSQL data file

To extract PostgreSQL data file:

1. Decompress the backup file previously generated.
2. Navigate to the bin folder and copy the postgresbackup.tar file to another location. This file will have to be used as input to import the data to the Rack Power Manager software.

Install Rack Power Manager Hub Server

To Install RPM Software:

1. Download the latest version of RPM software to the server.
 2. Run the installation file.
 3. Click *Next* to continue with the installation.
 4. Accept the terms of the License Agreement, click *Next*.
 5. Click *Next* on the Installation Settings screen.
 6. Choose the RPM software installation location and click *Next*.
 7. Review the default RPM software TCP Port Settings tab, make any changes needed and click *Next*.
 8. On the PostgreSQL Installation screen, check the box to Use Existing Database if connecting to an existing and click *Next*.
- or-**
- Click *Next* to install a new instance.
9. For an existing PostgreSQL server, enter the IP address, port, username and password and click *Next*.
- or-**
- For a new instance, enter the install folder, port, and password and click *Next*. Click *Install* on the confirmation screen.
10. Click *Ok* on the Service Startup message.
 11. Click *Done*.

Importing the Data

To Import DSView database from a Windows Operating System:

1. To launch the migration utility, from the Windows server, click *Start - All Programs - Emerson - RPM1.0 - RPMDDataMigrationUtility*.
2. Click *Next* to continue.
3. Select DSView4 to RPM 1.0 and click *Next*.
4. Enter the server IP address of the RPM software hub server.
5. Enter the listening port for your hub server in the DB Server Port field.
6. Enter the database name in the DB Name field.
7. Enter the database username in the Username field.
8. Enter the password for the database in the Password field.
9. Browse or enter the location of the DSView4 Database in the DSView4 DB field. This is the postgresbackup.tar file that was extracted from the DSView4 backup
10. Click *Next*.
11. Assign the servers for migration and click *Next*.
12. Confirm the server assignments and click *Next*.
13. Click *Finish*.

To Import DSView Database from a Linux Operating System:

1. Navigate to the RPMDDataMigrationUtility folder. By default, this folder is located at `/usr/local/Emerson/RackPowerManager/RPMDDataMigrationUtility`. To launch the migration utility, enter **`.DBMigration.sh`** from the command line.
2. Click *Next* to continue.
3. Select DSView4 to RPM 1.0 and click *Next*.
4. Enter the server IP address of the RPM software hub server.
5. Enter the listening port for your hub server in the DB Server Port field.
6. Enter the database name in the DB Name field.
7. Enter the database username in the Username field.
8. Enter the password for the database in the Password field.

9. Browse or enter the location of the DSView4 Database in the DSView4 DB field. This is the postgresbackup.tar file that was extracted from the DSView4 backup
10. Click *Next*.
11. Assign the servers for migration and click *Next*.
12. Confirm the server assignments and click *Next*.
13. Click *Finish*.

Configure RPM Hub and Spoke server

To configure the hub server:

1. Stop the RPM service on the hub server.
2. Copy the backed up firmware, appliance templates and system properties over to the corresponding folders on the hub server.
3. Restart the hub server.

To configure the spoke server(s):

1. Stop the RPM service on the spoke service.
2. Copy the backed up firmware, appliance templates and system properties over to the corresponding folders on the spoke server.
3. Restart the spoke server.
4. Run data replication on each spoke server.

CHAPTER

4

Rack Power Manager Explorer Windows

When a user is logged in and authenticated, the Emerson Rack Power Manager Explorer window opens. From the Rack Power Manager Explorer window, you may view, access and manage units.

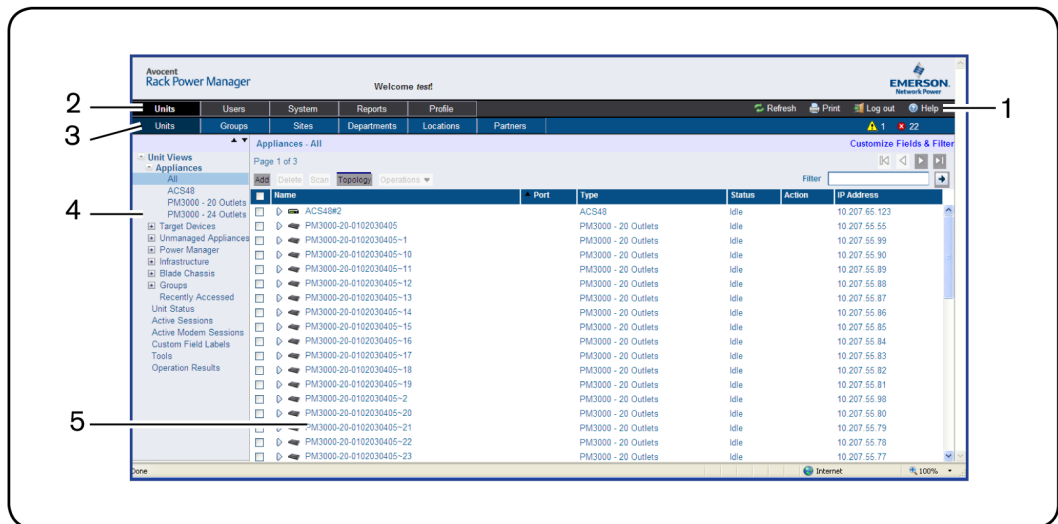


Figure 4.1: Example EmersonRack Power Manager Explorer Window Areas

Table 4.1: Rack Power Manager Explorer Window Area Descriptions

Number	Description
1	Top option bar - Use the top option bar to bookmark a Rack Power Manager software window, refresh a window display, print a page, log out of a software session or access online help. The name of the logged in user appears on the left side of the top option bar.
2	Tab bar - Use the tab bar to display and manage units, user accounts, reports, system settings and session profiles.
3	Top navigation bar - The selections in the top navigation bar vary, depending on the active tab in the tab bar. Topics relevant to each selection display in the side navigation bar.
4	Side navigation bar - Use the side navigation bar to select system information to display or edit in the content area. The side navigation bar contains arrows that affect its display.
5	Content area - The information specified by the tab bar, top navigation bar and side navigation bar selections is displayed and changed in the content area.

Using the Side Navigation Bar

The side navigation bar is used to display windows that specify settings or perform operations. The contents of the side navigation bar varies, depending on the tab and top navigation bar selections and the window that is displayed.

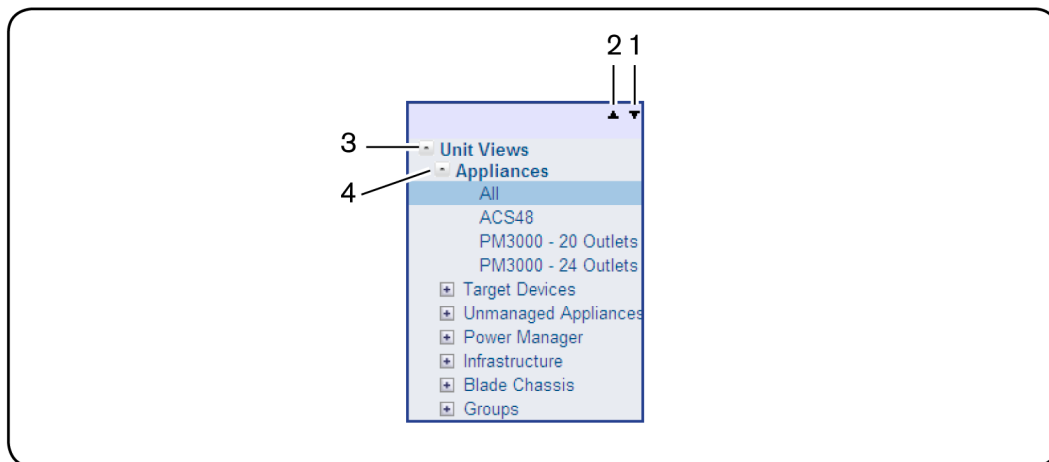


Figure 4.2: Example Side Navigation Bar

Table 4.2: Side Navigation Bar Descriptions

Number	Description
1	Expand All Nodes - Click this arrow in the upper right corner to expand all nodes and display additional links.
2	Collapse All Nodes - Click this arrow in the upper right corner to collapse all nodes and their links.
3	Collapse Node - Click this arrow to collapse an opened tree branch and its links.
4	Expand Node - Click this arrow to expand a closed tree branch and display its links.

You may choose whether an expanded node will collapse when another Expand Node arrow is selected. See *Changing user options* on page 39.

Using Windows

Sorting information in a window

The order of rows in a list may be changed by clicking the heading of one of the displayed columns. When you click a column heading, the order of the list rows will change to alphabetically ascending, based on that column. If you click the column heading a second time, the order will change to an alphabetically descending order.

If you are using the topology feature in a Units View window, see *Topology view* on page 110 for sorting criteria.

Filtering information in a window

Some Rack Power Manager software windows allow you to filter list information by providing a text string that will be used to retrieve matching items.

When filtering, you may use an asterisk (*) before and/or after text strings as a wildcard. For example, typing **emailserver*** and clicking *Filter* will display items with emailserver at the beginning (such as emailserver, emailserverbackup). Typing ***emailserver*** and clicking *Filter* will display items containing emailserver in any part of the name (such as emailserver, emailserverstore, tdemailserver, tdemailserver1).

Table 4.3 lists the ways you may specify text strings for filtering.

Table 4.3: Filter Text Strings

Typed in the Filter Field	Results
<String>	Entering a string displays a filtered list of items that contain the 'word' (that is, it will find matching strings that are followed by anything other than a letter or number). For example, typing email will list any items that contain the string email, followed by a space or punctuation mark. If you enter multiple words separated by spaces but without logical operators, OR is assumed, and each word is treated separately. For example, typing email server will display items containing email or server.
"<String>"	Surrounding the string with quotation marks displays a filtered list of items containing the exact string, including spacing and punctuation. For example, typing "email server" will display items that contain email server. The Rack Power Manager software will provide a closing quotation mark if it is omitted.
<String1> AND <String2>	Using the AND logical operator displays the items that contain both strings. For example, typing email and server will display items named email-server-3, email-server-2, server email and so on.
<String1> OR <String2>	Using the OR logical operator displays the items that contain at least one of the strings. For example, typing email or server will find any items that contain the string email or the string server.
(<String>)	Parentheses may be used to override the default (left to right) order of precedence during evaluation of a filter string. For example, searching for email and server or service would be the equivalent of ((email and server) or service), which may not be the intended search. The user may choose instead to change the order of precedence by grouping the search terms with parentheses, such as (email) and (server or service) .
NOT <String>	Preceding the string with NOT displays all items that do not contain the string. For example, typing not email will display all items except those containing email (email, email server, email-server-1 and so on will not display).

Using the Customize link in windows

Windows that contain a *Customize* or *Customize Fields and Filter* link allow you to change the following information:

- The number of items displayed per page in the window
- Which columns of information are displayed in Units View windows
- Which columns are included in a filter from a Units View window (available from the Customize Fields and Filter link only)

By clicking the *Customize* link, you can also show units that have been hidden in a Units View window.

NOTE: If you are in a Units View window, the link is displayed as “Custom Fields and Filter” and this window contains additional filtering options. On any other window, the link is displayed as “Customize”. The term “Customize link” is used throughout this document to refer to both links.

The items available for customizing and methods for changing them will vary, depending on the window being customized. Although the items that appear in windows may vary, the items that do appear are modified identically regardless of the window in which you clicked the *Customize* link.

To customize a window using the Customize link:

1. In a window containing a Customize link in the upper right corner, click the link. A View Customization window will open.
2. Add, remove or move fields in the window display:
 - To add one or more fields to the window display, select the fields in the Available Fields list, then click *Add*. The fields will be moved to the Fields to Show list.
 - To remove one or more fields from the window display, select the fields in the Fields to Show list, then click *Remove*. The fields will be moved to the Available Fields list.
 - To change the order that fields display from left to right in the window, select one or more fields in the Fields to Show list. Use the up or down arrow to change its order in the list.
3. To specify the number of items that appear in a window, use the arrow keys in the Items per Page field to select a number or type a number (1-2000). In Units View windows that have the topology view enabled, the number of items per page includes children, even if the display is collapsed and the children are not visible.
4. To show hidden items in a Units View window (see *Showing and hiding units* on page 112).
 - a. Check the *Show hidden items* checkbox.
 - b. Select *Visibility* from the Available Fields column, and then click *Add*. Visibility will move to the Fields to Show list.
5. To show group descendants in windows that display unit groups (see *Unit group hierarchy* on page 185), click the *Show group descendants* checkbox.
6. To expand a topology view automatically in a Units View window (see *Topology view* on page 110), click the *Expand view automatically* checkbox.

7. (Units View windows only) To specify which fields are included in a filter, select the field (s) from the Available Fields list and click the *Add* button. To remove fields from a filter, select the fields from the *Filter on these fields* list and click *Remove*.
8. To set the Fields to Show and List Items as the default, click *Set as Default*. This button will appear only if you are a Rack Power Manager software administrator. You will be prompted to confirm setting these values as the default. Confirm or cancel.
9. Click *Save* and then click *Finish*. The window being customized will open with the changes.

Displaying pages

Multiple page windows contain navigation buttons which may be used to quickly move among pages.

Table 4.4: Rack Power Manager Explorer Page Navigation Buttons

Button	Description
<	First Page - Navigates to the beginning of a list displayed in a window.
<<	Previous Page - Navigates to the previous page of a list displayed in a window.
>>	Next Page - Navigates to the next page of a list displayed in a window.
>	Last Page - Navigates to the end of a list displayed in a window.

Printing a window

All windows contain a print icon and text in the top option bar. When you print a window, all the information on the page is printed, not just the visible portion.

To print a window:

1. In the top option bar, click *PRINT* or the print icon. The Print dialog box will appear.
2. Specify options to use, then click *Print* to print the window and close the Print dialog box.

Refreshing a window

A window may be refreshed at any time by clicking *REFRESH* or the refresh icon in the top option bar.

By default, status information automatically refreshes every 30 seconds. This interval may be changed or disabled. See *Changing user options* on page 39.

Using keyboard commands

In addition to using a mouse, certain keyboard commands may be used to select and change items in windows.

Table 4.5: General Keyboard Commands

Key	Description
Tab	Transfers focus to the next control in the window, including the calendar
Shift-Tab	Transfers focus to the previous HTML control

Table 4.6 lists the keyboard commands that may be used when a calendar is enabled and has focus.

Table 4.6: Calendar Keyboard Commands

Key	Description
Enter or Space	Displays or closes the calendar.
Esc	Closes the calendar.
Page Up	Decrements the month by one month and selects the first day of the month.
Page Down	Increases the month by one month and selects the first day of the month.
Right Arrow	Increments the day by one day. If the last day of the month is selected and the Right Arrow key is pressed, the month is incremented to the next month.
Left Arrow	Decrements the day by one day. If the first day of the month is selected and the Left Arrow key is pressed, the month is decremented to the previous month.
Up Arrow	Decrements the weekday by one week. If the first weekday type of the month is selected and the Up Arrow key is pressed, the month is decremented to the previous month.
Down Arrow	Increments the weekday by one week. If the last weekday type of the month is selected and the Down Arrow key is pressed, the month is incremented to the next month.

Table 4.7 lists the keyboard commands that may be used when a spinner is enabled and has focus.

Table 4.7: Spinner Keyboard Commands

Key	Description
Up Arrow	Increments the spinner number by one
Down Arrow	Decrements the spinner number by one

Basic Operations

This chapter describes basic operations and settings, including global system properties, profiles, built-in user groups and preemption levels.

Rack Power Manager Help

The Rack Power Manager help is hosted on the Avocent web site. If you do not have continuous access to the Internet, you may wish to install the help on the local Rack Power Manager server.

NOTE: Help for Rack Power Manager software plug-ins is automatically installed on your local server and is not available from the Avocent web site.

Configuring the Rack Power Manager help location

Rack Power Manager administrators can change the Rack Power Manager help location at any time. Help is configured independently for each Rack Power Manager hub and spoke server.

To configure the Rack Power Manager help location:

1. Click the *System* tab, then click *Rack Power Manager Server*.
2. Click *Properties - Help Configuration* in the side navigation bar.
3. Specify the location of the help that will be accessed each time *Help - Rack Power Manager Management Software Help* is clicked.

Select *View help from the Avocent web site* to access the latest help for your Rack Power Manager software version from the Avocent web site (Internet connection required).

-or-

Select *View help from this Rack Power Manager server help location* to access the downloaded help from your local server. Complete the following procedure for *Installing Rack Power Manager help on a local server* on page 36.

4. Click *Save*.

NOTE: If your Rack Power Manager software version is several versions prior to the current version, the help may not be available on the Avocent web site. In this case, when you access the help from the web, you are prompted to save a .zip file of the help to the local device.

Installing Rack Power Manager help on a local server

You can automatically download the help from the Avocent web site using the Rack Power Manager software, or you can visit www.avocent.com/rpmhelp to browse for the appropriate version and save a .zip file of the help to local media.

To download or update Rack Power Manager help on the local server:

1. Click the *System* tab, then click *Rack Power Manager Server*.
2. Click *Properties - Help Configuration* in the side navigation bar.
3. Click the *Download Latest Help* button. The Rack Power Manager Help Download Wizard opens.
4. Select *From the Avocent web site* to download the latest help for your Rack Power Manager software version from the Avocent web site.

-or-
Select *From a local device* to retrieve the help from local media. To specify the location, click *Browse* or type the path in the field.
5. Click *Next*.
6. The Completed Successful window opens. Click *Finish*.

NOTE: If you reinstall or upgrade the Rack Power Manager software, the Rack Power Manager help location is reset to *From the Avocent web site*.

Global System Properties

Global system properties affect all Rack Power Manager servers in the system. That is, when global system properties are changed on a Rack Power Manager server, the next replication operation will apply those changes to all other Rack Power Manager servers in the system; see *Replication* on page 78.

Global system properties include:

- User credential properties - see *Specifying a user certificate* on page 41 and *Specifying an SSH key* on page 42
- Legal notice - see *Legal Notice* on page 37
- PCI Compliance - *PCI Compliance Configuration* on page 37

- Power settings - see *Power Settings* on page 38
- Automatic inheritance - see *Automatic Inheritance for Group Memberships and Properties* on page 131

Legal Notice

Administrators may enable or disable the display of a legal caption and disclaimer prior to users logging in to the Rack Power Manager software. When enabled, the legal disclaimer is displayed every time a user logs in.

The legal notice feature affects all Rack Power Manager servers in the system after replication; see *Replication* on page 78.

To enable or disable and configure the legal notice:

1. Click the *System* tab.
2. Click *Global Properties* in the top navigation bar.
3. Click *Legal Notice* in the side navigation bar. The Rack Power Manager System Logon Legal Notice window will open.
4. To enable the legal notice display:
 - a. Check the *Enable Legal Notice* checkbox.
 - b. Enter up to 80 characters in the Caption field. This is a required field.
 - c. Enter up to 512 characters in the Text field. Carriage returns may be used to separate lines. This is a required field.
 - d. Click *Save*.
5. To disable the legal notice display, uncheck the *Enable Legal Notice* checkbox and then click *Save*.

PCI Compliance Configuration

The Rack Power Manager software may be configured as Payment Card Industry (PCI) compliant. When PCI compliance is enabled, three settings are affected:

- Browser caching of secure web pages is disabled. This setting prevents the potential loss of confidential client data; however, this setting may not work effectively if older browsers are used.
- The browser prompt to save passwords is disabled. This setting prevents the potential loss of confidential client data.

- Weak SSL ciphers are disabled. This setting prevents the potential loss of data integrity.

NOTE: When PCI compliance is enabled, the exporting of the Rack Power Manager server CSR files, PEM certificates and SSH keys does not submit the request to the client's browser; instead the files are saved in the Rack Power Manager server user's home directory. The CSR filename is the name of the Rack Power Manager server with extension .p10, the PEM certificate filename is Rack Power Manager System Certificate.pem, and the SSH key filename is Rack Power Manager System Certificate.pub. For example, if the server is running on Windows XP and the name of the server is WinXPServer, the files are saved to [rootdrive]\Documents and Settings\[username]\ and the names are:

- CSR file = WinXPServer.p10
 - PEM certificate = Rack Power Manager System Certificate.pem
 - SSH key = Rack Power Manager System Certificate.pub
-

To enable PCI compliance:

1. Click the *System* tab.
2. Click *Global Properties* in the top navigation bar.
3. Click *PCI Compliance* in the side navigation bar. The PCI Compliance Properties window will open.
4. To enable PCI compliance, select *Make Rack Power Manager Server PCI Compliant*. Click *Save*.
5. Restart the Rack Power Manager server.
6. Run the MSI installer to push the Video Viewer files to the Internet Explorer clients accessing the Rack Power Manager software; follow the procedure in *Managing ActiveX® controls* on page 45.

NOTE: The PCI compliance setting is not replicated to other Rack Power Manager servers. You must configure PCI compliance settings individually for each server that you wish to be PCI compliant.

Power Settings

Configure the global power settings properties to specify how long the Rack Power Manager server will wait to receive a power operations response from a unit.

To configure power settings:

1. Click the *System* tab.
2. Click *Global Properties* in the top navigation bar.
3. Click *Power Settings* in the side navigation bar. The Power Settings Properties window will open.

4. Enter a number of seconds between 0 and 60 to specify the amount of time for the Rack Power Manager server to wait for power operations to complete. The preset value is 60 seconds.
5. Click *Save*.

Profiles

Profile information contains features and tasks that may affect actions when using the Rack Power Manager software. These include:

- User options
- Color scheme
- Changing a password
- Choice of serial session application
- Specifying a user certificate
- Specifying a user SSH key

Changing user options

To change user options:

1. Click the *Profile* tab. The Options window will open.
2. In the Navigation Tree Behavior area, select one option:
 - If you select *Automatically collapse navigation tree nodes*, a currently-expanded tree node will be collapsed when you select another tree node.
 - If you select *Preserve navigation tree state*, a currently-expanded tree node will remain expanded when you select another tree node.
 - If you select *Automatically fully expand navigation tree nodes*, all tree nodes will be expanded. This is equivalent to clicking the *Expand All Nodes* arrow in the side navigation bar; see *Using the Side Navigation Bar* on page 28.
3. Enable or disable prompts when leaving pages with unsaved changes:
 - Check *Skip prompt when leaving pages with unsaved changes*, if you do not want a message box to prompt you to save modified information when you leave a window.
 - Uncheck *Skip prompt when leaving pages with unsaved changes* if you want a message box to prompt you to save modified information when you leave a window.

4. Select a refresh rate or *Never*. By default, windows automatically refresh every 30 seconds. If you select *Never*, windows will only be refreshed when you click the *REFRESH* icon or text in the top option bar.
5. Click *Save*.

Changing the color scheme

When the color scheme is changed, it is changed only for the logged in user.

To change the color scheme:

1. Click the *Profile* tab.
2. Click *Preferences* in the top navigation bar.
3. Click *Color Scheme* in the side navigation bar. The Color Scheme window will open.
4. Click a color scheme to use. If the System Colors scheme is selected, the Rack Power Manager Explorer window will match the user's desktop color scheme.
5. Click *Save*. The color scheme will be applied to the Rack Power Manager Explorer window.

Changing your password

When the Rack Power Manager software internal authentication service is used, user accounts will indicate if users are allowed to change their password; see *User account restrictions and expiration settings* on page 217.

By default, passwords must contain at least three characters and will never expire. A different minimum character length and an expiration date may be configured; see *Rack Power Manager software internal authentication service* on page 82.

To change your password:

1. Click the *Profile* tab.
2. Click *Preferences* in the top navigation bar.
3. Click *Change Password* in the side navigation bar. The Change Password window will open.
4. Type your current password.
5. Type and confirm the new password.
6. Click *Save*.

Choosing the serial session application

You may specify the application to be used for serial sessions to Rack PDUs.

- Rack Power Manager software Telnet Viewer (Emerson Session Viewer)
- Win32 PuTTY Telnet/SSH application
- Third party application

NOTE: If you use a third party Telnet application, the first time you attempt to launch a session, you will be prompted to confirm the use of that application.

NOTE: Only the Rack Power Manager software Telnet Viewer is supported on Macintosh system clients.

To specify the serial session application:

1. Click the *Profile* tab.
2. Click *Applications* in the side navigation bar.
3. Check the checkbox for the application you want to use for serial sessions.
4. If you check *3rd Party Application*, enter the path and executable name of the application (maximum 256 characters) in the Serial Application field.

Specify any of the following parameters (up to 128 characters) in the Command Line Arguments field. When the serial session is launched, the actual values will be substituted.

%ADDRESS% - The IP address will be substituted.

%PORT% - The port number will be substituted.

%TNAME% - The target name will be substituted.

If the third party application does not automatically launch a command window, check the *Launch in Command Window* checkbox.

5. Click *Save*.

Specifying a user certificate

This property may be changed only for internal authentication users. See *Rack Power Manager software internal authentication service* on page 82.

A user may specify a certificate if the administrator has allowed it; see the procedure below. If the system certificate policy is enabled for user certificates (see *System certificate policy and trust store* on page 50), the user certificate used at login must meet the policy requirements.

As an alternative, the administrator may specify the certificate in the user account properties. See *User certificates* on page 216.

To enable user settable certificates:

NOTE: Only Rack Power Manager software administrators may access this procedure.

1. Check the *Allow user to set own certificate* checkbox.
2. Click *Save*.

To specify a user certificate:

NOTE: A user may access this procedure only if a Rack Power Manager software administrator has allowed it.

1. Click the *Profile* tab. Preferences will automatically be selected in the top navigation bar.
2. Click *Credentials* in the side navigation bar, then click *Certificate*.
3. Type the path and name of the certificate or browse to the certificate location.
4. Click *Save*. An updated Certificate window will open.

Specifying an SSH key

A user may specify an SSH key if the administrator has allowed it.

As an alternative to this method, the administrator may specify the SSH key in the user account properties. See *User SSH key* on page 216.

To enable user settable SSH keys:

NOTE: Only Rack Power Manager software administrators may access this procedure.

1. Click the *System* tab.
2. Click *Global Properties*.
3. Click *User Credential Properties* in the side navigation bar.
4. Check the *Allow user to set own SSH key* checkbox.
5. Click *Save*.

To specify an SSH key:

NOTE: A user may access this procedure only if a Rack Power Manager software administrator has enabled it.

1. Click the *Profile* tab. Preferences will automatically be selected in the top navigation bar.
2. Click *Credentials* in the side navigation bar, then select *SSH Key*.
3. Type the 1-256 character name of the file containing the public SSH key that was generated by a third party key generator or browse to the file location.

4. Click *Save*. An updated SSH Key window will open. The SSH key file will be uploaded to the Rack Power Manager server for use in authenticating the user.

Enabling user credential caching

User credential caching provides a single sign-on method for accessing units supported by certain plug-ins. If enabled, the credentials used to log in to the Rack Power Manager software are maintained in a secure internal cache. A supported plug-in, such as the Virtualization plug-in, can retrieve these credentials to log in to connected units.

To enable user credential caching:

NOTE: Only Rack Power Manager software administrators may access this procedure.

1. Click the *System* tab.
2. Click *User Credential Properties* in the side navigation bar.
3. Check the *Enable credential caching* checkbox.
4. Click *Save*.

Any currently logged in users must log out and log in again for their credentials to be cached.

Built-in User Groups

When a user account is added to the Rack Power Manager software system, the user may be assigned to any of the following built-in user groups:

- Rack Power Manager software administrators
- Appliance administrators
- User administrators
- Auditors
- Users

Table 5.1 lists the operations allowed for the built-in user groups.

Table 5.1: Built-In User Group Allowed Operations

Operation	Built-In User Group				
	Software Administrator	User Administrator	Appliance Administrator	Auditors	Users
Configure Rack Power Manager software system-level settings	Yes	No	No	No	No
Add, change, import and delete Rack Power Manager software	Yes	Yes	No	No	No
Backup and restore the Rack Power Manager software database	Yes	No	No	No	No
Register a spoke server	Yes	No	No	No	No
Add, change and delete units	Yes	No	Yes	No	No
Add, change and delete unit groups	Yes	Yes	Yes	No	No
Configure access rights	Yes	Yes	Yes	No	No
Add, change and delete sites, departments and locations	Yes	No	Yes	No	No
Add, change and delete external authentication services	Yes	Yes	No	No	No
Add, change, delete user accounts and user-defined user groups	Yes	Yes	No	No	No
All event-related operation	Yes	No	No	Yes	No
Change your own password	Yes	Yes	Yes	Yes	Yes

In addition to the built-in user groups, the Rack Power Manager software supports user-defined user groups; see *Grouping Units* on page 177.

Internet Explorer Considerations

When the Internet Explorer web browser is used, specific settings are required to enable the Rack Power Manager software to operate correctly.

- SSL (Secure Sockets Layer) certificates - Used for secure authentication between the Rack Power Manager software client and Rack Power Manager software hub server; see *Certificates* on page 49.
- ActiveX controls - Used to display Telnet application and serial sessions.
- Security Zones - Used to control the actions that may be performed within Internet Explorer. For example, the operation of JavaScript, which is used by the Rack Power Manager software, is dependent on security zone settings.
- Advanced Internet options - Used for miscellaneous settings that enhance the use of the Rack Power Manager software.

Managing ActiveX® controls

The Rack Power Manager software uses ActiveX controls to provide interactive content for viewers. (The Emerson Telnet Viewer uses Java; see *Java Installation* on page 12 for information.)

The functionality of the ActiveX controls is determined by the settings for the security zone being used by the Rack Power Manager software. See *Security zones* on page 46.

Administrators may prevent users from installing software on their computers. In this case, the Windows domain administrators may choose to “push” an MSI installer using a Group Policy. This will silently install the Avocent Session Viewers without requiring the user to install the software themselves. This will install only the viewers for Internet Explorer. The MSI file is located on the Rack Power Manager software DVD and in the webapp/applets directory on the Rack Power Manager server.

To download an ActiveX control on a Rack Power Manager software hub server using Windows (all operating systems except Windows XP with Service Pack 2):

1. In a Units View window that contains target devices (see *Accessing Units View windows* on page 111), click the link in the Action field or select an alternate action, if available.

You can also access a Unit Overview window for a target device and click the icon or link for the session type.

If this is the first time the ActiveX control has been requested by the Rack Power Manager software, an Avocent Session Viewer message box will appear, followed by a Security Warning dialog box.

2. Select *Always trust content from Avocent Huntsville Corporation*.
3. Click *Yes* to download the ActiveX control. When the control has been downloaded, a serial session will start in a Telnet Viewer window.

To download an ActiveX control on a Rack Power Manager software hub server using Windows XP with Service Pack 2:

1. In a Units View window that contains target devices (see *Accessing Units View windows* on page 111), click the link in the Action field or select an alternate action, if available.

You can also access a Unit Overview window for a target device and click the icon or link for the session type (see *Unit Overview Windows* on page 116).

If this is the first time the ActiveX control has been requested by the Rack Power Manager software, an Avocent Session Viewer message box will appear.

2. Click in the top yellow bar. A pop-up menu will appear. Click *Install*. A Security Warning dialog box will appear.
3. Click *Install* to install the ActiveX control.

Security zones

Internet Explorer restricts actions performed by the web browser, based on the security zone membership of the web site being accessed. Each security zone typically has its own security restrictions. The following four security zones are available in Internet Explorer:

- Trusted Sites - Web sites contained in the list of trusted sites.
- Restricted Sites - Web sites contained in the list of restricted sites.
- Local Intranet - Web sites accessed using a host name (for example, <https://sun-e2-callisto>).
- Internet - All other web sites, including those accessed using standard dot notation (for example, <https://10.0.0.1>).

By default, the Rack Power Manager software operates correctly in the Internet, Local Intranet and Trusted Sites security zones when accessing a hub server.

NOTE: A Rack Power Manager software hub server installed on a PC running the Windows 2003 Server will not operate correctly in the Internet security zone.

The current security zone appears in the lower right corner of the Rack Power Manager Explorer window.

To ensure that the Rack Power Manager software works correctly in security zones:

Specify settings for the Local Intranet and Internet security zones. When a Rack Power Manager software client accesses a hub server using a host name (for example, <https://avocent>), the Local Intranet security zone will be used. When a client accesses a hub server using a web address with periods (for example, <https://www.avocent.com>), the Internet security zone will be used.

-or-

Add the Rack Power Manager software hub server to the Trusted Sites list. The Rack Power Manager software client will always connect to the hub server using the Trusted Sites security zone. The Trusted Sites zone contains very low security settings and ensures successful communication between the client and the hub server.

To display or change the restrictions of a security zone:

1. In Internet Explorer, select *Tools - Internet Options*. The Internet Options dialog box appears.
2. Click the *Security* tab.
3. Select the security zone you wish to view.
4. Click *Custom Level*. The Security Settings dialog box appears.
5. Ensure that the following security settings are set to Enabled or Prompt. The Active Scripting setting should be set to Enabled.
 - Download Signed ActiveX Controls
 - Run ActiveX Controls and Plug-Ins
 - Launching Programs and Files in an IFRAME
 - Active Scripting
6. Click *OK* to save the settings and close the Security Settings dialog box.
7. Click *OK* to close the Internet Options dialog box.

To add a hub server to the Trusted Sites list:

NOTE: If Trusted Sites security zone settings have been modified from their defaults, ensure that the correct settings required for the Rack Power Manager software are specified, as indicated above.

1. In Internet Explorer, select *Tools - Internet Options*. The Internet Options dialog box appears.
2. Click the *Security* tab.
3. Click *Trusted Sites*, then click *Sites*. The Trusted Sites dialog box appears.

4. Type the web site address, in standard dot notation (xxx.xxx.xxx.xxx), for the Rack Power Manager software hub server (for example, https://10.0.0.1).
5. Click *Add*. The web site address will appear in the web sites list box.
6. Ensure that *Require server verification (https:) for all sites in this zone* is selected.
7. Click *OK* to save the settings and close the Trusted Sites dialog box.
8. Click *OK* to close the Internet Options dialog box.

Advanced Internet options

Internet Explorer contains advanced settings that may be specified to enhance use of the Rack Power Manager software. Changing these settings is not required, but is recommended for optimum results.

To specify advanced Internet options for the Rack Power Manager software:

1. In Internet Explorer, select *Tools - Internet Options*. The Internet Options dialog box appears.
2. Click the *Advanced* tab.
3. Select the following settings:
 - Always send URLs as UTF-8
 - Disable script debugging
 - Play animations in web pages
 - Show pictures
 - Print background colors and images
 - Use SSL 2.0
 - Use SSL 3.0
4. Select *Enable Integrated Windows Authentication* if the Rack Power Manager software is using Integrated Windows Authentication. See *Integrated Windows Authentication* on page 52.
5. Uncheck the following settings:
 - Always expand ALT text for images
 - Display a notification about every script error
6. Click *OK* to save the settings and close the dialog box.

Certificates

The Rack Power Manager software system uses certificates to provide secure transactions between components and to uniquely identify components in the system.

System certificate and SSH key

The Rack Power Manager software system generates and manages a system certificate and SSH key. The system certificate or SSH key may be exported to a local directory - the certificate's public key may then be used to validate the signature of data log files.

To view or export the system certificate or SSH key:

1. Click the *System* tab.
2. Click *Global Properties* in the top navigation bar.
3. In the side navigation bar, click *X.509 Certificates*, and then click *System Certificate*. The System Certificate window will open.
4. To export the system certificate in PEM format to a local directory, click *Export Certificate*. A pop-up window will open. The content of this window is browser-dependent, but it will usually prompt you to confirm the export operation. Confirm or cancel.

-or-

To export the SSH key in PUB format to a local directory, click *Export SSH Key*. A pop-up window will open. The content of this window is browser-dependent, but it will usually prompt you to confirm the export operation. Confirm or cancel.

Server certificates

A Rack Power Manager server certificate:

- Uniquely identifies the Rack Power Manager server to Rack Power Manager software clients connecting to the server using web browsers
- Uniquely identifies the Rack Power Manager server to other Rack Power Manager servers in the system and provides for secure transactions between them
- Provides for secure transactions between Rack Power Manager software clients and the Rack Power Manager software server

A Security Alert dialog box may appear if there are server certificate issues. See *Server certificates* on page 63 for information about certificate alerts and updating server certificates.

Client certificates

Rack Power Manager software client certificates (also known as user certificates) are used to authenticate client users during login when the Rack Power Manager software internal authentication service is configured in their user accounts. See *Adding User Accounts* on page 211.

To use Rack Power Manager software client certificates for authentication, a Rack Power Manager software administrator must first enable certificate authentication; see *Client session information* on page 69. Once this is enabled, the Rack Power Manager server will prompt the client web browser to send its user certificates.

The Rack Power Manager software client certificate must first be loaded into the client web browser and be associated with a user account. There are two ways to do this:

- The certificate location can be specified in a user account - see *User certificates* on page 216
- The Rack Power Manager software administrator may enable user-settable certificates, then the user may specify the certificate location - see *Specifying a user certificate* on page 41

If the system certificate policy (see below) is enabled for user certificates, the certificate used at login must meet the policy requirements.

Managed appliance certificates

Certificates are also used for authenticating and authorizing managed appliance sessions when a managed appliance is added in secure mode. See *Adding Units* on page 119.

System certificate policy and trust store

Rack Power Manager software administrators may configure the certificate policy by enabling/disabling settings. The trust store contains a list of all trusted certificate authorities known to the Rack Power Manager software. You may add, remove or modify the location of trust store entries.

To configure certificate policy settings:

1. Click the *System* tab.
2. Click *Global Properties* in the top navigation bar.
3. Click *X.509 Certificates* in the side navigation bar. The System Certificate Policy window will open.
4. Enable/disable checkboxes or select values as indicated for each setting.

Table 5.2: System Certificate Policy

Feature	Value when enabled
Chain Building	
Authority Info Access (AIA)	Permits the Rack Power Manager software to use the AIA certificate extension to locate a certificate's issuer.
Max chain length	Maximum allowable number of certificates (inclusive) between the leaf certificate and a trusted certificate. Valid range is 1-16.
Chain Validation	
Partial chains	Allows partial chains. (If disabled, partial chains will be considered invalid, even if the chain contains a trusted certificate.
Usage flags	A certificate may be used only for the reasons dictated in the certificate. For example, a certificate must be flagged as CA (Certificate Authority) to be considered a valid certificate issuer.
Validity period	The current date and time on the server must be within the window on each certificate in the chain.
Verify signatures	The signatures within the certificate chain are checked for validity.
Certificate Revocation Lists (CRL)	
CRL checks	If CRLs are available, they are checked to determine a certificate's revocation status.
Distribution points	CRLs may be located using the distribution point certificate extension.
Reject on error	The Rack Power Manager software will reject a certificate chain if a CRL is specified (either in the certificate or the Rack Power Manager trust store) and it cannot be read or is invalid.
Secure Sockets Layer (SSL)	
Name verification	Outbound SSL connections will verify server names.
Subject alternative names	The server names may match the certificate common name or one of the subject alternative names.
User Certificates	
Verify using trust store	User certificates presented to the Rack Power Manager software are verified using the System Trust Store.

5. Click *Save*.

To display and manage the trust store:

1. Click the *System* tab.
2. Click *Global Properties* in the top navigation bar.
3. In the side navigation bar, click *X.509 Certificates*, and then click *Trust Store*. The System Trust Store window will open, listing all trusted certificate authorities known to the Rack Power Manager software. By default, the list contains the standard CAs from Java.
4. To view or change information about a certificate, click on its name. The System Trust Store Entry window will open. You may change the CRL Location, which indicates where the CRL should be obtained for that CA. If you change the location, click *Save*. Then click *Close*.
5. To delete one or more certificates:
 - a. Click the checkbox to the left of the certificate name. To delete all certificates on the page, click the checkbox to the left of Name at the top of the list.
 - b. Click *Delete*.
 - c. You are prompted to confirm the deletion. Confirm or cancel the deletion.
6. To add a certificate:
 - a. Click *Add*. The New System Trust Store Entry window will open.
 - b. In the Certificate File field, enter the name of the file containing the X.509 certificate to upload into the trust store. The file may be binary or Base64 encoded.
 - c. In the CRL Location field, you may enter the location of the CRL for the uploaded certificate (maximum 256 characters). The supported protocols are http:// and ldap://.
 - d. Click *Add*.

Integrated Windows Authentication

The Rack Power Manager management software allows Rack Power Manager software clients to authenticate against Microsoft Windows NT domain and Microsoft Active Directory external authentication servers using Integrated Windows Authentication. This feature allows Single Sign-On (SSO) and is disabled by default. When running Windows Server 2003 or 2008 with Kerberos and NTLM authentication protocols, SSO is supported but it must first be configured in the web browser and AD server; see the documentation included with your browser and AD server or contact an Avocent technical support representative for assistance.

NOTE: When accessing the Rack Power Manager client using Integrated Windows Authentication, the browser URL must include the Rack Power Manager intranet name.

To use Integrated Windows Authentication for authentication, a Rack Power Manager software administrator must first enable it. See *Client session information* on page 69.

Firewalls

In a typical network configuration, as shown in Figure 5.1, the Rack Power Manager software client is located outside of the firewall and the Rack Power Manager server and managed appliances reside inside the firewall. In this case, the firewall must be configured to allow two TCP/IP ports inside the firewall.

One TCP port (default=443) is used for the HTTPS web browser connection between the Rack Power Manager software client and the Rack Power Manager server. The other TCP port (default=1078) is used for the Emerson Proxy Protocol to tunnel video and Telnet traffic. Both ports are configurable.

If you are using the Rack Power Manager management software through a firewall, we recommend the following:

- Place the Rack Power Manager server and all managed appliances within the same firewall Demilitarized Zone (DMZ). If the managed appliances are not in the same DMZ with the Rack Power Manager server, you must configure the firewall so all data may pass between the zones using TCP/IP ports 22 (SSH), 3211, 2068, 8192 and 3871. You must also configure the User Datagram Protocol (UDP) port 3211 so it may pass through the firewall for initial network discovery of appliances that do not have an IP address.

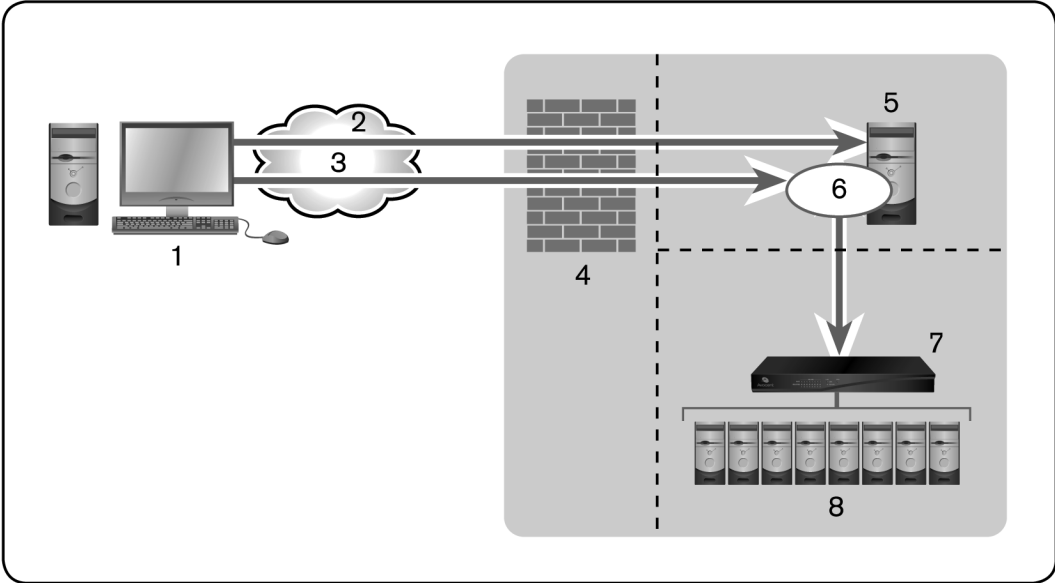


Figure 5.1: Typical Rack Power Manager Software System Firewall Configuration

Table 5.3: Typical Rack Power Manager Software System Firewall Configuration Descriptions

Number	Description	Number	Description
1	Rack Power Manager Software Client	5	Rack Power Manager Server
2	HTTPS	6	Proxy
3	Proxy	7	KVM Switch or Serial Console Appliance
4	Firewall	8	Target Devices

VPNs

A Virtual Private Network (VPN) is a secure network that uses public infrastructure and typically includes several Wide Area Network (WAN) components that may impact performance of the VPN.

Typically, two sites are connected in a VPN network using WANs and a router. This setup provides a secure network between the two sites, but processing is slow.

Several factors related to the network setup, including the Rack Power Manager software database replication schedule and methods of device access, can affect the speed of a multi-site VPN network. The trade-off must be made based on the network setup.

Frequent replication of the Rack Power Manager software database will increase WAN/VPN traffic but provide steady data reception at the local sites. Infrequent database replication made at the various sites decreases the WAN/VPN traffic but delays the reception of changes at the local site.

In addition, the methods used to access devices affects network speed. VPN access of a managed appliance is always slower than local access.

The Rack Power Manager management software supports VPNs that provide full transparency for IP addresses, as well as ports between sites and many VPNs that perform network address translation (NAT) between sites. For example, the VPN in Figure 5.2 could use NAT if Site A and Site B are separate companies that merged but have not resolved their IP addresses. See *NAT Devices* on page 56.

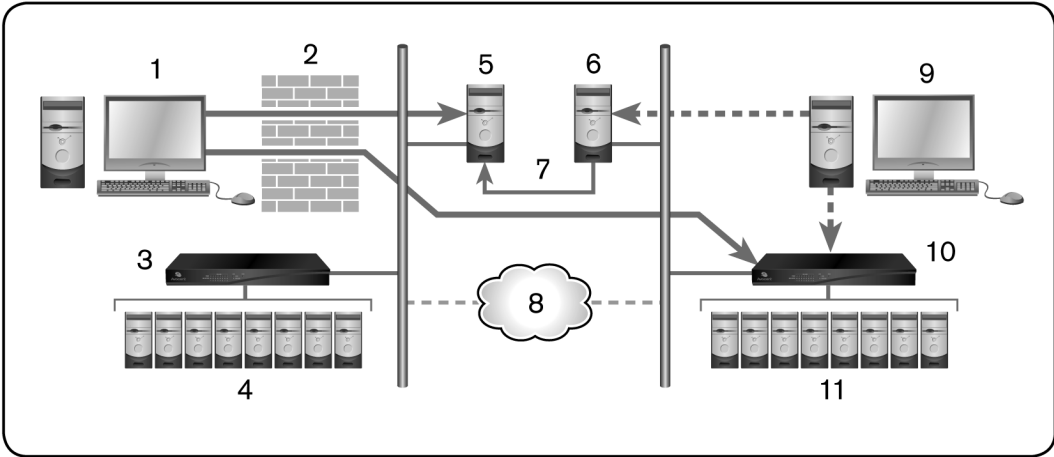


Figure 5.2: Rack Power Manager Software System on a VPN

Table 5.4: Typical Rack Power Manager Software System Firewall Configuration Descriptions

Number	Description	Number	Description
1	Rack Power Manager Software Client	7	Replication
2	Firewall	8	VPN

Number	Description	Number	Description
3	Site A	9	Rack Power Manager Software Client
4	Target Devices	10	Site B
5	Hub Server	11	Target Devices
6	Spoke Server		

NAT Devices

NAT devices enable a company to use more internal IP addresses than they have assigned to managed appliances. The IP addresses are not exposed outside of the NAT device.

NAT devices are typically used with a DSL broadband router. A Rack Power Manager software client is connected to the NAT device, as shown in Figure 1.6, which then connects to the corporate network using a VPN.

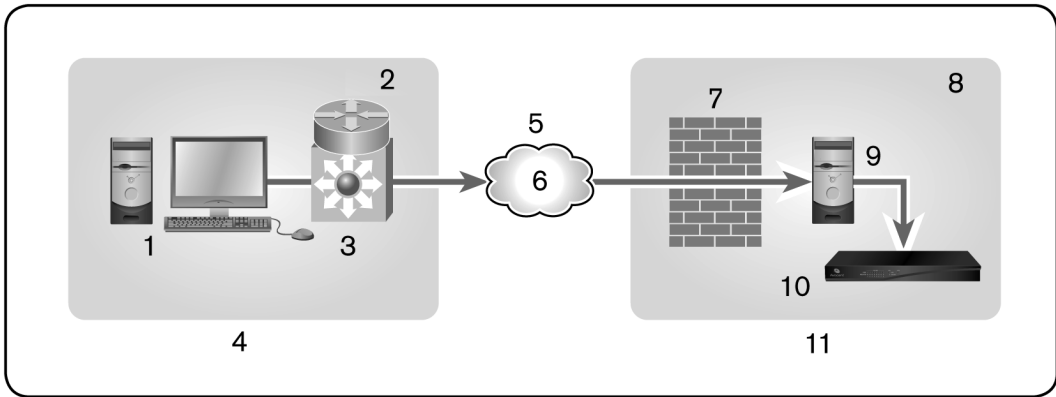


Figure 5.3: Single NAT Configuration (Client Only)

Table 5.5: Single NAT Configuration (Client Only) Descriptions

Number	Description	Number	Description
1	Rack Power Manager Software Client	7	Firewall
2	Private	8	Private
3	NAT Device	9	Rack Power Manager Server

Number	Description	Number	Description
4	Client	10	Managed Appliance
5	Public	11	Corporate
6	VPN		

Another scenario, shown in Figure 5.4, is when the corporate site also uses a NAT device to save IP addresses (double-NAT). Since the Rack Power Manager software client is trying to access a private resource inside the corporate site, the TCP/IP ports used for HTTPS and the proxy server must be configured to be exposed on the corporate NAT device.

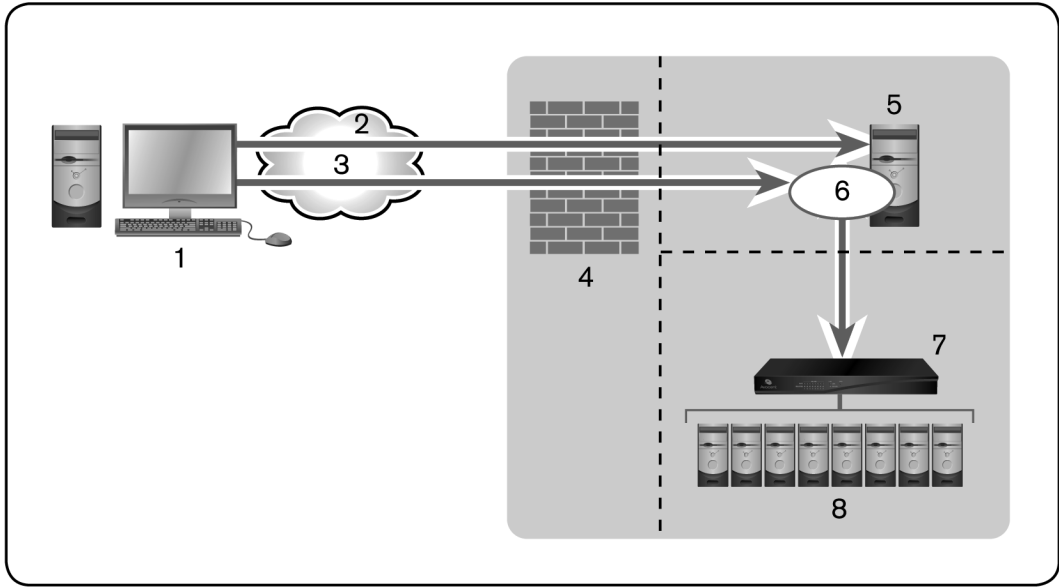


Figure 5.4: Double-NAT Configuration (Client and Corporate)

Table 5.6: Double-NAT Configuration (Client and Corporate) Descriptions

Number	Description	Number	Description
1	Rack Power Manager Software Client	5	Rack Power Manager Server
2	Public	6	NAT Device
3	Private	7	Managed Appliance
4	Firewall	8	Corporate

NOTE: NAT devices may not be connected between the Rack Power Manager server and any managed appliances.

Licenses

License keys permit the operation of the Rack Power Manager software on the hub server. They also specify the number of managed devices that may be controlled by the software and spoke servers allowed on a system. If a managed device is available through multiple connection methods, the managed device requires only one license as long as it is merged into a single connection in the Rack Power Manager software.

Licenses may also be required to enable additional features. See Table 5.7 for more information.

A demonstration (demo) license key may also be used for a trial period. When the trial elapses, login attempts will fail. A demo license key may be replaced with another demo license key or a permanent license. If additional license keys are added during the trial and the demo key expires, the add-on keys will have to be re-entered when a new license key is installed.

To display license information:

1. Click the *System* tab.
2. Click *Licenses* in the top navigation bar.
3. Click *Summary* in the side navigation bar. The License Summary window will open. Table 5.7 describes the window fields.

Table 5.7: License Summary Fields

Section	Field	Description
Installation Key or Demo Install Key	Serial Number	Serial number encoded in the license key for the Rack Power Manager software hub.
Client Server	Currently in Use	The total number of licenses for client servers that can be added to and managed by the Rack Power Manager system.
Data Logging Sessions	Licensed	Total number of licenses for data logging.
	Currently in Use	Number of licenses for data logging currently in use.
Plug-ins	Licensed	Total number of license IDs for plug-ins.
	Currently In Use	Number of license IDs for plug-ins currently in use.

Section	Field	Description
Auditor Appliances	Licensed	Total number of Auditor appliances licensed to be added as managed appliances.
	Currently in Use	Number of Auditor appliance licenses currently enabled.
Web Services API	Licensed	Status of the Web Services API licensing; may be enabled or disabled. For more information, see the Rack Power Manager SDK GUI Access API and Web Services API Installer/User Guide.
DS Zones	Licensed	Total number of DS zones that can be created.
PDU Count	Licensed	Total number of PDUs that can be added.

To display license keys:

1. Click the *System* tab.
2. Click *Licenses* in the top navigation bar.
3. Click *License Keys* in the side navigation bar. The License Keys window will open and list each installed license key and a description of the key. One of the following descriptions will display beside each key:
 - Adds <number> Backup Server(s) - Adds <N> backup (spoke) Rack Power Manager servers.
 - Adds <number> Backup Server(s) and Unlimited Client Sessions - Combines the keys for Adds <N> Backup Server(s) and Client Session Site License.
 - Installation Key - Enables first use of the Rack Power Manager software and sets the initial number of backup Rack Power Manager servers.
 - Demo License Key - Enables first use of the Rack Power Manager software for a certain period of time.
 - Add <number> Managed Devices - Increases the number of licensed managed devices.
 - Add <number> Power Strips - Increases the number of power strip devices.
 - Add <number> Auditor Appliance - Increases the number of auditor appliances that can be added.

Adding a new license key

To add a new license key:

1. Click the *System* tab.
2. Click *Licenses* in the top navigation bar.
3. Click *License Keys* in the side navigation bar. The License Keys window will open.
4. Click *Add*. The Add License Key window will open.
5. Type a valid new add-on license key in the License Key field.
6. Click *Save*. The License Keys window opens, containing a new row with the new license key.

System Information

The System Information window displays the total number of client sessions in use and the Rack Power Manager software version currently installed.

To view system information:

1. Click the *System* tab.
2. Click *Global Properties* in the top navigation bar.
3. Click *System Information* in the side navigation bar. The System Information window opens.

Rack Power Manager Servers

This chapter describes how to configure Rack Power Manager server properties, backup and restore hub servers and manage spoke servers.

Server Properties

Table 6.1 lists the Rack Power Manager server properties.

Table 6.1: Server Properties

Property	Description
Identity	Name of the Rack Power Manager server and the server’s role (hub or spoke).
Network	IP address (*) and port used by clients to access the server using the HTTPS (SSL) protocol. You may change the port number used for the HTTPS connection. NOTE: When the Rack Power Manager server is running on a Linux system, the IP address field may contain the loopback address. If this is not desired, edit the /etc/hosts file on the Linux system. Add a new line above the line that defines the loopback address. The new line should contain the IP address, followed by the host name. For example, the following new line adds the IP address 172.30.20.206 for the host name sun-jcv-fc3.avocent.com, above the existing line that defines the loopback address (127.0.0.1). - 172.30.20.206 sun-jcv-fc3.avocent.com - 127.0.0.1 localhost.localdomain sun-jcv-fc3.avocent.com localhost sun-jcv-fc3
	Rack Power Manager server certificate presented to Rack Power Manager software client web browsers.

Property	Description
Proxy Server	When the Avocent proxy server is used, Rack Power Manager software client KVM and serial session requests are sent through the Rack Power Manager server rather than directly to the KVM switch or serial console appliance, which prevents the exposure of the internal address of the managed appliance. You may change the proxy server configuration. EVR1500 environmental monitor, DSI5100 IPMI and generic appliance sessions are not sent through the Rack Power Manager server, even when the proxy is enabled.
SSH Server	Enables/disables the SSH server and specifies the port it uses.
Trap Destinations	The Rack Power Manager server polls KVM switches or serial console appliances to determine if they are responding. If the managed appliance does not respond, the Rack Power Manager server sends an SNMP Loss Of Communication (LCM) trap or alert to the external SNMP manager. When the Rack Power Manager server detects that the appliance is once again communicating, a Regained Communication (RCM) trap is sent from the Rack Power Manager software server. When a response change occurs during communication between the Rack Power Manager server and a managed appliance, the Rack Power Manager software writes the event to the event log and sends an SNMP trap to the configured trap destinations. Trap destinations may also be specified by clicking on a managed appliance and changing the SNMP appliance settings.
Rack Power Manager Client Sessions	Settings for inactivity time-out, authentication policy, Single Sign-On (SSO) for the session or restrictions to use specific IP addresses to start the sessions. Also displayed the number of client sessions currently in use.
Rack Power Manager Modem Session	Settings for dial-up sessions, including inactivity time-out, time to wait for a connection and dial-back number.
Email	IP address of the SMTP (Simple Mail Transfer Protocol) server that is used by the Rack Power Manager software to send email notifications.
Unit Status Polling	Enables/disables unit status polling for the Rack Power Manager server, and specifies the delay between polling cycles and the number of managed appliances that will be concurrently polled.
Spoke Servers	Enables you to manage the Rack Power Manager software spoke servers in your system.
Data Logging	Settings for data log file location, archiving and Syslog server.

To display server properties:

Click the *System* tab. *Rack Power Manager Server* will automatically be selected in the top navigation bar and *Identity* will automatically be selected in the side navigation bar. The Rack Power Manager Server Identity Properties window will open. The top of the side navigation bar will indicate the name of the Rack Power Manager software server.

To change server network properties:

1. Click the *System* tab.
2. Click *Network* in the side navigation bar. The Rack Power Manager Server Network Properties window will open.
3. Type a new Rack Power Manager server port number in the HTTPS Port field.

If the default value (443) is modified, the port number in the URL must be specified when accessing the Rack Power Manager software. For example, if the IP address of the hub server is 10.0.0.1 and the port number is changed to 444,

https://10.0.0.1:444/Rack Power Manager must be typed in the Address field of the web browser to access the Rack Power Manager software.

The selected port must be available on the Rack Power Manager server. If Rack Power Manager software clients are located on an external connection, the specified port must be open on the firewall.

4. Click *Save*. A confirmation dialog box will appear.

A web browser error message will appear when *Save* is clicked. This error message is a normal occurrence. To reestablish connection to the Rack Power Manager software, you must reconnect to the hub server by typing the URL with the new port number. For example, if you changed the port number to 334 for a hub server with an IP address of 10.0.0.1, type **https://10.0.0.1:334/Rack Power Manager** to access the Rack Power Manager management software.

5. Confirm or cancel the change.

Server certificates

Rack Power Manager software administrators manage server certificates. See *Certificates* on page 49 for a description of certificate types and procedures to manage certificate policy and the system trust store.

Security alerts

The Rack Power Manager software uses SSL (Secure Sockets Layer) to securely communicate between the Rack Power Manager software hub server and Rack Power Manager software clients. SSL provides secure authentication using certificates, which is data that identifies the PC with which communication will occur. A certificate is typically verified by another certificate from a trusted certificate authority.

When the Rack Power Manager software is initially installed, it generates a self-signed certificate for use with Rack Power Manager software clients. To replace this, a Rack Power

Manager software administrator may create a Certificate Signing Request (CSR) to submit to a trusted third party Certificate Authority (CA) for signature. The administrator may then replace the generated certificate with the new one. If the generated certificate is not replaced, the web browser will prompt a user whether to trust the generated certificate when a Rack Power Manager software client session is started.

Three tests are performed on a certificate each time a Rack Power Manager software client connects to the Rack Power Manager software hub server:

- Does the client web browser trust the certificate issuer?
- Has the certificate expired?
- Does the name on the Rack Power Manager server certificate match the name the Rack Power Manager software client used to access the Rack Power Manager server?

A Security Alert dialog box will appear if the answer to any of the three questions is No. To prevent the Security Alert message box from appearing when you connect to a the Rack Power Manager software hub server, all three questions must be answered Yes. When a Security Alert dialog box appears, you have the following choices:

- If you click *Yes*, a connection will be made with the Rack Power Manager software hub server and the Rack Power Manager software login window will appear, but the Security Alert dialog box will continue to appear each time you connect to the hub server.
- If you click *No*, a connection will not be made with the Rack Power Manager software hub server.
- If you click *View Certificate*, you may install the certificate; see below.

To correct certificate security alerts for client and hub server connections:

1. From the Rack Power Manager software client, open a client session; see *Opening a client session* on page 10. The Security Alert dialog box will appear.
2. Click *View Certificate*. The Certificate dialog box will appear.
3. Click *Install Certificate*. See the Internet Explorer documentation for more information.
4. Once the certificate is installed, ensure that the time setting on the Rack Power Manager software client PC is within the Valid from...to dates and that the Issued to and Issued by fields exactly match.

Invalid to...from dates typically occur when the Rack Power Manager software is installed on a server that is set to an invalid time. When a Rack Power Manager software client that is set to a valid time connects to the Rack Power Manager server

that is set to an invalid time, the following warning will appear in the Security Alert dialog box: “The security certificate date is invalid.”

Serial session security alerts

The Serial Session Viewer, which is used during a serial session, is a Java-based applet. Three certificate tests are performed by Java when the Rack Power Manager software connects to a serial device:

- Does the serial device trust the certificate issuer?
- Has the certificate expired?
- Does the name on the serial device certificate match the name of the Rack Power Manager software hub server certificate?

A warning dialog box will appear if the answer to all three questions is No. To prevent this warning dialog box from appearing when you connect to a serial device, all three questions must be answered Yes.

To correct certificate security alerts when connecting to a serial session:

1. In a Units View window that contains serial console appliance target devices (see *Accessing Units View windows* on page 111), click the *Serial Session* link in the Action field.

You can also access a Unit Overview window for a target device and click the *Serial Session* icon or link for the session type (see *Unit Overview Windows* on page 116).

2. If the certificate is trusted and has not expired, but there is a mismatch of the name on the Rack Power Manager software client certificate and the name on the Rack Power Manager software hub server certificate, a Warning - HTTPS dialog box will appear. Contact the issuer of your certificate.
3. When a Warning - Security dialog box appears, you have the following choices:
 - If you click *Yes*, a connection will be made with the appliance and the viewer will open, but the warning dialog box will continue to appear each time you connect to the serial console appliance.
 - If you click *No*, a connection will not be made with the serial console appliance.
 - If you click *Always*, the certificate will be added to the Java certificate store.

To create a CSR:

1. Click the *System* tab.

2. Click *Certificate* in the side navigation bar. The RPM Server Certificate Properties window will open.
3. Click *Get CSR*. A File Download dialog box will appear.
4. Click *Open*. The CSR is downloaded and displays in the configured text editor.

-or-

Click *Save*. The Save As dialog box will appear. Select a directory and filename and click *Save* to save the CSR.

5. Submit the CSR generated request to a CA to obtain a signed server certificate.
6. Update the Rack Power Manager server to use the certificate created by the CA.

To update certificate information on the Rack Power Manager server:

NOTE: You may also update a spoke server certificate on a hub server and update a hub server certificate on a spoke server; see *Managing hub and spoke server certificates* on page 67.

1. Click the *System* tab.
2. Click *Certificate* in the side navigation bar. The RPM Server Certificate Properties window will appear.
3. Click *Update*. The Update RPM Server Certificate Wizard will appear.
4. The Select Operation to Perform window will open.
 - Select *Create a new self-signed SSL server certificate* to create a minimal security SSL certificate without incurring the costs and overhead involved with a Certificate Authority (CA). Click *Next*, then go to step 5.
 - Select *Import a signed SSL server certificate* to import a more secure SSL certificate that has been approved (perhaps by a CA). The public key of the imported certificate must match the public key in the certificate that the Rack Power Manager server is currently using. This requires that both certificates be made on the same Rack Power Manager server. Click *Next*, then go to step 6.
5. The Type in Certificate Information window will open.
 - a. Type the name of the computer that will serve as the Rack Power Manager server on your intranet in the Common Name field. If the Rack Power Manager server is outside the intranet, type the server's full domain name in dot notation format (xxx.xxx.xxx.xxx).
 - b. Type the name of the organization (or country).

- c. Type the name of the organizational division or name under which the organization is doing business.
 - d. Type the complete city or location name. The City or Location field is required for organizations registered only at the local level.
 - e. Type the complete name of the state or province where the organization is located.
 - f. Type the two-character ISO country code for the country where the organization is located.
 - g. Click *Next*. Go to step 7.
6. The Select Certificate to Import window will open.

Type the full directory and filename for the SSL certificate file you wish to import to the Rack Power Manager server or browse to the file location.

The name of the SSL certificate file must be entered in case sensitive text if your operating system supports case sensitive filenames.

Imported certificates must have been generated from a CSR created on the same Rack Power Manager server to which you are importing the certificate.
 - h. Click *Next*.
 7. The Completed Successful window will open.
 8. Click *Finish*. The RPM Server Certificate Properties window will open, containing updated certificate information.

Managing hub and spoke server certificates

When a spoke server is registered with a hub server, a certificate trust relationship is established between the two servers. Certificate information must match on the hub server and the spoke servers for communication to take place between the servers. If the spoke server certificate is subsequently changed, a certificate mismatch will occur.

To update the certificate of a spoke server on the hub server:

NOTE: Certificates may only be viewed by Rack Power Manager software administrators and user administrators.

1. On the hub server, click the *System* tab. *RPM Server* will automatically be selected in the top navigation bar and the name of the Rack Power Manager software hub server will appear at the top of the side navigation bar.
2. Click *Spoke Servers* in the side navigation bar. The Spoke Servers window will open.

3. In the Spoke Servers window, click *Certificate*. The Spoke Server Certificate window will open including information about the spoke server certificate (Actual Certificate) and the certificate registered for this spoke server on the hub server (Registered Certificate).
4. The window displays the certificate on the spoke server and the certificate registered on the hub server.

If the Rack Power Manager management software cannot obtain the certificate information from the spoke server, a message will appear at the bottom of the RPM Server Certificate - Spoke Server window. The message states: *Remote server is not responding. Information displayed may not match remote side.*

- If the certificate information does not match, go to step 5.
 - If the certificate information matches, go to step 6.
5. Click *Update*. The spoke server certificate information will be updated on the hub server.
 6. Click *Close*. The Spoke Servers window will open.

To update the certificate of a hub server on a spoke server:

1. On the spoke server, click the *System* tab. *RPM Server* will automatically be selected in the top navigation bar and the name of the spoke server will appear at the top of the side navigation bar.
2. Click *Hub Server* in the side navigation bar. The Hub Server window will open.
3. In the Hub Server window, click *Certificate*. The Hub Server Certificate window will open including information about the spoke server certificate (Actual Certificate) and the certificate registered for this spoke server on the hub server (Registered Certificate).

If the Rack Power Manager software cannot obtain the certificate information from the hub server, a message will appear at the bottom of the RPM Server Certificate - Hub Server window. The message states: *Remote server is not responding. Information displayed may not match remote side.*

If the certificate information does not match, go to step 4.

4. Click *Update*. The hub server certificate information will be updated on the spoke server.

Server trap destinations

To specify trap destinations:

1. Click the *System* tab.
2. Click *Trap Destinations* in the side navigation bar. The RPM Server Trap Destinations window will open.

3. In each address field, type the IP addresses in standard dot notation (xxx.xxx.xxx.xxx) or the domain name for the computer that handles traps. Up to four computers may be specified.
4. Click *Save* to store the trap information in the Rack Power Manager software database on the host.

Client session information

To specify client session information:

1. Click the *System* tab.
2. Click *RPM Client Sessions* in the side navigation bar. The RPM Server Client Session Properties window opens. The number of client sessions currently in use is displayed.
3. Use the arrows to specify a time-out value (from 5-60 minutes) for inactivity of a Rack Power Manager user client session. The default is 15 minutes. When the time-out value has been exceeded, the session will end and the user must log in again.
4. Check the *Enable certificate authentication* checkbox to allow the Rack Power Manager software to automatically log in internal users if the user certificate (X.509 digital ID) installed in the Rack Power Manager software client web browser matches the certificate configured for the user. Certificates for users may be modified. See *User certificates* on page 216.

Web browser settings may need to be modified to allow users to automatically log in using certificates; see your web browser documentation.

-or-

Check the *Enable Integrated Windows® Authentication* checkbox to automatically log a user into the Rack Power Manager software using the Windows user's computer credentials.

Web browser settings may need to be modified to allow users to automatically log in using Integrated Windows Authentication; see your web browser documentation.

5. To enable only Rack Power Manager software clients with IP addresses entered in the Address List to communicate with managed appliances, check the *Restrict by address range* checkbox. To disable address restrictions for logging into the Rack Power Manager software, uncheck this checkbox.
6. Enable or disable *Allow login when user is a member of more than one authentication service* as desired. The preset value is disabled. When enabled, if a user belongs to multiple authentication services, the Rack Power Manager server uses the first authentication service

found to log the user in. When disabled, if a user belongs to multiple authentication services, the attempt to log in to the Rack Power Manager software fails.

When enabled, if a user has different access rights within each authentication service he belongs to, the user is granted access rights based on the first authentication service found by the Rack Power Manager server. In this case, a user may be granted different access rights at different login times.

NOTE: The *Allow login when user is a member of more than one authentication service* setting does not replicate to spoke servers. It is recommended that you uniformly enable or disable this setting on each Rack Power Manager hub and spoke server.

7. Click *Save* to store client session information in the Rack Power Manager software database on the host.

Email

To specify email properties:

1. Click the *System* tab.
2. Click *Email* in the side navigation bar. The RPM Server Email Server Properties window will open.
3. Type a new address for the SMTP server that sends email notifications as a domain name or an IP address in standard dot notation (xxx.xxx.xxx.xxx).
4. If your SMTP server requires login credentials, select *Login required to access SMTP server* and type a username and password, then confirm the password.
5. Click *Save* to store Rack Power Manager software email property information in the Rack Power Manager software database on the host.

Unit status polling

To use unit status polling:

1. Click the *System* tab.
2. Click *Unit Status Polling* in the side navigation bar. The RPM Server Unit Status Polling Properties window will open.
3. Select *Enable unit status polling*.
4. Type the number of seconds to wait between polling cycles (from 30-999 seconds). The default is 900 seconds (15 minutes). A smaller value results in greater accuracy.
5. Type the number of managed appliances that may simultaneously be polled to obtain status information (from 1-25 units). The default is 5. A larger number results in faster speed.

6. Click *Save* to store unit status information in the Rack Power Manager software database on the host.

Backing up and Restoring Hub Servers Manually

You may manually create a backup of your hub server. Two methods are available:

- From a command line in an MS-DOS window. This method may be used for Rack Power Manager software hub servers on supported Windows or Linux systems.
- Using the Backup and Restore Utility delivered with the Rack Power Manager software. The backup is saved as a .zip file containing the files needed to restore the Rack Power Manager management software. This method may be used for Rack Power Manager software hub servers on supported Windows systems only.

Client sessions will be temporarily disconnected during a manual backup. The sessions will be automatically reconnected when the backup is completed.

Hub server backups may also be automatically created as a task within the Rack Power Manager software. If you use the Backup RPM database and system files task, client sessions will not be temporarily disconnected. See *Task: Backup Rack Power Manager software database and system files* on page 265.

Manual backup and restore procedures require Rack Power Manager software administrator privileges.

To manually backup or restore a hub server using a command line on a supported Windows system:

1. In the Start menu on your desktop, select *Start - Programs - Accessories - Command Prompt*. A command prompt window will open.
2. Change directories to the directory in which the Rack Power Manager software is installed (typically C:\Program Files\Emerson\RPM1.0\bin).
3. Enter **RPMBBackupRestore** to display the Rack Power Manager Backup/Restore Utility dialog box. Follow the directions in *To manually back up a hub server using the Backup and Restore Utility dialog box* to back up the hub server using the dialog box or *To manually restore a hub server using the Backup and Restore Utility dialog box* to restore the hub server using the dialog box. (These procedures are described later in this section.)

-or-

To backup the Rack Power Manager software hub server, enter **RPMBBackupRestore -backup -archive "<archive name>" -passwd <password>**.

-or-

To restore the Rack Power Manager software hub server, enter **RPMBBackupRestore -restore -archive "<archive name>" -passwd <password>**.

"<archive name>" - Name of the archive, which must be enclosed by quotation marks (for example, "myarchive"). The -archive option and an archive name are required.

<password> - A password that encrypts the archive. The password is optional when creating a backup. If a password is specified when creating the backup, it will be required when restoring the backup.

To display help information, type **RPMBBackupRestore -horRPMBBackupRestore -help**.

For example, entering the following in a command prompt window will create a backup named db.zip with the password test.

RPMBBackupRestore.exe -backup -archive "db.zip" -passwd test

Entering the following in a command prompt window will restore a backup named db.zip with the password test.

RPMBBackupRestore.exe -restore -archive "db.zip" -passwd test

To manually backup or restore a hub server using a command line on a supported Linux system:

1. Access the command prompt on your system.
2. Change directories to the directory where the Rack Power Manager software is installed, which is typically /usr/local/RPMserver/bin.
3. To backup the Rack Power Manager software hub server, enter **RPMBBackupRestore.sh -backup -archive <archive name> -passwd <password> -overwrite**.
4. To restore the Rack Power Manager software hub server, enter **RPMBBackupRestore.sh -restore -archive <archive name> -passwd <password>**.

<archive name> - Name of the archive. The -archive option and an archive name are required.

<password> - A password that encrypts the archive. The password is optional when creating a backup. If a password is specified when creating the backup, it will be required when restoring the backup.

-overwrite - Enables overwriting of an existing archive during backup. If this parameter is omitted, no overwriting will occur.

To display help information, type **RPMBBackupRestore.sh -help**.

For example, entering the following in a command prompt window will create a backup named `dbasebackup.zip` with the password `test1`.

`RPMBBackupRestore.sh backup -archive dbasebackup.zip -passwd test1`

Entering the following in a command prompt window will restore a backup named `dbasebackup.zip` with the password `test1`.

`RPMBBackupRestore.sh restore -archive dbasebackup.zip -passwd test1`

To manually back up a hub server using the Backup and Restore Utility dialog box on a supported Windows system:

1. In the Start menu on your desktop, select *Start - Programs - Emerson Rack Power Manager - Backup and Restore Utility*. The Rack Power Manager Backup/Restore Utility dialog box will appear.
2. Click *Backup Database to a file*.
3. To password-protect the backup file, click *Enabled* and type a password in the Password field.
4. Click *Browse* and use the Save As dialog box to specify a directory and name for the backup file. Click *Save* when you are finished.
5. Click *Backup*. The Rack Power Manager software system backup files are saved.
6. Click *Close* to close the Rack Power Manager Backup/Restore Utility dialog box.

To manually restore a hub server using the Backup and Restore Utility on a supported Windows system:

1. In the Start menu on your desktop, select *Start - Programs - Emerson Rack Power Manager - Backup and Restore Utility*. The Rack Power Manager Backup/Restore Utility dialog box will appear.
2. From the Rack Power Manager Backup/Restore Utility dialog box, click *Restore the database from a file*.
3. If the backup file is password-protected, click *Enabled* and type its password in the Password field.
4. Click *Browse* and use the Save As dialog box to find the backup file.
5. Click *Restore*. The Rack Power Manager software system is restored from the backup files.
6. Click *Close* to close the Rack Power Manager Backup/Restore Utility dialog box.

Spoke Servers

Information on the hub server is replicated on one or more spoke servers. Information about each spoke server, such as IP address, port number and certificate, is stored in the hub server's database.

You may specify up to 15 computers as spoke servers. Contact Avocent for information about spoke server licenses. To install licenses, see *Licenses* on page 58.

A spoke server may be created by:

- Specifying a spoke server when installing the Rack Power Manager software.
- Converting a hub server to a spoke server by registering it as a spoke to another Rack Power Manager software hub server. The Rack Power Manager software system data on the hub server being converted will be lost and the converted hub server will replicate the data of the new specified hub server.

You may also change the properties of a spoke server or remove spoke servers from your system.

To display a list of spoke servers:

NOTE: The Spoke Servers window is only available on the hub server.

1. Click the *System* tab.
2. Click *RPM Server* in the top navigation bar. The side navigation bar will include the name of the server to which you are logged in.
3. Click *Properties* in the side navigation bar, and then click *Spoke Servers*. The Spoke Servers window will open.

You may change the fields that display by using the Customize link. See *Using the Customize link in windows* on page 30.

Each spoke server in the list includes status.

Table 6.2: Rack Power Manager Software Spoke Server Status

Status	Cause
Responding	Normal operation. The hub and spoke servers are communicating with each other using HTTPS.

Status	Cause
Not responding	The hub and spoke servers cannot communicate with each other using HTTPS. This typically indicates a network communication error. Ensure that network connectivity is occurring between the two servers.
Hub/Spoke Versions Not Compatible	The versions of Rack Power Manager software on the hub and spoke servers are not compatible.
Certificates Do Not Match	Certificates on the hub server and spoke servers do not match. See <i>Managing hub and spoke server certificates</i> on page 67 for information about updating the server certificates so that they will match.
Invalid Server or Versions Not Compatible	A server responded, but it is not compatible with the Rack Power Manager software. This typically occurs when communication is attempted with a server that does not contain the software, or if either server contains an older version of the software. Ensure that both servers are running the same Rack Power Manager software version.

To add a spoke server:

1. Install the Rack Power Manager software on the computer that will be used as a spoke server. See *Installing the Rack Power Manager Software* on page 6.
2. Configure the computer as a spoke server. See *Configuring the Rack Power Manager Software* on page 8.

To register a hub server as a spoke server:

Only Rack Power Manager software administrators may access this procedure.

NOTE: When registering a hub server as a spoke server on another Rack Power Manager software system, the information on the hub server being registered will be lost. Its database will be updated to match the new hub server to which it is being registered.

1. Click the *System* tab.
2. Click *RPM Server* in the top navigation bar. The side navigation bar will include the name of the server to which you are logged in.
3. Select *Tools* in the side navigation bar. The RPM Server Tools window will open.
4. Click the *Register as Spoke Server* icon or text. The Register Spoke Server Wizard will appear.
5. The Type in Hub RPM Server Address window will open.
 - a. Type the IP address of the hub server in standard dot notation (xxx.xxx.xxx.xxx) or the domain name of the hub server.

- b. Type the port number for the hub server.

If the default hub server port value (443) is modified, you must specify it when registering a spoke server so that register requests will be sent to the correct port on the hub server. For example, if the IP address of the hub server is 10.0.0.1 and the port number is changed to 444, type

https://10.0.0.1:444/RPM in the Address field of the Register Spoke Server Wizard.

- c. Click *Next*.
6. The Operation in Progress window will open briefly, followed by the Accept Hub RPM Server Certificate window. Click *Next*.
7. The Type in Hub RPM Server Administrator Credentials window will open. Click *Next*.
8. Type the name of a user with Rack Power Manager software administrator privileges on the hub server. Type a password for the user. Click *Next*.
9. The Operation In Progress window will open. The configuration of the spoke server will be saved to the database of the hub server and the spoke server's certificates will be installed on the hub server.
10. The Completed Successful window will open when the spoke server has been added.
11. Click *Finish*.

To change spoke server network properties:

NOTE: Spoke server network settings may need to be changed by Rack Power Manager software administrators when network settings are changed and the hub server did not automatically detect the changes. When changing the network settings, ensure that a port mismatch does not occur between the hub server and the spoke server.

1. On the hub server, click the *System* tab.
2. Click *RPM Server* in the top navigation bar. The side navigation bar will include the name of the server to which you are logged in.
3. Click *Properties* in the side navigation bar, and then click *Spoke Servers*. The Spoke Servers window will open.
4. Click on the name of the spoke server whose network properties you wish to change. The Spoke Server Network Properties window will open.
5. Change any of the following network settings:
 - Type a new computer name to use as the spoke server.
 - Type a new address in standard dot notation (xxx.xxx.xxx.xxx) for the spoke server.

- Type a new port number for the spoke server.
6. Click *Save* and then click *Close*. The Spoke Servers window will open.

To delete a spoke server:

1. On the hub server, click the *System* tab.
2. Click *RPM Server* in the top navigation bar. The side navigation bar will include the name of the server to which you are logged in.
3. Click *Properties* in the side navigation bar, and then click *Spoke Servers*. The Spoke Servers window will open.
4. Click the checkbox to the left of the spoke servers you wish to delete. To delete all spoke servers, click the checkbox to the left of Name at the top of the list.
5. Click *Delete*. A confirmation dialog box will appear.
6. Confirm or cancel the deletion.

NOTE: When a spoke server is deleted, it is no longer allowed to communicate with the hub server. Only spoke servers that are no longer active should be deleted. If a spoke server is still active, it may be re-registered using the Register Spoke Server wizard.

Promoting spoke servers

Promoting a spoke server to be a hub server is usually done only if the current hub server is no longer operational and will not be brought back into service. (For less severe problems with a hub server, the backup and restore operations can be used.)

If a spoke server must be promoted, be sure to run the replication task, if possible (see *Replication* on page 78) on all other spoke servers, then on the spoke server being promoted, immediately before the promotion. This will prevent loss of data from the other spoke servers.

(After the promotion of a spoke server to a hub, if the server that was originally the hub becomes operational again, it will have to register as a spoke server, since a system can have only one hub server.)

To promote a spoke server to be a hub server:

1. On the spoke server, click the *System* tab.
2. Click *Tools* in the side navigation bar.
3. Click *Promote to hub server*. The Promote Hub Server Wizard will appear.

4. Follow the prompts and heed the cautionary warnings in the wizard. The spoke server on which the wizard is running will become the hub server, and the other spoke servers will be advised of the changed configuration.

Replication

Replication is a task that synchronizes the hub and spoke server databases. By default, replication runs every 12 hours on each spoke server. A spoke server's first replication occurs automatically when the spoke server is added to the Rack Power Manager software system. You may change the interval that the replication task runs on each spoke server, or you may initiate an immediate replication.

During replication, the spoke server sends all of its database changes since the last replication to the hub server. The hub server then incorporates those changes and sends all of its database changes since the last replication to the spoke server (excluding the changes that spoke server just sent to the hub server).

If an item is added on a spoke server, and another item with the same name (but perhaps with different configuration parameters) is added on the hub server, then after replication, both items will appear on both the hub and spoke servers, with a tilde (~) and a number added to one of the names. The administrator should handle the issue appropriately - in some cases, the duplicate item may need to be renamed; in others, the duplicate item should be deleted.

When different changes are made to one existing item, two outcomes are possible. For example, assume an item is added and configured on the hub server and is then replicated to the spoke server. Later, an administrator changes something about the item on the spoke server. Another administrator then changes something about the item on the hub server. When the replication task runs, two things may happen.

In a few instances where no conflict occurs, both changes will be incorporated and replicated. For example, if the hub server's administrator adds username JaneDoe to the existing user-defined user group Accounting and the spoke server's administrator adds username JohnDoe to the Accounting user group, both names will be added and replicated.

In most other instances where the changes are mutually exclusive or some other conflict occurs, the most recent change will be the only change accepted and replicated. For example, if the hub server's administrator associates a unit with the Miami site, and the spoke server's administrator associates the same unit with the Chicago site, the change that was made closest to the time of replication (that is, the most recent change) will be accepted and replicated.

This emphasizes the importance of ensuring the hub and spoke servers' clocks are synchronized.

The exception to the last-change rule is when one of the actions deletes an item - in that case, the deletion is accepted and replicated, regardless of timing. For example, if a unit was deleted on the hub server, and then the contact information for the same unit was changed on the spoke server a minute later, the unit will be deleted when the replication task is run.

On a spoke server, you may enable a replication task property that forces the spoke server to retrieve a snapshot of the hub database rather than synchronizing changes back and forth. The snapshot is a copy of the hub at the time of the operation. This feature is not normally used; it is intended to help recover a system when replication has failed.

To display replication results and/or change the replication schedule for a spoke server:

1. On the spoke server, click the *System* tab.
2. Click *Tasks* in the top navigation bar. The Tasks window will open.
3. Select the *Database Replication* task. The Task Results - Database Replication window will open. This window contains the results of the most recent replication.
4. To display or change the replication schedule, click *Schedule* in the side navigation bar. The Task Schedule - Database Replication window will open.

By default, the replication task runs every 12 hours. You may change the schedule type, start time, date and interval.

5. To force the spoke server to retrieve a snapshot of the hub database rather than synchronizing changes, click *Properties* in the side navigation bar and then click the *Perform a hub database snapshot the next time this task executes* checkbox. This setting will be reset to unchecked after the operation completes.
6. If you made any changes, click *Save* and then *Close*.

You may also display the replication schedule from the hub server, but you cannot change it.

To initiate an immediate replication on a spoke server:

1. On the spoke server, click the *System* tab.
2. Click *Tasks* in the top navigation bar. The Tasks window will open.
3. Check the checkbox to the left of the Database Replication task and then click *Run Now*.

To display the replication schedule for a spoke server from the hub server:

1. On the hub server, click the *System* tab.
2. Click *Tasks* in the top navigation bar.

3. Select the *Database Replication* task for the spoke server you wish to view. The Task Schedule - Database Replication window will open.

Authentication Services

Users must be authenticated before they may access or perform any tasks in the Rack Power Manager management software system.

When users log in, they will be prompted for a username and password. The Rack Power Manager software will look up the login, determine the authentication service to use and forward the login credentials to the appropriate authentication service for verification. All authentication is performed over an HTTPS (SSL) encrypted link.

Some web browsers may store password information; see your web browser documentation.

Supported Authentication Services

The Rack Power Manager software is delivered with the RPM internal authentication service, which verifies a log in and password against user account information stored in the database on the Rack Power Manager software server.

The Rack Power Manager software also supports the following external authentication services:

- Microsoft Active Directory® *
- Novell®LDAP Services *
- Sun Solaris R9 LDAP Directory Server *
- Sun ONE™ LDAP Directory Server *
- Microsoft Windows® NT domain
- Cisco® Secure ACS 3.3 for Windows 2000/2003 server
- Microsoft IAS for Windows® 2000/2003 server
- FreeRADIUS for Red Hat RHL3
- Cisco® Secure ACS 3.3 for Windows 2000/2003 server
- RSA SecurID®

* Uses LDAP V3

If the Rack Power Manager server is configured for external authentication, login requests are re-directed to the configured external authentication server.

The Rack Power Manager software obtains external group membership and external user information when a user logs in. If a user's group membership changes or the user is deleted externally, the Rack Power Manager software will not see these changes until the next time the user logs in.

You may schedule a task that will automatically verify LDAP, Active Directory and NT external authentication servers to ensure that accounts are still valid; see *Task: Validating user accounts on an external authentication server* on page 272.

Authentication services may be managed only by Rack Power Manager software administrators and user administrators.

To display configured authentication services:

1. Click the *Users* tab.
2. Click *Authentication Services* in the top navigation bar. The User Authentication Services window will open.

The User Authentication Services window may be customized by using the Customize link. See *Using the Customize link in windows* on page 30.

To remove authentication services:

NOTE: The internal authentication service cannot be removed.

1. Click the *Users* tab.
2. Click *Authentication Services* in the top navigation bar. The User Authentication Services window will open.
3. Check the checkbox to the left of the authentication service(s) to delete. To delete all external authentication services on the page, check the checkbox to the left of Name at the top of the list.
4. Click *Delete*. A confirmation dialog box will appear.
5. Confirm or cancel the deletion.

Rack Power Manager software internal authentication service

To change the Rack Power Manager internal authentication service account policies:

1. Click the *Users* tab.

2. Click *Authentication Services* in the top navigation bar. The User Authentication Services window will open.
3. Click *RPM Internal*. The side navigation bar will change to include RPM Internal at the top and, below the name, the information you may define.
4. Click *Account Policies*. The Authentication Service User Account Policies - RPM Internal window will open.
5. Specify the password policies for the authentication service:
 - a. Type a number (from 1-64) in the Minimum Password Length field, or click the arrows to select a number.
 - b. Check the *Passwords Expire* checkbox to require a user to change the password after a certain number of days. Specify a number (from 1-365) in the Maximum Expiration (days) field, or select a number.
 - c. Select *Passwords must contain both alpha and numeric characters* if new passwords must contain at least one letter and one number.
 - d. Select *Passwords must contain both lower and upper case characters* if new passwords must contain at least one uppercase and one lowercase letter.

6. Specify the lockout policy for the authentication service:

To assign a specific number of user login attempts, check the *Lockout users after invalid login attempts* checkbox, then continue with step a.

If you leave this checkbox unchecked, unlimited user login attempts will be allowed. Skip to the last step.

- a. Type the number of allowable user login failures (from 1-25) in the Maximum Login Failures field, or select it from the menu.
- b. To permit user logins after a certain period of time, check the *Automatically unlock users after the lockout period* checkbox. Specify the lockout period (in minutes) by typing a number from 1-1,440 in the Maximum Lockout Period (minutes) field, or choose a value from the menu (1,440 minutes is equivalent to 24 hours).

If you leave this checkbox unchecked, locked user accounts must be manually unlocked by a Rack Power Manager software administrator or user administrator.

See *Unlocking User Accounts* on page 214.

7. Click *Save* and then click *Close*. The User Authentication Services window will open.

To change custom field labels for user accounts that use internal authentication:

1. Click the *Users* tab.
2. Click *Authentication Services* in the top navigation bar. The User Authentication Services window will open.
3. Click *RPM Internal*. The side navigation bar will change to include RPM Internal at the top and, below the name, information you may define.
4. Click *Custom Field Labels* in the side navigation bar. The Authentication Service User Account Custom Field Labels - RPM Internal window will open.
5. Type the text that you wish to appear in each of the six custom field labels.
6. Click *Save* and then click *Close*. The User Authentication Services window will open.

By default, the custom field labels do not display in the User Accounts - All window, but they may be added to the display (or added to the default display by an administrator), using the *Customize* link. See *Using the Customize link in windows* on page 30.

Active Directory external authentication service

NOTE: When adding an Active Directory external authentication service, you can allow trusted forests to be discovered. A forest is a group of domains, and a forest may have a trusted relationship with other forests. In some configurations, a user may belong to one forest but be assigned to groups in another forest. The Rack Power Manager server needs access to both forests to authenticate and authorize this user.

To add an Active Directory external authentication service:

1. Click the *Users* tab.
2. Click *Authentication Services* in the top navigation bar. The User Authentication Services window will open.
3. Click *Add*. The Add Authentication Service Wizard will appear.
4. The Provide Authentication Service Name and Type window will open.
 - a. Type a name for the external authentication service.
 - b. Select *Active Directory* from the menu.
 - c. Click *Next*.
5. The Specify Active Directory Connection Settings window will open.
 - a. Type the Active Directory domain name for the domain you wish to add in the AD Domain Name field.

- b. In the User Container field, specify the name of the container to search for user accounts. This will limit the search scope to that container. The name may be entered in several forms, optionally including a sub-domain. Valid forms are explained below by example.

Assume an Active Directory domain name of “sunrise.mycompany.com” with users in subfolder “sun/myusers.” The User Container field may be entered as:

Example 1 (no sub-domain): “sun.myusers”

Example 2 (no sub-domain): “ou=myusers,ou=sun”

If users are contained in a sub-domain such as “mktg.sunrise.mycompany.com”, valid forms are:

Example 1 (with sub-domain): “mktg.sunrise.mycompany.com/sun/myusers”

Example 2 (with sub-domain and no container specified):
“mktg.sunrise.mycompany.com/”

Example 3 (with sub-domain):
“ou=myusers,ou=sun,dc=mktg,dc=sunrise,dc=mycompany,dc=com”

- c. In the Group Container field, specify the name of the container to search for user groups. This will limit the search scope to that container. The name may be entered in several forms, optionally including a sub-domain. Valid forms are explained in step 5b above.
- d. In the Username Type menu, select the type of username. Each choice in the menu contains an example.

A Full Windows 2000 username is specified as username@domain.

A Partial Windows 2000 username is specified as username.

A Full Pre-Windows 2000 username is specified as domain\username.

A Partial Pre-Windows 2000 username is specified as username.

This option may only be configured for new authentication servers; it cannot be modified. Existing authentication servers are set to the Partial Windows 2000 Username type for compatibility.

- e. Specify a Secure Socket Layer (SSL) encryption mode:
- Click *Do Not Use SSL* to have authentication performed using unencrypted clear text instead of SSL encryption. This method is the least secure.
 - Click *Use SSL in Trust All Mode* to use SSL encryption for data transmission. All server certificates will be trusted and automatically accepted by the Rack Power

Manager software for transmitting data. This SSL method provides medium security.

This encryption mode is not recommended for wide area networks (WANs).

- Click *Use SSL in Certificate-based Trust Mode* to use SSL encryption for data transmission. The Rack Power Manager management software will approve the server and then the certificate before transmitting data. This SSL method provides maximum security.
- f. Click *Use Kerberos for User Authentication* to use the Kerberos protocol for authentication requests, including the browsing. If enabled, you must use DES encryption types for this account. If an account was created prior to Active Directory, the user's password must be changed after this setting is changed. In addition, the Active Directory server addresses must be resolvable to their host names via DNS.
When this is not checked, the LDAP protocol will be used.
- g. Click *Enable Chasing of Referrals* to allow the Active Directory server to refer Rack Power Manager software clients to additional directory servers.
- h. Specify the search mode:

Enable *Use Recursion to search groups* if you wish to have the AD service access the domain controller for the specified domain name. This search includes the "Member" attribute of ObjectClass=group. This search is recursive and finds nested groups. This search may be slow, depending on the number of groups and levels of nesting.

-or-

Enable *Use an Active Directory Global Catalog* to have the AD service access the global catalog for the specified domain name. The search includes the "TokenGroups" attribute of the ObjectClass=user. This search is faster but only retrieves the nested groups SIDs; subsequent calls must be made to find the group name and specific SIDs.

-or-

Enable *Use Windows 2003 Universal Group Caching* if you wish to have the AD service access the domain controller for the specified domain name. The search includes the "TokenGroups" attribute of the ObjectClass=user. This search is faster but only retrieves the nested groups SIDs; subsequent calls must be made to find the group name and specific SIDs. The Windows 2003 Universal Group Caching feature must be enabled in the Windows 2003 AD server.

- i. Click *Allow users and groups from newly discovered trusted forests* to allow logins by users that belong to the authentication service forest or its discovered trusted forests. If enabled, the Rack Power Manager will discover all trusted forests in the Active Directory service.

- j. Click *Next*.

If you selected *Use SSL in Certificate-based Trust Mode*, go to step 6.

If you selected *Do Not Use SSL* or *Use SSL in Trust All Mode*, go to step 8.

- 6. The Rack Power Manager server will try to find a server that has a trusted certificate chain (see *System certificate policy and trust store* on page 50). If no trusted certificate chain is found, then the Accept Certificate window will open and list all servers that belong to the domain. It will also list the reasons for rejection of the certificate chain.
- 7. Click *Next* to accept the certificate.
- 8. The Select Browsing Method window will open.

Click *Browse Anonymously* to browse users on the external Active Directory authentication server.

-or-

Click *Browse with user credentials* to browse users on the external Active Directory authentication based on credentials configured on the server. If this option is selected, do the following:

- a. Type the username for an Active Directory account that has browse rights in the User Name field. The login ID must be entered in case sensitive text if the Active Directory server is set up to use Kerberos. When using Kerberos, the browse account cannot be specified in the Full Pre-Windows 2000 Username form (domain\username). If the username is in a sub-domain of the Active Directory domain (specified in step 3a), then the username should be specified as <username>@<subdomain>.
- b. Type the password for an Active Directory account that has browse rights in the Password field.
- c. Click *Next*.
- 9. The Establish Connection with Authentication Service window will open briefly. If the external authentication service is added successfully, the Completed Successful window will open.
- 10. Click *Finish*. The User Authentication Services window will open with the new service listed.

NOTE: If the authentication service has trusted forests, the settings configured for the authentication service in the Add Authentication Service Wizard will be applied to the discovered trusted forests. However, the settings for each trusted forest can later be changed in the Authentication Service Connection Settings window.

See *User Authentication Services Window* on page 107 for more information about trusted forests.

To change settings for the Active Directory external authentication service:

1. Click the *Users* tab.
2. Click *Authentication Services* in the top navigation bar. The User Authentication Services window will open.
3. Click the name of the Active Directory (AD) service. The side navigation bar will change to include the name of the AD service at the top and, below the name, the information you may define.
4. Click *Connection* in the side navigation bar. The Authentication Service Connection Settings - AD window will open.
5. Type a name in the Service Name field to change the name of the service that appears in the Name column of the User Authentication Services window.
6. Type the domain name of the Active Directory service in the AD Domain Name field.
7. In the User Container field, specify the name of the container to search for user accounts. This will limit the search scope to that container. The name may be entered in several forms, optionally including a sub-domain. See *To add an Active Directory external authentication service:* on page 84 for an explanation of the valid forms.
8. In the Group Container field, specify the name of the container to search for user groups. This will limit the search scope to that container. The name may be entered in several forms, optionally including a sub-domain. See *To add an Active Directory external authentication service:* on page 84 for an explanation of the valid forms.
9. Specify a Secure Socket Layer (SSL) Encryption mode:
 - Click *Do Not Use SSL* to have authentication performed using unencrypted clear text instead of SSL encryption. This method is the least secure.
 - Click *Use SSL in Trust All Mode* to use SSL encryption for data transmission. All server certificates will be trusted and automatically accepted by the Rack Power Manager software for transmitting data. This SSL method provides medium security. This encryption mode is not recommended for wide area networks (WANs).

- Click *Use SSL in Certificate-based Trust Mode* to use SSL encryption for data transmission. The Rack Power Manager software will approve the server and then the certificate before transmitting data. This SSL method provides maximum security.-
10. Click *Use Kerberos for User Authentication* to use the Kerberos protocol for authentication requests, including the browsing. If enabled, you must use DES encryption types for this account. If an account was created prior to Active Directory, the user's password must be changed after this setting is changed. In addition, the Active Directory server addresses must be resolvable to their host names via DNS.

When this is not checked, the LDAP protocol will be used.

11. Click *Enable Chasing of Referrals* to allow the Active Directory server to refer Rack Power Manager software clients to additional directory servers.
12. Specify the search mode:

Enable *Use Recursion to search groups* if you wish to have the AD service access the domain controller for the specified domain name. This search includes the "Member" attribute of ObjectClass=group. This search is recursive and finds nested groups. This search may be slow, depending on the number of groups and levels of nesting.

-or-

Enable *Use an Active Directory Global Catalog* to have the AD service access the global catalog for the specified domain name. The search includes the "TokenGroups" attribute of the ObjectClass=user. This search is faster but only retrieves the nested groups SIDs; subsequent calls must be made to find the group name and specific SIDs.

-or-

Enable *Use Windows 2003 Universal Group Caching* if you wish to have the AD service access the domain controller for the specified domain name. The search includes the "TokenGroups" attribute of the ObjectClass=user. This search is faster but only retrieves the nested groups SIDs; subsequent calls must be made to find the group name and specific SIDs. The Windows 2003 Universal Group Caching feature must be enabled in the Windows 2003 AD server.

13. Click *Allow use of Users/Groups from Trusted Forests* to allow logins by users belonging to a forest that are assigned to groups in a different forest. If enabled, the Rack Power Manager will query all trusted forests in the Active Directory service to find the user and user groups to which the authenticated user belongs.

If you deselect *Allow use of Users/Groups from Trusted Forests*, any previously discovered trusted forests will be hidden from the User Authentication Services window and users belonging to trusted forests will not be permitted to log in.

14. Click *Save* to save your changes.
 - If you selected *Use SSL in Certificate-based Trust Mode*, the Certificates heading will appear in the side navigation bar. Go to step 13.
 - If you selected *Do Not Use SSL* or *Use SSL in Trust All Mode*, go to step 16.
15. Click *Certificates*. The Authentication Service Certificate Management - AD window opens and list all servers in that domain. A status of Trusted indicates the certificate is trusted, based on the certificate policy (see *System certificate policy and trust store* on page 50); Untrusted indicates the certificate cannot be trusted.
16. To register certificates:
 - a. To select one or more certificates, click the checkbox to the left of the server IP addresses. To select all certificates on the page, click the checkbox to the left of the IP Address heading.
 - b. Click *Register* above the IP Address list to register the certificates. The Accept SSL Certificate window will open.
 - c. Click *Save* to store the certificate values to the Rack Power Manager software database on the host or click *Close* if you do not wish to save the certificate values.

The Authentication Service Certificate Management window will open if only one certificate was selected. If more than one certificate was selected, each will appear in order in subsequent Accept SSL Certificate windows.
17. To unregister certificates:
 - a. To select one or more certificates, click the checkbox to the left of the server IP addresses. To unregister all certificates, click the checkbox to the left of the IP Address heading.
 - b. Click *Unregister* to unregister the certificates.
 - c. A confirmation message box will appear. Confirm or cancel the operation.
18. Click *Close*. The User Authentication Services window will open.

To change user browsing settings for the Active Directory external authentication service:

1. Click the *Users* tab.
2. Click *Authentication Services* in the top navigation bar. The User Authentication Services window will open.

3. Click the name of the AD service. The side navigation bar will change to include the name of the AD service at the top and, below the name, the information you may define.
4. From the side navigation bar, click *User Browsing*. The Authentication Service User Browsing - AD window will open.
5. Click *Browse Anonymously* to browse users on the external Active Directory authentication server.

-or-

Click *Browse with User Credentials* to browse users on the external Active Directory authentication based on credentials configured on the server. If this option is selected, do the following:

- a. Type the username for an Active Directory account that has browse rights in the User Name field. The log in ID must be entered in case sensitive text if the Active Directory server is set up to use Kerberos.
- b. Type the password for an Active Directory account that has browse rights in the Password field.

NOTE: The Rack Power Manager server verifies that the new credentials are valid for the AD service. If the credentials are invalid, an error message is displayed.

6. Click *Save* and then click *Close*. The User Authentication Services dialog box will appear.

Windows NT external authentication service

To add a Windows NT external authentication service:

1. Click the *Users* tab.
2. Click *Authentication Services* in the top navigation bar. The User Authentication Services window will open.
3. Click *Add*. The Add Authentication Service Wizard will appear.
4. The Provide Authentication Service Name and Type window will open.
 - a. Type a name for the external authentication service.
 - b. Select *Windows NT Domain* from the menu.
 - c. Click *Next*.
5. The Specify Windows NT Connection Settings window will open. Type the Windows NT domain name you wish to add in the Domain Name field, and then click *Next*.
6. The Select Browsing Method window will open.

Click *Browse Anonymously* to browse users on the external Windows NT authentication server.

-or-

Click *Browse with user credentials* to browse users on the external Windows NT authentication based on credentials configured on the server. If this option is selected, do the following:

- a. Type the username for a Windows NT account that has browse rights in the User Name field.
 - b. Type the password for a Windows NT account that has browse rights in the Password field.
 - c. Click *Next*.
7. The Establish Connection with Authentication Service window will briefly appear. If the external authentication service is added successfully, the Completed Successful window will open.
 8. Click *Finish*. The User Authentication Services window will open with the new service listed.

To change connection settings for the Windows NT external authentication service:

1. Click the *Users* tab.
2. Click *Authentication Services* in the top navigation bar. The User Authentication Services window will open.
3. Click the name of the Windows NT service. The side navigation bar will change to include the name of the service at the top and, below the name, the information you may define.
4. Click *Connection* in the side navigation bar. The Authentication Service Connection Settings - NT window will open.
5. Type a name in the Service Name field to change the name of the service that appears in the Name column of the User Authentication Services window.
6. Type the name of the Windows NT domain in the Domain Name field.
7. Click *Save* and then click *Close*. The User Authentication Services window will open.

To change user browsing settings for Windows NT external authentication services:

1. Click the *Users* tab.
2. Click *Authentication Services* in the top navigation bar. The User Authentication Services window will open.

3. Click the name of the Windows NT service. The side navigation bar will change to include the name of the Windows NT service at the top and, below the name, the information you may define.
4. Click *User Browsing* in the side navigation bar. The Authentication Service User Browsing - NT window will open.
5. Click *Browse Anonymously* to anonymously browse users on the external Windows NT authentication server.

-or-

Click *Browse with User Credentials* to browse users on the external Windows NT authentication based on credentials configured. If this option is selected, do the following:

- a. Type the username for an NT domain account that has browse rights in the User Name field.
 - b. Type the password for an NT domain account that has browse rights in the Password field.
6. Click *Save* and then click *Close*. The User Authentication Services dialog box will appear.

LDAP external authentication service

To add an LDAP external authentication service:

1. Click the *Users* tab.
2. Click *Authentication Services* in the top navigation bar. The User Authentication Services window will open.
3. Click *Add*. The Add Authentication Service Wizard will appear.
4. The Provide Authentication Service Name and Type window will open.
 - a. Type a name for the external authentication service.
 - b. Select *LDAP* from the Type menu.
 - c. Click *Next*.
5. The Specify LDAP Connection Settings window will open.
 - a. Type the address of the LDAP host in dot notation format (xxx.xxx.xxx.xxx) or type the DNS host name in the Host Address field.
 - b. Type the number of the port for connecting to the LDAP host in the Port Number field.
 - c. Specify an SSL encryption mode:

- Click *Do Not Use SSL* to have authentication performed using unencrypted clear text instead of SSL encryption. This method is the least secure and automatically sets the Port Number field to a default port number of 389.
- Click *Use SSL in Trust All Mode* to use SSL encryption for data transmission. All server certificates will be trusted and automatically accepted by the Rack Power Manager software for transmitting data. This SSL method provides medium security and automatically sets the Port Number field to a default port number of 636.

This encryption mode is not recommended for wide area networks (WANs).

Click *Use SSL in Certificate-based Trust Mode* to use SSL encryption for data transmission. The Rack Power Manager software will approve the server and then the certificate before transmitting data. This SSL method provides maximum security and automatically sets the Port Number field to a default port number of 636.

- d. Click *Enable Chasing of Referrals* if you wish to allow the LDAP server to refer Rack Power Manager software clients to additional directory servers.
- e. Click *Next*.

If you selected *Use SSL in Certificate-based Trust Mode*, go to step 6.

If you selected *Do Not Use SSL* or *Use SSL in Trust All Mode*, go to step 10.

6. The Rack Power Manager server will try to find a server that has a trusted certificate chain (see *System certificate policy and trust store* on page 50). If no trusted certificate chain is found, then the Accept Certificate window will open and list all servers that belong to the domain. It will also list the reasons for rejection of the certificate chain.
7. Click *Next* to accept the certificate.
8. The Specify LDAP User Schema window will open.
 - a. Type the Base distinguished name (DN) from which to begin searches. This is a required field unless the Directory Service has been configured to allow anonymous search. Each Search DN value must be separated by a comma.
 - b. Type the key attribute. The default value is common name (cn).
 - c. Type the object class. The default value is person.
 - d. Type the full name attribute. The default value is surname (sn).
 - e. Click *Next*.
9. The Specify LDAP Group Schema window will open.

- a. Type the Base distinguished name (DN) from which to begin searches. This is a required field unless the Directory Service has been configured to allow anonymous search. Each Search DN value must be separated by a comma.
 - b. Type the object class. The default value is group.
 - c. Type the member attribute. The default value is member.
 - d. Type the username member attribute (only the username, not the full LDAP object DN). The user's group membership will be located using this attribute in addition to the member attribute. This attribute is primarily used with NIS-like schemas.
 - e. Click *Next*.
10. The Select Browsing Method window will open.

Click *Browse Anonymously* to browse users on the external LDAP authentication server.

-or-

Click *Browse with user credentials* to browse users on the external LDAP authentication based on credentials configured on the server. If this option is selected, do the following:

 - a. Type a log in ID in the User Name field, in one of two forms: a fully qualified distinguished name or the username of an account in the base user DN.
 - b. Type the password for the LDAP user account in the Password field.
 - c. Click *Next*.
11. The Establish Connection with Authentication Service window will open briefly. If the external authentication service is added successfully, the Completed Successful window will open.
12. Click *Finish*. The User Authentication Services window will open with the new service listed.

To change connection settings for the LDAP external authentication service:

1. Click the *Users* tab.
2. Click *Authentication Services* in the top navigation bar. The User Authentication Services window will open.
3. Click the name of the LDAP service. The side navigation bar will change to include the name of the LDAP service at the top and, below the name, the information you may define.

4. Click *Connection* in the side navigation bar. The Authentication Service Connection Settings - LDAP window will open.
5. Type a name in the Service Name field to change the name of the service that appears in the Name column of the User Authentication Services window.
6. Type the address of the LDAP host, in dot notation format (xxx.xxx.xxx.xxx) in the Host Address field.
7. Type the number of the port you wish to use for connecting to the LDAP host in the Port Number field.
8. Specify a Secure Socket Layer (SSL) Encryption mode:
 - Click *Do Not Use SSL* to have authentication performed using unencrypted clear text instead of SSL encryption. This method is the least secure and automatically sets the Port Number field to a default port number of 389.
 - Click *Use SSL in Trust All Mode* to use SSL encryption for data transmission. All server certificates will be trusted and automatically accepted by the Rack Power Manager software for transmitting data. This SSL method provides medium security and automatically sets the Port Number field to a default port number of 636.

This encryption mode is not recommended for wide area networks (WANs).
 - Click *Use SSL in Certificate-based Trust Mode* to use SSL encryption for data transmission. The Rack Power Manager software will approve the server and then the certificate before transmitting data. This SSL method provides maximum security and automatically sets the Port Number field to a default port number of 636.
9. Click *Save* to save your changes.

If you selected *Use SSL in Certificate-based Trust Mode*, the Certificates heading will appear in the side navigation bar. Go to step 8.

If you selected *Do Not Use SSL* or *Use SSL in Trust All Mode*, go to step 15.
10. Click *Certificates*. The Authentication Service Certificate Management - LDAP window will open and list all servers that belong to the domain. A status of Trusted indicates the certificate is trusted, based on the certificate policy (see *System certificate policy and trust store* on page 50); Untrusted indicates the certificate cannot be trusted.
11. To register certificates, click the checkbox to the left of the server IP address(es). To select all server IP addresses on the page, click the checkbox to the left of the IP Address heading.
12. Click *Register* to register the certificates. The Accept SSL Certificate window will appear.

13. Click *Save* to store the certificate values to the Rack Power Manager software database on the host.

The Certificate Management window will open if only one certificate was selected. If more than one certificate was selected, each will appear in order in subsequent Accept SSL Certificate windows.

14. To unregister one or more certificates, check the checkbox to the left of the server IP address(es). To select all server IP addresses on the page, click the checkbox to the left of the IP Address heading.
15. Click *Unregister* to unregister the certificates.
16. A confirmation message box will appear. Confirm or cancel the operation.
17. Click *Close*. The User Authentication Services window will open.

To change user schema settings for the LDAP external authentication service:

1. Click the *Users* tab.
2. Click *Authentication Services* in the top navigation bar. The User Authentication Services window will open.
3. Click the name of the LDAP service. The side navigation bar will change to include the name of the LDAP service at the top and, below the name, the information you may define.
4. Click *Schema* in the side navigation bar. *Users* will automatically be selected and the Authentication Service User Schema - LDAP window will open.
5. Type the Base distinguished name (DN) from which to begin searches. This is a required field unless the Directory Service has been configured to allow anonymous search. Each Search DN value must be separated by a comma.
6. Type the key attribute. The default value is common name (cn).
7. Type the object class. The default value is person.
8. Type the full name attribute for the user. The default value is surname (sn).
9. Click *Save* and then click *Close*. The User Authentication Services dialog box will appear.

To change group schema settings for the LDAP external authentication service:

1. Click the *Users* tab.
2. Click *Authentication Services* in the top navigation bar. The User Authentication Services window will open.

3. Click the name of the LDAP service. The side navigation bar will change to include the name of the LDAP service at the top and, below the name, the information you may define.
4. Click *Schema* in the side navigation bar, and then click *Groups*. The Authentication Service Group Schema - LDAP window will open.
5. Type the Base distinguished name (DN) from which to begin searches. This is a required field unless the Directory Service has been configured to allow anonymous search.
6. Type the object class. The default value is *groupOfNames*.
7. Type the members attribute. The default value is *member*.
8. Type the username member attribute (only the username, not the full LDAP object DN). The user's group membership will be located using this attribute in addition to the member attribute. This attribute is primarily used with NIS-like schemas.
9. Click *Save* and then click *Close*. The User Authentication Services dialog box will appear.

To change user browsing settings for the LDAP external authentication service:

1. Click the *Users* tab.
2. Click *Authentication Services* in the top navigation bar. The User Authentication Services window will open.
3. Click the name of the LDAP service. The side navigation bar will change to include the name of the LDAP service at the top and, below the name, the information you may define.
4. Click *User Browsing* in the side navigation bar. The Authentication Service User Browsing - LDAP window will open.
5. Click *Browse Anonymously* to browse users on the external LDAP authentication server.

-or-

Click *Browse with User Credentials* to browse users on the external LDAP authentication based on credentials configured on the server. If this option is selected, do the following:

- a. Type a log in ID in the User Name field, in one of two forms: a fully qualified distinguished name or the username of an account in the base user DN.
 - b. Type the password for the LDAP user account in the *Password* field.
6. Click *Save* and then click *Close*. The User Authentication Services dialog box will appear.

RADIUS external authentication service

To add a RADIUS external authentication service:

1. On the RADIUS server that will be used as an external authentication service, add the Rack Power Manager server as a RADIUS client. Make a note of the configured shared secret and the available authentication type(s) on the RADIUS server.
2. From the Rack Power Manager Explorer, Click the *Users* tab.
3. Click *Authentication Services* in the top navigation bar. The User Authentication Services window will open.
4. Click *Add*. The Add Authentication Service Wizard will appear.
5. The Provide Authentication Service Name and Type window will open.
 - a. Type a 1-64 character name for the RADIUS authentication service.
 - b. Select *RADIUS* from the Type menu.
 - c. Click *Next*.
6. The Specify RADIUS Connection Settings window will open.
 - a. Type the address of the RADIUS host in dot notation format (xxx.xxx.xxx.xxx) or type the DNS host name in the Server Address field.
 - b. Type the number of the port (from 1-65535) for connecting to the RADIUS host in the Port Number field. The default is port 1812.
 - c. Click *Next*.
7. The Establish Connection with Authentication Service window will open briefly. If the external authentication service is contacted successfully, the Specify RADIUS Authentication Settings window will open.
 - a. Select the authentication type from the Authentication Type menu. Make sure it is one of the available authentication types noted in step 1.

PAP - Password Authentication Protocol
CHAP - Challenge Handshake Authentication Protocol (default)
MS-CHAP - Microsoft Challenge Handshake Authentication Protocol
MS-CHAP v2 - Microsoft Challenge Handshake Authentication Protocol
Version 2
 - b. In the Shared Secret field, type the shared secret (that was configured on the RADIUS server in step 1), which is a password protected field. Microsoft's implementation

allows up to 128 ASCII characters for the shared secret; other servers may have a different limit.

- c. Re-enter the shared secret in the Confirm Shared Secret field.
 - d. Click *Next*.
8. If the external authentication service is added successfully, the Completed Successful window will open.
 9. Click *Finish*. The User Authentication Services window will open with the new service listed.

To change settings for the RADIUS external authentication service:

1. Click the *Users* tab.
2. Click *Authentication Services* in the top navigation bar. The User Authentication Services window will open.
3. Click the name of the RADIUS service. The side navigation bar will change to include the name of the RADIUS service at the top and, below the name, the information you may define.
4. Click *Connection* in the side navigation bar. The Authentication Service Connection Settings - RADIUS window will open.
 - a. Type a 1-64 character name for the RADIUS authentication service.
 - b. Type the address of the RADIUS host in dot notation format (xxx.xxx.xxx.xxx) or type the DNS host name in the Server Address field.
 - c. Type the number of the port (from 1-65535) for connecting to the RADIUS host in the Port Number field. The default is port 1812.
 - d. Click *Save*.
5. To change the authentication type and/or shared secret, click *Settings* in the side navigation bar. The Authentication Service Authentication Settings - RADIUS window will open.
 - a. Select the authentication type from the Authentication Type menu.
 - PAP - Password Authentication Protocol
 - CHAP - Challenge Handshake Authentication Protocol (default)
 - MS-CHAP - Microsoft Challenge Handshake Authentication Protocol
 - MS-CHAP v2 - Microsoft Challenge Handshake Authentication Protocol Version 2

- b. In the Shared Secret field, type the shared secret, which is a password protected field. Microsoft's implementation allows up to 128 ASCII characters for the shared secret; other servers may have a different limit.
 - c. Re-enter the shared secret in the Confirm Shared Secret field.
 - d. Click *Save*.
6. Click *Close*. The User Authentication Services dialog box will appear.

TACACS+ external authentication service

Rack Power Manager software supports TACACS+ external authentication. Once the TACACS+ authentication service is added, you may map TACACS+ users to the Rack Power Manager software database by using the Add User Account wizard. The username added in the Rack Power Manager software should match the username configured in the TACACS+ server. For more information about adding users, see *Adding User Accounts* on page 211.

You may choose to associate users with internal Rack Power Manager software groups to control group level access rights. Or, you may choose to map users to external TACACS+ groups and control group level access rights using the TACACS+ service. There are two types of external TACACS+ groups that can be used: the TACACS+ standard privilege level attribute, or a custom group name attribute. To map users to external TACACS+ groups, use the Rack Power Manager software Add User Group wizard and specify the group type. For more information, see *Adding User-defined User Groups* on page 224.

To add a TACACS+ external authentication service:

1. On the TACACS+ server that will be used as an external authentication service, add the Rack Power Manager server as a TACACS+ client. Make a note of the configured shared secret and the available authentication type(s) on the TACACS+ server.
2. From the Rack Power Manager Explorer, Click the *Users* tab.
3. Click *Authentication Services* in the top navigation bar. The User Authentication Services window will open.
4. Click *Add*. The Add Authentication Service Wizard will appear.
5. The Provide Authentication Service Name and Type window will open.
 - a. Type a 1-64 character name for the TACACS+ authentication service.
 - b. Select *TACACS+* from the Type menu.
 - c. Click *Next*.
6. The Specify TACACS+ Connection Settings window will open.

- a. Type the address of the TACACS+ host or type the DNS host name in the Server Address field.
 - b. Type the number of the port (from 1-65535) connecting to the TACACS+ host in the Port Number field. The default port is 49.
 - c. Click *Next*.
7. The Establish Connection with Authentication Service window will open briefly. If the external authentication service is contacted successfully, the Specify TACACS+ Authentication Settings window will open.
 - a. Select the authentication type from the Authentication Type menu. Make sure it is one of the available authentication types noted in step 1.

PAP - Password Authentication Protocol
CHAP - Challenge Handshake Authentication Protocol (default)
MS-CHAP - Microsoft Challenge Handshake Authentication Protocol
 - b. In the Shared Secret field, type the shared secret (configured on the TACACS+ server in step 1), which is a password protected field. (For the shared secret, Microsoft's implementation allows up to 128 ASCII characters and Cisco's implementation allows up to 32 ASCII characters; other servers may have a different limit.)

NOTE: If you change the authentication type, you will be required to enter the shared secret.

- c. Re-enter the shared secret in the Confirm Shared Secret field.
 - d. Click *Next*.
8. The Specify TACACS+ Group Authorization Method window will open.
 - a. Click the corresponding radio button to choose one of the following options to manage group authorization:
 - RPM internal groups: Choose this option if you plan to associate TACACS+ users with Rack Power Manager software internal user groups.
 - TACACS+ privilege level attribute: Choose this option if you plan to associate TACACS+ users with external TACACS+ groups using the privilege level attribute.
 - TACACS+ custom attribute for group names: Choose this option if you plan to associate TACACS+ users with external TACACS+ groups using the custom group names attribute.
 - b. Click *Next*.

9. If you selected RPM internal groups and the external authentication service was added successfully, the Completed Successful window will open.

-or-

If you selected any other option, the Specify TACACS+ Server Group Authorization Settings window will open.

- a. In the Service field, type the appropriate TACACS+ service.

If you selected the privilege level attribute method in step 8, the default value shell will appear in the field by default.

If you selected the group name custom attribute method in step 8, the default value raccess will appear in the field by default.

- b. If the TACACS+ service requires a protocol for authorization requests, type the protocol in the Protocol field.

- c. In the Attribute Name field, type the attribute name that the Rack Power Manager server will receive after an authorization request.

If you selected the privilege level attribute method in step 8, the default value priv-lvl will appear by default.

If you selected the group name custom attribute method in step 8, the default value group_name will appear by default.

10. Click *Next*. If the external authentication service is added successfully, the Completed Successful window will open.

11. Click *Finish*. The User Authentication Services window will open with the new service listed.

To change settings for the TACACS+ external authentication service:

1. Click the *Users* tab.
2. Click *Authentication Services* in the top navigation bar. The User Authentication Services window will open.
3. Click the name of the TACACS+ service. The side navigation bar will change to include the name of the TACACS+ service at the top and, below the name, the information you may define.
4. Click *Connection* in the side navigation bar. The Authentication Service Connection Settings - TACACS+ window will open.
 - a. Type a 1-64 character name for the TACACS+ authentication service.

- b. Type the address of the TACACS+ host in dot notation format (xxx.xxx.xxx.xxx) or type the DNS host name in the Server Address field.
 - c. Type the number of the port (from 1-65535) for connecting to the TACACS+ host in the Port Number field. The default is port 49.
 - d. Click *Save*.
5. To change the authentication type and/or shared secret, click *Settings* in the side navigation bar. The Authentication Service Authentication Settings - TACACS+ window will open.
 - a. Select the authentication type from the Authentication Type menu.

PAP - Password Authentication Protocol
CHAP - Challenge Handshake Authentication Protocol (default)
MS-CHAP - Microsoft Challenge Handshake Authentication Protocol
 - b. In the Shared Secret field, type the shared secret, which is a password protected field. (For the shared secret, Microsoft's implementation allows up to 128 ASCII characters and Cisco's implementation allows up to 32 ASCII characters; other servers may have a different limit.)

NOTE: If you change the authentication type, you will be required to enter the shared secret.

- c. Re-enter the shared secret in the Confirm Shared Secret field.
 - d. Click *Save*.
6. To change the group authorization settings, click *Group Authorization* in the side navigation bar.

The Method field will display the group authorization method configured when the TACACS+ authentication service was added. This field cannot be changed.

 - a. In the Service field, type the appropriate TACACS+ service.

If TACACS+ privilege level attribute is the method, the default value is shell.
If TACACS+ custom attribute for group names is the method, the default value is raccess.
 - b. If the TACACS+ service requires a protocol for authorization requests, type the protocol in the Protocol field.
 - c. In the Attribute Name field, type the attribute name that the Rack Power Manager server will receive after an authorization request.

If TACACS+ privilege level attribute is the method, the default value is `priv-lvl`.

If TACACS+ custom attribute for group names is the method, the default value is `group_name`.

- d. Click *Save*.
7. Click *Close*. The User Authentication Services dialog box will appear.

RSA SecurID external authentication service

When an RSA SecurID external authentication service is added, the Rack Power Manager software obtains user authentication information and relays it to the RSA Authentication Manager. The RSA Authentication Manager's validation results are then relayed to the user. The Rack Power Manager software also supports new PIN operations, next tokencode operations, RSA Authentication Manager Replica functionality and name locking. The Rack Power Manager software is the agent type Net OS Agent.

See *RSA SecurID login* on page 11 for information about the login process when an RSA SecurID external authentication service is used. Consult the RSA Authentication Manager documentation for additional details.

For complete information about what is needed on the RSA server, see the RSA Secured Partner Solutions Directory on the RSA web site (rsasecurity.com).

To add an RSA SecurID external authentication service:

1. On the RSA server that will be used as an external authentication service, add the Rack Power Manager server as an RSA Agent Host.
2. From the Rack Power Manager Explorer, Click the *Users* tab.
3. Click *Authentication Services* in the top navigation bar. The User Authentication Services window will open.
4. Click *Add*. The Add Authentication Service Wizard will appear.
5. The Provide Authentication Service Name and Type window will open.
 - a. In the Name field, type a 1-64 character name for the RSA authentication service.
 - b. Select *RSA SecurID* from the Type menu.
 - c. Click *Next*.
6. The Specify RSA SecurID Connection Settings window will open. Type the 1-512 character path to the `sdconf.rec` file, or browse to the file location. (This file is created by

the RSA Authentication Manager, but is located on the Rack Power Manager software client machine.) Then, click *Next*.

The `sdconf.rec` file will be uploaded from the Rack Power Manager software client to the Rack Power Manager server. This file will be used as the initial RSA configuration file for all Rack Power Manager software servers.

If some Rack Power Manager servers require a different configuration, a different `sdconf.rec` file must be configured. Additionally, some installations may require an advanced option file (`sdopts.rec`) for load balancing. You may specify these files using the procedure to change settings for the RSA SecurID external authentication service.

7. The Establish Connection with Authentication Service window will open briefly. If the external authentication service is added successfully, the Completed Successful window will open.

Click *Finish*. The User Authentication Services window will open with the new service listed.

After the service is added, one or more RSA user accounts must be added to the Rack Power Manager software.

NOTE: The node secret file for the server will not be created until the first RSA user logs into the Rack Power Manager software.

To change settings for the RSA SecurID external authentication service:

1. Click the *Users* tab.
2. Click *Authentication Services* in the top navigation bar. The User Authentication Services window will open.
3. Click on the name of the SecurID service.
4. Click *Connection* in the side navigation bar. The Authentication Service Connection Settings window will open.
5. To change the name of the service:
 - a. Type a 1-64 character name in the Service Name field.
 - b. Click *Save*.
 - c. If that is the only change you are entering, click *Close*. Otherwise, continue with the next steps.
6. To clear the RSA SecurID node secret for one or more Rack Power Manager servers:
 - a. Click the checkbox to the left of the server name. To select all Rack Power Manager servers on the page, click the checkbox to the left of RPM Server at the top of the list.

- b. Click *Clear Node Secret*. A confirmation dialog box will appear.
 - c. Confirm or cancel the operation.
7. To update the RSA configuration files used by one or more Rack Power Manager servers to communicate with the RSA Authentication Manager software:
 - a. Click the checkbox to the left of the server name. To select all Rack Power Manager servers on the page, click the checkbox to the left of RPM Server at the top of the list.
 - b. Click *Update*. The Update RSA Configuration File window will open.
 - c. To change the `sdconf.rec` configuration file, enter the path in the `sdconf.rec` field or browse to the location.
 - d. To specify the advanced option `sdopts.rec` file for manual load balancing, enter the path in the `sdopts.rec` field or browse to the location.
 - e. Click *Save* and then click *Close*.

The RPM Service may need to be restarted when the RSA configuration is updated

User Authentication Services Window

Once added, the authentication services are listed in the User Authentication Services window. To view the window, click the *User* tab, then click *Authentication Services*. The authentication service name, type, enabled status and host name are displayed in the list.

If *Allow users and groups from newly discovered trusted forests* is enabled for an AD service, the discovered forests are displayed as a subset of the primary authentication service in the User Authentication Services window. The type is displayed as Active Directory - Trusted Forest.

The Enabled column displays a value of Yes or No. If the value is Yes, the users and groups of the authentication service are considered when the Rack Power Manager server attempts to authenticate and authorize a user; if the value is No, the authentication service is ignored. If the same username exists in multiple authentication services, you can use the Enabled status to control which authentication service will be used to find a user.

To enable or disable an authentication service:

1. Click the *User* tab, then click *Authentication Services* to open the User Authentication Services window.
2. Select the checkbox next to the authentication service you want to enable or disable.
3. To enable the trusted forest, click *Enable*.

-or-

To disable the trusted forest service, click *Disable*.

NOTE: All new authentication services are enabled by default, with the exception of new trusted forests which are disabled by default.

To refresh trusted forests:

NOTE: Refresh Trusted Forests is only applicable for Active Directory services for which discovering trusted forests was enabled.

1. Click the *User* tab, then click *Authentication Services* to open the User Authentication Services window.
2. Select the checkbox next to the primary AD authentication service.
3. Click *Refresh Trusted Forests*. New trusted forests are displayed in the list.

Units View Windows

Units View windows display list of units that have been added to the Rack Power Manager software database.

A user must have unit view access rights to open Units View windows; see *About Access Rights* on page 143.

Units are displayed in a table format with column headings. Use the checkbox to the left of each unit name to select/deselect the unit for an operation. To select all the units on a page, click the checkbox at the left of all the column headings at the top of the list - this is usually to the left of the Name column. Clicking this Select All checkbox will automatically enable the checkboxes for all units on that page. To deselect items that were previously selected, click on the checkbox.

When you click the checkbox at the top of the list, all units on the current page are selected (or deselected if they were previously all selected). If the list of units spans more than one page, units on subsequent pages will not be selected. You can specify how many items will appear on a Units View page (that is, the number of rows); see *Using the Customize link in windows* on page 30.

Types of Units View windows

There are four types of Units View windows, which are accessed by clicking tabs and side navigation bar links. Additional Units View windows may be added by plug-ins; see the plug-in documentation for more information. For information about using the collapse/expand icons in the side navigation bar, see *Using the Side Navigation Bar* on page 28.

Any Units View window that contains managed appliances may also be viewed using the topology feature, which displays a hierarchical structure; see *Topology view* on page 110.

- **All Appliances:** The Appliances - All window lists all managed appliances.
- **Appliance Type:** Appliance Type windows list all managed appliances of a particular type (for example, PM 3000 24 outlet switch). The Appliance Type links in the side navigation bar are listed under Appliances - All.

An appliance type will only be listed in the side navigation bar if an appliance of that type has been added to the Rack Power Manager software database and the user has access to it. For example, if a PM 3000 24 outlet switch has not been added, that type will not appear in the side navigation bar.

- **Mixed Views:** Mixed view windows may contain managed appliances, target devices or both. Several links in the side navigation bar will open mixed view Units View windows.
 - Recently Accessed - Units that the user has accessed most recently.
 - Groups - Units that have been assigned to a personal or global unit group.
 - Sites - Units that have been assigned to a site.
 - Departments - Units that have been assigned to a department.
 - Locations - Units that have been assigned to a location.
 - Custom fields - Units that have been assigned to custom groups. These group names may also have custom field labels.

See the *Units View Windows* on page 109 chapter for information about creating and managing groups.

Topology view

Units View windows that contain managed appliances support a topology feature that can be enabled/disabled. A topology view is a series of parent-child hierarchies. A parent is a managed appliance; children can be target devices, cascade switches (with target device children of their own) and power control devices (with socket children of their own).

When the topology feature is enabled in a Units View window that contains appliances, an arrow will appear next to each appliance. This arrow can be used to expand (open) an appliance display to list all the appliance ports. A Port column will be added next to the Name column. The port value is the port number on the appliance (or “SPC” if a power device is attached to an SPC port on a DSR switch), the port number on a cascaded switch or the socket number on a cascaded power device (for example, A1). By default, the topology view sorts by the Port column. The Port column is sorted by type, number and then unit name.

Expanding and collapsing the display follows the same rules as the side navigation bar. If the arrow is pointing right, clicking it causes the children to be displayed (expanding/opening the item). If the arrow is pointing down, clicking it causes the children to be hidden (collapsing/closing the item).

If a port has a cascade switch or power control device attached, the unit name for that port will include an arrow that can be used to expand/collapse the display of either all the ports on the cascade switch or all the sockets on the power control device.

Ports on an appliance or a cascade switch that do not have units attached are also listed. The Status column will indicate No Device Attached and the Type column will indicate the default valid connection type for that port. The Action column will indicate Attach Device; see the procedure in this section for how to attach device from this link.

If a target device is connected to multiple managed appliances, it will appear multiple times in a topology view. If you select one occurrence of an item, all other occurrences are also selected.

If you expand a display and select one or more child items, collapsing the display will hide those children and deselect them.

The Select All checkbox at the top of the list will only select displayed items on the current page. Items that are hidden in a collapsed unit cannot be selected with the Select All checkbox.

In a topology view, the number of items per page value applies to appliances and children, even if the display is collapsed and the children are not visible. You may also specify that the topology view expand automatically when the Topology button is clicked. See *Using the Customize link in windows* on page 30.

If you filter the display (see *Filtering information in a window* on page 29), and a child matches the filter criteria, the parent(s) automatically open. If only an appliance matches the filter criteria, the appliance is closed (unless the Expand View Automatically option is enabled).

To enable or disable a topology view:

In a Units View window (see *Accessing Units View windows* on page 111), click *Topology*.

Although you can enable the topology view in all Units View windows, it is only meaningful in windows that contain managed appliances (parent units that have children). If you enable topology view in a Units View window that contains only target devices, the only change will be the addition of the Port column to the display.

Accessing Units View windows

To enable a topology view in a Units View window, click *Topology* (see *Topology view* on page 110).

To access Units View windows:

Click the *Units* tab.

- To display managed appliances:

- a. Click *Appliances* in the side navigation bar. The Appliances - All window will open.
- b. To display an Appliance Type window, click one of the appliance type links in the side navigation bar.
- To display a list of units that you have accessed most recently, click *Recently Accessed* in the side navigation bar.
- To display units by groupings (if available), click the link in the side navigation bar.
 - Click *Sites* to open the Units in Sites window.
 - Click *Departments* to open the Units in Departments window.
 - Click *Locations* to open the Units in Locations window.
 - Click *Custom Field Labels* to display the Units in Custom Field window.

Showing and hiding units

Hiding turns off the display of units in the window, but does not remove the units from the Rack Power Manager software system.

To hide a unit:

1. In a Units View window (see *Accessing Units View windows* on page 111), click *Customize*. The Units View Customization window will open.
2. Click *Visibility* in the Available Fields column and then click *Add*. Visibility will be moved to the Fields to Show column.
3. Enable the *Show hidden items* checkbox if you wish to display hidden units in the Units View Customization window with a transparent icon.
4. Click *Save* and then click *Close*. The window will open, containing the Visibility column. The Visibility column will display Hide for each unit.
5. Click *Hide* for each unit.

The display of the selected unit will be turned off in the Units View window if *Show hidden items* was not selected in the Units View Customization window.

If *Show hidden items* was selected, the hidden unit will appear with a transparent icon.

To hide multiple units with one operation:

1. In a Units View window (see *Accessing Units View windows* on page 111), click the checkbox next to the units you want to hide from display. To select all units on the page, click the checkbox to the left of Name at the top of the list.
2. Click *Operations*, then select *Hide Units* from the drop-down menu.

To show hidden units:

1. In a Units View window (see *Accessing Units View windows* on page 111) click *Customize*. The Units View Customization window will open.
2. Click *Visibility* in the Available Fields column and then click *Add*. Visibility will be moved to the Fields to Show column.
3. Click *Show hidden items*.
4. Click *Save* and then click *Close*. The Units View window will open, containing the hidden items and the Visibility column. Hidden items will have a transparent icon and the Visibility field will contain Show.
5. Click *Show* in the Visibility column for the unit(s) you want to display. The unit will be made visible, the icon will no longer be transparent and the Visibility field will change to Hide.

Units View windows fields

The following fields may appear in Units View windows. You may enable or disable a field's display using the Customize link. See *Using the Customize link in windows* on page 30.

- Name in Appliance - Name of the unit as defined in the appliance. Click on the name to display or change unit information.
- Name in RPM - Name of the unit as defined in the Rack Power Manager software database.
- Type - Type of managed appliance model. Managed appliance types cannot be changed; to assign a type to a target device, see *Unit Overview Windows* on page 116.
- Status - Current activity level of a unit. Table 8.1 lists and describes the possible values.

Table 8.1: Unit Status Values

Unit type	Status and Icon	Icon	Description
Any unit	Idle	N/A	The unit is powered up with no connection.
Any unit	In Use		The unit has at least one active connection.
Any unit	Status Unknown		The status of the unit was reported to the software but cannot be obtained for an unknown reason.
Managed appliances	Not Responding		The managed appliance did not provide status information. This may occur for multiple reasons, such as the appliance is not powered up or it is disconnected from the Rack Power Manager software system.

- Action - Type of session that may be initiated. Although a unit may have multiple actions that may be performed, only one action will be displayed.

NOTE: Actions are also available from Connections windows.

Table 8.2: Action Links

Action link	Displays	Valid for*
<Connection Name>	Session interface	Appliances and/or TDs supported by plug-ins that define this connection type.

* In addition to the units listed in this column, one or more of these connection types may be valid for units supported by plug-ins. See the plug-in documentation for details.

- Site - See *Site, Department and Location Groups* on page 177.
- Browser URL - URL that may be used to access a target device, EVR1500 environmental monitor or generic appliance. This field will be empty if a URL is not available.
- Custom Field 1-3 - Custom fields assigned to units. If these fields have been defined with new names, the defined names will appear instead of the place holder names (Custom Field 1, Custom Field 2 and so on). See *Custom Fields* on page 180.
- Department - See *Site, Department and Location Groups* on page 177.
- RPM Software Server - Name of the server associated with the units.
- Location - Location assigned to the units. See *Site, Department and Location Groups* on page 177.
- Model Number - See *Unit Properties* on page 136.
- Part Number - See *Unit Properties* on page 136.
- Primary Contact, Primary Contact Phone, Secondary Contact and Secondary Contact Phone - Name and phone number of person(s) responsible for a unit. See *Unit Properties* on page 136.
- Serial Number - See *Unit Properties* on page 136.
- Telnet Port - Port number used for a Telnet connection to a target device. See *Unit Properties* on page 136.
- Visibility - Whether to display (Show) or not display (Hide) a unit in the Units View windows. See *Showing and hiding units* on page 112.

- Secure Mode - Displays a locked icon if secure mode is enabled on an appliance or an unlocked icon if it is not. Secure mode is set when an appliance is added (see *Adding Units* on page 119) and can be changed from the Operations menu (see *Managed Appliance Settings* on page 145).

NOTE: WebUI status and DHCP status fields are also available for supported DSR switches; see the DSR switch plug-in help for more information.

Multiple unit operations from a Units View window

From a Units View window, you may delete one or more units (see *Deleting Units* on page 124) or assign access rights for one or more units (see *About Access Rights* on page 143).

You may also use the Operations button/menu to initiate certain actions on one or more units.

- Hiding units from view - see *Showing and hiding units* on page 112
- Reboot - see *Importing data* on page 254
- Show version - see *Managed Appliance Settings* on page 145
- Push or pull names to/from the appliance - see *Manual name push* on page 128 and *Manual name pull* on page 128
- Wall power on, off or cycle - see *Power Device Sockets* on page 160
- Change unit properties - see *Unit Properties* on page 136

Custom operations defined in plug-ins may also be listed in the Operations menu.

A given action will be available only if at least one of the selected units supports the action. If a selected unit does not support the operation, it will be reported as such in the results window.

When one of these multiple unit operations is initiated and confirmed (if needed), a system task is created that will perform the operation on each unit. The Multiple Unit Operation window will open, indicating the operation has been submitted. This window contains a link that directs the user to the Operations Results window for the task.

To initiate and view results from multiple unit operations from a Units View window:

1. In a Units View window (see *Accessing Units View windows* on page 111), initiate the multiple unit operation as described in the procedures referenced above. If prompted, confirm the operation.
2. The Multiple Unit Operation window will open, indicating the operation has been submitted.

If you do not want to view the results of the operation, click *Close* and skip the rest of this procedure.

To view the results of the operation, click *Click here to view results*.

3. The Operations Results window will open, listing all multiple unit operations and any unit tasks that have been initiated (see *Using Tasks* on page 261). The entry for each operation includes:

- Name of the operation
- When the operation started
- When the operation finished (blank if not yet complete)
- Status or result of the operation

You may also access this window at any time by clicking the *Units* tab, then clicking *Operation Results* in the side navigation bar.

4. To view the results for an individual operation, click on the name. The Operation Results window for that operation type will open, indicating:
 - Status - Current status of the task
 - Summary - Number of successful/failed/total unit operations (for example, the summary of an operation with a status of 'Rebooting the unit(s)' might contain a 2/0/3 summary - 2 successful, 0 failed and 3 total units)
 - Name of the operation
 - Type of unit
 - When the operation started
 - How long the operation took
 - Status or result of the operation on the unit
5. Click *Close*.

Unit Overview Windows

The Unit Overview window contains the following information about an individual unit:

- Target Devices - Name, type and icon associated with the target device. You may also use this window to connect to the target device. The available connection methods are determined by the type of target device.

Power information appears only if the target device is a power device and the user has power control rights. In this case, the user may power up, power down or cycle the power of the target device.

- **Managed appliances** - Name and type of managed appliances and the tools that may be used to:
 - Reboot
 - Upgrade firmware
 - Resynchronize
 - Save or restore the configuration
 - Save or restore the user database

The available tasks depend on the type of managed appliance and the user's access rights on the managed appliance. (Custom tools defined by a plug-in may also be available.)

You may change the overview information for one target device from a Unit Overview window. From a Units View window, you can change the type or icon for several target devices in one operation. This may be helpful when you want to assign the same values to several units. See *Unit Properties* on page 136.

Other types of Unit Overview windows may be supported by plug-ins; see the plug-in documentation for more information.

To change the name of a managed appliance from the Unit Overview window:

1. In a Units View window containing appliances (see *Accessing Units View windows* on page 111), click on the name of an appliance. The Unit Overview window will open.
2. Type a name for the managed appliance. (You cannot change the type.)
3. Click *Save* and then click *Close*. The Units View window will open.

Unit Status Window

To use the Unit Status window:

1. Click the *Units* tab, then click *Unit Status* in the side navigation bar.
2. The Unit Status window opens.
3. You can filter what units are displayed by selecting a status from the Filter menu. Each unit status is color-coded. The default filtered status is Active Status which displays only currently active units.
4. You can select how often the Unit Status is updated by selecting a time from the Interval menu.

5. You can view the Unit Overview window by double-clicking the unit name, or right-clicking the unit name and selecting *Show Unit Overview*.

Adding and Deleting Units

This chapter describes how to add and delete units in the Rack Power Manager management software.

Adding Units

You may add:

- A single managed appliance
- Multiple managed appliances based on a range of IP addresses
- A generic appliance

When a managed appliance is added, Rack Power Manager software administrator, user administrator and appliance administrator privileges are automatically assigned to the managed appliance. A user with any of these privileges may:

- Reboot a managed appliance and disconnect sessions
- Administer local user accounts on the managed appliance
- Control outlet power

Appliance administrators and Rack Power Manager software administrators may also Flash upgrade a managed appliance and configure settings for a managed appliance.

Managed appliance rights may be changed. See *About Access Rights* on page 143.

The applicable X.509 certificate is automatically copied from the Rack Power Manager software to the unit being added. A certificate is a unique identifier of an individual managed appliance. (EVR1500 environmental monitors and generic appliances do not support certificates and may be added to multiple Rack Power Manager software systems.)

IPv4 and IPv6 network protocols

The Rack Power Manager software is a dual stack host that simultaneously supports both IPv4 and IPv6 network protocols.

NOTE: IPv6 is not supported by all appliance models. See the corresponding product or plug-in documentation for a list of specific appliance models that support IPv6.

Wizards that add units

In a Units View window, clicking *Add* invokes a wizard that guides you through the process of adding managed appliances and target devices to the Rack Power Manager software system. The units that are visible in the current Units View window determines which wizard will be invoked when you click *Add*.

- If you are in the Appliances - All window, you can add managed appliances of any type. You cannot add target devices from that window.
- If you are in the Units View window for a specific appliance type (such as PDUs - PM3000), you can only add more appliances of that type (PM3000 PDUs). You cannot add appliances of any other type or any target devices.
- If you are in the Recently Accessed window, you can add a managed appliance.

When a unit is added to the Rack Power Manager software database, it is also added to the current Units View. For example, if you are viewing units in the department named Accounting and click *Add*, the newly added unit will automatically be added to the Accounting department.

Adding a single managed appliance

To add a single managed appliance:

1. In a Units View window containing managed appliances (see *Accessing Units View windows* on page 111), click *Add*. The Add Appliance Wizard opens.
2. If you were not in an appliance type Units View window when you clicked *Add* in the first step, the Select Appliance Type window opens. Select *Add a single appliance by type*, then select a managed appliance from the product list. Click *Next*.

If you were in an appliance type Units View window when you clicked *Add* in the first step, go to the next step.

3. Enter the IP address for the appliance in the field provided.

If the appliance has already been configured with this IP address, click *Next*.

-or-

If the appliance has not yet been configured with an IP address, select *Appliance does not have an IP address assigned yet*. Complete the following steps:

- a. Plug in the appliance and turn it on.
 - b. (IPv4 addresses) Type the subnet mask in the field provided.
 - c. Enter a gateway in the field provided.
 - d. (IPv6 addresses) Select the prefix length from the menu. The preset value is 64 bits.
 - e. Click *Next*.
4. The Select Options window will open. (For more information about the options that affect adding target devices connected to the appliance, see *Topology Synchronization* on page 129.)

For appliances supported by plug-ins, the content of this window may differ; see the appropriate documentation.

- a. Enable the *Enable secure mode* checkbox if you want the managed appliance to only be accessible by this Rack Power Manager software system. In non-secure mode, the managed appliance may be added to multiple Rack Power Manager software systems.

This checkbox will not appear when adding a PM3000, which may only be added in Secure mode.
 - b. Under *Allow target devices that contain default names to be added for these type of connections*, you may enable the checkboxes for one or more connection types. Any target devices that contain default names in the managed appliance and support the enabled connection type in the managed appliance will be added to the Rack Power Manager software database.
 - c. Click *Next*.
5. If automatic inheritance is enabled, the Select Group(s) to Inherit window opens. Select the groups to which the appliance will belong and click *Add*. Attached target devices will inherit these group memberships. Click *Next*. For more information, see *Automatic Inheritance for Group Memberships and Properties* on page 131.

-or-

If you do not want to select groups at this time, click *Do not inherit group membership*.

6. The Apply Configuration Template window opens.

If you want to apply a configuration template to the appliance, select a template from the list and click *Next*.

-or-

If you do not want to apply a configuration template to the appliance, select *None* and click *Next*.

NOTE: For more information about configuration templates, see *Appliance Configuration Templates* on page 133.

7. Click *Finish*.

Adding managed appliances from a range or list of IP addresses

To add a managed appliance from a range or list of IP addresses:

1. In a Units View window containing managed appliances (see *Accessing Units View windows* on page 111), click *Add*. The Add Appliance Wizard will open.
2. The Select Add Unit Procedure window will open.
3. To enter IP addresses as a delimited list, click *Add multiple appliances*, then click *Next*. Enter IPv4 and/or IPv6 addresses, separated by either a comma (,) or a semi-colon (;).

-or-

To enter an IP address range, click *Discover appliances on the network from an IPv4 address range or an IPv6 subnet*, then click *Next*. Select *Use IPv4 address range* and type the IP address from which to begin and end the search in the corresponding fields, or select *Use IPv6 subnet* and type the IPv6 network prefix in the corresponding field. Click *Next*.

4. The Rack Power Manager software will search for managed appliances within the IP address range. When the search is completed, the Select Appliances to Add window will open, listing the results.
5. Add or remove appliances.
 - To add one or more managed appliances, select the managed appliances in the Appliances found list, then click *Add*. The managed appliances will be moved to the Appliances to Add list.
 - To remove one or more managed appliances, select the managed appliances in the Appliances to Add list, then click *Remove*. The managed appliances will be moved to the Appliances found list.

Click *Next*.

6. The Select Options window will open. (For more information about the options that affect adding target devices connected to the appliance, see *Topology Synchronization* on page 129.)

For appliances that are supported by plug-ins, the content of this window may differ; see the appropriate documentation.

- a. Click *Enable secure mode* if you want the managed appliance to only be accessible by this Rack Power Manager software system. In non-secure mode, the managed appliance may be added to multiple Rack Power Manager software systems.

NOTE: For appliances that require Secure mode, this checkbox will not be visible and the appliance will enable Secure mode automatically.

- b. Click *Next*.

7. The Adding Appliances window will open while the selected managed appliances are added to the Rack Power Manager software system.
8. The Apply Configuration Template window opens.

If you want to apply a configuration template to the appliance, select a template from the list and click *Next*.

-or-

If you do not want to apply a configuration template to the appliance, select *None* and click *Next*.

NOTE: For more information about configuration templates, see *Appliance Configuration Templates* on page 133.

9. Click *Finish*.

Adding a generic appliance

To add a generic appliance:

1. Click *Add* in a Units View window. The Add Unit Wizard will open.
2. The Select Add Unit Procedure window will open. Click *Add a single appliance*, then click *Next*.
3. The Select Appliance Type window will open. Select *Generic* from the product list, then click *Next*.
4. A Configure Generic Appliance Settings window will open.
 - a. Type the name.
 - b. Type either the address or the fully qualified domain name.
 - c. Type the Telnet port.
 - d. Type the web browser URL.
 - e. Click *Next*.

5. Click *Finish*.

Deleting Units

When you delete a unit, it is removed from the Rack Power Manager software database, and all associated connections will also be deleted.

You may also choose to delete target devices that are no longer connected when you run the Resync Wizard; see *Topology synchronization options in the Resync Wizard* on page 130.

To delete a power device, see *Power Devices* on page 157.

To delete a unit:

1. In a Units View window (see *Accessing Units View windows* on page 111), click the checkbox next to the unit name. To delete all units on the page, click the checkbox to the left of Name at the top of the list.
2. Click *Delete*. You are prompted to confirm the deletion.
3. Confirm or cancel the deletion.

Automatically deleting attached units

For target devices exclusively managed by a single appliance, you may specify that the target devices are automatically deleted when the managing appliance is deleted.

To modify target device delete policy settings:

1. Click the *System* tab.
2. Click *Global Properties* in the top navigation bar. Click *Units*, then click *Deletion* in the side navigation bar.

Synchronizing the Rack Power Manager Software Database

This chapter describes how to synchronize the Rack Power Manager software database with changes that occur on units.

Name Synchronization

Units and connections in the Rack Power Manager software system have a “Name in RPM”, which is the name stored in the Rack Power Manager software database. Some units (target devices, power devices and power device sockets) may also have a “Name in Appliance,” which is the name stored in the managed appliance.

The Rack Power Manager software name synchronization feature will “push” and/or “pull” names. You may enable the name push and name pull operations to run automatically. You may also push and pull names manually.

Name push

When the name of a cascade device is changed in the Rack Power Manager software database, a push operation will update the cascade device and power device socket names in the appliance.

Name pull

When the name of a cascade device or power device socket is changed in a managed appliance, a pull operation will update the cascade device name in the Rack Power Manager software database.

You may enable/disable automatic name push and automatic name pull. You may also manually initiate a push or pull operation at any time.

Automatic name push

When automatic name push is enabled, the name push operation occurs automatically when a name is changed in the Rack Power Manager software.

Table 10.1: Automatic Name Push Operation Effects

Unit	Effect
Appliance serial ports	If the target device for the serial port in the Rack Power Manager software database has a single appliance connection, the target device name will be pushed to the appliance. If the target device for the serial port in the Rack Power Manager software database has multiple appliance connections, the target device name will be pushed to the appliance for each appliance connection (for connection type(s) enabled in the Automatic Name Push Properties window).
Power devices	The power device name in the Rack Power Manager software database will be pushed to the appliance.
Power device sockets	If the target device for the power device socket in the Rack Power Manager software database has a single appliance connection, the target device name will be pushed to the appliance. If the target device for the power device socket in the Rack Power Manager software database has multiple appliance connections, the target device name will be pushed to each appliance for each appliance connection (for connection type(s) enabled in the Automatic Name Push Properties window).

To enable or disable automatic name push:

1. Click the *System* tab.
2. Click *Global Properties* in the top navigation bar.
3. Click *Units - Synchronization* in the side navigation bar, then click *Auto Name Push*.
4. The Automatic Name Push Properties window will open. To enable automatic name push, enable the *Push Names from RPM to appliances automatically* checkbox.

To disable automatic name push, disable the *Push Names from RPM to appliances automatically* checkbox and go to the last step.
5. Enable the checkboxes for one or more appliance connection types. The name in the Rack Power Manager software will be pushed to the appliance if the target device has a connection that matches the selected type.
6. Click *Save*.

Automatic name pull

When automatic name pull is enabled, the name pull operation occurs automatically when an appliance name is changed.

Table 10.2: Automatic Name Pull Operation Effects

Unit	Effect
Appliance serial ports	If the target device for the serial port in the Rack Power Manager software database has a single appliance connection, the target device name will be pulled from the appliance to update the target device name in the Rack Power Manager software database. If the target device for the serial port in the Rack Power Manager software database has multiple appliance connections, the target device name will be pulled from one of the appliance connections (based on the configured connection type priority) to update the target device name in the Rack Power Manager software database.
Power devices	The power device name will be pulled from the appliance to update the power device name in the Rack Power Manager software database.
Power device sockets	If the target device for the power device socket in the Rack Power Manager software database has a single appliance connection, the target device name will be pulled from the appliance to update the target device name in the Rack Power Manager software database. If the target device for the power device socket in the Rack Power Manager software database has multiple appliance connections, the target device name will be pulled from one of the appliance connections (based on the configured connection type priority) to update the target device name in the Rack Power Manager software database.

The following sections describe how to change a unit's Name in Appliance:

- Power device - see *Power Devices* on page 157
- Power device socket - see *Power Device Sockets* on page 160

To enable or disable automatic name pull:

1. Click the *System* tab.
2. Click *Global Properties* in the top navigation bar.
3. Click *Units - Synchronization* in the side navigation bar, then click *Auto Name Pull*.
4. The Automatic Name Pull Properties window will open. To enable automatic name pull, enable the *Pull Names from appliances to Rack Power Manager automatically* checkbox.
To disable automatic name pull, disable the *Pull Names from appliances to Rack Power Manager automatically* checkbox and go to the last step.
5. For target devices that have multiple connections, you may set the connection type priority by using the arrows to re-order the available types. This order determines which target device name will be pulled from one or more appliances to update the Rack Power Manager software database. The name will be pulled from only one appliance.
6. Click *Save*.

Manual name push

You may initiate a manual name push from a Units View window (see below) and from the following windows:

- Power Device window - see *Power Devices* on page 157
- Power Device Sockets window - see *Power Device Sockets* on page 160

To initiate a name push operation from a Units View window:

1. In a Units View window (see *Accessing Units View windows* on page 111), click the checkboxes next to one or more units. To select all units on the page, click the checkbox to the left of the heading at the top of the list.
2. Click *Operations*, then select *Push Names to Appliance* from the drop-down menu.
3. The Multiple Unit Operations window will open, containing a link to the Operation Results window; see *Multiple unit operations from a Units View window* on page 115.

Manual name pull

Table 10.3 describes what occurs when a name pull operation is initiated.

Table 10.3: Manual Name Pull Operation Effects

When pull is initiated for one or more:	The effect is
Appliance serial ports	The target device name will be pulled from the appliance to update the target device name in the Rack Power Manager software database.
Power devices	The power device name will be pulled from the appliance to update the power device name in the Rack Power Manager software database.
Power device sockets	The target device name will be pulled from the appliance to update the target device name in the Rack Power Manager software database.

You may initiate a manual name pull from a Units View window and from the following windows:

- Power Device window - see *Power Devices* on page 157
- Power Device Sockets window - see *Power Device Sockets* on page 160

To initiate a name pull operation from a Units View window:

1. In a Units View window (see *Accessing Units View windows* on page 111), click the checkboxes next to one or more units. To select all units on the page, click the checkbox to the left of the heading at the top of the list.
2. Click *Operations*, then select *Pull Names from Appliance* from the drop-down menu.
3. The Multiple Unit Operations window will open, containing a link to the Operation Results window; see *Multiple unit operations from a Units View window* on page 115.

Topology Synchronization

The topology synchronization operation updates the Rack Power Manager software database when a change occurs in a managed appliance. Examples of changes are the adding/removing a power device.

You may enable or disable automatic topology synchronization. You may also control topology synchronization manually by:

- Enabling or disabling options when the Add Unit Wizard runs.
- Enabling or disabling options when the Resync Wizard runs.
- Initiating a PDU from a Unit Overview window.
- Initiating a cascade switch merge operation on two multiuser cascade switches in the same appliance from a Units View window.
- Scheduling or manually running the update topology task (see *Task: Update topology for selected units* on page 273).

Automatic topology synchronization

NOTE: Automatic topology synchronization is not supported on some managed appliances, including the LANDesk® Server Manager. Alternatively, you may schedule the update topology task to keep these appliances synchronized with the Rack Power Manager software. See *Task: Update topology for selected units* on page 273.

To enable or disable automatic topology synchronization:

1. Click the *System* tab.
2. Click *Global Properties* in the top navigation bar.
3. Click *Units - Synchronization* in the side navigation bar, then click *Auto Topology*.
4. The Automatic Topology Properties window will open. To enable automatic topology synchronization, enable the *Update RPM with topology changes from appliances automatically* checkbox.

To disable automatic topology synchronization, disable the *Update Rack Power Manager with topology changes from appliances automatically* checkbox and go to the last step.

5. Click *Save*.

Topology synchronization options in the Add Unit Wizard

The Select Options window in the Add Unit Wizard allows you to specify the access mode and certain topology synchronization options.

- Enable/disable secure mode

This window is described in *Adding Units* on page 119.

Each of these options has a default value, which you may change.

To change the default values of the options in the Add Unit Wizard:

1. Click the *System* tab.
2. Click *Global Properties* in the top navigation bar.
3. Click *Wizard Defaults* in the side navigation bar, then click *Add Unit Wizard*.
4. The Add Unit Wizard Default Options window will open.
5. If you enable the *Enable secure mode* checkbox, by default, the unit will only be accessible by this Rack Power Manager software system. In non-secure mode, the unit may be added to multiple Rack Power Manager software systems.
6. If a target device has a default name, you may indicate that, by default, it can be added to the Rack Power Manager software database only if it supports specific connection type(s) in the appliance. Enable the checkboxes for the specific connection types.
7. Click *Save*.

Topology synchronization options in the Resync Wizard

The Select Resync Options window in the Resync Wizard allows you to specify certain topology synchronization options.

- Remove offline connections
- Delete target devices that no longer have connections

This window is described in *Resynchronizing units* on page 257.

Each of these options has a default value, which you may change.

To change the default values of the options in the Resync Wizard:

1. Click the *System* tab.
2. Click *Global Properties* in the top navigation bar.
3. Click *Wizard Defaults* in the side navigation bar, then click *Resync Wizard*.
4. The Resync Wizard Default Options window will open.
 - If you enable the *Remove offline connections* checkbox, by default, any appliance connections that are reported as offline in the appliance will be deleted from the Rack Power Manager software database. The Resync Wizard does not add offline connections to the Rack Power Manager software database.
 - If you enable the *Delete target devices that no longer have connections* checkbox, by default, any target devices that no longer have connections are permanently deleted from the Rack Power Manager software database.
 - If you enable the *Allow target devices with the same name to be merged into a single target device* checkbox, by default, the connection to a target device in the appliance will be merged with the connection(s) to an existing target device in the Rack Power Manager software database.
 - If a target device has a default name, you may indicate that, by default, it can be added to the Rack Power Manager software database only if it supports specific connection type(s) in the appliance. Enable the checkboxes for the specific connection types.
5. Click *Save*.

Automatic Inheritance for Group Memberships and Properties

You can allow new target devices to inherit group memberships and some properties from the appliances to which the target devices are attached. Only location, contacts, notes and custom field properties are inherited. For information about assigning properties to a unit, see *Unit Properties* on page 136.

To enable automatic inheritance:

1. Click the *System* tab.
2. Click *Global Properties* in the top navigation bar.
3. Click *Automatic Inheritance* in the side navigation bar.
4. Click *Save*.

When automatic inheritance is enabled, the following occurs:

- When you use the Add Unit Wizard to add an appliance, you can specify the group for which you want the appliance to belong. Attached target devices will inherit these group memberships. Or, you can select *Do not inherit group membership*. See *Adding a single managed appliance* on page 120. Properties are not inherited at this time because the new appliance does not yet have any properties assigned.
- When new attached target devices are discovered using automatic topology synchronization, the Resync Wizard or the update topology task, the new target devices inherit group memberships and location, contacts, notes and custom field properties from the appliance. For more information about these operations, see *Automatic topology synchronization* on page 129, *Resynchronizing units* on page 257 and *Task: Update topology for selected units* on page 273.

Managing Units

This chapter describes how to manage unit properties and settings, access rights and local account settings, and how to view unit asset and usage reports.

Appliance Configuration Templates

Appliance configuration templates allow Rack Power Manager administrators to quickly configure new units or replace failed units. You can create an appliance configuration template based on any supported unit in the Rack Power Manager software system. The appliance configuration template saves the properties of the model unit so that they can be applied to other units. Two classifications of settings are saved in appliance configuration templates:

- Personality data is specific to a single unit and is only applied during a replace appliance operation. An example of personality data is an IP address.
- Fixed data is specific to the unit family (such as PM 3000) but is not specific to a single unit. Fixed unit data, such as session time-outs, is applied during both an apply appliance configuration template operation and a replace appliance operation.

You can also create appliance configuration templates that are specific to a single unit. For example, once the unit is configured, you may wish to use the Save Last Known Good Configuration Template operation to create an appliance configuration template of the unit in that state. You can also use the Save Current Configuration Template to create an appliance configuration template of the unit in its current state. These templates can later be applied to the unit if needed.

NOTE: For appliances that do not support appliance configuration templates, the related buttons and links are not displayed.

Saving appliance configuration templates

Saving an appliance configuration template generates a Rack Power Manager event.

To save an appliance configuration template:

NOTE: This procedure creates an appliance configuration template that can be applied to any unit of the same family as the model unit.

1. In a Units View window containing appliances (see *Accessing Units View windows* on page 111), select the appliance you want to use as the model for the appliance configuration template. The Unit Overview window opens.
2. Click the *Save Configuration Template* icon or link. The Save Appliance Configuration Template Wizard opens.
3. Enter a name for the appliance configuration template. Click *Next*.
4. The Completed Successful window opens. Click *Finish*.

To save the last known good or current configuration template:

NOTE: This procedure creates appliance configuration templates that can only be applied to the selected unit.

In a Units View window containing appliances (see *Accessing Units View windows* on page 111), select the appliance for which you want to save an appliance configuration template. Click the *Save Last Known Good Configuration Template* or *Save Current Configuration Template* icon or link.

-or-

In a Units View window containing appliances, select the checkbox next to the appliance for which you want to apply the appliance configuration template. From the Operations menu, select *Save Last Known Good Configuration Template* or *Save Current Configuration Template*.

Modifying appliance configuration template properties

To view, modify or delete appliance configuration template files:

NOTE: Administrator rights are required to view and delete appliance configuration template files.

1. Click the *System* tab.
2. Click *Appliance Files* in the top navigation bar.
3. Click *Configuration Template* in the side navigation bar. A list of configuration templates is displayed.
4. To delete an appliance configuration template, select the checkbox next to the template(s) and click *Delete*.

5. To view the properties of an appliance configuration template, click the name of the template.
6. The appliance configuration template properties are displayed, including the name, supported unit type, creation date and the unit that created the template. To change the name, enter a new name and click *Save*.
7. Click *Close*.

Applying appliance configuration templates

Applying appliance configuration templates generates a Rack Power Manager event.

To apply an appliance configuration template to a new appliance:

1. In a Units View window containing appliances (see *Accessing Units View windows* on page 111), select the appliance for which you want to apply the appliance configuration template. The Unit Overview window opens. Click the *Apply Configuration Template* icon or link. The Save Appliance Configuration Template Wizard opens.

-or-

In a Units View window containing appliances, select the checkbox next to the appliance for which you want to apply the appliance configuration template. From the Operations menu, select *Apply Configuration Template*.

2. From the list, select the appliance configuration template you want to apply. Click *Save*.

-or-

Select *Apply Last Known Good Configuration Template*.

-or-

Select *Apply Current Configuration Template*.

3. The Completed Successful window opens. Click *Finish*.

Or, to apply the appliance configuration template during the Add Unit Wizard, see *Adding Units* on page 119.

To replace a failed appliance:

NOTE: Appliance replacement does not work in secure mode.

1. In a Units View window containing appliances (see *Accessing Units View windows* on page 111), select the appliance for which you want to apply the appliance configuration template. The Unit Overview window opens. Click the *Appliance Replacement* icon or link. The Save Appliance Configuration Template Wizard opens.

-or-

In a Units View window containing appliances, select the checkbox next to the appliance for which you want to apply the appliance configuration template. From the Operations menu, select *Appliance Replacement*.

2. Enter the IP address of the failed appliance.
3. From the list, select the appliance configuration template you want to apply. Click *Save*.
4. The *Completed Successful* window opens. Click *Finish*.

Unit Properties

A user with access rights may change the following properties for a unit:

- Overview - Specify the type and icon for a target device.
- Identity - May be helpful for quickly identifying information about a unit.
- Location (site, department and location) - May be helpful for identifying where a unit is. See *Site, Department and Location Groups* on page 177.
- Contacts - Identify the primary and secondary contacts may be helpful for quickly identifying the people to notify if an issue or question arises about a particular unit.
- Custom fields - Ten custom fields are available, in which you may specify any information you wish. For example, you may wish to define custom fields such as Program Manager, Building Number and so on. See *Custom Fields* on page 180.
- Notes.
- Network.

You may specify which properties display in a Units View window by using the *Customize* link. See *Using the Customize link in windows* on page 30.

You may change a single property for one or more units at a time, or you may change multiple properties for multiple units by using the Properties - Bulk Edit operation.

To change multiple properties for multiple units using the Properties - Bulk Edit operation:

1. In a Units View window (see *Accessing Units View windows* on page 111), select the checkboxes next to the appliances or target devices that you want to edit.
2. Click *Operations*, then select *Properties - Bulk Edit* from the drop-down menu.
3. The Bulk Edit Unit Properties window opens. The unit names are displayed in the left column, and the properties are displayed in the adjacent columns. You can scroll to view

columns, or specify which columns are displayed by clicking *Select Columns*. Select the properties that you want to be displayed, click *Add*, then click *Save*.

4. To edit unit properties, type the values in the appropriate fields. To quickly navigate the spreadsheet, use the **Tab** and **Shift + Tab** keystrokes to move right and left and the **Enter** and **Shift + Enter** keystrokes to move down and up.
5. Click *Save*.

To change the identity properties for a unit:

NOTE: Identity properties are visual representations only. Defining incorrect information may cause confusion (for example, mistyping a serial number).

1. In a Units View window (see *Accessing Units View windows* on page 111), click on the appliance.
2. Click *Properties* in the side navigation bar. The Unit Identification Properties window will open. To change information, type a part number, serial number, model number and/or asset tag number.
3. Click *Save* and then click *Close*. The Units View window will open.

To change the location properties for a unit:

NOTE: Location properties are visual representations only. Defining incorrect information may cause confusion (for example, a mistyped room number).

1. In a Units View window (see *Accessing Units View windows* on page 111), click on the appliance.
2. Click *Properties* in the side navigation bar and then click *Location* in the side navigation bar. The Unit Location Properties window will open.
3. Type or use the menus to select the site, department and/or location for the unit.
4. Click *Save* and then click *Close*. The Units View window will open.

To change the location properties for one or more units from a Units View window:

1. In a Units View window (see *Accessing Units View windows* on page 111), click the checkbox next to the unit(s). To change location properties for all units in the page, click the checkbox to the left of Name at the top of the list. (If the page contains units that do not support location properties, they will not be affected.)
2. Click *Operations*, then select *Properties* from the drop-down menu.
3. The Multiple Unit Properties window will open. Click *Location*.

4. Type or use the menus to specify the site, department and/or location for the units.
5. Click *Save* and then click *Close*. The Units View window will open.

To change the contact properties for a unit:

1. In a Units View window (see *Accessing Units View windows* on page 111), click on the appliance.
2. Click *Properties* in the side navigation bar and then click *Contacts* in the side navigation bar. The Unit Contacts window will open. Type the names and phone numbers of the primary and secondary contacts.
3. Click *Save* and then click *Close*. The Units View window will open.

To change the contact properties for one or more units from a Units View window:

1. In a Units View window (see *Accessing Units View windows* on page 111), click the checkbox next to the unit(s). To change contact properties for all units in the page, click the checkbox to the left of Name at the top of the list. (If the page contains units that do not support contact properties, they will not be affected.)
2. Click *Operations*, then select *Properties* from the drop-down menu.
3. The Multiple Unit Properties window will open.
 - To change the primary contact information, click *Primary Contact*. Type names and phone numbers for the primary contact.
 - To change the secondary contact information, click *Secondary Contact*. Type names and phone numbers for the secondary contact.
4. Click *Save* and then click *Close*. The Units View window will open.

To change the custom fields for a unit:

1. In a Units View window (see *Accessing Units View windows* on page 111), click on the appliance.
2. Click *Properties* in the side navigation bar, then click *Custom Fields* in the side navigation bar. The Unit Custom Fields window will open. To change information, type the information in each of the custom fields.
3. Click *Save* and then click *Close*. The Units View window will open.

To change the custom fields for one or more units from a Units View window:

1. In a Units View window (see *Accessing Units View windows* on page 111), click the checkbox next to the unit(s). To change custom fields for all units in the page, click the

checkbox to the left of Name at the top of the list. (If the page contains units that do not support custom fields, they will not be affected.)

2. Click *Operations*, then select *Properties* from the drop-down menu.
3. The Multiple Unit Properties window will open. Click *Custom Fields*.
4. Type the information in each of the custom fields.
5. Click *Save* and then click *Close*. The Units View window will open.

To change the note properties for a unit:

1. In a Units View window (see *Accessing Units View windows* on page 111), click on the appliance or target device name.
2. Click *Properties* in the side navigation bar and then click *Notes* in the side navigation bar. The Unit Notes window will open. Type description, accounting and comment information.
3. Click *Save* and then click *Close*. The Units View window will open.

To change the note properties for one or more units from a Units View window:

1. In a Units View window (see *Accessing Units View windows* on page 111), click the checkbox next to the unit(s). To change note properties for all units in the page, click the checkbox to the left of Name at the top of the list. (If the page contains units that do not support note properties, they will not be affected.)
2. Click *Operations*, then select *Properties* from the drop-down menu.
3. The Multiple Unit Properties window will open. Click *Notes*.
4. Type description, accounting and comment information.
5. Click *Save* and then click *Close*. The Units View window will open.

To change the network properties for a target device:

NOTE: Defining incorrect information for these properties may cause network connection errors.

1. In a Units View window containing target devices (see *Accessing Units View windows* on page 111), click on the target device name.
2. Click *Properties* in the side navigation bar and then click *Network* in the side navigation bar. The Unit Network Properties window will open.
 - Type the address or the fully qualified domain name for the target device.

- Type the Telnet port number to use for Telnet connections to the target device. If this field is left blank, Telnet will not be enabled for the target device.
 - Type the URL for a web browser connection to the target device.
 - Select the Rack Power Manager server that is in charge of the target device.
3. Click *Save* and then click *Close*. The Units View window will open.

To change the network properties for a managed appliance:

1. In a Units View window containing appliances (see *Accessing Units View windows* on page 111) click on the appliance name.
2. Click *Properties* in the side navigation bar and then click *Network* in the side navigation bar. The Unit Network Properties window will open.
 - Type the address or the fully qualified domain name.

If you are changing the appliance IP address, you should first change it in the Appliance Network Settings window before changing it in the Unit Network Properties window. See *Managed Appliance Settings* on page 145.
 - Select the Rack Power Manager server in charge of the managed appliance.
3. Click *Save* and then click *Close*. The Units View window will open.

To change the Rack Power Manager server network property for one or more units from a Units View window:

1. In a Units View window (see *Accessing Units View windows* on page 111), click the checkbox next to the unit(s). To change the Rack Power Manager server property for all units in the page, click the checkbox to the left of Name at the top of the list. (If the page contains units that do not support note properties, they will not be affected.)
2. Click *Operations*, then select *Properties* from the drop-down menu.
3. The Multiple Unit Properties window will open. Click *Network*. Select the Rack Power Manager server in charge of the units.
4. Click *Save* and then click *Close*. The Units View window will open.

Unit Overview Settings

You can configure settings for any level of the infrastructure (company, data center, row of racks or racks), or for individual power and environmental devices.

To view the status:

1. Click the *Units* tab.
2. Click *Units* in the top navigation bar.
3. Click *Power Manager* or *Infrastructure* in the side navigation bar.
4. Click on an infrastructure level or power device. The Unit overview window opens.
5. Click *Power Manager* in the side navigation bar.
6. Click *Status* in the side navigation bar. The latest power monitoring data gathered for the unit is displayed. Data provided varies based on the unit selected but may include current, power and voltage for each phase, total current, power and voltage, humidity and temperature. The list also displays if any thresholds were exceeded for any value.
7. Click *Close*.

To configure power units:

1. Click the *Units* tab.
2. Click *Units* in the top navigation bar.
3. Click *Power Manager* or *Infrastructure* in the side navigation bar.
4. Click on an infrastructure level or power device. The Unit overview window opens.
5. Click *Power Manager* in the side navigation bar.
6. Click *Configuration* in the side navigation bar.
7. If you selected infrastructure level, enter the maximum power consumption in watts in the field provided. If you selected a data center, also enter the cost per kilowatt hour in the field provided. This information is required for data center cost reports.

-or-

If you selected a power device, configuration data received from the power device is displayed. In the Settings area, enter the maximum total current, maximum power consumption, maximum current phase and maximum power consumption per phase in the fields provided. The appropriate values for these settings can be found on the label on the power device hardware; see the power device installer/user guide for more information.

8. Click *Save*, then click *Close*.

To modify thresholds for rows of racks, racks or power devices:

1. Click the *Units* tab.

2. Click *Units* in the top navigation bar.
3. Click *Power Manager* or *Infrastructure* in the side navigation bar.
4. To modify thresholds for a unit, click on the name of a row of racks, rack or power device. The Unit Overview window opens. Click *Power Manager* in the side navigation bar.

-or-

To modify thresholds for multiple units of the same type at once, select the row of racks, rack or power device from the list and click *Configure Thresholds* from the Operations menu.

5. Specify the threshold values for total current, power consumption, internal/external temperature, relative humidity, phase/circuit current and phase/circuit power consumption in the fields provided. For each category, enter the following values:
 - High Critical - When the actual rating is above this value, a high critical alarm is sent.
 - High Warning - When the actual rating is above this value, a high warning alarm is sent. This alarm is designed to indicate when the value is approaching a critical level, so it is recommended that the high warning value be slightly lower than the high critical value.
 - Low Warning - When the actual rating is below this value, a low warning alarm is sent. This alarm is designed to indicate when the value is approaching a critical level, so it is recommended that the low warning value be slightly higher than the low critical value.
 - Low Critical - When the actual rating is below this value, a low critical alarm is sent.
6. Click *Submit*, then click *Close*.

When a threshold is met, an RPM software event is generated.

To monitor consistency (racks and rows of racks):

1. Click the *Units* tab.
2. Click *Units* in the top navigation bar.
3. Click *Power Manager* or *Infrastructure* in the side navigation bar.
4. Click on an infrastructure level or power device. The Unit overview window opens.
5. Click *Power Manager* in the side navigation bar.
6. Click *Monitoring Consistency* in the side navigation bar.

7. To move all members of the selected rack or row of racks to the same RPM server, select the server name from the menu and click *Save*.

To configure data monitoring for racks:

1. Click the *Units* tab.
2. Click *Units* in the top navigation bar.
3. Click *Power Manager* or *Infrastructure* in the side navigation bar.
4. Click on an infrastructure level or power device. The Unit overview window opens.
5. Click *Power Manager* in the side navigation bar.
6. Click *Monitoring* in the side navigation bar.
7. Select the units you want to monitor data and click *Add*.

-or-

Select the units that you do not want to monitor and click *Remove*.

About Access Rights

Access rights indicate which users and user groups may access units in the Rack Power Manager software system. Access rights also indicate which actions are allowed.

For target devices, you may specify whether a user or members of a user group are allowed to:

- View the unit in a Units View window (this right is enabled automatically if any other access right for the target device is enabled)
- Control target device power

For certain managed appliances, you may specify whether a user or members of a user group are allowed to:

- View the appliance in Units View windows (this right is enabled automatically if any other access right for the managed appliance is enabled)
- Reboot appliance and disconnect sessions - see *Importing data* on page 254
- Flash upgrade appliance - see *Upgrading firmware* on page 256
- Configure unit settings - see *Managed Appliance Settings* on page 145
- Configure appliance local user accounts

For example, you may allow users to configure settings on a managed appliance, but not allow them to reboot and disconnect sessions on it. Access rights may also be specified for all units in the Rack Power Manager software system or for a specific unit.

By default, supported embedded units have the same access rights as generic units.

How access rights can be assigned

There are several ways you may assign access rights.

- You may assign access control rights from a unit perspective. From this perspective, you select one or more units, specify the users/user groups for which rights will be assigned, then allow/deny the permission to perform the action for each user/user group. See *Unit Access Rights* on page 144.
- You may also assign access control rights from a unit group perspective. This is similar to assigning access control rights for a unit, except all units that belong to the selected unit group will be affected. See *Changing the unit group properties* on page 189.
- You may also assign access control rights from a user perspective. You select a user account, specify the units for which rights will be assigned, then indicate the permission to perform the action (none, allow, deny or inherit) for each unit. See *User Access Rights* on page 220.
- You may assign access control rights from a user group perspective. This is similar to assigning access control rights for a user, except all users who are members of the selected user group will be affected. See *User Group Access Rights* on page 229.

Unit Access Rights

Rack Power Manager software administrators may assign unit access rights.

To add or remove access rights from a Units View window:

1. In a Units View window (see *Accessing Units View windows* on page 111):
 - To add/remove access to one or more units, click the checkboxes next to the units, and then click *Rights*.
 - To add/remove access to all units on the page, click the checkbox to the left of Name at the top of the list, and then click *Rights*.
2. The Unit Access Rights window will open. To add or remove a user or user group from the Access Rights Assignment list, click *Edit List*. The Unit Access Rights User Selection window will open.

- To add one or more users or user groups, select the users or user groups from the Available list, then click *Add*. The users and/or user groups will be moved to the List to Update list.
- To remove one or more users or user groups, select the users or user groups from the List to Update list, then click *Remove*. The users and user groups will be moved to the Available list.

Click *OK*. The Unit Access Rights window will contain the current list of users/user groups. When a user/user group is added to the list, default access rights will be displayed.

3. To set access rights, select a user or user group from the User and User Groups list, then enable or disable a checkbox in the Access Rights table for each access right.
 - Allow - the access right is allowed for the user/group.
 - Deny - the access right is denied for the user/group.
 - Inherit - the access right is inherited from the unit group(s) to which the selected user/group belongs. When Inherit is selected, the Allow and Deny checkboxes will become gray and unchangeable, and indicate the inherited value. If the inherited settings indicated both Allow and Deny, the inherited value is Deny, which takes precedence.

To disable the inherit functionality, uncheck the Inherit checkbox.

 - If none of the checkboxes are checked, the access right is neither allowed nor denied.
4. Repeat the preceding step to change access rights for other users/user groups.
5. Click *Save* and then click *Close*. The Units View window will open.

Managed Appliance Settings

To change the network settings of a managed appliance:

NOTE: The MAC address cannot be changed.

1. In a Units View window containing appliances (see *Accessing Units View windows* on page 111), click on the appliance name.
2. Click *Appliance Settings* in the side navigation bar and then click *Network*. The Appliance Network Settings window will open. To change information:
 - Type an IP address, in standard dot notation (xxx.xxx.xxx.xxx).

If you change the appliance IP address in the Appliance Network Settings window, you must then also change the address in the Unit Network Properties window. See *Unit Properties* on page 136. (When changing an IP address, always change it in the Appliance Network Settings window before changing it in the Unit Network Properties window.)

- Type a subnet, in standard dot notation (xxx.xxx.xxx.xxx).
 - Type a gateway, in standard dot notation (xxx.xxx.xxx.xxx).
 - Specify a LAN speed. This network setting will not appear for CPS appliances.
 - Enable or disable DHCP or BootP (KVM switches).
 - Enable or disable ICMP ping reply.
3. Click *Save* and then click *Close*. The Units View window will open.

To change the IP addresses of Rack Power Manager servers used for managed appliance authentication:

1. In a Units View window containing appliances (see *Accessing Units View windows* on page 111), click on the appliance name.
2. Click *Appliance Settings* in the side navigation bar and then click *Authentication Servers*. The Appliance Authentication Servers Settings window will open. To change information, type an IP address, in standard dot notation (xxx.xxx.xxx.xxx), for up to four Rack Power Manager servers the managed appliance will use for authentication.
3. Click *Save* and then click *Close*. The Units View window will open.

To display version information for one or more managed appliances from a Units View window:

1. In a Units View window containing appliances (see *Accessing Units View windows* on page 111), click the checkbox next to the unit(s). To display information about all units in the page, click the checkbox to the left of Name at the top of the list.
2. Click *Operations*, then select *Show Versions* from the drop-down menu.
3. A Multiple Unit Operation window will open, containing a link to view results; see *Multiple unit operations from a Units View window* on page 115.

The results window includes the unit name, type and when the version information retrieval began.

The Appliance Version field will contain the main firmware version; if a unit did not or cannot report a firmware version, dashes are displayed.

The Boot Version field contains the boot firmware version. If a unit does not support a boot version but has an appliance version, N/A will be displayed. Dashes will be displayed if a unit does not support either appliance or boot firmware.

The Status field indicates the result of the display (for example, Show Versions complete or Show Versions not supported).

To display version information for a managed appliance:

1. In a Units View window containing appliances (see *Accessing Units View windows* on page 111), click on an appliance name.
2. Click *Appliance Settings* in the side navigation bar and then *Versions*. The Appliance Version Information window will open, containing the following information:
 - For serial console appliances - bootstrap and application versions
3. Click *Close*. The Units View window will open.

To enable or disable secure mode on an appliance:

1. In a Units View window containing appliances (see *Accessing Units View windows* on page 111), click the checkbox next to the unit(s).
2. Click *Operations*, then select *Enable Secure Mode* from the drop-down menu.

Managed Appliance SNMP Settings

The SNMP protocol is used to communicate management information between network management applications and Rack Power Manager software managed appliances using TCP/IP and IPX protocols. Other external SNMP managers (such as Tivoli® and HP OpenView) may communicate with your managed appliances by accessing MIB-II (Management Information Base) and the public portion of the enterprise MIB. MIB-II is a standard MIB that many SNMP target devices support. The managed appliances will send their traps directly to the external SNMP manager in addition to sending it to the server.

The following settings appear under SNMP in the side navigation bar:

- **System** - Enables/disables SNMP. When you enable SNMP, the managed appliance will log SNMP received messages over UDP (User Datagram Protocol) port 161. UDP port 162 is used to listen for incoming traps.
- **Managers** - Stations that can manage the managed appliance.
- **Community** - Communities to which the traps belong.
- **Destinations** - Stations that can receive SNMP traps.
- **Traps** - Available traps and enabled/disabled traps.

The traps must be also configured on each managed appliance using the Command Line Interface (CLI). The address of the server running the Rack Power Manager software must be configured as a trap recipient, the proper community must be set and each desired trap must be enabled.

SNMP traps are logged in the event log file. See *Displaying the Event Log* on page 284. SNMP traps may also be configured from a system task. See *Task: Configure SNMP trap settings on a managed appliance* on page 266.

To change SNMP settings for a managed appliance:

1. In a Units View window containing appliances (see *Accessing Units View windows* on page 111), click on the appliance name.
2. Click *Appliance Settings* in the side navigation bar and then click *SNMP* in the side navigation bar. The Appliance SNMP System Settings window will open.
3. To enable SNMP, select *Enabled* in the Enable SNMP menu. If desired, change the name and description of the managed appliance and type a contact. Then, click *Save*.
4. To enable SNMP manager settings, click *Managers* in the side navigation bar. The Appliance SNMP Manager Settings window will open. Type the IP addresses, in standard dot notation (xxx.xxx.xxx.xxx), for up to four SNMP managers. Then, click *Save*.
5. To specify SNMP community settings, click *Community* in the side navigation bar. The Appliance SNMP Community Settings window will open. Type the SNMP community names for reading, writing and SNMP traps. Then, click *Save*.
6. To specify SNMP destination settings, click *Destinations* in the side navigation bar. The Appliance SNMP Destination Settings window will open. Type the IP addresses, in standard dot notation (xxx.xxx.xxx.xxx), for up to four SNMP destinations. Then, click *Save*.
7. To enable or disable SNMP traps, click *Traps* in the side navigation bar. The Appliance SNMP Trap Settings window will open. Select one of the following:
 - *Enabled* turns a trap on; *Disabled* turns a trap off.
 - *Enable All* turns all traps on; *Disable All* turns all traps off.
8. Click *Save* and then click *Close*. The Units View window will open.

Bulk Configuration of Individual settings

The bulk configuration allows administrators to select individual settings for selected power devices and view or modify those settings.

To modify individual power device settings:

1. Click on the *Units* tab.
2. Select the power device.
3. From the *Operations* tab, select *Configuration - Bulk Edit*.
4. Modify any of the following settings:
 - a. Name
 - b. Maximum Total Current
 - c. Maximum Power Consumption
 - d. Maximum Current Per-Phase/Circuit
 - e. Maximum Power Consumption Per-Phase/Circuit
5. Click *Save* to save the changes or *Close* to quit without saving the changes.

Infrastructure View

The rack power manager plug-in logs all historical data for power and environmental devices.

To operate the reporting capabilities within rack power manager, you must organize units in an infrastructure view. Each infrastructure may contain up to four levels in the following hierarchy:

“company,” “data center,” “row of racks” and “rack”; racks contain power and environmental devices. Power management reports are available for all infrastructure levels. Reports include total power consumption, threshold events, power consumption per phase, total energy consumption, temperature and energy costs for each unit. Comparative reports juxtapose the historical data of multiple units.

The information provided here is supplemental to the Rack Power Manager help.

Prerequisites

Before power data can be collected, the following configuration must be complete:

- The voltage and power factor must be configured for each power device for which you want to collect data; see the RPM help (keywords: power devices).
- An infrastructure with power and/or environmental devices must be configured. The Power Management link in the side navigation bar displays the organization configured from the Infrastructure window. Data monitoring must also be enabled on the units from the Infrastructure window.

In an infrastructure organization, a row of racks contains racks that each contain power and/or environmental devices. For RPM systems consisting of hub and spoke servers, a row of racks and the racks and devices it contains must be assigned to the same RPM server. For example, a row of racks assigned to a hub server must not contain racks that are assigned to a spoke server. This configuration is required for the power management plug-in to accurately collect and aggregate historical data.

For more information, see the RPM help (keywords: infrastructure).

Power Management Plug-in Settings

The following settings are globally applied to the RPM server.

To modify power management plug-in settings:

1. Click the *Systems* tab, then click *Plug-ins* in the top navigation bar.
2. Click *Power Management* in the list of plug-ins.
3. Click *Settings* in the side navigation bar.
4. In the Archive Interval section, select the maximum number of months that power monitoring logs should be stored before being automatically exported to .csv files.
5. In the Unit Nomenclature area, specify the temperature unit, power 3-phase description and currency to be used in power reports.
6. In the Plug-In Standard Properties area, specify the interval at which power monitoring data is collected.
7. Click *Save*.

Asset and Usage Reports

You can view Asset and Usage reports as a pie chart, bar chart or table by clicking the appropriate button. If multiple charts are tiled on the screen, you can change the size of the charts by dragging the triangle on the Size bar to the right or left. To print a report in a printer-friendly format, click the printer icon.

Unit Reports

Unit reports display power, energy, costs, percentage load and other power management data for a single infrastructure level or power device.

To view unit reports:

1. Click the *Units* tab.
2. Click *Units* in the top navigation bar.
3. Click *Power Manager* or *Infrastructure* in the side navigation bar.
4. Click on an infrastructure or power or environmental device name. The unit Overview window opens.
5. Click *Power Manager* in the side navigation bar.
6. Click *Reports*.
7. Select a report from the Reports menu. Available reports vary based on the type of unit selected and what data each unit supports.
8. Enter the date and time range for the report in the fields provided.
9. Click *Run Report*.
10. The report is displayed as a line graph. Click the bar chart or table view icons to change the view, or click the interpolation icon to show only data points. If applicable, you may click the colored boxes below the report to show or hide report data for a category.
11. (Optional) If you selected an energy report, click the dollar sign (\$) icon to view cost information. The cost is calculated based on the cost per kilowatt hour rate configured for the data center.
12. Click *Export Data* if you wish to export and save the report data as .csv file.
13. Click *Close*.

To view status reports:

1. Click the *Reports* tab.
2. Click *Power* in the top navigation bar.
3. Select *PDU* or *PDU Power Range* from the Reports menu. The report is displayed in table format.
4. Click *Export Data* if you wish to export and save the report data as .csv file.
5. Click *Close*.

Asset

To view Asset reports:

1. Click the *Reports* tab, then click *Asset* in the top navigation bar.
2. Select one of the following reports in the side navigation bar:
 - *Appliance Models* - Displays the number of units for each appliance model the user has added to the Rack Power Manager software.
 - *Appliance Versions* - Displays the firmware version(s) for each appliance model managed by the Rack Power Manager software.
 - *Units* - Displays the total number of units, sorted by type.
3. Click *Export Data* if you wish to export and save the report data as a .csv file.
4. Click *Schedule Export Task* if you wish to create a task that exports Asset Report data at specific intervals. See *Task: Exporting an Asset Report to a .csv file* on page 269.

Usage

To view Usage reports:

1. Click the *Reports* tab, then click *Usage* in the top navigation bar.
2. Select one of the following reports in the side navigation bar:
 - *Sessions Per Day* - Displays the number of sessions opened to a target device from the Rack Power Manager software each day during the last seven days.
 - *Frequently Accessed Targets* - Displays the number of sessions opened from the Rack Power Manager software for each target device during the last seven days.
3. Click the arrow next to *Today* to select the number of days to include in the report data. If you select *Custom*, enter the dates and times in the fields provided. If you select *Last nn days*, enter the number of days in the field provided.
4. Click *Run Report*.
5. The report is displayed as a line graph. Click the bar chart or table view icons to change the view, or click the interpolation icon to show only data points. If applicable, you may click the colored boxes below the report to show or hide report data for a category.
6. Click *Export Data* if you wish to export and save the report data as a .csv file.
7. Click *Schedule Export Task* if you wish to create a task that exports Usage Report data at specific intervals. See *Task: Exporting a Usage Report to a .csv file* on page 270.

Scheduled Reports

The schedule reports feature allows schedule creation of every report selected by the user, options to decide on the frequency, the option to save the reports and the option to email the reports.

To create a scheduled report:

1. Click the *System* tab.
2. Click on *Scheduled Reports* in the top navigation bar.
3. Click *Add*.
4. Enter or select the following:
 - a. Schedule
 - b. Frequency
 - c. Type of report
 - d. Email recipients
 - e. Chart type
 - f. File type
5. Click *Save* and *Close*.

To Remove a scheduled report:

1. Click the *System* tab.
2. Click on *Scheduled Reports* in the top navigation bar.
3. Click the checkbox next to the report(s).
4. Click *Delete*.
5. Click *Save* and *Close*.

To run a report:

1. Click the *System* tab.
2. Click on *Scheduled Reports* in the top navigation bar.
3. Click the checkbox next to the report(s).
4. Click *Run Now*.

To modify/update a scheduled report:

1. Click the *System* tab.
2. Click on *Scheduled Reports* in the top navigation bar.
3. Click on the task to be modified/updated.
4. Make modifications/updates.
5. Click *Save* and *Close*.

Segregated Temperature Readings

Two separate reports are available for displaying internal and external temperatures for selected PDUs, racks or rows of racks.

To create a report for an internal or external temperature for individual PDUs:

1. Click on the *Units* tab.
2. Click on the desired *PDU*.
3. Click *Rack Power Manager* and then click *Reports*.
4. From the drop-down menu, select either Internal or External Temperature Report.
5. Select the desired date/time and click *Close*
or
Click *Run Report*.

To create comparative temperature reports:

1. Click *Reports*.
2. Click *Power*.
3. From the drop-down menu, select either Comparative Internal or External temperature report.
4. Select the PDU, rack or row of racks for the report.
5. Select the desired date/time and click *Close*
or
Click *Run Report*.

Tiered Energy Cost Setting

NOTE: Peak hours and off peak hours cannot overlap. Off peak hour energy rate cannot be more than the peak hour energy rate.

To modify peak/off peak hour rate and time:

1. Click the *Units* tab.
2. Select the data center from the side navigation bar.
3. Click *Power Manager - Settings - Configuration*.
4. Enter the Maximum Power Consumption.
5. Enter the Peak Rate Cost per kilowatt Hour and set the desired timeframe.

-or-

Click the checkbox *Off Peak Rate Same as Peak Rate*, enter the Off Peak Rate Cost per kilowatt Hour and set the desired timeframe.

6. Click *Save* and *Close*.

Power Devices and Power Device Sockets

See *Power devices* on page 3 for information about the power device types and models that are supported on Avocent appliances.

This section applies to PDUs that are connected serially through an ACS or KVM switch.

Power Devices

To display a list of power devices attached to an appliance or initiate a push/pull name operation:

1. In a Units View window containing appliances (see *Accessing Units View windows* on page 111), click on the appliance name.
2. Click *Appliance Settings* in the side navigation bar and then click *Ports* and then click *Power device*. The Power Devices Attached to Appliance window will open.
3. To initiate a pull or push name operation (see *Name Synchronization* on page 125), click the checkboxes to the left of one or more device name(s). To select all names on the page, click the box to the left of Appliance Name at the top of the list.
 - For a pull operation, click *Pull Name*.
 - For a push operation, click *Push Name*.

Customizing the Power Devices Attached to Appliance window

The display fields and content of the Power Devices Attached to Appliance window will differ according to the power device type and models. For details, see the product documentation. Use the *Customize* link to add or remove fields in the display; see *Using the Customize link in windows* on page 30.

The following fields are always displayed, regardless of the power device type and model.

- Name in Appliance - Name of the power device in the appliance
- Name in RPM - Name of the power device in the Rack Power Manager software database

- Status

NOTE: To successfully add or remove a power device, the power device must be in an online state.

To add or remove a power device:

1. In a Units View window containing appliances (see *Accessing Units View windows* on page 111), click on the appliance name. The Unit Overview window will open.
2. Click *Manage Power Devices* in the Tools area. The Power Management Wizard will appear.

(You may also access the Power Management Wizard by clicking the following sequence in the side navigation bar: *Appliance Settings - Ports - Power Devices - Manage*.)

3. The Select Action window will open.
 - To add a power device, enable the *Add Power Devices* radio button.
 - To remove a power device, enable the *Remove Power Devices* radio button.Click *Next*.
4. The Select Parameters window will open.
 - a. In the Port menu, select the port where the power device will be added or removed.
 - For a serial console appliance, select the physical port number in the Port menu.
 - For an appliance supported by a plug-in, select the appropriate port value.
 - b. If you are adding a power device, select the type in the Power Device Type menu.
 - c. Click *Next*.
5. A Completed Successful or Completed Unsuccessful window will open, indicating the results of the addition or removal. Click *Finish*.

To change power device settings:

1. In a Units View window containing appliances (see *Accessing Units View windows* on page 111), click on the appliance name.
2. Click *Appliance Settings* in the side navigation bar, click *Ports* and then *Power device* in the side navigation bar. The Power Devices Attached to Appliance window will open. (For DSR switches that have two SPC ports, one row will appear for each power device.)
3. Click on the name of a power device. The Power Device Settings window will open.

Some fields are read-only. For fields that can be modified, enter or select new values. (If you change the appliance name and the automatic name pull feature is enabled, see *Automatic name pull* on page 126 for the effect.)

4. Select a voltage and enter a power factor in the fields provided. These values are required if you wish to monitor power data on a power device.
5. Click *Save* and then click *Close*. The Power Devices Attached to Appliances window will open.
6. Click *Close*. The Units View window will open.

Upgrading the firmware of a Cyclades power device

You may upgrade the firmware of a Cyclades power device attached to a DSR switch. There are two ways to do this:

- From a Unit Overview window, using the Upgrade Firmware wizard - see *Upgrading firmware* on page 256.
- Using the Task wizard - see *Task: Updating the firmware of an appliance type* on page 271.
 - In the Select Task to Add window, select *Upgrade firmware of selected units*.
 - In the Select Unit Type window, you may select by product family (Cyclades Power Devices) or unit type (specific power device types)

If multiple power devices are installed in a daisy chain configuration, the most remote power device will be upgraded first.

Power Device Input Feed

The ability to display and change power device input feed information is currently supported on Avocent SPC power control devices, Server Technology power devices and Cyclades PM Intelligent Power Distribution Units (IPDU).

To display power device input feed information:

1. In a Units View window containing appliances (see *Accessing Units View windows* on page 111), click on the appliance name.
2. Click *Appliance Settings* in the side navigation bar, click *Ports* and then *Power device* in the side navigation bar. The Power Devices Attached to Appliance window will open. (For DSR switches that have two SPC ports, one row will appear for each power device.)
3. Click on the name of a power device.

4. Click *Input Feeds* in the side navigation bar. The Power Device Input Feeds window will open.

Customizing the Power Device Input Feeds window

The following fields may be displayed in the Power Device Input Feeds window. For detailed field descriptions, see the product documentation. Use the *Customize* link to add or remove fields in the display. See *Using the Customize link in windows* on page 30.

- Input Feed Name
- Status - Unknown, on, off, cycling, pending off, pending on, pending cycle or no status
- Load
- Alarm Threshold - a trap will be sent if the Load value reaches the Alarm Threshold value
- Load Max - a trap will be sent if the Load value is greater than the Load Max value
- Load Min - a trap will be sent if the Load value is less than the Load Min value

To change power device input feed information:

1. In a Units View window containing appliances (see *Accessing Units View windows* on page 111), click on the appliance name.
2. Click *Appliance Settings*, click *Ports* and then *Power devices* in the side navigation bar. The Power Devices Attached to Appliance window will open.
3. Click on the name of a power device.
4. Click *Input Feeds* in the side navigation bar. The Power Device Input Feeds window will open.
5. Click on an input feed name. The Power Device Input Feed Settings window will open. Some fields are read-only. For fields that can be modified, enter or select new values.
6. Click *Save* and then click *Close*. The Power Device Sockets window will open.
7. Click *Close*. The Power Devices Attached to Appliance window will open.
8. Click *Close*. The Units View window will open.

Power Device Sockets

To display information about power device sockets or initiate a push/pull operation:

1. In a Units View window containing appliances (see *Accessing Units View windows* on page 111), click on the appliance name.

2. Click *Appliance Settings*, click *Ports* and then *Power devices* in the side navigation bar. The Power Devices Attached to Appliance window will open.
3. Click on the name of a power device.
4. Click *Sockets* in the side navigation bar. The Power Device Sockets window will open.

If you change the IP address of a managed appliance that is attached to a power device, the appliance may need rebooting. In this case, a Reboot Required icon will be displayed in the top left corner of the Power Device Sockets window. Click the icon to reboot the managed appliance.

5. To initiate a pull or push name operation (see *Name Synchronization* on page 125):
 - a. Click the checkboxes to the left of one or more device name(s). To select all names on the page, click the box to the left of Appliance Name at the top of the list.
 - b. For a pull operation, click *Pull Name*.
 - c. For a push operation, click *Push Name*.

Customizing the Power Device Sockets window

The display fields and content of the Power Device Sockets window will differ according to the power device type and models. For details, see the product documentation. Use the *Customize* link to add or remove fields in the display. See *Using the Customize link in windows* on page 30.

The following fields are always displayed, regardless of the power device type and model.

- Socket - Socket (outlet) number.
- Appliance Name - Name of the power device socket in the appliance.
- Unit Name - Name of the power device socket in the Rack Power Manager software database.

To change power device socket settings:

1. In a Units View window containing appliances (see *Accessing Units View windows* on page 111), click on the appliance name.
2. Click *Appliance Settings* in the side navigation bar, click *Ports* and then *Power device* in the side navigation bar. The Power Devices Attached to Appliance window will open.
3. Click on the name of a power device.
4. Click *Sockets* in the side navigation bar. The Power Device Sockets window will open.
5. Click on a power device socket. The Power Device Socket Settings window will open.

Some fields are read-only. For fields that can be modified, enter or select new values. (If you change the appliance name and the automatic name pull feature is enabled, see *Automatic name pull* on page 126 for the effect.)

6. Click *Save* and then click *Close*. The Power Device Sockets window will open.
7. Click *Close*. The Power Devices Attached to Appliance window will open.
8. Click *Close*. The Units View window will open.

Power Control of Devices Attached to Power Devices

There are several ways to power up, power down or power cycle a target device that is attached to a power device socket.

- From a Power Device Sockets window
- From a Units View window containing power devices
- From the Video Viewer - see *Power Control of Devices Attached to Power Devices* on page 249
- From the Telnet Viewer - see *Power Control of Devices Attached to Power Devices* on page 249
- From the DSR Remote Operations software

To control power from a Power Device Sockets window:

1. In a Units View window containing appliances, click on the appliance name.
2. Click *Appliance Settings* in the side navigation bar, click *Ports* and then *Power device* in the side navigation bar. The Power Devices Attached to Appliance window will open.
3. Click on the name of a power device.
4. Click *Sockets*. The Power Device Sockets window will open.
5. Click the checkbox to the left of the power device socket(s). To select all sockets on the page, click the checkbox to the left of Socket at the top of the list.
6. Click *On*, *Off* or *Cycle* to power up, power down or power cycle (off and then on) the selected power device sockets. The Power field for the selected sockets will reflect the state.
7. For certain power device types and models, administrators may also lock or unlock a socket's current state by clicking *Lock* or *Unlock*. This sets the control field of the selected socket(s) to the specified value; users other than administrators cannot change the state. The default value is *Unlock*.

To control power from a Units View window:

1. In a Units View window containing power devices, click the checkbox next to the power device(s). To select all power devices in the page, click the checkbox to the left of Name at the top of the list. (If any of the selected units are not power devices, the operation will be ignored for them.)
2. Click *Operations*, then select *Wall Power On*, *Wall Power Off* or *Wall Power Cycle* from the drop-down menu.
3. A Multiple Unit Operation window will open, containing a link to view results; see *Multiple unit operations from a Units View window* on page 115.

Power Operations

To perform power operations on a power device or rack:

1. Click the *Units* tab.
2. Click *Units* in the top navigation bar.
3. Click *Power Manager* or *Infrastructure* in the side navigation bar.
4. Click on a power device or rack name. The Unit overview window opens. Click the corresponding Tools icon or link to turn on, turn off or power cycle the power device.

-or-

Select the power device(s) from the list and select *Power Unit On*, *Power Unit Off* or *Power Cycle Unit* from the Operations menu.

Unit Sessions and Connections

This chapter describes how to view and manage unit sessions and connections in the Rack Power Manager software.

Managed Appliance Session Settings

From the Appliance Sessions window, you may display session information and change appliance session settings.

Exit macros may be used by and reside on certain switches.

Customizing the Appliance Sessions window

The following fields may be displayed in the Appliance Sessions window for managed appliances. Use the Customize link to add or remove fields in the display. See *Using the Customize link in windows* on page 30.

- Duration - Length of the Rack Power Manager software session.
- User - Name of user who initiated the Rack Power Manager software session.

To display session information:

1. In a Units View window containing appliances (see *Accessing Units View windows* on page 111), click on the appliance name.
2. Click *Appliance Settings* in the side navigation bar and then click *Sessions*. The Appliance Sessions window will open.
3. To display information about a specific session, click on the name of the session. The Active Session Information window will open, including information about the active session.
4. Click *Close*. The Appliance Sessions window will open.
5. Click *Close*. The Units View window will open.

Connections to Units

The *Connections* link displays managed appliance connections.

- The Appliance Connections window lists all connections from the managed appliance to cascade switches or target devices. You may rename the units which are part of the connection path through this window.

NOTE: Merged target devices appear as separate connections in the Connections window.

SSH Passthrough Sessions

An SSH Passthrough session is a serial session opened to a unit without the use of a web browser. From an SSH client, a user with access rights can establish a connection to any PDU managed by the Rack Power Manager software that supports Secure Shell 2 (SSH2) and Emerson DS Authentication 2 Protocol (ADSAP2) protocol.

The Rack Power Manager server provides user authentication and, if events are enabled, logs SSH Passthrough session events. You can also share SSH Passthrough sessions with multiple users across multiple Rack Power Manager servers. Serial sessions initiated from the Rack Power Manager client software may also be shared if the Avocent Session Viewer is preconfigured as the serial viewer.

Shared serial sessions provide server redundancy. If a Rack Power Manager server is no longer available, a user may establish an SSH Passthrough session to a different Rack Power Manager server.

Configuring SSH Passthrough

- Enable the SSH server
- Enable SSH Passthrough; see *Enabling SSH Passthrough* on page 167.
- (Optional) Enable SSH port sharing; see *SSH port sharing* on page 168.

Only Rack Power Manager software administrators may enable the SSH servers, SSH Passthrough and SSH port sharing.

Enabling SSH Passthrough

To enable or disable SSH Passthrough:

1. Click the *System* tab.
2. Click *RPM Server* in the top navigation bar.

3. Click *SSH Passthrough* in the side navigation bar. The SSH Passthrough Properties window opens.
4. To enable SSH Passthrough, select the *Enable SSH Passthrough* checkbox.
-or-
To disable SSH Passthrough, uncheck the *Enable SSH Passthrough* checkbox.
5. In the event of a network failure, you may establish an SSH Passthrough session to the target device through Modem Dial-Up. To allow this capability, select the *Enable Modem Dial-Up Connections* checkbox. If the main network connection is unavailable when trying to open an SSH Passthrough session, you will be notified that the network is unreachable and a connection over modem dial-up is being established.
-or-
To prevent connections through Modem Dial-Up, uncheck the *Enable Modem Dial-Up Connections* checkbox. If the main network connection fails, the SSH Passthrough connection will fail without attempting an alternate connection.

NOTE: Modem dial-up connections are only available on supported ACS console servers.

6. Click *Save*.
7. If you have not already done so, click the *SSH Server page* link and enable the SSH server. Enabling or disabling SSH Passthrough will generate a Rack Power Manager software system event.

SSH port sharing

SSH Passthrough sessions and/or Emerson Session Viewer sessions can be shared to allow other users to view the session data. You can also enable hub/spoke forwarding to allow sessions from multiple Rack Power Manager servers to be shared simultaneously. The first user to open an SSH Passthrough or Avocent Session Viewer session has read/write access; all subsequent users who share the session have read-only access. Users can enter a command to obtain read/write access, but only one user at a time can possess read/write access.

To configure SSH Passthrough port sharing:

1. Click the *System* tab.
2. Click *RPM Server* in the top navigation bar.
3. Click *SSH Passthrough* in the side navigation bar. The SSH Passthrough Properties window opens.
4. To enable shared SSH Passthrough sessions, select the *Enable Port Sharing* checkbox.

5. To allow simultaneous shared SSH Passthrough sessions from multiple Rack Power Manager servers, select the *Enable Hub/Spoke Forwarding* checkbox.

If hub/spoke forwarding is enabled, shared SSH Passthrough sessions are centralized to the Rack Power Manager server that owns the appliance to which the session is opened.

NOTE: The appliance is owned by the Rack Power Manager server to which it was first added. To determine which Rack Power Manager server owns an appliance, go the appliance Unit Overview Page and click *Properties - Network*. The RPM Server menu displays the name of the server that owns the appliance. See *Unit Properties* on page 136 for more information.

6. To allow sharing among SSH Passthrough sessions and Avocent Session Viewer sessions, select the *Enable RPM Client Serial Sessions* checkbox.
7. Click *Save*.

Configuring the Avocent Session Viewer

To allow sharing among sessions initiated from the Rack Power Manager client software, you must preconfigure the Avocent Session Viewer as the serial viewer.

To configure the Avocent Session Viewer:

1. Click the *Profile* tab.
2. Click *Applications* in the side navigation bar.
3. Select the *Avocent Session Viewer* checkbox.
4. Click *Save*.

For more information about serial session applications, see *Choosing the serial session application* on page 41.

SSH Passthrough Sessions

You may establish an SSH connection to a PDU by specifying the appropriate name in the SSH command. You may also establish an SSH session to a target device with multiple connections, but the appliance name and port number must be entered in place of the target device name.

NOTE: It is recommended that no more than 2048 concurrent data logging and SSH Passthrough sessions be open.

Preemption

Your SSH session may be interrupted or disconnected based on the appliance preemption levels. If the appliance supports Rack Power Manager software preemption levels, then user

preemption rights will be determined based on the preemption levels set in the Rack Power Manager software.

Logging in with a User SSH key

A user SSH key may be used instead of a password to authenticate the user before establishing an SSH Passthrough session. See *User SSH key* on page 216 to configure the key.

Establishing an SSH Passthrough connection to a unit

To establish an SSH Passthrough connection to a target device or appliance console:

NOTE: If you are using the Linux or Unix SSH command, you will need to specify the port by entering **-p** and the port number. The default port number is 4122. For more information or to change the port number, see *Enabling SSH Passthrough* on page 167.

1. To connect to a target device or appliance console, open your SSH client and enter the following values in the provided text fields:
 - **<zone1/username>:**
Specify the highest level zone for which you have access rights. If a zone is not specified for the username, the top level zone is assumed. If you do not have access to this zone, the connection attempt fails.
 - **<zone2/targetdevice name>@** (to connect to a target device)

-or-
<zone2/appliance name>@ (to connect to an appliance console)
If the appliance resides in a zone below your highest level zone, specify a zone. If a zone is not specified, it is assumed that unit belongs to the zone specified for the username. If the unit does not reside in this zone, the connection attempt fails.
 - host name or IP address of the Rack Power Manager server

NOTE: If DS Zones are not enabled, you do not need to specify a zone for the username or appliance. For more information about zones, see *DS Zones* on page 197.

To connect to a target device using the Linux or Unix SSH command, enter a command in the following format:

<zone1/username>:<zone2/target device name>@<host name or IP address of Rack Power Manager server>

For example, a command to open an SSH session to a target device may look like this:

ssh -p 4122 zone1/jsmith:zone2/Boston@172.30.19.101

To connect to an appliance console using the Linux or Unix SSH command, enter a command in the following format:

<username>:<appliance name>:@<host name or IP address of Rack Power Manager server>

For example, a command to open an SSH session to an appliance console may look like this:

ssh -p 4122 zone1/jsmith:zone2/ACS_Lab:@172.30.19.101

NOTE: The colon is used to delimit different arguments; however, if a colon is contained within the name, then a double backslash may be used as an escape sequence to include the colon in the name. For example, if the username is "sanders:", a command to open an SSH session to a target device may look like this:

ssh -p 4122 zone1/sanders\:::zone2/Boston:5@172.26.5.100

2. If a user SSH key has been configured, the session is automatically authenticated based on the key. The user SSH key must be stored on the Rack Power Manager server specified in See "To connect to a target device or appliance console, open your SSH client and enter the following values in the provided text fields:" on page 170.

-or-

When prompted, enter the password for the username. If you enter an incorrect password three times, the login failed event will be generated and the SSH session will be closed.

The user credentials for the target device are validated by the Rack Power Manager server. If the user is valid, the Rack Power Manager software database determines the IP address of the appliance and the X.509 certificate for establishing the connection. If the user is invalid, the session closes immediately.

3. If more than one connection exists to the target device, the SSH connection attempt fails and the Rack Power Manager software informs the user of the failure reason. To connect to a target device with multiple connections, specify the appliance name and port instead of the target device name. The appliance name must be identical to the appliance name in the Rack Power Manager software database, and the port must be the exact port number that appears in the Units view in the Rack Power Manager software.

To connect to a target device with multiple connections, open your SSH client and enter the following values in the provided text fields:

- **<zone1/username>:**
- **<zone2/appliancename>:port@**
- host name or IP address of the Rack Power Manager server

To connect to a target device with multiple connections using the Linux or Unix SSH command, enter a command in the following format:

<zone1/username>:<zone2/appliance name:port>@<host name or IP address of Rack Power Manager server>

4. The SSH client attempts to establish an SSH connection to the appliance or target device. If a successful connection is established, the Rack Power Manager server acts as a proxy between the user and target device.

If an SSH Passthrough session to the same appliance or target device is already open, your session is shared with the previously connected users. You have read-only access to the session, but you may enter a command to obtain read/write access. See *Transferring read/write access* on page 174.

5. If the console port on the target device requires additional authentication, the user is prompted to log in.

Escape key sequence

An escape key sequence is a combination of characters that can be sent to the Rack Power Manager server to affect an SSH Passthrough or Emerson Session Viewer session. The default escape sequence is **^Ec**, which can be followed by an escape key to send a command to a target device. Some escape key sequences are limited to only the user with read/write access.

In this chapter, the preset escape Sequence **^Ec** is used in all examples to indicate the configured escape sequence.

Table 14.1: Rack Power Manager Software - Supported SSH Passthrough Session Escape Keys

Escape Keys	Description	Escape Keys	Description
.	Disconnect	?	Print this message
a	Attach read/write rights	e	Change escape sequence [the preset value is ^Ec]
!?	Displays break sequence list*	0-9	Send specific break sequence*
r	Replay last 30 lines of log	<cr>	Ignore/abort command
*Only users with read/write access can send these escape key sequences.			

To modify the escape sequence:

From an SSH Passthrough session, enter the following command:

^Ece[new escape sequence]

For example: **^Ece^Ac** changes the escape sequence from **^Ec** to **^Ac**.

To enter an escape key sequence:

From an SSH Passthrough session, enter a command in the following format:

^Ec[escape key]

For example: ^Ec1? displays the break sequence list.

After entering an escape key sequence, the SSH client displays a message indicating success or failure.

Break sequences

NOTE: SSH port sharing must be enabled before you can configure break sequences.

A break sequence is a user-defined combination of characters that can be sent as a command to a target device during an SSH Passthrough or Emerson Session Viewer session. A break sequence is sent when the corresponding escape key sequence is typed by the user. The Rack Power Manager software supports ASCII and UTF-8 characters and special break keys. Only the user with read/write access to the SSH session can send a break sequence to a target device.

You can configure up to 10 break sequences to be used in SSH Passthrough sessions.

The following special break keys are supported:

Table 14.2: Rack Power Manager Software - Supported SSH Passthrough Session Break Keys

Break Character	Description	Break Character	Description
\a	Alert	\z	Serial break [defined as Telnet break: IAC (\337), BREAK(\363)]
\b	Backspace	\\	Backslash
\d	Delay [preset value is 250 milliseconds]	\^	Circumflex
\f	Form-feed	ooo	Octal representation of a character (where ooo is one to three octal digits)
\n	New line	\c	Character c
\r	Carriage return	^?	Delete
\t	Tab	^c	Control character (c is "and"ed with 0x1f)
\v	Vertical tab	[UTF-8]	Any utf8 character

To configure break sequences:

1. Click the *System* tab.
2. Click *RPM Server* in the top navigation bar.
3. Click *SSH Passthrough* in the side navigation bar. The SSH Passthrough Properties window opens.
4. In the Delay field, you may enter the number of milliseconds to delay a command if **ld** is entered.
5. Enter the break sequence description in the Description field, then enter the break sequence in the Break Sequence field. Descriptions and break sequences are limited to 64 characters. Field numbers 0-9 are available for up to 10 break sequences.

To send a break sequence:

1. From an SSH Passthrough session, enter the escape sequence for the break sequence definition in the following format:

^Ecl[break sequence number 0-9]

For example: **^Ecl5**

2. The break sequence is sent to the target device and a confirmation message appears.

-or-

The SSH client indicates that the break sequence is invalid or contains a syntax error. You can correct the error and resend the break sequence.

Transferring read/write access

Only one user at a time can have read/write access to a shared SSH Passthrough or Emerson Session Viewer session. The first user who opens the session has read/write access. If that user exits a shared session, read/write access is granted to a randomly selected user who is sharing the session. A user with read-only access can enter a command to obtain read/write access.

To obtain read/write access:

1. From a shared SSH Passthrough or Avocent Session Viewer session where you have read-only access, enter the following command:

^Eca

2. The user with read/write access receives a message that read/write access has been transferred to the specified user.
3. You receive a message that the user has lost read/write access.

You now have sole read/write privileges to the SSH Passthrough or Avocent Session Viewer session. Transferring read/write access generates Rack Power Manager software system events.

Disconnecting a session

To disconnect an SSH session:

1. From an SSH Passthrough session, enter the following command:
^Ec.
2. Your session is closed. If you had read/write access to the session, read/write access is granted to a randomly selected user who is sharing the session.

Displaying session output

If a data log was created for the SSH Passthrough session, you can enter a command to display the last 30 lines (limited to 16384 characters) of the data log on the SSH client. The last 30 lines may include previous SSH sessions, but will only display target device output, not user actions.

NOTE: To display session output, data logging must be enabled and the user must have access rights to unit. See *User Access Rights* on page 220.

To display session output:

1. From an SSH Passthrough session, enter the following command:
^Ecr
2. The client displays the last 30 lines of the data log.

-or-

If you do not have access rights or if a data log was not created, an error message is displayed.

Grouping Units

The Rack Power Manager Explorer automatically groups managed appliances by the type of appliance (PM3000 24 Outlet switch, Liebert® MPH). Target devices are automatically grouped based on the type to which they are assigned.

You may also add and change the following types of groups:

- Sites
- Departments
- Locations
- Custom fields - Custom fields allow a user to create groupings of units which are accessed by all Rack Power Manager software users
- Personal and global unit groups - Global unit groups may be seen by all users; personal unit groups are visible only to the user who created the group

Site, Department and Location Groups

You may create one or more site, department and location names and then associate units with them. For example, you could create sites names such as Austin and Sunrise, department names such as Software Development and Human Resources or location names such as Lab Room 101 and System Administrator's Office.

Site, Department and/or Location columns may be included in a Units View window display, using the Customize link. See *Using the Customize link in windows* on page 30.

To group units by site, department or location, you first create a site/department/location, then associate units with it. Sites/departments/locations that contain units to which a user does not have access rights will not appear in the side navigation bar. The site/department/location must also have at least one unit associated with it to be displayed in the side navigation bar.

To add a site, department or location:

1. Click the *Units* tab.

2. To add a site, click *Sites* in the top navigation bar. The Sites window will open.

To add a department, click *Departments* in the top navigation bar. The Departments window will open.

To add a location, click *Locations* in the top navigation bar. The Locations window will open.

3. Click *Add*. The Add Site, Add Department or Add Location window will open.
4. Type a name, then click *Add*. The Sites, Departments or Locations window will open.

A site, department or location will not be listed in the side navigation bar until a unit has been associated with it.

To delete a site, department or location:

1. Click the *Units* tab.
2. To delete a site click *Sites* in the top navigation bar. The Sites window will open.
To delete a department, click *Departments* in the top navigation bar. The Departments window will open.
To delete a location, click *Locations* in the top navigation bar. The Locations window will open.
3. Click the checkbox to the left of one or more sites/departments/locations. To delete all sites/departments/locations in the page, click the checkbox to the left of Name at the top of the list.
4. Click *Delete*. A confirmation dialog box will appear.
5. Confirm or cancel the deletion.

To change the name of a site, department or location:

1. Click the *Units* tab.
2. To change the name of a site, click *Sites* in the top navigation bar. The Sites window will open.
To change the name of a department, click *Departments* in the top navigation bar. The Departments window will open.
To change the name of a location, click *Locations* in the top navigation bar. The Locations window will open.
3. Click on the name of a site/department/location. The Site/Department/Location Name window will open.
4. Type a new 1-64 character name.

5. Click *Save* and then click *Close*. The Sites, Departments or Locations window will open.

To associate or change the association of an existing unit to a site, department or location:

1. Click the *Units* tab.
2. Click one of the links listed in Table 15.1 in the side navigation bar to display the corresponding window for the units you wish to associate, change or remove the association.

Table 15.1: Links for Managing Sites, Departments or Location Associations

Link	Window	Changes Site Associations For
A link under Target Devices	Target Devices	Target devices only
A link under Appliances	Appliances	Managed appliances only
Sites	Units in Site	Units
Groups	Units in Group	Units
A link under Custom Field	Units in Custom Fields	Units
Recently Accessed	Recently Accessed Units	Units

3. Click on the name of a unit. The Unit Overview window will open.
4. Click *Properties* in the side navigation bar, then click *Location*.
5. From the menus, select the site, department and/or location to associate with the unit. If you do not wish to associate the unit with any site, department or location choose the top (empty) item from the menu.
6. Click *Save* and then click *Close*.

To display the units associated with a site, department or location:

1. Click the *Units* tab.
2. To display units associated with a site, click *Sites* in the side navigation bar. The Units in Site window will open, with a list of units associated with the first alphabetically-listed site.

To display units associated with a department, click *Departments* in the side navigation bar. The Units in Departments window will open, with a list of units associated with the first alphabetically-listed department.

To display units associated with a location, click *Locations* in the side navigation bar. The Units in Location window will open, with a list of units associated with the first alphabetically-listed location.

3. Click on a site, department, location link in the side navigation bar to display another entry in the unit list.

Custom Fields

Ten custom fields are available. To use the custom fields, first change the default labels on the fields (Custom Field 1, Custom Field 2 and Custom Field 3) and then associate a custom label with a unit. The custom fields may be displayed in Units View windows using the Customize link. See *Using the Customize link in windows* on page 30.

To define custom fields:

NOTE: You must have Software Administrator or Appliance Administrator access to define custom fields.

1. Click the *Units* tab.
2. Click *Custom Field Labels* in the side navigation bar. The Unit Custom Field Labels window will open.
3. For each custom field, type the 1-64 character name for the first custom field label. The first and second level custom fields for units will appear under this heading in the side navigation bar; all other custom fields will not appear in the side navigation bar but may be displayed in the content area by clicking *Customize* and adding the field.
4. Click *Save*.

The Custom Field Labels name will continue to appear in the side navigation bar until you associate the custom label with a unit.

To associate a custom label with a unit:

1. In a Units View window (see *Accessing Units View windows* on page 111), click on a unit. The Unit Overview window will open.
2. Click *Properties* in the side navigation bar and then click *Custom Fields*. The Unit Custom Fields window will open.
3. In the each field, type the 1-64 character name to associate with the corresponding label. You may also leave the field blank.
4. Click *Save* and then click *Close*. The Appliance - All window will open. The side navigation bar will include the names of the defined and associated custom fields.

Example: Custom fields

In the following example, a Rack Power Manager software administrator wants to examine a unit test configuration. The units will be placed in one of two categories: an initial configuration or a final configuration category. The administrator also wants to identify the unit's managers. At the present time, the Rack Power Manager software administrator has one DSR1021 switch and one EVR1500 environmental monitor to add to the test configuration category and one generic appliance to add to the final configuration category.

1. First, the Rack Power Manager software administrator will define the custom fields.
 - a. Click the *Units* tab.
 - b. Click *Custom Field Labels* in the side navigation bar. The Unit Custom Field Labels window will open.
 - c. In Label 1, type **Test Configuration**. All first-level custom fields for units will appear under this heading in the side navigation bar.
 - d. In Label 2, type **Appliances and target devices**. All second-level custom fields for units will appear under this heading in the side navigation bar.
 - e. In Label 3, type **Manager**. This custom field will not appear in the side navigation bar, but may be displayed in the content area by using the *Customize* link.
 - f. Click *Save* to save the changes.

Custom Field Labels will still appear in the side navigation bar because the administrator has not yet defined any custom fields for the units.
2. A DSR1021 switch has been added to the system, but will need to go into a category named Initial Configuration, since it has not yet been verified for the final configuration. The administrator will associate the DSR1021 switch managed by John Smith to the custom fields as follows:
 - a. Click *Appliances* in the side navigation bar. The Appliances - All window will open.
 - b. Click on the DSR1021 switch. The Unit Overview window will open.
 - c. Click *Properties* in the side navigation bar and then click *Custom Fields*. The Unit Custom Fields window will open, including the custom field names defined in step 1.
 - d. In the Test Configuration field, type **Initial Configuration**.
 - e. In the Appliances and target devices field, type **DSR1021 Switches**.
 - f. In the Manager field, type **John Smith**.

- Figure 15.1 indicates how the side navigation bar will appear after the example procedure. Clicking on a custom field link displays the units associated with that custom field.

Figure 15.1 indicates how the side navigation bar will appear after the example procedure. Clicking on a custom field link displays the units associated with that custom field.

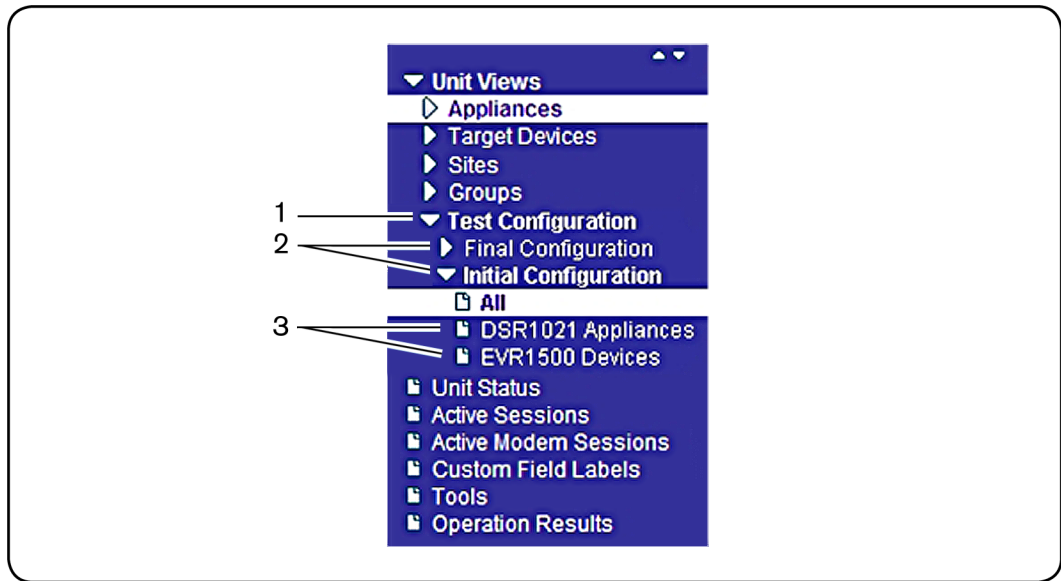


Figure 15.1: Custom Fields Example: Side Navigation Bar

Table 15.2: Custom Fields Example: Side Navigation Bar Descriptions

Number	Description
1	System-wide first-level custom field label
2	Unit first-level custom field labels
3	Unit second-level custom field labels

Unit Groups

Unit groups may be used to organize units. You may create nested unit groups (unit groups within unit groups) to organize units hierarchically. Units may belong to multiple groups. For example, you may have a DSR switch that belongs to two global groups and three personal groups.

There are two types of unit groups: global and personal. A global unit group can be viewed by any user logged into the Rack Power Manager software. A personal unit group may only be viewed by the person who created it. Up to 32 personal unit groups may be created by a user.

There are two top-level system-defined unit group containers: global root and personal root. These group containers cannot be deleted. They can contain other unit groups, but not individual units. All global unit groups are descendents of global root. All personal unit groups are descendents of personal root.

There is also a system-defined unit group named Unassigned, which is a descendent of the global root. This unit group automatically contains all units that are not assigned to any other global unit groups. This group cannot be deleted, and you cannot add subgroups (children) to the Unassigned unit group.

Global unit groups may only be created, modified or deleted by users with Rack Power Manager software administrator, user administrator or appliance administrator privileges. The global root, personal root and unassigned unit groups cannot be deleted.

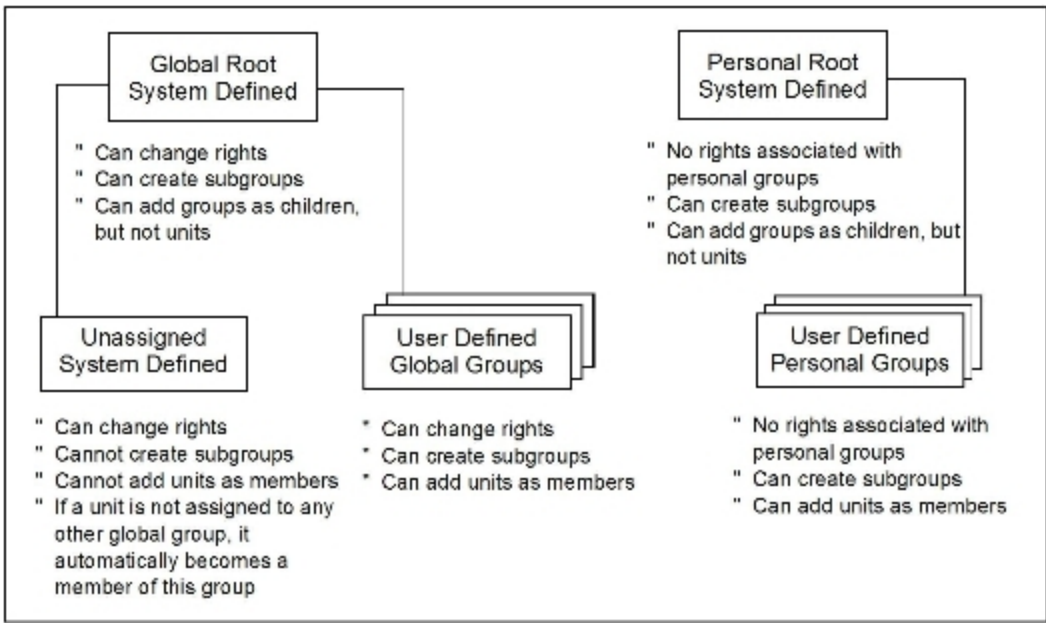


Figure 15.2: Unit Groups Structure

Table 15.3: Unit Groups Features

Group Type	Can change rights?	Can have sub-groups?	Can add units as members?
System Defined			
Global Root	Yes	Yes	No, can only add groups
Unassigned	Yes	No	No
Personal Root	No	Yes	No, can only add groups
User Defined			
Global Groups	Yes	Yes	Yes
Personal Groups	No	Yes	Yes

Unit group hierarchy

There are two primary ways to view unit groups:

- Unit Groups window - clicking the *Units* tab and then *Groups* in the top navigation bar
- Units View Groups window - clicking the *Units* tab and then *Groups* in the side navigation bar

Global groups that contain units the user cannot access will not be displayed, unless there are descendent groups containing units the user is allowed to access.

All personal unit groups are displayed in the Unit Groups window, even if they do not contain any units. In Units View Groups windows, groups will not be listed unless they have assigned units.

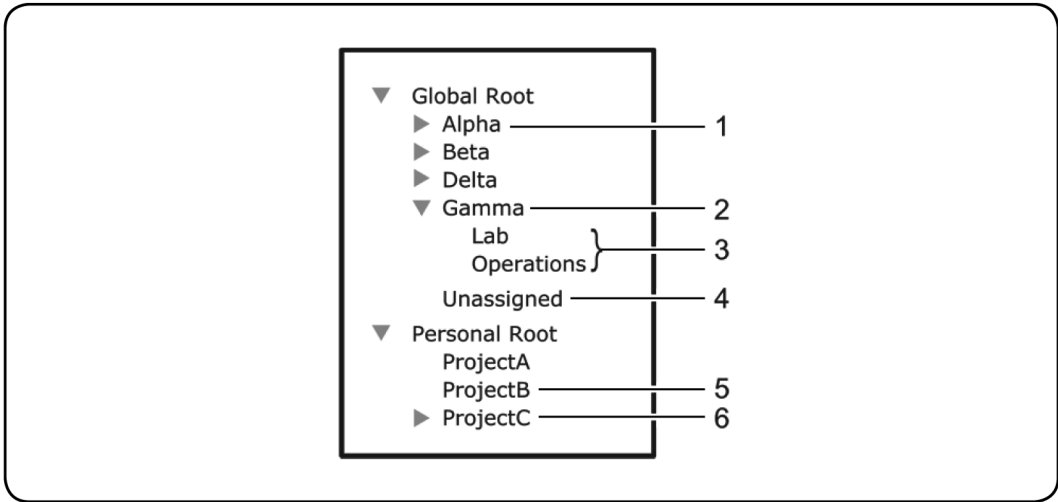


Figure 15.3: Unit Group Hierarchy Example

Table 15.4: Unit Group Hierarchy Example Descriptions

Number	Description	Number	Description
1	Global unit group Alpha has one or more subgroups	4	Global unit group Unassigned has all units that are not assigned to a group; it cannot have subgroups
2	Global Unit group Gamma has two subgroups	5	Personal unit group ProjectB has no subgroups
3	These unit groups do not have subgroups (in a Units view Group window, a document icon will appear to the left)	6	Personal unit group ProjectC has one or more subgroups

In the example, four unit groups have been created in the global root group, and each of those four unit groups contain groups. The unit group Gamma has been selected, and indicates it has two subgroups, Lab and Operations. The Unassigned global group will contain any units that are not assigned to another global unit group.

Three personal unit groups have been created. The ProjectA and ProjectB unit groups do not have subgroups. The ProjectC unit group has one or more subgroups.

To display a list of unit groups in the Unit Groups window:

1. Click the *Units* tab.
2. Click *Groups* in the top navigation bar. The Unit Groups window will open. If a unit group has subgroups (children), an arrow will be displayed next to its name.
 - To display a list of groups in the global root group, click *Global Root*. The first global unit group listed will automatically be selected. Click on the arrow next to a group to expand it and display subgroup names.
 - To display a list of groups in the personal root group, click *Personal Root*. The first personal unit group listed will automatically be selected. Click on the arrow next to a group to expand it and display subgroup names.

You may customize the number of items per page that appear in this window; see *Using the Customize link in windows* on page 30.

To display a list of unit groups in a Units View window:

NOTE: When you create a unit group, you may indicate whether it (and any of its child unit groups) will be displayed in the side navigation bar.

1. Click the *Units* tab.
2. Click *Groups* in the side navigation bar. The Groups - Global Root window will open.
 - If a unit group has subgroups (children), an arrow will be displayed next to its name.
When a selected group has subgroups, the window will display either the immediate children of the unit group or all descendants of the unit group, depending on the Show group descendants setting.
 - If a unit group does not have subgroups, a document icon will be displayed next to its name in the side navigation bar.

When you click on a unit group in the side navigation bar that has a document icon (that is, it has no subgroups), a window will open, listing the units in the group. This window can include the same fields as other Units View windows; see *Units View windows fields* on page 113. You may enable or disable a field display using the Customize link. See *Using the Customize link in windows* on page 30.

When you customize this window, you may also enable/disable the display of descendants. When enabled and a unit group is selected in a side navigation bar, the window will display all descendants of the group. When disabled, only the immediate children of the selected group will be displayed.

To display information about a unit group:

1. Click the *Units* tab.
2. Click *Groups* in the top navigation bar.
3. Click the group container or the parent group of the unit group you want to display information about.
4. Click on the unit group name.
5. The side navigation bar will contain information links about the selected unit group.
 - Click *Name* in the side navigation bar to display the unit group name.
 - Click *Members* in the side navigation bar to display the unit group members.
 - Click *Groups* to display a list of groups that are members of the unit group.
 - Click *Units* to display a list of units that are members of the unit group.
 - Click *Access Rights* in the side navigation bar to display the unit group access rights.
6. Click *Close*.

Adding or deleting a unit group**To add a unit group:**

1. Click the *Units* tab.
2. Click *Groups* in the top navigation bar. The Unit Groups window will open.
3. Click the checkbox next to the group container (Global Root or Personal Root) or the group name that you want to be the parent of the new unit group.
4. Click *Add*. The Add Unit Group window will open.
5. Type a 1-64 character name for the unit group. The name must be unique within the parent group. For example, two groups can be named “development” but they cannot both be members of the unit group “Huntsville.” (This unique name restriction does not apply to personal unit groups that are owned by different users.)
6. If you do not want the unit group (or any of its child unit groups) to appear in the side navigation bar, enable the *Do not display this unit group nor any child unit groups as unit views* checkbox.
7. If you do not want the units in the unit group to belong to any other unit group, select *Exclusive*.

8. If you want to add another unit group in the same hierarchy, click *Add/New*. The Add Unit Group window opens.

-or-

If you do not want to add another group, click *Add/Close*. The Unit Groups window closes.

To delete a unit group:

NOTE: Deleting a unit group deletes the group only; the units still exist in the Rack Power Manager software system. You cannot delete any system-defined unit groups (global root, personal root and unassigned.)

1. Click the *Units* tab.
2. Click *Groups* in the top navigation bar. The Unit Groups window will open.
3. Click the checkbox next to the unit group to be deleted.
4. Click *Delete*. A confirmation dialog box will appear.
5. Confirm or cancel the deletion.

Changing the unit group properties

Access rights indicate which users and user groups may access units in the Rack Power Manager software system. Access rights also indicate which actions are allowed. See *About Access Rights* on page 143. You can assign access rights from a unit group perspective, as described in this section. Using this method, selected users and members of selected user groups are allowed or prohibited from initiating certain actions on all units in the unit group.

Access rights for a unit group default to inherit if they are not explicitly granted to a user or user group. For example, if you create unit group A and subgroup B, by default any access rights you assign to group A will be propagated to group B.

There are other ways to assign access rights; see *How access rights can be assigned* on page 144.

To change unit group properties:

1. Click the *Units* tab.
2. Click *Groups* in the top navigation bar. The Unit Groups window will open.
3. Click on the name of a unit group. The Unit Group Name window will open.
4. Type a new 1-64 character name in the Group field. The name must be unique within the parent group. For example, two groups can be named “development” but they cannot both

be members of the unit group “Huntsville.” (This unique name restriction does not apply to personal unit groups that are owned by different users.)

5. If you do not want the unit group (or any of its child unit groups) to appear in the side navigation bar, enable the *Do not display this unit group nor any child unit groups as unit views* checkbox.
6. If you do not want the units in the unit group to belong to any other unit group, select *Exclusive*.
7. Click *Save* and then click *Close*.

To add or remove members in a unit group:

NOTE: Removing a unit group or unit member from a unit group does not delete the group/unit from the Rack Power Manager software system or any other group to which it belongs.

1. Click the *Units* tab.
2. Click *Groups* in the top navigation bar. The Unit Groups window will open.
3. To add or remove a group member of the unit group, click *Members* in the side navigation bar and then click *Groups*.

To add or remove a unit member of the unit group, click *Members* in the side navigation bar, and then click *Units*.

NOTE: If you select a group container (Global Root or Personal Root), you can only add unit groups as members - you cannot add units; therefore, when you click *Members* in the side navigation bar, *Groups* is the only choice. You cannot add units or groups to the global unassigned unit group.

4. The Unit Group Members (Units) or Unit Group Members (Groups) window will open. Click *Assign*.
5. The Assign Units to Unit Group window will open.

NOTE: Once a unit is added to an exclusive unit group, it cannot be added to any other groups. If a unit is already a member of a non-exclusive group and is then added to an exclusive group, the unit is automatically removed from the non-exclusive group.

- To add one or more units to the unit group, select the unit(s) from the Available Units list, then click *Add*. The units will be moved to the Units to Assign list.
 - To remove one or more units already assigned to the unit group, select the unit(s) from the Units to Assign list, then click *Remove*. The units will be moved to the Available Units list.
6. Click *Save* and then click *Close*. The Unit Group Members window will open.
 7. Click *Close*. The Unit Groups window will open.

To add or remove access rights for one or more unit groups:

1. Click the *Units* tab.
2. Click *Groups* in the top navigation bar. The Unit Groups window will open.
3. Click the checkbox to the left of one or more unit groups, then click *Rights*. The Unit Group Access Rights window will open.

If you are setting access rights for one unit group, you may click on the unit group name, then click *Access Rights* in the side navigation bar to access the Unit Group Access Rights window.

4. To add or remove a user or user group from the User and User Groups list:
 - a. Click *Edit List*. The Unit Access Rights User Selection window will open.
 - To add one or more users or user groups, select the user(s) or user group(s) from the Available list, then click *Add*. The users and/or user groups will be moved to the List to Update list.
 - To remove one or more users or user groups, select the user(s) or user group(s) from the List to Update list, then click *Remove*. The users and user groups will be moved to the Available list. (Inherited users and user groups can only be removed from the first unit group that specified any access rights other than inherit.)
 - b. Click *OK*. The Unit Access Rights window will display the current list of users and/or user groups. When a user or user group is added to the list, the default access rights will be displayed.
5. To set access rights, select a user or user group from the User and User Groups list, then enable or disable a checkbox in the Access Rights table for each access right.
 - Allow - the access right is allowed for the user/user group.
 - Deny - the access right is denied for the user/user group.
 - Inherit - the access right is inherited from the unit group(s) to which the selected user/user group belongs. When Inherit is selected, the Allow and Deny checkboxes will become gray and unchangeable, and indicate the inherited value. If the inherited settings indicated both Allow and Deny, the inherited value is Deny, which takes precedence.

To disable the inherit functionality, uncheck the Inherit checkbox.

If none of the checkboxes are checked, the access right is neither allowed nor denied.

If the unit group contains both appliances and target devices, all rights will be displayed and may be enabled, even though they may not necessarily be valid for the unit.

6. Repeat the preceding steps to change access rights for other users or user groups.
7. Click *Save* and then click *Close*. If a connection or power control action is enabled, the appropriate link will appear in the Action column of Units Views windows containing that group or units in that group.

Custom Groups

Custom groups may be created to calculate actual power usage. Custom groups would also allow power control operations for a group of target devices.

Adding or deleting a custom group query

To add a custom group:

1. Click the *Units* tab.
2. Click *Groups* in the top navigation bar.
3. Click the *Custom Group* menu. The Custom Group window opens.
4. In the Custom Groups window, click *Add*.
5. Type a 1-64 character name for the unit group.
6. If you do not want the custom group to appear in the side navigation bar, enable the *Do not display this unit group nor any child unit groups as unit views* checkbox.
7. If you do not want the units in the custom group to belong to any other group, select *Exclusive*.
8. If you want to add another custom group in the same hierarchy, click *Add/New*. The Add Custom Group window opens.

-or-

If you do not want to add another group, click *Add/Close*. The Custom Group window closes.

To delete a custom group:

1. Click the *Units* tab.
2. Click *Groups* in the top navigation bar.
3. Click the *Custom Group* menu. The Custom Group window will open.

4. Click the checkbox next to the unit group to be deleted.
5. Click *Delete*. A confirmation dialog box will appear.
6. Confirm or cancel the deletion.

Changing the custom group properties

To modify a custom group name:

1. Click the *Units* tab.
2. Click *Groups* in the top navigation bar.
3. Click the *Custom Group* menu. The Custom Group window will open.
4. To modify the name of the group, click on the custom group name and make the necessary changes.
5. Click *Close*.

Changing the custom group rights

You can assign access rights from a custom group perspective, as described in this section. Using this method, selected users and members of selected user groups are allowed or prohibited from initiating certain actions on all units in the custom group.

To add or remove access rights for one or more custom groups:

1. Click the *Units* tab.
2. Click *Groups* in the top navigation bar.
3. Click the *Custom Group* menu. The Custom Groups window opens.
4. Click the checkbox to the left of one or more custom groups, then click *Rights*. The Custom Group Access Rights window will open.
5. The Access Rights window will display the current list of users and/or user groups. When a user or user group is added to the list, the default access rights will be displayed.
6. To set access rights, select a user or user group from the User and User Groups list, then enable or disable a checkbox in the Access Rights table for each access right.
 - Allow - the access right is allowed for the user/user group.
 - Deny - the access right is denied for the user/user group.
 - Inherit - the access right is inherited from the unit group(s) to which the selected user/user group belongs. When Inherit is selected, the Allow and Deny checkboxes will become gray and unchangeable, and indicate the inherited value. If the inherited

settings indicated both Allow and Deny, the inherited value is Deny, which takes precedence.

To disable the inherit functionality, uncheck the Inherit checkbox.

If none of the checkboxes are checked, the access right is neither allowed nor denied.

7. Repeat the preceding steps to change access rights for other users or user groups.
8. Click *Save* and then click *Close*. If a connection or power control action is enabled, the appropriate link will appear in the Action column of Units Views windows containing that group or units in that group.

To add or modify the threshold values of a custom group:

1. Click the *Units* tab.
2. Click *Groups* in the top navigation bar.
3. Click the *Custom Group* menu. The Custom Groups window opens.
4. Click the checkbox to the left of the custom group, then click *Thresholds*.
5. Modify the values.
6. Click *Save* and then click *Close*.

Custom Group Reports and Scheduled Tasks

Individual reports, export data and schedule tasks can be done based on custom groups that have been created.

To generate individual reports and export data for a custom group:

1. Click the *Units* tab.
2. Click *Groups* in the top navigation bar.
3. Click the *Custom Group* menu. The Custom Groups window opens.
4. Click the checkbox to the left of the custom group, then click *Reports*.
5. Select the type of report: Comparative Power, Comparative Energy or Comparative Percentage Load.
6. Click *Run Report*.
7. The report is displayed as a line graph. Click the bar chart or table view icons to change the view, or click the interpolation icon to show only data points. If applicable, you may click the colored boxes below the report to show or hide report data for a category.

8. (Optional) If you selected an energy report, click the dollar sign (\$) icon to view cost information. The cost is calculated based on the cost per kilowatt hour rate configured for the data center.
9. Click *Export Data* if you wish to export and save the report data as .csv file.
10. Click *Close*.

To generate comparative reports and export data for a custom group:

1. Click the *Reports* tab, then click *Power* in the top navigation bar.
2. Select the Comparative Report.
3. Select the Custom Group from the drop-down menu.
4. Click *Run Report*.
5. Click *Export Data* if you wish to export and save the report data as a .csv file.

To schedule a task for a custom group:

1. Click the *System* tab.
2. Click *Tasks* in the top navigation bar. The Tasks window will open.
3. Click *Add*.
4. From the Task Type drop-down menu, select *Control Power of Custom Groups*.
5. Enter the Frequency and the Task name in the appropriate fields and click *Next*.
6. Select the Custom Group(s) and the desired task.
7. Click *Save* and *Close*.

To delete a task for a custom group:

1. Click the *System* tab.
2. Click *Tasks* in the top navigation bar. The Tasks window will open.
3. Click the checkbox next to the task(s).
4. Click *Delete*.

To run a task for a custom group:

1. Click the *System* tab.
2. Click *Tasks* in the top navigation bar. The Tasks window will open.
3. Click the checkbox next to the task(s).

4. Click *Run Now*.

DS Zones

DS Zones provide virtual segregation of data center resources, including appliances, target devices and virtual machines. Each zone operates as an independent subset of the Rack Power Manager software system, and units can be transferred to different zones. Users belong to a single zone, but may switch to other zones if they have access rights. You can restrict a user's access to a zone, preventing the user from viewing or accessing other zone's resources, or you can grant a user access to multiple zones. To prevent one zone from starving another of licenses, manage the distribution of licenses and add-on features by assigning a number of licenses to each zone.

Managing and Accessing Zones

Enabling DS Zones

Before you can create or access zones, you must add a DS Zones license key to the Rack Power Manager software (see *Adding a new license key* on page 60). The license key specifies the number of zones that can exist in the Rack Power Manager software. This number cannot be exceeded; if you need additional zones, you must purchase another license key or delete existing zones to free licenses.

NOTE: If you do not have a DS Zones license enabled, the Rack Power Manager software does not display any windows or links related to zones.

Creating zones

Once the DS Zones license key is enabled, the Rack Power Manager software automatically includes a top level zone. You can create up to two sublevels of zones below the top level zone, but you cannot create additional top level zones. You can create as many individual zones as your license key allows.

To create a new zone:

1. Click the *System* tab, then click *Zones*. The Zones window opens and lists any previously created zones.

2. Select the checkbox next to the zone to which you want to add a sublevel zone. Click *Add*. The Add Zone Wizard opens.
3. Enter a unique zone name. Click *Next*.
4. The Assign Zone Licenses window opens. For each license type, enter the number of licenses that can be used by this zone in the Assigned Licenses field. The number of available licenses is listed in the Available Licenses column. For details on zone licenses, see *Assigning zone licenses* on page 200.
5. Click *Next*.
6. The Assign Zone Rights window opens. For each access rights group, select *Allow* or *Deny*. For details on zone rights, see *Managing zone access rights* on page 201.
7. Click *Next*.
8. The *Completed Successful* window opens. Click *Finish*.

Accessing zones

When logging into the Rack Power Manager software, specify the highest level zone for which you have access rights. If your access rights include other zones, you may switch to those zones once logged in.

When in a zone, you cannot view or access units that belong to another zone. The zone you are currently in is referred to as the active zone and is displayed in the top option bar.

To specify zone log in options:

1. Click the *System* tab, then click *Global Properties*.
2. Select *Zones* in the side navigation bar.
3. Select *List all Zones as drop-down menu* to allow the user to select a zone from a list.

-or-

Select *Request the Zone as text field* to require the user to type the zone name in text field when logging in.

4. Click *Save*.

To log in to a zone:

1. Enter the URL of the Rack Power Manager server host in the address bar of a web browser.
2. Enter a valid username and password in the fields provided.

3. Specify the highest level zone for which you have access rights by typing the zone in the Zone field.

-or-

Specify the highest level zone for which you have access rights by selecting a zone name from the Zone menu.

NOTE: If you do not specify a zone, Rack Power Manager software attempts to log you in to the top level zone. If you do not have access rights to the top level zone, the login attempt fails.

4. Click *Login*.

To switch zones:

Click the *System* tab, then click *Zones*. The Zones window opens and lists all created zones. Select the checkbox next to the zone to which you want to switch and click *Switch*.

-or-

In the top left corner of the window, your username and the active zone list is displayed. Click the name of the zone to open a pop-up menu, then select the zone to which you want to switch.

Transferring units to a zone

You can transfer managed appliances, blade chassis, hypervisor managers or hypervisor servers to zones for which you have access rights. All associated target devices are transferred with the unit, and any merged target device connections are split. You cannot independently move a target device.

NOTE: If you are transferring units that require licenses, the zone to which you are moving the units must be assigned the appropriate licenses (see *Assigning zone licenses* on page 200). If the zone does not have sufficient licenses, the transfer fails.

1. In a Units View window (see *Accessing Units View windows* on page 111), click the checkbox next to the unit(s) you wish to move.
2. Click *Operations*, then select *Move Units to Zone* from the drop-down menu. The Move Units Wizard opens.
3. From the list provided, select the zone to which you wish to move the unit(s). Click *Next*.
4. The *Completed Successful* window opens. Click *Finish*.

You can access the units and associated target devices when you are active in the zone that owns the units.

Managing zone properties

Once you have created a zone, you can modify the zone name, license distribution and access rights.

To modify the zone name:

1. Click the *System* tab, then click *Global Properties*.
2. Select *Zones* in the side navigation bar.
3. Click the name of zone you wish to modify.
4. Click *Name* in the side navigation bar.
5. Enter a unique zone name in the field. The current zone path in relation to higher level zones is displayed.
6. Click *Save*.

Assigning zone licenses

You can manage the distribution of licenses among zones. Assigning licenses to each zone prevents one zone from starving other zones of licenses. You can control which add-on features a zone may use, how many licenses of each feature a zone may use, and how many sublevel zones can be created.

You must specify at least one client session license for each zone, including the top level zone; for other license types, you may specify an assigned license value of zero. The number of licenses assigned to one zone cannot exceed the number of licenses assigned to the parent zone. In addition, the total number of assigned licenses for all zones cannot exceed the number of licenses in the Rack Power Manager software system.

NOTE: For more information on what operations each license type allows, see *Licenses* on page 58.

To assign zone licenses:

1. Click the *System* tab, then click *Global Properties*.
2. Select *Zones* in the side navigation bar.
3. Click the name of zone you wish to modify.
4. Click *Licenses* in the side navigation bar.
5. The Assign Zone Licenses window opens. For each license type, enter the number of licenses that can be used by this zone in the Assigned Licenses field. The number of available licenses in the zone is listed in the Available Licenses column.
6. Click *Save*.

Managing zone access rights

When operating a Rack Power Manager software system with zones, there are multiple layers of access rights to consider.

First, you can allow or deny access rights per zone. If you deny an access right group for a zone, no users in that zone, including administrative users, can perform the associated actions. In addition, a user cannot create a sublevel zone with access rights that were denied in the parent zone. If you allow an access right group for a zone, specified users in this zone and sublevel zones can perform the associated actions.

The next layers of access rights are user groups and users. Within a zone, you can assign specific access rights to user groups. For example, for a zone with Firmware Management allowed, you could choose to only allow the administrative user group to manage firmware, and prevent other user groups from managing firmware by restricting the group access rights. To further control user access rights, you can also assign access rights to individual users.

An administrative user in the top level zone is considered a super user and can manage access rights for any user in any zone. Administrative users in sublevel zones with appropriate access rights can manage user access rights for their zone and other zones for which they have access.

When enabled for a zone, these access right groups permit qualified users to perform the following actions:

- Zone Management - Create zones and modify zone properties from the System - Zones window. Users with access rights can also switch to other zones.
- User and User Groups Management - Add or delete users and user groups, and perform other user and user group management operations from the Users tab.
- Unit and Unit Groups Management - Add or delete units and unit groups, and perform other unit and unit group management operations from the Units tab.
- File Management - Add or delete appliance files from the System - Appliance Files window.
- Tasks Management - View, schedule and run tasks from the System - Tasks window.
- Firmware Management - Upgrade appliance firmware.
- System Management - View and modify some system settings.
- Log Viewing - View event logs, data logs and reports under the Reports tab.

To allow or deny access rights for a zone:

1. Click the *System* tab, then click *Global Properties*.
2. Select *Zones* in the top navigation menu.

3. Click the name of zone you wish to modify.
4. Click *Access Rights* in the top navigation menu.
5. The Assign Zone Rights window opens. For each access rights group, select *Allow* or *Deny*.
6. Click *Save*.

Using Zones

Zones operate as independent subsets of the Rack Power Manager software system. When logged into a zone, most actions only affect your active zone, even if you have access rights to other zones. However, some actions are restricted or are only available to super users (administrative users belonging to the top level zone). All actions require appropriate zone access rights. Users must also be qualified with user and user group access rights. The following sections describe under what circumstances an action may be performed and how it affects the Rack Power Manager software system.

Units actions in a zone

NOTE: As an exception, a modem is still available to all zones even if it is moved to a sublevel zone.

Table 16.1: Unit Actions in a Zone

Action	User Status Required for Action	Zone(s) Affected
View units	Any qualified user	Active zone only.
Add or delete units	Any qualified user	Active zone only.
Update unit properties	Any qualified user	Active zone only. NOTE: Appliance IP addresses must be unique across all zones.
Move units to another zone	Any qualified user	To other zones for which he has access rights.
Use unit operations and tools	Any qualified user	Active zone only. NOTE: If the operation or tool involves multiple units, all units must be in the same zone.
View unit groups	Any qualified user	Active zone only.

Action	User Status Required for Action	Zone(s) Affected
Add unit groups	Any qualified user	Active zone only. NOTE: The user group name must be unique within the active zone, but can be duplicated in other zones. When a zone is created, three groups are automatically created: global root, unassigned and personal root.
Delete unit groups	Any qualified user	Active zone only. NOTE: The global root, unassigned and personal root groups cannot be deleted.
Assign units to unit groups	Any qualified user	Active zone only.
Add or remove sites, departments or locations	Any qualified user	Active zone only. NOTE: The site, department or location name must be unique within the active zone, but can be duplicated in other zones. If a unit is moved to another zone, any associated sites, departments or locations are deleted.
Import or export units, unit groups, users, user groups and associated relationships	Any qualified user	To or from the active zone only.

User actions in a zone

Table 16.2: User Actions in a Zone

Action	User Status Required for Action	Zone(s) Affected
View user accounts	Any qualified user	Active zone only.

Action	User Status Required for Action	Zone(s) Affected
Add or delete users	Any qualified user	Active zone only. NOTE: When adding a user, the username must be unique within the active zone, but can be duplicated in other zones. When using the Add User Wizard, only authentication services and groups that belong to the active zone can be selected.
Move users or user groups to a zone	Not permitted for any user	Users and user groups cannot be moved user to another zone. NOTE: A user or user group is permanently owned by the zone that was active when the user was added, but a user can visit (switch to) other zones. If necessary, you can delete a user or user group from its zone and recreate it in another zone.
View user groups	Any qualified user	Active zone only.
Add or delete user groups	Any qualified user NOTE: Built-in user groups cannot be deleted.	Active zone only. NOTE: The user group name must be unique within the active zone, but can be duplicated in other zones. When using the Add User Group Wizard, only authentication services that belong to the active zone can be selected.
View or export authentication services	Any qualified user	Active zone only.

Action	User Status Required for Action	Zone(s) Affected
Add authentication services	Any qualified user	Active zone only. The same authentication service cannot be reused in multiple zones. The authentication service must be added to each zone where it will be used. As a result, virtual users may end up in multiple zones, but each instance of the user in a zone is treated as unique user in the Rack Power Manager software system.
Move authentication services	Not permitted for any user	An authentication service cannot be moved to another zone. NOTE: An authentication service is permanently owned by the zone that was active when the authentication services was added. If necessary, you can delete an authentication service from its zone and recreate it in another zone
Assign unit access rights to users	Any qualified user	Active zone only. Both the user and unit must belong to the active zone.
Assign users to groups	Any qualified user	Active zone only. Both the user and group must belong to the active zone.
View effective rights for users	Any qualified user	Active zone only.

Reports, events and data logging actions in a zone

Table 16.3: Reports, Events and Data Logging Actions in a Zone

Action	User Status Required for Action	Zone(s) Affected
View system logs and events	Any qualified user	For all zones for which he has access rights.

Action	User Status Required for Action	Zone(s) Affected
View or export data logs	Any qualified user	Active zone only.
View and modify email notifications	Any qualified user	Active zone only.
Modify log retention	Super users only	All zones.
Modify events	Super users only	All zones.
View usage and asset reports	Any qualified user	Active zone only.

Modifying system settings in a zone

Table 16.4: Modifying System Settings in a Zone

Action	User Status Required for Action	Zone(s) Affected
Modify Rack Power Manager server settings	Super users only	All zones.
Modify global properties	Super users only	All zones.
Back up the Rack Power Manager server database and system files	Super users only	All zones.
Schedule power control	Any qualified user	All zones.
Export event log	Any qualified user	Active zone only.
Migrate units	Any qualified user	Active zone only.
Pull names from selected units	Any qualified user	Active zone only.
Test modem connection	Any qualified user	All zones.
Update topology	Any qualified user	Active zone only.
Upgrade firmware	Any qualified user	Active zone only.
Validate external authentication services user accounts	Any qualified user	Active zone only.
View appliance files	Any qualified user	Active zone only.

Action	User Status Required for Action	Zone(s) Affected
Manage plug-ins	Super users only	All zones.
Configure SNMP trap settings	Any qualified user	Active zone only.
Import system settings	Super users only	To the top level zone only. The top level zone must be active at the time of import.

Managing User Accounts

This chapter describes how to manage user accounts. The Rack Power Manager software allows you to:

- Add, change and delete user accounts
- Unlock user accounts
- Specify user account restrictions
- Change user group membership
- Display user and user group access rights to target devices and managed appliances
- Add and delete user-defined user groups
- Display, assign and remove user group members from built-in or user-defined user groups

User Accounts Windows

User accounts are displayed and managed through User Accounts windows.

To display the User Accounts window:

1. Click the *Users* tab. The User Accounts - All window will open.
2. To display the names of users in a built-in or user-defined user group, click the group name link under User Accounts in the side navigation bar. The User Accounts window for that group will open, listing all the users in the group.
3. To select a user, click on a username in a User Accounts window.

Customizing the User Accounts window

The User Name field is usually displayed in the User Accounts window. One of the icons in Table 17.1 will appear to the left of the usernames and represent the status of each Rack Power Manager software user.

Table 17.1: User Status Icons

Icon	Authentication Method	Status
Face	All	Enabled - The user can log in and use the Rack Power Manager software.
Face with a red X	Internal	Disabled - The user cannot log in to the Rack Power Manager software. See <i>User account restrictions and expiration settings</i> on page 217.
Padlock	Internal	Locked - The user account has been locked; the user cannot log in to the Rack Power Manager software because the maximum number of log in failures has been exceeded. See <i>Authentication Services</i> on page 81 and <i>Unlocking User Accounts</i> on page 214.
Question mark	External	Suspicious - The user account exists, but the external authentication server no longer contains the account.
Face with a clock	All	Expired - The user account is configured with an expiration date, which has passed. Expired user accounts remain in the system until deleted. See <i>User account restrictions and expiration settings</i> on page 217.

The following fields may be displayed in the User Accounts window. Use the Customize link to add or remove fields in the display. See *Using the Customize link in windows* on page 30.

- Full Name - Another name for a user. For example, a user may have a username of Sunrise1 and a full name defined as Mary Jones. See *Username* on page 215.
- Status - User account status: Enabled, Disabled, Locked, Suspicious or Expired. One of the user status icons in Table 17.1 will appear to the left of the username.
- Preemption Level - Effective preemption level of a user.

When a User Accounts window contains this column or a Group Preemption Level column, values are not displayed for external users (users validated with external authentication services). To display an external user's effective and group preemption level, select the user's name and then click *Preemption Levels* in the side navigation bar.

- Authentication Server - Name of the internal or external authentication server. See *Authentication Services* on page 81.
- Business Address - Business address defined in the user's properties. See *Address* on page 219.
- Business Mobile - Business mobile phone number defined in the user's properties. See *Phone contact* on page 219.

- **Business Phone** - Business phone number defined in the user's properties. See *Phone contact* on page 219.
- **Default E-Mail** - Default email account defined in the user's properties. See *Email contact* on page 219.
- **E-Mail 1-E-Mail 5** - Up to five additional email accounts defined in the user's properties. See *Email contact* on page 219.
- **Custom Field 1- Custom Field 6** - Custom fields for the user. If you have specified text for a custom field, that text will display when you display the field. See *Custom field properties* on page 220.
- **Group Preemption Level** - Highest preemption level of all groups to which the user belongs. For example, if a user belongs to appliance administrators (with a group preemption level of 3) and auditors (with a group preemption level of 1), this field will display 3.

When a User Accounts window contains this column or a Preemption Level column, values are not displayed for external users (users validated with external authentication services). You may display an external user's effective and group preemption level by selecting the user's name and then clicking *Preemption Levels* in the side navigation bar.

- **Home Address** - Home address defined in the user's properties. See *Address* on page 219.
- **Home Phone** - Home phone number defined in the user's properties. See *Phone contact* on page 219.
- **Mobile Phone** - Mobile phone number defined in the user's properties. See *Phone contact* on page 219.
- **Pager** - Pager number defined in the user's properties. See *Phone contact* on page 219.
- **User Preemption Level** - User preemption level defined in the user's properties.

Adding User Accounts

The following information is configured when a user account is created:

- Whether the user will be authenticated using the Rack Power Manager software internal authentication or an external authentication server. See *Authentication Services* on page 81.
- The user groups in which the user will be included. Each user group contains specific access rights that allow a user to perform specific actions. See *User Groups* on page 223.
- The preemption level for interrupting or disconnecting serial or KVM sessions.

You must have Rack Power Manager software administrator or user administrator rights to add a user.

To add a user account:

1. Click the *Users* tab.
2. Click *Add*. The Add User Account Wizard will appear.
3. The Select Authentication Service window will open. This window lists the Rack Power Manager software internal service and all the external authentication services that have been added, which may be used to authenticate users when they log in. See *Authentication Services* on page 81.

Select an authentication service and then click *Next*.

- If you selected *RPM Internal*, go to step 4.
 - If you selected any other authentication service, go to step 5.
4. The Type in User Credentials window will open.
 - a. Type a username, password and confirm the password of the user you are adding.

Usenames may contain up to 256 non-case sensitive characters (if a RADIUS external authentication service will be used, the limit is 253 characters).

Usenames are case-preserving. For example, if an account named JDoe is created, it will be saved as JDoe in the Rack Power Manager server, but a user may log in as JDoe, jdoe, JDOe and so on.

Passwords may contain 3-64 characters. Passwords will never expire unless *User must change password at next login* is selected in the Unit Password window, or Passwords Expire information is specified in the Authentication Service User Account Policies window. A Rack Power Manager software administrator may specify a different minimum character length and change expiration criteria. See *Authentication Services* on page 81.

- b. To enable users to set their own passwords when they log in to the Rack Power Manager software, click *User must change password at next login*.
 - c. To designate the account as a service account, select the *Service Account* checkbox. A service account cannot be used to log in to the Rack Power Manager software. A service account can be used to impersonate another user over the Web Services API or GUI Access API. For more information, see the Rack Power Manager software SDK online help.

NOTE: A service account may only be created if you selected the Rack Power Manager software internal authentication service in step 3.

- d. Click *Next*. Go to step 6.
5. The Specify User Name window will open.

If you selected RADIUS, TACACS+ or RSA SecurID in step 3:

- a. Enable the Specify user on external authentication service radio button.
- b. Type the username that is configured on the RADIUS, TACACS+ or RSA SecurID server.
- c. Click *Next*.

If you selected any other type of external authentication service in step 3, you may either specify the username or find the user on the external authentication service.

- To specify the user, enable the *Specify user on external authentication service* radio button and type the name of the user. Then click *Next*.

Usenames may contain up to 256 characters. Usumames may or may not be case sensitive, depending on the requirements of the external authentication server.

- To find the user, enable the *Find user on external authentication service* radio button. The Select User from External Authentication Service window will open.

If the list of users contains more than 5000 entries, a message will indicate that not all items are displayed. You may filter the list by using the Filter button and the adjacent text field. Specifying a username in the text field will return all valid matches. If filtering on another item (such as full name), you must include a wildcard. See *Filtering information in a window* on page 29.

Select one or more users from the list, then click *Next*.

6. Assign the user to user groups from the Available Groups list, which includes all built-in and user-defined groups. Select one or more groups and click *Add*. The group names will move to the Member Of list, and the new user(s) will be added to those groups. Click *Next*.
7. From the Preemption Levels menu, select a preemption level from 1-4; the higher the number, the higher the preemption level.
8. Click *Finish*. The user(s) have been added.

The Rack Power Manager software obtains external group membership and external user information when a user logs in. If a user's group membership changes or the user is deleted

externally, the Rack Power Manager software will not see those changes until the next time that user logs in.

Deleting User Accounts

To delete one or more user accounts:

1. Click the *Users* tab.
2. Click the checkbox to the left of the username(s). To delete all users on the page, click the checkbox to the left of User Name at the top of the list.
3. Click *Delete*. A confirmation dialog box will appear.
4. Confirm or cancel the deletion.

Unlocking User Accounts

If lock-out settings have been specified for the Rack Power Manager internal authentication service and a user exceeds these settings, the user will not be allowed to attempt another log in until a certain amount of time has passed. Users that have been locked out will appear with a lock next to their name in the User Accounts window and *Locked* will appear in the Status column.

User administrators or administrators may manually unlock the user accounts.

To unlock one or more user accounts:

1. Click the *Users* tab.
2. In a User Accounts window, click the checkbox to the left of the username(s).
3. Click *Unlock*.

Resetting a User Account Password

A Rack Power Manager software administrator or user administrator may reset a user's password. When a password is reset, the user will be required to login by typing **password** as their password, then enter and verify a new password for their account the next time they start a new Rack Power Manager software session.

To reset a user account password:

1. Click the *Users* tab.
2. Click the checkbox to the left of the user(s) to reset the password.
3. Click *Reset Password*. A confirmation dialog box will appear.

4. Confirm or cancel the reset.

Changing User Account Properties

If you have Rack Power Manager software administrator or user administrator privileges, you may change the following account properties for a user:

- The user (login) name and full name
- The certificate associated with the user
- The SSH key associated with the user
- Login password
- Account login restrictions and expiration settings
- The user groups to which the user is assigned
- User preemption levels
- Home and business addresses
- Home, business, mobile and pager phone numbers
- Primary email address and up to five additional email addresses
- Notes you wish to add about the user
- Up to six custom fields

Some properties may be changed only if the user account will be using the Rack Power Manager software internal authentication service. See *Authentication Services* on page 81.

Username

The username information that you may specify for a user includes:

- User Name - The name that the Rack Power Manager software uses to log in and identify the user.
- Full Name - The actual name of the user.

For example, you may use Engr10 as the username and Jonathan Z. Smith as the full name to identify the person associated with the username.

To change the name of a user:

1. Click the *Users* tab.
2. Click on a username. The User Name window will open.

3. Type the username for the user.
4. Type the full name of the user.
5. Click *Save* and then click *Close*.

User certificates

Certificates may be changed only for internal authentication users. If the system certificate policy is enabled for user certificates (see *System certificate policy and trust store* on page 50), the user certificate used at login must meet the policy requirements.

As an alternative to using this method, the user may change the certificate in the profile settings, but only if the administrator has enabled a global setting to allow it. See *Specifying a user certificate* on page 41.

To change the certificate associated with a user:

1. Click the *Users* tab.
2. Click on a username. The User Name window will open.
3. Click *Credentials* in the side navigation bar and then click *Certificate*. The User Certificate window will open. If a certificate has failed a test required in the system certificate policy, the failure information is displayed.
4. Type the path and name of the certificate or browse to the certificate location.
5. Click *Save* and then click *Close*.

User SSH key

A configurable SSH key may be used by a serial console appliance to authenticate a Rack Power Manager software user who is using an out of band client (for example, someone using a PuTTY SSH client that was not started by the Rack Power Manager software). The user supplies the public/private SSH key when connecting to the serial console appliance (only RSA keys with a maximum length of 1024 bits are allowed). The appliance then verifies the public key against the one stored for the user in the Rack Power Manager software.

As an alternative to using this method, the user may specify the SSH key in the profile settings, but only if the administrator has enabled a global setting to allow it. See *Specifying an SSH key* on page 42.

To specify a user SSH key:

1. Click the *Users* tab.
2. Click on a username. The User Name window will open.

3. Click *Credentials* in the side navigation bar and then click *SSH Key*. The User SSH Key window will open.
4. Type the 1-256 character name of the file containing the public SSH key that was generated by a third party key generator or browse to the file location.
5. Click *Save* and then click *Close*. The SSH key file will be uploaded to the Rack Power Manager server for use in authenticating the user.

User password

A user's password may be changed or you may specify that a user must enter a new password during the next login. The password may be changed only for internal authentication users.

To change a user password or force a new password:

1. Click the *Users* tab.
2. In a User Accounts window, click on a username. The User Name window will open.
3. Click *Password* in the side navigation bar. The User Password window will open.
4. Type the new password for the user and verify the new password.
5. To force a user to define a new password during the next login, enable the *User must change password at next login* checkbox.
6. Click *Save* and then click *Close*.

User account restrictions and expiration settings

Account restriction and expiration settings may be changed only for internal authentication users.

To change user account restrictions and expiration settings:

1. Click the *Users* tab.
2. Click on a username. The User Name window will open.
3. Click *Restrictions* in the side navigation bar. The User Account Restrictions window will open.
4. To change account restrictions:
 - To prevent the user from logging into the Rack Power Manager software, enable the *Disable user account* checkbox. (Users with open sessions will remain logged in.) To re-enable the user account, uncheck the *Disable user account* checkbox.

- To force a user to define a new password during the next login, enable the *User must change password at next login* checkbox.
- To prevent the user from changing the password, enable the *User cannot change password* checkbox.
- To prevent a user's password from expiring, enable the *Click Password never expires* checkbox.
- To designate the account as a service account, enable the *Service Account* checkbox. A service account cannot be used to log in to the Rack Power Manager software. A service account can be used to impersonate another user over the Web Services API or GUI Access API. For more information, see the Rack Power Manager software SDK online help.

NOTE: A service account may only be created if you are using the Rack Power Manager software internal authentication service.

5. To change account expiration settings:
 - To indicate no expiration date, enable the *Never* radio button.
 - To specify an expiration date, enable the *End of* radio button. Then click the button to the right of the adjacent field, and a calendar will be displayed. Select the date when the user account will expire.

When a user account expires, it remains in the Rack Power Manager software system until the account is deleted.

6. Click *Save* and then click *Close*.

User group membership

See *User Groups* on page 223.

To change the group membership of a user:

1. Click the *Users* tab.
2. Click on a username. The User Name window will open.
3. Click *User Groups* in the side navigation bar. The User Group Membership window will open.
4. To add a user to one or more groups, select the group(s) in the Available Groups list, then click *Add*. The columns will be moved to the Member Of list.

5. To remove the user from one or more groups, select the group(s) in the Member Of list, then click *Remove*. The groups will be moved to the Available Groups list.
6. Click *Save* and then click *Close*.

The Rack Power Manager software obtains external group membership and external user information when a user logs in. If a user's group membership changes or the user is deleted externally, the Rack Power Manager software will not see those changes until the next time that user logs in.

Address

The user address may be changed only for internal authentication users.

To specify address information for a user:

1. Click the *Users* tab.
2. Click on a username. The User Name window will open.
3. Click *Addresses* in the side navigation bar. The User Address Properties window will open.
4. Type the home address and business address of the user.
5. Click *Save* and then click *Close*.

Phone contact

The phone contact may be changed only for internal authentication users.

To specify phone contact information for a user:

1. Click the *Users* tab.
2. Click on a username. The User Name window will open.
3. Click *Telephones* in the side navigation bar. The User Telephone Properties window will open.
4. Type the home phone number, business phone number, mobile phone number, mobile business phone number and/or pager number of the user.
5. Click *Save* and then click *Close*.

Email contact

Email contacts may be changed only for internal authentication users.

To specify email contact information for user:

1. Click the *Users* tab.

2. In a User Accounts window, click on a username. The User Name window will open.
3. Click *E-Mail Addresses* in the side navigation bar. The User E-Mail Properties window will open.
4. Type the primary email address of the user and up to five additional email addresses.
5. Click *Save* and then click *Close*.

User notes

User notes may be changed only for internal authentication users.

To specify notes about a user:

1. Click the *Users* tab.
2. Click on a username. The User Name window will open.
3. Click *Notes* in the side navigation bar. The User Notes window will open.
4. Type any information you wish.
5. Click *Save* and then click *Close*.

Custom field properties

You may specify any information you wish in the six custom fields. Custom field properties may be changed only for internal authentication users.

To change the custom fields:

1. Click the *Users* tab.
2. Click on a username.
3. Click *Custom Fields* in the side navigation bar. The User Custom Fields window will open.
4. Type information in the fields.
5. Click *Save* and then click *Close*.

User Access Rights

Access rights indicate whether a user is allowed to perform certain actions on a unit in the Rack Power Manager software system. See *About Access Rights* on page 143 for detailed information and a list of actions that can be enabled/disabled for target devices and managed appliances.

You may assign access control rights from a user perspective. You select a user account, specify the units for which rights will be assigned, then indicate the permission to perform the action (none, allow, deny or inherit) for each unit. That procedure is described in this section.

There are other ways to assign access rights:

- From a user group perspective - see *User Group Access Rights* on page 229
- From a unit perspective - see *Unit Access Rights* on page 144
- From a unit group perspective - see *Changing the unit group properties* on page 189

To display a user's access rights:

1. Click the *Users* tab.
2. Click on a username. The User Name window will open.
3. Click *Effective Rights* in the side navigation bar and then click *All Units* or *Appliances*. The Appliance Effective Rights window will open. Columns indicate the available actions for the unit.
 - Black check mark - The user has been granted access for this right.
 - Gray check mark - A group to which the user belongs has been granted access for this right.
 - Black X - The user has been denied access for this right.
 - Gray X - A group to which the user belongs has been denied access for this right.
 - No check mark - No access has been granted or denied for this right.
4. Click *Close* when you are finished reviewing the access rights. The User Accounts window will open.

Customizing Appliance Access Rights windows

The Name field is always displayed in the Appliance Access Rights window. The action fields may also be displayed (see *About Access Rights* on page 143). Use the Customize link to add or remove fields in the display. See *Using the Customize link in windows* on page 30.

To add or remove access rights through a user account:

1. Click the *Users* tab.
2. Click on a username.
3. Click *Access Rights* in the side navigation bar. The User Access Rights window will open.

4. To add or remove a unit or unit group from the Unit and Unit Groups list, click *Edit List*. The User Access Rights Unit Selection window will open.
 - To add one or more units/unit groups, select the units/groups in the Available list, then click Add. The units/unit groups will be moved to the List to Update list.
 - To remove one or more units/unit groups, select the units/groups in the List to Update list, then click Remove. The units/unit groups will be moved to the Available list. (Inherited users and user groups can only be removed from the first unit group that specified any access rights other than inherit.)
5. Click *OK*. The User Access Rights window will display the current list of units/unit groups.
6. To add/remove access rights for a unit/unit group, select a unit or unit group from the Unit and Unit Groups list, then enable or disable a checkbox in the Access Rights table for each access right.
 - Allow - the access right is allowed for the user.
 - Deny - the access right is denied for the user.
 - Inherit - the access right is inherited from the unit group(s) to which the selected unit/unit group belongs. When *Inherit* is selected, the Allow and Deny checkboxes will become gray and unchangeable, and indicate the inherited value. If the inherited settings indicated both Allow and Deny, the inherited value is Deny, which takes precedence.

To disable the inherit functionality, uncheck the Inherit checkbox.
 - If none of the checkboxes are checked, the access right is neither allowed nor denied.
7. Repeat the preceding step for other units/unit groups.
8. Click *Save* and then click *Close*.

User Groups

Users that have been added to the Rack Power Manager software system may be added to the following two types of user groups:

- **Built-In** - The Rack Power Manager management software is delivered with six predefined user groups: Appliance Administrators, Auditors, Rack Power Manager software administrators, Everyone, User Administrators and Users. All users are automatically included in the Everyone user group when they are added to the Rack Power Manager software system. Users may be added to any of the other user groups. The privileges that a user has to perform tasks on the Rack Power Manager software system is dependent on the built-in user group to which the user is a member. See *Built-in User Groups* on page 43.
- **User-defined** - You may also define custom groups, based on any criteria you wish. For example, you may want to define groups based on user administrators with read-only access, software developers at a specific location, global network infrastructure personnel based on job title and so on.

Built-in user groups appear in the User Groups - Built-in window and user-defined user groups appear in the User Groups - User Defined window. The Preemption Level column will indicate the preemption level of each user group. The windows may also display the following fields. Use the Customize link to add or remove fields in the display: See *Using the Customize link in windows* on page 30.

- **Authentication Server** - Name of the authentication server assigned to the user. See *Authentication Services* on page 81.
- **Role** - Role of a user-defined user group, which may be None, User, Auditor, Appliance Administrator, User Administrator or Rack Power Manager Administrator. The role column for a built-in user group or a user-defined user group with a role of None will be empty.
- **Type** - Type of user group, which will be built-in or user-defined.

To display user groups:

1. Click the *Users* tab.

2. Click *Groups* in the top navigation bar. *Built-In* will automatically be selected in the side navigation bar and the User Groups - Built-in window will open. To display the user-defined groups, click *User-Defined* in the side navigation bar. The User Groups - User Defined window will open.

Group naming in external authentication services

Groups in Active Directory (AD) external authentication services are specified using a combination of their Active Directory folder and group name, minus the group container specified in the Rack Power Manager software.

The group container defaults to the AD domain root if it is unspecified.

For example, if you have an AD external authentication service for the “sw.eng.mydomain.com” domain with no group container specified, the “Domain Users” group in the “sw.eng.mydomain.com/Users” folder will have a Rack Power Manager software equivalent of “Users/Domain Users”.

Using the same example, but with a group container of “Users”, the Rack Power Manager software equivalent is “Domain Users”.

Using the same example, but with a group container of “mydomain.com”, the Rack Power Manager software equivalent is “eng/sw/Users/Domain Users”.

Groups in LDAP external authentication services are specified using a modified distinguishedName of their LDAP object, minus the group base DN specified in the Rack Power Manager software.

For example, if you have an LDAP external authentication service with a group base DN of “ou=myldap,c=US”, the “cn=Admin Users,ou=Users,o=myldap,c=US” group will have a Rack Power Manager software equivalent of “Admin Users”.

Using the same example, but with the “cn=Admin Users,c=Sunrise,ou=Users,o=myldap,c=US” group, the Rack Power Manager software equivalent is “Sunrise/Admin Users”.

Adding User-defined User Groups

If you are using Rack Power Manager software internal authentication, you may add your own custom user-defined user groups and then add other users that use Rack Power Manager internal authentication as members.

External user-defined user groups (on external authentication servers) may be added, but their membership is not controlled by the Rack Power Manager software.

NOTE: You must have Rack Power Manager software administrator or user administrator rights to add user-defined user groups.

Rack Power Manager software internal, RADIUS, LDAP, Windows NT or Active Directory authentication services

To add a user-defined user group:

1. Click the *Users* tab. Click *Groups* in the top navigation bar. Click *User-Defined* in the side navigation bar. The User Groups - User Defined window will open.
2. Click *Add*. The Add User Group wizard will appear.
3. The Select Authentication Service window will open. This window lists all authentication services that may be used to authenticate the user group when the user logs in. See *Authentication Services* on page 81.

Click on the name of an authentication service and then click *Next*.

- If you selected *Rack Power Manager Internal* as the authentication service, go to step 4.
- If you selected any other type of authentication service, go to step 5.

NOTE: If you are adding a group to the TACACS+ authentication service, see *TACACS+ external authentication services* on page 226 for more information.

4. The Type in Internal Group Name window will open. Type the name for the new user group you wish to create. User-defined user group names are case-preserving and may contain up to 256 characters. Go to step 7.

NOTE: When access rights are assigned to internal user groups, the internal group users must also be members of a built-in user group to define their role in the Rack Power Manager software. See *Built-in User Groups* on page 43.

5. The Specify External Group window opens. Complete one of the following steps, then click *Next*:
 - Click *Specify a group on external authentication service* and type the name of the group in the field.

User group names may contain up to 256 non-case sensitive characters. User group names are case-preserving if the user group on the external authentication server is case sensitive. See *Group naming in external authentication services* on page 224.
 - Click *Import the external group - Everyone* to consider any user on the external authentication server as a member of this user group.

- Click *Find a group on external authentication service* to choose from the list of groups on the external authentication service. If the list of groups contains more than 5000 entries, a message will indicate that not all items are displayed.

You may filter the list by using the Filter button and the adjacent text field. If you are using an Active Directory Server, you can choose the filter method.

Click *Filter in Rack Power Manager Server (legacy)* to use a traditional filtering method; see *Filtering information in a window* on page 29.

-or-

Click *Filter in Active Directory Server* to use a modified filtering method that only provides matches to the filter string based on the common name (CN) of the group. This filter uses LDAP search syntax. This method passes the filter to the AD server allowing the AD server to return the matches, which provides faster results than the legacy filter method.

Select one or more external authentication service groups from the list.

6. Select a role for the user group(s). See *Built-in User Groups* on page 43 for information about user roles.
7. From the Preemption Levels menu, select a preemption level from 1-4; the higher the number, the higher the preemption level.
8. Click *Finish*.

TACACS+ external authentication services

To add a TACACS+ user group:

1. Click the *Users* tab. Click *Groups* in the top navigation bar. Click *User-Defined* in the side navigation bar. The User Groups - User Defined window will open.
2. Click *Add*. The Add User Group wizard will appear.
3. The Select Authentication Service window will open. This window lists all authentication services that may be used to authenticate the user group when the user logs in. Select an appropriate TACACS+ authentication service from the list. Click *Next*.
4. If the TACACS+ service you selected is configured to use the privilege level attribute method, the Specify External Group Name window will open and display a list of privilege levels 0-15 (the higher the number, the higher the level of access).

Select a privilege level from the list. The Rack Power Manager server will assign a group name based on the privilege level you select. For example, if you choose level 7, the group name will be Privilege Level 7.

Click *Next*.

-or-

If the TACACS+ service you selected is configured to use the group name custom attribute method, the Specify External Group Name window will open and display a Name field. Type the name for the external user group on the external authentication service. The group name must correspond to one of the values configured in the TACACS+ service.

Click *Next*.

5. Select a role for the user group(s), then click *Next*. See *Built-in User Groups* on page 43 for information about user roles.
6. From the Preemption Levels menu, select a preemption level from 1-4; the higher the number, the higher the preemption level.
7. Click *Finish*.

Deleting User-defined User Groups

You may delete any user-defined user groups that have been created in the Rack Power Manager software system. You must have Rack Power Manager software administrator or user administrator rights to delete user-defined user groups.

To delete a user-defined user group:

1. Click the *Users* tab. Click *Groups* in the top navigation bar. Click *User-Defined* in the side navigation bar. The User Groups - User Defined window will open.
2. Click the checkbox to the left of the user group(s) to be deleted. To delete all user groups listed in the window, click the checkbox to the left of Name at the top of the list.
3. Click *Delete*. A confirmation dialog box will appear.
4. Confirm or cancel the deletion.

User Group Properties

To display the properties of a built-in user group:

1. Click the *Users* tab. Click *Groups* in the top navigation bar. *Built-In* will automatically be selected in the side navigation bar and the User Groups - Built-in window will open.
2. Click on a user group name. The User Group Properties window will open. The display includes read-only properties for each group: name, type and preemption level.
3. Click *Close* when you are finished. The User Groups - Built-in window will open.

To display or change the properties of a user-defined user group:

1. Click the *Users* tab. Click *Groups* in the top navigation bar. Click *User-Defined* in the side navigation bar. The User Groups - User Defined window will open.
2. Click on a user group name. The User Group Properties window will open.
3. To change the name of the user group, type a new 1-256 character name in the Name field.

NOTE: If the user group belongs to a TACACS+ service that uses the privilege level attribute method, the Name field will be disabled.

4. To change the preemption level, type a number (from 1-4; the higher the number, the higher the preemption level) in the Preemption Level field or select a value from the menu.
5. To change the role of the user group, select a role from the menu. If you do not wish to assign a role to the user group, select *None*.
6. Click *Save* and then click *Close*. The User Groups - User Defined window will open.

Changing User Group Members

When users are created, they may be assigned to one or more built-in or user-defined user groups. You may add or remove users to or from the built-in and user-defined user groups.

To add or remove user group members:

NOTE: Members may only be assigned to or removed from user groups defined on the internal Rack Power Manager authentication service.

1. Click the *Users* tab.
2. Click *Groups* in the top navigation bar. *Built-In* will automatically be selected in the side navigation bar and the User Groups - Built-in window will open. To display the User Groups - User Defined window, click *User-Defined* in the side navigation bar.
3. Click on a user group name. The User Group Properties window will open.
4. Click *Members* in the side navigation bar. The User Group Members window will open.
5. Click *Assign*. The Assign Users to User Group window will open.
6. To add one or more users to the user group, select the user(s) in the Available Users list, then click *Add*. The users will be moved to the Members list.
7. To remove one or more users from the user group, select the user(s) in the Members list, then click *Remove*. The users will be moved to the Available Users list.
8. Click *Save* and then click *Close*. The User Group Members window will open.

9. Click *Close*. The User Groups - Built-In or User Groups - User Defined window will open (depending on which groups you were working with).

You may also add or remove a user from a built-in or user-defined user group by clicking on a username in a User Accounts window and changing its user group membership. See *Changing User Group Members* on page 228.

User Group Access Rights

Access rights indicate whether a user is allowed to perform certain actions on a unit in the Rack Power Manager software system. See *About Access Rights* on page 143 for detailed information and a list of actions that are available for target devices and managed appliances.

You may assign access control rights from a user group perspective. You select a user group, specify the units for which rights will be assigned, then indicate the permission to perform the action (none, allow, deny or inherit) for each unit. That procedure is described in this section.

There are other ways to assign access rights:

- From a user perspective - see *User Access Rights* on page 220
- From a unit perspective - see *Unit Access Rights* on page 144
- From a unit group perspective - see *Changing the unit group properties* on page 189

To display user group access rights:

1. Click the *Users* tab.
2. Click *Groups* in the top navigation bar. *Built-In* will automatically be selected in the side navigation bar and the User Groups - Built-in window will open. To display the User Groups - User Defined window, click *User-Defined* in the side navigation bar.
3. Click on a user group name. The User Group Properties window will open.
4. Click *Effective Rights* in the side navigation bar and then click *All Units*, *Target Devices* or *Appliances*. The Target Devices Effective Rights window or Appliance Effective Rights window will open. Columns indicate the available actions for the unit.
 - Black check mark - the user has been granted access for this right
 - Gray check mark - a group to which the user belongs has been granted access for this right
 - Black X - the user has been denied access for this right
 - Gray X - a group to which the user belongs has been denied access for this right
 - No check mark - no access has been granted or denied for this right

5. Click *Close* when you are finished. The User Accounts - All window will open.

To add or remove user group access rights:

1. Click the *Users* tab.
2. Click *Groups* in the top navigation bar.
3. *Built-In* will automatically be selected in the side navigation bar and the User Groups - Built-in window will open. To display the User Groups - User Defined window, click *User-Defined* in the side navigation bar.
4. Click on a user group name.
5. Click *Access Rights* in the side navigation bar. The User Group Access Rights window will open.
6. To add or remove a unit or unit group from the Unit and Unit Groups list, click *Edit List*. The User Group Access Rights Unit Selection window will open.
 - To add one or more units/unit groups, select the units/groups in the Available list, then click Add. The units/unit groups will be moved to the List to Update list.
 - To remove one or more units/unit groups, select the units/groups in the List to Update list, then click Remove. The units/unit groups will be moved to the Available list.
7. Click *OK*. The User Group Access Rights window will display the current list of units/unit groups.
8. To add/remove access rights for a unit/unit group, select a unit or unit group from the Unit and Unit Groups list, then enable or disable a checkbox in the Access Rights table for each access right.
 - Allow - the access right is allowed for members of the user group.
 - Deny - the access right is denied for members of the user group.
 - Inherit - the access right is inherited from the unit group(s) to which the selected unit/unit group belongs. When *Inherit* is selected, the Allow and Deny checkboxes will become gray and unchangeable, and indicate the inherited value. If the inherited settings indicated both Allow and Deny, the inherited value is Deny, which takes precedence.

To disable the inherit functionality, uncheck the Inherit checkbox.
 - If none of the checkboxes are checked, the access right is neither allowed nor denied.
9. Repeat the preceding step for other units/unit groups.
10. Click *Save* and then click *Close*.

Using the Telnet Viewer

The Rack Power Manager management software ships bundled with a built-in proprietary Telnet Viewer that provides features unavailable in many other Telnet programs. These features include configurable session properties tailored for each device, configurable user preferences for all sessions, a scripting function for automatic device login, a macro function and a logging function.

About the Telnet Viewer

Telnet Viewer is supported for managed PDUs only. Any other appliances will not have Telnet sessions.

NOTE: Throughout this chapter, the term “appliance” or “managed appliance” will be used to indicate a supported CPS appliance, CCM appliance or generic appliance that supports Telnet Viewer connections.

When a session is established with a supported appliance, the Telnet client switches to SSH (Secure Shell) mode and opens an SSH shell to/through the appliance. The SSH shell can use any of the Telnet client’s terminal emulations. See *Security Property* on page 234.

The Telnet Viewer uses the credentials provided by the Rack Power Manager software to establish a session and will automatically accept the appliance server key. The username and password provided by the users when they log in are authenticated by the authentication service configured in the Rack Power Manager software.

Requirements

The Telnet Viewer is actually an applet that runs within the Java 1.5.0_02 plug-in (JRE). The Telnet Viewer may also work with other Java versions. The Rack Power Manager software client automatically downloads and installs the JRE (Java Runtime Environment) the first time the Video Viewer or the Telnet Viewer is launched. See *Java Installation* on page 12 for information about user interaction with the JRE installer.

Telnet Viewer Window Features

A new Telnet Viewer window will open for each new Telnet session established by a user. The Telnet Viewer window contains menus, a toolbar and a window that provides virtual terminal emulation.

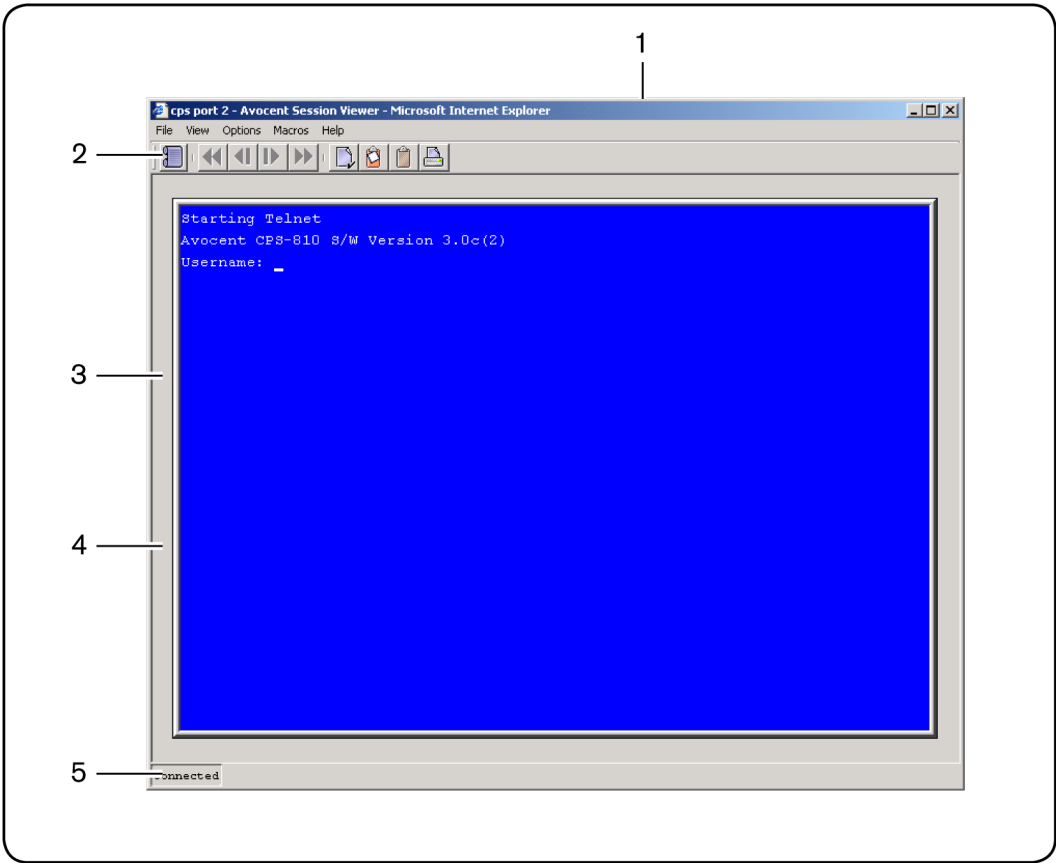


Figure 19.1: Telnet Viewer Window

Table 19.1: Telnet Viewer Window Descriptions

Number	Description
1	Title Bar: Displays the name of the target device being viewed.

Number	Description
2	Toolbar: Allows you to access many of the features in the Telnet Viewer. See Table 19.2 for a description of the toolbar icons.
3	Virtual Terminal window: Interacts with your target device through this window. By default the window size is 80 characters x 24 lines.
4	Viewer window: Resizes the window when you click and hold on the frame. Although the window may be resized, the Virtual Terminal window will remain the same size.
5	Status Bar: Displays one of the following: Connected - Displays during normal terminal emulation in a Telnet Viewer session. Logging - Displays when logging is enabled. Logging Paused - Displays when logging is paused.
NOTE: The Close button may not be present on all operating systems.	
NOTE: On supported Macintosh system clients, the Telnet Viewer opens in a self-contained window and is not included in the Application Menu.	

Telnet Viewer window toolbar

Table 19.2 describes the Telnet Viewer window's toolbar icons.

Table 19.2: Telnet Viewer Window Toolbar Icons

Icon	Description
	Session Settings - Displays the Session Properties dialog box
	Help - Displays the Rack Power Manager software help
	Copy Screen - Copies a screen of Telnet Viewer session data to the system clipboard
	Copy Buffer - Copies the contents of the Telnet Viewer session buffer to the system clipboard

Icon	Description
	Copy Text - Copies highlighted text in a Telnet Viewer session screen to the system clipboard
	Restore - Restores the ability to highlight screen text when autoscaling is enabled and the virtual terminal window has been scaled
	Paste - Pastes the contents of the system clipboard into a Telnet Viewer session
	Prints a screen of Telnet Viewer session data

Security Property

A fully functional SSH2 (Secure Shell Version 2) Client is built into the Telnet Viewer. The SSH2 Client is Java-based and provides a secure method for accessing target devices.

The Telnet Viewer provides the following security features:

- Strict host key checking
- Support ciphers for AES (128-, 192-, 256-bit), Blowfish, Twofish, Cast, 3DES and Arcfour
- Diffie-Hellman key exchange support
- SSH-RSA key types
- Supported for hmac-md5, hmac-sha1, hmac-sha1-96, hmac-md5-96 and hmac-ripemd160

The Rack Power Manager software will determine whether to create a Telnet or SSH2 connection when you start a session with an appliance. A serial connection provides SSH2 serial access to the target device from the appliance. Terminal emulation options are supported using both types of connections.

The SSH2 client is started when you initiate a session with an appliance port from the Rack Power Manager Explorer. The Rack Power Manager server is contacted, which in turn contacts the target device connected to the appliance port and exchanges X.509 certificates with the target device. The target device also supplies a session certificate, private key and appliance certificate.

These certificates are then passed back to the SSH2 client, which uses them to determine the SSH2 host key and the user SSH2 key. The Telnet Viewer will then establish a session with the target device (or through the proxy server if there is a proxy server connection). The Telnet

Viewer then passes the RSA public key from the session certificate when establishing the SSH connection. Finally, the virtual terminal window will open using an SSH2 shell over SSH connection.

SSH2 settings may be viewed by clicking on an appliance name in the Rack Power Manager Explorer and selecting *Appliance Settings - Sessions - Settings* in the side navigation bar to display the Properties - Sessions - Settings window.

Opening a Session

A Rack Power Manager management software Telnet Viewer session is opened using the Rack Power Manager Explorer by clicking on *Telnet Session* or *Serial Session* in the Action column of the target device. If the target device is attached to an appliance port, Telnet Session will appear. If the target device is attached to an appliance that is also attached to a serial device, Serial Session will appear.

NOTE: If multiple connection methods are available, an alternate actions arrow will appear to the right of the action. Clicking the alternate action arrow will display a list of other actions, in descending order of priority, which may be selected to launch the corresponding window type.

To open a Telnet Viewer session:

In a Units View window containing target devices (see *Accessing Units View windows* on page 111), click *Telnet Session* or *Serial Session* in the Action field or the Alternate Action menu. Alternative, you can click the Telnet Session or Serial Session icon in the Unit Overview window for the target device (see *Unit Overview Windows* on page 116).

The Telnet Viewer window will open.

NOTE: You can share a Telnet Viewer session with an SSH serial session. See *SSH Passthrough Sessions* on page 167.

Customizing the Telnet Viewer

You may specify preferences that will be used for every Telnet Viewer session, regardless of the device to which you connect. These application preferences are entered from the Telnet Viewer window when you are connected to a device or port. After the preferences are entered, they are applied to devices/ports during subsequent sessions.

To change the window background and/or text color:

1. Select *Options - Preferences* from the menu. The Preferences dialog box will appear.
2. To change the background color, click the *Background/Normal Mode* box in the Colors section and select a color. The default color is blue.

3. To change the text color, click the *Text/Normal Mode* box in the Colors section and select a color. The default color is white.

To change the cursor appearance:

1. Select *Options - Preferences* from the menu. The Preferences dialog box will appear.
2. In the Caret list, choose *Block* to display the cursor as a block or choose *Underline* to display the cursor as an underline. The default value is Underline.

To enable/disable an exit warning prompt for Telnet Viewer sessions:

1. Select *Options - Preferences* from the menu. The Preferences dialog box will appear.
2. Enable or disable the *Prompt on Exit* checkbox. When the exit warning prompt is enabled, a message appears when you select *Telnet - Exit*. You may then choose to exit or continue the session. When disabled, the session closes without further prompting. The default value is enabled.

To enable/disable autoscaling:

1. Select *Options - Preferences* from the menu. The Preferences dialog box will appear.
2. Enable or disable the *Auto Scale* checkbox. When autoscaling is enabled, the user may reduce or expand the virtual terminal window by dragging a corner of the window. When autoscaling is disabled, the virtual terminal window will not scale when the view is changed; instead, scroll bars will appear around the window. The default value is enabled.

Customizing Session Properties

When you are connected to an appliance or port using the Rack Power Manager software Telnet Viewer, you may specify session properties that will be stored and reused every time you connect to the selected appliance or port. When you select *Options - Session Properties* in the Rack Power Manager software Telnet Viewer, the Session Properties dialog box will appear containing Terminal, Login Scripts and Logging tabs.

To change the terminal window size:

1. Select *Options - Session Properties* from the menu or click the *Session Settings* icon in the toolbar. The Session Properties dialog box will appear.
2. Click the *Terminal* tab.
3. In the Rows list, choose a value of *24* or *48*. The default value is 24.
4. In the Columns list, choose a value of *80* or *132*. The default value is 80.

To change the terminal emulation mode:

1. Select *Options - Session Properties* from the menu or click the *Session Settings* icon in the toolbar. The Session Properties dialog box will appear.
2. Click the *Terminal* tab.
3. From the Terminal Emulation list, choose one option. The default value is VT100.
Terminal Emulation on page 298 contains encoding and decoding information for each of the terminal emulation types.

NOTE: When connecting to an appliance, the terminal type setting must match the terminal emulation type.

To change the Telnet Viewer Arrow key sequences:

When the Terminal Emulation mode is VT100, VT100+, VT102, VT52, VT220 or VT320, you may specify either VT100 or ANSI **Arrow** key sequences.

Table 19.3: Arrow Key Sequences

Key	VT100	ANSI	VT52
Up Arrow	<Esc> [A	<Esc> OA	<Esc> A
Down Arrow	<Esc> [B	<Esc> OB	<Esc> B
Right Arrow	<Esc> [C	<Esc> OC	<Esc> C
Left Arrow	<Esc> [D	<Esc> OD	<Esc> D

NOTE: When the Terminal Emulation mode is VT52, the **Arrow** keys are interpreted as indicated in this column, regardless of the value in the Arrow Keys list.

1. Select *Options - Session Properties* from the menu or click the *Session Settings* icon in the toolbar. The Session Properties dialog box will appear.
2. Click the *Terminal* tab.
3. In the Arrow Keys list, choose either *VT100* or *ANSI*. The default value is VT100.

To change the terminal type:

1. Select *Options - Session Properties* from the menu or click the *Session Settings* icon in the toolbar. The Session Properties dialog box will appear.
2. Click the *Terminal* tab.

3. In the Terminal Type box, enter a value of up to 40 characters, beginning with a letter and ending with a letter or digit. Valid characters are the letters A-Z, digits 0-9, forward slash, dash, left parenthesis and right parenthesis. The terminal type must be entered in the Terminal Type field exactly as shown in Table 19.4.

Table 19.4: Terminal Emulation and Type

Terminal Emulation	Terminal Type
VT52	DEC-VT52
VT100	DEC-VT100
VT100+	DEC-VT100
VT102	DEC-VT102
VT220	DEC-VT220
VT320	DEC-VT320

To change the linefeed settings:

1. Select *Options - Session Properties* from the menu or click the *Session Settings* icon in the toolbar. The Session Properties dialog box will appear.
2. Click the *Terminal* tab.
3. When connecting to devices that do not insert a carriage return in incoming or outgoing data, automatically inserting a line after each line of data can prevent overwriting data when a new line is received.

If the *New Line Mode - Inbound* box is checked, an inbound carriage return from the device will be treated as if both a carriage return and a linefeed were received. If not checked, a linefeed is not added to an inbound carriage return.

If the *New Line Mode - Outbound* box is checked, an outbound carriage return to the device will always be followed by a linefeed character. If not checked, a linefeed is not sent with a carriage return. The default value is disabled for inbound and outbound.

To enable/disable line wrap:

1. Select *Options - Session Properties* from the menu or click the *Session Settings* icon in the toolbar. The Session Properties dialog box will appear.
2. Click the *Terminal* tab.

3. Enable or disable the *Auto wrap line* checkbox. When line wrap is enabled, characters wrap onto the next line when a new character is received and the cursor is at the end of the line. When disabled, new characters will overwrite the last character on the current line when the cursor is at the end of the line. The default value is enabled.

To enable/disable local echo:

1. Select *Options - Session Properties* from the menu or click the *Session Settings* icon in the toolbar. The Session Properties dialog box will appear.
2. Click the *Terminal* tab.
3. When you are connected to a device that does not repeat or echo the data that you type, you may enable Local Echo mode. Otherwise, the Telnet Viewer will not display the text you type. However, if you are connected to a device that echoes data, and you are in Local Echo mode, all of the data you type will appear on your terminal twice.

Enable or disable the *Local echo* checkbox. The default value is disabled.

To enable/disable 7-bit ASCII:

1. Select *Options - Session Properties* from the menu or click the *Session Settings* icon in the toolbar. The Session Properties dialog box will appear.
2. Click the *Terminal* tab.
3. Enable or disable the *Strip 8th bit* checkbox. The default value is disabled.

Login scripts

The Telnet Viewer has a login scripting function that enables you to automatically log in to a device. A login script is built with a sequence of expect and send strings, and initial transmission characters that work with them. To use a login script, you must enable automatic login in a checkbox.

The first Initial character (that is, the first entry in the Initial character column) specifies what is sent to the device as soon as the Telnet Viewer session is established. This is selected from a list containing the choices: None, CR (carriage return), CR+LF (carriage return and linefeed), ESC (Escape) and CTRL+P (Control and P).

The first Expect string indicates what the device will send as its first prompt.

The first Send string indicates what the login script will send to the device after it receives the first Expect string.

You may then build additional Expect and Send strings according to what the particular device will prompt for and what will be sent in response.

To build a login script and enable/disable automatic login:

1. Select *Options - Session Properties* from the menu or click the *Session Settings* icon in the toolbar. The Session Properties dialog box will appear.
2. Click the *Login Scripts* tab.
3. Enable or disable the *Automate login* checkbox. The default value is disabled.
4. In the Initial Character list, select one option: CR (carriage return), CR+LF (carriage return and linefeed), ESC (Escape), CTRL+P (Control+P sequence, 0X10 in hex) or None (no initial transmission character).
5. In the Expect box, type the 1-32 alphanumeric character string that you expect from the device. Spaces are allowed.
6. In the Send box, type the 0-32 alphanumeric character string that you wish to send in response to the Expect string. Spaces are allowed, and a blank field is valid. A CR or CR+LF is appended to the string, based on the New Line Mode - Outbound setting.
7. Repeat the Expect and Send entries as needed, to a maximum of four each.

Reviewing Session Data

During a Telnet Viewer session, you may review the accumulated screen contents by using the scroll bar or the **Arrow** keys. To return to the current session location, press **Enter**. The size of the buffer containing session data that can be reviewed is configurable.

You may optionally choose to change the color of the text and/or the background when you are reviewing session data. When you return to the current session location, the colors will return to those specified in the Telnet Viewer's configuration (see *Customizing the Telnet Viewer* on page 235).

While you are reviewing collected data, new incoming data is buffered, but it will not be displayed until you return to the current session location. You may not enter outgoing data.

To change the maximum number of lines in the session buffer:

1. Select *Options - Session Properties* from the menu or click the *Session Settings* icon in the toolbar. The Session Properties dialog box will appear.
2. Click the *Terminal* tab.
3. In the History Buffer Size box, type a value from 1-1000. The default value is 256.

To change the background and/or text color when reviewing session data:

1. Select *Options - Preferences* from the menu. The Preferences dialog box will appear.

2. To change the background color, click the *Background/History Mode* box in the Colors section and select a color. The default color is blue.
3. To change the text color, click the *Text/History Mode* box in the Colors section and select a color. The default color is white.

Macros

NOTE: Three additional types of macros are available in the Rack Power Manager software. Exit macros, created within the Rack Power Manager Explorer, reside on DS1800 digital switches and DSR switches and are used by these switches. Global macros and personal macros are created using the Video Viewer window and are used with KVM sessions with target devices attached to DS1800 digital switches and DSR switches. None of these macros may be used or are compatible with a Telnet Viewer.

The Rack Power Manager software Telnet Viewer has a macro function that allows you to create and use macros during Telnet Viewer sessions. A macro comprises a series of keystrokes that you define. Additionally, you may specify a hotkey in the macro's definition. When you define a macro and enable its inclusion in the Macros menu, you may execute the macro during a Telnet Viewer session either by selecting it from the Macros menu or by pressing the defined hotkey on your keyboard.

You may also define one or more global macro or personal macro groups, then add macros to the groups. Personal macro groups may be created by any user and are only available for use on the target device on which they are created. Global macros may only be created by a Rack Power Manager software administrator and are available for use by any user on the Rack Power Manager software system.

A macro may belong to more than one macro group or belong to both personal and global macro groups; however, a macro does not have to belong to a macro group. Selecting *Macros - Configure - Groups* takes you to the Configure Macro Groups dialog box which contains a list of defined macro groups from which you may select one group or all defined groups. The macros in the selected group(s) are then available for use during subsequent Telnet Viewer sessions with that device/port.

After defining a macro or a macro group, you may edit or delete it at any time. When you delete a macro or macro group, you are prompted for confirmation. When you change a macro group name, each macro belonging to the changed macro group is updated, but the change is not visible until the next Telnet Viewer session is established. When you delete a macro group, you delete only its name - the individual macros in the group are not affected.

To create a macro:

1. Select *Macros - Configure - Macros* from the menu. The Configure Macros dialog box appears.

2. Click *Create*. The Configure Macros dialog box expands to display an Edit Macro area.
3. In the Macro Name field, Type a 1-64 character name for the macro.
4. To define a hotkey for the macro, choose one from the Key list. To add a modifier to the hotkey, check the *Control*, *Shift* or *Alt* boxes. (A macro's hotkey is accessible only when the macro belongs to the active macro group.)
5. By default, the *Include in Menu* box is checked, indicating the macro will appear in the Macros menu. If you do not wish to include the macro in the Macros menu, uncheck this box. In this case, if the macro definition includes a hotkey, you will still be able to use the hotkey to run the macro, even if the macro's name does not appear in the Macros menu.
6. Type the macro string in the Keystrokes box. For non-printing and special character code sequences, use the following escape sequences:

New line: \n

Carriage return: \r

Form feed: \f

Horizontal tab: \t

Backspace: \b

Delay character (500 ms): \d

Hexadecimal code sequence: \0x<NN>, where <NN> is the hexadecimal byte. For example, the **Ctrl+D** character sequence may be sent by using 0x04.

Octal code sequence: \0<NNN>, where <NNN> is the octal byte. For example, the **Ctrl+D** character sequence may be sent by using 0004.

7. From the Control Code menu, select the sequence to invoke with the selected characters.
8. In the Access Rights area, specify whether you wish for the macro to be a global macro (available to all users) or a personal macro (available only to the current user).

You must have Rack Power Manager software administrator privileges to use the Access Rights area.

9. Click *OK*. The Configure Macros dialog box returns to its abbreviated display and the macro appears in the Macros area.
10. Click *OK* to close the Configure Macros dialog box.

To edit an existing macro:

NOTE: You must have Rack Power Manager software administrator privileges to edit Global Macros.

1. Select *Macros - Configure - Macros* from the menu. The Configure Macros dialog box appears.
2. In the Macros table, select the macro you wish to edit.
3. Click *Edit*. The Configure Macros dialog box expands to display an Edit Macro area containing the information defined for the macro.
4. Edit the macro properties as needed.
5. Click *OK*. The changes are saved and the Configure Macros dialog box returns to its abbreviated view.
6. Repeat steps 2-5 to edit additional macros.
7. Click *OK* to close the Configure Macros dialog box.

To delete a macro:

NOTE: You must have Rack Power Manager software administrator privileges to delete Global Macros.

1. Select *Macros - Configure - Macros* from the menu. The Configure Macros dialog box appears.
2. Select the macro in the Macros table that you wish to delete.
3. Click *Delete*. A dialog box appears, prompting you to confirm the deletion.
4. Confirm or cancel the deletion.

To use a macro:

1. Select the macro from the Macros menu (if the macro's definition includes a hotkey, press the hotkey or hotkey sequence. A macro's hotkey is accessible only when the macro belongs to the active macro group) or select *Macros - Configure - Macros* from the menu. The Configure Macros dialog box appears.
2. Select the macro in the Macros table that you wish to run.
3. Click *Run*.

Macro groups

To create a macro group:

1. Select *Macros - Configure - Groups* from the menu. The Configure Macro Groups dialog box appears.
2. Click the *Create* button. The Configure Macros dialog box expands to display a Create Group area.

3. In the Group Name field, type a 1-64 character name for the macro group.
4. To add one or more macros to the macro group, select the macro(s) from the Macros Available list, then click *Add*. The macros will be moved to the Macros In Group list.
5. To remove one or more macros from the macro group, select the macro(s) from the Macros In Group list, then click *Remove*. The macros will be moved to the Macros Available list.
6. In the Access Rights area, specify whether you want the macro group to be a Global Macro group (available to all users) or a Personal Macro group (available only to the current user).

You must have Rack Power Manager software administrator privileges to assign access rights.
7. Click *OK*. The Configure Macro Groups dialog box returns to its abbreviated view.
8. Click *OK* to close the Configure Macro Groups dialog box.

To enable a macro group for use during Telnet Viewer sessions:

NOTE: You must have Rack Power Manager software administrator privileges to enable a macro group.

1. Select *Macros - Configure - Groups* from the menu. The Configure Macro Groups dialog box appears.
2. In the Macro Groups table, select the macro group you wish to enable.
3. Click the *Edit* button. The Configure Macro Groups dialog box expands to display an Edit Group area containing the information defined for the macro.
4. Enable the *Active Group* checkbox.
5. Click *OK*. The changes are saved and the Configure Macro Groups dialog box returns to its abbreviated view.

To edit an existing macro group:

NOTE: You must have Rack Power Manager software administrator privileges to edit global macro groups.

1. Select *Macros - Configure - Groups* from the menu. The Configure Macro Groups dialog box appears.
2. In the Macro Groups table, select the macro group you wish to edit.
3. Click the *Edit* button. The Configure Macro Groups dialog box expands to display an Edit Group area containing the information defined for the macro.
4. Edit the macro group properties as needed.

5. Click *OK*. The changes are saved and the Configure Macro Groups dialog box returns to its abbreviated view.
6. Repeat steps 2-5 to edit additional macro groups.
7. Click *OK* to close the Configure Macro Groups dialog box.

To delete a macro group:

NOTE: You must have Rack Power Manager software administrator privileges to delete global macro groups.

1. Select *Macros - Configure - Groups* from the menu. The Configure Macro Groups dialog box appears.
2. Select the macro group in the Macro Groups table that you wish to delete.
3. Click the *Delete* button. A dialog box appears, prompting you to confirm the deletion.
4. Confirm or cancel the deletion.

Logging

The Telnet Viewer has a logging function that saves the contents of a Telnet Viewer session to a file. You may enable automatic logging or dynamically start logging at any time. Additionally, you may pause, resume and stop logging, regardless of whether it was started automatically or dynamically.

While logging is occurring or when it is paused, a Logging Status label appears in the status panel at the bottom of the Rack Power Manager management software Telnet Viewer window.

NOTE: When you enable or disable automatic logging, the logging will begin or end at the start of the next Rack Power Manager software Telnet Viewer session to that device. If you change the default log file directory used for automatic logging, the change does not take effect until the next session to that device.

Log files

The format of log filenames is shown below, where <mmddyy> represents the month, day and year, and <hhmmss> represents the current hour, minute and second in military time:

```
scvTelnet<mmddyy>_<hhmmss>.log
```

The default log directory is session-specific, that is, each Telnet Viewer session may have its own location for storing logfiles. You may change the name of the file and the location of the directory that stores the logfiles. If you do not change the default directory, logfiles are stored in your home directory.

You may display a log file at any time, using a standard text editor. The screen buffer is written to the log file when the buffer is full, or when logging is paused or stopped. To ensure the log file is up-to-date, either pause or stop the logging.

To change the default log file directory:

1. Select *Options - Session Properties* from the menu or click the *Session Settings* icon in the toolbar. The Session Properties dialog box will appear.
2. Click the *Logging* tab. The Default Directory field displays the current default location for logfiles.
3. Click the *Browse* button. The Set Directory dialog box appears.
4. Select a directory from the Look in list or create a new directory. To create a new directory:
 - a. Click the *Create New Folder* button. A new directory named New Folder appears in the directory list.
 - b. Click the *New Folder* entry in the directory list to highlight it. Then, click the entry again to edit its name. Type in a new name. Press **Enter**. The directory appears in alphabetical order in the directory list.
 - c. Select the newly-created directory in the directory list. The Filename field will now contain the name of the new directory.
5. Click the *Set Directory* button to select the newly-created or selected directory as the default log file directory. The Set Directory dialog box will close.
6. The Default Directory field now contains the name of the newly-created or selected directory. Click *OK* to save the new information.

To enable automatic logging:

1. Select *Options - Session Properties* from the menu or click the *Session Settings* icon in the toolbar. The Session Properties dialog box will appear.
2. Click the *Logging* tab.
3. Enable the *Logging* checkbox.
4. The Default Directory field displays the current default location for logfiles. If that is the desired directory, click *OK*. (You may change the default directory.)

Automatic logging will begin when you initiate the next Telnet Viewer session to that device. At that time, the Logging Status label will indicate *Logging*.

To disable automatic logging:

1. Select *Options - Session Properties* from the menu or click the *Session Settings* icon in the toolbar. The Session Properties dialog box will appear.
2. Click the *Logging* tab.
3. Disable the *Logging* checkbox.
4. Click *OK*.

Automatic logging will stop when you close the Telnet Viewer session. When logging stops, the Logging Status label disappears.

To start dynamic logging:

1. Select *Options - Logging - Start* from the menu. The Log dialog box appears.
2. The Look in list contains the default log file directory and the Filename field contains the default log filename. Using this filename format is recommended; however, you may change it for the duration of this Telnet Viewer session. If you choose to use the default log filename, skip to step 4.
3. To change the default log filename for the duration of the dynamic logging session, you may select a directory from the Look in list. The directory list may contain directories and files. To create a new directory:
 - a. Click the *Create New Folder* button. A new directory named New Folder appears in the directory list.
 - b. Click the *New Folder* entry in the directory list to highlight it. Then click the entry again to edit its name. Type in a new name. Press **Enter**. The directory appears in alphabetical order in the directory list.
 - c. Double-click the newly-created directory in the directory list. The Filename field will now contain the name of the new directory.
 - d. Type a new filename in the Filename field. If you enter a filename that already exists, the new file will overwrite the old file.
4. You are prompted to confirm the directory selection and begin logging. Confirm or cancel the logging start.

When logging begins, the Logging Status label will indicate *Logging*.

To pause logging:

Select *Options - Logging - Pause* from the menu. The Logging Status label will change to *Logging Paused*.

To resume logging:

Select *Options - Logging - Resume* from the menu. The Logging Status label will change to *Logging*.

To stop logging:

Select *Options - Logging - Stop* from the menu. The Logging Status label will disappear.

Copying, Pasting and Printing Session Data

In the Telnet Viewer you may:

- Copy a screen of Telnet Viewer session data to the system clipboard
- Copy all of the Telnet Viewer session buffer contents to the system clipboard
- Copy a highlighted portion of the Telnet Viewer session data to the system clipboard
- Paste the contents of the system clipboard into a Telnet Viewer session or into another application
- Print a screen of the Telnet Viewer session data

Information that is copied from a Rack Power Manager software Telnet Viewer session may be pasted into other applications. Similarly, information copied from other applications may be pasted into a Telnet Viewer session.

NOTE: Only textual data may be copied and pasted in the Rack Power Manager software Telnet Viewer.

To copy a Telnet Viewer session window screen:

Select *Options - Copy Screen* from the menu or click the *Copy Screen* icon in the toolbar.

The screen contents will be saved to the system clipboard. You may then paste the clipboard contents into a Telnet Viewer session or into another application.

To copy all of the Telnet Viewer session buffer contents:

Select *Options - Copy Buffer* from the menu or click the *Copy Buffer* icon in the toolbar.

The entire buffer will be copied to the system clipboard (regardless of the amount of data in it. You may then paste the clipboard contents into a Telnet Viewer session or into another application.

To highlight and copy a portion of a Telnet Viewer window screen:

NOTE: When autoscaling has been enabled and the window has been scaled, you will not be able to highlight text until you click the *Restore* icon in the toolbar.

1. Use the mouse to drag-select the portion of the screen text you wish to copy.

2. Select *Options - Copy Text* from the menu.

-or-

Click the *Copy Text* icon in the toolbar.

-or-

Right-click and select *Copy Text* from the pop-up menu.

The highlighted text will be copied to the system clipboard. You may then paste the clipboard contents into a Telnet Viewer session or into another application.

To paste system clipboard contents:

1. Place textual data on the system clipboard, using a text editor or other application.
2. Initiate a Telnet Viewer session.
3. At the point where you wish to paste the clipboard contents, select *Options - Paste* from the menu or click the *Paste* icon in the toolbar.

To print a Telnet Viewer window screen:

1. Select *Options - Print Screen* from the menu or click the *Print Screen* icon in the toolbar.
2. The operating system's print dialog box appears. Make the appropriate settings. The screen contents will then be sent to the printer.

Power Control of Devices Attached to Power Devices

NOTE: A user must have Rack Power Manager software administrator privileges to control the power of a target device.

If a target device attached to an appliance port is connected to a power device outlet and the target device has been accessed in a serial session, you may power up, power down or cycle (power down and then power up) the target device using the Power Control dialog box.

NOTE: This operation is valid only during serial sessions.

The Options - Power menu option will not be available if the target device cannot be power controlled using the Rack Power Manager software, or if the user does not have power control access rights.

The current state of the power device outlet appears in the Current Power Status area of the dialog box. As you change the power state, the information is updated in real time.

Depending on the configuration of a power device outlet, it may not immediately respond to a power change request (for example, it may be configured to remain off for a specific period of time).

To power up, power down, or power cycle a target device:

1. Select *Options - Power* from the Telnet Viewer main window. The Power Control dialog box will appear.
2. Click *On*, *Off* or *Cycle*.
3. Click *Close* to close the dialog box.

Closing a Telnet Viewer Session

To close a Telnet Viewer session:

Select *File - Exit* from the Telnet Viewer window.

Using Tools

The Rack Power Manager management software contains tools that may be used to perform various actions on units. This chapter describes the available tools and how to use them.

Using Unit Tools

The Unit Tools window contains tools that allow a user to:

- Export unit information to a .csv (comma separated value) file
- Export unit access rights information to a .csv file
- Simultaneously merge multiple power outlets
- Import data in an XML format into the Rack Power Manager software database

To display the Units Tools window:

1. Click the *Units* tab.
2. Click *Tools* in the side navigation bar. The Unit Tools window will open.

Exporting units

The Export Units tool will export information about units into a .csv file. Unit names are always exported. The following unit properties may be selected for export:

Action (default action) Primary contact phone
 Browser URL Secondary contact
 Custom field 1-3 Secondary contact phone
 Department Serial number
 Rack Power Manager server name Site
 IP address Status (at time of export)
 Location Telnet port
 Model number Type
 Part number Visibility (show or hide)
 Primary contact

You may also export a topology report, regardless of any properties selected for export. A topology report contains the following columns:

- Port - (target devices or cascade switches only) Port number on the appliance to which the target device or cascade switch is connected.
- Type - (managed appliances only) Appliance type, if known.
- Level - Level of connection from the appliance. A managed appliance is level 0. A target device attached to a managed appliance is 1, and so on.

The output .csv file may be viewed in a text editor or spreadsheet application, such as Microsoft Excel.

To export units:

1. Click the *Units* tab.
2. Click *Tools* in the side navigation bar. The Unit Tools window will open.
3. Click the *Export Units* icon or link. The Export Units Wizard will appear.
4. To add one or more properties to be exported, select the properties in the Available Properties list, then click *Add*. The properties will be moved to the Properties to Export list.
5. To remove one or more properties to be exported, select the properties from the Properties to Export list, then click *Remove*. The properties will be moved to the Available Properties list.
6. To change the order in which properties are listed in the output .csv file, select one or more properties in the Properties to Export list and use the up and down arrows to move the selected properties up or down in the listing.
7. To create a topology report, enable the *Export Topology* checkbox. If any properties are also being exported, they will be listed after the topology information in the report.
8. Click *Next*.
9. The Save Process window will open. Click *Next*.
10. The Completed Successful window will open, along with a File Download dialog box.
11. Click *Open*. The file will download and open. By default, .csv files are configured to open in Microsoft Excel. If Microsoft Excel is not installed on your computer, you will be prompted to select a text editor to use for opening the .csv file.

The default filename of the .csv file is unitproperties.csv. Subsequent files that you export will be incremented (unitproperties[1].csv, unitproperties[2].csv and so on).

-or-

Click *Save*. The Save As dialog box will appear. Select a directory and filename and click *Save* to save the .csv file.

12. Click *Finish*. The Units Tools window will open.

Exporting access rights

The Export Access Rights tool will export permission information about units from the Rack Power Manager management software host. The unit name and the user/user group to which the unit has access rights will be exported. Additionally, the unit access right settings will be exported; see *About Access Rights* on page 143.

The output .csv file may be viewed in a text editor or spreadsheet application, such as Microsoft Excel.

To export access rights:

1. Click the *Units* tab.
2. Click *Tools* in the side navigation bar. The Unit Tools window will open.
3. Click the *Export Access Rights* icon or link. The Export Access Rights Wizard will appear.
4. Select either *All Units*, *Appliances*, *Target Devices* or *Unit Groups*, for the unit type and click *Next*.
5. The Save Process window will open. Read the text, then click *Next*.
6. When prompted, enter the location and filename where the exported access rights will be saved.
7. The Completed Successful window will open, along with a File Download dialog box.
8. Click *Open*. The file will download and open. By default, .csv files are configured to open in Microsoft Excel. If Microsoft Excel is not installed on your computer, you will be prompted to select a text editor to use for opening the .csv file.

The default filename of the .csv file is `appliance_rights.csv` if you are exporting managed appliance rights or `target_device_rights.csv` if you are exporting target device rights. Subsequent files that you export will be incremented (`target_device_rights[1].csv`, `target_device_rights[2].csv` and so on).

-or-

Click *Save*. The Save As dialog box will appear. Select a directory and filename and click *Save* to save the .csv file.

9. Click *Finish*. The Units Tools window will open.

Importing data

You can use the Import Data Wizard to migrate data from the AlterPath™ Manager to the Rack Power Manager software. First, you will need to export the data from the AlterPath Manager into an XML format that is recognized by Rack Power Manager software. See the AlterPath Manager Data Migration Technical Bulletin for more information.

To import data:

1. Click the *Units* tab.
2. Click *Tools* in the side navigation bar. The Unit Tools window will open.
3. Click the *Import Data* icon or link. The Import Data Wizard will appear.
4. In the File field, type the path and name of the import file or browse to the file location. The file must be a valid Rack Power Manager software data import file in an XML format. Click *Next*.
5. The Select Import Options window will open. Specify the User Password Options. Select *Set the user's password to the user's username* or *Set the user's password to a default value*. If you choose a default password value, type a 3-64 character password in the Password and Confirm Password fields.
6. Specify the Account Options. Depending on which options you choose, you may select multiple checkboxes. Only valid combinations will be enabled. You may choose from the following options:
 - Disable user account
 - User must change password at next login
 - User cannot change password
 - Password never expires
7. Click *Next*. The Import In Progress message will display until the import attempt is complete. If the import is successful, the Completed Successful window will open and display a summary of the results.

If the import was not successful, the Completed Unsuccessful window will open and display the errors that caused the import to fail. If some items could not be imported, a message will direct you to a .csv file with more information. You may attempt to import the data again.
8. Click *Finish*.

Although data has been imported from the AlterPath Manager to the Rack Power Manager software system, the units are not yet compatible with the Rack Power Manager software. To complete the configuration and import process, you must use the Migrate Units task. When creating the Migrate Units task, it is recommend that you select *Enable Secure Mode* for the units.

Using the Managed Appliance Tools

The Rack Power Manager management software contains tools that allow you to perform the following actions on a supported PDU:

- Reboot
- Upgrade the firmware
- Resynchronize the managed appliance so that it reflects the current Rack Power Manager software system configuration
- Save or restore the configuration
- Save or restore the database of local users

To access the managed appliance tools:

1. Click the *Units* tab. In the side navigation bar, click one of the following:
 - *Appliances* - The Appliances - All window will open. You may also click on a link below Appliances to display only specific types of managed appliances in an Appliances window.
 - *Sites* and then click on a site link - A Units in Site window will open.
 - A custom field label and then the label you specified for the managed appliance - The Units in Custom Fields window will open.
 - *Recently Accessed* - The Recently Accessed Units window will open.
2. Click on the name of a managed appliance. The Unit Overview window will open. The tools are listed in the Tools section of the window.

Rebooting

To reboot one or more managed appliances from a Units View window:

1. In a Units View window (see *Accessing Units View windows* on page 111), click the checkbox next to the appliance. To reboot all managed appliances in the page, click the checkbox to the left of Name at the top of the list. (If the page lists units other than managed appliances, they will not be affected.)

2. Click *Operations*, then select *Reboot* from the menu. A confirmation dialog box will appear.
3. Confirm or cancel the reboot. If confirmed, all active sessions will be disconnected. A Multiple Unit Operation window will open, containing a link to another window where results may be viewed; see *Multiple unit operations from a Units View window* on page 115.

To reboot a managed appliance from a Unit Overview window:

NOTE: To reboot a serial console appliance, you must have Reboot Appliance access rights. By default, users who are members of the Rack Power Manager software administrators, user administrators and appliance administrators built-in groups have this access right. See *About Access Rights* on page 143.

1. In the Unit Overview window, click the *Reboot* icon or link. A confirmation dialog box will appear.
2. Confirm or cancel the reboot. If confirmed, all active sessions will be disconnected.

Upgrading firmware

To upgrade the firmware on a managed appliance:

NOTE: A valid Flash file must exist in the Rack Power Manager server's firmware repository to use this command. Optionally, one or more managed appliances may be Flash upgraded as a task. See *Task: Updating the firmware of an appliance type* on page 271.

1. In the Unit Overview window, click the *Upgrade Firmware* icon or link. The Upgrade Appliance Firmware Wizard will appear.

NOTE: If the firmware is being upgraded for Liebert® MPX/MPH PDUs, ensure that the current On Board Web Interface(OBWI) access username and password is updated. Click the MPX/MPH PDU and select *Appliance Settings - OBWI Access Settings* to update the username and password.

2. The Select Firmware Files window will open.
 - To add one or more Flash files to the update list, select the file(s) in the Available Firmware Files list, then click *Add*. The properties will be moved to the Firmware Files to Update list.
 - To remove one or more firmware files from the update list, select the file(s) from the Firmware Files to Update list, then click *Remove*. The firmware files will be moved to the Available Firmware Files list.
 - The firmware on each managed appliance will be upgraded in the order shown in the Update list. A reboot will be automatically performed between each firmware update. To change the order in which firmware files are installed on the managed

appliance, select one or more firmware files in the Firmware Files to Update list and use the up and down arrows to move the selected firmware files up or down in the listing.

Click *Next*.

3. The Type in Task Name window will open. Type a 1-64 character name for the upgrade firmware task, then click *Next*.
4. The Completed Successful window will open. To check the progress of the upgrade task, click the *Click here to view results* link. (You may also check the upgrade task progress while the task is running by clicking the *System* tab and then clicking *Tasks* in the top navigation bar; however, the upgrade task will be removed from the task list when it completes.)
5. Click *Finish*. The Unit Overview window will open.

Resynchronizing units

When a unit changes its configuration, it may not be properly represented in the Rack Power Manager software system. For example, a target device may be added, removed or moved. Resynchronizing will update these and other changes made to the unit within the Rack Power Manager software system.

Resynchronizing will force a check of the entire Rack Power Manager software system. The process requires a large amount of time and network bandwidth and should only be performed when necessary.

Alternatively, you may use the automatic topology synchronization feature or synchronize selected units manually from a Units View window. See *Topology Synchronization* on page 129.

To resynchronize a unit:

1. In the Unit Overview window, click the *Resync* icon or link. The Resync Unit Wizard will appear.
2. The Select Resync Options window will open. (For more information about the resync options, see *Topology synchronization options in the Resync Wizard* on page 130.)
 - a. Enable the *Remove offline connections* checkbox to remove from the Rack Power Manager software database any connections to target devices that are reported as offline in the appliance. The Resync Wizard does not add offline connections to the Rack Power Manager software database.

- b. Enable the *Delete target devices that no longer have connections* checkbox to delete those target devices permanently from the Rack Power Manager software database.
 - c. Enable the *Allow target devices with the same name to be merged into a single target device* checkbox to allow the Rack Power Manager software to treat multiple target devices with the same name as one unit with multiple access methods.
 - d. Enable the *Allow target devices that contain default names to be added* checkbox to allow target devices that have default names in the managed appliances to be added to the Rack Power Manager software database.
 - e. Click *Next*.
3. If the unit does not require resynchronizing, the Completed Successful window will open. If the unit requires resynchronizing, the Changes Detected in Appliance window will open. Click *Next* and go to step 7. If one or more cascade switches are attached to the KVM switch, the Cascade Switch Configuration window will open. Go to step 4.
4. Select the type of each detected cascade switch.
5. Type a name for each cascade switch.
6. Optionally, combine any multiuser cascade switches. Click the checkboxes of the cascade switches that you wish to merge, and then click *Merge*.

To unmerge any cascade switches that you have merged, click the checkbox of the merged cascade switch and then click *Split*.
7. Click *Next*. The Completed Successful window will open.
8. Click *Finish*. The Unit Overview window will open.

Saving a managed appliance configuration

You may save the configuration of a PDU to a file. The configuration file will contain information about the managed appliance, including the following:

- Global settings
- Port settings
- SNMP trap settings
- SNMP manager settings
- The names of connected target devices

For information on restoring a configuration file, see *Restoring a managed appliance configuration* on page 259.

To save a managed appliance configuration to a file:

1. In the Unit Overview window, click the *Save Configuration* icon or link. The Save Appliance Configuration Wizard will appear.
2. Type a description of the configuration that will be saved and may be used if you wish to restore the configuration at a later time, and then click *Next*.
3. The Completed Successful window will open.
4. Click *Finish*. The Unit Overview window will open.

Restoring a managed appliance configuration

You may restore the configuration of a KVM switch or serial console appliance. To restore the configuration, a previously-saved configuration file must exist. See *Saving a managed appliance configuration* on page 258.

Appliance configuration files are stored in the Rack Power Manager server appliance files repository. You may display the available configuration files by clicking the *System* tab, clicking *Appliance Files* in the top navigation bar and clicking *Configuration* in the side navigation bar.

To restore a managed appliance configuration:

1. In the Unit Overview window, click the *Restore Configuration* icon or link. The Restore Appliance Configuration Wizard will appear.
2. Click the radio button to the left of the file containing the configuration you wish to restore, and then click *Next*.
3. The Completed Successful window will open.
4. Click *Finish*. The Unit Overview window will open.
5. Reboot the managed appliance to enable the restored configuration. See *Importing data* on page 254.

Saving a managed appliance user database

NOTE: You may not save the user database of a DS1800 digital switch or DSR 1161, DSR 2161, DSR 4160, DSR 800 switch.

To save the user database of a managed appliance:

1. In the Unit Overview window, click the *Save User Database* icon or link. The Save Appliance User Database Wizard will appear.
2. Type a description of the user database that will be saved and can be used if you wish to restore the database, and then click *Next*.
3. The Completed Successful window will open.
4. Click *Finish*. The Unit Overview window will open.

Restoring a managed appliance user database

NOTE: You may not restore the user database of a DS1800 digital switch or DSR1161, DSR2161, DSR4160 or DSR800 switch.

You may restore the local user database of a KVM switch or serial console appliance. To restore the user database, a previously saved user database file must exist. See *Saving a managed appliance user database* on page 259.

User database files are stored in the Rack Power Manager server appliance files repository. You may display the available database files by clicking the *System* tab, clicking *Appliance Files* in the top navigation bar and clicking *User Database* in the side navigation bar.

To restore the user database of a managed appliance:

1. In the Unit Overview window, click the *Restore User Database* icon or link. The Restore Appliance User Database Wizard will appear.
2. Click the radio button to the left of the managed appliance user database you wish to restore, and then click *Next*.
3. The Completed Successful window will open.
4. Click *Finish*. The Unit Overview window will open.
5. Reboot the managed appliance to enable the restored user database. See *Importing data* on page 254.

Using Tasks

You may add, delete and change tasks from the Tasks window. The Tasks window lists all tasks configured in the Rack Power Manager management software system and allows you to manually run tasks.

Using the Tasks Window

To display the Tasks window:

1. Click the *System* tab.
2. Click *Tasks* in the top navigation bar. The Tasks window will open.

Customizing the Tasks window

The following fields may be displayed in the Tasks window: Use the Customize link to add or remove fields in the display. See *Using the Customize link in windows* on page 30.

- Runs On - Server(s) on which the task will run.
- Next Run - Next date and time on which the task is scheduled to run. This field will be blank for a task scheduled on a remote Rack Power Manager server.
- Last Run - Date and time of the last run of the task. This field will be blank for a task scheduled on a remote Rack Power Manager server.
- Schedule - How often and when the task is scheduled.
- Status - Status of a task. An icon in the Name column also indicates the task status.

Table 21.1: Task Status Icons

Icon	Task
	Idle - Task is not currently running
	Running - Task is currently running
	Stopping - Task has run but has not completely stopped
	Disabled - Task was prevented from executing
	Remote - Task is scheduled on a remote Rack Power Manager server

Adding tasks

You may use the Add Task Wizard to run the following tasks:

- Backup the Rack Power Manager software database and system files
- Configure SNMP trap settings on appliance
- Control power of target devices
- Control power of custom groups
- Export event log to comma separated values (.csv) file
- Migrate units (configures and upgrades Rack Power Manager software or AlterPath Manager software units)
- Send IPMI chassis control command to target devices
- Test modem connections to selected units
- Upgrade firmware of selected appliances of the same type
- Validate external authentication server user accounts
- Pull names from selected units
- Update topology for selected units
- Backup the Power Manager database
- Restore the Power Manager database

Specifying when to run tasks

You may choose to run tasks at the following times:

- **Run task now** - Runs the task immediately after you click *Finish* when adding the task in the Add Task Wizard. The Status column will indicate Running and the running icon will appear to the left of the task name.
- **One time only** - Runs the task once at a specific time on a specific date.
- **Periodic** - Runs the task a certain number of times per hour or day, beginning at a specific time on a specific date.
- **Daily** - Runs the task once every day, once Monday-Friday or regularly for a certain number of days (every 2 days, every 3 days and so on), beginning at a specific time on a specific date.
- **Weekly** - Runs the task once each week or regularly over a certain number of weeks (every 2 weeks, every 3 weeks and so on), beginning at a specific time on a specific date. You may also specify which days you wish for the task to run.
- **Monthly** - Runs the task once each month or regularly over a certain number of months (every 2 months, every 3 months and so on) beginning at a specific time on a specific date. You may also specify specific months for the task to run.

To run a task periodically:

1. In the Select When to Run the Task window of the Add Task Wizard, click *Periodic*.
2. The Specify Periodic Schedule window will open.
 - a. Select the hour, minute and AM or PM to indicate when to begin running the task.
 - b. Click *Every (minutes)* and select a number of minutes or click *Every (hours)* and select a number of hours.
 - c. Click on the calendar button or the field to the left of the calendar button and select a date to begin running the task. To use the calendar:
 - Click on the year and select a year.
 - Click on the month name and select a month or use the arrows at the top of the calendar to move forward and backward by month.
 - Click on a day in the calendar to close the calendar and fill the field to the left of the calendar with the date you have selected.

To run a task daily:

1. In the Select When to Run the Task window of the Add Task Wizard, click *Daily*.
2. The Specify Daily Schedule window will open.
 - a. Select the hour, minute and AM or PM to indicate when to begin running the task.

- b. Click *Every Day* to run the task each day of the week (Sunday-Saturday).
-or-
Click *Weekdays* to run the task once each weekday (Monday-Friday).
-or-
Click *Every (days)* and select the number of consecutive days (1-365).
- c. Click on the calendar button or the field to the left of the calendar button and select a date to begin running the task. To use the calendar:
 - Click on the year and select a year.
 - Click on the month name and select a month or use the arrows at the top of the calendar to move forward and backward by month.
 - Click on a day in the calendar to close the calendar and fill the field to the left of the calendar with the date you have selected.

To run a task weekly:

1. In the Select When to Run the Task window of the Add Task Wizard, click *Weekly*.
2. The Specify Weekly Schedule window will open.
 - a. Select the hour, minute and AM or PM to indicate when to begin running the task.
 - b. Click *Every (weeks)* and select the number of consecutive weeks (1-52).
 - c. Select the day of week to run the task from the list box. Multiple weeks may be selected by pressing **Ctrl** while clicking on the weeks.
 - d. Click on the calendar button or the field to the left of the calendar button and select a date to begin running the task. To use the calendar:
 - Click on the year and select a year.
 - Click on the month name and select a month or use the arrows at the top of the calendar to move forward and backward by month.
 - Click on a day in the calendar. The calendar will close and fill the field to the left of the calendar with the selected date.

To run a task monthly:

1. In the Select When to Run the Task window of the Add Task Wizard, click *Monthly*.
2. The Specify Monthly Schedule window will open.
 - a. Select the hour, minute and AM or PM to indicate when to begin running the task.

- b. Click *Day* and select the day of the month to run the task.
-or-
Click *The* and select a week and a day of the week to run the task. For example, if you wish to run the task each second Tuesday of the month, select *second* from the first menu and *Tuesday* from the second menu.
- c. Select the month to run the task from the list box. Multiple months may be selected by pressing **Ctrl** while clicking on the months.
- d. Click on the calendar button or the field to the left of the calendar button and select a date to begin running the task. To use the calendar:
 - Click on the year and select a year.
 - Click on the month name and select a month or use the arrows at the top of the calendar to move forward and backward by month.
 - Click on a day in the calendar. The calendar will close and fill the field to the left of the calendar with the selected date.

Adding Tasks Using the Add Task Wizard

Tasks may be added only by Rack Power Manager software administrators.

Task: Backup Rack Power Manager software database and system files

This task creates a compressed .zip file containing a backup of your Rack Power Manager software system. The backup file contains everything necessary to fully restore the Rack Power Manager software hub server. The backup file is named rpmBackup.zip by default, but you may also append the date and time to the end of the backup filename.

If a backup is restored to a server with a different IP address, managed appliances may not be able to authenticate until the new Rack Power Manager server IP address has been programmed into the managed appliances.

Once this task is added, you may run it on demand at any time; see *Running tasks manually* on page 274. You may also create a backup manually; see *Backing up and Restoring Hub Servers Manually* on page 71.

To add the task:

1. Click the *System* tab.
2. Click *Tasks* in the top navigation bar. The Tasks window will open.
3. Click *Add*. The Add Task Wizard will appear.

4. Select *Backup RPM database and system files* from the drop-down menu. Type a 1-64 character name for the task.
5. Select a time to run the task, then click *Next*. See *Specifying when to run tasks* on page 262.
6. The Specify RPM System Backup Properties dialog box will appear.
 - a. Type the directory location in which to create the system backup, which may be a physical local drive on the Rack Power Manager server or a shared network location specified by a UNC (Universal Naming Convention) path. The Location field cannot be set to a mapped network drive. The directory name must be entered in case sensitive text if your operating system supports case sensitive filenames.
 - b. If the specified directory location is a network path that requires a login, enable the *Login required to access shared drive location* checkbox. Then type the username and password and confirm the password of a user account that has read/write access to the network share location.
 - c. To encrypt the created system backup file, enable the *Encrypt Backup File* checkbox, then type a password to lock and unlock the encrypted file.
 - d. To append the date and time (in military time) to the end of the system backup filename, enable the *Use date and time for file naming* checkbox. For example, if you are creating the backup file on October 1, 2005 at 10:04 pm, the file created will be named rpmBackup1001052204.zip.

If a system backup file already exists in the specified directory and this option is not enabled, the existing backup file will be overwritten when the new backup file is created.
7. Click *Finish*.

Task: Configure SNMP trap settings on a managed appliance

This task turns SNMP traps on or off for one or more managed appliances of a particular type. To specify SNMP trap settings for other types of managed appliances, you must create additional tasks.

Once this task is added, you may run it on demand at any time; see *Running tasks manually* on page 274. You may also configure SNMP trap settings manually; see *Managed Appliance SNMP Settings* on page 147.

To add the task:

1. Click the *System* tab.

2. Click *Tasks* in the top navigation bar. The Tasks window will open.
3. Click *Add*. The Add Task Wizard will appear.
4. Select *Configure SNMP trap settings on appliance* from the drop-down menu. Type a 1-64 character name for the task.
5. Select a time to run the task (see *Specifying when to run tasks* on page 262), then click *Next*.
6. The Select Unit Group window will open. Select *All Appliances* or select a unit group, then click *Next*.
7. The Select Appliance Type window will open. Select the type of managed appliance for which to configure SNMP traps, then click *Next*.
8. The Select Appliances window will open. Select one or more managed appliances from the Available Appliances list, then click *Add*. The unit(s) will be moved to the Appliances to Configure list. Then click *Next*.
9. The Configure SNMP Traps window will open. Change the trap state by selecting one of the following from each trap menu, then click *Next*.
 - *No Change* - uses the trap on/off state already configured.
 - *Enable* - turns the trap on.
 - *Disable* - turns the trap off.

-or-

Click one of the following buttons:

 - *No Change All* - uses the on/off states already configured.
 - *Enable All* - turns all traps on.
 - *Disable All* - turns all traps off.
10. Click *Finish*.

Task: Exporting an event log .csv file

This task exports selected fields from the Rack Power Manager software system event log to a .csv file. The exported event log may be stored on a local or network drive. The event log is named eventlog.csv by default, but you may also append the date and time to the end of the event log. The output .csv file may be viewed in a text editor or spreadsheet application, such as Microsoft Excel.

Once this task is added, you may run it on demand at any time; see *Running tasks manually* on page 274. You may also save an event log using the Export Event Log tool. See *Creating an Event Log .csv File* on page 288.

To add the task:

1. Click the *System* tab.
2. Click *Tasks* in the top navigation bar. The Tasks window will open.
3. Click *Add*. The Add Task Wizard will appear.
4. Select *Export event log to a comma separated values (.CSV) file* from the drop-down menu. Type a 1-64 character name for the task.
5. Select a time to run the task (see *Specifying when to run tasks* on page 262), then click *Next*.
6. The Specify Export Event Log Properties window will open.
 - a. Type the directory in which to create the event log, which may be a physical local drive on the Rack Power Manager server or at a shared network location specified by a UNC path. The location cannot be set to a mapped network drive. The directory name must be entered in case sensitive text if your operating system supports case sensitive filenames.
 - b. If the specified directory location is a network drive that requires a log in, enable the *Login required to access shared drive location* checkbox. Then, type the username and password and confirm the password of a user account that has read/write access to the network share location.
 - c. To append the date and time (in military time) to the end of the event log file, enable the *Use date and time for file naming* checkbox. For example, if you are creating the event log file on October 1, 2005 at 10:04 pm, the file created will be named eventlog1001052204.csv.

If an event log exists in the specified directory and you do not enable this option, it will be overwritten when the new event log is created.
 - d. Click *Next*.
7. The Select Event Log Columns to Export window will open.
8. To add one or more columns to export, select the column(s) from the Available Columns list, then click *Add*. The column(s) will be moved to the Columns to Export list.

9. To remove one or more columns to export, select the column(s) from the Columns to Export list, then click *Remove*. The column(s) will be moved to the Available Columns list.
10. To change the order in which exported columns are listed in the output .csv file, select one or more columns in the Columns to Export list and use the up and down arrows to move the selected columns up or down in the listing.
11. Click *Finish*.

Task: Exporting an Asset Report to a .csv file

This task exports Asset Report data from the Rack Power Manager software system to a .csv file. The exported file may be stored on a local or network drive. The exported report is named *assetreport.csv* by default, but you may also append the date and time to the end of the file. The output .csv file may be viewed in a text editor or spreadsheet application, such as Microsoft Excel.

Once this task is added, you may run it on demand at any time; see *Running tasks manually* on page 274.

To add the task:

1. Click the *System* tab.
2. Click *Tasks* in the top navigation bar. The Tasks window will open.
3. Click *Add*. The Add Task Wizard will appear.
4. Select *Export Asset Report to a comma separated values (.CSV) file* from the drop-down menu. Type a 1-64 character name for the task.
5. Select a time to run the task (see *Specifying when to run tasks* on page 262), then click *Next*.
6. The Specify Export Asset Report Properties window opens.
 - a. Type the directory in which to create the file, which may be a physical local drive on the Rack Power Manager server or at a shared network location specified by a UNC path. The location cannot be set to a mapped network drive. The directory name must be entered in case sensitive text if your operating system supports case sensitive filenames.
 - b. If the specified directory location is a network drive that requires a log in, enable the *Login required to access shared drive location* checkbox. Then, type the username and password and confirm the password of a user account that has read/write access to the network share location.

- c. To append the date and time (in military time) to the end of the file name, enable the *Use date and time for file naming* checkbox. For example, if you are creating the file on October 1, 2010 at 10:04 pm, the file created will be named `assetreport1001102204.csv`.

If an exported report file exists in the specified directory and you do not enable this option, it will be overwritten when the new file is created.

7. Click *Finish*.

Task: Exporting a Usage Report to a .csv file

This task exports selected fields from the Rack Power Manager software system Usage Reports to a .csv file. The exported file may be stored on a local or network drive. The exported report is named `usagereport.csv` by default, but you may also append the date and time to the end of the file. The output .csv file may be viewed in a text editor or spreadsheet application, such as Microsoft Excel.

Once this task is added, you may run it on demand at any time; see *Running tasks manually* on page 274.

To add the task:

1. Click the *System* tab.
2. Click *Tasks* in the top navigation bar. The Tasks window will open.
3. Click *Add*. The Add Task Wizard will appear.
4. Select *Export Usage Report to a comma separated values (CSV) file* from the drop-down menu. Type a 1-64 character name for the task.
5. Select a time to run the task (see *Specifying when to run tasks* on page 262), then click *Next*.
6. The Specify Export Usage Report Properties window opens.
 - a. Type the directory in which to create the file, which may be a physical local drive on the Rack Power Manager server or at a shared network location specified by a UNC path. The location cannot be set to a mapped network drive. The directory name must be entered in case sensitive text if your operating system supports case sensitive filenames.
 - b. If the specified directory location is a network drive that requires a log in, enable the *Login required to access shared drive location* checkbox. Then, type the username and password and confirm the password of a user account that has read/write access to the network share location.

- c. To append the date and time (in military time) to the end of the file name, enable the *Use date and time for file naming* checkbox. For example, if you are creating the file on October 1, 2010 at 10:04 pm, the file created will be named `usagereport1001102204.csv`.

If an exported report file exists in the specified directory and you do not enable this option, it will be overwritten when the new file is created.
- d. Click *Next*.
7. The Select Last Number of Days to Export window opens. Specify the number of days in the field provided.
8. Click *Finish*.

Task: Updating the firmware of an appliance type

This task upgrades the firmware of selected DS1800 digital switches, DSI5100, CPS or CCM appliances or DSR switches. To upgrade other types of managed appliances, you must create additional tasks.

Firmware must be available before using this command. See *Firmware Management* on page 276.

Once this task is added, you may run it on demand at any time; see *Running tasks manually* on page 274.

To add the task:

1. Click the *System* tab.
2. Click *Tasks* in the top navigation bar. The Tasks window will open.
3. Click *Add*. The Add Task Wizard will appear.
4. Select *Upgrade firmware of selected appliances of the same type* from the drop-down menu. Type a 1-64 character name for the task.
5. Select a time to run the task (see *Specifying when to run tasks* on page 262), and then click *Next*.
6. The Select Unit Group window will open. Select *All Appliances* or select a particular unit group to upgrade from the menu. See *Unit Groups* on page 183. Then click *Next*.

NOTE: If the firmware is being upgraded for Liebert® MPX/MPH PDUs, ensure that the current On Board Web Interface(OBWI) access username and password is updated. Click the MPX/MPH PDU and select *Appliance Settings - OBWI Access Settings* to update the username and password.

7. The Select Appliance Type window will open. Select the type of managed appliance that you wish to upgrade, then click *Next*.
8. The Select Appliances window will open. Select one or more managed appliance to be upgraded from the Available Appliances list, then click *Add*. The appliances will be moved to the Appliances to Configure list.
9. Click *Finish*.

Task: Validating user accounts on an external authentication server

This task may be used to ensure that LDAP, Active Directory and NT external authentication services contain accounts for users. Any user accounts not found on the external authentication server will be flagged as suspicious (a question mark icon will appear to the left of the user's name). Suspicious accounts are indicated in event log files.

Once this task is added, you may run it on demand at any time; see *Running tasks manually* on page 274.

To add the task:

1. Click the *System* tab.
2. Click *Tasks* in the top navigation bar. The Tasks window will open.
3. Click *Add*. The Add Task Wizard will appear.
4. Select *Validate external authentication server user accounts* from the drop-down menu. Type a 1-64 character name for the task.
5. Select a time to run the task (see *Specifying when to run tasks* on page 262).
6. Click *Finish*.

Task: Pull names from selected units

Automatic name pull (see *Automatic name pull* on page 126) is not supported on some managed appliances. To keep these appliances synchronized with the Rack Power Manager software, you may instead schedule the pull names task.

NOTE: For more information about LANDesk Server Manager integration, see the Rack Power Manager Software Plug-in for LANDesk Server Manager online help.

This task may be used to pull names from a managed appliance and update the Rack Power Manager software database. This task performs the same operations as the Pull Names from Appliance option in the Operations menu (see *Name Synchronization* on page 125).

Once this task is added, you may run it on demand at any time; see *Running tasks manually* on page 274.

To add the task:

1. Click the *System* tab.
2. Click *Tasks* in the top navigation bar. The Tasks window opens.
3. Click *Add*. The Add Task Wizard appears.
4. Select *Pull Names from selected units* from the drop-down menu. Type a 1-64 character name for the task.
5. Select a time to run the task (see *Specifying when to run tasks* on page 262), then click *Next*.
6. The Select Unit Group window opens. Select *All Units* or select a unit group, then click *Next*.
7. The Select Unit window opens. Select the units to be included in the topology update, click *Add*.
8. Click *Finish*.

Task: Update topology for selected units

Automatic topology synchronization (see *Automatic topology synchronization* on page 129) is not supported on some units supported by plug-ins. To keep these units synchronized with the Rack Power Manager software, you may instead schedule the update topology task.

This task updates the Rack Power Manager software database when a change occurs in a units. Examples of changes are the adding/removing of a cascade switch or power device. This task performs the same operations as the Resync Unit Wizard (see *Resynchronizing units* on page 257).

Once this task is added, you may run it on demand at any time; see *Running tasks manually* on page 274.

To add the task:

1. Click the *System* tab.
2. Click *Tasks* in the top navigation bar. The Tasks window opens.
3. Click *Add*. The Add Task Wizard appears.
4. Select *Update Topology for selected units* from the drop-down menu. Type a 1-64 character name for the task.

5. Select a time to run the task (see *Specifying when to run tasks* on page 262), then click *Next*.
6. The Select Unit Group window opens. Select *All Units* or select a unit group, then click *Next*.
7. The Select Unit window opens. Select the units to be included in the topology update, click *Add*, then click *Next*.
8. The Select Options window opens.
 - a. If you enable the *Remove offline connections* checkbox, any units connections that are reported as offline in the unit will be deleted from the Rack Power Manager software database. The Update topology for selected units task does not add offline connections to the Rack Power Manager software database
 - b. If you enable the *Delete target devices that no longer have connections* checkbox, target devices that no longer have connections will be permanently deleted from the Rack Power Manager software database.
 - c. If you enable the *Allow target devices with the same name to be merged into a single target device* checkbox, the connection to a target device in the unit will be merged with the connection(s) to an existing target device in the Rack Power Manager software database.
 - d. If you enable the *Allow target devices that contain default names to be added for these type of connections* checkbox, you may then enable one or more connection type checkboxes. Any target devices that contain default names in the unit will be added to the Rack Power Manager software database only if the connection type in the unit matches an enabled connection type in this window.
9. Click *Finish*.

Running tasks manually

Although tasks are scheduled to run at particular times using the Add Task Wizard, you may run an existing task at any time.

To manually run tasks:

1. Click the *System* tab.
2. Click *Tasks* in the top navigation bar. The Tasks window will open.
3. Click the checkbox to the left of the task(s) you wish to run. To select all tasks on the page, click the checkbox to the left of Name at the top of the list.

Remote tasks that are scheduled on another Rack Power Manager server may not be run from the Rack Power Manager server to which you are logged in. To run a remote task, you must log in to the Rack Power Manager server on which the task was created.

4. Click *Run Now*. The icon to the left of the task name will change to the running icon and the status of the task will change to Running.

Displaying task results

The Task Results window displays the status of the most current run of tasks, including successful and unsuccessful runs and information on each run.

The following fields display in the Task Results window for the Configure SNMP trap settings on appliance, Control power of target devices, Migrate Units, Send IPMI chassis control command to target devices and Upgrade firmware of selected appliances of the same type tasks:

- Name - Names of the unit on which the task is running or has been run
- Start Time - Exact time at which each task run occurred
- Duration - Date and time of the task run
- Status - Result of the task run

To display the results of a task:

1. Click the *System* tab.
2. Click *Tasks* in the top navigation bar. The Tasks window will open.
3. Click the name of the task. The Task Results window will display, containing information about the task.

Deleting tasks

NOTE: Remote tasks, which are scheduled on another Rack Power Manager server, may not be deleted from the Rack Power Manager server to which you are logged in. To delete a remote task, you must log in to the Rack Power Manager server on which the task was created.

To delete a task:

1. Click the *System* tab.
2. Click *Tasks* in the top navigation bar. The Tasks window will open.
3. Click the checkbox to the left of the task(s) you wish to delete. To delete all tasks on the page, click the checkbox to the left of Name column at the top of the list.
4. Click *Delete*. A confirmation dialog box will appear.

5. Confirm or cancel the deletion.

Changing tasks

NOTE: Remote tasks, which are scheduled on another Rack Power Manager server, may not be modified from the Rack Power Manager server to which you are logged in. To change a remote task, you must log in to the Rack Power Manager server on which the task was created.

You may change the schedule and properties for existing tasks. (The Validate external authentication server user accounts task does not contain properties.)

To change a task schedule:

1. Click the *System* tab.
2. Click *Tasks* in the top navigation bar. The Tasks window will open.
3. Click on the name of the task.
4. Click *Schedule* in the side navigation bar. The Task Schedule window will open. Select the type of task you wish to schedule and complete the information. See *Specifying when to run tasks* on page 262.

To change the properties of a task:

1. Click the *System* tab.
2. Click *Tasks* in the top navigation bar. The Tasks window will open.
3. Click on the name of the task.
4. Click *Properties* in the side navigation bar. The Task Properties window will open.
5. Change the properties of the task. See the operating sequence for the task type in *Adding Tasks Using the Add Task Wizard* on page 265.

Firmware Management

The Flash firmware files for DS1800 digital switches, DSI5100, CPS and CCM appliances and DSR switches may be added, viewed and deleted using the Appliance Firmware Files window. Once a Flash firmware file(s) has been added, you may use the file(s) to upgrade the managed appliance.

To display the Appliance Firmware Files window:

1. Click the *System* tab.
2. Click *Appliance Files* in the top navigation bar. The Appliance Firmware Files window will open.

Customizing the Appliance Firmware Files window

The Version, firmware Type, Appliance Type, Creation Date and Time, Description, Language and Country fields may appear in the display. Use the Customize link to add or remove fields in the display. See *Using the Customize link in windows* on page 30.

To add a firmware file:

1. Click the *System* tab.
2. Click *Appliance Files* in the top navigation bar. The Appliance Firmware Files window will open.
3. Click *Add*. The Add Firmware File Wizard will appear.
4. Enter the directory and filename (or browse to the location) of the firmware file you want to add to the Rack Power Manager software appliance files repository.
5. Type a description of the firmware file in the Description field.
6. Click *Next*. The firmware is added and the Completed Successful window appears.
7. Click *Finish*. The Appliance Firmware Files window will open.

NOTE: Once the file is uploaded, it is no longer needed on the Rack Power Manager software client from which it was uploaded.

To display firmware information:

1. Click the *System* tab.
2. Click *Appliance Files* in the top navigation bar. The Appliance Firmware Files window will open.
3. Click on the version of a firmware file. The Firmware File Properties window will open.
4. The display includes the firmware version, appliance type, firmware creation date, country and language of the firmware. If you wish, you may change the description of the firmware file in the Description field.
5. Click *Save* and then click *Close*. The Appliance Firmware - All window will open and contain the firmware information if you saved the changes.

To delete firmware:

1. Click the *System* tab.
2. Click *Appliance Files* in the top navigation bar. The Appliance Firmware Files window will open.
3. Click the checkbox next to the firmware you want to delete.

4. Click *Delete*. A confirmation dialog box will appear.
5. Confirm or cancel the deletion.

Events and Event Logs

When an enabled, defined event occurs in the Rack Power Manager software system, it is saved in the event log. You may display the event log content, view details about an individual event log entry or delete an event log entry. You may have an email notification sent to one or more addresses when an event occurs. You may change the event log's retention period and export the event log's content.

NOTE: You must be a member of the Rack Power Manager software administrator or auditor user group to access event configuration and display windows.

Event Severity and Categories

Events are classified by severity and category.

Event severity

Table 22.1 describes the event severity levels. The icon appears in event log displays.

Table 22.1: Event Severity Levels

Severity	Icon	Description
Monitor		Events that are periodic and expected.
Information		Events that are neither periodic nor problematic.
OK		Events that are in a normal or cleared state. This value typically appears at event start up or after leaving a previous event state.
Non-critical		Abnormal events that require correcting at a later time.
Critical		Abnormal events of a more serious nature that may require quicker action, such as the failure of a scheduled task or loss of communication
Non-recoverable		Severe abnormal events impacting your Rack Power Manager management software session and requires immediate corrective action.

Severity icons

For users who are members of the Rack Power Manager software administrators or auditor user groups, the non-critical, critical and non-recoverable icons also appear near the right edge of the top navigation bar in the RPM Explorer window when events of that severity occur. Each icon is accompanied by a total count of new events of that severity. The counter is decremented when an event of that severity is deleted from the event log or when an event's state is changed from New to Acknowledged (see *Event states* on page 286). The counter is incremented when a new event of that severity is added to the log or when an event's state is changed from Acknowledged to New.

Event categories

Defined events can be classified in the following categories:

- Access control
- Appliance
- Authentication
- Data logging
- External
- IPMI
- Modem
- Sessions
- SSH Passthrough
- System
- Tasks
- Units
- Unit status
- Users

Email Notifications

The Rack Power Manager software may be configured to send one or more users an email notification when an enabled event occurs.

- You may specify which events will trigger an email notification.

- You may also specify one or more unit groups - an email notification will be sent only when a specified unit-related event occurs on a unit that is a member of the specified unit group(s).

If a specified event that is not tied to a unit occurs (for example, Rack Power Manager server started), an email notification will be sent, regardless of the any specified unit groups.

NOTE: A mail server that supports Simple Mail Transfer Protocol (SMTP) must be configured to receive email event notifications.

Customizing the Email Notifications window

The Email Subject column is always displayed in the Email Notifications window: The display may include From Address and To Address fields. Use the Customize link to add or remove fields in the display. See *Using the Customize link in windows* on page 30.

To configure an email notification:

1. Click the *Reports* tab.
2. Click *Email Notifications* in the side navigation bar. The Email Notifications window will open.
3. Click *Add*. The Add Email Notification Wizard will appear.
4. The Specify Email Properties window will open.
 - a. In the Send To field, type the email addresses of the persons you want to notify. Separate multiple addresses with a comma (.). This field has a limit of 1024 characters.
 - b. In the From field, type the email address (up to 64 characters) of the person you wish to designate as the sender of the notification.
 - c. In the Subject field, type a subject heading (up to 64 characters) for the notification.
 - d. Click *Next*.
5. The Select Events to Trigger Email Notification window will open.
 - To add one or more events, select the event(s) from the Available Events list, then click *Add*. The event(s) will be moved to the Events To Notify list.
 - To remove one or more events, select the event(s) from the Events To Notify list, then click *Remove*. The event(s) will be moved to the Available Events list.

Click *Next*.
6. The Select Unit Groups to Trigger Email Notification window will open.

- To add one or more unit groups, select the unit group(s) from the Available Unit Groups list, then click *Add*. The unit group(s) will be moved to the Selected Unit Groups list.
- To remove one or more unit groups, select the unit group(s) from the Selected Unit Groups list, then click *Remove*. The unit group(s) will be moved to the Available Unit Groups list.

Click Next.

7. The Completed Successful window will open. Click *Finish*.

To change an email notification:

1. Click *Email Notifications* in the side navigation bar. The Email Notifications window will open.
2. Click on the email subject of the notification you wish to change. The Email Notification Properties window will appear.
3. To change the notification information:
 - a. In the Send To field, enter or remove the email addresses of persons you want to notify. Separate multiple addresses with a comma (.). This field has a limit of 1024 characters.
 - b. In the From field, change the email address (up to 64 characters) of the person you wish to designate as the sender of the notification.
 - c. In the Subject field, change the subject heading (up to 64 characters) for the notification
4. To change the events:
 - To add one or more events, select the event(s) from the Available Events list, then click *Add*. The events will be moved to the Events To Notify list.
 - To remove one or more events, select the event(s) from the Events To Notify list, then click *Remove*. The events will be moved to the Available Events list.
5. To change the unit groups:
 - To add one or more unit groups, select the unit group(s) from the Available Unit Groups list, then click *Add*. The unit group(s) will be moved to the Selected Unit Groups list.

- To remove one or more unit groups, select the unit group(s) from the Selected Unit Groups list, then click *Remove*. The unit group(s) will be moved to the Available Unit Groups list.
6. Click *Save* and then click *Close*. The Email Notifications window will open.

To test an email notification:

Once an email notification has been created, you may send a test message to ensure that the notification is delivered to the specified recipients.

1. Click *Email Notifications* in the side navigation bar. The Email Notifications window will open.
2. Click the checkbox to the left of the notification(s) to be tested. To select all notifications on the page, click the checkbox to the left of Email Subject at the top of the list.
3. Click *Test*. You will be prompted to confirm the test.
4. Confirm or cancel the test.

To delete an email notification:

1. Click *Email Notifications* in the side navigation bar. The Email Notifications window will appear.
2. Click the checkbox to the left of the notifications to delete. To select all notifications on the page, click the checkbox to the left of Email Subject at the top of the list.
3. Click *Delete*. You will be prompted to confirm the deletion.
4. Confirm or cancel the deletion.

Enabling and Disabling Event Logging

The logging of individual events that occur in the Rack Power Manager software system may be enabled or disabled. When an enabled event occurs, it is written to the event log. When an event is disabled, its occurrence will not be logged until the event is enabled.

By default the Enabled Log Events window lists the event name and whether it is enabled or disabled. (The enabled/disabled state differs from an event's state in the event log; see *Event states* on page 286.) You may change which fields and the number of items per page that will be displayed in the Enabled Log Events window by clicking the *Customize* link (see *Using the Customize link in windows* on page 30). This may be helpful if you want to sort the list by a field such as category or event ID.

To enable or disable logging of one or more events:

1. Click the *Reports* tab.
2. Click *Enabled Events* in the side navigation bar. The Enabled Log Events window will open, listing all enabled and disabled log events. If you want to display only the events in a particular category, click the category link in the side navigation bar.
3. Click the checkbox to the left of one or more events. To select all events on the page, click the checkbox to the left of Log Event at the top of the list.
4. Click *Enable* or *Disable*. (Events cannot be enabled unless they are already disabled. Similarly, events cannot be disabled unless they are already enabled).

The Enabled Log Events window will refresh with the new information.

Displaying the Event Log

There are several ways to customize event log displays.

- You may display all events (or at least the most recent 5000) in the log.
- You may display events of a particular severity or a particular category.
- You may display events that occurred during a specified interval.
- You may display events based on their state; see *Event states* on page 286.

Event log display fields

The following fields are always displayed in the Event Log window:

- Severity - See *Event severity* on page 279. Clicking this field will display the Event Information window, which contains details about the event.
- Date/Time - Displays the date and time of an event in the client computer's time zone.
- Description - Short description of an event.

The following fields may be displayed. Use the Customize link to add or remove fields in the display. See *Using the Customize link in windows* on page 30.

- State - New or Acknowledged. See *Event states* on page 286. This field is displayed only when the Show All button is enabled. Its display is not affected by customization.
- Category - Category of an event log entry.
- Detailed Description - Detailed information, which may include the name of a target device, session type, user and so on. For example, a MIB-II interface link up trap might

contain *Appliance change of state* in the Description column, while the Detailed Description column contains *Generic link up interface 1*.

- Rack Power Manager Server - Name of the Rack Power Manager server where the event was logged.
- Event ID - Unique event identifier, which can be useful for sorting displays.
- Trap Enterprise - Enterprise object identifier for a received SNMP trap. (The Trap Enterprise field in an Event Log window is named Enterprise OID in the Event Information window.)
- Unit - Name of a managed appliance for the event.
- User - User associated with the event. For example, when a Unit Deleted event is detected, this field contains the username of the initiator.

To display the event log:

Click the *Reports* tab. The Event Log - All window will open.

- To display event log entries by severity, click *Severity Level* in the side navigation bar, and then click one of the levels. (See the Note below for an alternative way to display the event log by certain severity levels.)
- To display event log entries by category, click *Event Category* in the side navigation bar, and then click one of the categories.
- To display event log entries that occurred during a specified interval, see *Using the date filter* on page 287.
- By default, the display includes event log entries with a state of New (see *Event states* on page 286) and the State column is not displayed. To view events with an Acknowledged state in the display, enable the *Show All* button. The State column will be added to the display, and the list will include events with any state (New or Acknowledged). Acknowledged events will be grayed-out to differentiate them from New events, but any event can be selected.

To remove events with an Acknowledged state from the display, disable the *Show All* button. The State column will be removed from the display, and only unacknowledged (state = New) events will appear.

NOTE: You may also display a list of only the new non-critical, critical or non-recoverable event log entries by clicking the appropriate icon in the right portion of the top navigation bar (see Table 22.1 for pictures).

To display details of an event log entry:

1. Click the *Reports* tab.

2. In an Event Log window, click on a link in the Severity column. The Event Information window will open.

See *Event log display fields* on page 284 for descriptions of information in the Event Details section of the display.

The Event History table contains any state change information. This includes when the state was changed, the type of change (for example, Changed from New to Acknowledged), and who (username) made the state change.

3. Click *Close*. The Event Log window will open.

To delete one or more event log entries:

1. In an Event Log window, click the checkbox to the left of the event(s) to delete. To select all events on the page, click the checkbox to the left of Severity at the top of the list.
2. Click *Delete*. A confirmation dialog box will appear.
3. Confirm or cancel the deletion.

Event states

When an event first occurs and is placed in the event log, it is considered to be in a New state. You may delete the event, which will remove it from displays and from the event log. However, if you wish to prevent an event from being displayed but not delete it from the event log, you may acknowledge the event, which will change its state from New to Acknowledged.

You may also change an event's state from Acknowledged to New again. This can be useful if you mistakenly changed an event's state to Acknowledged. The Event Information window for each event contains an Event History that indicates when that event's state was changed and by whom.

When you change a non-recoverable, critical or non-critical event's state to Acknowledged, the counter next to that severity icon in the top navigation bar will be decremented. If you change one of these events from Acknowledged to New, the counter is incremented.

In an event log display, if the Show All button is not enabled, the display will only include events with a New state. If the Show All button is enabled, events in any state (New or Acknowledged) will be included. Acknowledged events will be grayed-out.

To change the state of one or more event log entries:

1. Click the *Reports* tab. The Event Log - All window will open. You may tailor the display by severity, category or date, if desired.
2. Click the checkbox to the left of the events whose state you wish to change. To select all events on the page, click the checkbox in the heading at the top of the list.

3. Click *Set State* and then select *Acknowledged* or *New* from the drop-down list.

Using the date filter

The event log retains all events occurring in the Rack Power Manager software system for the specified retention time. By default, the 5000 most recent events are displayed. You may use the date filter to display older events or to display events from any interval in the retention time.

To use the date filter:

1. Click the *Reports* tab.
2. In any Event Log window, click *Date Filter*. The Date Filter window will open.
3. In the first drop-down menu in the From line, select *Events On* to select the start date and time.
4. Click on the calendar button or the field to the left of the calendar button and select a start date. To use the calendar:
 - a. Click on the year and select a year from the drop-down menu.
 - b. Click on the month name and select a month from the drop-down menu, or use the arrows at the top of the calendar to move forward and backward by month.
 - c. Click on a day in the calendar to close the calendar and fill the field to the left of the calendar with the date you have selected.
5. Select an hour, minute and which half of the day for the start date.
6. In the first drop-down menu in the To line, select *Events On* to select the end date and time.
7. Repeat steps 4 and 5 to specify the end date.
8. Click *Apply*. The previous event log view window will open with the event range specified in the Filter Date window.

The Clear Date Filter button will appear in the event log view window. To clear date filtering, click this button.

Changing the Event Log Retention Period

By default, an event log is retained for seven days (one week). You may specify a retention period of up to 365 days (one year).

NOTE: Event log information is stored in the Rack Power Manager software database and is replicated. Increasing the event log retention time may impact the performance of the Rack Power Manager software system. It is recommended that old event log entries be archived to .csv files by scheduling tasks; see *Task: Exporting an event log .csv file* on page 267. You may also export event logs at any time; see *Creating an Event Log .csv File* on page 288.

To change the event log retention period:

1. Click the *Reports* tab.
2. Click *Log Retention* in the side navigation bar. The Event Log Retention Time window will open.
3. Type a number of days (from 1-365) in the Days field, or select it using the menu.
4. Click *Save*.

Creating an Event Log .csv File

All or selected columns of the event log can be exported as a comma separated values (.csv) file. The output event log file is named eventlog.csv by default, but you may change the name when it is saved. The .csv file may be viewed in a text editor or spreadsheet application, such as Microsoft Excel.

NOTE: To create a task to export the event log to a .csv file, see *Task: Exporting an event log .csv file* on page 267.

To create an event log .csv file:

1. Click the *Reports* tab.
2. Click *Tools* in the side navigation bar. The Event Log Tools window will open.
3. Click the *Export Event Log* icon or text. The Export Event Log Wizard will appear.
4. The Select Columns to Export window will open.
 - To add one or more columns to export, select the column(s) from the Available Columns list, then click *Add*. The columns will be moved to the Columns to Export list.
 - To remove one or more columns, select the column(s) from the Columns to Export list, then click *Remove*. The columns will be moved to the Available Columns list.
 - To change the order in which exported columns are listed in the output .csv file, select one or more columns in the Columns to Export list and use the up and down arrows to move the selected columns up or down in the listing.

Click *Next*.

5. The Save Process window will open, explaining how the file will be saved. Click *Next*.

6. The Completed Successful window will open, along with a File Download dialog box.
7. From the File Download dialog box, click *Open*. The file will be downloaded and will open on the Rack Power Manager software client. By default, .csv files are configured to open in Microsoft Excel. If Microsoft Excel is not installed on your computer, you will be prompted to select a text editor to open the .csv file.

-or-

From the File Download dialog box, click *Save*. The Save As dialog box will appear. Select a directory and filename and click *Save* to save the .csv file.

8. Click Finish. The Event Log Tools window will open.

Plug-ins

A plug-in provides support for a specific appliance type (model) in the Rack Power Manager software. A plug-in is packaged into a single archive file that can be shipped and added independently of the Rack Power Manager software. Rack Power Manager supports 3rd party rack PDUs using an appliance plug-in.

Although plug-ins are created independently, a particular Rack Power Manager software release may include one or more plug-ins that have already been added to the software. The release notes will indicate if any plug-ins are included. If a plug-in is included, you will not need to add it to the hub or spoke servers.

This chapter describes how to add and manage plug-ins in the Rack Power Manager software. Once you successfully complete the sequence for adding a plug-in, you may add appliances of that type and initiate other operations from the Rack Power Manager software that are supported in that plug-in.

NOTE: You must have Rack Power Manager software administrator access rights to view, add and manage plug-ins.

Plug-ins are created using the Plug-in API in the Rack Power Manager Software Development Kit (SDK).

Recommended Sequence for Adding/Upgrading Plug-ins

To add or upgrade a plug-in:

1. Ensure that scheduled replication will not occur during the adding or upgrading of plug-ins - you may need to change the replication schedule temporarily.
2. Perform a replication operation on every spoke server. See *Replication* on page 78.
3. Perform a backup of the Rack Power Manager software database. See *Backing up and Restoring Hub Servers Manually* on page 71.
4. Add or upgrade the plug-in on the hub server.
 - To add a plug-in, see *Adding Plug-ins* on page 292.

- To upgrade a plug-in, see *Upgrading a plug-in* on page 295.
5. Add or upgrade the plug-in on each spoke server. All spoke servers should have the same plug-ins at the same version.
 6. Perform a replication operation on every spoke server.
 7. Perform a backup of the Rack Power Manager software database.
 8. If you changed the replication schedule in step 1, you may change it back to its original values.

Adding Plug-ins

For optimal operation, the hub and all of the spoke servers should have the same version of a plug-in installed. Follow the steps described in *Recommended Sequence for Adding/Upgrading Plug-ins* on page 291.

During the add operation on the hub server, new data types defined in the plug-in are registered in the Rack Power Manager software database. After the plug-in is added to the spoke server and a replication operation is initiated, the registration information on the hub server is propagated to the spoke server.

On the hub server, a new plug-in becomes active when it is added. On a spoke server, a new plug-in becomes active only after the plug-in is added to the hub and then to the spoke and a subsequent replication completes successfully.

For some plug-ins, you may need to add a license key to the Rack Power Manager software system before adding the plug-in to any server. See the documentation included with the plug-in or contact your Emerson representative to determine if a key is needed. To add a license, see *Licenses* on page 58.

To add a plug-in:

1. Click the *System* tab.
2. Click *Plug-ins* in the top navigation bar.
3. Click *Add*. The Add Plug-in Wizard will open.
4. The Select Plug-in window will open. Enter the name or browse to the location of the plug-in file, then click *Next*.
5. The Overview window will open. This window contains read-only information about the plug-in. Click *Next*.

6. The Adding Plug-in page will open while the plug-in is added to the Rack Power Manager software system.
7. The Completed Successful window will open. Click *Finish*.

NOTE: If you added a plug-in for a Cyclades™ appliance, you must disable the Cyclades Web Manager to maintain security standards. For information about how to disable the Cyclades Web Manager, see the online help for the Cyclades appliance plug-in.

Displaying Plug-in Information

You may display information about all plug-ins that have been added as well as information about a single plug-in on the Rack Power Manager server where you are logged in.

To display plug-in information:

1. Click the *System* tab.
2. Click *Plug-ins* in the top navigation bar. The Plug-ins window will open.
3. To display information about one plug-in, click the plug-in name. The Plug-in overview window will open.

Information in the Overview area is read-only.

The RPM Servers table lists the status of the plug-in on each Rack Power Manager server. Each row includes the name of the server and the plug-in version plus the administrative and operational status of the plug-in on that server.

Table 23.1: Plug-ins Display Information

Field	Description
Name	Plug-in name, acquired from the plug-in.
Version	Plug-in version (on this server), acquired from the plug-in when it was added or upgraded.
Overall Status	Same - The plug-in's operational status, administrative status and version is the same on all Rack Power Manager servers. Mixed - The plus-in's operational status, administrative status and version is not the same on all Rack Power Manager servers.

Field	Description
Administrative Status	Administrative status on this server. Valid values are: - RPM server not responding - (<i>This value is valid only when a single plug-in has been selected.</i>) The Rack Power Manager software could not obtain plug-in status on this server. To examine server status, click the <i>System</i> tab, then <i>RPM Server</i> in the top navigation bar. If you are on a hub server, click <i>Spoke Servers</i> in the side navigation bar and then select the appropriate server. If you are on a spoke server, click <i>Hub Server</i> in the side navigation bar. Replication needed - The plug-in has been added, but replication is required before the plug-in can be used. - Active - The plug-in is registered and operational. Disabled - The plug-in has been disabled. - Not installed - The plug-in has not been added to this server. If the Rack Power Manager software can obtain information from the status service about this plug-in (from other servers where it is installed), the Name field will contain the plug-in's name. If the status service does not provide this information, the Name field will contain the plug-in's domain and ID.
Operational Status	Operational status on this server. Valid values are: - Inactive - The plug-in is not running. - Active - The plug-in is running. - Initializing - The plug-in is starting up. Shutting down - The plug-in is stopping. - Upgrading - The plug-in is in the upgrade process.
Detailed Operational Status *	Detailed status acquired from the plug-in.
Description *	Descriptive information acquired from the plug-in.
Languages *	Language information acquired from the plug-in.
Appliance Type *	Appliance type information acquired from the plug-in.
Vendor *	Owning vendor of the plug-in, according to information acquired from the plug-in.
*By default, these fields are not displayed in the Plug-ins window. Use the Customize link to specify which fields you want to display; see <i>Using the Customize link in windows</i> on page 30. These fields are always displayed in the individual plug-ins' overview windows.	

Managing Plug-ins

After a plug-in has been added, you may upgrade it to another (generally, newer) version. You may also disable a plug-in if necessary for troubleshooting, and then (re)activate it.

- You may initiate an action only for plug-ins on the Rack Power Manager server you are currently logged into.
- The plug-in must currently have an administrative status that allows the action (for example, you can activate a plug-in only if its current administrative status is disabled).

Upgrading a plug-in

When you upgrade the existing version of a plug-in, follow the steps described in *Recommended Sequence for Adding/Upgrading Plug-ins* on page 291.

To upgrade a plug-in:

1. Click the *System* tab.
2. Click *Plug-ins* in the top navigation bar. The Plug-ins window will open.
3. Click on the name of plug-in to be upgraded. The plug-in overview window will open.
4. In the Rack Power Manager Servers area, click the checkbox next to the Rack Power Manager server you are currently logged into.
5. Click *Upgrade*. The Upgrade Plug-in Wizard will open.
6. Enter the name or browse to the location of the plug-in file, then click *Next*.
7. The Overview window will open. This window contains read-only information about the plug-in. Click *Next*.
8. The Upgrading Plug-in page will open while the plug-in is being upgraded.
9. The Completed Successful window will open. Click *Finish*.

Disabling and activating a plug-in

When a plug-in is disabled, you cannot use any features and operations supported by that plug-in. Appliances and target devices that were added to the Rack Power Manager software system before the plug-in was disabled will still appear in Units View windows, but you will not be able to acquire status from those units, and links that initiate connections to those units will not be available. You will not be able to add more appliances of that type until the plug-in is (re)activated.

A disabled plug-in will remain disabled if the Rack Power Manager software is restarted.

To disable a plug-in:

1. Click the *System* tab.
2. Click *Plug-ins* in the top navigation bar. The Plug-ins window will open.
3. Click on the name of plug-in to be disabled. The plug-in overview window will open.
4. In the RPM Servers area, click the checkbox next to the Rack Power Manager server you are currently logged into.
5. Click *Disable*. A confirmation dialog box will appear.
6. Confirm or cancel the action.

To activate a plug-in:

1. Click the *System* tab.
2. Click *Plug-ins* in the top navigation bar. The Plug-ins window will open.
3. Click on the name of plug-in to be activated. The plug-in overview window will open.
4. In the RPM Servers area, click the checkbox next to the Rack Power Manager server you are currently logged into.
5. Click *Activate*. A confirmation dialog box will appear.
6. Confirm or cancel the action.

APPENDICES

Appendix A: Technical Support

Our Technical Support staff is ready to assist you with any installation or operating issues you encounter with your Avocent product. If an issue should develop, follow the steps below for the fastest possible service:

To resolve an issue:

1. Check the pertinent section of the manual to see if the issue can be resolved by following the procedures outlined.
2. Check our web site at www.avocent.com/support to search the knowledge base or use the online service request.
3. Call the Avocent Technical Support location nearest you.

Appendix B: Terminal Emulation

This appendix contains information about the keys, sequences, encoding and decoding for the Rack Power Manager management software terminal emulation modes when using the Telnet Viewer. Encode refers to how the client interface processes typed keys. Decode refers to how the client interface processes data coming from the target device.

The terminal emulation mode is set by selecting *Options - Session Properties* in the Telnet Viewer window and then using the Terminal Emulation drop-down menu in the Session Properties dialog box. See *Customizing Session Properties* on page 236.

VT terminal emulation

Table B.1 lists the VT key and keypad numeric codes. Emerson encodes all applicable keys as numeric; decoding is not supported.

Table B.1: VT Key and Keypad Numeric Codes

Key	Keypad Numeric Code
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9
- (dash)	- (dash)
, (comma)	, (comma)
. (period)	. (period)
Enter	Same as Return key

VT100+ terminal emulation

The VT100+ emulation provides compatibility with the Microsoft headless server EMS serial port interface. The Rack Power Manager software Telnet Viewer VT100+ terminal emulation works identically to VT100, with the exception of support for the function keys listed in Table B.2.

Table B.2: VT100+ Function Key Support

Function	Sequence	Function	Sequence
Home	<Esc> h	F4 **	<Esc> 4
End	<Esc> k	F5	<Esc> 5
Insert	<Esc> +	F6	<Esc> 6
Delete *	<Esc> -	F7	<Esc> 7
Page Up	<Esc> ?	F8	<Esc> 8
Page Down	<Esc> /	F9	<Esc> 9
F1 **	<Esc> 1	F10	<Esc> 0
F2 **	<Esc> 2	F11	<Esc> !
F3 **	<Esc> 3	F12	<Esc> @

* ASCII, VT52, VT100, VT102, VT220 and VT320 modes send hex 7F when the **Delete** key is pressed.

** VT100, VT102, VT220 and VT320 modes map the **F1-F4** keys to the **PF1-PF4** keys.

VT102 terminal emulation

VT102 terminal emulation works identically to VT100 with additional support for decoding receive codes as described in Table B.3.

Table B.3: VT102 Receive Codes

VT102 Receive Code	
Delete Character (DHC)	Deletes n characters starting with the character at the current cursor position, and moves all remaining characters left n positions. n spaces are inserted at the right margin.

VT102 Receive Code	
Insert Line (IL)	Inserts n lines at the line where the cursor is currently positioned. Lines displayed below the cursor position move down. Lines moved past the bottom margin are lost.
Delete Line (DL)	Deletes n lines starting with the line where the cursor is currently positioned. As lines are deleted, lines below the cursor position move up.

VT100 terminal emulation

Table B.4 lists the VT100 special key and control (**Ctrl**) key combinations and indicates Emerson encoding/decoding support, where Yes = supported and No = not supported.

Table B.4: VT100 Special Keys and Control Keys

Keys	Hex Code	Function Mnemonic	Encode/Decode
Return	0D	CR	Yes/Yes
Linefeed	0A	LF	Yes/Yes
Backspace	08	BS	Yes/Yes
Tab	09	HT	Yes/Yes
Spacebar	20	(SP)	Yes/Yes
Esc	1B	Esc	Yes/No
Ctrl+Spacebar	00	NUL	Yes/No
Ctrl+A	01	SOH	Yes/No
Ctrl+B	02	STX	Yes/No
Ctrl+C	03	ETX	Yes/No
Ctrl+D	04	EOT	Yes/No
Ctrl+E	05	ENO	Yes/No
Ctrl+F	06	ACK	Yes/No
Ctrl+G	07	BELL	Yes/Yes

Keys	Hex Code	Function Mnemonic	Encode/Decode
Ctrl+H	08	BS	Yes/Yes
Ctrl+I	09	HT	Yes/Yes
Ctrl+J	0A	LF	Yes/Yes
Ctrl+K	0B	VT	Yes/No
Ctrl+L	0C	FF	Yes/No
Ctrl+M	0D	CR	Yes/No
Ctrl+N	0E	SO	Yes/No
Ctrl+O	0F	SI	Yes/No
Ctrl+P	10	DLE	Yes/No
Ctrl+Q	11	DC1 or XON	Yes/No
Ctrl+R	12	DC2	Yes/No
Ctrl+S	13	DC3 or XOFF	Yes/No
Ctrl+T	14	DO4	Yes/No
Ctrl+U	15	NAK	Yes/No
Ctrl+V	16	SYN	Yes/No
Ctrl+W	17	ETB	Yes/No
Ctrl+X	18	CAN	Yes/No
Ctrl+Y	19	EM	Yes/No
Ctrl+Z	1A	SUB	Yes/No
Ctrl+[	1B	Esc	Yes/No
Ctrl+\	1C	FS	Yes/No
Ctrl+]	1D	GS	Yes/No
Ctrl+^	1E	RS	Yes/No
Ctrl+_	1F	US	Yes/No

Table B.5 lists the VT100 ANSI mode and cursor keys for set and reset modes. Encoding and decoding is supported for all the cursor keys listed.

Table B.5: VT100 ANSI Set and Reset Mode Cursor Keys

Cursor Key	Mode Reset	Mode Set
Up	Esc[A	EscOA
Down	Esc[B	EscOB
Right	Esc[C	EscOC
Left	Esc[D	EscOD

Table B.6 lists the VT100 PF1-PF4 key definitions. Encoding of each listed key is supported; decoding is not applicable.

Table B.6: VT100 PF1-PF4 Key Definitions

Key	Code Sequence
F1	Esc[OP
F2	Esc[OQ
F3	Esc[OR
F4	Esc[OS

Table B.7 lists the ANSI mode control sequences for VT100 terminal emulation and indicates Avocent encoding/decoding support, where Yes = supported and No = not supported.

Table B.7: VT100 ANSI Mode Control Sequences

Control Sequence	Definition	Encode/Decode
Esc[Pn; Pn R	Cursor Position Report	No/No
Esc[Pn D	Cursor Backward	No/Yes
Esc[Pn B	Cursor Down	No/Yes
Esc[Pn C	Cursor Forward	No/Yes

Control Sequence	Definition	Encode/Decode
Esc[Pn; Pn H	Cursor Position	No/Yes
Esc[Pn A	Cursor Up	No/Yes
Esc[Pn c	Device Attributes	No/No
Esc# 8	Screen Alignment Display	No/Yes
Esc# 3	Double Height Line - Top Half	No/No
Esc# 4	Double Height Line - Bottom Half	No/No
Esc# 6	Double Width Line	No/No
Esc Z	Identify Terminal	No/No
Esc =	Keypad Application Mode	No/No
Esc >	Keypad Numeric Mode	No/No
Esc[Ps q	Load LEDs	No/No
Esc 8	Restore Cursor	No/Yes
Esc[<sol>; <par>;	Report Terminal Parameters <nbits>; <xspeed>; <rspeed>; <clkmul>; <flags>x	No/No
Esc[<sol> x	Request Terminal Parameters	No/No
Esc 7	Save Cursor	No/Yes
Esc[Pn; Pn r	Set Top and Bottom Margins	Yes/Yes
Esc# 5	Single Width Line	No/No
Esc[2; Ps y	Invoke Confidence Test	No/No
Esc[Ps n	Device Status Report	No/Yes
Esc[Ps J	Erase in Display	No/Yes
Esc[Ps K	Erase in Line	No/Yes
Esc H	Horizontal Tabulation Set	Yes/Yes
Esc[Pn; Pn f	Horizontal and Vertical Position	No/Yes

Control Sequence	Definition	Encode/Decode
Esc D	Index	No/Yes
Esc E	Next Line	No/Yes
Esc M	Reverse Index	No/Yes
Esc c	Reset to Initial State	No/No
Esc [Ps; Ps;...;Ps 1	Reset Mode	No/No
Esc (A	Select Character Set G0 U.K.	No/No
Esc) A	Select Character Set G1 U.K.	No/No
Esc (B	Select Character Set G0 ASCII	Yes/Yes
Esc) B	Select Character Set G1 ASCII	Yes/Yes (limited support)
Esc (0	Select Character Set G0 Spec. Graphics	Yes/Yes (limited support)
Esc) 0	Select Character Set G1 Spec. Graphics	Yes/Yes (limited support)
Esc (1	Select Character Set G0 Alt. Character ROM Standard Character Set	No/No
Esc) 1	Select Character Set G1 Alt. Character ROM Standard Character Set	No/No
Esc (2	Select Character Set G0 Alt. Character ROM Special Graphics	No/No
Esc) 2	Select Character Set G1 Alt. Character ROM Special Graphics	No/No
Esc [Ps;...; Ps m	Select Graphic Rendition	No/No
Esc Ps;...;Ps h	Set Mode	No/No
Esc [Ps g	Tabulation Clear	No/No
Esc [Ps;Ps;...; Ps m	Character Attributes 7 - Reverse Video On	No/Reverse Video only

Control Sequence	Definition	Encode/Decode
Esc[K or Esc[0 K	Erase from cursor to end of line	No/Yes
Esc[1 K	Erase from beginning of line to cursor	No/No
Esc[2 K	Erase entire line containing cursor	No/No
Esc[J or Esc[0 J	Erase from cursor to end of screen	No/Yes
Esc[1 J	Erase from beginning of screen to cursor	No/No
Esc[2 J	Erase entire screen	No/No
Esc[Ps;Ps;...Ps q	Programmable LEDs	No/No
Esc[Pt; Pb r	Scrolling Region	No/No
Esc[g or Esc[0 g	Clear tab at current column	Yes/Yes
Esc[3 g	Clear all tabs	Yes/Yes
Esc[2 0 h	Modes to Set - New Line - Only supports Linefeed/New Line Column mode wraparound	No/Yes
Esc[2 0 l	Modes to Reset - Linefeed - Only supports Linefeed/New Line Column mode wraparound	No/Yes
Esc[? 1 h	Modes to Set - Cursor Key Mode Appl.	No/No
Esc[? 1 l	Modes to Reset - Cursor Key Mode Cursor	No/No
>Esc[? 2 l	Modes to Reset VT52	No/No
Esc[? 3 h	Modes to Set - 132 columns	No/No
Esc[? 3 l	Modes to Reset - 80 columns	No/No
Esc[? 4 h	Modes to Set - Smooth Scroll	No/No
Esc[? 4 l	Modes to Reset - Jump Scroll	No/No
Esc[? 5 h	Modes to Set - Reverse Screen Mode	No/No
Esc[? 5 l	Modes to Reset - Normal Screen Mode	No/No
Esc[? 6 h	Modes to Set - Relative Origin Mode	No/No
Esc[? 6 l	Modes to Reset - Absolute Origin Mode	No/No

Control Sequence	Definition	Encode/Decode
Esc[? 7 h	Modes to Set - Wraparound On	No/No
Esc[? 7 l	Modes to Reset - Wraparound Off	No/No
Esc[? 8 h	Modes to Set - Auto Repeat On	No/No
Esc[? 8 l	Modes to Reset - Auto Repeat Off	No/No
Esc[? 9 h	Modes to Set - Interlace On	No/No
Esc[? 9 l	Modes to Reset - Interlace Off	No/No
Esc[6 n	Report Cursor Position - Invoked by	No/No
Esc[P1; Pc R	Report Cursor Position - Response is	No/No
Esc[5 n	Status Report - Invoked by	No/No
Esc[0 n	Status Report - Response is terminal OK	No/No
Esc[3 n	Status Report - Response is terminal not OK	No/No
Esc[x or Esc[0 c	What are you? Invoked by	No/Yes
Esc[? 1; Ps c	What are you? Response is	No/Yes
Esc c	Reset	No/No
Esc# 8	Fill screen with Es	No/Yes
Esc[2; Ps y	Invoke Test(s)	No/No

VT220 terminal emulation

Table B.8 lists the keystroke mapping (encoding) for VT220 emulation.

Table B.8: VT220 Encoding

VT220 Keyboard	PC Keyboard	VT220 Keyboard Byte Sequence
Delete	Delete	0x7F
Left Arrow	Left Arrow	Esc[D

VT220 Keyboard	PC Keyboard	VT220 Keyboard Byte Sequence
Right Arrow	Right Arrow	Esc[C
Up Arrow	Up Arrow	Esc[A
Down Arrow	Down Arrow	Esc[B
Keypad /	Keypad /	/
Keypad *	Keypad *	*
Keypad -	Keypad -	-
Keypad +	Keypad +	+
Keypad .	Keypad .	.
Keypad 0..9	Keypad 0..9	>0..9
F1	F1	EscOP
F2	F2	EscOQ
F3	F3	EscOR
F4	F4	EscOS
F6	F6	Esc[17 ~
F7	F7	Esc[18 ~
F8	F8	Esc[19 ~
F9	F9	Esc[20 ~
F10	F10	Esc[21 ~
F11	F11	Esc[23 ~
F12	F12	Esc[24 ~
F13	Ctrl - F5	Esc[25 ~
F14	Ctrl - F6	Esc[26 ~
F15	Ctrl - F7	Esc[28 ~

VT220 Keyboard	PC Keyboard	VT220 Keyboard Byte Sequence
F16	Ctrl - F8	Esc[29~
F17	Ctrl - F9	Esc[31~
F18	Ctrl - F10	Esc[32~
F19	Ctrl - F11	Esc[33~
F20	Ctrl - F12	Esc[34~

Table B.9 lists the decoding for VT220 terminal emulation.

Table B.9: VT220 Decoding

VT220 Keyboard Function	VT220 Keyboard Byte Sequence
Index	Esc D
New Line	Esc E
Reverse Index	Esc M
Escape	Esc O
Save cursor and attributes	Esc 7
Restore cursor and attributes	Esc 8
Up Arrow	Esc [A
Down Arrow	Esc [B
Right Arrow	Esc [C
Left Arrow	Esc [D
Set cursor to home position	Esc [H
Set cursor to home position	Esc [f
Character attributes	Esc [m
Erase from cursor to end of line	>Esc [K

VT220 Keyboard Function	VT220 Keyboard Byte Sequence
Erase from cursor to end of screen	Esc[j
Programmable LEDs	Esc[q
What are You?	Esc[c
Set Mode	Esc[?
Delete 1 Character	Esc[P
Insert 1 Line	Esc[L
Delete 1 Line	Esc[M
Up Arrow	Esc[OA
Down Arrow	Esc[OB
Right Arrow	Esc[OC
Left Arrow	Esc[OD
Fill Screen with Es	Esc#8
Up Arrow amount specified by Pn	Esc[PnA
Down Arrow amount specified by Pn	Esc[PnB
Right Arrow amount specified by Pn	Esc[PnC
Left Arrow amount specified by Pn	Esc[PnD
Erase parts of current line	Esc[PnK
Erase parts of current screen	Esc[PnJ
Direct Cursor Addressing	Esc[PnH
Direct Cursor Addressing	Esc[Pnf
Programmable LEDs	Esc[Pnq
Scrolling Region	Esc[Pnr
Clear tabs	Esc[Png

VT220 Keyboard Function	VT220 Keyboard Byte Sequence
Device status report	Esc [P n n
What are you?	Esc [P n c
Sat Mode	Esc [P n h
Delete Pn Characters	Esc [P n P
Insert Pn Characters	Esc [P n L
Delete Pn Lines	Esc [P n M
Insert Character	Esc [P n @
Erase Pn Characters	Esc [P n X

VT52 terminal emulation

Table B.10 lists the keystroke mapping (encoding) for VT52 terminal emulation.

Table B.10: VT52 Encoding

VT52 Keyboard	PC Character Sequence	VT52 Keyboard Byte Sequence
Delete	Delete	0x7F
Up Arrow	Up Arrow	Esc A
Down Arrow	Down Arrow	Esc B
Right Arrow	Right Arrow	Esc C
Left Arrow	Left Arrow	Esc D
Shift-F1	PF1	Esc P
Shift-F2	PF2	Esc Q
Shift-F3	PF3	Esc R
Shift-F4	PF4	Esc S

Table B.11 lists the decoding for VT52 terminal emulation.

Table B.11: VT52 Decoding

VT52 Keyboard Function	VT52 Keyboard Byte Sequence
Cursor Up	Esc A
Cursor Down	Esc B
Cursor Right	Esc C
Cursor Left	Esc D
Cursor Home	Esc H
Reverse Linefeed	Esc I
Erase to end of screen	Esc J
Erase to end of line	Esc K

Table B.12 lists the VT52 and ANSI auxiliary keypad definitions. Encoding of each listed keypad key is supported; decoding is not applicable.

Table B.12: VT52 ANSI Mode Auxiliary Keypad Definitions

Keys	Keypad Numeric Code	VT52 Keypad	ANSI Keyboard
0	0	Esc ? p	Esc O p
1	1	Esc ? q	Esc O q
2	2	Esc ? r	Esc O r
3	3	Esc ? s	Esc O s
4	4	Esc ? t	Esc O t
5	5	Esc ? u	Esc O u
6	6	Esc ? v	Esc O v
7	7	Esc ? w	Esc O w
8	8	Esc ? x	Esc O x
9	9	Esc ? y	Esc O y
-(dash)	-(dash)	Esc ? m	Esc O m

Keys	Keypad Numeric Code	VT52 Keypad	ANSI Keyboard
, (comma)	, (comma)	Esc ? l	Esc O l
. (period)	. (period)	Esc ? n	Esc O n
Enter	Same as Return key	Esc ? m	Esc O m

VT320 terminal emulation

Table B.13 lists the keystroke mapping (encoding) for VT320 terminal emulation.

Table B.13: VT320 Encoding

VT320 Keyboard	PC Character Sequence	VT320 Keyboard Byte Sequence
Escape Key (Esc)	Esc	0x1B
F1	F1	Esc O P
F2	F2	Esc O Q
F3	F3	Esc O R
F4	F4	Esc O S
F6	F6	Esc [1 7 ~
F7	F7	Esc [1 8 ~
F8	F8	Esc [1 9 ~
F9	F9	Esc [2 0 ~
F10	F10	Esc [2 1 ~
F11	F11	Esc [2 3 ~
F12	F12	Esc [2 4 ~
F13	Ctrl - F5	Esc [2 5 ~
F14	Ctrl - F6	Esc [2 6 ~
F15	Ctrl - F7	Esc [2 8 ~

VT320 Keyboard	PC Character Sequence	VT320 Keyboard Byte Sequence
F16	Ctrl - F8	Esc[29~
F17	Ctrl - F9	Esc[31~
F18	Ctrl - F10	Esc[32~
F19	Ctrl - F11	Esc[33~
F20	Ctrl - F12	Esc[34~
Insert	Insert	Esc[1~
Home	Home	Esc[2~
Delete	Delete	Hex 7 F
End	End	Esc[5~
Up Arrow	Up Arrow	Esc[A
Down Arrow	Down Arrow	Esc[B
Left Arrow	Left Arrow	Esc[D
Right Arrow	Right Arrow	Esc[C

Table B.14 lists the decoding for VT320 terminal emulation.

Table B.14: VT320 Decoding

VT320 Keyboard Function	VT320 Keyboard Byte Sequence
Index	Esc D
New Line	Esc E
Reverse Index	Esc M
Escape O	Esc O
Save cursor and attributes	Esc 7
Restore cursor and attributes	Esc 8

VT320 Keyboard Function	VT320 Keyboard Byte Sequence
Up Arrow	Esc[A
Down Arrow	Esc[B
Right Arrow	Esc[C
Left Arrow	Esc[D
Set cursor to home position	Esc[H
Set cursor to home position	Esc[f
Character Attributes	Esc[m
Erase from cursor to end of line	Esc[K
Erase from cursor to end of screen	Esc[J
Programmable LEDs	Esc[q
What are You?	Esc[c
Set Mode	Esc[?
Delete 1 Character	Esc[P
Insert 1 Line	Esc[L
Delete 1 Line	Esc[M
Up Arrow	Esc O A
Down Arrow	Esc O B
Right Arrow	Esc O C
Left Arrow	Esc O D
Fill Screen with Es	Esc # 8
Up Arrow amount specified by Pn	Esc[Pn A
Down Arrow amount specified by Pn	Esc[Pn B
Right Arrow amount specified by Pn	Esc[Pn C

VT320 Keyboard Function	VT320 Keyboard Byte Sequence
Left Down Arrow amount specified by Pn	Esc[Pn D
Erase parts of current line	Esc[Pn K
Erase parts of current screen	Esc[Pn J
Direct Cursor Addressing	Esc[Pn H
Direct Cursor Addressing	Esc[Pn f
Programmable LEDs	Esc[Pn q
Scrolling Region	Esc[Pn r
Clear tabs	Esc[Pn g
Device status report	Esc[Pn n
What are you?	Esc[Pn c
Sat Mode	Esc[Pn h
Delete Pn Characters	Esc[Pn P
Insert Pn Lines	Esc[Pn L
Delete Pn Lines	Esc[Pn M
Insert Character	Esc[Pn @
Erase Pn Characters	Esc[Pn X

Appendix C: Regaining Access to the Rack Power Manager Software

Access to a Rack Power Manager software system may be lost due to reasons such as:

- Being locked out by the Rack Power Manager software
- Deleting the last Rack Power Manager software administrator
- Forgetting the Rack Power Manager software administrator password

To regain access to a Rack Power Manager software system:

1. Contact Avocent Technical Support. You will be provided with the resetpassword.zip archive file.
2. Extract the resetpassword.zip archive file into the <RPM Installation Directory>\bin directory on the Rack Power Manager software hub server using a third party product.
3. From the Control Panel, select *Administrative Tools - Services* and stop the Avocent Rack Power Manager software service.
4. Open a terminal window, change directories to the <RPM Installation Directory>/bin directory and enter **resetpassword.bat**. A code successfully generated message will appear in the terminal window, along with a request code in the same format as the following:

341D3DAD-E71A15B1-66D77BBD-E655BB6C

NOTE: Request codes are valid for only four hours.

5. Contact Avocent Technical Support and provide the generated request code.
6. Avocent Technical Support will provide you with a reset code.
7. In a terminal window, enter **resetpassword.bat <reset code>**. A *Message reset performed successfully* message will appear in the terminal window, along with the Administrator username and password for the Rack Power Manager management software.
8. From the Control Panel, select *Administrative Tools - Services* and restart the Avocent Rack Power Manager software service.
9. You may now log into the Rack Power Manager management software.

