Avocent® Rack Power Manager

Installer/User Guide

Technical Support Site

If you encounter any installation or operational issues with your product, check the pertinent section of this manual to see if the issue can be resolved by following outlined procedures. Visit https://www.VertivCo.com/en-us/support/ for additional assistance.

TABLE OF CONTENTS

1 PRODUCT OVERVIEW

Avocent® Rack Power Manager software is a standalone web browser-based, centralized rack PDU management solution. It provides all centralized management capabilities related to rack PDU devices, which includes the ability to perform power control actions and run power consumption reports for outlets, PDUs, racks and so on. This document supports versions up to and including release 1.5. Service Pack 7 (SP7).

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

1.1 System Components

This rack PDU management solution consists of the Rack Power Manager management software, server and software client.

Rack Power Manager management software

The Rack Power Manager software resides on the Rack Power Manager hub server and provides a web gateway and services for managing rack PDUs.

Users can connect to the Rack Power Manager server from Rack Power Manager software clients and then use the Rack Power Manager Explorer Windows to communicate with the system.

Rack Power Manager hub and spoke servers

A single Rack Power Manager hub server (sometimes called a host or dedicated server), contains the Rack Power Manager management software. The hub server is responsible for maintaining the master copy of the Rack Power Manager database of configuration, as well as user, unit and system information. It also provides services for authentication, access control, logging events, monitoring and license management.

In addition to the hub server, one or more spoke (backup) servers can be configured to perform database replication of the hub server by distributing Rack Power Manager software functionality across multiple sites. Spoke servers are primarily used for redundancy of all PDU management and to improve scalability. The hub server acts as the coordinator for database replication between itself and any spoke servers in the Rack Power Manager software system. Power consumption data is not replicated to all spokes, however, when a report is created it gathers the data from the hub and all the spokes.

After the hub server and optional spoke servers are configured, you can create and configure the access levels for users within your network environment. You can 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 has web browser access to the Rack Power Manager management software installed on the Rack Power Manager server. The Rack Power Manager software client uses HTTPS (Hypertext Transfer Protocol with SSL encryption) for management functions, such as sending a request to the Rack Power Manager server, which then sends a command to the managed appliance or PDU. The managed appliance or PDU then performs the requested function.

1.1.1 Third party products

Third party products are not a part of the Rack Power Manager software and are provided by an external source. The following third party products are supported:

- 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.
- An 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.
- A third party Telnet viewer can be used for serial sessions instead of the Rack Power Manager software.

1.2 Supported Power Devices and Appliances

Avocent® and Vertiv™ models are supported when connected serially through an Avocent or Vertiv appliance or directly over the network. Liebert® and other models are supported only when connected directly through the network.

See the latest release notes for the details.

1.2.1 IPv4 and IPv6 network protocols

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

2 INSTALLATION

The Rack Power Manager software database is installed on the hub server. Rebooting the hub server is not required prior to using the Rack Power Manager software. After the Rack Power Manager software is installed and the hub server is configured, users can log in as a Rack Power Manager software client using a supported web browser. (Supported web browsers are provided in the latest release notes.) Next, the Rack Power Manager software can be installed and configured on the spoke servers. See Spoke Servers on page 52.

NOTE: A license key permits the operation of the Rack Power Manager software on the hub server and specifies the number of clients that can use the software. See Viewing and Adding Licenses on page 40.

Proceed to learn more about the following:

- Preparing for software installation
- Installing/uninstalling the software
- Configuring the software and upgrade considerations
- Changing your password
- Starting a client session
- Ending a Rack Power Manager software session
- Installing Java®

2.1 Minimum System Requirements

The following are the minimum system requirements for the Rack Power Manager software servers, operating systems and browsers.

2.1.1 Servers

The following are the server specifications:

- One or more 2+ GHz Multi-Core CPU
- 6+ GB RAM
- 250+ GB HDD
- 1 GBT/10 GB per second LAN

2.1.2 Operating systems

See the latest release notes for the details.

2.1.3 Browsers

See the latest release notes for the details.

NOTE: When using Firefox®, the Telnet viewer requires Java.

2.2 Before Installing and Configuring the Rack Power Manager Software

The managed appliance/PDU hardware is installed before the Rack Power Manager software is installed. For a hub server, retrieve the license key from Vertiv and provide a username and password to use for initial log in. For a spoke server, identify the associated hub server and provide the name/password of its Rack Power Manager software administrator.

2.3 Installing the Rack Power Manager Software

The Rack Power Manager software can be installed on a physical server or a virtual media server (VM) and the installation instructions described in this section apply to both scenarios. The Rack Power Manager management software can be installed by downloading the software from www.VertivCo.com.

To install the Rack Power Manager software from a DVD:

1. Log in to the hub server as **Administrator** or **root** and insert the Rack Power Manager software DVD.
2. In the menu of installation options, click *Install Rack Power Manager Software*.

   -or-

   For Microsoft® Windows®, if autorun is not enabled, enter **<drive:>\RPM\win32\setup.exe**, where <drive:> is the letter of your DVD drive. A dialog box indicates that the server meets the minimum requirements for installation.

   -or-

   For Linux®, issue the following command to mount the DVD volume: **mount <device> <mount point>**, where <device> and <mount point> are the DVD Linux device name and mount point directory name of your server, respectively. For example, to mount the first IDE cdrom on /media/cdrom, enter the **mount /dev/cdrom /media/cdrom** command.

To install the Rack Power Manager software from a downloaded file:

1. Using your web browser go to www.VertivCo.com and click the *Support* link.
2. On the Technical Support window, click the *Product Upgrades* link and select *RPM Software Upgrades*.
3. If desired, navigate to the required version to download the installer. The installer filename is setup.exe for Windows and install.bin for Linux.
4. Double-click the downloaded installation package (setup.exe).

   -or-

   For Linux, enter the **less /<mount point>/RPM/readme** command to access the readme file. For example, the **less /media/cdrom/Rack Power Manager/readme** command accesses the readme file on the /media/cdrom mount point.

5. If the current version of the Rack Power Manager software is already installed and the Installed Product Found: Same Version message appears, click *OK* to reinstall the software or click *Cancel*.
6. In the Introduction window, follow the on-screen instructions and for a new database installation, click *Next* to install a new PostgreSQL database. Then select a location to install the database, enter the port number and password and click *Install - Done*.

   -or-

   For an existing PostgreSQL database installation, click the Use Existing Database checkbox and click *Next*. Then enter the database IP address, username, password and listening port number and on the Installation Settings Confirmation window, click *Install - Done*.

2.4 After Installation

After the Rack Power Manager software is installed, you can configure the software using a web browser.

To begin configuration of the Rack Power Manager software:

NOTE: Normally, a Security Alert dialog box displays certificate information and a warning that the generator of the certificate is not trusted. This occurs because the Rack Power Manager server certificate created during server installation is a self-signed certificate.

From the Security Alert dialog box, you can choose to trust the certificate and import the certificate in to the Rack Power Manager software client web browser.

-or-

Obtain a server certificate from a Certificate Authority (CA) trusted by the web browser.

-or-

Click *X* (Cancel) in the top right corner to configure the Rack Power Manager software at a later time.

2.5 Configuring the Rack Power Manager Software

If this is your first Rack Power Manager server installation, the hub server should be installed before any spoke servers are added. See Understanding Certificates on page 33.

To configure the Rack Power Manager software:

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

   -or-

   If you quit after the Rack Power Manager software installation process by closing the window, from your desktop, click *Start - Programs - Vertiv - RPM 1.0 - RPM Software*.

2. In the Select RPM Server Role window, click *Hub* to assign the dedicated server as the hub server, click *Next* and go to step 3 to complete this procedure.

   -or-

   Click *Spoke* to assign the server as a spoke server, click *Next* and go to step 6 to complete this procedure.

3. Follow the on-screen instructions and click *Finish*.
4. From your web browser, in the Rack Power Manager User Login window, enter the username and password specified during configuration.
5. In the Type in Hub Server Address and Port window, enter the address of the hub server.

   -or-

   Enter the DNS name in the Address field and click *Next*.

6. In the Accept Rack Power Manager Server Certificate window, click *Next* to accept the certificate.
7. In the Type in Hub Administrator Credentials window, enter a valid username and password for a user with software administrator privileges on the hub server and click *Next*.
8. In the Completed Successful window, click *Finish*.

2.6 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), are automatically installed by the Rack Power Manager server host.

The Rack Power Manager software uses SSL encryption to ensure data integrity and privacy when sending data between the Rack Power Manager software host and the web browser on the client. 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 software administrator verifies the credentials of the user. Security alerts related to the certificates on the Rack Power Manager software host may appear. See Understanding Certificates on page 33.

2.6.1 Opening a client session

Before opening a client session, make sure you do the following:

- Enable cookies and JavaScript® on the web browser of the client.
- Configure the web browser. If you are using Internet Explorer®, see Internet Explorer® Considerations on page 30.

NOTE: If Rack Power Manager Software Client Certificate Authentication or Rack Power Manager Software Client Integrated Windows Authentication is being used, the user is not required to log in. See Understanding Certificates on page 33.

To open a client session:

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

   https://<servername>:<port number configured during installation>/RPM

   In this case, <servername> is the DNS name of the host system or the IP address.

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

   -or-

   If you are opening the session on the Rack Power Manager server, click *Start - Programs - Vertiv Rack Power Manager - RPM Software*.

NOTE: If the default options are selected during installation, the correct format is https://<servername>/RPM.

2. Accept all appearing security alerts as the client connects to the Rack Power Manager server.

NOTE: If an RSA SecurID® external authentication service is added to the Rack Power Manager software, see the following section.

3. On the Rack Power Manager Explorer User Login window, enter a valid username and password in the provided fields.

NOTE: Depending on the settings specified by the administrator, you may be required to change your password before being allowed to complete the log in process. See Adding User Accounts on page 140.

4. Click *Login* to open the applicable window, which depends on the rights assigned to the Rack Power Manager user that is logging in.

RSA SecurID® login

When an RSA SecurID® external authentication service is 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 and 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 is 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 can enter a PIN or allow the RSA server to generate it

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

2.7 Uninstalling the Rack Power Manager Software

The Rack Power Manager software can be uninstalled.

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

1. From the Start menu on your desktop, click *Settings - Control Panel*, and from the Control Panel, click *Add/Remove Programs*.
2. From the Add/Remove Programs dialog box, select *Rack Power Manager* and click *Change/Remove*.
3. From the Uninstall Rack Power Manager User Guide window, click *Uninstall*.

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

1. Open a terminal and navigate to the Uninstall directory under the RPM install folder. The default location is /usr/local/Vertiv/RackPowerManager/Uninstall.
2. Enter **./Uninstall_RackPowerManager** to uninstall the Rack Power Manager and follow the displayed instructions.

To close a Rack Power Manager software session:

From the Rack Power Manager software session in Internet Explorer®, click *LOGOUT* or the log out icon.

2.8 Java Installation

On non-Windows clients, Telnet requires Java version 1.7. Other versions may also work with a Telnet Applet.

On Windows clients, Java is required to run the Vertiv Telnet viewer. If the Win32 PuTTY Telnet viewer is selected in the profile of the user, 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. For more information, see Accessing the Unit Views windows on page 77.

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. See the Macintosh operating system documentation for more information.

To configure Java to find the JRE:

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

To install the JRE on a Windows client:

1. From the Rack Power Manager software, click the *Units* tab and in the Unit Views window, click a PDU.
2. In the Unit Overview window, click the *Appliance Session* link.
3. Download the JRE installer and close all browser windows.
4. Run the installer and restart the browser.
5. Click a PDU, and in the Unit Overview window, click the *Appliance Session* 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 the configuration of your system, 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. From the Rack Power Manager software, click the *Units* tab and in the Unit Views window, click a PDU.
2. In the Unit Overview window, click the *Appliance Session* link.
3. Download the JRE installer and close all browser windows.
4. Run the installer and restart the browser.
5. Click a PDU, and in the Unit Overview window, click the *Appliance Session* link.

3 TRANSITIONING

Plug-ins that support DSView™ management software version 3 or higher can be transitioned to the Rack Power Manager software as well.

3.1 Transitioning DSView™ 3 Software/Plug-ins to Rack Power Manager Software

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

NOTE: To safely upgrade to the Rack Power Manager software and to provide a roll-back path in case of upgrade failures, perform each of the following steps. If your DSView 3 software 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.

3.1.1 Replicating data

Perform a replication of all DSView 3 software spoke servers. Then, 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 - Tasks* tabs.
2. In the Tasks window, click the Database Replication task checkbox and click *Run Now*.

3.1.2 Backing up the DSView 3 software

With DSView 3 software administrator privileges, you can use the command line or the DSView™ software backup and restore utility to manually back up the DSView software hub and spoke servers. For hub servers on supported Windows operating systems, a command line is accessed from an MS-DOS window. The backup and restore system task is located in the DSView 3 software web user interface (UI) (see Task: Backing up the Rack Power Manager software database and system files on page 181). The backup is saved as a .zip file containing the files needed to restore the DSView software. Both backup methods include the database, firmware, plug-ins, appliance templates and system properties.

NOTE: Client sessions are temporarily disconnected during a manual backup and then automatically reconnected when the backup is complete.

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

1. From the Start menu on your desktop, click *Programs - Accessories - Command Prompt*.
2. At the prompt, change the directory to the directory where the DSView 3 software is installed (typically C:\Program Files\Avocent DSView 3\bin).
3. Enter **DSView BackupRestore** to display the DSView 3 Backup and Restore Utility dialog box.
4. Enter **DSViewBackupRestore -backup -archive "<archive name>" -passwd <password>** to back up the DSView 3 software hub server.

   Example: Enter **DSViewBackupRestore.exe -backup -archive "db.zip" -passwd test** in a command prompt window to create a backup named db.zip with the password test.

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

1. Access the command prompt on your system and change the directory to the directory where the DSView 3 software is installed (typically /usr/local/dsviewserver/bin).

2. Enter **DSViewBackupRestore.sh -backup -archive <archive name> -passwd <password> -overwrite** to back up the DSView™ 3 software hub server.

   Example, enter **DSViewBackupRestore.sh backup -archivedbasebackup.zip -passwdtest1** in a command prompt window to create a backup named dbasebackup.zip with the password test1.

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

1. From the Start menu on your desktop, click *Programs - Avocent DSView 3- Backup and Restore Utility*.
2. In the DSView 3 Backup/Restore Utility dialog box, click *Backup Database to a file*.
3. For the password-protected backup file, click *Enabled* and enter a password.
4. Click *Browse*, use the Save As dialog box to specify a directory and name for the backup file and click *Save*.
5. Click *Backup* to save the DSView 3 software system backup files and click *Close*.

3.1.3 Backing up the Rack Power Manager database

This task creates a folder containing a backup of the Rack Power Manager database. The default name for the backup folder is dsviewPluginBackup;<SYSTEM NAME>, but you can 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 - Tasks* tabs.
2. In the Tasks window, click *Add*.
3. In the Add Task Wizard, from the drop-down menu, select *Backup Power Manager database* and enter a name (1-64 characters) for the task.
4. Select a time to run the task and click *Next*.
5. In the Specify Power Manager Database Backup Properties window, enter the directory location for the created backup file, which can be a physical local drive on the DSView 3 server or a shared network location specified by a UNC (Universal Naming Convention) path.

NOTE: The directory name must be entered in case sensitive text if your operating system supports case sensitive filenames, and the Location field cannot be set to a mapped network drive.

6. If the specified directory location is a network path that requires logging in, enable the Login required to access shared drive location checkbox. Then enter the username and password and confirm the password of a user account that has read/write access to the network share location.
7. If you enabled the Login required to access shared drive location checkbox, append the date and time (in military time) to the end of the system backup folder by enabling 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 created folder is named dsviewBackup1001052204;<Machine Name>.

NOTE: 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 is overwritten when the new backup folder is created.

8. Click *Finish*, navigate to the etc folder of this backup folder and manually compress the etc folder into a zip file.

9. Use the etc zip folder in all subsequent steps that require the backup of a Power Management database.

3.1.4 Installing the Rack Power Manager software on the hub server

After backing up the Power Management database, install the hub server.

To install the Rack Power Manager software:

1. Download the latest version of the software to the server, run the installation file and click *Next*.
2. Accept the terms of the License Agreement and click *Next*.
3. In the Installation Settings window, click *Next*.
4. Choose the installation location for the Rack Power Manager software and click *Next*.
5. Review the default Rack Power Manager software TCP Port Settings tab, make any changes and click *Next*.
6. In the PostgreSQL Installation window, if the database exists, enable the Use Existing Database checkbox and click *Next*.

   -or-

   For a new instance, click *Next*.
7. For an existing PostgreSQL server, enter the IP address, port, username and password, then click *Next*.

   -or-

   For a new instance, enter the install folder, port and password, then click *Next*, and on the confirmation window, click *Install*.
8. In the Service Startup dialog box, click *OK* and *Done*.

NOTE: The license must be configured before beginning migration.

3.1.5 Using the migration utility to export data

The DSView™ software data migration utility, installed with the Rack Power Manager software, allows you to convert from the embedded DSView software or Power Management (PMP) database type to PostgreSQL data format.

NOTE: The license must be configured before beginning migration.

To export the DSView™ 3 software backup data in PostgreSQL format from a Windows operating system:

1. From the Windows server, click *Start - All Programs - Vertiv - RPM1.0 - DSViewDataMigrationUtility* to launch the migration utility.
2. From the Export tab drop-down menu, select the type of server from which you are exporting, *Hub* or *Spoke*.
3. From the drop-down menu, select the database type to be backed up, *DSView* software or Power Management database.

NOTE: If you have a DSView software backup and a Power Management database backup, run the utility for each database type.

4. In the Data Backup File Path field, enter the path or browse to the location of the DSView software backup or PMP database backup file.

NOTE: If using a PMP database backup file, this is the previously created zip file of the etc folder.

5. In the Migration File Path field, enter or browse to the location to save the exported file and click *Export*.

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

1. From the Linux server, navigate to the DSViewDataMigrationUtility folder.

NOTE: The path /usr/local/Vertiv/RackPowerManager/DSViewDataMigrationUtility is the default location.

2. From the command line, enter ./DataMig.sh to launch the migration utility.
3. Select option two to export the data.
4. From the Export tab drop-down menu, select the type of server from which you are exporting, *Hub* or *Spoke*.
5. From the drop-down menu, select the database type to be backed up, *DSView* software or Power Management database.

NOTE: If you have a DSView™ software backup and a Power Management database backup, run the utility for each database type.

6. Enter the location of the DSView software backup or PMP database backup file.

NOTE: If using a PMP database backup file, this is the previously created zip file of the etc folder.

7. Enter the location to save the migration file, verify the settings and enter Y to continue the export.

3.1.6 Using the migration utility to import data

The Rack Power Manager data migration utility migrates the exported data you get from the previous steps into the Rack Power Manager database.

NOTE: The license must be configured before beginning migration.

To import the DSView software or DSView + PMP software database from a Windows operating system:

1. From the Windows server, click *Start - All Programs - Vertiv - RPM1.0 - RPMDataMigrationUtility* to launch the migration utility and click *Next*.
2. Select *DSView3+PMP to RPM 1.0* and click *Next*.
3. Enter the server IP address of the Rack Power Manager software hub server.
4. Enter the listening port for your hub database server in the DB Server Port field.
5. Enter the database username and password and click *Next*.
6. In the DSView Hub Database field, enter or browse to the location that you saved the DSView 3 software export file.
7. In the PMP Database field, enter the path or browse to the location of the exported PMP database file and click *Next*.
8. Assign the data from the servers on your DSView software system to your Rack Power Manager system and click *Next*.
9. Confirm the server assignments and click *Next*.
10. If you have assigned data to the Rack Power Manager spoke server, after the prompt, enter the DB server port, username and password of the spoke DB servers and click *Next*.

11. Click *Finish*.

To import the PMP database from a Linux operating system:

1. From the Linux server, navigate to the RPMDataMigrationUtility folder.

NOTE: The default path is /usr/local/Vertiv/RackPowerManager/DSViewDataMigrationUtility.

2. From the command line, enter **./DBMigration.sh** to launch the migration utility and click *Next*.
3. Select *DSView3+PMP to RPM 1.0* and click *Next*.
4. Enter the IP address of the Rack Power Manager software hub server.
5. Enter the listening port for your hub database server in the DB Server Port field.
6. Enter the database username and password and click *Next*.
7. In the DSView™ Hub Database field, enter or browse to the location that you saved the DSView™ 3 software export file.
8. In the PMP Database field, enter the path or browse to the location of the exported PMP database file and click *Next*.
9. Assign the data from the servers on your DSView™ software system to your Rack Power Manager system and click *Next*.
10. Confirm the server assignments and click *Next*.
11. If you have assigned data to the Rack Power Manager spoke server, at the prompt, enter the database server port, username and password of the spoke server and click *Next*.
12. Click *Finish*.

3.1.7 Configuring the Rack Power Manager hub and spoke servers

After the hub and spoke servers are installed, you can configure them.

To configure the hub server:

1. From the hub server, select the following applicable method to stop the Rack Power Manager service:
   - For Windows, from your desktop Start icon, select *Control Panel - Administrative Tools - Services*, select *RPM Service* and click *Stop*.
   - For Linux, execute the **/etc/init.d/rpmserver stop** command from a terminal window.
2. Copy the backed up firmware, appliance templates and system properties to the corresponding folders on the hub server.
3. Restart the hub server.

To configure the spoke servers:

1. From the spoke server, stop the Rack Power Manager service.
2. Copy the backed up firmware, appliance templates and system properties to the corresponding folders on the spoke server.
3. Restart the spoke server.
4. Run data replication on each spoke server.

3.2 Transitioning DSView™ 4 or Higher Software to Rack Power Manager Software

Before transitioning from DSView software version 4 or higher to the Rack Power Manager software, ensure that you budget sufficient time to perform the procedure for the hub and all spoke servers

concurrently. This process includes replicating the DSView™ spoke servers, backing up the hub, extracting the PostgreSQL data file, installing the Rack Power Manager hub server and importing the data. After importing the data, you can proceed to configure the Rack Power Manager hub and spoke server.

3.2.1 Replicating data

When performing a replication of DSView™ software spoke servers, run the replication task twice to ensure the entire system has fully replicated and all spokes are in sync with the hub server.

To initiate an immediate replication on a spoke server:

1. From the spoke server, click the *System - Tasks* tabs.
2. In the Tasks window, click the Database Replication checkbox and click *Run Now*.

3.2.2 Backing up the DSView™ software

With DSView software administrator privileges, you can use the command line or the DSView software backup and restore utility to manually back up the DSView software hub and spoke servers. For hub servers on supported Windows operating systems, a command line is accessed from the MS-DOS window. The backup and restore system task is located in the DSView software web UI (see Task: Backing up the Rack Power Manager software database and system files on page 181). The backup is saved as a .zip file containing the files needed to restore the DSView software. Both backup methods include the database, firmware, plug-ins, appliance templates and system properties.

NOTE: Client sessions are temporarily disconnected during a manual backup and automatically reconnected when the backup is complete.

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

1. Access the command prompt on your system and change the directory to the directory where the DSView software is installed, which is typically /usr/local/dsviewserver/bin.
2. Enter **DSViewBackupRestore.sh -backup -archive <archive name> -passwd <password> -overwrite** to back up the DSView software hub server.

   Example: To create a backup named dbasebackup.zip with the password test1, in a command prompt window, enter **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 operating system:

1. From the Start menu on your desktop, click *Programs - Avocent DSView - Backup and Restore Utility*.
2. In the DSView Backup/Restore Utility dialog box, click *Backup Database to a file*.
3. Click *Enabled* and enter a password in the Password field to password-protect the backup file.
4. Click *Browse*, and in the Save As dialog box, specify a directory and name for the backup file and click *Save*.
5. Click *Backup* and *Close*.

3.2.3 Extracting the PostgreSQL data file

After the DSView software is backed up, you can extract the PostgreSQL data file.

To extract the PostgreSQL data file:

1. Decompress the previously generated backup file.
2. Navigate to the bin folder and copy the postgresbackup.tar file to another location.

NOTE: This file is used as input to import the data to the Rack Power Manager software.

3.2.4 Installing the Rack Power Manager software on the hub server

After extracting the PostgreSQL data file, you can install the software on the hub server.

To install the Rack Power Manager software:

1. Download the latest version of Rack Power Manager software to the server, run the installation file and click *Next*.
2. Accept the terms of the License Agreement and click *Next*.
3. In the Installation Settings window, click *Next*.
4. Choose the location for the Rack Power Manager software installation and click *Next*.
5. Review the default Rack Power Manager software TCP Port Settings tab, make any necessary changes and click *Next*.
6. If connecting to an existing PostgreSQL server, in the PostgreSQL Installation window, click the Use Existing Database checkbox and click *Next*. Then enter the IP address, port, username and password and click *Next*.

   -or-

   If installing a new instance, click *Next*, enter the install folder, port and password and click *Next*. Then in the confirmation window, click *Install*.

7. In the Service Startup dialog box, click *OK* and *Done*.

NOTE: The license must be configured before beginning migration.

3.2.5 Importing the data

After installing the software, you can import the data.

To import the DSView™ software database from a Windows operating system:

1. From the Start menu on your desktop, click *All Programs - Vertiv - RPM1.0 - RPMDataMigrationUtility* to launch the migration utility and click *Next*.
2. Select *DSView 4 to RPM 1.0* and click *Next*.
3. Enter the IP address of the Rack Power Manager software hub server.
4. Enter the listening port for your hub server in the DB Server Port field.
5. Enter the username and password.
6. In the DSView™ 4 DB field, browse or enter the location of the DSView 4 software database (the postgresbackup.tar file extracted from the DSView 4 software backup) and click *Next*.
7. Assign the servers for migration and click *Next*.
8. Confirm the server assignments, click *Next* and *Finish*.

To import the DSView software database from a Linux operating system:

1. From the Linux server, navigate to the RPMDataMigrationUtility folder.

NOTE: The default path is /usr/local/Vertiv/RackPowerManager/RPMDataMigrationUtility.

2. From the command line, enter **./DBMigration.sh** to launch the migration utility and click *Next*.
3. Select *DSView 4 to RPM 1.0* and click *Next*.
4. Enter the IP address of the Rack Power Manager hub server.
5. Enter the listening port for your hub server in the DB Server Port field.
6. Enter the username and password.
7. In the DSView™ 4 DB field, browse or enter the location of the DSView 4 software database (the postgresbackup.tar file extracted from the DSView 4 software backup) and click *Next*.
8. Assign the servers for migration and click *Next*.
9. Confirm the server assignments, click *Next* and *Finish*.

3.2.6 Configuring the Rack Power Manager hub and spoke servers

After the hub and spoke servers are installed you can configure them.

To configure the hub server:

1. From the hub server, stop the Rack Power Manager service.
2. Copy the backed up firmware, appliance templates and system properties to the corresponding folders on the hub server.
3. Restart the hub server.

To configure the spoke servers:

1. From the spoke server, stop the Rack Power Manager service.
2. Copy the backed up firmware, appliance templates and system properties to the corresponding folders on the spoke server.
3. Restart the spoke server.
4. Run data replication on each spoke server.

3.3 Integrating With DSView™ 3 or DSView™ 4.5 Software Data

With DSView 4.5 management software, you can integrate DSView 3 or DSView 4.5 software data, such as users, appliances/PDUs, infrastructure, access rights and so on, with your Rack Power Manager 1.5 software data. After integration, any changes to DSView™ or Rack Power Manager software are synchronized across both systems. If synchronization is not desired, see De-registering Servers on page 56.

NOTE: See www.VertivCo.com to download the necessary documents to complete the following procedures.

To integrate DSView 3 and Rack Power Manager 1.5 software data:

1. Follow the DSView 4.5 software installation steps in the DSView™ 4.5 Management Software User Guide.
2. Follow the steps in the DSView™ 4 Management Software Transition Technical Bulletin to transition the DSView 3 software to DSView 4.5 software.
3. Install the Rack Power Manager 1.5 software and configure the license.
4. As an Administrator, log in to the DSView 4.5 software.

5. Follow the instructions in the DSView 4.5 Management Software User Guide under Rack Power Manager Software Integration.

To integrate DSView 4.5 and Rack Power Manager 1.5 software data:

1. Install the Rack Power Manager 1.5 software and configure the license.
2. As an Administrator, log in to the DSView 4.5 software.
3. Follow the instructions in the DSView™ 4.5 Management Software User Guide under Rack Power Manager Software Integration.

This page intentionally left blank.

4 RACK POWER MANAGER EXPLORER WINDOWS

When a user is logged in and authenticated, the Rack Power Manager Explorer window allows you to view, access and manage units.

Figure 4.1 Example Rack Power Manager Explorer Window Areas

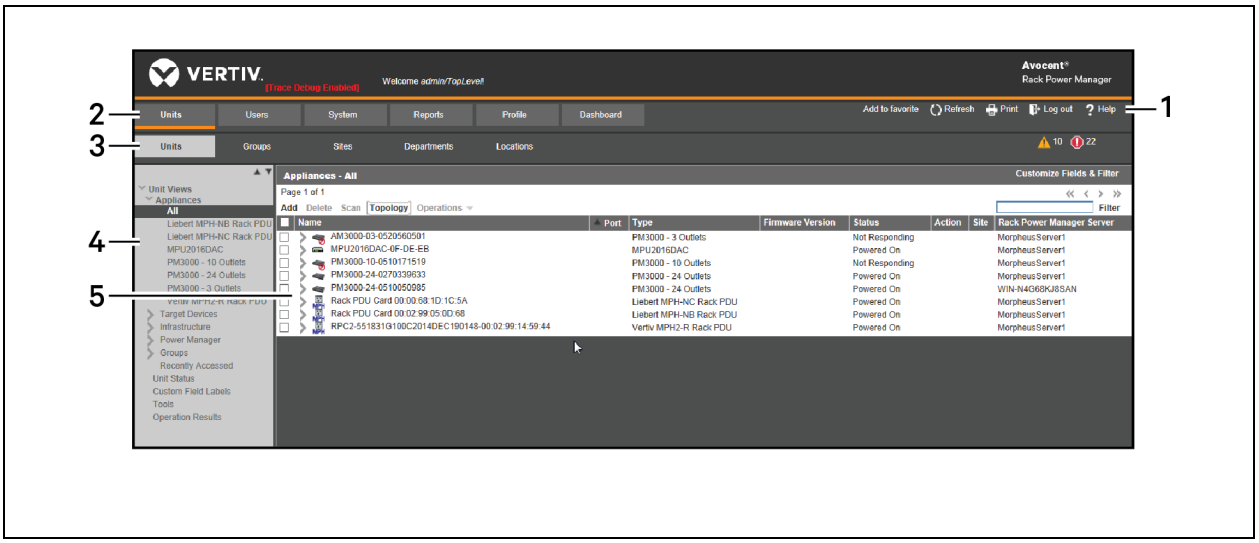


Table 4.1 Explorer Window Area Descriptions

ITEM	NAME	FUNCTION
1	Option bar	Used to bookmark and refresh software windows, print a screen, log out of a software session, access online help and display the name of the logged in user.
2	Tab bar - first tier	Used to display and manage units, user accounts, system settings, reports, session profiles and the dashboard.
3	Tab bar - second tier	Selections vary depending on the active tab in the first tier. Topics relevant to each selection display in the side bar.
4	Side bar	Used to select system information to be displayed or edited in the content area. The arrows at the top of the side bar allow you to expand or collapse the list of selections.
5	Content area	Displays the information selected using the tab bars and side bar.

4.1 Using the Tab Bars

The tab bar displays the Units, Users, System, Reports and Profile tabs. When clicked, these tabs display the dynamic tabs on a second tier of tabs. The contents of the second tier vary depending on the selected tab on the first tier. Together the tabs allow you to access windows from the side bar.

4.2 Using the Side Bar

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

Figure 4.2 Example Side Bar

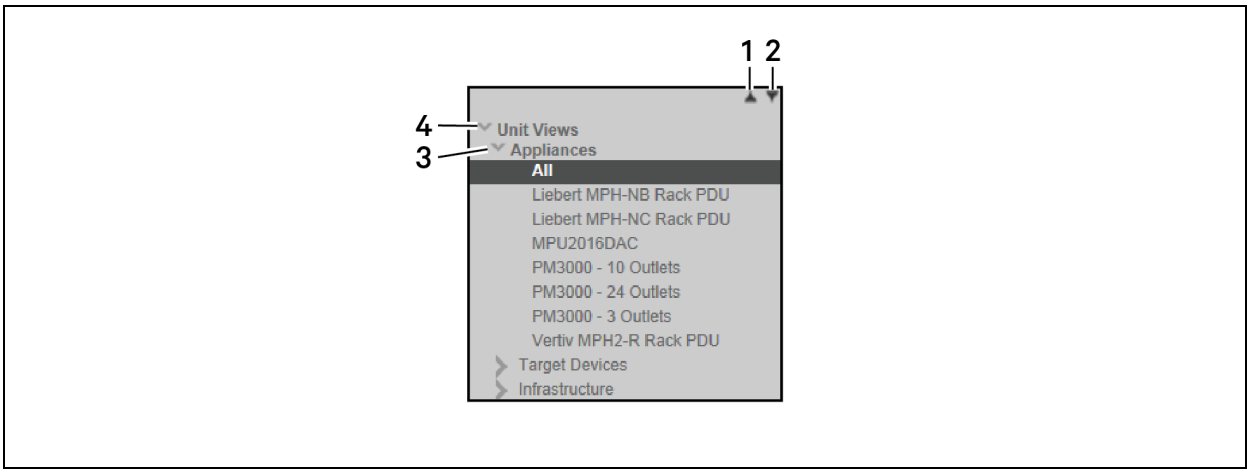


Table 4.2 Side Bar Descriptions

ITEM	NAME	FUNCTION
1	Expand all nodes	Expands all nodes and displays additional links
2	Collapse all nodes	Collapses all nodes and their links
3	Collapse a single node	Collapses an opened tree branch and its links
4	Expand a single node	Expands a closed tree branch and displays its links

Expanded nodes can be configured to collapse when another expanded node arrow is selected. See Changing user options on page 27.

4.3 Using Windows

Windows can be sorted, filtered, refreshed, customized and printed.

4.3.1 Sorting information

Rows in a window are listed alphabetically and can be changed to ascending or descending order by clicking the header of each column.

If you are using the topology feature in a Unit Views window, see Topology View on page 78 for sorting criteria.

4.3.2 Filtering information in a window

Some windows in the Rack Power Manager software allow you to filter information by providing a text string that is used to retrieve matching items. The following table lists the possible text strings for filtering.

When filtering, you can also use an asterisk (*) before and/or after text strings as a wildcard. For example, enter **emailserver*** and click *Filter* to display items with emailserver at the beginning, such as emailserver or emailserverbackup. Enter ***emailserver*** and click *Filter* to display items containing emailserver in any part of the name, such as emailserver, emailserverstore, tdemailserver or tdemailserver1.

Table 4.3 Filter Text Strings

ENTRY OPTIONS	RESULTS	EXAMPLE
<String>	Entering a string displays a filtered list of items that contain the word, that is, it finds matching strings that are followed by anything other than a letter or number.	Entering email displays 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, enter email server to 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.	Entering email server displays items that contain email server. The Rack Power Manager software provides a closing quotation mark if it is omitted.
<String1> AND <String2>	Using the AND logical operator displays the items that contain both strings.	Entering email and server displays 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.	Entering email or server to find any items that contain the string email or the string server.
(<String>)	Parentheses can be used to override the default order (left to right) of precedence during evaluation of a filter string.	Searching for email and server or service is the equivalent of ((email and server) or service), which may not be the intended search. You can 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.	Entering not email displays all items except those containing email; therefore, email, email server, email-server-1 and so on, do not display.

4.3.3 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 in the window
- The columns of information displayed in the Unit Views windows
- Which columns are included in a filter from a Unit Views window (available from the Customize Fields and Filter link only)

By clicking the *Customize* link, you can also display units that have been hidden in a Unit Views window.

NOTE: In a Unit Views window, which typically contains filtering options, the link is displayed as "Custom Fields and Filter." 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 vary depending in the window being customized. Although the items appearing in windows may vary, the items that do appear are modified identically regardless of the window in which you clicked the *Customize* link.

For more information, see the following:

- Showing and hiding units on page 77
- Unit group hierarchy on page 120
- Topology View on page 78

To customize a window using the Customize link:

1. From the applicable window, click *Customize*.
2. From the Unit Views Customization window, select the fields in the Available Fields list and click *Add* to add one or more fields to the window.

   -or-

Select one or more fields in the Fields to Show list and click the up or down arrow to reorder the list from left to right.

-or-

Select one or more fields in the Fields to Show list and click *Remove* to remove the fields from the window.

3. Use the arrow keys in the Items per Page field to select a number or enter a number of items (1-2000) to appear in the window.

NOTE: In Unit Views windows that have the topology view enabled, the number of items per window includes children, even if the display is collapsed and the children are not visible.

4. Click the Show hidden items checkbox, and under List Fields, select *Visibility* from the Available Fields column and click *Add* to show hidden items in a Unit Views window.
5. Click the Show group descendants checkbox to show group descendants in windows that display unit groups.
6. Click the Expand view automatically checkbox to expand a topology view automatically in a Unit Views window.
7. For Unit Views windows only, under Customize filter, select the fields from the Available Fields list and click *Add* to specify which fields are included in a filter.

   -or-

   Select the fields from the *Filter* and click *Remove* to remove fields from a filter.

8. Click *Set as Default* to set the Fields to Show and List Items as the default, and when prompted, confirm or cancel the setup.

NOTE: This button appears only if you are a Rack Power Manager software administrator.

9. After your modifications are complete, click *Save* and *Finish*, then verify the changes in the window.

4.3.4 Displaying windows

Multiple windows contain navigation buttons which can be used to go to lists or portions of lists.

Table 4.4 Explorer Navigation Buttons

BUTTON	NAME	FUNCTION
|<	First Page	Navigates to the beginning of a list
<<	Previous Page	Navigates to the previous page of a list
>>	Next Page	Navigates to the next page of a list
>|	Last Page	Navigates to the end of a list

4.3.5 Refreshing a window

A window can be refreshed at any time by clicking *Refresh* or the refresh icon in the option bar. The default automatically refreshes status information every 30 seconds; however, this interval can be changed or disabled. See Changing user options on page 27.

4.3.6 Printing a window

All windows contain a print icon and text on the option bar. When you print a window, all the information in the window is printed, regardless of currently being visible.

To print a window:

1. From the option bar, click *Print* or the print icon.
2. Specify options to use in the Print dialog box, then click *Print* and close.

4.4 Using Keyboard Commands

In addition to using a mouse, certain keyboard commands can 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

The following table lists the keyboard commands that are available when a calendar is enabled and displayed.

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	Increments 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 first day in the following month is selected.
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 last day in the previous month is selected.
Up Arrow	Decrements the weekday by one week. If the first weekday in the month is selected and the up arrow key is pressed, the same weekday in the previous month is selected.
Down Arrow	Increments the weekday by one week. If the last weekday in the month is selected and the down arrow key is pressed, the same weekday in the following month is selected.

This page intentionally left blank.

5 BASIC CONFIGURATION

Basic configurations include configuring the location to access your help information, global system properties, certificates and licensing, authentication, system configuration, profiles, assigning users to pre-defined user groups and Internet Explorer considerations.

5.1 Rack Power Manager Help

The Rack Power Manager help is hosted on the Vertiv 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 Vertiv™ web site.

5.1.1 Configuring the Rack Power Manager help location

Each Rack Power Manager hub and spoke server accesses the help information independently. Rack Power Manager administrators can specify the location from which the help is accessed at any time.

To configure the Rack Power Manager help location:

1. Click the *System - RPM Server* tabs.
2. In the side bar, click *Properties - Help Configuration*.
3. Select *View help from Vertiv web site (requires internet connection)* to access the latest help for your Rack Power Manager software version from the Vertiv web site.

   -or-

   Select *View help from this RPM server help location* to access the downloaded help from your local server. Then complete the following procedure Installing the Rack Power Manager help onto a local server on page 25.

NOTE: The View help from this RPM server help location radio button is enabled only after you download the help by clicking the *Download Latest Help* button.

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 Vertiv 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.

5.1.2 Installing the Rack Power Manager help onto a local server

You can automatically download the help information from the Vertiv web site using the Rack Power Manager software, or you can visit www.VertivCo.com to browse for the appropriate version and save a .zip file of the help to local media. The Rack Power Manager Help Download Wizard guides you through the process.

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

1. Click the *System - RPM Server* tabs.
2. In the side bar, click *Properties - Help Configuration*.
3. Click the *Download Latest Help* button.

4. Select *From the Vertiv web site* to download the latest help for your Rack Power Manager software version from the Vertiv™ web site.

   -or-

   Select *From a local device* to retrieve the help from local media and specify the location by clicking *Browse* or entering the path in the field.

5. Click *Next*, and in the Completed Successful window, click *Finish*.

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

5.2 Global System Properties

Global system properties affect all Rack Power Manager servers in the system. When global system properties are changed on a Rack Power Manager server, the next replication operation applies those changes to all other Rack Power Manager servers in the system.

For more information, see the following:

- Replication on page 55
- Specifying a user certificate on page 28
- Legal Notice on page 26
- Power Settings on page 26
- Automatic Inheritance for Group Memberships and Properties on page 90

5.3 Legal Notice

Administrators can 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 55.

To enable or disable and configure the legal notice:

1. Click the *System - Global Properties* tabs.
2. In the side bar, click *Legal Notice*, and in the RPM System Logon Legal Notice window, click the Enable Legal Notice checkbox.
3. Enter the caption using up to 80 characters (required).
4. Enter the text using up to 512 characters and carriage returns to separate lines (required).
5. Click *Save*.

To disable the legal notice:

Uncheck the Enable Legal Notice checkbox and click *Save*.

5.4 Power Settings

The properties for the global power settings can be configured to specify how long the Rack Power Manager server waits to receive power operations and power cycle times from a unit. The preset values are 60 seconds.

To configure power settings:

1. Click the *System - Global Properties* tabs.
2. In the side bar, click *Power Settings*.
3. In the Power Settings Properties window, enter information or click the arrows to specify the maximum time-out for power operations and the maximum power cycle wait time for the Rack Power Manager server.
4. Click *Save*.

5.5 Profiles

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

- Changing user options
- Changing a password
- Using a serial session application
- Specifying a user certificate
- Specifying a user SSH key

5.5.1 Changing user options

Various options are available for users, such as enabling/disabling functions for the navigation tree, enabling/disabling prompts and setting the refresh rate. The default automatically refreshes windows every 30 seconds. If you select *Never*, windows are only refreshed when you click the *Refresh* icon or text in the option bar.

For more information, see Using the Side Bar on page 19.

To change user options:

1. Click the *Profile* tab, and in the Options window under Navigation Tree Behavior, select *Automatically collapse navigation tree nodes* to collapse a currently expanded tree node when you select another tree node.

   -or-

   Select *Preserve navigation tree state* to keep a currently expanded tree node expanded when you select another tree node.

   -or-

   Select *Automatically fully expand navigation tree nodes* to expand all tree nodes (equivalent to clicking the *Expand All Nodes* arrow in the side bar).

2. If you do not want to be prompted to save modified information when you leave a window, click *Skip prompt when leaving pages with unsaved changes*.
3. Under View Options, from the drop-down menu, select a refresh rate or *Never*.
4. Click *Save*.

5.5.2 Changing your password

When the Rack Power Manager software internal authentication service is used, administrators can configure user account passwords to be changed by the users. Users can then change their personal

password from the Profile - Preferences - Change Password window. See User account restrictions and expiration settings on page 144.

The default requires passwords to contain at least three characters and never expire. A different minimum character length and an expiration date can be configured. See Rack Power Manager software internal authentication service on page 58.

To change your password:

1. Click the *Profile* - *Preferences* tabs.
2. In the side bar, click *Change Password*.
3. In the Change Password window, enter your old password.
4. Enter and confirm your new password and click *Save*.

5.5.3 Choosing the serial session application

The following applications can be used for serial sessions to rack PDUs:

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

- Win32 PuTTY Telnet/SSH Application
- Avocent Session Viewer
- 3rd Party Application

If you select the *3rd Party Application* option for your session, you can specify the path and executable name (up to 256 characters) and any of the following command line arguments (up to 128 characters). When the serial session is launched, the actual values are substituted as follows:

- %ADDRESS% - The IP address is substituted.
- %PORT% - The port number is substituted.
- %TNAME% - The target name is substituted

NOTE: Confirmation is required when launching the first session for third party Telnet applications.

To specify the serial session application:

1. Click the *Profile* tab, and in the side bar, click *Applications*.
2. Under Serial Sessions, click the checkbox for the application you want to use.
3. If you check *3rd Party Application*, in the Serial Application field, enter the path and executable name of the application, and in the Command Line Arguments field, specify the parameters.

NOTE: If the third party application does not automatically launch a command window, click the Launch in Command Window checkbox.

4. Click *Save*.

5.5.4 Specifying a user certificate

This property can be changed only by internal authentication users. If the administrator has allowed it, a user can specify a certificate. The user certificate (used when logging in) must meet the policy requirements.

As an alternative, the administrator can specify the certificate in the user account properties.

For more information, see the following:

- Rack Power Manager software internal authentication service on page 58
- System certificate policy and trust store on page 34
- User certificates on page 143

To enable user settable certificates:

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

1. Click the *System - Global Properties* tabs, and in the side bar, click *User Credentials*.
2. Click the Allow user to set own Certificate checkbox and click *Save*.

To specify a user certificate:

NOTE: A user must be granted access by a Rack Power Manager software administrator to perform this procedure.

NOTE: If the third party application does not automatically launch a command window, click the Launch in Command Window checkbox.

1. Click the *Profile* tab and review the automatically selected preferences.
2. In the side bar, click *Credentials* and click *Certificate*.
3. Enter the path and name of the certificate or browse to the certificate location.
4. Click *Save* and verify the Certificate window is updated.

5.5.5 Specifying an SSH key

With permission from the administrator, a user can specify an SSH key. As an alternative, the administrator can specify the SSH key in the user account properties. See User SSH key on page 143.

To enable user settable SSH keys:

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

1. Click the *System - Global Properties* tabs.
2. In the side bar, click *User Credentials*.
3. Click the Allow user to set own SSH Key checkbox and click *Save*.

To specify an SSH key:

1. Click the *Profile* tab and review the automatically selected preferences.
2. In the side bar, click *Credentials* and select *SSH Key*.
3. Enter the name (1-256 characters) or browse to the file containing the public SSH key generated by a third party key generator.
4. Click *Save* and in the window, verify the updated SSH Key to be uploaded to the Rack Power Manager server for use in authenticating the user.

5.5.6 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 can retrieve these credentials to log in to connected units.

To enable user credential caching:

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

1. Click the *System - Global Properties* tabs, and in the side bar, click *User Credential Properties*.
2. Click the Enable credential caching checkbox and click *Save*.

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

5.6 Pre-defined User Groups

When a user account is added to the Rack Power Manager software system, the user can be assigned to any of the following pre-defined user groups:

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

The following table lists the allowed operations for the pre-defined user groups.

Table 5.1 Pre-defined User Group Allowed Operations

OPERATION	PRE-DEFINED USER GROUP				
	RACK POWER MANAGER 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 pre-defined user groups, the Rack Power Manager software supports user-defined user groups. See Grouping Units on page 115.

5.7 Internet Explorer® Considerations

When using the Rack Power Manager software with the Internet Explorer® web browser, consider the following:

- SSL certificates are used for secure authentication between the Rack Power Manager software client and Rack Power Manager software hub server. See Understanding Certificates on page 33.
- ActiveX controls are used to display Telnet application and serial sessions.
- Security Zones are used to control the actions that are performed within Internet Explorer®, for example, the operation of JavaScript is dependent on security zone settings.
- Advanced Internet options is used for miscellaneous settings that enhance the use of the Rack Power Manager software.

5.7.1 Managing ActiveX® controls

The Rack Power Manager software uses ActiveX controls to provide interactive content for viewers. The functionality of the ActiveX controls is determined by the settings for the security zone being used by the software. See Java Installation on page 7 and the following section.

Users can be prevented from installing software on their servers when Windows domain administrators "push" an MSI using a group policy. This operation silently installs the Avocent session viewers for Internet Explorer without requiring the user to install the software. 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. Click the *Units* tab, and in the Appliances - All window with populated target devices, click the link in the Action field or select an alternate action, if available.
2. If desired, access a Unit Overview window for a target device and click the icon or link for the session type.
3. If this is the first time the ActiveX control is requested by the Rack Power Manager software, in the Security Warning dialog box, select *Always trust content from Vertiv .*
4. Click *Yes* to download the ActiveX control and start a serial session 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. Click the *Units* tab, and in the Appliances - All window with populated target devices, click the link in the Action field or select an alternate action, if available.
2. If desired, access a Unit Overview window for a target device and click the icon or link for the session type.
3. If this is the first time the ActiveX control is requested by the Rack Power Manager software, in the Avocent session viewer, click in the top yellow bar and in the pop-up menu, click *Install*.
4. In the Security Warning dialog box, click *Install* to install the ActiveX control.

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

The default setting ensures the Rack Power Manager software operates correctly in the Internet, Local Intranet and Trusted Sites security zones when accessing a hub server. The following security zones are available for Internet Explorer web sites:

- 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, such as https://sun-e2-callisto
- Internet - All other web sites, including those accessed using standard dot notation, such as https://10.0.0.1

NOTE: When Rack Power Manager software is installed on a hub server running Windows 2003, it does not operate correctly in the Internet security zone.

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

1. From Internet Explorer®, select *Control Panel - Internet Options* and specify settings for the Local intranet and Internet security zones.
2. Configure a Rack Power Manager software client to access a hub server using a host name (for example, https://avocent), to use the Local intranet security zone.

   -or-

   Configure a client to access a hub server using a web address with periods (for example, https://www.VertivCo.com), to use the Internet security zone.

   -or-

   Add the hub server to the Trusted Sites list to ensure the client always connects 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. From Internet Explorer, select *Tools - Internet Options*.
2. In the Internet Options dialog box, click the *Security* tab.
3. Select the security zone to be displayed and click *Custom Level*.
4. In the Security Settings dialog box, verify the Active Scripting setting is set to Enabled and ensure the following security settings are set to Enabled or Prompt:
   - Download Signed ActiveX Controls
   - Run ActiveX Controls and Plug-Ins
   - Launching Programs and Files in an IFRAME
5. Click *OK* to save the settings and close the Security Settings dialog box.
6. 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 the required settings (indicated previously) are specified for the Rack Power Manager software.

1. From Internet Explorer, select *Tools - Internet Options*.
2. In the Internet Options dialog box, click the *Security* tab.
3. Click *Trusted Sites - Sites*.
4. In the Trusted Sites dialog box, enter the web site address for the Rack Power Manager software hub server.
5. Click *Add* and verify the web site address appears in the web sites list box.
6. Make sure *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.

5.7.3 Advanced Internet options

Internet Explorer® contains advanced settings to enhance the use of Rack Power Manager software. Changing these settings is recommended for optimum results.

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

1. From Internet Explorer, select *Tools - Internet Options*.
2. In the Internet Options dialog box, click the *Advanced* tab.
3. Select the following applicable 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 36.
5. Uncheck the following applicable 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.

5.8 Understanding Certificates

The Rack Power Manager software system uses certificates to provide secure transactions between components and to uniquely identify components in the system. Certificates can be used for a system, server, client or managed appliance.

System certificate

The Rack Power Manager software system generates and manages a system certificate. The system certificate can be exported to a local directory so the public key of the certificate can be used to validate the signature of data log files.

To view or export the system certificate:

1. Click the *System - Global Properties* tabs.
2. In the side bar, click *X.509 Certificates - System Certificate*.
3. In the System Certificate window, click *Export Certificate* to export the system certificate in PEM format to a local director.
4. In the pop-up window, confirm or cancel the export operation.

NOTE: The content of this window is browser-dependent, but usually prompts you to confirm the operation.

Server certificates

A Rack Power Manager server certificate is used to identify servers and secure transactions as follows:

- 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 is displayed if there are server certificate issues. See Server certificates on page 44 for information about certificate updates and alerts.

Client certificates

A Client (or user) certificate is used to authenticate a user when logging in to the Rack Power Manager software. Prior to logging in, an administrator must configure the internal authentication service policies and the user account in the Rack Power Manager software and then enable certificate authentication. After authentication is enabled, the Rack Power Manager server prompts the client web browser to send its user certificates.

If the system certificate policies are enabled, logging in must meet the policy requirements and the certificate must be loaded in to the client web browser. Requirements include specifying the certificate location in the user account. The Rack Power Manager software administrator can, as an alternate method, enable user-settable certificates and then specify the certificate location for the user.

For more information, see the following:

- Adding User Accounts on page 140
- Client session information on page 48
- User certificates on page 143
- Specifying a user certificate on page 28

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 83.

5.8.1 System certificate policy and trust store

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

Table 5.2 System Certificate Policy

FEATURE	VALUE WHEN ENABLED
Chain Building	
Authority Information Access (AIA)	Permits the Rack Power Manager software to use the AIA certificate extension to locate the issuer of a certificate.
Maximum chain length	Maximum allowable number of certificates (1-16) including both the leaf certificate and trusted certificates.
Chain Validation	
Partial chains	Allows partial chains. If disabled, partial chains are considered invalid, even if the chain contains a trusted certificate.
Usage flags	Each certificate must 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	Each certificate in the chain dictates that the current date and time on the server must be within the window.
Verify signatures	Signatures within the certificate chain are checked for validity.
Certificate Revocation Lists (CRL)	
CRL checks	If CRLs are available, they are checked to determine the revocation status of a certificate.
Distribution points	CRLs can be located using the distribution point certificate extension.
Reject on error	If a CRL is specified (either in the certificate or the Rack Power Manager trust store) and it cannot be read or is invalid, the Rack Power Manager software rejects the certificate chain.
Secure Sockets Layer (SSL)	
Name verification	Outbound SSL connections verify server names.
Subject alternative names	Server names can 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.

To configure certificate policy settings:

1. Click the *System - Global Properties* tabs.
2. In the side bar, click *X.509 Certificates*.
3. In the System Certificate Policy window, click checkboxes or select values for each setting and click *Save*.

To display and manage the trust store:

1. Click the *System - Global Properties* tabs.
2. In the side bar, click *X.509 Certificates - Trust Store*.

NOTE: The System Trust Store window opens with a list of all trusted certificate authorities known to the Rack Power Manager software. (The default list contains the standard CAs from Java.)

3. Click a certificate to open the System Trust Store Entry window and change the location where the CRL can be obtained for that CA, then click *Save* and *Close*.

   -or-

   Click one or more checkboxes of the certificates, then click *Delete* and at the prompt, confirm or cancel the deletion.

4. Click *Add* to add a certificate.

5. From the New System Trust Store Entry window, in the Certificate File field, enter the name of the file (binary or Base64 encoded) containing the X.509 certificate to upload to the trust store.
6. In the CRL Location field, enter the location of the CRL (http:// or ldap://) for the uploaded certificate (up to 256 characters) and click *Add*.

5.9 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. The default setting for this feature allows Single Sign-On (SSO) and is disabled. 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 Vertiv 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.

A Rack Power Manager software administrator must first enable Integrated Windows Authentication to use it. See Client session information on page 48.

5.10 Firewalls

In a typical network configuration, as shown in the following figure, the Rack Power Manager software client is located outside 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 Vertiv 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, 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 can pass between the zones using TCP/IP ports 22, 3211, 2068, 8192 and 3871. You must also configure the User Datagram Protocol (UDP) port 3211 to 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

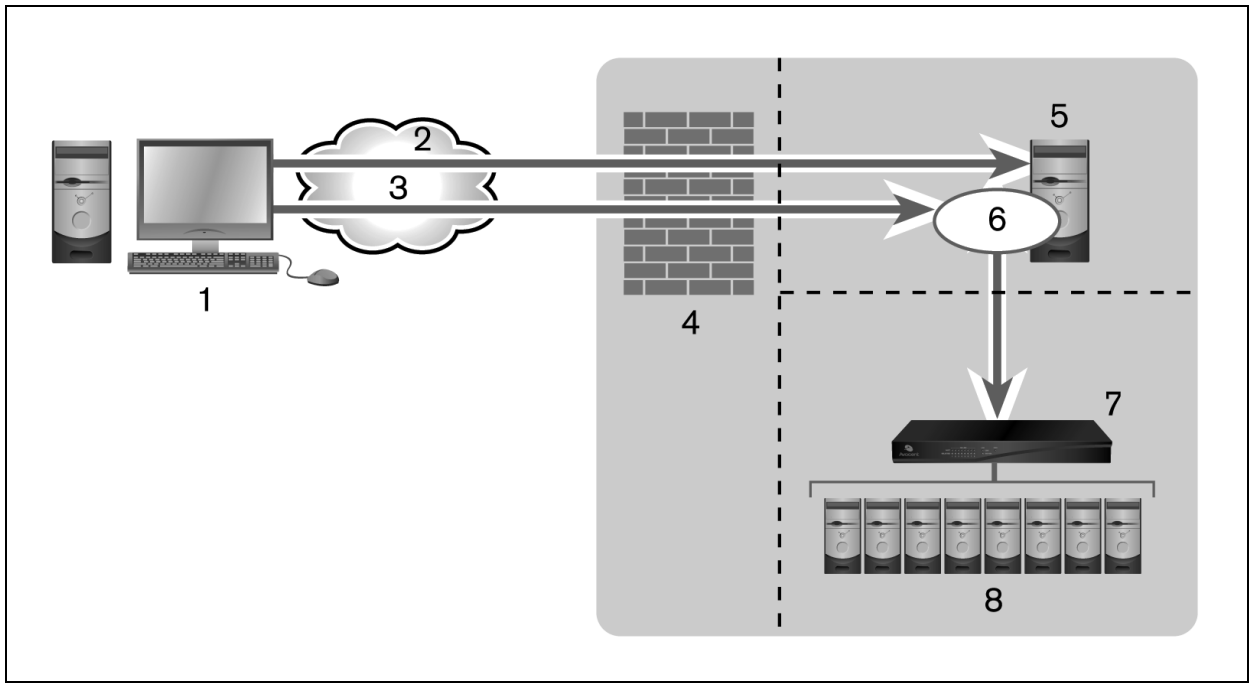


Table 5.3 Typical Software System Firewall Configuration Descriptions

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

5.11 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 increases WAN/VPN traffic but provides 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 the following figure could use NAT if Site A and Site B are separate companies that merged, but have not resolved their IP addresses. See the following section.

Figure 5.2 Rack Power Manager Software System on a VPN

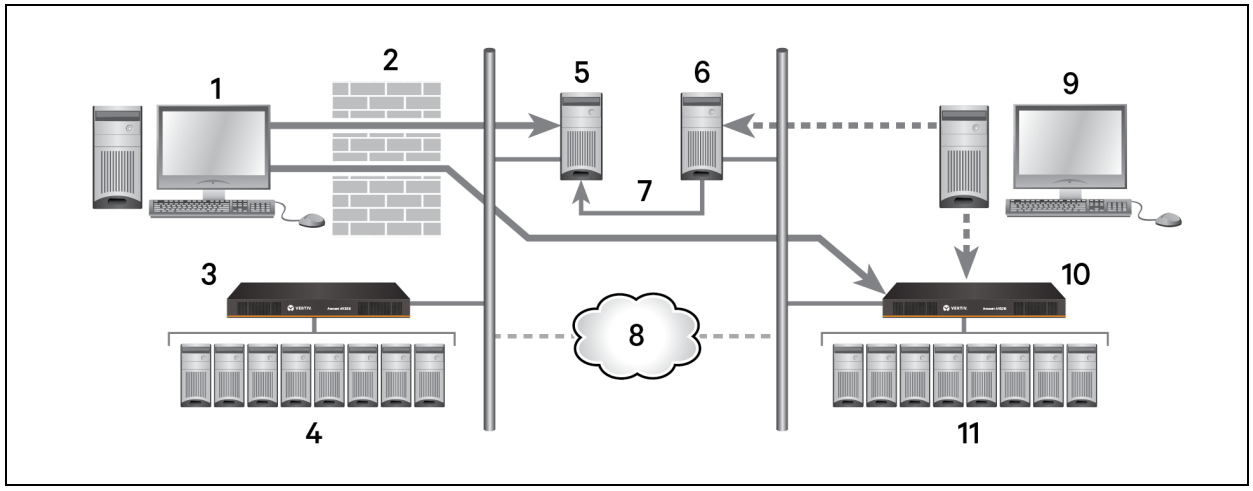


Table 5.4 Typical Software System Firewall Configuration Descriptions

ITEM	DESCRIPTION	ITEM	DESCRIPTION
1	Rack Power Manager Software Client	7	Replication
2	Firewall	8	VPN
3	Site A	9	Rack Power Manager Software Client
4	Target Devices	10	Site B
5	Hub Server	11	Target Devices
6	Spoke Server		

5.12 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 the following figure, which then connects to the corporate network using a VPN.

Figure 5.3 Single NAT Configuration (Client Only)

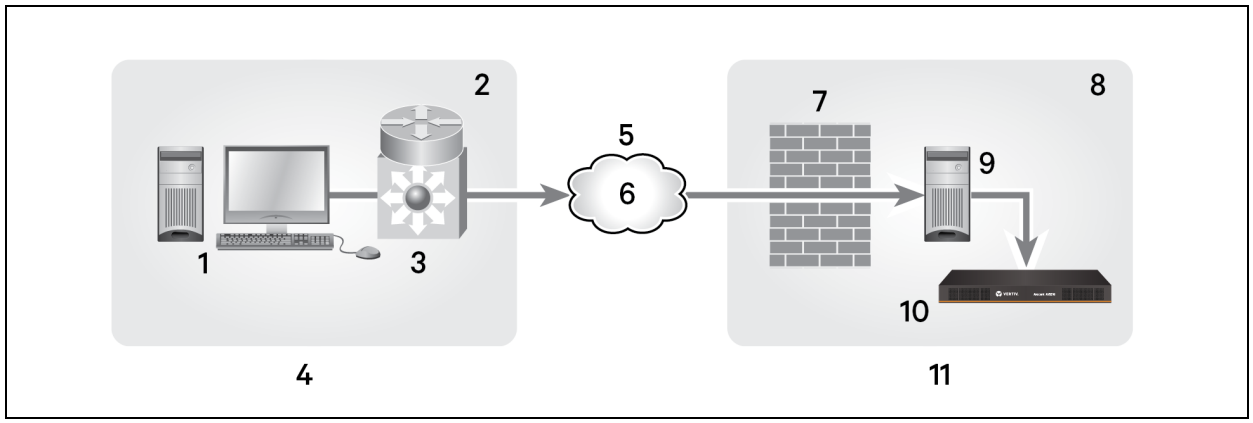


Table 5.5 Single NAT Configuration (Client Only) Descriptions

ITEM	DESCRIPTION	ITEM	DESCRIPTION
1	Rack Power Manager Software Client	7	Firewall
2	Private	8	Private
3	NAT Device	9	Rack Power Manager Server
4	Client	10	Managed Appliance
5	Public	11	Corporate
6	VPN		

In another scenario, shown in the following figure, the corporate site also uses a NAT device to save IP addresses (double-NAT). Because 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)

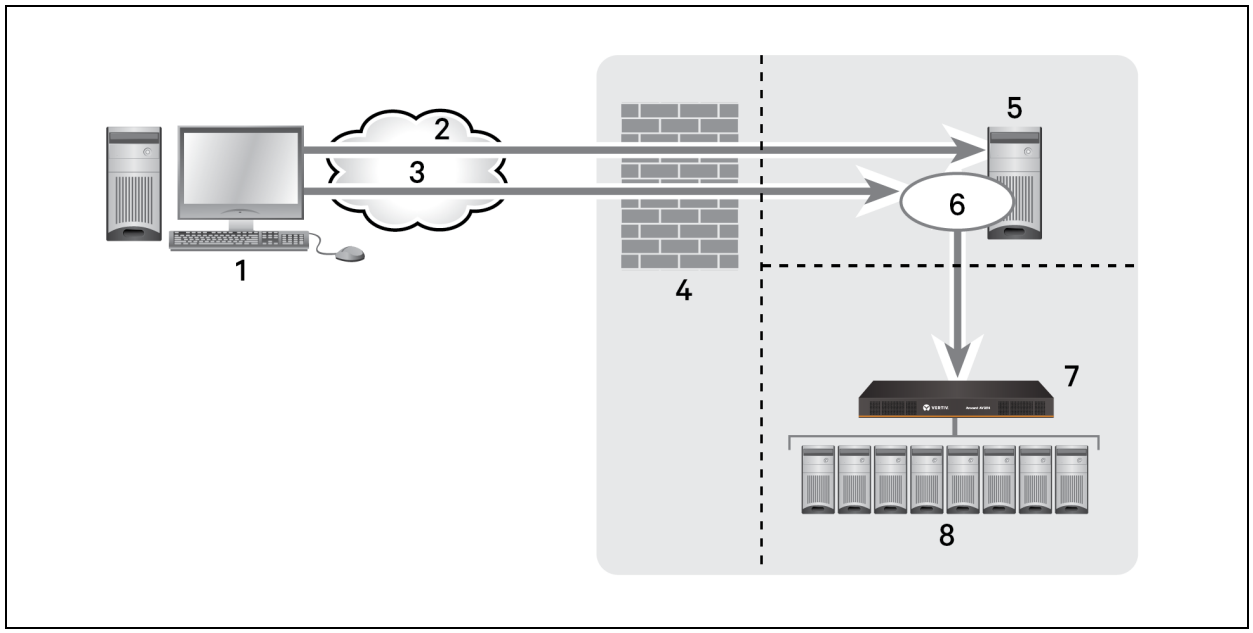


Table 5.6 Double-NAT Configuration (Client and Corporate) Descriptions

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 cannot be connected between the Rack Power Manager server and managed appliances.

5.13 Viewing and Adding Licenses

License keys permit the operation of the Rack Power Manager software on the hub server and specify the number of managed devices that can be controlled by the software. They also specify how many spoke servers are allowed in a system.

If a managed device is available through multiple connection methods, the managed device may require only one license if the connections are merged into a single connection in the Rack Power Manager software.

Licenses may also be required to enable additional features. See the following table for more information.

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	Total number of client server licenses 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.
Auditor Appliances	Licensed	Total number of auditor appliances that are 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 (enabled or disabled). 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.

The License Key window lists each installed license key with one of the following descriptions:

- 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

If desired, a demonstration (demo) license key is available for a trial period. When the trial period ends, the license key can 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 must be re-entered after the new license keys are installed.

To display license information:

1. Click the *System - Licenses* tabs.
2. In the side bar, click *Summary*.

To display license keys:

1. Click the *System - Licenses* tabs.
2. In the side bar, click *License Keys*.

To add a new license key:

1. Click the *System - Licenses* tabs.

2. In the side bar, click *License Keys*.
3. In the License Keys window, click *Add*.
4. In the Add License Key window, enter a valid new add-on license key in the License Key field.
5. Click *Save,* and in the License Keys window, verify the new row and license key.

5.14 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 - Global Properties* tabs.
2. In the side bar, click *System Information*.

6 RACK POWER MANAGER SERVERS

Managing Rack Power Manager servers includes configuring properties for identification and location on the network, certificate and proxy server protection, trap destinations and events, client sessions, modem sessions, email, unit polling status, spoke server management and data logging. In addition, you can back up and restore servers manually or automatically and configure hub and spoke servers for replication.

6.1 Server Properties

The following table lists the server properties of the Rack Power Manager.

Table 6.1 Server Properties

PROPERTY	DESCRIPTION
Identity	Name of the Rack Power Manager server and the role of the server (hub or spoke).
Network	IP address (*) and port used by clients to access the server using the HTTPS (SSL) protocol. The port number for the HTTPS connection can be changed. 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, on the Linux system in the /etc/hosts file, add a 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
Certificate	Rack Power Manager server certificate presented to Rack Power Manager software client web browsers.
Proxy Server	When the Avocent proxy server is used, Rack Power Manager software client serial session requests are sent through the Rack Power Manager server rather than directly to the serial console appliance. This prevents exposure of the internal address of the managed appliance.
Trap Destinations	Rack Power Manager server polls serial console appliances to determine if they are responding.
Rack Power Manager Client Sessions	Session settings for inactivity time-out, authentication policy, Single Sign-On (SSO) or restrictions to use specific IP addresses to start the sessions; also displays the number of client sessions currently in use.
Rack Power Manager Modem Session	Dial-up session settings, 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 are concurrently polled.
Spoke Servers	Enables you to manage the spoke servers in your system.

To display server properties:

From the System tab, *Rack Power Manager Server* is automatically selected in the top bar and *Identity* is automatically selected in the side bar. In the Rack Power Manager Server Identity Properties window, verify the name of the Rack Power Manager software server.

To change server network properties:

1. Click the *System* tab, and in the side bar, click *Network*.
2. In the RPM Server Network Properties window, in the HTTPS Port field, enter a new Rack Power Manager server port number and click *Save*.

NOTE: 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 entered in the Address field of the web browser to access the Rack Power Manager software.**

NOTE: 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.

3. After the confirmation dialog box and web browser error message appear (a normal occurrence), enter the URL with the new port number to reestablish the connection to the Rack Power Manager hub server/software.

NOTE: For example, if you changed the port number to 334 for a hub server with an IP address of 10.0.0.1, enter https://10.0.0.1:334/Rack Power Manager **to access the Rack Power Manager management software.**

4. Confirm or cancel the change.

6.1.1 Server certificates

Server certificates are managed by the Rack Power Manager software administrators. See Understanding Certificates on page 33 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 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 communicating server. 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 the self-signed certificate, a Rack Power Manager software administrator can create a Certificate Signing Request (CSR) to submit to a trusted third party Certificate Authority (CA) for signature. The administrator can then replace the generated certificate with the new one. If the generated certificate is not replaced, the web browser prompts a user to trust or not trust the generated certificate when a Rack Power Manager software client session is started.

The following tests/questions are processed 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 appears if the answer to any of these questions is No. To prevent the Security Alert dialog box from appearing when you connect to a 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 is made with the Rack Power Manager software hub server and the Rack Power Manager software log in window is displayed, but the Security Alert dialog box continues to appear each time you connect to the hub server.
- If you click *No*, a connection is not made with the Rack Power Manager software hub server.

- If you click *View Certificate*, you can install the certificate.

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

1. From the Rack Power Manager software client, open a client session.

NOTE: For more information about client sessions, see Opening a client session on page 6.

2. In the Security Alert dialog box, click *View Certificate*.
3. In the Certificate dialog box, click *Install Certificate*.
4. After the certificate is installed, verify the time configuration on the Rack Power Manager software client is within the Valid from...to dates and the Issued to/Issued by fields match.

NOTE: 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 warning "The security certificate date is invalid." appears in the Security Alert dialog box.

For more information, see the Internet Explorer documentation.

Serial session security alerts

The viewer used during a serial session is a Java-based applet. The following certificate tests are performed by Java when the Rack Power Manager software connects to a serial device:

- Verify the serial device trusts the certificate issuer
- Verify the certificate has not expired
- Verify the name on the serial device certificate matches the name of the Rack Power Manager software hub server certificate

A warning dialog box appears if the answer to all three questions is No. To prevent this warning 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. From a Unit Overview window for a target device, click the *Serial Session* icon or link for the session type.
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, and the Warning - HTTPS dialog box appears, contact the issuer of your certificate.
3. When a Warning - Security dialog box appears, click *Yes* to make a connection with the appliance and open the viewer, but continue to display the warning dialog box each time you connect to the serial console appliance.

   -or-

   Click *No* to not make a connection with the serial console appliance.

   -or-

   Click *Always* to add the certificate to the Java certificate store.

To create a CSR:

1. Click the *System* tab, and in the side bar, click *Certificate*.

2. In the Rack Power Manager Server Certificate Properties window, click *Get CSR*.
3. In the File Download dialog box, click *Open* to download and open the CSR in the configured text editor.

   -or-

   Click *Save* and in the Save As dialog box, select a directory and filename and click *Save*.
4. Submit the CSR generated request to a CA to obtain a signed server certificate.
5. 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 can 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 47.

1. Click the *System* tab, and in the side bar, click *Certificate*.
2. In the RPM Server Certificate Properties window, click *Update*.
3. From the Update Rack Power Manager Server Certificate Wizard, in the Select Operation to Perform window, 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), then click *Next* and go to step 4.

   -or-

   Select *Import a signed SSL server certificate* to import a more secure SSL certificate that is approved (perhaps by a CA), click *Next* and go to step 6.

NOTE: 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.

4. In the Type in Certificate Information window, add the following information.

Table 6.2 Type in Certificate Information Window Entries

FIELD	DESCRIPTION
Common Name	Enter the name of the server to be the Rack Power Manager server on your intranet. If the Rack Power Manager server is outside the intranet, enter the full domain name for the server.
Organization	Enter the name of the organization and organizational division or name under which the organization is doing business.
Location	Enter the complete name of the city or location of the organization (required for organizations registered only at the local level).
State/Province	Enter the complete name of the state or province and the two-character ISO country code for the country where the organization is located.

5. Click *Next* and go to step 7.
6. In the Select Certificate to Import window, enter or browse to the full directory and filename for the SSL certificate file to be imported to the Rack Power Manager server, then click *Next*.

NOTE: If your operating system supports case sensitive filenames, the name of the SSL certificate file is case sensitive.

NOTE: Imported certificates must be generated from a CSR created on the same Rack Power Manager server to which you are importing the certificate.

7. In the Completed Successful window, click *Finish* and verify the updated certificate information in the Rack Power Manager Server Certificate Properties window.

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 occurs.

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

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

1. Click the *System* tab of the hub server, verify the *RPM Server* is automatically selected in the top bar and the name of the Rack Power Manager software hub server appears in the side bar.
2. In the side bar, click *Spoke Servers*.
3. In the Spoke Servers window, click *Certificate* to view information about the spoke server certificate (Actual Certificate) and the certificate registered for this spoke server on the hub server (Registered Certificate).
4. If the Rack Power Manager management software cannot obtain the certificate information from the spoke server, the message *Remote server is not responding. Information displayed may not match remote side* appears at the bottom of the RPM Server Certificate - Spoke Server window. If the certificate information does not match, go to step 5.

   -or-

   If the certificate information matches, go to step 6.
5. Click *Update* to update the spoke server certificate information on the hub server.
6. Click *Close* to open the Spoke Servers window.

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

NOTE: On the spoke server, from the System tab, the *RPM Server* is automatically selected in the top bar and the name of the spoke server is displayed in the side bar.

1. In the side bar, click *Hub Server*.
2. In the Hub Server window, click *Certificate* to view the Hub Server Certificate window with information about the spoke server certificate (Actual Certificate) and the certificate registered for this spoke server on the hub server (Registered Certificate).

NOTE: If the Rack Power Manager software cannot obtain the certificate information, the following message is displayed on the bottom of the RPM Server Certificate - Hub Server window:
Remote server is not responding. Information displayed may not match remote side.

3. If the certificate information does not match, click *Update* to update the hub server certificate information on the spoke server.

6.1.2 Server trap destinations

After the Rack Power Manager server polls switches/appliances, if a 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 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 can also be specified by clicking a managed appliance and changing the SNMP appliance settings.

To specify trap destinations:

1. Click the *System* tab, and in the side bar, click *Trap Destinations*.
2. In the RPM Server Trap Destinations window, in each address field, enter up to four IP addresses or the domain name for the computer that handles traps.
3. Click *Save* to store the trap information in the Rack Power Manager software database on the host.

6.1.3 Client session information

The default time for a client session is 15 minutes. When the time-out value is exceeded, the session ends and the user must log in again.

The user certificate (X.509 digital ID) that is installed in the Rack Power Manager software client web browser, must match the certificate configured for the user. Certificates for users can be modified. See User certificates on page 143.

NOTE: Web browser settings may need to be modified to allow users to automatically log in using certificates or Integrated Windows Authentication. See your web browser documentation.

You can enable or disable to allow a member with more than one authentication service to log in. 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 log in times.

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 for each Rack Power Manager hub and spoke server.

To specify client session information:

1. Click the *System* tab, and in the side bar, click *RPM Client Sessions*.
2. In the RPM Server Client Session Properties window (with the number of currently active client sessions), click the arrows to specify a time-out value (5-60 minutes) for inactivity of a Rack Power Manager client session.
3. Click the Enable certificate authentication checkbox to allow the Rack Power Manager software to automatically log in internal users.

   -or-

   Click the Enable Integrated Windows Authentication checkbox to automatically log a user in to the Rack Power Manager software using the Windows server credentials of the user.
4. Enable only Rack Power Manager software clients with IP addresses entered in the Address List to communicate with managed appliances by checking the Restrict by address range checkbox.

-or-

Disable address restrictions for logging in to the Rack Power Manager software, by checking this checkbox.

5. Enable or disable *Allow login when user is a member of more than one authentication service* as desired.
6. Click *Save* to store client session information in the Rack Power Manager software database on the host.

6.1.4 Security Settings

In Rack Power Manager SP5, the PCI Compliance window is replaced by the RPM Security Settings window, which includes security settings for the SSL protocol (including PCI Compliance), your browser and appliances.

The *Disable SSLv3* (default) and *TLS1.0*. SSL protocol options are available for more security. The SSL protocol options are as follows:

- Disable SSLv3
- Disable SSLv3 for Browsers Only
- Disable TLS1.0 and SSLv3
- Disable TLS1.0 and SLv3 for Browsers Only
- Use JRE Settings

NOTE: For JRE configuration information, contact Technical Support.

Under the SSL protocol settings are the Browser options: Very High, High and Customize. These options apply for the connection from the client browser to the Rack Power Manager server. The default browser security option is Very High, which applies for current browsers. High is used for services that don't need compatibility with legacy clients (mostly WinXP), but still need to support a wide range of clients. Customize allows you to define the ciphers accepted by the Rack Power Manager server.

For the connection from the Rack Power Manager server to the appliance, the options are also Very High, High and Customize. The default option is Very High, which contains the strongest cipher. The High option is provided for older browsers and the Customize option is provided to allow you to select or remove specific ciphers.

To select the security settings:

1. Click *System - RPM Security Settings*.
2. Enable the applicable protocol, browser and appliance checkboxes.
3. If applicable, enable the Include FIPS140 Ciphers checkbox.
4. Click *Save*.

6.1.5 Email

Configuring the SMTP server allows you to send email notifications as a domain name or an IP address.

To specify email properties:

1. Click the *System* tab, and in the side bar, click *Email*.
2. In the RPM Server Email Server Properties window, enter a new address for the SMTP server that sends email notifications as a domain name or an IP address.

3. If your SMTP server requires login credentials, select *Login required to access SMTP server* and enter a username and password, then confirm the password.
4. Click *Save* to store Rack Power Manager software email property information in the Rack Power Manager software database on the host.

6.1.6 Unit status polling

When Unit Status Polling is enabled, an Administrator can poll the status of one, a range or all appliances enrolled in the Rack Power Manager software. If you do not want to poll all of the available appliances, a filter allows you to select/deselect the applicable appliances.

To use Unit Status Polling:

1. Click the *System* tab of the RPM hub server, and in the side bar, click *Unit Status Polling*.
2. In the RPM Server Unit Status Polling Properties window, check the Enable unit status polling checkbox.
3. Enter the number of seconds to wait between polling cycles (1-999 seconds). The default is 900 seconds (15 minutes). A smaller value results in greater accuracy.
4. Enter the number of managed appliances that can be polled simultaneously to obtain status information (1-50 units). The default is five. A larger number results in faster speed.
5. If polling all the appliances, skip this step.

   -or-

   If polling one or more specific appliances, check the Enable Selective Polling checkbox and use the following instructions to select the appliances as necessary:

   - From the Enabled Appliances and Enabled Groups boxes, click the appliances or groups to be excluded from polling and click *Add*.
   - From the Excluded Appliances and Excluded Groups boxes, click the appliances or groups to be polled and click *Remove*.

NOTE: When selecting a range or all appliances, click the first desired appliance, press the Shift key, then scroll to and click the last desired appliance in the range.

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

6.2 Backing up and Restoring Hub Servers Manually

With software administrator privileges you can manually back up and restore Rack Power Manager servers. You can manually create a backup of your hub server using one of the following methods:

- From a command line in an MS-DOS window, you can create a backup 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, you can save the backup as a .zip file containing the files needed to restore the Rack Power Manager management software. This method can be used for Rack Power Manager software hub servers on supported Windows systems only.

NOTE: Client sessions are temporarily disconnected during a manual backup and automatically reconnected when the backup is complete.

For information to back up and restore servers automatically, see Task: Backing up the Rack Power Manager software database and system files on page 181.

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

1. From the Start menu on your desktop, click *Programs - Accessories - Command Prompt*.
2. At the command prompt, change the directory to the directory in which the Rack Power Manager Backup Restore utility is installed, which is typically C:\Program Files\Vertiv\RPM 1.0\BackupRestore.
3. Enter **RPMBackupRestore** to display the Rack Power Manager Backup/Restore Utility dialog box and go to one of the following applicable procedure.

   -or-

   Enter **RPMBackupRestore -backup -archive "<archive name>" -passwd <password>** to back up the Rack Power Manager software hub server.

   -or-

   Enter **RPMBackupRestore -restore -archive "<archive name>" -passwd <password>** to restore the Rack Power Manager software hub server.

   Examples:

   - "<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 is required when restoring the backup.

   -or-

   Enter **RPMBackupRestore -h** or **RPMBackupRestore -help** to display help information.

   Examples:

   - In a command prompt window, enter **RPMBackupRestore.exe -backup -archive "db.zip"-passwd test** to create a backup named db.zip with the password test.
   - In a command prompt window, enter **RPMBackupRestore.exe -restore -archive "db.zip"-passwd test** to restore a backup named db.zip with the password test.

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

1. From the Start menu on your desktop, access the command prompt on your system.
2. Change the directory to the directory where the Rack Power Manager Backup Restore utility is installed, which is typically /usr/local/Vertiv/RackPowerManager/BackupRestore.
3. Enter **RPMBackupRestore.sh -backup -archive <archive name> -passwd <password> -overwrite** to back up the **Rack Power Manager** software hub server.

   -or-

   Enter **RPMBackupRestore.sh -restore -archive <archive name> -passwd <password>** to restore the Rack Power Manager software hub server.

   Examples:

- <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 is required when restoring the backup.
- -overwrite - Enables overwriting of an existing archive during backup. If this parameter is omitted, no overwriting occurs.

-or-

Enter **RPMBackupRestore.sh -help** to display help information.

Examples:

- In a command prompt window, enter **RPMBackupRestore.sh backup -archive dbasebackup.zip-passwd test1** to create a backup named dbasebackup.zip with the password test1.
- In a command prompt window, enter **RPMBackupRestore.sh restore -archive dbasebackup.zip-passwd test1** to restore a backup named dbasebackup.zip with the password test1.

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

1. From the Start menu on your desktop, click *Programs - Avocent Rack Power Manager - RPMBackupRestore*.
2. In the Rack Power Manager Backup/Restore Utility dialog box, click *Backup Database to a file*.
3. If you are password-protecting the backup file, click *Enabled* and enter a password in the Password field.
4. Click *Browse*, use the Save As dialog box to specify a directory and name for the backup file and click *Save*.
5. Click *Backup* to save the Rack Power Manager software system backup files.
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. From the Start menu on your desktop, click *Programs - AvocentRack Power Manager - RPMBackupRestore*.
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 enter its password in the Password field.
4. Click *Browse* and use the Save As dialog box to find the backup file.
5. Click *Restore* to restore the Rack Power Manager software system from the backup files and click *Close*.

6.3 Spoke Servers

Information about each spoke server, such as IP address, port number and certificate, is stored in the database of the hub server. The hub server database can be replicated on up to 15 spoke servers. After spoke servers are configured, you can change their properties or remove them from your system.

A spoke server can be created using one of the following methods:

- 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 is lost and the converted hub server replicates the data of the new specified hub server.

The side bar includes the name of the server to which you are logged in. The Spoke Servers window (only available on the hub server) displays the status of each spoke server in the list. For information to change the fields, see Using the Customize link in windows on page 21.

For information to install licenses, see Viewing and Adding Licenses on page 40.

To display a list of spoke servers:

1. Click the *System - RPM Server* tabs.
2. In the side bar, click *Properties* and click *Spoke Servers*.

Table 6.3 Software Spoke Server Status

STATUS	CAUSE
Responding	Normal operation; the hub and spoke servers use HTTPS to communicate with each other.
Not Responding	The hub and spoke servers cannot communicate with each other using HTTPS; typically indicates a network communication error. Ensure that network connectivity is occurring between the two servers.
Hub/Spoke Versions Not Compatible	The versions of the hub and spoke servers are not compatible.
Certificates Do Not Match	Certificates for the hub and spoke servers do not match. See Managing hub and spoke server certificates on page 47 to update server certificates.
Invalid Server or Versions Not Compatible	A server responded, but it is not compatible with the Rack Power Manager software; typically occurs when communication is attempted with a server that does not contain the software or if the servers are not running the same Rack Power Manager software version.

To add a spoke server:

1. Install the Rack Power Manager software on the server to be used as a spoke server.
2. Configure the server as a spoke server.

For more information, see Installing the Rack Power Manager Software on page 4 and Configuring the Rack Power Manager Software on page 5.

To register a hub server as a spoke server:

Only Rack Power Manager software administrators can 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 is lost. Its database is updated to match the new hub server to which it is being registered.

1. Click the *System - RPM Server* tabs.
2. In the side bar, select *Tools*.
3. In the RPM Server Tools window, click the *Register as Spoke Server* icon or text.
4. From the Register Spoke Server Wizard, in the Type in Hub RPM Server Address window, enter the IP address or domain name and port number of the hub server and click *Next*.

NOTE: If the default hub server port value (443) is modified, you must specify it when registering a spoke server, so that registered requests are 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, enter https://10.0.0.1:444/RPM **in the Address field of the Register Spoke Server Wizard.**

5. From the Operation in Progress window, in the Accept Hub RPM Server Certificate window, click *Next*.
6. In the Type in Hub RPM Server Administrator Credentials window, click *Next*.
7. Enter the name and password of a user with Rack Power Manager software administrator privileges on the hub server and click *Next*.
8. In the Completed Successful window, click *Finish*.

To change spoke server network properties:

NOTE: Spoke server network settings may need to be changed by a Rack Power Manager software administrator if network settings are changed and the hub server does 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. From the hub server, click the *System - RPM Server* tabs.
2. In the side bar, click *Properties* and *Spoke Servers*.
3. In the Spoke Servers window, click the checkbox or name of the spoke server whose network properties are to be changed.
4. In the Spoke Server Network Properties window, enter a new computer name, address and port number for the spoke server.
5. Click *Save* and *Close*.

To delete a spoke server:

1. From the hub server, click the *System - RPM Server* tabs.
2. In the side bar, click *Properties* and *Spoke Servers*.
3. In the Spoke Servers window, click the checkbox of the spoke servers to be deleted.
4. Click *Delete* and confirm or cancel the deletion.

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

Promoting spoke servers

If the current hub server is no longer operational and will not be brought back into service, a spoke server can be promoted to a hub server. (For less severe problems with a hub server, the back up and restore operations can be used.)

If a spoke server must be promoted to a hub server, it is recommended to run the replication task, if possible, on all other spoke servers. Then immediately before the promotion, run the replication task on the spoke server being promoted to prevent loss of data from the other spoke servers. See the following section.

After the promotion of the spoke server on which the wizard is running to the hub server, the other spoke servers are advised of the changed configuration. If the server that was originally the hub server becomes operational again, it must be registered as a spoke server because a system can have only one hub server.

To promote a spoke server to a hub server:

1. From the spoke server, click the *System* tab, and in the side bar, click *Tools*.
2. Click *Promote to hub server* and follow the prompts in the Promote Hub Server Wizard.

6.4 Replication

Replication is a task that synchronizes the hub and spoke server databases. The first replication of a spoke server occurs automatically when the spoke server is added to the Rack Power Manager software system. The default configuration runs the replication every 12 hours on each spoke server; however, you can change the interval that the replication task runs on each spoke server, or you can 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 the spoke server just sent to the hub server).

The following are additional replication rules:

- 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 appear on both the hub and spoke servers, with a tilde (~) and a number added to one of the names. In some cases, the replicated item may need to be renamed or deleted.
- The power and environmental data collected from the PDUs are not replicated between the servers.
- When different changes are made to an existing item, two outcomes are possible. For example, assume an item is added and configured on the hub server and then replicated to a spoke server. Later, an administrator changes something about the item on the spoke server and then another administrator 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 are incorporated and replicated. For example, if the administrator of the hub server adds username JaneDoe to the existing user-defined Accounting user group and the administrator of the spoke server adds username JohnDoe to the Accounting user group, both names are added and replicated.
- In most other instances where the changes are mutually exclusive or some other conflict occurs, the most recent change is the only change accepted and replicated. For example, if the administrator of the hub server associates a unit with the Miami site, and the administrator of the spoke server associates the same unit with the Chicago site, the change made closest to the time of replication (that is, the most recent change) is accepted and replicated. This emphasizes the importance of ensuring the clocks of the hub and spoke servers are synchronized.

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

- On a spoke server, you can 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 fails.

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

1. From the spoke server, click the *System - Tasks* tabs.
2. In the Tasks window, select the *Database Replication* task.
3. From the Task Results - Database Replication window, in the side bar, click *Schedule*.
4. If desired, in the Task Schedule - Database Replication window, change the schedule type, start time, date and interval.

NOTE: Instead of synchronizing changes, you may want to force the spoke server to retrieve a snapshot of the hub database. If so, in the side bar, click *Properties* and click the Perform a hub database snapshot the next time this task executes checkbox.

NOTE: This configuration is reset to unchecked after the operation is complete.

5. If you made any changes, click *Save* and *Close*.

NOTE: The replication schedule can also be displayed from the hub server, but without the ability to make changes.

To initiate an immediate replication on a spoke server:

1. From a spoke server, click the *System - Tasks* tabs.
2. On the Tasks window, click the Database Replication task checkbox and click *Run Now*.

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

1. From a hub server, click the *System - Tasks* tabs.
2. Select the *Database Replication* task for the spoke server to be viewed.

6.5 De-registering Servers

If the DSView or Rack Power Manager software system detects residual integration data, the De-register button is enabled. Clicking the *De-register* button allows you to remove any residual integration data from the applicable server.

To de-register a server:

1. Click the *System - Tools* tabs and click *De-register*.
2. Select a user password reset type and click *Next*.
3. Reset the password, click *Save* and click *Finish*.

NOTE: If network errors occur during the de-registration process, the local data is cleared.

To synchronize the DSView and Rack Power Manager software:

1. Click the *System - Tasks* tabs and click *RPM and DSView Replication*.
2. Click *Run Now*.

7 AUTHENTICATION SERVICES

Users must be authenticated before accessing or performing any tasks in the Rack Power Manager software system. When logging in, a username and password are required (1-64 characters). The Rack Power Manager software looks up the login information, determines the authentication service to use and forwards the login credentials to the appropriate authentication service for verification. All authentication is performed over an HTTPS (SSL) encrypted link.

Some web browsers store password information. For more information, see your web browser documentation.

7.1 Supported Authentication Services

The Rack Power Manager software is delivered with its internal authentication service, which verifies the login name 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
- 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 the group membership of a user changes or the user is deleted externally, the Rack Power Manager software does not see these changes until the user logs in the next time.

You can schedule a task to automatically verify LDAP, Active Directory and NT external authentication servers to ensure that accounts are still valid. For more information, see Task: Validating user accounts on an external authentication server on page 186.

Authentication services are managed only by software and user administrators of the Rack Power Manager.

To display configured authentication services:

Click the *Users - Authentication* tabs.

NOTE: In addition, you can click the *Customize* link to modify the User Authentication Services window. See Using the Customize link in windows on page 21.

To remove external authentication services:

NOTE: The internal authentication service cannot be removed.

1. Click the *Users - Authentication* tabs.
2. In the User Authentication Services window, click the checkboxes of the authentication services to be deleted.
3. Click *Delete*, and in the confirmation dialog box, confirm or cancel the deletion.

7.1.1 Rack Power Manager software internal authentication service

In the Authentication Service User Account Policies - RPM Internal window, you can specify the following policies:

- Enter a number (1-64) in the Minimum Password Length field or click the arrows to select a number.
- Click the Passwords Expire checkbox to require a user to change the password after a certain number of days. Specify or select a number (1-365) in the Maximum Expiration (days) field.
- Select *Passwords must contain both alpha and numeric characters* to require at least one letter and one number.
- Select *Passwords must contain both lower and upper case characters* to require at least one uppercase and one lowercase letter.

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

1. Click the *Users - Authentication* tabs.
2. In the User Authentication Services window, click *RPM Internal*.

NOTE: The side bar adds RPM Internal with the updated information.

3. In the side bar, click *Account Policies*.
4. In the Authentication Service User Account Policies - RPM Internal window, specify the applicable password policies for the authentication service.
5. Check the Lockout users after invalid login attempts checkbox and in the Maximum Login Failures field, enter or select the number of allowable user log in failures (1-25).

NOTE: If this checkbox remains unchecked, allowing unlimited user log in attempts, proceed to the last step.

-or-

Permit user logins after a certain period of time by checking the Automatically unlock users after the lockout period checkbox, and selecting a value from the menu or entering a lockout period (1-440 minutes) in the Maximum Lockout Period field.

NOTE: 1,440 minutes is equivalent to 24 hours.

NOTE: If this checkbox remains unchecked, locked user accounts must be manually unlocked by a Rack Power Manager software administrator or user administrator. See Unlocking User Accounts on page 142.

6. Click *Save* and *Close*.

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

1. Click the *Users - Authentication* tabs.

2. In the User Authentication Services window, click *RPM Internal*.

NOTE: The side bar adds RPM Internal with the updated information.

3. In the side bar, click *Custom Field Labels*.
4. In the Authentication Service User Account Custom Field Labels - RPM Internal window, enter the text for each of the six custom field labels.
5. Click *Save* and *Close*.

NOTE: The default does not display the custom field labels in the User Accounts - All window, but they can 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 21.

7.1.2 Active Directory external authentication service

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 can have a trusted relationship with other forests. In some configurations, a user can 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.

In the User Container field, specify the name of the container to search for user accounts. This limits the search scope to that container. The name can be entered in several forms, optionally including a sub-domain. The following valid forms are explained by the examples:

- Assume an Active Directory domain name of “sunrise.mycompany.com” with users in subfolder “sun/myusers.” The User Container field can 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”

Existing authentication servers are set to the Partial Windows 2000 Username type for compatibility. The following username types can only be configured for new authentication servers and cannot be modified:

- 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.

If the authentication service has trusted forests, the settings configured for the authentication service in the Add Authentication Service Wizard are 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 73 for more information about trusted forests.

Search modes

The search modes in the following table can be enabled.

Table 7.1 Search Mode Descriptions

MODE	PURPOSE	DESCRIPTION
Use Recursion to search groups	Enables the AD service to access the domain controller for the specified domain name	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.
Use an Active Directory Global Catalog	Enables the AD service to access the global catalog for the specified domain name	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.
Use Windows 2003 Universal Group Caching	Enables the AD service to access the domain controller for the specified domain name	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.

SSL Encryption Modes

The SSL encryption modes in the following table can be enabled.

Table 7.2 SSL Encryption Modes

MODE	FUNCTION
Do Not Use SSL	Click to have authentication performed using unencrypted clear text instead of SSL encryption. This method is the least secure.
Use SSL in Trust All Mode	Click to use SSL encryption for data transmission. All server certificates are 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).
Use SSL in Certificate-based Trust Mode	Click to use SSL encryption for data transmission. The Rack Power Manager management software approves the server and then the certificate before transmitting data. This SSL method provides maximum security.

To add an Active Directory external authentication service:

1. Click the *Users - Authentication* tabs.
2. In the User Authentication Services window, click *Add*.
3. From the Add Authentication Service Wizard, when the Provide Authentication Service Name and Type windows are displayed, enter a name for the external authentication service.
4. From the menu, select *Active Directory* and click *Next*.
5. In the Specify Active Directory Connection Settings window, enter the Active Directory domain name for the domain to be added in the AD Domain Name field.
6. In the User Container and Group Container fields, specify the name of the container to search for user and group accounts.

NOTE: This limits the search scope to that container. The name can be entered in several forms, optionally including a sub-domain.

7. In the Username Type menu, select a username type, then click an SSL encryption mode.
8. Click *Use Kerberos for User Authentication* to use the Kerberos protocol for authentication requests, including the browsing.

NOTE: If enabled, you must use DES encryption types for this account. If an account was created prior to Active Directory, the password of the user 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 is used.

9. Click *Enable Chasing of Referrals* to allow the Active Directory server to refer Rack Power Manager software clients to additional directory servers.
10. Select a search mode (*Use Recursion to search groups*, *Use an Active Directory Global Catalog* or *Use Windows 2003 Universal Group Caching*).
11. 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, then click *Next*.

NOTE: If enabled, the Rack Power Manager discovers all trusted forests in the Active Directory service.

12. If you selected *Use SSL in Certificate-based Trust Mode*, go to step 13.

    -or-

    If you selected *Do Not Use SSL* or *Use SSL in Trust All Mode*, go to step 14.

NOTE: The Rack Power Manager server tries to find a server that has a trusted certificate chain (see System certificate policy and trust store on page 34). If no trusted certificate chain is found, the Accept Certificate window displays all servers that belong to the domain and reasons for rejection of the certificate chain.

13. Click *Next* to accept the certificate.
14. On the Select Browsing Method window, 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.

15. If *Browse with user credentials* is selected, enter the username of an Active Directory account that has browse rights in the User Name field, enter the password for an Active Directory account with browse rights in the Password field and click *Next*.

NOTE: 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), the username should be specified as <username>@<subdomain>.

16. In the Completed Successful window, click *Finish*, then verify the new service is listed in the User Authentication Services window.

To change settings for the Active Directory external authentication service:

1. Click the *Users - Authentication* tabs.
2. In the User Authentication Services window, click the name of the Active Directory (AD) service.
3. When the side bar changes to include the name of the AD service and the information you can define, click *Connection*.

4. In the Authentication Service Connection Settings - AD window, enter 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.
5. In the AD Domain Name field, enter the domain name of the Active Directory service.
6. In the User Container and Group Container fields, specify the name of the container to search for user and group accounts.

NOTE: This limits the search scope to that container. The name can be entered in several forms, optionally including a sub-domain. See To add an Active Directory external authentication service: on page 60 for an explanation of the valid forms.

7. Click an SSL encryption mode (*Do Not Use SSL*, *Use SSL in Trust All Mode* or *Use SSL in Certificate-based Trust Mode*.
8. Click *Use Kerberos for User Authentication* to use the Kerberos protocol for authentication requests, including the browsing.

NOTE: If enabled, you must use DES encryption types for this account. If an account was created prior to Active Directory, the password of the user 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 is used.

9. Click *Enable Chasing of Referrals* to allow the Active Directory server to refer Rack Power Manager software clients to additional directory servers.
10. Enable a search mode (*Use Recursion to search groups*, *Use an Active Directory Global Catalog* or *Use Windows 2003 Universal Group Caching)*.
11. 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 queries all trusted forests in the Active Directory service to find the user and user groups to which the authenticated user belongs.

    -or-

    Deselect *Allow use of Users/Groups from Trusted Forests* to hide any previously discovered trusted forests in the User Authentication Services window and prevent users belonging to trusted forests from logging in.

12. Click *Save* and if you selected *Use SSL in Certificate-based Trust Mode* (the Certificates heading appears in the side bar), go to step 11.

    -or-

    If you selected *Do Not Use SSL* or *Use SSL in Trust All Mode*, go to step 14.

13. Click *Certificates* to display the Authentication Service Certificate Management - AD window with a list of all servers in that domain with their status.

NOTE: A status of Trusted indicates the certificate is trusted, based on the certificate policy (see System certificate policy and trust store on page 34); Untrusted indicates the certificate cannot be trusted.

14. If registering certificates, select one or more certificates, click the checkbox of each server IP address, then click *Register* above the IP Address list to register the certificates. In the Accept SSL Certificate window, 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.

NOTE: The Authentication Service Certificate Management window opens if only one certificate is selected. If more than one certificate is selected, each appears in order in subsequent Accept SSL Certificate windows.

15. If unregistering certificates, select one or more certificates, click the checkbox of each server IP address and click *Unregister*.
16. In the dialog box, confirm or cancel the operation and click *Close*.

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

1. Click the *Users - Authentication* tabs.

NOTE: In the User Authentication Services window, click the name of the AD service. The side bar changes to include the name of the AD service at the top, and below the name, the information you may define.

2. In the side bar, click *User Browsing*.
3. In the Authentication Service User Browsing - AD window, 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. Then enter the username and password for an Active Directory account that has browse rights and click *Next*.

NOTE: If the Active Directory server is configured to use Kerberos, the log in ID is case sensitive.

4. After the Rack Power Manager server verifies the new credentials, click *Save* and *Close*.

7.1.3 Windows® NT external authentication service

To add a Windows NT external authentication service:

1. Click the *Users - Authentication* tabs.
2. In the User Authentication Services window, click *Add*.
3. From the Add Authentication Service Wizard, in the Provide Authentication Service Name and Type window, enter a name for the external authentication service.
4. From the menu, select *Windows NT Domain* and click *Next*.
5. In the Specify Windows NT Connection Settings window, enter the Windows NT domain name to be added in the Domain Name field and click *Next*.
6. In the Select Browsing Method window, 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 service based on credentials configured on the server, then enter the username and password for a Windows NT account that has browse rights and click *Next*.

7. In the Completed Successful window, click *Finish*.

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

1. Click the *Users - Authentication* tabs.
2. In the User Authentication Services window, click the name of the Windows® NT service.

NOTE: The side bar changes to include the name of the service at the top, and below the name, the information you may define.

3. In the side bar, click *Connection*.
4. In the Authentication Service Connection Settings - NT window, enter 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.
5. Enter the name of the Windows NT domain in the Domain Name field.
6. Click *Save* and *Close*.

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

1. Click the *Users - Authentication* tabs.
2. In the User Authentication Services window, click the name of the Windows NT service.

NOTE: The side bar changes to include the name of the Windows NT service at the top, and also below the name, the information you may define.

3. In the side bar, click *User Browsing*.
4. In the Authentication Service User Browsing - NT window, 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 service based on configured credentials, then enter the username and password for an NT domain account that has browse rights.

5. Click *Save* and *Close*.

7.1.4 LDAP external authentication service

Authentication can be performed using unencrypted clear text or SSL encryption modes. The SSL options and the default port numbers are described in the following table.

Table 7.3 Secure Socket Layer (SSL) Encryption Mode Descriptions

MODE	DESCRIPTION	PORT NUMBER (FACTORY DEFAULT)
Do Not Use SSL (Unencrypted clear text)	Least secure; automatically configures the service for unencrypted clear text	389
SSL in Trust All Mode	Medium security (not recommended for WANs); all server certificates are trusted and automatically accepted by the Rack Power Manager software for transmitting data.	636
SSL in Certificate-based Trust Mode	Maximum security; the Rack Power Manager software approves the server and then the certificate before transmitting data.	636

The factory defaults for the user schema are listed in the following table.

Table 7.4 Changing Schema Settings

USER SCHEMA ATTRIBUTES	FACTORY DEFAULT
Key attribute	common name (cn)
Object class	person
Full name attribute for the user	surname (sn)

To add an LDAP external authentication service:

1. Click the *Users - Authentication* tabs.
2. In the User Authentication Services window, click *Add*.
3. From the Add Authentication Service Wizard, in the Provide Authentication Service Name and Type window, enter a name for the external authentication service.
4. From the Type menu, select *LDAP* and click *Next*.
5. In the Specify LDAP Connection Settings window, enter the address of the LDAP host or in the Host Address field, enter the DNS host name. Then in the Port Number field, enter the number of the port to be connected to the LDAP host.
6. Click *Do Not Use SSL* or *Use SSL in Trust All Mode*.
7. Click *Use SSL in Certificate-based Trust Mode* and if you wish to allow the LDAP server to refer Rack Power Manager software clients to additional directory servers, click *Enable Chasing of Referrals* and click *Next*.
8. If you selected *Use SSL in Certificate-based Trust Mode*, go to step 9.

   -or-

   If you selected *Do Not Use SSL* or *Use SSL in Trust All Mode*, go to step 13.

NOTE: The Rack Power Manager server tries to find a server that has a trusted certificate chain (see System certificate policy and trust store on page 34). If no trusted certificate chain is found, the Accept Certificate window displays all servers that belong to the domain and reasons for rejection of the certificate chain.

9. Click *Next* to accept the certificate.
10. In the Specify LDAP User Schema window, enter the Base distinguished name (DN) for searches.

NOTE: This is a required field unless the Directory Service is configured to allow anonymous searches. Each Search DN value must be separated by a comma.

11. Enter the key attribute, object class and full name attributes, then click *Next*.

NOTE: The defaults for the key attributes are common name (cn), object class is person and full name attribute is surname (sn).

12. In the Specify LDAP Group Schema window, enter the DN for searches, object class, member attribute and username member attribute (only the username, not the full LDAP object DN), then click *Next*.

NOTE: This a required field unless the Directory Service is configured to allow anonymous searches. Each Search DN value must be separated by a comma.

NOTE: Defaults are object class - group, member attribute - member, enter the username member attribute (only the username, not the full LDAP object DN). The group membership of the user is located using this attribute in addition to the member attribute. This attribute is primarily used with NIS-like schemas.

13. In the Select Browsing Method window, 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 server based on credentials configured on the server. In the User Name field, enter a log-in ID (a fully qualified distinguished name or the username of an account in the base user DN) and the LDAP user account password and click *Next*.

14. In the Completed Successful window, click *Finish*.

To change connection settings for the LDAP external authentication service:

1. Click the *Users - Authentication* tabs.
2. In the User Authentication Services window, click the name of the LDAP service.
3. After the side bar updates with the name of the LDAP service with its editable information, click *Connection* in the side bar.
4. In the Authentication Service Connection Settings - LDAP window, enter 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.
5. In the Host Address field, enter the address of the LDAP host.
6. In the Port Number field, enter the number of the port to be used for connecting to the LDAP host.
7. Specify an SSL Encryption mode and click *Save*.
8. If you selected *Use SSL in Certificate-based Trust Mode*, after the Certificates heading appears in the side bar, go to step 8.

   -or-

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

9. Click *Certificates* and in the Authentication Service Certificate Management - LDAP window, list all servers that belong to the domain.

NOTE: A status of Trusted indicates the certificate is trusted based on the certificate policy (see System certificate policy and trust store on page 34); Untrusted indicates the certificate cannot be trusted.

10. Click the checkbox of the server IP addresses to be registered, then click *Register* and in the Accept SSL Certificate window, click *Save* to store the certificate values to the Rack Power Manager software database on the host.

NOTE: If only one certificate is selected, the Certificate Management window opens. If more than one certificate is selected, each appears in order in subsequent Accept SSL Certificate windows.

-or-

Click the checkbox of the server IP addresses to be unregistered, then click *Unregister* and in the confirmation box, confirm or cancel the operation and click *Close*.

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

1. Click the *Users - Authentication* tabs.
2. In the User Authentication Services window, click the name of the LDAP service. The side bar changes to include the name of the LDAP service with the information you define.
3. In the side bar, click *Schema* (*Users* is automatically selected).
4. In the Authentication Service User Schema - LDAP window, enter the Base distinguished name (DN) for searches (required unless the Directory Service is configured to allow anonymous searches).

NOTE: Each Search DN value must be separated by a comma.

5. Enter the key attribute, object class and full name attribute for the user.
6. Click *Save* and *Close*.

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

1. Click the *Users - Authentication* tabs.
2. In the User Authentication Services window, click the name of the LDAP service.

NOTE: The side bar changes to include the name of the LDAP service at the top and, below the name, the information you may define.

3. In the side bar, click *Schema* and then click *Groups*.
4. In the Authentication Service Group Schema - LDAP window, enter the DN for searches.

NOTE: This is a required field unless the Directory Service is configured to allow anonymous searches.

5. Enter the object class, members attribute and the username member attribute (only the username, not the full LDAP object DN).

NOTE: The group membership of the user is located using this attribute in addition to the member attribute. This attribute is primarily used with NIS-like schemas.

6. Click *Save* and *Close*.

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

1. Click the *Users - Authentication* tabs.
2. In the User Authentication Services window, click the name of the LDAP service.

NOTE: The side bar changes to include the name of the LDAP service at the top with its editable information.

3. In the side bar, click *User Browsing*.
4. In the displayed Authentication Service User Browsing - LDAP window, click *Browse Anonymously* to browse users on the external LDAP authentication server and go to step 6.

   -or-

   Click *Browse with User Credentials* to browse users on the external LDAP authentication server based on credentials configured on the server and go to step 5.

5. In the User Name field, enter a login ID (a fully qualified distinguished name or the username of an account in the base user DN) and enter the password for the LDAP user account in the *Password* field.
6. Click *Save* and *Close*.

7.1.5 RADIUS external authentication service

A RADIUS external authentication service can be assigned. The name for the RADIUS authentication service can be 1-64 characters. The port number to be used to connect the RADIUS host can be 1-65535. The default port number is 1812.

Table 7.5 Available Authentication Types

AUTHENTICATION TYPE	DESCRIPTION
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

To add a RADIUS external authentication service:

1. On the RADIUS server to be used as an external authentication service, add the Rack Power Manager server as a RADIUS client and 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* and in the User Authentication Services window, click *Add*.
4. From the Add Authentication Service Wizard, in the Provide Authentication Service Name and Type window, enter a name for the RADIUS authentication service.
5. From the Type menu, select *RADIUS* and click *Next*.
6. In the Specify RADIUS Connection Settings window, enter the address of the RADIUS host or enter the DNS host name in the Server Address field.
7. In the Port Number field, enter the port number (1-65535) to be used to connect the RADIUS host and click *Next*.
8. After the Establish Connection with Authentication Service and the Specify RADIUS Authentication Settings windows open, in the Authentication Type menu, select the authentication type and verify it is one of the available authentication types noted in step 1.
9. In the Shared Secret field (password protected) and Confirm Shared Secret fields, enter the shared secret (configured on the RADIUS server in step 1) and click *Next*.

NOTE: The Microsoft implementation allows up to 128 ASCII characters for the shared secret; other servers may have a different limit.

10. In the Completed Successful window, click *Finish*, and in the User Authentication Services window, verify the new service is listed.

To change settings for the RADIUS external authentication service:

1. Click the *Users* - *Authentication* tabs.
2. In the User Authentication Services window, click the name of the RADIUS service.

3. After the RADIUS service is displayed with its editable information, in the side bar, click *Connection* and in the Authentication Service Connection Settings - RADIUS window, enter a name (1-64 characters) for the RADIUS authentication service.
4. Enter the address of the RADIUS host or enter the DNS host name in the Server Address field.
5. In the Port Number field, enter the number of the port (1-65535) to be used to connect the RADIUS host and click *Save*.The default is port 1812.
6. To change the authentication type and/or shared secret, in the side bar, click *Settings* and in the Authentication Service Authentication Settings - RADIUS window, from the Authentication Type menu, select one of the authentication types.
7. In the Shared Secret and Confirm Shared Secret fields (password protected), enter the shared secret, click *Save* and click *Close*.

NOTE: The Microsoft® implementation allows up to 128 ASCII characters for the shared secret; other servers may have a different limit.

7.1.6 TACACS+ external authentication service

Rack Power Manager software supports TACACS+ external authentication. After the TACACS+ authentication service is added, you can map TACACS+ users to the Rack Power Manager software database by using the Add User Account wizard. When TACACS+ backup is added, if the primary TACACS+ authentication server cannot be reached, the backup server can be used for authentication. 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 140.

You can also associate users with internal Rack Power Manager software groups to control group level access rights. Or, you can 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 150.

Authentication types on the TACACS+ server are:

- PAP - Password Authentication Protocol
- CHAP - Challenge Handshake Authentication Protocol (default)
- MS-CHAP - Microsoft Challenge Handshake Authentication Protocol

Table 7.6 Factory Default Settings for Group Authorization

FIELD	FIELD DESCRIPTION	METHOD	FACTORY DEFAULT RESPONSE
Service	Appropriate TACACS+ service	Privilege level attribute	Value shell
		Custom attribute for group names	Value access
Protocol	If TACACS+ service requires a protocol for authorization requests, enter the protocol		
Attribute Name	Rack Power Manager server receives after an authorization request	Privilege level attribute Custom attribute for group names	Value priv-lvl Value group_name

To add a TACACS+ external authentication service:

1. On the TACACS+ server to be used as an external authentication service, add the Rack Power Manager server as a TACACS+ client.

2. Make a note of the configured shared secret and the available authentication types on the TACACS+ server.
3. From the Rack Power Manager Explorer, click the *Users* tab.
4. Click *Authentication* and in the User Authentication Services window, click *Add*.
5. From the Add Authentication Service Wizard, in the Provide Authentication Service Name and Type window, enter a name for the TACACS+ authentication service.
6. From the Type menu, select *TACACS+* and click *Next*.
7. In the Specify TACACS+ Connection Settings window, in the Server Address field, enter the address of the TACACS+ host or enter the DNS host name.
8. In the Port Number field, enter the port number (1-65535) to connect to the TACACS+ host and click *Next*. The default port is 49.

   -or-

   If you are adding a backup server for TACACS+ authentication, enter the backup host address for the backup server and the port number (1-65535) to connect to the backup server.

9. After the Establish Connection with Authentication Service window opens, from the Authentication Type menu in the Specify TACACS+ Authentication Settings window, select the authentication type and verify it is one of the available authentication types noted in step 1.

   In the Shared Secret field (password protected) and the Confirm Shared Secret field, enter the shared secret (configured on the TACACS+ server in step 1).

NOTE: For the shared secret, the Microsoft® implementation allows up to 128 ASCII characters and the Cisco implementation allows up to 32 ASCII characters; other servers may have a different limit.

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

10. Click *Next*.

    -or-

    If you are adding a backup server for TACACS+ authentication, select the Backup Authentication Type from the Authentication Type menu and verify it is one of the available authentication types noted in step 1. Then in the Shared Secret field (password protected) and the Confirm Shared Secret field, enter the shared secret (configured on the TACACS+ server in step 1).

NOTE: For the shared secret, the Microsoft implementation allows up to 128 ASCII characters and the Cisco implementation allows up to 32 ASCII characters; other servers may have a different limit.

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

11. Click *Next* and if you selected Rack Power Manager internal groups and the external authentication service is added successfully, in the Completed Successful window, click *Finish*.

    -or-

    If you selected any other option, when the Specify TACACS+ Server Group Authorization Settings window opens, enter the appropriate TACACS+ service, protocol and attribute name as listed in the following table and click *Next*.

Table 7.7 Factory Defaults for Step 8 Selections

FIELD	FIELD DESCRIPTION	METHOD	FACTORY DEFAULT RESPONSE
Service	Step 8 for the appropriate TACACS+ service	Privilege level attribute	Value shell
		Group name custom attribute	Value access
Protocol	If TACACS+ service requires a protocol for authorization requests, enter the protocol		
Attribute Name	Step 8 that the Rack Power Manager server receives after an authorization request	Privilege level attribute Group name custom attribute method	Value priv-lvl Value group_name

To change settings for the TACACS+ external authentication service:

1. Click the *Users - Authentication* tabs.
2. In the User Authentication Services window, click the name of the TACACS+ service.

NOTE: The side bar changes to include the name of the TACACS+ service at the top, and also below the name, the information you may define.

3. In the side bar, click *Connection* and in the Authentication Service Connection Settings - TACACS+ window, enter a name for the TACACS+ authentication service.
4. In the Server Address field, enter the address of the TACACS+ host or enter the DNS host name, and in the Port Number field, enter the port number (1-65535) for connecting to the TACACS+ host (default is port 49).
5. Click *Save*.

   -or-

   If you are adding a back up server for TACACS+ authentication, enter the information provided in the following table.

Table 7.8 Backup Server Entries

FIELD	ENTRY DESCRIPTION
Backup Host Address	Address for the backup server
Backup Port Number	Port number (1-65535) connecting to the backup server
Maximum Socket Timeout	Amount of time to wait for a response from the primary host server

6. If you are changing the authentication type and/or shared secret, in the side bar, click *Settings* and in the Authentication Service Authentication Settings - TACACS+ window, select the PAP, CHAP or MS-CHAP authentication type and in the Shared Secret field (password protected) and Confirm Shared Secret field, enter the shared secret.

NOTE: For the shared secret, the Microsoft implementation allows up to 128 ASCII characters and the Cisco implementation allows up to 32 ASCII characters; other servers may have a different limit.

NOTE: If you change the authentication type, you must enter the shared secret.

7. Click *Next*.

   -or-

   If you are adding a backup TACACS+ server, from the Authentication Type menu, select the Backup Authentication Type and verify it is one of the available authentication types noted in

step 1. Then in the Backup Shared Secret field (password protected) and Backup Confirm Shared Secret field, enter the shared secret and click *Next*.

NOTE: For the shared secret, the Microsoft® implementation allows up to 128 ASCII characters and the Cisco implementation allows up to 32 ASCII characters; other servers may have a different limit.

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

8. If you are changing the group authorization settings, in the side bar, click *Group Authorization*.

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

In the Group Authorization fields, enter the appropriate TACACS+ service, a protocol for authorization requests (if required by the TACACS+ service) and the attribute name that the Rack Power Manager server receives after an authorization request.

9. Click *Save* and *Close*.

7.2 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 validation results of the RSA Authentication Manager 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.

When adding an RSA SecurID external authentication service, the sdconf.rec file is created by the RSA Authentication Manager, but is located on the Rack Power Manager software client machine. The sdconf.rec file is uploaded from the Rack Power Manager software client to the Rack Power Manager server. This file is 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. To specify these files, see the procedure to change settings for the RSA SecurID external authentication service.

For information about the log in process when an RSA SecurID external authentication service is used, see Opening a client session on page 6. Consult the RSA Authentication Manager documentation for additional details.

For RSA server requirements, see the RSA Secured Partner Solutions Directory on the RSA web site (rsasecurity.com).

To add an RSA SecurID external authentication service:

1. From the RSA server to 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* and in the User Authentication Services window, click *Add*.
4. From the Add Authentication Service Wizard, in the Provide Authentication Service Name and Type window, enter a name for the RSA authentication service.
5. From the Type menu, select *RSA SecurID* and click *Next*.

6. In the Specify RSA SecurID® Connection Settings window, enter the path (1-512 characters) or browse to the *sdconf.rec* file and click *Next*.
7. In the Establish Connection with Authentication Service window, verify the external authentication service is added, and in the Completed Successful window, click *Finish*.
8. In the User Authentication Services window, verify the new service is listed, then add one or more RSA user accounts to the Rack Power Manager software.

NOTE: The node secret file for the server is not created until the first RSA user logs in to the Rack Power Manager software.

To change settings for the RSA SecurID external authentication service:

1. Click the *Users - Authentication* tabs.
2. In the User Authentication Services window, click the name of the SecurID service.
3. In the side bar, click *Connection*.
4. In the Authentication Service Connection Settings window, enter a new service name (1-64 characters) and click *Save*. If that is the only change you are entering, click *Close*.

   -or-

   Click the checkboxes of the servers to clear the RSA SecurID node secret instances, click *Clear Node Secret* and in the confirmation dialog box, confirm or cancel the operation.

   -or-

   Click the checkboxes of the servers to update the RSA configuration files used by the servers to communicate with the RSA Authentication Manager software and click *Update*. Then, in the Update RSA Configuration File window, enter or browse to the sdconf.rec path, enter or browse to the sdopts.rec path to the advanced option sdopts.rec file for manual load balancing, then click *Save* and *Close*.
5. If necessary, restart the RPM service when the RSA configuration is updated.

7.3 User Authentication Services Window

After added, the authentication services are listed in the User Authentication Services window. To view the window with the authentication service name, type, enabled status and host name, click the *User* tab and click *Authentication Services*.

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 is used to find a user.

To enable or disable an authentication service (trusted forest service):

1. Click the *Users - Authentication* tabs.
2. Select the authentication service and click *Enable* or *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 *Users - Authentication* tabs.
2. Select the primary AD authentication service and click *Refresh Trusted Forests*.

8 UNDERSTANDING UNIT VIEWS WINDOWS

With unit access rights you can view the Unit Views windows. These windows display the units (power or target devices and appliances) that can be used to access power devices to perform an operation.

The four types of Units windows, accessed by clicking tabs and side bar links, are as follows:

- All Appliances windows: List all managed appliances.
- Appliance Type windows: List all managed appliances of a particular type (for example, an Avocent® Power Management (PM) 3000 Distribution Unit with 24-outlets). The Appliance Type links in the side bar are listed under Appliances - All.

  An appliance type is only listed in the side bar if an appliance of that type is added to the Rack Power Manager software database and the user has access to it. For example, if a PM 3000 24-outlet PDU has not been added, that type does not appear in the side bar.
- Target Device windows: List all receptacles under a power device.
- Mixed View windows: Contain managed appliances, target devices or both. The following links in the side bar open mixed 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.

The units in these windows can be selected either by enabling or disabling the checkbox next to the name of each unit or by clicking the checkbox in the column header to select all the units displayed in the window.

NOTE: If the list of units spans more than one window, only the units on the current page are selected. See Using the Customize link in windows on page 21.

If you click any header in the table, an arrow appears beside the column name. Clicking the arrow again reverses the order of the items in the list. In the Version column, you can also hover your mouse cursor over each version to display when the firmware version was retrieved.

Any Units window that contains managed appliances can also be viewed using the topology feature, which displays a hierarchical structure. See Topology View on page 78.

In order to add Units windows using plug-ins, see the Avocent® DSView™ and Rack Power Manager Software Plug-in Technical Bulletin.

For more information, see the following:

- Using the Side Bar on page 19
- About Access Rights on page 100

8.1 Units Views Window Fields

The following fields may appear in Units windows. You can enable or disable a field using the Customize link. See Using the Customize link in windows on page 21.

- Name in Appliance - Name of the unit as defined in the appliance. Click 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 80.
- Status - Current activity level of a unit. The following table lists and describes the possible values.

Table 8.1 Unit Status Values

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 can 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 can be initiated. Although a unit may have multiple actions that can be performed, only one action is 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 target devices 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 Avocent® DSView™ and Rack Power Manager Software Plug-in Technical Bulletin for details.		

- Site - See Site, Department and Location Groups on page 115.
- Browser URL - URL that can be used to access a target device, Avocent® EVR 1500 environmental monitor and control appliance or a generic appliance. This field is 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 appear instead of the place holder names (Custom Field 1, Custom Field 2 and so on). See Custom Fields on page 116.
- Department - See Site, Department and Location Groups on page 115.
- 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 115.
- Model Number - See Unit Properties on page 95.

- Part Number - See Unit Properties on page 95.
- 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 95.
- Serial Number - See Unit Properties on page 95.
- Telnet Port - Port number used for a Telnet connection to a target device. See Unit Properties on page 95.
- Visibility - Whether to display (Show) or not display (Hide) a unit in the Units windows. See Showing and hiding units on page 77.
- 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 and can be changed from the Operations menu.
- MAC Address - Lists the appliance's MAC address; this information is gathered during enrollment and periodically through the plug-in maintenance task if the unit is enrolled. For information on adding or removing this column, see Using the Customize link in windows on page 21.

NOTE: The MAC address column is only available for the Server Tech Sentry 3 and 4 PDU, RPC-2000 PDU and RPC-1000 PDU, APC MasterSwitch RPDU Support and Liebert® GXT4™ UPS device.

For more information, see the following:

- Adding Units on page 83
- Managed Appliance Settings on page 102

8.1.1 Accessing the Unit Views windows

The Unit Views windows can be accessed using one of the following methods:

- Click the *Units* tab, and in the side bar, click *Appliances*.
- In the Appliances - All window, in the side bar, click one of the appliance type links.
- In the Appliances window, click the *Units* tab to display a list of recently accessed units.
- In the side bar, click *Recently Accessed*.
- Click the *Units* tab to display units by groupings (if available) and in the side bar, click the applicable link to open the associated window (*Sites, Departments, Locations* or *Custom Field Labels*).

8.1.2 Showing and hiding units

Hiding units removes units from the window, but does not remove the units from the Rack Power Manager software system. See Accessing the Unit Views windows on page 77.

To hide a unit:

1. Click the *Units* tab, and from a Unit Views window, click *Customize*.
2. In the Unit Views Customization Available Fields column, click *Visibility* and click *Add* to move Visibility to the Fields to Show column.
3. Enable the Show hidden items checkbox to display hidden units in the Unit Views Customization window with a transparent icon.
4. Click *Save* and *Close* and in the window with the Visibility column, click *Hide* for each unit.

NOTE: The display of the selected unit is powered off in the Unit Views window if *Show hidden items* is not selected in the Unit Views Customization window. If *Show hidden items* is selected, the hidden unit appears with a transparent icon.

To hide multiple units with one operation:

1. Click the *Units* tab, and from a Unit Views window, click the checkbox of the units to be hidden.
2. Click *Operations*, and from the drop-down menu, select *Hide Units*.

To show hidden units:

1. Click the *Units* tab, and from a Unit Views window, click *Customize*.
2. In the Units View Customization window, click *Visibility* in the Available Fields column and click *Add*.
3. Click *Show hidden items*, click *Save* and *Close*.
4. In the Units View window containing the hidden items and the Visibility column (hidden items have a transparent icon and the Visibility field contain Show), click *Show* in the Visibility column for the units to be displayed. The unit is made visible, the icon is no longer transparent and the Visibility field changes to Hide.

8.2 Topology View

From the Units tab, the Topology link allows you to access Unit Views windows that contain managed appliances. The topology view, which can be enabled or disabled, is a series of parent-child hierarchies. A parent is a managed appliance and children can be target devices, cascaded 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 Unit Views window that contains appliances, an arrow appears next to each appliance. The arrow can be used to expand (open) an appliance window to display all the appliance ports in a Port column next to the Name column. The port value can be the port number on the appliance, the port number on a cascaded switch or the socket number on a cascaded power device (for example, A1). The default setting for 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 bar. If the arrow is pointing right, clicking it causes the children to be displayed (expands the item). If the arrow is pointing down, clicking it causes the children to be hidden (collapses the item).

If a port has a cascaded switch or power control device attached, the unit name for that port includes an arrow that can be used to expand or 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 cascaded switch that do not have units attached are also listed. The Status column indicates No Device Attached and the Type column indicates the default valid connection type for that port. The Action column indicates Attach Device. See the procedure in this section for how to attach a device from this link.

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

The Select All checkbox at the top of the list only selects displayed items on the current window. 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 window value applies to appliances and children even if the display is collapsed and the children are not visible. You can also specify that the topology view expand automatically when the *Topology* button is clicked.

If you filter the display and a child matches the filter criteria, the parents automatically open. If only an appliance matches the filter criteria, the appliance is closed (unless the Expand View Automatically option is enabled).

For more information, see the following:

- Filtering information in a window on page 20
- Accessing the Unit Views windows on page 77
- Using the Customize link in windows on page 21

To enable or disable a topology view:

In a Unit Views window, click *Topology*.

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

8.3 Multiple Operations from a Unit Views Window

From a Unit Views window, you can delete one or more units (see Deleting Units on page 86) or assign access rights for one or more units (see About Access Rights on page 100).

You can also use the Operations button/menu to initiate any of the following actions on one or more units:

- Hide units from view, see Showing and hiding units on page 77
- Show version, see Managed Appliance Settings on page 102
- Push or pull names to or from the appliance, see Name Synchronization (Push and Pull) on page 87
- Wall power on, off or cycle, see Power Device Sockets on page 111
- Change unit properties, see Unit Properties on page 95

Custom operations that are defined in plug-ins can also be listed in the Operations menu.

A given action is available only if at least one of the selected units supports the action. If a selected unit does not support the operation, it is reported in the Operation Results window.

When one of these multiple unit operations is initiated and confirmed (if needed), a system task is created that performs the operation on each unit. The Multiple Unit Operation window indicates the operation is submitted and a link directs you to the Operations Results window for the task.

To initiate and view results using multiple unit operations from a Unit Views window:

1. From a Unit Views window, initiate the multiple unit operation as described previously, and if prompted, confirm the operation.
2. In the Multiple Unit Operation window, select *Click here to view results.*

   -or-

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

The Operations Results window lists all multiple unit operations and any unit tasks that have been initiated. The entry for each operation includes the name, start and end dates and status. See Using the Tasks Window on page 179.

NOTE: At any time, you can click the *Units* tab and click *Operation Results* in the side bar to access this window.

To view the results for an individual operation:

In the Operation Results window, click the name (for example, *Status*) and click *Close*.

8.4 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 can 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 you have power control rights. In this case, you can turn on, turn off or cycle the power of the target device.
- Managed appliances - Name and type of the managed appliance. Also, depending on the type of managed appliance and the access rights you have for the managed appliance, tools are provided to:
  - Reboot
  - Upgrade the firmware
  - Resynchronize
  - Save or restore the last known good configuration or the current configuration
  - Save or restore the user database
  - Save and apply a configuration template

NOTE: Custom tools are also available as defined by the plug-ins.

The overview information for a single target device can be changed from a Unit Overview window. From a Units tab window, you can also change the type, icon and values for several target devices in one operation. This may be helpful when you want to assign the same values to several units.

For more information, see the following:

- Unit Properties on page 95
- Accessing the Unit Views windows on page 77
- Appliance Configuration Templates on page 93

Other types of Unit Overview windows may be supported by plug-ins; see the Avocent® DSView™ and Rack Power Manager Software Plug-in Technical Bulletin for more information.

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

1. Click the *Units* tab, and in the Appliances - All window containing appliances, click the name of an appliance.
2. In the Unit Overview window, enter a name for the managed appliance.

NOTE: The type cannot be changed.

3. Click *Save* and *Close*.

8.5 Unit Status Window

Units are filtered by selecting a status from the Filter menu. Each unit status is color-coded. The default setting is the filtered status Active Status, which displays only currently active units.

To use the Unit Status window:

1. Click the *Units* tab, and in the side bar, click *Unit Status*.
2. In the Unit Status window, select a status from the Filter menu.
3. Select how often the Unit Status is updated by selecting a time from the Interval menu.
4. Double-click the unit name or right-click the unit name and select *Show Unit Overview* to view the Unit Overview window.

This page intentionally left blank.

9 ADDING AND DELETING UNITS

Units can be added and deleted in the Rack Power Manager management software.

9.1 Adding Units

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

- 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 can also Flash upgrade a managed appliance and then configure the appliance. Managed appliance rights can be changed.

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.

The method for adding appliances to the Rack Power Manager software, depends on whether the appliance is a single managed appliance, a group of managed appliances (based on a range of IP addresses) or a generic appliance, which is not managed.

For more information, see the following:

- Accessing the Unit Views windows on page 77
- Adding a single managed appliance on page 84
- Adding managed appliances from a range or list of IP addresses on page 85
- Adding a generic appliance on page 86
- Automatic Inheritance for Group Memberships and Properties on page 90
- Appliance Configuration Templates on page 93
- About Access Rights on page 100

NOTE: IPv6 is not supported by all appliance models. See the Avocent® DSView™ and Rack Power Manager Software Plug-in Technical Bulletin for a list of specific appliance models that support IPv6.

9.1.1 Wizards that add units

From a Units window, a wizard is invoked to guide you through the process of adding managed appliances and target devices to the Rack Power Manager software system. The following types of units in the current Units window determine which wizard is invoked when you click *Add*:

- From the Appliances - All window, you can add managed appliances of any type. You cannot add target devices.
- From the Units window for a specific appliance type, such as a PM 3000 PDU, you can only add more appliances of that type (PM 3000 PDUs). You cannot add appliances of any other type or any target devices.
- From 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 the Accounting department units and click *Add*, the newly added unit is automatically added to the Accounting department.

9.1.2 Adding a single managed appliance

A single appliance can be added from the Unit Views window or from any appliance type window other than the Unit Views window.

In non-secure mode, the managed appliance can be added to multiple Rack Power Manager software systems.

For more information about the options that affect adding target devices connected to the appliance, see Topology Synchronization on page 89.

For appliances supported by a plug-in, the window content may differ; see the Avocent® DSView™ and Rack Power Manager Software Plug-in Technical Bulletin.

NOTE: The Enable secure mode checkbox does not appear when adding a PM 3000, which can only be added in Secure mode.

To add a single managed appliance:

1. Click the *Units* tab, in the Appliances - All window containing managed appliances, click *Add* to open the Add Appliance Wizard.

   -or-

   From an appliance type Unit Views window, click *Add*.

   -or-

   From any appliance type window other than the Unit Views window, click *Add* to open the Select Appliance Type window. Then select *Add a single appliance by type*, select a managed appliance from the product list and click *Next*.

2. In the Select Address Configuration of Appliance window, enter or verify the IP address of the appliance.

   -or-

   If the appliance has not been configured with an IP address, select *Appliance does not have an IP address assigned yet,* plug in the appliance, turn it on and complete the following steps.

   a. Enter or select the subnet mask (IPv4 only), gateway and prefix length (IPv6 only), then click *Next*.
   b. If you want the managed appliance to only be accessible by this Rack Power Manager software system, in the Select Options window, click the Enable secure mode checkbox.
   c. Then under *Allow target devices that contain default names to be added for these types of connections*, enable the checkboxes of one or more connection types and click *Next*.

NOTE: Any target devices that contain default names in the managed appliance and support the enabled connection type in the managed appliance are added to the Rack Power Manager software database.

3. Verify or select the SNMP Version, SNMPv1 or SNMPv3, and enter or select the SNMP parameters.

NOTE: These SNMP settings must match with the SNMP settings for the appliance. The Authentication password must match the authentication passphrase and the privacy password should match the privacy passphrase, otherwise the DSView™ software system cannot enroll the appliance or receive the trap.

4. If you want to apply a configuration template to the appliance, in the Apply Configuration Template window, select a template from the list and click *Next*.

   -or-

   Select *None* and click *Next*.

5. Click *Finish*.

9.1.3 Adding managed appliances from a range or list of IP addresses

Multiple managed appliances can be added to the Rack Power Manager software system using a range of IP addresses. In non-secure mode, managed appliances can be added to multiple Rack Power Manager software systems. For appliances that require Secure mode, the appliance enables Secure mode automatically.

NOTE: IPv4 and IPv6 addresses are always separated by either a comma (,) or a semi-colon (;).

For more information, see the following:

- Topology Synchronization on page 89
- Appliance Configuration Templates on page 93
- Accessing the Unit Views windows on page 77

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

1. Click the *Units* tab, and in the Unit Views - Appliances - All window with populated managed appliances, click *Add*.
2. From the Add Appliance Wizard, in the Select Add Unit Procedure window, enter IP addresses as a delimited list, click *Add multiple appliances* and click *Next*.

   -or-

   Enter an IP address range by clicking *Discover appliances on the network from an IPv4 address range or an IPv6 subnet* and clicking *Next*. Then select *Use IPv4 address range* and enter the starting and ending IP addresses or select *Use IPv6 subnet* and enter the IPv6 network prefix and click *Next*.

NOTE: After the Rack Power Manager software completes the search for managed appliances within the IP address range, the results are listed in the Select Appliances to Add window.

3. In the Appliances found list, select one or more managed appliances, click *Add* or *Remove* to move the managed appliances to/from the Appliances to Add list and click *Next*.

NOTE: For appliances that are supported by plug-ins, the window may differ; see the appropriate documentation.

4. Click *Enable secure mode* if you want the managed appliance to only be accessible by this Rack Power Manager software system and click *Next*.

5. After the selected managed appliances are added to the Rack Power Manager system, in the Apply Configuration Template window, select a template to apply to the appliance, click *Next* and *Finish*.

   -or-

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

9.1.4 Adding a generic appliance

Generic appliances and EVR 1500 environmental monitors do not support certificates and can be added to multiple Rack Power Manager software systems.

To add a generic appliance:

1. Click the *Units* tab and click *Add*.
2. From the Add Unit Wizard, in the Select Add Unit Procedure window, click *Add a single appliance* and click *Next*.
3. In the Select Appliance Type window, select *Generic* from the product list and click *Next*.
4. In the Configure Generic Appliance Settings window, enter the name, either the address or the fully qualified domain name, Telnet port and Web browser URL.
5. Click *Next* and *Finish*.

9.2 Deleting Units

Deleting a unit removes a power device or associated appliance from the Rack Power Manager software database and deletes all of its associated connections (power device sockets). Target devices that are no longer connected when you run the Resync Wizard can also be deleted.

For more information, see the following:

- Topology synchronization options in the Resync Wizard on page 90
- Power Devices on page 109
- Accessing the Unit Views windows on page 77

To delete a unit:

1. Click the *Units* tab.
2. In the Appliances - All window, click the checkbox of the units to be deleted.
3. Click *Delete* and confirm or cancel the deletion.

9.2.1 Automatically deleting attached units

For target devices exclusively managed by a single appliance, you can 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 - Global Properties tabs*.
2. In the side bar, click *Units*, and in the side bar, click *Delete*.

10 SYNCHRONIZING THE DATABASE AND UNIT NAMES

The Rack Power Manager software database can be synchronized with changes that occur on units.

10.1 Name Synchronization (Push and Pull)

The names of units (appliances, target devices and power devices) and their connections (power device sockets) are stored in the software database of the Rack Power Manager. Some units and connections also have a name stored in their associated, managed appliance. The names in the database can be synchronized with the names in the appliance by “pushing” names from the database to the appliance and/or “pulling” names from the appliance to the database.

When the name of a cascaded device is changed in the software database, the "push" operation updates the name of the cascaded device and/or its power device socket in the managing appliance.

When the name of a cascaded device or its power device socket is changed in the managed appliance, the "pull" operation updates the name of the cascaded device and/or its power device socket in the software database.

Synchronization can be performed manually or configured to run automatically at any time.

10.1.1 Synchronizing names manually

A name can be pushed or pulled manually from the Power Devices, Power Device Sockets and Units windows. For more information, see the following:

- Power Devices on page 109
- Power Device Sockets on page 111
- Accessing the Unit Views windows on page 77

The following table describes what occurs when a name pull operation is initiated.

Table 10.1 Manual Name Pull Operation Effects

WHEN PULL IS INITIATED FOR ONE OR MORE:	EFFECT
Appliance serial ports	The target device name is pulled from the appliance to update the target device name in the Rack Power Manager software database.
Power devices	The power device name is pulled from the appliance to update the power device name in the Rack Power Manager software database.
Power device sockets	The target device name is pulled from the appliance to update the target device name in the Rack Power Manager software database.

To initiate a name push operation from a Units window:

1. Click the *Units* tab and in the window, click the checkbox of one or more units.
2. Click *Operations*, and from the drop-down menu, select *Push Names to Appliance*.
3. In the Multiple Unit Operations window (with a link to the Operation Results window), see Multiple Operations from a Unit Views Window on page 79.

To initiate a name pull operation from a Units window:

1. Click the *Units* tab and in the window, click the checkbox of one or more units.
2. Click *Operations*, and from the drop-down menu, select *Pull Names from Appliance*.

3. In the Multiple Unit Operations window (with a link to the Operation Results window), see Multiple Operations from a Unit Views Window on page 79.

10.1.2 Synchronizing names automatically

In addition to manual push/pull synchronization, a name can be pushed or pulled automatically when a name is changed in the database. The following table describes the effects when the automatic name push operation is configured to take place when a name is changed in the database.

The automatic name pull operation can be configured to take place automatically when a name is changed in the appliance.

For more information, see the following:

- Power Devices on page 109
- Power Device Sockets on page 111

Table 10.2 Automatic Name Push/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 is pushed to the appliance or is 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 is pushed to the appliance for each appliance connection (for the connection type(s) enabled in the Automatic Name Push Properties window) or is 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 in the Rack Power Manager software database is pushed to the appliance or the power device name is 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 is pushed to the appliance or the target device name is 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 is pushed to each appliance for each appliance connection (for connection type(s) enabled in the Automatic Name Push Properties window) or the target device name is 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.

To enable or disable automatic name push:

1. Click the *System - Global Properties* tabs.
2. In the side bar, click *Units - Synchronization* and click *Auto Name Push*.
3. In the Automatic Name Push Properties window, enable or disable the Push Names from RPM to appliances automatically checkbox.
4. Enable the checkboxes of one or more appliance connection types and click *Save*.

NOTE: If the target device has a connection that matches the selected type, the name in the Rack Power Manager software is pushed to the appliance.

To enable or disable automatic name pull:

1. Click the *System - Global Properties* tabs.
2. In the side bar, click *Units - Synchronization* and *Auto Name Pull*.
3. In the Automatic Name Pull Properties window, enable the Pull Names from appliances to Rack Power Manager automatically checkbox.

   -or-

Disable the Pull Names from appliances to Rack Power Manager automatically checkbox and go to the last step.

4. For target devices with multiple connections, you can set the connection type priority by using the arrows to re-order the available types. This order determines which target device name is pulled from one or more appliances to update the Rack Power Manager software database. The name is pulled from only one appliance.
5. Click *Save*.

10.2 Topology Synchronization

The topology synchronization operation is used to update the Rack Power Manager software database when a change, such as adding or removing a power device, occurs in a managed appliance.

You can enable or disable automatic topology synchronization or control topology synchronization manually by doing the following:

- 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 window
- Scheduling or manually running the update topology task (see Task: Updating topology for selected units on page 187)

10.2.1 Automatic topology synchronization

NOTE: Automatic topology synchronization is not supported on some managed appliances, such as the LANDesk® Server Manager. Alternatively, you can schedule the update topology task to keep these appliances synchronized with the Rack Power Manager software. See Task: Updating topology for selected units on page 187.

To enable or disable automatic topology synchronization:

1. Click the *System - Global Properties* tabs.
2. In the side bar, click *Units*, and under Synchronization, click *Auto Topology Update*.
3. In the Automatic Topology Update Properties window, enable the Update RPM with topology changes from appliances automatically checkbox.

   -or-

   Disable the Update RPM with topology changes from appliances automatically checkbox and go to the last step.
4. Click *Save*.

10.2.2 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. This window is described in Adding Units on page 83.

Each of the options has a default value that can be changed.

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

1. Click the *System - Global Properties* tabs.

2. In the side bar, click *Wizard Defaults* and *Add Unit Wizard*.
3. In the Add Unit Wizard Default Properties window, click to enable the Enable secure mode checkbox (default), to ensure the unit is only accessible by this Rack Power Manager software system.

   -or-

   In non-secure mode, add the unit to multiple Rack Power Manager software systems.
4. If a target device has a default name, you can configure the default to add the name to the Rack Power Manager software database only if it supports specific connection types in the appliance.
5. Enable the checkboxes for the specific connection types and click *Save*.

10.2.3 Topology synchronization options in the Resync Wizard

The Select Resync Options window in the Resync Wizard allows you to specify the following topology synchronization options:

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

In the Resync Wizard Default Properties window, you can enable or disable any of the following actions and achieve the described result with the default setting.

Table 10.3 Resync Wizard Default Options

CHECKBOX NAME	ENABLED CHECKBOX RESULTS
Remove offline connections	Deletes any appliance connections that are reported as offline in the appliance from the Rack Power Manager software database. The Resync Wizard does not add offline connections to the Rack Power Manager software database.
Delete target devices that no longer have connections	Permanently deletes any target devices that no longer have connections from the Rack Power Manager software database.
Allow target devices with the same name to be merged into a single target device	Merges a connection to a target device in the appliance with one or more connections to an existing target device in the Rack Power Manager software database.
If a target device has a default name	Enables the supported connection types to add the target device to the Rack Power Manager software database.

Each of these options has a default value that can be changed. See more about this window in Resynchronizing units on page 175.

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

1. Click the *System - Global Properties* tabs.
2. In the side bar, click *Wizard Defaults* and click *Resync Wizard*.
3. In the Resync Wizard Default Properties window, enable or disable the applicable actions and click *Save*.

10.3 Automatic Inheritance for Group Memberships and Properties

New target devices can be allowed to inherit group memberships and also some properties from the appliances to which the target devices are attached.

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 inherit these group memberships from the appliance.

  Or, if you select *Do not inherit group membership*, properties are not inherited at this time because the new appliance does not yet have any properties assigned.

- When you use automatic topology synchronization, the Resync Wizard or the update topology task to discover recently attached target devices, the new target devices inherit group memberships and location, contacts, notes and custom field properties from the appliance.

For more information, see the following:

- Unit Properties on page 95
- Adding a single managed appliance on page 84
- Automatic topology synchronization on page 89
- Resynchronizing units on page 175
- Task: Updating topology for selected units on page 187

To enable automatic inheritance:

1. Click the *System - Global Properties* tabs.
2. In the side bar, click *Automatic Inheritance*, click the checkbox to allow inheritance and click *Save*.

This page intentionally left blank.

11 MANAGING UNITS

Managing units includes creating configuration templates, assigning properties to units, configuring infrastructure levels for devices, assigning access rights to users and user groups, configuring managed appliances, modifying individual power device settings, unit reports and assets and configuring tiered energy costs.

11.1 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 to apply the properties to other units. The following classifications are saved in appliance configuration templates:

- Personality data, such as an IP address, is specific to a single unit and is only applied during the operation to replace an appliance.
- Fixed data, such as within a PM 3000 PDU, is specific to the unit family and not to a single unit. Fixed unit data (such as session time-outs) is applied when applying or replacing an appliance configuration template.

You can also create appliance configuration templates that are specific to a single unit for later use. For example, you may want to create a template for the previous configuration or current configuration of an appliance/unit.

NOTE: For appliances that do not support appliance configuration templates, the related buttons and links are not displayed.

11.1.1 Saving appliance configuration templates

Saving an appliance configuration template generates a Rack Power Manager event.

After locating an appliance or unit in the Appliances - All window, you can click the checkbox or name of the appliance/unit to view or manage that unit. For more information, see Accessing the Unit Views windows on page 77.

To save an appliance configuration template:

NOTE: This procedure creates an appliance configuration template that can only be applied to any unit in the same family as the model unit.

1. Click the *Units* tab, and in a Unit Views window, select the appliance to be used as the model for the appliance configuration template.
2. In the Unit Overview window, click the *Save Configuration Template* icon or link.
3. From the Save Appliance Configuration Template Wizard, enter a name for the appliance configuration template and click *Next*.
4. In the Completed Successful window, click *Finish*.

To save the last known good or current configuration template:

NOTE: This procedure creates an appliance configuration template that can only be applied to the selected unit.

Click the *Units* tab, and in a Unit Views window, select the appliance to be saved as an appliance configuration template. Click the *Save Last Known Good Configuration Template* or *Save Current Configuration Template* icon or link.

-or-

Click the *Units* tab, and in a Unit Views window, click the checkbox of the appliance to be assigned the appliance configuration template. From the Operation menu, select *Save Last Known Good Configuration Template* or *Save Current Configuration Template*.

11.1.2 Modifying appliance configuration template properties

After locating an appliance or unit in the Appliances - All window, you can click the checkbox or name of the appliance/unit to view its properties or manage that unit.

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 - Appliance Files* tabs.
2. In the side bar, click *Configuration Template*.
3. Click the name of the template to view its properties, including the name, supported unit type, creation date and the unit that created the template.

   -or-

   With the properties displayed, enter a new name and click *Save*.

   -or-

   Click the checkbox of the templates and click *Delete*.
4. Click *Close*.

11.1.3 Applying appliance configuration templates

After locating an appliance or unit in the Units window, you can select the checkbox or name of the appliance/unit to view or manage that unit. For more information, see Accessing the Unit Views windows on page 77.

Applying appliance configuration templates generates a Rack Power Manager event.

To apply an appliance configuration template to a new appliance:

1. Click the *Units* tab, and in a Unit Views window, click the checkbox of the appliance to be assigned the appliance configuration template and in the Unit Overview window, click the *Apply Configuration Template* icon or link.

   -or-

   Click the *Units* tab, and in a Unit Views window, click the checkbox of the appliance to be assigned 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 and click *Save*.

   -or-

   Select *Apply Last Known Good Configuration Template*.

-or-

Select *Apply Current Configuration Template*.

3. In the Completed Successful window, click *Finish*.

   -or-

   See Adding Units on page 83 to apply the appliance configuration template during the Add Unit Wizard process.

To replace an appliance:

NOTE: Appliance replacement does not work in secure mode.

1. Click the *Units* tab, and in a Unit Views window, click the checkbox of the appliance to be assigned the appliance configuration template and in the Unit Overview window, click the *Appliance Replacement* icon or link.

   -or-

   Click the *Units* tab, and in a Unit Views window, click the checkbox of the appliance to be assigned the appliance configuration template. From the Operations menu, select *Appliance Replacement*.

2. Enter the IP address of the appliance to be replaced.
3. From the list, select the appliance configuration template you want to apply and click *Save*.
4. In the Completed Successful window, click *Finish*.

11.2 Unit Properties

A user with access rights can change the following properties of a unit:

- Overview - Specify the type and icon for a target device.
- Identity - Quickly identify information about a unit.
- Location (site, department and location) - Identify where a unit is. See Site, Department and Location Groups on page 115.
- Contacts - Identify the primary and secondary contacts, such as the people to notify if an issue or question arises about a particular unit.
- Custom fields - Specify information in ten custom fields. For example, you can define custom fields such as Program Manager, Building Number and so on. See Custom Fields on page 116.
- Notes - Include notes.
- Network - Include network information.

You can specify which properties are displayed in a Units View window by using the *Customize* link. See Using the Customize link in windows on page 21.

A single property for one or more units can be changed at a time, or you can change multiple properties for multiple units by using the Properties - Bulk Edit operation.

After locating an appliance or unit in the Units View window, you can select the checkbox or name of the appliance/unit to manage or review that unit. For more information, see Accessing the Unit Views windows on page 77.

To change multiple properties for multiple units using the Properties - Bulk Edit operation:

1. Click the *Units* tab, and in the Unit Views window, click the checkboxes of the appliances or target devices to be edited.
2. Click *Operations*, and from the drop-down menu, select *Properties - Bulk Edit*.
3. In the Bulk Edit Unit Properties window, scroll to view the columns, specify the columns to be displayed by clicking *Select Columns* or selecting the properties to be displayed, click *Add* and *Save*.

NOTE: The unit names are displayed in the left column and the properties are displayed in the adjacent columns.

4. Enter the values in the appropriate fields.

NOTE: To quickly navigate the spreadsheet, press the Tab **and** Shift + Tab **keys to move right and left and press the** Enter **and** Shift + Enter **keys 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. Click the *Units* tab, and in the Appliances - All window, click the appliance's name.
2. In the side bar, click *Properties*.
3. In the Unit Identification Properties window, enter a part number, serial number, model number and/or asset tag number.
4. Click *Save* and *Close*.

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. Click the *Units* tab, and in the Appliances - All window, click the appliance's name.
2. In the side bar, click *Properties* and *Location*.
3. In the Unit Location Properties window, enter or use the menus to select the site, department and/or location for the unit.
4. Click *Save* and *Close*.

To change the location properties for one or more units from a Unit Views window:

1. Click the *Units* tab, and in the Appliances - All window, click the applicable unit checkboxes.

NOTE: Units that do not support location properties are not affected.

2. Click *Operations,* and from the drop-down menu, select *Properties*.
3. In the Multiple Unit Properties window, click *Location*.
4. Enter or use the menus to select the site, department and/or location for the units.
5. Click *Save* and *Close*.

To change the contact properties for a unit:

1. Click the *Units* tab, and in the Appliances - All window, click the appliance and in the side bar, click *Properties*.
2. In the side bar, click *Contacts,* and in the Unit Contacts window, enter the names and phone numbers of the primary and secondary contacts.
3. Click *Save* and *Close*.

To change the contact properties for one or more units from a Unit Views window:

1. Click the *Units* tab, and in the Appliances - All window, click the applicable unit checkboxes.

NOTE: Units that do not support location properties are not affected.

2. Click *Operations*, and from the drop-down menu, select *Properties*.
3. In the Multiple Unit Properties window, click *Primary Contact* and enter names and phone numbers for the primary contact.

   -or-

   Click *Secondary Contact* and enter names and phone numbers for the secondary contact.
4. Click *Save* and *Close*.

To change the custom fields for a unit:

1. Click the *Units* tab, and in the Unit Views window, click the appliance's name.
2. In the side bar, click *Properties - Custom Fields*.
3. In the Unit Custom Fields window, enter the information in each of the custom fields.
4. Click *Save* and *Close*.

To change the custom fields for one or more units from a Unit Views window:

1. Click the *Units* tab, and in the Unit Views window, click the applicable unit checkboxes.

NOTE: Units that do not support custom fields are not affected.

2. Click *Operations*, and from the drop-down menu, select *Properties*.
3. In the Multiple Unit Properties window, click *Custom Fields*.
4. Enter the information in each of the custom fields.
5. Click *Save* and *Close*.

To change the note properties for a unit:

1. Click the *Units* tab, and in the Appliances - All window, click the appliance or target device name.
2. In the side bar, click *Properties* and *Notes*.
3. In the Unit Notes window, enter description, accounting and comment information.
4. Click *Save* and *Close*.

To change the note properties for one or more units from a Unit Views window:

1. Click the *Units* tab, and in the Appliances - All window, click the applicable unit checkboxes.

NOTE: Units that do not support note properties are not affected.

2. Click *Operations,* and from the drop-down menu, select *Properties*.
3. In the Multiple Unit Properties window, click *Notes*.
4. In the Unit Notes window, enter description, accounting and comment information.
5. Click *Save* and *Close*.

To change the network properties for a target device:

NOTE: Defining incorrect information for these properties may cause network connection errors.

1. Click the *Units* tab, and in the Appliances - All window with populated target devices, click the target device name.
2. In the side bar, click *Properties* and *Network*.
3. In the Unit Network Properties window, enter the address or the fully qualified domain name for the target device.
4. Enter the Telnet port number for Telnet connections to the target device.

NOTE: If this field is left blank, Telnet is not enabled for the target device.

5. Enter the URL for a web browser connection to the target device.
6. Select the Rack Power Manager server that is in charge of the target device.
7. Click *Save* and *Close*.

To change the network properties for a managed appliance:

1. Click the *Units* tab, and in the Appliances - All window with populated appliances, click the appliance name.
2. In the side bar, click *Properties* and *Network*.
3. In the Unit Network Properties window, enter the address or the fully qualified domain name.

NOTE: If you are changing the IP address of the appliance, change the IP address in the Appliance Network Settings window before changing it in the Unit Network Properties window. See Managed Appliance Settings on page 102.

4. Select the Rack Power Manager server to be in charge of the managed appliance.
5. Click *Save* and *Close*.

To change the Rack Power Manager server network property for one or more units from a Unit Views window:

1. Click the *Units* tab, and in the Appliances - All window, click the checkboxes of the units to be updated.

NOTE: Units that do not support note properties are not affected.

2. Click *Operations,* and from the drop-down menu, select *Properties*.
3. In the Multiple Unit Properties window, click *Network* and select the Rack Power Manager server to be in charge of the units.
4. Click *Save* and *Close*.

11.3 Unit Overview Settings

Any level of the infrastructure (company, data center, row of racks or racks), individual power and environmental devices can be configured. Specific threshold values can also be configured for total current, power consumption, internal/external temperature, relative humidity, phase/circuit current and

phase/circuit power consumption in the fields provided. The following values are available for each category:

- 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 threshold, 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 threshold, 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.

When a threshold is met, a software event is generated.

To view the status:

1. Click the *Units* -*Units* tabs.
2. In the side bar, click *Power Manager* or *Infrastructure*.
3. Click an infrastructure level or power device.
4. From the Unit Overview window, in the side bar, click *Power Manager*.
5. In the side bar, click *Status* to display the most recent power monitoring data for the unit and click *Close*.

NOTE: The displayed data is based on the selected unit and can include current, power and voltage for each phase, total current, power and voltage, humidity and temperature. Exceeded thresholds are also displayed.

To configure power units:

1. Click the *Units* -*Units* tabs.
2. In the side bar, click *Power Manager* or *Infrastructure*.
3. Click an infrastructure level or power device.
4. From the Unit Overview window, in the side bar, click *Power Manager* - *Settings* - *Configuration*.
5. If you selected an infrastructure level other than Data Center, enter the maximum power consumption in watts.

   -or-

   If you selected a *Data Center*, enter the cost per kilowatt hour.

NOTE: This information is required for data center cost reports.

   -or-

   If you selected a power device to display configuration data received from the power device, 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.

NOTE: The appropriate values for these settings can be found on the label of the power device hardware. See the installer/user guide of the power device for more information.

6. Click *Save* and *Close*.

To modify thresholds for rows of racks, racks or power devices:

1. Click the *Units -Units* tabs.
2. In the side bar, click *Power Manager* or *Infrastructure*.
3. Modify the thresholds for a unit by clicking the name of a row of racks, rack or power device. Then from the Unit Overview window, in the side bar, click *Power Manager*.

   -or-

   Modify the thresholds for multiple units of the same type simultaneously by selecting the row of racks, rack or power device from the list and from the Operations menu, clicking *Configure Thresholds*.
4. In the fields, specify the threshold values for total current, power consumption, internal/external temperature, relative humidity, phase/circuit current and phase/circuit power consumption.
5. Click *Submit* and *Close*.

To monitor consistency (racks and rows of racks):

1. Click the *Units -Units* tabs.
2. In the side bar, click *Power Manager* or *Infrastructure*.
3. Click an infrastructure level or power device.
4. From the Unit Overview window, in the side bar, click *Power Manager - Monitoring Consistency*.
5. From the menu, select the Rack Power Manager server to monitor all members of the selected rack or row of racks and click *Save*.

To configure data monitoring for racks:

NOTE: For PM 2000 and PM 3000 PDUs, the PDU shown on the Unit Overview page has three levels. The top level acts like a container, the second level shows the PDU and the third level shows the outlets under the PDU. When configuring data monitoring for PM 2000 and PM 3000 PDUs, do not add the first level container; only add the second level (PDU) or/and third level (outlets) to the rack.

1. Click the *Units -Units* tabs.
2. In the side bar, click *Power Manager* or *Infrastructure*.
3. Click an infrastructure level or power device.
4. From the Unit Overview window, in the side bar, click *Power Manager - Monitoring*.
5. Select the units you want to monitor and click *Add*.

   -or-

   Select the units you do not want to monitor and click *Remove*.

11.4 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 can specify if a user or members of a user group are allowed to:

- View the unit in a Units 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 can specify if a user or members of a user group are allowed to:

- View the appliance in the Units windows (this right is enabled automatically if any other access right for the managed appliance is enabled)
- Flash upgrade appliance - see Upgrading firmware on page 174
- Configure unit settings - see Managed Appliance Settings on page 102
- Configure appliance local user accounts

For example, you can allow users to configure settings on a managed appliance, but restrict them from rebooting and disconnecting sessions on it. Access rights can also be specified for all units in the Rack Power Manager software system or for a specific unit.

The default setting allows supported embedded units to have the same access rights as generic units.

11.4.1 How access rights can be assigned

Access/control rights can be assigned from the unit, unit group, user or user group perspectives as follows:

- From the unit perspective, you can 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.
- From a unit group perspective, you can assign access control rights the same as for a unit, except all units that belong to the selected unit group are affected.
- From a user perspective, you can 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.
- From a user group perspective, you can assign access control rights the same as for a user, except all users who are members of the selected user group will be affected.

For more information, see the following:

- Changing the unit group properties on page 122
- User Access Rights on page 146
- User Group Access Rights on page 153

11.5 Unit Access Rights

The Unit Access Rights window contains the current list of users/user groups. When a user/user group is added to the list, default access rights are displayed. Rack Power Manager software administrators can assign unit access rights.

After locating an appliance or unit in the Unit Views window, you can select its checkbox or name to view or manage it.

When assigning a user or user group from the User and User Groups list, enable or disable a checkbox in the Access Rights table for each access right. The following table describes the function of the access rights options.

Table 11.1 Access Rights Options

OPTION	DESCRIPTION
Allow	Access right is allowed for the user/group
Deny	Access right is denied for the user/group.
Inherit	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 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.

For more information, see Accessing the Unit Views windows on page 77.

To add or remove access rights from a Unit Views window:

1. Click the *Users - Access Rights* tabs.
2. From the Access Rights window, assign access rights to User/user groups and Unit/Unit Groups combinations.
3. From the User and User Groups list, select a user or user group, then click to enable or disable a checkbox in the Access Rights table for each access right. To disable the inherit functionality, uncheck the Inherit checkbox.

NOTE: 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 *Close*.

11.6 Managed Appliance Settings

After locating an appliance or unit in the Units window, you can select the checkbox or name of the appliance/unit to manage or review that unit. For more information, see Accessing the Unit Views windows on page 77.

NOTE: When changing the network settings of a managed appliance, the MAC address cannot be changed.

To change the network settings of a managed appliance:

1. Click the *Units* tab and in a Unit Views window, click the appliance name.
2. In the side bar, click *Appliance Settings* and click *Network*, then in the Appliance Network Settings window, do one of the following:
   - Enter IP address, subnet and gateway.

NOTE: If you change the appliance IP address in the Appliance Network Settings window, also change the address in the Unit Network Properties window. See Unit Properties on page 95. Always make IP address changes in the Appliance Network Settings window before making changes in the Unit Network Properties window.

   - Specify LAN speed. This network setting does not appear for CPS appliances.
   - Enable or disable DHCP or BootP (KVM switches).
   - Enable or disable ICMP ping reply.
3. Click *Save* and *Close*.

To change the IP addresses of Rack Power Manager servers used for managed appliance authentication:

1. Click the *Units* tab and in a Unit Views window, click the appliance name.

2. In the side bar, click *Appliance Settings,* then click *Authentication Servers*.
3. In the Appliance Authentication Servers Settings window, enter IP addresses for up to four Rack Power Manager servers the managed appliance will use for authentication.
4. Click *Save* and *Close*.

To display version information for one or more managed appliances from a Units window:

1. Click the *Units* tab and in a Unit Views window, click the checkbox of the applicable units.
2. Click *Operations*, and from the drop-down menu, select *Show Versions*.
3. In the Multiple Unit Operation window, click the link to view the following information.

Table 11.2 Version Information

FIELD	DESCRIPTION
Results window	Includes unit name, type and when the version information retrieval began.
Appliance Version field	Contains the main firmware version; if a unit did not or cannot report a firmware version, dashes are displayed.
Boot Version field	Contains the boot firmware version. If a unit does not support a boot version but has an appliance version, N/A is displayed and dashes are displayed if a unit does not support either appliance or boot firmware.
Status field	Indicates the result of the display (for example, Show Versions complete or Show Versions not supported).

See Multiple Operations from a Unit Views Window on page 79.

To display version information for a managed appliance:

1. Click the *Units* tab and in a Unit Views window, click an appliance name.
2. In the side bar, click *Appliance Settings - Versions*.
3. Click *Close*.

To enable or disable secure mode on an appliance:

1. Click the *Units* tab and in a Unit Views window, click the checkbox of the units.
2. Click *Operations*, and from the drop-down menu, select *Enable Secure Mode*.

11.7 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 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 bar:

- System - Enables/disables SNMP. When you enable SNMP, the managed appliance logs 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 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. SNMP traps can also be configured from a system task.

After locating an appliance or unit in the Unit Views window, you can select the checkbox or name of the appliance/unit to manage or review that unit.

For more information, see the following:

- Displaying the Event Log on page 192
- Task: Configuring SNMP trap settings on a managed appliance on page 182
- Accessing the Unit Views windows on page 77

To change SNMP settings for a managed appliance:

1. Click the *Units* tab and in a Unit Views window, click the appliance name.
2. In the side bar, click *Appliance Settings* X and *SNMP*.
3. In the Appliance SNMP System Settings window, enable SNMP by selecting *Enabled* in the Enable SNMP menu, and if desired, change the name and description of the managed appliance, enter a contact and click *Save*.
4. If enabling SNMP manager settings, in the side bar, click *Managers*, and in the Appliance SNMP Manager Settings window, enter the IP addresses for up to four SNMP managers and click *Save*.
5. If specifying SNMP community settings, in the side bar, click *Community*, and in the Appliance SNMP Community Settings window, enter the SNMP community names for reading, writing and SNMP traps and click *Save*.
6. If specifying SNMP destination settings, in the side bar, click *Destinations,* and in the Appliance SNMP Destination Settings window, enter the IP addresses for up to four SNMP destinations and click *Save*.
7. If enabling or disabling SNMP traps, in the side bar, click *Traps*, and in the Appliance SNMP Trap Settings window, select *Enabled* to turn a trap on; *Disabled* to turn a trap off.

   -or-

   Select *Enable All* to turn all traps on; *Disable All* to turn all traps off.
8. Click *Save* and *Close*.

11.8 Bulk Configuration of Individual Settings

Bulk configuration allows administrators to select, view and modify individual settings for selected power devices. Information that can be modified is as follows:

- Name
- Part number
- Model number
- Serial number
- Asset tag number
- Primary contact
- Primary contact phone

- Secondary contact
- Secondary contact phone
- Custom fields 1-10

To modify individual power device settings:

1. Click the *Units* tab and click the power device's name.
2. From the *Operations* tab, select *Properties - Bulk Edit* and edit the settings.
3. Click *Save* or *Close*.

11.9 Reports and Infrastructure Hierarchy

The Rack Power Manager plug-in allows you to log all historical data for power and environmental devices (which are usually contained in racks). In order to use the reporting capabilities in Rack Power Manager, you must organize the units in an infrastructure hierarchy containing up to four of the following levels:

- Company
- Data Center
- Row of Racks
- Rack

Power manager reports can be created for all the infrastructure levels. Reports can be created for total power consumption, threshold events, power consumption per phase and total energy consumption, temperature and energy costs for each unit. Comparative reports are also provided with historical data of multiple units. For other types of reports, see Custom Group Reports and Scheduled Tasks on page 125.

11.9.1 Prerequisites

Before power data can be collected, the following must be complete:

- An infrastructure with power and/or environmental devices must be configured. The Power Manager link in the side bar displays the organization configured from the Infrastructure window.
- The voltage and power factor must be configured for each power device to collect data. See Unit Overview Settings on page 98.
- Data monitoring must be enabled in the units from the Infrastructure window.

In an infrastructure hierarchy, each rack contains power and/or environmental devices. For Rack Power Manager software systems consisting of hub and spoke servers, a row of racks and the racks and devices it contains must be assigned to the same Rack Power Manager 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.

11.9.2 Power manager plug-in settings

The following settings are globally applied to the Rack Power Manager server.

To modify the power manager plug-in settings:

1. Click the *System - Plug-ins* tabs.
2. In the list of plug-ins, click *Power Manager*.
3. In the side bar, click *Settings*.

4. Under Unit Nomenclature, specify the temperature unit, power 3-phase description and currency to be used in power reports.
5. Under Plug-In Standard Properties, specify the interval at which power monitoring data is collected and click *Save*.

11.9.3 Asset reports

The following are types of asset reports, which can be viewed as a pie chart, bar chart or table:

- 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.

Available reports vary based on the type of unit selected and what data each unit supports. If multiple charts are tiled in the window, you can change the size of the charts by dragging the triangle on the size bar to the right or left.

To view asset reports:

1. Click the *Reports* - *Asset* tabs.
2. On the Asset Report window, select one of the report type icons.
3. Click *Export Data* to export and save the report data as a .csv file.
4. Click *Schedule Export Task* to create a task that exports Asset Report data at specific intervals. See Task: Exporting an Asset Report to a .csv file on page 184.

To print a report in a printer-friendly format:

Click the printer icon.

11.9.4 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* - *Units* tabs.
2. In the side bar, click *Power Manager* or *Infrastructure*.
3. Click an infrastructure or power or environmental device name.
4. From the Unit Overview window, in the side bar, click *Power Manager*.
5. Click *Reports* and select a report from the Reports menu.
6. Enter the date and time range for the report in the fields provided and click *Run Report*.
7. View the line graph, click the bar chart or table view icons to change the view or click the interpolation icon to show only data points.

NOTE: If applicable, you can also 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.

NOTE: Cost is calculated based on the cost per kilowatt hour rate configured for the data center.

9. Click *Export Data* and *Close*.

To view status reports:

1. Click the *Reports - Power* tabs.
2. From the Reports menu (displayed in table format), select *PDU* or *PDU Power Range*.
3. Click *Export Data* and *Close*.

11.9.5 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 - Schedule Reports* tabs.
2. Click *Add* and enter the schedule information.
3. Click *Save* and *Close*.

To remove a scheduled report:

1. Click the *System - Schedule Reports* tabs.
2. Click the report checkbox and click *Delete*.
3. Click *Save* and *Close*.

To run a report:

1. Click the *System - Schedule Reports* tabs.
2. Click the report checkbox and click *Run Now*.

To modify a scheduled report:

1. Click the *System - Schedule Reports* tabs.
2. Click the task and make the modifications/updates.
3. Click *Save* and *Close*.

11.9.6 Segregated Temperature Reading Reports

Two separate reports are available for displaying internal and external temperatures for selected PDUs, racks or rows of racks.

NOTE: Currently, segregation of internal and external temperature is only performed for PM 2000 and PM 3000 PDUs. For all other PDUs, only external temperature reports are applicable.

To create a report for an internal or external temperature for individual PDUs:

1. Click the *Units* tab and click the desired *PDU*.
2. Click *Rack Power Manager* and click *Reports*.
3. From the drop-down menu, select either *Internal* or *External Temperature Report*.
4. Select the desired date/time and click *Close*.

   -or-

   Click *Run Report*.

To create comparative temperature reports:

1. Click the *Reports - Power* tabs.
2. From the Reports drop-down menu, select either *Comparative Internal* or *External temperature* report.
3. Select the PDU, rack or row of racks for the report.
4. Select the desired date/time and click *Close*.

   -or-

   Click *Run Report*.

11.10 Tiered Energy Cost Setting

When calculating energy costs, peak hours and off peak hours cannot overlap, and the off peak hour energy rate cannot be more than the peak hour energy rate.

To modify the peak/off peak hour rate and time:

1. Click the *Units* tab and select the data center from the side bar.
2. Click *Power Manager - Settings - Configuration* and enter the Maximum Power Consumption.
3. Enter the Peak Rate Cost per kWh and set the desired timeframe.

   -or-

   Click the Off Peak Rate Same as Peak Rate checkbox, enter the Off Peak Rate Cost per kWh and set the desired timeframe.

4. Click *Save* and *Close*.

12 POWER DEVICES AND SOCKETS

PDUs can be connected serially through an ACS Advanced Console Server or KVM switch. See Supported Power Devices and Appliances on page 2 for information about the power device types and models that are supported on Avocent® or Vertiv™ appliances.

12.1 Power Devices

After locating an appliance or unit in the Unit Views window, you can select the checkbox or name of the appliance/unit to manage or review that unit. For more information, see Accessing the Unit Views windows on page 77 and Synchronizing the Database and Unit Names on page 87.

To display a list of power devices attached to an appliance or initiate a push/pull names operation:

1. Click the *Units* tab, and in the Appliances- All window, click the name of the appliance.
2. In the side bar, click *Appliance Settings*, then click *Ports* and *Power devices*.
3. In the Power Devices window, click the checkbox of the applicable devices.
4. For a pull operation, click *Pull Names*.

   -or-

   For a push operation, click *Push Names*.
5. Click *Close*.

12.1.1 Customizing the Power Devices Attached to Appliance window

The display fields and content of the Power Devices Attached to Appliance window differ according to the power device type and models. For details, see the product documentation. Click the *Customize* link to add or remove fields in the display; see Using the Customize link in windows on page 21.

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 - Status of the power device

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. Click the *Units* tab, and in the Appliances - All window, click the name of the appliance.
2. From the Unit Overview window, under Tools, click *Manage Power Devices*.
3. From the Power Management Wizard, in the Select Action window, enable the Add Power Devices radio button and click *Next*.

   -or-

   Enable the Remove Power Devices radio button to remove a power device and click *Next*.

NOTE: The Power Management Wizard is displayed by clicking *Appliance Settings - Ports - Power Devices - Manage* in the side bar.

4. From the Select Parameters window, in the Port menu, select the port where the power device is to be added or removed.

-or-

Select the physical port number in the Port menu for a serial console appliance.

-or-

Select the appropriate port value for an appliance supported by a plug-in.

5. If you are adding a power device, in the Power Device Type menu, select the type.
6. Click *Next*, and in the Completed Successful window, click *Finish*.

To change power device settings:

1. Click the *Units* tab, and in the Appliances - All window, click the name of the appliance.
2. In the side bar, click *Appliance Settings*, *Ports* and *Power devices*.
3. In the Power Devices Attached to Appliance window, click the name of a power device and in the Power Device Settings window, modify, enter or select new values in the editable fields.

NOTE: If you change the appliance name and the automatic name pull feature is enabled, see for the effect.

4. Select a voltage and enter a power factor (required to monitor power data on a power device).
5. Click *Save* and *Close*.
6. In the Power Devices Attached to Appliances window, click *Close*.

Upgrading the firmware of a Cyclades™ power device

To upgrade the firmware of a Cyclades power device:

If you want to use the Upgrade Firmware wizard from a Unit Overview window, see Upgrading firmware on page 174 for more information.

-or-

If you want to upgrade using the Task wizard, follow the instructions in Task: Updating the firmware of an appliance type on page 185. Then, in the Select Task to Add window, select *Upgrade firmware of selected units*. In the Select Unit Type window, you can select by product family (Cyclades Power Devices) or unit type (specific power device type).

If multiple power devices are installed in a daisy chain configuration, the most remote power device is upgraded first.

12.2 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 (IPDUs).

After locating a power device or an associated appliance in the Unit Views window, you can click the checkbox or name of the appliance/unit to manage or review that unit. For more information, see Accessing the Unit Views windows on page 77.

To display power device input feed information:

1. Click the *Units* tab, and in the Appliances- All window, click the name of the appliance.
2. In the side bar, click *Appliance Settings* and *Ports*.

3. In the side bar, click *Power devices*.
4. In the Power Devices Attached to Appliance window, click the name of a power device.
5. In the side bar, click *Input Feeds*.

12.2.1 Customizing the Power Device Input Feeds window

The following fields can be displayed in the Power Device Input Feeds window. For field descriptions, see the product documentation. Click the *Customize* link to add or remove fields in the display. See Using the Customize link in windows on page 21.

- Input Feed Name
- Status - Unknown, on, off, cycling, pending off, pending on, pending cycle or no status
- Load
- Alarm Threshold - Sends a trap if the Load value reaches the Alarm Threshold value
- Load Max - Sends a trap if the Load value is greater than the Load Max value
- Load Min - Sends a trap if the Load value is less than the Load Min value

To change power device input feed information:

1. Click the *Units* tab, and in the Appliances- All window, click the name of the appliance.
2. In the side bar, click *Appliance Settings*, click *Ports* and *Power devices*.
3. In the Power Devices Attached to Appliance window, click the name of a power device.
4. In the side bar, click *Input Feeds*.
5. In the Power Device Input Feeds window, click an input feed name.
6. In the Power Device Input Feed Settings window, modify, enter or select new values in the editable fields.
7. Click *Save* and *Close*.
8. In the Power Device Sockets window, click *Close*.
9. In the Power Devices Attached to Appliance window, click *Close*.

12.3 Power Device Sockets

After locating an appliance or unit in the Unit Views window, you can select the checkbox or name of the appliance/unit to manage or review that unit. For more information, see Accessing the Unit Views windows on page 77 and Name Synchronization (Push and Pull) on page 87.

To display information about power device sockets or initiate a push/pull operation:

1. Click the *Units* tab, and in the Appliances- All window, click the name of the appliance.
2. In the side bar, click *Appliance Settings*, then click *Ports* and *Power devices*.
3. In the Power Devices Attached to Appliance window, click the name of a power device.
4. In the side bar, click *Sockets*.

NOTE: 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 is displayed in the top left corner of the Power Device Sockets window. Click the icon to reboot the managed appliance.

5. In the Power Device Sockets window, click the checkboxes of the applicable units and click *Pull Name* or *Push Name*.

12.3.1 Customizing the Power Device Sockets window

The display fields and content of the Power Device Sockets window 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 21.

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. Click the *Units* tab, and in the Appliances- All window, click the name of the appliance.
2. In the side bar, click *Appliance Settings*, click *Ports* and *Power devices*.
3. In the Power Devices Attached to Appliance window, click the name of a power device.
4. In the side bar, click *Sockets*.
5. In the Power Device Sockets window, click a power device socket.
6. In the Power Device Socket Settings window, modify, enter or select new values in the editable fields.

NOTE: If you change the appliance name and the automatic name pull feature is enabled, see Synchronizing the Database and Unit Names on page 87 for effects.

7. Click *Save* and *Close*.
8. In the Power Device Sockets window, click *Close*.
9. In the Power Devices Attached to Appliance window, click *Close*.

12.4 Power Control of Devices Attached to Power Devices

The following are ways to turn on, turn off or power cycle a target device that is attached to a power device socket:

- From a Power Device Sockets window
- From a Unit Views window containing power devices
- From the Video Viewer or from the Telnet viewer

To control power from a Power Device Sockets window:

1. Click the *Units* tab, and in the Appliances - All window, click the appliance's name.
2. In the side bar, click *Appliance Settings*, click *Ports* and *Power devices*.
3. In the Power Devices Attached to Appliance window, click the name of a power device and click *Sockets*.
4. In the Power Device Sockets window, click the applicable power device socket checkboxes.
5. 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 reflects the state.

NOTE: For certain power device types and models, administrators can also lock or unlock the current state of a socket 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 Unit Views window:

1. Click the *Units* tab, and in the Appliances - All window, click the appliance's name.

NOTE: If any of the selected units are not power devices, the operation is ignored by them.

2. From the drop-down menu, click *Operations* and select *Wall Power On, Wall Power Off* or *Wall Power Cycle*.
3. In a Multiple Unit Operation window (containing a link to view results), see Multiple Operations from a Unit Views Window on page 79.

12.5 Power Operations

Power operations can be performed on a power device or rack.

To perform power operations on a power device or rack:

1. Click the *Units* tab and click *Power Manager* or *Infrastructure* in the side bar.
2. Click a power device or rack name, and in the Unit Overview window under Tools, click *Power Unit On*, *Power Unit Off* or *Power Cycle Unit*.

   -or-

   Click the checkbox of the power device or rack, click the *Operations* drop-down menu and select *Power Unit On, Power Unit Off* or *Power Cycle* Unit.

This page intentionally left blank.

13 GROUPING UNITS

The Rack Power Manager Explorer automatically groups managed appliances and targets by the type of appliance (PM 3000 24-outlet PDU, Liebert® MPH PDU). Target devices are automatically grouped by the type to which they are assigned.

You can also add and change the following types of groups:

- Sites
- Departments
- Locations
- Custom fields - Custom fields allow you to create groupings of units that can be accessed by all Rack Power Manager software users
- Personal and global unit groups - Global unit groups can be seen by all users; personal unit groups are visible only to the user who created the group

13.1 Site, Department and Location Groups

One or more site, department and location names, as well as associated units can be named. For example, you can 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. Names can have 1-64 characters.

Site, Department and/or Location columns can be included in a Unit Views window display using the Customize link. See Using the Customize link in windows on page 21.

To group units by site, department or location, first create a site/department/location and then associate units with it. The site/department/location must have at least one unit associated with it and the user must have access rights to the unit before the unit can be displayed in the side bar.

To add a site, department or location:

1. Click the *Units* tab and click *Sites*, *Departments* or *Locations*.
2. In the applicable window (Sites, Departments or Locations), click *Add*, enter a name and click *Add*.

NOTE: A site, department or location is not listed in the side bar until it is associated with a unit.

To delete a site, department or location:

1. Click the *Units* tab, and click *Sites*, *Departments* or *Locations*.
2. In the applicable window, click the checkbox of one or more sites, departments or locations.
3. Click *Delete*, and in the confirmation dialog box, confirm or cancel the deletion.

To change the name of a site, department or location:

1. Click the *Units* tab and click *Sites*, *Departments* or *Locations*.
2. In the applicable window, click the checkbox of one or more sites, departments or locations and enter a new name.
3. Click *Save* and *Close*.

To associate or change the association of an existing unit to a site, department or location:

1. Click the *Units* tab, and in the side bar, click the applicable links listed in the following table.

Table 13.1 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

2. When the corresponding window opens for the units you wish to associate with, change or remove from the association, click the name of a unit.
3. In the Unit Overview window, in the side bar, click *Properties* and *Location*.
4. From the menus, select the site, department and/or location to associate with the unit.

   -or-

   If you do not wish to associate the unit with any site, department or location, select the top (empty) item from the menu.
5. Click *Save* and *Close*.

To display the units associated with a site, department or location:

1. Click the *Units* tab and click *Sites*, *Departments* or *Locations*.
2. In the Units in Site window (with a list of units associated with the first alphabetically-listed site, department or location), in the side bar, click a site, department or location link to display another entry in the unit list.

13.2 Custom Fields

You must have Software Administrator or Appliance Administrator access to define custom fields. Ten custom fields are available. To use the custom fields, first change the default names on the fields (Custom Field 1, Custom Field 2 and Custom Field 3) to new names (1-64 characters), and then associate a custom label with a unit. The custom fields can be displayed in the Units windows using the Customize link. See Using the Customize link in windows on page 21.

After locating an appliance or unit in the Unit Views window, you can select the checkbox or name of the appliance/unit to manage that unit. For more information, see Accessing the Unit Views windows on page 77.

The first and second level custom fields for units appear under the Custom Field Labels heading in the side bar; all other custom fields do not appear in the side bar, but can be displayed in the content area by clicking *Customize* and adding the field.

To define custom fields:

1. Click the *Units* tab.
2. In the side bar, click *Custom Field Labels*.
3. In the Unit Custom Field Labels window, for each custom field, enter the name for the first custom field label and click *Save*.

NOTE: The Custom Field Labels name continues to appear in the side bar until you associate the custom label with a unit.

To associate a custom label with a unit:

1. Click the *Units* tab, and in the Appliances - All window, click a unit.
2. From the Unit Overview window, in the side bar, click *Properties* and *Custom Fields*.
3. From the Unit Custom Fields window, enter the name to associate with the corresponding label or leave the field blank.
4. Click *Save* and *Close*, then in the Appliances - All window, verify the side bar includes the names of the defined and associated custom fields.

Example Part 1: Customizing fields

In this example, a software administrator for the Rack Power Manager wants to examine a unit test configuration. The units are to be placed in one of two categories: an initial configuration or a final configuration category. The administrator also wants to identify the managers of the unit. At the present time, the Rack Power Manager software administrator has one EVR 1500 environmental monitor to add to the test configuration category and one generic appliance to add to the final configuration category. The Rack Power Manager software administrator defines the custom field, and adds a switch to the system by associating a switch to the custom fields.

To define custom field labels:

1. Click the *Units* tab, and in the side bar, click *Custom Field Labels*.
2. In the Unit Custom Field Labels window, in Label 1, enter Test Configuration.
3. After the first-level custom fields for units appear in the side bar under this heading, in Label 2, enter Appliances and target devices.
4. After the second-level custom fields for units appear in the side bar under this heading, in Label 3, enter Manager.

NOTE: This custom field does not appear in the side bar, but can be displayed in the content area by clicking the *Customize* link.

5. Click *Save* to save the changes.

NOTE: Custom Field Labels continue to appear in the side bar because the administrator has not yet defined any custom fields for the units.

Example Part 2: Testing

The test configuration also includes an EVR 1500 environmental monitor that is managed by Mary Jones. The EVR 1500 environmental monitor has not been verified for the final configuration, so the administrator will include it in the Initial Configuration category.

To configure the initial configuration for testing:

1. Click the *Units* tab.
2. In the Appliances - All window, click the *EVR1500* environmental monitor.
3. From the Unit Overview window's side bar, click *Properties* - *Custom Fields*.
4. From the Unit Custom Fields window (with the custom field names defined in step 1), enter Initial Configuration in the Test Configuration field.
5. In the Appliances and target devices field, enter EVR1500 Environmental Monitors.

6. In the Manager field, enter **Mary Jones**.
7. Click *Save* and *Close*.

Example Part 3: Creating a category for the final test results

The configuration of a generic appliance is verified, so the administrator wants to create a category named Final Configuration that will contain the final test units. The category contains one generic appliance managed by Tim Brown.

To create a category for the final test results:

1. Click the *Units* tab.
2. In the Appliances - All window, click the generic appliance.
3. After the Unit Overview window opens, in the side bar, click *Properties - Custom Fields*. The Unit Custom Fields window opens, including the custom field names you defined in step 1.
4. In the Test Configuration field, enter **Final Configuration**.
5. In the Appliances and target devices field, enter **Generic Appliances**.
6. In the Manager field, enter **Tim Brown**.
7. Click *Save* and *Close*.

The following figure shows how the side bar appears after the example procedure. Clicking a custom field link displays the units associated with that custom field.

Figure 13.1 Custom Fields Example: Side Bar

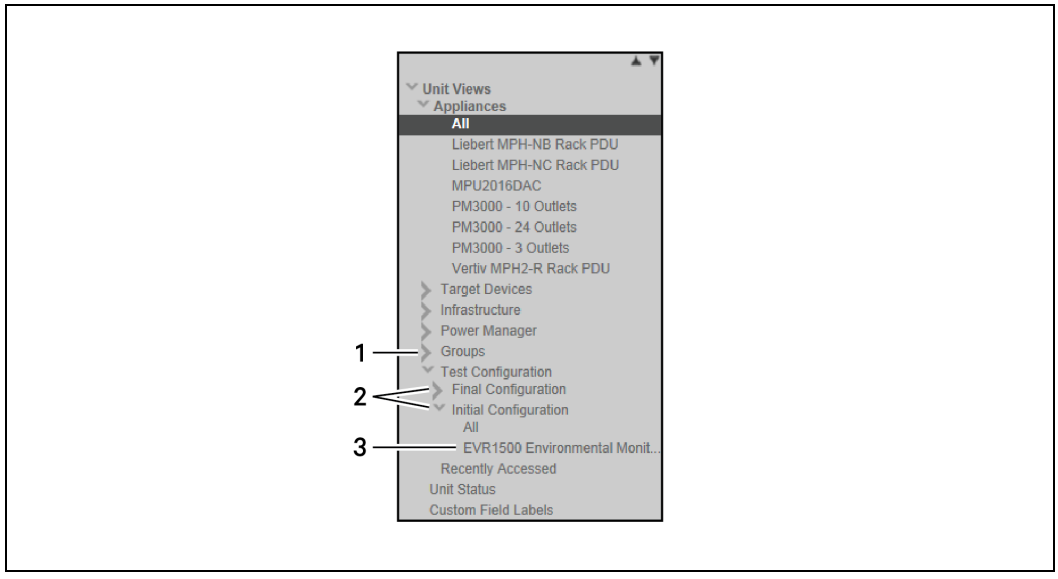


Table 13.2 Custom Fields Example: Side Bar Descriptions

ITEM	DESCRIPTION
1	System-wide first-level custom field label
2	Unit first-level custom field labels
3	Unit second-level custom field labels

13.3 Unit Groups

Unit Groups can be pre-defined or user-defined.

Clicking the *Units - Groups* tabs displays the Unit Groups window with the pre-defined container options (Global Root and Personal Root) for your groups. The Unassigned group, included in the Global Root container, is also a pre-defined group container. If a unit is not assigned to any other global group, it automatically becomes a member of the unassigned group. These pre-defined group containers cannot be deleted.

Clicking *Add* allows you to create user-defined unit groups, which can be Global Unit Groups or Personal Unit Groups. All global unit groups are descendants of the Global Root container and all personal unit groups are descendants of the Personal Root container. These group containers can contain other unit groups, but not individual units.

Table 13.3 Unit Groups Rights

GROUP TYPE	CAN CHANGE RIGHTS	CAN HAVE SUBGROUPS	CAN ADD GROUPS AS CHILDREN (NOT UNITS)	CAN ADD UNITS AS A MEMBER
Pre-defined				
Global Root	Yes	Yes	Yes	No, can only add groups
Unassigned	Yes	No	N/A	No
Personal Root	No	Yes	Yes	No, can only add groups
User-defined				
Global Groups	Yes	Yes	N/A	Yes
Personal Groups	No	Yes	N/A	Yes

13.3.1 Global root containers

Global root containers consist of unassigned groups and user-defined global groups. Global groups can only be created, modified or deleted by users with Rack Power Manager software administrator, user administrator or appliance administrator privileges. Global groups can be viewed by any user logged in to the Rack Power Manager software.

13.3.2 Personal root containers

Personal root containers consist of user-defined personal groups. Up to 32 personal unit groups can be created by a user. A personal unit group can only be viewed by the person who created it. This group has no rights associated with personal groups.

13.3.3 Nesting

You can create nested unit groups (unit groups within unit groups) to organize units hierarchically. Units can also belong to multiple groups.

13.3.4 Unit group hierarchy

Unit groups can be accessed using the Unit Groups window or the Unit Views Groups window via the Units tab. All personal unit groups are displayed in the Unit Groups window, even if they do not contain any units. In Unit Views Groups windows, groups are not listed unless they have assigned units.

Global groups containing units that cannot be accessed by a user are not displayed unless there are descendent groups containing units the user is allowed to access.

Example: Unit Group Hierarchy

As shown in the following figure and table, the Global Root group has four unit groups, and each of the four unit groups contain groups. The Gamma unit group is selected and it has two subgroups, Lab and Operations. The Unassigned global root group contains 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.

Figure 13.2 Example of Unit Group Hierarchy

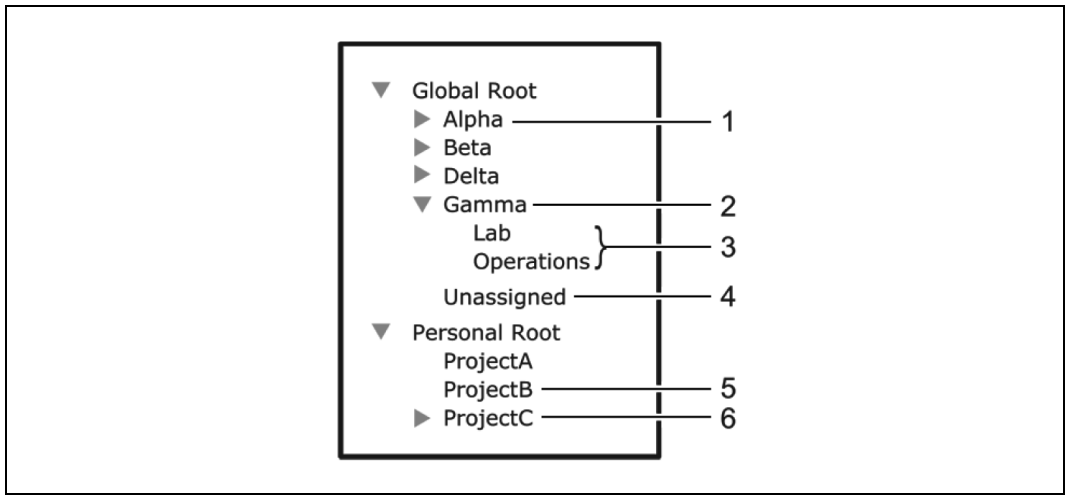


Table 13.4 Unit Group Hierarchy Example Descriptions

ITEM	DESCRIPTION	ITEM	DESCRIPTION
1	Global Unit Group Alpha with 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 with two subgroups	5	Personal unit group ProjectB with no subgroups
3	Unit groups without subgroups (in a Groups window, a document icon appears to the left)	6	Personal unit group ProjectC with one or more subgroups

The following are tips for displaying a list of unit groups in a Unit Views - Groups window:

- When you create a unit group, you can indicate if it (and any of its child unit groups) is displayed in the side bar. If a unit group has subgroups (children), an arrow is displayed next to its name.
- When the selected group has subgroups, the window displays 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 is displayed next to its name in the side bar. When you click a unit group in the side bar that has a document icon, a window opens, listing the units in the group. This window can include the same fields as other Unit Views windows; see Units Views Window Fields on page 76.
- You can enable or disable displaying a field using the Customize link. See Using the Customize link in windows on page 21. When you customize this window, you can also enable/disable the display of descendants. When enabled and a unit group is selected in a side bar, all descendants of the group are displayed. When disabled, only the immediate children of the selected group are displayed.

To display a list of unit groups in the Unit Groups window:

1. Click the *Units - Groups* tabs.
2. In the Unit Groups window, click *Global Root* or *Personal Root*.
3. The first unit group listed is automatically selected. Click the arrow next to a group to expand it and display subgroup names.

NOTE: If a unit group has subgroups (children), an arrow is displayed next to its name.

The number of items appearing in this window can be customized; see Using the Customize link in windows on page 21.

To display a list of unit groups in a Unit Views window:

NOTE: When you create a unit group, you can indicate if it and any of its child unit groups are displayed in the side bar.

1. Click the *Units* tab, and in the side bar, click *Groups*.
2. In the Groups - Global Root window, click a unit group in the side bar that has a document icon (that is, it has no subgroups) and view the list of units in the group.

NOTE: This window can include the same fields as other Unit Views windows; see Units Views Window Fields on page 76. You can enable or disable a field display using the Customize link. See Using the Customize link in windows on page 21.

NOTE: When you customize this window, you can also enable/disable the display of descendants. When enabled and a unit group is selected in the side bar, all descendants of the group are displayed. When disabled, only the immediate children of the selected group are displayed.

To display information about a unit group:

1. Click the *Units - Groups* tabs.
2. Click the group container or the parent group of the unit group you want to display information about.
3. Click the unit group name and in the side bar, select the applicable link to view the name, members, groups, units in the group or group access rights about a unit group.
4. Click *Close*.

13.3.5 Adding or deleting a unit group

Pre-defined unit group containers (global root, personal root or unassigned) are defaults and cannot be deleted; however, a unit group in a pre-defined unit group can be added or deleted. Unit group names can be 1-64 characters and must be unique within the parent group.

NOTE: Deleting a unit group deletes the group only; the units still exist in the Rack Power Manager software system.

To add a unit group:

1. Click the *Units - Groups* tabs.
2. In the Unit Groups window, click the checkbox of the group container (Global Root or Personal Root) or the group name that you want to be the parent of the new unit group.
3. Click *Add*, and in the Add Unit Group window, enter a name for the unit group.
4. If you do not want the unit group (or any of its child unit groups) to appear in the side bar, enable the Do not display this unit group nor any child unit groups as unit views checkbox.
5. If you do not want the units in the unit group to belong to any other unit group, select *Exclusive*.
6. If you want to add another unit group in the same hierarchy, click *Add/New*.

   -or-

   If you do not want to add another group, click *Add/Close*.

To delete a unit group:

1. Click the *Units - Groups* tabs.
2. In the Unit Groups window, click the checkbox of the unit group to be deleted.
3. Click *Delete,* and in confirmation dialog box, confirm or cancel the deletion.

13.3.6 Changing the unit group properties

Access rights indicate which users and user groups can access units in the Rack Power Manager software system. Access rights also indicate which actions are allowed. See About Access Rights on page 100. 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, the default setting also grants the access rights you assign to group A to group B. Unit group names can be 1-64 characters.

The following are access right options:

- 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.

For other ways to assign access rights, see How access rights can be assigned on page 101.

To change unit group properties:

1. Click the *Units - Groups* tabs.
2. In the Unit Groups window, click the name of a unit group.
3. In the Unit Group Name window, enter a new name in the Group field.

NOTE: 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.)

4. If you do not want the unit group (or any of its child unit groups) to appear in the side bar, enable the Do not display this unit group nor any child unit groups as unit views checkbox.
5. If you do not want the units in the unit group to belong to any other unit group, select *Exclusive*.
6. Click *Save* and *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 - Groups* tabs.
2. From the Unit Groups window, in the side bar, click *Members* and then click *Groups* to add or remove a group member of the unit group.

   -or-

   In the side bar, click *Members* to add or remove a unit member of the unit group, 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 bar, *Groups* is the only choice. You cannot add units or groups to the global unassigned unit group.

3. If the Unit Group Members (Units) or Unit Group Members (Groups) window opens, click *Assign*.
4. In the Assign Units to Unit Group window, select one or more units from the Available Units list and click *Add* to move the Units to the Assign list.

NOTE: After 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.

   -or-

   Select one or more units from the Units to Assign list and click *Remove* to move the units to the Available Units list.

5. Click *Save - Close*, and in the Unit Group Members window, click *Close*.

To add or remove access rights for one or more unit groups:

See Unit Access Rights on page 101.

13.4 Custom Groups

Custom groups can be created for calculating actual power usage. Custom groups also allow power control operations for a group of target devices. When configuring custom groups, the unit group names can be 1-64 characters.

13.4.1 Adding, deleting or modifying a custom group

Custom group queries can be added or deleted.

To add a custom group:

1. Click the *Units - Groups* tabs.
2. Click the *Custom Group* menu, and in the Custom Group window, click *Add* and enter a name for the unit group.
3. If you do not want the custom group to appear in the side bar, enable the Do not display this unit group nor any child unit groups as unit views checkbox.
4. If you do not want the units in the custom group to belong to any other group, select *Exclusive*.
5. If you want to add another custom group in the same hierarchy, click *Add/New*.

   -or-

   If you do not want to add another group, click *Add/Close*.

To delete a custom group:

1. Click the *Units - Groups* tabs.
2. Click the *Custom Group* menu, and in the Custom Group window, click the checkbox of the unit group to be deleted.
3. Click *Delete*, and in the confirmation dialog box, confirm or cancel the deletion.

To modify a custom group name:

1. Click the *Units - Groups* tabs.
2. Click the *Custom Group* menu, and in the Custom Group window, click the custom group name, modify as necessary and click *Close*.

13.4.2 Changing the custom group rights

Access rights can be accessed from a custom group perspective. 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 as follows:

- 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 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 add or remove access rights for one or more custom groups:

See Unit Access Rights on page 101.

NOTE: If a connection or power control action is enabled, the appropriate link appears in the Action column of Unit 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 - Groups* tabs.
2. Click the *Custom Group* menu, and in the Custom Groups window, click the checkbox of the custom group and click *Thresholds*.
3. Modify the values, click *Save* and *Close*.

13.4.3 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 - Groups* tabs.
2. Click the *Custom Group* menu, and in the Custom Groups window, click the checkbox of the custom group and click *Reports*.
3. Select the type of report: Comparative Power, Comparative Energy or Comparative Percentage Load and click *Run Report*.
4. From the report (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 can click the colored boxes below the report to show or hide report data for a category.
5. (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.
6. If you wish to export and save the report data as a .csv file, click *Export Data* and *Close*.

To generate comparative reports and export data for a custom group:

1. Click the *Reports - Power* tabs.
2. Select the Comparative Report and from the drop-down menu, select the Custom Group.
3. Click *Run Report*, and if you wish to export and save the report data as a .csv file, click *Export Data*.

To schedule a task for a custom group:

1. Click the *System - Tasks* tabs, and in the Tasks window, click *Add*.
2. From the Task Type drop-down menu, select *Control Power of Custom Groups*.
3. Enter the Frequency and the Task name in the appropriate fields and click *Next*.
4. Select the Custom Group(s) and the desired task, then click *Save* and *Close*.

To delete a task for a custom group:

1. Click the *System - Tasks* tabs.
2. In the Tasks window, click the checkbox of the applicable tasks and click *Delete*.

To run a task for a custom group:

1. Click the *System - Tasks* tabs.
2. In the Tasks window, click the checkbox of the applicable tasks and click *Run Now*.

13.5 Dashboard

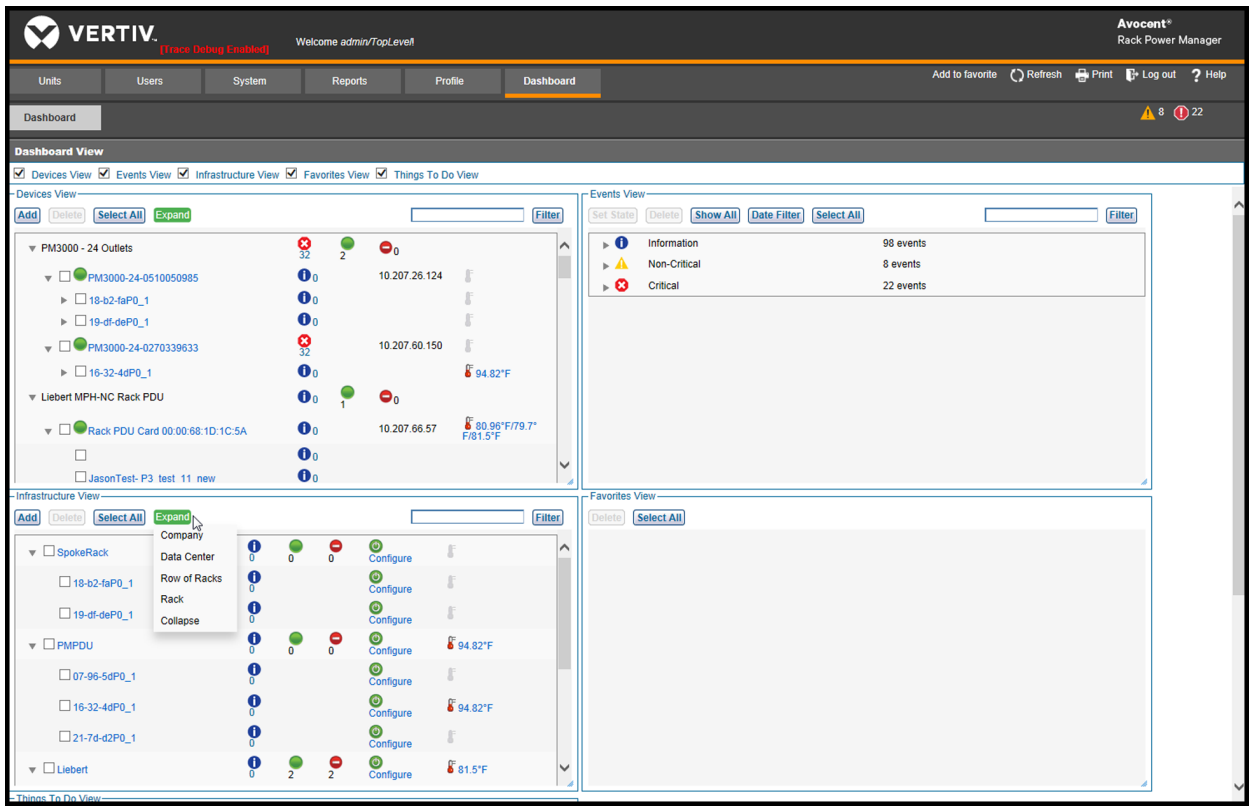
The Rack Power Manager Dashboard provides a central location to display the real-time status of your data center. The checkboxes on the top of the window can be enabled to display up to five views. Your Dashboard view selections are remembered and the same views are displayed when you log in again. The available views are listed in the following table.

Table 13.5 Dashboard View Descriptions

VIEW	DESCRIPTION
Devices View	Displays assets by the model/type, including any events; also displays the temperature readings reported by the temperature sensors attached to PDUs; includes an expand feature to expand the selected nodes.
Events View	Displays assets by the severity of events.
Infrastructure View	Displays assets by their location in the infrastructure, including any events; also displays the temperature readings reported by the temperature sensors attached to PDUs; includes an expand feature to expand the selected nodes.
Favorites View	Used to create bookmarks to any of your Avocent Rack Power Manager windows and for more specific concerns.
Things To Do View	Displays reminders about the remaining required items to be configured within Rack Power Manager.

NOTE: For device events displayed in the Devices and Infrastructure View, the highest category event reported for that device is displayed. For example, if a device has Information, OK, Non-Critical and Critical events, the Critical events icon is shown for that device.

Figure 13.3 Rack Power Manager Dashboard



At any time, you can click the *Select All* or *Unselect All* toggle button at the top of the Devices, Infrastructure, Events and Favorites views to select all or none of the items in the applicable view.

13.5.1 Devices View

The Devices View is used to add or delete PDUs and devices, such as PDU cards or receptacles, or display their status in the Rack Power Manager software. You can display your infrastructure's hierarchy by clicking the arrow beside each item in the list or clicking the *Expand* button and selecting one of the following levels:

- Level 1 displays the models, for example, the Liebert® MPX™ Rack PDU, and their number of events, number of online devices and number of offline devices.
- Level 2 displays the PDUs or power devices, such as the Rack PDU Card, and their number of events, percentage loads and IP address. Temperature readings are also displayed at the PDU level, and you can click the temperature readings to see more details, such as the sensor name and date/time at which the reading was taken. If there are multiple connected sensors, the readings are separated by a slash (/).
- Level 3 displays the receptacles and their number of events.

NOTE: The *Collapse* option is used to collapse all the levels.

To add PDUs/devices:

Click the *Add* button, follow the displayed Add Appliance Wizard and click *Save*.

To delete PDUs/devices:

Select one or more PDUs or devices and click the *Delete* button.

To search for a PDUs/devices:

Enter the search string in the filter box and click the *Filter* button.

To view the events by level:

1. In the Devices View, select the model or type and click the number beside the event icon.
2. From the displayed pop-up of all events for that level, click an event to display the Event Details window.

13.5.2 Infrastructure View

In the Infrastructure View, PDUs and devices in the Avocent® Rack Power Manager software can be added or deleted. This view also displays the status of the PDUs and devices. You can expand your infrastructure's levels by clicking the arrow beside each item in the list or clicking the *Expand* button and selecting one of the following infrastructure levels:

- *Company* displays all the companies and their data centers.
- *Data Center* displays all the companies, their data centers and the rows of racks in each data center.
- *Row of Racks* displays all the companies, their data centers, the rows of racks in each data center and all the racks in a row of racks.
- *Rack* displays all the companies, their data centers, rows of racks in each data center, the racks in each row and all the PDUs in a rack.

NOTE: The *Collapse* option is used to collapse all the items.

The number of events and percentage loads, online devices and offline devices are displayed in the Company, Data Center, Row of Racks and Rack levels. The maximum value of all the temperature readings

of the assigned PDUs are displayed at the Rack level and the number of events, percentage loads and temperature readings are displayed for the PDUs and devices, if available. Clicking the temperature readings displays more details, such as the sensor name and date/time at which the reading was taken.

To add a new infrastructure entity (Company, Data Center, Row of Racks or Racks):

1. Under Infrastructure View, click the *Add* button to go to the Add Unit Wizard.
2. Select an entity (Company, Data Center, Row of Racks or Racks) and click *Next*.
3. In the displayed Add Unit Wizard, enter the name of the entity.
4. If applicable, click the drop-down arrow and select the level the entity will be a member of.
5. Select the next entity level's member, then click *Add* and *Next*.
6. If adding a rack, enable or disable the Add data monitoring to the selected units checkbox.
7. After the confirmation message, click *Finish*.

To assign PDUs or receptacles to an infrastructure entity:

Select the entity and click the *Add* button to display the Membership screen where you can assign PDUs and receptacles to the entity.

To delete one or more PDUs, receptacles or entities:

Select one or more PDUs, receptacles or entities and click the *Delete* button.

To search for a PDU, receptacle or entity:

Enter the search string in the filter box and click the *Filter* button.

To view the events related to a level:

Click the number of events to display a pop-up with details of all events for that level.

To view more information about an event:

Click the description to display the event's details.

NOTE: The percentage load values in the Devices View and Infrastructure View are only shown if maximum power consumption for that entity has been configured.

Maximum power consumption (W)

After adding PDUs, receptacles or entities, the maximum power consumption can be configured in watts. The consumption configuration window can be accessed directly from the dashboard or by clicking *Units View - Power Manager* in the side bar.

To configure maximum power consumption from the dashboard:

1. After the entity is added to a rack, from the Dashboard, select the entity and click the entities' *Configure* icon.
2. In the Configuration window, enter the maximum power consumption in Watts and click *Save*.

To configure maximum power consumption from the Unit Views Window:

1. After the entity is added to a rack, under Unit Views in the side bar, select an entity (such as a rack PDU).
2. Click *Power Manager (Data Monitoring) - Settings - Configuration*.
3. On the Configuration window, enter the settings and click *Save*.

13.5.3 Events View

The Events View displays the total number of events for each type of event (Information, OK, Non-Critical and Critical). Selecting any event displays the list of events for that type of event. See Event Severity Levels on page 191.

Each event's description, date of occurrence and state is also provided. The state originates as a New (unacknowledged) event and can be manually updated to an Acknowledged event after it is seen (see Event states on page 194).

To view more information about an event:

Click the arrow to expand the appropriate event category and click the event description to display the Event Details window.

To delete one or more events:

Select the events and click the *Delete* button.

To search for one or more events:

1. Enter the search string in the filter box and click the *Filter* button to display all events containing the entered text.
2. Click the *Clear* button to clear the filter box and display all events.

To change the state of one or more events:

1. Click the event type arrow to expand the list and then click to enable the checkbox of the relevant events.
2. Click the *Set State* button to display the Set State window.
3. Select *New* or *Acknowledged* and click *OK*.

To filter the events by date:

1. Click the *Date Filter* button to display the Date Filter Screen.
2. Follow the instructions in Using the date filter on page 194.

13.5.4 Favorites View

In the Favorites View, you can create bookmarks for any windows in the Rack Power Manager user interface. After a bookmark is no longer needed, it can be deleted from the dashboard.

To create a bookmark using the Favorites View:

1. Navigate to the window for which you are going to create a bookmark.
2. Click the *Add to favorite* link located on the top right side of the window.
3. In the Add Favorite pop-up window, enter a name for the favorite.
4. Select the User radio button to display the bookmark only to the currently logged in user.

   -or-

   Select the System radio button to display the bookmark to all the users.
5. Click the *OK* button.

To delete bookmarks:

1. In the Favorites View, select one or more bookmarks.
2. Click the *Delete* button.

13.5.5 Things To Do View

The Things To Do View is provided as a reference for any tasks you may have missed during the installation of a device. The Avocent® Rack Power Manager software automatically provides suggestions based on what tasks you complete.

An example of a suggestion is PDU not added to a Rack. This suggestion may appear if you have enrolled a PDU in the Rack Power Manager and you realize the Rack Power Manager is not monitoring this PDU for power and environmental data. The Things To Do View displays a suggestion to add such PDUs to a rack. Clicking the suggestion opens the Add Unit Wizard to assign this PDU to a rack. After you assign the PDU to a rack, the suggestion is automatically removed from the list.

Another example suggestion is Thresholds not configured for a PDU/Rack/Row Rack. When thresholds are not configured, you may not get alerts when something goes wrong in your data center. A suggestion is displayed in the Things To Do View for each instance to prevent this scenario. You can click the suggestion to go to the Thresholds configuration window of that entity. After you configure the thresholds for an entity, the suggestion is automatically removed from the Things To Do View.

After a reminder is no longer required, you can click the *Don't show again* button to delete it.

14 MANAGING DS ZONES

DS (DSView) 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 with access rights, may switch to other zones. You can restrict a user from accessing a zone, prevent a user from viewing or accessing resources from another zone or you can grant a user access to multiple zones. In order to prevent one zone from starving another zone of licenses, you can manage the distribution of licenses and add-on features by assigning a number of licenses to each zone.

14.1 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 Viewing and Adding Licenses on page 40). 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 your DS Zones license is not enabled, the Rack Power Manager software does not display any windows or links related to zones.

14.2 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.

NOTE: As an exception, a modem is still available to all zones even if it is moved to a sublevel zone.

Table 14.1 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; IP addresses for appliances 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; for an operation or tool involving multiple units, all units must be in the same zone.
View unit groups	Any qualified user	Active zone only.
Add unit groups	Any qualified user	Active zone only. 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. 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. 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.

Table 14.2 User Actions in a Zone

ACTION	USER STATUS REQUIRED FOR ACTION	ZONE(S) AFFECTED
View user accounts	Any qualified user	Active zone only.
Add or delete users	Any qualified user	Active zone only. 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 to another zone. A user or user group is permanently owned by the zone that is active when the user is 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 pre-defined user groups cannot be deleted.	Active zone only. 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.
Add authentication services	Any qualified user	Active zone only. The same authentication service cannot be reused in multiple zones and 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 a 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 and is permanently owned by the zone that is active when the authentication service is 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; user and unit must belong to the active zone.
Assign users to groups	Any qualified user	Active zone only; user and group must belong to the active zone.
View effective rights for users	Any qualified user	Active zone only.

Table 14.3 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	All zones for which the user has access rights
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

Table 14.4 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
Manage plug-ins	Super users only	All zones
Configure SNMP trap settings	Any qualified user	Active zone only
Import system settings	Super users only	Active top level zone only

14.3 Creating Zones

After 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 under the top level zone, but you cannot create additional top level zones. You can create as many individual zones as your license key allows.

For more information, see the following:

- Managing zone access rights on page 137
- Assigning zone licenses on page 136

To create a new zone:

1. Click the *System - Zones* tabs.

2. In the Zones window (with previously created zones), select the checkbox of the zone to which you are adding a sublevel zone and click *Add*.
3. From the Add Zone Wizard, enter a unique zone name and click *Next*.
4. On the Assign Zone Licenses window in the Assigned Licenses field, enter the number of licenses that can be used by this zone for each license type, then click *Next*.

NOTE: The number of available licenses is listed in the Available Licenses column.

5. In the Assign Zone Rights window, for each access rights group, select *Allow* or *Deny*.
6. Click *Next* and on the Completed Successful window, click *Finish*.

14.4 Accessing Zones

When logging into the Rack Power Manager software, specify the highest level zone for which you have access rights. If you do not specify a zone, the 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.

The zone you are currently in is referred to as the active zone and is displayed in the option bar. When in a zone, you cannot view or access units that belong to another zone. If your access rights include other zones, you can switch to those zones after you are logged in.

To specify zone log in options:

1. Click the *System - Global Properties* tabs.
2. In the side bar, select *Zones*.
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 enter the zone name in a 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 provided fields.
3. In the Zone field, enter the highest level zone for which you have access rights.

   -or-

   From the Zone menu, click the zone name of the highest level zone for which you have access rights.
4. Click *Login*.

To switch zones:

Click the *System - Zones* tabs, and in the Zones window, select the checkbox of the zone to be switched and click *Switch*.

-or-

In the top left corner of the window, click the name of the zone to open a pop-up menu, then select the zone to be switched.

14.5 Transferring Units to Zones

Managed appliances, blade chassis, hypervisor managers or hypervisor servers can be transferred to zones with access rights. All associated target devices are transferred with the unit and merged target device connections are split, however you cannot move a target device independently.

If you are transferring units that require licenses, the zone to which you are moving the units must be assigned the appropriate licenses. If the zone does not have sufficient licenses, the transfer fails.

The units and associated target devices are accessible when the zone that owns the units is active.

For more information, see Accessing the Unit Views windows on page 77 and the following section.

To transfer units to zones:

1. Click the *Units* tab, and in the Appliances - All window, click the checkbox of the units to be moved.
2. Click *Operations* and from the drop-down menu, select *Move Units to Zone*.
3. From the Move Units Wizard, select the zone to own the units and click *Next*.
4. In the *Completed Successful* window, click *Finish*.

14.6 Managing Zone Properties

After 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 - Global Properties* tabs.
2. In the side bar, click *Zones* and click the name of zone to be modified.
3. In the side bar, click *Name* and enter a unique zone name in the field and click *Save*.

NOTE: The current zone path in relation to higher level zones is displayed.

Assigning zone licenses

You can manage the distribution of licenses among zones by assigning licenses to each zone. This prevents one zone from starving other zones of licenses. You can also 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.

At least one client session license must be specified for each zone, including the top level zone. For other license types, you can 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.

For more information about the operations each license type allows, see Viewing and Adding Licenses on page 40.

To assign zone licenses:

1. Click the *System - Global Properties* tabs.
2. In the side bar, select *Zones* and click the name of the zones you wish to modify.
3. In the side bar, click *Licenses*.

4. In the Assign Zone Licenses window, Assigned Licenses field, for each license type, enter the number of licenses that can be used by this zone and 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 can select 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 on 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 - Global Properties* tabs.
2. In the top navigation menu, select *Zones* and click the name of the zones you wish to modify.
3. In the top navigation menu, click *Access Rights*.
4. In the Assign Zone Rights window, for each access rights group, select *Allow* or *Deny* and click *Save*.

This page intentionally left blank.

15 MANAGING USER ACCOUNTS

When managing 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 pre-defined or user-defined user groups

15.1 Using the User Accounts Windows

User accounts are displayed and managed through User Accounts windows.

To display the User Accounts window:

1. Click the *Users* tab, and in the side bar, click the group to display the names of users in a pre-defined or user-defined user group.
2. In the User Accounts window for that group, click a username.

Customizing the User Accounts window

The User Name field is usually displayed in the User Accounts window. One of the icons listed in the following table appears to the left of the usernames and represents the status of each Rack Power Manager software user.

Table 15.1 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 User account restrictions and expiration settings on page 144.
Padlock	Internal	Locked - The user account is locked; the user cannot log in to the Rack Power Manager software because the maximum number of log in failures is exceeded. See Authentication Services on page 57 and Unlocking User Accounts on page 142.
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 User account restrictions and expiration settings on page 144.

The following fields can 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 21.

- 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 143.
- Status - User account status: Enabled, Disabled, Locked, Suspicious or Expired. One of the user status icons in the previous table appears to the left of the username.

- Authentication Server - Name of the internal or external authentication server. See Authentication Services on page 57.
- Business Address - Business address defined in the user's properties. See Address on page 145.
- Business Mobile - Business mobile phone number defined in the user's properties. See Phone contact on page 145.
- Business Phone - Business phone number defined in the user's properties. See Phone contact on page 145.
- Default E-Mail - Default email account defined in the user's properties. See Email contact on page 145.
- E-Mail 1 to E-Mail 5 - Up to five additional email accounts defined in the user's properties. See Email contact on page 145.
- Custom Field 1 to Custom Field 6 - Custom fields for the user. If you have specified text for a custom field, that text is displayed when you display the field. See Custom field properties on page 146.
- Home Address - Home address defined in the user's properties. See Address on page 145.
- Home Phone - Home phone number defined in the user's properties. See Phone contact on page 145.
- Mobile Phone - Mobile phone number defined in the user's properties. See Phone contact on page 145.
- Pager - Pager number defined in the user's properties. See Phone contact on page 145.

15.2 Adding User Accounts

With software administrator or user administrator rights, you can add a user account to the system database.

The following information is configured when a user account is created:

- Assigning user authentication using the Rack Power Manager software internal authentication or an external authentication server. See Authentication Services on page 57.
- Assigning users to user groups and assigning specific actions to a user. See User Groups on page 149.

From the Add User Account Wizard, the Authentication Service window lists the Rack Power Manager software internal service and all previously added external authentication service, which can be used to authenticate users when they log in.

The Rack Power Manager software obtains external group membership and external user information when a user logs in. If a group membership of a user changes or the user is deleted externally, the Rack Power Manager software does not see those changes until the next time that user logs in.

In the Select User from External Authentication Service window, if the list of users contains more than 5000 entries, a message indicates that not all items are displayed.

The Member Of list includes all pre-defined and user-defined groups.

15.2.1 Usernames and passwords

There are differences in the username and password policies depending on the window and the external authentication server.

In the Type in User Credentials window, usernames can contain up to 256 non-case sensitive characters. If a RADIUS external authentication service is used, the limit is 253 characters. Usernames are case-preserving. For example, if an account named JDoe is created, it is saved as JDoe in the Rack Power Manager server, but you can log in as JDoe, jdoe, JDOe and so on. Passwords can contain 3-64 characters. Passwords 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 can specify a different minimum character length and change expiration criteria. See Authentication Services on page 57.

In the Specify User Name window, usernames can contain up to 256 characters. Usernames may or may not be case sensitive, depending on the requirements of the external authentication server.

15.2.2 Service accounts

A service account can also be created if you select the Rack Power Manager software internal authentication service on the Authentication Service window. A service account can be used to impersonate another user over the Web Services API or GUI Access API, but cannot be used to log in to the Rack Power Manager software. For more information, see the Avocent® DSView™ Management and Rack Power Manager Software Full Software Development Kit Installer/User Guide.

To add a user account:

1. Click the *Users* tab, and in the User Accounts - All window, click *Add*.
2. In the Select Authentication Service window, select an authentication service and click *Next*.
3. If you selected *RPM Internal*, go to step 3.

   -or-

   If you selected any other authentication service, go to step 4.
4. In the Type in User Credentials window, enter a username and password, then confirm the user's password you are adding. If desired, click *User must change password at next login* to allow users to set their own passwords when they log in and click the Service Account checkbox to designate the account as a service account.
5. In the Specify User Name window, enable the Specify user on external authentication service radio button, enter the username that is configured for the RADIUS, TACACS+ or RSA SecurID server and click *Next*.

   -or-

   Click the Find user on external authentication service radio button to display the list of users. Select one or more users from the list and click *Next*.

NOTE: You can filter the list by using the *Filter* button and the adjacent text field. Specifying a username in the text field returns 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 20.

6. In the Assign User Credentials and Groups window, select one or more groups from the Available Groups list, click *Add* to move the group names to the Member Of list, then click *Finish*.

15.3 Deleting User Accounts

One or more user accounts can be deleted at a time.

To delete one or more user accounts:

1. Click the *Users* tab, click the checkbox of the usernames.
2. Click *Delete*, and in the confirmation dialog box, confirm or cancel the deletion.

15.4 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 is not allowed to attempt another log in until a certain amount of time has passed. Users that are locked out have a lock next to their name in the User Accounts window and *Locked* appears in the Status column.

User administrators or administrators can 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 of one or more usernames and click *Unlock*.

15.5 Resetting a User Account Password

A Rack Power Manager software administrator or user administrator can reset the password of a user. After a password is reset, the next time the user starts a new Rack Power Manager software session, the user is required to log in by entering **password** as their password and then entering and verifying a new password for their account.

To reset a user account password:

1. Click the *Users* tab and click the checkbox of the user.
2. Click *Reset Password* and in the confirmation dialog box, confirm or cancel the reset.

15.6 Changing User Account Properties

If you have Rack Power Manager software administrator or user administrator privileges, you can change the following account properties for a user:

- User (log in) name and full name
- Certificate associated with the user
- Log in password
- Account log in restrictions and expiration settings
- User groups to which the user is assigned
- 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

If the user account will be using the Rack Power Manager software internal authentication service, some properties can be changed. See Authentication Services on page 57.

15.6.1 Username

The username information includes the actual full name of the user and the username that the Rack Power Manager software uses to log in and identify the user. For example, you can 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 and click a username.
2. In the User Name window, enter the username for the user.
3. Enter the full name of the user.
4. Click *Save* and *Close*.

15.6.2 User certificates

Certificates can 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 34), the user certificate used at login must meet the policy requirements.

As an alternative to using this method, the user can 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 28.

To change the certificate associated with a user:

1. Click the *Users* tab and click a username.
2. From the User Name window, in the side bar, click *Credentials* and *Certificate*.

NOTE: The User Certificate window indicates if a certificate has failed a test required in the system certificate policy.

3. Enter the path and name of the certificate or browse to the certificate location.
4. Click *Save* and *Close*.

15.6.3 User SSH key

A configurable SSH key (1-256 characters) can be used by a serial console appliance to authenticate a Rack Power Manager software user who is using an out of band client, such as someone using a PuTTY SSH client that was not started by the Rack Power Manager software. When connecting to the serial console appliance, the user supplies the public/private SSH key, which the appliance verifies against the user key stored in the Rack Power Manager software.

NOTE: RSA keys must have a maximum length of 1024 bits.

As an alternative to using this method, if the administrator has enabled a global setting to allow it, the user can specify the SSH key in the profile settings. See Specifying an SSH key on page 29.

To specify a user SSH key:

1. Click the *Users* tab and click a username.
2. From the User Name window, in the side bar, click *Credentials* and *SSH Key*.
3. In the User SSH Key window, enter the name or browse to the file location containing the public SSH key (generated by a third party key generator).
4. Click *Save* and *Close* to upload the SSH key file to the Rack Power Manager server for authenticating the user.

15.6.4 User password

An administrator can change a user password or specify that a user must enter a new password during the next log in. Only passwords for internal authentication users can be changed.

To change a user password or force a new password:

1. Click the *Users* tab, and in a User Accounts window, click a username.
2. From the User Name window, in the side bar, click *Password*.
3. From the User Password window, enter and verify the new password for the user.
4. If desired, force a user to define a new password during the next log in by enabling the User must change password at next login checkbox.
5. Click *Save* and *Close*.

15.6.5 User account restrictions and expiration settings

Account restriction and expiration settings can be changed only for internal authentication users. An expired user account remains in the Rack Power Manager software system until the account is deleted.

If you are using the Rack Power Manager software internal authentication service, a user account can be configured as a service account. A service account can be used to impersonate another user over the Web Services API or GUI Access API, but cannot be used to log in to the Rack Power Manager software. For more information, see the Avocent® DSView™ Management and Rack Power Manager Software Full Software Installer/User Guide.

To change user account restrictions and expiration settings:

1. Click the *Users* tab and click a username.
2. From the User Name window, in the side bar, click *Restrictions*.
3. From the User Account Restrictions window, configure the desired account restrictions described in the following table.

Table 15.2 Configuring Account Restrictions

RESTRICTION	SETTING
Prevent the user from logging in to the Rack Power Manager software	Enable the Disable user account checkbox or re-enable the user account by unchecking the Disable user account checkbox. (Users with open sessions remain logged in.)
Force a user to define a new password during the next login	Enable the User must change password at next login checkbox.
Prevent the user from changing the password	Enable the User cannot change password checkbox.
Prevent a password from expiring	Enable the Click Password never expires checkbox.
Designate the account as a service account	Enable the Service Account checkbox.

4. Configure the account with no expiration date by enabling the Never radio button.

   -or-

   Specify an expiration date by enabling the End of radio button, clicking the button of the adjacent field, and in the displayed calendar, selecting the date for account expiration.

5. Click *Save* and *Close*.

15.6.6 User group membership

The Rack Power Manager software obtains external group membership and external user information when a user logs in. If the group membership of a user changes or the user is deleted externally, the Rack Power Manager software does not see those changes until the next time that user logs in. See User Groups on page 149.

To change the group membership of a user:

1. Click the *Users* tab and click a username.
2. From the User Name window, in the side bar, click *User Groups*.
3. In the User Group Membership window, add a user to one or more groups by selecting the group(s) in the Available Groups list and clicking *Add* to move the columns to the Member Of list.

   -or-

   Remove the user from one or more groups by selecting the group(s) in the Member Of list and clicking *Remove* to move the groups to the Available Groups list.
4. Click *Save* and *Close*.

15.6.7 Address

The user address may be changed only for internal authentication users.

To specify address information for a user:

1. Click the *Users* tab and click a username.
2. From the User Name window, in the side bar, click *Addresses*.
3. In the User Address Properties window, enter the home address and business address of the user.
4. Click *Save* and *Close*.

15.6.8 Phone contact

The phone contact can be changed only for internal authentication users.

To specify phone contact information for a user:

1. Click the *Users* tab and click a username.
2. From the User Name window, in the side bar, click *Telephones*.
3. In the User Telephone Properties window, enter the home phone number, business phone number, mobile phone number, mobile business phone number and/or pager number of the user.
4. Click *Save* and *Close*.

15.6.9 Email contact

Email contacts can be changed only for internal authentication users.

To specify email contact information for user:

1. Click the *Users* tab, and in a User Accounts window, click a username.
2. From the User Name window, in the side bar, click *E-Mail Addresses*.

3. In the User E-Mail Properties window, enter the primary email address of the user and up to five additional email addresses.
4. Click *Save* and *Close*.

15.6.10 User notes

User notes can be changed only for internal authentication users.

To specify notes about a user:

1. Click the *Users* tab and click a username.
2. From the User Name window, in the side bar, click *Notes*.
3. In the User Notes window, enter any information you wish.
4. Click *Save* and *Close*.

15.6.11 Custom field properties

You can specify any information in the six custom fields. Custom field properties can be changed only for internal authentication users.

To change the custom fields:

1. Click the *Users* tab and click a username.
2. In the side bar, click *Custom Fields*.
3. In the User Custom Fields window, enter information in the fields.
4. Click *Save* and *Close*.

15.7 User Access Rights

Access rights indicate if a user is allowed to perform certain actions on a unit in the Rack Power Manager software system. From a user perspective, you can assign access control rights by selecting a user account, specifying the units for the rights to be assigned and indicating the permission to perform the action (none, allow, deny or inherit) for each unit.

After the configuration is complete, you can verify the following available actions for the unit:

- Black check mark - The user is granted access for this right.
- Gray check mark - A group to which the user belongs is granted access for this right.
- Black X - The user is denied access for this right.
- Gray X - A group to which the user belongs is denied access for this right.
- No check mark - No access is granted or denied for this right.

The following are additional ways to assign access rights:

- From a user group perspective - see User Group Access Rights on page 153
- From a unit perspective - see Unit Access Rights on page 101
- From a unit group perspective - see Changing the unit group properties on page 122

See About Access Rights on page 100 for detailed information and a list of actions that can be enabled/disabled for target devices and managed appliances.

To display the access rights of a user:

1. Click the *Users* tab and click a username.

2. From the User Name window, in the side bar, click *Effective Rights*, then click *All Units* or *Appliances*.
3. In the Appliance Effective Rights window, verify the access rights of the user and click *Close*.

Customizing Appliance Access Rights windows

The Name field is always displayed in the Appliance Access Rights window. The action fields can also be displayed and the Customize link can be used to add or remove fields in the display. See About Access Rights on page 100 and Using the Customize link in windows on page 21.

The following are the options to add/remove access rights for a unit/unit group:

- 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 one or more unit groups to which the selected unit/unit group belongs. When *Inherit* is selected, the Allow and Deny checkboxes become gray and unchangeable, and indicate the inherited value. If the inherited settings indicate both Allow and Deny, the inherited value, Deny 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.

To add or remove access rights through a user account:

See Unit Access Rights on page 101.

15.8 Data Export Accounts

Data Export accounts are database accounts with read-only access to power and environmental data collected by the Rack Power Manager software. After an account is saved, you can use third party reporting software to access the Data Export windows and create your own custom reports.

To create a data export account:

1. Click the *Users* tab, and in the side bar, click *Data Export Accounts*.
2. Click *Add*, specify a username and password and click *Save*.

This page intentionally left blank.

16 USER GROUPS

Users that have been added to the Rack Power Manager software system can be added to user groups. User groups include the pre-defined role types, which appear in the Roles window or user-defined role types, which appear in the User Defined window. These group types, selected from the *Users - Groups* tabs, are described as follows:

- Roles (default) are the six pre-defined user group options: Appliance Administrators, Auditors, RPM 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 can be added to any of the other user groups. The privileges that allow a user to perform tasks on the Rack Power Manager software system are dependent on the role to which the user is a member. See Pre-defined User Groups on page 30.
- User-Defined custom groups are based on your criteria. 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.

The windows can also display the following fields. Click the *Customize* link to add or remove fields in the display. See Using the Customize link in windows on page 21.

- Authentication Server - Name of the authentication server assigned to the user. See Authentication Services on page 57.
- Role - Role of a user-defined user group, which can be None, User, Auditor, Appliance Administrator, User Administrator or Rack Power Manager Administrator. The role column for a pre-defined user group or a user-defined user group with a role of None is empty.
- Type - Type of user group, which can be pre-defined or user-defined.

To display user groups:

1. Click the *Users - Groups* tabs.
2. With *Roles* automatically selected, verify the pre-defined user groups.

   -or-

   In the side bar, click *User-Defined* to display the user-defined groups.

16.1 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 distinguished name 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.”

16.2 Adding User-defined User Groups

With Rack Power Manager software administrator or user administrator rights, you can add user-defined user groups. If you are using Rack Power Manager software internal authentication, you can 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) can be added, but their membership is not controlled by the Rack Power Manager software.

Rack Power Manager software internal, RADIUS, LDAP, Windows NT or Active Directory authentication services

The User Defined window lists all authentication services that can be used to authenticate the user group when the user logs in.

User group names can 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.

The external authentication service provides a list of the groups. If the list of groups contains more than 5000 entries, a message indicates that not all items are displayed. You can filter the list and if you are using an Active Directory Server, you can select the filter method, either by the traditional filtering method in the legacy *Rack Power Manager Server* or using a modified filtering method that only provides matches to the filter string based on the common name (CN) of the group. The modified 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.

For more information, see the following:

- Authentication Services on page 57
- Group Naming in External Authentication Services on page 149
- Filtering information in a window on page 20

To add a user-defined user group:

1. Click the *Users - Groups* tabs.
2. In the side bar, click *User-Defined*.
3. In the User Defined window, click *Add*.
4. In the Select Authentication Service window, click the *Rack Power Manager Internal* authentication service, click *Next* and go to step 5.

   -or-

   Click any other type of authentication service, click *Next* and go to step 6.

NOTE: If you are adding a group to the TACACS+ authentication service, see Adding User-defined User Groups on page 150 for more information.

5. In the Type in Internal Group Name window, enter the name for the new user group and go to step 8.

NOTE: When access rights are assigned to internal user groups, the internal group users must also be members of a pre-defined user group to define their role in the Rack Power Manager software. See Pre-defined User Groups on page 30.

6. In the Specify External Group window, click *Specify a group on external authentication service* and enter the name of the group in the field.

   -or-

   Click *Import the external group - Everyone* to consider any user on the external authentication server as a member of this user group.

   -or-

   Click *Find a group on external authentication service* to select from the list of groups on the external authentication service, then click the *Filter* button and the adjacent text field.

   -or-

   When using an Active Directory Server, click *Filter in Rack Power Manager Server (legacy)* or *Filter in Active Directory Server* (modified) and select one or more external authentication service groups from the list.

7. Click *Next*, select a role for the user group(s) and click *Finish*. See Pre-defined User Groups on page 30.

TACACS+ external authentication services

TACACS+ service can be configured to use the privilege level attribute method or the group name custom attribute method. When using the privilege level attribute method, there are 0-15 privilege levels. The higher the number, the higher the level of access.

See Pre-defined User Groups on page 30 for information about user roles.

To add a TACACS+ user group:

1. Click the *Users - Groups* tabs.
2. In the side bar, click *User-Defined*.
3. In the User Defined window, click *Add*.
4. In the Select Authentication Service window, select an appropriate TACACS+ authentication service and click *Next*.
5. If the TACACS+ service you selected is configured to use the privilege level attribute method, in the Specify External Group Name window, select a privilege level and click *Next*.

NOTE: The Rack Power Manager server assigns a group name based on the privilege level you select. For example, if you select level 7, the group name is Privilege Level 7.

   -or-

   If the TACACS+ service you selected is configured to use the group name custom attribute method, in the Specify External Group Name window, enter the name for the external user group on the external authentication service and click *Next*.

NOTE: The group name must correspond to one of the values configured in the TACACS+ service.

6. Select a role for one or more user groups and click *Finish*.

16.3 Deleting User-defined User Groups

With Rack Power Manager software administrator or user administrator rights, you can delete any user-defined user groups that are created in the Rack Power Manager software system.

To delete a user-defined user group:

1. Click the *Users - Groups* tabs.
2. In the side bar, click *User-Defined* and in the User Defined window, click the checkbox of the user groups to be deleted.
3. Click *Delete*, and in the confirmation dialog box, confirm or cancel the deletion.

16.4 User Group Properties

The User Group Properties window for pre-defined user groups displays read-only properties for each group. The properties are name (1-256 characters) and type.

To display the properties of a pre-defined user group:

1. Click the *Users - Groups* tabs.

NOTE: Roles is automatically selected in the side bar.

2. In the Roles window, click a user group name and in the side bar, click *Properties*.
3. In the User Group Properties window, view the properties and click *Close*.

To display or change the properties of a user-defined user group:

1. Click the *Users - Groups* tabs.
2. In the side bar, click *User-Defined*.
3. In the User Defined window, click a user group name and in the side bar, click *Properties*.
4. In the User Group Properties window, view or enter a new 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 is disabled.

5. If applicable, select a new role from the menu or select *None*.
6. Click *Save* and *Close*.

16.5 Changing User Group Members

When creating users, you can assign them to one or more pre-defined or user-defined user groups and then add or remove them from the groups. Members can only be assigned to or removed from user groups defined on the internal Rack Power Manager authentication service. You can also add or remove a user from a pre-defined or user-defined user group by clicking a username in a User Accounts window and changing its user group membership. See Changing User Group Members on page 152.

To add or remove user group members:

1. Click the *Users - Groups* tabs.

NOTE: Roles is automatically selected in the side bar.

2. From the Roles window, in the side bar, click *User-Defined*.
3. In the User Defined window, click a user group name, and in the side bar, click *Properties*.

4. In the User Group Properties window, in the side bar, click *Members*.
5. In the User Group Members window, click *Assign*.
6. In the Assign Users to User Group window, select the users in the Available Users list and click *Add* to move users to the Members list.
7. Select the users in the Members list and click *Remove* to move users to the Available Users list.
8. Click *Save* and *Close*, then in the User Group Members window, click *Close*.

NOTE: The Roles or User Defined window opens, depending on the selected group for this procedure.

16.6 User Group Access Rights

Access rights indicate if a user is allowed to perform certain actions on a unit in the Rack Power Manager software system. See About Access Rights on page 100 for detailed information and a list of actions that are available for target devices and managed appliances.

Access control rights can be assigned from a user group perspective. This means you select a user group, specify the units for which rights are to be assigned, then indicate the permission to perform the action (none, allow, deny or inherit) for each unit.

The following are other ways to assign access rights:

- From a user perspective - see User Access Rights on page 146
- From a unit perspective - see Unit Access Rights on page 101
- From a unit group perspective - see Changing the unit group properties on page 122

In the Target Devices Effective Rights window or Appliance Effective Rights window, the columns indicate the available actions for the unit, such as:

- Black check mark - the user is granted access for this right
- Gray check mark - a group to which the user belongs is granted access for this right
- Black X - the user is denied access for this right
- Gray X - a group to which the user belongs is denied access for this right
- No check mark - no access is granted or denied for this right

The Access Rights table options are:

- 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 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 display user group access rights:

1. Click the *Users - Groups* tabs.

NOTE: Roles is automatically selected in the side bar.

2. In the Roles window, click a user group name and click *Properties*.

   -or-

In the side bar, click *User-Defined* to display the User Defined window, click a user group name and click *Properties*.

3. In the User Group Properties window, verify or enter a user group name.
4. In the side bar, click *Effective Rights*, then click *All Units*, *Target Devices* or *Appliances*.
5. In the Target Devices Effective Rights window or Appliance Effective Rights window, view the available actions for the unit and click *Close*.

To add or remove user group access rights:

See Unit Access Rights on page 101.

17 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.

The Telnet viewer is supported for managed PDUs only. Any other appliances do not have Telnet sessions.

NOTE: Throughout this chapter, the term “appliance” or “managed appliance” is 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 terminal emulations of the Telnet client. See Security Property on page 157.

The Telnet viewer uses the credentials provided by the Rack Power Manager software to establish a serial session and automatically accepts the server key of the appliance. 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 1.7 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 7 for information about user interaction with the JRE installer.

17.1 Telnet Viewer Window Features

A new Telnet viewer window opens 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 17.1 Telnet Viewer Window

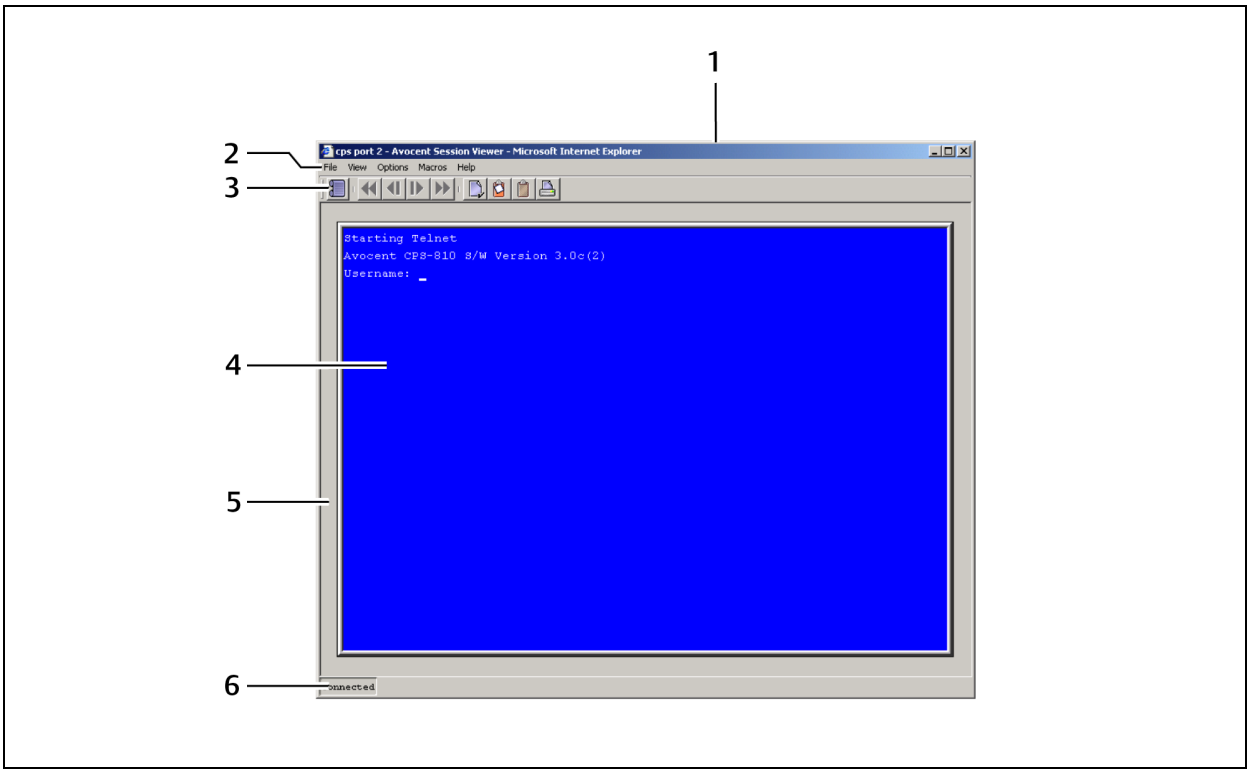


Table 17.1 Telnet Viewer Window Descriptions

ITEM	NAME	DESCRIPTION
1	Title Bar	Displays the name of the target device being viewed.
2	Tab Bar	Allows you to access the Tenet viewer windows.
3	Toolbar	Allows you to navigate in the Telnet viewer.
4	Virtual Terminal window	Accesses to your target device; the default setting for the window size is 80 characters x 24 lines.
5	Viewer Frame	Sizes the window when you click and hold on the frame. Although the size of the window can be changed, the Virtual Terminal window remains the same size.
6	Status Bar	Displays one of the following: Connected - Normal terminal emulation in a Telnet viewer session. Logging - Logging is enabled. Logging Paused - 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.

17.1.1 Telnet viewer window toolbar

The following table describes the icons in the Telnet viewer window.

Table 17.2 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 the Telnet viewer session data to the system clipboard
	Copy Buffer - Copies the contents of the Telnet viewer session buffer to the system clipboard
	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 is scaled
	Paste - Pastes the contents of the system clipboard into a Telnet viewer session
	printer - Prints a screen of Telnet viewer session data

17.2 Security Property

A fully functional SSH2 (Secure Shell Version 2) Client is built in to 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 determines 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 opens 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 bar to display the Properties - Sessions - Settings window.

17.3 Opening a Session

The management software can be used to open a session to a PDU.

To open a session to the PDU:

1. Click the *Units* tab and from a Unit Views window containing PDUs, click the PDU.
2. On the Unit Overview page, click *Telnet Session*.

NOTE: This launches the viewer and opens a Telnet session with the PDU.

17.4 Customizing the Telnet Viewer

You can specify preferences for every Telnet viewer session, regardless of the device to which you are connected. 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. From the *Options* tab drop-down menu, select *Preferences*.
2. In the Preferences dialog box in the Colors section, click the Background/Normal Mode box and select a color. (The default color is blue.)

   -or-

   Click the Text/Normal Mode box and select a color. (The default color is white.)

To change the cursor appearance:

1. From the *Options* tab drop-down menu, select *Preferences*.
2. In the Preferences dialog box, in the Caret list, select *Block* to display the cursor as a block.

   -or-

   Select *Underline* (default) to display the cursor as an underline.

To enable/disable an exit warning prompt for Telnet viewer sessions:

1. From the *Options* tab drop-down menu, select *Preferences*.
2. In the Preferences dialog box, enable (default).

   - or-

   Disable the Prompt on Exit checkbox.

NOTE: When the exit warning prompt is enabled, a message appears when you select *Telnet - Exit*. You can then exit or continue the session. When disabled, the session closes without further prompting.

To enable/disable autoscaling:

1. From the *Options* tab drop-down menu, select *Preferences*.
2. In the Preferences dialog box, enable (default).

-or-

Disable the Auto Scale checkbox.

NOTE: 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 does not scale when the view is changed; instead, scroll bars appear around the window.

17.5 Customizing Session Properties

When you are connected to an appliance or port using the Rack Power Manager software Telnet viewer, you can specify session properties to 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 appears containing Terminal, Login Scripts and Logging tabs.

To change the terminal window size:

1. From the *Options* tab drop-down menu, select *Session Properties*.

   -or-

   In the toolbar, click the *Session Settings* icon.
2. In the Session Properties dialog box, click the *Terminal* tab.
3. In the Rows list, select a value of *24* or *48*. The default value is 24.
4. In the Columns list, select a value of *80* or *132*. The default value is 80.

To change the terminal emulation mode:

1. From the *Options* tab drop-down menu, select *Session Properties*.

   - or-

   In the toolbar, click the *Session Settings* icon.
2. In the Session Properties dialog box, click the *Terminal* tab.
3. From the Terminal Emulation list, select one option. The default value is VT100. Terminal Emulation on page 205 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 17.3 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
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. From the *Options* tab drop-down menu, select *Session Properties*.

   -or-

   In the toolbar, click the *Session Settings* icon.

2. In the Session Properties dialog box, click the *Terminal* tab.
3. In the Arrow Keys list, select either *VT100* or *ANSI*. The default value is VT100.

To change the terminal type:

1. From the *Options* tab drop-down menu, select *Session Properties*.

   -or-

   In the toolbar, click the *Session Settings* icon.

2. In the Session Properties dialog box, 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 the following table.

Table 17.4 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. From the *Options* tab drop-down menu, select *Session Properties*.

   -or-

   In the toolbar, click the *Session Settings* icon.

2. In the Session Properties dialog box, 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 checkbox 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 checkbox 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. From the *Options* tab drop-down menu, select *Session Properties*.

   -or-

   In the toolbar, click the *Session Settings* icon.
2. In the Session Properties dialog box, 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 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. From the *Options* tab drop-down menu, select *Session Properties*.

   -or-

   In the toolbar, click the *Session Settings* icon.
2. In the Session Properties dialog box, click the *Terminal* tab.
3. When you are connected to a device that does not repeat or echo the data that you enter, you can enable Local Echo mode. Otherwise, the Telnet viewer does not display the text you enter. However, if you are connected to a device that echoes data, and you are in Local Echo mode, all of the data you enter appears on your terminal twice.

   Enable or disable the Local echo checkbox. The default value is disabled.

To enable/disable 7-bit ASCII:

1. From the *Options* tab drop-down menu, select *Session Properties*.

   -or-

   In the toolbar, click the *Session Settings* icon.
2. In the Session Properties dialog box, click the *Terminal* tab.
3. Enable or disable the Strip 8th bit checkbox.

17.5.1 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 the automatic login in a checkbox.

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 (no initial transmission character), 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 sends as its first prompt. The first Send string indicates what the login script sends to the device after it receives the first Expect string.

You can then build additional Expect and Send strings according to what the particular device prompts for and what is sent in the response.

To build a login script and enable/disable automatic login:

1. From the *Options* tab drop-down menu, select *Session Properties* or in the toolbar, click the *Session Settings* icon.
2. In the Session Properties dialog box, 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, CR+LF, ESC, CTRL+P* (Control+P sequence, 0X10 in hex) or *None*.
5. In the Expect box, enter the alphanumeric string (1-32 characters) that you expect from the device. Spaces are allowed.
6. In the Send box, enter the alphanumeric string (0-32 characters) 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.

17.6 Reviewing Session Data

During a Telnet viewer session, you can 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 is configurable.

You can also 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 return to those specified in the configuration of the Telnet viewer (see Customizing the Telnet Viewer on page 158).

While you are reviewing collected data, new incoming data is buffered, but it is not displayed until you return to the current session location. You cannot enter outgoing data.

To change the maximum number of lines in the session buffer:

1. From the *Options* tab drop-down menu, select *Session Properties*.

   -or-

   In the toolbar, click the *Session Settings* icon.
2. In the Session Properties dialog box, click the *Terminal* tab.
3. In the History Buffer Size field, enter a value from 1-1000. The default value is 256.

To change the background and/or text color when reviewing session data:

1. From the *Options* tab drop-down menu, select *Preferences*.

2. In the Preferences dialog box in the Colors section, click the Background/History Mode box and select a color. (The default color is blue.)

   -or-

   Click the Text/History Mode box and select a color. (The default color is white.)

17.7 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 and are used on DS1800 digital switches. Global macros and personal macros are created using the Video Viewer window. None of these macros can 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 definition of a macro. 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.

A name can be 1-64 characters.

To create a macro:

1. From the *Macros* tab, select *Configure - Macros*.
2. In the Configure Macros dialog box, click *Create*.
3. From the Configure Macros dialog box Edit Macro area, in the Macro Name field, enter a name for the macro.
4. To define a hotkey for the macro, select one from the Key list. To add a modifier to the hotkey, click the *Control*, *Shift* or *Alt* boxes. (The hotkey of a macro is accessible only when the macro belongs to the active macro group.)
5. The default setting has the *Include in Menu* box checked, indicating the macro appears 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 are still able to use the hotkey to run the macro, even if the name oof the macro does not appear in the Macros menu.

6. Enter 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).

NOTE: You must have Rack Power Manager software administrator privileges to use the Access Rights area.

9. Click *OK* to return to the abbreviated view and display the macro 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. From the *Macros* tab, select *Configure - Macros*.
2. From the Configure Macros dialog box, in the Macros table, select the macro you wish to edit and click *Edit*.
3. From the expanded Configure Macros dialog box, in the Edit Macro area, edit the macro properties as needed.
4. Click *OK* to save the changes and return to the abbreviated view of the Configure Macros dialog box.
5. Repeat steps 2-4 to edit additional macros.
6. 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. From the *Macros* tab, select *Configure - Macros*.
2. From the Configure Macros dialog box, in the Macros table, select the macro you wish to delete.
3. Click *Delete* and confirm or cancel the deletion.

To use a macro:

1. From the Macros menu, select the Macro (if the macro definition includes a hotkey, press the hotkey or hotkey sequence. A macro hotkey is accessible only when the macro belongs to the active macro group) or from the Macros menu, select *Configure - Macros* from the menu.
2. From the Configure Macros dialog box, in the Macros table, select the macro and click *Run*.

17.7.1 Macro groups

To create a macro group:

1. Click the *Macros* tab and select *Configure - Groups*.
2. In the Configure Macro Groups dialog box, click the *Create* button.
3. From the expanded Configure Macros dialog box, in the Create Group area Group Name field, enter 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).

NOTE: You must have Rack Power Manager software administrator privileges to assign access rights.

7. Click *OK* and at the abbreviated view of the Configure Macro Groups dialog box, click *OK*.

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. Click the *Macros* tab and select *Configure - Groups*.
2. In the Configure Macro Groups dialog box, 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 and click *OK* to save the changes and return to the abbreviated view of the Configure Macro Groups dialog box.

To edit an existing macro group:

NOTE: You must have Rack Power Manager software administrator privileges to edit global macro groups.

1. Click the *Macros* tab and select *Configure - Groups*.
2. In the Configure Macro Groups dialog box, 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* to save the changes and return to the abbreviated view of the Configure Macro Groups dialog box.
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. Click the *Macros* tab and select *Configure - Groups*.
2. In the Configure Macro Groups dialog box, select the macro group in the Macro Groups table that you wish to delete.
3. Click the *Delete* button and from the dialog box, confirm or cancel the deletion.

17.8 Logging

The Telnet viewer has a logging function that saves the contents of a Telnet viewer session to a file. You can enable automatic logging or dynamically start logging at any time. Additionally, you can 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 following is the format of log filenames, 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 log files. You can change the name of the file and the location of the directory that stores the log files. If you do not change the default directory, log files 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. Click the *Options* tab and select *Session Properties* or in the toolbar, click the *Session Settings* icon.
2. In the Session Properties dialog box, click the *Logging* tab.
3. In the Default Directory field with the current default location for log files, click the *Browse* button.
4. In the Set Directory dialog box, select a directory from the Look in list or create a new directory.
5. If desired, to create a new directory, click the *Create New Folder* button. A new directory named New Folder appears in the directory list.
    a. Click the *New Folder* entry in the directory list to highlight it. Then, click the entry again to edit its name. Enter in a new name. Press Enter. The directory appears in alphabetical order in the directory list.

b. Select the newly-created directory in the directory list. The Filename field will now contain the name of the new directory.

6. 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.
7. 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. Click the *Options* tab and select *Session Properties* or in the toolbar, click the *Session Settings* icon.
2. In the Session Properties dialog box, click the *Logging* tab and then enable the Logging checkbox.
3. The Default Directory field displays the current default location for log files. 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. Click the *Options* tab and select *Session Properties* or in the toolbar, click the *Session Settings* icon.
2. In the Session Properties dialog box, click the *Logging* tab.
3. Disable the Logging checkbox and click *OK*.

Automatic logging stops when you close the Telnet viewer session. When logging stops, the Logging Status label disappears.

To start dynamic logging:

1. Click the *Options* tab and select *Logging - Start*.
2. The Log dialog box appears, 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. Enter 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. Enter a new filename in the Filename field. If you enter a filename that already exists, the new file will overwrite the old file.
4. At the prompt, confirm the directory selection and begin logging or cancel logging.

To pause logging:

From the Options tab, select *Logging - Pause*.

To resume logging:

From the Options tab, select *Logging - Resume*.

To stop logging:

From the Options tab, select *Logging - Stop*.

17.9 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:

From the Options tab, select *Copy Screen* or on the toolbar, click the *Copy Screen* icon.

The window contents are 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:

From the Options tab, select *Copy Buffer* or on the toolbar, click the *Copy Buffer* icon.

The entire buffer is 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:

NOTE: When autoscaling is enabled and the window is scaled, you cannot highlight text until you click the *Restore* icon on the toolbar.

1. Use the mouse to drag-select the portion of the screen text you wish to copy.
2. Click the *Options* tab and select *Copy Text*.

   -or-

   On the toolbar, click the *Copy Text* icon.

   -or-

   Right-click and select *Copy Text* from the pop-up menu.

The highlighted text is copied to the system clipboard. You can paste the clipboard contents into a Telnet viewer session or in to 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, from the menu, select *Options - Paste* or on the toolbar, click the *Paste* icon.

To print a Telnet viewer window screen:

1. Click the *Options* tab and select *Print Screen* or on the toolbar, click the *Print Screen* icon.
2. In the operating system print dialog box, make the appropriate settings to send the screen contents to the printer.

17.10 Power Control of Devices Attached to Power Devices

NOTE: You 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 is accessed in a serial session, you can 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 is not 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 turn on, turn off or power cycle a target device:

1. From the Telnet viewer window, select *Options - Power*.
2. In the Power Control dialog box, click *On*, *Off* or *Cycle*.
3. Click *Close* to close the dialog box.

17.11 Closing a Telnet Viewer Session

To close a Telnet viewer session:

From the Telnet viewer window, select *File - Exit*.

This page intentionally left blank.

18 USING TOOLS

The Rack Power Manager management software contains tools that can be used to perform various actions on units.

18.1 Using the Units Tools Window

The Units Tools window contains tools that allow you 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

To display the Units Tools window:

From the Units tab, in the side bar, click *Tools*.

18.1.1 Exporting units

The Export Units tool is used to export information about units into a .csv file. Unit names are always exported and the following unit properties can be selected for export:

- Action (default action; primary contact phone)
- Appliance Version
- Asset Tag Number
- Browser URL (secondary contact)
- Custom field 1-10 (secondary contact phone)
- Department (serial number)
- DHCP
- IP Address
- Location (Telnet port)
- Migration Status
- Model Number (type)
- OSCAR™ (graphical user interface)
- Part Number (visibility - show or hide)
- Primary Contact
- Primary Contact Phone
- Rack Power Manager Server (name site)
- Secondary Contact
- Secondary Contact Phone
- Secure Mode
- Serial Number
- Site
- Status
- Telnet Port
- Type
- Visibility

You can also export a topology report, regardless of any properties selected for export. A topology report contains the following columns:

- Port - Port number on the appliance to which the target device or cascade switch is connected (target devices or cascade switches only).
- Type - Appliance type, if known (managed appliances only).
- 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 can be viewed in a text editor or spreadsheet application, such as Microsoft® Excel®. The default is configured to open the .csv files in Microsoft Excel. If Microsoft Excel is not installed on your computer, you are prompted to select a text editor to open the .csv file.

The default filename of the .csv file is unitproperties.csv. Subsequent exported files are incremented (unitproperties[1].csv, unitproperties[2].csv and so on).

To export units:

1. Click the *Units* tab, and in the side bar, click *Tools*.
2. In the Unit Tools window, click *Export Units*.
3. From the Export Units Wizard, if applicable, select one or more properties from the Available Properties or Properties to Export list and click *Add* or *Remove* to move the properties to the desired list.
4. If applicable, select one or more properties in the Properties to Export list and use the up and down arrows to move the selected properties to change the order of the properties in the output .csv file.
5. To create a topology report, enable the Export Topology checkbox and click *Next*.

NOTE: If any properties are also being exported, they are listed after the topology information in the report.

6. In the Save Process window, click *Next*.
7. After the Completed Successful window and File Download dialog box open, click *Open* to download and open the file.

   -or-

   Click *Save* and select a directory and filename in the Save As dialog box. Then click *Save* to save the .csv file.

8. Click *Finish*.

18.1.2 Exporting access rights

From the Rack Power Manager management software host, the Export Access Rights tool exports permissions information about units. The unit name and the user/user group to which the unit has access rights are exported, as well as the unit access right settings. See About Access Rights on page 100.

If you are exporting managed appliance rights, the default filename of the .csv file is appliance_rights.csv. If you are exporting target device rights, the default name is target_device_rights.csv. Subsequent files that you export are incremented (target_device_rights[1].csv, target_device_rights[2].csv and so on). The output .csv file can be viewed in a text editor or spreadsheet application. The default setting opens the

.csv files in Microsoft® Excel®; however, if Microsoft® Excel® is not installed on your computer, you are prompted to select a text editor to use for opening the .csv file.

To export access rights:

1. Click the *Units* tab, in the side bar, click *Tools*.
2. In the Unit Tools window, click *Export Access Rights*.
3. From the Export Access Rights Wizard, in the drop-down menu, select the *All Units*, *Appliances*, *Outlets* or *Unit Groups* type and click *Next*.
4. In the Save Process window, read the text and click *Next*.
5. When prompted, enter the location and filename where the exported access rights are to be saved.
6. In the File Download dialog box, click *Open*.

   -or-

   Click *Save* and select a directory and filename in the Save As dialog box. Then click *Save* to keep the .csv file.
7. Click *Finish*.

18.2 Using the Managed Appliance Tools

The Rack Power Manager management software contains tools to complete the following tasks on supported PDUs:

- Rebooting
- Upgrading the firmware
- Resynchronizing the managed appliance to reflect the current Rack Power Manager software system configuration
- Saving or restoring the configuration
- Saving or restoring the database of local users

To access the managed appliance tools:

1. Click the *Units* tab, and in the side bar, click *Appliances*.
2. Under Appliances, click a link to display specific types of managed appliances.

   -or-

   Click *Sites* and click a site link.

   -or-

   Click the Custom Field Labels and the label you specified for the managed appliance.

   -or-

   Click *Recently Accessed*.
3. Click the name of a managed appliance to view the applicable tool options in the Unit Overview window.

18.2.1 Rebooting

Rebooting managed appliances from the Unit Views or Unit Overview window disconnects all active sessions.

From the Unit Views window, a Multiple Unit Operation window opens, containing a link to another window where results can be viewed.

You must have Reboot Appliance access rights to reboot a serial console appliance. The default setting allows pre-defined groups, such as Rack Power Manager software administrators, user administrators and appliance administrators to have this access right.

For more information, see the following:

- Multiple Operations from a Unit Views Window on page 79
- Accessing the Unit Views windows on page 77
- About Access Rights on page 100

To reboot one or more managed appliances from a Unit Views window:

1. From the *Units - Unit Views* tab, and in the Appliances - All window with populated managed appliances, click the checkboxes of the applicable appliances.

NOTE: Rebooting does not affect the unmanaged units.

2. Click *Operations* and from the menu, select *Reboot*.
3. In the confirmation dialog box, confirm or cancel the reboot.

To reboot a managed appliance from a Unit Overview window:

1. From the Unit Overview window, click *Reboot*.
2. In the confirmation dialog box, confirm or cancel the reboot.

18.2.2 Upgrading firmware

The firmware on each managed appliance is upgraded in the order shown in the Update list. A reboot is automatically performed between each firmware update.

A valid Flash file must exist in the firmware repository of the Rack Power Manager server 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 185.

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.

To upgrade the firmware on a managed appliance:

1. From the Unit Overview window, click *Upgrade Firmware*.
2. From the Upgrade Appliance Firmware Wizard, in the Select Firmware Files window, select one or more files in the Available Firmware Files list or Firmware Files to Update list and click *Add* or *Remove* to the Flash files to the desired list.

   -or-

Select one or more files in the Firmware Files to Update list and use the up and down arrows to move the selected files up or down in the list.

3. Click *Next*, and in the Type in Task Name window, enter a name (1-64 characters) for the upgrade firmware task and click *Next*.
4. From the Completed Successful window, click the *Click here to view results* link.
5. Optionally, you can click the *System - Tasks* tabs to view the progress.
6. When complete and the upgrade task is removed from the task list, click *Finish*.

18.2.3 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 updates these and other changes made to the unit within the Rack Power Manager software system.

Resynchronizing forces 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 can use the automatic topology synchronization feature or synchronize selected units manually from a Unit Views window. See Topology Synchronization on page 89.

For more information about the resync options, see Topology synchronization options in the Resync Wizard on page 90.

To resynchronize a unit:

1. From the Unit Overview window, click *Resync*.
2. In the Select Resync Options window, enable the Remove offline connections checkbox to remove any connections from the Rack Power Manager software database 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.

   -or-

   Enable the Delete target devices that no longer have connections checkbox to delete those target devices permanently from the Rack Power Manager software database.

   -or-

   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.

   -or-

   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.

3. Click *Next*, and if the unit does not require resynchronizing, go to step 6.

   -or-

   If the unit requires resynchronizing, click *Next* on the Changes Detected in Appliance window, and proceed to the next step.

4. Select the type of each detected cascade switch and enter a name for each cascade switch.

5. If combining any multiuser cascade switches, click the checkboxes of the cascade switches that you wish to merge and click *Merge*.

   -or-

   If unmerging cascade switches, click the checkbox of the merged cascade switch and click *Split*.

6. Click *Next*, and in the Completed Successful window, click *Finish*.

18.2.4 Saving a managed appliance configuration

You can save the configuration of a PDU to a file. The configuration file contains information about the managed appliance, including the following:

- Global settings
- Port settings
- SNMP trap settings
- SNMP manager settings
- Names of connected target devices

For information on restoring a configuration file, see the following section.

To save a managed appliance configuration to a file:

1. From the Unit Overview window, click *Save Configuration*.
2. From the Save Appliance Configuration Wizard, enter a description of the configuration to be saved (if restoring the configuration at a later time) and click *Next*.
3. In the Completed Successful window, click *Finish*.

18.2.5 Restoring a managed appliance configuration

The configuration of a serial console appliance can be restored. In order to restore the configuration, a previously-saved configuration file must exist. See the previous section to save a managed appliance configuration.

Appliance configuration files are stored in the Rack Power Manager server appliance files repository. You can display the available configuration files by clicking the *System - Appliance Files* tabs and clicking *Configuration* in the side bar.

To restore a managed appliance configuration:

1. From the Unit Overview window, click *Restore Configuration*.
2. From the Restore Appliance Configuration Wizard, click the radio button of the file containing the configuration to be restored and click *Next*.
3. In the Completed Successful window, click *Finish*.
4. In the Unit Overview window, reboot the managed appliance to enable the restored configuration.

18.2.6 Saving a managed appliance user database

NOTE: The user database of a DS1800 digital switch cannot be saved.

To save the user database of a managed appliance:

1. From the Unit Overview window, click *Save User Database*.

2. From the Save Appliance User Database Wizard, enter a description of the user database to be saved (if you wish to restore the database) and click *Next*.
3. In the Completed Successful window, click *Finish*.

18.2.7 Restoring a managed appliance user database

NOTE: The user database of a DS1800 digital switch cannot be restored.

A previously saved user database file must exist to restore the local user database of a serial console appliance. See the previous section to save a managed appliance user database.

User database files are stored in the Rack Power Manager server appliance files repository.

To display available database files:

Click the *System - Appliance Files* tabs, and in the side bar, click *User Database*.

To restore the user database of a managed appliance:

1. In the Unit Overview window, click *Restore User Database*.
2. In the Restore Appliance User Database Wizard, click the radio button of the managed appliance user database to be restored and click *Next*.
3. In the Completed Successful window, click *Finish*.
4. In the Unit Overview window, reboot the managed appliance to enable the restored user database.

This page intentionally left blank.

19 MANAGING TASKS

The following tasks can be added, deleted and changed from the Tasks window:

- Backing up the software database and system files
- Configuring SNMP trap settings on an appliance
- Controlling the power of target devices
- Controlling the power of custom groups
- Exporting an event log to comma separated values (.csv) file
- Upgrading firmware of selected appliances of the same type
- Validating external authentication server user accounts
- Pulling names from selected units
- Updating topology for selected units

19.1 Using the Tasks Window

The Tasks window lists all tasks configured in the Rack Power Manager management software system and allows you to schedule or manually run tasks.

The following fields can 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 21 to modify fields.

- Runs On - Server(s) on which the task runs.
- Next Run - Next date and time the task is scheduled to run. This field is 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 is 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 19.1 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

19.2 Adding and Running Tasks

Tasks can be run in the following intervals:

- Run task now - Runs the task immediately after you click *Finish* when adding the task in the Add Task Wizard. The Status column indicates the task is running and the running icon is displayed beside 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 can also specify which days to run the task.
- 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 can also specify which months to run the task.

To run a task periodically:

1. Click the *Systems - Tasks* tabs and click *Add*.
2. In the drop-down menu on the Select Task to Add window, select the task type and enter the task name.
3. Select *Periodic* in the Frequency drop-down menu and click *Next*.
4. In the Schedule the task window, select (from the Calendar drop-down menu) or enter the date to begin running the task. Then, use the drop-down menus to select the hour, minute and AM or PM.
5. Click the Every (minutes) or the Every (hours) radio button, use the arrows to select the applicable number of minutes or hours and click *Next*.
6. If desired, specify the applicable RPM System Backup Properties and click *Finish*.

To run a task daily:

1. Click the *System - Tasks* tabs.
2. In the Select a task to schedule window, click *Add*.
3. In the drop-down menu on the Select Task to Add window, select the task type and enter the task name.
4. Select *Daily* from the Frequency drop-down menu and click *Next*.
5. In the Schedule the task window, select (from the calendar drop-down menu) or enter the date to begin running the task. Then, use the drop-down menus to select the hour, minute and AM or PM.
6. Click Every Day, Weekdays or Every (days), and if you select Every (days), select the number of consecutive days (1-365) and click *Finish*.
7. If desired, specify the applicable RPM System Backup Properties and click *Finish*.

To run a task weekly:

1. Click the *System - Tasks* tabs.
2. In the Select a task to schedule window, click *Add*.
3. In the drop-down menu on the Select Task to Add window, select the task type and enter the task name.

4. Select *Weekly* in the Frequency drop-down menu and click *Next*.
5. In the Schedule the task window, select (from the calendar drop-down menu) or enter the date to begin running the task. Then, use the drop-down menus to select the hour, minute and AM or PM.
6. For recurring tasks *Every (weeks)*, select the number of weeks between running the task (1-52) and select the day of the week to run the task from the list box.

NOTE: Multiple weeks can be selected by pressing Ctrl while clicking the weeks.

7. If desired, specify the applicable RPM System Backup Properties and click *Finish*.

To run a task monthly:

1. Click the *System - Tasks* tabs.
2. In the Select a task to schedule window, click *Add*.
3. In the drop-down menu on the Select Task to Add window, select the task type and enter the task name.
4. Select *Monthly* from the Frequency drop-down menu and click *Next*.
5. In the Schedule the task window, select (from the calendar drop-down menu) or enter the date to begin running the task. Then, use the drop-down menus to select the hour, minute and AM or PM.
6. For recurring tasks, click the Day radio button, select the number of days the task is to occur.
7. Click the radio button, click a week, a day of the week and month 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.

NOTE: Multiple months can be selected by pressing Ctrl while clicking the months.

8. If desired, specify the applicable RPM System Backup Properties and click *Finish*.

19.3 Running Tasks Manually

Although tasks are scheduled to run at particular times using the Add Task Wizard, you can also run an existing task at any time. When a task is running, the icon of the task name changes to the running icon and the status of the task changes to Running.

Remote tasks that are scheduled on another Rack Power Manager server cannot 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.

To manually run tasks:

1. Click the *System - Tasks* tabs.
2. In the Tasks window, click the checkbox of the tasks you wish to run and click *Run Now*.

19.4 Adding Tasks Using the Add Task Wizard

Tasks may be added only by Rack Power Manager software administrators. When adding a task, the task name can be 1-64 characters.

19.4.1 Task: Backing up the Rack Power Manager software database and system files

Servers can be backed up and restored automatically by creating a task within the Rack Power Manager software. This task creates a compressed .zip file, which contains a backup of your Rack Power Manager

software system with everything necessary to fully restore the Rack Power Manager software hub server. The default name of the backup file is rpmBackup.zip, but you can append the date and time to the end of the backup filename. After this task is added, you can run it manually at any time.

The directory location of the backup file can be a physical local drive on the Rack Power Manager server or a shared network location specified by a UNC (Universal Naming Convention) path, but cannot be set to a mapped network drive.

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 is programmed into the managed appliances. Also, if your operating system supports case sensitive filenames, the directory name must be entered in case sensitive text.

NOTE: If you use the Backup RPM database and system files task, client sessions are not temporarily disconnected.

For more information, see the following:

- Adding and Running Tasks on page 179
- Running Tasks Manually on page 181
- Backing up and Restoring Hub Servers Manually on page 50

To add the task:

1. Click the *System - Tasks* tabs.
2. In the Tasks window, click *Add*.
3. In the Select Task to Add window, from the Task Type drop-down menu, select *Backup Databases and System files*.
4. Enter a name for the task, select the frequency to run the task and click *Next*.
5. In the Specify RPM System Backup Properties dialog box, enter the directory location in which to create the system backup.
6. If the specified directory location is a network path that requires a login, enable the Login required to access shared drive location checkbox.
7. After enabling the Login required to access shared drive location checkbox, enter the username and password and confirm the password of a user account that has read/write access to the network share location.
8. Encrypt the created system backup file by enabling the Encrypt Backup File checkbox, then enter a password to lock or unlock the encrypted file.
9. Append the date and time (in military time) to the end of the system backup filename by clicking the Use date and time for file naming checkbox. For example, if you create the backup file on October 1, 2005 at 10:04 PM, the created file is named rpmBackup1001052204.zip.

NOTE: If a system backup file already exists in the specified directory and this option is not enabled, the existing backup file is overwritten when the new backup file is created.

10. Click *Finish*.

19.4.2 Task: Configuring 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 traps for other types of managed appliances, you must create additional tasks.

After this task is added, you can run it manually at any time.

For more information, see the following:

- Adding and Running Tasks on page 179
- Running Tasks Manually on page 181
- Managed Appliance SNMP Settings on page 103

To add the task:

1. Click the *System - Tasks* tabs.
2. In the Tasks window, click *Add*.
3. In the Select Task to Add window, from the Task Type drop-down menu, select *Configure SNMP trap settings on appliance* and enter a name for the task.
4. Select a time to run the task and click *Next*.
5. In the Select Unit Group window, select *All Appliances* or select a unit group and click *Next*.
6. In the Select Appliance Type window, select the type of managed appliance for which to configure SNMP traps and click *Next*.
7. In the Select Appliances window, select one or more managed appliances from the Available Appliances list, click *Add* to move the units to the Appliances to Configure list and click *Next*.
8. In the Configure SNMP Traps window, select one of the following from each trap menu to change the trap state and 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
9. Click *Finish*.

19.4.3 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.

After this task is added, you may run it on demand at any time.

For more information, see the following:

- Running Tasks Manually on page 181
- Creating an Event Log .csv File on page 195
- Adding and Running Tasks on page 179

To add the task:

1. Click the *System - Tasks* tabs.
2. In the Tasks window, click *Add*.

3. In the Select Task to Add window, from the Task Type drop-down menu, select *Export event log to a comma separated values (.CSV) file* and enter a name for the task.
4. Select a time to run the task and click *Next*.
5. In the Specify Export Event Log Properties window, enter 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.
6. 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, enter the username and password and confirm the password of a user account that has read/write access to the network share location.
7. If applicable, 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.

NOTE: 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.

8. Click *Next*.
9. In the Select Event Log Columns to Export window, add one or more columns to export by selecting the column(s) from the Available Columns list and click *Add* to move the columns to the Columns to Export list.

   -or-

   Select the column(s) from the Columns to Export list and click *Remove* to remove one or more columns to export.

   -or-

   Select one or more columns in the Columns to Export list and use the up and down arrows to change the order in which exported columns are listed in the output .csv file.
10. Click *Finish*.

19.4.4 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 directory can be a physical local drive on the Rack Power Manager server or at a shared network location specified by a UNC path, but the location cannot be set to a mapped network drive. The directory name must also be entered in case sensitive text if your operating system supports case sensitive filenames. After this task is added, you can run it manually at any time.

The exported file can be stored on a local or network drive. The default name for the exported report is assetreport.csv, but you can append the date and time (in military time) to the end of the filename. For example, if you are creating the file on October 1, 2010 at 10:04 PM, the created file is named assetreport1001102204.csv. The output .csv file can be viewed in a text editor or spreadsheet application, such as Microsoft Excel.

For more information, see the following:

- Adding and Running Tasks on page 179
- Running Tasks Manually on page 181

To add the task:

1. Click the *System - Tasks* tabs.
2. In the Tasks window, click *Add*.
3. In the Select Task to Add window, from the Task Type drop-down menu, select *Export Asset Report to a comma separated values (.CSV) file* and enter a name for the task.
4. Select a time to run the task and click *Next*.
5. In the Specify Export Asset Report Properties window, enter the directory in which to create the file.
6. 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, enter the username and password and confirm the password of a user account that has read/write access to the network share location.
7. If desired, enable the Use date and time for file naming checkbox.

NOTE: If an exported report file exists in the specified directory and you do not enable the Use date and time for file naming checkbox, the existing file is overwritten when the new file is created.

8. Click *Finish*.

19.4.5 Task: Updating the firmware of an appliance type

This task upgrades the firmware of selected DS1800 digital switches, DSI5100, CPS or CCM appliances. To upgrade other types of managed appliances, you must create additional tasks.

The firmware must be available before using this command.

After this task is added, you can run it manually at any time.

For more information, see the following:

- Firmware Management on page 189
- Running Tasks Manually on page 181
- Adding and Running Tasks on page 179
- Unit Groups on page 119

To add the task:

1. Click the *System - Tasks* tabs.
2. In the Tasks window, click *Add*.
3. In the Select Task to Add window, from the Task Type drop-down menu, select *Upgrade firmware of selected appliances of the same type*.
4. Enter a name for the task, select a time to run the task and click *Next*.
5. In the Select Unit Group window, from the menu, select *All Appliances* or select a particular unit group to upgrade and 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.

6. In the Select Appliance Type window, select the type of managed appliance to be upgraded and click *Next*.

7. In the Select Appliances window, select one or more managed appliance to be upgraded from the Available Appliances list and click *Add* to move the appliances to the Appliances to Configure list.
8. Click *Finish*.

19.4.6 Task: Validating user accounts on an external authentication server

This task is 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 are flagged as suspicious (a question mark icon appears beside the username). Suspicious accounts are indicated in event log files. After this task is added, you can run it manually at any time.

For more information, see the following:

- Adding and Running Tasks on page 179
- Running Tasks Manually on page 181

To add the task:

1. Click the *System - Tasks* tabs.
2. In the Tasks window, click *Add*.
3. In the Select Task to Add window, from the Task Type drop-down menu, select *Validate external authentication server user accounts*.
4. Enter a name for the task and from the Frequency drop-down menu, select a time to run the task, then click *Finish*.

19.4.7 Task: Pulling names from selected units

This task is 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. After this task is added, you can run it manually at any time.

For managed appliances that do not support automatic name pull, you can instead schedule the pull names task to keep the appliances synchronized with the Rack Power Manager software.

For more information, see the following:

- Name Synchronization (Push and Pull) on page 87
- Adding and Running Tasks on page 179
- Running Tasks Manually on page 181

To add the task:

1. Click the *System - Tasks* tabs.
2. In the Tasks window, click *Add*.
3. In the Select Task to Add window, from the Task Type drop-down menu, click *Pull Names from selected units* and enter a name for the task.
4. Select a time to run the task and click *Next*.
5. In the Select Unit Group window, select *All Units* or select a unit group and click *Next*.
6. In the Select Unit window, select the units to be included in the topology update, then click *Add* and *Finish*.

19.4.8 Task: Updating topology for selected units

This task updates the Rack Power Manager software database when a change occurs in a power device or an associated appliance, such as adding/removing a cascade switch or power device. After this task is added, you can run it manually at any time.

NOTE: This task performs the same operations as the Resync Unit Wizard.

Automatic topology synchronization is not supported on some units supported by plug-ins. To keep these units synchronized with the Rack Power Manager software, you can instead schedule the update topology task.

Table 19.2 Select Options Window Task Descriptions

CHECKBOX	TASK DESCRIPTION
Remove offline connections	Deletes any unit connections that are reported as offline in the unit, from the Rack Power Manager software database.
Delete target devices that no longer have connections	Permanently deletes target devices that no longer have connections, from the Rack Power Manager software database.
Allow target devices with the same name to be merged into a single target device	Merges the connection to a target device in the unit with the connection(s) to an existing target device in the Rack Power Manager software database.
Allow target devices that contain default names to be added for these types of connections	Adds any target devices that contain default names in the unit to the Rack Power Manager software database only if the connection type in the unit matches an enabled connection type in this window. This selection allows you to enable one or more connection type checkboxes.

For more information, see the following:

- Resynchronizing units on page 175
- Automatic topology synchronization on page 89
- Adding and Running Tasks on page 179
- Running Tasks Manually on page 181

To add the task:

1. Click the *System - Tasks* tabs.
2. In the Tasks window, click *Add*.
3. In the Select Task to Add window, from the Task Type drop-down menu, select *Update Topology for selected units* and enter a name for the task.
4. Select a time to run the task and click *Next*.
5. In the Select Unit Group window, select *All Units* or select a unit group and click *Next*.
6. In the Select Unit window, select the units to be included in the topology update, click *Add* and *Next*.
7. In the Select Options window, click the desired task and click *Finish*.

19.5 Displaying Task Results

The Task Results window displays the status of the most recently run tasks.

The following fields are displayed 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 - Tasks* tabs.
2. In the Tasks window, click the name of the task and verify the displayed information.

19.6 Changing Tasks

This task is used to change the schedule and properties for existing tasks. (The Validate external authentication server user accounts task does not contain properties.)

NOTE: Remote tasks that are scheduled on another Rack Power Manager server cannot 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 is created.

To change a task schedule:

1. Click the *System - Tasks* tabs.
2. In the Tasks window, click the name of the task.
3. In the side bar, click *Schedule*.
4. In the Task Schedule window, see Adding and Running Tasks on page 179 to select the type of task to be scheduled and complete the information.

To change the properties of a task:

1. Click the *System - Tasks* tabs.
2. In the Tasks window, click the name of the task.
3. In the side bar, click *Properties*.
4. In the Task Properties window, change the properties of the task.

NOTE: See the operating sequence for the task type in Adding Tasks Using the Add Task Wizard on page 181.

19.7 Deleting Tasks

Remote tasks that are scheduled on another Rack Power Manager server cannot 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 is created.

To delete a task:

1. Click the *System - Tasks* tabs.
2. In the Tasks window, click the checkboxes of the tasks to be deleted and click *Delete*.
3. On the confirmation dialog box, confirm or cancel the deletion.

20 FIRMWARE MANAGEMENT

The Flash firmware files for Avocent® DS1800 digital switches, Avocent® DSI5100 proxy appliance, Avocent® CPS serial over IP network appliance and Avocent® CCM console management appliances may be added, viewed and deleted in the Appliance Firmware Files window. After one or more Flash firmware files are added, you can use the files to upgrade the managed appliance.

To display the Appliance Firmware Files window:

Click the *System - Appliance Files* tabs.

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. After the file is uploaded, it is no longer needed on the Rack Power Manager software client from which it was uploaded. See Using the Customize link in windows on page 21.

To add a firmware file:

1. Click the *System - Appliance Files* tabs.
2. In the Appliance Firmware Files window, click *Add*.
3. From the Add Firmware File Wizard, 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.
4. Enter a description of the firmware file and click *Next*.
5. In the Completed Successful window, click *Finish*.

To display firmware information:

1. Click the *System - Appliance Files* tabs.
2. From the Appliance Firmware Files window, in the top bar, click *Appliance Files* and click the version of the firmware file.
3. In the Firmware File Properties window, if applicable, change the firmware file description, then click *Save* and *Close*.

To delete firmware:

1. Click the *System - Appliance Files* tabs.
2. In the Appliance Firmware Files window, click the checkbox of the firmware to be deleted.
3. Click *Delete*, and in the confirmation dialog box, confirm or cancel the deletion.

This page intentionally left blank.

21 MANAGING EVENTS AND EVENT LOGS

Events are predefined and are classified by severity and category. Events can also be enabled or disabled. When an enabled, defined event occurs in the Rack Power Manager software system, it is saved in the event log. You can display the event log content, view details about an individual event log entry or delete an event log entry. The retention period of the event log can be changed and content of the event log can be exported. An email notification can be sent to one or more addresses when an event occurs.

NOTE: You must be a member of the Rack Power Manager software administrator or auditor user group to access event configuration and display windows.

21.1 Event Severity Levels

The following table describes severity levels and associated icons for events, which are displayed in the event logs.

Table 21.1 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.

For software administrators or auditor user groups of the Rack Power Manager, the non-critical, critical and non-recoverable icons also appear near the right edge of the top bar in the Rack Power Manager 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 the state of an event is changed from New to Acknowledged (see Event states on page 194). The counter is incremented when a new event of that severity is added to the log or when the state of an event is changed from Acknowledged to New.

21.2 Event Categories

Defined events can be classified in the following categories:

- Access control
- Appliance
- Authentication
- External
- IPMI

- Modem
- Sessions
- System
- Tasks
- Units
- Unit status
- Users

21.3 Enabling and Disabling Event Logging

The logging of individual events that occur in the Rack Power Manager software system can be enabled or disabled. Events cannot be enabled unless they are already disabled and cannot be disabled unless they are already enabled. When an enabled event occurs, it is written to the event log. When an event is disabled, its occurrence is not logged until the event is enabled.

The default setting for the Enabled Log Events window lists the event name and if it is enabled or disabled. (The enabled/disabled state differs from the state of an event in the event log; see Event states on page 194.) You can change fields and the number of items per window to be displayed in the Enabled Log Events window by clicking the *Customize* link (see Using the Customize link in windows on page 21). 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, and in the side bar, click *Enabled Events*.
2. From the Enabled Log Events window, in the side bar, click a category link to display only events in that category.
3. Click the applicable event checkboxes on the page and click *Enable* or *Disable*.
4. Verify the Enabled Log Events window refreshes with the new information.

21.4 Displaying the Event Log

Event logs can be customized by displaying the following event categories:

- All events (or at least the most recent 5000) in the log
- Events of a particular severity or a particular category
- Events that occurred during a specified interval
- Events based on their state

The Event Information window displays the Event History table containing state changes, including when a state is changed, the type of change and who made the change.

Event log display fields

The following fields are always displayed in the Event Log window:

- Severity - Displays the Event Information window, which contains details about the event.
- Date/Time - Displays the date and time of an event in the time zone of the client server.
- Description - Displays a short description of an event.

The following fields can be displayed. Use the Customize link to add or remove fields in the display. See Using the Customize link in windows on page 21.

- State - New or Acknowledged. See Event states on page 194. 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:

From the *Reports* tab, in the Event Log - All window, perform one of the following procedures:

- To display event log entries by severity, click *Severity Level* in the side bar and click one of the levels.
- To display event log entries by category, click *Event Category* in the side bar and click one of the categories.
- To display event log entries that occurred during a specified interval, see Using the date filter on page 194.
- To display events with the Acknowledged state and display the State column, click the *Show All* button. (The State column is added to the display and the list includes events with either the New or Acknowledged state. Acknowledged events are grayed-out to differentiate them from those with the New state, but any event can be selected.)

  -or-

  To remove events with an Acknowledged state from the display and hide the State column, click the *Show All* button again. (The State column is removed from the display and only unacknowledged events, such as an event with the New state are displayed.)

NOTE: You can also display a list of only the new non-critical, critical or non-recoverable event log entries by clicking the appropriate icon in the top bar.

To display details of an event log entry:

1. Click the *Reports* tab.
2. In an Event Log window, click a link in the Severity column and click *Close*.

To delete one or more event log entries:

1. Click the *Reports* tab, and in the Event Log window, click the checkboxes of the events to be deleted.
2. Click *Delete,* and in the confirmation dialog box, confirm or cancel the deletion.

21.4.1 Event states

When an event first occurs and is placed in the event log, it is considered to be in the New state. You can delete the event, which removes it from the event log. However, if you wish to prevent an event from being displayed without deleting it from the event log, you can acknowledge the event, which changes its state from New to Acknowledged.

You can also change the state of an event from Acknowledged to New again. This can be useful if you mistakenly change the state of an event to Acknowledged. The Event Information window for each event contains an Event History that indicates when the state of an event is changed and by whom.

When you change a non-recoverable, critical or non-critical event state to Acknowledged, the counter next to that severity icon in the top bar is decremented. If you change one of these events from Acknowledged to New, the counter is incremented.

Event logs can be filtered by severity, category or date. In a displayed event log, if the Show All button is not enabled, the display only includes events with the state New. If the Show All button is enabled, events in any state (New or Acknowledged) are included and Acknowledged events are grayed-out.

To change the state of one, more than one or all event log entries:

1. Click the *Reports* tab, and in the Event Log - All window, click the applicable event checkboxes.
2. Click *Set State*, and from the drop-down list, select *Acknowledged* or *New*.

21.4.2 Using the date filter

The event log retains all events occurring in the Rack Power Manager software system for the specified retention time. You can display older events or display events from any interval in the retention time. The default configuration displays the 5000 most recent events.

To use the date filter:

1. Click the *Reports* tab, and in any Event Log window, click *Date Filter*.
2. From the Date Filter window, in the From: drop-down menu, select *Events On* to select the start date and time.
3. Click the calendar icon or calendar field.
4. Click a day in the calendar to close the calendar and fill the calendar field with the selected date.

NOTE: The arrows on the top of the calendar can be used to move forward and backward by month.

5. Select an hour, minute and *AM* or *PM* for the start date.
6. In the To: drop-down menu, select *Events On* to select the end date and time.
7. Repeat steps 3 and 4 to specify the end date and click *Apply*.

NOTE: The previous Event Log view window opens with the event range specified in the Filter Date window. In the Event Log view window, you can click the *Clear Date Filter* button to clear date filtering.

21.5 Changing the Event Log Retention Period

Event log information is stored in the Rack Power Manager software database and can be replicated. The default setting retains the event log for seven days. You can specify a retention period of up to 365 days.

NOTE: 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 183. You can also export event logs at any time; see the next section.

To change the event log retention period:

1. Click the *Reports* tab, and in the side bar, click *Log Retention*.
2. In the Event Log Retention Time window, enter the number of days (1-365) in the Days field or use the menu.
3. Click *Save*.

21.6 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 .csv file can be viewed in a text editor or spreadsheet application, such as Microsoft Excel. The default name for the output event log file, eventlog.csv, can be changed when it is saved.

NOTE: To create a task to export the event log to a .csv file, see Task: Exporting an event log .csv file on page 183.

To create an event log .csv file:

1. Click the *Reports* tab, and in the side bar, click *Tools*.
2. In the Event Log Tools window, click the *Export Event Log* icon or text.
3. If applicable, in the Select Columns to Export window, select the columns from the Available Columns list or Columns to Export list and click *Add* or *Remove* to move the columns to the desired list.

   -or-

   Change the order in which exported columns are listed in the output .csv file by selecting one or more columns in the Columns to Export list and using the up and down arrows to move the selected columns up or down in the listing.
4. Click *Next* and in the displayed Save Process window (explaining how the file is saved), click *Next*.
5. In the File Download dialog box, click *Open* and open the file on the Rack Power Manager software client.

NOTE: The default is set to open the .csv files in Microsoft Excel. If Microsoft Excel is not installed on your computer, a prompt allows you to select a text editor to open the .csv file.

   -or-

   From the File Download dialog box, click *Save*, and in the Save As dialog box, select a directory and filename, then click *Save*.
6. Click *Finish*.

21.7 Configuring Email Notifications

The Rack Power Manager software can be configured to send one or more users an email notification when an enabled event occurs. Requirements for this feature include:

- A mail server that supports Simple Mail Transfer Protocol (SMTP) must be configured in order to receive email event notifications.

- The Send to field for email addresses must not exceed 1024 characters and multiple addresses must be separated with a comma (,).
- The email address in the From field and the Subject heading fields must be 1-64 characters.

You can specify which events trigger an email notification or specify an email notification is 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, such as when a Rack Power Manager server starts, an email notification is sent, regardless of any specified unit groups. After an email notification is created, you can send a test message to ensure that the notification is delivered to the specified recipients.

21.7.1 Event notifications to other applications using the Web Service

The Rack Power Manager software can be configured to send or receive web service notifications when an enabled event occurs.

NOTE: Contact Vertiv Technical Support to configure web service notifications to third party hardware or software.

To configure web service notifications:

1. Click *Reports - Event Log - Web Service Notifications*.
2. To add a web service notification, click *Add*, configure the fields on the Add Web Service Notification Wizard and click *Save*.

   -or-

   To remove a web service notification, click *Delete - OK*.

   -or-

   To change the settings of a web service notification, click *Edit*, configure the fields on the Edit Web Service Notification Wizard and click *Save*.

21.7.2 Customizing the Email Notifications window

The Email Subject column is always displayed in the Email Notifications window; however, the Customize link can be used to add or remove fields in the display, such as the From Address and To Address fields. See Using the Customize link in windows on page 21.

To configure an email notification:

1. Click the *Reports* tab, and in the side bar, click *Email Notifications*.
2. In the Email Notifications window, click *Add*.
3. From the Add Email Notification Wizard, in the Send To field of the Specify Email Properties window, enter the email addresses of the persons to be notified.
4. In the From field, enter the email address of the person you wish to designate as the sender of the notification.
5. In the Subject field, enter a subject heading for the notification and click *Next*.
6. If applicable, in the Select Events to Trigger Email Notification window, select the events from the Available Events list or Events To Notify list and click *Add* or *Remove* to move the events to the desired list.
7. Click *Next*.

8. If applicable, in the Select Unit Groups to Trigger Email Notification window, select the unit groups from the Available Unit Groups list or Selected Unit Groups list and click *Add* or *Remove* to move the units to the desired list.
9. Click *Next*, and in the Completed Successful window, click *Finish*.

To change an email notification:

1. Click the *Reports - Event Log* tabs, and in the side bar, click *Email Notifications*.
2. In the Email Notifications window, click the email subject of the notification you wish to change.
3. In the Email Notification Properties window, update the Send To, From and Subject fields.

   -or-

   Select the events or unit groups from the lists and click *Add* or *Remove* to move the events or unit groups to the desired list.
4. Click *Save* and *Close*, then in the Email Notifications window, confirm the change.

To test email notifications:

1. Click the *Reports - Event Log* tabs, and in the side bar, click *Email Notifications*.
2. In the Email Notifications window, click the checkboxes of the notifications to be tested.
3. Click *Test* and confirm or cancel the test.

To delete email notifications:

1. Click the *Reports - Event Log* tabs, and in the side bar, click *Email Notifications*.
2. In the Email Notifications window, click the checkboxes of the notifications to be deleted.
3. Click *Delete* and confirm or cancel the deletion.

21.8 Collecting and Archiving Data

Based on the configuration, the Rack Power Manager stores power and environmental data that is collected from the PDUs and sensors during each collection cycle. The dynamic partitioning function helps you to manage the large amounts of collected data. This function uses partitions to group data into one of the four quarters in a year, with each partition including 3 months of data. The data is then displayed in quarterly tables. For example, all records created between January 01, 2014 and March 31, 2014 are stored in the table for the first quarter of 2014. Similarly, records created between April 01, 2014 and June 30, 2014 are stored in the table for the second quarter of 2014.

The dynamic partitioning function also allows you to archive older, unused partitions of data, and thereby control the size of the database for better performance. Before archiving data, the Archive Settings window must be configured, and then from the Archived Data window you can view the partitions. From the Plug-in maintenance task you can access the Schedule window and configure the intervals at which the Rack Power Manager checks for any partitions to be archived.

21.8.1 Best practices to manage archival

The following are best practices for archiving to achieve optimal performance:

- When a backup of the Rack Power Manager software is performed, either through tasks or the backup and restore tool, the software does not back up the archives. This is because backing up archives can increase the size of backups. If you are concerned about the data in the

archives, you must perform a manual backup. The Archive Settings window is configured in the following procedure.

- Archiving data reduces the hard-disk space consumed by the Rack Power Manager database, and thereby improves its performance. As a default, the archive directory points to a location within the Rack Power Manager install folder. It is advisable to revise the location to a shared location on a different file server so the archives do not consume space on the Rack Power Manager server.
- When migrating the Rack Power Manager software from one server to another, the usual route is to create a backup of the Rack Power Manager system and restore it to the new server. As mentioned in bullet 1, the archives are not backed up in the backup file, so you can manually copy the archives from the old server to the new server under the archive directory or you can ignore this step.
- When loading archives into the database from the Archived Data window, it is advisable to keep the archives loaded in the database for the least amount of time possible. Loading an archive into the database increases its size and can affect the performance. You can check the status column in the Archived Data window to know the status of the archives. When the status is Archived, it has been unloaded from the database and is best for performance.

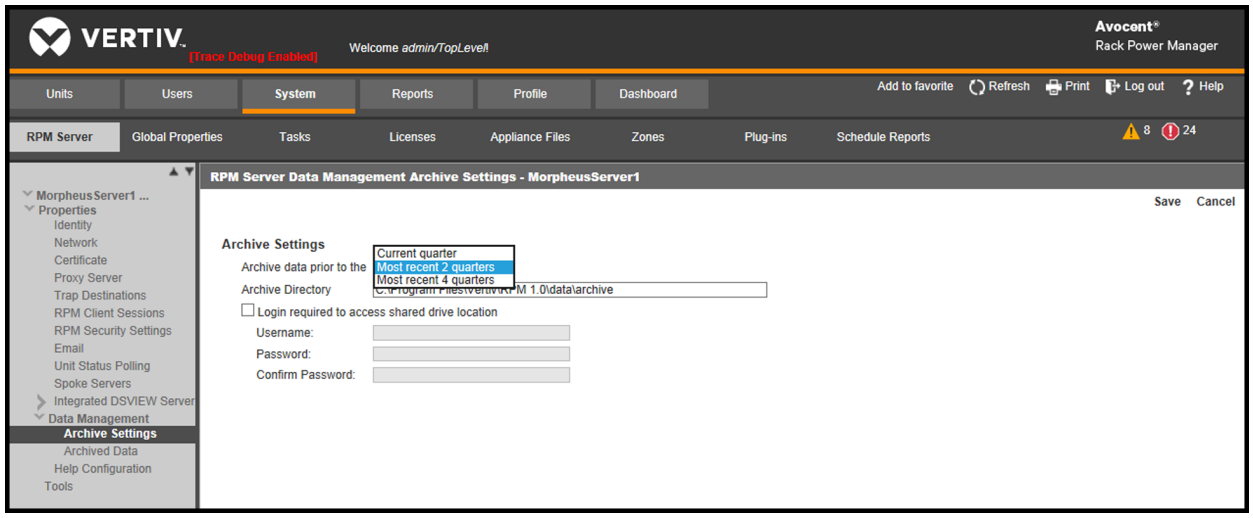
21.8.2 Archive Settings window

The Archive Settings window is used to select the partitions of data to be archived. All data prior to the selected quarter is archived; therefore, you must first consider the most recent quarters to keep active and then from the drop-down menu, select that quarter to archive all data before that quarter. The options are:

- Current quarter - Archives all partitions prior to the current quarter
- Most recent 2 quarters - Archives all partitions prior to the most recent 2 quarters
- Most recent 4 quarters - Archives all partitions prior to the most recent 4 quarters

The Archive Directory field is used to specify the location where you want to archive the partitions. If a login is required to access this location, you can enable the Login required to access shared drive location checkbox and specify the username and password in the appropriate fields.

Figure 21.1 Archive Settings Window



To configure the Archive Settings window:

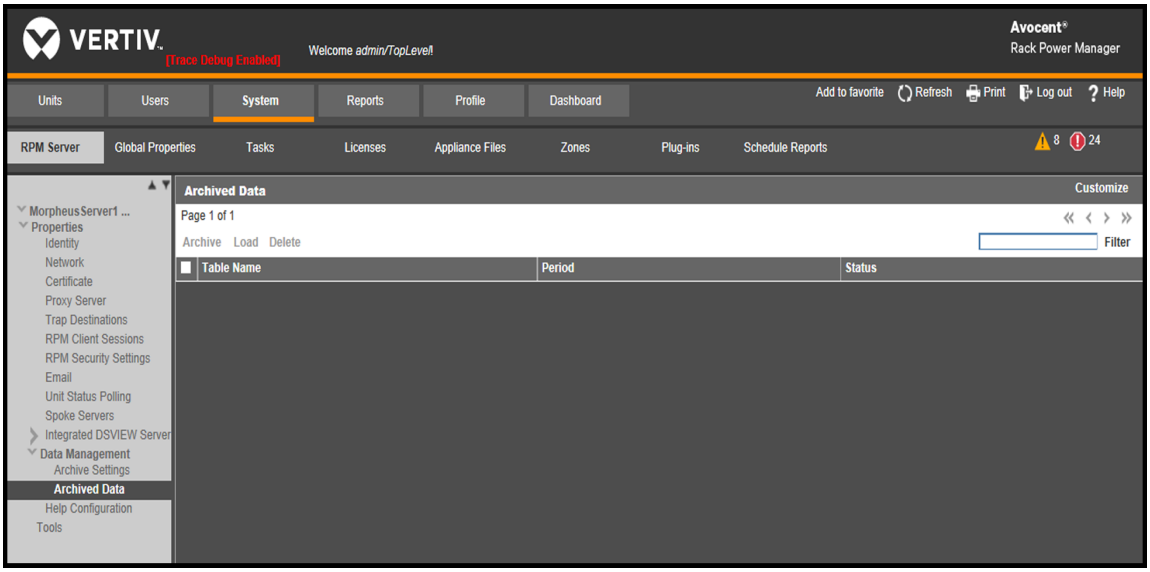
1. Click the *System - RPM Server* tabs, then click *Data Management - Archive Settings*.
2. From the drop-down menu, select the oldest quarter to keep active.
3. In the Archive Directory field, specify the location where you want the Rack Power Manager to archive the partitions.
4. Enable or disable the Login required to access shared drive location checkbox.
5. If a log in is required to access the location to archive the partitions, specify the username and password in the appropriate fields.

21.8.3 Archived Data window

The Archived Data window displays all partitions that have been archived. On this window, you can load archived partitions into the database, archive a loaded partition or delete one or more archived partitions. This window includes the name of the database table that is archived, the time period of the data that is archived and the status of the archived data. The possible values under the Status column are:

- Loaded in DB: Displayed if an archived partition has been loaded into the database
- Archived: Displayed if an archived partition is not loaded into the database
- Loading: Displayed when a data backup is being loaded into the database
- Archiving: Displayed when a partition from the database is being archived

Figure 21.2 Archived Data Screen



To access the Archived Data window:

Click the *System - RPM Server* tabs, then click *Data Management - Archived Data*.

To load archived partitions into the database:

From the Archived Data window, select the table names and click the *Load* button.

NOTE: Loading archived partitions into the database enables you to view data in these partitions through the reporting module.

To archive a loaded partition:

From the Archived Data window, select the table names that have been loaded and click the *Archive* button.

NOTE: Archived data is not loaded to the database and cannot be viewed in reports for this period through the reporting module.

To permanently delete archived partitions from the file system:

From the Archived Data window, select the archived partitions and click the *Delete* button.

NOTE: Deleting a partition destroys all of its data and removes this data from reports for this period.

21.8.4 Plug-in maintenance task

This task controls the intervals at which the Rack Power Manager checks for any partitions to be archived as per the previously described archive settings. In the window, the Runs On column displays the server on which this task is run. You can click the task for the appropriate server and navigate to the Schedule window to view the configured schedule for the archived task.

To access this task:

Click the *System - Tasks* tabs and on the Tasks window, click *Plugin Maintenance*.

22 MANAGING PLUG-INS

A plug-in provides support for a specific appliance type (model) that is configured 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. Only users with administrator privileges can view and manage plug-ins.

Plug-ins are created using the Plug-in API in the Rack Power Manager Software Development Kit (SDK). 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 indicate if any plug-ins are included with the Rack Power Manager software. If a plug-in is included, you do not need to add it to the hub or spoke servers.

NOTE: The Rack Power Manager software supports third party rack PDUs using an appliance plug-in.

22.1 Adding/Upgrading Plug-in Sequence

After you successfully complete the sequence for adding a plug-in, you can add appliances of the same type and initiate other operations (supported by that plug-in) from the Rack Power Manager software.

After a plug-in is added, you can upgrade it to another version. For troubleshooting purposes, you can also disable a plug-in and reactivate it afterwards. You can initiate an action only for plug-ins on the Rack Power Manager server to which you are currently logged in. However, 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.

To add or upgrade a plug-in:

1. Ensure that scheduled replication does not occur while adding or upgrading plug-ins, and if necessary, change the replication schedule temporarily.
2. Replicate each spoke server. See Replication on page 55.
3. Back up the Rack Power Manager software database. See Backing up and Restoring Hub Servers Manually on page 50.
4. Add or upgrade the plug-in on the hub server. See Adding a Plug-in on page 202 or Upgrading a Plug-in on page 203.
5. Add or upgrade the plug-in on each spoke server.

NOTE: All spoke servers should have the same plug-ins and the plug-ins must be the same version.

6. Replicate each spoke server.
7. Back up the Rack Power Manager software database.
8. If you changed the replication schedule in step 1, you can change it back to its original values.

22.2 Displaying Plug-in Information

You can 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 - Plug-ins* tabs.
2. In the Plug-ins window, click the name of the plug-in.

NOTE: Information in the Overview area is read-only.

From the RPM Servers table you can view 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 22.1 Plug-ins Window Description

FIELD	VALUES	DESCRIPTION
Name	Plug-in name	Name acquired from the plug-in.
Version	Plug-in version (on this server)	Version acquired from the plug-in when it is added or upgraded.
Overall Status	Same	Operational status, administrative status and version of the plug-in is the same on all Rack Power Manager servers.
	Mixed	Operational status, administrative status and version of the plug-in is not the same on all Rack Power Manager servers.
Administrative Status	Rack Power Manager server not responding (This value is valid only when a single plug-in is selected.)	Response when the Rack Power Manager software cannot obtain plug-in status on this server. For examining the server status, click the *System - RPM Server* tabs. If you are on a hub server, in the side bar, click *Spoke Servers* and then select the appropriate server. -or- If you are on a spoke server, in the side bar, click *Hub Server*.
	Replication needed	Plug-in is added, but replication is required before the plug-in can be used.
	Active	Plug-in is registered and operational.
	Disabled	Plug-in is disabled.
	Not installed	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 contains the name of the plug-in. If the status service does not provide this information, the Name field contains the domain and ID of the plug-in.
Operational Status (on this server)	Inactive	Plug-in is not running.
	Active	Plug-in is running.
	Initializing	Plug-in is starting up.
	Shutting down	Plug-in is stopping.
	Upgrading	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.	
*The default setting does not display these fields in the Plug-ins window. Use the Customize link to specify which fields you want to display; see Using the Customize link in windows on page 21. These fields are always displayed in the overview window of each plug-in.		

22.3 Adding a Plug-in

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 Adding/Upgrading Plug-in Sequence on page 201.

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 Vertiv representative to determine if a key is needed. To add a license, see Viewing and Adding Licenses on page 40.

To add a plug-in:

1. Click the *System - Plug-ins* tabs and click *Add*.
2. From the Add Plug-in Wizard, in the Select Plug-in window, enter the name or browse to the location of the plug-in file and click *Next*.
3. In the Overview window, verify the read-only information about the plug-in and click *Next*.
4. In the Completed Successful window, 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.

22.4 Upgrading a Plug-in

When you upgrade the existing version of a plug-in, follow the steps described in Adding/Upgrading Plug-in Sequence on page 201.

To upgrade a plug-in:

1. Click the *System - Plug-ins* tabs.
2. In the Plug-ins window, click the name of the plug-in to be upgraded.
3. In the Overview window under RPM Servers, click the checkbox of the Rack Power Manager server you are currently logged in to and click *Upgrade*.
4. In the Select Plug-in File window, enter or browse to the location of the plug-in file and click *Next*.
5. In the Overview window, verify the read-only information about the plug-in and click *Next*.
6. In the Completed Successful window, click *Finish*.

22.5 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 are added to the Rack Power Manager software system before the plug-in is disabled appear in Unit Views windows, but you cannot acquire status information from those units, and links that initiate connections to those units are not available. You cannot add more appliances of that type until the plug-in is (re)activated.

A disabled plug-in remains disabled if the Rack Power Manager software is restarted.

To disable/activate a plug-in:

1. Click the *System - Plug-ins* tabs.
2. In the Plug-ins window, click the name of the plug-in to be disabled/activated.
3. In the Overview window under RPM Servers, click the checkbox of the Rack Power Manager server you are currently logged in to and click *Disable* or *Activate*.

4. In the confirmation dialog box, confirm or cancel the action.

22.6 Liebert® GXT4™ UPS Support

After a GXT4 UPS is discovered and added to a rack, the Power Manager (Data Monitoring) link and additional functionality appear in the left navigation side bar of the Rack Power Manager. The additional functionality includes links to display the status, configure thresholds and configure reports for the GXT4 UPS.

NOTE: See the Avocent® DSView™ and Rack Power Manager Software Plug-in Technical Bulletin for details on how to discover and manage a GXT4 UPS.

From the Thresholds link, you can configure the Battery Minutes Remaining, Battery Percentage Charge Remaining, Output Current and Input Current thresholds. After the thresholds are configured, the following events occur if a reading is not within the threshold requirements:

- Low Critical - The reading is lower than the configured threshold value.
- Low Warning - The reading is lower than the configured threshold value.
- High Critical - The reading is higher than the configured threshold value.
- High Warning - The reading is higher than the configured threshold value.

To configure thresholds for the GXT4 UPS:

Enter the thresholds for each event level and click *Save*.

The Reports link displays the available reports for the selected UPS. The following are the possible reports:

- Battery Minutes Remaining: Number of minutes remaining on the battery over a selected time period.
- Percentage Battery Charge Remaining: Percentage charge remaining on the battery over a selected time period.
- Battery Voltage: Voltage on the batteries over a selected time period.
- Output Voltage: Output voltage of the UPS over a selected time period.
- Output Current: Output current of the UPS over a selected time period.
- Input Voltage: Input voltage of the UPS over a selected time period.
- Input Current: Input current of the UPS over a selected time period.
- Events: Triggered threshold violation events for this UPS.

To create a report:

1. Click the *Units* tab and select *GXT4 UPS*.
2. Select a report from the drop-down menu.
3. Select the start and end dates and time, and then click *Run Report*.
4. After the results are displayed, select the desired view icon.

APPENDICES

Appendix A: 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 159.

A.1 VT terminal emulation

The following table lists the VT key and keypad numeric codes. Vertiv™ encodes all applicable keys as numeric; decoding is not supported.

Table A.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

A.2 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 the following table.

Table A.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.			

A.3 VT102 terminal emulation

VT102 terminal emulation works identically to the VT100 with additional support for decoding receive codes as described in the following table.

Table A.3 VT102 Receive Codes

VT102 RECEIVE CODE	DEFINITION
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.
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.

A.4 VT100 terminal emulation

The following table lists the VT100 special key and control (Ctrl) key combinations and indicates Vertiv™ encoding/decoding support, where Yes = supported and No = not supported.

Table A.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
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

KEYS	HEX CODE	FUNCTION MNEMONIC	ENCODE/DECODE
Ctrl+]	1D	GS	Yes/No
Ctrl+^	1E	RS	Yes/No
Ctrl+_	1F	US	Yes/No

The following table 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 A.5 VT100 ANSI Set and Reset Mode Cursor Keys

CURSOR KEY	MODE RESET	MODE SET
Up	Esc [A	Esc O A
Down	Esc [B	Esc O B
Right	Esc [C	Esc O C
Left	Esc [D	Esc O D

The following table lists VT100 PF1-PF4 key definitions. Encoding of each listed key is supported; decoding is not applicable.

Table A.6 VT100 PF1-PF4 Key Definitions

KEY	CODE SEQUENCE
F1	Esc [O P
F2	Esc [O Q
F3	Esc [O R
F4	Esc [O S

The following table lists the ANSI mode control sequences for VT100 terminal emulation and indicates Vertiv encoding/decoding support, where Yes = supported and No = not supported.

Table A.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
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
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)

CONTROL SEQUENCE	DEFINITION	ENCODE/DECODE
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	Character Attributes 7 - Reverse Video On	No/Reverse Video only
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
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

CONTROL SEQUENCE	DEFINITION	ENCODE/DECODE
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

A.5 VT220 terminal emulation

The following table lists the keystroke mapping (encoding) for VT220 emulation.

Table A.8 VT220 Encoding

VT220 KEYBOARD	PC KEYBOARD	VT220 KEYBOARD BYTE SEQUENCE
Delete	Delete	0x7F
Left Arrow	Left Arrow	Esc [D
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	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 ~
F16	Ctrl - F8	Esc [2 9 ~
F17	Ctrl - F9	Esc [3 1 ~
F18	Ctrl - F10	Esc [3 2 ~
F19	Ctrl - F11	Esc [3 3 ~
F20	Ctrl - F12	Esc [3 4 ~

The following table lists the decoding for VT220 terminal emulation.

Table A.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
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
Left 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

VT220 KEYBOARD FUNCTION	VT220 KEYBOARD BYTE SEQUENCE
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 Characters	Esc [Pn L
Delete Pn Lines	Esc [Pn M
Insert Character	Esc [Pn @
Erase Pn Characters	Esc [Pn X

A.6 VT52 terminal emulation

The following table lists the keystroke mapping (encoding) for VT52 terminal emulation.

Table A.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

The following table lists the decoding for VT52 terminal emulation.

Table A.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

The following table lists the VT52 and ANSI auxiliary keypad definitions. Encoding of each listed keypad key is supported; decoding is not applicable.

Table A.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
, (comma)	, (comma)	Esc ? l	Esc O l
. (period)	. (period)	Esc ? n	Esc O n
Enter	Same as Return key	Esc ? m	Esc O m

A.7 VT320 terminal emulation

The following table lists the keystroke mapping (encoding) for VT320 terminal emulation.

Table A.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 ~
F16	Ctrl - F8	Esc [2 9 ~
F17	Ctrl - F9	Esc [3 1 ~
F18	Ctrl - F10	Esc [3 2 ~
F19	Ctrl - F11	Esc [3 3 ~
F20	Ctrl - F12	Esc [3 4 ~
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

The following table lists the decoding for VT320 terminal emulation.

Table A.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
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
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

VT320 KEYBOARD FUNCTION	VT320 KEYBOARD BYTE SEQUENCE
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 B: Regaining Access to the Rack Power Manager Software

Access to a Rack Power Manager software system can 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 Vertiv™ Technical Support to get the resetpassword.zip archive file.
2. Using a third party product, extract the *resetpassword.zip* archive file in to the <RPM Installation Directory>\bin directory on the Rack Power Manager software hub server.
3. From your desktop Start icon, select *Control Panel - Administrative Tools - Services*, select *RPM Service* and click *Stop*.
4. Open a terminal window, change directories to the <RPM Installation Directory>/bin directory and enter **resetpassword.bat**. A code successfully generated message appears 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 Vertiv Technical Support and provide the generated request code.
6. After Vertiv Technical Support provides you with a reset code, in a terminal window, enter **resetpassword.bat <reset code>**.
7. After the *Reset performed successfully* message, Administrator username and password for the Rack Power Manager management software appear in the window, select *Administrative Tools - Services* from the Control Panel and restart the Avocent® Rack Power Manager software service.
8. Log in to the Rack Power Manager management software.

This page intentionally left blank.

VertivCo.com | Vertiv Headquarters, 1050 Dearborn Drive, Columbus, OH, 43085, USA

590-1821-501A