Contents

Environment 65

Logs 68

Administration: Security 76

Administration: Network Features 81

Administration: Notification 98

Administration: General Options 108

USER'S GUIDE
Metered Rack PDU

Introduction

Product Features

The Dell® Metered Rack Power Distribution Unit (PDU) is a stand-alone, network-manageable power distribution device that monitors the current, voltage, and power for the Rack PDU.

You can manage a Rack PDU through its Web interface, its command line interface, or Simple Network Management Protocol (SNMP):

- Access the Web interface using Hypertext Transfer Protocol or using secure HTTP (HTTPS) with Secure Sockets Layer (SSL). See Logging On to the Web Interface.
- Access the command line interface through a serial connection, Telnet, or Secure SHell (SSH). See About the Command Line Interface.
- Use an SNMP browser and the Dell Management Information Base (MIB) to manage your Rack PDU.

Rack PDUs have these additional features:

- Voltage, current, and power monitoring for the device and each phase as applicable.
- Configurable alarm thresholds that provide network and visual alarms to help avoid overloaded circuits.
- Three levels of user access accounts: Administrator, Device User, and Read-Only User.
- Event and data logging. The event log is accessible by Telnet, Secure CoPy (SCP), File Transfer Protocol (FTP), serial connection, or Web browser (using HTTPS access with SSL, or using HTTP access). The data log is accessible by Web browser, SCP, or FTP.

USER'S GUIDE
Metered Rack PDU

- E-mail notifications for Rack PDU and system events.
- SNMP traps, Syslog messages, and e-mail notifications based on the severity level or category of the Rack PDU and system events.
- Security protocols for authentication and encryption.

The Rack PDU does not provide power surge protection. To ensure that the device is protected from power failure or power surges, connect the Rack PDU to an uninterruptible power supply (UPS).

Access priorities for logging on

Only one user at a time can log on to the Rack PDU. The priority for access, beginning with the highest priority, is as follows:

- Local access to the command line interface from a computer with a direct serial connection to the Rack PDU
- Telnet or Secure SHell (SSH) access to the command line interface from a remote computer
- Web access

See SNMP for information about how SNMP access to the Rack PDU is controlled.

Types of user accounts

The Rack PDU has three levels of access (Administrator, Device User, and Read-Only User), which are protected by user name and password requirements.

- An Administrator can use all of the menus in the Web interface and all of the commands in the command line interface. The default user name and password are both **admin**.
- A Device User can access only the following:
  - In the Web interface, the menus on the **Device Manager** tab, the **Environment** tab, and the event and data logs, accessible under the **Events** and **Data** headings on the left navigation menu of the **Logs** tab. The event and data logs display no button to clear the log.
  - In the command line interface, the equivalent features and options.

  The default user name and password are both **device**.
- A Read-Only User has the following restricted access:
  - Access through the Web interface only.
  - Access to the same tabs and menus as a Device User, but without the capability to change configurations, control devices, delete data, or use file transfer options. Links to configuration options are visible but disabled. The event and data logs display no button to clear the log.

  The default user name and password are both **readonly**.

To set **User Name** and **Password** values for the three account types, see Setting user access.

Getting Started

To start using the Rack PDU:

1. Install the Rack PDU using the *Rack Power Distribution Unit Installation Instructions* that were shipped with your Rack PDU.
2. Apply power and connect to your network. Follow the directions in the *Rack Power Distribution Unit Installation Instructions*.
3. Establish network settings. (See Establishing Network Settings.)
4. Begin using the Rack PDU by way of one of the following:
   - Web Interface
   - Command Line Interface
   - Rack PDU Front Panel

Establishing Network Settings

You must configure the following TCP/IP settings before the Rack PDU can operate on a network using one of the following:

- IP address of the Rack PDU
- Subnet mask
- Default gateway

If a default gateway is unavailable, use the IP address of a computer that is located on the same subnet as the Rack PDU and that is usually running. The Rack PDU uses the default gateway to test the network when traffic is very light.

Do not use the loopback address (127.0.0.1) as the default gateway address for the Rack PDU. It disables the card and requires you to reset TCP/IP settings to their defaults using a local serial login.

TCP/IP configuration methods

Use one of the following methods to define the TCP/IP settings needed by the Rack PDU:

- Appendix B: Security Handbook
- BOOTP and DHCP configuration
- Command Line Interface

BOOTP and DHCP configuration

The Rack PDU default TCP/IP configuration setting of **BOOTP & DHCP** assumes that a properly configured BOOTP or DHCP server is available to provide TCP/IP settings to Rack PDUs. The Rack PDU first attempts to discover a properly configured BOOTP server, and then a DHCP server. It repeats this pattern until it discovers a BOOTP or DHCP server.

A user configuration (INI) file can function as a BOOTP or DHCP boot file. For more information, see Use an .ini File.

BOOTP. For the Rack PDU to use a BOOTP server to configure its TCP/IP settings, it must find a properly configured RFC951-compliant BOOTP server.

In the BOOTPTAB file of the BOOTP server, enter the Rack PDU's MAC address, IP address, subnet mask, and default gateway, and, optionally, a bootup file name. Look for the MAC address on the bottom of the Rack PDU or on the Quality Assurance slip included in the package.

When the Rack PDU reboots, the BOOTP server provides it with the TCP/IP settings.

- If you specified a bootup file name, the Rack PDU attempts to transfer that file from the BOOTP server using TFTP or FTP. The Rack PDU assumes all settings specified in the bootup file.
- If you did not specify a bootup file name, you can configure the other settings of the Rack PDU remotely through its Web Interface or Command Line Interface.

To create a bootup file, see your BOOTP server documentation.

DHCP. You can use an RFC2131/RFC2132-compliant DHCP server to configure the TCP/IP settings for the Rack PDU.

This section summarizes the Rack PDU's communication with a DHCP server. For more detail about how a DHCP server can configure the network settings for a Rack PDU, see DHCP response options.

1. The Rack PDU sends out a DHCP request that uses the following to identify itself:
   - A Vendor Class Identifier
   - A Client Identifier (by default, the MAC address of the Rack PDU)
   - A User Class Identifier (by default, the identification of the application firmware installed on the Rack PDU)
2. A properly configured DHCP server responds with a DHCP offer that includes all the settings that the Rack PDU needs for network communication. The DHCP offer also includes the Vendor Specific Information option (DHCP option 43). The Rack PDU can be configured to ignore DHCP offers that do not encapsulate the vendor cookie in DHCP option 43 using the following hexadecimal format. (The Rack PDU does not require this cookie by default.)

   ```
   Option 43 = 01 04 31 41 50 43
   ```

   Where:
   - The first byte (`01`) is the code.
   - The second byte (`04`) is the length.
   - The remaining bytes (`31 41 50 43`) are the vendor cookie.

See your DHCP server documentation to add code to the Vendor Specific Information option.

❗ **Note:** By selecting the **Require vendor specific cookie to accept DHCP Address** check box in the Web interface, you can require the DHCP server to provide a vendor cookie, which supplies information to the Rack PDU **Administration > Network**>**TCP/IP**>**DHCP**.

Command Line Interface

1. Log on to the command line interface. See Logging on to the Command Line Interface.
2. Contact your network administrator to obtain the IP address, subnet mask, and default gateway for the Rack PDU.
3. Use these three commands to configure network settings. (Text in italics indicates a variable.)
   a. `tcpip -i` *`yourIPaddress`*
   b. `tcpip -s` *`yourSubnetMask`*
   c. `tcpip -g` *`yourDefaultGateway`*

   For each variable, type a numeric value that has the format *`xxx.xxx.xxx.xxx`*.

   For example, to set a system IP address of 156.205.14.141, type the following command and press ENTER:

   ```
   tcpip -i 156.205.14.141
   ```
4. Type **`exit`**. The Rack PDU restarts to apply the changes.

Recovering from a Lost Password

You can use a local computer (a computer that connects to the Rack PDU or other device through the serial port) to access the command line interface.

1. Select a serial port at the local computer, and disable any service that uses that port.
2. Connect the provided serial cable to the selected port on the computer and to the Serial port at the Rack PDU.
3. Run a terminal program (such as HyperTerminal®) and configure the selected port for 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control.
4. Press ENTER, repeatedly if necessary, to display the **User Name** prompt. If you are unable to display the **User Name** prompt, verify the following:
   - The serial port is not in use by another application.
   - The terminal settings are correct as specified in step 3.
   - The correct cable is being used as specified in step 2.
5. Press the **Reset** button. The Status LED will flash alternately orange and green. Press the **Reset** button a second time immediately while the LED is flashing to reset the user name and password to their defaults temporarily.
6. Press ENTER, repeatedly if necessary, to display the **User Name** prompt again, then use, **dell,** for the user name and password. (If you take longer than 30 seconds to log on after the **User Name** prompt is redisplayed, you must repeat step 5 and log on again.)
7. At the command line interface, use the following commands to change the **User Name** and **Password** settings, both of which are now **dell**:

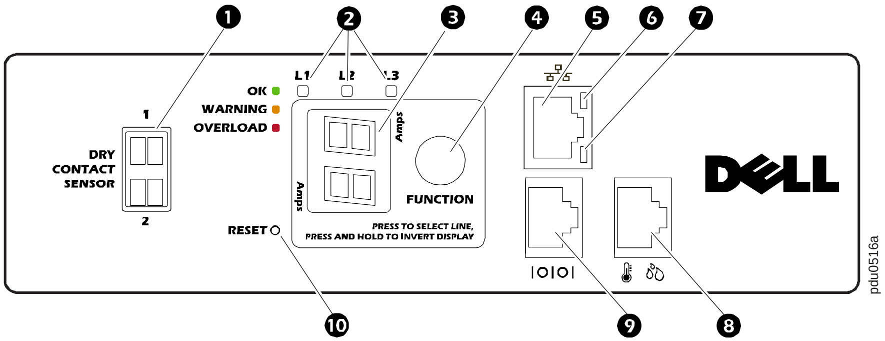
   ```
   user -an yourAdministratorName
   user -ap yourAdministratorPassword
   ```

   For example, to change the Administrator user name to **Don Adams**, type:

   ```
   user -an Don Adams
   ```

8. Type quit or exit to log off, reconnect any serial cable you disconnected, and restart any service you disabled.

Rack PDU Front Panel



Item		Function
❶	Dry contact inputs	Connector for two dry contact devices.
❷	Phase LEDs Note: for single-phase Rack PDUs, only one LED is present.	When no alarms are present, the LED display shows a phase current, and a green Phase LED indicates for which phase. The system automatically cycles through each phase, displaying the phase current for three seconds. If an alarm is present for one phase, the applicable Phase LED turns on and stays on while the alarm condition is present. The LED will illuminate orange for a Warning alarm or red for a Critical alarm. If an alarm is present for more than one phase, the system will automatically cycle through each phase with an alarm, illuminating the Phase LEDs for three seconds.
❸	LED display	Shows the phase current for the currently illuminated Phase LED.

Item		Function
❹	Function button	• To manually display the current for each phase, repeatedly press the button. The current displays for 30 seconds or until you press the button again. (This functionality is not available for single-phase Rack PDUs.) • To display the IP address, press and hold for five seconds until **IP** appears; then release. On the LED display, the address will appear two digits at a time and then the cycle will repeat. • To invert the display, press and hold for ten seconds until the **AA** pattern appears. Continue holding the button until AA is oriented as desired then release the button.
❺	10/100 Base-T Connector	Port for connecting the Rack PDU to the network.
❻	10/100 LED	See 10/100 LED.
❼	Network Status LED	See Network Status LED.
❽	Temp/Humidity sensor port	Port for connecting a Rack PDU Temperature Sensor (G853N) or a Rack PDU Temperature/ Humidity Sensor (H621N).
❾	RJ-45 Serial Port	Port for connecting the Rack PDU to a terminal emulator program for local access to the command line interface. Use the supplied serial cable.
❿	Reset Button	To restart the interface of the Rack PDU without affecting the outlets, press and release the Reset button.

Network Status LED

Condition	Description
Off	The Rack PDU is connected to an unknown network.
Solid Green	The Rack PDU has valid TCP/IP settings.
Flashing Green	The Rack PDU does not have valid TCP/IP settings.
Solid Orange	A hardware failure has been detected in the Rack PDU.
Flashing Orange	The Rack PDU is making BOOTP requests.
Flashing Orange and Green (alternating)	The Rack PDU is making DHCP requests.

10/100 LED

Condition	Description
Off	The device that connects the Rack PDU to the network is off or not operating correctly.
Flashing Green	The Rack PDU is receiving data packets from the network at 10 Megabits per second (Mbps).
Flashing Orange	The Rack PDU is receiving data packets from the network at 100 Megabits per second (Mbps).
Solid Green or Orange	The Rack PDU is receiving no network traffic.

Command Line Interface

About the Command Line Interface

You can use the command line interface to view the status of and manage the Rack PDU. In addition, the command line interface enables you to create scripts for automated operation.

You can configure all parameters of a Rack PDU (including those for which there are not specific CLI commands) by using the CLI to transfer an INI file to the Rack PDU. The CLI uses XMODEM to perform the transfer. However, you cannot read the current INI file through XMODEM.

Logging on to the Command Line Interface

To access the command line interface, you can use either a local (serial) connection or a remote (Telnet or SSH) connection with a computer on the same local area network (LAN) as the Rack PDU.

Remote access to the command line interface

You can access the command line interface through Telnet or SSH. Telnet is enabled by default. Enabling SSH disables Telnet.

To enable or disable these access methods, use the Web interface. On the **Administration** tab, select **Network** on the top menu bar, and then the **access** option under **Console** on the left navigation menu.

Telnet for basic access. Telnet provides the basic security of authentication by user name and password, but not the high-security benefits of encryption.

To use Telnet to access the command line interface:

1. From a computer on the same network as the Rack PDU, at a command prompt, type `telnet` and the IP address for the Rack PDU (for example, `telnet 139.225.6.133`, when the Rack PDU uses the default Telnet port of 23), and press ENTER.
   If the Rack PDU uses a non-default port number (from 5000 to 32768), you must include a colon or a space, depending on your Telnet client, between the IP address (or DNS name) and the port number.
2. Enter the user name and password (by default, **admin** and **admin** for an Administrator, or **device** and **device** for a Device User).

📖 If you cannot remember your user name or password, see Recovering from a Lost Password.

SSH for high-security access. If you use the high security of SSL for the Web interface, use SSH for access to the command line interface. SSH encrypts user names, passwords, and transmitted data. The interface, user accounts, and user access rights are the same whether you access the command line interface through SSH or Telnet, but to use SSH, you must first configure SSH and have an SSH client program installed on your computer.

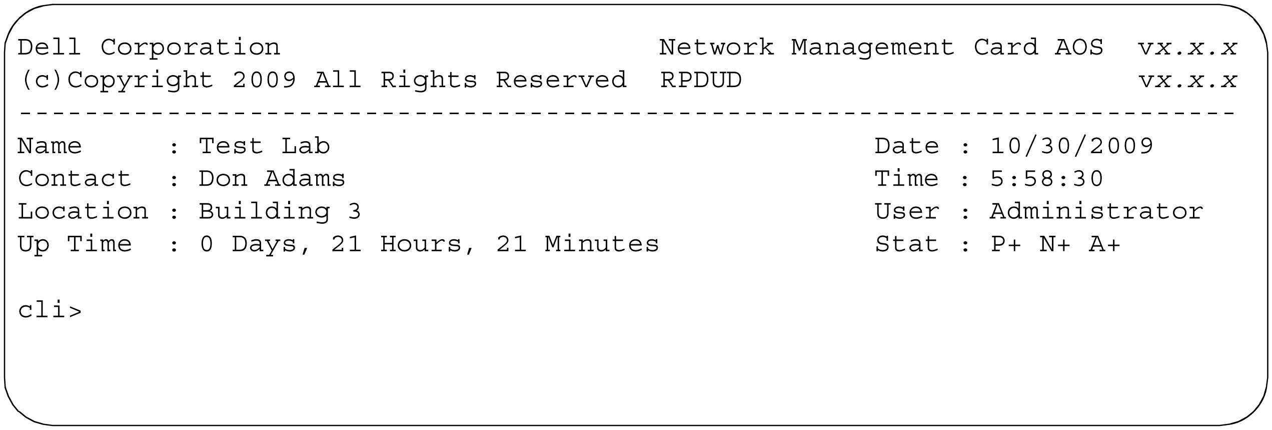
Local access to the command line interface

For local access, use a computer that connects to the Rack PDU through the serial port to access the command line interface:

1. Select a serial port at the computer and disable any service that uses that port.
2. Connect the supplied serial cable from the selected serial port on the computer to the serial port on the Rack PDU.
3. Run a terminal program (e.g., HyperTerminal) and configure the selected port for 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control.
4. Press ENTER, and at the prompts, enter your user name and password.

About the Main Screen

The main screen that is displayed when you log on to the command line interface of a Rack PDU:



```
Dell Corporation                                       Network Management Card AOS   vx.x.x
(c)Copyright 2009 All Rights Reserved  RPDUD                                         vx.x.x
---------------------------------------------------------------------------
Name     : Test Lab                                    Date : 10/30/2009
Contact  : Don Adams                                   Time : 5:58:30
Location : Building 3                                  User : Administrator
Up Time  : 0 Days, 21 Hours, 21 Minutes                Stat : P+ N+ A+

cli>
```

Main screen information fields:

- Two fields identify the operating system (AOS) and application (APP) firmware versions. The application firmware name identifies the type of device that connects to the network. In the preceding example, the application firmware for the Rack PDU is displayed.

  ```
  Network Management Card AOSvx.x.x

  RPDUD vx.x.x
  ```

- Three fields identify the system name, contact person, and location of the Rack PDU. (In the control console, use the **System** menu to set these values.)

  ```
  Name: Test Lab

  Contact: Don Adams

  Location: Building 3
  ```

- An **Up Time** field reports how long the Rack PDU has been running since it was last turned on or reset.

  ```
  Up Time: 0 Days, 21 Hours, 21 Minutes
  ```

- Two fields identify when you logged in, by date and time.

  ```
  Date: 10/30/2009

  Time: 5:58:30
  ```

- A **User** field identifies whether you logged in through the **Administrator** or **Device** user account. (The **Read-Only User** account cannot access the control console.)

  ```
  User : Administrator
  ```

- A **Stat** field reports the Rack PDU status.

```
Stat : P+ N+ A+
```

P+	The Dell operating system is functioning properly.
N+	The network is functioning properly.
N?	A BOOTP request cycle is in progress.
N–	The Rack PDU failed to connect to the network.
N!	Another device is using the Rack PDU IP address.
A+	The application is functioning properly.
A–	The application has a bad checksum.
A?	The application is initializing.
A!	The application is not compatible with the AOS.

If P+ is not displayed, contact Dell support staff.

Using the Command Line Interface

At the command line interface, use commands to configure the Rack PDU. To use a command, type the command and press ENTER. Commands and arguments are valid in lowercase, uppercase, or mixed case. Options are case-sensitive.

While using the command line interface, you can also do the following:

- Type **?** and press ENTER to view a list of available commands, based on your account type.
- To obtain information about the purpose and syntax of a specified command, type the command, a space, and **?** or the word **help**. For example, to view RADIUS configuration options, type:

  ```
  radius ?
  ```

  or

  ```
  radius help
  ```

- Press the UP arrow key to view the command that was entered most recently in the session. Use the UP and DOWN arrow keys to scroll through a list of up to ten previous commands.
- Type at least one letter of a command and press the TAB key to scroll through a list of valid commands that match the text you typed in the command line.
- Type **exit** or **quit** to close the connection to the command line interface.

Command Syntax

Item	Description
-	Options are preceded by a hyphen.
< >	Definitions of options are enclosed in angle brackets. For example: `-dp <device password>`
[ ]	If a command accepts multiple options or an option accepts mutually exclusive arguments, the values may be enclosed in brackets.
|	A vertical line between items enclosed in brackets or angle brackets indicates that the items are mutually exclusive. You must use one of the items.

Example of a command that supports multiple options:

```
user [-an <admin name>] [-ap <admin password>]
```

In this example, the user command accepts the option **`-an`**, which defines the Administrator user name, and the option **`-ap`**, which defines the Administrator password. To change the Administrator user name and password to XYZ:

1. Type the user command, one option, and the argument **`XYZ`**:

   ```
   user -ap XYZ
   ```

2. After the first command succeeds, type the user command, the second option, and the argument **`XYZ`**:

   ```
   user -an XYZ
   ```

Example of a command that accepts mutually exclusive arguments for an option:

```
alarmcount -p [all | warning | critical]
```

In this example, the option -p accepts only three arguments: all, warning, or critical. For example, to view the number of active critical alarms, type:

`alarmcount -p critical`

The command will fail if you type an argument that is not specified.

Command Response Codes

The command response codes enable scripted operations to detect error conditions reliably without having to match error message text:

The CLI reports all command operations with the following format:

E [0-9] [0-9] [0-9] : Message

Code	Message	Code	Message
`E000`	Success	`E105`	Command Prefill
`E001`	Successfully Issued	`E106`	Command failed
`E100`	Command failed	`E200`	Input error
`E101`	Command not found	`E201`	No response
`E102`	Parameter error	`E202`	User already exists
`E103`	Command line error	`E203`	User does not exist
`E104`	User level denial	`E204`	User does not have access to this command

Network Management Card Command Descriptions

?

Access: Administrator, Device User

Description: View a list of all the CLI commands available to your account type. To view help text for a specific command, type the command followed by a question mark.

Example: To view a list of options that are accepted by the **`alarmcount`** command, type:

```
alarmcount ?
```

about

Access: Administrator, Device User

Description: View hardware and firmware information. This information is useful in troubleshooting and enables you to determine if firmware upgrade is needed.

alarmcount

Access: Administrator, Device User

Description:

Option	Arguments	Description
-p	all	View the number of active alarms reported by the Rack PDU. Information about the alarms is provided in the event log.
	warning	View the number of active warning alarms.
	critical	View the number of active critical alarms.

Example: To view all active warning alarms, type:

```
alarmcount -p warning
```

boot

Access: Administrator only

Description: Define how the Rack PDU will obtain its network settings, including the IP address, subnet mask, and default gateway. Then configure the BOOTP or DHCP server settings.

Option	Argument	Description
-b <boot mode>	dhcpBootp | dhcp | bootp | manual	Define how the TCP/IP settings will be configured when the Rack PDU turns on, resets, or restarts. See TCP/IP and Communication Settings for information about each boot mode setting.
-a	remainDhcpBootp | gotoDhcpOrBootp	`dhcpBootp` boot mode only. Specify whether the Rack PDU will retain the `dhcpBootp` boot mode setting or switch to `bootp` or `dhcp` boot mode after it receives its network settings.
-o	stop | prevSettings	`bootp` and `dhcpBootp` boot modes only. If the Rack PDU receives no valid response to five requests for a network assignment, stop requesting network settings until the Rack PDU is restarted or use the previously configured settings so the Rack PDU remains accessible.
-f	<#>	`bootp` and `dhcpBootp` boot modes only. Enter the number of retries that will occur when no valid response is received, or zero (0) for an unlimited number of retries.
-c	enable | disable	`dhcp` and `dhcpBootp` boot modes only. Enable or disable the requirement that the DHCP server provide the vendor cookie.
-s	<#>	`dhcp` and `dhcpBootp` boot modes only. Enter the number of retries that will occur when no valid response is received, or zero (0) for an unlimited number of retries.
The default values for these three settings generally do not need to be changed: -v <vendor class>: DELL -i <client id>: The MAC address of the Rack PDU, which uniquely identifies it on the local area network (LAN) -u <user class>: The name of the application firmware module		

Example: To use a DHCP server to obtain network settings:

1. Type **`boot -b dhcp`**
2. Enable the requirement that the DHCP server provide the vendor cookie:
   `boot -c enable`
3. Define the number of retries that will occur if the Rack PDU does not receive a valid response from the initial request: **`boot -s 5`**

cd

Access: Administrator, Device User

Description: Navigate to a folder in the directory structure of the Rack PDU.

Example 1: To change to the **`ssh`** folder and confirm that an SSH security certificate was uploaded to the Rack PDU:

1. Type **`cd ssh`** and press ENTER.
2. Type **`dir`** and press ENTER to list the files stored in the SSH folder.

Example 2: To return to the main directory folder, type:

```
cd ..
```

date

Access: Administrator only

Definition: Configure the date used by the Rack PDU.

To configure an NTP server to define the date and time for the Rack PDU, see Set the Date and Time.

Option	Argument	Description
-d	<“datestring”>	Configure the current date. Use the date format specified by the `date -f` command.
-t	<00:00:00>	Configure the current time, in hours, minutes, and seconds. Use the 24-hour clock format.
-f	mm/dd/yy | dd.mm.yyyy | mmm-dd-yy | dd-mmm-yy | yyyy-mm-dd	Select the numerical format in which to display all dates in this user interface. Each letter m (for month), d (for day), and y (for year) represents one digit. Single-digit days and months are displayed with a leading zero.

Example 1: To display the date using the format yyyy-mm-dd, type:

```
date -f yyyy-mm-dd
```

Example 2: To define the date as October 30, 2009, using the format configured in the preceding example, type:

```
date -d “2009-10-30”
```

Example 3: To define the time as 5:21:03 p.m., type:

```
date -t 17:21:03
```

delete

Access: Administrator only

Description: Delete the event or data log, or delete a file in the file system.

Argument	Description
<file name>	Type the name of the file to delete.

Example: To delete the event log:

1. Navigate to the folder that contains the file to delete. For example, to navigate to the **logs** folder, type:

   ```
   cd logs
   ```

2. To view the files in the **logs** folder, type:

   ```
   dir
   ```

   The file **`event.txt`** is listed.

3. Type **`delete event.txt`**.

dir

Access: Administrator, Device User

Description: View the files and folders stored on the Rack PDU.

eventlog

Access: Administrator, Device User

Description: View the date and time you retrieved the event log, the status of the Rack PDU, and the status of sensors connected to the Rack PDU. View the most recent device events and the date and time they occurred. Use the following keys to navigate the event log:

Key	Description
ESC	Close the event log and return to the command line interface.
ENTER	Update the log. Use this command to view events that were recorded after you last retrieved the log.
SPACEBAR	View the next page of the event log.
`B`	View the preceding page of the event log. This command is not available at the main page of the event log.
`D`	Delete the event log. Follow the prompts to confirm or deny the deletion. Deleted events cannot be retrieved.

exit

Access: Administrator, Device User

Description: Exit from the command line interface session.

format

Access: Administrator only

Description: Reformat the file system of the Rack PDU and erase all security certificates, encryption keys, configuration settings, and the event and data logs.

! To reset the Rack PDU to its default configuration, use the **`resetToDef`** command.

FTP

Access: Administrator only

Description: Enable or disable access to the FTP server. Optionally, change the port setting to the number of any unused port from 5001 to 32768 for added security.

Option	Argument	Definition
-p	<port number>	Define the TCP/IP port that the FTP server uses to communicate with the Rack PDU (21 by default). The FTP server uses both the specified port and the port one number lower than the specified port.
-S	enable | disable	Configure access to the FTP server.

Example: To change the TCP/IP port to 5001, type:

```
ftp -p 5001
```

help

Access: Administrator, Device User

Description: View a list of all the CLI commands available to your account type. To view help text for a specific command, type the command followed by the **help** command: **user help**

Example 1: To view a list of commands available to a Device User, type:

```
help
```

Example 2: To view a list of options that are accepted by the **alarmcount** command, type:

```
alarmcount ?
```

ping

Access: Administrator, Device User

Description. Determine whether the device with the IP address or DNS name you specify is connected to the network. Four inquiries are sent to the address.

Argument	Description
<IP address or DNS name>	Type an IP address with the format *xxx.xxx.xxx.xxx*, or the DNS name configured by the DNS server.

Example: To determine whether a device with an IP address of 150.250.6.10 is connected to the network, type:

```
ping 150.250.6.10
```

portSpeed

Access: Administrator

Description:

Option	Arguments	Description
-s	auto | 10H | 10F | 100H | 100 F	Define the communication speed of the Ethernet port. The `auto` command enables the Ethernet devices to negotiate to transmit at the highest possible speed. See Port Speed for more information about the port speed settings.

Example: To configure the TCP/IP port to communicate using 100 Mbps with half-duplex communication (communication in only one direction at a time), type:

```
portspeed -s 100H
```

prompt

Access: Administrator, Device User

Description: Configure the command line interface prompt to include or exclude the account type of the currently logged-in user. Any user can change this setting; all user accounts will be updated to use the new setting.

Option	Argument	Description
-s	long	The prompt includes the account type of the currently logged-in user.
	short	The default setting. The prompt is four characters long: `cli>`

Example: To include the account type of the currently logged-in user in the command prompt, type:

```
prompt -s long
```

quit

Access: Administrator, Device User

Description: Exit from the command line interface session.

radius

Access: Administrator only

Description: View the existing RADIUS settings, enable or disable RADIUS authentication, and configure basic authentication parameters for up to two RADIUS servers.

For a summary of RADIUS server configuration and a list of supported RADIUS servers, see Configuring the RADIUS Server.

Additional authentication parameters for RADIUS servers are available at the Web interface of the Rack PDU. See RADIUS for more information.

For detailed information about configuring your RADIUS server, see Appendix B: Security Handbook.

Option	Argument	Description
-a	local | radiusLocal | radius	Configure RADIUS authentication: **`local`**—RADIUS is disabled. Local authentication is enabled. **`radiusLocal`**—RADIUS, then Local Authentication. RADIUS and local authentication are enabled. Authentication is requested from the RADIUS server first. If the RADIUS server fails to respond, local authentication is used. **`radius`**—RADIUS is enabled. Local authentication is disabled.
-p1 -p2	<server IP>	The server name or IP address of the primary or secondary RADIUS server. **NOTE:** RADIUS servers use port 1812 by default to authenticate users. To use a different port, add a colon followed by the new port number to the end of the RADIUS server name or IP address.

Option	Argument	Description
-s1 -s2	<server secret>	The shared secret between the primary or secondary RADIUS server and the Rack PDU.
-t1 -t2	<server timeout>	The time in seconds that the Rack PDU waits for a response from the primary or secondary RADIUS server.

Example 1:

To view the existing RADIUS settings for the Rack PDU, type **`radius`** and press ENTER.

Example 2: To enable RADIUS and local authentication, type:

```
radius -a radiusLocal
```

Example 3: To configure a 10-second timeout for a secondary RADIUS server, type:

```
radius -t2 10
```

reboot

Access: Administrator only

Description: Restart the interface of the Rack PDU.

resetToDef

Access: Administrator only

Description:

Option	Arguments	Description
-p	all | keepip	Reset all configuration changes, including event actions, device settings, and, optionally, TCP/IP configuration settings.

Example: To reset all of the configuration changes except the TCP/IP settings for the Rack PDU, type:

```
resetToDef -p keepip
```

system

Access: Administrator only

Description:

Option	Argument	Description
-n	<system name>	Define the device name, the name of the person responsible for the device, and the physical location of the device. **NOTE:** If you define a value with more than one word, you must enclose the value in quotation marks.
-c	<system contact>	
-l	<system location>	

Example 1: To configure the device location as `Test Lab`, type:

```
system -l "Test Lab"
```

Example 2: To configure the system name as `Don Adams`, type:

```
system -n "Don Adams"
```

tcpip

Access: Administrator only

Description: Manually configure these network settings for the Rack PDU:

Option	Argument	Description
-i	<IP address>	Type the IP address of the Rack PDU, using the format *xxx.xxx.xxx.xxx*
-s	<subnet mask>	Type the subnet mask for the Rack PDU.
-g	<gateway>	Type the IP address of the default gateway. **Do not** use the loopback address (127.0.0.1) as the default gateway.
-d	<domain name>	Type the DNS name configured by the DNS server.
-h	<host name>	Type the host name that the Rack PDU will use.

Example 1: To view the network settings of the Rack PDU, type **`tcpip`** and press ENTER.

Example 2: To manually configure an IP address of **`150.250.6.10`** for the Rack PDU, type:

```
tcpip -i 150.250.6.10
```

user

Access: Administrator only

Description: Configure the user name and password for each account type, and configure the inactivity timeout.

For information on the permissions granted to each account type (Administrator, Device User, and Read-Only User), see Types of user accounts.

Option	Argument	Description
-an -dn -rn	<admin name> <device name> <read-only name>	Set the case-sensitive user name for each account type. The maximum length is 10 characters.
-ap -dp -rp	<admin password> <device password> <read-only password>	Set the case-sensitive password for each account type. The maximum length is 32 characters. Blank passwords (passwords with no characters) are not allowed.
-t	<minutes>	Configure the time (3 minutes by default) that the system waits before logging off an inactive user.

Example: To change the Administrator user name to XYZ, type:

```
user -an XYZ
```

To change the Administrator password to XYZ, type:

```
user -ap XYZ
```

web

Access: Administrator only

Description: Enable access to the Web interface using HTTP or HTTPS.

For additional security, you can change the port setting for HTTP and HTTPS to any unused port from 5000 to 32768. Users must then use a colon (:) in the address field of the browser to specify the port number. For example, for a port number of 5000 and an IP address of 152.214.12.114:

```
http://152.214.12.114:5000
```

Option	Argument	Definition
-S	disable | http | https	Configure access to the Web interface. When HTTPS is enabled, data is encrypted during transmission and authenticated by digital certificate.
-ph	<http port #>	Define the TCP/IP port used by HTTP to communicate with the Rack PDU (80 by default).
-ps	<https port #>	Define the TCP/IP port used by HTTPS to communicate with the Rack PDU (443 by default).

Example: To prevent all access to the Web interface, type:

```
web -S disable
```

xferINI

Access: Administrator only

Description: Use XMODEM to upload an INI file while you are accessing the command line interface through a serial connection. After the upload completes:

- If there are any system or network changes, the command line interface restarts and you must log in again.
- If you selected a baud rate for the file transfer that is not the same as the default baud rate for the Rack PDU, you must reset the baud rate to the default to reestablish communication with the Rack PDU.

xferStatus

Access: Administrator only

Description: View the result of the last file transfer.

See Verifying Upgrades and Updates for descriptions of the transfer result codes.

Device Command Descriptions

devLowLoad

Access: Administrator, Device User

Description: Set or view the low-load threshold in Kilowatts for the device.

Example 1: To view the low-load threshold, type:

```
cli> devLowLoad
E000: Success
0.5 kW
```

Example 2: To set the low-load threshold, type:

```
cli> devLowLoad 1.0
E000: Success
```

devNearOver

Access: Administrator, Device User

Description: Set or view the near-overload threshold in kilowatts for the device.

Example 1: To view the near-overload threshold, type:

```
cli> devNearOver
E000: Success
20.5 kW
```

Example 2: To set the near-overload threshold, type:

```
cli> devNearOver 21.3
E000: Success
```

devOverLoad

Access: Administrator, Device User

Description: Set or view the overload threshold in kilowatts for the device.

Example 1: To view the overload threshold, type:

```
cli> devOverLoad
E000: Success
25.0 kW
```

Example 2: To set the overload threshold, type:

```
cli> devOverLoad 25.5
E000: Success
```

devReading

Access: Administrator, Device User

Description: View the total power in kilowatts or total energy in kilowatt-hours for the device.

Argument	Definition
power	View the total power in kilowatts
energy	View the total energy in kilowatt-hours

Example 1: To view the total power, type:

```
cli> devReading power
E000: Success
5.2 kW
```

Example 2: To view the total energy, type:

```
cli> devReading energy
E000: Success
200.1 kWh
```

humLow

Access: Administrator, Device User

Description: Set or view the low humidity threshold as a percent of the relative humidity.

Example 1: To view the low humidity threshold, type:

```
cli> humLow
E000: Success
10 %RH
```

Example 2: To set the low humidity threshold, type:

```
cli> humLow 12
E000: Success
```

humMin

Access: Administrator, Device User

Description: Set or view the minimum humidity threshold as a percent of the relative humidity.

Example 1: To view the minimum humidity threshold, type:

```
cli> humMin
E000: Success
6 %RH
```

Example 2: To set the minimum humidity threshold, type:

```
cli> humMin 8
E000: Success
```

humReading

Access: Administrator, Device User

Description: View the humidity value from the sensor.

Example: To view the humidity value, type:

```
cli> humReading
E000: Success
25 %RH
```

inNormal

Access: Administrator, Device User

Description: View the normal state for each dry contact input.

Example: To view the normal state for each dry contact input, type:

```
cli> inNormal
E000: Success
1: Open
2: Open
```

inReading

Access: Administrator, Device User

Description: View the current state of each dry contact input.

Example: To view the state of the dry contact inputs, type:

```
cli> inReading
E000: Success
1: Open
2: Open
```

phLowLoad

Access: Administrator, Device User

Description: Set or view the phase low-load threshold in kilowatts. To specify phases, choose from the following options. Type: `all`, a single phase, a range, or a comma-separated list of phases.

Example 1: To set the low-load threshold for all phases to 1 kW, type:

```
cli> phLowLoad all 1
E000: Success
```

Example 2: To view the low-load threshold for phases 1 through 3, type:

```
cli> phLowLoad 1-3
E000: Success
1: 1 A
2: 1 A
3: 1 A
```

phNearOver

Access: Administrator, Device User

Description: Set or view the phase near-overload threshold in Kilowatts. To specify phases, choose from the following options. Type: `all`, a single phase, a range, or a comma-separated list of phases.

Example 1: To set the near-overload threshold for all phases to 10 kW, type:

```
cli> phNearOver all 10
E000: Success
```

Example 2: To view the near-overload threshold for phases 1 through 3, type:

```
cli> phNearOver 1-3
E000: Success
1: 10 A
2: 10 A
3: 10 A
```

phOverLoad

Access: Administrator, Device User

Description: Set or view the phase overload threshold in kilowatts. To specify phases, choose from the following options. Type: `all`, a single phase, a range, or a comma-separated list of phases.

Example 1: To set the overload threshold for all phases to 13 kW, type:

```
cli> phOverLoad all 13
E000: Success
```

Example 2: To view the overload threshold for phases 1 through 3, type:

```
cli> phOverLoad 1-3
E000: Success
1: 13 A
2: 13 A
3: 13 A
```

phReading

Access: Administrator, Device User

Description: View the current, voltage, or power for a phase. Set or view the phase near-overload threshold in kilowatts. To specify phases, choose from the following options. Type: `all`, a single phase, a range, or a comma-separated list of phases.

Example 1: To view the measurement for current for phase 3, type:

```
cli> phReading 3 current
E000: Success
3: 4 A
```

Example 2: To view the voltage for each phase, type:

```
cli> phReading all voltage
E000: Success
1: 120 V
2: 120 V
3: 120 V
```

Example 3: To view the power for phase 2, type:

```
cli> phReading 2 power
E000: Success
2: 40 W
```

prodInfo

Access: Administrator, Device User

Description: View information about the Rack PDU.

Example:

```
cli> prodInfo
E000: Success
AOS vX.X.X.X
Metered Rack PDU vX.X.X.X
Model:                DELL6803
Present Outlets:      12
Switched Outlets:     0
Metered Outlets:      0
Max Current:          20 A
Phases:               1
```

tempHigh

Access: Administrator, Device User

Description: Set or view the high-temperature threshold in either Fahrenheit or Celsius.

Example 1: To set the high-temperature threshold to 70º Fahrenheit, type:

```
cli> tempHigh F 70
E000: Success
```

Example 2: To view the high-temperature threshold in Celsius, type:

```
cli> tempHigh C
E000: Success
21 C
```

Example 3: To view the high-temperature threshold in Fahrenheit, type:

```
cli> tempHigh F
E000: Success
70 F
```

tempMax

Access: Administrator, Device User

Description: Set or view the max-temperature threshold in either Fahrenheit or Celsius.

Example 1: To set the max-temperature threshold to 80º Fahrenheit, type:

```
cli> tempMax F 80
E000: Success
```

Example 2: To view the max-temperature threshold in Celsius, type:

```
cli> tempMax C
E000: Success
27 C
```

Example 3: To view the max-temperature threshold in Fahrenheit, type:

```
cli> tempMax F
E000: Success
80 F
```

tempReading

Access: Administrator, Device User

Description: View the temperature value in either Fahrenheit or Celsius from the sensor.

Example: To view the temperature value in Fahrenheit, type:

```
cli> tempReading F
E000: Success
51.1 F
```

whoami

Access: Administrator, Device User

Description: View the user name of the active user.

Example:

```
cli> whoami
E000: Success
admin
```

Web Interface

Supported Web Browsers

You can use Microsoft® Internet Explorer® (IE) 7.x and higher (on Windows® operating systems only), Firefox version 3.0.6 and higher, by Mozilla Corporation (on all operating systems) to access the Rack PDU through its Web interface. Other commonly available browsers also may work but have not been fully tested.

The Rack PDU cannot work with a proxy server. Before you can use a Web browser to access the Rack PDU's Web interface, you must do one of the following:

- Configure the Web browser to disable the use of a proxy server for the Rack PDU.
- Configure the proxy server so that it does not proxy the specific IP address of the Rack PDU.

Logging On to the Web Interface

Overview

You can use the DNS name or IP address of the Rack PDU for the URL address of the Web interface. Use your case-sensitive user name and password to log on. The default user name and password differs by account type:

- **admin/admin** for an Administrator
- **device/device** for a Device User
- **readonly/readonly** for a Read-Only User

If you are using HTTPS as your access protocol, your login credentials are compared with information in a server certificate. If the certificate was created with the Security Wizard and an IP address was specified as the common name in the certificate, you must use an IP address to log on to the Rack PDU. If a DNS name was specified as the common name on the certificate, you must use a DNS name to log on.

For information about the Web page that appears when you log on to the Web interface, see About the Home Tab.

URL address formats

Type the DNS name or IP address of the Rack PDU in the Web browser's URL address field and press ENTER. When you specify a non-default Web server port in Internet Explorer, you must include `http://` or `https://` in the URL.

Common browser error messages at log-on.

Error Message	Cause of the Error	Browser
"You are not authorized to view this page" or "Someone is currently logged in..."	Someone else is logged on	Internet Explorer, Firefox
"This page cannot be displayed."	Web access is disabled, or the URL was not correct	Internet Explorer
"Unable to connect."		Firefox

URL format examples.

- For a DNS name of Web1:
  - – `http://Web1` if HTTP is your access mode.
  - – `https://Web1` if HTTPS is your access mode.
- For a System IP address of 139.225.6.133 and the default Web server port (80):
  - – `http://139.225.6.133` if HTTP is your access mode.
  - – `https//139.225.6.133` if HTTPS is your access mode.
- For a System IP address of 139.225.6.133 and a non-default Web server port (5000):
  - – `http://139.225.6.133:5000` if HTTP is your access mode.
  - – `https://139.225.6.133:5000` if HTTPS is your access mode.

Web Interface Features

Read the following to familiarize yourself with basic Web interface features for your Rack PDU.

Tabs

The following tabs are available:

- **Home**: Appears when you log on. View active alarms, the load status of the Rack PDU, and the most recent Rack PDU events. For more information, see About the Home Tab.
- **Device Manager**: View the load status for the Rack PDU, configure load thresholds, and view and manage the peak load measurement. For more information, see About the Device Manager Tab.
- **Environment**: View temperature and humidity sensor data, if sensors are connected to the **Rack PDU**.
- **Logs**: View event, data, and system logs.
- **Administration**: Configure security, network connection, notification, and general settings.

Device status icons

At the upper right corner of every tab, one or more icons and accompanying text indicate the current operating status of the Rack PDU:

❌	**Critical**: A critical alarm exists, which requires immediate action.
⚠	**Warning**: An alarm condition requires attention and could jeopardize your data or equipment if not addressed.
✓	**No Alarms**: No alarms are present and the Rack PDU is operating normally.

To return to the **Home** tab, click a device status icon from any tab.

Quick Links

At the lower left of the interface, there are three configurable links. The default settings follow:

- **Link 1**: dell.com
- **Link 2**: dell.com/home
- **Link 3:** dell.com/business

To reconfigure the links, see Configure Links.

Other Web interface features

- The IP address appears in the upper left corner.
- A context-sensitive **Help** link and **Log off** link are located in the upper right corner.

About the Home Tab

Use the Home tab to view active alarms, the load status of the Rack PDU, and the most recent Rack PDU events.

The Overview view

Path: Home > Overview

The top of the Overview indicates the alarm status. If one or more alarms are present, the number and type of alarms are indicated with a link to the **Alarm Status** view, where you can view descriptions of each alarm. If no alarms exist, the Overview displays, “No Alarms Present.”

In the **Load Status** area, view the load for the device in kW and for the phases in Amps, as applicable. The green, yellow, and red meter shows the current load status: normal, near overload, or overload. Note that if a low load threshold was configured the meter will also include a blue segment to the left of the green. Hover over the colors to view the configured load thresholds.

Click **More** to go to the **Device Manager** tab to configure thresholds and to view and manage peak load information.

In the device parameters area, view the name, contact, location, current rating, type of user account accessing the Rack PDU, and the amount of time the Rack PDU has been operating since the last reboot from either a power cycle or a reboot of the Management Interface. [For more information, see Reset the Rack PDU.]

In the **Recent Device Events** area, view, in reverse chronological order, the events that occurred most recently and the dates and times they occurred. A maximum of five events are shown at one time. Click **More Events** to go to the **Logs** tab to view the entire event log.

The Alarm Status view

Path: Home > Alarm Status

The **Alarm Status** view provides a description of all alarms present.

For details about a temperature or humidity threshold violation, click the Environment tab.

About the Device Manager Tab

Path: Device Manager

Use the **Device Manager** tab to perform the following:

- View the load status for the Rack PDU
- Configure load thresholds
- Configure a name and location for the Rack PDU.
- View and manage the peak load measurement

Viewing the load status and peak load

Path: Device Manager > *Load Management options*

Use the **Load Management** menu options to view the load for the device and phases (for a 3-phase Rack PDU). The indicator in the green, yellow, and red meter shows the current load status: normal, near overload, or overload. If a low load threshold was configured, the meter will include a blue segment to the left of the green. When viewing the **Device Load**, the triangle above the meter indicates peak load.

❗ Click **kW | BTU** in the upper right corner to toggle the load values between kilowatts and British Thermal Units (BTU).

Configuring Load Thresholds

Path: Device Manager > *Load Management options*

To configure load thresholds:

1. Click the **Device Manager** tab.
2. Using the Load Management menu, set the thresholds for the device and phases (for a 3-phase Rack PDU). The configurable thresholds are **Overload Alarm**, **Near Overload Warning**, and **Low Load Warning**.
3. Click **Apply**.

Configuring the Name and Location of the Rack PDU

Path: Device Manager > Load Management > Device Load

The name and location you enter appear on the **Home** tab.

> You can set the Name and Location through either the Device Manager tab or the Administration tab. A change in one affects the other.

1. Click the **Device Manager** tab, then **device load** from the **Load Management** menu.
2. Enter a name and location.
3. Click **Apply**.

Resetting Peak Load and kWh

Path: Device Manager > Device Load

1. Click the **Device Manager** tab, then **device load** from the **Load Management** menu.
2. Click the **Peak Load** and **Kilowatt-Hours** check boxes as desired.
3. Click **Apply**.

Configuring Temperature and Humidity Sensors

Path: Environment > Temperature & Humidity

Through the **Temperature & Humidity** page, when you have a temperature or a temperature and humidity sensor connected to the Rack PDU, you can set thresholds for Warning and Critical alarm generation (see Device status icons for details on each type of alarm).

For temperature:

- If the high temperature threshold is reached, the system generates a Warning alarm.
- If the maximum temperature threshold is reached, the system generates a Critical alarm.

Similarly, for humidity:

- If the low humidity threshold is reached, the system generates a Warning alarm.
- If the minimum humidity threshold is reached, the system generates a Critical alarm.

❗ Click the thermometer symbol in the upper right corner to toggle between fahrenheit and celsius.

To configure temperature and humidity sensors:

1. Enter values for minimum, maximum, high, and low thresholds.
2. Enter **Hysteresis** values. (See Hysteresis for details.)
3. Enable alarm generation as desired.
4. Click **Apply**.

Hysteresis. This value specifies how far past a threshold the temperature or humidity must return to clear a threshold violation.

- For Maximum and High temperature threshold violations, the clearing point is the threshold minus the hysteresis.
- For Minimum and Low humidity threshold violations, the clearing point is the threshold plus the hysteresis.

Increase the value for Temperature Hysteresis or Humidity Hysteresis to avoid multiple alarms if temperature or humidity that has caused a violation then wavers slightly up and down. If the hysteresis value is too low, such wavering can cause and clear a threshold violation repeatedly.

Example of rising but wavering temperature: The maximum temperature threshold is 85°F, and the temperature hysteresis is 3°F. The temperature rises above 85°F, violating the threshold. It then wavers down to 84°F and then up to 86°F repeatedly, but no clearing event and no new violation occur. For the existing violation to clear, the temperature would have to drop to 82°F (3°F below the threshold).

Example of falling but wavering humidity: The minimum humidity threshold is 18%, and the humidity hysteresis is 8%. The humidity falls below 18%, violating the threshold. It then wavers up to 24% and down to 13% repeatedly, but no clearing event and no new violation occur. For the existing violation to clear, the humidity would have to rise to above 26% (8% past the threshold).

Configuring Dry Contact Inputs

Path: Environment > Dry Contact Inputs

Through the **Dry Contact Inputs** page, view the current status and state for the dry contacts, and configure the dry contacts.

Parameter	**Description**
Name	A name for this input contact. *Maximum*: 20 characters.
Alarm Status	**Normal** if this input contact is not reporting an alarm, or the severity of the alarm, if this input contact is reporting an alarm
State	The current state of this input contact: **Closed** or **Open**.
Alarm Generation	Enable or disable this input contact. When disabled, the contact generates no alarm even when it is in the abnormal position
Normal State	The normal (non-alarm) state of this input contact: **Closed** or **Open**.

Using the Event and Data Logs

Event log

Path: Logs > Events > *options*

You can view, filter, or delete the event log. By default, the log displays all events recorded during the last two days in reverse chronological order.

For lists of all configurable events and their current configuration, select the **Administration** tab, **Notification** on the top menu bar, and **by event** under **Event Actions** on the left navigation menu.

See Configuring by event.

To display the event log (Logs > Events > log):

- By default, view the event log as a page of the Web interface. The most recent event is recorded on page 1. In the navigation bar below the log:
  - Click a page number to open a specific page of the log.
  - Click **Previous** or **Next** to view the events recorded immediately before or after the events listed on the open page.
  - Click **<<** to return to the first page or click **>>** to view the last page of the log.
- To see the listed events on one page, click **Launch Log in New Window** from the event log page to display a full-screen view of the log.

In your browser's options, JavaScript® must be enabled for you to use the **Launch Log in New Window** button.

You can also use FTP or Secure CoPy (SCP) to view the event log. See How to use FTP or SCP to retrieve log files.

To filter the log (Logs > Events > log):

- **Filtering the log by date or time:** To display the entire event log, or to change the number of days or weeks for which the log displays the most recent events, select **Last**. Select a time range from the drop-down menu, then click **Apply**. The filter configuration is saved until the Rack PDU restarts.
  To display events logged during a specific time range, select **From**. Specify the beginning and ending times (using the 24-hour clock format) and dates for which to display events, then click **Apply**. The filter configuration is saved until the Rack PDU restarts.
- **Filtering the log by event**: To specify the events that display in the log, click **Filter Log**. Clear the checkbox of an event category or alarm severity level to remove it from view. Text at the upper right corner of the event log page indicates that a filter is active.
  As Administrator, click **Save As Default** to save this filter as the default log view for all users. If you do not click **Save As Default**, the filter is active until you clear it or until the Rack PDU restarts.
  To remove an active filter, click **Filter Log**, then **Clear Filter (Show All)**.

Events are processed through the filter using **OR** logic.

- Events that you do not select from the **Filter By Severity** list never display in the filtered event log, even if the event occurs in a category you selected from the **Filter by Category** list.
- Events that you do not select from the **Filter by Category** list never display in the filtered event log, even if devices in the category enter an alarm state you selected from the **Filter by Severity** list.

To delete the log (Logs > Events > log):

To delete all events recorded in the log, click **Clear Log** on the Web page that displays the log. Deleted events cannot be retrieved.

To disable the logging of events based on their assigned severity level or their event category, see Configuring by event.

To configure reverse lookup (Logs > Events > reverse lookup):

Reverse lookup is disabled by default. Enable this feature unless you have no DNS server configured or have poor network performance because of heavy network traffic.

With reverse lookup enabled, when a network-related event occurs, both the IP address and the domain name for the networked device associated with the event are logged in the event log. If no domain name entry exists for the device, only its IP address is logged with the event. Since domain names generally change less frequently than IP addresses, enabling reverse lookup can improve the ability to identify addresses of networked devices that are causing events.

To resize the event log (Logs > Events > size):

By default, the event log stores 400 events. You can change the number of events the log stores. When you resize the event log, all existing log entries are deleted. To avoid losing log data, use FTP or SCP to retrieve the log before you enter a new value in the **Event Log Size** field.

See How to use FTP or SCP to retrieve log files.

When the log is full, the older entries are deleted.

Data log

Path: Logs > Data > *options*

The data log records the current and power for the device and phases (for a 3-phase Rack PDU), as applicable, as well as temperature and humidity and dry contact data at the specified time interval. Each entry is listed by the date and time the data was recorded.

To display the data log (Logs > Data > log):

- By default, view the data log as a page of the Web interface. The most recent data item is recorded on page 1. From the navigation menu below the log:
  - Click a page number to open a specific page of the log.
  - Click **Previous** or **Next** to view the data recorded immediately before or after the data that is listed on the open page.
  - Click **<<** to return to the first page of the log, or click **>>** to view the last page of the log.
- To see the listed data on one page, click **Launch Log in New Window** from the data log page to display a full-screen view of the log.

In your browser's options, JavaScript must be enabled for you to use the **Launch Log in New Window** button.

Alternatively, you can use FTP or SCP to view the data log. See How to use FTP or SCP to retrieve log files.

To filter the log by date or time (Logs > Data > log):

To display the entire data log or to change the number of days or weeks for which the log displays the most recent events, select **Last**. Select a time range from the drop-down menu, then click **Apply**. The filter configuration is saved until the device restarts.

To display data logged during a specific time range, select **From**. Specify the beginning and ending times (using the 24-hour clock format) and dates for which to display data, then click **Apply**. The filter configuration is saved until the device restarts.

To delete the data log:

To delete all data recorded in the log, click **Clear Data Log** on the Web page that displays the log. Deleted data cannot be retrieved.

To set the data collection interval (Logs > Data > interval):

Define, in the **Log Interval** setting, how frequently data is sampled and stored in the data log, and view the calculation of how many days of data the log can store, based on the interval you selected. When the log is full, the older entries are deleted. To avoid automatic deletion of older data, enable and configure data log rotation, described in the next section.

To configure data log rotation (Logs > Data > rotation):

Set up a password-protected data log repository on a specified FTP server. Enabling rotation causes the contents of the data log to be appended to the file you specify by name and location. Updates to this file occur at the upload interval you specify.

Parameter	Description
Data Log Rotation	Enable or disable (the default) data log rotation.
FTP Server Address	The location of the FTP server where the data repository file is stored.
User Name	The user name required to send data to the repository file. This user must also be configured to have read and write access to the data repository file and the directory (folder) in which it is stored.
Password	The password required to send data to the repository file.
File Path	The path to the repository file.
Filename	The name of the repository file (an ASCII text file).

Parameter	Description
Delay *X* hours between uploads.	The number of hours between uploads of data to the file.
Upload every *X* minutes	The number of minutes between attempts to upload data to the file after an upload failure.
Up to *X* times	The maximum number of times the upload will be attempted after an initial failure.
Until Upload Succeeds	Attempt to upload the file until the transfer is completed.

To resize the data log (Logs > Data > size):

By default, the data log stores 400 events. You can change the number of data points the log stores. When you resize the data log, all existing log entries are deleted. To avoid losing log data, use FTP or SCP to retrieve the log before you enter a new value in the **Data Log Size** field.

📖 See How to use FTP or SCP to retrieve log files.

When the log is full, the older entries are deleted.

How to use FTP or SCP to retrieve log files

An Administrator or Device User can use FTP or SCP to retrieve a tab-delineated event log file (*event.txt*) or data log file (*data.txt*) and import it into a spreadsheet.

- The file reports all events or data recorded since the log was last deleted or (for the data log) truncated because it reached maximum size.
- The file includes information that the event log or data log does not display.
  - The version of the file format (first field)
  - The date and time the file was retrieved
  - The **Name**, **Contact**, and **Location** values and IP address of the Rack PDU
  - The unique **Event Code** for each recorded event (*event.txt* file only)

The Rack PDU uses a four-digit year for log entries. You may need to select a four-digit date format in your spreadsheet application to display all four digits.

If you are using the encryption-based security protocols for your system, use Secure CoPy (SCP) to retrieve the log file.

If you are using unencrypted authentication methods for the security of your system, use FTP to retrieve the log file.

See Appendix B: Security Handbook for information on available protocols and methods for setting up the type of security you need.

To use SCP to retrieve the files. To use SCP to retrieve the *event.txt* file, use the following command:

```
scp username@hostname_or_ip_address:event.txt ./event.txt
```

To use SCP to retrieve the *data.txt* file, use the following command:

```
scp username@hostname_or_ip_address:data.txt ./data.txt
```

To use FTP to retrieve the files. To use FTP to retrieve the *event.txt* or *data.txt* file:

1. At a command prompt, type `ftp` and the IP address of the Rack PDU, and press ENTER.

   If the **Port** setting for the **FTP Server** option (set through the **Network** menu of the **Administration** tab) has been changed from its default (**21**), you must use the non-default value in the FTP command. For Windows FTP clients, use the following command, including spaces. (For some FTP clients, you must use a colon instead of a space between the IP address and the port number.)

   ```
   ftp>open ip_address port_number
   ```

   To set a non-default port value to enhance security for the FTP Server, see FTP Server. You can specify any port from 5001 to 32768.

2. Use the case-sensitive **User Name** and **Password** for Administrator or Device User to log on. For Administrator, **admin** is the default for **User Name** and **Password**. For the Device User, the defaults are **device** for **User Name** and **Password**.
3. Use the **get** command to transmit the text of a log to your local drive.

   ```
   ftp>get event.txt
   ```

   or

   ```
   ftp>get data.txt
   ```

4. You can use the **del** command to clear the contents of either log.

   ```
   ftp>del event.txt
   ```

   or

   ```
   ftp>del data.txt
   ```

   You will not be asked to confirm the deletion.

   - If you clear the data log, the event log records a deleted-log event.
   - If you clear the event log, a new *event.txt* file records the event.

5. Type `quit` at the `ftp>` prompt to exit from FTP.

Local Users

Setting user access

Path: Administration > Security > Local Users > *options*

The Administrator user account always has access to the Rack PDU.

The Device User and Read-Only User accounts are enabled by default. To disable the Device User or Read-Only User accounts, select the user account from the left navigation menu, then clear the **Enable** checkbox.

You set the case-sensitive user name and password for each account type in the same manner. Maximum length is 10 characters for a user name and 32 characters for a password. Blank passwords (passwords with no characters) are not allowed.

For information on the permissions granted to each account type (Administrator, Device User, and Read-Only User), see Types of user accounts.

Account Type	Default User Name	Default Password	Permitted Access
Administrator	admin	admin	Web interface and command line interface
Device User	device	device	
Read-Only User	readonly	readonly	Web interface only

Remote Users

Authentication

Path: Administration > Security > Remote Users > Authentication Method

Use this option to select how to administer remote access to the Rack PDU.

For information about local authentication (not using the centralized authentication of a RADIUS server), see the Appendix B: Security Handbook.

The Rack PDU supports the authentication and authorization functions of RADIUS (Remote Authentication Dial-In User Service).

- When a user accesses the Rack PDU or other network-enabled device that has RADIUS enabled, an authentication request is sent to the RADIUS server to determine the user's permission level.
- RADIUS user names used with the Rack PDU are limited to 32 characters.

Select one of the following:

- **Local Authentication Only**: RADIUS is disabled. Local authentication is enabled.
- **RADIUS, then Local Authentication**: RADIUS and local authentication are enabled. Authentication is requested from the RADIUS server first. If the RADIUS server fails to respond, local authentication is used.
- **RADIUS Only**: RADIUS is enabled. Local authentication is disabled.

If **RADIUS Only** is selected, and the RADIUS server is unavailable, improperly identified, or improperly configured, remote access is unavailable to all users. You must use a serial connection to the command line interface and change the **access** setting to **local** or **radiusLocal** to regain access. For example, the command to change the access setting to **local** would be:

```
radius -a local
```

RADIUS

Path: Administration > Security > Remote Users > RADIUS

Use this option to do the following:

- List the RADIUS servers (a maximum of two) available to the Rack PDU and the time-out period for each.
- Click **Add Server**, and configure the parameters for authentication by a new RADIUS server.
- Click a listed RADIUS server to display and modify its parameters.

RADIUS Setting	Definition
RADIUS Server	The server name or IP address of the RADIUS server. **NOTE:** RADIUS servers use port 1812 by default to authenticate users. To use a different port, add a colon followed by the new port number to the end of the RADIUS server name or IP address.
Secret	The shared secret between the RADIUS server and the Rack PDU.
Timeout	The time in seconds that the Rack PDU waits for a response from the RADIUS server.
Test Settings	Enter the Administrator user name and password to test the RADIUS server path that you have configured.
Skip Test and Apply	Do not test the RADIUS server path.
Switch Server Priority	Change which RADIUS server will authenticate users if two configured servers are listed and **RADIUS, then Local Authentication** or **RADIUS Only** is the enabled authentication method.

Configuring the RADIUS Server

Summary of the configuration procedure

You must configure your RADIUS server to work with the Rack PDU.

For examples of the RADIUS users file with Vendor Specific Attributes (VSAs) and an example of an entry in the dictionary file on the RADIUS server, see Appendix B: Security Handbook.

1. Add the IP address of the Rack PDU to the RADIUS server client list (file).
2. Users must be configured with Service-Type attributes unless Vendor Specific Attributes (VSAs) are defined. If no Service-Type attributes are configured, users will have read-only access (on the Web interface only).

   See your RADIUS server documentation for information about the RADIUS users file, and see Appendix B: Security Handbook for an example.

3. VSAs can be used instead of the Service-Type attributes provided by the RADIUS server. VSAs require a dictionary entry and a RADIUS users file. In the dictionary file, define the names for the ATTRIBUTE and VALUE keywords, but not for the numeric values. If you change numeric values, RADIUS authentication and authorization will fail. VSAs take precedence over standard RADIUS attributes.

Configuring a RADIUS server on UNIX® with shadow passwords

If UNIX shadow password files are used (/etc/passwd) with the RADIUS dictionary files, the following two methods can be used to authenticate users:

- If all UNIX users have administrative privileges, add the following to the RADIUS "user" file. To allow only Device Users, change the DELL-Service-Type to `Device`.

```
DEFAULT       Auth-Type = System
              DELL-Service-Type = Admin
```

- Add user names and attributes to the RADIUS "user" file, and verify the password against /etc/passwd. The following example is for users `bconners` and `thawk`:

```
bconners       Auth-Type = System
               DELL-Service-Type = Admin
thawk          Auth-Type = System
               DELL-Service-Type = Device
```

Supported RADIUS servers

Supported RADIUS servers: FreeRADIUS and Microsoft IAS 2003. Other commonly available RADIUS applications may work but have not been fully tested.

Inactivity Timeout

Path: Administration > Security > Auto Log Off

Use this option to configure the time (3 minutes by default) that the system waits before logging off an inactive user. If you change this value, you must log off for the change to take effect.

This timer continues to run if a user closes the browser window without first logging off by clicking **Log Off** at the upper right. Because that user is still considered to be logged on, no user can log on until the time specified as **Minutes of Inactivity** expires. For example, with the default value for **Minutes of Inactivity**, if a user closes the browser window without logging off, no user can log on for 3 minutes.

TCP/IP and Communication Settings

TCP/IP settings

Path: Administration > Network > TCP/IP

The **TCP/IP** option on the left navigation menu, selected by default when you choose **Network** on the top menu bar, displays the current IP address, subnet mask, default gateway, and MAC address of the Rack PDU.

On the same page, **TCP/IP Configuration** provides the following options for how the TCP/IP settings will be configured when the Rack PDU turns on, resets, or restarts: **Manual**, **BOOTP**, **DHCP**, and **DHCP & BOOTP**.

For information on DHCP and DHCP options, see **RFC2131** and **RFC2132**.

Setting	Description
Manual	The IP address, subnet mask, and default gateway must be configured manually. Click **Next>>**, and enter the new values.

1. The default values for these three settings on the configuration pages generally do not need to be changed:
   - •**Vendor Class**: DELL
   - •**Client ID**: The MAC address of the Rack PDU, which uniquely identifies it on the local area network (LAN)
   - •**User Class**: The name of the application firmware module

Setting	Description
BOOTP	A BOOTP server provides the TCP/IP settings. At 32-second intervals, the Rack PDU requests network assignment from any BOOTP server: • If the Rack PDU receives a valid response, it starts the network services. • If the Rack PDU finds a BOOTP server, but a request to that server fails or times out, the Rack PDU stops requesting network settings until it is restarted. • By default, if previously configured network settings exist, and the Rack PDU receives no valid response to five requests (the original and four retries), it uses the previously configured settings so that it remains accessible. Click **Next>>** to access the BOOTP Configuration page to change the number of retries or the action to take if all retries fail [1]: • **Maximum retries**: Enter the number of retries that will occur when no valid response is received, or zero (0) for an unlimited number of retries. • **If retries fail**: Select **Use prior settings** (the default) or **Stop BOOTP request**.
DHCP	The default setting. At 32-second intervals, the Rack PDU requests network assignment from any DHCP server. • If the Rack PDU receives a valid response, it does not require the vendor cookie from the DHCP server in order to accept the lease and start the network services. • If the Rack PDU finds a DHCP server, but the request to that server fails or times out, it stops requesting network settings until it is restarted[1]. • **Require vendor specific cookie to accept DHCP Address**: By selecting this check box, you can require the DHCP server to provide a cookie which supplies information to the Rack PDU.

[1] The default values for these three settings on the configuration pages generally do not need to be changed:

- **Vendor Class**: DELL
- **Client ID**: The MAC address of the Rack PDU, which uniquely identifies it on the local area network (LAN)
- **User Class**: The name of the application firmware module

Setting	Description
DHCP & BOOTP	The default setting. The Rack PDU tries to obtain its TCP/IP settings from a BOOTP server first, and then, if it cannot discover a BOOTP server, from a DHCP server. If it obtains its TCP/IP settings from either server, it switches this setting to **BOOTP** or **DHCP**, depending on the type of server that supplied the TCP/IP settings to the Rack PDU. Click **Next>>** to configure the same settings that are on the **BOOTP Configuration** and **DHCP Configuration** pages[1] and to specify that the **DHCP and BOOTP** setting be retained after either type of server provides the TCP/IP values.

1. The default values for these three settings on the configuration pages generally do not need to be changed:
   - **Vendor Class**: DELL
   - **Client ID**: The MAC address of the Rack PDU, which uniquely identifies it on the local area network (LAN)
   - **User Class**: The name of the application firmware module

DHCP response options

Each valid DHCP response contains options that provide the TCP/IP settings that the Rack PDU needs to operate on a network, and other information that affects the operation of the Rack PDU.

Vendor Specific Information (option 43). The Rack PDU uses this option in a DHCP response to determine whether the DHCP response is valid. This option contains up to two specific options in a TAG/LEN/DATA format: the Vendor Cookie and the Boot Mode Transition.

- **Vendor Cookie. Tag 1, Len 4, Data "1APC"**
  Option 43 communicates to the Rack PDU that a DHCP server is configured to service the Dell Rack PDUs. By default, the Rack PDU does not require this cookie.

  To enable the requirement of a vendor cookie, see DHCP.

  Following, in hexadecimal format, is an example of a Vendor Specific Information option that contains the vendor cookie:

  ```
  Option 43 = 0x01 0x04 0x31 0x41 0x50 0x43
  ```

- **Boot Mode Transition. Tag 2, Len 1, Data 1/2**
  This option 43 setting enables or disables **Remain in DHCP & BOOTP mode after accepting TCP/IP settings**, which, by default, is disabled.
  - A data value of 1 enables **Remain in DHCP & BOOTP mode after accepting TCP/IP settings**. Whenever the Rack PDU reboots, it will request its network assignment first from a BOOTP server, and then, if necessary, from a DHCP server.
  - A data value of 2 disables the option **Remain in DHCP & BOOTP mode after accepting TCP/IP settings** option. The **TCP/IP Configuration** setting option switches to **DHCP** when the Rack PDU accepts the DHCP response. Whenever the Rack PDU reboots, it will request its network assignment from a DHCP server only.

  Following, in hexadecimal format, is an example of a Vendor Specific Information option that contains the vendor cookie and the **disable** setting for **Boot Mode Transition**:

  ```
  Option 43 = 0x01 0x04 0x31 0x41 0x50 0x43 0x02 0x01 0x01
  ```

TCP/IP options. The Rack PDU uses the following options within a valid DHCP response to define its TCP/IP settings. All of these options except the first are described in **RFC2132**.

- **IP Address** (from the **yiaddr** field of the DHCP response, described in **RFC2131)**: The IP address that the DHCP server is leasing to the Rack PDU.
- **Subnet Mask** (option 1): The Subnet Mask value that the Rack PDU needs to operate on the network.
- **Router,** i.e., Default Gateway (option 3): The default gateway address that the Rack PDU needs to operate on the network.
- **IP Address Lease Time** (option 51): The time duration for the lease of the IP Address to the Rack PDU.
- **Renewal Time, T1** (option 58): The time that the Rack PDU must wait after an IP address lease is assigned before it can request a renewal of that lease.
- **Rebinding Time, T2** (option 59): The time that the Rack PDU must wait after an IP address lease is assigned before it can seek to rebind that lease.

Other options. The Rack PDU also uses these options within a valid DHCP response. All of these options except the last are described in **RFC2132**.

- **Network Time Protocol Servers** (option 42): Up to two NTP servers (primary and secondary) that the Rack PDU can use.
- **Time Offset** (option 2): The offset of the Rack PDU's subnet, in seconds, from Coordinated Universal Time (UTC).
- **Domain Name Server** (option 6): Up to two Domain Name System (DNS) servers (primary and secondary) that the Rack PDU can use.
- **Host Name** (option 12): The host name that the Rack PDU will use (32-character maximum length).
- **Domain Name** (option 15): The domain name that the Rack PDU will use (64-character maximum length).
- **Boot File Name** (from the **file** field of the DHCP response, described in **RFC2131**): The fully qualified directory-path to a user configuration file (.ini file) to download. The **siaddr** field of the DHCP response specifies the IP address of the server from which the Rack PDU will download the .ini file. After the download, the Rack PDU uses the .ini file as a boot file to reconfigure its settings.

Port Speed

Path: Administration > Network > Port Speed

The **Port Speed** setting defines the communication speed of the TCP/IP port.

- For **Auto-negotiation** (the default), Ethernet devices negotiate to transmit at the highest possible speed, but if the supported speeds of two devices are unmatched, the slower speed is used.
- Alternatively, you can choose 10 Mbps or 100 Mbps, each with the option of half-duplex (communication in only one direction at a time) or full-duplex (communication in both directions on the same channel simultaneously).

DNS

Path: Administration > Network > DNS > *options*

Use the options under **DNS** on the left navigation menu to configure and test the Domain Name System (DNS):

- Select **servers** to specify the IP addresses of the primary and optional secondary DNS server. For the Rack PDU to send e-mail, at least the IP address of the primary DNS server must be defined.
  - The Rack PDU waits up to 15 seconds for a response from the primary DNS server or the secondary DNS server (if a secondary DNS server is specified). If the Rack PDU does not receive a response within that time, e-mail cannot be sent. Therefore, use DNS servers on the same segment as the Rack PDU or on a nearby segment (but not across a wide-area network [WAN]).
  - After you define the IP addresses of the DNS servers, verify that DNS is working correctly by entering the DNS name of a computer on your network to look up the IP address for that computer.

- Select **naming** to define the host name and domain name of the Rack PDU:
  - **Host Name**: After you configure a host name here and a domain name in the **Domain Name** field, users can enter a host name in any field in the Rack PDU interface (except e-mail addresses) that accepts a domain name.
  - **Domain Name**: You need to configure the domain name here only. In all other fields in the Rack PDU interface (except e-mail addresses) that accept domain names, the Rack PDU adds this domain name when only a host name is entered.
    - To override all instances of the expansion of a specified host name by the addition of the domain name, set the domain name field to its default, `somedomain.com`, or to `0.0.0.0`.
    - To override the expansion of a specific host name entry (for example, when defining a trap receiver), include a trailing period. The Rack PDU recognizes a host name with a trailing period (such as *`mySnmpServer.`*) as if it were a fully-qualified domain name and does not append the domain name.
- Select **test** to send a DNS query that tests the setup of your DNS servers:
  - As **Query Type**, select the method to use for the DNS query:
    - **by Host**: the URL name of the server
    - **by FQDN**: the fully-qualified domain name
    - **by IP**: the IP address of the server
    - **by MX**: the Mail Exchange used by the server
  - As **Query Question**, identify the value to be used for the selected query type:

Query Type Selected	Query Question to Use
by Host	The URL
by FQDN	The fully qualified domain name, *`my_server.my_domain`*.
by IP	The IP address
by MX	The Mail Exchange address

  - View the result of the test DNS request in the **Last Query Response** field.

Web

Path: Administration > Network > Web > *options*

Option	Description
access	To activate changes to any of these selections, log off from the Rack PDU: • **Disable**: Disables access to the Web interface. (To re-enable access, log in to the command line interface, then type the command **`http -S enable`**. For HTTPS access, type **`https -S enable`**.) • **Enable HTTP** (the default): Enables Hypertext Transfer Protocol (HTTP), which provides Web access by user name and password, but does not encrypt user names, passwords, and data during transmission. • **Enable HTTPS**: Enables Hypertext Transfer Protocol (HTTPS) over Secure Sockets Layer (SSL). SSL encrypts user names, passwords, and data during transmission, and authenticates the Rack PDU by digital certificate. When HTTPS is enabled, your browser displays a small lock icon. See “Creating and Installing Digital Certificates” in Appendix B: Security Handbook to choose among the several methods for using digital certificates.

	HTTP Port: The TCP/IP port (80 by default) used to communicate by HTTP with the Rack PDU.
	HTTPS Port: The TCP/IP port (443 by default) used to communicate by HTTPS with the Rack PDU.
	For either of these ports, you can change the port setting to any unused port from 5000 to 32768 for additional security. Users must then use a colon (:) in the address field of the browser to specify the port number. For example, for a port number of 5000 and an IP address of 152.214.12.114:
	`http://152.214.12.114:5000`
	`https://152.214.12.114:5000`

Option	Description
ssl certificate	Add, replace, or remove a security certificate. **Status**: • **Not installed**: A certificate is not installed, or was installed by FTP or SCP to an incorrect location. Using **Add or Replace Certificate File** installs the certificate to the correct location, **/ssl** on the Rack PDU. • **Generating**: The Rack PDU is generating a certificate because no valid certificate was found. • **Loading**: A certificate is being activated on the Rack PDU. • **Valid certificate**: A valid certificate was installed or was generated by the Rack PDU. Click on this link to view the contents of the certificate. **If you install an invalid certificate, or if no certificate is loaded when you enable SSL, the Management Card generates a default certificate, a process which delays access to the interface for up to one minute.** You can use the default certificate for basic encryption-based security, but a security alert message displays whenever you log on. **Add or Replace Certificate File**: Enter or browse to the certificate file created with the Security Wizard. See “Creating and Installing Digital Certificates” in Appendix B: Security Handbook to choose a method for using digital certificates created by the Security Wizard or generated by the Rack PDU. **Remove**: Delete the current certificate.

Console

Path: Administration > Network > Console > *options*

Option	Description

access	Choose one of the following for access by Telnet or Secure SHell (SSH):
	• **Disable**: Disables all access to the command line interface.
	• **Enable Telnet** (the default): Telnet transmits user names, passwords, and data without encryption.
	• **Enable SSH**: SSH transmits user names, passwords, and data in encrypted form, providing protection from attempts to intercept, forge, or alter data during transmission.
	Configure the ports to be used by these protocols:
	• **Telnet Port**: The Telnet port used to communicate with the Rack PDU (23 by default). You can change the port setting to any unused port from 5000 to 32768 for additional security. Users must then use a colon (:) or a space, as required by your Telnet client program, to specify the non-default port. For example, for port 5000 and an IP address of 152.214.12.114, your Telnet client requires one of the these commands:
	`telnet 152.214.12.114:5000`
	`telnet 152.214.12.114 5000`
	• **SSH Port**: The SSH port used to communicate with the Rack PDU (22 by default). You can change the port setting to any unused port from 5000 to 32768 for additional security. See the documentation for your SSH client for the command line format required to specify a non-default port.

Option	Description
ssh host key	**Status** indicates the status of the host key (private key): • **SSH Disabled: No host key in use:** When disabled, SSH cannot use a host key. • **Generating**: The Rack PDU is creating a host key because no valid host key was found. • **Loading**: A host key is being activated on the Rack PDU. • **Valid**: One of the following valid host keys is in the **/ssh** directory (the required location on the Rack PDU): •A 1024-bit or 2048-bit host key created by the Security Wizard •A 2048-bit RSA host key generated by the Rack PDU **Add or Replace**: Browse to and upload a host key file created by the Security Wizard. To use the Security Wizard, see the Appendix B: Security Handbook. **NOTE:** To reduce the time required to enable SSH, create and upload a host key in advance. **If you enable SSH with no host key loaded, the Rack PDU takes up to one minute to create a host key, and the SSH server is not accessible during that time.** **Remove**: Remove the current host key.

To use SSH, you must have an SSH client installed. Most Linux and other UNIX platforms include an SSH client, but Microsoft Windows operating systems do not. Clients are available from various vendors.

SNMP

All user names, passwords, and community names for SNMP are transferred over the network as plain text. If your network requires the high security of encryption, disable SNMP access or set the access for each community to Read. (A community with Read access can receive status information and use SNMP traps.)

For detailed information on enhancing and managing the security of your system, see Appendix B: Security Handbook.

SNMPv1

Path: Administration > Network > SNMPv1 > *options*

Option	Description
access	**Enable SNMPv1 Access:** Enables SNMP version 1 as a method of communication with this device.
access control	You can configure up to four access control entries to specify which Network Management Systems (NMSs) have access to this device. The opening page for access control, by default, assigns one entry to each of the four available SNMPv1 communities, but you can edit these settings to apply more than one entry to any community to grant access by several specific IP addresses, host names, or IP address masks. To edit the access control settings for a community, click its community name. • If you leave the default access control entry unchanged for a community, that community has access to this device from any location on the network. • If you configure multiple access control entries for one community name, the limit of four entries requires that one or more of the other communities must have no access control entry. If no access control entry is listed for a community, that community has no access to this device. **Community Name:** The name that an NMS must use to access the community. The maximum length is 15 ASCII characters, and the default community names for the four communities are **`public`**, **`private`**, **`public2`**, and **`private2`**. **NMS IP/Host Name:** The IP address, IP address mask, or host name that controls access by NMSs. A host name or a specific IP address (such as 149.225.12.1) allows access only by the NMS at that location. IP addresses that contain 255 restrict access as follows: • 149.225.12.**255**: Access only by an NMS on the 149.225.12 segment. • 149.225.**255.255**: Access only by an NMS on the 149.225 segment. • 149.**255.255.255**: Access only by an NMS on the 149 segment. • 0.0.0.0 (the default setting) which can also be expressed as 255.255.255.255: Access by any NMS on any segment. **Access Type**: The actions an NMS can perform through the community. • **Read**: GETS only, at any time • **Write**: GETS at any time, and SETS when no user is logged onto the Web interface or command line interface. • **Write+**: GETS and SETS at any time. • **Disable**: No GETS or SETS at any time.

SNMPv3

Path: Administration > Network > SNMPv3 > *options*

For SNMP GETs, SETs, and trap receivers, SNMPv3 uses a system of user profiles to identify users. An SNMPv3 user must have a user profile assigned in the MIB software program to perform GETs and SETs, browse the MIB, and receive traps.

To use SNMPv3, you must have a MIB program that supports SNMPv3.

The Rack PDU supports SHA or MD5 authentication and AES or DES encryption.

Option	Description
access	**SNMPv3 Access:** Enables SNMPv3 as a method of communication with this device.

Option	Description
user profiles	By default, lists the settings of four user profiles, configured with the user names **dell snmp profile1** through **dell snmp profile4**, and no authentication and no privacy (no encryption). To edit the following settings for a user profile, click a user name in the list. **User Name:** The identifier of the user profile. SNMP version 3 maps GETs, SETs, and traps to a user profile by matching the user name of the profile to the user name in the data packet being transmitted. A user name can have up to 32 ASCII characters. **Authentication Passphrase:** A phrase of 15 to 32 ASCII characters (**`dell auth passphrase`**, by default) that verifies that the NMS communicating with this device through SNMPv3 is the NMS it claims to be, that the message has not been changed during transmission, and that the message was communicated in a timely manner, indicating that it was not delayed and that it was not copied and sent again later at an inappropriate time. **Privacy Passphrase:** A phrase of 15 to 32 ASCII characters (**`dell crypt passphrase`**, by default) that ensures the privacy of the data (by means of encryption) that an NMS is sending to this device or receiving from this device through SNMPv3. **Authentication Protocol:** The Dell implementation of SNMPv3 supports SHA and MD5 authentication. Authentication will not occur unless an authentication protocol is selected. **Privacy Protocol:** The Dell implementation of SNMPv3 supports AES and DES as the protocols for encrypting and decrypting data. Privacy of transmitted data requires that a privacy protocol is selected and that a privacy passphrase is provided in the request from the NMS. When a privacy protocol is enabled but the NMS does not provide a privacy passphrase, the SNMP request is not encrypted. **Note:** You cannot select the privacy protocol if no authentication protocol is selected.

Option	Description
access control	You can configure up to four access control entries to specify which NMSs have access to this device. The opening page for access control, by default, assigns one entry to each of the four user profiles, but you can edit these settings to apply more than one entry to any user profile to grant access by several specific IP addresses, host names, or IP address masks. • If you leave the default access control entry unchanged for a user profile, all NMSs that use that profile have access to this device. • If you configure multiple access entries for one user profile, the limit of four entries requires that one or more of the other user profiles must have no access control entry. If no access control entry is listed for a user profile, no NMS that uses that profile has any access to this device. To edit the access control settings for a user profile, click its user name. **Access:** Mark the **Enable** checkbox to activate the access control specified by the parameters in this access control entry. **User Name:** From the drop-down list, select the user profile to which this access control entry will apply. The choices available are the four user names that you configure through the **user profiles** option on the left navigation menu. **NMS IP/Host Name:** The IP address, IP address mask, or host name that controls access by the NMS. A host name or a specific IP address (such as 149.225.12.1) allows access only by the NMS at that location. An IP address mask that contains 255 restricts access as follows: • 149.225.12.**255**: Access only by an NMS on the 149.225.12 segment. • 149.225.**255.255**: Access only by an NMS on the 149.225 segment. • 149.**255.255.255**: Access only by an NMS on the 149 segment. • 0.0.0.0 (the default setting) which can also be expressed as 255.255.255.255: Access by any NMS on any segment.

FTP Server

Path: Administration > Network > FTP Server

The **FTP Server** settings enable (by default) or disable access to the FTP server and specify the TCP/IP port (21 by default) that the FTP server uses to communicate with the Rack PDU. The FTP server uses both the specified port and the port one number lower than the specified port.

You can change the **Port** setting to the number of any unused port from 5001 to 32768 for added security. Users must then use a colon (:) to specify the non-default port number. For example, for port 5001 and IP address 152.214.12.114, the command would be `ftp 152.214.12.114:5001`.

FTP transfers files without encryption. For higher security, disable the FTP server, and transfer files with Secure CoPy (SCP). Selecting and configuring Secure SHell (SSH) enables SCP automatically.

For detailed information on enhancing and managing the security of your system, see Appendix B: Security Handbook.

Event Actions

Path: Administration > Notification > Event Actions > *options*

Types of notification

You can configure event actions to occur in response to an event or group of events. These actions notify users of the event in any of several ways:

- Active, automatic notification. The specified users or monitoring devices are contacted directly.
  - E-mail notification
  - SNMP traps
  - Syslog notification
- Indirect notification
  - Event log. If no direct notification is configured, users must check the log to determine which events have occurred

    You can also log system performance data to use for device monitoring. See Data log for information on how to configure and use this data logging option.
  - Queries (SNMP GETs)

    For more information, see SNMP. SNMP enables an NMS to perform informational queries. For SNMPv1, which does not encrypt data before transmission, configuring the most restrictive SNMP access type (READ) enables informational queries without the risk of allowing remote configuration changes.

Configuring event actions

Notification parameters. For events that have an associated clearing event, you can also set the following parameters as you configure events individually or by group, as described in the next two sections. To access the parameters, click the receiver or recipient name.

Parameter	Description
Delay x time before sending	If the event persists for the specified time, a notification is sent. If the condition clears before the time expires, no notification is sent.
Repeat at an interval of *x* time	The notification is sent at the specified interval (e.g., every 2 minutes).
Up to *x* times	During an active event, the notification repeats for this number of times.
Until condition clears	The notification is sent repeatedly until the condition clears or is resolved.

Configuring by event. To define event actions for an individual event:

1. Select the **Administration** tab, **Notification** on the top menu bar, and **by event** under **Event Actions** on the left navigation menu.
2. In the list of events, review the marked columns to see whether the action you want is already configured. (By default, logging is configured for all events.)
3. To view or change the current configuration, such as recipients to be notified by e-mail or paging, or Network Management Systems (NMSs) to be notified by SNMP traps, click on the event name.

! If no Syslog server is configured, items related to Syslog configuration are not displayed.

When viewing details of an event's configuration, you can change the configuration, enable or disable event logging or Syslog, or disable notification for specific e-mail recipients or trap receivers, but you cannot add or remove recipients or receivers. To add or remove recipients or receivers, see the following:

- Identifying Syslog servers
- E-mail recipients
- Trap Receivers

Configuring by group. To configure a group of events simultaneously:

1. Select the **Administration** tab, **Notification** on the top menu bar, and **by group** under **Event Actions** on the left navigation menu.
2. Choose how to group events for configuration:
   - Choose **Grouped by severity**, and then select all events of one or more severity levels. You cannot change the severity of an event.
   - Choose **Grouped by category**, and then select all events in one or more pre-defined categories.
3. Click **Next>>** to move from page to page to do the following:

   a. Select event actions for the group of events.

   - To choose any action except **Logging** (the default), you must first have at least one relevant recipient or receiver configured.
   - If you choose **Logging** and have configured a Syslog server, select **Event Log** or **Syslog** (or both) on the next page.

   b. Select whether to leave the newly configured event action enabled for this group of events or to disable the action.

Active, Automatic, Direct Notification

E-mail notification

Overview of setup. Use the Simple Mail Transfer Protocol (SMTP) to send e-mail to up to four recipients when an event occurs.

To use the e-mail feature, you must define the following settings:

- The IP addresses of the primary and, optionally, the secondary Domain Name System (DNS) servers

  See DNS.

- The IP address or DNS name for **SMTP Server** and **From Address**

  See SMTP.

- The e-mail addresses for a maximum of four recipients

  See E-mail recipients.

You can use the **To Address** setting of the **recipients** option to send e-mail to a text-based pager.

SMTP.

Path: Administration > Notification > E-mail > server

Setting	Description
Local SMTP Server	The IP address or DNS name of the local SMTP server. **NOTE:** This definition is required only when **SMTP Server** is set to **Local**. See E-mail recipients.
From Address	The contents of the **From** field in e-mail messages sent by the Rack PDU: • In the format *user@* [*IP_address*] (if an IP address is specified as **Local SMTP Server**) • In the format *user@domain* (if DNS is configured and the DNS name is specified as **Local SMTP Server**) in the e-mail messages. **NOTE:** The local SMTP server may require that you use a valid user account on the server for this setting. See the server's documentation.

E-mail recipients.

Path: Administration > Notification > E-mail > recipients

Identify up to four e-mail recipients.

Setting	Description
To Address	The user and domain names of the recipient. To use e-mail for paging, use the e-mail address for the recipient's pager gateway account (for example, `myacct100@skytel.com`). The pager gateway will generate the page. To bypass the DNS lookup of the mail server's IP address, use the IP address in brackets instead of the e-mail domain name, e.g., use jsmith@[xxx.xxx.x.xxx] instead of jsmith@company.com. This is useful when DNS lookups are not working correctly. **NOTE:** The recipient's pager must be able to use text-based messaging.

Setting	Description
SMTP Server	Select one of the following methods for routing e-mail: • **Local**: Through the Rack PDU’s SMTP server. This setting (recommended) ensures that the e-mail is sent before the Rack PDU’s 20-second time-out, and, if necessary, is retried several times. Also do one of the following: • Enable forwarding at the Rack PDU’s SMTP server so that it can route e-mail to external SMTP servers. Typically, SMTP servers are not configured to forward e-mail. Check with the administrator of your SMTP server before changing its configuration to allow forwarding. • Set up a special e-mail account for the Rack PDU to forward e-mail to an external mail account. • **Recipient**: Directly to the recipient’s SMTP server. With this setting, the Rack PDU tries to send the e-mail only once. On a busy remote SMTP server, the time-out may prevent some e-mail from being sent. When the recipient uses the Rack PDU’s SMTP server, this setting has no effect.
E-mail Generation	Enables (by default) or disables sending e-mail to the recipient.
Format	The long format contains Name, Location, Contact, IP address, serial number of the device, date and time, event code, and event description. The short format provides only the event description.

E-mail test.

Path: Administration>Notification>E-mail>test

Send a test message to a configured recipient.

SNMP traps

Trap Receivers.

Path: Administration > Notification > SNMP Traps > trap receivers

View trap receivers by NMS IP/Host Name. You can configure up to six trap receivers.

- To configure a new trap receiver, click **Add Trap Receiver**.
- To modify or delete a trap receiver, first click its IP address or host name to access its settings. (If you delete a trap receiver, all notification settings configured under Event Actions for the deleted trap receiver are set to their default values.)
- To specify the trap type for a trap receiver, select either the SNMPv1 or SNMPv3 radio button. For an NMS to receive both types of traps, you must configure two trap receivers for that NMS, one for each trap type.

Item	Definition
Trap Generation	Enable (the default) or disable trap generation for this trap receiver.
NMS IP/Host Name	The IP address or host name of this trap receiver. The default, 0.0.0.0, leaves the trap receiver undefined.

SNMPv1 option.

Item	Definition
Community Name	The name (`public` by default) used as an identifier when SNMPv1 traps are sent to this trap receiver.
Authenticate Traps	When this option is enabled (the default), the NMS identified by the NMS IP/Host Name setting will receive authentication traps (traps generated by invalid attempts to log on to this device). To disable that ability, unmark the checkbox.

SNMPv3 option. Select the identifier of the user profile for this trap receiver. (To view the settings of the user profiles identified by the user names selectable here, choose **Network** on the top menu bar and **user profiles** under **SNMPv3** on the left navigation menu.)

See SNMPv3 for information on creating user profiles and selecting authentication and encryption methods.

SNMP Trap Test

Path: Administration > Notification > SNMP Traps > test

Last Test Result. The result of the most recent SNMP trap test. A successful SNMP trap test verifies only that a trap was sent; it does not verify that the trap was received by the selected trap receiver. A trap test succeeds if all of the following are true:

- The SNMP version (SNMPv1 or SNMPv3) configured for the selected trap receiver is enabled on this device.
- The trap receiver is enabled.
- If a host name is selected for the **To** address, that host name can be mapped to a valid IP address.

To. Select the IP address or host name to which a test SNMP trap will be sent. If no trap receiver is configured, a link to the **Trap Receiver** configuration page is displayed.

Syslog

Path: Logs > Syslog > *options*

The Rack PDU can send messages to up to four Syslog servers when an event occurs. The Syslog servers record events that occur at network devices in a log that provides a centralized record of events.

This user’s guide does not describe Syslog or its configuration values in detail. See **RFC3164** for more information about Syslog.

Identifying Syslog servers.

Path: Logs > Syslog > servers

Setting	Definition
Syslog Server	Uses IP addresses or host names to identify from one to four servers to receive Syslog messages sent by the Rack PDU.
Port	The user datagram protocol (UDP) port that the Rack PDU will use to send Syslog messages. The default is **514**, the UDP port assigned to Syslog.

Syslog settings.

Path: Logs > Syslog > settings

Setting	**Definition**
Message Generation	Enables (by default) or disables the Syslog feature.
Facility Code	Selects the facility code assigned to the Rack PDU's Syslog messages (**User**, by default). **NOTE: User** best defines the Syslog messages sent by the Rack PDU. **Do not** change this selection unless advised to do so by the Syslog network or system administrator.
Severity Mapping	Maps each severity level of Rack PDU or Environment events to available Syslog priorities. You should not need to change the mappings. The following definitions are from RFC3164: • **Emergency**: The system is unusable • **Alert**: Action must be taken immediately • **Critical**: Critical conditions • **Error**: Error conditions • **Warning**: Warning conditions • **Notice**: Normal but significant conditions • **Informational**: Informational messages • **Debug**: Debug-level messages Following are the default settings for the **Local Priority** settings: • **Severe** is mapped to **Critical** • **Warning** is mapped to **Warning** • **Informational** is mapped to **Info** **NOTE:** To disable Syslog messages, see Configuring event actions.

Administration: General Options

Identification

Path: Administration > General > Identification

Define the **Name** (the device name), **Location** (the physical location), and **Contact** (the person responsible for the device) used by the SNMP agent of the Rack PDU. These settings are the values used for the MIB-II **sysName**, **sysContact**, and **sysLocation** Object Identifiers (OIDs).

📖 For more information about MIB-II OIDs, see the Dell Management Information Base (MIB).

Set the Date and Time

Method

Path: Administration > General > Date & Time > mode

Set the time and date used by the Rack PDU. You can change the current settings manually or through a Network Time Protocol (NTP) Server:

- **Manual Mode**: Do one of the following:
  - Enter the date and time for the Rack PDU.
  - Mark the checkbox **Apply Local Computer Time** to match the date and time settings of the computer you are using.
- **Synchronize with NTP Server**: Have an NTP Server define the date and time for the Rack PDU.

Setting	Definition
Primary NTP Server	Enter the IP address or domain name of the primary NTP server.
Secondary NTP Server	Enter the IP address or domain name of the secondary NTP server, when a secondary server is available.
Time Zone	Select a time zone. The number of hours preceding each time zone in the list is the offset from Coordinated Universal Time (UTC), formerly Greenwich Mean Time.
Update Interval	Define how often, in hours, the Rack PDU accesses the NTP Server for an update. *Minimum*: 1; *Maximum*: 8760 (1 year).
Update Using NTP Now	Initiate an immediate update of the date and time by the NTP Server.

Daylight saving

Path: Administration > General > Date & Time > daylight saving

Enable traditional United States Daylight Saving Time (DST), or enable and configure a customized daylight saving time to match how Daylight Saving Time is implemented in your local area. DST is disabled by default.

When customizing Daylight Saving Time (DST):

- If the local DST always starts or ends on the fourth occurrence of a specific weekday of a month (e.g, the fourth Sunday), choose **Fourth/Last**. If a fifth Sunday occurs in that month in a subsequent year, the time setting still changes on the fourth Sunday.
- If the local DST always starts or ends on the last occurrence of a specific weekday of a month, whether it is the fourth or the fifth occurrence, choose **Fifth/Last**.

Format

Path: Administration > General > Date & Time > date format

Select the numerical format in which to display all dates in this user interface. In the selections, each letter m (for month), d (for day), and y (for year) represents one digit. Single-digit days and months are displayed with a leading zero.

Use an .ini File

Path: Administration > General > User Config File

Use the settings from one Rack PDU to configure another. Retrieve the config.ini file from the configured Rack PDU, customize that file (e.g., to change the IP address), and upload the customized file to the new Rack PDU. The file name can be up to 64 characters, and must have the.ini suffix.

Status	Reports the progress of the upload. The upload succeeds even if the file contains errors, but a system event reports the errors in the event log.
Upload	Browse to the customized file and upload it so that the current Rack PDU can use it to set its own configuration.

To retrieve and customize the file of a configured Rack PDU, see How to Export Configuration Settings.

Instead of uploading the file to one Rack PDU, you can export the file to multiple Rack PDUs by using an FTP or SCP script.

Event Log and Temperature Units

Path: Administration > General > Preferences

Color-code event log text

This option is disabled by default. Mark the **Event Log Color Coding** checkbox to enable color-coding of alarm text recorded in the event log. System-event entries and configuration-change entries do not change color.

Text Color	Alarm Severity
Red	**Critical**: A critical alarm exists, which requires immediate action.
Orange	**Warning**: An alarm condition requires attention and could jeopardize your data or equipment if its cause is not addressed.
Green	**Alarm Cleared**: The conditions that caused the alarm have improved.
Black	**Normal**: No alarms are present. The Rack PDU and all connected devices are operating normally.

Change the default temperature scale

Select the temperature scale (Fahrenheit or Celsius) in which to display all temperature measurements in this user interface.

Reset the Rack PDU

Path: Administration > General > Reset/Reboot

Action	Definition
Reboot Management Interface	Restarts the interface of the Rack PDU.
Reset All[1]	Clear the **Exclude TCP/IP** checkbox to reset all configuration values; mark the **Exclude TCP/IP** checkbox to reset all values except TCP/IP
Reset Only[1]	**TCP/IP settings**: Set TCP/IP Configuration to **DHCP & BOOTP**, its default setting, requiring that the Rack PDU receive its TCP/IP settings from a DHCP or BOOTP server. See TCP/IP and Communication Settings.
	Event configuration: Reset all changes to event configuration, by event and by group, to their default settings.
	RPDU to Defaults: Resets only Rack PDU settings, not network settings, to their defaults.
1. Resetting may take up to a minute.	

Configure Links

Path: Administration > General > Quick Links

Select the **Administration** tab, **General** on the top menu bar, and **Quick Links** on the left navigation menu to view and change the URL links displayed at the bottom left of each page of the interface.

By default, these links access the following Web pages:

- **Link 1**: dell.com
- **Link 2**: dell.com/home
- **Link 3:** dell.com/business

To reconfigure any of the following, click the link name in the **Display** column:

- **Display**: The short link name displayed on each interface page
- **Name**: A name that fully identifies the target or purpose of the link
- **Address**: Any URL—for example, the URL of another device or server

About the Rack PDU

Path: Administration > General > About

The hardware information is useful for troubleshooting problems with the Rack PDU. The serial number and MAC address are also available on the Rack PDU itself.

Firmware information for the Application Module, Dell OS (AOS), and Boot Monitor indicates the name, the firmware version, and the date and time each firmware module was created. This information is also useful in troubleshooting.

Management Uptime is the length of time the interface has been running continuously.

How to Export Configuration Settings

Retrieving and Exporting the .ini File

Summary of the procedure

An Administrator can retrieve the .ini file of a Rack PDU and export it to another Rack PDU or to multiple Rack PDUs.

1. Configure a Rack PDU to have the settings you want to export.
2. Retrieve the .ini file from that Rack PDU.
3. Customize the file to change at least the TCP/IP settings.
4. Use a file transfer protocol supported by the Rack PDU to transfer a copy to one or more other Rack PDUs. For a transfer to multiple Rack PDUs, use an FTP or SCP script.

Each receiving Rack PDU uses the file to reconfigure its own settings and then deletes it.

Contents of the .ini file

The config.ini file you retrieve from a Rack PDU contains the following:

- *section headings* and *keywords* (only those supported for the device from which you retrieve the file)*:* Section headings are category names enclosed in brackets ([ ]). Keywords, under each section heading, are labels describing specific Rack PDU settings. Each keyword is followed by an equals sign and a value (either the default or a configured value).
- The **`Override`** keyword: With its default value, this keyword prevents the exporting of one or more keywords and their device-specific values. For example, in the **`[NetworkTCP/IP]`** section, the default value for **`Override`** (the MAC address of the Rack PDU) blocks the exporting of values for the **`SystemIP`**, **`SubnetMask`**, **`DefaultGateway`**, and **`BootMode`**.

Detailed procedures

Retrieving. To set up and retrieve an .ini file to export:

1. If possible, use the interface of a Rack PDU to configure it with the settings to export. Directly editing the .ini file risks introducing errors.
2. To use FTP to retrieve config.ini from the configured Rack PDU:

   a. Open a connection to the Rack PDU, using its IP address:

   ```
   ftp> open ip_address
   ```

   b. Log on using the Administrator user name and password.

   c. Retrieve the config.ini file containing the Rack PDU’s settings:

   ```
   ftp> get config.ini
   ```

   The file is written to the folder from which you launched FTP.

Customizing. You must customize the file before you export it.

1. Use a text editor to customize the file.
   - Section headings, keywords, and pre-defined values are not case-sensitive, but string values that you define are case-sensitive.
   - Use adjacent quotation marks to indicate no value. For example, `LinkURL1=""` indicates that the URL is intentionally undefined.
   - Enclose in quotation marks any values that contain leading or trailing spaces or are already enclosed in quotation marks.
   - To export scheduled events, configure the values directly in the .ini file.
   - To export a system time with the greatest accuracy, if the receiving Rack PDUs can access a Network Time Protocol server, configure `enabled` for `NTPEnable`:

     ```
     NTPEnable=enabled
     ```

     Alternatively, reduce transmission time by exporting the `[SystemDate/Time]` section as a separate .ini file.
   - To add comments, start each comment line with a semicolon (`;`).
2. Copy the customized file to another file name in the same folder:
   - The file name can have up to 64 characters and must have the .ini suffix.
   - Retain the original customized file for future use. **The file that you retain is the only record of your comments.**

Transferring the file to a single Rack PDU. To transfer the .ini file to another Rack PDU, do either of the following:

- From the Web interface of the receiving Rack PDU, select the **Administration** tab, **General** on the top menu bar, and **User Config File** on the left navigation menu. Enter the full path of the file, or use **Browse**.
- Use any file transfer protocol supported by Rack PDUs, i.e., FTP, FTP Client, SCP, or TFTP. The following example uses FTP:

  a. From the folder containing the copy of the customized .ini file, use FTP to log in to the Rack PDU to which you are exporting the .ini file:

  ```
  ftp> open ip_address
  ```

  b. Export the copy of the customized .ini file to the root directory of the receiving Rack PDU:

  ```
  ftp> put filename.ini
  ```

Exporting the file to multiple Rack PDUs. To export the .ini file to multiple Rack PDUs, use FTP or SCP, but write a script that incorporates and repeats the steps used for exporting the file to a single Rack PDU.

The Upload Event and Error Messages

The event and its error messages

The following event occurs when the receiving Rack PDU completes using the .ini file to update its settings.

```
Configuration file upload complete, with number valid values
```

If a keyword, section name, or value is invalid, the upload by the receiving Rack PDU succeeds, and additional event text states the error.

Event text	Description
Configuration file warning: Invalid keyword on line *number*. Configuration file warning: Invalid value on line *number*.	A line with an invalid keyword or value is ignored.
Configuration file warning: Invalid section on line *number.*	If a section name is invalid, all keyword/value pairs in that section are ignored.
Configuration file warning: Keyword found outside of a section on line *number*.	A keyword entered at the beginning of the file (i.e., before any section headings) is ignored.
Configuration file warning: Configuration file exceeds maximum size.	If the file is too large, an incomplete upload occurs. Reduce the size of the file, or divide it into two files, and try uploading again.

Messages in config.ini

A Rack PDU from which you download the config.ini file must be discovered successfully in order for its configuration to be included. If the Rack PDU is not present or is not discovered, the config.ini file contains a message under the appropriate section name, instead of keywords and values. For example:

```
      Rack PDU not discovered
```

If you did not intend to export the configuration of the Rack PDU as part of the .ini file import, ignore these messages.

Errors generated by overridden values

The **`Override`** keyword and its value will generate error messages in the event log when it blocks the exporting of values.

See Contents of the .ini file for information about which values are overridden.

Because the overridden values are device-specific and not appropriate to export to other Rack PDUs, ignore these error messages. To prevent these error messages, delete the lines that contain the **`Override`** keyword and the lines that contain the values that they override. Do not delete or change the line containing the section heading.

How to Upgrade Firmware

Benefits of upgrading firmware

When you upgrade the firmware on the Rack PDU:

- You obtain the latest bug fixes and performance improvements.
- New features become available for immediate use.

Keeping the firmware versions consistent across your network ensures that all Rack PDUs support the same features in the same manner.

Firmware files

A firmware version consists of three modules: An Operating System (AOS) module, an application module, and a boot monitor (bootmon) module. Each module contains one or more Cyclical Redundancy Checks (CRCs) to protect its data from corruption during transfer.

The Operating System (AOS), application, and boot monitor module files used with the Rack PDU share the same basic format:

`dell_`*`hardware-version`*`_`*`type`*`_`*`firmware-version.bin`*

- **`dell`**: Indicates that this is a Dell file.
- ***`hardware-version`*****: `hw0`*x*** identifies the version of the hardware on which you can use this binary file.
- ***`type`*****:** Identifies whether the file is the Operating System (AOS) module, the application module, or the boot monitor module for the Rack PDU.
- ***`version`*****:** The version number of the file.
- **`bin`**: Indicates that this is a binary file.

❗ If the boot monitor module must be updated, a boot monitor module is included in the firmware release. Otherwise, the boot monitor module that is installed on the card is compatible with the firmware update.

Firmware File Transfer Methods

To upgrade the firmware of a Rack PDU, use one of these methods:

- From a networked computer on any supported operating system, use FTP or SCP to transfer the individual AOS and application firmware modules.
- For a Rack PDU that is not on your network, use XMODEM through a serial connection to transfer the individual firmware modules from your computer to the Rack PDU.

❗ When you transfer individual firmware modules, **you must** transfer the Operating System (AOS) module to the Rack PDU before you transfer the application module.

Use FTP or SCP to upgrade one Rack PDU

FTP. To use FTP to upgrade one Rack PDU over the network:

- The Rack PDU must be connected to the network, and its system IP, subnet mask, and default gateway must be configured.
- The FTP server must be enabled at the Rack PDU.
- The firmware files must have been downloaded from Dell.com.

To transfer the files:

1. At a computer on the network, open a command prompt window. Go to the directory that contains the firmware files, and list the files:

```
C:\>cd\dell
C:\dell>dir
```

For the listed files, *xxx* represents the firmware version number:

- **dell_hw05_aos_*xxx*.bin**
- **dell_hw05_application_*xxx*.bin**

2. Open an FTP client session:

   ```
   C:\dell>ftp
   ```

3. Type `open` and the IP address of the Rack PDU, and press ENTER. If the **port** setting for the FTP Server has changed from its default of **21**, you must use the non-default value in the FTP command.

   - For Windows FTP clients, separate a non-default port number from the IP address by a space. For example:

     ```
     ftp> open 150.250.6.10 21000
     ```

   - Some FTP clients require a colon instead before the port number.

4. Log on as Administrator; **admin** is the default user name and password.
5. Upgrade the AOS. (In the example, *xxx* is the firmware version number):

   ```
   ftp> bin
   ftp> put dell_hw05_aos_xxx.bin
   ```

6. When FTP confirms the transfer, type **quit** to close the session.
7. After 20 seconds, repeat step 2 through step 5. In step 5, use the application module file name.

SCP. To use Secure CoPy (SCP) to upgrade firmware for the Rack PDU:

1. Identify and locate the firmware modules described in the preceding instructions for FTP.
2. Use an SCP command line to transfer the AOS firmware module to the Rack PDU. The following example uses *xxx* to represent the version number of the AOS module:

   ```
   scp dell_hw05_aos_xxx.bin
   dell@158.205.6.185:dell_hw05_aos_xxx.bin
   ```

3. Use a similar SCP command line, with the name of the application module, to transfer the application firmware module to the Rack PDU.

How to upgrade multiple Rack PDUs

Use FTP or SCP to upgrade multiple Rack PDUs. To upgrade multiple Rack PDUs using an FTP client or using SCP, write a script which automatically performs the procedure.

Use XMODEM to upgrade one Rack PDU

To use XMODEM to upgrade one Rack PDU that is not on the network, you must first download the firmware files from Dell.com.

To transfer the files:

1. Select a serial port at the local computer and disable any service that uses the port.
2. Connect the provided serial configuration cable to the selected port and to the serial port at the Rack PDU.
3. Run a terminal program such as HyperTerminal, and configure the selected port for 57600 bps, 8 data bits, no parity, 1 stop bit, and no flow control.
4. Press the RESET button on the Rack PDU, then immediately press the ENTER key twice, or until the Boot Monitor prompt displays: **`BM>`**
5. Type **`XMODEM`**, then press ENTER.
6. From the terminal program's menu, select XMODEM, then select the binary AOS firmware file to transfer using XMODEM. After the XMODEM transfer is complete, the Boot Monitor prompt returns.
7. To install the application module, repeat step 5 and step 6. In step 6, use the application module file name.
8. Type **`reset`** or press the Reset button to restart the Rack PDU.

For information about the format used for firmware modules, see Firmware files.

Verifying Upgrades and Updates

Verify the success or failure of the transfer

To verify whether a firmware upgrade succeeded, use the `xferStatus` command in the command line interface to view the last transfer result, or use an SNMP GET to the **mfiletransferStatusLastTransferResult** OID.

Last Transfer Result codes

Code	Description
Successful	The file transfer was successful.
Result not available	There are no recorded file transfers.
Failure unknown	The last file transfer failed for an unknown reason.
Server inaccessible	The TFTP or FTP server could not be found on the network.
Server access denied	The TFTP or FTP server denied access.
File not found	The TFTP or FTP server could not locate the requested file.
File type unknown	The file was downloaded but the contents were not recognized.
File corrupt	The file was downloaded but at least one Cyclical Redundancy Check (CRC) failed.

Verify the version numbers of installed firmware.

Use the Web interface to verify the versions of the upgraded firmware modules by selecting the **Administration** tab, **General** on the top menu bar, and **About** on the left navigation menu, or use an SNMP GET to the MIB II **sysDescr** OID. In the command line interface, use the `about` command.

Troubleshooting

Rack PDU Access Problems

Problem	Solution
Unable to ping the Rack PDU	If the Rack PDU's Status LED is green, try to ping another node on the same network segment as the Rack PDU. If that fails, it is not a problem with the Rack PDU. If the Status LED is not green, or if the ping test succeeds, perform the following checks: • Verify all network connections. • Verify the IP addresses of the Rack PDU and the NMS. • If the NMS is on a different physical network (or subnetwork) from the Rack PDU, verify the IP address of the default gateway (or router). • Verify the number of subnet bits for the Rack PDU's subnet mask.
Cannot allocate the communications port through a terminal program	Before you can use a terminal program to configure the Rack PDU, you must shut down any application, service, or program using the communications port.
Cannot access the command line interface through a serial connection	Make sure that you did not change the baud rate. Try 2400, 9600, 19200, or 38400.
Cannot access the command line interface remotely	• Make sure you are using the correct access method, Telnet or Secure SHell (SSH). An Administrator can enable these access methods. By default, Telnet is enabled. Enabling SSH automatically disables Telnet. • For SSH, the Rack PDU may be creating a host key. The Rack PDU can take up to one minute to create the host key, and SSH is inaccessible for that time.

Problem	Solution
Cannot access the Web interface	• Verify that HTTP or HTTPS access is enabled. • Make sure you are specifying the correct URL — one that is consistent with the security system used by the Rack PDU. SSL requires **https**, not **http**, at the beginning of the URL. • Verify that you can ping the Rack PDU. • Verify that you are using a Web browser supported for the Rack PDU. See Supported Web Browsers. • If the Rack PDU has just restarted and SSL security is being set up, the Rack PDU may be generating a server certificate. The Rack PDU can take up to one minute to create this certificate, and the SSL server is not available during that time.

Appendix A: List of Supported Commands

Network Management Card Command Descriptions

```
?
about
alarmcount
    [-p [all | warning | critical]]
boot
    [-b <dhcpBootp | dhcp | bootp | manual>]
    [-a <remainDhcpBootp | gotoDhcpOrBootp>]
    [-o <stop | prevSettings>]
    [-f <retry then fail #>]
    [-c <dhcp cookie> [enable | disable]]
    [-s <retry then stop #>]
    [-v <vendor class>]
    [-i <client id>]
    [-u <user class>]
cd
date
    [-d <"datestring">]
    [-t <00:00:00>]
    [-f [mm/dd/yy | dd.mm.yyyy | mmm-dd-yy |
    dd-mmm-yy | yyyy-mm-dd]]
delete
dir
eventlog
exit
format
ftp
    [-p <port number>]
    [-S <enable | disable>]
help
ping
    [<IP address or DNS name>]
portspeed
    [-s [auto | 10H | 10F | 100H | 100F]]
prompt
    [-s [long | short]]
quit
radius
    [-a <access> [local | radiusLocal | radius]]
    [-p# <server IP>]
    [-s# <server secret>]
    [-t# <server timeout>]
reboot
resetToDef
    [-p [all | keepip]]
system
    [-n <system name>]
    [-c <system contact>]
    [-l <system location>]
tcpip
    [-i <IP address>]
    [-s <subnet mask>]
    [-g <gateway>]
    [-d <domain name>]
    [-h <host name>]
user
    [-an <Administrator name>]
    [-dn <Device User name>]
    [-rn <Read-Only User name>]
    [-ap <Administrator password>]
    [-dp <Device User password>]
    [-rp <Read-Only User password>]
    [-t <inactivity timeout in minutes>]
web
    [-S <disable | http | https>]
    [-ph <http port #>]
    [-ps <https port #>]
xferINI
xferStatus
```

Device Command Descriptions

```
devLowLoad
    [<power>]
devNearOver
    [<power>]
devOverLoad
    [<power>]
devReading
    [<“power” | “energy”>]
humLow
    [<humidity>]
humMin
    [<humidity>]
humReading
inNormal
inReading
phLowLoad
    [<“all” | phase#> <current>]
phNearOver
    [<“all” | phase#> <current>]
phOverLoad
    [<“all” | phase#> <current>]
phReading
    [<“all” | phase#> <“current” | “voltage” | “power”>]
prodInfo
tempHigh
    [<“F” | “C”> <temperature>]
tempMax
    [<“F” | “C”> <temperature>]
tempReading
    [<“F” | “C”>]
whoami
```

Appendix B: Security Handbook

Content and Purpose of This Appendix

This appendix documents security features for firmware version 5.*x*.*x* for Dell® Rack PDUs which enable Rack PDUs to function remotely over the network.

This appendix documents the following protocols and features, how to select which ones are appropriate for your situation, and how to set up and use them within an overall security system:

- Telnet and Secure SHell (SSH)
- Secure Sockets Layer (SSL)
- RADIUS
- SNMPv1 and SNMPv3

In addition, this appendix documents how to use the Rack PDU Security Wizard to create the components required for the high security available through SSL and SSH.

Security Features

Protection of passwords and passphrases

No password or passphrase is stored on the Rack PDU in plain text.

- Passwords are hashed using a one-way hash algorithm.
- Passphrases, which are used for authentication and encryption, are encrypted before they are stored on the Rack PDU.

Summary of access methods

Serial access to the command line interface.

Security Access	Description
Access is by user name and password.	Always enabled.

Remote access to the command line interface.

Security Access	Description
Available methods: • User name and password • Selectable server port • Access protocols that can be enabled or disabled • Secure SHell (SSH)	For high security, use SSH. • With Telnet, the user name and password are transmitted as plain text. • Enabling SSH disables Telnet and provides encrypted access to the command line interface to provide additional protection from attempts to intercept, forge, or alter data during transmission.

SNMPv1 and SNMPv3.

Security Access	Description
Available methods (SNMPv1): • Community Name • Host Name • NMS IP filters • Agents that can be enabled or disabled • Four access communities with read/write/disable capability	For both SNMPv1 and SNMPv3, the host name restricts access to the Network Management System (NMS) at that location only, and the NMS IP filters allow access only to the NMSs specified by one of the IP address formats in the following examples: • 159.215.12.1: Only the NMS at the IP address 159.215.12.1. • 159.215.12.255: Any NMS on the 159.215.12 segment. • 159.215.255.255: Any NMS on the 159.215 segment. • 159.255.255.255: Any NMS on the 159 segment. • 0.0.0.0 or 255.255.255.255: Any NMS. SNMPv3 has additional security features that include the following: • An authentication passphrase to ensure that an NMS trying to access the Rack PDU is the NMS it claims to be. • Encryption of data during transmission, with a privacy passphrase required for encrypting and decrypting.
Available methods (SNMPv3): • Four User Profiles • Authentication through an authentication passphrase • Encryption through a privacy passphrase • SHA or MD5 authentication • AES or DES encryption algorithm • NMS IP filters	

File transfer protocols.

Security Access	Description
Available methods: • User name and password • Selectable server port • FTP Server and access protocols that can be enabled or disabled • Secure CoPy (SCP)	With FTP, the user name and password are transmitted as plain text, and files are transferred without encryption. Use SCP to encrypt the user name and password and the files being transferred, such as firmware updates, configuration files, log files, Secure Sockets Layer (SSL) certificates, and Secure SHell (SSH) host keys. If you choose SCP as your file transfer protocol, enable SSH and disable FTP.

Web server.

Security Access	Description
Available methods: • User name and password • Selectable server port • Web interface access that can be enabled or disabled • Secure Sockets Layer (SSL)	In basic HTTP authentication mode, the user name and password are transmitted base-64 encoded (with no encryption). SSL is available on Web browsers supported for use with the Management Card or network-enabled device and on most Web servers. The Web protocol HyperText Transfer Protocol over Secure Sockets Layer (HTTPS) encrypts and decrypts page requests to the Web server and pages returned by the Web server to the user.

RADIUS.

Security Access	Description
Available methods: • Centralized authentication of access rights • A server secret shared between the RADIUS server and the Rack PDU or device	RADIUS (Remote Authentication Dial-In User Service) is an authentication, authorization, and accounting service used to centrally administer remote access for each Rack PDU. (The Rack PDU supports the authentication and authorization functions.)

Access priorities

The priority for access, beginning with the highest priority, is as follows:

- Local access to the command line interface from a computer with a direct serial connection to the Rack PDU
- Telnet or Secure SHell (SSH) access to the command line interface from a remote computer
- Web access

Change default user names and passwords immediately

After installation and initial configuration of the Rack PDU, immediately change the user names and passwords from their defaults to unique user names and passwords to establish basic security.

Port assignments

If Telnet, the FTP server, SSH/SCP, or the Web server uses a non-standard port, a user must specify the port in the command line or Web address used to access the Rack PDU. A non-standard port number provides an additional level of security. The ports are initially set at the standard “well known ports” for the protocols. To increase security, reset the ports to any unused port numbers from 5001 to 32768 for the FTP server and from 5000 to 32768 for the other protocols and servers. (The FTP server uses both the specified port and the port one number lower than the specified port.)

User names, passwords, and community names with SNMPv1

All user names, passwords, and community names for SNMPv1 are transferred over the network as plain text. A user who is capable of monitoring the network traffic can determine the user names and passwords required to log on to the accounts of the command line interface or Web interface of the Rack PDU. If your network requires the higher security of the encryption-based options available for the command line interface and Web interface, disable SNMPv1 access or set its access to **Read**. (**Read** access allows you to receive status information and use SNMPv1 traps.)

To disable SNMPv1 access, on the **Administration** tab, select **Network** on the top menu bar and **access** under the **SNMPv1** heading on the left navigation menu. Clear the **Enable SNMPv1 access** checkbox and click **Apply**.

To set SNMPv1 access to **Read**, on the **Administration** tab, select **Network** on the top menu bar and **access control** under the **SNMPv1** heading on the left navigation menu. Then, for each configured Network Management System (NMS), click the community names and set the access type to **Read**.

Authentication

You can choose security features for the Rack PDU that control access by providing basic authentication through user names, passwords, and IP addresses, without using encryption. These basic security features are sufficient for most environments in which sensitive data are not being transferred.

SNMP GETS, SETS, and Traps

For enhanced authentication when you use SNMP to monitor or configure the Rack PDU, choose SNMPv3. The authentication passphrase used with SNMPv3 user profiles ensures that a Network Management System (NMS) attempting to communicate with the Rack PDU is the NMS it claims to be, that the message has not been changed during transmission, and that the message was not delayed, copied, and sent again later at an inappropriate time. SNMPv3 is disabled by default.

The Dell implementation of SNMPv3 allows the use of the SHA-1 or MD5 protocol for authentication.

Web interface and command line interface

To ensure that data and communication between the Rack PDU and the client interfaces (the command line interface and the Web interface) cannot be intercepted, you can provide a greater level of security by using one or more of the following encryption-based methods:

- For the Web interface, use the Secure Sockets Layer (SSL) protocol
- To encrypt user names and passwords for command line interface access, use the Secure SHell (SSH) protocol
- To encrypt user names, passwords, and data for the secure transfer of files, use the Secure CoPy (SCP) protocol

For more information on encryption-based security, see Encryption.

Encryption

SNMP GETS, SETS, and Traps

For encrypted communication when you use SNMP to monitor or configure the Rack PDU, choose SNMPv3. The privacy passphrase used with SNMPv3 user profiles ensures the privacy of the data (by means of encryption, using the AES or DES encryption algorithm) that an NMS sends to or receives from the Rack PDU.

Secure SHell (SSH) and Secure CoPy (SCP) for the command line interface

The Secure SHell protocol. SSH provides a secure mechanism to access computer consoles, or *shells,* remotely. The protocol authenticates the server (in this case, the Rack PDU) and encrypts all transmissions between the SSH client and the server.

- SSH is a high-security alternative to Telnet. Telnet does not provide encryption.
- SSH protects the user name and password, which are the credentials for authentication, from being used by anyone intercepting network traffic.
- To authenticate the SSH server (the Rack PDU) to the SSH client, SSH uses a host key unique to the SSH server. The host key is an identification that cannot be falsified, and it prevents an invalid server on the network from obtaining a user name and password by presenting itself as a valid server.

For information on supported SSH client applications, see Telnet and Secure SHell (SSH). To create a host key, see Create an SSH Host Key.

- The Rack PDU supports SSH version 2, which provides protection from attempts to intercept, forge, or change data during transmission.
- When you enable SSH, Telnet is automatically disabled.
- The interface, user accounts, and user access rights are the same whether you access the command line interface through SSH or Telnet.

Secure CoPy. SCP is a secure file transfer application that you can use instead of FTP. SCP uses the SSH protocol as the underlying transport protocol for encryption of user names, passwords, and files.

- When you enable and configure SSH, you automatically enable and configure SCP. No further configuration of SCP is needed.
- You must explicitly disable FTP. It is not disabled by enabling SSH. To disable FTP, on the **Administration** tab, select **Network** on the top menu bar and **FTP Server** on the left navigation menu. Clear the **Enable** checkbox and click **Apply**.

Secure Sockets Layer (SSL) for the Web interface

For secure Web communication, enable Secure Sockets Layer (SSL) by selecting HTTPS as the protocol mode to use for access to the Web interface of the Rack PDU. HyperText Transfer Protocol over Secure Sockets Layer (HTTPS) is a Web protocol that encrypts and decrypts page requests from the user and pages that are returned by the Web server to the user.

The Rack PDU supports SSL version 3.0 and the associated Transport Layer Security (TLS) version 1.0. Most browsers let you select the version of SSL to enable.

When SSL is enabled, your browser displays a small lock icon. 🔒

SSL uses a digital certificate to enable the browser to authenticate the server (in this case, the Rack PDU). The browser verifies the following:

- The format of the server certificate is correct
- The expiration date and time of the server certificate have not passed
- The DNS name or IP address specified when a user logs on matches the common name in the server certificate
- The server certificate is signed by a trusted certifying authority

Each major browser manufacturer distributes CA root certificates of the commercial Certificate Authorities in the certificate store (cache) of its browser so that it can compare the signature on the server certificate to the signature on a CA root certificate.

You can use the Rack PDU Security Wizard to create a certificate signing request to an external Certificate Authority, or if you do not want to use an existing Certificate Authority, you can create a Dell root certificate to upload to the certificate store (cache) of the browser. You can also use the Wizard to create a server certificate to upload to the Rack PDU.

See Creating and Installing Digital Certificates for a summary of how these certificates are used.
To create certificates and certificate requests, see Create a Root Certificate and Server Certificates and Create a Server Certificate and Signing Request.

SSL also uses various algorithms and encryption ciphers to authenticate the server, encrypt data, and ensure the integrity of the data, i.e., that it has not been intercepted and sent by another server.

Web pages that you have recently accessed are saved in the cache of your Web browser and allow you to return to those pages without re-entering your user name and password. Always close your browser session before you leave your computer unattended.

Creating and Installing Digital Certificates

Purpose

For network communication that requires a higher level of security than password encryption, the Web interface of the Rack PDU supports the use of digital certificates with the Secure Sockets Layer (SSL) protocol. Digital certificates can authenticate the Rack PDU (the server) to the Web browser (the SSL client).

! You can generate a 1024-bit key, or you can generate a 2048-bit key, which provides complex encryption and a higher level of security.

The sections that follow summarize the three methods of creating, implementing, and using digital certificates to help you determine the most appropriate method for your system.

- Method 1: Use the default certificate auto-generated by the Rack PDU.
- Method 2: Use the Rack PDU Security Wizard to create a CA certificate and a server certificate.
- Method 3: Use the Rack PDU Security Wizard to create a certificate-signing request to be signed by the root certificate of an external Certificate Authority and to create a server certificate.

! You can also use Method 3 if your company or agency operates its own Certificate Authority. Use the Rack PDU Security Wizard in the same way, but use your own Certificate Authority in place of a commercial Certificate Authority.

Choosing a method for your system

Using the Secure Sockets Layer (SSL) protocol, you can choose any of the following methods for using digital certificates.

Method 1: Use the default certificate auto-generated by the Rack PDU. When you enable SSL, you must reboot the Rack PDU. During rebooting, if no server certificate exists, the Rack PDU generates a default server certificate that is self-signed but that you cannot configure.

Method 1 has the following advantages and disadvantages.

- **Advantages:**
  - Before they are transmitted, the user name and password and all data to and from the Rack PDU are encrypted.
  - You can use this default server certificate to provide encryption-based security while you are setting up either of the other two digital certificate options, or you can continue to use it for the benefits of encryption that SSL provides.
- **Disadvantages:**
  - The Rack PDU takes up to 1 minute to create this certificate, and the Web interface is not available during that time. (This delay occurs the first time you log on after you enable SSL.)
  - This method does not include the authentication provided by a CA certificate (a certificate signed by a Certificate Authority) that Methods 2 and 3 provide. There is no CA Certificate cached in the browser. Therefore, when you log on to the Rack PDU, the browser generates a security alert, indicating that a certificate signed by a trusted authority is not available, and asks if you want to proceed. To avoid this message, you must install the default server certificate into the certificate store (cache) of the browser of each user who needs access to the Rack PDU, and each user must always use the fully qualified domain name of the server when logging on to the Rack PDU.
  - The default server certificate has the serial number of the Rack PDU in place of a valid *common name* (the DNS name or the IP address of the Rack PDU). Therefore, although the Rack PDU can control access to its Web interface by user name, password, and account type (e.g., **Administrator**, **Device-Only User**, or **Read-Only User**), the browser cannot authenticate which Rack PDU is sending or receiving data.

  - The length of the *public key* (RSA key) that is used for encryption when setting up an SSL session is 2048 bits, by default.

Method 2: Use the Rack PDU Security Wizard to create a CA certificate and a server certificate. Use the Rack PDU Security Wizard to create two digital certificates:

- A *CA root certificate* (Certificate Authority root certificate) that the Rack PDU Security Wizard uses to sign all server certificates and which you then install into the certificate store (cache) of the browser of each user who needs access to the Rack PDU.
- A *server certificate* that you upload to the Rack PDU. When the Rack PDU Security Wizard creates a server certificate, it uses the CA root certificate to sign the server certificate.

The Web browser authenticates the Rack PDU sending or requesting data:

- To identify the Rack PDU, the browser uses the *common name* (IP address or DNS name of the Rack PDU) that was specified in the server certificate's *distinguished name* when the certificate was created.
- To confirm that the server certificate is signed by a "trusted" signing authority, the browser compares the signature of the server certificate with the signature in the root certificate cached in the browser. An expiration date confirms whether the server certificate is current.

Method 2 has the following advantages and disadvantages.

- **Advantages:**
  - Before they are transmitted, the user name and password and all data to and from the Rack PDU are encrypted.
  - You choose the length of the *public key* (RSA key) that is used for encryption when setting up an SSL session (use 1024 bits, which is the default setting, or use 2048 bits to provide complex encryption and a high level of security).
  - The server certificate that you upload to the Rack PDU enables SSL to authenticate that data are being received from and sent to the correct Rack PDU.

This provides an extra level of security beyond the encryption of the user name, password, and transmitted data.

  - The root certificate that you install to the browser enables the browser to authenticate the server certificate of the Rack PDU to provide additional protection from unauthorized access.

- **Disadvantage:**
  Because the certificates do not have the digital signature of a commercial Certificate Authority, you must load a root certificate individually into the certificate store (cache) of each user's browser. (Browser manufacturers already provide root certificates for commercial Certificate Authorities in the certificate store within the browser, as described in Method 3.)

Method 3: Use the Rack PDU Security Wizard to create a certificate-signing request to be signed by the root certificate of an external Certificate Authority and to create a server certificate. Use the Rack PDU Security Wizard to create a request (a **.csr** file) to send to a Certificate Authority. The Certificate Authority returns a signed certificate (a **.crt** file) based on information you submitted in your request. You then use the Rack PDU Security Wizard to create a server certificate (a **.p15** file) that includes the signature from the root certificate returned by the Certificate Authority. Upload the server certificate to the Rack PDU.

You can also use Method 3 if your company or agency operates its own Certificate Authority. Use the Rack PDU Security Wizard in the same way, but use your own Certificate Authority in place of a commercial Certificate Authority.

Method 3 has the following advantages and disadvantages.

- **Advantages:**
  - Before they are transmitted, the user name and password and all data to and from the Rack PDU are encrypted.
  - You have the benefit of authentication by a Certificate Authority that already has a signed root certificate in the certificate cache of the browser. (The CA certificates of commercial Certificate Authorities are distributed as part of the browser software,

and a Certificate Authority of your own company or agency has probably already loaded its CA certificate to the browser store of each user's browser.) Therefore, you do not have to upload a root certificate to the browser of each user who needs access to the Rack PDU.

- You choose the length of the *public key* (RSA key) that is used for setting up an SSL session (use 1024 bits, which is the default setting, or use 2048 bits to provide complex encryption and a high level of security).
- The server certificate that you upload to the Rack PDU enables SSL to authenticate that data are being received from and sent to the correct Rack PDU. This provides an extra level of security beyond the encryption of the user name, password, and transmitted data.
- The browser matches the digital signature on the server certificate that you uploaded to the Rack PDU with the signature on the CA root certificate that is already in the browser's certificate cache to provide additional protection from unauthorized access.

- **Disadvantages:**
  - Setup requires the extra step of requesting a signed root certificate from a Certificate Authority.
  - An external Certificate Authority may charge a fee for providing signed certificates.

Firewalls

Although some methods of authentication provide a higher level of security than others, complete protection from security breaches is almost impossible to achieve. Well-configured firewalls are an essential element in an overall security scheme.

Using the Rack PDU Security Wizard

The Rack PDU Security Wizard creates components needed for high security for a Rack PDU on the network when you are using Secure Sockets Layer (SSL) and related protocols and encryption routines.

Authentication by certificates and host keys

Authentication verifies the identity of a user or a network device (such as a Rack PDU). Passwords typically identify computer users. However, for transactions or communications requiring more stringent security methods on the Internet, the Rack PDU supports more secure methods of authentication.

- Secure Sockets Layer (SSL), used for secure Web access, uses digital certificates for authentication. A digital *CA root* certificate is issued by a Certificate Authority (CA) as part of a public key infrastructure, and its digital signature must match the digital signature on a server certificate on the Rack PDU.
- Secure SHell (SSH), used for remote terminal access to the command line interface of the Rack PDU, uses a public *host key* for authentication.

How certificates are used. Most Web browsers, including all browsers supported by Rack PDUs, contain a set of CA root certificates from all of the commercial Certificate Authorities.

Authentication of the server (in this case, the Rack PDU) occurs each time a connection is made from the browser to the server. The browser checks to be sure that the server's certificate is signed by a Certificate Authority known to the browser.

For authentication to occur:

- Each server (Rack PDU) with SSL enabled must have a server certificate on the server itself.
- Any browser that is used to access the Web interface of the Rack PDU must contain the CA root certificate that signed the server certificate.

If authentication fails, a browser message asks you whether to continue even though it cannot authenticate the server.

If your network does not require the authentication provided by digital certificates, you can use the default certificate that the Rack PDU generates automatically. The default certificate's digital signature will not be recognized by browsers, but a default certificate enables you to use SSL for the encryption of transmitted user names, passwords, and data. (If you use the default certificate, the browser prompts you to agree to unauthenticated access before it logs you on to the Web interface of the Rack PDU.)

How SSH host keys are used. An SSH *host key* authenticates the identity of the server (the Rack PDU) each time an SSH client contacts that server. Each server with SSH enabled must have an SSH host key on the server itself.

Files you create for SSL and SSH security

Use the Rack PDU Security Wizard to create these components of an SSL and SSH security system:

- The server certificate for the Rack PDU, if you want the benefits of authentication that such a certificate provides. You can create either of the following types of server certificate:
  - A server certificate signed by a custom CA root certificate also created with the Rack PDU Security Wizard. Use this method if your company or agency does not have its own Certificate Authority and you do not want to use an external Certificate Authority to sign the server certificate.
  - A server certificate signed by an external Certificate Authority. This Certificate Authority can be one that is managed by your own company or agency or can be one of the commercial Certificate Authorities whose CA root certificates are distributed as part of a browser's software.
- A certificate signing request containing all the information required for a server certificate except the digital signature. You need this request if you are using an external Certificate Authority.
- A CA root certificate.
- An SSH host key that your SSH client program uses to authenticate the Rack PDU when you log on to the command line interface.

You define whether the public keys for SSL certificates and the host keys for SSH that are created with the Rack PDU Security Wizard are 1024-bit RSA keys (the default setting), or 2048-bit RSA keys, which provide complex encryption and a higher level of security.

If you do not create and use SSL server certificates and SSH host keys with the Rack PDU Security Wizard, the Rack PDU generates 2048-bit RSA keys.

Only Dell Rack PDU products can use server certificates, host keys, and CA root certificates created by the Rack PDU Security Wizard. These files will not work with products such as OpenSSL® and Microsoft® Internet Information Services (IIS).

Create a Root Certificate and Server Certificates

Summary

Use this procedure if your company or agency does not have its own Certificate Authority and you do not want to use a commercial Certificate Authority to sign your server certificates.

❗ Define the size of the public RSA key that is part of the certificate generated by the Rack PDU Security Wizard.You can generate a 1024-bit key, or you can generate a 2048-bit key, which provides complex encryption and a higher level of security. (The default key generated by the Rack PDU, if you do not use the Wizard, is 2048 bits.)

- Create a CA root certificate that will sign all server certificates to be used with Rack PDU. During this task, two files are created:
  - The file with the **.p15** suffix is an encrypted file that contains the Certificate Authority's private key and public root certificate. This file signs server certificates.
  - The file with the **.crt** suffix contains only the Certificate Authority's public root certificate. Load this file into each Web browser that will be used to access the Rack PDU so that the browser can validate the server certificate of that Rack PDU.
- Create a server certificate, which is stored in a file with a **.p15** suffix. During this task, you are prompted for the CA root certificate that signs the server certificate.
- Load the server certificate onto the Rack PDU.
- For each Rack PDU that requires a server certificate, repeat the tasks that create and load the server certificate.

The procedure

Create the CA root certificate.

1. If the Rack PDU Security Wizard is not already installed on your computer, obtain and run the installation program (**Rack PDU Security Wizard.exe)**.
2. On the Windows **Start** menu, select **Programs**, then **Rack PDU Security Wizard**.
3. On the screen labeled **Step 1**, select **CA Root Certificate** as the type of file to create, and then select the length of the key to generate (use 1024 bits, which is the default setting, or use 2048 bits to provide complex encryption and a high level of security).
4. Enter a name for this file, which will contain the Certificate Authority's public root certificate and private key. The file must have a **.p15** suffix and, by default, will be created in the installation folder **C:\Program Files\Dell\Rack PDU Security Wizard**.
5. On the screen labeled **Step 2**, provide the information to configure the CA root certificate. The **Country** and **Common Name** fields are the only required fields. For the **Common Name** field, enter an identifying name of your company or agency. Use only alphanumeric characters, with no spaces.

   ❗ By default, a CA root certificate is valid for 10 years from the current date and time, but you can edit the **Validity Period Start** and **Validity Period End** fields.

6. On the next screen, review the summary of the certificate. Scroll downward to view the certificate's unique serial number and fingerprints. To make any changes to the information you provided, click **Back**. Revise the information.

   ❗ The certificate's subject information and the certificate's issuer information should be identical.

7. The last screen verifies that the certificate was created and displays information you need for the next tasks:
   - The location and name of the **.p15** file that you will use to sign the server certificates.
   - The location and name of the **.crt** file, which is the CA root certificate to load into the browser of each user who needs to access the Rack PDU.

Load the CA root certificate to your browser. Load the **.crt** file to the browser of each user who needs to access the Rack PDU.

See the help system of the browser for information on how to load the **.crt** file into the browser's certificate store (cache). Following is a summary of the procedure for Microsoft Internet Explorer.

1. Select **Tools**, then **Internet Options** from the menu bar.
2. In the dialog box, on the **Content** tab click **Certificates** and then **Import**.
3. The Certificate Import Wizard guides you through the rest of the procedure. The file type to select is X.509, and the CA Public Root Certificate is the **.crt** file created in the procedure Create a Root Certificate and Server Certificates.

Create an SSL Server User Certificate.

1. On the Windows **Start** menu, select **Programs**, then **Rack PDU Security Wizard**.
2. On the screen labeled **Step 1**, select **SSL Server Certificate** as the type of file, and then select the length of the key to generate (use 1024 bits, which is the default setting, or use 2048 bits to provide complex encryption and a high level of security).
3. Enter a name for this file, which will contain the server certificate and the private key. The file must have a **.p15** suffix and, by default, will be created in the folder **C:\Program Files\Dell\Rack PDU Security Wizard**.
4. Click **Browse**, and select the CA root certificate created in the procedure Create a Root Certificate and Server Certificates. The CA Root Certificate is used to sign the Server User Certificate being generated.

5. On the screen labeled **Step 2**, provide the information to configure the server certificate. **Country** and **Common Name** are the only required fields. For the **Common Name** field, enter the IP address or DNS name of the server (the Rack PDU). By default, a server certificate is valid for 10 years but you can edit the **Validity Period Start** and **Validity Period End** fields.

   ❗ Because the configuration information is part of the signature, the information for every certificate must be unique. The configuration of a server certificate cannot be the same as the configuration of the CA root certificate. (The expiration date is not considered part of the unique configuration. Some other configuration information must also differ.)

6. On the next screen, review the summary of the certificate. Scroll downward to view the certificate's unique serial number and fingerprints. To make any changes to the information you provided, click **Back**. Revise the information.
7. The last screen verifies that the certificate has been created and instructs you to load the server certificate to the Rack PDU. It displays the location and name of the Server Certificate, which has a **.p15** file suffix and contains the private key and public root certificate of the Rack PDU.

Load the server certificate to the Rack PDU.

1. On the **Administration** tab, select **Network** on the top menu bar and **ssl certificate** under the **Web** heading on the left navigation menu.
2. Select **Add or Replace Certificate File**, and browse to the server certificate, the **.p15** file you created in the procedure Create a Root Certificate and Server Certificates. (The default location is **C:\Program Files\Dell\Rack PDU Security Wizard**.)

❗ You can use FTP or Secure CoPy (SCP) instead to transfer the server certificate. For SCP, the command to transfer a certificate named **cert.p15** to a Rack PDU with an IP address of 156.205.6.185 would be:

```
scp cert.p15 dell@156.205.6.185
```

Create a Server Certificate and Signing Request

Summary

Use this procedure if your company or agency has its own Certificate Authority or if you plan to use a commercial Certificate Authority to sign your server certificates.

- Create a Certificate Signing Request (CSR). The CSR contains all the information for a server certificate except the digital signature. This process creates two output files:
  - The file with the **.p15** suffix contains the private key of the Rack PDU.
  - The file with the **.csr** suffix contains the certificate signing request, which you send to an external Certificate Authority.
- When you receive the signed certificate from the Certificate Authority, import that certificate. Importing the certificate combines the **.p15** file containing the private key and the file containing the signed certificate from the external Certificate Authority. The output file is a new encrypted server certificate file with a **.p15** suffix.
- Load the server certificate onto the Rack PDU.
- For each Rack PDU that requires a server certificate, repeat the tasks that create and load the server certificate.

The procedure

Create the Certificate Signing Request (CSR).

1. If the Rack PDU Security Wizard is not already installed on your computer, obtain and run the installation program (**Rack PDU Security Wizard.exe)**.
2. On the Windows **Start** menu, select **Programs**, then **Rack PDU Security Wizard**.
3. On the screen labeled **Step 1**, select **Certificate Request** as the type of file to create, and then select the length of the key to generate (use 1024 bits, which is the default setting, or use 2048 bits to provide complex encryption and a high level of security).

4. Enter a name for this file, which will contain the private key of the Rack PDU. The file must have a **.p15** suffix and, by default, will be created in the installation folder **C:\Program Files\Dell\Rack PDU Security Wizard**.
5. On the screen labeled **Step 2**, provide the information to configure the certificate signing request (CSR), i.e., the information that you want the signed server certificate to contain. The **Country** and **Common Name** fields are required. Other fields are optional. For the **Common Name** field, enter the IP Address or DNS name of the Rack PDU.

   By default, a server certificate is valid for 10 years from the current date and time, but you can edit the **Validity Period Start** and **Validity Period End** fields.

6. On the next screen, review the summary of the certificate. Scroll downward to view the unique serial number and fingerprints of the certificate. To make any changes to the information you provided, click **Back**. Revise the information.

   The certificate's subject information and the certificate's issuer information should be identical.

7. The last screen verifies that the certificate signing request was created and displays the location and name of the file, which has a **.csr** extension.
8. Send the certificate signing request to an external Certificate Authority, either a commercial Certificate Authority or, if applicable, a Certificate Authority managed by your own company or agency.

   See the instructions provided by the Certificate Authority regarding the signing and issuing of server certificates.

Import the signed certificate. When the external Certificate Authority returns the signed certificate, import the certificate. This procedure combines the signed certificate and the private key into an SSL server certificate that you then upload to the Rack PDU.

1. On the Windows **Start** menu, select **Programs**, then **Rack PDU Security Wizard**.
2. On the screen labeled **Step 1**, select **Import Signed Certificate**.
3. Browse to and select the signed server certificate that you received from the external Certificate Authority. The file has a **.cer** or **.crt** suffix.
4. Browse to and select the file you created in step 4 of the task Create the Certificate Signing Request (CSR). This file has a **.p15** extension, contains the private key of the Rack PDU, and, by default, is in the installation folder **C:\Program Files\Dell\Rack PDU Security Wizard**.
5. Specify a name for the output file that will be the signed server certificate that you upload to the Rack PDU. The file must have a **.p15** suffix.
6. Click **Next** to generate the server certificate. **Issuer Information** on the summary screen confirms that the external Certificate Authority signed the certificate.
7. The last screen verifies that the certificate has been created and instructs you to load the server certificate to the Rack PDU. It displays the location and name of the server certificate, which has a **.p15** file extension and contains the private key of the Rack PDU and the public key obtained from the **.cer** or **.crt** file.

Load the server certificate to the Rack PDU.

1. On the **Administration** tab, select **Network** on the top menu bar and **ssl certificate** under the **Web** heading on the left navigation menu.
2. Select **Add or Replace Certificate File**, and browse to the server certificate, the **.p15** file you created in the procedure Create a Root Certificate and Server Certificates. (The default location is **C:\Program Files\Dell\Rack PDU Security Wizard**.)

Alternatively, you can use FTP or Secure CoPy (SCP) to transfer the server certificate to the Rack PDU. For SCP, the command to transfer a certificate named **cert.p15** to a Rack PDU with an IP address of 156.205.6.185 would be:

```
scp cert.p15 dell@156.205.6.185
```

Create an SSH Host Key

Summary

This procedure is optional. If you select SSH encryption, but do not create a host key, the Rack PDU generates a 2048-bit RSA key when it reboots. You define whether the host keys for SSH that are created with the Rack PDU Security Wizard are 1024-bit or 2048-bit RSA keys.

You can generate a 1024-bit key, or you can generate a 2048-bit key, which provides complex encryption and a higher level of security.

- Use the Rack PDU Security Wizard to create a host key, which is encrypted and stored in a file with the **.p15** suffix.
- Load the host key onto the Rack PDU.

The procedure

Create the host key.

1. If the Rack PDU Security Wizard is not already installed on your computer, obtain and run the installation program (**Rack PDU Security Wizard.exe)**.
2. On the Windows **Start** menu, select **Programs**, then **Rack PDU Security Wizard**.
3. On the **Step 1** screen, select **SSH Server Host Key** as the type of file to create, and then select the length of the key to generate (use 1024 bits, which is the default setting, or use 2048 bits to provide complex encryption and a high level of security).
4. Enter a name for this file, which will contain the host key. The file must have a **.p15** suffix. By default, the file will be created in the installation folder **C:\Program Files\Dell\Rack PDU Security Wizard**.
5. Click **Next** to generate the host key.
6. The summary screen displays the SSH version 2 fingerprints, which are unique for each host key and identify the host key. After you load the host key onto the Rack PDU, you can verify that the correct host key was uploaded by verifying that the fingerprints displayed here match the SSH fingerprints on the Rack PDU, as displayed by your SSH client program.
7. The last screen verifies that the host key was created, instructs you to load the host key to the Rack PDU, and displays the location and name of the host key, which has a **.p15** file suffix.

Load the host key to the Rack PDU.

1. On the **Administration** tab, select **Network** on the top menu bar, and **ssh host key** under the **Console** heading on the left navigation menu.
2. Select **Add or Replace Host Key**, and browse to the host key, the **.p15** file you created in the procedure Create the host key. (The default location is **C:\Program Files\Dell\Rack PDU Security Wizard**.)
3. At the bottom of the **User Host Key** page, note the SSH fingerprint. Log on to the Rack PDU through your SSH client program, and verify that the correct host key was uploaded by verifying that these fingerprints match the fingerprints that the client program displays.

❗ Alternatively, you can use FTP or Secure CoPy (SCP) to transfer the host key file to the Rack PDU. For SCP, the following command would transfer a host key named **hostkey.p15** to a Rack PDU with an IP address of 156.205.6.185:

```
scp hostkey.p15 dell@156.205.6.185
```

Command Line Interface Access and Security

Users with Administrator or Device User accounts can access the command line interface through Telnet or Secure SHell (SSH), depending on which is enabled. (An Administrator can enable these access methods by selecting the **Administration** tab, then **Network** on the top menu bar and **access** under the **Console** heading on the left navigation menu.) By default, Telnet is enabled. Enabling SSH automatically disables Telnet.

Telnet for basic access. Telnet provides the basic security of authentication by user name and password, but not the high-security benefits of encryption.

SSH for high-security access. If you use the high security of SSL for the Web interface, use Secure SHell (SSH) for access to the command line interface. SSH encrypts user names, passwords and transmitted data.

The interface, user accounts, and user access rights are the same whether you access the command line interface through SSH or Telnet, but to use SSH, you must first configure SSH and have an SSH client program installed on your computer.

Telnet and Secure SHell (SSH)

While SSH is enabled, you cannot use Telnet to access the command line interface. Enabling SSH enables SCP automatically.

When SSH is enabled and its port is configured, no further configuration is required to use Secure CoPy (SCP). SCP uses the same configuration as SSH.

To use SSH, you must have an SSH client installed. Most Linux and other UNIX® platforms include an SSH client, but Microsoft Windows operating systems do not. SSH clients are available from various vendors.

To configure the options for Telnet and Secure SHell (SSH):

1. On the **Administration** tab of the Web interface, select **Network** on the top

menu bar, and select **access** under the **Console** heading on the left navigation menu.

2. Configure the port settings for Telnet and SSH.

   For information on the extra security a non-standard port provides, see Port assignments.

3. Under **Console** on the left navigation menu, select **ssh host key**, specify a host key file previously created with the Rack PDU Security Wizard, and load it to the Rack PDU.

   If you do not specify a host key file here, if you install an invalid host key, or if you enable SSH with no host key installed, the Rack PDU generates an RSA host key of 2048 bits. For the Rack PDU to create a host key, it must reboot. **The Rack PDU can take up to 1 minute to create this host key, and SSH is not accessible during that time.**

   Alternatively, from a command line interface such as the command prompt on Windows operating systems, you can use FTP or Secure CoPy (SCP) to transfer the host key file.

4. Display the *fingerprint* of the SSH host key for SSH version 2. Most SSH clients display the fingerprint at the start of a session. Compare the fingerprint displayed by the client to the fingerprint that you recorded from the Web interface or command line interface of the Rack PDU.

Web Interface Access and Security: HTTP and HTTPS (with SSL)

HyperText Transfer Protocol (HTTP) provides access by user name and password, but does not encrypt user names, passwords, and data during transmission. HyperText Transfer Protocol over Secure Sockets Layer (HTTPS) encrypts user names, passwords, and data during transmission, and provides authentication of the Rack PDU by means of digital certificates.

See Creating and Installing Digital Certificates to choose among the several methods for using digital certificates.

To configure HTTP and HTTPS:

1. On the **Administration** tab, select **Network** on the top menu bar and **access** under **Web** on the left navigation menu.
2. Enable either HTTP or HTTPS and configure the ports that each of the two protocols will use. Changes take effect the next time you log on. When SSL is activated, your browser displays a small lock icon.

   For information on the extra security a non-standard port provides, see Port assignments.

3. Select **ssl certificate** under **Web** on the left navigation menu to determine whether a server certificate is installed on the Rack PDU. If a certificate was created with the Rack PDU Security Wizard but is not installed:
   - In the Web interface, browse to the certificate file and upload it to the Rack PDU.
   - Alternatively, use the Secure CoPy (SCP) protocol or FTP to upload the certificate file to the Rack PDU.

   Creating and uploading a server certificate in advance reduces the time required to enable HTTPS. If you enable HTTPS with no server certificate loaded, the Rack PDU creates one when it reboots. **The Rack PDU can take up to 1 minute to create the certificate, and the SSL server is unavailable during that time.**

   A certificate that the Rack PDU generates has some limitations. See Method 1: Use the default certificate auto-generated by the Rack PDU.

4. If a valid digital server certificate is loaded, the **Status** field displays the link.

Valid Certificate. Click the link to display the parameters of the certificate.

Parameter	Description
Issued To:	**Common Name (CN)**: The IP Address or DNS name of the Rack PDU. This field controls how you must log on to the Web interface. • If an IP address was specified for this field when the certificate was created, use an IP address to log on. • If the DNS name was specified for this field when the certificate was created, use the DNS name to log on. If you do not use the IP address or DNS name that was specified for the certificate, authentication fails, and you receive an error message asking if you want to continue. For a server certificate generated by default by the Rack PDU, this field displays the serial number of the Rack PDU instead. **Organization (O)**, **Organizational Unit (OU**), and **Locality, Country:** The name, organizational unit, and location of the organization using the server certificate. For a server certificate generated by default by the Rack PDU, the **Organizational Unit (OU)** field displays “Internally Generated Certificate.” **Serial Number**: The serial number of the server certificate.
Issued By:	**Common Name (CN)**: The Common Name as specified in the CA root certificate. For a server certificate generated by default by the Rack PDU, this field displays the serial number of the Rack PDU instead. **Organization (O)** and **Organizational Unit (OU**): The name and organizational unit of the organization that issued the server certificate. If the server certificate was generated by default by the Rack PDU or device, this field displays “Internally Generated Certificate.”
Validity:	**Issued on**: The date and time at which the certificate was issued. **Expires on**: The date and time at which the certificate expires.

Parameter	Description
Fingerprints	Each of the two fingerprints is a long string of alphanumeric characters, punctuated by colons. A fingerprint is a unique identifier to further authenticate the server. Record the fingerprints to compare them with the fingerprints contained in the certificate, as displayed in the browser. **SHA1 Fingerprint**: A fingerprint created by a Secure Hash Algorithm (SHA-1). **MD5 Fingerprint**: A fingerprint created by a Message Digest 5 (MD5) algorithm.

Supported RADIUS Functions and Servers

Supported functions

Supported authentication and authorization functions: Remote Authentication Dial-In User Service (RADIUS). Use RADIUS to administer remote access for each Rack PDU centrally. When a user accesses the Rack PDU, an authentication request is sent to the RADIUS server to determine the permission level of the user.

For more information on permission levels, see Types of user accounts.

Supported RADIUS servers

Supported RADIUS servers: FreeRADIUS and Microsoft IAS 2003. Other commonly available RADIUS applications may work but have not been fully tested.

Configure the Rack PDU

Authentication

RADIUS user names used with Rack PDU are limited to 32 characters.

On the **Administration** tab, select **Security** on the top menu bar. Then, under **Remote Users** on the left navigation menu, select **authentication** to define an authentication method:

- **Local Authentication Only**: RADIUS is disabled. Local authentication is enabled.
- **RADIUS, then Local Authentication**: Both RADIUS and local authentication are enabled. Authentication is requested from the RADIUS server first; local authentication is used only if the RADIUS server fails to respond.
- **RADIUS Only**: RADIUS is enabled. Local authentication is disabled.

If **RADIUS Only** is selected, and the RADIUS server is unavailable, improperly identified, or improperly configured, remote access is unavailable to all users. You must use a serial connection to the command line interface and change the RADIUS access setting to `local` or `radiusLocal` to regain access. For example, the command to change the access setting to `local` would be:

```
radius -a local
```

RADIUS

To configure RADIUS, on the **Administration** tab, select **Security** on the top menu bar. Then, under **Remote Users** on the left navigation menu, select **RADIUS**.

Setting	Definition
RADIUS Server	The server name or IP address of the RADIUS server. **NOTE:** RADIUS servers use port 1812 by default to authenticate users. To use a different port, add a colon followed by the new port number to the end of the RADIUS server name or IP address.
Secret	The secret shared between the RADIUS server and the Rack PDU.
Reply Timeout	The time in seconds that the Rack PDU waits for a response from the RADIUS server.
Test Settings	Enter the Administrator user name and password to test the RADIUS server path that you have configured.
Skip Test and Apply	Do not test the RADIUS server path.

If two configured servers are listed and **RADIUS, then Local Authentication** or **RADIUS Only** is the enabled authentication method, you can change which RADIUS server will authenticate users by clicking the **Switch Server Priority** button.

Configure the RADIUS Server

You must configure your RADIUS server to work with the Rack PDU. The examples in this section may differ somewhat from the required content or format of your specific RADIUS server. In the examples, any reference to outlets applies only to Rack PDU devices that support outlet users.

1. Add the IP address of the Rack PDU to the RADIUS server client list (file).
2. Users must be configured with Service-Type attributes unless Vendor Specific Attributes (VSAs) are defined instead. If no Service-Type attribute is configured, the user has read-only access (to the Web interface only). The two acceptable values for Service-Type are Administrative-User (6), which gives the user Administrator permissions, and Login-User (1), which gives the user Device permissions.

   See your RADIUS server documentation for information about the RADIUS users file.

Example using Service-Type Attributes

In the following example of a RADIUS users file:

- **`RPDUAdmin`** corresponds to **`Service-Type: Administrative-User, (6)`**
- **`RPDUDevice`** corresponds to **`Service-Type: Login-User, (1)`**
- **`RPDUReadOnly`** corresponds to **`Service-Type: null`**

```
RPDUAdmin      Auth-Type = Local, Password = "admin"
   Service-Type = Administrative-User

RPDUDevice     Auth-Type = Local, Password = "device"
   Service-Type = Login-User

RPDUReadOnly   Auth-Type = Local, Password = "readonly"
```

Examples using Vendor Specific Attributes

Vendor Specific Attributes (VSAs) can be used instead of the Service-Type attributes provided by your RADIUS server. This method requires a dictionary entry and a RADIUS users file. In the dictionary file, you can define the names for the ATTRIBUTE and VALUE keywords, but not the numeric values. If you change the numeric values, RADIUS authentication and authorization will not work correctly. VSAs take precedence over standard RADIUS attributes.

Dictionary file. Following is an example of a RADIUS dictionary file (dictionary.dell):

```
#
# dictionary.dell
#
#
VENDOR   DELL 318
#
# Attributes
#
ATTRIBUTE DELL-Service-Type 1 integer DELL
ATTRIBUTE DELL-Outlets      2 string DELL

VALUE DELL-Service-Type Admin    1
VALUE DELL-Service-Type Device   2
VALUE DELL-Service-Type ReadOnly 3
#
# For devices with outlet users only
#
VALUE DELL-Service-Type Outlet   4
```

RADIUS Users file with VSAs. Following is an example of a RADIUS users file with VSAs:

```
VSAAdmin    Auth-Type = Local, Password = "admin"
            DELL-Service-Type = Admin

VSADevice   Auth-Type = Local, Password = "device"
            DELL-Service-Type = Device

VSAReadOnly Auth-Type = Local, Password = "readonly"
            DELL-Service-Type = ReadOnly

# Give user access to device outlets 1, 2 and 3.
VSAOutlet   Auth-Type = Local, Password = "outlet"
            DELL-Service-Type = Outlet,
            DELL-Outlets = "1,2,3"
```

See the following related topics:

- Types of user accounts for information on the three basic user permission levels (Administrator, Device User, and Read-Only User).
- Supported RADIUS servers for information on RADIUS servers tested and supported.

Example with UNIX shadow passwords. If UNIX shadow password files are used (**/etc/passwd**) with the RADIUS dictionary files, the following two methods can be used to authenticate users:

- If all UNIX users have administrative privileges, add the following to the RADIUS “user” file. To allow only Device Users, change the Dell-Service-Type to **`Device`**.

```
DEFAULT   Auth-Type = System
          DELL-Service-Type = Admin
```

- Add user names and attributes to the RADIUS "user" file, and verify the password against **/etc/passwd**. The following example is for users **`bconners`** and **`thawk`**:

```
bconners        Auth-Type = System
                DELL-Service-Type = Admin
thawk           Auth-Type = System
                DELL-Service-Type = Outlet
                DELL-Outlets = "1,2,3"
```

Index

USER'S GUIDE

Metered Rack PDU

03/2010 Part Number 990-3877-001

www.dell.com | support.dell.com