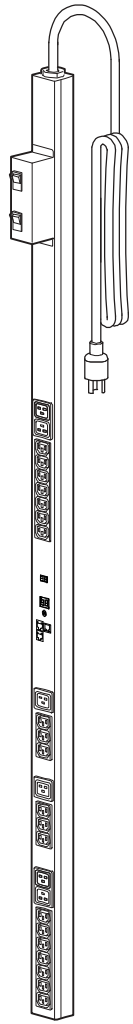
Руководство пользователя

Управляемое устройство Rack PDU



РУКОВОДСТВО
Управляемое устройство Rack PDU

Содержание

РУКОВОДСТВО Управляемое устройство Rack PDU

РУКОВОДСТВО Управляемое устройство Rack PDU

Введение

Характеристики продукта

Управляемое устройство распределения питания для монтажа в стойку (Rack Power Distribution Unit (PDU)) Dell® – это автономное управляемое по сети устройство распределения питания. Устройство Rack PDU передает отслеживаемые значения подключенных нагрузок. Сигналы тревоги, задаваемые пользователем, позволяют предотвратить перегрузку цепей. Устройство Rack PDU обеспечивает полный контроль над розетками посредством удаленных команд и настроек пользовательского интерфейса.

Управлять устройством Rack PDU можно с помощью веб-интерфейса, интерфейса командной строки (CLI), или простого протокола сетевого управления (SNMP):

- Доступ к веб-интерфейсу осуществляется по протоколу передачи гипертекста (Hypertext Transfer Protocol) или HTTP (HTTPS) на уровне защищенных сокетов (Secure Sockets Layer – SSL). См. раздел Вход в веб-интерфейс.
- Доступ к интерфейсу командной строки осуществляется с помощью последовательного подключения, Telnet или Secure Shell (SSH). См. раздел Об интерфейсе командной строки.
- Используйте браузер SNMP и справочник Dell Management Information Base (MIB) для управления вашим устройством Rack PDU.

Устройство Rack PDU имеет дополнительные характеристики:

- Контроль пиковых нагрузок, мощности и энергии для всех подключенных нагрузок.
- Контроль напряжения, электрического тока и мощности для фаз.
- Контроль мощности для каждой розетки.

- Конфигурируемые пороговые значения для подачи сетевых и визуальных аварийных сигналов помогают предотвратить перегрузку цепей.
- Четыре уровня учетных записей пользовательского доступа: Администратор, Пользователь устройства, Пользователь только для чтения, и Пользователь розетки питания.
- Индивидуальный контроль розеток.
- Настраиваемые задержки подачи питания.
- До двадцати четырех учетных записей пользователей для розеток.
- Протоколирование событий и данных. К журналу событий можно получить доступ с помощью Telnet, Secure CoPy (SCP), протокола передачи файлов (FTP), последовательного подключения или веб-браузера (используя доступ по HTTPS с SSL или доступ по HTTP). К журналу данных доступ осуществляется через веб-браузер, SCP или FTP.
- Уведомления по электронной почте о событиях устройства Rack PDU и системных событий.
- SNMP-ловушки, сообщения Syslog и уведомления по электронной почте основаны на степени опасности или категории событий устройства Rack PDU и событий системы.
- Протоколы системы защиты для аутентификации или шифрования.

Устройство Rack PDU не обеспечивает защиту цепи питания от перенапряжения. Для того, чтобы защитить устройство от сбоев питания или скачков напряжения, подключите устройство Rack PDU к источнику бесперебойного питания (UPS).

Приоритет доступа для входа

На устройство Rack PDU единовременно может зайти только один пользователь. Предусмотрен следующий приоритет доступа, начиная с максимального:

- Локальный доступ к интерфейсу командной строки с компьютера с помощью прямого подключения к Rack PDU через последовательный порт
- Доступ Telnet или Secure Shell (SSH) к интерфейсу командной строки с удаленного компьютера
- Доступ через интернет

См. SNMP с описанием того, как с помощью протокола SNMP осуществляется доступ к Rack PDU.

Типы учетных записей

Устройство Rack PDU имеет четыре уровня доступа (Администратор, Пользователь устройства, Пользователь только для чтения и Пользователь розетки), которые защищены именем пользователя и паролем.

- Пользователь с доступом «Администратор» может использовать все меню веб-интерфейса и все команды в интерфейсе командной строки. Имя пользователя и пароль по умолчанию задаются как **admin**.
- Пользователь с доступом «Пользователь» имеет доступ только к перечисленным ниже позициям.
  - В веб-интерфейсе: меню на вкладке **Device Manager** (Диспетчер устройств), вкладка **Environment** (Окружающая среда), а также журналы событий и данных, доступ к которым осуществляется через заголовки **Events** (События) и **Data** (Данные) на левой панели управления меню на вкладке **Logs** (Журналы). При отображении журналов событий и данных кнопка для стирания журнала не предусматривается.
  - В интерфейсе командной строки: к эквивалентным функциям и опциям.

  Имя пользователя и пароль по умолчанию задаются как **device**.
- Пользователь с доступом «Только для чтения» имеет перечисленные ниже ограниченные возможности доступа.
  - Доступ только через веб-интерфейс.
  - Доступ к тем же вкладкам и меню, что и при доступе «Пользователь устройства», но без возможности изменения конфигурации, устройств управления, удаления данных или использования опций передачи файлов. Связь с опциями конфигурации видна, но отключена. При отображении журналов событий и данных кнопка для стирания журнала не предусматривается.

  Имя пользователя и пароль по умолчанию задаются как **readonly**.

Чтобы установить значения **Имя пользователя** и **Пароль** для трех типов учетных записей, см. Настройка доступа пользователя.

- Пользователь розетки имеет перечисленные ниже ограниченные возможности доступа.
  - Доступ через веб-интерфейс и интерфейс командной строки.
  - Доступ к тем же меню, что и при доступе «Пользователь устройства», но с ограниченной возможностью изменения конфигурации, устройств управления, удаления данных или использования опций передачи файлов. Связь с опциями конфигурации видна, но отключена. У пользователя розетки есть доступ к параметру меню **Управление розетками**, который позволяет пользователю контролировать розетки, назначенные администратором. Пользователь розетки не может очистить журналы событий или данных.

  Имя пользователя и пароль определяются администратором при добавлении нового пользователя розетки.

Начало работы

Для начала работы с Rack PDU:

1. Установите Rack PDU, используя *Руководство по установке устройства распределения питания для монтажа в стойку (Rack Power Distribution Unit)*, прилагаемое к устройству.
2. Подключите к источнику питания и к сети. Процедуры установки см. в *Руководстве по установке устройства распределения питания для монтажа в стойку (Rack Power Distribution Unit)*.
3. Настройте сетевые параметры. (См. раздел Установка сетевых настроек.)
4. Начните использование устройства Rack PDU одним из следующих способов:
   - Веб-интерфейс
   - Интерфейс командной строки
   - Передняя панель устройства Rack PDU

Установка сетевых настроек

Для того чтобы устройство Rack PDU могло работать в сети, необходимо установить следующие параметры конфигурации TCP/IP:

- IP-адрес устройства Rack PDU
- Маска подсети
- Основной шлюз

Если основной шлюз недоступен, то используйте IP-адрес компьютера, расположенного в той же подсети, что и Rack PDU, и чаще всего включенного. Блок Rack PDU использует шлюз по умолчанию для проверки сети при очень слабой загрузке трафика.

Не используйте адрес замыкания на себя (127.0.0.1) в качестве адреса основного шлюза для устройства Rack PDU. При этом плата отключается, и вам придется выполнить сброс настроек TCP/IP в значения по умолчанию с помощью регистрации через локальный последовательный порт.

Методы настройки TCP/IP

Для настройки необходимых для Rack PDU параметров TCP/IP используйте один из следующих методов:

- Настройка BOOTP и DHCP
- Интерфейс командной строки

Настройка BOOTP и DHCP

Настройка по умолчанию конфигурации TCP/IP **DHCP**, предполагает наличие правильно сконфигурированного сервера DHCP, который предоставляет настройки TCP/IP для Rack PDU. Также можно сконфигурировать настройки BOOTP.

Пользовательский файл конфигурации (INI) может выполнять функции файла загрузки BOOTP или DHCP. Для получения дополнительных сведений см. Использование файла .ini.

BOOTP. Rack PDU будет использовать сервер BOOTP для конфигурации параметров TCP/IP, если обнаружит правильно настроенный сервер BOOTP, совместимый с RFC951.

В файле BOOTPTAB на сервере BOOTP введите MAC-адрес и IP-адрес, маску подсети и шлюз по умолчанию устройства Rack PDU. Можно также ввести имя файла загрузки. MAC-адрес указан на основании Rack PDU или на бланке контроля качества, имеющемся в упаковке.

При перезагрузке Rack PDU сервер BOOTP предоставляет устройству необходимые параметры TCP/IP.

- Если имя загрузочного файла указано, то Rack PDU постарается переслать этот файл с сервера BOOTP с помощью протоколов TFTP или FTP. Rack PDU считает, что все настройки указаны в файле bootup.
- Если не было указано имя файла загрузки, можно настроить другие параметры Rack PDU удаленно через Веб-интерфейс или Интерфейс командной строки.

Для создания загрузочного файла см. документацию по серверу BOOTP.

DHCP. Вы можете использовать сервер DHCP, соответствующий стандарту RFC2131/RFC2132, для установки параметров TCP/IP для устройства Rack PDU.

В этом разделе дается краткое описание процесса коммуникации Rack PDU с сервером DHCP. Для получения подробной информации о настройке параметров Rack PDU сервером DHCP, см. Параметры отклика DHCP.

1. Rack PDU отправляет запрос DHCP, в котором для идентификации устройства используются следующие данные:
   - Идентификатор класса поставщиков
   - Идентификатор клиента (по умолчанию указывается MAC-адрес Rack PDU).
   - Идентификатор класса пользователя (по умолчанию указывается микропрограмма, установленная на Rack PDU).
2. Правильно сконфигурированный сервер DHCP выдает ответ на запрос DHCP, который содержит все параметры, необходимые устройству Rack PDU для работы в сети. Предлагаемый набор параметров DHCP также включает параметр «Информация о поставщике» (DHCP, параметр 43). Устройство Rack PDU можно настроить так, чтобы оно игнорировало предлагаемые параметры DHCP, если в параметре 43 DHCP не указан файл cookie поставщика в следующем шестнадцатеричном формате. (Устройство Rack PDU не требует этого cookie-файла по умолчанию.)

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

   Где:
   - первый байт (`01`) – это код;
   - второй байт (`04`) – длина.
   - остальные байты (`31 41 50 43`) – файл cookie поставщика.

Сведения о том, как добавить код с информацией о конкретном поставщике, см. в документации по серверу DHCP.

Примечание: Установите флажок **Требовать определенный cookie от поставщика для принятия адреса DHCP** в веб-интерфейсе, чтобы DHCP-сервер предоставлял cookie-файл поставщика, передающий информацию на Rack PDU **Администрирование > Сеть >TCP/IP > настройки ipv4**.

Интерфейс командной строки

1. Войдите в интерфейс командной строки. См. раздел Вход в интерфейс командной строки.
2. Для получения IP-адреса, маски подсети и шлюза по умолчанию для Rack PDU обратитесь к администратору сети.
3. Для настройки сетевых параметров воспользуйтесь следующими тремя командами. (Переменные обозначены курсивом.)

   a. `tcpip -i` *`IP_адрес`*

   b. `tcpip -s` *`маска_подсети`*

   c. `tcpip -g` *`шлюз_по_умолчанию`*

   Для каждой переменной введите цифровое значение в формате *`xxx.xxx.xxx.xxx`*.

   Например, чтобы установить для системного IP-адреса значение 156.205.14.141, введите следующую команду и нажмите ENTER:
   `tcpip -i 156.205.14.141`
4. Введите **`exit`**. Устройство Rack PDU перезапускается, чтобы изменения вступили в силу.

Восстановление утерянного пароля

Для доступа к интерфейсу командной строки можно использовать локальный компьютер (компьютер, подключенный к Rack PDU или иному устройству через последовательный порт).

1. Выберите последовательный порт на локальном компьютере и отключите все службы, использующие этот порт.
2. Подключите прилагаемый последовательный кабель к выбранному порту на компьютере и к последовательному порту на устройстве Rack PDU.
3. Запустите на компьютере программу эмуляции терминала (например HyperTerminal®) и настройте следующие параметры для выбранного порта: скорость передачи 9600 бит/с, 8 бит данных, без проверки четности, 1 стоповый бит, без контроля потока.
4. Нажмите клавишу ENTER при необходимости несколько раз для вывода запроса на ввод имени пользователя **User Name**. Если запрос на ввод имени **User Name** не отображается, убедитесь в том, что:

– Последовательный порт не используется другим приложением.
– Параметры терминала соответствуют параметрам, указанным в операции 3.
– Соответствующий кабель используется, как указано в операции 2.

5. Нажмите клавишу **Reset**. Индикатор состояния начнет мигать поочередно оранжевым и зеленым. Нажмите клавишу **Reset** еще раз, пока мигает индикатор, для временного возврата значений по умолчанию имени пользователя и пароля.
6. Нажмите несколько раз клавишу ENTER для повторного отображения запроса **User Name**, затем укажите значение **dell** для имени пользователя и пароля. (Если после повторного отображения запроса на ввод параметра **User Name** процедура входа занимает более 30 секунд, необходимо повторить операцию 5 и процедуру входа.)

7. В интерфейсе командной строки используйте следующие команды для изменения параметров **User Name** и **Password**, заменив значение **dell**:

   `user -an` ***`имя_администратора`***

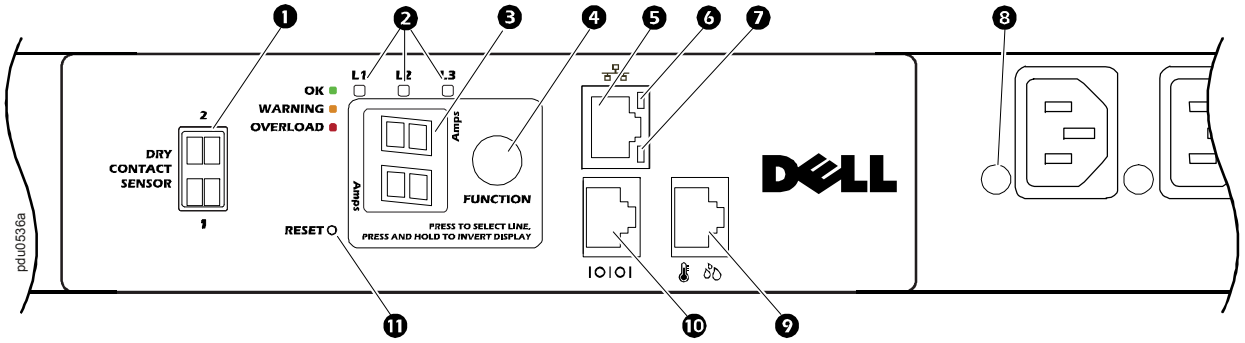
   `user -ap` ***`пароль_администратора`***

   Например, чтобы изменить имя Administrator на **Don Adams**, введите:

   `user -an Don Adams`

8. Для выхода из системы введите **`quit`** или **`exit`**, подключите ранее отсоединенный кабель последовательного интерфейса и повторно запустите отключенную службу.

Передняя панель устройства Rack



Компонент		Функция
1	Сухие контакты	Соединитель для двух устройств с сухими контактами.
2	Индикаторы фазы Примечание: у однофазных устройств Rack PDU имеется только один индикатор.	При отсутствии сигналов тревоги на дисплее индикатора отображается ток фазы, а зеленый индикатор показывает, какой именно фазы. Система циклически отображает ток каждой фазы в течение трех секунд в автоматическом режиме. При возникновении сигнала для одной фазы загорается соответствующий индикатор фазы. Он горит всё время, пока присутствует условие сигнала. Индикатор загорится оранжевым светом в случае сигнала предупреждения или красным светом в случае критического сигнала. При возникновении сигнала для более, чем одной фазы, система циклически отображает каждую такую фазу. Каждый индикатор фаз загорается на три секунды.

Компонент		Функция
❸	Дисплей индикатора	Отображается ток фазы для горящего в данный момент индикатора фазы.
❹	Кнопка «Function» (Функция)	• Чтобы вручную отобразить ток для каждой фазы, несколько раз нажмите на эту кнопку. Ток будет отображаться в течение 30 секунд или пока вы не нажмете на кнопку снова. (Эта функция недоступна для однофазных устройств Rack PDU.) • Для отображения IP-адреса нажмите и удерживайте кнопку в течение 5 секунд, пока не появится **IP**-адрес; затем отпустите кнопку. На дисплее отобразится адрес по две цифры, затем цикл повторится. • Для инвертирования дисплея нажмите кнопку и удерживайте в течение десяти секунд пока не появится схема **AA**. Продолжайте удерживать кнопку, пока схема AA не будет расположена так, как нужно, затем отпустите кнопку.
❺	Разъем 10/100 base-T	Порт для подключения устройства Rack PDU к сети.
❻	Индикатор 10/100	См. раздел Светодиодный индикатор 10/100.
❼	Светодиодный индикатор состояния сети	См. раздел Светодиодный индикатор состояния сети.
❽	Светодиодный индикатор состояния розетки	Загорается зеленым светом при активации розетки. (На каждую розетку имеется светодиодный индикатор.)
❾	Порт датчика температуры/ влажности	Порт для подключения датчика температуры устройства Rack PDU (G853N) или датчика температуры/влажности устройства Rack PDU (H621N).

Компонент		Функция
⑩	Последовательный порт RJ-45	Порт для подключения устройства Rack PDU к программе эмулятора терминала для локального доступа к интерфейсу командной строки. Используйте прилагаемый последовательный кабель.
⑪	Кнопка сброса	Для того, чтобы перезапустить интерфейс устройства Rack PDU, не влияя на состояние розеток, нажмите и отпустите кнопку Reset.

Светодиодный индикатор состояния сети

Состояние	Описание
Выкл	Возможна одна из следующих ситуаций: • На Rack PDU не подается входное питание. • Rack PDU работает неправильно. Вероятно, требуется ремонт или замена.
Непрерывный зеленый	Параметры TCP/IP Rack PDU заданы правильно.
Мигающий зеленый	Настройки TCP/IP Rack PDU установлены неправильно.
Непрерывный оранжевый	В устройстве Rack PDU обнаружен аппаратный сбой.
Мигающий оранжевый	Устройство Rack PDU выполняет запросы BOOTP.
Мигающий зеленый и оранжевый (попеременно)	Если светодиод мигает с низкой частотой, это означает, что Rack PDU выполняет запросы DHCP. Если светодиод мигает часто, это означает, что выполняется запуск Rack PDU.

1. Если сервер BOOTP или DHCP не используется, информацию о конфигурировании настроек TCP/IP устройства Rack PDU см. в разделе Установка сетевых настроек.
2. Об использовании сервера DHCP см. Настройки TCP/IP линии связи.

Светодиодный индикатор 10/100

Состояние	Описание
Выкл	Возможна одна или несколько из следующих ситуаций: • На Rack PDU не подается входное питание. • Отключен или неисправен кабель, соединяющий Rack PDU с сетью. • Отключено устройство, соединяющее Rack PDU с сетью. • Rack PDU работает неправильно. Вероятно, требуется ремонт или замена.
Непрерывный зеленый	Устройство Rack PDU подключено к сети, работающей со скоростью 10 Мбит/с.
Непрерывный оранжевый	Устройство Rack PDU подключено к сети, работающей со скоростью 100 Мбит/с.
Мигающий зеленый	Rack PDU принимает или передает пакеты данных со скоростью 10 Мбит/с.
Мигающий оранжевый	Rack PDU принимает или передает пакеты данных со скоростью 100 Мбит/с.

Интерфейс командной строки

Об интерфейсе командной строки

Интерфейс командной строки используется для отображения состояния и управления устройством Rack PDU. Кроме того, интерфейс командной строки позволяет создавать сценарии работы в автоматическом режиме. Администратор имеет полный доступ к интерфейсу командной строки, Пользователь устройства и Пользователь розетки имеют ограниченный доступ, а доступ пользователю, обладающему правами только для чтения, полностью ограничен. (Подробней об этом см. Типы учетных записей.)

Можно конфигурировать все параметры Rack PDU (включая те, для которых нет особых команд интерфейса командной строки) путем использования интерфейса для загрузки INI-файла в устройство Rack PDU. Для передачи данных интерфейс командной строки использует XMODEM. При этом, нельзя осуществлять чтение текущего INI-файла с помощью модема XMODEM.

Вход в интерфейс командной строки

Для доступа к интерфейсу командной строки можно использовать локальное подключение (по последовательному каналу связи) или удаленное подключение (Telnet или SSH) с помощью компьютера, находящегося в той же сети, что и Rack PDU.

Удаленный доступ к интерфейсу командной строки

Доступ к интерфейсу командной строки можно выполнять с помощью протокола Telnet или SSH. По умолчанию используется протокол Telnet. При включении SSH автоматически отключается Telnet.

Для включения и отключения этих способов доступа используйте веб-интерфейс. Выберите вкладку **Administration** (Администрирование) и пункт **Network** (Сеть) в верхней части строки меню, а затем параметр **access** (доступ) в области **Console** (Консоль) в левом меню навигации.

Протокол Telnet для стандартного доступа. Протокол Telnet обеспечивает стандартную аутентификацию по имени пользователя и паролю, однако не имеет преимуществ шифрования, обеспечивающих высокий уровень защиты.

Для использования Telnet для доступа к интерфейсу командной строки:

1. С компьютера, находящегося в той же ЛВС, что и Rack PDU, в командной строке введите **`telnet`** и укажите IP-адрес устройства Rack PDU (например, **`telnet 139.225.6.133`**, если Rack PDU использует стандартный порт Telnet – 23) и нажмите ENTER.
   Если устройство Rack PDU использует нестандартный номер порта (в диапазоне от 5000 до 32768), необходимо вставить запятую или пробел между IP-адресом (или DNS-именем) и номером порта, в зависимости от используемого клиента Telnet. (Эти команды относятся к общему случаю: некоторые клиенты не позволяют указывать порт в качестве аргумента, а некоторые могут потребовать дополнительных команд).
2. Введите имя пользователя и пароль (по умолчанию, **admin** и **admin** для Администратора или **device** и **apc** для Пользователя устройства).

Если вы не можете вспомнить имя пользователя или пароль, см. Восстановление утерянного пароля.

SSH для доступа с высоким уровнем защиты. Если для обеспечения надежной защиты веб-интерфейса используется SSL, для доступа к интерфейсу командной строки нужно использовать протокол SSH. SSH выполняет шифрование имен пользователей, паролей и передаваемых данных. Вне зависимости от способа доступа к интерфейсу командной строки (SSH или Telnet), учетные записи пользователей и права доступа пользователей остаются неизменными. Однако, чтобы пользоваться SSH, необходимо сначала установить на компьютере клиентскую программу SSH и выполнить ее настройку.

Локальный доступ к интерфейсу командной строки

Для осуществления локального доступа используйте компьютер, подключенный к Rack PDU через последовательный порт, с помощью интерфейса командной строки:

1. Выберите последовательный порт на компьютере и отключите все службы, использующие этот порт.
2. Подключите кабель последовательного интерфейса к порту компьютера и разъему последовательного порта на Rack PDU.
3. Запустите программу терминала (например, HyperTerminal), настройте следующие параметры для выбранного порта: 9600 бит/с, 8 бит данных, без проверки четности, 1 стоповый бит, без контроля потока.
4. Нажмите ENTER, в появившейся строке приглашения введите имя пользователя и пароль.

О главном экране

Ниже приведен пример главного экрана, который отображается при загрузке из интерфейса командной строки устройства 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>
```

Информационные поля главного экрана:

- Два поля отображают версии микропрограммного обеспечения: операционной системы (AOS) и приложения (APP). Имя приложения микропрограммного обеспечения определяет тип устройства, подключенного к сети. В приведенном примере показано микропрограммное приложение для Rack PDU.

  ```
  Network Management Card AOS  vx.x.x

  RPDUD vx.x.x
  ```

- Три поля определяют имя системы, имя контактного лица и местоположение Rack PDU. (Для задания данных значений используйте меню **System** (Система) в консоли управления.)

  ```
  Name: Test Lab

  Contact: Don Adams

  Location: Building 3
  ```

- Поле **Up Time** (Время работы) показывает, как долго устройство Rack PDU работает с момента последнего включения или перезагрузки.

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

- Два поля показывают, когда вы зашли в систему: дату и время.

  ```
  Date : 10/30/2009

  Time : 5:58:30
  ```

- Поле **User** (Пользователь) показывает, зашли ли вы в систему с использованием учетной записи **Administrator** (Администратор) или **Device user** (Пользователь устройства). (Учетная запись **Пользователь только для чтения** не обеспечивает доступ к интерфейсу командной строки.)

  ```
  User : Administrator
  ```

- Поле **Stat** отображает состояние устройства Rack PDU.

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

P+	Операционная система Dell работает нормально.

Только IPv4	Только IPv6	IPv4 и IPv6*	Описание
N+	**N+**	**N4+ N6+**	Сеть работает нормально.
N?	**N6?**	**N4? N6?**	Выполняется цикл запроса BOOTP.
N–	**N6–**	**N4– N6–**	Ошибка подключения Rack PDU к сети.
N!	**N6!**	**N4! N6!**	Другое устройство использует IP-адрес Rack PDU.

* Значения N4 и N6 могут отличаться друг от друга: например, может быть N4- N6+.

A+	Приложение работает нормально.
A–	Приложение дает неверную контрольную сумму.
A?	Идет инициализация приложения.
A!	Приложение несовместимо с операционной системой AOS.

Если P+ не отображается, вам может помочь Персонал технической поддержки компании Dell.

Использование интерфейса командной строки

С помощью интерфейса командной строки вводят команды конфигурации Rack PDU. Чтобы использовать команду, введите ее и нажмите ENTER. Команды и аргументы можно вводить в нижнем, верхнем и смешанных регистрах. Функции зависят от регистра.

При использовании интерфейса командной строки можно также выполнять следующие операции.

- Введите **?** и нажмите ENTER, чтобы вывести на экран список команд, доступных в вашей учетной записи.
- Для получения информации о назначении и синтаксисе указанной команды наберите команду, пробел и **?** или слово **help**. Например, для просмотра вариантов конфигурации RADIUS наберите:

  radius ?

  или

  radius help

- Нажмите кнопку UP (стрелка вверх), чтобы увидеть команду, введенную недавно в течение данной сессии. Используя кнопки UP (вверх) и DOWN (вниз), можно просмотреть до десяти введенных ранее команд.
- Введите хотя бы одну букву команды и нажмите кнопку TAB (табуляция), чтобы получить на экране список доступных команд, которые содержат введенный в командной строке текст.
- Введите **exit** или **quit**, чтобы закрыть соединение с интерфейсом командной строки.

Синтаксис команд

Компонент	Описание
-	Параметрам предшествует дефис.
< >	Определения параметров указываются в угловых скобках. Например: `-dp <device password> (пароль устройства)`
[ ]	Если команда принимает различные параметры или параметр принимает взаимоисключающие значения, то эти значения могут указываться в квадратных скобках.
|	Вертикальная линия между компонентами в квадратных или угловых скобках указывает на то, что они взаимоисключающие. Необходимо выбрать один из компонентов.

Пример команды, поддерживающей несколько параметров:

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

В этом примере команда user получает параметр **`-an`**, который определяет имя администратора, а параметр **`-ap`** определяет пароль администратора. Чтобы изменить имя и пароль администратора на XYZ, необходимо выполнить следующие действия.

1. Ввести команду пользователя, один из параметров и значение **`XYZ`**:
   `user -ap XYZ`
2. После успешного выполнения первой команды введите команду, второй параметр и значение **`XYZ`**:
   `user -ap XYZ`

Пример команды, которая использует несколько взаимоисключающих значений параметра:

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

В этом примере параметр -p принимает только три значения: all, warning или critical. Например для просмотра ряда активных критичных аварийных сигналов наберите:

`alarmcount -p critical`

Если ввести значение параметра, которое не определено, команда не будет выполнена.

Коды отклика команд

Коды отклика команд позволяют сценариям работы уверенно распознать условия возникновения ошибок, не требуя точного совпадения текста сообщений об ошибках:

Интерфейс командной строки сообщает обо всех командных операциях в следующем формате:

E [0-9] [0-9] [0-9] : Сообщение об ошибке

Код	Сообщение	Код	Сообщение
E000	Успешно	E105	Предварительное заполнение команды
E001	Успешно задана	E106	Данные отсутствуют
E002	Чтобы изменения вошли в силу, требуется перезагрузка	E107	Потеряна последовательная связь с устройством Rack PDU
E100	Сбой команды		
E101	Команда не обнаружена		
E102	Ошибка параметра		
E103	Ошибка командной строки		
E104	Отказ пользователю данного уровня		

Описания команд карты сетевого управления

?

Доступ: Администратор, Пользователь устройства, Пользователь розетки

Описание: Просмотр списка всех команд интерфейса командной строки для учетной записи вашего типа. Для просмотра текста справки для конкретной команды наберите эту команду и поставьте после нее знак вопроса.

Пример: Для просмотра списка параметров, принимаемых командой **`alarmcount`**, введите:

```
alarmcount ?
```

about

Доступ: Администратор, Пользователь устройства, Пользователь розетки

Описание: Просмотр информации о программно-аппаратном обеспечении. Эта информация полезна в случае поиска неисправностей, она позволяет определить, нужно ли обновлять микропрограммное обеспечение.

alarmcount

Доступ: Администратор, Пользователь устройства, Пользователь розетки

Описание:

Параметр	Значения	Описание
-p	all	Показывает количество активных сигналов, сообщаемых Rack PDU. Информация об аварийных сигналах содержится в журнале событий.
	warning	Показывает количество активных предупреждающих сигналов.
	critical	Показывает количество активных критических сигналов.

Пример: Для просмотра всех активных предупреждающих сигналов введите:

```
alarmcount -p warning
```

boot

Доступ: Только Администратор

Описание: Определяет, каким образом Rack PDU получает свои сетевые настройки, включая IP-адрес, маску подсети, шлюз по умолчанию. Затем настройте параметры сервера BOOTP или DHCP.

Параметр	Значение	Описание
-b <boot mode>	dhcp | bootp | manual	Определяет, каким образом будут конфигурироваться настройки TCP/IP при включении, сбросе и перезапуске Rack PDU. См. Настройки TCP/IP линии связи для получения сведений о каждом параметре режима загрузки.
-c	enable | disable	Только для режимов загрузки `dhcp` и `dhcpBootp`. Включает и отключает требование, чтобы DHCP-сервер выдавал cookie-файл поставщика.
Значения по умолчанию для этих трех настроек обычно менять не требуется: -v <vendor class> (класс поставщика): DELL -i <client id> (идентификатор клиента): MAC-адрес Rack PDU, который позволяет однозначно идентифицировать устройство в сети -u <user class> (класс пользователя): название модуля микропрограммы приложения		

Пример: Чтобы использовать сервер DHCP для получения сетевых параметров, выполните следующее:

1. Введите **`boot -b dhcp`**
2. Включите требование, чтобы DHCP-сервер выдавал cookie-файл поставщика:
   `boot -c enable`

cd

Доступ: Администратор, Пользователь устройства, Пользователь розетки

Описание: Переход к папке в файловой структуре устройства Rack PDU.

Пример 1: Чтобы перейти в папку **ssh** и убедиться, что сертификат безопасности SSH был загружен в Rack PDU:

1. Наберите **cd ssh** и нажмите ENTER.
2. Для получения списка файлов, хранящихся в папке SSH, наберите **dir** и нажмите ENTER.

Пример 2: Чтобы вернуться в в папку главного каталога, введите:

```
cd ..
```

console

Доступ: Только Администратор

Описание: Укажите, могут ли пользователи иметь доступ к интерфейсу командной строки с помощью протокола Telnet, включаемого по умолчанию, или Secure Shell (SSH), обеспечивающего защиту за счет передачи имен пользователей, паролей и данных в шифрованном виде. Для дополнительной безопасности можно изменить настройку порта Telnet или SSH. В противном случае, отключите сетевой доступ к интерфейсу командной строки.

Параметр	Значение	Описание
-S	disable | telnet | ssh	Настройте доступ к интерфейсу командной строки или используйте команду 'disable' (отключить) для запрещения доступа. Включение SSH дает возможность использовать SCP и отключает Telnet.
-pt	<telnet port n>	Определяет порт Telnet, используемый для связи с Rack PDU (по умолчанию – 23).
-ps	<SSH port n>	Определяет порт SSH, используемый для связи с Rack PDU (по умолчанию – 22).
-b	2400 | 9600 | 19200 | 38400	Настройте скорость передачи последовательного порта (по умолчанию 9600 бит/с).

Пример 1: Чтобы обеспечить доступ SSH к интерфейсу командной строки, наберите:

```
console -S ssh
```

Пример 2: Чтобы изменить порт Telnet на 5000, наберите:

```
console -pt 5000
```

date

Доступ: Только Администратор

Описание: Конфигурирует дату, используемую Rack PDU.

О конфигурации сервера NTP на определение даты и времени для Rack PDU см. Задание даты и времени.

Параметр	Значение	Описание
-d	<“datestring”>	Задает текущую дату. Используйте формат данных, задаваемый командой `date -f`.
-t	<00:00:00>	Задает текущее время в часах, минутах и секундах. Используйте 24-часовой формат времени.
-f	mm/dd/yy | dd.mm.yyyy | mmm-dd-yy | dd-mmm-yy | yyyy-mm-dd	Выберите цифровой формат, в котором будут отображаться все даты данного пользовательского интерфейса. Каждая буква m (месяц), d (день) и y (год) представляет один разряд. Однозначные дни и месяцы отображаются с ведущим нулем (перед значащей цифрой).
-z	<time zone offset>	Для указания часового пояса задайте разницу относительно времени по Гринвичу (GMT). Это даст возможность синхронизироваться с другими людьми в различных часовых поясах.

Пример 1: Для отображения даты в формате гггг-мм-дд наберите:

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

Пример 2: Чтобы указать дату 30 октября 2009 года в формате, указанном в предыдущем примере, наберите:

```
date -d “2009-10-30”
```

Пример 3: Чтобы задать время 5:21:03 p.m., наберите:

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

delete

Доступ: Только Администратор

Описание: Удаляет файл в файловой системе.

Значение	Описание
<file name>	Введите имя файла, предназначенного для удаления.

dir

Доступ: Администратор, Пользователь устройства, Пользователь розетки

Описание: Просмотр файлов и папок, хранящихся в Rack PDU.

dns

Доступ: Только Администратор

Описание: Настройка параметров системы доменных имен (DNS) вручную.

Параметр	Значение	Описание
-OM	enable | disable	Принудительно задаются ручные настройки DNS.
-p	<primary DNS server>	Задается первичный DNS-сервер.
-s	<secondary DNS server>	Задается вторичный DNS-сервер.
-d	<domain name>	Задается имя домена.
-n	<domain name IPv6>	Задается имя домена IPv6.
-h	<host name>	Задается имя хоста.

eventlog

Доступ: Администратор, Пользователь устройства, Пользователь розетки

Описание: Показывает дату и время по журналу событий, состояние Rack PDU и состояние датчиков, подключенных к Rack PDU. Показывает наиболее поздние события устройства и дату и время, когда эти события произошли. Для перемещения по журналу событий используются следующие клавиши:

Клавиша	Описание
ESC	Журнал событий закрывается, и экран возвращается к интерфейсу командной строки.
ENTER	Обновляется отображение журнала. Используйте эту команду для просмотра событий, которые были зарегистрированы после последней операции поиска и отображения журнала.
ПРОБЕЛ	Просмотр следующей страницы журнала событий.
B	Просмотр предыдущей страницы журнала событий. Эта команда отсутствует на главной странице журнала событий.
D	Удаление журнала событий. Следуйте подсказкам для подтверждения или отклонения удаления. Удаленные события восстановить невозможно.

exit

Доступ: Администратор, Пользователь устройства, Пользователь розетки

Описание: Выход из сеанса интерфейса командной строки.

format

Доступ: Только Администратор

Описание: Переформатирует файловую систему Rack PDU и стирает все сертификаты безопасности, ключи шифрования, настройки конфигурации и журналы регистрации событий и дат.

Чтобы перезагрузить Rack PDU с исходной конфигурацией, используйте команду **`resetToDef`**.

FTP

Доступ: Только Администратор

Описание: Включает и отключает доступ к серверу FTP. Для дополнительной защиты можно также изменить настройку порта, указав номер любого неиспользуемого порта в диапазоне от 5001 до 32768.

Параметр	Значение	Описание
-p	<port number>	Определяет порт TCP/IP, который используется FTP-сервером для обмена данными с Rack PDU (по умолчанию – 21). Сервер FTP использует как указанный порт, так и порт с номером на единицу меньше.
-S	enable | disable	Настройка доступа к FTP-серверу.

Пример: Чтобы изменить порт TCP/IP на 5001, введите:

```
ftp -p 5001
```

help

Доступ: Администратор, Пользователь устройства, Пользователь розетки

Описание: Просмотр списка всех команд интерфейса командной строки для учетной записи вашего типа. Для просмотра текста справки по конкретной команде наберите эту команду, а следом за ней **`help`**.

Пример 1: Для просмотра списка команд, разрешенных для Пользователя, введите:

```
help
```

Пример 2: Для просмотра списка параметров, принимаемых командой **`alarmcount`**, введите:

```
alarmcount help
```

netstat

Доступ: Администратор, Пользователь устройства, Пользователь розетки

Описание: Выполняется просмотр состояния сети и всех активных адресов IPv4 и IPv6.

ntp

Доступ: Администратор

Описание: Просмотр и настройка параметров протокола сетевого времени.

Параметр	Значение	Описание
-OM	enable | disable	Принудительно задаются ручные настройки.
-p	<primary NTP server>	Укажите первичный сервер.
-s	<secondary NTP server>	Укажите вторичный сервер.

Пример 1: Для принудительного задания ручных настроек наберите:

```
ntp -OM enable
```

Пример 2: Для указания первичного NTP-сервера наберите:

```
ntp -p 150.250.6.10
```

ping

Доступ: Администратор, Пользователь устройства

Описание. Определяет, подключено ли к сети устройство с заданным IP-адресом или именем DNS. На указанный адрес посылается четыре запроса.

Значение	Описание
<IP address or DNS name>	Наберите IP-адрес в формате *xxx.xxx.xxx.xxx* или имя DNS, сконфигурированное DNS-сервером.

Пример: Чтобы определить, подключено ли к сети устройство с IP-адресом 150.250.6.10, введите:

```
ping 150.250.6.10
```

portSpeed

Доступ: Администратор

Описание:

Параметр	Значения	Описание
-s	auto | 10H | 10F | 100H | 100 F	Определяет скорость передачи данных через порт Ethernet. Команда `auto` включает устройства Ethernet для согласования передачи данных с максимально возможной скоростью. Дополнительную информацию о параметрах настройки скорости передачи порта см. в разделе Скорость передачи порта.

Пример: Чтобы настроить порт TCP/IP на обмен данными со скоростью 100 Мбит/с в полу-дуплексном режиме (единовременная связь только в одном направлении), введите:

```
portspeed -s 100H
```

prompt

Доступ: Администратор, Пользователь устройства

Описание: Конфигурация приглашения интерфейса командной строки для включения или исключения типа учетной записи пользователя, работающего в системе в данный момент. Любой пользователь может изменить эту настройку; все пользовательские учетные записи будут обновлены и будут использовать новую настройку.

Параметр	Значение	Описание
-s	long	Приглашение включает в себя тип учетной записи пользователя, находящегося в данный момент в системе.
	short	Настройка по умолчанию. Длина приглашения составляет четыре символа: `cli>`

Пример: Чтобы добавить в приглашение тип учетной записи пользователя, находящегося в данный момент в системе, введите:

```
prompt -s long
```

quit

Доступ: Администратор, Пользователь устройства, Пользователь розетки

Описание: Закрытие сеанса интерфейса командной строки (работает так же, как и команда exit).

radius

Доступ: Только Администратор

Описание: Выполняет просмотр существующих настроек RADIUS, включает и отключает идентификацию RADIUS и конфигурирует основные параметры авторизации максимум для двух серверов RADIUS.

Краткое описание конфигурации сервера RADIUS и список поддерживаемых серверов RADIUS приводится в руководстве Конфигурирование сервера RADIUS.

Дополнительные параметры идентификации для серверов RADIUS приведены в веб-интерфейсе устройства Rack PDU. Дополнительные сведения см. в разделе RADIUS.

Подробней о конфигурации сервера RADIUS см. Приложение Б: Руководство по безопасности.

Параметр	Значение	Описание
-a	local | radiusLocal | radius	Настройка идентификации RADIUS: **`local`**—RADIUS отключен. Локальная аутентификация включена. **`radiusLocal`**—RADIUS, затем локальная аутентификация. Включается RADIUS и локальная аутентификация. Сначала запрашивается аутентификация от сервера RADIUS. Если сервер RADIUS не отвечает, то используется локальная аутентификация. **`radius`**—RADIUS включен. Локальная аутентификация отключена.

Параметр	Значение	Описание
-p1 -p2	<server IP>	Имя или IP-адрес первичного или вторичного сервера RADIUS. **ПРИМЕЧАНИЕ:** Серверы RADIUS используют для аутентификации пользователей порт 1812 по умолчанию. Чтобы использовать другой порт, добавьте к имени или к IP-адресу сервера RADIUS двоеточие и укажите новый номер порта.
-s1 -s2	<server secret>	Секретная фраза, известная первичному и вторичному серверам RADIUS, а также Rack PDU.
-t1 -t2	<server timeout>	Время в секундах, в течение которого устройство Rack PDU ждет отклика от первичного или вторичного сервера RADIUS.

Пример 1:

Чтобы просмотреть существующие настройки RADIUS для Rack PDU, введите **`radius`** и нажмите ENTER.

Пример 2: Чтобы включить идентификацию RADIUS и локальную идентификацию, наберите:

```
radius -a radiusLocal
```

Пример 3: Чтобы задать 10-секундный период ожидания для вторичного сервера RADIUS, введите:

```
radius -t2 10
```

reboot

Доступ: Только Администратор

Описание: Перезапуск интерфейса Rack PDU.

resetToDef

Доступ: Только Администратор

Описание:

Параметр	Значения	Описание
-p	all | keepip	Выполняется сброс всех измененных параметров, включая действующие события, параметры устройства и, по желанию, параметры конфигурации TCP/IP.

Пример: Чтобы сбросить все изменения параметров конфигурации, за исключением настроек TCP/IP для Rack PDU, введите:

```
resetToDef -p keepip
```

snmp, snmpv3

Доступ: Только Администратор

Описание: Включение или отключение SNMP 1 или SNMP 3.

Параметр	Значения	Описание
-S	enable | disable	Включение или отображение соответствующей версии SNMP 1 или 3.

Пример: Для включения SNMP версии 1 наберите:

```
snmp -S enable
```

system

Доступ: Только Администратор

Описание: Выполняется просмотр и установка имени системы, контактного лица, местоположения, а также даты и времени, текущего пользователя и состояния системы высокого уровня P, N, A (подробнее о состоянии системы см. О главном экране).

Параметр	Значение	Описание
-n	<system name>	Определяет имя устройства, имя ответственного за это устройство и физическое местоположение устройства. **ПРИМЕЧАНИЕ:** Если для определения значения используется более одного слова, то это значение должно быть заключено в кавычки.
-c	<system contact>	
-l	<system location>	

Пример 1: Для задания местоположения устройства **`Test Lab`** (испытательная лаборатория), введите:

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

Пример 2: Чтобы задать имя ответственного **`Don Adams`**, введите:

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

tcpip

Доступ: Только Администратор

Описание: Выполняется просмотр и ручная настройка следующих параметров сети для Rack PDU:

Параметр	Значение	Описание
-i	<IP address>	Введите IP-адрес Rack PDU, используя формат *xxx.xxx.xxx.xxx*
-s	<subnet mask>	Введите маску подсети для Rack PDU.
-g	<gateway>	Введите IP-адрес шлюза, используемого по умолчанию. **Не используйте** адрес замыкания на себя (127.0.0.1) в качестве адреса шлюза по умолчанию.
-d	<domain name>	Введите имя DNS, сконфигурированное DNS-сервером.
-h	<host name>	Введите имя хоста, которое будет использовать Rack PDU.

Пример 1: Чтобы просмотреть существующие настройки RADIUS для Rack PDU, введите **`radius`** и нажмите ENTER.

Пример 2: Чтобы вручную задать IP-адрес **`150.250.6.10`** для Rack PDU, введите:

```
tcpip -i 150.250.6.10
```

tcpip6

Доступ: Только Администратор

Описание: Выполняется включение IPv6, просмотр и ручная настройка следующих параметров сети для Rack PDU:

Параметр	Значение	Описание
-S	enable | disable	Включение или выключение IPv6.
-man	enable | disable	Выполняется включение ручной адресации для задания адреса IPv6 Rack PDU.
-auto	enable | disable	Позволяет устройству Rack PDU автоматически настраивать адрес IPv6.
-i	<IPv6 address>	Задается адрес IPv6 устройства Rack PDU.
-g	<IPv6 gateway>	Задается адрес IPv6 шлюза, используемый по умолчанию.
-d6	router | statefull | stateless | never	Задается режим DHCPv6: с параметрами управляемого маршрутизатора, с сохранением состояния (адрес и другая информация, поддерживающая состояние), без указания состояния (информация, отличная от адреса, без поддержания состояния), без параметров.

Пример 1: Для просмотра имеющихся сетевых параметров Rack PDU наберите **`tcpip6`** и нажмите ВВОД.

Пример 2: Для ручной настройки адреса IPv6 **`2001:0:0:0:0:FFD3:0:57ab`** устройства Rack PDU наберите:

```
tcpip -i 2001:0:0:0:0:FFD3:0:57ab
```

user

Доступ: Только Администратор

Описание: Задаются имя пользователя, пароль и время неактивности для учетных записей Администратора, Пользователя устройства и Пользователя только для чтения.

Информацию о разрешениях для каждого типа учетной записи см. в разделе Типы учетных записей.

Параметр	Значение	Описание
-an -dn -rn	<admin name> <device name> <read-only name>	Для каждого типа учетной записи задается имя пользователя, зависящее от регистра. Максимальная длина – 10 символов.
-ap -dp -rp	<admin password> <device password> <read-only password>	Для каждого типа учетной записи задается пароль, зависящий от регистра. Максимальная длина – 32 символа. Пустые пароли (без символов) не допускаются.
-t	<минуты>	Выполняется настройка времени (3 минуты по умолчанию), по истечении которого неактивный пользователь отключается от системы.

Пример 1: Чтобы изменить имя администратора на XYZ, введите:

```
user -ap XYZ
```

Пример 2: Чтобы изменить время выхода из системы, установив его на 10 мин, наберите:

```
user -t 10
```

web

Доступ: Только Администратор

Описание: Включает доступ к веб-интерфейсу с использованием HTTP и HTTPS.

С целью повышения безопасности можно изменить настройку порта для HTTP и HTTPS, задав любой неиспользуемый порт от 5000 до 32768. Для указания номера порта пользователи должны использовать двоеточие (:) в адресном поле браузера. Например, для задания номера порта 5000 и IP-адреса 152.214.12.114 введите:

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

Параметр	Значение	Описание
-S	disable | http | https	Настройка доступа к веб-интерфейсу. При включении HTTPS данные шифруются во время передачи и авторизуются с помощью цифрового сертификата.
-ph	<http port #>	Определяет порт TCP/IP, который используется протоколом HTTP для обмена данными с Rack PDU (по умолчанию – 80).
-ps	<https port #>	Определяет порт TCP/IP, который используется протоколом HTTPS для обмена данными с Rack PDU (по умолчанию – 443).

Пример: Чтобы полностью заблокировать доступ к веб-интерфейсу, введите:

```
web -S disable
```

xferINI

Доступ: Только Администратор

Описание: Использует XMODEM для загрузки INI-файла при обращении через последовательный порт с помощью интерфейса командной строки. После завершения загрузки:

- Если произошли какие-либо изменения в системе или сети, интерфейс командной строки будет перезапущен, и вам придется войти в систему еще раз.
- Если была выбрана скорость обмена для передачи файлов, отличная от заданной по умолчанию для Rack PDU, необходимо установить скорость, равную заданной по умолчанию, чтобы восстановить связь с Rack PDU.

xferStatus

Доступ: Только Администратор

Описание: Просмотр результатов последней передачи файла.

Описание кодов результатов передачи приводится в разделе Проверка обновлений и исправлений.

Описание команд устройства

devLowLoad

Доступ: Администратор, Пользователь устройства

Описание: Задает или показывает порог низкой мощности в кВт для данного устройства.

Пример 1: Чтобы просмотреть порог низкой мощности, введите:

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

Пример 2: Для задания порогового значения низкой мощности величиной в 1 кВт укажите:

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

devNearOver

Доступ: Администратор, Пользователь устройства

Описание: Задает или показывает близкий к перегрузке порог мощности в кВт для данного устройства.

Пример 1: Чтобы просмотреть близкий к перегрузке порог мощности, введите:

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

Пример 2: Для задания порогового значения, близкого к перегрузке, равного 21,3 кВт укажите:

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

devOverLoad

Доступ: Администратор, Пользователь устройства

Описание: Задает или показывает порог перегрузки в кВт для данного устройства.

Пример 1: Чтобы просмотреть порог перегрузки, введите:

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

Пример 2: Для задания порогового значения перегрузки, равного 25,5 кВт, укажите:

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

devReading

Доступ: Администратор, Пользователь устройства

Описание: Просмотр суммарной мощности устройства в киловаттах или энергии в киловатт-часах.

Значение	Описание
power	Просмотр суммарной мощности в киловаттах
energy	Просмотр потребленной энергии в киловатт-часах

Пример 1: Чтобы просмотреть суммарную мощность, введите:

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

Пример 2: Чтобы просмотреть суммарную потребленную энергию, введите:

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

devStartDly

Доступ: Администратор, Пользователь устройства

Описание: Позволяет задавать и просматривать величину временного интервала (в секундах), который добавляется к времени задержки включения каждой розетки (Power On Delay) после подачи питания на Rack PDU. Допустимые значения находятся в диапазоне от 1 до 300 секунд или «никогда» (никогда не включать).

Пример 1: Для просмотра времени задержки холодного старта введите:

```
cli> devStartDly
E000: Success
5 seconds
```

Пример 2: Чтобы задать время задержки холодного старта равным 6 секундам, введите:

```
cli> devStartDly 6
E000: Success
```

humLow

Доступ: Администратор, Пользователь устройства

Описание: Задание или просмотр нижнего порога влажности в процентах относительной влажности.

Пример 1: Чтобы просмотреть нижний порог влажности, введите:

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

Пример 2: Чтобы задать нижний порог влажности, введите:

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

humMin

Доступ: Администратор, Пользователь устройства

Описание: Задание или просмотр минимального порога влажности в процентах относительной влажности.

Пример 1: Чтобы просмотреть минимальный порог влажности, введите:

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

Пример 2: Чтобы задать минимальный порог влажности, введите:

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

humReading

Доступ: Администратор, Пользователь устройства, Пользователь розетки.

Описание: Просмотр значения влажности, измеренного датчиком.

Пример: Чтобы просмотреть значение влажности, введите:

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

inNormal

Доступ: Администратор, Пользователь устройства

Описание: Просмотр нормального состояния сухих входных контактов.

Пример: Чтобы просмотреть нормальное состояние сухих входных контактов, введите:

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

inReading

Доступ: Администратор, Пользователь устройства

Описание: Просмотр текущего состояния сухих входных контактов.

Пример: Чтобы просмотреть состояние сухих входных контактов, введите:

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

olAssignUsr

Доступ: Администратор

Описание: Назначает управление розетками для пользователя, имеющегося в локальной базе данных.

Значение	Описание
all	Все розетки устройства.
<outlet name>	Имя, заданное для определенной розетки. (См. раздел olName).
<outlet#>	Отдельный номер или диапазон номеров, задаваемый с помощью дефиса, или список значений номеров отдельных розеток и диапазонов номеров, разделяемых запятыми.
<user>	Пользователь, имеющийся в локальной базе данных. (См. раздел userAdd).

Пример 1: Чтобы назначить пользователю по имени Бобби розетки 3, с 5 по 7 и 10, введите:

```
cli> olAssignUsr 3,5-7,10 bobby
E000: Success
```

Пример 2: Чтобы назначить пользователю по имени Билли все розетки, введите:

```
cli> olAssignUsr all billy
E000: Success
```

olCancelCmd

Доступ: Администратор, Пользователь устройства и Пользователь розетки, но только для розеток, назначенных данным пользователям.

Описание: Отменяет все запланированные команды для розетки или группы розеток.

Значение	Описание
all	Все розетки устройства.
<outlet name>	Имя, заданное для определенной розетки. (См. раздел olName).
<outlet#>	Отдельный номер или диапазон номеров, задаваемый с помощью дефиса, или список значений номеров отдельных розеток и диапазонов номеров, разделяемых запятыми.

Пример: Чтобы отменить все команды для розетки 3, введите:

```
cli> olCancelCmd 3
E000: Success
```

olDlyOff

Доступ: Администратор, Пользователь устройства и Пользователь розетки, но только для розеток, назначенных данным пользователям.

Описание: Отключает розетку или группу розеток по истечении периода задержки отключения питания Power Off Delay (см. olOff).

Значение	Описание
all	Все розетки устройства.
<имя розетки>	Имя, заданное для определенной розетки. (См. раздел olName).
<outlet#>	Отдельный номер или диапазон номеров, задаваемый с помощью дефиса, или список значений номеров отдельных розеток и диапазонов номеров, разделяемых запятыми.

Пример 1: Чтобы отключить розетки 3, с 5 по 7 и 10, введите:

```
cli> olDlyOff 3,5-7,10
E000: Success
```

Пример 2: Чтобы отключить все розетки, введите:

```
cli> olDlyOff all
E000: Success
```

olDlyOn

Доступ: Администратор, Пользователь устройства и Пользователь розетки, но только для розеток, назначенных данным пользователям.

Описание: Включает розетку или группу розеток по истечении периода задержки включения питания Power On Delay (см. olOnDelay).

Значение	Описание
all	Все розетки устройства.
<outlet name>	Имя, заданное для определенной розетки. (См. раздел olName).
<outlet#>	Отдельный номер или диапазон номеров, задаваемый с помощью дефиса, или список значений номеров отдельных розеток и диапазонов номеров, разделяемых запятыми.

Пример 1: Чтобы включить розетки 3, с 5 по 7 и 10, введите:

```
cli> olDlyOn 3,5-7,10
E000: Success
```

Пример 2: Чтобы включить розетку с заданным именем Outlet1, введите:

```
cli> olDlyOn outlet1
E000: Success
```

olDlyReboot

Доступ: Администратор, Пользователь устройства и Пользователь розетки, но только для розеток, назначенных данным пользователям.

Описание: Повторно подает питание на розетку или группу розеток. Указанные розетки отключаются от питания по истечении заданного периода ожидания отключения Power Off Delay (см. olOffDelay). По истечении самого длительного для выбранных розеток периода перезагрузки (см. olRbootTime) на эти розетки будет подано питание по истечении периодов задержки включения (см. olOnDelay), заданных для указанных розеток.

Значение	Описание
all	Все розетки устройства.
<outlet name>	Имя, заданное для определенной розетки. (См. раздел olName).
<outlet#>	Отдельный номер или диапазон номеров, задаваемый с помощью дефиса, или список значений номеров отдельных розеток и диапазонов номеров, разделяемых запятыми.

Пример 1: Чтобы переподключить розетки 3, с 5 по 7 и 10, введите:

```
cli> olDlyReboot 3,5-7,10
E000: Success
```

Пример 2: Чтобы переподключить розетку с заданным именем Outlet1, введите:

```
cli> olDlyReboot outlet1
E000: Success
```

olGroups

Доступ: Администратор, Пользователь устройства и Пользователь розетки.

Описание: Перечень групп синхронизации розеток, заданных для Rack PDU (подробней см. Настройка и управление группами розеток).

Пример: Чтобы вывести перечень групп синхронизации розеток, введите:

```
cli> olGroups
E000: Success
Группа розеток A:
159.215.6.141 -> Розетки: 2,4,5
159.215.6.143 -> Розетки: 2,8
Группа розеток B:
159.215.6.141 -> Розетки: 1
159.215.6.166 -> Розетки: 1
```

olLowLoad

Доступ: Администратор, Пользователь устройства и Пользователь розетки, но только для розеток, назначенных данным пользователям.

Описание: Позволяет задавать и просматривать пороговое значение низкой мощности розетки.

Значение	Описание
all	Все розетки устройства.
<outlet name>	Имя, заданное для определенной розетки. (См. раздел olName).
<outlet#>	Отдельный номер или диапазон номеров, задаваемый с помощью дефиса, или список значений номеров отдельных розеток и диапазонов номеров, разделяемых запятыми.
<power>	Новое пороговое значение розетки (Вт).

Пример 1: Для задания порогового значения низкой мощности величиной в 2 Вт для всех розеток укажите:

```
cli> olLowLoad all 2
E000: Success
```

Пример 2: Для просмотра порогового значения низкой мощности для розеток 3 и с 5 по 7 введите:

```
cli> olLowLoad 3,5-7
E000: Success
3: BobbysServer: 2 W
5: BillysServer: 2 W
6: JoesServer: 2 W
7: JacksServer: 2 W
```

olName

Доступ: Администратор, Пользователь устройства и Пользователь розетки, но только для розеток, назначенных данным пользователям.

Описание: Позволяет задавать и просматривать имя, заданное розетке.

Значение	Описание
all	Все розетки устройства.
<outlet#>	Отдельный номер или диапазон номеров, задаваемый с помощью дефиса, или список значений номеров отдельных розеток и диапазонов номеров, разделяемых запятыми.
<newname>	Имя для указанной розетки. Используйте только буквы и цифры.

Пример: Чтобы задать имя розетки 3 для сервера BobbysServer введите:

```
cli> olName 3 BobbysServer
E000: Success
3: BobbysServer
5: BillysServer
6: JoesServer
7: JacksServer
```

olNearOver

Доступ: Администратор, Пользователь устройства и Пользователь розетки, но только для розеток, назначенных данным пользователям.

Описание: Позволяет задавать и просматривать пороговое значение мощности розетки, близкое к перегрузке.

Значение	Описание
all	Все розетки устройства.
<outlet name>	Имя, заданное для определенной розетки. (См. раздел olName).
<outlet#>	Отдельный номер или диапазон номеров, задаваемый с помощью дефиса, или список значений номеров отдельных розеток и диапазонов номеров, разделяемых запятыми.
<power>	Новое пороговое значение розетки (Вт).

Пример 1: Для просмотра порогового значения мощности, близкой к перегрузке, для розеток 3 и с 5 по 7 введите:

```
cli> olNearOver 3,5-7
E000: Success
3: BobbysServer: 5 W
5: BillysServer: 6 W
6: JoesServer: 5 W
7: JacksServer: 4 W
```

Пример 2: Для задания порогового значения мощности, близкой к перегрузке, для розеток 3 и с 5 по 7 на 6 ватт введите:

```
cli> olNearOver 3,5-7 6
E000: Success
3: BobbysServer: 6 W
5: BillysServer: 6 W
6: JoesServer: 6 W
7: JacksServer: 6 W
```

olOff

Доступ: Администратор, Пользователь устройства и Пользователь розетки, но только для розеток, назначенных данным пользователям.

Описание: Отключает розетку или группу розеток без задержки.

Значение	Описание
all	Все розетки устройства.
<outlet name>	Имя, заданное для определенной розетки. (См. раздел olName).
<outlet#>	Отдельный номер или диапазон номеров, задаваемый с помощью дефиса, или список значений номеров отдельных розеток и диапазонов номеров, разделяемых запятыми.

Пример 1: Чтобы отключить розетку 3 и розетки с 5 по 7, введите:

```
cli> olOff 3,5-7
E000: Success
```

olOffDelay

Доступ: Администратор, Пользователь устройства и Пользователь розетки, но только для розеток, назначенных данным пользователям.

Описание: Позволяет задавать и просматривать время задержки для команды отключения с задержкой Off Delayed (см. olDlyOff) и для команды повторного подключения с задержкой Reboot Delayed (см. olDlyReboot).

Значение	Описание
all	Все розетки устройства.
<имя розетки>	Имя, заданное для определенной розетки. (См. раздел olName).
<outlet#>	Отдельный номер или диапазон номеров, задаваемый с помощью дефиса, или список значений номеров отдельных розеток и диапазонов номеров, разделяемых запятыми.
<time>	Время задержки задается в диапазоне от 1 до 7200 секунд (2 часов).

Пример 1: Чтобы задать 9-секундную задержку отключения розеток 3 и с 5 по 7, введите:

```
cli> olOffDelay 3,5-7 9
E000: Success
```

Пример 2: Чтобы просмотреть значение задержек отключения, заданных командой Off Delayed, для розеток 3 и с 5 по 7, введите:

```
cli> olOffDelay 3,5-7
E000: Success
3: BobbysServer: 9 sec
5: BillysServer: 9 sec
6: JoesServer: 9 sec
7: JacksServer: 9 sec
```

olOn

Доступ: Администратор, Пользователь устройства и Пользователь розетки, но только для розеток, назначенных данным пользователям.

Описание: Включает розетку или группу розеток без задержки.

Значение	Описание
all	Все розетки устройства.
<outlet name>	Имя, заданное для определенной розетки. (См. раздел olName).
<outlet#>	Отдельный номер или диапазон номеров, задаваемый с помощью дефиса, или список значений номеров отдельных розеток и диапазонов номеров, разделяемых запятыми.

Пример 1: Чтобы включить розетку 3 и розетки с 5 по 7, введите:

```
cli> olOn 3,5-7
E000: Success
```

olOnDelay

Доступ: Администратор, Пользователь устройства и Пользователь розетки, но только для розеток, назначенных данным пользователям.

Описание: Позволяет задавать и просматривать время задержки для команды включения с задержкой On Delayed (см. olDlyOn) и для команды повторного подключения с задержкой Reboot Delayed (см. olDlyReboot).

Значение	Описание
all	Все розетки устройства.
<outlet name>	Имя, заданное для определенной розетки. (См. раздел olName).
<outlet#>	Отдельный номер или диапазон номеров, задаваемый с помощью дефиса, или список значений номеров отдельных розеток и диапазонов номеров, разделяемых запятыми.
<time>	Время задержки задается в диапазоне от 1 до 7200 секунд (2 часов).

Пример 1: Чтобы задать 6-секундную задержку включения розеток 3 и с 5 по 7, введите:

```
cli> olOnDelay 3,5-7 6
E000: Success
```

Пример 2: Чтобы просмотреть значение задержек включения, заданных командой On Delayed, для розеток 3 и с 5 по 7, введите:

```
cli> olOnDelay 3,5-7
E000: Success
3: BobbysServer: 6 sec
5: BillysServer: 6 sec
6: JoesServer: 6 sec
7: JacksServer: 6 sec
```

olOverLoad

Доступ: Администратор, Пользователь устройства и Пользователь розетки, но только для розеток, назначенных данным пользователям.

Описание: Позволяет задавать и просматривать пороговое значение мощности перегрузки розетки.

Значение	Описание
all	Все розетки устройства.
<outlet name>	Имя, заданное для определенной розетки. (См. раздел olName).
<outlet#>	Отдельный номер или диапазон номеров, задаваемый с помощью дефиса, или список значений номеров отдельных розеток и диапазонов номеров, разделяемых запятыми.
<powe>	Новое пороговое значение розетки (Вт).

Пример 1: Для просмотра порогового значения мощности перегрузки для розеток 3 и с 5 по 7 введите:

```
cli> olOverLoad 3,5-7
E000: Success
3: BobbysServer: 7 W
5: BillysServer: 8 W
6: JoesServer: 7 W
7: JacksServer: 6 W
```

Пример 2: Для задания порогового значения мощности перегрузки для розеток 3 и с 5 по 7 на 7 ватт введите:

```
cli> olOverLoad 3,5-7 7
E000: Success
3: BobbysServer: 7 W
5: BillysServer: 7 W
6: JoesServer: 7 W
7: JacksServer: 7 W
```

olRbootTime

Доступ: Администратор, Пользователь устройства и Пользователь розетки, но только для розеток, назначенных данным пользователям.

Описание: Позволяет задавать и просматривать величину интервала времени для команды Reboot Delayed, в течение которого розетка будет оставаться отключенной (см. olDlyReboot).

Пример 1: Чтобы увидеть интервалы времени, в течение которых розетка 3 и розетки с 5 по 7 будут оставаться отключенными в ходе переподключения, введите:

```
cli> olRbootTime 3,5-7
E000: Success
3: BobbysServer: 4 sec
5: BillysServer: 5 sec
6: JoesServer: 7 sec
7: JacksServer: 2 sec
```

Пример 2: Чтобы задать интервалы времени, в течение которых розетка 3 и розетки с 5 по 7 будут оставаться отключенными в ходе переподключения, введите:

```
cli> olRebootTime 3,5-7 10
E000: Success
3: BobbysServer: 10 sec
5: BillysServer: 10 sec
6: JoesServer: 10 sec
7: JacksServer: 10 sec
```

olReading

Доступ: Администратор, Пользователь устройства и Пользователь розетки, но только для розеток, назначенных данным пользователям.

Описание: Позволяет просматривать значения силы тока, мощности и потребляемой энергии одной розетки или группы розеток.

Значение	Описание
all	Все розетки устройства.
<outlet name>	Имя, заданное для определенной розетки. (См. раздел olName).
<outlet#>	Отдельный номер или диапазон номеров, задаваемый с помощью дефиса, или список значений номеров отдельных розеток и диапазонов номеров, разделяемых запятыми.
current | power | energy	Новое пороговое значение розетки (Вт).

Пример 1: Для просмотра значения силы тока для розеток 3 и с 5 по 7 введите:

```
cli> olReading 3,5-7 current
E000: Success
3: BobbysServer: 4 A
5: BillysServer: 5 A
6: JoesServer: 7 A
7: JacksServer: 2 A
```

Пример 2: Чтобы просмотреть мощность для розетки 3, введите:

```
cli> olReading 3 power
E000: Success
3: BobbysServer: 40 W
```

Пример 3: Чтобы просмотреть потребляемую энергию для розетки JoesServer, введите:

```
cli> olReading joesserver energy
E000: Success
6: JoesServer: 7.3 kWh
```

olReboot

Доступ: Администратор, Пользователь устройства и Пользователь розетки, но только для розеток, назначенных данным пользователям.

Описание: Переподключает питание розетки или группы розеток без задержки. Если задано более одной розетки, то все указанные розетки будут повторно подключены одновременно.

Значение	Описание
all	Все розетки устройства.
<outlet name>	Имя, заданное для определенной розетки. (См. раздел olName).
<outlet#>	Отдельный номер или диапазон номеров, задаваемый с помощью дефиса, или список значений номеров отдельных розеток и диапазонов номеров, разделяемых запятыми.

Пример: Чтобы переподключить розетку 3 и розетки с 5 по 7, введите:

```
cli> olReboot 3,5-7
E000: Success
```

olStatus

Доступ: Администратор, Пользователь устройства и Пользователь розетки, но только для розеток, назначенных данным пользователям.

Описание: Позволяет просматривать статус указанных розеток.

Значение	Описание
all	Все розетки устройства.
<outlet name>	Имя, заданное для определенной розетки. (См. раздел olName).
<outlet#>	Отдельный номер или диапазон номеров, задаваемый с помощью дефиса, или список значений номеров отдельных розеток и диапазонов номеров, разделяемых запятыми.

Пример: Для просмотра состояния розеток 3 и с 5 по 7 введите:

```
cli> olStatus 3,5-7
E000: Success
3: BobbysServer: On
5: BillysServer: Off
6: JoesServer: Off
7: JacksServer: On
```

olUnasgnUsr

Доступ: Администратор

Описание: Отключает управление розетками для пользователя, имеющегося в локальной базе данных.

Значение	Описание
all	Все розетки устройства.
<outlet name>	Имя, заданное для определенной розетки. (См. раздел olName).
<outlet#>	Отдельный номер или диапазон номеров, задаваемый с помощью дефиса, или список значений номеров отдельных розеток и диапазонов номеров, разделяемых запятыми.
<user>	Пользователь, имеющийся в локальной базе данных. (См. раздел userList).

Пример 1: Чтобы отключить пользователя по имени Бобби от управления розетки 3 и розеток с 5 по 7 и 10, введите:

```
cli> olUnasgnUsr 3,5-7,10 bobby
E000: Success
```

Пример 2: Чтобы отключить пользователя по имени Билли от управления всеми розетками, введите:

```
cli> olUnasgnUsr all billy
E000: Success
```

phLowLoad

Доступ: Администратор, Пользователь устройства.

Описание: Задание или просмотр нижнего порога мощности по фазам в киловаттах. Чтобы выбрать фазу, укажите одно из следующих значений. Введите: **все**, одна фаза, диапазон или перечень фаз через запятую.

Пример 1: Чтобы задать пороговое нижнее значение нагрузки для всех фаз равным 1 кВт, введите:

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

Пример 2: Чтобы просмотреть пороговое нижнее значение нагрузки для фаз 1 - 3, введите:

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

phNearOver

Доступ: Администратор, Пользователь устройства.

Описание: Задание или просмотр порога мощности фазы, близкого к перегрузке, в киловаттах. Чтобы выбрать фазу, укажите одно из следующих значений. Введите: **все**, одна фаза, диапазон или перечень фаз через запятую.

Пример 1: Чтобы задать близкое к перегрузке пороговое значение мощности для всех фаз равным 10 кВт, введите:

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

Пример 2: Чтобы просмотреть близкое к перегрузке пороговое значение для фаз 1 – 3, введите:

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

phOverLoad

Доступ: Администратор, Пользователь устройства.

Описание: Задание или просмотр порога перегрузки в киловаттах. Чтобы выбрать фазу, укажите одно из следующих значений. Введите: **все**, одна фаза, диапазон или перечень фаз через запятую.

Пример 1: Чтобы задать пороговое значение перегрузки для всех фаз равным 13 кВт, введите:

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

Пример 2: Чтобы просмотреть пороговое значение перегрузки для фаз 1 – 3, введите:

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

phReading

Доступ: Администратор, Пользователь устройства.

Описание: Просмотр значений тока, напряжения и мощности по фазам. Задание или просмотр порога мощности фазы, близкого к перегрузке, в киловаттах. Чтобы выбрать фазу, укажите одно из следующих значений. Введите: **все**, одна фаза, диапазон или перечень фаз через запятую.

Пример 1: Чтобы просмотреть измерения тока в фазе 3, введите:

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

Пример 2: Чтобы увидеть значения напряжения в каждой фазе, введите:

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

Пример 3: Чтобы увидеть значения мощности в фазе 2, введите:

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

phRestrictn

Доступ: Администратор

Описание: Позволяет задавать и просматривать параметры ограничения перегрузок для предотвращения включения розеток в момент нарушения порога перегрузки. Допустимые аргументы: **нет**, **возле порога** и **свыше порога**. Чтобы выбрать фазу, укажите одно из следующих значений. Введите: **все**, одна фаза, диапазон или перечень фаз через запятую.

Пример 1: Чтобы задать ограничение перегрузки для фазы номер 3 равным нулю, введите:

```
cli> phRestrictn 3 none
E000: Success
```

Пример 2: Чтобы просмотреть ограничения перегрузки для всех фаз, введите:

```
cli> phRestrictn all
E000: Success
1: over
2: near
3: none
```

prodInfo

Доступ: Администратор, Пользователь устройства, Пользователь розетки

Описание: Просмотр информации о Rack PDU.

Пример:

```
cli> prodInfo
E000: Success
AOS vX.X.X.X

Managed Rack PDU vX.X.X.X
Model:              DELL6xxx
Present Outlets:    12
Switched Outlets:   12
Metered Outlets:    0
Max Current:        20 A
Phases:             1
```

sensorName

Доступ: Администратор, Пользователь устройства

Описание: Позволяет задавать и просматривать имена, присвоенные разъему датчиков температуры и влажности устройства Rack PDU.

Пример 1: Чтобы задать разъему имя «Sensor1», введите:

```
cli> sensorName Sensor1
E000: Success
```

Пример 2: Чтобы впоследствии просмотреть имя разъема датчиков, введите:

```
cli> sensorName
E000: Success
Sensor1
```

tempHigh

Доступ: Администратор, Пользователь устройства

Описание: Задание или просмотр порога верхнего значения температуры в градусах Фаренгейта или Цельсия.

Пример 1: Чтобы задать порог верхнего значения температуры равным 70 по шкале Фаренгейта, введите:

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

Пример 2: Чтобы посмотреть верхний температурный предел в градусах Цельсия, введите:

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

Пример 3: Чтобы посмотреть верхний температурный предел в градусах Фаренгейта, введите:

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

tempMax

Доступ: Администратор, Пользователь устройства

Описание: Задание или просмотр порога максимального значения температуры в градусах Фаренгейта или Цельсия.

Пример 1: Чтобы задать порог максимального значения температуры равным 80 по шкале Фаренгейта, введите:

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

Пример 2: Чтобы посмотреть максимальный температурный предел в градусах Цельсия, введите:

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

Пример 3: Чтобы посмотреть максимальный температурный предел в градусах Фаренгейта, введите:

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

tempReading

Доступ: Администратор, Пользователь устройства, Пользователь розетки.

Описание: Просмотр значения температуры на датчике в градусах Фаренгейта или Цельсия.

Пример: Чтобы посмотреть значение температуры в градусах Фаренгейта, введите:

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

userAdd

Доступ: Администратор

Описание: Позволяет добавлять пользователя в локальную базу пользователей.

Пример: Чтобы добавить пользователя по имени Бобби, введите:

```
cli> userAdd Bobby
E000: Success
```

userDelete

Доступ: Администратор

Описание: Позволяет удалять пользователя из локальной базы пользователей.

Пример: Чтобы удалить пользователя по имени Бобби, введите:

```
cli> userDelete Bobby
E000: Success
```

userList

Доступ: Администратор, Пользователь устройства и Пользователь розетки, но только для розеток, назначенных данным пользователям.

Описание: Позволяет просматривать перечень пользователей и розетки, назначенные им.

Пример 1: При загрузке с правами администратора введите:

```
cli> userList
E000: Success
Local: admin: 1,2,3,4,5,6,7,8
Local: Bobby: 1,3
Local: Billy: 2,5
Local: Joe: 4,6
Local: Jack: 7,8
```

Пример 2: При загрузке под учетной записью Билли введите:

```
cli> userList
E000: Success
Local: Billy: 2,5
```

userPasswd

Доступ: Администратор.

Описание: Позволяет задавать пароль Пользователя розетки.

Пример: Чтобы задать пароль пользователя Бобби «abc123», введите:

```
cli> userPasswd Bobby abc123 abc123
E000: Success
```

whoami

Доступ: Администратор, Пользователь устройства, Пользователь розетки

Описание: Просмотр имени активного пользователя.

Пример:

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

Веб-интерфейс

Поддерживаемые интернет-обозреватели

Для доступа к Rack PDU через веб-интерфейс можно использовать браузер Microsoft® Internet Explorer® (IE) версии 7.x или выше (только для операционных систем Windows®) или Mozilla® Firefox® версии 3.0.6 или выше (для всех операционных систем). Другие популярные браузеры также могут использоваться, но они не прошли полную проверку.

Rack PDU не работает с прокси-сервером. Перед тем как использовать интернет-обозреватель для доступа к веб-интерфейсу Rack PDU, необходимо выполнить следующее:

- Сконфигурируйте интернет-обозреватель, чтобы отключить функцию использования прокси-сервера для Rack PDU.
- Сконфигурируйте прокси-сервер таким образом, чтобы он не работал по указанному IP-адресу Rack PDU.

Вход в веб-интерфейс

Обзор

Можно использовать доменное имя DNS или системный IP-адрес Rack PDU для адреса URL веб-интерфейса. Для входа в систему используйте имя пользователя и пароль, зависящие от регистра. Имя пользователя по умолчанию и пароль зависит от типа учетной записи:

- **admin/admin** для Администратора
- **device/device** для Пользователя устройства
- **readonly/readonly** для Пользователя, имеющего доступ только для чтения

Для учетной записи Пользователя розетки нет имени пользователя и пароля по умолчанию. Имя пользователя, пароль и другие характеристики учетной записи Пользователя розетки должен задать администратор. См. Конфигурация пользователя розетки.

Если в качестве протокола доступа используется HTTPS (SSL/TLS), то реквизиты доступа сравниваются с информацией в сертификате сервера. Если этот сертификат был создан с помощью программы-мастера Security Wizard, а IP-адрес был определен в сертификате как общее имя, вы должны использовать IP-адрес для входа в Rack PDU. Если в сертификате в качестве общего имени было указано DNS-имя, вы должны использовать для входа в систему DNS-имя.

Информацию о веб-странице, появляющейся при входе в веб-интерфейс, см. в разделе О вкладке «Home» (Начало).

Форматы URL-адресов

Введите имя DNS или IP-адрес Rack PDU в строке URL-адреса интернет-обозревателя и нажмите ENTER. Если в браузере Internet Explorer указывается порт сервера не по умолчанию, то в URL необходимо добавить **`http://`** или **`https://`**.

Наиболее распространенные сообщения об ошибках браузера при входе в систему.

Сообщение об ошибке	Причина ошибки	Веб-обозреватель
«У вас нет прав для просмотра этой страницы» или «Кто-то в данный момент вошел в систему...»	Кто-то другой зашел в систему	Internet Explorer, Firefox
«Невозможно отобразить данную страницу».	Доступ к веб-странице запрещен или адрес URL указан неправильно	Internet Explorer
«Подключение невозможно».		Firefox

Примеры формата URL-адреса.

- Для DNS-имени Web1:
  - **`http://Web1`**, если HTTP является вашим режимом доступа.
  - **`https://Web1`**, если HTTPS является вашим режимом доступа.
- Для системного IP-адреса 139.225.6.133 и порта сервера веб-сайта (80):
  - **`http://139.225.6.133`**, если HTTP является вашим режимом доступа.
  - **`https//139.225.6.133`**, если HTTPS (HTTP с SSL) является вашим режимом доступа.
- Для системного IP-адреса 139.225.6.133 и порта сервера веб-сайта не по умолчанию (5000):
  - **`http://139.225.6.133:5000`**, если HTTP является вашим режимом доступа.
  - **`https://139.225.6.133:5000`**, если HTTPS (HTTP с SSL) является вашим режимом доступа.
- Для системного IPv6-адреса 2001:db8:1::2c0:b7ff:fe00:1100 и порта сервера веб-сайта не по умолчанию (5000):
  - **`http://[2001:db8:1::2c0:b7ff:fe00:1100]:5000`**, если HTTP является вашим режимом доступа.

Функции веб-интерфейса

Для ознакомления с основными функциями веб-интерфейса Rack PDU, прочтите следующее.

Вкладки

Имеются следующие вкладки:

- **Home (Начало)**: Появляется при входе в систему. На ней отображаются активные сигналы, статус загрузки и самые последние события Rack PDU. Для получения дополнительных сведений см. О вкладке «Home» (Начало).
- **Device Manager** (Диспетчер устройств): Просмотр информации о статусе нагрузки, конфигурирование порогов нагрузки, просмотр и управление измерением пиковой нагрузки на всех подсоединенных устройствах, фазах и розетках, если применимо. Контроль и управление розетками. Для получения дополнительных сведений см. О вкладке «Device Manager» (Менеджер устройств).
- **Environment (Окружающая среда)**: Просмотр данных датчика температуры и влажности, если датчик подключен к **Rack PDU**.
- **Logs** (Журналы): Журналы регистрации событий, данных и системные журналы.
- **Administration** (Администрирование): Настройка безопасности, связи в сети, уведомления и общих параметров.

Значки состояния устройства

Один или более значков вместе с сопроводительным текстом указывают на текущее рабочее состояние Rack PDU:

	**Critical** (Критический): Критический аварийный сигнал, требующий немедленных действий.
	**Warning** (Внимание): Состояние тревоги требует внимания и может подвергнуть опасности данные или оборудование, если такового внимания уделено не будет.
	**No Alarms** (Сигналов тревоги нет): Сигналов тревоги нет, Rack PDU работает нормально.

В верхнем правом углу каждой страницы веб-интерфейса отображаются те же значки, которые отображаются на странице «Home» (Начало) с сообщениями о состоянии Rack PDU:

- Значок **Нет сигналов тревоги** указывает на отсутствие аварийной ситуации.
- Один или оба других значка (**Critical** и **Warning**) указывают на наличие аварийной ситуации, после каждого значка указывается количество активных аварийных сигналов данного уровня серьезности.

Чтобы вернуться к вкладке **Home** (Начало) для просмотра краткого сообщения о состоянии Rack PDU, включая активные аварийные сигналы, нажмите на значок состояния на любой странице интерфейса.

Быстрые ссылки

В нижней части экрана, слева, находятся три конфигурируемые ссылки. Значения по умолчанию следующие:

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

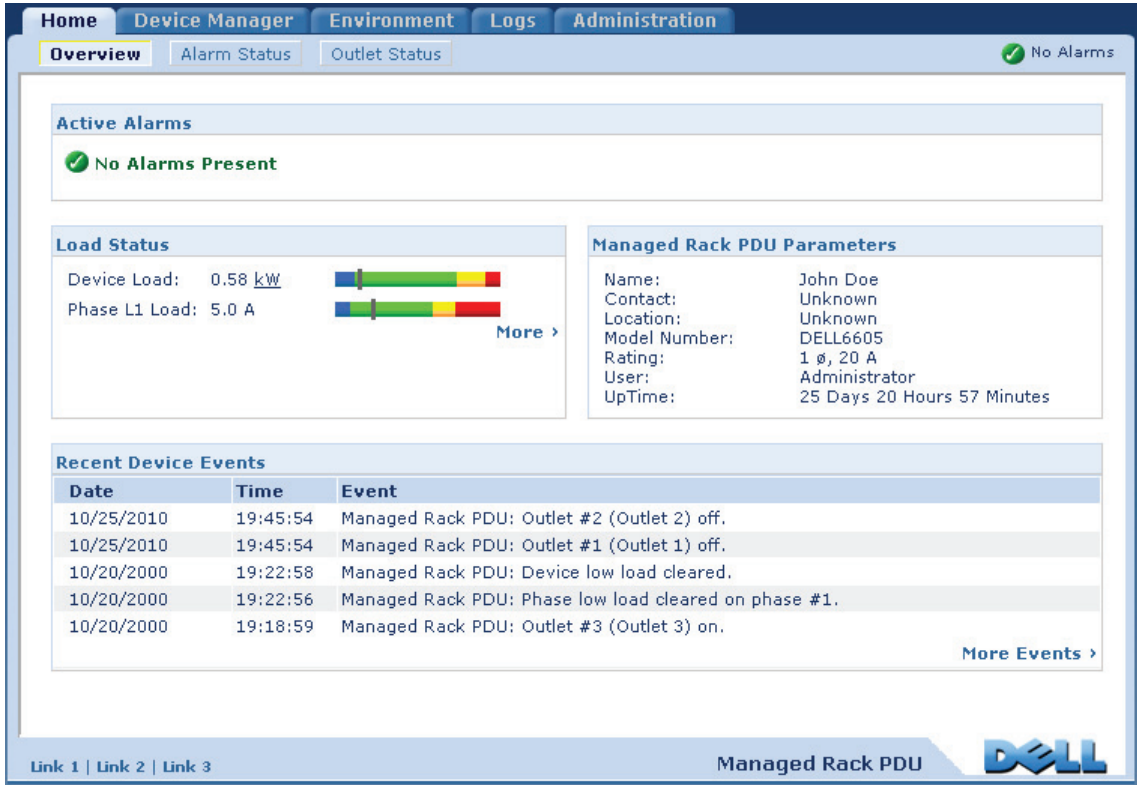
Перенастройка этих ссылок описана в разделе Конфигурирование связей.

Другие функции веб-интерфейса

- В левом верхнем углу показан IP-адрес.
- Ссылка на контекстную справку **Help** и ссылка **Log off** (Выйти) расположены в правом верхнем углу.

О вкладке «Home» (Начало)

На вкладке «Home» (Начало) отображаются активные сигналы тревоги, статус нагрузки Rack PDU и последние события на Rack PDU.

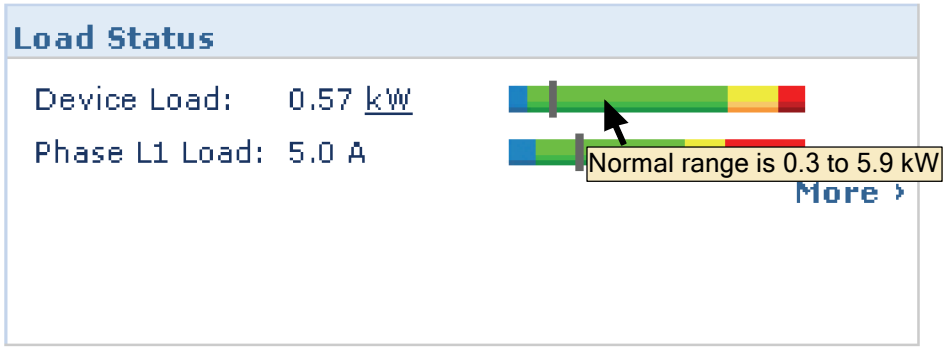


Окно «Overview» (Обзор)

Путь: Home > Overview

В верхней части окна «Overview» (обзор) показано состояние сигнализации. Если действуют одно или несколько условий сигнализации, их номер и тип отображается вместе со ссылкой на окно **Alarm Status** (Состояние сигналов), в котором вы можете увидеть описание каждого из сигналов. Если предупреждающие сигналы отсутствуют, на экране обзора будет сообщение: «No Alarms Present» (Сигналов тревоги нет).

В зоне **Load Status** (Состояние нагрузки) отображается нагрузка на устройстве в кВт и по фазам в А, если это применимо. Зелено-желто-красный индикатор показывает текущее состояние нагрузки: нормальное, близкое к перегрузке или перегрузку. Помните, что при сконфигурированном нижнем пороге индикатор также будет отображать синий сегмент рядом с зеленым. Наведите курсор на цветовые сегменты для просмотра сконфигурированных порогов нагрузки.



Щелкните **More** (Еще), чтобы перейти на вкладку **Device Manager** (Диспетчер устройств), с помощью которой можно конфигурировать пороги сигнализации, а также просматривать и обрабатывать информацию о пиковых нагрузках.

В области параметров устройства можно просмотреть имя, контактную информацию, местоположение, текущий рейтинг, тип учетной записи пользователя, входящего в систему Rack PDU, и время, в течение которого устройство работало с последней перезагрузки цикла питания или перезагрузки интерфейса управления. (Для получения дополнительных сведений см. Восстановление настроек Rack PDU.)

В зоне **Recent Device Events** (Последние события устройства) показаны в обратном хронологическом порядке недавно произошедшие события и время и дата, когда они произошли. Одновременно показывается не более пяти событий. Щелкните **More Events** (Больше событий), чтобы перейти на вкладку **Logs** (Журналы) и увидеть весь журнал регистрации событий.

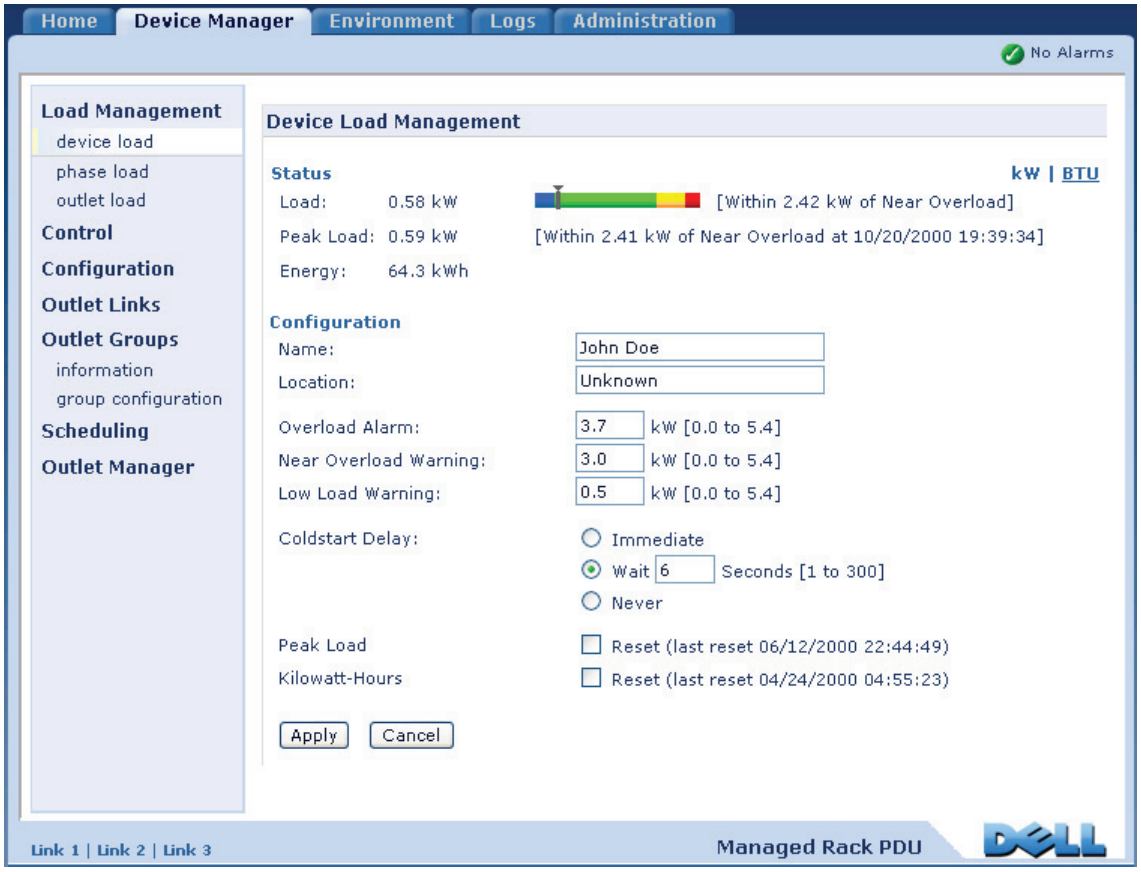
Экран состояния предупреждающих сигналов

Путь: Home > Alarm Status

Экран **Alarm Status** (Состояние сигналов) дает описание всех установленных предупреждающих сигналов.

Подробней о нарушении пороговых значений температуры или влажности – см. вкладку «Environment» (Окружающая среда).

Управление устройством



О вкладке «Device Manager» (Менеджер устройств)

Путь: Device Manager

Используйте вкладку **Device Manager** (Менеджер устройств) для:

- Просмотра состояния нагрузки Rack PDU
- Конфигурации порогов нагрузки для всех указанных подключенных устройств и фаз
- Управления и контроля розеток
- Конфигурации имени и местоположения для Rack PDU
- Просмотра и управления пиковыми нагрузками
- Щелкните ссылки пользовательских конфигураций, чтобы открыть веб-страницы для устройств, подключенных к Rack PDU

Просмотр информации о статусе нагрузки и пиковой нагрузке

Путь: Device Manager > *Load Management options*

Индикатор, светящийся зеленым, желтым и красным, отображают текущее состояние нагрузки: нормальное, близкое к перегрузке или перегрузку. Если сконфигурирован порог нагрузки, индикатор будет отображать еще и голубой сегмент слева от зеленого. При отображении **Device Load** (Нагрузка устройства) треугольник над измерителем показывает пиковую нагрузку.

Щелкните **kW | BTU** в правом верхнем углу для переключения отображаемых значений в киловаттах или британских тепловых единицах (BTU).

Конфигурация порогов нагрузки

Путь: Device Manager > *Load Management options*

Чтобы настроить пороги нагрузки:

1. Щелкните вкладку **Device Manager** (Менеджер устройств).
2. Для конфигурации пороговых значений нагрузки для устройств или фаз выберите соответствующий пункт в меню «Load Management» (Управление нагрузкой).
3. Задайте пороги **перегрузки**, **предупреждения о перегрузке** и **низкой нагрузки**.
4. Нажмите **Apply** (Применить).

Конфигурация имени и местоположения Rack PDU

Путь: Device Manager > Load Management > Device Load

Имя и местоположение, введенное на вкладке **Home** (Начало).

Имя и местоположение можно задать как с помощью вкладки «Device Manager» (Менеджер устройств), так и с помощью вкладки «Administration» (Администрирование). Изменение параметров на одной вкладке приведет к изменению на другой.

1. Выберите вкладку **Device Manager** (Менеджер устройств), после чего выберите пункт **device load** (нагрузка устройства) в меню **Load Management** (Управление нагрузкой).
2. Введите имя и местоположение.
3. Нажмите **Apply** (Применить).

Задание задержки холодного пуска

Путь: Device Manager > Device Load

Задержка холодного пуска является значением времени в секундах, прибавляемом к каждому значению задержки подачи питания «Power On Delay» для каждой розетки после подачи питания на Rack PDU. Допустимые значения – от 1 до 300 секунд, **Immediate** (Немедленно) или **Never** (Не включать).

1. Выберите вкладку **Device Manager** (Менеджер устройств), после чего выберите пункт **device load** (нагрузка устройства) в меню **Load Management** (Управление нагрузкой).
2. Выберите величину **Coldstart Delay** (Задержка холодного пуска).
3. Нажмите **Apply** (Применить).

Сброс пиковой нагрузки и кВт-ч

Путь: Device Manager > Device Load

1. Выберите вкладку **Device Manager** (Менеджер устройств), после чего выберите пункт **device load** (нагрузка устройства) в меню **Load Management** (Управление нагрузкой).
2. Установите флажки **Peak Load** (Пиковая нагрузка) и **Kilowatt-Hours** (Киловатт-часы), по желанию.
3. Нажмите **Apply** (Применить).

Настройка и управление группами розеток

Терминология «группа розеток»

Группа розеток состоит из розеток, которые логически связаны друг с другом в одном устройстве Rack PDU. Розетки, находящиеся в группе, включаются, отключаются и переподключаются синхронно:

- *Локальная группа розеток* состоит из двух или более розеток в устройстве Rack PDU. Будут синхронизированы розетки только в этой группе.
- *Группа глобальных розеток* состоит из двух или более розеток в устройстве Rack PDU. Одна розетка конфигурируется как *глобальная,* которая логически связывает группу розеток с группами розеток, расположенных на других устройствах Rack PDU, число которых может доходить до трех. Все розетки в связанных группах глобальных розеток синхронизированы.
  - В случае групп глобальных розеток *группа-инициатор* является группой, которая инициировала действие.
  - В случае групп глобальных розеток *группой-последователем* называется любая другая группа розеток, синхронизированная с группой-инициатором.

В случае применения управляющего воздействия к розеткам, являющихся членами группы, их синхронизация будет осуществляться следующим образом:

- В случае группы глобальных розеток используются периоды задержки и продолжительности перезагрузки, заданные для глобальной розетки из группы-инициатора.
- В случае группы локальных розеток будут применены периоды задержки и продолжительности перезагрузки розетки, имеющей самый маленький номер в группе.

Назначение и преимущества групп розеток

Используя группы синхронизированных розеток устройства Rack PDU, вы можете быть уверены, что все розетки включаются, отключаются и перезагружаются синхронно. Управляющие действия на синхронизированной группе розеток имеют следующие преимущества.

- Синхронное отключение и включение источников питания серверов с двумя шнурами питания предотвращает появление сообщения об ошибке подачи питания при запланированном отключении и перезагрузке системы.
- Синхронизация розеток с помощью групп обеспечивает более точное время отключения и перезапуска, чем в случае использования периодов задержки отдельных розеток.
- Глобальная розетка отображается на пользовательских интерфейсах всех устройств Rack PDU, с которыми она связана.

Системные требования для групп розеток

Для того, чтобы создать и использовать группы синхронизированных розеток:

- Необходимо иметь сеть 10/100Base-T TCP/IP с концентратором или маршрутизатором Ethernet, которые используют источник питания, не зависящий от синхронизируемых компьютеров и других устройств.
- Если необходимо синхронизировать группы розеток различных устройств Rack PDU, эти устройства Rack PDU должны соответствовать следующим требованиям:
  - Они должны принадлежать одной подсети.
  - Они должны использовать микропрограммное обеспечение, имеющее одинаковый номер версии модуля операционной системы (AOS) и модуля приложений.
- Необходимо иметь компьютер, который может инициировать синхронизированные операции управления через веб-интерфейс или интерфейс командной строки Rack PDU или через SNMP.
- Группы синхронизированных розеток должны иметь одинаковый Multicast IP-адрес. Проверьте, чтобы все коммутаторы Ethernet, подключенные к устройствам Rack PDU, обеспечивали передачу данных по сети Multicast для этого IP-адреса.

Правила конфигурации групп розеток

Для системы, использующей группы розеток, применимы следующие правила:

- Устройство Rack PDU может использовать более одной группы розеток, но розетка должна относиться только к одной группе розеток.
- Группа локальных розеток, не имеющая глобальных розеток, должна содержать две и более розеток.
- Можно синхронизировать группу глобальных розеток устройства Rack PDU с группой глобальных розеток на любом из трех других устройств Rack PDU.
  - В группе глобальных розеток можно назначить только одну розетку, которая будет связана с группами розеток других Rack PDU с целью синхронизации. Эта глобальная розетка может быть единственной розеткой в этой группе, эта же группа может состоять из нескольких розеток.
  - Чтобы связать группы розеток устройства Rack PDU для синхронизации, эти устройства Rack PDU должны иметь одинаковое имя Multicast (Device Multicast Name) и адрес Multicast (Device Multicast Address) и использовать одинаковую версию микропрограммного обеспечения Rack PDU.
  - Глобальная розетка одной группы должна иметь тот же физический номер, что и глобальная розетка в любой другой группе розеток, с которой связана эта группа.
- Чтобы создать и сконфигурировать группу розеток, необходимо использовать веб-интерфейс или экспортировать настройки из файла конфигурации (.ini-файла) конфигурируемого Rack PDU. Интерфейс командной строки позволяет увидеть, является ли розетка членом группы розеток, и позволяет применять управляющие действия к группе розеток, но не позволяет задавать или конфигурировать группу розеток.

Включение групп розеток

Выберите вкладку **Device Manager** (Менеджер устройств) и выберите пункт **Group Configuration** (Конфигурация группы) в меню **Outlet Groups** (Группы розеток). Сконфигурируйте требуемые параметры и нажмите **Apply** (Применить).

Разрешение создания групп розеток.

Параметр	Описание
Device Level Outlet Group (Группа розеток уровня устройств)	Чтобы создать группу розеток, необходимо задать этот параметр. По умолчанию этот параметр отключен.

Enable support for global outlet groups (linked groups). (Включение поддержки групп глобальных розеток (связанных групп).).

Параметр	Описание
Multicast Name (Имя Multicast)	Чтобы связать группы розеток на нескольких устройствах Rack PDU, необходимо указать одинаковое имя и IP-адрес Multicast на каждом из устройств Rack PDU. **ПРИМЕЧАНИЕ:** Может быть сконфигурировано до четырех устройств, имеющих одинаковые имя и IP-адрес Multicast.
Multicast IP (IP-адрес Multicast)	

Включение шифрования и авторизации групп розеток.

Параметр	Описание
Authentication Phrase (Фраза аутентификации)	Фраза, содержащая от 15 до 32 ASCII-символов, которая подтверждает, что устройство обменивается данными с другими устройствами, что это устройство не было изменено в процессе передачи, и что это сообщение было передано своевременно. Фраза аутентификации показывает, что она была передана без задержки и не была скопирована и не передана снова в неподходящее время.
Encryption Phrase (Фраза шифрования)	Фраза, содержащая от 15 до 32 ASCII-символов, которая обеспечивает приватность передаваемых данных (путем шифрования).

Настройка порта группы розеток.

Параметр	Описание
Outlet Group Port (Порт группы розеток)	Номер порта, с помощью которого устройство будет обмениваться данными с другими устройствами.

Устройства, синхронизируемые с группами розеток на других устройствах, должны иметь одинаковую фразу аутентификации, фразу шифрования и номер порта группы. Эти значения скрыты от пользователя.

Создание группы локальных розеток

1. Выберите вкладку **Device Manager** (Менеджер устройств) и выберите пункт **Information** (Информация) в меню **Outlet Groups** (Группы розеток).
2. Проверьте, чтобы группы розеток были включены. (См. раздел Включение групп розеток).
3. Выберите **Create Local Outlet Group** (Создать группу локальных розеток).
4. В пункте **Select Local Outlets** (Выбор локальных розеток) выберите все розетки, которые будут входить в группу, и присвойте этой группе имя в поле **Outlet Group Name** (Имя группы розеток). Нужно выбрать, по крайней мере, две розетки.

Создание нескольких групп глобальных розеток

Чтобы создать несколько групп глобальных розеток, которые будут связаны с группами розеток других устройств Rack PDU:

1. Выберите вкладку **Device Manager** (Менеджер устройств) и выберите пункт **Information** (Информация) в меню **Outlet Groups** (Группы розеток).
2. Убедитесь, что группы розеток включены, и что параметры Multicast (имя и IP-адрес) одинаковы для всех связанных устройств Rack PDU. (См. раздел Включение групп розеток.)
3. Выберите **Создать группу глобальных розеток**.
4. Для каждой создаваемой группы глобальных розеток выберите розетки, поставив соответствующий флажок. Затем нажмите **Apply** (Применить). Например, выберите пять розеток, чтобы создать пять групп розеток, каждая из которых содержит одну глобальную розетку.
5. О том, как добавить розетки в любую из созданных групп глобальных розеток, см. Правка и удаление группы розеток.

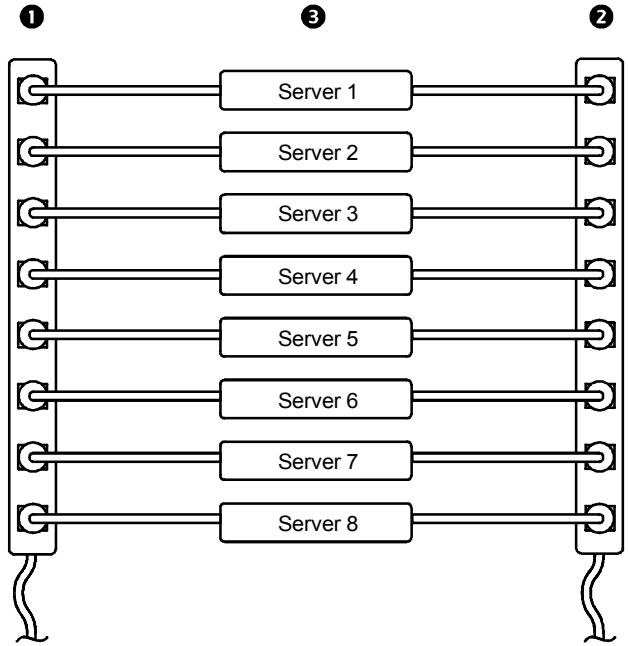
Правка и удаление группы розеток

1. Выберите вкладку **Device Manager** (Менеджер устройств) и выберите пункт **Information** (Информация) в меню **Outlet Groups** (Группы розеток).
2. В пункте **Configured Outlet Groups** (Сконфигурированные группы розеток) выберите номер или имя редактируемой или удаляемой группы розеток.
3. При редактировании группы розеток можно делать следующее:
   - Переименовать группу розеток.
   - Добавить или удалить розетки, поставив или убрав соответствующий флажок, отмечающий эти розетки.

   Нельзя удалить розетку из группы, которая содержит только две розетки, если только остающаяся розетка не является глобальной.
4. Чтобы удалить группу розеток, выберите пункт **Delete Outlet Group** (Удалить группу розеток).

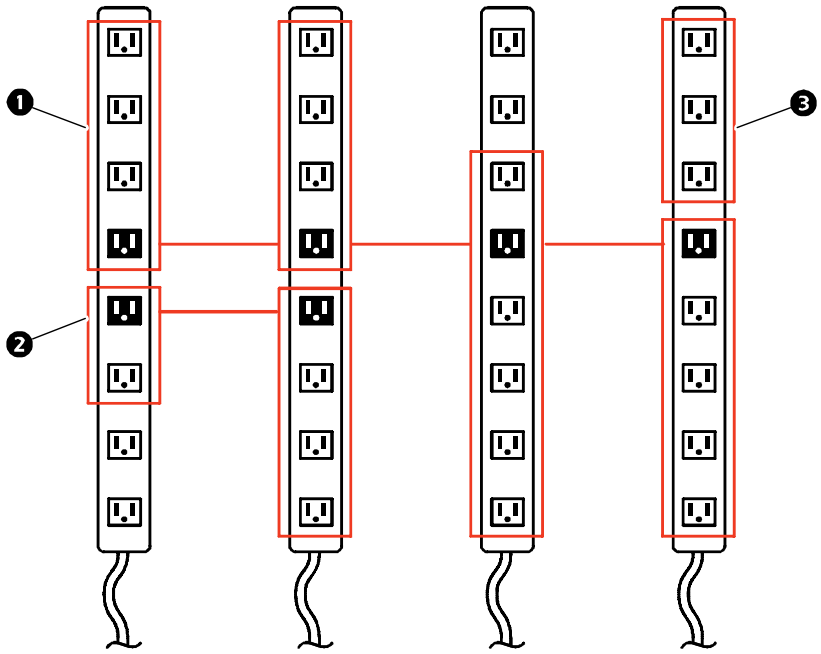
Типовые конфигурации группы розеток

Приведенные ниже конфигурации имеют два устройства Rack PDU, каждое из которых содержит восемь групп розеток. Каждая группа розеток содержит одну глобальную розетку. Каждая группа розеток ❶ первого устройства Rack PDU связана с группой розеток ❷ с тем же местоположением на втором устройстве Rack PDU. Один шнур питания двухшнурового сервера ❸ подключен к розетке первого устройства Rack PDU, его другой шнур подключен к соответствующей розетке второго устройства Rack PDU, что гарантирует, что напряжение питания, подаваемое на сервер от обоих источников, будет включаться и отключаться синхронно, по управляющему воздействию розеток.



Данная конфигурация показывает три набора синхронизированных розеток. Глобальные розетки показаны черным. Группы розеток заключены в красные рамки.

❶	Показанные четыре группы глобальных розеток синхронизируют в общей сложности 19 розеток.
❷	Две группы глобальных розеток синхронизируют 6 розеток, 2 в одной группе и 4 – в другой.
❸	Эта группа локальных розеток синхронизирует 3 розетки в одном устройстве Rack PDU.



Проверка настроек и конфигурации для групп глобальных розеток

Чтобы убедиться, что настройки соответствуют всем системным требованиям для групп розеток, и что группы розеток сконфигурированы правильно, выберите пункт **Information** (Информация) в пункте **Outlet Groups** (Группы розеток) навигационного меню, расположенного в левой части веб-интерфейса, чтобы просмотреть группы и их подключения:

- Раздел **Configured Outlet Groups** (Сконфигурированные группы розеток) отображает следующее:
  - Все сконфигурированные группы розеток на данном Rack PDU.
  - Розетки в каждой группе по номеру розетки.
  - Все группы розеток на других устройствах Rack PDU, с которыми синхронизирована группа глобальных розеток. Каждое устройство Rack PDU идентифицируется по IP-адресу, все глобальные розетки показаны полужирным шрифтом.
- Раздел **Global Outlet Overview** (Обзор глобальных розеток) отображает следующее:
  - IP-адрес текущего устройства Rack PDU.
  - IP-адрес любого устройства Rack PDU, которое содержит глобальные розетки, синхронизируемые с группами розеток на других устройствах Rack PDU.
  - Все глобальные розетки, сконфигурированные на Rack PDU, независимо от того, синхронизированы они с группами розеток на данном Rack PDU или нет.

Настройки для розеток и групп розеток

Инициация управляющего действия

Если управляющее действие приложено к розеткам или группам розеток, то для этого действия будут применены следующие задержки:

- В случае отдельной розетки (не входящей в состав группы розетки) действие будет использовать периоды задержек и продолжительности перезагрузки, заданные для данной розетки.
- В случае группы глобальных розеток действие будет использовать периоды задержки и продолжительности перезагрузки, заданные для глобальной розетки.
- В случае группы локальных розеток действие будет использовать периоды задержки для розетки, имеющей самый маленький номер в группе.

Для того, чтобы управлять розетками на устройстве Rack PDU:

1. Выберите вкладку **Device Manager** (Менеджер устройств) и выберите пункт **Control** (Управление) в меню навигации в левой части экрана.
2. Поставьте флажки возле отдельных розеток или групп розеток, которыми собираетесь управлять, или поставьте флажок **All Outlets** (Все розетки).
3. Выберите **Control Action** (Управляющее действие) из списка, после чего нажмите **Next>>** (Далее). На странице подтверждения, которая объясняет выбранное действие, укажите, применять или не применять это действие.

Допустимые управляющие действия.

Параметр	Описание
No Action (Web interface only) (Нет действия (только веб-интерфейс))	Нет действия.
On Immediate (Включить немедленно)	Подает питание на выбранные розетки.
On Delayed (Включение по задержке)	Подает питание на все выбранные розетки в соответствии со значениями **Power On Delay** (Задержка подачи питания).†
Off Immediate (Отключить немедленно)	Отключает питание на выбранных розетках.
Off Delayed (Отключение по задержке)	Отключает питание на всех выбранных розетках в соответствии со значениями **Power Off Delay** (Задержка отключения питания).†
Reboot Immediate (Немедленная перезагрузка)	Отключает питание на всех выбранных розетках. Затем подает питание на эти розетки в соответствии с значениями **Reboot Duration** (Продолжительность перезагрузки).†
Reboot Delayed (Перезагрузка с задержкой)	Отключает питание на всех выбранных розетках в соответствии со значениями **Power Off Delay** (Задержка отключения питания). Ожидает момента, когда все розетки будут отключены (максимальное значение **Reboot Duration** (Продолжительность перезагрузки)), а затем подает напряжение на все розетки в соответствии с заданными значениями **Power On Delay** (Задержка подачи питания).†

† Если выбрана локальная группа розеток, будут использоваться значения задержек и продолжительности перезагрузки, заданные для розетки с самым маленьким номером в группе. Если выбрана глобальная группа розеток, будут использоваться значения задержек и продолжительности перезагрузки, заданные для глобальной розетки.

Параметр	Описание
Cancel Pending Commands (Отмена отложенных команд)	Отменяет все отложенные команды для выбранных розеток и оставляет их в текущем состоянии. **ПРИМЕЧАНИЕ:** В случае групп глобальных розеток можно отменить команду только из интерфейса группы-инициатора. Это действие отменяет команду для группы-инициатора и всех последующих групп розеток.

† Если выбрана локальная группа розеток, будут использоваться значения задержек и продолжительности перезагрузки, заданные для розетки с самым маленьким номером в группе. Если выбрана глобальная группа розеток, будут использоваться значения задержек и продолжительности перезагрузки, заданные для глобальной розетки.

Конфигурация настроек и имени розетки

Доступны следующие настройки:

Настройка	Описание
Name (Имя)	Задает имя одной или нескольких розеток. Имя отображается в окне состояния рядом с номером розетки.
External Link (Внешняя линия связи)	Связывает HTTP или HTTPS с веб-сайтом или IP-адресом. • **http://www.dell.com** связывает розетку с веб-сайтом Dell. • **http://*pdu_ip_address***, где ***pdu_ip_address*** – IP-адрес устройства Rack PDU, и связывает розетку с веб-интерфейсом Rack PDU по указанному IP-адресу, позволяя авторизованным пользователям заходить в систему.
Power On Delay (Задержка при включении питания)	Задает интервал времени в секундах, в течение которого устройство Rack PDU находится в ожидании после выдачи команды на подачу питания на розетку. **ПРИМЕЧАНИЕ:** Для конфигурации режима, когда розетка остается выключенной все время, поставьте флажок **Never** (Никогда), расположенный рядом с полем **Power On Delay** (Задержка при включении питания).
Power Off Delay (Задержка при отключении питания)	Задает интервал времени в секундах, в течение которого устройство Rack PDU находится в ожидании после выдачи команды на отключение питания розетки. **ПРИМЕЧАНИЕ:** Для конфигурации режима, когда розетка остается включенной все время, поставьте флажок **Never** (Никогда), расположенный рядом с полем **Power Off Delay** (Задержка при отключении питания).
Reboot Duration (Продолжительность перезагрузки)	Задает продолжительность в секундах, когда розетка остается выключенной до момента повторного подключения.

Чтобы задать параметры или имя розетки, выберите вкладку **Device Manager** (Менеджер устройства), а затем пункт **Configuration** (Конфигурация) из меню навигации, расположенного в левой части экрана. Нажмите кнопку **Configure Multiple Outlets** (Конфигурировать несколько розеток) в разделе **Outlet Configuration** (Конфигурация розеток) или щелкните имя розетки.

- Конфигурация нескольких розеток:
  - Поставьте флажки рядом с номерами розеток, которые хотите настраивать, или поставьте флажок **All Outlets** (Все розетки).
  - Введите значения **Name** (Имя) и **Link** (Линия связи), после чего нажмите кнопку **Apply** (Применить), расположенную внизу списка.
  - Задайте значения **задержки подачи питания**, **задержки отключения питания** и **продолжительности перезагрузки**, после чего нажмите кнопку **Apply** (Применить), расположенную внизу списка.
- Конфигурация настроек одной розетки:
  - Введите значения **Name** (Имя) и **Link** (Линия связи), после чего нажмите кнопку **Apply** (Применить), расположенную внизу списка.
  - Задайте значения **задержки подачи питания**, **задержки отключения питания** и **продолжительности перезагрузки**, после чего нажмите кнопку **Apply** (Применить), расположенную внизу списка.

Планирование действий розетки

Действия, которые можно планировать

Для того, чтобы сконфигурировать значения **задержки включения питания**, **задержки отключения питания** и **продолжительности перезагрузки** для каждой из розеток, см. Конфигурация настроек и имени розетки. Хотя для планирования действий розетки необходимо использовать веб-интерфейс, можно задавать эти значения как через веб-интерфейс, так и с помощью интерфейса командной строки.

В случае действий, которые применяются к группе розеток, необходимо, чтобы группы розеток были доступны в начале планируемого действия. Например, если **отключение с задержкой** запланировано на 16:00, то **задержка отключения** начнется в 16:00. Даже если вы включите группы розеток в течение данного периода **задержки отключения питания** перед тем как любые розетки будут отключены по запланированному действию, данное действие будет применено только к отдельной розетке, но не к группе розеток.

Для всех выбранных розеток можно запланировать любое действие из приводимых в таблице, которое будет выполняться ежедневно, с интервалом в одну, две, четыре или восемь недель, или только один раз.

Параметр	Описание
No Action (Действия отсутствуют)	Нет действия.
On Immediate (Включить немедленно)	Подает питание на выбранные розетки.
On Delayed (Включение по задержке)	Подает питание на все выбранные розетки в соответствии со значениями **задержек подачи питания**.†
Off Immediate (Отключить немедленно)	Отключает питание на выбранных розетках.
Off Delayed (Отключение по задержке)	Отключает питание на всех выбранных розетках в соответствии со значениями **задержек отключения питания**.†
Reboot Immediate (Немедленная перезагрузка)	Отключает питание на всех выбранных розетках. Затем подает питание на эти розетки в соответствии с значениями **продолжительности перезагрузки**.†
Reboot Delayed (Перезагрузка с задержкой)	Отключает питание на всех выбранных розетках в соответствии со значениями **задержек отключения питания**. Ожидает момента, когда все розетки будут отключены (максимальное значение **продолжительности перезагрузки**), а затем подает напряжение на все розетки в соответствии с заданными значениями **задержки подачи питания**.†

† Если выбрана локальная группа розеток, будут использоваться значения задержек и продолжительности перезагрузки, заданные для розетки с самым маленьким номером в группе. Если выбрана глобальная группа розеток, будут использоваться значения задержек и продолжительности перезагрузки, заданные для глобальной розетки.

Планирование события розетки

1. В веб-интерфейсе выберите вкладку **Device Manager** (Менеджер устройств), после чего выберите пункт **Scheduling** (Планирование) в меню навигации, расположенном слева.
2. На странице **Outlet Scheduling** (Планирование розетки) укажите, как часто будет происходить указанное действие (**One-Time** (Однократно), **Daily** (Ежедневно) или **Weekly** (Еженедельно)), после чего нажмите кнопку **Next** (Далее).

   Если выбрано значение **Weekly** (Еженедельно), можно указать, будет ли происходить событие каждую неделю или раз в две, четыре или восемь недель.

3. На странице **Schedule a Daily Action** (Планирование ежедневных действий), в текстовом поле **Name of event** (Имя события) замените имя по умолчанию, **`Outlet Event`** (Событие розетки), на имя, которое будет определять новое событие.
4. Для выбора типа и времени события используйте раскрывающиеся списки.

   Формат даты для единовременного события – *мм*/*дд*, формат времени для всех событий – *чч*/*мм*, при этом час указывается в виде двузначного числа по 24-часовому формату.

   - Событие, которое запланировано на ежедневное выполнение или один раз в интервал, задаваемый в поле **Weekly** (Еженедельно), будет происходить через запланированный интервал, до тех пор пока указанное событие не будет удалено или отключено.
   - Можно запланировать, чтобы однократное событие происходило только один раз в 12 месяцев, в запланированный день. Например, 26 декабря 2010 года можно запланировать одноразовое событие, которое произойдет в любой день, начиная с текущей даты до 26 декабря 2011 года.

5. Используйте флажки, чтобы отметить те розетки, на которые будет распространяться указанное действие. Можно выбрать одну или несколько отдельных розеток, либо выбрать **All Outlets** (Все розетки).
6. Нажмите **Apply** (Применить), чтобы подтвердить планирование события, или **Cancel** (Отмена), чтобы удалить его.

После подтверждения события на экране появится страница со сводной информацией, отображающая новое событие в списке запланированных событий.

Редактирование, включение, отключение и удаление запланированного события розетки

1. В веб-интерфейсе выберите вкладку **Device Manager** (Менеджер устройств), после чего выберите пункт **Scheduling** (Планирование) в меню навигации, расположенном слева.
2. В списке событий в разделе **Scheduled Outlet Action** (Запланированные действия розетки) на странице **Scheduling** (Планирование) щелкните имя события.
3. На странице **Daily/Weekly scheduled action detail** (Сведения о ежедневном/еженедельном запланированном действии) можно выбрать любое действие из перечисленных ниже:

– Изменить параметры события, такие как имя события, время, на которое оно запланировано, и розетки, на которые оно воздействует.

– В поле **Status of event** (Статус события) в верхней части страницы можно выполнить следующее:

- Отключить событие, оставив настройки всех его параметров, с тем чтобы иметь возможность задействовать его позже. Отключенное событие не произойдет. Событие активируется по умолчанию при его создании.
- Активировать событие, если ранее оно было **Disable** (Отключено).
- Удалить событие, изъяв его полностью из системы. Удаленное событие не может быть найдено.

4. По завершении внесения изменений на указанной странице щелкните **Apply** (Применить), чтобы подтвердить сделанные изменения, или нажмите **Cancel** (Отмена).

Меню Менеджера розеток

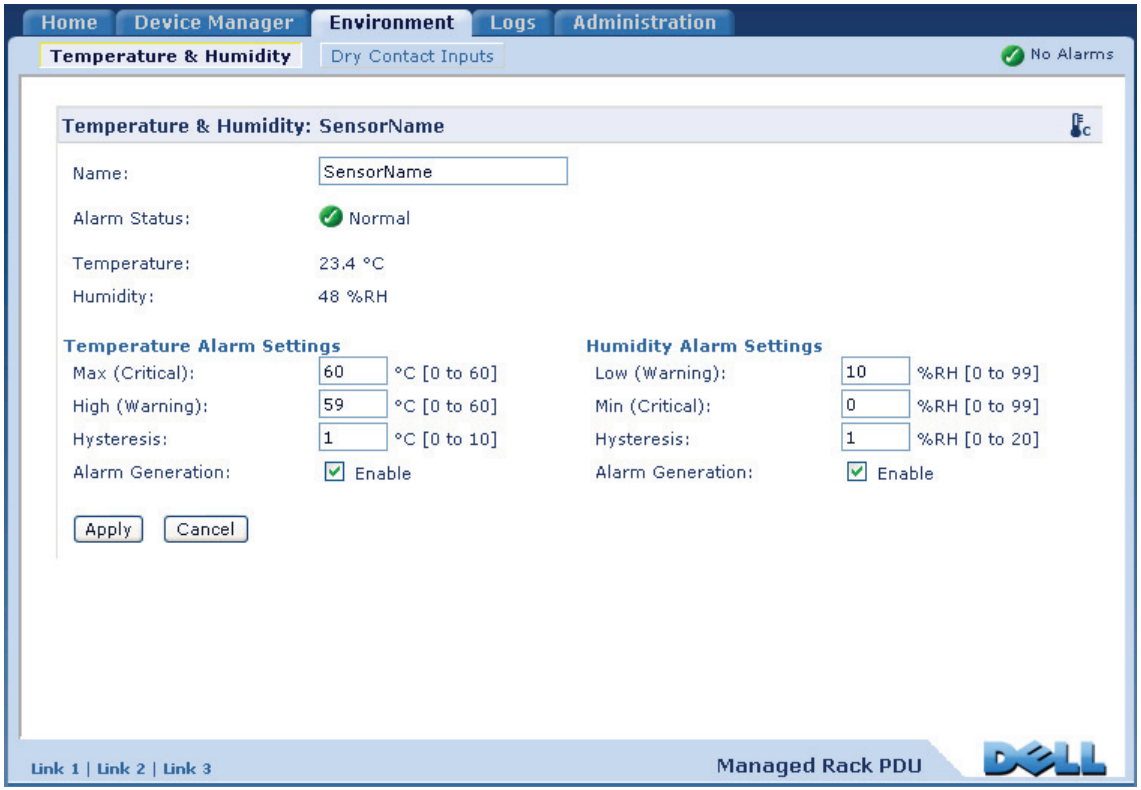
Создает и конфигурирует учетные записи пользователей розеток. Отдельные розетки могут быть назначены пользователю с учетной записью «Пользователь розетки». Учетная запись пользователя розетки позволяет управлять только назначенными розетками. Конфигурация розеток разрешена пользователям с правами Администратора. Менеджер устройств имеет ограниченные права конфигурации розеток.

Конфигурация пользователя розетки

1. В веб-интерфейсе выберите вкладку **Device Manager** (Менеджер устройств), после чего выберите пункт **Outlet Manager** (Менеджер розетки) в меню навигации, расположенном слева.
2. Нажмите кнопку **Add New User** (Добавить нового пользователя).
3. Введите значения для следующих параметров и нажмите **Apply** (Применить), чтобы подтвердить сделанные изменения.

Параметр	Описание
User Name (Имя пользователя)	Задает имя пользователя розетки. Имя «New User» (Новый пользователь) является зарезервированным и не допускается. **ПРИМЕЧАНИЕ:** Имя пользователя, показанное оранжевым, отображает отключенные учетные записи пользователей.
Password (Пароль)	Задает пароль пользователя розетки.
User Description (Описание пользователя)	Позволяет задать идентификацию/описание пользователя розетки.
Account Status (Статус учетной записи)	Позволяет активировать, отключать и удалять учетную запись пользователя розетки.
Device outlet access (Доступ к розетке устройства)	Позволяет выбирать розетки, к которым пользователь имеет доступ.

Экран Environment



Настройка датчиков температуры и влажности

Путь: Environment > Temperature & Humidity

На странице **Temperature & Humidity** (Температура и влажность) при наличии датчика температуры или датчика температуры и влажности, подключенного к устройству Rack PDU, можно настроить пороговые значения для индикаторов «Warning» (Предупреждающий) и «Critical» (Критический) (подробную информацию о каждом типе индикаторов см. в разделе Значки состояния устройства).

Для температуры:

- При достижении высокого порогового значения температуры в системе срабатывает индикатор «Warning».
- При достижении максимального порогового значения температуры в системе срабатывает индикатор «Critical».

Для влажности:

- При достижении низкого порогового значения температуры в системе срабатывает индикатор «Warning».
- При достижении минимального порогового значения температуры в системе срабатывает индикатор «Critical».

Для переключения между значениями по Фаренгейту и Цельсию нужно нажать на значок термометра в правом верхнем углу.

Для настройки датчиков температуры и влажности:

1. Введите минимальное, максимальное, высокое и низкое пороговые значения.
2. Введите значение **Hysteresis** (Гистерезис). (Подробную информацию см. в разделе Гистерезис.)
3. Включите срабатывание индикатора при необходимости.
4. Нажмите **Apply** (Применить).

Гистерезис. Это значение указывает, как далеко нужно перейти пороговое значение температуры или влажности, чтобы вернуться в состояние до нарушения порогового значения.

- Для нарушения пороговых значений температуры «Maximum» (Максимум) и «High» (Высокое), точка стирания – это пороговое значение минус гистерезис.
- Для нарушения пороговых значений влажности «Minimum» (Минимум) и «Low» (Низкое), точка стирания – это пороговое значение плюс гистерезис.

Следует увеличить гистерезис температуры или гистерезис влажности, чтобы избежать появления многочисленных сигналов тревоги, если температура или влажность, вызвавшая это нарушение, незначительно колеблется. Если значение гистерезиса слишком мало, то такие колебания могут многократно вызывать и устранять нарушения порогового значения.

Пример поднятия температуры с колебаниями. Максимальное пороговое значение температуры составляет 85 °F, а гистерезис температуры – 3 °F. Температура поднимается выше 85 °F, нарушая пороговое значение. Затем она опускается до 84 °F и снова опускается до 86 °F, не доходя до точки стирания события и не вызывая нового нарушения порогового значения. Для удаления имеющегося нарушения необходимо, чтобы температура опустилась ниже 82 °F (на 3 °F меньше порогового значения).

Пример понижения влажности с колебаниями. Минимальное пороговое значение влажности составляет 18 %, а гистерезис влажности равен 8 %. Влажность понижается до 18 %, приводя к нарушению порогового значения. Затем она поднимается до 24 % и снова опускается до 13 %, не доходя до точки стирания события и не вызывая нового нарушения порогового значения. Для удаления имеющегося нарушения необходимо, чтобы влажность поднялась выше 26 % (на 8 % больше порогового значения).

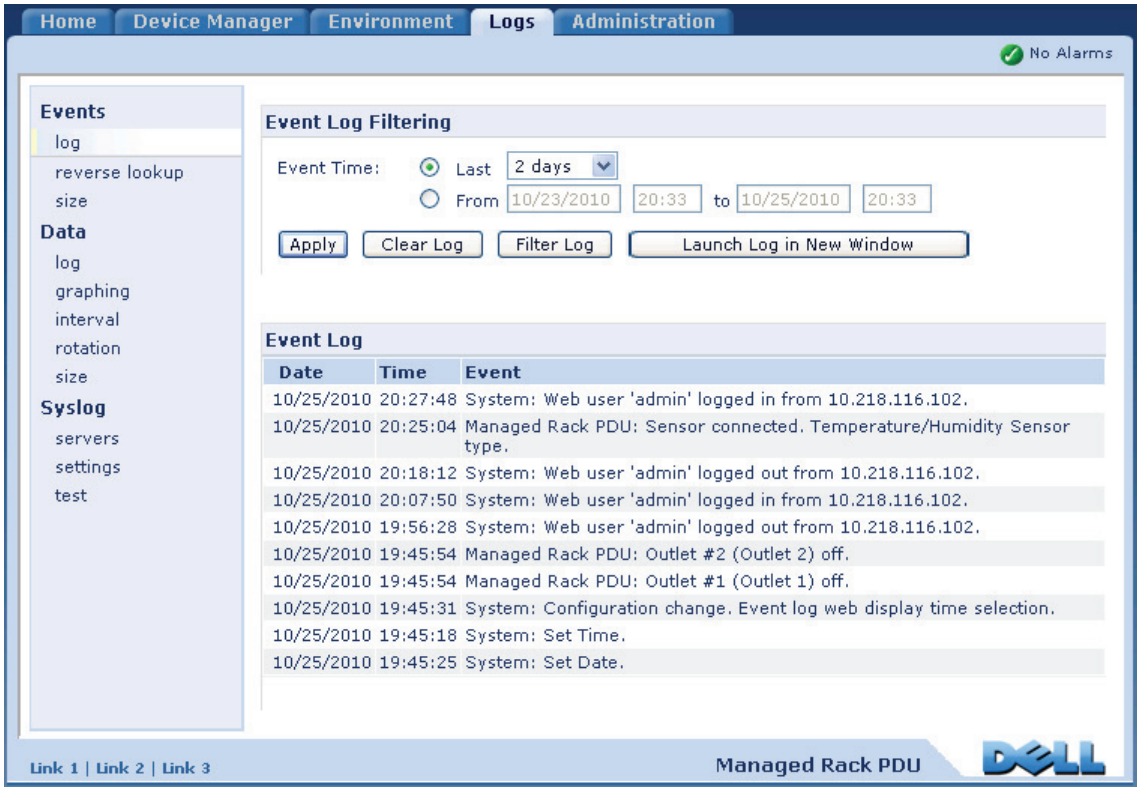
Настройка сухих контактов

Путь: Environment > Dry Contact Inputs

На странице **Dry Contact Inputs** (Сухие контакты), можно просмотреть текущий статус и состояние сухих контактов, и настроить необходимые параметры.

Параметр	Описание
Name (Имя)	Имя данного входного контакта. *Максимальная длина*: 20 символов.
Alarm Status (Состояние тревоги)	**Normal** (Нормальное), если данный входной контакт не сообщает о сигнале тревоги или не сообщает о степени опасности при сообщении о сигнале тревоги.
State (Состояние)	Текущее состояние данного входного контакта. **Closed** (Замкнут) или **Open** (Разомкнут).
Alarm Generation (Срабатывание сигнала тревоги)	Подключение или отключение данного входного контакта. При отключении данный контакт не формирует сигнала тревоги, даже если он находится в ненормальном положении.
Normal State (Нормальное состояние)	Нормальное (неаварийное) состояние данного входного контакта. **Closed** (Замкнут) или **Open** (Разомкнут).

Журналы


Home
Device Manager
Environment
Logs
Administration
No Alarms
Events
log
reverse lookup
size
Data
log
graphing
interval
rotation
size
Syslog
servers
settings
test
Event Log Filtering
Event Time:
Last
2 days
From
10/23/2010
20:33
to
10/25/2010
20:33
Apply
Clear Log
Filter Log
Launch Log in New Window
Event Log
Date
Time
Event
10/25/2010 20:27:48 System: Web user 'admin' logged in from 10.218.116.102.
10/25/2010 20:25:04 Managed Rack PDU: Sensor connected. Temperature/Humidity Sensor type.
10/25/2010 20:18:12 System: Web user 'admin' logged out from 10.218.116.102.
10/25/2010 20:07:50 System: Web user 'admin' logged in from 10.218.116.102.
10/25/2010 19:56:28 System: Web user 'admin' logged out from 10.218.116.102.
10/25/2010 19:45:54 Managed Rack PDU: Outlet #2 (Outlet 2) off.
10/25/2010 19:45:54 Managed Rack PDU: Outlet #1 (Outlet 1) off.
10/25/2010 19:45:31 System: Configuration change. Event log web display time selection.
10/25/2010 19:45:18 System: Set Time.
10/25/2010 19:45:25 System: Set Date.
Link 1 | Link 2 | Link 3
Managed Rack PDU

Использование журналов событий и данных

Журнал событий

Путь: Logs > Events > *options*

Журнал событий можно просматривать, фильтровать или удалять. По умолчанию журнал отображает в обратном хронологическом порядке все события, записанные в течение последних двух дней.

Для получения списков всех настраиваемых событий и их текущих настроек выберите вкладку **Administration** (Администрирование), затем позицию **Notification** (Уведомление) в верхней строке меню и **by event** (по событию) под заголовком **Event Actions** (Действия для событий) на левой панели меню управления.

См. раздел Конфигурирование по событию.

Для отображения журнала событий (Logs > Events > log):

- По умолчанию журнал событий можно просматривать как страницу веб-интерфейса. Самые последние события записаны на странице 1. В строке навигации под журналом выполните следующие операции.
  - Нажмите номер страницы, чтобы открыть конкретную страницу журнала.
  - Нажмите **Previous** (Предыдущий) или **Next** (Следующий) для просмотра событий, записанных непосредственно до или после событий, указанных на открытой странице.
  - Нажмите **<<** для возврата к первой странице или **>>** для просмотра последней страницы журнала.

- Для просмотра перечисленных на странице событий нажмите **Launch Log in New Window** (Запустить журнал в новом окне) со страницы журнала событий, чтобы отобразить журнал в полноэкранном виде.

  В опциях вашего браузера должен быть включен JavaScript®, чтобы можно было использовать кнопку **Launch Log in New Window** (Запустить журнал в новом окне).

  Для просмотра журнала событий можно также использовать FTP или Secure CoPy (SCP). См. раздел Как использовать FTP или SCP для поиска файлов в журнале.

Для фильтрования журнала событий (Logs > Events > log):

- **Фильтрование журнала по дате или по времени.** Для отображения всего журнала событий или для изменения количества дней или недель, для которых в журнале отображаются последние события, выберите позицию **Last** (Последнее). Выберите временной диапазон из разворачивающегося меню, а затем нажмите **Apply** (Применить). Настройка фильтра сохраняется до перезапуска Rack PDU.
  Для отображения данных, зарегистрированных в течение конкретного временного диапазона, выберите **From** (С). Укажите начальное и конечное время (в 24-часовом формате), а также даты для отображения событий, затем нажмите **Apply** (Применить). Настройка фильтра сохраняется до перезапуска Rack PDU.
- **Фильтрование журнала по событиям**: Для указания событий, отображенных в журналах, нажмите **Filter Log** (Фильтровать журнал). Снимите флажок в окне категории событий или степени опасности (серьезности) сигналов тревоги. Текст в верхнем правом углу страницы журнала событий говорит о том, что фильтр включен.
  В качестве администратора нажмите **Save As Default** (Сохранить как элемент по умолчанию), чтобы сохранить этот фильтр для отображения журнала по умолчанию для всех пользователей. Если вы не нажимаете на позиции **Save As Default**, то фильтр остается активным до тех пор, пока вы его не очистите, или

до перезапуска Rack PDU.

Для удаления активного фильтра нажмите **Filter Log** (Фильтровать журнал), затем **Clear Filter (Show All)** (Очистить фильтр (показать все)).

События обрабатываются фильтром с помощью логического оператора **OR (ИЛИ)**.

- События, которые не выбраны из списка **Filter By Severity** (Фильтровать по степени опасности), никогда не отображаются в отфильтрованном журнале событий даже в том случае, если событие происходит в категории, выбранной из списка **Filter by Category** (Фильтровать по категории).
- События, которые не выбраны из списка **Filter by Category**, никогда не отображаются в отфильтрованном журнале событий даже в том случае, если устройства в данной категории переходит в состояние, вызывающее тревогу, выбранное из списка **Filter by Severity**.

Для удаления журнала (Logs > Events > log):

Для удаления всех событий, записанных в журнале нажмите **Clear Log** (Очистить журнал) на веб-странице с отображением этого журнала. Удаленные события восстановить невозможно.

Описание отключения регистрации в журнале событий на основании присвоенной степени опасности или категории события см. в разделе Конфигурирование по событию.

Для настройки обратного просмотра (Logs > Events > reverse lookup):

Обратный просмотр отключен по умолчанию. Включите эту функцию, если у вас отсутствует настроенный сервер DNS или плохо работает сеть из-за плотного трафика.

Если при выключенном обратном просмотре в сети происходит событие, то и IP-адрес и имя домена сетевого устройства, связанного с этим событием, заносятся в журнал событий. Если в устройстве отсутствует запись имени домена, то в связи с событием в журнале регистрируется только IP-адрес. Поскольку доменные имена изменяются реже, чем IP-адреса, то включение обратного просмотра может улучшить идентификацию сетевых устройств, являющихся причиной возникновения событий.

Для изменения размера журнала событий (Logs > Events > size):

По умолчанию в журнале событий может храниться до 400 событий. Количество событий, хранящихся в журнале, можно изменить. Изменение журнала событий приведет к удалению из журнала всех текущих записей. Чтобы избежать потери данных в журнале, используйте FTP или SCP для поиска (последующего восстановления) информации в журнале, прежде чем ввести новое значение в поле **Event Log Size** (Размер журнала событий).

См. раздел Как использовать FTP или SCP для поиска файлов в журнале.

После того как журнал заполнен, начинается удаление самых старых записей.

Журнал данных

Путь: Logs > Data > *options*

В журнал данных записываются ток и мощность для устройства, а также фазы (для трехфазного Rack PDU), если применимо, кроме того, температура, влажность и данные сухого контакта в указанный отрезок времени. Для каждой записи данных указывается время и дата регистрации.

Для отображения журнала данных (Logs > Data > log):

- По умолчанию журнал данных можно просматривать как страницу веб-интерфейса. Самые последние данные записаны на странице 1. В строке навигации под журналом выполните следующие операции.
  - Нажмите номер страницы, чтобы открыть конкретную страницу журнала.
  - Нажмите **Previous** (Предыдущий) или **Next** (Следующий) для просмотра данных, записанных непосредственно до или после данных, указанных на открытой странице.
  - Нажмите **<<** для возврата к первой странице или **>>** для просмотра последней страницы журнала.
- Для просмотра перечисленных на странице данных нажмите **Launch Log in New Window** (Запустить журнал в новом окне) со страницы журнала данных, чтобы отобразить журнал в полноэкранном виде.

В опциях вашего браузера должен быть включен JavaScript, чтобы можно было использовать кнопку **Launch Log in New Window**.

Для просмотра журнала данных можно также использовать FTP или SCP. См. раздел Как использовать FTP или SCP для поиска файлов в журнале.

Для фильтрования журнала по данным или времени (Logs > Data > log):

Для отображения всего журнала данных или для изменения количества дней или недель, для которых в журнале отображаются последние данные, выберите позицию **Last** (Последнее). Выберите временной диапазон из разворачивающегося меню, а затем нажмите **Apply** (Применить). Настройка фильтра сохраняется до перезапуска устройства.

Для отображения данных, зарегистрированных в течение конкретного временного диапазона, выберите **From** (С). Укажите начальное и конечное время (в 24-часовом формате), а также даты для отображения данных, а затем нажмите **Apply** (Применить). Настройка фильтра сохраняется до перезапуска устройства.

Для удаления журнала данных:

Для удаления всех данных, записанных в журнале, нажмите **Clear Data Log** (Очистить журнал данных) на странице с отображением этого журнала. Поиск удаленных данных не выполняется.

Для установки интервала сбора данных (Logs > Data > interval):

Определите в настройке **Log Interval** (Интервал журнала), как часто производится выборка и сохранение данных в журнале данных и просмотрите расчет количества дней, в течение которых возможно сохранение информации на основании выбранного интервала. После того как журнал заполнен, начинается удаление самых старых записей. Чтобы избежать автоматического удаления старых данных, включите и настройте обновление журнала данных в соответствии с описанием в следующем разделе.

Для настройки обновления журнала данных (Logs > Data > rotation):

Создайте защищенный паролем архив журнала данных на указанном FTP-сервере. Включение обновления вызывает прикрепление содержимого журнала данных к файлу с указанным вами именем и местоположением. Обновление этого файла происходит с заданным интервалом загрузки.

Параметр	Описание
Data Log Rotation (Обновление журнала данных)	Включение или отключение (по умолчанию) обновления журнала данных.
FTP Server Address (Адрес FTP-сервера)	Местоположение FTP-сервера, на котором хранится файл с архивом данных.
User Name (Имя пользователя)	Имя пользователя, необходимое для отправки данных в файл с архивом данных. Данный пользователь должен обладать правом доступа к чтению и записи данных в файле архива и к каталогу (папке), в котором этот файл хранится.
Password (Пароль)	Пароль, необходимый для отправки данных в файл с архивом данных.
File Path (Путь к файлу)	Путь к файлу архива данных.
Filename (Имя файла)	Имя файла архива данных (тестовый ASCII файл).
Delay *X* hours between uploads (Задержка *X* часов между загрузками).	Количество часов между загрузками данных в файл.
Upload every *X* minutes (Загружать каждые *X* минут)	Количество минут между попытками загрузить данные в файл после сбоя загрузки.
Up to *X* times (До *X* раз)	Максимальное количество попыток загрузки после исходного сбоя.
Until Upload Succeeds (До успешного завершения загрузки)	Попытка загрузки файла до завершения передачи.

Для изменения размера журнала данных (Logs > Data > size):

По умолчанию в журнале данных может храниться до 1000 записей. Количество записей, хранящихся в журнале, можно изменить. Изменение размера журнала данных приведет к удалению из журнала всех текущих записей. Чтобы избежать потери записей в журнале, используйте FTP или SCP для поиска в журнале, прежде чем ввести новое значение в поле **Размер журнала данных**.

См. раздел Как использовать FTP или SCP для поиска файлов в журнале.

После того как журнал заполнен, начинается удаление самых старых записей.

Как использовать FTP или SCP для поиска файлов в журнале

Администратор или Пользователь устройства может использовать FTP или SCP для поиска разделенного табуляторами файла регистрации событий (*event.txt*) или файла регистрации данных (*data.txt*) и импортирования его в электронные таблицы.

- Файл содержит отчет обо всех событиях и данных с момента последнего удаления журнала или (для журнала данных) усечения после достижения максимального размера.
- Этот файл включает в себя информацию, которая не отображается в файле событий или в файле данных.
  - Версия формата файла (первое поле)
  - Дата и время поиска файла
  - **Name** (Имя), **Contact** (Контакт) и **Location** (Расположение), а также IP-адрес Rack PDU
  - Уникальный **Event Code** (Код события) для каждого зарегистрированного события (только файл *event.txt*)

В Rack PDU для записей в журнале используется четырехразрядная запись года. Вы можете выбрать четырехразрядный формат даты в своей программе электронных таблиц для отображения всех четырех разрядов.

Если вы используете протоколы защиты на основе шифрования, то для поиска файла журнала применяется Secure CoPy (SCP).
Если вы используете нешифрованные методы аутентификации для защиты системы, для поиска файла журнала применяется FTP.

Для получения сведений об имеющихся протоколах и способах установки необходимой защиты см. Приложение Б: Руководство по безопасности.

Использование SCP для поиска этих файлов. Чтобы использовать SCP для поиска файла *event.txt*, воспользуйтесь командой:

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

Чтобы использовать SCP для поиска файла *data.txt*, воспользуйтесь следующей командой:

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

Использование FTP для поиска этих файлов. Использование FTP для поиска файла *event.txt* или *data.txt*:

1. После появления командной подсказки наберите **`ftp`** и IP-адрес Rack PDU, а затем нажмите ENTER.

   Если настройка **Port** (Порт) для опции **FTP Server** (Сервер FTP) (устанавливаемая с помощью меню **Network** (Сеть) на вкладке **Administration** (Администрирование)) была изменена со значения по умолчанию (**21**), то в команде FTP необходимо использовать значение не по умолчанию. Для клиентов Windows FTP используйте следующую команду, включая пробелы. (Для некоторых клиентов FTP необходимо использовать двоеточие вместо пробела между IP-адресом и номером порта.)

   `ftp>open ip_адрес номер_порта`

   Описание установки значения порта не по умолчанию для повышения защищенности FTP-сервера приводится в разделе Сервер FTP. Можно указать любой порт от 5001 до 32768.

2. Для входа в систему используйте зависящее от регистра **Имя пользователя** и **Пароль** для Администратора или Пользователя устройства. Для Администратора **admin** – это значение для **Имени пользователя** и **Пароля** по умолчанию. Для Пользователя значение по умолчанию – **device** – для **Имени пользователя** и **Пароля**.
3. Используйте команду **get** для сохранения данных журнала на ваш локальный диск.

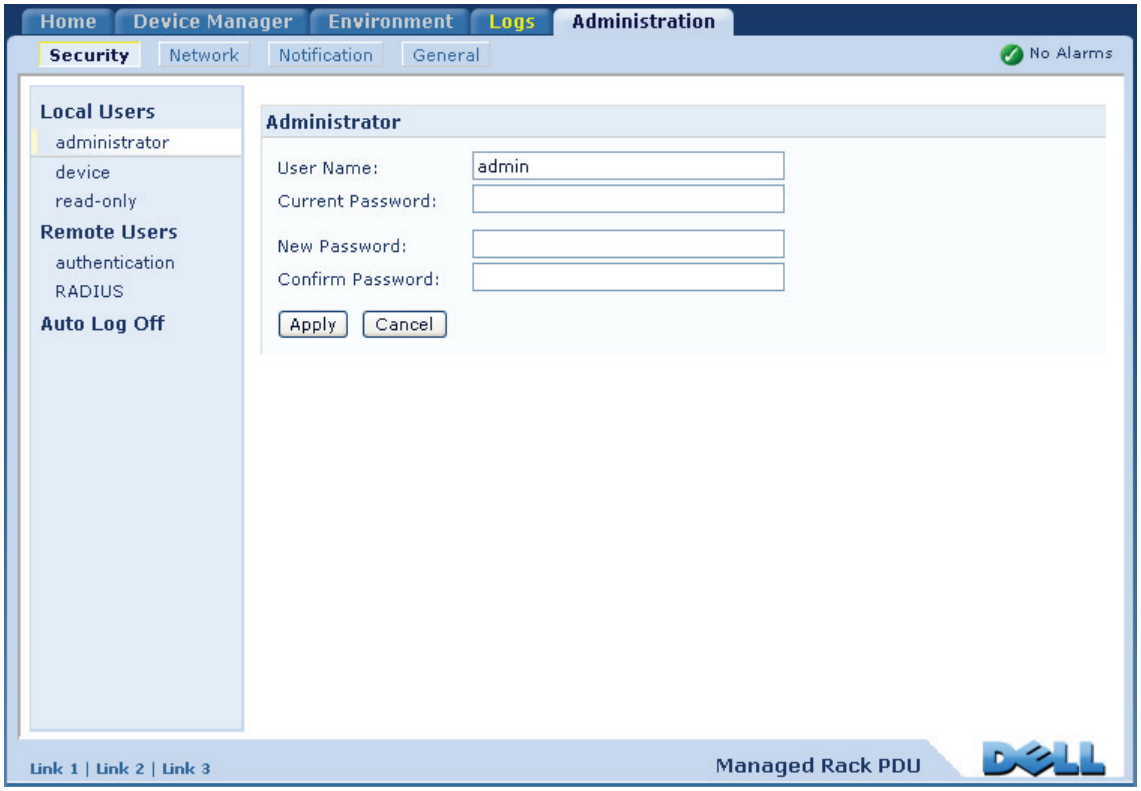
   `ftp>get event.txt`

   или

   `ftp>get data.txt`

4. Наберите **`quit`** по подсказке **`ftp>`**, чтобы выйти из FTP.

Администрирование: Безопасность



Локальные пользователи

Настройка доступа пользователя

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

Учетная запись пользователя Администратор всегда обеспечивает доступ к Rack PDU.

Учетные записи Пользователь устройства и Только для чтения включаются по умолчанию. Для отключения учетных записей Пользователь или Только для чтения выберите соответствующую учетную запись на левой панели меню управления, а затем снимите флажок **Enable** (Включить).

Точно таким же образом укажите зависящее от регистра имя пользователя и пароль. Максимальная длина составляет 64 символа для имени пользователя и 64 символа для пароля. Пустые пароли (без символов) не допускаются.

Информацию о разрешениях для каждого типа учетной записи см. в разделе Типы учетных записей.

Для учетной записи пользователя розетки нет имени пользователя и пароля по умолчанию. Имя пользователя, пароль и другие характеристики учетной записи пользователя розетки должен задать администратор. См. Конфигурация пользователя розетки.

Тип учетной записи	Имя пользователя по умолчанию	Пароль по умолчанию	Разрешенный доступ
Администратор	admin	администратор	Веб-интерфейс и интерфейс командной строки
Пользователь устройства	device	устройство	
Только для чтения	readonly	только для чтения	Только веб-интерфейс

Удаленные пользователи

Аутентификация

Путь: Administration > Security > Remote Users > Authentication Method

Используйте эту опцию для управления удаленным доступом к Rack PDU.

Информацию о локальной аутентификации (не включающей централизованную аутентификацию через сервер RADIUS) см. в разделе Приложение Б: Руководство по безопасности.

Rack PDU поддерживает функции аутентификации и авторизации RADIUS (пользовательская служба удаленной аутентификации).

- Если пользователь осуществляет доступ к Rack PDU или к другому сетевому устройству, к которому подключен RADIUS, то аутентификационный запрос передается на сервер RADIUS, чтобы определить уровень допуска пользователя.
- Имена пользователей RADIUS, используемые в Rack PDU, ограничены 32 символами.

Выберите один из следующих вариантов:

- **Local Authentication Only** (Только локальная аутентификация): RADIUS отключен. Локальная аутентификация включена.
- **RADIUS, then Local Authentication** (RADIUS, затем локальная аутентификация): Включаются RADIUS и локальная аутентификация. Сначала запрашивается аутентификация от сервера RADIUS. Если сервер RADIUS не отвечает, то используется локальная аутентификация.

- **RADIUS Only** (Только RADIUS): RADIUS включен. Локальная аутентификация отключена.

Если выбирается **RADIUS Only**, а сервер RADIUS недоступен, неправильно идентифицирован или неправильно сконфигурирован, то удаленный доступ невозможен для всех пользователей. Необходимо использовать подключение к интерфейсу командной строки по последовательному каналу связи и изменить настройку **доступа** на **local** или **radiusLocal** для восстановления доступа. Например, команда изменения настройки доступа на **local** имеет следующий вид:

```
radius -a local
```

RADIUS

Путь: Administration > Security > Remote Users > RADIUS

Используйте этот параметр, чтобы выполнить указанные ниже операции.

- Перечислите серверы RADIUS (максимум два), доступные для Rack PDU и период тайм-аута для каждого из них.
- Нажмите ссылку и настройте параметры для аутентификации нового сервера RADIUS.
- Нажмите на сервер RADIUS из списка для отображения и изменения его параметров.

Настройка RADIUS	Описание
RADIUS Server (Сервер RADIUS)	Имя сервера или IP-адрес (IPv4 или IPv6) сервера RADIUS. Для настройки сервера нажмите на ссылку. **ПРИМЕЧАНИЕ:** Для аутентификации пользователей серверы RADIUS по умолчанию используют порт 1812. Чтобы использовать другой порт, добавьте к имени или к IP-адресу сервера RADIUS двоеточие и укажите новый номер порта.
Secret (Секрет)	Общий секрет для сервера RADIUS и Rack PDU.
Timeout (Время ожидания ответа)	Время в секундах, в течение которого Rack PDU ждет ответа от сервера RADIUS.
Test Settings (Настройки тестирования)	Введите имя пользователя Администратора и пароль для тестирования пути к серверу RADIUS, который вы сконфигурировали.
Skip Test and Apply (Пропустить тестирование и применить)	Не тестировать путь к серверу RADIUS.

Конфигурирование сервера RADIUS

Краткое описание процедуры конфигурирования

Для работы с Rack PDU необходимо сконфигурировать сервер RADIUS.

Примеры пользовательских файлов RADIUS с атрибутами, зависящими от поставщика (VSA), и пример записи в словарный файл на сервере RADIUS приведены в разделе Приложение Б: Руководство по безопасности.

1. Добавьте IP-адрес Rack PDU к списку (файлу) клиентов сервера RADIUS.
2. Пользователи должны быть настроены с атрибутами Service-Type (тип обслуживания), если не заданы атрибуты поставщика. Если атрибуты Service-Type не указаны, то у пользователя будет доступ только для чтения (только на веб-интерфейсе).

   Сведения о пользовательском файле RADIUS приведены в документации к серверу, примеры можно найти в разделе Приложение Б: Руководство по безопасности.

3. Вместо атрибутов Service-Type, предусматриваемых сервером RADIUS, можно использовать VSA. Для VSA требуется запись в словаре и в пользовательском файле RADIUS. В словарном файле определите имена для ключевых слов АТРИБУТ и ЗНАЧЕНИЕ, но не для цифровых значений. Изменение цифровых значений приводит к сбою аутентификации и авторизации RADIUS. VSA имеет преимущество перед стандартными атрибутами RADIUS.

Конфигурирование сервера RADIUS для UNIX® с теневыми паролями

Если файлы теневого пароля UNIX (/etc/passwd) используются вместе со словарными файлами RADIUS, то для аутентификации пользователей можно применить два указанных ниже метода:

- Если все пользователи UNIX имеют административные привилегии, добавьте следующие операции для «пользовательского» файла RADIUS. Чтобы допустить только Пользователей устройств, замените DELL-Service-Type (Тип обслуживания DELL) на **`Device (Устройство)`**.

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

- Добавьте имена пользователей и атрибуты к «пользовательскому» файлу RADIUS и проверьте пароли для /etc/passwd. Следующий пример относится к пользователям **`bconners`** и **`thawk`**:

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

Поддерживаемые серверы RADIUS

Поддерживаются FreeRADIUS и Microsoft IAS 2003. Другие общедоступные приложения RADIUS также могут использоваться, но они не прошли полную проверку.

Время ожидания ответа

Путь: Administration > Security > Auto Log Off

Используйте этот параметр для настройки времени (3 минуты по умолчанию), по истечении которого неактивный пользователь отключается от системы. При изменении этого значения необходимо выйти из системы, чтобы изменение вступило в силу.

Таймер продолжает работу, если пользователь закрывает окно браузера, не выйдя предварительно из системы нажатием клавиши **Log Off** (Завершение сеанса), расположенной вверху справа. Поскольку считается, что пользователь все еще в системе, другой пользователь не может войти в систему, пока не истечет время, заданное параметром **Minutes of Inactivity** (Минуты отсутствия активности). Например, если пользователь закрывает окно браузера, не выйдя из системы, при значении параметра **Minutes of Inactivity**, заданном по умолчанию, то другой пользователь не может войти в систему в течение 3 минут.

Администрирование: Уведомление

Действия для событий

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

Типы уведомлений

Чтобы добиться требуемой реакции на событие или группу событий, можно конфигурировать действия для событий. Эти действия будут уведомлять пользователя о событии одним из указанных способов:

- Активное, автоматическое уведомление. Указанные пользователи контролируемых устройств будут уведомляться непосредственно.
  - Уведомление по электронной почте
  - Прерывания SNMP
  - Уведомление системного журнала (Syslog)
- Косвенное уведомление
  - Журнал событий. Если не сконфигурирована передача прямых уведомлений, пользователи должны проверять журнал, чтобы смотреть, какие события произошли

    Можно также регистрировать данные о работе системы с целью использования этих данных для контроля работы устройств. См. Журнал данных, чтобы ознакомиться с конфигурированием и использованием функции регистрации данных.
  - Запросы (SNMP GET)

    Для получения дополнительных сведений см. раздел SNMP. SNMP позволяет NMS использовать информационные запросы. В случае протокола SNMPv1, который не обеспечивает шифрования данных перед передачей, задание наиболее ограниченного типа доступа SNMP (READ) позволяет выполнять информационные запросы без риска дистанционного изменения конфигурации.

Конфигурирование действий для событий

Параметры уведомлений. Для событий, которые имеют связанное событие очистки, можно задать следующие параметры, конфигурируя отдельные события или группы событий, как описано в последующих двух разделах. Чтобы получить доступ к указанным параметрам, щелкните приемник или имя получателя.

Параметр	Описание
Delay x time before sending (Задержка *x* перед отправкой)	Если событие продолжает действовать в течение указанного промежутка времени, посылается уведомление. Если данное условие исчезает до того, как истек заданный интервал времени, уведомление не посылается.
Repeat at an interval of *x* time (Повторять через интервал *x* минут)	Уведомление посылается в указанный промежуток времени (например, каждые 2 минуты).
Up to *x* times (До *x* раз)	Пока событие действует, уведомление будет повторено указанное число раз.
Until condition clears (До устранения условия возникновения)	Уведомление посылается регулярно до того момента, пока условие не исчезнет или не будет устранено.

Конфигурирование по событию. Для определения ответных действий на отдельное событие:

1. Выберите вкладку **Administration** (Администрирование), пункт **Notification (Уведомление)** в верхней строке меню и укажите параметр **by event** (по событию) в пункте **Event Actions** (Действия для событий) в левом меню навигации.
2. В перечне событий найдите помеченные столбцы, чтобы проверить, сконфигурированы ли те действия, которые вы собираетесь использовать. (По умолчанию, регистрация указана для всех событий).

3. Чтобы посмотреть или изменить текущую конфигурацию, например, получателей, которые будут уведомлены по электронной почте или пейджеру, или систем NMS, которые должны быть уведомлены по прерываниям SNMP, щелкните имя события.

Если сервер Syslog не сконфигурирован, пункты, относящиеся к конфигурации Syslog показаны не будут.

При просмотре параметров конфигурации события можно изменить конфигурацию, включить или отключить регистрацию событий или журнал Syslog, или отключить уведомление определенных получателей электронной почты или приемников прерываний, но нельзя добавить или удалить получателей и устройства-приемники. Чтобы добавить или удалить адресаты или устройства-приемники, смотрите следующее:

- Идентификация серверов Syslog
- Получатели электронной почты
- Приемник прерываний

Конфигурирование по группе. Чтобы сконфигурировать группу событий:

1. Выберите вкладку **Administration** (Администрирование), пункт **Notification** (Уведомление) в верхней строке меню и укажите параметр **by group** (по группе) в пункте **Event Actions** (Действия для событий) в левом меню навигации.
2. Выберите, каким образом группировать события для конфигурации:
   - Выберите пункт **Grouped by severity** (События по степени опасности), после чего выберите все события одного или нескольких уровней опасности. Изменять уровень опасности события нельзя.
   - Выберите пункт **Grouped by category** (События по категории), после чего выберите все события одной или нескольких предварительно заданных категорий.

3. Нажмите **Next>>**, чтобы уйти с указанной страницы, и выполните следующее:

   a. Выберите действия для события для группы событий.

   - Чтобы выбрать любое из действий, за исключением **Logging** (Ведение журнала) (по умолчанию), для начала необходимо иметь, как минимум, одного сконфигурированного действительного получателя или одно устройство-приемник.
   - Если вы указали **Logging** (Ведение журнала) и сконфигурировали сервер Syslog, выберите на следующей странице **Event Log** (Журнал событий) или **Syslog** (или оба журнала).

   b. Укажите, хотите ли вы сохранить новое сконфигурированное действие на событии для группы событий или отключить данное действие.

Активное автоматическое прямое уведомление

Уведомление по электронной почте

Обзор настроек. Используйте протокол SMTP для отправки сообщений электронной почты сразу четырем получателям при возникновении события.

Чтобы использовать функцию отправки электронной почты, необходимо задать следующие параметры:

- IP-адреса первичного и, дополнительно, вторичного сервера доменных имен (DNS).

  
  См. раздел DNS.

- IP-адрес или имя DNS для параметров **SMTP Server** (SMTP-сервер) и **From Address** (Адрес отправителя).

  
  См. раздел SMTP.

- Адреса электронной почты для четырех получателей (максимум).

  
  См. раздел Получатели электронной почты.

Можно использовать настройку **To Address** (Адрес получателя) параметра **recipients** (получатели) для отправки электронной почты на текстовый пейджер.

SMTP.

Путь: Administration > Notification > E-mail > server

Настройка	Описание
Local SMTP Server (Локальный сервер SMTP)	Адрес IPv4/IPv6 или имя DNS локального сервера SMTP. **ПРИМЕЧАНИЕ:** Этот параметр требуется определять только в том случае, если **SMTP Server** (Сервер SMTP) задан как **Local** (Локальный). См. раздел Получатели электронной почты.
From Address (Адрес отправителя)	Содержание поля **From** (От) в сообщениях электронной почты отправляется устройством Rack PDU: • В формате *пользователь*@ [*IP_адрес*] (если IP-адрес указан как **Local SMTP Server**) • В формате *пользователь@домен* (если сконфигурирован DNS, и имя DNS указано как **Local SMTP Server**) в сообщениях электронной почты. **ПРИМЕЧАНИЕ:** Локальный сервер SMTP может потребовать учетную запись сервера для задания данной настройки. См. документацию сервера.

Получатели электронной почты.

Путь: Administration > Notification > E-mail > recipients

Определяет до четырех получателей электронной почты.

Настройка	Описание
To Address (Адрес получателя)	Имя пользователя и доменное имя получателя. Чтобы использовать адрес для уведомления на пейджер, задайте адрес электронной почты шлюза пейджерной учетной записи получателя (например, **`myacct100@skytel.com`**). Шлюз пейджера будет генерировать сообщение. Чтобы обойти поиск DNS-имени IP-адреса почтового сервера, в скобках укажите IP-адрес вместо имени домена электронной почты, например, используйте jsmith@[xxx.xxx.x.xxx] вместо jsmith@company.com. Это полезно, когда поиск имен DNS работает неправильно. **ПРИМЕЧАНИЕ:** Пейджер получателя должен быть способен получать текстовые сообщения.
E-mail Generation (Создание сообщения электронной почты)	Включает (по умолчанию) или отключает отправку электронной почты получателю.

Настройка	Описание

SMTP Server (Сервер SMTP)	Выберите один из следующих способов доставки электронной почты:
	• **Local** (Локальный): Через сервер SMTP Rack PDU. Данная настройка (рекомендуемая) гарантирует, что сообщение будет отправлено до истечения времени ожидания Rack PDU, равного 20 с, и, в случае необходимости, попытка отправить сообщение повторяется несколько раз. Кроме того, выполните одно из следующих действий:
	  • Включите пересылку на сервере SMTP Rack PDU, с тем чтобы он мог переправлять электронную почту на внешние серверы SMTP. Обычно серверы SMTP не сконфигурированы для пересылки электронной почты. Проверьте с администратором ваш сервер SMTP перед изменением конфигурации с целью разрешить пересылку.
	  • Укажите специальную учетную запись электронной почты для Rack PDU, чтобы переправлять почту на внешнюю учетную почтовую запись.
	• **Получатель**: Непосредственно на сервер SMTP получателя. С указанной настройкой Rack PDU попытается оправить электронную почту только один раз. Если удаленный сервер SMTP занят, настройка времени ожидания может предотвратить отсылку некоторых писем.
	Если получатель использует SMTP-сервер Rack PDU, данная настройка не работает.

Format (Формат)	Длинный формат содержит имя, местоположение, контакт, IP-адрес, серийный номер устройства, дату и время, код и описание события. Короткий формат содержит только описание события.
User Name Password Confirm Password (Имя пользователя Пароль Подтверждение пароля)	Если почтовый сервер требует аутентификации, укажите здесь имя пользователя и пароль. Таким образом будет выполняться простейшая аутентификация, но не SSI.

Тестирование электронной почты.

Путь: Administration > Notification > E-mail > test

Посылает тестовое сообщение указанному получателю.

Прерывания SNMP

Приемник прерываний.

Путь: Administration > Notification > SNMP Traps > trap receivers

Просмотр приемников прерываний по имени IP-адреса/хоста NMS. Можно задать до шести приемников прерываний.

- Чтобы сконфигурировать новый приемник прерываний, щелкните пункт **Add Trap Receiver** (Добавить приемник прерываний).
- Чтобы изменить настройки или удалить приемник прерываний, щелкните вначале IP-адрес или имя хост-узла, чтобы получить доступ к его настройкам. (Если вы удалите приемник прерываний, все настройки уведомлений, сконфигурированные в пункте «Event Actions» (Действия для событий) для удаленного приемника прерываний, вернутся в исходное положение, заданное по умолчанию).
- Чтобы указать тип прерывания для данного приемника, задайте с помощью переключателя значение SNMPv1 или SNMPv3. Чтобы система NMS могла получать оба типа прерываний, необходимо сконфигурировать для данной NMS два приемника прерываний, по одному на каждый тип прерывания.

Компонент	Описание
Trap Generation (Создание системного прерывания)	Включает (по умолчанию) или отключает генерацию прерывания для данного приемника прерываний.
NMS IP/Host Name (Имя IP-адреса/хоста NMS)	Адрес IPv4/IPv6 или имя хост-узла данного приемника прерываний. По умолчанию, настройки 0.0.0.0 оставляют приемник прерываний неопределенным.

Параметр SNMPv1.

Компонент	Описание
Community Name (Имя сообщества)	Имя (по умолчанию **public**), используемое в качестве идентификатора при отправке прерываний SNMPv1 на данный приемник.
Authenticate Traps (Аутентификация прерываний)	Если данная функция активирована (по умолчанию), система NMS, определяемая настройкой «NMS IP/Host Name» (Имя IP-адреса/хоста NMS), будет получать аутентификационные прерывания (прерывания, генерируемые неудачными попытками регистрации на данном устройстве). Чтобы отключить эту возможность, снимите флажок.

Параметр SNMPv3. Задает идентификатор профиля пользователя для данного приемника прерываний. (Чтобы увидеть настройки профилей пользователя, определяемые именами пользователей, выбираемых здесь, укажите **Network** (Сеть) в верхней строке меню и **user profiles** (профили пользователя) в пункте **SNMPv3** в левом меню навигации).

См. SNMPv3 о создании профилей пользователей и о выборе способов аутентификации и шифрования.

Тестирование прерываний SNMP

Путь: Administration > Notification > SNMP Traps > test

Последний результат тестирования. Результат последнего теста прерывания SNMP. Успешный тест прерывания SNMP подтверждает только то, что прерывание было отправлено, но не проверяет его получение выбранным приемником прерываний. Тест прерываний считается успешным, если все из перечисленных условий будут верны:

- На данном устройстве доступна одна из версий SNMP (SNMPv1 или SNMPv3), конфигурируемая для указанного приемника прерываний.
- Приемник прерываний включен.
- Если имя хост-узла указывается в поле адреса **To** (К), данное имя может быть заменено на действительный IP-адрес.

Параметр «To» (К). Укажите IP-адрес или имя хост-узла, на который будет послан тест прерывания SNMP. Если приемник прерывания не сконфигурирован, будет отображаться ссылка на страницу конфигурации **Trap Receiver** (Получатель прерываний).

Syslog

Путь: Logs > Syslog > *options*

Rack PDU может посылать сообщения сразу на четыре сервера Syslog в случае возникновения события. Серверы Syslog регистрируют события, произошедшие в сетевых устройствах в журналах, которые обеспечивают централизованную регистрацию событий.

Руководство пользователя не содержит подробных описаний сервера Syslog и его конфигурации. См. **RFC3164** для получения подробной информации о серверах Syslog.

Идентификация серверов Syslog.

Путь: Logs > Syslog > servers

Настройка	Описание
Syslog Server (Сервер Syslog)	Использует адреса IPv4/IPv6 или имена хост-узлов для идентификации одного из четырех серверов для получения сообщений Syslog, посылаемых устройством Rack PDU.
Port (Порт)	Порт протокола пользовательских датаграмм (UDP), который использует Rack PDU для отправки сообщений Syslog. По умолчанию имеет значение **514**, порт UDP назначен для Syslog.
Протокол	Выбор языка сообщений Syslog.

Настройки системного журнала.

Путь: Logs > Syslog > settings

Настройка	Описание
Message Generation (Создание сообщения)	Включает (по умолчанию) или отключает функцию системного журнала Syslog.
Facility Code (Код объекта)	Выбирает код объекта, назначенный для сообщений системного журнала Rack PDU (по умолчанию – **User** (Пользователь)). **ПРИМЕЧАНИЕ:** Параметр **User** (Пользователь) лучше всего определяет настройки сообщений Syslog, посылаемых Rack PDU. **Не изменяйте** эти настройки, не проконсультировавшись с администратором Syslog или системным администратором.
Severity Mapping (Сопоставление степени опасности)	Сопоставляет каждый уровень опасности событий Rack PDU или среды с соответствующими приоритетами Syslog. Необходимости менять сопоставления нет. Следующие определения взяты из RFC3164: • **Emergency** (Аварийная ситуация): Система не работает • **Alert** (Оповещение): Следует незамедлительно предпринять меры • **Critical** (Критический): Критичные условия • **Error** (Ошибка): Условия ошибки • **Warning** (Предупреждение): Условия предупреждения • **Notice** (Примечание): Нормальные условия, но требуют внимания • **Informational** (Информационный): Информационное сообщение • **Debug** (Отладка): Сообщения уровня отладки Ниже приведены настройки, установленные по умолчанию для параметров **Local Priority** (Локальный приоритет): • Параметр **Severe** соответствует **Critical** (Критический) • Параметр **Warning** соответствует **Warning** (Предупреждение) • Параметр **Informational** соответствует **Info** (Информация) **ПРИМЕЧАНИЕ:** Чтобы отключить сообщения Syslog, см. Конфигурирование действий для событий.

Пример теста и формата Syslog.

Путь: Logs > Syslog > test

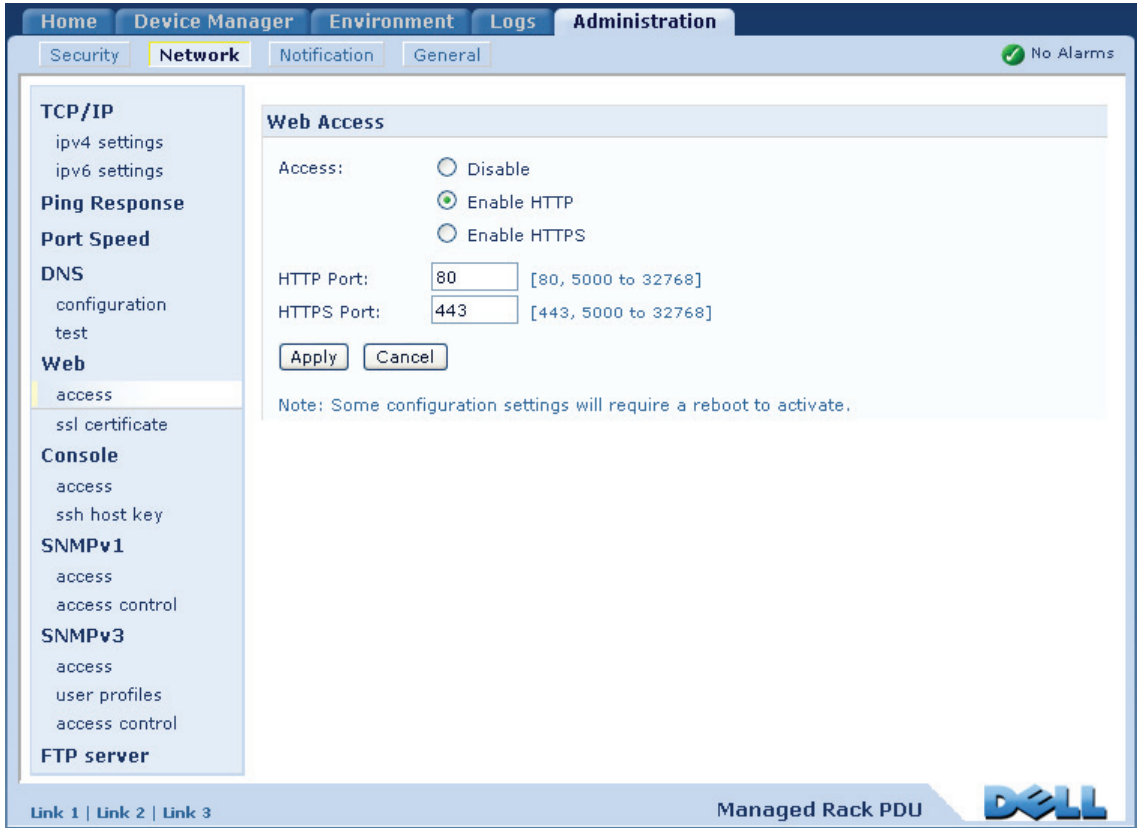
Отправляет тестовое сообщение на серверы Syslog, сконфигурированные в опции **servers** (серверы).

1. Выберите уровень опасности, который будет присвоен тестовому сообщению.
2. Определите тестовое сообщение согласно требуемым полям сообщения.

– Приоритет (PRI): приоритет Syslog, указанный для сообщаемого события, а также код объекта сообщений, отправляемых устройством Rack PDU.
– Заголовок: отметка времени и IP-адрес Rack PDU.
– Тело сообщения (MSG):
  • Поле TAG, за которым следует двоеточие и пробел, определяет тип события.
  • Поле CONTENT представляет собой текст сообщения о событии, за которым следует (дополнительно) пробел и код события.

  Например: **`Dell: Test Syslog`** is valid.

Администрирование: Сетевые характеристики



Настройки TCP/IP линии связи

Настройки TCP/IP

Путь: Administration > Network > TCP/IP

Параметр **TCP/IP** в левом меню навигации, заданный по умолчанию при выборе пункта **Network** (Сеть) в верхней строке меню, отображает текущий адрес IPv4, маску подсети, шлюз по умолчанию, адрес MAC и режим загрузки Rack PDU.

Сведения о DHCP и параметрах настройки DHCP – см. **RFC2131** и **RFC2132**.

Настройка	Описание
Enable (Включить)	С помощью данного флага включается и отключается IPv4.
Manual (Вручную)	Конфигурирование IPv4 вручную путем задания IP-адреса, маски подсети и шлюза по умолчанию.

1. Обычно параметры, заданные по умолчанию для указанных трех настроек, не требуют изменения:
   - **Vendor Class** (Класс поставщика): DELL
   - **Client ID** (Идентификатор клиента): MAC-адрес устройства Rack PDU, однозначно определяющий ее в локальной вычислительной сети (LAN)
   - **User Class** (Класс пользователя): Название модуля микропрограммы приложения

Настройка	Описание
BOOTP	Сервер BOOTP задает настройки TCP/IP. Каждые 32 секунды устройство Rack PDU запрашивает сетевые настройки у любого из серверов BOOTP: • Если Rack PDU получает достоверный отклик, оно запускает сетевые службы. • Если Rack PDU обнаруживает BOOTP-сервер, но запрос данного сервера не удается, либо превышает время ожидания, Rack PDU прекращает запрос сетевых настроек до момента перезапуска. • По умолчанию, если настройки сети предварительно заданы, а устройство Rack PDU не получает достоверного отклика на пять своих запросов (исходный и четыре повторных), оно будет использовать ранее установленные настройки, то есть останется доступным. Нажмите **Next>>** (Далее) и перейдите на страницу конфигурации BOOTP, чтобы изменить количество предпринимаемых попыток или действий в случае, если все эти попытки окажутся неудачными [1]: • **Maximum retries** (Максимальное число попыток): Укажите число попыток, предпринимаемых в случае получения недостоверных откликов, или выберите ноль (0) в случае неограниченного количества попыток. • **If retries fail** (Если попытки неудачны): Выберите **Use prior settings** (Использовать первичные настройки) (по умолчанию) или **Stop BOOTP request** (Остановить запрос BOOTP).

1. Обычно параметры, заданные по умолчанию для указанных трех настроек, не требуют изменения:
   •**Vendor Class** (Класс поставщика): DELL
   •**Client ID** (Идентификатор клиента): MAC-адрес устройства Rack PDU, однозначно определяющий ее в локальной вычислительной сети (LAN)
   •**User Class** (Класс пользователя): Название модуля микропрограммы приложения

Настройка	Описание
DHCP	Настройка по умолчанию. Каждые 32 секунды устройство Rack PDU запрашивает сетевые настройки у любого из серверов DHCP: • Если Rack PDU получает достоверный отклик, файл cookie поставщика из сервера DHCP для получения выделяемых параметров и запуска сетевых служб не требуется. • Если устройство Rack PDU обнаруживает DHCP-сервер, но запрос данного сервера не удается либо превышает время ожидания, оно прекращает запрос сетевых настроек до момента перезапуска[1]. • **Require vendor specific cookie to accept DHCP Address** (Запрашивать файл cookie, характерный для поставщика, чтобы принять адрес DHCP): Поставив этот флажок, вы можете затребовать от сервера DHCP файл cookie, поставляющий информацию в Rack PDU.

1. Обычно параметры, заданные по умолчанию для указанных трех настроек, не требуют изменения:
   •**Vendor Class** (Класс поставщика): DELL
   •**Client ID** (Идентификатор клиента): MAC-адрес устройства Rack PDU, однозначно определяющий ее в локальной вычислительной сети (LAN)
   •**User Class** (Класс пользователя): Название модуля микропрограммы приложения

Параметры отклика DHCP

Каждый достоверный отклик DHCP содержит параметры, задающие настройки TCP/IP, необходимые для работы Rack PDU в сети, а также другую информацию, влияющую на работу Rack PDU.

Vendor Specific Information (Сведения о поставщике) (параметр 43). Rack PDU использует этот параметр отклика DHCP для определения достоверности ответа. Данный параметр содержит специальные параметры в формате TAG/LEN/DATA, называемые Cookie поставщика. По умолчанию этот параметр отключен.

- **Vendor Cookie. Tag 1, Len 4, Data "1APC"**
  Параметр 43 сообщает Rack PDU, что сервер DHCP настроен на обслуживание устройств Dell Rack PDU.
  Далее в шестнадцатеричном формате представлен пример информации, определяемой поставщиком, в которой содержатся данные cookie поставщика:

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

Параметры TCP/IP. Rack PDU использует для определения своих настроек TCP/IP следующие параметры, содержащиеся в достоверном отклике DHCP. Все указанные параметры, за исключением первого, описаны в **RFC2132**.

- **IP Address** (из поля **yiaddr** отклика DHCP, описанного в **RFC2131)**: IP-адрес, выдаваемый сервером DHCP Rack PDU.
- **Subnet Mask** (параметр 1): Маска подсети указывает параметры, необходимые для работы Rack PDU в сети.
- **Router**, т.е. шлюз по умолчанию (параметр 3): Адрес шлюза по умолчанию, необходимый для работы Rack PDU в сети.
- **IP Address Lease Time** (параметр 51): Промежуток времени, за который выдается IP-адрес для Rack PDU.
- **Renewal Time, T1** (параметр 58): Время, которое Rack PDU должно ожидать после выдачи IP-адреса, перед тем как оно сможет запросить обновление этого назначения.

- **Rebinding Time, T2** (параметр 59): Время, которое Rack PDU должно ожидать после выдачи IP-адреса, перед тем как оно сможет повторить попытку продлить использование адреса.

Другие параметры. Rack PDU также использует следующие параметры, содержащиеся в достоверном отклике DHCP. Все указанные параметры, за исключением последнего, описаны в **RFC2132**.

- **Network Time Protocol Servers** (параметр 42): Rack PDU может использовать до двух NTP-серверов: первичный (основной) и вторичный (вспомогательный).
- **Time Offset** (параметр 2): Сдвиг времени подсети Rack PDU относительно универсального координированного времени (UTC), задаваемый в секундах.
- **Domain Name Server** (параметр 6): Rack PDU может использовать до двух серверов доменных имен (DNS) (первичный и вторичный).
- **Host Name** (параметр 12): Имя хост-узла, которое использует Rack PDU (максимальная длина – 32 символа).
- **Domain Name** (параметр 15): Доменное имя, которое будет использовать Rack PDU (максимум 64 символа).
- **Boot File Name** (из поля **file** отклика DHCP, описанного в **RFC2131**): Полностью определенный путь до пользовательского файла конфигурации (.ini-файла), используемого при загрузке. Поле **siaddr** отклика DHCP определяет IP-адрес сервера, с которого Rack PDU осуществляет загрузку .ini-файла. После загрузки Rack PDU использует .ini-файл в качестве загрузочного файла с целью изменения настроек.

Путь: Administration > Network > TCP/IP > IPv6 settings

Настройка	Описание
Enable (Включить)	С помощью данного флага включается и отключается IPv6.
Manual (Вручную)	Конфигурирование IPv6 вручную путем задания IP-адреса и шлюза по умолчанию.
Auto Configuration (Автоматическая конфигурация)	При выборе параметра «Автоматическая конфигурация» система получает префиксы адресов от маршрутизатора (если таковой имеется). Она использует указанные префиксы для автоматического конфигурирования IPv6-адресов.

Настройка	Описание
DHCPv6 Mode (Режим DHCPv6)	**Router Controlled (Управляемый маршрутизатор)**: Выбор указанного режима означает, что DHCPv6 управляется флагами Managed (M) и Other (O), получаемыми в сообщениях маршрутизатора IPv6. При получении сообщения маршрутизатора сетевая плата управления проверяет, выставлены ли в нем флаги M или O. Сетевая плата управления анализирует состояние «битов» M (флаг Managed Address Configuration (Конфигурация управляемого адреса)) и O (флаг Other Stateful Configuration (Другая конфигурация с сохранением информации)) для следующих случаев: • *Ни один флаг не задан*: Показывает, что сеть не имеет инфраструктуры DHCPv6. Сетевая плата управления использует сообщения маршрутизатора и ручные настройки для получения адресов, не являющихся link-local (используемых для связи в пределах одного сегмента сети), а также другие настройки. • *Заданы флаги M или M и O*: В этом случае имеется полная конфигурация адреса DHCPv6. DHCPv6 используется для получения адресов И прочих настроек конфигурации. Этот режим называется DHCPv6 stateful (с сохранением адресов). Если получен флаг M, конфигурация адреса DHCPv6 остается действительной до того момента, пока рассматриваемый интерфейс не будет закрыт. Такой режим остается в действии, даже если последующие пакеты сообщений маршрутизатора не будут содержать флага M. Если первым будет получен флаг O, а затем – флаг M, сетевая плата управления произведет полную конфигурацию адреса по получении флага M. • *Задан только флаг O:* В этом случае сетевая плата управления отсылает пакет DHCPv6 Info-Request (пакет запроса информации). DHCPv6 будет использоваться для конфигурирования «других» параметров (таких как местоположение DNS-серверов), но НЕ для получения адресов. Этот режим называется «DHCPv6 stateless» (без сохранения адресов). **Address and Other Information** (Адрес и другие сведения): При включении этой радио-кнопки DHCPv6 будет использоваться для получения адресов И других параметров настройки. Этот режим называется «DHCPv6 stateful» (с сохранением адресов). **Non-Address Information Only** (Только сведения, за исключением адресов): При включении этой радио-кнопки DHCPv6 будет использоваться для конфигурации «других» параметров (таких как местоположение DNS-серверов), НО не для получения адресов. Этот режим называется «DHCPv6 stateless» (без сохранения адресов). **Never** (Никогда): Выбор данного параметра отключает DHCPv6.

Ответ ping

Путь: Administration > Network > Ping Response

Поставьте флаг «Включить» для параметра **IPv4 Ping Response** (Ответ ping IPv4), чтобы сетевая плата управления могла отвечать на сигналы эхо-тестирования. Если флаг снят, сетевая плата управления не будет откликаться на эхо-запросы. Такой режим не применяется для IPv6.

Скорость передачи порта

Путь: Administration > Network > Port Speed

Параметр **Port Speed** (Скорость порта) задает скорость обмена данными порта TCP/IP.

- При задании параметра **Auto-negotiation** (Автосогласование) (задается по умолчанию) устройства Ethernet определяют максимально возможную скорость передачи данных, при этом если скорости передачи данных двух устройств не совпадают, обмен будет вестись на более низкой скорости.
- Как вариант, можно выбрать скорость передачи 10 или 100 мбит/с, задав при этом полу-дуплексный (в каждый момент данные передаются только в одном направлении) или дуплексный (данные передаются в обоих направлениях по одному каналу одновременно) режим.

DNS

Путь: Administration > Network > DNS > *options*

Используйте параметры пункта **DNS** для конфигурирования и тестирования системы доменных имен (DNS):

- Выберите **Primary DNS Server** (Первичный DNS-сервер) или **Secondary DNS Server** (Вторичный DNS-сервер) для задания адресов IPv4 и IPv6 основного или дополнительного DNS-серверов. Чтобы отправлять электронную почту с помощью Rack PDU, необходимо, как минимум, указать IP-адрес первичного DNS-сервера.
  - Rack PDU ожидает отклика от первичного или вторичного DNS-серверов (если вторичный DNS-сервер указан) в течение 15 секунд. Если Rack PDU не получает отклика в указанное время, электронное письмо не будет отправлено. Поэтому используйте DNS-серверы в том же или соседнем сегменте, где расположено устройство Rack PDU (но не в других удаленных сегментах сети [WAN]).
  - После задания IP-адресов DNS-серверов проверьте, чтобы система DNS работала правильно, для чего введите DNS-имя компьютера в вашей сети и посмотрите IP-адрес этого компьютера.
- **Host Name** (Имя хоста): После задания здесь имени хост-узла и указания доменного имени в поле **Domain Name** (Имя домена), пользователь может указывать имя хост-узла в любом поле интерфейса Rack PDU (кроме адресов электронной почты), которые работают с доменным именем.
- **Domain Name (IPv4)** (Имя домена (IPv4)): Необходимо указать доменное имя только здесь. Устройство Rack PDU добавит указанное доменное имя во всех других связанных с доменными именами полях интерфейса (кроме адреса электронной почты) только тогда, когда будет введено имя хост-узла.
  - Чтобы иметь возможность задавать все значения расширения указанного имени хост-узла путем добавления доменного имени, задайте значение доменного имени по умолчанию, `somedomain.com`, или значение `0.0.0.0`.

  - Чтобы изменить расширение конкретного имени хост-узла (например, при определении приемника прерываний), поставьте точку (trailing period). Rack PDU распознает имя хост-узла с точкой (например, *mySnmpServer.*) как полноценное доменное имя и не будет добавлять доменное имя.
- **Domain Name (IPv6)** (Имя домена (IPv6)): Определяет доменное имя IPv6.
- Выберите пункт **test** (тестирование), чтобы направить DNS-запрос, тестирующий настройки ваших DNS-серверов:
  - В качестве **Query Type** (Тип запроса) укажите один из следующих типов запросов DNS:
    - **by Host** (по имени хост-узла): URL-имя сервера
    - **by FQDN** (по полному доменному имени): полное доменное имя
    - **by IP** (по IP-адресу): IP-адрес сервера
    - **by MX** (по MX): система обмена почтой (Mail Exchange), используемая сервером
  - В качестве параметра **Query Question** (Вопрос в запросе) укажите значение, которое будет использовано для выбранного типа запроса:

Выбранный тип запроса	**Используемый запрос**
by Host	Адрес URL
by FQDN	Полное доменное имя, *my_server.my_domain*.
by IP	IP-адрес
by MX	Адрес Mail Exchange

  - Посмотрите результаты тестирования запроса DNS в поле **Last Query Response** (Последний ответ на запрос).

Web

Путь: Administration > Network > Web > *options*

Параметр	Описание

access (доступ)	Чтобы активировать сделанные изменения, выйдите из программы Rack PDU:
	• **Disable** (Отключить): отключает доступ к веб-интерфейсу. (Чтобы вновь открыть доступ, войдите в интерфейс командной строки и введите команду **`http -S enable`**. Чтобы получить доступ к протоколу HTTPS, введите команду **`https -S enable`**.)
	• **Enable HTTP** (Включить HTTP) (по умолчанию): Делает доступным обмен данными по протоколу передачи гипертекста (HTTP), который обеспечивает Web-доступ по имени пользователя и паролю, но не шифрует имена пользователей, пароли и передаваемые данные.
	• **Enable HTTPS** (Включить HTTPS): Делает доступным обмен данными по протоколу передачи гипертекста (HTTPS) на уровне защищенных сокетов (SSL). Протокол SSL кодирует имена пользователей, пароли и передаваемые данные, а также аутентифицирует Rack PDU по цифровому сертификату. При включенном режиме HTTPS браузер отображает маленький значок замка.
	
	Описание различных способов использования цифровых сертификатов – см. «Создание и установка цифровых сертификатов» в разделе Приложение Б: Руководство по безопасности.
	
	HTTP Port (Порт HTTP): Порт TCP/IP (по умолчанию 80), используемый Rack PDU для обмена данными по протоколу HTTP.
	
	HTTPS Port (Порт HTTPS): Порт TCP/IP (по умолчанию 443), используемый Rack PDU для обмена данными по протоколу HTTPS.
	
	С целью обеспечения дополнительной защиты можно изменить значения настроек любого из указанных портов, выбрав неиспользуемый порт в диапазоне от 5000 до 32768. Для задания номера порта необходимо поставить двоеточие (:) в адресном поле программы-браузера. Например, для номера порта 5000 и IP-адреса 152.214.12.114:
	`http://152.214.12.114:5000`
	`https://152.214.12.114:5000`

Параметр	Описание
ssl certificate (сертификат ssl)	Добавление, замена и удаление сертификатов безопасности. **Состояние**: • **Not installed** (Не установлен): Сертификат не установлен, или был установлен FTP или SCP в неправильном месте. С помощью команды **Add or Replace Certificate File** (Добавить или заменить файл сертификата) установите сертификат в надлежащее место, **/ssl** на Rack PDU. • **Generating** (Генерируется): Rack PDU генерирует сертификат, поскольку не обнаружен действующий сертификат. • **Loading** (Загружается): Сертификат должен активироваться на устройстве Rack PDU. • **Valid certificate** (Действительный сертификат): Действующий сертификат был установлен или сгенерирован Rack PDU. Щелкните эту ссылку, чтобы увидеть содержимое сертификата. **Если был установлен недействительный сертификат или сертификат не был загружен при включенном SSL,** Rack PDU **генерирует сертификат по умолчанию, этот процесс может вызвать задержку обращения к интерфейсу примерно на одну минуту.** Сертификат по умолчанию можно использовать для обеспечения основных функций безопасности, путем шифрования данных, но при этом при входе в систему будет выводиться предупреждение о безопасности. **Add or Replace Certificate File** (Добавить или заменить файл сертификата): Укажите или найдите файл сертификата, созданный программой мастера безопасности Security Wizard. Описание различных способов использования цифровых сертификатов, созданных программой Security Wizard или сгенерированных Rack PDU, – см. «Создание и установка цифровых сертификатов» в разделе Приложение Б: Руководство по безопасности. **Remove** (Удалить): Удаляет текущий сертификат.

Консоль

Путь: Administration > Network > Console > *options*

Параметр	Описание
access (доступ)	Выберите один из следующих вариантов доступа с использованием протокола Telnet или Secure SHell (SSH): • **Disable** (Отключить): Отключает доступ к интерфейсу командной строки. • **Enable Telnet** (Включить Telnet) (настройка по умолчанию): Протокол Telnet передает имена пользователей, пароли и данные без шифрования. • **Enable SSH** (Включить SSH): Протокол SSH передает имена пользователей, пароли и данные в закодированном виде, обеспечивая защиту от попыток перехвата, подделки или искажения данных в процессе обмена. Сконфигурируйте порты, используемые этими протоколами: • **Telnet Port** (Порт Telnet): Порт Telnet (по умолчанию 23) используется для обмена данными с Rack PDU. С целью обеспечения дополнительной защиты можно изменить настройку порта, выбрав неиспользуемый порт в диапазоне от 5000 до 32768. Для определения порта, не заданного по умолчанию, необходимо использовать двоеточие (:) или пробел, как требует того клиентская программа Telnet. Например, для порта 5000 и IP-адреса 152.214.12.114 клиентская программа Telnet требует использования одной из следующих команд: `telnet 152.214.12.114:5000` `telnet 152.214.12.114:5000` • **SSH Port** (Порт SSH): Порт SSH (по умолчанию 22) используется для обмена данными с Rack PDU. С целью обеспечения дополнительной защиты можно изменить настройку порта, выбрав неиспользуемый порт в диапазоне от 5000 до 32768. Формат команд командной строки, необходимых для задания порта, не используемого по умолчанию, приведен в документации программы-клиента SSH.

Параметр	Описание
ssh host key (хост-ключ ssh)	**Status** (Состояние) показывает состояние хост-ключа (секретного ключа): • **SSH Disabled отсутствуют используемые ключи хоста.** (SSH отключено): В отключенном режиме SSH не может использовать хост-ключ. • **Generating** (Генерируется): Rack PDU создает хост-ключ, поскольку не было найдено ни одного действующего ключа. • **Loading** (Загружается): Хост-ключ должен активироваться на устройстве Rack PDU. • **Valid** (Действительный): Один из следующих хост-ключей находится в директории **/ssh** (рекомендуемое местоположение на устройстве Rack PDU): •1024- или 2048-битовый хост-ключ создан программой Security Wizard •2048-битовый хост-ключ RSA создан Rack PDU **Add or Replace** (Добавить или заменить): Найти или загрузить файл хост-ключа, созданного программой Security Wizard. Для использования программы Security Wizard см. Приложение Б: Руководство по безопасности. **ПРИМЕЧАНИЕ:** Чтобы сократить время, необходимое для включения SSH, создайте и загрузите хост-ключ заблаговременно. **Если вы включили SSH, не загрузив хост-ключ,** Rack PDU **потратит примерно одну минуту для создания ключа, и сервер SSH будет недоступен всё это время.** **Remove** (Удалить): Удаляет текущий хост-ключ.

Чтобы использовать SSH, необходимо иметь установленный клиент SSH. Большинство платформ Linux и UNIX имеют в своем составе клиент SSH, но операционная система Microsoft Windows не имеет такового. Известны клиентские программы различных производителей.

SNMP

Все имена пользователей, пароли и имена сообществ для SNMP передаются по сети в текстовом формате. Если сеть требует высокую степень защиты, отключите доступ SNMP или установите для всех сообществ доступ на чтение. (Сообщество с доступом на чтение может получать информацию о статусе и использовать прерывания SNMP.)

Подробную информацию об укреплении и управлении безопасностью системы см. в разделе Приложение Б: Руководство по безопасности.

SNMPv1

Путь: Administration > Network > SNMPv1 > *options*

Параметр	Описание
access (доступ)	**Enable SNMPv1 Access** Включает SNMP версии 1 в качестве способа обмена данными с указанным устройством.

Параметр	Описание
access control (управление доступом)	Допускается конфигурировать до четырех записей управления доступом, чтобы определить, какая из сетевых систем управления (NMS) имеет доступ к данному устройству. Открываемая страница управления доступом по умолчанию назначает один параметр для каждого из четырех доступных сообществ SNMPv1; эти параметры можно изменить таким образом, чтобы применить к каждому из сообществ более одной записи для обеспечения доступа путем предоставления нескольких конкретных адресов IPv4 и IPv6, имен хост-узлов и масок IP-адресов. Чтобы отредактировать настройки управления доступа для сообщества, щелкните имя этого сообщества. • Если оставить параметры управления доступом, заданные по умолчанию, неизменными, это сообщество будет обладать доступом к данному устройству из любой точки сети. • Если задать несколько записей управления доступом для одного имени сообщества, ограничение в виде четырех записей потребует, чтобы одно или несколько сообществ не имели записей управления доступом. Если для сообщества не задана запись управления доступом, указанное сообщество не будет иметь доступа к данному устройству. **Community Name** Имя, которое система NMS должна использовать для доступа. Максимальная длина составляет 15 символов ASCII, имена, заданные по умолчанию для четырех сообществ, следующие: **`public`**, **`private`**, **`public2`** и **`private2`**. **NMS IP/Host Name** Адрес IPv4 или IPv6, маска IP-адреса или имя хост-узла, который управляет доступом систем NMS. Имя хост-узла или определенный IP-адрес (такой как 149.225.12.1) открывает доступ только системе NMS в данном сегменте сети. IP-адреса, содержащие 255, ограничивают доступ следующим образом: • 149.225.12.**255**: Доступ NMS только в сегменте 149.225.12. • 149.225.**255.255**: Доступ NMS только в сегменте 149.225. • 149.**255.255.255**: Доступ NMS только в сегменте 149. • 0.0.0.0 (настройки по умолчанию), которые могут быть также представлены в виде 255.255.255.255: Доступ любой системы NMS в любом сегменте. **Access Type** (Тип доступа): Действия, которые может выполнять NMS в сообществе. • **Read** (Чтение): только получать (GET) информацию, в любое время • **Write** (Запись): получать (GET) в любое время и размещать (SET) информацию, если другие пользователи не работают в веб-интерфейсе или в интерфейсе командной строки. • **Write+** (Запись+): получать (GET) и размещать (SET) информацию в любое время. • **Disable** (Отключить): запрещено получать (GET) и размещать (SET) информацию в любое время.

SNMPv3

Путь: Administration > Network > SNMPv3 > *options*

Для запросов GET и SET протокола SNMP и приемников прерываний в SNMPv3 при идентификации пользователей используется система профилей пользователей. Пользователь SNMPv3 должен иметь профиль пользователя, назначенный в программе MIB для выполнения операций GET/SET, просмотра MIB и получения прерываний.

Для использования SNMPv3 необходимо иметь программу MIB с поддержкой SNMPv3.

Rack PDU поддерживает аутентификацию SHA или MD5, а также шифрование AES или DES.

Параметр	Описание
access (доступ)	**SNMPv3 Access** (Доступ SNMPv3): Включает SNMPv3 в качестве способа обмена данными с указанным устройством.

Параметр	Описание
user profiles (профили пользователя)	По умолчанию содержит настройки четырех пользовательских профилей, сконфигурированных с именами пользователей от **dell snmp profile1** до **dell snmp profile4**, не требует аутентификации и конфиденциальности (не использует шифрования). Чтобы изменить следующие настройки пользовательского профиля, щелкните имя пользователя в указанном списке. **User Name** (Имя пользователя): Идентификатор профиля пользователя. SNMP версии 3 отображает функции GET, SET и обеспечивает захват в пользовательский профиль путем сличения имени пользователя профиля с именем пользователя в передаваемом пакете данных. Имя пользователя может содержать до 32 символов ASCII. **Authentication Passphrase** (Парольная фраза аутентификации): Фраза, содержащая от 15 до 32 символов ASCII (**`фраза dell auth`**, принята по умолчанию), которая удостоверяет, что NMS, обменивающаяся данными с данным устройством через SNMPv3 является именно той системой NMS, за которую она себя выдает; данное сообщение не было искажено в ходе передачи и было передано вовремя, не было задержано и не было скопировано и послано вторично поздней, в несоответствующее время. **Privacy Passphrase** (Конфиденциальная парольная фраза): Фраза от 15 до 32 символов ASCII (по умолчанию **`фраза dell crypt passphrase`**), которая гарантирует конфиденциальность данных (с помощью шифрования), передаваемых NMS на данное устройство или получаемых от него по протоколу SNMPv3. **Authentication Protocol (Протокол аутентификации):** Протокол SNMPv3, реализованный в Dell, поддерживает аутентификацию SHA и MD5. Аутентификация не выполняется до тех пор, пока не будет задан протокол аутентификации. **Privacy Protocol** (Протокол конфиденциальности): Протокол SNMPv3, реализованный в Dell, поддерживает в качестве протоколов шифрования и дешифрования данных протоколы AES и DES. Конфиденциальность передаваемых данных требует, чтобы был задан протокол конфиденциальности и чтобы в запросе NMS была передана фраза-пароль конфиденциальности. Если протокол конфиденциальности активирован, но NMS не передала фразу-пароль конфиденциальности, запрос SNMP не будет зашифрован. **Примечание:** Нельзя выбрать протокол конфиденциальности, если не выбран протокол аутентификации.

Параметр	Описание
access control (управление доступом)	Допускается конфигурировать до четырех записей управления доступом, чтобы определить, какая из систем NMS имеет доступ к данному устройству. Открываемая страница управления доступом по умолчанию назначает по одной записи для каждого из четырех профилей пользователей; эти записи можно изменить таким образом, чтобы применить к каждому из профилей более одной записи, с тем чтобы обеспечить доступ путем предоставления нескольких адресов IP, имен хост-узлов и масок IP-адресов. • Если оставить заданные по умолчанию записи управления доступом для данного профиля пользователя без изменения, все системы NMS, использующие этот профиль, будут иметь доступ к указанному устройству. • Если задать несколько записей управления доступа для одного профиля пользователя, ограничение в виде четырех записей потребует, чтобы один или несколько профилей не имели записей управления доступом. Если для профиля пользователя не указана ни одна запись управления доступом, то NMS, использующие данный профиль, не будут иметь доступ к указанному устройству. Чтобы отредактировать настройки управления доступа для профиля пользователя, щелкните имя этого пользователя. **Access** (Доступ): Поставьте флажок **Enable** (Включить), чтобы активировать управление доступом, определяемое параметрами, указанными в данной записи. **User Name** (Имя пользователя): В раскрывающемся списке выберите профиль пользователя, для которого будет применена данная запись управления доступом. Можно выбрать любые из четырех имен пользователей, которые были сконфигурированы с помощью команды **user profiles** в левом меню навигации. **NMS IP/Host Name** (Имя IP-адреса/хоста NMS): IP-адрес, маска IP-адреса или имя хост-узла, который управляет доступом NMS. Имя хост-узла или определенный IP-адрес (такой как 149.225.12.1) открывает доступ только системе NMS в данном сегменте сети. Маска IP-адреса, которая содержит число 255, ограничивает доступ следующим образом: • 149.225.12.**255**: Доступ NMS только в сегменте 149.225.12. • 149.225.**255.255**: Доступ NMS только в сегменте 149.225. • 149.**255.255.255**: Доступ NMS только в сегменте 149. • 0.0.0.0 (настройки по умолчанию), которые могут быть также представлены в виде 255.255.255.255: Доступ любой системы NMS в любом сегменте.

Сервер FTP

Путь: Administration > Network > FTP Server

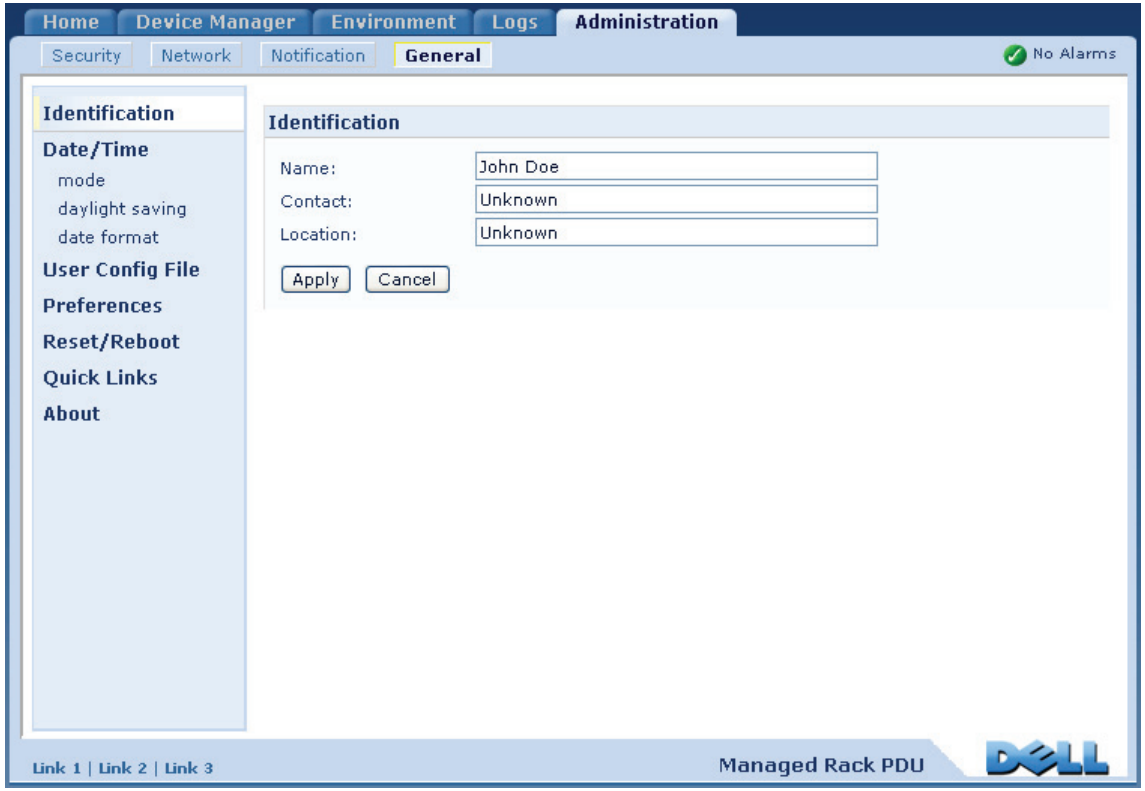
Настройки **FTP Server** (FTP-сервер) открывают (по умолчанию) или закрывают доступ к FTP-серверу и определяют порт TCP/IP (по умолчанию – 21), который используется FTP-сервером для обмена данными с устройством Rack PDU. FTP-сервер использует как указанный порт, так и порт с номером на единицу меньше.

С целью повышения безопасности можно изменить настройку **Port** (Порт) на номер любого неиспользуемого порта в диапазоне от 5001 до 32768. Для выбора номера порта, отличного от заданного по умолчанию, необходимо использовать символ двоеточия (:). Например, для порта 5001 и IP-адреса 152.214.12.114 команда должна иметь вид **`ftp 152.214.12.114:5001`**.

Протокол FTP передает файлы без их шифрования. С целью повышения безопасности отключите FTP-сервер и пересылайте файлы с помощью протокола SCP. Выбор и конфигурирование Secure SHell (SSH) автоматически включает SCP.

Подробную информацию об укреплении и управлении безопасностью системы см. в разделе Приложение Б: Руководство по безопасности.

Администрирование: Основные функции



Идентификация

Путь: Administration > General > Identification

Определите **Name** (имя устройства), **Location** (местоположение устройства) и **Contact** (лицо, ответственное за устройство) агента SNMP Rack PDU. Эти настройки и значения используются для объектных идентификаторов (OIDs) MIB-II **sysName**, **sysContact** и **sysLocation**.

Дополнительные сведения о MIB-II OIDs см. в Справочнике Dell Management Information Base (MIB).

Задание даты и времени

Установки

Путь: Administration > General > Date & Time > mode

Задает время и дату, используемые Rack PDU. Можно изменять текущие настройки вручную или с помощью сервера сетевого протокола службы времени (NTP):

- **Manual Mode (Ручной режим)**: Выполните одно из следующих действий:
  - Введите дату и время для Rack PDU.
  - Поставьте флажок **Apply Local Computer Time (Применение локального времени ПК)**, чтобы дата и время совпадали с компьютерными часами.
- **Synchronize with NTP Serve (Синхронизировать с NTP-сервером)**: Дает возможность NTP-серверу задавать дату и время Rack PDU.

Настройка	Описание
Primary NTP Server (Первичный NTP-сервер)	Введите IP-адрес или доменное имя первичного NTP-сервера.
Secondary NTP Server (Вторичный NTP-сервер)	Введите IP-адрес или доменное имя вторичного NTP-сервера, если таковой имеется.
Time Zone (Часовой пояс)	Выберите часовой пояс. Количество часов, предшествующее каждому часовому поясу, указанному в списке, показывает смещение относительно универсального координированного времени (UTC), известного ранее как время по Гринвичу.
Update Interval (Интервал обновления)	Задает промежуток времени в часах, определяющий, как часто Rack PDU будет обращаться к NTP-серверу для обновления данных. *Минимальное значение*: 1; *Максимальное значение*: 8760 (1 год).
Update Using NTP Now (Немедленное обновление данных при помощи NTP)	Запускает моментальное обновление даты и времени по NTP-серверу.

Переход на летнее время

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

Позволяет использовать летнее время США (DST) или указать собственное поясное летнее время в соответствии с правилами установки летнего времени в вашем регионе. По умолчанию параметр DST отключен.

При настройке летнего времени (DST):

- Если местное летнее время всегда начинается и заканчивается в четвертый день недели определенного месяца (например, в четвертое воскресенье), выберите параметр **Fourth/Last**. Если в данном году в указанном месяце есть пятое воскресенье, переход на летнее время все равно произойдет на четвертое воскресенье.
- Если местное летнее время всегда начинается и заканчивается в последний, четвертый или пятый день недели определенного месяца, выберите параметр **Fifth/Last**.

Формат

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

Выберите цифровой формат, в котором будут отображаться все даты данного пользовательского интерфейса. В формате каждая буква m (месяц), d (день) и y (год) отображают одну цифру. Однозначные дни и месяцы отображаются с ведущим нулем (перед значащей цифрой).

Использование файла .ini

Путь: Administration > General > User Config File

Используйте настройки одного Rack PDU (Устройство распределения питания для монтажа в стойку), чтобы сконфигурировать другое. Возьмите файл config.ini, содержащий настройки Rack PDU, измените эти настройки (например, измените IP-адрес) и загрузите обновленный файл в новое устройство Rack PDU. Имя файла может содержать до 64 символов и должно иметь суффикс .ini.

Status (Состояние)	Показывает выполнение процесса загрузки. Загрузка будет завершена, даже если файл содержит ошибки, но система сообщит об имеющихся ошибках в журнале событий.
Upload (Загрузить)	Найдите исправленный файл и загрузите его, так чтобы указанное устройство Rack PDU могло использовать его для задания собственных настроек.

О том, как получить и редактировать файл для конфигурации Rack PDU, см. Экспорт параметров конфигурации.

Вместо загрузки файла в Rack PDU вы можете экспортировать его в несколько Rack PDU, используя скрипт SCP или командный файл FTP.

Журнал событий и единицы измерения температуры

Путь: Administration > General > Preferences

Выделения цветом текста в журнале событий

По умолчанию эта функция отключена. Поставьте флажок **Event Log Color Coding (Цветовая кодировка журнала событий)**, чтобы получить возможность выделять цветом сообщения о неисправностях, регистрируемые в журнале событий. Записи системных событий и изменения конфигурации не изменят свой цвет.

Цвет текста	Опасность неисправности
Красный	**Critical**: Критический аварийный сигнал, требующий немедленных действий.
Оранжевый	**Warning**: Тревожная сигнализация требует внимания, поскольку не решенная вовремя проблема может привести к потере данных и порче оборудования, если не устранить вызвавшую ее причину.
Зеленый	**Alarm Cleared**: Условия, которые вызвали тревогу, устранены.
Черный	**Normal**: Сигналов тревоги нет. Rack PDU и все подключенные к ней устройства работают нормально.

Изменение температурной шкалы, заданной по умолчанию.

Выберите шкалу измерения температуры (по Фаренгейту или по Цельсию), на которой на пользовательском интерфейсе будут отображаться измеренные температуры.

Восстановление настроек Rack PDU

Путь: Administration > General > Reset/Reboot

Действие	Описание
Перезагрузить интерфейс управления	Перезапуск интерфейса Rack PDU.
Сбросить все[1]	Уберите флажок в поле **Exclude TCP/IP (Исключить TCP/IP)**, чтобы сбросить все настройки конфигурации; поставьте флажок **Exclude TCP/IP**, чтобы сбросить все настройки, кроме настроек TCP/IP
Только перезапустить[1]	**TCP/IP settings (Настройки TCP/IP)**: Задайте для настроек TCP/IP значения **DHCP & BOOTP** — значения, принятые по умолчанию, которые требуются для того, чтобы устройство Rack PDU получало свои настройки TCP/IP от серверов DHCP или BOOTP. См. раздел Настройки TCP/IP линии связи.
	Event configuration (Конфигурация события): Сброс всех изменений конфигурации событий в значения, принятые по умолчанию, по событию или группе событий.
	RPDU to Defaults (Значения ИБП по умолчанию): Сбрасывает только настройки ИБП в исходные значения, сетевые настройки не меняются.
1. Сброс параметров может занять до одной минуты.	

Конфигурирование связей

Путь: Administration > General > Quick Links

Выберите вкладку **Administration (Администрирование)**, пункт **General (Общие)** в верхнем меню и пункт **Quick Links (Быстрые ссылки)** в левом меню навигации, чтобы иметь возможность увидеть и изменить связи URL, показываемые в нижнем левом углу каждого экрана интерфейса.

По умолчанию, указаны три ссылки, ведущие на веб-страницы:

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

Чтобы изменить конфигурацию одного из указанных ниже элементов, щелкните имя ссылки в столбце **Display (Дисплей)**:

- **Display**: Краткое имя ссылки, отображаемое на каждой странице интерфейса
- **Name**: Имя, которое полностью определяет назначение или сетевой адрес ссылки
- **Address**: Любой URL-адрес, например, URL-адрес другого устройства или сервера

О Rack PDU

Путь: Administration > General > About

Сведения об оборудовании используются при устранении неисправностей Rack PDU. Серийный номер и MAC-адрес также указаны на самой Rack PDU.

Сведения о микропрограммном обеспечении модулей Application Module, APC OS (AOS) и APC Boot Monitor указывают название, версию микропрограммы, а также дату и время создания каждого модуля. Эта информация также используется при устранении неисправностей.

Параметр **Management Uptime (Бесперебойная работа управления)** показывает продолжительность непрерывной работы интерфейса.

Экспорт параметров конфигурации

Получение и экспорт файла .ini

Краткое описание процедуры

Администратор может получать .ini-файлы устройства Rack PDU и экспортировать их в другое Rack PDU или в несколько Rack PDU.

1. Сконфигурируйте устройство Rack PDU, чтобы получить настройки, которые вы хотите экспортировать.
2. Получите .ini-файл из этого устройства Rack PDU.
3. Отредактируйте файл, изменив как минимум настройки TCP/IP.
4. Используйте протокол передачи файлов, поддерживаемый Rack PDU, для загрузки копии файла в одну или несколько Rack PDU. Для загрузки файла в несколько Rack PDU используйте скрипт FTP или SCP.

Каждое из устройств Rack PDU использует полученный файл для конфигурации собственных настроек, после чего удаляет его.

Содержание файла .ini

Файл config.ini, полученный из Rack PDU, содержит:

- *заголовки разделов* и *ключевые слова* (только поддерживаемые устройством, с которого вы получили этот файл)*:* Заголовки разделов представляют собой имена категорий, заключенные в скобки ([ ]). Ключевые слова в каждом из заголовков раздела представляют собой метки, описывающие определенные настройки Rack PDU. После каждого ключевого слова следует знак равенства и значение (принятое по умолчанию или заданное при конфигурировании).

- Ключевое слово **Override**: При заданном значении по умолчанию, данное ключевое слово препятствует экспорту одного или нескольких ключевых слов и их значений, определяемых устройством. Например, в разделе **[NetworkTCP/IP]** значение по умолчанию для слова **Override** (MAC-адрес Rack PDU) блокирует экспорт параметров **SystemIP**, **SubnetMask**, **DefaultGateway** и **BootMode**.

Подробные процедуры

Получение. Для задания и получения .ini-файла для экспорта:

1. Если возможно, используйте интерфейс Rack PDU для конфигурирования его настроек для экспорта. Непосредственное изменение содержимого .ini-файла может вызвать ошибки.
2. Для использования FTP для получения файла config.ini из сконфигурированного Rack PDU:
   a. Включите связь с Rack PDU, используя для этого его IP-адрес:

      ftp> open *ip_address*

   b. Войдите, используя учетную запись и пароль администратора.
   c. Получите файл config.ini, содержащий настройки Rack PDU:

      ftp> get *config.ini*

      Файл будет сохранен в папке, из которой был запущен FTP.

Настройка. Файл необходимо отредактировать, перед тем как экспортировать его.

1. Для редактирования файла используйте текстовый редактор.
   - Заголовки разделов, ключевые слова и предварительно заданные значения не зависят от регистра, но строковые переменные, задаваемые пользователем, зависят от регистра.
   - Чтобы указать, что значение не задано, используйте кавычки. Например, **`LinkURL1=""`** показывает, что URL специально не определен.
   - Заключайте в кавычки любые значения, которые содержат предшествующие или последующие разделы или уже заключены в кавычки.
   - Для экспорта запланированных событий конфигурируйте значения непосредственно в .ini-файле.
   - Для экспорта системного времени с максимальной точностью, если принимающее устройство Rack PDU имеет доступ к серверу протокола сетевого времени, настройте как **`enabled`** параметр **`NTPEnable`**:

     `NTPEnable=enabled`

     В противном случае, сократите время передачи, путем экспорта раздела **`[SystemDate/Time]`** в виде отдельного .ini-файла.
   - При добавлении комментариев начинайте каждую строку комментария с символа «точка с запятой» (`;`).
2. Скопируйте отредактированный файл в файл с другим именем в эту же папку:
   - Имя файла может содержать до 64 символов и должно иметь суффикс .ini.
   - Сохраните исходный отредактированный файл для использования в будущем. **Сохраненный вами файл является единственным, который содержит ваши комментарии.**

Передача файла на одно устройство Rack PDU. Для передачи .ini-файла на другое устройство Rack PDU выполните одно из указанных действий:

- В веб-интерфейсе Rack PDU-приемника выберите вкладку **Administration** (Администрирование), пункт **General** (Общие) в верхней строке меню и **User Config File** (Файл конфигурации пользователя) в левом меню навигации. Укажите полный путь к файлу или воспользуйтесь командой **Browse** (Обзор).
- Используйте любой из протоколов, поддерживаемых Rack PDU, например, FTP, FTP Client, SCP или TFTP. В приведенном примере используется протокол FTP:
  a. Из папки, содержащей копию отредактированного .ini-файла, запустите FTP, чтобы войти в устройство Rack PDU, в которое собираетесь экспортировать .ini-файл.

     ```
     ftp> open ip_address
     ```

  b. Экспортируйте копию отредактированного .ini-файла в корневой каталог Rack PDU-приемника.

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

Экспорт файла на несколько Rack PDU. Чтобы экспортировать .ini-файл на несколько Rack PDU, используйте FTP или SCP, но напишите скрипт, который содержит и повторяет операции, используемые для экспорта файла на одно устройство Rack PDU.

Сообщения о событиях загрузки и ошибках

Сообщения о событии и ошибках, связанных с ним

Следующее событие происходит в том случае, когда принимающее Rack PDU заканчивает использование .ini-файла для обновления своих настроек.

`Configuration file upload complete, with` *`number`* `valid values (Загрузка файла конфигурации завершена с` *`число`* `правильными значениями)`

Если ключевое слово, имя раздела или значения оказываются неверными, загрузка в Rack PDU завершается и выдается дополнительное сообщение об ошибке.

Текст сообщения о событии	Описание
Предупреждение по файлу конфигурации: Invalid keyword on line *number* (Неверное ключевое слово в строке *номер*). Предупреждение по файлу конфигурации: Invalid value on line *number* (Неверное значение в строке *номер*).	Строка с неверным ключевым словом или значением игнорируется.
Предупреждение по файлу конфигурации: Invalid section on line *number* (Неверная секция в строке *номер*).	Если имя секции указано неверно, все пары ключевых слов и значений в данной секции игнорируются.

Текст сообщения о событии	Описание
Предупреждение по файлу конфигурации: Keyword found outside of a section on line *number* (Ключевое слово обнаружено вне секции в строке *номер*).	Ключевое слово, введенное в начале файла (то есть перед заголовком секции), игнорируется.
Предупреждение по файлу конфигурации: Configuration file exceeds maximum size (Размер файла конфигурации превышает предельно допустимый).	Если размер файла велик, происходит неполная загрузка. Уменьшите размер файла или разбейте его на два файла и повторите загрузку еще раз.

Сообщение в файле config.ini

Устройство Rack PDU, с которого загружается файл config.ini, должно быть обнаружено успешно для включения его конфигурации. Если устройство Rack PDU отсутствует или не обнаружено, файл config.ini в соответствующей секции, вместо ключевого слова или значений, будет содержать сообщение. Например:

```
Rack PDU not discovered (Устройство Rack PDU не
обнаружено)
```

Если вы не собираетесь экспортировать конфигурацию устройства Rack PDU как часть импортированного .ini-файла, игнорируйте эти сообщения.

Ошибки, генерируемые заблокированными параметрами

При блокировке экспорта параметров ключевое слово **`Override`** и его значение генерируют сообщения об ошибке в журнале событий.

Сведения о том, какие параметры могут блокироваться, см. в разделе Содержание файла .ini.

Поскольку блокируемые параметры относятся к конкретным устройствам и не пригодны для экспорта в другие Rack PDU, игнорируйте эти сообщения об ошибках. Чтобы предотвратить появление этих сообщений, удалите строки, содержащие ключевое слово **`Override`**, и строки, содержащие блокируемые параметры. Не удаляйте и не изменяйте строки, содержащие заголовки секций.

Передача файлов

Обновление микропрограммы

Преимущества обновления микропрограммы

После обновления микропрограммного обеспечения устройства Rack PDU:

- можно исправить ошибки и повысить производительность,
- обеспечить новые функции для использования в работе.

Если на всех серверах Rack PDU, установленных в сети используется единая версия микропрограммного обеспечения, то можно быть уверенным, что все сервера единым образом поддерживают одинаковый набор функциональных возможностей.

Файлы микропрограммы

Версия микропрограммы состоит из трех модулей: модуля операционной системы (AOS), модуля приложений и модуля монитора загрузки. Каждый модуль содержит один или несколько циклических тестов (CRC), с целью предохранения данных от повреждения при передаче.

Файлы модулей операционной системы AOS, приложений и монитора загрузки, используемые устройством Rack PDU, имеют одинаковый базовый формат:

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

- **dell**: указывает на то, что это файл Dell.
- ***hardware-version***: **hw0*x*** указывает версию аппаратного обеспечения, с которым можно использовать этот двоичный файл.
- ***type***: указывает, является ли данный файл модулем операционной системы AOS, модулем приложения или модулем монитора загрузки Rack PDU.
- ***version***: номер версии файла.
- **bin**: указывает на то, что это двоичный файл.

Информацию о номере версии каждого модуля микропрограммы Rack PDU см. в разделе О Rack PDU.

Методы передачи файлов микропрограммы

Для обновления микропрограммы устройства Rack PDU используйте один из следующих методов:

- На компьютере, подключенном к сети и работающем с любой поддерживаемой операционной системой, для передачи отдельных модулей операционной системы AOS и прикладной микропрограммы используйте FTP или SCP.
- Для передачи отдельных модулей от компьютера на устройство Rack PDU, не подключенное к сети, вы можете использовать протокол XMODEM по последовательному подключению.

При передаче отдельных модулей микропрограммы модуль операционной системы AOS **должен** быть передан на Rack PDU до передачи модуля приложений.

Для обновления одного Rack PDU используйте протокол FTP или SCP

FTP. При использовании протокола FTP для обновления по сети одного Rack PDU:

- Устройство Rack PDU должно быть подключено к сети, должны быть сконфигурированы его системный IP-адрес, маска подсети и шлюз по умолчанию.
- Сервер FTP должен быть разрешен в настройках Rack PDU.
- Файлы микропрограммы должны быть загружены с Dell.com.

Для передачи файлов:

1. Откройте на сетевом компьютере окно с командной строкой. Перейдите в папку, содержащую файлы обновления микропрограммного обеспечения, и проверьте их:

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

   В указанных файлах *xxx* показывает номер версии микропрограммы:

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

2. Откройте клиентский сеанс FTP:

   C:\dell>ftp

3. Наберите команду **open**, затем укажите IP-адрес Rack PDU и нажмите клавишу ENTER. Если настройка **port** FTP-сервера отличается от значения по умолчанию, равного **21**, необходимо использовать эту новую настройку в строке команды FTP.
   - Для клиентов Windows FTP отделяйте номер порта от IP-адреса пробелом. Например:

     ftp> open 150.250.6.10 21000
   - Некоторые клиенты FTP требуют ставить перед номером порта двоеточие.
4. Войдите в систему с правами администратора; по умолчанию **admin** является и именем пользователя, и паролем.
5. Выполните обновление операционной системы (AOS). (В примере *xxx* – номер версии микропрограммного обеспечения):

   ftp> bin
   ftp> put dell_hw05_aos_*xxx*.bin
6. Когда FTP-сервер подтвердит передачу, введите **quit**, чтобы закрыть сеанс.
7. Через 20 секунд повторите шаги 2–5. В шаге 5 используйте имя файла модуля приложения.

SCP. Чтобы выполнить обновление микропрограммного обеспечения Rack PDU при помощи Secure CoPy (SCP), выполните следующие операции:

1. Определите и найдите модули микропрограммного обеспечения, описанные в предыдущих командах для FTP.
2. С помощью командной строки SCP выполните передачу модуля микропрограммного обеспечения AOS на Rack PDU. В данном примере *xxx* показывает номер версии модуля AOS:

   scp dell_hw05_aos_xxx.bin
   dell@158.205.6.185:dell_hw05_aos_xxx.bin
3. Для передачи прикладного модуля микропрограммы на Rack PDU используйте подобную командную строку SCP с именем модуля приложения.

Обновление нескольких Rack PDU

Использование протоколов FTP и SCP для обновления нескольких Rack PDU.

Для обновления нескольких Rack PDU с использованием клиента FTP или протокола SCP, напишите скрипт, который будет автоматически выполнять процедуру.

Использование XMODEM для обновления одного Rack PDU

Чтобы использовать XMODEM для обновления одного Rack PDU, не подключенного к сети, сначала загрузите файлы микропрограммы с сайта Dell.com.

Для передачи файлов:

1. Выберите последовательный порт на локальном компьютере и отключите все службы, использующие этот порт.
2. Подключите последовательный конфигурационный кабель, поставляемый в комплекте, к выбранному порту и к серийному порту устройства Rack PDU.
3. Запустите на компьютере программу терминала (например, HyperTerminal) и настройте следующие параметры для выбранного порта: скорость передачи 57600 бит/с, 8 бит данных, без проверки четности, 1 стоповый бит, без контроля потока.
4. Нажмите кнопку RESET на Rack PDU, после чего сразу же дважды нажмите кнопку ENTER, или до появления приглашения монитора загрузки Boot Monitor: **`BM>`**
5. Введите **`XMODEM`** и нажмите ENTER.
6. В меню программы терминала выберите XMODEM, затем выберите двоичный файл микропрограммного обеспечения AOS, который будет передан с помощью XMODEM. По завершении передачи XMODEM на экране появится приглашение монитора загрузки Boot Monitor.
7. Чтобы установить модуль приложений, повторите шаги 5 и 6. На шаге 6 укажите имя файла модуля приложений.
8. Наберите **`reset`** или нажмите кнопку «Reset», чтобы перезапустить Rack PDU.

Дополнительные сведения о формате модулей микропрограмм см. в разделе Файлы микропрограммы.

Проверка обновлений и исправлений

Проверка результатов передачи

Чтобы проверить, успешно ли было загружено микропрограммное обеспечение, используйте команду **`xferStatus`**, вводимую в командной строке интерфейса, чтобы увидеть результат последней передачи, или используйте SNMP GET в **mfiletransferStatusLastTransferResult** OID.

Коды результатов последней передачи

Код	Описание
Successful (Успешно)	Передача файлов была успешной.
Result not available (Результат не доступен)	Нет сообщений о пересылке файлов.
Failure unknown (Ошибка неизвестна)	Последняя передача файлов была неудачной по неизвестной причине.
Server inaccessible (Сервер недоступен)	Сервер TFTP или FTP не найден в сети.
Server access denied (Доступ к серверу закрыт)	Доступ к серверу TFTP или FTP закрыт.
File not found (Файл не найден)	Сервер TFTP или FTP не смогли найти запрашиваемый файл.
File type unknown (Неизвестный тип файла)	Файл был загружен, но содержимое его не распознано.
File corrupt (Файл поврежден)	Файл был загружен, но, как минимум, один код CRC ошибочен.

Проверка номеров версий установленного микропрограммного обеспечения.

Используйте веб-интерфейс для проверки версий модулей обновленного микропрограммного обеспечения, для чего выберите вкладку **Administration** (Администрирование), пункт **General** (Общие) в верхней строке меню и **About** (О программе) в левом меню навигации, или используйте команду SNMP GET в MIB II **sysDescr** OID. В интерфейсе командной строки введите команду **`about`**.

Устранение проблем

Rack PDU – проблемы доступа

Неисправность	Решение
Невозможно выполнить эхо-тестирование Rack PDU	Если индикатор состояния Rack PDU светится зеленым, попробуйте послать команду эхо-тестирования на другой узел того же сегмента сети, в котором расположено устройство Rack PDU. Если тестирование не работает, то Rack PDU исправно. Если индикатор состояния горит не зеленым, а другим светом или если эхо-тестирование проходит успешно, проверьте следующее: • Проверьте сетевые подключения. • Проверьте IP-адреса Rack PDU и NMS. • Если NMS аппаратно находится в другой сети (или подсети), отличной от сети Rack PDU, проверьте IP-адрес шлюза по умолчанию (или маршрутизатора). • Проверьте число бит подсети для маски подсети Rack PDU.
Невозможно выделить коммуникационный порт через программу терминала	Перед тем как использовать программу терминала для конфигурирования Rack PDU, следует отключить все приложения, службы и программы, которые используют данный коммуникационный порт.
Невозможен доступ через интерфейс командной строки по каналу последовательного обмена	Проверьте, что вы не меняли настройки скорости обмена данными. Попробуйте установить значения 2400, 9600, 19200 или 38400 бит/с.

Неисправность	Решение
Невозможен удаленный доступ через интерфейс командной строки	• Проверьте, что вы используете правильный способ доступа, Telnet или Secure SHell (SSH). Администратор может включить эти способы доступа. По умолчанию включен протокол Telnet. При включении SSH автоматически отключается Telnet. • При использовании SSH Rack PDU может создавать ключ хост-узла. Rack PDU требуется до одной минуты для создания ключа хост-узла, в это время SSH будет недоступен.
Невозможно получить доступ через веб-интерфейс	• Убедитесь, что доступ HTTP или HTTPS открыт. • Убедитесь, что вы указали правильное значение URL, согласующееся с системой безопасности, используемой Rack PDU. SSL требует указать параметр **https**, а не **http** в начале адреса URL. • Проверьте, чтобы выполнялось эхо-тестирование Rack PDU. • Убедитесь, что вы используете браузер, поддерживаемый Rack PDU. См. раздел Поддерживаемые интернет-обозреватели. • Если устройство Rack PDU только что перезагрузилось, и была установлена система безопасности SSL, возможно, Rack PDU создает сертификат сервера. Для создания этого сертификата Rack PDU потребуется до одной минуты, в это время сервер SSL будет недоступен.

Приложение A: Список

Описания команд платы сетевого управления

```
?
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
console
    [-S<disable | telnet | ssh>]
    [-pt <telnet port n>]
    [-ps <SSH port n>]
    [-b <2400 | 9600 | 19200 | 38400>]
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
dns
    [-OM <enable | disable>]
    [-p <primary DNS server>]
    [-s <secondary DNS server>]
    [-d <domain name>]
    [-n <domain name IPv6>]
    [-h <host name>]
```

eventlog
exit
format
ftp
    [-p <port number>]
    [-S <enable | disable>]
help
netstat
ntp
    [-OM <enable | disable>]
    [-p <primary NTP server>]
    [-s <secondary NTP server>]
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>]
snmp, snmpv3
    [-S <enable | disable>]
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>]

tcpip6
[-S <enable | disable>]
[-man <enable | disable>]
[-auto <enable | disable>]
[-i <IPv6 address>]
[-g <IPv6 gateway>]
[-d6 <router | stateful | stateless | never>]
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

Описание команд устройства

devLowLoad
[<power>]
devNearOver
[<power>]
devOverLoad
[<power>]
devReading
[<“power” | “energy”>]
devStartDly
humLow
[<humidity>]
humMin
[<humidity>]
humReading
inNormal
inReading
olAssignUsr
[<“all” | outlet name | outlet# > <user>]
olCancelCmd
[<“all” | outlet name | outlet#>]

olDlyOff
[<“all” | outlet name | outlet#>]
olDlyOn
[<“all” | outlet name | outlet#>]
olDlyReboot
[<“all” | outlet name | outlet#>]
olGroups
olLowLoad
[<“all” | outlet name | outlet#> <power>]
olName
[<“all” | outlet# > <new name>]
olNearOver
[<“all” | outlet name | outlet#> <power>]
olOff
[<“all” | outlet name | outlet# >]
olOffDelay
[<“all” | outlet name | outlet#> <time>]
olOn
[<“all” | outlet name | outlet#>]
olOnDelay
[<“all” | outlet name | outlet#> <time>]
olOverLoad
[<“all” | outlet name | outlet#> <power>]
olRbootTime
[<“all” | outlet name | outlet#> <time>]
olReading
[<“all” | outlet name | outlet# > <current | power | energy>]
olReboot
[<“all” | outlet name | outlet# >]
olStatus
[<“all” | outlet name | outlet# >]
olUnasgnUsr
[<“all” | outlet name | outlet# > <user>]
phLowLoad
[<“all” | phase#> <current>]
phNearOver
[<“all” | phase#> <current>]
phOverLoad
[<“all” | phase#> <current>]
phReading
[<“all” | phase#> <“current” | “voltage” | “power”>]
phRestrictn
[<“all” | phase#> <none | near | over>]

prodInfo
tempHigh
    [<“F” | “C”> <temperature>]
tempMax
    [<“F” | “C”> <temperature>]
tempReading
    [<“F” | “C”>]
userAdd
    [<new user>]
userDelete
    [<user>]
userList
userPasswd
    [<user> <new password> <new password>]
whoami

Приложение Б: Руководство по

Содержание и назначение данного приложения

Данное приложение документирует функции безопасности микропрограммного обеспечения версии 5.*x.x* для Dell® Rack PDU (Устройство распределения питания для монтажа в стойку), позволяющие устройствам Rack PDU работать автономно, не будучи подключенными к сети.

Данное приложение документирует перечисленные ниже протоколы и функции, а также описывает, как выбирать указанные функции для конкретной ситуации и как настраивать и использовать их в рамках общей системы безопасности:

- Telnet и Secure Shell (SSH)
- Secure Sockets Layer (SSL)
- RADIUS
- SNMPv1 и SNMPv3

Кроме этого, данное приложение описывает, как использовать программу-мастер безопасности Rack PDU Security Wizard для создания компонентов, необходимых для обеспечения высокого уровня безопасности, доступного при использовании SSL и SSH.

Характеристики безопасности

Защита паролей и секретных фраз

Пароли и секретные фразы не хранятся в Rack PDU в виде открытого текста.

- Пароли хешируются с помощью однонаправленного алгоритма хеширования.
- Секретные фразы, которые используются для авторизации и шифрования, шифруются перед тем, как помещаются в память Rack PDU.

Обзор методов доступа

Последовательный доступ к интерфейсу командной строки.

Безопасный доступ	Описание
Доступ осуществляется по имени пользователя и паролю.	Всегда доступен.

Удаленный доступ к интерфейсу командной строки.

Безопасный доступ	Описание
Доступные методы: • Имя пользователя и пароль • Выбираемый порт сервера • Протоколы доступа, которые могут быть активированы и отключены • Безопасный командный процессор (SSH)	Для обеспечения высокой безопасности используйте SSH. • При использовании Telnet имя пользователя и пароль передаются в виде открытого текста. • Включение SSH отключает Telnet и задействует шифрованный вход к интерфейсу командной строки, что обеспечивает дополнительную защиту от попыток перехвата, фальсификации или изменения данных при их передаче.

SNMPv1 и SNMPv3.

Безопасный доступ	Описание
Доступные методы (SNMPv1): • Имя сообщества • Имя хоста • Фильтры NMS IP • Агенты, которые могут быть активированы и отключены • Четыре сообщества доступов с возможностями чтения/записи/отключения	Для методов SNMPv1 и SNMPv3 имя хоста запрещает доступ к системе управления сетью (NMS) только в данном месте, а фильтры NMS IP разрешают доступ только к NMS, определенных по одному из форматов IP-адреса в следующих примерах: • 159.215.12.1: Только NMS на IP-адресе 159.215.12.1. • 159.215.12.255: Любой NMS на сегменте 159.215.12. • 159.215.255.255: Любой NMS на сегменте 159.215. • 159.255.255.255: Любой NMS на сегменте 159. • 0.0.0.0 или 255.255.255.255: Любой NMS. SNMPv3 имеет дополнительные функции безопасности, которые включают следующее: • Секретная фраза авторизации для проверки того, что NMS, пытающийся получить доступ к Rack PDU, является запрещенным NMS. • Шифровка данных при передаче, с секретной фразой, используемой для шифрования и дешифрования.
Доступные методы (SNMPv3): • Для профилей пользователей • Авторизация с использованием секретной фразы авторизации • Шифрование с помощью секретной фразы конфиденциальности • Авторизация SHA или MD5 • Алгоритм шифрования AES или DES • Фильтры NMS IP	

Протокол передачи файлов.

Безопасный доступ	Описание
Доступные методы: • Имя пользователя и пароль • Выбираемый порт сервера • FTP-серверы и протоколы доступа, которые могут быть активированы и отключены • Secure CoPy (SCP)	В случае использования FTP имя пользователя и пароль передаются в виде открытого текста, файлы передаются без шифрования. Для шифрования имени пользователя и пароля, а также передаваемых файлов (обновления микропрограммы, файлы конфигурации, файлы журнала, сертификаты Secure Sockets Layer (SSL) и хост-ключи Secure Shell (SSH)) используется SCP. Если в качестве протокола передачи файлов выбран SCP, включите SSH и отключите FTP.

Веб-сервер

Безопасный доступ	Описание
Доступные методы: • Имя пользователя и пароль • Выбираемый порт сервера • Веб-интерфейсы доступа, которые могут быть активированы и отключены • Протокол защищенных сокетов (SSL)	В основном режиме авторизации HTTP имя пользователя и пароль передаются кодированными на основе позиционной системы счисления с основанием 64 (base-64) (без шифрования). SSL имеется в интернет-обозревателях, используемых с картой управления Management Card или устройствами с сетевым доступом, а также на большинстве веб-серверов. Веб-протокол передачи гипертекста через уровень защищенных сокетов (HTTPS) шифрует и дешифрует запросы к страницам веб-серверов и страницы, возвращаемые веб-сервером пользователю.

RADIUS.

Безопасный доступ	Описание
Доступные методы: • Централизованная авторизация прав доступа • Общая секретная фраза сервера RADIUS и Rack PDU или устройства	RADIUS (Remote Authentication Dial-In User Service – пользовательская служба удаленной аутентификации) является сервисом аутентификации, авторизации и учета, используемым для централизованного управления удаленным доступом к каждому устройству Rack PDU. (Rack PDU поддерживает функции аутентификации и авторизации.)

Приоритеты доступа

Предусмотрен следующий приоритет доступа, начиная с максимального:

- Локальный доступ к интерфейсу командной строки с компьютера, подключенного к Rack PDU через прямое последовательное соединение
- Доступ Telnet или Secure Shell (SSH) к интерфейсу командной строки с удаленного компьютера
- Доступ через интернет

Немедленно измените имена пользователей и пароли по умолчанию

После установки и начального конфигурирования устройства Rack PDU необходимо немедленно изменить имена пользователей и пароли по умолчанию на уникальные имена и пароли для обеспечения безопасности на стандартном уровне.

Назначения портов

Если сервер Telnet, FTP, SSH/SCP или веб-сервер использует нестандартный порт, пользователю необходимо указать его в командной строке или в строке веб-адреса, используемого для доступа к Rack PDU. Нестандартный номер порта обеспечивает повышенный уровень безопасности. Порты изначально устанавливаются на стандартные, «хорошо известные» протоколам порты. Чтобы повысить безопасность, переустановите порт на любой из неиспользуемых номеров портов в диапазоне от 5001 до 32768 для FTP-сервера и от 5000 до 32768 для других протоколов и серверов. (FTP-сервер использует указанный порт и порт с номером на единицу меньше указанного).

Имена пользователей, пароли и имена сообществ с SNMPv1

Все имена пользователей, пароли и групповые имена для SNMPv1 передаются по сети в виде обычного текста. Пользователь, имеющий возможность контролировать сетевой трафик, может определять имена пользователей и пароли, необходимые для входа в учетные записи интерфейса командной строки или веб-интерфейс устройства Rack PDU. Если ваша сеть требует повышенной безопасности функций интерфейса командной строки и веб-интерфейса, использующих шифрование, отключите доступ SNMPv1 или задайте режим доступа как **Read** (Чтение). (Доступ **Read** (Чтение) позволяет получать информацию состояния и использовать SNMPv1-ловушки).

Чтобы отключить доступ SNMPv1, выберите на вкладке **Administration** (Администрирование) пункт **Network** (Сеть) в строке меню и пункт **access** (доступ) в заголовке **SNMPv1** в левом меню навигации. Уберите флажок **Enable SNMPv1 access** (Разрешить доступ SNMPv1) и нажмите **Apply** (Применить).

Чтобы задать доступ SNMPv1 как **Read**, выберите на вкладке **Administration** (Администрирование) пункт **Network** (Сеть) в строке меню и пункт **access** (доступ) **control** в заголовке **SNMPv1** в левом меню навигации. Затем, для каждой сконфигурированной системы NMS выберите имена сообществ и задайте тип доступа как **Read** (Чтение).

Аутентификация

Вы можете установить для Rack PDU функции безопасности, которые будут контролировать доступ путем стандартной аутентификации через имя пользователя, пароль и IP-адрес без применения шифрования. Эти базовые функции безопасности достаточны для большинства случаев применения, в которых не осуществляется передача жизненно важных данных.

SNMP GETS, SETS и Traps

Для расширенной аутентификации, использующей протокол SNMP для контроля или конфигурации Rack PDU, выберите функцию SNMPv3. Парольная фраза аутентификации, используемая с профилями пользователя SNMPv3, удостоверяет, что Система сетевого управления (Network Management System – NMS), обменивающаяся данными с Rack PDU, является именно той системой NMS, за которую она себя выдает; данное сообщение не было искажено в ходе передачи, не было задержано и не было скопировано и послано вторично поздней, в несоответствующее время. SNMPv3 отключен по умолчанию.

Реализация SNMPv3 в оборудовании Dell позволяет использовать для аутентификации протокол SHA-1 или MD5.

Веб-интерфейс и интерфейс командной строки

Чтобы быть уверенным, что данные и линия связи между интерфейсом Rack PDU и интерфейсами клиента (интерфейсом командной строки или веб-интерфейсом) не будут перехвачены, можно задать более высокий уровень безопасности путем использования одного или нескольких методов на базе шифрования, перечисленных ниже:

- Для веб-интерфейса используйте протокол защищенных сокетов (SSL)
- Для шифрования имен пользователей и паролей для доступа через интерфейс командной строки используется протокол Secure Shell (SSH)
- Для шифрования имен пользователей, паролей и данных для безопасной передачи файлов, используйте протокол Secure CoPy (SCP)

Дополнительные сведения о безопасности, основанной на шифровании, изложены в разделе Шифрование.

Шифрование

SNMP GETS, SETS и Traps

Для передачи шифрованных данных с использованием протокола SNMP для контроля или конфигурации Rack PDU выберите SNMPv3. Секретная фраза, используемая с пользовательскими профилями SNMPv3, гарантирует конфиденциальность данных (с помощью шифрования с использованием алгоритмов шифрования AES или DES), которые система NMS посылает или получает от Rack PDU.

Протоколы Secure Shell (SSH) и Secure CoPy (SCP) для интерфейса командной строки

Протокол Secure Shell. SSH представляет механизм обеспечения безопасного доступа компьютерных консолей, или *оболочек,* дистанционно. Протокол аутентифицирует сервер (в данном случае, Rack PDU) и шифрует все данные, передаваемые между клиентом SSH и сервером.

- SSH – альтернатива Telnet, отличающаяся повышенной безопасностью. Telnet не осуществляет шифрование.
- SSH защищает имя пользователя и пароль, предъявляемые для авторизации, от использования посторонними лицами, осуществившими перехват сетевого трафика.
- Для аутентификации сервера SSH (Rack PDU) клиенту SSH, протокол SSH использует хост-ключ, уникальный для SSH-сервера. Хост-ключ представляет собой идентификационные данные, которые невозможно подделать, он предотвращает получение имени пользователя и пароля недействительным сервером, который выдает себя за действительный.

Информацию о поддерживаемых клиентских приложениях SSH см. в разделе Telnet и Secure Shell (SSH). О том, как создать хост-ключ, см. раздел Создание хост-ключа SSH.

- Rack PDU поддерживает протокол SSH версии 2, обеспечивающий защиту от попыток перехвата, фальсификации или изменения данных в процессе их передачи.
- При включении SSH будет автоматически отключен Telnet.
- Интерфейс, учетные записи и права доступа пользователей будут одинаковыми при доступе через интерфейс командной строки как с использованием SSH, так и Telnet.

Secure CoPy. SCP – безопасное приложение для передачи файлов, используемое вместо FTP. SCP использует протокол SSH в качестве основного транспортного протокола для шифровки имен пользователей, паролей и файлов.

- При задействовании и конфигурации SSH вы автоматически включаете и конфигурируете SCP. Дальнейшей конфигурации SCP не требуется.
- Вы должны специально отключить FTP. Он не отключается при задействовании SSH. Чтобы отключить FTP, на вкладке **Administration** (Администрирование) выберите **Network** (Сеть) в верхнем меню и выберите параметр **FTP Server** (Сервер FTP Server) в левом навигационном меню. Уберите флажок **Enable** (Включить) и нажмите **Apply** (Применить).

Протокол защищенных сокетов (Secure Sockets Layer – SSL) для веб-интерфейса

В случае использования безопасных веб-соединений, включите протокол защищенных сокетов SSL, выбрав в качестве протокола доступа к веб-интерфейсу Rack PDU протокол HTTPS. Протокол передачи гипертекстов на уровне защищенных сокетов (HTTPS) представляет собой протокол, который производит шифрование и дешифрование страниц, запрашиваемых пользователем, и страниц, возвращаемых пользователю веб-сервером.

Rack PDU поддерживает SSL версии 3.0 и связанный с ним протокол безопасности на транспортном уровне (TLS) версии 1.0. Большинство программ-обозревателей позволяют выбрать версию SSL для использования.

Если протокол SSL включен, ваша программа-обозреватель будет отображать маленький значок в виде замка. 

SSL использует цифровой сертификат, позволяющий браузеру аутентифицировать сервер (в нашем случае – Rack PDU). Браузер проверяет следующее:

- Формат сертификата сервера правильный
- Дата и время истечения срока действия сертификата сервера не прошли
- Имя DNS или IP-адрес, указанные при входе пользователя, соответствуют общему имени в сертификате сервера
- Сертификат сервера подписан доверенным органом сертификации

Все ведущие производители программ-браузеров распространяют корневые сертификаты CA коммерческих сертификационных служб в хранилище сертификатов (кэш) своих браузеров, так что браузеры могут сравнить подпись сертификата сервера с подписью в корневом сертификате CA.

Можно использовать программу-мастер безопасности Rack PDU Security Wizard для создания запроса подписания сертификата внешнему сертифицирующему органу, а также создать корневой сертификат Dell для загрузки его в хранилище (кэш) браузера. Можно также использовать программу-мастер для создания серверного сертификата для загрузки в Rack PDU.

См. раздел Создание и установка цифровых сертификатов, где приводятся сведения об использовании сертификатов.
О том, как создать сертификаты и запросы сертификатов, см. разделы Создание корневого сертификата и сертификатов серверов и Создание сертификата сервера и запроса на подписание.

SSL также использует различные алгоритмы и коды шифрования для аутентификации сервера, шифрования данных и обеспечения целостности данных, то есть, то, что они не будут перехвачены и отправлены на другой сервер.

Часто посещаемые веб-страницы хранятся в кэш-памяти вашего веб-обозревателя, что позволяет зайти на эти страницы без повторного ввода имени пользователя и пароля. Всегда закрывайте сессию обозревателя, перед тем как оставить компьютер без присмотра.

Создание и установка цифровых сертификатов

Назначение

Для работы в сети, требующей более высокого уровня безопасности, чем парольное шифрование, веб-интерфейс устройства Rack PDU поддерживает использование цифровых сертификатов с протоколом SSL. Цифровые сертификаты могут аутентифицировать Rack PDU (сервер) в веб-браузере (SSL-клиенте).

Можно сгенерировать 1024-битный или 2048-битный ключ, обеспечивающий комплексное шифрование и более высокий уровень безопасности.

Последующие разделы обобщают три метода создания, развертывания и использования цифровых сертификатов с целью помочь вам определить наиболее подходящий метод для вашей системы.

- Метод 1: Использование сертификата по умолчанию, автоматически сгенерированного устройством Rack PDU.
- Метод 2: Использование программы-мастера Rack PDU Security Wizard для создания сертификата CA и сертификата сервера.
- Метод 3: Использование программы-мастера Rack PDU Security Wizard с целью создания запроса на подписание сертификата для подписания его корневым сертификатом внешнего сертификационного органа и для создания серверного сертификата.

Можно также использовать метод 3, если ваша компания или агентство работают с собственным сертифицирующим органом. Используйте программу-мастер безопасности Rack PDU Security Wizard как обычно, но вместо коммерческого сертифицирующего органа укажите собственный.

Выбор метода для вашей системы

При использовании протокола защищенных сокетов (SSL) вы можете выбрать любой из следующих методов использования цифровых сертификатов.

Метод 1: Использование сертификата по умолчанию, автоматически сгенерированного устройством Rack PDU. При включении SSL необходимо перезагрузить Rack PDU. Если не существует сертификата сервера, во время перезагрузки устройство Rack PDU генерирует самоподписываемый сертификат сервера по умолчанию, который нельзя конфигурировать.

Метод 1 имеет следующие преимущества и недостатки.

- **Преимущества:**
  - Имя пользователя, пароль и другие данные шифруются перед их передачей с и на устройство Rack PDU.
  - Можно использовать заданный по умолчанию серверный сертификат, обеспечивающий безопасность на основе шифрования при настройке одной из двух функций цифрового сертификата, либо можно продолжить его эксплуатацию, используя преимущества шифрования, предоставляемые протоколом SSL.
- **Недостатки:**
  - Устройству Rack PDU требуется до 1 минуты для создания этого сертификата, а веб-интерфейс в это время недоступен. (Эта задержка происходит при первой загрузке после подключения протокола SSL.)
  - Данный метод не содержит аутентификации, предоставляемой сертификатом CA (сертификатом, подписанным сертификационным органом) которые обеспечивают методы 2 и 3. Сертификат CA не кэшируется в браузере. Поэтому при входе пользователя в систему Rack PDU браузер выводит предупреждение о безопасности, указывающее на то, что сертификат, подписанный надежным центром сертификации, недоступен, а затем выводится запрос о необходимости продолжения работы. Чтобы данное сообщение не выводилось, необходимо установить сертификат сервера по

умолчанию в хранилище сертификатов (кэш) браузера каждого пользователя, которому необходим доступ к Rack PDU, и каждый пользователь должен всегда использовать полное доменное имя сервера при входе в систему Rack PDU.

– В сертификате сервера по умолчанию в качестве действительного *стандартного имени* (DNS-имя или IP-адрес Rack PDU) указан серийный номер Rack PDU. Поэтому несмотря на то, что устройство Rack PDU может контролировать доступ к веб-интерфейсу с помощью имени пользователя, пароля и типа учетной записи (напр., **Администратор**, **Пользователь устройства** или **Пользователь только для чтения**), браузер не может определить, какое устройство Rack PDU отправляет или принимает данные.
– По умолчанию, длина *открытого ключа* (ключа RSA), используемого для шифрования при настройке сессии SSL, составляет 2048 бит.

Метод 2: Использование программы-мастера Rack PDU Security Wizard для создания сертификата CA и сертификата сервера. Используйте программу-мастер Rack PDU Security Wizard для создания двух цифровых сертификатов:

- *Корневой сертификат CA* (корневой сертификат сертификационного органа), используемый программой Rack PDU Security Wizard для подписи всех серверных сертификатов, и который затем будет установлен в хранилище сертификатов (кэш) браузера каждому из пользователей, желающих иметь доступ к Rack PDU.
- *Сертификат сервера*, загружаемый в Rack PDU. Создавая сертификат сервера, программа-мастер Rack PDU Security Wizard использует корневой сертификат CA для подписи серверного сертификата.

Веб-браузер аутентифицирует Rack PDU, отправляющий или запрашивающий данные:

- Для аутентификации Rack PDU браузер использует *общее имя* (IP-адрес или имя DNS устройства Rack PDU) которое было указано в *различающемся имени* сертификата сервера при создании этого сертификата.

- Чтобы подтвердить, что сертификат сервера подписан «проверенным» сертифицирующим органом, браузер сравнивает подпись серверного сертификата с подписью корневого сертификата, хранящегося в кэш-памяти браузера. Дата срока годности подтверждает, действителен ли сертификат сервера.

Метод 2 имеет следующие преимущества и недостатки.

- **Преимущества:**
  - Имя пользователя, пароль, а также все данные, передаваемые на Rack PDU и поступающие с него, шифруются перед передачей.
  - При настройке сессии SSL вы определяете длину *открытого ключа* (RSA key), который используется для шифрования (можно указать 1024 бита, значение, используемое по умолчанию, или 2048 бит, чтобы обеспечить более сложное шифрование и более высокий уровень безопасности).
  - Сертификат сервера, загружаемый в Rack PDU, позволяет протоколу SSL определить, что передаваемые данные поступают и отправляются на требуемое устройство Rack PDU. Это обеспечивает дополнительный уровень безопасности, помимо шифрования имени пользователя, пароля и передаваемых данных.
  - Корневой сертификат, устанавливаемый в браузере, позволяет браузеру проверять подлинность серверного сертификата Rack PDU, что обеспечивает дополнительную защиту от несанкционированного доступа.
- **Недостаток:**
  Поскольку сертификаты не имеют цифровой подписи коммерческого органа сертификации, вы должны загрузить корневой сертификат в хранилище (кэш) браузера каждого пользователя. (Производители браузеров уже поставляют корневые сертификаты для коммерческих органов сертификации в хранилище сертификатов своих браузеров, как показано в методе 3.)

Метод 3: Использование программы-мастера Rack PDU Security Wizard с целью создания запроса на подписание сертификата для подписания его корневым сертификатом внешнего сертификационного органа и для создания серверного сертификата. Используйте программу Rack PDU Security Wizard для создания запроса (**csr**-файла), который будет послан в сертификационный орган. Сертификационный орган вернет подписанный сертификат (**.crt**-файл) на основе информации, предоставленной в вашем запросе. Затем, с помощью программы Rack PDU Security Wizard, создается сертификат сервера (**.p15**-файл), который включает в себя подпись корневого сертификата, присланного сертификационным органом. Загрузите сертификат сервера в устройство Rack PDU.

Можно также использовать метод 3, если ваша компания или агентство работают с собственным сертифицирующим органом. Используйте программу-мастер безопасности Rack PDU Security Wizard как обычно, но вместо коммерческого сертифицирующего органа укажите собственный.

Метод 3 имеет следующие преимущества и недостатки.

- **Преимущества:**
  - Имя пользователя, пароль, а также все данные, передаваемые на Rack PDU и поступающие с него, шифруются перед передачей.
  - Вы будете обладать преимуществами в аутентификации, предоставляемые органом сертификации, который уже имеет подписанный корневой сертификат в кэше сертификатов браузера. (Сертификаты CA коммерческих сертификационных органов распространяются в составе программного обеспечения браузеров, сертификационный орган вашей компании или агентства, вероятно, разместил свой сертификат CA в хранилищах браузеров всех пользователей). Поэтому вам не требуется загружать корневой сертификат в браузеры всех пользователей, которым требуется доступ к Rack PDU.

  - При настройке сессии SSL вы можете задать длину *открытого ключа* (RSA key), который используется для шифрования (можно указать 1024 бита – значение, используемое по умолчанию, или 2048 бит, чтобы обеспечить более сложное шифрование и более высокий уровень безопасности).
  - Сертификат сервера, загружаемый в Rack PDU, позволяет протоколу SSL определить, что передаваемые данные поступают и отправляются на требуемое устройство Rack PDU. Это обеспечивает дополнительный уровень безопасности, помимо шифрования имени пользователя, пароля и передаваемых данных.
  - Чтобы обеспечить дополнительную защиту от неавторизованного доступа, браузер сравнивает цифровую подпись сертификата сервера, который загружен в Rack PDU, с подписью корневого сертификата CA, который находится в кэше сервера.
- **Недостатки:**
  - Процедура настройки требует выполнения дополнительного шага запроса подписанного корневого сертификата в сертификационном органе.
  - Внешний сертификационный орган может потребовать плату за поставку подписанных сертификатов.

Сетевые экраны

Хотя некоторые методы аутентификации обеспечивают уровень безопасности выше, чем другие методы, полной защиты от прорывов системы безопасности достичь практически невозможно. Правильно сконфигурированные сетевые экраны являются существенным элементом в общей схеме безопасности.

Использование Rack PDU Security Wizard

Программа-мастер безопасности Rack PDU Security Wizard создает компоненты, необходимые для обеспечения повышенной безопасности Rack PDU в сети при использовании протокола защищенных сокетов (SSL), а также подобных протоколов и процедур кодирования.

Аутентификация с помощью сертификатов и хост-ключей

Аутентификация проверяет подлинность пользователя или сетевого устройства (например, Rack PDU). Пароль обычно проверяет подлинность компьютерных пользователей. Тем не менее, для обмена данными или связи, требующей более строгих методов обеспечения безопасности в интернете, Rack PDU поддерживает более безопасные методы аутентификации.

- Протокол защищенных сокетов (SSL), используемый для безопасного доступа через интернет, использует для аутентификации цифровые сертификаты. Цифровой *корневой сертификат CA* выпускается органом сертификации (CA) как часть инфраструктуры открытых ключей, и его цифровая подпись должна соответствовать цифровой подписи сертификата сервера на Rack PDU.
- Протокол SSH, используемый для удаленного доступа через терминал к интерфейсу командной строки устройства Rack PDU, осуществляет аутентификацию с помощью общедоступного *хост-ключа*.

Использование сертификатов. Большинство веб-браузеров, включая браузеры, поддерживаемые устройствами Rack PDU, содержит набор корневых сертификатов CA всех коммерческих органов сертификации.

Аутентификация сервера (в нашем случае Rack PDU) проводится всякий раз, когда устанавливается связь между браузером и сервером. Браузер проводит проверку, чтобы убедиться, что сертификат сервера, подписанный органом сертификации, известен ему.

Для аутентификации необходимо, чтобы:

- Каждый сервер (Rack PDU) с включенным протоколом SSL должен иметь сертификат сервера, расположенный на самом сервере.
- Любой браузер, используемый для доступа к веб-интерфейсу Rack PDU, должен содержать корневой сертификат CA, которым подписан сертификат сервера.

Если процесс аутентификации завершился неудачей, сообщение браузера предложит вам продолжить работу, несмотря на то, что браузеру не удалось аутентифицировать сервер.

Если ваша сеть не требует аутентификации, выполняемой на базе цифровых сертификатов, вы можете использовать сертификат по умолчанию, который генерируется устройством Rack PDU автоматически. Цифровая подпись стандартного сертификата не будет распознана браузером, но стандартный сертификат позволяет использовать протокол SSL для шифрования передаваемых имен пользователей, паролей и данных. (Если вы используете стандартный сертификат, браузер предложит вам воспользоваться неавторизованным доступом, перед тем как войдет в веб-интерфейс Rack PDU.)

Использование хост-ключей SSH. *Хост-ключ* SSH проверяет подлинность сервера (Rack PDU) при каждом обращении SSH-клиента к этому серверу. Каждый сервер с включенным протоколом SSH должен иметь хост-ключ SSH, располагаемый на самом сервере.

Файлы, создаваемые для обеспечения безопасности SSL и SSH

Используйте программу-мастер Rack PDU Security Wizard для создания этих компонентов системы безопасности SSL и SSH:

- Сертификат сервера для Rack PDU, если вы хотите использовать преимущества аутентификации, которые дает этот сертификат. Вы можете создать любой из перечисленных ниже типов сертификатов сервера:

  - Сертификат сервера, подписанный корневым сертификатом CA, также созданным с помощью программы Rack PDU Security Wizard. Используйте указанный метод, если ваша компания или агентство не имеют собственного сертификационного органа, и вы не хотите использовать внешний сертификационный орган для подписи серверного сертификата.
  - Серверный сертификат, подписанный внешним сертификационным органом. Этот сертификационный орган может быть одним из тех, которые управляются вашей компанией или агентством, или одним из коммерческих сертификационных органов, чьи корневые сертификаты CA распространяются в составе программного обеспечения браузеров.
- Запрос на подпись сертификата, содержащий все данные, необходимые для серверного сертификата, за исключением цифровой подписи. Данный запрос необходим, если вы используете внешний сертификационный орган.
- Корневой сертификат CA.
- Хост-ключ SSH, который использует ваш SSH-клиент для аутентификации Rack PDU при входе в интерфейс командной строки.

Вы определяете, будут ли открытые ключи сертификатов SSL и хост-ключи для протокола SSH, создаваемые с помощью программы Rack PDU Security Wizard, 1024-битными RSA-ключами (значение по умолчанию) или 2048-битными RSA-ключами, обеспечивающими сложное шифрование и повышенный уровень безопасности.

Если вы не создали серверных сертификатов SSL и хост-ключей SSH с помощью программы Rack PDU Security Wizard, устройство Rack PDU сгенерирует 2048-битные RSA-ключи.

Только на устройствах Rack PDU компании Dell используются сертификаты сервера, хост-ключи и корневые сертификаты CA, созданные программой Security Wizard. Эти файлы не будут работать с такими продуктами, как OpenSSL® и Microsoft® Internet Information Services (IIS).

Создание корневого сертификата и сертификатов серверов

Сводка

Используйте данную процедуру, если ваша компания или агентство не имеют собственного сертификационного органа, и вы не хотите использовать коммерческий сертификационный орган для подписи своего серверного сертификата.

Укажите размер открытого ключа RSA, являющегося частью сертификата, генерируемого с помощью Rack PDU Security Wizard. Вы можете сгенерировать 1024-битный или 2048-битный ключ, обеспечивающий более сложное шифрование и более высокий уровень безопасности. (По умолчанию, ключ, генерируемый Rack PDU, имеет 2048 бит, если вы не пользуетесь мастером безопасности.)

- Создайте корневой сертификат CA, который будет подписывать все сертификаты сервера, используемые с устройством Rack PDU. В ходе выполнения этой задачи создаются два файла:
  - Файл с расширением **.p15** представляет собой шифрованный файл, содержащий сертификат секретного ключа и открытого корневого ключа органа сертификации. Данный файл подписывает сертификаты сервера.
  - Файл с расширением **.crt** содержит только открытый корневой сертификат органа сертификации. Загрузите этот файл во все веб-браузеры, которые будут использоваться для доступа к Rack PDU, с тем чтобы браузер мог проверить подлинность сертификата сервера устройства Rack PDU.
- Создайте сертификат сервера, который хранится в файле с расширением **.p15**. При выполнении этой задачи вам будет предложен корневой сертификат CA, который подписывает сертификат сервера.
- Загрузите сертификат сервера в устройство Rack PDU.
- Для каждого устройства Rack PDU, требующего сертификат сервера, повторите задачу, с помощью которой создается и загружается сертификат сервера.

Процедура

Создание корневого сертификата CA.

1. Если программа Rack PDU Security Wizard не установлена на вашем компьютере, найдите и запустите программу установки (**Rack PDU Security Wizard.exe)**.
2. В меню Windows **Start** (Пуск) выберите пункт **Programs** (Программы), затем – **Rack PDU Security Wizard**.
3. На экране, отмеченном как **Step 1** (Шаг 1), выберите **CA Root Certificate** (Корневой сертификат CA) в качестве файла, который необходимо создать, а затем выберите длину генерируемого ключа (1024 бит является значением по умолчанию; значение 2048 бит обеспечивает комплексное шифрование и высокий уровень безопасности).
4. Введите имя этого файла, который будет содержать открытый корневой сертификат и секретный ключ сертификационного органа. Файл должен иметь расширение **.p15** и, по умолчанию, будет создан в папке установки **C:\Program Files\Dell\Rack PDU Security Wizard**.
5. В диалоговом окне с меткой **Step 2** (Шаг 2) введите информацию конфигурации корневого сертификата CA. Поля, которые требуется заполнить, **Country** (Страна) и **Common Name** (Общее имя). В поле **Common Name** (Общее имя) введите название вашей компании или агентства. Используйте только буквы и цифры, без пробелов.

По умолчанию, корневой сертификат CA действителен 10 лет с момента получения, но вы можете отредактировать поля **Validity Period Start** (Начало срока действия) и **Validity Period End** (Конец срока действия).

6. В следующем диалоговом окне проверьте общие сведения о сертификате. Пролистайте вниз уникальный серийный номер и метки сертификата. Чтобы внести изменения в сообщенные вами сведения, нажмите **Back** (Назад). Откорректируйте информацию.

Информация о субъекте сертификата и информация стороны, выдавшей сертификат, должны быть идентичны.

7. Последнее диалоговое окно подтверждает, что сертификат выдан, и отображает сведения, которые потребуются вам при выполнении последующих задач:
   - Местоположение и имя **.p15**-файла, который будет использоваться для подписи сертификатов сервера.
   - Местоположение и имя файла с расширением **.crt** , который является корневым сертификатом CA, предназначенным для загрузки в браузер каждого пользователя, нуждающегося в доступе к Rack PDU.

Загрузка корневого сертификата CA в браузер Загрузите файл **.crt** в браузер каждого пользователя, которому нужен доступ к Rack PDU.

О том, как загрузить **.crt**-файл в хранилище сертификатов браузера (кэш), см. Справку. Ниже описаны основные действия для браузера Microsoft Internet Explorer.

1. Выберите пункт меню **Tools** (Сервис), затем **Internet Options** (Свойства обозревателя).
2. В диалоговом окне, на вкладке **Content** (Содержимое) щелкните **Certificates** (Сертификаты) и затем **Import** (Импорт).
3. Программа-мастер Certificate Import Wizard поможет вам выполнить остальную часть процедуры. Необходимо выбрать тип файла X.509, открытый корневой сертификат CA (Public Root Certificate) – файл **.crt** , созданный в процедуре Создание корневого сертификата и сертификатов серверов.

Создание пользовательского сертификата сервера SSL.

1. В меню Windows **Start** (Пуск) выберите пункт **Programs** (Программы), затем – **Rack PDU Security Wizard**.
2. В диалоговом окне, помеченном **Step 1** (Шаг 1), выберите **SSL Server Certificate** (Серверный сертификат CA) в качестве типа создаваемого файла и выберите затем длину генерируемого ключа (1024 бит – значение по умолчанию или 2048 бит, чтобы обеспечить сложное шифрование и повышенный уровень секретности).
3. Введите имя данного файла, который будет содержать сертификат сервера и секретный ключ. Файл должен иметь расширение **.p15** и, по умолчанию, будет создан в папке **C:\Program Files\Dell\Rack PDU Security Wizard**.
4. Щелкните **Browse** (Обзор) и выберите корневой сертификат CA, созданный в процедуре Создание корневого сертификата и сертификатов серверов. Корневой сертификат CA используется для подписания генерируемых пользовательских сертификатов сервера.

5. В диалоговом окне с меткой **Step 2** (Шаг 2) введите информацию конфигурации сертификата сервера. Поля, которые требуется заполнить – **Country** (Страна) и **Common Name** (Общее имя). В поле **Common Name** введите IP-адрес или имя DNS сервера (Rack PDU). По умолчанию, серверный сертификат действителен 10 лет с момента получения, но вы можете отредактировать поля **Validity Period Start** (Начало срока действия) и **Validity Period End** (Конец срока действия).

   Поскольку информация о конфигурации является частью подписи, информация для каждого из сертификатов должна быть уникальной. Конфигурация серверного сертификата не может быть такой же, как конфигурация корневого сертификата CA. (Дата окончания срока действия не считается уникальной конфигурацией. Должна различаться другая часть информации конфигурации.)

6. В следующем диалоговом окне проверьте общие сведения о сертификате. Пролистайте вниз уникальный серийный номер и метки сертификата. Чтобы внести изменения в сообщенные вами сведения, нажмите **Back** (Назад). Откорректируйте информацию.
7. Последнее диалоговое окно подтверждает, что сертификат выдан, и содержит инструкции по загрузке сертификата в Rack PDU. Оно отображает местоположение и имя сертификата сервера, имеющего расширение **.p15**, и содержит секретный ключ и открытый корневой сертификат Rack PDU.

Загрузка сертификата сервера в Rack PDU.

1. На вкладке **Administration** (Администрирование) выберите пункт **Network** (Сеть) в строке меню и пункт **ssl certificate** под заголовком **Web** (Веб) в левом меню навигации.

2. Выберите **Add or Replace Certificate File** (Добавить или заменить файл сертификата) и найдите файл сертификата, файл с расширением **.p15**, созданный в процедуре Создание корневого сертификата и сертификатов серверов. (Местоположение по умолчанию: **C:\Program Files\Dell\Rack PDU Security Wizard**.)

Для передачи сертификата сервера можно воспользоваться FTP или Secure CoPy (SCP). В случае использования протокола SCP команда для отправки сертификата с именем **cert.p15** в устройство Rack PDU с IP-адресом 156.205.6.185 выглядит так:

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

Создание сертификата сервера и запроса на подписание

Сводка

Используйте данную процедуру, если ваша компания или агентство имеет собственный сертификационный орган, или если вы не хотите использовать коммерческий сертификационный орган для подписи своего серверного сертификата.

- Создайте запрос подписи сертификата (CSR). CSR содержит всю информацию сертификата сервера, за исключением цифровой подписи. Данный процесс создает два файла:
  - Файл с расширением **.p15** содержит секретный ключ Rack PDU.
  - Файл с расширением **.csr** содержит запрос подписи сертификата, который вы отправляете в сторонний орган сертификации.
- При получении подписанного сертификата из органа сертификации, импортируйте этот сертификат. При импортировании сертификата происходит объединение файла **.p15**, содержащего секретный ключ, и файла, содержащего сертификат, подписанный внешним сертифицирующим органом. Результирующим файлом является новый шифрованный сертификат сервера с расширением **.p15**.
- Загрузите сертификат сервера в устройство Rack PDU.
- Для каждого устройства Rack PDU, требующего сертификат сервера, повторите задачу, с помощью которой создается и загружается сертификат сервера.

Процедура

Создание запроса на подписание сертификата (Certificate Signing Request – CSR).

1. Если программа Rack PDU Security Wizard не установлена на вашем компьютере, найдите и запустите программу установки (**Rack PDU Security Wizard.exe)**.
2. В меню Windows **Start** (Пуск) выберите пункт **Programs** (Программы), затем – **Rack PDU Security Wizard**.
3. В диалоговом окне, помеченном **Step 1** (Шаг 1), выберите **Certificate Request** (Запрос сертификата) в качестве типа создаваемого файла и выберите затем длину генерируемого ключа (1024 бит – значение по умолчанию или 2048 бит, чтобы обеспечить сложное шифрование и повышенный уровень секретности).
4. Введите имя файла, который будет содержать секретный ключ Rack PDU. Файл должен иметь расширение **.p15** и, по умолчанию, будет создан в папке установки **C:\Program Files\Dell\Rack PDU Security Wizard**.
5. В диалоговом окне, помеченном **Step 2** (Шаг 2), сообщите сведения для конфигурации запроса подписи сертификата (CSR), то есть те сведения, которые, по вашему мнению, должен содержать подписанный сертификат сервера. Поля, которые требуется заполнить – **Country** (Страна) и **Common Name** (Общее имя). Другие поля являются необязательными. В поле **Common Name** введите IP-адрес или имя DNS устройства Rack PDU.

По умолчанию, сертификат сервера действителен 10 лет с момента получения, но вы можете отредактировать поля **Validity Period Start** (Начало срока действия) и **Validity Period End** (Конец срока действия).

6. В следующем диалоговом окне проверьте общие сведения о сертификате. Пролистайте вниз уникальный серийный номер и метки сертификата. Чтобы внести изменения в сообщенные вами сведения, нажмите **Back** (Назад). Откорректируйте информацию.

Информация о субъекте сертификата и информация стороны, выдавшей сертификат, должны быть идентичны.

7. Последнее окно подтверждает, что запрос подписи сертификата создан, и отображает местоположение и имя файла, имеющего расширение **.csr**.
8. Направьте запрос на подпись сертификата во внешний орган сертификации: коммерческий или, если имеется возможность, сертификационный орган, управляемый вашей компанией или агентством.

См. инструкции, предоставляемые органом сертификации, относительно подписания и издания серверных сертификатов.

Импорт подписанного сертификата. После того как внешний сертификационный орган вернет подписанный сертификат, импортируйте полученный сертификат. Данная процедура объединяет подписанный сертификат и секретный ключ в серверный сертификат SSL, который затем загружается в Rack PDU.

1. В меню Windows **Start** (Пуск) выберите пункт **Programs** (Программы), затем – **Rack PDU Security Wizard**.
2. В диалоговом окне **Step 1** (Шаг 1) выберите **Import Signed Certificate** (Импорт подписанного сертификата).
3. Найдите и выберите подписанный сертификат сервера, полученный от внешнего сертифицирующего органа. Этот файл будет иметь расширение **.cer** или **.crt**.

4. Найдите и выделите файл, созданный в пункте step 4 задачи Создание запроса на подписание сертификата (Certificate Signing Request – CSR). Данный файл, имеющий расширение **.p15**, содержит закрытый ключ для Rack PDU и, по умолчанию, находится в папке установки **C:\Program Files\Dell\Rack PDU Security Wizard**.
5. Задайте имя выходного файла, который будет представлять собой подписанный сертификат сервера и будет загружаться в Rack PDU. Файл должен иметь расширение **.p15**.
6. Нажмите **Next** (Далее) для генерации сертификата сервера. **Issuer Information** (Информация о стороне, выдавшей сертификат) в общем окне подтверждает, что внешний орган сертификации подписал сертификат.
7. Последнее диалоговое окно подтверждает, что сертификат выдан, и содержит инструкции по загрузке сертификата в Rack PDU. Оно отображает местоположение и имя сертификата сервера, имеющего расширение **.p15** и содержащего секретный ключ устройства Rack PDU и открытый ключ, полученный из файла **.cer** или **.crt**.

Загрузка сертификата сервера в Rack PDU.

1. На вкладке **Administration** (Администрирование) выберите пункт **Network** (Сеть) в строке меню и пункт **ssl certificate** (сертификат ssl) под заголовком **Web** (Веб) в левом меню навигации.
2. Выберите **Add or Replace Certificate File** (Добавить или заменить файл сертификата) и найдите файл сертификата, файл с расширением **.p15** , созданный в процедуре Создание корневого сертификата и сертификатов серверов. (Местоположение по умолчанию: **C:\Program Files\Dell\Rack PDU Security Wizard**.)

Кроме того, для передачи сертификата сервера в Rack PDU можно воспользоваться протоколом FTP или Secure CoPy (SCP). Команда для передачи сертификата с именем **cert.p15** на Rack PDU с IP-адресом 156.205.6.185 для SCP будет следующей:

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

Создание хост-ключа SSH

Сводка

Данная процедура является необязательной. Если вы выберете использование шифрования SSH, но не создадите хост-ключа, устройство Rack PDU при перезагрузке сгенерирует 2048-битный ключ RSA. Вы должны указать, будет ли хост-ключ для SSH, создаваемый программой Rack PDU Security Wizard, иметь 1024 или 2048 бит.

Можно сгенерировать 1024-битный или 2048-битный ключ, который обеспечивает комплексное шифрование и высокий уровень безопасности.

- Используйте программу Rack PDU Security Wizard для создания хост-ключа, который будет зашифрован и помещен в файл с расширением **.p15**.
- Загрузите хост-ключ в устройство Rack PDU.

Процедура

Создание хост-ключа.

1. Если программа Rack PDU Security Wizard не установлена на вашем компьютере, найдите и запустите программу установки (**Rack PDU Security Wizard.exe)**.
2. В меню Windows **Start** (Пуск) выберите пункт **Programs** (Программы), затем – **Rack PDU Security Wizard**.
3. В диалоговом окне **Step 1** (Шаг 1) выберите **SSH Server Host Key** (Хост-ключ сервера SSH) в качестве типа создаваемого файла и выберите затем длину генерируемого ключа (1024 бит – значение по умолчанию или 2048 бит, чтобы обеспечить сложное шифрование и повышенный уровень секретности).
4. Задайте имя файла, в котором будет содержаться хост-ключ. Файл должен иметь расширение **.p15**. По умолчанию, файл будет создан в папке установки **C:\Program Files\Dell\Rack PDU Security Wizard**.
5. Нажмите **Next** (Далее) для генерации хост-ключа.
6. Итоговое окно показывает метки SSH версии 2, которые являются уникальными для каждого из хост-ключей и идентифицируют хост-ключи. После загрузки хост-ключей в Rack PDU вы можете проверить правильность их загрузки: для этого проверьте, чтобы метки, показанные здесь, совпадали с метками SSH на устройстве Rack PDU, которые показывает программа SSH-клиента.
7. Последнее окно служит для проверки того, что хост-ключ был создан, дает инструкции по загрузке хост-ключей в Rack PDU и показывает местоположение и имя файла хост-ключа, который будет иметь расширение **.p15**.

Загрузка хост-ключа в Rack PDU.

1. На вкладке **Administration** (Администрирование) выберите пункт **Network** (Сеть) в строке меню и пункт **ssh host key** (хост-ключ ssh) под заголовком **Console** (Консоль) в левом меню навигации.
2. Выберите **Add or Replace Host Key** (Добавить или заменить хост-ключ) и найдите файл хост-ключа с расширением **.p15**, созданный в процедуре Создание хост-ключа. (Местоположение по умолчанию: **C:\Program Files\Dell\Rack PDU Security Wizard**.)
3. В нижней части страницы **User Host Key** (Хост-ключ пользователя) находится метка SSH. Зайдите в Rack PDU через программу SSH-клиента и проверьте, что был загружен правильный хост-ключ, для чего проверьте, чтобы его метки совпадали с метками, показываемыми программой-клиентом.

Кроме того, для передачи файла хост-ключа в Rack PDU можно воспользоваться протоколом FTP или Secure CoPy (SCP). В случае использования протокола SCP команда для отправки хост-ключа с именем **cert.p15** в устройство Rack PDU с IP-адресом 156.205.6.185 выглядит так:

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

Доступ к интерфейсу командной строки и безопасность

Пользователь учетной записи «администратор» или «пользователь устройства» может получить доступ к интерфейсу командной строки с помощью Telnet или Secure SHell (SSH) в зависимости от включенных методов. (Администратор может включить эти методы доступа, выбрав вкладку **Administration** (Администрирование), затем выбрав **Network** (Сеть) в верхнем меню и указав параметр **access** (доступ) под заголовком **Console** (Консоль) в левом навигационном меню). По умолчанию включен протокол Telnet. При включении SSH автоматически отключается Telnet.

Протокол Telnet для стандартного доступа. Протокол Telnet обеспечивает стандартную аутентификацию по имени пользователя и паролю, однако не имеет преимуществ шифрования, обеспечивающих высокий уровень защиты.

Протокол SSH для доступа с высоким уровнем защиты. Если для обеспечения высокой защиты веб-интерфейса используется SSL, для доступа к интерфейсу командной строки нужно использовать протокол Secure SHell (SSH). Программа SSH выполняет шифрование имен пользователей, паролей и передаваемых данных.

Вне зависимости от способа доступа к интерфейсу командной строки (SSH или Telnet), учетные записи пользователей и права доступа пользователей остаются неизменными. Однако, чтобы пользоваться SSH, необходимо сначала установить на компьютере клиентскую программу SSH и выполнить ее настройку.

Telnet и Secure Shell (SSH)

При включенном режиме SSH невозможно использовать Telnet для доступа к интерфейсу командной строки. Включение SSH включает SCP автоматически.

Если протокол SSH включен, и его порт сконфигурирован, никаких дальнейших конфигураций для использования Secure CoPy (SCP) не требуется. SCP использует настройки протокола SSH.

Чтобы использовать SSH, необходимо иметь установленный клиент SSH. Большинство ОС Linux и других UNIX® платформ имеют SSH-клиент, но ОС Microsoft Windows не имеет такового. Имеются SSH-клиенты различных производителей.

Для настройки параметров Telnet и Secure Shell (SSH):

1. На вкладке веб-интерфейса **Administration** (Администрирование) выберите пункт **Network** (Сеть) в строке меню и пункт **access** (доступ) под заголовком **Console** (Консоль) в левом меню навигации.
2. Конфигурация настроек порта для Telnet и SSH.

   Подробней о повышенной безопасности, обеспечиваемой заданием нестандартных портов, см. раздел Назначения портов.

3. На вкладке **Console** (Консоль) в левом меню навигации, выберите **ssh host key** (хост-ключ ssh), укажите файл хост-ключа, предварительно созданный с помощью программы Rack PDU Security Wizard, и загрузите его в Rack PDU.

   Если вы не указали файл хост-ключа, установили недействительный хост-ключ или активировали протокол SSH без установленного хост-ключа, устройство Rack PDU сгенерирует хост-ключ RSA длиной 2048 бит. Чтобы устройство Rack PDU создало хост-ключ, нужно перезагрузить его. **Создание ключа устройством** Rack PDU **может занять до 1 минуты, в течение этого времени SSH будет недоступным.**

   В качестве альтернативы, для передачи файла хост-ключа можно использовать команды FTP или Secure CoPy (SCP) в интерфейсе командной строки, например, строке приглашения ОС Windows.

4. Настройте отображение *идентификационной метки* хост-ключа SSH для SSH версии 2. Большинство клиентов SSH отображают данную метку в начале сессии. Проверьте, что метка, отображаемая клиентом, и метка веб-интерфейса или командной строки Rack PDU совпадают.

Веб-интерфейс – доступ и безопасность: HTTP и HTTPS (с SSL)

Протокол передачи гипертекста (HTTP) предоставляет доступ с помощью имени пользователя и пароля, при этом имя пользователя, пароль и передаваемые данные не шифруются. Протокол передачи гипертекстов через защищенный сокет (HTTPS) шифрует имена пользователей, пароли и данные в момент передачи, а также осуществляет авторизацию Rack PDU посредством цифровых сертификатов.

Для выбора метода использования цифровых сертификатов см. Создание и установка цифровых сертификатов.

Для конфигурации HTTP и HTTPS:

1. На вкладке **Administration** (Администрирование) выберите пункт **Network** (Сеть) в строке меню и пункт **access** (доступ) под заголовком **Web** (Веб) в левом меню навигации.
2. Включите HTTP или HTTPS и сконфигурируйте порты для каждого из указанных протоколов. Изменения вступят в действие после следующей перезагрузки. Если протокол SSL включен, ваша программа-обозреватель будет отображать маленький значок в виде замка.

Подробней о повышенной безопасности, обеспечиваемой заданием нестандартных портов, см. раздел Назначения портов.

3. Выберите **ssl certificate** (сертификат ssl) под заголовком **Web** (Веб) в левом меню навигации, чтобы определить, установлен ли сертификат сервера на устройстве Rack PDU. Если сертификат был создан с помощью программы Rack PDU Security Wizard, но не установлен:
   - В веб-интерфейсе найдите файл сертификата и загрузите его в Rack PDU.
   - С помощью протоколов Secure CoPy (SCP) или FTP загрузите файл сертификата в Rack PDU.

Предварительное создание и загрузка сертификата сервера позволит сократить время, требуемое для включения протокола HTTPS. Если протокол HTTPS включен, а ни один сертификат сервера не загружен, устройство Rack PDU создаст сертификат при последующей перезагрузке. **Создание сертификата устройством Rack PDU может занять до 1 минуты, в течение этого времени SSL будет недоступным.**

Сертификат, сгенерированный Rack PDU, имеет некоторые ограничения. См. Метод 1: Использование сертификата по умолчанию, автоматически сгенерированного устройством Rack PDU.

4. Если загружен действительный цифровой сертификат сервера, то в поле **Status** (Состояние) будет видна ссылка **Valid Certificate** (Действительный сертификат). Щелкните ссылку, чтобы увидеть параметры сертификата.

Параметр	Описание
Issued To: (Выпущен для:)	**Common Name (CN)**: IP-адрес или DNS-имя устройства Rack PDU. Это поле показывает, какое имя вы должны использовать для загрузки в веб-интерфейс. • Если при создании сертификата для данного поля был указан IP-адрес, используйте для загрузки IP-адрес. • Если при создании сертификата для данного поля было указано имя DNS, используйте для загрузки имя DNS. Если вы не используете IP-адрес или имя DNS, указанные в сертификате, авторизация не пройдет, и вам будет передано сообщение об ошибке и предложение продолжить загрузку. Для сертификата сервера, сгенерированного по умолчанию устройством Rack PDU в этом поле отображается серийный номер Rack PDU. **Organization (O)**, **Organizational Unit (OU)** и **Locality, Country:** Имя, название подразделения и местоположение организации, использующей сертификат сервера. Для сертификата сервера, сгенерированного по умолчанию устройством Rack PDU, в поле **Organizational Unit (OU)** отображается «Внутренне сгенерированный сертификат». **Serial Number**: Серийный номер серверного сертификата.
Issued By: (Выпущен:)	**Common Name (CN)**: Общее имя, которое указано в корневом сертификате CA. Для сертификата сервера, сгенерированного по умолчанию устройством Rack PDU в этом поле отображается серийный номер Rack PDU. **Organization (O)** и **Organizational Unit (OU)**: Имя организации и название подразделения, которое выпустило сертификат сервера. Если сертификат сервера был сгенерирован по умолчанию устройством Rack PDU, в этом поле отображается «Внутренне сгенерированный сертификат».

Параметр	Описание
Validity: (Срок действия:)	**Issued on**: Дата и время выпуска сертификата. **Expires on**: Дата и время окончания срока действия сертификата.
Fingerprints (Метки):	Каждая из двух меток представляет собой длинную строку цифровых и буквенных символов, разделенных запятыми. Метка является уникальным идентификатором для последующей аутентификации сервера. Запишите метки для сравнения их с метками, содержащимися в сертификате, как показано в браузере. **SHA1 Fingerprint**: Метка, созданная алгоритмом хеширования Secure Hash Algorithm (SHA-1). **MD5 Fingerprint**: Метка, созданная алгоритмом Message Digest 5 (MD5).

Поддерживаемые функции и серверы RADIUS

Поддерживаемые функции

Поддерживаемые функции аутентификации и авторизации: Служба дистанционной аутентификации пользователей Remote Authentication Dial-In User Service (RADIUS). RADIUS используется для централизованного администрирования дистанционного доступа к каждому устройству Rack PDU. При обращении пользователя к Rack PDU запрос аутентификации отправляется на сервер RADIUS с целью определения уровня доступа данного пользователя.

Дополнительную информацию об уровнях допуска см. в разделе Типы учетных записей.

Поддерживаемые серверы RADIUS

Поддерживаемые серверы RADIUS: FreeRADIUS и Microsoft IAS 2003. Другие часто используемые приложения RADIUS могут работать, но они не были всесторонне протестированы.

Конфигурация Rack PDU

Аутентификация

Имена пользователей RADIUS, используемые Rack PDU (Устройство распределения питания для монтажа в стойку), не должны превышать в длину 32 символа.

На вкладке **Administration** (Администрирование) выберите пункт **Security** (Безопасность) в строке меню. Затем, в пункте **Remote Users** (Удаленные пользователи) в левом меню навигации выберите пункт **authentication** (аутентификация), чтобы определить метод аутентификации:

- **Local Authentication Only** (Только локальная аутентификация): RADIUS отключен. Локальная аутентификация включена.
- **RADIUS, then Local Authentication** (RADIUS, затем локальная аутентификация): RADIUS и локальная аутентификация включены. Сначала запрашивается аутентификация от сервера RADIUS; локальная аутентификация используется только, если сервер RADIUS не отвечает.
- **RADIUS Only** (Только RADIUS): RADIUS включен. Локальная аутентификация отключена.

Если выбран режим **RADIUS Only**, а сервер RADIUS недоступен, неверно идентифицирован или неверно сконфигурирован, удаленный доступ будет запрещен для всех пользователей. Чтобы восстановить доступ, необходимо воспользоваться последовательным подключением к интерфейсу командной строки и изменить настройки доступа RADIUS на **`local`** или **`radiusLocal`**. Например, команда изменения настройки доступа на **`local`** имеет следующий вид:

```
radius -a local
```

RADIUS

Чтобы настроить RADIUS, на вкладке **Administration** (Администрирование) выберите пункт **Security** (Безопасность) в строке меню. Затем, в пункте **Remote Users** (Удаленные пользователи) в левом меню навигации выберите пункт **RADIUS**.

Настройка	Описание
RADIUS Server (Сервер RADIUS)	Имя сервера или IP-адрес сервера RADIUS. **ПРИМЕЧАНИЕ:** Серверы RADIUS по умолчанию используют для аутентификации пользователей порт 1812. Чтобы использовать другой порт, добавьте к имени сервера RADIUS или к IP-адресу двоеточие с последующим указанием номера нового порта.
Secret (Секрет)	Общая секретная фраза сервера RADIUS и устройства Rack PDU.
Reply Timeout (Время ожидания ответа)	Время в секундах, в течение которого Rack PDU ждет ответа от сервера RADIUS.
Test Settings (Настройки тестирования)	Введите имя пользователя администратора и пароль для тестирования пути к серверу RADIUS, который вы сконфигурировали.
Skip Test and Apply (Пропустить тестирование и применить)	Не тестировать путь к серверу RADIUS.

Если перечислены два сконфигурированных сервера, и указаны режимы **RADIUS, then Local Authentication** (RADIUS, затем локальная аутентификация) или **RADIUS Only** (только RADIUS), вы можете выбрать, какой из серверов RADIUS будет авторизовать пользователей, выбрав переключатель приоритета серверов **Switch Server Priority**.

Конфигурирование сервера RADIUS

Для работы с Rack PDU вы должны сконфигурировать сервер RADIUS. Примеры в данном разделе могут разниться в деталях от требуемого содержимого или формата настроек вашего сервера RADIUS. В примерах упоминание выходов применимо только к тем устройствам Rack PDU, которые поддерживают выходных потребителей.

1. Добавьте IP-адрес Rack PDU в список клиентов сервера RADIUS (файл).
2. Пользователи должны быть сконфигурированы с атрибутами типов служб, если не определены атрибуты производителя (VSA). Если ни один атрибут типов служб не сконфигурирован, пользователь будет иметь доступ только на чтение (только к веб-интерфейсу). Имеется два приемлемых значения: Service-Type (тип службы) и Administrative-User (администратор-пользователь) (6), которые дают пользователю права администратора, и одно значение Login-User (загрузка-пользователь) (1), дающее пользователю права доступа Пользователь устройства.

Подробнее о файле пользователей RADIUS см. документацию по серверу RADIUS.

Пример использования атрибутов Service-Type

В следующем примере пользовательского файла RADIUS:

- **RPDUAdmin** соответствует типу
  Service-Type: Administrative-User, (6)
- **RPDUDevice** соответствует типу **Service-Type: Login-User, (1)**
- **RPDUReadOnly** соответствует типу **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"
```

Пример использования атрибутов изготовителя

Атрибуты пользователя (VSA) могут применяться вместо атрибутов Service-Type, предоставляемых сервером RADIUS. Этот метод требует наличия словарной статьи и файла пользователей RADIUS. В файле словаря можно определять имена ключевых слов ATTRIBUTE (атрибут) и VALUE (значение), но не численные значения. Если вы измените численные значения, аутентификация и авторизация RADIUS не будут работать корректно. VSA имеет преимущество перед стандартными атрибутами RADIUS.

Файл словаря. Ниже приведен пример файла словаря RADIUS (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
```

Файл пользователей RADIUS с атрибутами VSA. Ниже приведен пример файла RADIUS с атрибутами VSA:

```
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

# Дает пользователям доступ к выходам устройства  1, 2 и 3.
VSAOutlet    Auth-Type = Local, Password = "outlet"
             DELL-Service-Type = Outlet,
             DELL-Outlets = "1,2,3"
```

См. связанные темы:

- информацию о трех основных уровнях допуска пользователя (Администратор, Пользователь устройства и Пользователь только для чтения) см. в разделе Типы учетных записей.
- информацию о протестированных и поддерживаемых серверах RADIUS см. в разделе Поддерживаемые серверы RADIUS.

Пример с теневыми паролями UNIX. Если используются файлы теневых паролей UNIX (**/etc/passwd**) при наличии файлов словарей RADIUS можно использовать два метода аутентификации пользователей:

- Если все пользователи UNIX имеют административные привилегии, добавьте следующие операции для «пользовательского» файла RADIUS. Чтобы задать доступ только для пользователей устройства (Device Users), измените атрибут Dell-Service-Type на **`Device`** (Устройство).

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

- Добавьте имена пользователей и атрибуты в «пользовательский» файл RADIUS и проверьте пароль, сравнив его с **/etc/passwd**. Следующий пример относится к пользователям **`bconners`** и **`thawk`**:

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

Предметный указатель

S

T

X

A

Б

В

Г

Д

Е

Ж

З

И

К

Л

М

Н

О

П

P

C

Т

У

Ф

Х

Ч

Ш

Э

РУКОВОДСТВО

Управляемое устройство Rack PDU

11/2010 Номер детали 990-3926-028

www.dell.com | support.dell.com