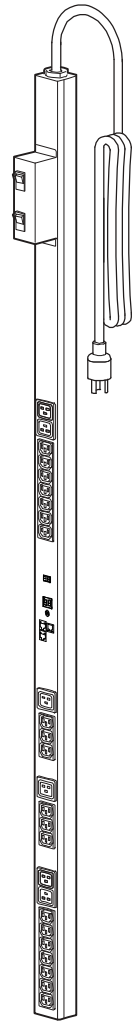
Benutzer-handbuch

Managed Rack Power Distribution Unit (Überwachte Verteilerleiste)



BENUTZERHANDBUCH

Metered Rack PDU (Überwachte Verteilerleiste)

Inhalt

Einführung 1

Funktionen des Produkts 1
Erste Schritte 4
Festlegen der Netzwerkeinstellungen 5
Zugriff nach Verlust des Passworts 9

Frontblende der Rack PDU 11

Befehlszeile 16

Wissenswertes zur Befehlszeile 16
Anmelden über die Befehlszeile 16
Wissenswertes zur Hauptmaske 19
Verwendung der Befehlszeile 22
Befehlssyntax 23
Befehlsrückgabe-Codes 24
Beschreibung der Befehle der Netzwerkmanagement-Karte 25
Beschreibung der Gerätebefehle 48

Web-Oberfläche 86

Unterstützte Web-Browser 86
Anmelden bei der Web-Oberfläche 87
Funktionen der Web-Oberfläche 90
Wissenswertes zur Registerkarte „Home“ 93

Verwaltung des Geräts 96

Wissenswertes zur Registerkarte Device Manager 97
Anzeigen des Lastzustands und der Spitzenlast 97
Konfigurieren von Lastgrenzwerten 98
Konfigurieren von Name und Standort der Rack PDU 99
Einstellen der Kaltstartverzögerung 99
Zurücksetzen der Spitzenlast und der kWh-Zahl 100
Konfigurieren und Steuern der Ausgangsanschlussgruppen 100
Einstellungen für Ausgangsanschlüsse und Ausgangsanschlussgruppen 112
Planen von Ausgangsanschlussvorgängen 117
Menü Outlet Manager 123

Umgebung 124

Konfigurieren von Temperatur- und Feuchtigkeitssensoren 125
Konfigurieren potentialfreier Eingangskontakte 127

Protokolle 128

Daten- und Ereignisprotokolle 129

Verwaltung: Sicherheit 139

Lokale Benutzer 140
Remote-Benutzer 142
Konfigurieren des RADIUS-Servers 145
Timeout bei Inaktivität 147

Verwaltung: Benachrichtigung 148

Ereignisaktionen 149
Aktive, automatische, direkte Benachrichtigung 153

Verwaltung: Netzwerkfunktionen 163

TCP/IP und Kommunikationseinstellungen 164
Ping-Antwort 170
Port Speed 171
DNS 172
Web 175
Console 177
SNMP 179
FTP Server 184

Verwaltung: Allgemeine Optionen 185

Identifizierung 186
Einstellen von Datum und Uhrzeit 187
Verwendung einer INI-Datei 189
Ereignisprotokoll und Temperatureinheiten 190
Zurücksetzen der Rack PDU. 191
Konfigurieren der Links 192
Informationen zur Rack PDU 192

Exportieren von Konfigurationseinstellungen 193

Abrufen und Exportieren der INI-Datei 193
Ereignis- und Fehlermeldungen zur Dateiübertragung 197

Dateiübertragungen 199

Aktualisieren der Firmware 199
Übertragungsverfahren für Firmware-Dateien 201
Überprüfen von Upgrades und Aktualisierungen 204

Problembehandlung 206

Rack PDU Probleme beim Zugriff 206

Anhang A: Liste der unterstützten Befehle 208

Anhang B: Sicherheitshandbuch 213

Zweck und Inhalt dieses Anhangs 213
Sicherheitsfunktionen 214
Authentifizierung 219
Encryption 220
Erstellen und Installieren von digitalen Zertifikaten 225
Firewalls 230
Verwendung des Sicherheitsassistenten (Security Wizard) der Rack PDU 231
Erstellen eines Stammzertifikats und der Server-Zertifikate 235
Erstellen eines Server-Zertifikats und eines Signing Request 240
Erstellen eines SSH-Host-Schlüssels 245
Zugriff über die Befehlszeile und Sicherheitsaspekte 248
Telnet und Secure Shell (SSH) 249
Zugriff über die Befehlszeile und Sicherheitsaspekte: HTTP und HTTPS (mit SSL) 251
Unterstützte RADIUS-Funktionen und -Server 255
Konfigurieren der Rack PDU 256
Konfigurieren des RADIUS-Servers 258

Index 262

Einführung

Funktionen des Produkts

Bei der Dell® Managed Rack Power Distribution Unit (PDU) handelt es sich um eine eigenständige, über das Netzwerk administrierbare Stromverteilerleiste. Die Rack PDU ermöglicht eine Remote-Überwachung der angeschlossenen Lasten in Echtzeit. Benutzerdefinierte Alarme warnen vor potenziellen Überlastungen der Schaltkreise. Die Rack PDU gibt Ihnen über Remote-Befehle und Einstellmöglichkeiten der Benutzeroberfläche die uneingeschränkte Kontrolle über die Ausgangsanschlüsse.

Sie können eine Rack PDU über die dazugehörige Web-Oberfläche, über die Befehlszeile oder über das Simple Network Management Protocol (SNMP) verwalten:

- Der Zugriff auf die Web-Oberfläche kann über das Hypertext Transfer Protocol (HTTP) oder über Secure HTTP (HTTPS) mit Secure Sockets Layer (SSL) erfolgen. Siehe Anmelden bei der Web-Oberfläche.
- Der Zugriff auf die Befehlszeile kann über eine serielle Datenverbindung, Telnet oder Secure Shell (SSH). Siehe Wissenswertes zur Befehlszeile.
- Für die Verwaltung der Rack PDU verwenden Sie einen SNMP-Browser und die Dell Management Information Base (MIB).

Rack PDUs verfügen darüber hinaus über die folgenden Funktionen:

- Überwachung von Spitzenlast, Leistung und Stromverbrauch für alle angeschlossenen Lasten
- Überwachung von Spannung, Stromstärke und Leistung für alle Phasen
- Leistungsüberwachung für die einzelnen Ausgangsanschlüsse
- Konfigurierbare Grenzwerte für die Auslösung von Netzwerk- und LED-Alarmen bei drohender Schaltkreisüberlastung
- Vier Ebenen für Benutzer-Zugriffskonten: Administrator, Benutzer „Gerät“, Benutzer „schreibgeschützt“ und Benutzer „Ausgangsanschluss“

- Unabhängige Ausgangsanschlusssteuerung
- Konfigurierbare Einschaltverzögerungen
- Bis zu 24 unabhängige Benutzerkonten für Ausgangsanschlüsse
- Ereignis- und Datenprotokollierung Auf das Ereignisprotokoll kann über Telnet, Secure CoPy (SCP), File Transfer Protocol (FTP), eine serielle Verbindung oder einen Web-Browser (per HTTPS mit SSL, oder per HTTP) zugegriffen werden. Auf das Datenprotokoll kann über einen Web-Browser, SCP oder FTP zugegriffen werden.
- E-Mail-Benachrichtigungen für Rack PDU- und Systemereignisse.
- SNMP-Trap, Syslog-Nachrichten und E-Mail-Benachrichtigungen in Abhängigkeit vom Schweregrad oder der Kategorie des jeweiligen Rack PDU- oder Systemereignisses.
- Sicherheitsprotokolle für Authentifizierung und Verschlüsselung.

Die Rack PDU bietet keinen Überspannungsschutz. Schließen Sie zum Schutz des Geräts vor Stromausfällen oder Spannungsspitzen eine unterbrechungsfreie Stromversorgung (USV) an die Rack PDU an.

Zugriffsprioritäten für die Anmeldung

Es kann sich immer nur ein Benutzer gleichzeitig bei der Rack PDU anmelden. Die Zugriffspriorität lautet wie folgt (in absteigender Folge):

- Lokaler Zugriff auf die Befehlszeile über einen Computer mit direkter serieller Verbindung zur Rack PDU
- Telnet- oder SSH-Zugriff auf die Befehlszeile über einen Remote-Computer
- Web-Zugriff

Informationen über die Kontrolle des Zugriffs auf die Rack PDU über SNMP finden Sie unter SNMP.

Benutzerkontotypen

Die Rack PDU kennt vier (Administrator, Benutzer „Gerät“, Benutzer „schreibgeschützt“ und Benutzer „Ausgangsanschluss“); diese sind jeweils durch Benutzername und Passwort geschützt.

- Ein Administrator darf alle Menüs der Web-Oberfläche und alle Befehle der Befehlszeile benutzen. Als Benutzername und Passwort ist jeweils **admin** vorgegeben.
- Ein Benutzer „Gerät“ kann ausschließlich auf folgende Komponenten zugreifen:
  - Auf der Web-Oberfläche die Menüs der Registerkarten **Device Manager** (Geräte-Manager) und **Environment** (Umgebung) sowie der im linken Navigationsmenü des Registers **Logs** (Protokolle) mit **Events** und **Data** betitelten Ereignis- und Datenprotokolle. Zu den Ereignis- und Datenprotokollen wird eine Schaltfläche zum Löschen der Protokolldaten angezeigt.
  - In der Befehlszeile stehen entsprechende Funktionen und Optionen zur Verfügung.

  Als Benutzername und Passwort ist jeweils **device** vorgegeben.
- Der Benutzer „schreibgeschützt“ verfügt lediglich über die folgenden, eingeschränkten Zugriffsmöglichkeiten:
  - Zugriff ausschließlich über die Web-Oberfläche.
  - Zugriff auf dieselben Registerkarten und Menüs wie ein Benutzer „Gerät“, jedoch ohne die Möglichkeit, Konfigurationen zu ändern, Geräte zu steuern, Daten zu löschen oder Optionen für Dateiübertragungen zu verwenden. Die Links zu den Konfigurationsoptionen werden zwar angezeigt, sind jedoch deaktiviert. Zu den Ereignis- und Datenprotokollen wird eine Schaltfläche zum Löschen der Protokolldaten angezeigt.

  Als Benutzername und Passwort ist jeweils **readonly** vorgegeben.

Informationen zum Ändern des **Benutzernamens** und des **Passworts** bei diesen vier Kontoarten finden Sie unter Einrichten von Zugriffsrechten.

- Der Benutzer „Ausgangsanschluss“ verfügt lediglich über die folgenden, eingeschränkten Zugriffsmöglichkeiten:
  - Zugriff über die Web-Oberfläche und die Befehlszeile
  - Zugriff auf dieselben Menüs wie ein Benutzer „Gerät“, jedoch ohne die Möglichkeit, Konfigurationen zu ändern, Geräte zu steuern, Daten zu löschen oder Optionen für Dateiübertragungen zu verwenden. Die Links zu den Konfigurationsoptionen werden zwar angezeigt, sind jedoch deaktiviert. Der Benutzer „Ausgangsanschluss“ hat Zugriff auf den Menübefehl **Outlet Control** (Ausgangsanschlusssteuerung), der ihm die Steuerung der ihm vom Administrator zugewiesenen Ausgangsanschlüsse ermöglicht. Der Benutzer „Ausgangsanschluss“ darf keine Ereignis- oder Datenprotokolle löschen.

  Benutzername und Passwort werden beim Anlegen eines neuen Benutzers „Ausgangsanschluss“ vom Administrator festgelegt.

Erste Schritte

So nehmen Sie die Rack PDU in Betrieb:

1. Bauen Sie die Rack PDU unter Beachtung der mitgelieferten *Einbauanleitung für die Rack-Stromverteilerleiste* ein.
2. Schließen Sie das Gerät an das Stromnetz und an das Netzwerk an. Halten Sie sich dabei an die *Einbauanleitung für die Rack-Stromverteilerleiste*.
3. Legen Sie die Netzwerkeinstellungen fest (siehe Festlegen der Netzwerkeinstellungen).
4. Sie können die Rack PDU auf eine der folgenden Arten in Betrieb nehmen:
   - Web-Oberfläche
   - Befehlszeile
   - Frontblende der Rack PDU

Festlegen der Netzwerkeinstellungen

Bevor die Rack PDU im Netzwerk betrieben werden kann, müssen Sie die folgenden Einstellungen für TCP/IP festlegen:

- IP-Adresse der Rack PDU
- Teilnetzmaske
- Standard-Gateway

Wenn kein Standard-Gateway zur Verfügung steht, geben Sie die IP-Adresse eines Computers an, der sich in demselben Teilnetz wie die Rack PDU befindet und normalerweise in Betrieb ist. Bei geringem Netzwerkverkehr verwendet die Rack PDU das Standard-Gateway, um das Netzwerk zu testen.

Die Loopback-Adresse (127.0.0.1) nicht als Adresse des Standard-Gateways für die Rack PDU verwenden. Damit deaktivieren Sie die Karte und müssen die TCP/IP-Einstellungen über eine serielle lokale Anmeldung auf die Standardwerte zurücksetzen.

Konfigurationsmethoden für TCP/IP

Verwenden Sie eine der folgenden Methoden, um die von der Rack PDU benötigten TCP/IP-Einstellungen vorzunehmen:

- Konfiguration über BOOTP und DHCP
- Befehlszeile

Konfiguration über BOOTP und DHCP

Die Standardeinstellung für die TCP/IP-Konfiguration, **DHCP**, setzt voraus, dass ein ordnungsgemäß konfigurierter DHCP-Server verfügbar ist, von dem die Rack PDU ihre TCP/IP-Einstellungen beziehen kann. Sie können diese Einstellung auch für BOOTP konfigurieren.

Sie können eine benutzerdefinierte Initialisierungsdatei (INI-Datei) zur Anmeldung an einem BOOTP- oder DHCP-Server verwenden. Weitere Informationen finden Sie unter Verwendung einer INI-Datei.

BOOTP. Damit die Rack PDU einen BOOTP-Server zum Konfigurieren ihrer TCP/IP-Einstellungen verwenden kann, muss sie einen ordnungsgemäß konfigurierten, RFC951-konformen BOOTP-Server vorfinden.

Geben Sie in der Datei BOOTPTAB des BOOTP-Servers die MAC-Adresse, die IP-Adresse, die Teilnetzmaske und den Standard-Gateway der Rack PDU sowie den Namen einer gegebenenfalls verwendeten Initialisierungsdatei ein. Die MAC-Adresse befindet sich auf der Bodenplatte der Rack PDU oder auf dem Qualitätskontrollabschnitt im Paket.

Bei einem Neustart der Rack PDU erhält dieser vom BOOTP-Server die TCP/IP-Einstellungen.

- Wenn Sie den Namen einer Bootdatei eingegeben haben, versucht die Rack PDU, die betreffende Datei über TFTP oder FTP vom BOOTP-Server zu laden. Die Rack PDU übernimmt alle Einstellungen aus der Bootdatei.
- Wenn Sie keine Initialisierungsdatei angegeben haben, können Sie die anderen Einstellungen der Rack PDU per Remote-Zugriff über ihre Web-Oberfläche oder über die Befehlszeile konfigurieren.

Informationen zur Erstellung einer Initialisierungsdatei finden Sie in der Dokumentation Ihres BOOTP-Servers.

DHCP. Sie können mithilfe eines RFC2131/RFC2132-konformen DHCP-Servers die TCP/IP-Einstellungen für die Rack PDU konfigurieren.

In diesem Abschnitt sind die wesentlichen Schritte bei der Kommunikation der Rack PDU mit einem DHCP-Server zusammengefasst. Ausführlichere Informationen zur Verwendung eines DHCP-Servers zum Konfigurieren einer Rack PDU finden Sie unter Optionen in DHCP-Antworten.

1. Die Rack PDU sendet eine DHCP-Anfrage die folgende Daten zur Identifizierung enthält:
   - einen Vendor Class Identifier (Herstellerklassenkennung)
   - einen Client Identifier (Client-Kennung, standardmäßig die MAC-Adresse der Rack PDU)
   - einen User Class Identifier (Benutzerklassenkennung, standardmäßig die Kennung der Anwendungsfirmware der Rack PDU)
2. Ein korrekt konfigurierter DHCP-Server antwortet mit einem DHCP-Angebot, das alle Einstellungen beinhaltet, die von der Rack PDU für die Netzwerkkommunikation benötigt werden. Das DHCP-Angebot enthält auch die Option „Vendor Specific Information“ DHCP-Option 43). Die Rack PDU kann so konfiguriert werden, dass sie DHCP-Angebote ignoriert, die in der Option 43 nicht das entsprechende Hersteller-Cookie im nachfolgenden beschriebenen Hexadezimalformat enthalten. (In der Grundeinstellung benötigt die Rack PDU dieses Cookie nicht.)

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

   Hierbei gilt:
   - Das erste Byte (`01`) ist der Code.
   - Das zweite Byte (`04`) ist die Länge.
   - Die übrigen Bytes (`31 41 50 43`) sind das Hersteller-Cookie.

Die Dokumentation zum DHCP-Server enthält Informationen über das Hinzufügen von Code zur Option „Herstellerspezifische Informationen“.

Hinweis: Indem Sie das Kontrollkästchen **Require vendor specific cookie to accept DHCP Address** (Anbieterspezifisches Cookie zum Akzeptieren der DHCP-Adresse erforderlich) auf der Web-Oberfläche markieren, können Sie den DHCP-Server anweisen, ein Hersteller-Cookie bereitzustellen, das Informationen an die Rack PDU übergibt (**Administration > Network>TCP/IP>ipv4 settings**).

Befehlszeile

1. Melden Sie sich an der Befehlszeile an. Siehe Anmelden über die Befehlszeile.
2. Wenden Sie sich an Ihren Netzwerkadministrator, um die IP-Adresse, die Teilnetzmaske und das Standard-Gateway für die Rack PDU zu erhalten.
3. Verwenden Sie zur Konfigurierung der Netzwerkeinstellungen diese drei Befehle. (Kursiver Text steht für eine Variable.)
   a. `tcpip -i` *`IhreIPaddresse`*
   b. `tcpip -s` *`IhreTeilnetzMaske`*
   c. `tcpip -g` *`IhrStandard-Gateway`*

   Geben Sie für jede Variable einen numerischen Wert im Format *`xxx.xxx.xxx.xxx`* ein.

   Wenn Sie beispielsweise die System-IP-Adresse 156.205.14.141 einstellen möchten, geben Sie den folgenden Befehl ein und betätigen Sie anschließend die EINGABETASTE:

   `tcpip -i 156.205.14.141`
4. Geben Sie **`exit`** ein. Die Rack PDU wird neu gestartet, um die Änderungen zu übernehmen.

Zugriff nach Verlust des Passworts

Der Zugriff auf die Befehlszeile der Rack PDU kann über einen lokalen Computer oder ein anderes Gerät erfolgen, das über die serielle Schnittstelle mit der Rack PDU verbunden ist.

1. Wählen Sie einen seriellen Anschluss auf dem lokalen Computer aus und deaktivieren Sie sämtliche Dienste, die diesen Anschluss verwenden.
2. Verbinden Sie das mitgelieferte serielle Kabel mit dem betreffenden Anschluss am Computer und mit dem seriellen Anschluss der Rack PDU.
3. Führen Sie ein Terminalprogramm (beispielsweise HyperTerminal®) aus und konfigurieren Sie den ausgewählten Anschluss mit 9600 bps, 8 Datenbits, ohne Paritätsbit, 1 Stoppbit und ohne Datenflusskontrolle.
4. Drücken Sie die EINGABETASTE ggf. zweimal, um die Eingabeaufforderung **User Name** aufzurufen. Wird die Eingabeaufforderung **User Name** nicht angezeigt, überprüfen Sie Folgendes:
   - Der serielle Anschluss wird von keiner anderen Anwendung verwendet.
   - Die Terminaleinstellungen sind richtig eingestellt (siehe Schritt 3).
   - Das richtige Kabel wird, wie in Schritt 2 angegeben, verwendet.
5. Drücken Sie die Taste **Reset**. Die Status-LED blinkt abwechselnd orange und grün. Drücken Sie die **Reset**-Taste sofort ein zweites Mal, während die LED blinkt, um den Benutzernamen und das Passwort temporär auf die Standardeinstellung zurückzusetzen.
6. Drücken Sie die EINGABETASTE so oft wie nötig, bis die Eingabeaufforderung **User Name** erneut angezeigt wird. Geben Sie dann den Standardwert **dell,** als Benutzernamen und als Passwort ein. (Wenn Sie nach erneuter Anzeige der Eingabeaufforderung **User Name** für die Anmeldung länger als 30 Sekunden benötigen, müssen Sie Schritt 5 wiederholen und sich erneut anmelden.)
7. Verwenden Sie in der Befehlszeile folgende Befehle, um die Einstellungen für

Benutzername und **Passwort** zu ändern, die standardmäßig **dell** lauten:

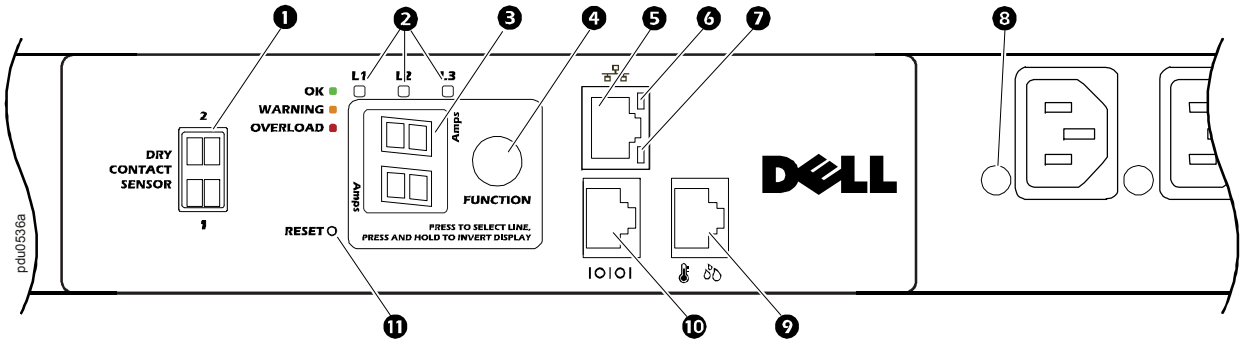
```
user -an IhrAdministratorName
user -ap IhrAdministratorPasswort
```

Wenn Sie beispielsweise den Benutzernamen des Administrators in **Don Adams** umändern möchten, geben Sie Folgendes ein:

```
user -an Don Adams
```

8. Geben Sie `quit` oder `exit` ein, um sich abzumelden, schließen Sie gelöste serielle Kabel wieder an und starten Sie gegebenenfalls deaktivierte Dienste neu.

Frontblende der Rack PDU



Element		Beschreibung
❶	Potentialfreie Eingangskontakte	Anschluss für zwei Einheiten mit potentialfreiem Kontakt.
❷	Phasen-LEDs Hinweis: Bei einphasigen Rack PDUs ist nur eine LED vorhanden.	Wenn keine Alarme vorliegen, meldet die LED-Anzeige einen Phasenstrom, und eine grüne Phasen-LED zeigt die dazugehörige Phase an. Das System durchläuft automatisch die einzelnen Phasen und zeigt jeweils für drei Sekunden die Stromstärke auf der betreffenden Phase an. Wenn für eine Phase ein Alarm vorliegt, schaltet sich die dazugehörige Phasen-LED ein und bleibt so lange eingeschaltet, wie der Alarmzustand vorliegt. Bei einem Alarm der Kategorie „Warnung“ leuchtet die LED orangefarben, bei einem Alarm der Kategorie „Kritisch“ leuchtet die LED rot. Wenn für mehr als eine Phase ein Alarm vorliegt, durchläuft das System automatisch die betroffenen Phasen. Dabei leuchten die dazugehörigen Phasen-LEDs jeweils drei Sekunden lang auf.

Element		Beschreibung
❸	LED-Anzeige	Meldet den zur momentan leuchtenden Phasen-LED gehörenden Phasenstrom.
❹	Funktionstaste	• Durch wiederholtes Drücken der Taste können Sie die Stromstärke auf den einzelnen Phasen manuell anzeigen. Die Stromstärke wird 30 Sekunden lang oder bis zum Loslassen der Taste angezeigt. (Bei einphasigen Rack PDUs ist diese Funktion nicht verfügbar.) • Zum Anzeigen der IP-Adresse halten Sie die Taste mindestens fünf Sekunden lang gedrückt, bis **IP** angezeigt wird; lassen Sie die Taste anschließend wieder los. An der LED-Anzeige erscheinen von der Adresse immer zwei Ziffern gleichzeitig, danach wird der Adressbereich erneut durchlaufen. • Zum Invertieren der Anzeige halten Sie die Taste mindestens 10 Sekunden lang gedrückt, bis die Buchstabenfolge **AA** angezeigt wird. Halten Sie die Taste so lange gedrückt, bis „AA“ in der gewünschten Orientierung angezeigt wird, und lassen Sie die Taste dann wieder los.
❺	10/100 Base-T-Anschluss	Anschluss zum Verbinden der Rack PDU mit dem Netzwerk.
❻	10/100-LED	Siehe 10/100-LED.
❼	Netzwerk-Status-LED	Siehe Netzwerk-Status-LED.
❽	Ausgangsanschlussstatus-LED	Leuchtet grün, wenn der Ausgangsanschluss eingeschaltet ist. (Zu jedem Ausgangsanschluss gibt es eine LED.)
❾	Anschluss für Temperatur-/ Feuchtigkeitssensor	Anschluss für einen Rack PDU-Temperatursensor (G853N) oder einen Rack PDU-Temperatur-/ Feuchtigkeitssensor (H621N).

Element		Beschreibung
⑩	Serieller RJ-45-Anschluss	Anschluss zum Verbinden der Rack PDU mit einem Terminal-Emulatorprogramm für lokalen Zugriff auf die Befehlszeile. Verwenden Sie hierfür das mitgelieferte serielle Kabel.
⑪	Reset-Taste	Drücken Sie die Reset-Taste, um die Schnittstelle der Rack PDU ohne Auswirkungen auf die Ausgangsanschlüsse neu zu starten, und lassen Sie die Taste anschließend wieder los.

Netzwerk-Status-LED

Zustand	Beschreibung
Off	Eine der folgenden Situationen liegt vor: • Die Rack PDU erhält keinen Betriebsstrom. • Die Rack PDU funktioniert nicht richtig und muss repariert oder ersetzt werden.
Grünes Dauerleuchten	Die Rack PDU besitzt gültige TCP/IP-Einstellungen.
Grünes Blinken	Die Rack PDU besitzt keine gültigen TCP/IP-Einstellungen.
Orangefarbenes Dauerleuchten	In der Rack PDU wurde ein Hardwarefehler erkannt.
Orangefarbenes Blinken	Die Rack PDU übermittelt BOOTP-Anfragen.
Grünes und orangefarbenes Blinken (abwechselnd)	Wenn die LED langsam blinkt, sendet die Rack PDU DHCP-Anfragen. Wenn die LED schnell blinkt, wird die Rack PDU gerade gestartet.

1. Wenn Sie keinen BOOTP- oder DHCP-Server verwenden, lesen Sie bitte die Anleitung zum Konfigurieren der TCP/IP-Einstellungen der Rack PDU unter Festlegen der Netzwerkeinstellungen.
2. Bei Verwendung eines DHCP-Servers finden Sie entsprechende Informationen unter TCP/IP und Kommunikationseinstellungen.

10/100-LED

Zustand	Beschreibung
Aus	Mindestens eine der folgenden Situationen liegt vor: • Die Rack PDU erhält keinen Betriebsstrom. • Das zum Anschluss der Rack PDU an das Netzwerk verwendete Kabel wurde abgezogen oder ist defekt. • Das zum Anschluss der Rack PDU an das Netzwerk verwendete Gerät ist ausgeschaltet. • Die Rack PDU selbst funktioniert nicht richtig und muss repariert oder ersetzt werden.
Grünes Dauerleuchten	Die Rack PDU ist mit einem Netzwerk verbunden, das mit einer Geschwindigkeit von 10 Megabit pro Sekunde (MBit/s) arbeitet.
Orangefarbenes Dauerleuchten	Die Rack PDU ist mit einem Netzwerk verbunden, das mit einer Geschwindigkeit von 100 Megabit pro Sekunde (MBit/s) arbeitet.
Grünes Blinken	Die Rack PDU sendet oder empfängt gerade Daten. das mit einer Geschwindigkeit von 10 Megabit pro Sekunde (MBit/s) arbeitet.
Orangefarbenes Blinken	Die Rack PDU sendet oder empfängt gerade Daten. mit einer Geschwindigkeit von 100 MBit/s.

Befehlszeile

Wissenswertes zur Befehlszeile

Mithilfe der Befehlszeile können Sie sich den Status der Rack PDU anzeigen lassen und diese verwalten. Darüber hinaus bietet die Befehlszeile die Möglichkeit, Skripte für den automatischen Betrieb zu erstellen. Ein Administrator hat uneingeschränkten Zugriff auf die Befehlszeile, die Benutzer „Gerät“ und „Ausgangsanschluss“ haben darauf beschränkten Zugriff, und der Benutzer „schreibgeschützt“ hat darauf überhaupt keinen Zugriff.(Einzelheiten hierzu finden Sie unter Benutzerkontotypen.)

Sie können sämtliche Parameter einer Rack PDU (auch solche, die nicht über die Befehlszeile eingestellt werden können) durch Übertragen einer INI-Datei an die Rack PDU mithilfe der Befehlszeile konfigurieren. Für die Datenübertragung verwendet die Befehlszeile das Protokoll XMODEM. Sie können jedoch die aktuelle INI-Dateien nicht mittels XMODEM auslesen.

Anmelden über die Befehlszeile

Für den Zugriff auf die Befehlszeile können Sie entweder eine lokale (serielle) Verbindung oder eine Remote-Verbindung (über Telnet oder SSH) über einen im selben Netzwerk wie die Rack PDU befindlichen Computer verwenden.

Fernzugriff auf die Befehlszeile

Sie können über Telnet oder SSH auf die Befehlszeile zugreifen. Standardmäßig ist Telnet aktiviert. Wenn SSH aktiviert wird, wird Telnet deaktiviert.

Zum Aktivieren oder Deaktivieren dieser Zugriffsmethoden verwenden Sie die Web-Oberfläche. Wählen Sie auf der Registerkarte **Administration** in der oberen Menüleiste die Option **Network** und wählen Sie dann im linken Navigationsmenü unter **Console** die Option **Access** (Zugriff).

Telnet für einfachen Zugriff. Telnet bietet als einfachen Sicherheitsmechanismus eine Authentifizierung mit Anmeldename und Passwort. Es bietet jedoch nicht die Sicherheit einer verschlüsselten Anmeldung.

So greifen Sie über Telnet auf die Befehlszeile zu:

1. Geben Sie auf einem im gleichen Netzwerk wie die Rack PDU, befindlichen Computer in einer Befehlszeile den Befehl **`telnet`** ein, gefolgt von der IP-Adresse der Rack PDU (Beispiel: **`telnet 139.225.6.133`**, wenn die Rack PDU den Telnet-Standard-Port 23 verwendet), und drücken Sie die EINGABETASTE.
   Wenn die Rack PDU einen Nicht-Standard-Port (zwischen 5000 und 32768) verwendet, müssen Sie je nach Telnet-Client einen Doppelpunkt oder ein Leerzeichen zwischen der IP-Adresse (oder dem DNS-Namen) und der Port-Nummer einfügen. (Diese Befehle funktionieren in den meisten Fällen; manche Clients erlauben es jedoch nicht, den Port als Argument zu übergeben, so dass in solchen Fällen unter Umständen zusätzliche Befehle benötigt werden.)
2. Geben Sie Benutzernamen und Passwort ein (Standardwerte: **admin** und **admin** für einen Administrator bzw. **device** und **device** für den Benutzer „Gerät“).

Sollten Sie Ihren Benutzernamen oder Ihr Passwort vergessen haben, lesen Sie bitte die Anleitung unter Zugriff nach Verlust des Passworts.

SSH für den Zugriff auf hoher Sicherheitsstufe. Wenn Sie für die Web-Oberfläche den hohen Sicherheitsstandard von SSL nutzen möchten, verwenden Sie SSH für den Zugriff auf die Befehlszeile. SSH verschlüsselt Benutzernamen, Passwörter und die übertragenen Daten. Die Schnittstelle, die Benutzerkonten und die Zugriffsrechte des Benutzers sind immer gleich, unabhängig davon, ob der Zugriff auf die Befehlszeile über SSH oder Telnet erfolgt. Um SSH verwenden zu können, müssen Sie SSH jedoch zuerst konfigurieren und einen SSH-Client auf dem Computer installieren.

Lokaler Zugriff auf die Befehlszeile

Sie können über einen lokalen Computer, der über die serielle Schnittstelle der Rack PDU mit dieser verbunden ist, auf die Befehlszeile zugreifen:

1. Wählen Sie eine serielle Schnittstelle auf dem Computer aus, und deaktivieren Sie sämtliche Dienste, die diese Schnittstelle verwenden.
2. Verbinden Sie das mitgelieferte serielle Kabel mit dem betreffenden seriellen Anschluss am Computer und mit dem seriellen Anschluss der Rack PDU.
3. Starten Sie ein Terminalprogramm (z. B. HyperTerminal) und konfigurieren Sie die gewählte Schnittstelle wie folgt: 9600 bps, 8 Datenbits, keine Parität, ein Stoppbit, keine Datenflusskontrolle.
4. Drücken Sie die EINGABETASTE und geben Sie hinter den entsprechenden Eingabeaufforderungen Ihren Benutzernamen und Ihr Passwort ein.

Wissenswertes zur Hauptmaske

Die nachfolgende Abbildung zeigt ein Beispiel für die Hauptmaske, die angezeigt wird, wenn Sie sich über die Befehlszeile bei einer Rack PDU anmelden.

```
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>
```

Informationsfelder in der Hauptmaske:

- Zwei Felder geben die Firmwareversionen des Betriebssystems (AOS) und der Anwendung (APP) an. Der Name der Anwendungsfirmware bezeichnet den Typ des mit dem Netzwerk verbundenen Geräts. Im vorstehenden Beispiel wird die Anwendungsfirmware der Rack PDU angezeigt.

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

  RPDUD vx.x.x
  ```

- Drei Felder identifizieren den Systemnamen, eine Kontaktperson und den Standort der Rack PDU. (In der Steuerkonsole stellen Sie diese Werte über das Menü **System** ein.)

  ```
  Name: Test Lab

  Contact: Don Adams

  Location: Building 3
  ```

- Im Feld **Up Time** können Sie die Betriebszeit der Rack PDU seit dem letzten Anschalten oder Zurücksetzen ablesen.

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

- In zwei Feldern wird das Datum und die Uhrzeit der Anmeldung angegeben.

  ```
  Date: 10/30/2009

  Time: 5:58:30
  ```

- Das Feld **User** (Benutzer) zeigt an, ob Sie sich mit dem Benutzerkonto **Administrator** oder **Device** (Gerät) angemeldet haben. (Ein **Benutzer „schreibgeschützt“** kann auf die Befehlszeile nicht zugreifen.)

  ```
  User : Administrator
  ```

- Im Feld **Stat** wird der Status der Rack PDU angezeigt.

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

P+	Das Dell-Betriebssystem funktioniert einwandfrei.

Nur IPv4	Nur IPv6	IPv4 und IPv6*	Beschreibung
N+	**N+**	**N4+ N6+**	Das Netzwerk funktioniert einwandfrei.
N?	**N6?**	**N4? N6?**	Ein BOOTP-Anfragezyklus ist gerade im Gange.
N–	**N6–**	**N4– N6–**	Die Rack PDU konnte keine Verbindung zum Netzwerk herstellen.
N!	**N6!**	**N4! N6!**	Ein anderes Gerät verwendet die IP-Adresse der Rack PDU.
* Die Werte N4 und N6 können sich voneinander unterscheiden: Denkbar wäre beispielsweise ein Eintrag in der Form N4- N6+.			

A+	Die Anwendung funktioniert einwandfrei.
A–	Die Anwendung hat eine ungültige Prüfsumme.
A?	Die Anwendung wird initialisiert.
A!	Die Anwendung ist zum AOS nicht kompatibel.

Bitte wenden Sie sich an den Kundendienst von Dell Support-Mitarbeiter, sollte der Wert P+ nicht angezeigt werden.

Verwendung der Befehlszeile

Zum Konfigurieren der Rack PDU über die Befehlszeile müssen Sie bestimmte Befehle eingeben. Damit ein Befehl ausgeführt wird, müssen Sie diesen eingeben und die EINGABETASTE drücken. Befehle und Argumente sind in Groß- und Kleinschreibung und in gemischter Form zulässig. Bei Optionen wird zwischen Groß- und Kleinschreibung unterschieden.

Beim Arbeiten mit der Befehlszeile haben Sie auch folgende Möglichkeiten:

- Geben Sie **?** ein und drücken Sie die EINGABETASTE, um eine Liste der für Ihren Kontotyp verfügbaren Befehle angezeigt zu bekommen.
- Informationen zur Funktion und Syntax eines bestimmten Befehls erhalten Sie, wenn Sie den Befehl und dahinter ein Leerzeichen und **?** bzw. das Wort **help** eingeben. Wenn Sie sich beispielsweise die Konfigurationsoptionen für RADIUS ansehen möchten, geben Sie Folgendes ein:

  radius ?

  oder

  radius help

- Wenn Sie die Pfeiltaste NACH OBEN drücken, wird der in der laufenden Sitzung zuletzt eingegebene Befehl angezeigt. Sie können mit den Pfeiltasten NACH OBEN und NACH UNTEN eine Liste mit den letzten 10 Befehlen durchlaufen.
- Geben Sie mindestens den ersten Buchstaben eines Befehls ein und drücken Sie die TABULATORTASTE, um eine Liste der gültigen Befehle zu durchlaufen, die Ihrer Eingabe entsprechen.
- Geben Sie **exit** oder **quit** ein, um die Befehlszeile zu schließen.

Befehlssyntax

Element	Beschreibung
-	Optionen wird ein Bindestrich vorangestellt.
< >	Argumentbeschreibungen erscheinen in Spitzklammern. Beispiel: `-dp <Geräte-Passwort>`
[ ]	Bei Befehlen, die mehrere Optionen gleichzeitig haben können, sowie bei Optionen, die mehrere einander gegenseitig ausschließende Argumente haben können, erscheinen die entsprechenden Werte in eckigen Klammern.
|	Eine vertikale Linie zwischen Elementen, die in eckigen Klammern oder in Spitzklammern erscheinen, bedeutet, dass sich die betreffenden Elemente gegenseitig ausschließen. Sie können immer nur eines dieser Elemente verwenden.

Beispiel für einen Befehl, der mehrere Optionen haben kann:

```
user [-an <Administrator-Name>] [-ap <Administrator-Passwort>]
```

In diesem Beispiel akzeptiert der Befehl user die Option **`-an`**, die den Benutzernamen des Administrators definiert, sowie die Option **`-ap`**, die das Passwort des Administrators definiert. So ändern Sie den Benutzernamen und das Passwort des Administrators in XYZ um:

1. Geben Sie den Befehl „user“, eine Option und als Argument **`XYZ`** ein:
   `user -ap XYZ`
2. Nachdem der erste Befehl verarbeitet wurde, geben Sie den Befehl „user“, die zweite Option und als Argument **`XYZ`** ein:
   `user -an XYZ`

Beispiel für einen Befehl, der zu einer Option mehrere sich gegenseitig ausschließende Argumente akzeptiert:

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

In diesem Beispiel akzeptiert die Option -p nur eines von drei möglichen Argumenten: „all“, „warning“ oder „critical“. Geben Sie beispielsweise Folgendes ein, um sich die Zahl der aktiven kritischen Alarme anzusehen:

`alarmcount -p critical`

Wenn Sie den Befehl mit einem ungültigen Argument eingeben, erscheint eine Fehlermeldung.

Befehlsrückgabe-Codes

Anhand von Befehlsrückgabe-Codes können über Skripts ausgeführte Prozesse Fehlerzustände zuverlässig erkennen, ohne Fehlermeldungstexte auswerten zu müssen:

Die Befehlszeile meldet die Verarbeitung aller Befehle im folgenden Format:

E [0-9][0-9][0-9]: Fehlermeldung

Code	Meldung	Code	Meldung
E000	Success	E105	Befehl vorbelegt
E001	Erfolgreich ausgeführt	E106	Daten nicht verfügbar
E002	Befehl wird erst nach Neustart wirksam	E107	Serielle Kommunikation mit der Rack PDU unterbrochen
E100	Befehl fehlgeschlagen		
E101	Befehl nicht gefunden		
E102	Parameterfehler		
E103	Befehlszeilenfehler		
E104	Wegen fehlender Benutzerrechte zurückgewiesen		

Beschreibung der Befehle der Netzwerkmanagement-Karte

?

Zugriff: Administrator, Benutzer „Gerät“, Benutzer „Ausgangsanschluss“

Beschreibung: Anzeigen sämtlicher Befehle, die mit Ihrem Kontotyp über die Befehlszeile verwendet werden können. Wenn Sie Hilfe zu einem bestimmten Befehl benötigen, geben Sie den Befehl und dahinter ein Fragezeichen ein.

Beispiel: Geben Sie Folgendes ein, um alle für den Befehl **`alarmcount`** zulässigen Optionen angezeigt zu bekommen:

```
alarmcount ?
```

about

Zugriff: Administrator, Benutzer „Gerät“, Benutzer „Ausgangsanschluss“

Beschreibung: Zum Anzeigen von Hardware- und Firmware-Informationen. Diese Informationen sind bei der Fehlersuche nützlich und können verwendet werden, um festzustellen, ob ein Firmware-Update benötigt wird.

alarmcount

Zugriff: Administrator, Benutzer „Gerät“, Benutzer „Ausgangsanschluss“

Beschreibung:

Option	Argumente	Beschreibung
-p	all	Zeigt die Anzahl der von der Rack PDU gemeldeten aktiven Alarme an. Nähere Informationen zu den einzelnen Alarmen finden sich im Ereignisprotokoll.
	warning	Zeigt die Anzahl der aktiven Warnungen an.
	critical	Zeigt die Anzahl der aktiven kritischen Alarme an.

Beispiel: Geben Sie Folgendes ein, um alle aktiven Alarme angezeigt zu bekommen:

```
alarmcount -p warning
```

boot

Zugriff: Nur Administrator

Beschreibung: Hiermit legen Sie fest, wie die Rack PDU ihre Netzwerkeinstellungen (IP-Adresse, Teilnetzmaske, Standard-Gateway) beziehen soll. Konfigurieren Sie anschließend die Einstellungen für den BOOTP- oder DHCP-Server.

Option	Argument	Beschreibung
-b <Startmethode>	dhcp | bootp | manual	Hiermit legen Sie fest, wie die TCP/IP-Einstellungen beim Einschalten, beim Zurücksetzen oder bei einem Neustart der Rack PDU konfiguriert werden sollen. Informationen zu den Einstellungen der verschiedenen Startmethoden finden Sie unter TCP/IP und Kommunikationseinstellungen.
-c	enable | disable	Nur für die Startmethoden `dhcp` und `dhcpBootp`. Hiermit aktivieren oder deaktivieren Sie die Vorschrift, dass der DHCP-Server das Hersteller-Cookie bereitstellen muss.
Die Standardwerte für diese drei Einstellungen müssen normalerweise nicht geändert werden: -v <Vendor Class>: DELL -i <Client ID>: Die MAC-Adresse der Rack PDU, die diese im Netzwerk eindeutig identifiziert. -u <User Class>: Der Name des Moduls der Anwendungs-Firmware		

Beispiel: So verwenden Sie einen DHCP-Server, um die Netzwerkeinstellungen zu beziehen:

1. Geben Sie **`boot -b dhcp`** ein.
2. Aktivieren Sie die Vorschrift, dass der DHCP-Server das Hersteller-Cookie bereitstellen muss.
   `boot -c enable`

cd

Zugriff: Administrator, Benutzer „Gerät“, Benutzer „Ausgangsanschluss“

Beschreibung: Mit diesem Befehl navigieren Sie zu einem Ordner in der Ordnerstruktur der Rack PDU.

Beispiel 1: So wechseln Sie in den Ordner **`ssh`** und bestätigen, dass das SSH-Sicherheitszertifikat an die Rack PDU übertragen wurde:

1. Geben Sie **`cd ssh`** ein und drücken Sie die EINGABETASTE.
2. Geben Sie **`dir`** ein und drücken Sie die EINGABETASTE, um die im SSH-Ordner befindlichen Dateien angezeigt zu bekommen.

Beispiel 2: Geben Sie Folgendes ein, um zum Hauptordner zurückzukehren:

```
cd ..
```

console

Zugriff: Nur Administrator

Beschreibung: Hiermit legen Sie fest, ob Benutzer über das standardmäßig aktiviert Telnet oder über Secure Shell (SSH) auf die Befehlszeile zugreifen können. SSH bietet einen besseren Schutz, da es Benutzernamen, Passwörter und Daten in verschlüsselter Form überträgt. Für zusätzliche Sicherheit können Sie den für Telnet bzw. SSH eingestellten Port ändern. Sie können den Netzwerkzugriff auf die Befehlszeile auch vollständig deaktivieren.

Option	Argument	Beschreibung
-S	disable | telnet | ssh	Konfigurieren Sie den Zugriff auf die Befehlszeile oder verwenden Sie den Befehl „disable“, um den Zugriff völlig zu unterbinden. Wenn SSH aktiviert wird, wird automatisch SCP aktiviert und Telnet deaktiviert.
-pt	<telnet port n>	Hiermit legen Sie den Telnet-Port fest, über den der Datenaustausch mit dem Rack PDU erfolgen soll (Voreinstellung: 23).
-ps	<SSH port n>	Hiermit legen Sie den SSH-Port fest, über den der Datenaustausch mit dem Rack PDU erfolgen soll (Voreinstellung: 22).
-b	2400 | 9600 | 19200 | 38400	Hiermit konfigurieren Sie die Geschwindigkeit des seriellen Datenanschlusses (Voreinstellung: 9600 bps).

Beispiel 1: Geben Sie Folgendes ein, um den Zugriff auf die Befehlszeile über SSH zu aktivieren:

```
console -S ssh
```

Beispiel 2: Geben Sie Folgendes ein, um den Telnet-Port auf 5000 zu ändern:

```
console -pt 5000
```

date

Zugriff: Nur Administrator

Beschreibung: Hiermit konfigurieren Sie das von der Rack PDU verwendete Datum.

Wenn Sie einen NTP-Server konfigurieren möchten, von dem die Rack PDU das Datum und die Uhrzeit beziehen soll, lesen Sie bitte die Anleitung unter Einstellen von Datum und Uhrzeit.

Option	Argument	Beschreibung
-d	<"Datum-szeichenfolge">	Konfigurieren Sie das aktuelle Datum. Verwenden Sie das vom Befehl `date -f` vorgegebene Datumsformat.
-t	<00:00:00>	Hiermit konfigurieren Sie die aktuelle Uhrzeit in Stunden, Minuten und Sekunden. Verwenden Sie dabei das 24-Stunden-Zeitformat.
-f	mm/dd/yy | dd.mm.yyyy | mmm-dd-yy | dd-mmm-yy | yyyy-mm-dd	Wählen Sie das Zahlenformat, in dem alle Datumsangaben über diese Benutzerschnittstelle angezeigt werden sollen. Jeder der Buchstaben m (für Monat), d (für Tag) und y (für Jahr) steht für eine Ziffer. Tage und Monate, die einer einzigen Ziffer entsprechen, werden mit vorangestellter Null angezeigt.
-z	<Zeitzonen-Differenz>	Hiermit geben Sie die Differenz zwischen Ihrer Zeitzone und der Normalzeit GMT ein. Dadurch können Sie eine Synchronisierung mit Personen in anderen Zeitzonen durchführen.

Beispiel 1: Geben Sie Folgendes ein, um das Datum im Format yyyy-mm-dd angezeigt zu bekommen:

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

Beispiel 2: Geben Sie Folgendes ein, um das Datum „30. Oktober 2009“ in dem Format zu definieren, das im vorhergehenden Beispiel konfiguriert wurde:

```
date -d "2009-10-30"
```

Beispiel 3: Geben Sie Folgendes ein, um die Uhrzeit "17:21:03 h" zu definieren:

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

delete

Zugriff: Nur Administrator

Beschreibung: Hiermit löschen Sie eine Datei im Dateisystem.

Argument	Beschreibung
<Dateiname>	Geben Sie den Namen der zu löschenden Datei ein.

dir

Zugriff: Administrator, Benutzer „Gerät“, Benutzer „Ausgangsanschluss“

Beschreibung: Hiermit zeigen Sie eine Liste der auf der Rack PDU gespeicherten Dateien und Ordner an.

dns

Zugriff: Nur Administrator

Beschreibung: Hiermit konfigurieren Sie die DNS-Einstellungen manuell.

Parameter	Argument	Beschreibung
-OM	enable | disable	Hiermit überschreiben Sie die manuell konfigurierten DNS-Einstellungen.
-p	<primärer DNS-Server>	Hiermit legen Sie den primären DNS-Server fest.
-s	<sekundärer DNS-Server>	Hiermit legen Sie den sekundären DNS-Server fest.
-d	<Domänenname>	Hiermit legen Sie den Domänennamen fest.
-n	<Domänenname IPv6>	Hiermit legen Sie den Domänennamen für IPv6 fest.
-h	<Host-Name>	Hiermit legen Sie den Hostnamen fest.

eventlog

Zugriff: Administrator, Benutzer „Gerät“, Benutzer „Ausgangsanschluss“

Beschreibung: Hiermit können Sie sich Datum und Uhrzeit des letzten Abrufs des Ereignisprotokolls, den Status der Rack PDU sowie den Status der an die Rack PDU angeschlossenen Sensoren anzeigen lassen. Außerdem können Sie sich die zuletzt aufgetretenen Geräte-Ereignisse, jeweils mit Datum und Uhrzeit, anzeigen lassen. Mit den folgenden Tasten können Sie innerhalb des Ereignisprotokolls navigieren:

Schlüssel	Beschreibung
ESC	Hiermit schließen Sie das Ereignisprotokoll und kehren zur Befehlszeile zurück.
ENTER	Hiermit aktualisieren Sie die Protokollanzeige. Mit diesem Befehl können Sie sich Ereignisse anzeigen lassen, die nach dem letzten Abrufen und Anzeigen des Protokolls aufgetreten sind.
LEERTASTE	Hiermit zeigen Sie die nächste Seite des Ereignisprotokolls an.
B	Hiermit zeigen Sie die vorherige Seite des Ereignisprotokolls an. Dieser Befehl steht auf der Hauptseite des Ereignisprotokolls nicht zur Verfügung.
D	Hiermit löschen Sie das Ereignisprotokoll. Beantworten Sie die Rückfragen, um den Löschvorgang zu bestätigen oder abzulehnen. Gelöschte Ereignisse können nicht wiederhergestellt werden.

exit

Zugriff: Administrator, Benutzer „Gerät“, Benutzer „Ausgangsanschluss“

Beschreibung: Hiermit schließen Sie die Befehlszeile.

format

Zugriff: Nur Administrator

Beschreibung: Hiermit formatieren Sie das Dateisystem der Rack PDU neu und löschen sämtliche Sicherheitszertifikate, Verschlüsselungsschlüssel, Konfigurationseinstellungen sowie die Ereignis- und Datenprotokolle.

Zum Zurücksetzen der Rack PDU auf ihre Standardkonfiguration verwenden Sie den Befehl **`resetToDef`**.

FTP

Zugriff: Nur Administrator

Beschreibung: Hiermit aktivieren oder deaktivieren Sie den Zugriff auf den FTP-Server. Sie haben auch die Möglichkeit, die Port-Einstellung auf einen beliebigen freien Port zwischen 5001 und 32768 zu ändern, um die Sicherheit zu erhöhen.

Option	Argument	Beschreibung
-p	<Port-Nummer>	Hiermit legen Sie den TCP/IP-Port fest, über den der FTP-Server mit der Rack PDU kommunizieren soll (Voreinstellung: 21). Der FTP-Server verwendet stets den eingestellten Port und den unmittelbar darunter befindlichen Port.
-S	enable | disable	Hiermit konfigurieren Sie den Zugriff auf den FTP-Server.

Beispiel: Geben Sie Folgendes ein, um den TCP/IP-Port auf 5001 zu ändern:

```
ftp -p 5001
```

help

Zugriff: Administrator, Benutzer „Gerät“, Benutzer „Ausgangsanschluss“

Beschreibung: Anzeigen sämtlicher Befehle, die mit Ihrem Kontotyp über die Befehlszeile verwendet werden können. Wenn Sie Hilfe zu einem bestimmten Befehl benötigen, geben Sie den Befehl und dahinter das Wort **`help`** ein.

Beispiel 1: Geben Sie Folgendes ein, um sämtliche Befehle angezeigt zu bekommen, die einem Benutzer „Gerät“ zur Verfügung stehen.

```
help
```

Beispiel 2: Geben Sie Folgendes ein, um alle für den Befehl **`alarmcount`** zulässigen Optionen angezeigt zu bekommen:

```
alarmcount help
```

netstat

Zugriff: Administrator, Benutzer „Gerät“, Benutzer „Ausgangsanschluss“

Beschreibung: Hiermit bekommen Sie den Status des Netzwerks und aller aktiven IPv4- und IPv6-Adressen angezeigt.

ntp

Zugriff: Administrator

Beschreibung: Hiermit können Sie sich die NTP-Parameter anzeigen lassen und konfigurieren.

Option	Argument	Beschreibung
-OM	enable | disable	Hiermit überschreiben Sie die manuell konfigurierten Einstellungen.
-p	<Primärer NTP-Server>	Hiermit legen Sie den primären Server fest.
-s	<Sekundärer NTP-Server>	Hiermit legen Sie den sekundären Server fest.

Beispiel 1: Geben Sie Folgendes ein, um die manuell konfigurierte Einstellung überschreiben zu können:

```
ntp -OM enable
```

Beispiel 2: Geben Sie Folgendes ein, um den primären NTP-Server festzulegen:

```
ntp -p 150.250.6.10
```

ping

Zugriff: Administrator, Benutzer „Gerät“

Beschreibung. Hiermit können Sie feststellen, ob die Einheit mit der angegebenen IP-Adresse oder dem angegebenen DNS-Namen mit dem Netzwerk verbunden ist. Dabei werden vier Anfragen an die betreffende Adresse gesendet.

Argument	Beschreibung
<IP-Adresse oder DNS-Name>	Geben Sie eine IP-Adresse im Format *xxx.xxx.xxx.xxx* oder den vom DNS-Server konfigurierten DNS-Namen ein.

Beispiel: Geben Sie Folgendes ein, um festzustellen, ob eine Einheit mit der IP-Adresse 150.250.6.10 mit dem Netzwerk verbunden ist:

```
ping 150.250.6.10
```

portSpeed

Zugriff: Administrator

Beschreibung:

Option	Argumente	Beschreibung
-s	auto | 10H | 10F | 100H | 100F	Hiermit konfigurieren Sie die Übertragungsgeschwindigkeit des Ethernet-Anschlusses. Mit dem Befehl `auto` wird es den Ethernet-Geräten ermöglicht, die höchstmögliche Geschwindigkeit für die Datenübertragung auszuhandeln. Weitere Informationen zu den Einstellungen für die Anschlussgeschwindigkeit finden Sie unter Port Speed.

Beispiel: Geben Sie Folgendes ein, um den TCP/IP-Port auf eine Übertragungsgeschwindigkeit von 100 MBit/s im Halb-Duplex-Betrieb (d. h. Datenübertragung immer nur ein eine Richtung) einzustellen:

```
portspeed -s 100H
```

prompt

Zugriff: Administrator, Benutzer „Gerät“

Beschreibung: Hiermit legen Sie fest, ob der Kontotyp des momentan angemeldeten Benutzers in der Befehlszeile angezeigt werden soll oder nicht. Diese Einstellung kann von jedem Benutzer geändert werden; alle Benutzerkonten werden an die neue Einstellung angeglichen.

Option	Argument	Beschreibung
-s	long	Die Befehlszeile enthält den Kontotyp des momentan angemeldeten Benutzers.
	short	Die Standardeinstellung. Die Eingabeaufforderung hat eine Länge von vier Zeichen: `cli>`

Beispiel: Geben Sie Folgendes ein, wenn der Kontotyp des momentan angemeldeten Benutzers in der Befehlszeile angezeigt werden soll:

```
prompt -s long
```

quit

Zugriff: Administrator, Benutzer „Gerät“, Benutzer „Ausgangsanschluss“

Beschreibung: Hiermit schließen Sie die Befehlszeile (funktionsgleich mit dem Befehl „exit“).

radius

Zugriff: Nur Administrator

Beschreibung: Hiermit können Sie sich die aktuellen RADIUS-Einstellungen anzeigen lassen, die RADIUS-Authentifizierung aktivieren oder deaktivieren und grundlegende Authentifizierungsparameter für bis zu zwei RADIUS-Server konfigurieren.

Eine Übersicht über die RADIUS-Server-Konfiguration sowie eine Liste der unterstützten RADIUS-Server finden Sie unter Konfigurieren des RADIUS-Servers.

Auf der Web-Oberfläche der Rack PDU stehen zusätzliche Authentifizierungsparameter für RADIUS-Server zur Verfügung. Weitere Informationen finden Sie unter RADIUS.

Ausführliche Informationen zum Konfigurieren des von Ihnen verwendeten RADIUS-Servers finden Sie in Anhang B: Sicherheitshandbuch.

Option	Argument	Beschreibung
-a	local | radiusLocal | radius	Konfigurieren der RADIUS-Authentifizierung: **`local`** – RADIUS ist deaktiviert. Lokale Authentifizierung ist aktiviert. **`radiusLocal`** – Zuerst lokale Authentifizierung, dann RADIUS-Authentifizierung. RADIUS-Authentifizierung und lokale Authentifizierung sind aktiviert. Die Authentifizierung wird zuerst beim RADIUS-Server angefordert. Wenn der RADIUS-Server nicht reagiert, wird die lokale Authentifizierung verwendet. **`radius`** – RADIUS ist aktiviert. Lokale Authentifizierung ist deaktiviert.

Option	Argument	Beschreibung
-p1 -p2	<Server IP>	Der Servername oder die IP-Adresse des primären oder sekundären RADIUS-Servers. **HINWEIS:** RADIUS-Server verwenden normalerweise Port 1812, um Benutzer zu authentifizieren. Wenn Sie einen anderen Port verwenden möchten, hängen Sie an den Namen des RADIUS-Servers oder an dessen IP-Adresse einen Doppelpunkt an, gefolgt von der neuen Port-Nummer.
-s1 -s2	<server secret>	Der vom primären oder sekundären RADIUS-Server und der Rack PDU verwendete geheime Schlüssel.
-t1 -t2	<Server-Timeout>	Die Zeit in Sekunden, die die Rack PDU auf eine Antwort vom primären oder sekundären RADIUS-Server wartet.

Beispiel 1:

Geben Sie **`radius`** ein und drücken Sie die EINGABETASTE, um die aktuellen RADIUS-Einstellungen für die Rack PDU angezeigt zu bekommen.

Beispiel 2: So aktivieren Sie die RADIUS-Authentifizierung und die lokale Authentifizierung.

```
radius -a radiusLocal
```

Beispiel 3: Geben Sie Folgendes ein, um einen Timeout von 10 Sekunden für einen sekundären RADIUS-Server zu konfigurieren:

```
radius -t2 10
```

reboot

Zugriff: Nur Administrator

Beschreibung: Hiermit starten Sie die Schnittstelle der Rack PDU neu.

resetToDef

Zugriff: Nur Administrator

Beschreibung:

Option	Argumente	Beschreibung
-p	all | keepip	Hiermit setzen Sie alle Konfigurationsänderungen zurück, auch Ereignisvorgänge, Geräteeinstellungen und gegebenenfalls TCP/IP-Konfigurationseinstellungen.

Beispiel: Geben Sie Folgendes ein, um alle an der Rack PDU vorgenommenen Konfigurationsänderungen außer den TCP/IP-Einstellungen zurückzusetzen:

```
resetToDef -p keepip
```

snmp, snmpv3

Zugriff: Nur Administrator

Beschreibung: Hiermit aktivieren oder deaktivieren Sie SNMP 1 oder SNMP 3.

Option	Argumente	Beschreibung
-S	enable | disable	Hiermit aktivieren Sie die betreffende SNMP-Version (1 oder 3) oder zeigen diese an.

Beispiel: Geben Sie Folgendes ein, um die SNMP-Version 1 zu aktivieren:

```
snmp -S enable
```

system

Zugriff: Nur Administrator

Beschreibung: Hiermit können Sie den Systemnamen, den Ansprechpartner und den Standort anzeigen und einstellen sowie das Datum und die Uhrzeit, den angemeldeten Benutzer und den höchstrangigen Systemstatus (P, N oder A) anzeigen - siehe Wissenswertes zur Hauptmaske.

Option	Argument	Beschreibung
-n	<Systemname>	Hiermit legen Sie den Gerätenamen, den Namen der für das Gerät verantwortlichen Person und den physischen Standort des Geräts fest. **HINWEIS:** Wenn Sie einen aus mehreren Wörtern bestehenden Wert eingeben, müssen Sie Ihre Eingabe in doppelte Anführungszeichen setzen.
-c	<Systemkontakt>	
-l	<Systemposition>	

Beispiel 1: Geben Sie Folgendes ein, um den Gerätestandort **`Labor für Prüfzwecke`** zu konfigurieren:

```
system -l "Labor für Prüfzwecke"
```

Beispiel 2: Geben Sie Folgendes ein, um den Systemnamen **`Don Adams`** festzulegen:

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

tcpip

Zugriff: Nur Administrator

Beschreibung: Hiermit konfigurieren Sie folgende Netzwerkeinstellungen für die Rack PDU manuell und zeigen diese an:

Option	Argument	Beschreibung
-i	<IP-Adresse>	Geben Sie die IP-Adresse der Rack PDU im Format *xxx.xxx.xxx.xxx* ein.
-s	<Teilnetzmaske>	Geben Sie die Teilnetzmaske für die Rack PDU ein.
-g	<Gateway>	Geben Sie die IP-Adresse des Standard-Gateways ein. **Verwenden Sie nicht** die Loopback-Adresse (127.0.0.1) als Standard-Gateway.
-d	<Domänenname>	Geben Sie den vom DNS-Server konfigurierten DNS-Namen ein.
-h	<Host-Name>	Geben Sie den Host-Namen ein, den die Rack PDU verwenden soll.

Beispiel 1: Geben Sie **`tcpip`** ein und drücken Sie die EINGABETASTE, um die Netzwerkeinstellungen der Rack PDU angezeigt zu bekommen.

Beispiel 2: Geben Sie Folgendes ein, um die IP-Adresse **`150.250.6.10`** für die Rack PDU manuell zu konfigurieren:

```
tcpip -i 150.250.6.10
```

tcpip6

Zugriff: Nur Administrator

Beschreibung: Hiermit aktivieren Sie IPv6, konfigurieren folgende Netzwerkeinstellungen für die Rack PDU manuell und zeigen diese an:

Option	Argument	Beschreibung
-S	enable | disable	IPv6 aktivieren oder deaktivieren.
-man	enable | disable	Hiermit aktivieren Sie die manuelle Adressierung für die IPv6-Adresse der Rack PDU.
-auto	enable | disable	Hiermit aktivieren Sie die automatische Konfiguration der IPv6-Adresse durch die Rack PDU.
-i	<IPv6-Adresse>	Hiermit legen Sie die IPv6-Adresse der Rack PDU fest.
-g	<IPv6-Gateway>	Hiermit stellen Sie die IPv6-Adresse des Standardgateways ein.
-d6	router | stateful | stateless | never	Hiermit stellen Sie die DHCPv6-Betriebsart über die Parameter „router“, „statefull“ (der Status der Adresse und anderer Daten wird jeweils beibehalten), „stateless“ (mit Ausnahme der Adresse wird der Status nicht beibehalten) und „never“ (nie) ein.

Beispiel 1: Geben Sie **`tcpip6 tcpip`** ein und drücken Sie die EINGABETASTE, um die Netzwerkeinstellungen der Rack PDU angezeigt zu bekommen.

Beispiel 2: Geben Sie Folgendes ein, um die IPv6-Adresse **`2001:0:0:0:0:FFD3:0:57ab`** für die Rack PDU manuell zu konfigurieren:

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

user

Zugriff: Nur Administrator

Beschreibung: Hiermit konfigurieren Sie den Benutzernamen, das Passwort und die Wartezeit bis zur automatischen Abmeldung bei Inaktivität für die Kontotypen „Administrator“, „Gerät“ und „schreibgeschützt“.

Informationen zu den Berechtigungen, die Sie den einzelnen Kontotypen erteilen können, finden Sie unter Benutzerkontotypen.

Option	Argument	Beschreibung
-an -dn -rn	<Name des Administrators> <Name des Geräts> <Name des Benutzers mit Lesezugriff>	Hiermit legen Sie den Benutzernamen für die einzelnen Kontotypen fest. Dabei wird zwischen Groß- und Kleinschreibung unterschieden. Die Höchstlänge beträgt 10 Zeichen.
-ap -dp -rp	<Administrator-Passwort> <Geräte-Passwort> <Passwort für Lesezugriff>	Hiermit legen Sie das Passwort für die einzelnen Kontotypen fest. Dabei wird zwischen Groß- und Kleinschreibung unterschieden. Die Höchstlänge beträgt 32 Zeichen. Leere Passwörter (Passwörter, die keine Zeichen enthalten), sind nicht zulässig.
-t	<Minuten>	Hiermit konfigurieren Sie die Zeit (in der Voreinstellung drei Minuten), die das System abwartet, bevor es einen inaktiven Benutzer automatisch abmeldet.

Beispiel 1: Geben Sie Folgendes ein, um den Benutzernamen des Administrators in XYZ umzuändern:

```
user -an XYZ
```

Beispiel 2: Geben Sie Folgendes ein, um die Wartezeit bis zur automatischen Abmeldung in 10 Minuten umzuändern:

```
user -t 10
```

web

Zugriff: Nur Administrator

Beschreibung: Hiermit aktivieren Sie den Zugriff auf die Web-Oberfläche über HTTP oder HTTPS.

Sie können die Sicherheit weiter erhöhen, indem Sie den HTTP- und HTTPS-Port auf eine freien Port-Nummer zwischen 5000 und 32768 umändern. Der Benutzer muss dann die eingestellte Port-Nummer im Adressfeld des Browsers mit einem Doppelpunkt (:) zur Adresse hinzufügen. Für die IP-Adresse 152.214.12.114 und die Port-Nummer 5000 lautet die Eingabe beispielsweise wie folgt:

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

Option	Argument	Beschreibung
-S	disable | http | https	Hiermit konfigurieren Sie den Zugriff auf die Web-Oberfläche. Wenn HTTPS aktiviert ist, werden die Daten während der Übertragung verschlüsselt und über ein digitales Zertifikat authentifiziert.
-ph	<HTTP-Port-Nr.>	Hiermit legen Sie den TCP/IP-Port fest, über den der HTTP-Datenaustausch mit der Rack PDU erfolgen soll (Voreinstellung: 80).
-ps	<HTTPS-Port-Nr.>	Hiermit legen Sie den TCP/IP-Port fest, über den der HTTPS-Datenaustausch mit der Rack PDU erfolgen soll (Voreinstellung: 443).

Beispiel: Geben Sie Folgendes ein, um jeglichen Zugriff auf die Web-Oberfläche zu verhindern:

```
web -S disable
```

xferINI

Zugriff: Nur Administrator

Beschreibung: Über das Protokoll XMODEM können Sie mittels der Befehlszeile eine INI-Datei über die serielle Schnittstelle an die Rack PDU übertragen. Nach erfolgter Übertragung ist Folgendes zu beachten:

- Wenn es Veränderungen am System oder am Netzwerk gegeben hat, wird die Befehlszeile neu gestartet, und Sie müssen sich neu anmelden.
- Wenn Sie eine von der Einstellung für die Rack PDU abweichende Baud-Rate für die Dateiübertragung gewählt haben, müssen Sie die Baud-Rate wieder auf die Standardeinstellungen setzen, um die Verbindung zur Rack PDU wieder herzustellen.

xferStatus

Zugriff: Nur Administrator

Beschreibung: Hiermit zeigen Sie die Ergebnisse der letzten Dateiübertragung an.

Eine Beschreibung der Codes für die Übertragungsergebnisse finden Sie unter Überprüfen von Upgrades und Aktualisierungen.

Beschreibung der Gerätebefehle

devLowLoad

Zugriff: Administrator, Benutzer „Gerät“

Beschreibung: Hiermit legen Sie den unteren Lastgrenzwert des Geräts in Kilowatt fest oder lassen sich diesen anzeigen.

Beispiel 1: Geben Sie Folgendes ein, um den unteren Lastgrenzwert angezeigt zu bekommen:

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

Beispiel 2: Geben Sie Folgendes ein, um den unteren Lastgrenzwert auf 1 kW einzustellen:

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

devNearOver

Zugriff: Administrator, Benutzer „Gerät“

Beschreibung: Hiermit legen Sie den Grenzwert für drohende Überlastung des Geräts in Kilowatt fest oder lassen sich diesen anzeigen.

Beispiel 1: Geben Sie Folgendes ein, um den Grenzwert für drohende Überlastung angezeigt zu bekommen:

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

Beispiel 2: Geben Sie Folgendes ein, um den Grenzwert für drohende Überlastung auf 21,3 kW einzustellen:

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

devOverLoad

Zugriff: Administrator, Benutzer „Gerät“

Beschreibung: Hiermit legen Sie den Überlastungsgrenzwert des Geräts in Kilowatt fest oder lassen sich diesen anzeigen.

Beispiel 1: Geben Sie Folgendes ein, um den Überlastungsgrenzwert angezeigt zu bekommen:

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

Beispiel 2: Geben Sie Folgendes ein, um den Überlastungsgrenzwert auf 25,5 kW einzustellen:

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

devReading

Zugriff: Administrator, Benutzer „Gerät“

Beschreibung: Hiermit können Sie sich die Gesamtleistung des Geräts in Kilowatt oder den Gesamtstromverbrauch des Geräts in Kilowattstunden anzeigen lassen.

Argument	Beschreibung
power	Hiermit bekommen Sie die Gesamtleistung in Kilowatt angezeigt.
energy	Hiermit bekommen Sie den Gesamtstromverbrauch in Kilowatt angezeigt.

Beispiel 1: Geben Sie Folgendes ein, um die Gesamtleistung angezeigt zu bekommen:

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

Beispiel 2: Geben Sie Folgendes ein, um den Gesamtstromverbrauch angezeigt zu bekommen:

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

devStartDly

Zugriff: Administrator, Benutzer „Gerät“

Beschreibung: Dieser Befehl dient zum Einstellen oder Anzeigen der Wartezeit (in Sekunden), die zur Einschaltverzögerung der einzelnen Ausgangsanschlüsse hinzu addiert werden soll, nachdem die Rack PDU mit Strom versorgt wurde. Zulässiger Wertebereich: 1 bis 300 Sekunden oder „never“ (nie einschalten).

Beispiel 1: Geben Sie Folgendes ein, um die Kaltstartverzögerung angezeigt zu bekommen:

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

Beispiel 2: Geben Sie Folgendes ein, um die Kaltstartverzögerung auf sechs Sekunden einzustellen:

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

humLow

Zugriff: Administrator, Benutzer „Gerät“

Beschreibung: Hiermit legen Sie den unteren Grenzwert für die Feuchtigkeit als Prozentsatz der relativen Feuchtigkeit fest oder lassen sich diesen Wert anzeigen.

Beispiel 1: Geben Sie Folgendes ein, um den unteren Grenzwert für die Feuchtigkeit angezeigt zu bekommen:

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

Beispiel 2: Geben Sie Folgendes ein, um den unteren Grenzwert für die Feuchtigkeit festzulegen:

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

humMin

Zugriff: Administrator, Benutzer „Gerät“

Beschreibung: Hiermit legen Sie den Minimalwert für die Feuchtigkeit als Prozentsatz der relativen Feuchtigkeit fest oder lassen sich diesen Wert anzeigen.

Beispiel 1: Geben Sie Folgendes ein, um den Minimalwert für die Feuchtigkeit angezeigt zu bekommen:

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

Beispiel 2: Geben Sie Folgendes ein, um den Minimalwert für die Feuchtigkeit festzulegen:

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

humReading

Zugriff: Administrator, Benutzer „Gerät“, Benutzer „Ausgangsanschluss“

Beschreibung: Hiermit lassen Sie sich den vom Sensor gemeldeten Feuchtigkeitswert anzeigen.

Beispiel: Geben Sie Folgendes ein, um den Feuchtigkeitswert angezeigt zu bekommen:

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

inNormal

Zugriff: Administrator, Benutzer „Gerät“

Beschreibung: Hiermit lassen Sie sich den Normalzustand der einzelnen potentialfreien Eingangskontakte anzeigen.

Beispiel: Geben Sie Folgendes ein, um den Normalzustand der einzelnen potentialfreien Eingangskontakte angezeigt zu bekommen:

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

inReading

Zugriff: Administrator, Benutzer „Gerät“

Beschreibung: Hiermit lassen Sie sich den aktuellen Zustand der einzelnen potentialfreien Eingangskontakte anzeigen.

Beispiel: Geben Sie Folgendes ein, um den aktuellen Zustand der einzelnen potentialfreien Eingangskontakte angezeigt zu bekommen:

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

olAssignUsr

Zugriff: Administrator

Beschreibung: Hiermit weisen Sie die Steuerung der Ausgangsanschlüsse einem in der lokalen Datenbank enthaltenen Benutzer zu.

Argument	Beschreibung
all	Alle Ausgangsanschlüsse des Geräts.
<outlet name>	Der für einen bestimmten Ausgangsanschluss konfigurierte Name. (Siehe olName.)
<outlet#>	Eine einzelne Zahl oder ein durch zwei Zahlen und einen Bindestrich definierter Zahlenbereich oder eine Auflistung einzelner Ausgangsanschlussnummern und dazugehöriger Zahlenbereiche mit Kommatrennung der Datenfelder.
<user>	Ein in der lokalen Datenbank enthaltener Benutzer. (Siehe userAdd.)

Beispiel 1: Geben Sie Folgendes ein, um dem Benutzer „Peter“ die Ausgangsanschlüsse 3, 5 bis 7 und 10 zuzuweisen:

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

Beispiel 2: Geben Sie Folgendes ein, um dem Benutzer „Gerd“ alle Ausgangsanschlüsse zuzuweisen:

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

olCancelCmd

Zugriff: Administrator, Benutzer „Gerät“ und Benutzer „Ausgangsanschluss“, jedoch nur für Ausgangsanschlüsse, denen der Benutzer zugewiesen ist.

Beschreibung: Bricht alle noch ausstehenden Befehle für einen Ausgangsanschluss oder eine Ausgangsanschlussgruppe ab.

Argument	Beschreibung
all	Alle Ausgangsanschlüsse des Geräts.
<outlet name>	Der für einen bestimmten Ausgangsanschluss konfigurierte Name. (Siehe olName.)
<outlet#>	Eine einzelne Zahl oder ein durch zwei Zahlen und einen Bindestrich definierter Zahlenbereich oder eine Auflistung einzelner Ausgangsanschlussnummern und dazugehöriger Zahlenbereiche mit Kommatrennung der Datenfelder.

Beispiel: Geben Sie Folgendes ein, um alle Befehle für Ausgangsanschluss 3 abzubrechen:

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

olDlyOff

Zugriff: Administrator, Benutzer „Gerät“ und Benutzer „Ausgangsanschluss“, jedoch nur für Ausgangsanschlüsse, denen der Benutzer zugewiesen ist.

Beschreibung: Dieser Befehl schaltet einen Ausgangsanschluss oder eine Ausgangsanschlussgruppe nach Ablauf der Abschaltverzögerung ab (siehe olOff)..

Argument	Beschreibung
all	Alle Ausgangsanschlüsse des Geräts.
<outlet name>	Der für einen bestimmten Ausgangsanschluss konfigurierte Name. (Siehe olName.)
<outlet#>	Eine einzelne Zahl oder ein durch zwei Zahlen und einen Bindestrich definierter Zahlenbereich oder eine Auflistung einzelner Ausgangsanschlussnummern und dazugehöriger Zahlenbereiche mit Kommatrennung der Datenfelder.

Beispiel 1: Zum Abschalten der Ausgangsanschlüsse 3, 5 bis 7 und 10 geben Sie Folgendes ein:

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

Beispiel 2: Zum Abschalten aller Ausgangsanschlüsse geben Sie Folgendes ein:

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

olDlyOn

Zugriff: Administrator, Benutzer „Gerät“ und Benutzer „Ausgangsanschluss“, jedoch nur für Ausgangsanschlüsse, denen der Benutzer zugewiesen ist.

Beschreibung: Dieser Befehl schaltet einen Ausgangsanschluss oder eine Ausgangsanschlussgruppe nach Ablauf der Einschaltverzögerung ein (siehe olOnDelay).

Argument	Beschreibung
all	Alle Ausgangsanschlüsse des Geräts.
<outlet name>	Der für einen bestimmten Ausgangsanschluss konfigurierte Name. (Siehe olName.)
<outlet#>	Eine einzelne Zahl oder ein durch zwei Zahlen und einen Bindestrich definierter Zahlenbereich oder eine Auflistung einzelner Ausgangsanschlussnummern und dazugehöriger Zahlenbereiche mit Kommatrennung der Datenfelder.

Beispiel 1: Zum Einschalten der Ausgangsanschlüsse 3, 5 bis 7 und 10 geben Sie Folgendes ein:

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

Beispiel 2: Zum Einschalten eines Ausgangsanschlusses mit dem konfigurierten Namen „Ausgang1“ geben Sie Folgendes ein:

```
cli> olDlyOn Ausgang1
E000: Success
```

olDlyReboot

Zugriff: Administrator, Benutzer „Gerät“ und Benutzer „Ausgangsanschluss“, jedoch nur für Ausgangsanschlüsse, denen der Benutzer zugewiesen ist.

Beschreibung: Dieser Befehl startet Ausgangsanschlüsse oder Ausgangsanschlussgruppen neu. Die angegebenen Ausgangsanschlüsse werden auf Grundlage der konfigurierten Abschaltverzögerung abgeschaltet (siehe olOffDelay). Nach Ablauf der längsten Neustartdauer (siehe olRbootTime) der ausgewählten Ausgangsanschlüsse schalten sich die Ausgangsanschlüsse nach und nach auf Grundlage der jeweils konfigurierten Einschaltverzögerung ein (siehe olOnDelay).

Argument	Beschreibung
all	Alle Ausgangsanschlüsse des Geräts.
<outlet name>	Der für einen bestimmten Ausgangsanschluss konfigurierte Name. (Siehe olName.)
<outlet#>	Eine einzelne Zahl oder ein durch zwei Zahlen und einen Bindestrich definierter Zahlenbereich oder eine Auflistung einzelner Ausgangsanschlussnummern und dazugehöriger Zahlenbereiche mit Kommatrennung der Datenfelder.

Beispiel 1: Zum Neustarten der Ausgangsanschlüsse 3, 5 bis 7 und 10 geben Sie Folgendes ein:

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

Beispiel 2: Zum Neustarten eines Ausgangsanschlusses mit dem konfigurierten Namen „Ausgang1“ geben Sie Folgendes ein:

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

olGroups

Zugriff: Administrator, Benutzer „Gerät“ und Benutzer „Ausgangsanschluss“

Beschreibung: Mit diesem Befehl werden die auf der Rack PDU definierten Stromeingangs-Synchronisationsgruppen aufgelistet. (Weitere Informationen finden Sie unter Konfigurieren und Steuern der Ausgangsanschlussgruppen.)

Beispiel: Geben Sie Folgendes ein, um die Synchronisationsgruppen aufzulisten:

```
cli> olGroups
E000: Success
Outlet Group A:
159.215.6.141 -> Outlets: 2,4,5
159.215.6.143 -> Outlets: 2,8
Outlet Group B:
159.215.6.141 -> Outlets: 1
159.215.6.166 -> Outlets: 1
```

olLowLoad

Zugriff: Administrator, Benutzer „Gerät“ und Benutzer „Ausgangsanschluss“, jedoch nur für Ausgangsanschlüsse, denen der Benutzer zugewiesen ist.

Beschreibung: Mit diesem Befehl legen Sie die unteren, eine Warnmeldung auslösenden Lastgrenzwerte bestimmter Ausgangsanschlüsse fest oder lassen sich diese anzeigen.

Argument	Beschreibung
all	Alle Ausgangsanschlüsse des Geräts.
<outlet name>	Der für einen bestimmten Ausgangsanschluss konfigurierte Name. (Siehe olName.)
<outlet#>	Eine einzelne Zahl oder ein durch zwei Zahlen und einen Bindestrich definierter Zahlenbereich oder eine Auflistung einzelner Ausgangsanschlussnummern und dazugehöriger Zahlenbereiche mit Kommatrennung der Datenfelder.
<power>	Der neue Grenzwert für den Ausgangsanschluss in Watt.

Beispiel 1: Geben Sie Folgendes ein, um den unteren Lastgrenzwert für alle Ausgangsanschlüsse auf 2 Watt einzustellen:

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

Beispiel 2: Geben Sie Folgendes ein, um den unteren Lastgrenzwert der Ausgangsanschlüsse 3 sowie 5 bis 7 angezeigt zu bekommen:

```
cli> olLowLoad 3,5-7
E000: Success
3: PetersServer: 2 W
5: GerdsServer: 2 W
6: BiancasServer: 2 W
7: KemalsServer: 2 W
```

olName

Zugriff: Administrator, Benutzer „Gerät“ und Benutzer „Ausgangsanschluss“, jedoch nur für Ausgangsanschlüsse, denen der Benutzer zugewiesen ist.

Beschreibung: Mit diesem Befehl legen Sie den Namen eines Ausgangsanschluss fest oder lassen sich diesen anzeigen.

Argument	Beschreibung
all	Alle Ausgangsanschlüsse des Geräts.
<outlet#>	Eine einzelne Zahl oder ein durch zwei Zahlen und einen Bindestrich definierter Zahlenbereich oder eine Auflistung einzelner Ausgangsanschlussnummern und dazugehöriger Zahlenbereiche mit Kommatrennung der Datenfelder.
<newname>	Der Name für einen bestimmten Ausgangsanschluss. Es sind nur Buchstaben und Zahlen zulässig.

Beispiel: Geben Sie Folgendes ein, um Ausgangsanschluss 3 den Namen „PetersServer“ zuzuweisen:

```
cli> olName 3 PetersServer
E000: Success
3: PetersServer:
5: GerdsServer:
6: BiancasServer:
7: KemalsServer:
```

olNearOver

Zugriff: Administrator, Benutzer „Gerät“ und Benutzer „Ausgangsanschluss“, jedoch nur für Ausgangsanschlüsse, denen der Benutzer zugewiesen ist.

Beschreibung: Mit diesem Befehl legen Sie die eine Warnmeldung auslösenden Grenzwerte bei drohender Überlastung bestimmter Ausgangsanschlüsse fest oder lassen sich diese anzeigen.

Argument	Beschreibung
all	Alle Ausgangsanschlüsse des Geräts.
<outlet name>	Der für einen bestimmten Ausgangsanschluss konfigurierte Name. (Siehe olName.)
<outlet#>	Eine einzelne Zahl oder ein durch zwei Zahlen und einen Bindestrich definierter Zahlenbereich oder eine Auflistung einzelner Ausgangsanschlussnummern und dazugehöriger Zahlenbereiche mit Kommatrennung der Datenfelder.
<power>	Der neue Grenzwert für den Ausgangsanschluss in Watt.

Beispiel 1: Geben Sie Folgendes ein, um den Grenzwert bei drohender Überlastung der Ausgangsanschlüsse 3 sowie 5 bis 7 angezeigt zu bekommen:

```
cli> olNearOver 3,5-7
E000: Success
3: PetersServer: 5 W
5: GerdsServer: 6 W
6: BiancasServer: 5 W
7: KemalsServer: 4 W
```

Beispiel 2: Geben Sie Folgendes ein, um den Grenzwert bei drohender Überlastung der Ausgangsanschlüsse 3 sowie 5 bis 7 auf 6 Watt einzustellen:

```
cli> olNearOver 3,5-7 6
E000: Success
3: PetersServer: 6 W
5: GerdsServer: 6 W
6: BiancasServer: 6 W
7: KemalsServer: 6 W
```

olOff

Zugriff: Administrator, Benutzer „Gerät“ und Benutzer „Ausgangsanschluss“, jedoch nur für Ausgangsanschlüsse, denen der Benutzer zugewiesen ist.

Beschreibung: Mit diesem Befehl schalten Sie einen Ausgangsanschluss oder eine Ausgangsanschlussgruppe ohne Verzögerung aus.

Argument	Beschreibung
all	Alle Ausgangsanschlüsse des Geräts.
<outlet name>	Der für einen bestimmten Ausgangsanschluss konfigurierte Name. (Siehe olName.)
<outlet#>	Eine einzelne Zahl oder ein durch zwei Zahlen und einen Bindestrich definierter Zahlenbereich oder eine Auflistung einzelner Ausgangsanschlussnummern und dazugehöriger Zahlenbereiche mit Kommatrennung der Datenfelder.

Beispiel 1: Zum Abschalten der Ausgangsanschlüsse 3 sowie 5 bis 7 geben Sie Folgendes ein:

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

olOffDelay

Zugriff: Administrator, Benutzer „Gerät“ und Benutzer „Ausgangsanschluss“, jedoch nur für Ausgangsanschlüsse, denen der Benutzer zugewiesen ist.

Beschreibung: Dieser Befehl dient zum Einstellen oder Anzeigen der Verzögerung für den Befehl „Off Delayed“ (siehe olDlyOff) und „Reboot Delayed“ (siehe olDlyReboot).

Argument	Beschreibung
all	Alle Ausgangsanschlüsse des Geräts.
<outlet name>	Der für einen bestimmten Ausgangsanschluss konfigurierte Name. (Siehe olName.)
<outlet#>	Eine einzelne Zahl oder ein durch zwei Zahlen und einen Bindestrich definierter Zahlenbereich oder eine Auflistung einzelner Ausgangsanschlussnummern und dazugehöriger Zahlenbereiche mit Kommatrennung der Datenfelder.
<time>	Die Dauer der Verzögerung. Zulässiger Bereich: 1 bis 7200 Sekunden (2 Stunden).

Beispiel 1: Geben Sie Folgendes ein, um eine Verzögerung von 9 Sekunden vor Abschaltung der Ausgangsanschlüsse 3 sowie 5 bis 7 einzustellen:

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

Beispiel 2: Geben Sie Folgendes ein, um den Befehl „Off Delayed“ für die Ausgangsanschlüsse 3 sowie 5 bis 7 angezeigt zu bekommen:

```
cli> olOffDelay 3,5-7
E000: Success
3: PetersServer: 9 s
5: GerdsServer: 9 s
6: BiancasServer: 9 s
7: KemalsServer: 9 sec
```

olOn

Zugriff: Administrator, Benutzer „Gerät“ und Benutzer „Ausgangsanschluss“, jedoch nur für Ausgangsanschlüsse, denen der Benutzer zugewiesen ist.

Beschreibung: Mit diesem Befehl schalten Sie einen Ausgangsanschluss oder eine Ausgangsanschlussgruppe ohne Verzögerung ein.

Argument	Beschreibung
all	Alle Ausgangsanschlüsse des Geräts.
<outlet name>	Der für einen bestimmten Ausgangsanschluss konfigurierte Name. (Siehe olName.)
<outlet#>	Eine einzelne Zahl oder ein durch zwei Zahlen und einen Bindestrich definierter Zahlenbereich oder eine Auflistung einzelner Ausgangsanschlussnummern und dazugehöriger Zahlenbereiche mit Kommatrennung der Datenfelder.

Beispiel 1: Zum Einschalten der Ausgangsanschlüsse 3 sowie 5 bis 7 geben Sie Folgendes ein:

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

olOnDelay

Zugriff: Administrator, Benutzer „Gerät“ und Benutzer „Ausgangsanschluss“, jedoch nur für Ausgangsanschlüsse, denen der Benutzer zugewiesen ist.

Beschreibung: Dieser Befehl dient zum Einstellen oder Anzeigen der Verzögerung für den Befehl „On Delayed“ (siehe olDlyOn) und „Reboot Delayed“ (siehe olDlyReboot).

Argument	Beschreibung
all	Alle Ausgangsanschlüsse des Geräts.
<outlet name>	Der für einen bestimmten Ausgangsanschluss konfigurierte Name. (Siehe olName.)
<outlet#>	Eine einzelne Zahl oder ein durch zwei Zahlen und einen Bindestrich definierter Zahlenbereich oder eine Auflistung einzelner Ausgangsanschlussnummern und dazugehöriger Zahlenbereiche mit Kommatrennung der Datenfelder.
<time>	Die Dauer der Verzögerung. Zulässiger Bereich: 1 bis 7200 Sekunden (2 Stunden).

Beispiel 1: Geben Sie Folgendes ein, um eine Verzögerung von 6 Sekunden vor Einschaltung der Ausgangsanschlüsse 3 sowie 5 bis 7 einzustellen:

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

Beispiel 2: Geben Sie Folgendes ein, um den Befehl „On Delayed“ für die Ausgangsanschlüsse 3 sowie 5 bis 7 angezeigt zu bekommen:

```
cli> olOnDelay 3,5-7
E000: Success
3: PetersServer: 6 s
5: GerdsServer: 6 s
6: BiancasServer: 6 s
7: KemalsServer: 6 sec
```

olOverLoad

Zugriff: Administrator, Benutzer „Gerät“ und Benutzer „Ausgangsanschluss“, jedoch nur für Ausgangsanschlüsse, denen der Benutzer zugewiesen ist.

Beschreibung: Mit diesem Befehl legen Sie die Warngrenzwerte bei Überlastung bestimmter Ausgangsanschlüsse fest oder lassen sich diese anzeigen.

Argument	Beschreibung
all	Alle Ausgangsanschlüsse des Geräts.
<outlet name>	Der für einen bestimmten Ausgangsanschluss konfigurierte Name. (Siehe olName.)
<outlet#>	Eine einzelne Zahl oder ein durch zwei Zahlen und einen Bindestrich definierter Zahlenbereich oder eine Auflistung einzelner Ausgangsanschlussnummern und dazugehöriger Zahlenbereiche mit Kommatrennung der Datenfelder.
<power>	Der neue Grenzwert für den Ausgangsanschluss in Watt.

Beispiel 1: Geben Sie Folgendes ein, um den Überlastungsgrenzwert der Ausgangsanschlüsse 3 sowie 5 bis 7 angezeigt zu bekommen:

```
cli> olOverLoad 3,5-7
E000: Success
3: PetersServer: 7 W
5: GerdsServer: 8 W
6: BiancasServer: 7 W
7: KemalsServer: 6 W
```

Beispiel 2: Geben Sie Folgendes ein, um den Überlastungsgrenzwert der Ausgangsanschlüsse 3 sowie 5 bis 7 auf 7 Watt einzustellen:

```
cli> olOverLoad 3,5-7 7
E000: Success
3: PetersServer: 7 W
5: GerdsServer: 7 W
6: BiancasServer: 7 W
7: KemalsServer: 7 W
```

olRbootTime

Zugriff: Administrator, Benutzer „Gerät“ und Benutzer „Ausgangsanschluss“, jedoch nur für Ausgangsanschlüsse, denen der Benutzer zugewiesen ist.

Beschreibung: Dieser Befehl dient zum Festlegen oder Anzeigen der Wartezeit bis zum Neustart eines Ausgangsanschluss bei Verwendung des Befehls „Reboot Delayed“ (siehe olDlyReboot).

Beispiel 1: Geben Sie Folgendes ein, um die eingestellte Wartezeit bis zur Einschaltung der Ausgangsanschlüsse 3 sowie 5 bis 7 bei einem Neustart angezeigt zu bekommen:

```
cli> olRbootTime 3,5-7
E000: Success
3: PetersServer: 4 s
5: GerdsServer: 5 s
6: BiancasServer: 7 s
7: KemalsServer: 2 sec
```

Beispiel 2: Geben Sie Folgendes ein, um die Wartezeit bis zur Einschaltung der Ausgangsanschlüsse 3 sowie 5 bis 7 bei einem Neustart einzustellen:

```
cli> olRebootTime 3,5-7 10
E000: Success
3: PetersServer: 10 s
5: GerdsServer: 10 s
6: BiancasServer: 10 s
7: KemalsServer: 10 sec
```

olReading

Zugriff: Administrator, Benutzer „Gerät“ und Benutzer „Ausgangsanschluss“, jedoch nur für Ausgangsanschlüsse, denen der Benutzer zugewiesen ist.

Beschreibung: Mit diesem Befehl lassen Sie sich die Stromstärke, die Leistung oder den Stromverbrauch eines Ausgangsanschlusses oder einer Ausgangsanschlussgruppe anzeigen.

Argument	Beschreibung
all	Alle Ausgangsanschlüsse des Geräts.
<outlet name>	Der für einen bestimmten Ausgangsanschluss konfigurierte Name. (Siehe olName.)
<outlet#>	Eine einzelne Zahl oder ein durch zwei Zahlen und einen Bindestrich definierter Zahlenbereich oder eine Auflistung einzelner Ausgangsanschlussnummern und dazugehöriger Zahlenbereiche mit Kommatrennung der Datenfelder.
current | power | energy	Der neue Grenzwert für den Ausgangsanschluss in Watt.

Beispiel 1: Geben Sie Folgendes ein, um die Stromstärke der Ausgangsanschlüsse 3 sowie 5 bis 7 angezeigt zu bekommen:

```
cli> olReading 3,5-7 current
E000: Success
3: PetersServer: 4 A
5: GerdsServer: 5 A
6: BiancasServer: 7 A
7: KemalsServer: 2 A
```

Beispiel 2: Geben Sie Folgendes ein, um die Leistung von Ausgangsanschluss 3 angezeigt zu bekommen:

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

Beispiel 3: Geben Sie Folgendes ein, um den Stromverbrauch des Ausgangsanschlusses „BiancasServer“ angezeigt zu bekommen:

```
cli> olReading biancasserver energy
E000: Success
6: BiancasServer: 7.3 kWh
```

olReboot

Zugriff: Administrator, Benutzer „Gerät“ und Benutzer „Ausgangsanschluss“, jedoch nur für Ausgangsanschlüsse, denen der Benutzer zugewiesen ist.

Beschreibung: Dieser Befehl dient zum Neustarten von Ausgangsanschlüssen oder Ausgangsanschlussgruppen ohne Verzögerung. Wenn mehr als ein Ausgangsanschluss angegeben wird, werden die betreffenden Ausgangsanschlüsse gleichzeitig neu gestartet.

Argument	Beschreibung
all	Alle Ausgangsanschlüsse des Geräts.
<outlet name>	Der für einen bestimmten Ausgangsanschluss konfigurierte Name. (Siehe olName.)
<outlet#>	Eine einzelne Zahl oder ein durch zwei Zahlen und einen Bindestrich definierter Zahlenbereich oder eine Auflistung einzelner Ausgangsanschlussnummern und dazugehöriger Zahlenbereiche mit Kommatrennung der Datenfelder.

Beispiel: Zum Neustarten der Ausgangsanschlüsse 3 sowie 5 bis 7 geben Sie Folgendes ein:

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

olStatus

Zugriff: Administrator, Benutzer „Gerät“ und Benutzer „Ausgangsanschluss“, jedoch nur für Ausgangsanschlüsse, denen der Benutzer zugewiesen ist.

Beschreibung: Mit diesem Befehl zeigen Sie den Status der angegebenen Ausgangsanschlüsse an.

Argument	Beschreibung
all	Alle Ausgangsanschlüsse des Geräts.
<outlet name>	Der für einen bestimmten Ausgangsanschluss konfigurierte Name. (Siehe olName.)
<outlet#>	Eine einzelne Zahl oder ein durch zwei Zahlen und einen Bindestrich definierter Zahlenbereich oder eine Auflistung einzelner Ausgangsanschlussnummern und dazugehöriger Zahlenbereiche mit Kommatrennung der Datenfelder.

Beispiel: Geben Sie Folgendes ein, um den Status der Ausgangsanschlüsse 3 sowie 5 bis 7 angezeigt zu bekommen:

```
cli> olStatus 3,5-7
E000: Success
3: PetersServer: On
5: GerdsServer: Off
6: BiancasServer: Off
7: KemalsServer: On
```

olUnasgnUsr

Zugriff: Administrator

Beschreibung: Hiermit entziehen Sie einem in der lokalen Datenbank enthaltenen Benutzer die Kontrolle über einen Ausgangsanschluss.

Argument	Beschreibung
all	Alle Ausgangsanschlüsse des Geräts.
<outlet name>	Der für einen bestimmten Ausgangsanschluss konfigurierte Name. (Siehe olName.)
<outlet#>	Eine einzelne Zahl oder ein durch zwei Zahlen und einen Bindestrich definierter Zahlenbereich oder eine Auflistung einzelner Ausgangsanschlussnummern und dazugehöriger Zahlenbereiche mit Kommatrennung der Datenfelder.
<user>	Ein in der lokalen Datenbank enthaltener Benutzer. (Siehe userList.)

Beispiel 1: Geben Sie Folgendes ein, um dem Benutzer „Peter“ die Kontrolle über die Ausgangsanschlüsse 3, 5 bis 7 und 10 zu entziehen:

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

Beispiel 2: Geben Sie Folgendes ein, um dem Benutzer „Gerd“ die Kontrolle über alle Ausgangsanschlüsse zuzuweisen:

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

phLowLoad

Zugriff: Administrator, Benutzer „Gerät“

Beschreibung: Hiermit legen Sie den unteren Lastgrenzwert bestimmter Phasen des Geräts in Kilowatt fest oder lassen sich diesen anzeigen. Wählen Sie eine der folgenden Optionen, um einzelne Phasen festzulegen. Geben Sie Folgendes ein: **`all`**, eine einzelne Phase, einen Phasenbereich oder eine durch Kommata getrennte Aufzählung von Phasen.

Beispiel 1: Geben Sie Folgendes ein, um den unteren Lastgrenzwert für alle Phasen auf 1 kW einzustellen:

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

Beispiel 2: Geben Sie Folgendes ein, um den unteren Lastgrenzwert der Phasen 1 bis 3 angezeigt zu bekommen:

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

phNearOver

Zugriff: Administrator, Benutzer „Gerät“

Beschreibung: Hiermit legen Sie den Grenzwert für drohende Überlastung der Phase in Kilowatt fest oder lassen sich diesen anzeigen. Wählen Sie eine der folgenden Optionen, um einzelne Phasen festzulegen. Geben Sie Folgendes ein: **`all`**, eine einzelne Phase, einen Phasenbereich oder eine durch Kommata getrennte Aufzählung von Phasen.

Beispiel 1: Geben Sie Folgendes ein, um den Grenzwert für drohende Überlastung für alle Phasen auf 10 kW einzustellen:

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

Beispiel 2: Geben Sie Folgendes ein, um den Grenzwert für drohende Überlastung der Phasen 1 bis 3 angezeigt zu bekommen:

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

phOverLoad

Zugriff: Administrator, Benutzer „Gerät“

Beschreibung: Hiermit legen Sie den Überlastungsgrenzwert einer Phase in Kilowatt fest oder lassen sich diesen anzeigen. Wählen Sie eine der folgenden Optionen, um einzelne Phasen festzulegen. Geben Sie Folgendes ein: **`all`**, eine einzelne Phase, einen Phasenbereich oder eine durch Kommata getrennte Aufzählung von Phasen.

Beispiel 1: Geben Sie Folgendes ein, um den Überlastungsgrenzwert für alle Phasen auf 13 kW einzustellen:

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

Beispiel 2: Geben Sie Folgendes ein, um den Überlastungsgrenzwert für die Phasen 1 bis 3 angezeigt zu bekommen:

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

phReading

Zugriff: Administrator, Benutzer „Gerät“

Beschreibung: Hiermit lassen Sie sich die Stromstärke, Spannung oder Leistung einer Phase anzeigen. Hiermit legen Sie den Grenzwert für drohende Überlastung der Phase in Kilowatt fest oder lassen sich diesen anzeigen. Wählen Sie eine der folgenden Optionen, um einzelne Phasen festzulegen. Geben Sie Folgendes ein: **`all`**, eine einzelne Phase, einen Phasenbereich oder eine durch Kommata getrennte Aufzählung von Phasen.

Beispiel 1: Geben Sie Folgendes ein, um die gemessene Stromstärke der Phase 3 angezeigt zu bekommen:

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

Beispiel 2: Geben Sie Folgendes ein, um die Spannung der einzelnen Phasen angezeigt zu bekommen:

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

Beispiel 3: Geben Sie Folgendes ein, um die Leistung von Phase 2 angezeigt zu bekommen:

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

phRestrictn

Zugriff: Administrator

Beschreibung: Dieser Befehl dient zum Einstellen oder Anzeigen der Überlast-Sperrfunktion, die eine Einschaltung von Ausgangsanschlüssen verhindert, deren Überlast-Alarmgrenzwert überschritten wurde. Zulässige Argumente: **`none`**, **`near`** und **`over`**. Wählen Sie eine der folgenden Optionen, um einzelne Phasen festzulegen. Geben Sie Folgendes ein: **`all`**, eine einzelne Phase, einen Phasenbereich oder eine durch Kommata getrennte Aufzählung von Phasen.

Beispiel 1: Geben Sie Folgendes ein, um die Überlastsperre für Phase 3 auf „none“ (keine) einzustellen:

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

Beispiel 2: Geben Sie Folgendes ein, um die Einstellung der Überlastsperre für alle Phasen angezeigt zu bekommen:

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

prodInfo

Zugriff: Administrator, Benutzer „Gerät“, Benutzer „Ausgangsanschluss“

Beschreibung: Hiermit lassen Sie sich Informationen zur Rack PDU anzeigen.

Beispiel:

```
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

Zugriff: Administrator, Benutzer „Gerät“

Beschreibung: Dieser Befehl dient zum Einstellen oder Anzeigen des Namens für den Temperatur-/Feuchtigkeitssensor-Anschluss der Rack PDU.

Beispiel 1: Geben Sie Folgendes ein, um den Namen „Sensor1“ für den Anschluss festzulegen:

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

Beispiel 2: Geben Sie Folgendes ein, um danach den Namen des Sensoranschlusses angezeigt zu bekommen:

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

tempHigh

Zugriff: Administrator, Benutzer „Gerät“

Beschreibung: Hiermit legen Sie den Grenzwert für zu hohe Temperatur in Grad Fahrenheit oder Celsius fest.

Beispiel 1: Geben Sie Folgendes ein, um den Grenzwert für zu hohe Temperatur auf 70º Fahrenheit einzustellen:

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

Beispiel 2: Geben Sie Folgendes ein, um den Grenzwert für zu hohe Temperatur in Grad Celsius angezeigt zu bekommen:

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

Beispiel 3: Geben Sie Folgendes ein, um den Grenzwert für zu hohe Temperatur in Grad Fahrenheit angezeigt zu bekommen:

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

tempMax

Zugriff: Administrator, Benutzer „Gerät“

Beschreibung: Hiermit legen Sie den Grenzwert für die Höchsttemperatur in Grad Fahrenheit oder Celsius fest.

Beispiel 1: Geben Sie Folgendes ein, um den Grenzwert für die Höchsttemperatur auf 80º Fahrenheit einzustellen:

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

Beispiel 2: Geben Sie Folgendes ein, um den Grenzwert für die Höchsttemperatur in Grad Celsius angezeigt zu bekommen:

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

Beispiel 3: Geben Sie Folgendes ein, um den Grenzwert für die Höchsttemperatur in Grad Fahrenheit angezeigt zu bekommen:

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

tempReading

Zugriff: Administrator, Benutzer „Gerät“, Benutzer „Ausgangsanschluss“

Beschreibung: Hiermit lassen Sie sich die vom Sensor gemessene Temperatur in Grad Fahrenheit oder Grad Celsius anzeigen.

Beispiel: Geben Sie Folgendes ein, um die Temperatur in Grad Fahrenheit angezeigt zu bekommen:

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

userAdd

Zugriff: Administrator

Beschreibung: Mit diesem Befehl fügen Sie einen Benutzer „Ausgangsanschluss“ zur lokalen Benutzerdatenbank hinzu.

Beispiel: Geben Sie Folgendes ein, um den Benutzer „Peter“ hinzuzufügen:

```
cli> userAdd Peter
E000: Success
```

userDelete

Zugriff: Administrator

Beschreibung: Mit diesem Befehl entfernen Sie einen Benutzer „Ausgangsanschluss“ aus der lokalen Benutzerdatenbank.

Beispiel: Geben Sie Folgendes ein, um den Benutzer „Peter“ zu entfernen:

```
cli> userDelete Peter
E000: Success
```

userList

Zugriff: Administrator, Benutzer „Gerät“ und Benutzer „Ausgangsanschluss“, jedoch nur für Ausgangsanschlüsse, denen der Benutzer zugewiesen ist.

Beschreibung: Mit diesem Befehl bekommen Sie die Benutzer und die ihnen zugewiesenen Ausgangsanschlüsse angezeigt.

Beispiel 1: Wenn Sie als Administrator angemeldet sind, geben Sie Folgendes ein:

```
cli> userList
E000: Success
Local: admin: 1,2,3,4,5,6,7,8
Local: Peter: 1,3
Local: Gerd: 2,5
Local: Bianca: 4,6
Local: Kemal: 7,8
```

Beispiel 2: Wenn Sie als Benutzer „Gerd“ angemeldet sind, geben Sie Folgendes ein:

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

userPasswd

Zugriff: Administrator.

Beschreibung: Mit diesem Befehl bekommen Sie das Passwort eines Benutzers „Ausgangsanschluss“ angezeigt.

Beispiel: Geben Sie Folgendes ein, um das Passwort von Peter auf „abc123“ einzustellen:

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

whoami

Zugriff: Administrator, Benutzer „Gerät“, Benutzer „Ausgangsanschluss“

Beschreibung: Hiermit lassen Sie sich den Benutzernamen des aktiven Benutzers anzeigen.

Beispiel:

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

Web-Oberfläche

Unterstützte Web-Browser

Für den Zugriff auf die Rack PDU über die Web-Oberfläche können Sie den Microsoft® Internet Explorer® (IE) 7.x oder höher (nur unter Windows®-Betriebssystemen) oder Mozilla® Firefox® 3.0.6 oder höher (unter allen Betriebssystemen) verwenden. Eventuell funktionieren auch andere Browser, diese wurden von uns jedoch nicht umfassend getestet.

Die Rack PDU funktioniert nicht in Verbindung mit einem Proxy-Server. Sie müssen einen der folgenden Schritte durchführen, ehe Sie einen Web-Browser für den Zugriff auf die Web-Oberfläche der Rack PDU verwenden können:

- Die Verwendung eines Proxy-Servers für die Rack PDU im Web-Browser deaktivieren.
- Den Proxy-Server so konfigurieren, dass er nicht als Proxy für die IP-Adresse der Rack PDU dient.

Anmelden bei der Web-Oberfläche

Übersicht

Sie können den DNS-Namen oder die IP-Adresse der Rack PDU als URL-Adresse der Web-Oberfläche verwenden. Melden Sie sich mit Ihrem Benutzernamen und Passwort unter Beachtung der Groß-/Kleinschreibung an. Die Voreinstellung für den Benutzernamen und das Passwort ist je nach Kontotyp verschieden:

- **admin/admin** für einen Administrator
- **device/device** für einen Benutzer „Gerät“
- **readonly/readonly** für einen Benutzer „schreibgeschützt“

Für Benutzer mit dem Kontotyp „Ausgangsanschluss“ sind Benutzername und Passwort nicht voreingestellt. Bei einem Benutzer mit dem Kontotyp „Ausgangsanschluss“ muss ein Administrator den Benutzernamen, das Passwort und weitere Kontoeigenschaften festlegen. Siehe Konfigurieren eines Benutzern „Ausgangsanschluss“.

Wenn Sie als Anmeldeprotokoll HTTPS (SSL/TLS) verwenden, werden Ihre Anmeldedaten mit Informationen in einem Server-Zertifikat verglichen. Wenn das Zertifikat mit dem Security Wizard (Sicherheitsassistenten) erstellt und als gemeinsamer Name eine IP-Adresse im Zertifikat angegeben wurde, können Sie sich nur mit der IP-Adresse bei der Rack PDU anmelden. Wenn im Zertifikat als gemeinsamer Name ein DNS-Name angegeben wurde, müssen Sie den DNS-Namen verwenden, um sich anzumelden.

Informationen über die Webseite, die nach dem Anmelden an der Weboberfläche angezeigt wird, finden Sie unter Wissenswertes zur Registerkarte „Home“.

URL-Adressformate

Geben Sie den DNS-Namen oder die IP-Adresse der Rack PDU in das URL-Adressfeld des Web-Browsers ein und drücken Sie die EINGABETASTE. Wenn Sie im Internet Explorer einen von der Standardeinstellung abweichenden Web-Server-Port festlegen, müssen Sie die URL mit **`http://`** bzw. **`https://`** einleiten.

Typische Fehlermeldungen verschiedener Browser bei der Anmeldung.

Fehlermeldung	Fehlerursache	Browser
„Sie haben keine Berechtigung, diese Seite anzuzeigen“ oder „Ein anderer Benutzer ist bereits angemeldet...“	Ein anderer Benutzer ist bereits angemeldet.	Internet Explorer, Firefox
„Diese Seite kann nicht angezeigt werden.“	Der Web-Zugriff ist deaktiviert oder die URL wurde nicht richtig eingegeben.	Internet Explorer
„Verbindungsaufbau nicht möglich.“		Firefox

Beispiele für das URL-Format.

- Für den DNS-Namen von Web1:
  - **`http://Web1`**, wenn als Zugriffsmethode HTTP verwendet wird.
  - **`https://Web1`**, wenn als Zugriffsmethode HTTPS verwendet wird.
- Für die System-IP-Adresse 139.225.6.133 und den standardmäßigen Port auf dem Web-Server (80):
  - **`http://139.225.6.133`**, wenn als Zugriffsmethode HTTP verwendet wird.
  - **`https://139.225.6.133`**, wenn als Zugriffsmethode HTTPS (HTTP mit SSL) verwendet wird.
- Für die System-IP-Adresse 139.225.6.133 und einen nicht standardmäßigen Port auf dem Web-Server (5000):
  - **`http://139.225.6.133:5000`**, wenn als Zugriffsmethode HTTP verwendet wird.
  - **`https://139.225.6.133:5000`**, wenn als Zugriffsmethode HTTPS (HTTP mit SSL) verwendet wird
- Für die IPv6-Systemadresse 2001:db8:1::2c0:b7ff:fe00:1100 und einen nicht standardmäßigen Port auf dem Web-Server (5000):
  - **`http://[2001:db8:1::2c0:b7ff:fe00:1100]:5000`**, wenn als Zugriffsmethode HTTP verwendet wird

Funktionen der Web-Oberfläche

Bitte lesen Sie die folgenden Informationen, um sich mit den Grundfunktionen der Web-Oberfläche der Rack PDU vertraut zu machen.

Registerkarten

Die folgenden Registerkarten sind verfügbar:

- **Home** (Start): Wird bei der Anmeldung angezeigt. Hier werden die aktiven Alarme, der Laststatus der Rack PDU und die neuesten Rack PDU-Ereignisse angezeigt. Weitere Informationen finden Sie unter Wissenswertes zur Registerkarte „Home“.
- **Device Manager** (Gerätemanager): Auf dieser Registerkarte können Sie sich den Laststatus ansehen, Lastgrenzwerte konfigurieren sowie die gemessenen Spitzenlasten für alle angeschlossenen Geräte, Phasen und Ausgangsanschlüsse je nach Bedarf einsehen und verwalten. Darüber hinaus können Sie hier Ausgangsanschlüsse verwalten und steuern. Weitere Informationen finden Sie unter Wissenswertes zur Registerkarte Device Manager.
- **Environment** (Umgebung): Auf dieser Registerkarte können Sie sich die Daten eines gegebenenfalls an der **Rack PDU** angeschlossenen Temperatur- und Feuchtigkeitssensors ansehen.
- **Logs** (Protokolle): Auf dieser Seite werden Ereignis-, Daten- und Systemprotokolle angezeigt.
- **Administration** (Verwaltung): Zum Konfigurieren der Sicherheitseinstellungen, der Netzwerkverbindung, der Benachrichtigungen sowie allgemeiner Einstellungen.

Symbole für den Gerätestatus

Ein oder mehrere Symbole und entsprechender Begleittext lassen den momentanen Betriebszustand der Rack PDU erkennen:

	**Critical**: Es liegt ein kritischer Alarm vor, der ein sofortiges Eingreifen erfordert.
	**Warnung**: Es liegt ein Alarm vor, dem genauer nachgegangen werden muss, und der zu einer Gefahr für Daten oder Hardware werden könnte, wenn seine Ursache nicht behoben wird.
	**Keine Alarme**: Es liegen keine Alarm vor und die Rack PDU funktioniert normal.

Auf jeder Seite der Web-Oberfläche erscheinen in der rechten oberen Ecke die momentan auf der Startseite angezeigten Symbole für den Status der Rack PDU:

- Das Symbol **Keine Alarme**, wenn kein Alarm vorliegt.
- Mindestens eines der beiden anderen Symbole (**Kritischer Zustand** und **Warnung**), falls Alarme vorliegen, und hinter dem jeweiligen Symbol die Anzahl der Alarme des betreffenden Schweregrads.

Klicken Sie auf einer beliebigen Seite der Web-Oberfläche auf ein Schnellstatus-Symbol, um zur Startseite **Home** zurückzukehren und sich die Zusammenfassung des Rack PDU-Status mit allen aktiven Alarmen anzusehen.

Quick Links

Links unten auf jeder Seite befinden sich drei konfigurierbare Links. Zu diesen gehören die folgenden Standardeinstellungen:

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

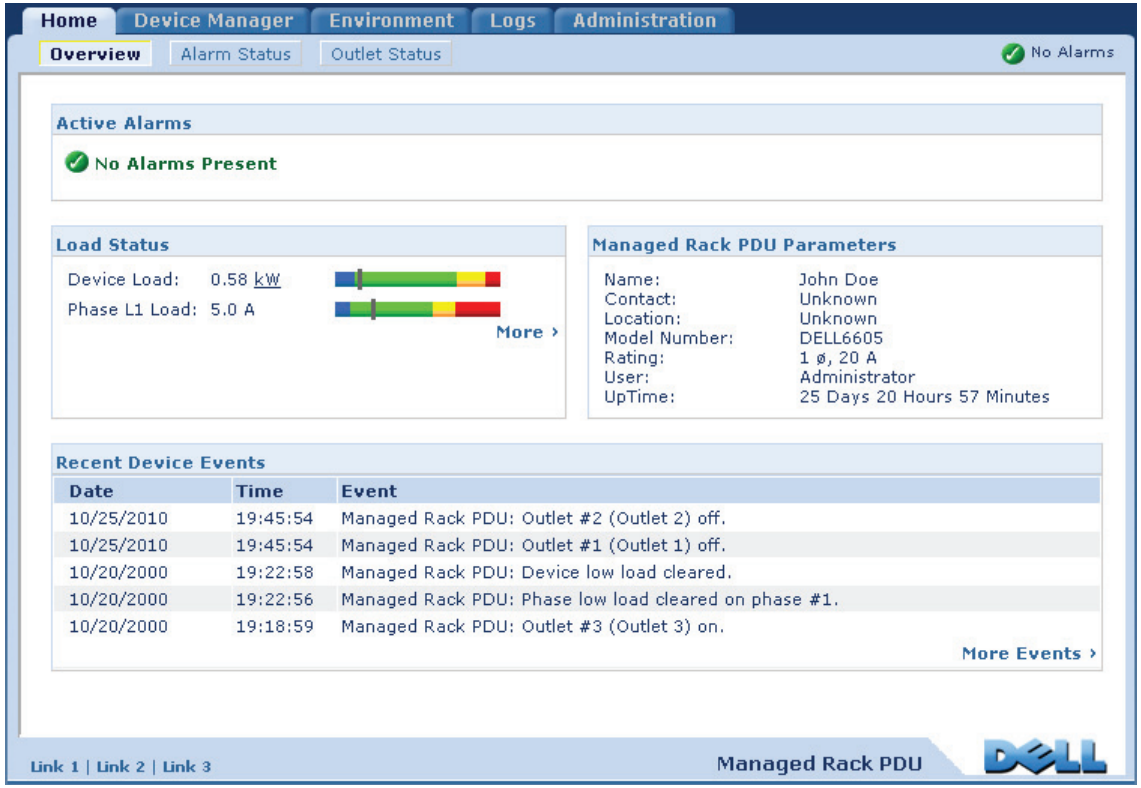
Das Umkonfigurieren dieser Links ist unter Konfigurieren der Links beschrieben.

Sonstige Funktionen der Web-Oberfläche

- Die IP-Adresse wird in der linken oberen Ecke angezeigt.
- Der Link **Help** zum Aufrufen der kontextsensitiven Hilfe und der Link **Log off** befinden sich in der rechten oberen Ecke des Fensters.

Wissenswertes zur Registerkarte „Home“

Auf der Registerkarte „Home“ werden die aktiven Alarme, der Laststatus der Rack PDU und die neuesten Rack PDU-Ereignisse angezeigt.

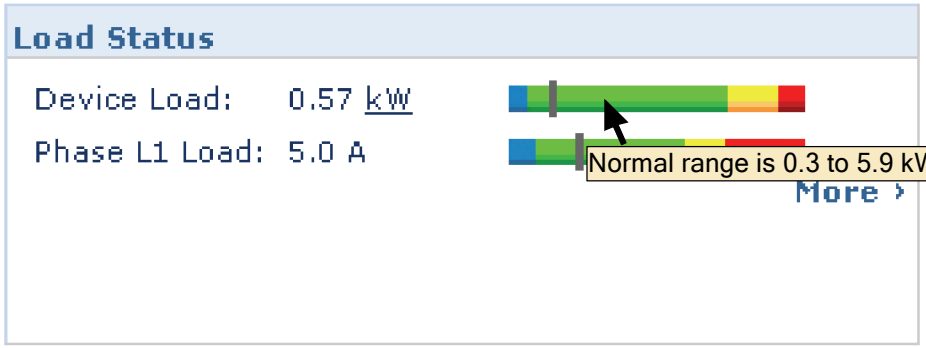


Die Übersichtsanzeige

Befehlsfolge: Home > Overview

Ganz oben in der Übersichtsanzeige wird Alarmstatus angezeigt. Wenn ein oder mehrere Alarme vorliegen, werden Anzahl und Art der Alarme zusammen mit einem Link zur Ansicht **Alarm Status** angezeigt, wo Beschreibungen zu den einzelnen Alarmen angezeigt werden. Wenn kein Alarm vorliegt, wird in der Übersicht die Meldung „No Alarms Present“ (Keine Alarme vorhanden) angezeigt.

Im Bereich **Load Status** (Laststatus) wird die Last des Geräts in kW bzw. die Last der einzelnen Phasen in Ampere angezeigt. Die grüne, gelbe und rote Messanzeige lassen den aktuellen Laststatus erkennen: „normal“, „drohende Überlastung“ oder „Überlastung“. Wenn ein unterer Überlastgrenzwert konfiguriert wurde, enthält die Messanzeige links neben dem grünen Bereich auch ein blaues Segment. Bewegen Sie die Maus über die Farben, um die konfigurierten Lastgrenzwerte angezeigt zu bekommen.



Klicken Sie auf **More** (Mehr), um die Registerkarte **Device Manager** (Geräte-Manager) zu öffnen. Dort können Sie Grenzwerte konfigurieren und sich Informationen zu Spitzenlasten ansehen und diese verwalten.

Im Bereich für die Geräteparameter können Sie sich zur betreffenden Rack PDU Angaben wie Name, Kontaktperson, Standort, Nennstrom, zugriffsberechtigte Benutzerkonten und die Einschaltdauer der Rack PDU seit dem letzten Neustart der Hardware bzw. der Verwaltungsschnittstelle anzeigen lassen. (Weitere Informationen finden Sie unter Zurücksetzen der Rack PDU.)

Im Bereich **Recent Device Events** (Letzte Geräteereignisse) werden die zuletzt aufgetretenen Ereignisse mit Datum und Uhrzeit ihres Auftretens in umgekehrter chronologischer Reihenfolge angezeigt. Es werden maximal fünf Ereignisse gleichzeitig angezeigt. Klicken Sie auf **More Events** (Mehr Ereignisse), um zur Registerkarte **Logs** (Protokolle) zu wechseln und dort das gesamte Ereignisprotokoll einzusehen.

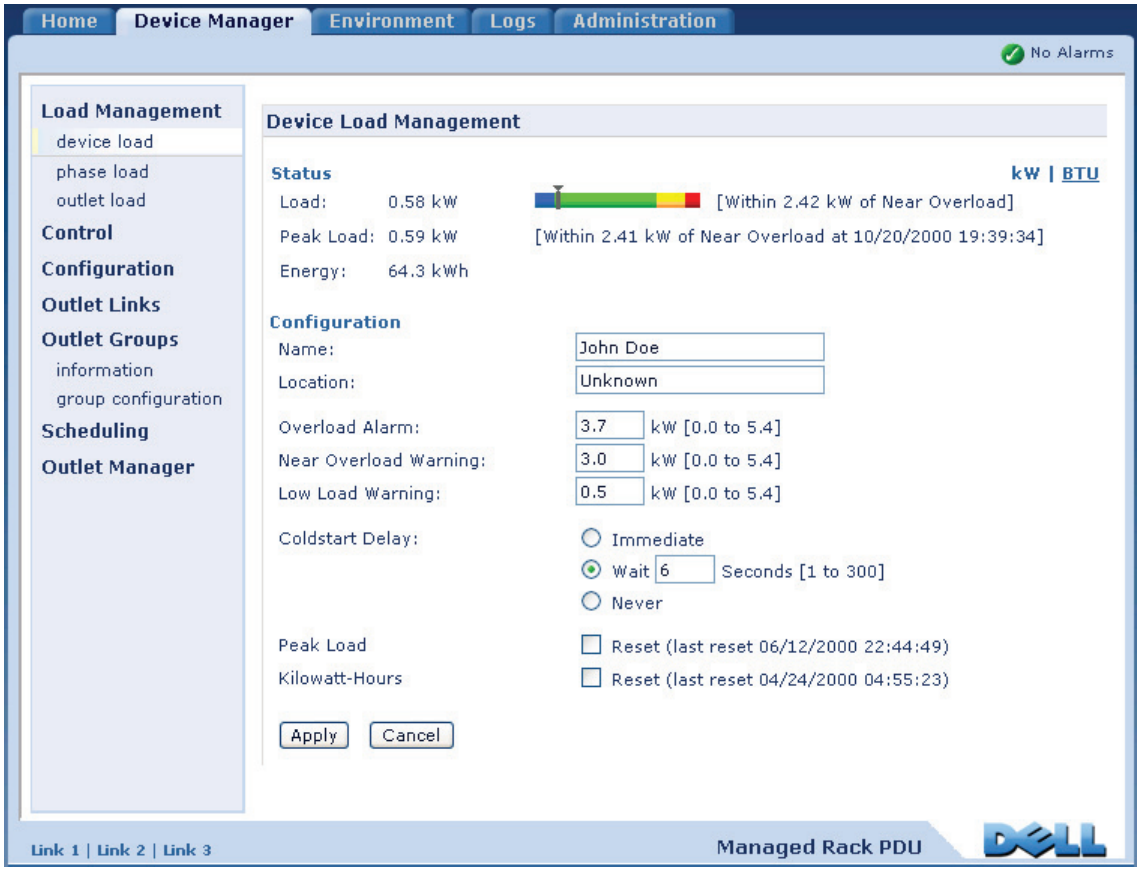
Die Anzeige „Alarm Status“

Befehlsfolge: Home > Alarm Status

Die Anzeige **Alarm Status** enthält eine Beschreibung aller vorhandenen Alarme.

Klicken Sie auf die Registerkarte „Environment“ (Umgebung), um sich Einzelheiten zu einer Verletzung der Temperatur- oder Feuchtigkeitsgrenzwerte anzeigen zu lassen.

Verwaltung des Geräts



Wissenswertes zur Registerkarte Device Manager

Befehlsfolge: Device Manager

Die Registerkarte **Device Manager** (Geräte-Manager) bietet folgende Möglichkeiten:

- Anzeigen des Laststatus der Rack PDU
- Konfigurieren der Lastgrenzwerte für alle angeschlossenen Geräte bzw. Phasen
- Verwalten und Steuern der Ausgangsanschlüsse
- Konfigurieren eines Namens und Standorts für das Rack PDU
- Anzeigen und Verwalten der Spitzenlastmessungen
- Per Mausklick auf benutzerdefinierte Links Webseiten für bestimmte mit der Rack PDU verbundene Geräte öffnen.

Anzeigen des Lastzustands und der Spitzenlast

Befehlsfolge: Device Manager > *Load Management Optionen*

Der Zeiger auf der grünen, gelben und roten Skala lässt den aktuellen Laststatus erkennen: „normal“, „drohende Überlastung“ oder „Überlastung“. Wenn ein unterer Überlastgrenzwert konfiguriert wurde, enthält die Skala links neben dem grünen Bereich auch ein blaues Segment. Bei der Anzeige der **Device Load** (Gerätelast) zeigt der Keil oberhalb der Skala auf die Spitzenlast.

Klicken Sie in der rechten oberen Ecke auf **kW | BTU**, um die Lastwerte wahlweise in Kilowatt oder British Thermal Units (BTU) angezeigt zu bekommen.

Konfigurieren von Lastgrenzwerten

Befehlsfolge: Device Manager > *Load Management Optionen*

So konfigurieren Sie Lastgrenzwerte:

1. Klicken Sie auf die Registerkarte **Device Manager** (Geräte-Manager).
2. Zum Konfigurieren von Lastgrenzwerten für das Gerät oder die Phasen wählen Sie die entsprechende Option aus dem Menü „Load Management“ (Lastmanagement).
3. Stellen Sie die Grenzwerte **Overload Alarm** (Überlastungsalarm), **Near Overload Warning** (Warnung bei drohender Überlastung) und **Low Load Warning** (Warnung bei zu niedriger Last) ein.
4. Klicken Sie auf **Apply** (Übernehmen).

Konfigurieren von Name und Standort der Rack PDU

Befehlsfolge: Device Manager > Load Management > Device Load

Der von Ihnen eingegebene Namen und Standort wird auf der Registerkarte **Home** angezeigt.

Sie können den Namen und Standort wahlweise über die Registerkarte „Device Manager“ (Geräte-Manager) oder über die Registerkarte „Administration“ festlegen. Änderungen auf der einen Registerkarte wirken sich automatisch auch auf die andere Registerkarte aus.

1. Klicken Sie auf die Registerkarte **Device Manager** (Geräte-Manager) und wählen Sie anschließend **device load** (Gerätelast) aus dem Menü **Load Management** (Lastmanagement) aus.
2. Geben Sie einen Namen und den Standort ein.
3. Klicken Sie auf **Apply** (Übernehmen).

Einstellen der Kaltstartverzögerung

Befehlsfolge: Device Manager > Device Load

Die Kaltstartverzögerung ist die Wartezeit (in Sekunden), die zur Einschaltverzögerung der einzelnen Ausgangsanschlüsse hinzu addiert werden soll und bis zur Einschaltung verstreichen muss, nachdem die Rack PDU mit Strom versorgt wurde. Zulässige Werte: 1 bis 300 Sekunden, **Immediate** (Sofort einschalten) oder **Never** (Nie einschalten).

1. Klicken Sie auf die Registerkarte **Device Manager** (Geräte-Manager) und wählen Sie anschließend **device load** (Gerätelast) aus dem Menü **Load Management** (Lastmanagement) aus.
2. Wählen Sie eine Option für die Funktion **Coldstart Delay** (Kaltstartverzögerung).
3. Klicken Sie auf **Apply** (Übernehmen).

Zurücksetzen der Spitzenlast und der kWh-Zahl

Befehlsfolge: Device Manager > Device Load

1. Klicken Sie auf die Registerkarte **Device Manager** (Geräte-Manager) und wählen Sie anschließend **device load** (Gerätelast) aus dem Menü **Load Management** (Lastmanagement) aus.
2. Markieren Sie die Kontrollkästchen **Peak Load** (Spitzenlast) und **Kilowatt-Hours** (Kilowattstunden) wie es die Situation erfordert.
3. Klicken Sie auf **Apply** (Übernehmen).

Konfigurieren und Steuern der Ausgangsanschlussgruppen

Nomenklatur bei Ausgangsanschlussgruppen

Eine *Ausgangsanschlussgruppe* besteht aus Ausgangsanschlüssen, die auf ein und demselben Rack PDU logisch miteinander verbunden sind. Ausgangsanschlüsse, die einer Ausgangsanschlussgruppe angehören, werden synchron eingeschaltet, ausgeschaltet und neu gestartet:

- Eine *lokale Ausgangsanschlussgruppe* besteht aus mindestens zwei Ausgangsanschlüssen einer Rack PDU. Hierbei sind nur die Ausgangsanschlüsse der betreffenden Gruppe synchronisiert.
- Eine *globale Ausgangsanschlussgruppe* besteht aus mindestens einem Ausgangsanschluss einer Rack PDU. Ein Ausgangsanschluss wird als *globaler Ausgangsanschluss konfiguriert* und dadurch logisch mit den Ausgangsanschlussgruppen von bis zu drei anderen Rack PDUs verbunden. Alle Ausgangsanschlüsse in den verbundenen globalen Ausgangsanschlüssen sind synchronisiert.
  - Bei globalen Ausgangsanschlussgruppen ist die *auslösende Ausgangsanschlussgruppe* diejenige Gruppe, die einen Vorgang in Gang gesetzt hat.

– Bei globalen Ausgangsanschlussgruppen ist eine *mitlaufende Ausgangsanschlussgruppe* eine beliebige andere Ausgangsanschlussgruppe, die mit der auslösenden Ausgangsanschlussgruppe synchronisiert ist.

Wenn Sie einen Steuerungsvorgang auf Ausgangsanschlüsse anwenden, die einer Ausgangsanschlussgruppe angehören, werden die Ausgangsanschlüsse wie folgt synchronisiert:

- Verwenden Sie für eine globale Ausgangsanschlussgruppe die für den globalen Ausgangsanschluss der auslösenden Ausgangsanschlussgruppe festgelegten Wartezeiten und dessen Neustartdauer.
- Bei einer lokalen Ausgangsanschlussgruppe verwenden die Ausgangsanschlüsse die Wartezeiten und die Neustartdauer des Ausgangsanschlusses mit der niedrigsten laufenden Nummer in der Gruppe.

Zweck und Vorteile von Ausgangsanschlussgruppen

Mithilfe von Gruppen synchronisierter Ausgangsanschlüsse von Rack PDUs können Sie sicherstellen, dass die Ausgangsanschlüsse synchronisiert eingeschaltet, ausgeschaltet und neu gestartet werden. Die synchronisierte Ausführung von Steuerungsvorgängen mithilfe von Ausgangsanschlussgruppen bietet folgende Vorteile:

- Das synchronisierte Herunter- und Hochfahren der Stromversorgung von Servern mit zweifacher Stromzuleitung verhindert eine irrtümliche Meldung von Stromausfällen bei einem planmäßigen Herunterfahren oder Neustart des Systems.
- Das Synchronisieren von Ausgangsanschlüssen mithilfe von Ausgangsanschlussgruppen ermöglicht eine präzisere zeitliche Abfolge des Herunterfahrens und Neustartens als bei einer Steuerung über die Wartezeiten der einzelnen Ausgangsanschlüsse.
- Ein globaler Ausgangsanschluss wird auf der Benutzeroberfläche aller mit ihm verbundener Rack PDUs angezeigt.

Systemanforderungen für Ausgangsanschlussgruppen

Voraussetzungen für die Einrichtung und Synchronisation von Ausgangsanschlussgruppen:

- Sie benötigen ein 10/100Base-T TCP/IP-Netzwerk mit einem Ethernet-Hub oder -Switch, dessen Stromquelle nicht von den zur Synchronisation vorgesehenen Computern oder sonstigen Geräten mitbenutzt wird.
- Sollen Ausgangsanschlussgruppen zwischen mehreren Rack PDUs gleichzeitig synchronisiert werden, müssen die betreffenden Rack PDUs die folgenden Anforderungen erfüllen:
  - Sie müssen sich im selben Teilnetz befinden.
  - Das Betriebssystemmodul (AOS) und das Anwendungsmodul der Firmware müssen bei allen Rack PDUs die gleiche Versionsnummer haben.
- Sie benötigen einen Computer, der die synchronisierten Steuerungsvorgänge über die Web-Oberfläche oder die Befehlszeile der Rack PDUs bzw. über SNMP anstoßen kann.
- Die zur Synchronisation vorgesehenen Ausgangsanschlussgruppen müssen dieselbe Multicast-IP-Adresse haben. Stellen Sie sicher, das jeder mit den Rack PDUs verbundene Ethernet-Switch für die jeweilige Multicast-IP-Adresse Multicast-Netzverkehr zulässt.

Regeln für das Konfigurieren von Ausgangsanschlussgruppen

Für ein System, das Ausgangsanschlussgruppen verwendet, gelten die folgenden Regeln:

- Ein Rack PDU kann mehrere Ausgangsanschlussgruppen haben, jeder Ausgangsanschluss kann jedoch nur einer einzigen Ausgangsanschlussgruppe angehören.
- Eine lokale Ausgangsanschlussgruppe, die keinen globalen Ausgangsanschluss besitzt, muss aus mindestens zwei Ausgangsanschlüssen bestehen.
- Sie können eine globale Ausgangsanschlussgruppe einer Rack PDU mit je einer globalen Ausgangsanschlussgruppe dreier anderer Rack PDUs synchronisieren.
  - Sie können in einer globalen Ausgangsanschlussgruppe immer nur einen Ausgangsanschluss als globalen Ausgangsanschluss festlegen und diesen zum Zwecke der Synchronisierung mit den Ausgangsanschlussgruppen anderer Rack PDUs verbinden. Bei diesem globalen Ausgangsanschluss kann es sich um den einzigen Ausgangsanschluss der betreffenden Gruppe handeln, oder die Gruppe kann sich aus mehreren Ausgangsanschlüssen zusammensetzen.
  - Damit Ausgangsanschlussgruppen von Rack PDUs zur Synchronisation miteinander verbunden werden können, müssen die betreffenden Rack PDUs denselben Multicast-Gerätenamen, dieselbe Multicast-Geräteadresse und dieselbe Version der Rack PDU-Firmware verwenden.
  - Ein globaler Ausgangsanschluss einer Ausgangsanschlussgruppe muss dieselbe Ausgangsanschlussnummer wie der Ausgangsanschluss einer anderen Ausgangsanschlussgruppe haben, mit der dieser verbunden werden soll.
- Zum Erstellen und Konfigurieren von Ausgangsanschlussgruppen müssen Sie die Web-Oberfläche verwenden oder die Einstellungen einer konfigurierten Rack PDU in eine Konfigurationsdatei (INI-Datei) exportieren. Über die Befehlszeile können Sie feststellen, ob ein Ausgangsanschluss einer Ausgangsanschlussgruppe angehört, und können Steuervorgänge auf eine Ausgangsanschlussgruppe anwenden; Sie können jedoch über die Befehlszeile keine Ausgangsanschlussgruppen einrichten oder konfigurieren.

Aktivieren von Ausgangsanschlussgruppen

Klicken Sie auf die Registerkarte **Device Manager** (Gerätemanager) und wählen Sie die Option **Group Configuration** (Gruppenkonfiguration) im linken Navigationsmenü **Outlet Groups** (Ausgangsanschlussgruppen). Konfigurieren Sie die folgenden Parameter und klicken Sie dann auf **Apply** (Übernehmen).

Erstellung von Ausgangsanschlussgruppen aktivieren.

Parameter	Beschreibung
Device Level Outlet Group	Zum Erstellen einer Ausgangsanschlussgruppe müssen Sie diesen Parameter aktivieren. In der Grundeinstellung ist der Parameter deaktiviert.

Unterstützung für globale Ausgangsanschlussgruppen (verbundene Gruppen) aktivieren.

Parameter	Beschreibung
Multicast Name	Damit Sie die Ausgangsanschlussgruppen mehrerer Rack PDUs gleichzeitig miteinander verbinden können, müssen Sie für jede dieser Rack PDUs den gleichen Multicast-Namen und die gleiche Multicast-IP-Adresse festlegen. **HINWEIS:** Sie können bis zu vier Geräte mit dem gleichen Multicast-Namen und der gleichen Multicast-IP-Adresse konfigurieren.
Multicast IP	

Aktivieren der Verschlüsselung und Authentifizierung von Ausgangsanschlussgruppen.

Parameter	Beschreibung
Authentication Phrase	Bei der Authentifizierungsphrase handelt es sich um eine Folge aus 15 bis 32 ASCII-Zeichen, mit der verifiziert wird, dass das Gerät mit anderen Geräten kommuniziert, und dass die entsprechenden Nachrichten auf dem Übertragungsweg nicht verändert und rechtzeitig übergeben wurden. Die Authentifizierungsphrase stellt sicher, dass die Nachricht im normalen Zeitrahmen übermittelt und somit nicht aufgehalten wurde, z. B. durch Kopieren und zeitversetztes Neuversenden.
Encryption Phase	Die Verschlüsselungsphrase ist einer Folge aus 15 bis 32 ASCII-Zeichen, mit der die Geheimhaltung der Daten (durch Verschlüsselung) sichergestellt wird.

Einstellen des Ports der Ausgangsanschlussgruppe.

Parameter	Beschreibung
Outlet Group Port	Hierbei handelt es sich um die Port-Nummer, über die das Gerät mit anderen Geräten kommuniziert.

Damit sich ein Gerät mit den Ausgangsanschlussgruppen anderer Geräte synchronisieren kann, müssen alle beteiligten Geräte die gleiche Authentifizierungsphrase, Verschlüsselungsphrase und Gruppen-Port-Nummer verwenden. Diese Werte sind für den Benutzer nicht sichtbar.

Erstellen einer lokalen Ausgangsanschlussgruppe

1. Wählen Sie auf der Registerkarte **Device Manager** (Geräte-Manager) die Option **Information** aus dem linken Navigationsmenü **Outlet Groups** (Ausgangsanschlussgruppen).
2. Überzeugen Sie sich davon, dass die Ausgangsanschlussgruppen aktiviert sind. (Siehe Aktivieren von Ausgangsanschlussgruppen.)
3. Klicken Sie auf **Create Local Outlet Group** (Lokale Ausgangsanschlussgruppe erstellen).
4. Wählen Sie unter **Select Local Outlets** (Lokale Ausgangsanschlussgruppen wählen) die einzelnen Ausgangsanschlüsse aus, die Sie in die Gruppe aufnehmen möchten, und geben Sie für die Gruppe im Feld **Outlet Group Name** (Name der Ausgangsanschlussgruppe) einen Namen ein. Sie müssen mindestens zwei Ausgangsanschlüsse auswählen.

Erstellen mehrerer globaler Ausgangsanschlussgruppen

So richten Sie mehrere globale Ausgangsanschlussgruppen ein, die Sie mit Ausgangsanschlussgruppen anderer Rack PDUs verbinden können:

1. Wählen Sie auf der Registerkarte **Device Manager** (Geräte-Manager) die Option **Information** aus dem linken Navigationsmenü **Outlet Groups** (Ausgangsanschlussgruppen).
2. Überzeugen Sie sich davon, dass Ausgangsanschlussgruppen aktiviert sind, und dass die Multicast-Parameter (Name und IP-Adresse) für alle miteinander zu verbindenden Rack PDUs identisch sind. (Siehe Aktivieren von Ausgangsanschlussgruppen.)
3. Klicken Sie auf **Create Global Outlet Groups** (Globale Ausgangsanschlussgruppen erstellen).
4. Wählen Sie zu jeder von Ihnen erstellten globalen Ausgangsanschlussgruppe einen Ausgangsanschluss, indem Sie auf das dazugehörige Kontrollkästchen klicken. Klicken Sie dann auf **Apply** (Übernehmen). Wählen Sie beispielsweise fünf Ausgangsanschlüsse aus, um fünf Ausgangsanschlussgruppen zu erstellen, die jeweils aus einem globalen Ausgangsanschluss bestehen.
5. Informationen dazu, wie Sie Ausgangsanschlüsse zu den von Ihnen erstellten globalen Ausgangsanschlussgruppen hinzufügen können, finden Sie unter Bearbeiten oder Löschen einer Ausgangsanschlussgruppe.

Bearbeiten oder Löschen einer Ausgangsanschlussgruppe

1. Wählen Sie auf der Registerkarte **Device Manager** (Geräte-Manager) die Option **Information** aus dem linken Navigationsmenü **Outlet Groups** (Ausgangsanschlussgruppen).
2. Klicken Sie unter **Configured Outlet Groups** (Konfigurierte Ausgangsanschlussgruppen) auf die Nummer oder den Namen der Ausgangsanschlussgruppe, die Sie bearbeiten oder löschen möchten.

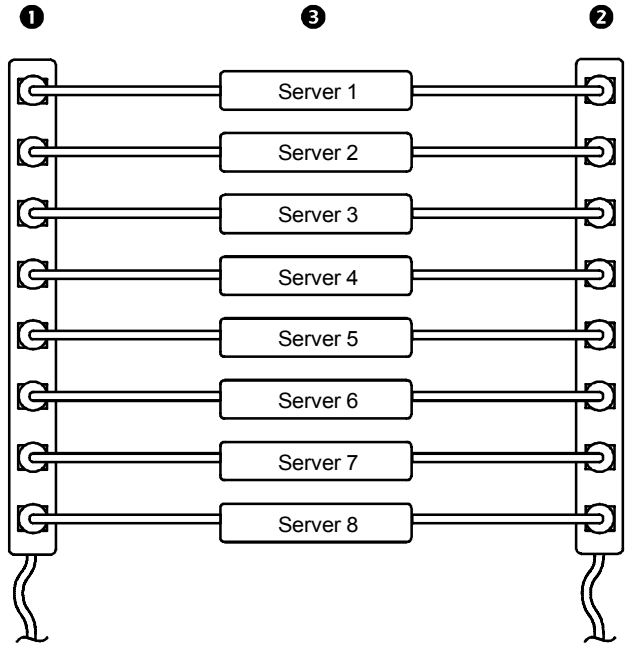
3. Beim Bearbeiten einer Ausgangsanschlussgruppe haben Sie folgende Möglichkeiten:
   - die Ausgangsanschlussgruppe umbenennen
   - Ausgangsanschlüsse durch Aktivieren oder Deaktivieren der dazugehörigen Kontrollkästchen hinzufügen oder entfernen.

   Bei einer Ausgangsanschlussgruppe mit nur zwei Ausgangsanschlüssen können Sie einen davon nur dann entfernen, wenn es sich bei dem verbleibenden Ausgangsanschluss um einen globalen Ausgangsanschluss handelt.

4. Zum Löschen der Ausgangsanschlussgruppe klicken Sie auf **Delete Outlet Group** (Ausgangsanschlussgruppe löschen).

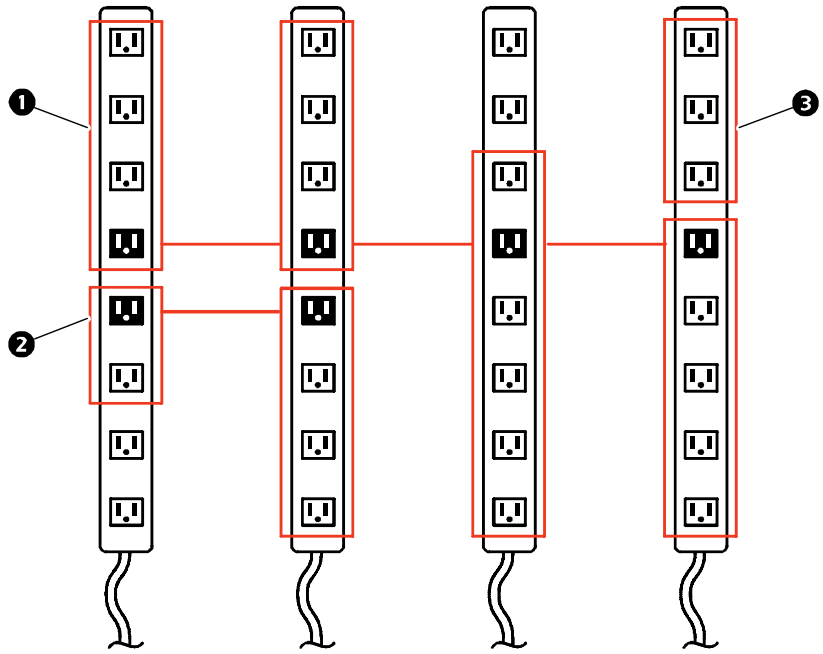
Typische Konfigurationen von Ausgangsanschlussgruppen

Die folgende Konfiguration zeigt zwei Rack PDUs mit je acht Ausgangsanschlussgruppen. Jede dieser Ausgangsanschlussgruppen besteht aus einem einzigen globalen Ausgangsanschluss. Die einzelnen Ausgangsanschlussgruppen ❶ der ersten Rack PDU sind jeweils mit der entsprechend positionierten Ausgangsanschlussgruppe ❷ der zweiten Rack PDU verbunden. Eines der Stromkabel eines Servers mit zweifacher Stromzuleitung ❸ ist mit den einzelnen Ausgangsanschlüssen der ersten Rack PDU verbunden, und das zweite Stromkabel ist mit dem entsprechenden Ausgangsanschluss der zweiten Rack PDU verbunden, damit nach Ansteuerung eines Ausgangsanschlusses die Stromversorgung des Servers aus beiden Stromquellen synchron ein- oder ausgeschaltet wird.



Die folgende Konfiguration zeigt drei Zusammenschlüsse mit synchronisierten Ausgangsanschlüssen. Globale Ausgangsanschlüsse sind schwarz dargestellt. Ausgangsanschlussgruppen sind rot umrandet.

❶	Durch diese vier globalen Ausgangsanschlussgruppen werden insgesamt 19 Ausgangsanschlüsse synchronisiert.
❷	Durch diese beiden globalen Ausgangsanschlussgruppen werden sechs Ausgangsanschlüsse synchronisiert, zwei in der einen Gruppe und vier in der anderen.
❸	Durch diese lokale Ausgangsanschlussgruppe werden drei Ausgangsanschlüsse der selben Rack PDU synchronisiert.



Überprüfen von Einrichtung und Konfiguration der globalen Ausgangsanschlussgruppen

Um sicherzustellen, dass das System alle Anforderungen an Ausgangsanschlussgruppen erfüllt, und dass Sie diese korrekt konfiguriert haben, wählen Sie die Option **Information** aus dem linken Navigationsmenü **Outlet Groups** (Ausgangsanschlussgruppen) auf der Web-Oberfläche. Danach können Sie sich die Gruppen und ihre Verbindungen ansehen:

- Der Bereich **Configured Outlet Groups** (Konfigurierte Ausgangsanschlussgruppen) enthält folgende Informationen:
  - Alle konfigurierten Ausgangsanschlussgruppen der aktuellen Rack PDU.
  - Die Ausgangsanschlüsse der einzelnen Gruppen nach Ausgangsanschlussnummer.
  - Etwaige andere Ausgangsanschlussgruppen auf anderen Rack PDUs, mit denen eine globale Ausgangsanschlussgruppe synchronisiert ist. Jede Rack PDU wird durch ihre IP-Adresse identifiziert, und alle globalen Ausgangsanschlüsse werden in Fettschrift angezeigt.
- Der Bereich **Global Outlet Overview** (Übersicht: Globale Ausgangsanschlüsse) enthält folgende Informationen:
  - Die IP-Adresse der aktuellen Rack PDU.
  - Die IP-Adresse etwaiger Rack PDUs mit globalen Ausgangsanschlüssen, die zur Synchronisation mit Ausgangsanschlüssen anderer Rack PDUs zur Verfügung stehen.
  - Alle auf den Rack PDUs konfigurierten globalen Ausgangsanschlüsse, unabhängig davon, ob diese mit Ausgangsanschlüssen der aktuellen Rack PDU synchronisiert sind.

Einstellungen für Ausgangsanschlüsse und Ausgangsanschlussgruppen

Starten eines Steuerungsvorgangs

Wenn Sie einen Steuerungsvorgang auf Ausgangsanschlüsse oder Ausgangsanschlussgruppen anwenden, geschieht dies mit den folgenden Verzögerungen:

- Bei einem einzelnen Ausgangsanschluss (der keiner Ausgangsanschlussgruppe angehört) unterliegt der Vorgang den folgenden, für den betreffenden Ausgangsanschluss definierten Wartezeiten und dessen Neustartdauer.
- Bei einer globalen Ausgangsanschlussgruppe unterliegt der Vorgang den für den globalen Ausgangsanschluss festgelegten Wartezeiten und dessen Neustartdauer.
- Bei einer lokalen Ausgangsanschlussgruppe unterliegt der Vorgang den Wartezeiten und der Neustartdauer, die für den globalen Ausgangsanschluss definiert wurden.

So steuern Sie die Ausgangsanschlüsse der Rack PDU:

1. Wählen Sie auf der Registerkarte **Device Manager** (Geräte-Manager) die Option **Control** (Steuerung) aus dem linken Navigationsmenü.
2. Markieren Sie die Kontrollkästchen für die einzelnen Ausgangsanschlüsse oder Ausgangsanschlussgruppen, die Sie steuern möchten, oder markieren Sie das Kontrollkästchen **All Outlets** (Alle Ausgangsanschlüsse).
3. Wählen Sie unter **Control Action** einen Steuerungsvorgang aus der Liste aus und klicken Sie auf **Next >>**(Weiter). Auf der folgenden Seite wird der Vorgang erklärt. Wählen Sie „Apply“ (Übernehmen), um den Vorgang zu bestätigen, oder „Cancel“ (Abbrechen).

Wählbare Steuerungsvorgänge.

Option	Beschreibung
No Action (Web-Oberfläche)	Nichts unternehmen.
On Immediate	Die Stromversorgung der ausgewählten Ausgangsanschlüsse sofort einschalten.
On Delayed	Die Stromversorgung der einzelnen Ausgangsanschlüsse in Abhängigkeit von dem Wert einschalten, der für die Einstellung **Power On Delay** (Einschaltverzögerung) jeweils festgelegt wurde.†
Off Immediate	Die Stromversorgung der ausgewählten Ausgangsanschlüsse sofort unterbrechen.
Off Delayed	Die Stromversorgung der einzelnen Ausgangsanschlüsse in Abhängigkeit von dem Wert einschalten, der für die Einstellung **Power Off Delay** (Abschaltverzögerung) jeweils festgelegt wurde.†
Reboot Immediate	Die Stromversorgung der ausgewählten Ausgangsanschlüsse unterbrechen. Anschließend die Stromversorgung der einzelnen Ausgangsanschlüsse in Abhängigkeit von dem Wert wieder einschalten, der für die Einstellung **Reboot Duration** (Neustartdauer) jeweils festgelegt wurde.†

† Wenn eine lokale Ausgangsanschlussgruppe ausgewählt ist, werden nur die konfigurierten Wartezeiten und die Neustartdauer des Ausgangsanschlusses mit der niedrigsten Nummer in der Gruppe verwendet. Wenn eine globale Ausgangsanschlussgruppe ausgewählt ist, werden nur die konfigurierten Wartezeiten und die Neustartdauer des globalen Ausgangsanschlusses verwendet.

Option	Beschreibung
Reboot Delayed	Die Stromversorgung der einzelnen Ausgangsanschlüsse in Abhängigkeit von dem Wert einschalten, der für die Einstellung **Power Off Delay** (Abschaltverzögerung) jeweils festgelegt wurde. Warten, bis alle Ausgangsanschlüsse abgeschaltet sind (abhängig vom höchsten Wert der Einstellung **Reboot Duration**), dann die Stromversorgung der einzelnen Ausgangsanschlüsse in Abhängigkeit von dem Wert wieder einschalten, der für die Einstellung **Power On Delay** (Einschaltverzögerung) jeweils festgelegt wurde.†
Cancel Pending Commands	Alle für die ausgewählten Ausgangsanschlüsse anstehenden Befehlen abbrechen und diese in ihrem derzeitigen Zustand belassen. **HINWEIS:** Bei globalen Ausgangsanschlussgruppen können Sie einen Befehl nur über die Schnittstelle der auslösenden Ausgangsanschlussgruppe abbrechen. Dieser Vorgang bricht den Befehl für die auslösende Ausgangsanschlussgruppe und alle mitlaufenden Ausgangsanschlussgruppen ab.

† Wenn eine lokale Ausgangsanschlussgruppe ausgewählt ist, werden nur die konfigurierten Wartezeiten und die Neustartdauer des Ausgangsanschlusses mit der niedrigsten Nummer in der Gruppe verwendet. Wenn eine globale Ausgangsanschlussgruppe ausgewählt ist, werden nur die konfigurierten Wartezeiten und die Neustartdauer des globalen Ausgangsanschlusses verwendet.

Konfigurieren der Einstellungen und des Namens eines Ausgangsanschlusses

Die folgenden Einstellungen sind verfügbar:

Einstellung	Beschreibung
Name	Für einen oder mehrere Ausgangsanschlüsse einen Namen festlegen. In Statusanzeigen wird der Name neben der Nummer des Ausgangsanschlusses angezeigt.
External Link	Mit dieser Einstellung definieren Sie einen HTTP- oder HTTPS-Link zu einer Website oder IP-Adresse. • **http://www.dell.com** verlinkt den Ausgangsanschluss mit der Website von Dell. • **http://*pdu_ip_address*** (hierbei steht ***pdu_ip_address*** für die IP-Adresse der Rack PDU) verlinkt den Ausgangsanschluss mit der Web-Oberfläche der Rack PDU an der angegebenen IP-Adresse und ermöglicht es damit autorisierten Benutzern, sich anzumelden.
Power On Delay	Mit dieser Einstellung legen Sie fest, wie viele Sekunden die Rack PDU nach Eingabe des entsprechenden Befehls wartet, bis sie die Stromversorgung über einen Ausgangsanschluss freigibt. **HINWEIS:** Wenn ein Ausgangsanschluss immer ausgeschaltet bleiben soll, markieren Sie das Kontrollkästchen **Never** (Nie) neben der Option **Power On Delay** (Einschaltverzögerung).
Power Off Delay	Mit dieser Einstellung legen Sie fest, wie viele Sekunden die Rack PDU nach Eingabe des entsprechenden Befehls wartet, bis sie die Stromversorgung über einen Ausgangsanschluss beendet. **HINWEIS:** Wenn ein Ausgangsanschluss immer eingeschaltet bleiben soll, markieren Sie das Kontrollkästchen **Never** (Nie) neben der Option **Power Off Delay** (Abschaltverzögerung).
Reboot Duration	Mit dieser Einstellung legen Sie fest, wie viele Sekunden ein Ausgangsanschluss vor einem Neustart ausgeschaltet bleiben soll.

Klicken Sie auf die Registerkarte **Device Manager** (Gerätemanager) und wählen Sie die **Configuration** im linken Navigationsmenü. Klicken Sie auf die Schaltfläche **Configure Multiple Outlets** (Mehrere Ausgangsanschlüsse) im Bereich **Outlet Configuration** (Ausgangsanschlusskonfiguration), oder klicken Sie auf den Namen des Ausgangsanschlusses.

- So konfigurieren Sie die Einstellungen für mehrere Ausgangsanschlüsse:
  - Markieren Sie die Kontrollkästchen neben den Nummern der Ausgangsanschlüsse, die Sie ändern möchten, oder markieren Sie das Kontrollkästchen **All Outlets** (Alle Ausgangsanschlüsse).
  - Geben Sie Werte für die Einstellungen **Name** und **Link**, ein und klicken Sie auf die Schaltfläche **Apply** (Übernehmen) direkt unter der Liste.
  - Geben Sie Werte für die Einstellungen **Power On Delay** (Einschaltverzögerung), **Power Off Delay** (Abschaltverzögerung) oder **Reboot Duration** (Neustartdauer) ein, und klicken Sie auf die Schaltfläche **Apply** (Übernehmen) direkt unter der Liste.
- So konfigurieren Sie Einstellungen für einen einzelnen Ausgangsanschluss:
  - Geben Sie Werte für die Einstellungen **Name** und **Link**, ein und klicken Sie auf die Schaltfläche **Apply** (Übernehmen) direkt unter der Liste.
  - Geben Sie Werte für die Einstellungen **Power On Delay** (Einschaltverzögerung), **Power Off Delay** (Abschaltverzögerung) oder **Reboot Duration** (Neustartdauer) ein, und klicken Sie auf die Schaltfläche **Apply** (Übernehmen) direkt unter der Liste.

Planen von Ausgangsanschlussvorgängen

Planbare Vorgänge

Informationen dazu, wie Sie für die einzelnen Ausgangsanschlüsse Werte für die Einstellungen **Power On Delay** (Einschaltverzögerung), **Power Off Delay** (Abschaltverzögerung) und **Reboot Duration** (Neustartdauer) konfigurieren, finden Sie unter Konfigurieren der Einstellungen und des Namens eines Ausgangsanschlusses. Sie können Ausgangsanschlussvorgänge nur über die Web-Oberfläche planen; zum Einstellen dieser Werte können Sie jedoch wahlweise die Web-Oberfläche oder die Befehlszeile verwenden.

Damit ein Vorgang auf eine Ausgangsanschlussgruppe angewandt werden kann, müssen die Ausgangsanschlussgruppen zu Beginn der geplanten Vorgangs aktiviert sein. Wenn der Vorgang **Off Delayed** (Verzögerte Abschaltung) beispielsweise für 16:00 Uhr geplant ist, beginnt der Vorgang **Power Off Delay** (Abschaltverzögerung) um 16:00 Uhr. Wenn Sie Ausgangsanschlussgruppen während dieser **Abschaltverzögerung** aktivieren, d. h. vor der planmäßigen Abschaltung irgendeines der Ausgangsanschlüsse, wird der Vorgang nur auf den jeweiligen Ausgangsanschluss angewandt, nicht auf die Ausgangsanschlussgruppe.

Sie können die in der nachfolgenden Tabelle aufgeführten Vorgänge für die von Ihnen ausgewählten Ausgangsanschlüsse täglich, in Intervallen von einer, zwei, vier oder acht Wochen oder nur einmal nach Zeitplan ausführen lassen.

Option	Beschreibung
No Action	Nichts unternehmen.
On Immediate	Die Stromversorgung der ausgewählten Ausgangsanschlüsse sofort einschalten.
On Delayed	Die Stromversorgung der einzelnen Ausgangsanschlüsse in Abhängigkeit von dem Wert einschalten, der für die Einstellung **Power On Delay** (Einschaltverzögerung) jeweils festgelegt wurde.†
Off Immediate	Die Stromversorgung der ausgewählten Ausgangsanschlüsse sofort unterbrechen.
Off Delayed	Die Stromversorgung der einzelnen Ausgangsanschlüsse in Abhängigkeit von dem Wert einschalten, der für die Einstellung **Power Off Delay** (Abschaltverzögerung) jeweils festgelegt wurde.†
Reboot Immediate	Die Stromversorgung der ausgewählten Ausgangsanschlüsse unterbrechen. Anschließend die Stromversorgung der einzelnen Ausgangsanschlüsse in Abhängigkeit von dem Wert wieder einschalten, der für die Einstellung **Reboot Duration** (Neustartdauer) jeweils festgelegt wurde.†

† Wenn eine lokale Ausgangsanschlussgruppe ausgewählt ist, werden nur die konfigurierten Wartezeiten und die Neustartdauer des Ausgangsanschlusses mit der niedrigsten Nummer in der Gruppe verwendet. Wenn eine globale Ausgangsanschlussgruppe ausgewählt ist, werden nur die konfigurierten Wartezeiten und die Neustartdauer des globalen Ausgangsanschlusses verwendet.

Option	Beschreibung
Reboot Delayed	Die Stromversorgung der einzelnen Ausgangsanschlüsse in Abhängigkeit von dem Wert einschalten, der für die Einstellung **Power Off Delay** (Abschaltverzögerung) jeweils festgelegt wurde. Warten, bis alle Ausgangsanschlüsse abgeschaltet sind (abhängig vom höchsten Wert der Einstellung **Reboot Duration**), dann die Stromversorgung der einzelnen Ausgangsanschlüsse in Abhängigkeit von dem Wert wieder einschalten, der für die Einstellung **Power On Delay** (Einschaltverzögerung) jeweils festgelegt wurde.†

† Wenn eine lokale Ausgangsanschlussgruppe ausgewählt ist, werden nur die konfigurierten Wartezeiten und die Neustartdauer des Ausgangsanschlusses mit der niedrigsten Nummer in der Gruppe verwendet. Wenn eine globale Ausgangsanschlussgruppe ausgewählt ist, werden nur die konfigurierten Wartezeiten und die Neustartdauer des globalen Ausgangsanschlusses verwendet.

Planen eines Ausgangsanschlussvorgangs

1. Wählen Sie auf der Web-Oberfläche die Registerkarte **Device Manager** (Geräte-Manager) und wählen Sie die Option **Scheduling** (Planung) aus dem linken Navigationsmenü.
2. Geben Sie auf der Seite **Outlet Scheduling** (Ausgangsanschlusszeitplan) an, wie oft der Vorgang ausgeführt werden soll (**One-Time** (Einmalig), **Daily** (Täglich) oder **Weekly** (Wöchentlich)) und klicken Sie auf die Schaltfläche **Next** (Weiter).

   Wenn Sie sich für die Option **Weekly** (Wöchentlich) entscheiden, können Sie wählen, ob der Vorgang einmal wöchentlich oder alle zwei, vier oder acht Wochen durchgeführt werden soll.

3. Ersetzen Sie auf der Seite **Schedule a Daily Action** (Täglichen Vorgang planen) im Textfeld **Name of event** (Name des Ereignisses) den vorgegebenen Namen **`Outlet Event`** Ausgangsanschlussereignis) durch einen beschreibenden Namen für das neue Ereignis.

4. Verwenden Sie die Dropdown-Listenfelder, um den Ereignistyp und den Zeitpunkt des Ereignisses auszuwählen.

   Das Datumsformat für einmalige Ereignisse ist *mm*/*tt*, und das Zeitformat für alle Ereignisse ist *hh*/*mm*, wobei die zweistellige Stundenzahl im 24-Stunden-Format angegeben wird.

   - Ein Ereignis, das nach Zeitplan täglich oder in einem von der Auswahl **Weekly** (Wöchentlich) bereitgestellten Intervall stattfinden soll, wird so lange planmäßig durchgeführt, bis das Ereignis gelöscht oder deaktiviert wird.
   - Sie können den Zeitplan für ein einmaliges Ereignis so erstellen, dass dieses nur an einem einzigen Tag innerhalb der nächsten 12 Monate nach Erstellung des Zeitplans erfolgt. Sie könnten beispielsweise am 26. Dezember 2010 ein einmaliges Ereignis an einem beliebigen Datum vor dem 26. Dezember 2011 planen.

5. Verwenden Sie die Kontrollkästchen, um auszuwählen, welche Ausgangsanschlüsse von dem Vorgang betroffen sein sollen. Sie können einen oder mehrere einzelne Ausgangsanschlüsse oder **All Outlets** (Alle Ausgangsanschlüsse) wählen.
6. Klicken Sie auf **Apply** (Übernehmen), um den Zeitplan zu bestätigen, oder wählen Sie **Cancel** (Abbrechen), um ihn zu verwerfen.

Wenn Sie das Ereignis bestätigen, wird die Übersichtsseite noch einmal angezeigt. Das neue Ereignis befindet sich jetzt in der Liste der geplanten Ereignisse.

Bearbeiten, Deaktivieren, Aktivieren oder Löschen eines geplanten Ausgangsanschlussereignisses

1. **Wählen** Sie auf der Web-Oberfläche die Registerkarte **Device Manager** (Geräte-Manager) und wählen Sie die Option **Scheduling** (Planung) aus dem linken Navigationsmenü.
2. Klicken Sie in der Ereignisliste im Bereich **Scheduled Outlet Action** (Geplanter Ausgangsanschlussvorgang) auf der Seite **Scheduling** (Zeitplan) auf den Namen des Ereignisses.
3. Auf der Seite **Daily/Weekly scheduled action detail** (Details zum täglich/wöchentlich geplanten Vorgang) haben Sie folgende Möglichkeiten:

– Die Details des Ereignisses ändern, z. B. seinen Namen, seinen Zeitplan und die von ihm betroffenen Ausgangsanschlüsse.

– Unter **Status of event** (Status des Ereignisses) ganz oben auf der Seite können Sie die folgenden Aufgaben durchführen:

  • Das Ereignis deaktivieren und die dafür konfigurierten Details unverändert lassen, um es später erneut aktivieren zu können. Ein deaktiviertes Ereignis kann nicht stattfinden. Wenn Sie ein Ereignis erstellen, wird es immer auch aktiviert.

  • Das Ereignis aktivieren, wenn es zuvor auf **Disable** (Deaktivieren) eingestellt war.

  • Das Ereignis löschen und somit komplett aus dem System entfernen. Gelöschte Ereignisse können nicht wiederhergestellt werden.

4. Wenn Sie keine weiteren Änderungen auf dieser Seite mehr vornehmen möchten, klicken Sie auf **Apply** (Übernehmen), um die Änderungen zu bestätigen, oder klicken Sie auf **Cancel** (Abbrechen).

Menü Outlet Manager

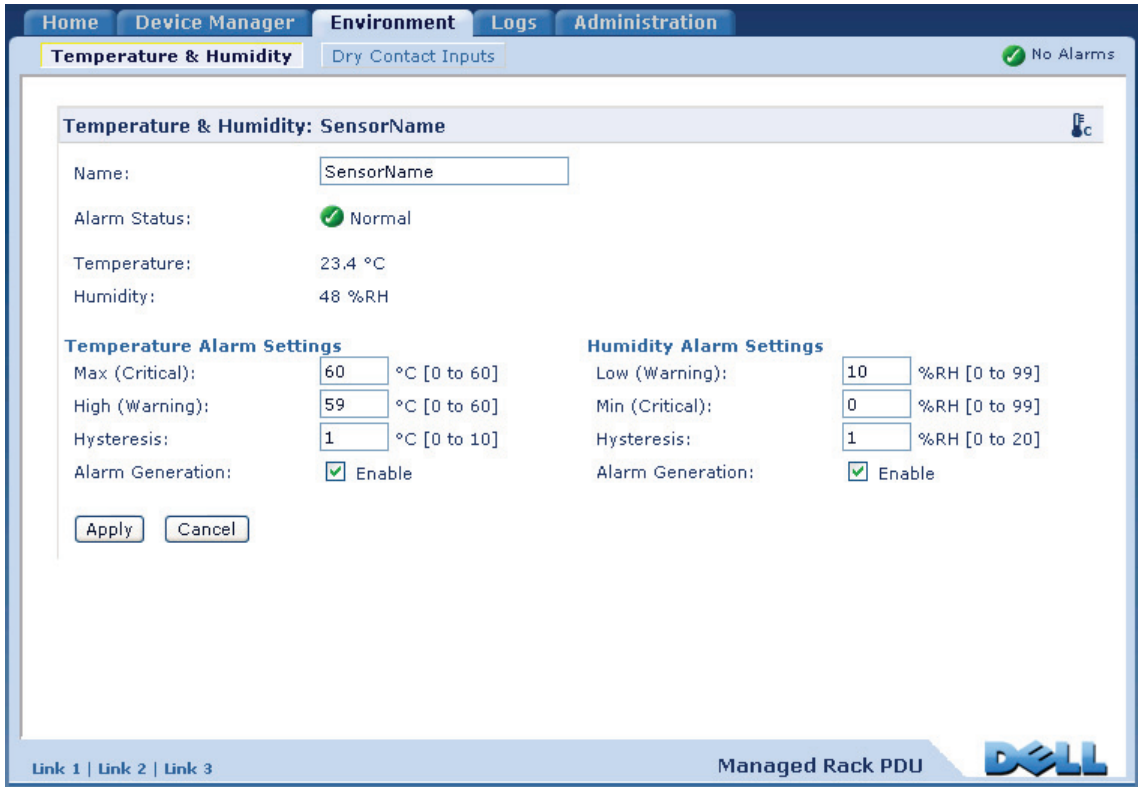
Dieses Menü dient zum Erstellen und Konfigurieren von Benutzerkonten des Typs „Ausgangsanschluss“. Einem Benutzer mit dem Kontotyp „Ausgangsanschluss“ können einzelne Ausgangsanschlüsse zugewiesen werden. Benutzer mit dem Kontotyp „Ausgangsanschluss“ können nur die ihnen zugewiesenen Ausgangsanschlüsse steuern. Die Konfiguration der Ausgangsanschlüsse ist Benutzern mit Administratorrechten vorbehalten. Die Geräte-Manager hat begrenzte Rechte zum Konfigurieren von Ausgangsanschlüssen.

Konfigurieren eines Benutzern „Ausgangsanschluss“

1. Wählen Sie auf der Web-Oberfläche die Registerkarte **Device Manager** (Geräte-Manager) und wählen Sie die Option **Outlet Manager** (Ausgangsanschluss-Manager) aus dem linken Navigationsmenü.
2. Klicken Sie auf die Schaltfläche **Add New User** (Neuer Benutzer).
3. Geben Sie die Informationen zu den folgenden Optionen ein und klicken Sie auf **Apply** (Übernehmen), um die Änderungen zu bestätigen.

Option	Beschreibung
User Name	Mit dieser Option legen Sie den Namen des Benutzers „Ausgangsanschluss“ fest. „New User“ ist reserviert und darf nicht verwendet werden. **HINWEIS:** Ein Benutzername in orangefarbener Schrift bedeutet, dass das Benutzerkonto deaktiviert wurde.
Password	Mit dieser Option legen Sie das Passwort des Benutzers „Ausgangsanschluss“ fest.
User Description	Mit dieser Option legen Sie die Identifizierung/Beschreibung des Benutzers „Ausgangsanschluss“ fest.
Account Status	Diese Option dient zum Aktivieren, Deaktivieren oder Löschen des Benutzerkontos vom Typ „Ausgangsanschluss“.
Device outlet access	Mit dieser Option wählen Sie die Ausgangsanschlüsse aus, auf die der Benutzer zugreifen darf.

Umgebung


Home
Device Manager
Environment
Logs
Administration
Temperature & Humidity
Dry Contact Inputs
No Alarms
Temperature & Humidity: SensorName
Name:
SensorName
Alarm Status:
Normal
Temperature:
23.4 °C
Humidity:
48 %RH
Temperature Alarm Settings
Max (Critical):
60
°C [0 to 60]
High (Warning):
59
°C [0 to 60]
Hysteresis:
1
°C [0 to 10]
Alarm Generation:
Enable
Humidity Alarm Settings
Low (Warning):
10
%RH [0 to 99]
Min (Critical):
0
%RH [0 to 99]
Hysteresis:
1
%RH [0 to 20]
Alarm Generation:
Enable
Apply
Cancel
Link 1 | Link 2 | Link 3
Managed Rack PDU

Konfigurieren von Temperatur- und Feuchtigkeitssensoren

Befehlsfolge: Environment > Temperature & Humidity

Wenn ein Temperatur- oder Feuchtigkeitssensor an die Rack PDU angeschlossen ist, können Sie über die Seite **Temperature & Humidity** (Temperatur und Feuchtigkeit) Grenzwerte für die Auslösung von Alarmen der Kategorie „Warnung“ oder „Kritisch“ festlegen (Einzelheiten zu diesen beiden Alarmkategorien finden Sie unter Symbole für den Gerätestatus).

Für die Temperatur:

- Wenn der Grenzwert für zu hohe Temperatur erreicht wird, erzeugt das System einen Alarm der Kategorie „Warnung“.
- Wenn der Grenzwert für die Höchsttemperatur erreicht wird, erzeugt das System einen Alarm der Kategorie „Kritisch“.

Ähnlich verhält es sich für die Feuchtigkeit:

- Wenn der Grenzwert für zu niedrige Feuchtigkeit erreicht wird, erzeugt das System einen Alarm der Kategorie „Warnung“.
- Wenn der Grenzwert für die Mindestfeuchtigkeit erreicht wird, erzeugt das System einen Alarm der Kategorie „Kritisch“.

Klicken Sie auf das Thermometer-Symbol in der rechten oberen Ecke, um zwischen Fahrenheit und Celsius umzuschalten.

So konfigurieren Sie Temperatur- und Feuchtigkeitssensoren:

1. Geben Sie Grenzwerte für Minimal- und Maximalwerte sowie für zu hohe und zu niedrige Werte ein.
2. Geben Sie **Hysterese**werte ein. (Einzelheiten hierzu finden Sie unter Hysterese.)
3. Aktivieren Sie die Alarmerzeugung nach Ihren Vorstellungen.
4. Klicken Sie auf **Apply** (Übernehmen).

Hysterese. Mit diesem Wert wird festgelegt, wie weit sich die Temperatur oder Luftfeuchtigkeit nach einer Grenzwertverletzung wieder unterhalb des Grenzwerts bewegen muss, damit die Grenzwertverletzung gelöscht wird.

- Bei Verletzungen des Temperarurgrenzwerts „Höchstwert“ und „Hoch“ wird der Grenzwert abzüglich der Hysterese als Löschpunkt verwendet.
- Bei Verletzungen des Feuchtigkeitsgrenzwerts „Mindestwert“ und „Niedrig“ wird der Grenzwert zuzüglich der Hysterese als Löschpunkt verwendet.

Erhöhen Sie den Wert für die Temperatur-Hysterese oder die Luftfeuchtigkeits-Hysterese, um mehrfache Alarme zu vermeiden, wenn die Temperatur oder Luftfeuchtigkeit nach einer Grenzwertverletzung immer wieder leicht schwankt. Wenn der Hysteresewert zu niedrig ist, können durch solche Schwankungen wiederholt Grenzwertverletzungen ausgelöst und gelöscht werden.

Beispiel für eine steigende und zugleich schwankende Temperatur: Der Grenzwert für die Höchsttemperatur beträgt 85 °F und die Temperatur-Hysterese beträgt 3 °F. Die Temperatur steigt über 85 °F an, wodurch der Grenzwert verletzt wird. Danach schwankt die Temperatur wiederholt zwischen 84 °F und 86 °F, ohne dass es zu einem Löschereignis oder zu einer erneuten Grenzwertverletzung kommt. Damit die vorliegende Grenzwertverletzung gelöscht werden kann, müsste die Temperatur auf unter 82 °F abfallen (um 3 °F unter den Grenzwert).

Beispiel für eine abfallende und zugleich schwankende Luftfeuchtigkeit: Der Grenzwert für die Mindestluftfeuchtigkeit beträgt 18%, und die Luftfeuchtigkeits-Hysterese beträgt 8%. Die Luftfeuchtigkeit fällt auf unter 18% ab und verletzt somit dem Grenzwert. Danach schwankt die Luftfeuchtigkeit wiederholt zwischen 24% und 13%, ohne dass es zu einem Löschereignis oder zu einer erneuten Grenzwertverletzung kommt. Damit die vorliegende Grenzwertverletzung gelöscht werden kann, müsste die Luftfeuchtigkeit auf über 26% ansteigen (um 8% über den Grenzwert).

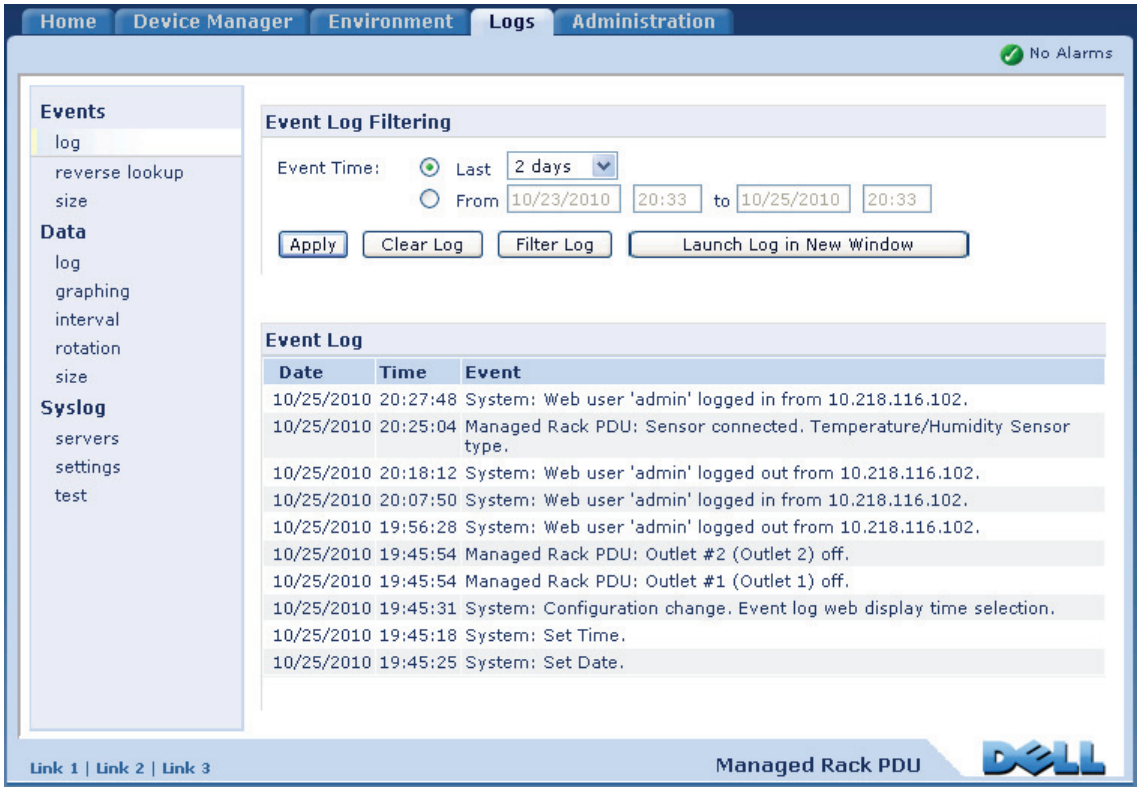
Konfigurieren potentialfreier Eingangskontakte

Befehlsfolge: Environment > Dry Contact Inputs

Über das Menü **Dry Contact Inputs** (Potentialfreie Eingangskontakte) können Sie sich den aktuellen Status und Zustand der potentialfreien Eingangskontakte ansehen und diese konfigurieren.

Parameter	Beschreibung
Name	Der Name dieses Eingangskontakts. *Maximum*: 20 Zeichen.
Alarmzustand	**Normal**, wenn dieser Eingangskontakt keinen Alarm meldet, bzw. der Schweregrad des Alarms, wenn dieser Eingangskontakt einen Alarm meldet.
Status	Der aktuelle Schaltzustand dieses Eingangskontakts: **Closed** (Geschlossen) oder **Open** (Geöffnet)
Alarm Generation (Alarmerzeugung)	Hiermit aktivieren oder deaktivieren Sie diesen Eingangskontakt. Ein deaktivierter Kontakt erzeugt auch bei einem abnormen Schaltzustand niemals einen Alarm.
Normal State (Normalzustand)	Der Normalzustand dieses Eingangskontakts (bei Nichtvorliegen eines Alarms): **Closed** (Geschlossen) oder **Open** (Geöffnet)

Protokolle


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

Daten- und Ereignisprotokolle

Ereignisprotokoll

Befehlsfolge: Logs > Events > *Optionen*

Sie können das Ereignisprotokoll anzeigen, filtern oder löschen. In der Grundeinstellung enthält das Protokoll alle Ereignisse, die während der letzten zwei Tage erfasst wurden, und zwar in umgekehrter chronologischer Reihenfolge.

Um eine Liste aller konfigurierbaren Ereignisse mit ihren aktuellen Einstellungen angezeigt zu bekommen, klicken Sie im linken Navigationsmenü auf die Registerkarte **Administration**, wählen Sie dann **Notification** (Benachrichtigung) und klicken Sie anschließend unter **Event Actions** (Ereignisaktionen) auf **by event** (nach Ereignis).

Siehe Konfigurieren nach Ereignis.

So zeigen Sie das Ereignisprotokoll an (Logs > Events > Protokoll):

- Das Ereignisprotokoll wird grundsätzlich als Seite auf der Web-Oberfläche angezeigt. Das neueste Ereignis wird auf Seite 1 angezeigt. In der Navigationsleiste unterhalb des Protokolls haben Sie folgende Möglichkeiten:
  - Klicken Sie auf eine Seitennummer, um eine bestimmte Seite des Protokolls zu öffnen.
  - Klicken Sie auf **Previous** (Zurück) oder **Next** (Weiter), um sich die Ereignisse anzusehen, die unmittelbar vor bzw. nach den auf der geöffneten Seite aufgeführten Ereignissen erfasst wurden.

– Klicken Sie auf **<<**, um zur ersten Seite zurückzukehren, oder klicken Sie auf **>>**, um sich die letzte Seite des Protokolls anzusehen.

- Wenn Sie sich die aufgeführten Ereignisse auf einer neuen Seite ansehen möchten, klicken Sie auf **Launch Log in New Window** (Protokoll in neuem Fenster öffnen). Das Protokoll wird dann in einer Vollbild-Ansicht angezeigt.

Damit die Schaltfläche **Launch Log in New Window** (Protokoll in neuem Fenster öffnen) funktioniert, muss JavaScript® in Ihrem Browser aktiviert sein.

Sie können sich das Ereignisprotokoll auch über FTP oder Secure CoPy (SCP) anzeigen lassen. Siehe Protokolldateien per FTP oder SCP abrufen.

So filtern Sie das Ereignisprotokoll (Logs > Events > Protokoll):

- **Filtern des Ereignisprotokolls nach Datum oder Uhrzeit:** Wenn Sie sich das gesamte Ereignisprotokoll anzeigen lassen möchten oder die Anzahl der Tage oder Wochen ändern möchten, für die im Ereignisprotokoll die jüngsten Ereignisse angezeigt werden, wählen Sie die Option **Last** (Letzte). Wählen Sie aus dem Dropdown-Listenfeld einen Zeitraum aus und klicken Sie dann auf **Apply** (Übernehmen). Die Filterkonfiguration bleibt gespeichert, bis die Rack PDU neu gestartet wird.
  Wenn Sie sich Ereignisse ansehen möchten, die während eines bestimmten Zeitraums erfasst wurden, wählen Sie die Option **From** (Von). Geben Sie die Anfangs- und Endzeiten (im 24-Stunden-Zeitformat) und die Tage an, für die Ereignisse angezeigt werden sollen, klicken Sie dann auf **Apply** (Übernehmen). Die Filterkonfiguration bleibt gespeichert, bis die Rack PDU neu gestartet wird.
- **Filtern des Protokolls nach Ereignissen**: Klicken Sie auf **Filter Log** (Protokoll filtern), um festzulegen, welche Ereignisse im Protokoll angezeigt werden sollen. Wenn Sie eine Ereigniskategorie oder einen Alarm-Schweregrad aus der Ansicht entfernen möchten, entfernen Sie das Häkchen aus dem daneben angezeigten Kontrollkästchen. Text in der rechten oberen Ecke des Ereignisprotokolls bedeutet, dass ein Filter aktiv ist.

Wenn Sie als Administrator angemeldet sind, klicken Sie auf **Save As Default** (Als Standard speichern), um diesen Filter als Protokoll-Standardansicht für alle Benutzer zu speichern. Wenn Sie nicht auf **Save As Default** (Als Standard speichern) klicken, bleibt der Filter aktiv, bis Sie ihn löschen oder die Rack PDU neu gestartet wird. Wenn Sie einen aktiven Filter entfernen möchten, klicken Sie auf **Filter Log** (Protokoll filtern) und anschließend auf **Clear Filter (Show All)** (Filter löschen (Alle zeigen)).

Zum Filtern von Ereignissen wird eine **ODER**-Logik angewandt.

- Ereignisse, die Sie nicht in der Liste **Filter by Category** (Nach Schweregrad filtern) ausgewählt haben, werden niemals im gefilterten Ereignisprotokoll angezeigt, selbst wenn das Ereignis in einer von Ihnen in der Liste **Filter by Category** (Nach Kategorie filtern) ausgewählten Kategorie eingetreten ist.
- Ereignisse, die Sie nicht in der Liste **Filter by Category** (Nach Kategorie filtern) ausgewählt haben, werden niemals im gefilterten Ereignisprotokoll angezeigt, selbst wenn Einheiten aus der betreffenden Kategorie einen von Ihnen in der Liste **Filter by Severity** (Nach Schweregrad filtern) ausgewählten Alarmzustand an das Protokoll übergeben haben.

So löschen Sie das Protokoll (Logs > Events > Protokoll):

Wenn Sie alle im Protokoll erfassten Ereignisse löschen möchten, klicken Sie auf der Webseite, auf der das Protokoll angezeigt wird, auf **Clear Log** (Protokoll löschen). Gelöschte Ereignisse können nicht wiederhergestellt werden.

Eine Anleitung zum Deaktivieren der Protokollierung von Ereignissen auf der Basis ihres Schweregrads oder ihrer Ereigniskategorie finden Sie unter Konfigurieren nach Ereignis.

So konfigurieren Sie umgekehrte Suchen (Logs > Events > Umgekehrte Suche):

Umgekehrte Suchen sind in der Grundeinstellung deaktiviert. Aktivieren Sie diese Funktion nur, wenn Sie keinen DNS-Server konfiguriert haben oder wenn sich das Netzwerk aufgrund zu starken Datenverkehrs träge verhält.

Wenn die Option „Umgekehrte Suche“ aktiviert ist, wird beim Eintreten eines Netzwerk-Ereignisses sowohl die IP-Adresse als auch der Domänennamen der für das Ereignis relevanten Netzwerkeinheit im Ereignisprotokoll erfasst. Wenn kein Domänennamen für die Einheit existiert, wird nur ihre IP-Adresse zusammen mit dem Ereignis protokolliert. Da sich Domänennamen im Allgemeinen weniger oft ändern als IP-Adressen, lassen sich die Adressen von Netzwerkeinheiten, die entsprechende Ereignisse auslösen, bei aktivierter umgekehrter Suche häufig leichter identifizieren.

So ändern Sie die Größe des Ereignisprotokolls (Logs > Events > Größe):

In der Grundeinstellung werden im Ereignisprotokoll 400 Ereignisse gespeichert. Sie können die Anzahl der im Protokoll gespeicherten Ereignissen ändern. Wenn Sie die Größe des Ereignisprotokolls ändern, werden alle bestehenden Protokolleinträge gelöscht. Rufen Sie die Protokolldatei zunächst per FTP oder SCP ab, um keine Protokolldaten zu verlieren, bevor Sie einen neuen Wert in das Feld **Ereignisprotokollgröße** eingeben.

Siehe Protokolldateien per FTP oder SCP abrufen.

Wenn das Protokoll voll ist, werden ältere Einträge gelöscht.

Datenprotokoll

Befehlsfolge: Logs > Data > *Optionen*

Im Datenprotokoll werden in festgelegten Intervallen die Stromstärke und Leistung des Geräts und seiner Phasen erfasst (Letzteres nur bei dreiphasigen Rack PDUs), ebenso Daten zur Temperatur, Feuchtigkeit und den potentialfreien Kontakten. Die Einträge werden nach Datum und Uhrzeit der Datenerfassung geordnet.

So zeigen Sie das Datenprotokoll an (Protokolle > Daten > Protokoll):

- Das Datenprotokoll wird grundsätzlich als Seite auf der Web-Oberfläche angezeigt. Das neueste Datenelement wird auf Seite 1 angezeigt. Im Navigationsmenü unterhalb des Protokolls haben Sie folgende Möglichkeiten:
  - Klicken Sie auf eine Seitennummer, um eine bestimmte Seite des Protokolls zu öffnen.
  - Klicken Sie auf **Previous** (Zurück) oder **Next** (Weiter), um sich die Datenelemente anzusehen, die unmittelbar vor bzw. nach den auf der geöffneten Seite aufgeführten Datenelementen erfasst wurden.
  - Klicken Sie auf **<<**, um zur ersten Seite des Protokolls zurückzukehren, oder klicken Sie auf **>>**, um sich die letzte Seite des Protokolls anzusehen.
- Wenn Sie sich die aufgeführten Datenelemente auf einer neuen Seite ansehen möchten, klicken Sie auf **Launch Log in New Window** (Protokoll in neuem Fenster öffnen). Das Protokoll wird dann in einer Vollbild-Ansicht angezeigt.

Damit die Schaltfläche **Launch Log in New Window** (Protokoll in neuem Fenster öffnen) funktioniert, muss JavaScript in Ihrem Browser aktiviert sein.

Sie können sich das Datenprotokoll auch über FTP oder SCP anzeigen lassen. Siehe Protokolldateien per FTP oder SCP abrufen.

So filtern Sie das Datenprotokoll nach Datum oder Uhrzeit (Logs > Data > Protokoll):

Wenn Sie sich das gesamte Datenprotokoll anzeigen lassen möchten oder die Anzahl der Tage oder Wochen ändern möchten, für die im Ereignisprotokoll die jüngsten Ereignisse angezeigt werden, wählen Sie die Option **Last** (Letzte). Wählen Sie aus dem Dropdown-Listenfeld einen Zeitraum aus und klicken Sie dann auf **Apply** (Übernehmen). Die Filterkonfiguration bleibt gespeichert, bis die Einheit neu gestartet wird.

Wenn Sie sich Datenelemente ansehen möchten, die während eines bestimmten Zeitraums erfasst wurden, wählen Sie die Option **From** (Von). Geben Sie die Anfangs- und Endzeiten (im 24-Stunden-Zeitformat) und die Tage an, für die Datenelemente angezeigt werden sollen, klicken Sie dann auf **Apply** (Übernehmen). Die Filterkonfiguration bleibt gespeichert, bis die Einheit neu gestartet wird.

So löschen Sie das Datenprotokoll:

Wenn Sie alle im Protokoll erfassten Datenelemente löschen möchten, klicken Sie auf der Webseite, auf der das Protokoll angezeigt wird, auf **Clear Data Log** (Datenprotokoll löschen). Gelöschte Daten können nicht wiederhergestellt werden.

So legen Sie das Intervall für die Erfassung der Daten fest (Logs > Data > Intervall):

Legen Sie mittels der Einstellung **Log Interval** (Protokollintervall) fest, wie oft Daten abgerufen und im Datenprotokoll gespeichert werden sollen, und sehen Sie sich die Berechnung des Erfassungszeitraums in Tagen an, der auf der Basis des von Ihnen ausgewählten Intervalls im Protokoll gespeichert werden kann. Wenn das Protokoll voll ist, werden ältere Einträge gelöscht. Wenn ältere Daten nicht automatisch gelöscht werden sollen, müssen Sie die Datenprotokollrotation aktivieren und konfigurieren, wie im folgenden Abschnitt beschrieben.

So konfigurieren Sie die Datenprotokollrotation (Logs > Data > Rotation):

Sie können ein kennwortgeschütztes Datenprotokoll-Archiv auf einem FTP-Server anlegen. Bei aktivierter Rotation wird der Inhalt des Datenprotokolls an eine Datei angehängt, deren Name und Speicherort von Ihnen festgelegt wird. Die Aktualisierung dieser Datei erfolgt in dem von Ihnen angegebenen Upload-Intervall.

Parameter	Beschreibung
Data Log Rotation	Hiermit aktivieren oder deaktivieren Sie die Datenprotokollrotation (in der Standardeinstellung).
FTP Server Address	Die Adresse des FTP-Servers, auf dem das Datenarchiv gespeichert wird.
User Name	Der Benutzername, der zum Senden von Daten an die Archivdatei benötigt wird. Dieser Benutzer muss außerdem Lese- und Schreibzugriff auf die Archivdatei und den Ordner haben, in dem diese gespeichert werden soll.
Password	Das Passwort, das zum Senden von Daten an die Archivdatei benötigt wird.
File Path	Der Pfad zur Archivdatei.
Filename	Der Name der Archivdatei (eine ASCII-Textdatei).
Delay *X* hours between uploads.	Der Abstand in Stunden, in dem Daten in die Datei übertragen werden.
Upload every *X* minutes	Die Zeit in Minuten, die nach einer fehlgeschlagenen Datenübertragung abgewartet wird, bevor erneut versucht wird, die Daten in die Datei zu schreiben.
Up to *X* times	Wie oft die Übertragung wiederholt wird, nachdem ein Übertragungsfehler erstmals eingetreten ist.
Until Upload Succeeds	Mit dieser Option wird versucht, die Daten immer wieder hochzuladen, bis die Übertragung erfolgreich verläuft.

So ändern Sie die Größe des Datenprotokolls (Logs > Data > Größe):

In der Grundeinstellung werden im Datenprotokoll 1000 Datenelemente gespeichert. Sie können die Anzahl der im Protokoll gespeicherten Datenelemente ändern. Wenn Sie die Größe des Datenprotokolls ändern, werden alle bestehenden Protokolleinträge gelöscht. Rufen Sie die Protokolldatei zunächst per FTP oder SCP ab, um keine Datensätze zu verlieren, bevor Sie einen neuen Wert in das Feld **Data Log Size** (Datenprotokollgröße) eingeben.

Siehe Protokolldateien per FTP oder SCP abrufen.

Wenn das Protokoll voll ist, werden ältere Einträge gelöscht.

Protokolldateien per FTP oder SCP abrufen

Administratoren und Benutzer „Gerät“ können eine Ereignisprotokolldatei (*event.txt*) bzw. Datenprotokolldatei (*data.txt*) mit Tabulatortrennung per FTP oder SCP abrufen und diese in eine Tabelle importieren.

- Diese Datei enthält alle Ereignisse oder Datenelemente, die seit dem letzten Löschen oder (im Falle des Datenprotokolls) Abkürzens der Datei bei Überschreitung ihrer Maximalgröße erfasst wurden.
- Diese Datei enthält Informationen, die im Ereignisprotokoll oder im Datenprotokoll nicht angezeigt werden.
  - die Version des Dateiformats (erstes Feld)
  - Datum und Uhrzeit des erstmaligen Abrufs der Datei
  - den **Namen**, **Ansprechpartner** und **Standort** sowie die IP-Adresse der Rack PDU
  - den eindeutigen **Ereigniscode** zu jedem erfassten Ereignis (nur in der Datei *event.txt*).

Die Rack PDU verwendet vierstellige Jahresangaben für Protokolleinträge. Unter Umständen müssen Sie in Ihrem Tabellenkalkulationsprogramm das Datumsformat auf vier Ziffern einstellen, damit das Datum vollständig angezeigt wird.

Falls Sie für Ihr System die verschlüsselten Sicherheitsprotokolle verwenden, verwenden Sie zum Abrufen der Protokolldatei Secure CoPy (SCP).
Falls Sie unverschlüsselte Authentifizierungsmethoden im Kontext der Systemsicherheit verwenden, verwenden Sie zum Abrufen der Protokolldatei FTP.

Weitere Informationen zu verfügbaren Protokollen und Methoden zur Einrichtung des gewünschten Sicherheitsniveaus finden Sie in Anhang B: Sicherheitshandbuch.

Abrufen der Dateien mittels SCP. Zum Abrufen der Datei *event.txt* per SCP verwenden Sie den folgenden Befehl:

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

Zum Abrufen der Datei *data.txt* per SCP verwenden Sie den folgenden Befehl:

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

Abrufen der Dateien mittels FTP. So rufen Sie die Datei *event.txt* oder *data.txt* per FTP ab:

1. Geben Sie in einer Befehlszeile **`ftp`** und die IP-Adresse der Rack PDU ein und drücken Sie die EINGABETASTE.

   Wenn die **Port**-Einstellung für den **FTP-Server** verändert wurde (über das Menü **Network** auf der Registerkarte **Administration**), sodass die Voreinstellung (**21**) nicht mehr gilt, müssen Sie im FTP-Befehl den geänderten, nicht standardmäßigen Wert verwenden. Für Windows FTP-Clients verwenden Sie den nachfolgenden Befehl, einschließlich der Leerzeichen. (Bei einigen FTP-Clients müssen Sie zwischen der IP-Adresse und der Port-Nummer einen Doppelpunkt statt eines Leerzeichens verwenden.)

   `ftp>open ip_adresse port_numner`

   Informationen zum Festlegen eines Nicht-Standard-Ports für den FTP-Server als zusätzliche Sicherheitsmaßnahme finden Sie unter FTP Server. Sie können einen beliebigen Port zwischen 5001 und 32768 festlegen.

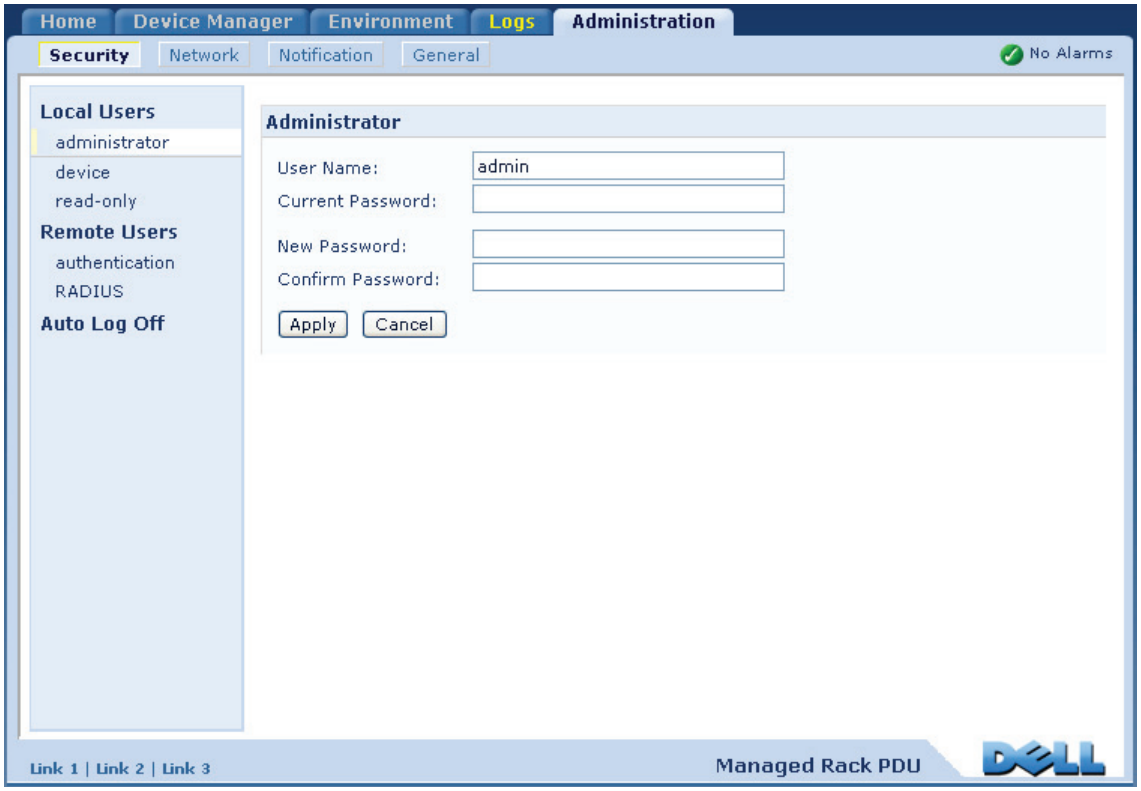
2. Als Administrator oder Benutzer „Gerät“ müssen Sie sich unter Beachtung der Groß-/Kleinschreibung mit Ihrem **Benutzernamen** und **Passwort** anmelden. Für Administratoren ist standardmäßig **admin** als **Benutzername** und **Passwort** vorgegeben. Für den Benutzer „Gerät“ ist standardmäßig **device** als **Benutzername** und **Passwort** vorgegeben.
3. Verwenden Sie den Befehl **get**, um den Text aus einem Protokoll auf die lokale Festplatte zu übertragen.

   `ftp>get event.txt`

   oder

   `ftp>get data.txt`
4. Geben Sie an der Befehlszeile **`ftp> quit`** ein, um FTP zu beenden.

Verwaltung: Sicherheit



Lokale Benutzer

Einrichten von Zugriffsrechten

Befehlsfolge: Administration > Security > Local Users > *Optionen*

Über das Benutzerkonto eines Administrators kann immer auf die Rack PDU zugegriffen werden.

Die Kontotypen „Benutzer 'Gerät'“ und „Benutzer 'schreibgeschützt'“ sind in der Voreinstellung aktiviert. Zum Deaktivieren des Kontotyps „Benutzer 'Gerät'“ oder „Benutzer 'schreibgeschützt'“ wählen Sie das betreffende Benutzerkonto im linken Navigationsmenü aus und entfernen Sie dann das Häkchen aus dem Kontrollkästchen **Enable** (Aktivieren).

Auf die gleiche Weise legen Sie unter Beachtung der Groß-/Kleinschreibung den Benutzernamen und das Passwort für die einzelnen Kontotypen fest. Die maximale Länge eines Benutzernamens oder Passworts darf maximal 64 Zeichen betragen. Leere Passwörter (Passwörter, die keine Zeichen enthalten), sind nicht zulässig.

Informationen zu den Berechtigungen, die Sie den einzelnen Kontotypen erteilen können, finden Sie unter Benutzerkontotypen.

Für Benutzer mit dem Kontotyp „Ausgangsanschluss“ sind Benutzername und Passwort nicht voreingestellt. Bei einem Benutzer mit dem Kontotyp „Ausgangsanschluss“ muss ein Administrator den Benutzernamen, das Passwort und weitere Kontoeigenschaften festlegen. Siehe Konfigurieren eines Benutzern „Ausgangsanschluss“.

Kontotyp	Standard-Benutzername	Standard-Passwort	Erlaubter Zugriff
Administrator	admin	admin	Web-Oberfläche und Befehlszeile
Benutzer „Gerät“	device	device	
Benutzer „schreibgeschützt“	readonly	readonly	Nur Web-Oberfläche

Remote-Benutzer

Authentifizierung

Befehlsfolge: Administration > Security > Remote Users > Authentication Method

Verwenden Sie diese Option, um auszuwählen, wie der Fernzugriff auf die Rack PDU verwaltet werden soll.

Informationen zur lokalen Authentifizierung (also ohne zentralisierte Authentifizierung über einen RADIUS-Server) finden Sie in Anhang B: Sicherheitshandbuch.

Die Rack PDU unterstützt die Authentifizierungs- und Autorisierungsfunktionen von RADIUS (Remote Authentication Dial-In User Service).

- Wenn ein Benutzer auf die Rack PDU oder eine andere RADIUS-fähige Netzwerkeinheit zugreift, wird eine Authentifizierungsanfrage an den RADIUS-Server gesendet, um die Zugriffsebene des Benutzers festzustellen.
- Für die Rack PDU verwendete RADIUS-Benutzernamen dürfen maximal 32 Zeichen enthalten.

Wählen Sie eine der folgenden Möglichkeiten:

- **Local Authentication Only**: RADIUS ist deaktiviert. Lokale Authentifizierung ist aktiviert.
- **RADIUS, then Local Authentication**: RADIUS-Authentifizierung und lokale Authentifizierung sind aktiviert. Die Authentifizierung wird zuerst beim RADIUS-Server angefordert. Wenn der RADIUS-Server nicht reagiert, wird die lokale Authentifizierung verwendet.
- **RADIUS Only**: RADIUS ist aktiviert. Lokale Authentifizierung ist deaktiviert.

Wenn **RADIUS Only** (Nur RADIUS) ausgewählt ist und wenn der RADIUS-Server nicht verfügbar ist, nicht richtig identifiziert wurde oder falsch konfiguriert ist, steht der Fernzugriff nicht zur Verfügung, unabhängig vom Benutzerkontotyp. In diesem Fall müssen Sie über die serielle Schnittstelle eine Befehlszeile öffnen und die **Zugriffseinstellung** in **local** oder **radiusLocal** umändern, um wieder Zugriff zu erhalten. Mit dem folgenden Befehl können Sie die Zugriffseinstellung beispielsweise in **local** umändern:

```
radius -a local
```

RADIUS

Befehlsfolge: Administration > Security > Remote Users > RADIUS

Diese Option bietet folgende Möglichkeiten:

- Die für die Rack PDU verfügbaren RADIUS-Server (maximal zwei) und ihre jeweiligen Timeout-Werte anzeigen.
- Auf einen Link klicken und die Parameter für die Authentifizierung über einen neuen RADIUS-Server konfigurieren.
- Auf einen der aufgeführten RADIUS-Server klicken und dessen Parameter anzeigen und ändern.

RADIUS-Einstellung	Beschreibung
RADIUS Server	Der Servername oder die IP-Adresse (IPv4 oder IPv6) des RADIUS-Servers. Klicken Sie auf einen Link, um den Server zu konfigurieren. **HINWEIS:**RADIUS-Server verwenden normalerweise Port 1812, um Benutzer zu authentifizieren. Wenn Sie einen anderen Port verwenden möchten, hängen Sie an den Namen des RADIUS-Servers oder an dessen IP-Adresse einen Doppelpunkt an, gefolgt von der neuen Port-Nummer.
Secret	Der vom RADIUS-Server und der Rack PDU verwendete geheime Schlüssel.

RADIUS-Einstellung	Beschreibung
Timeout	Die Zeit in Sekunden, die die Rack PDU auf eine Antwort vom RADIUS-Server wartet.
Test Settings	Geben Sie den Benutzernamen und das Passwort des Administrators sein, um den Pfad zu dem von Ihnen konfigurierten RADIUS-Server zu testen.
Skip Test and Apply	Hiermit wird der Test des Pfads zum RADIUS-Server unterlassen.

Konfigurieren des RADIUS-Servers

Das Konfigurationsverfahren im Überblick

Sie müssen den RADIUS-Server konfigurieren, um mit der Rack PDU arbeiten zu können.

Beispiele für die RADIUS-Benutzerdatei mit Vendor Specific Attributes (VSAs) und ein Beispiel für einen Eintrag in der Wörterbuchdatei auf dem RADIUS-Server finden Sie in Anhang B: Sicherheitshandbuch.

1. Hinzufügen der IP-Adresse der Rack PDU zur Client-Liste des RADIUS-Servers (Datei).
2. Zu jedem Benutzer muss ein Diensttyp-Attribut konfiguriert werden, sofern keine Vendor Specific Attributes (VSA) definiert sind. Wenn keine Diensttyp-Attribute konfiguriert sind, haben die Benutzer schreibgeschützten Zugriff (nur über die Web-Oberfläche).

   Informationen zur Radius-Benutzerdatei finden Sie in der Dokumentation zum RADIUS-Server und in Anhang B: Sicherheitshandbuch.

3. Statt der vom RADIUS-Server bereitgestellten Diensttyp-Attribute können auch VSA verwendet werden. Für VSA wird ein Wörterbucheintrag und eine RADIUS-Benutzerdatei benötigt. Definieren Sie in der Wörterbuchdatei die Bezeichnungen für die Schlüsselwörter ATTRIBUTE und VALUE, nicht jedoch für die numerischen Werte. Wenn Sie die numerischen Werte ändern, kann keine RADIUS-Authentifizierung und -Autorisierung durchgeführt werden. VSA haben Vorrang vor den standardmäßigen RADIUS-Attributen.

Konfigurieren eines RADIUS-Servers unter UNIX® mit Shadow-Passwörtern

Bei Verwendung von UNIX-Shadow-Passwortdateien (/etc/passwd) in Verbindung mit RADIUS-Wörterbuchdateien können Benutzer mit den beiden folgenden Methoden authentifiziert werden:

- Wenn alle UNIX-Benutzer über Administratorrechte verfügen, tragen Sie die nachstehenden Zeilen in die RADIUS-Benutzerdatei „user“ ein. Wenn die Berechtigung nur für den Benutzer „Gerät“ gelten soll, ändern Sie den DELL-Diensttyp („DELL-Service-Type“) in **`Device`** um.

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

- Fügen Sie Benutzernamen und Attribute in die RADIUS-Benutzerdatei „user“ ein und gleichen Sie das Passwort mit /etc/passwd ab. Das folgende Beispiel gilt für die Benutzer **`bconners`** und **`thawk`**:

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

Unterstützte RADIUS-Server

Das Produkt unterstützt FreeRADIUS und Microsoft IAS 2003. Andere gängige RADIUS-Anwendungen funktionieren möglicherweise auch, wurden jedoch von uns nicht eingehend getestet.

Timeout bei Inaktivität

Befehlsfolge: Administration > Security > Auto Log Off

Mit dieser Option konfigurieren Sie die Zeit (in der Voreinstellung drei Minuten), die das System abwartet, bevor es einen inaktiven Benutzer automatisch abmeldet. Wenn Sie diesen Wert ändern, müssen Sie sich abmelden, damit die Änderung wirksam wird.

Die Abmeldeuhr läuft weiter, wenn ein Benutzer das Browser-Fenster schließt, ohne sich zuvor durch Klicken auf die Schaltfläche **Log Off** (Abmelden) rechts oben abzumelden. Da ein solcher Benutzer weiterhin als angemeldet gilt, kann sich vor Ablauf der im Feld **Minutes of Inactivity** (Inaktivität in Minuten) festgelegten Wartezeit kein anderer Benutzer anmelden. Wenn beispielsweise für **Minutes of Inactivity** (Inaktivität in Minuten) der Standardwert gilt und ein Benutzer das Browser-Fenster schließt, ohne sich vorher abzumelden, kann sich danach drei Minuten lang kein anderer Benutzer anmelden.

Verwaltung: Benachrichtigung

Ereignisaktionen

Befehlsfolge: Administration > Notification > Event Actions > *Optionen*

Benachrichtigungsarten

Sie können Ereignisaktionen konfigurieren, die als Reaktion auf ein Ereignis oder eine Gruppe von Ereignissen durchgeführt werden. Durch diese Aktionen können Benutzer auf unterschiedliche Art und Weise über das Ereignis in Kenntnis gesetzt werden:

- Aktive, automatische Benachrichtigung. Die angegebenen Benutzer oder Überwachungsgeräte werden direkt kontaktiert.
  - E-Mail-Benachrichtigung
  - SNMP-Traps
  - Syslog-Benachrichtigung
- Indirekte Benachrichtigung
  - Ereignisprotokoll. Wenn keine direkte Benachrichtigung konfiguriert ist, muss der Benutzer im Protokoll nachsehen, ob Ereignisse eingetreten sind.

    Zur Überwachung bestimmter Geräte können Sie auch Daten zum Systemverhalten protokollieren. Informationen zur Konfiguration und Verwendung dieser Datenerfassungsoption finden Sie unter Datenprotokoll.
  - Abfragen (SNMP GETs)

    Weitere Informationen finden Sie unter SNMP. Über SNMP kann ein NMS in die Lage versetzt werden, Datenabfragen durchzuführen. Bei Verwendung von SNMPv1, das Daten unverschlüsselt überträgt, können Datenabfragen durch Konfigurieren des restriktivsten SNMP-Zugriffstyps (READ) ohne die Gefahr einer Konfigurationsänderung per Fernzugriff zugelassen werden.

Konfigurieren von Ereignisaktionen

Benachrichtigungsparameter. Wie in den folgenden beiden Abschnitten beschrieben, können Sie für Ereignisse mit zugehörigem Löschereignis beim Konfigurieren von einzelnen Ereignissen oder Ereignisgruppen auch die nachstehend beschriebenen Parameter einstellen. Zum Öffnen dieser Parameter klicken Sie auf den Namen des Adressaten bzw. Empfängers.

Parameter	Beschreibung
Delay *x* time before sending	Wenn das Ereignis während der angegebenen Zeit andauert, wird eine Benachrichtigung gesendet. Wenn dieser Zustand vor Ablauf der angegebenen Zeit endet, wird keine Benachrichtigung gesendet.
Repeat at an interval of *x* time	Die Benachrichtigung wird im angegebenen Intervall wiederholt gesendet (alle 2 Minuten).
Up to *x* times	Während eines aktiven Ereignisses wird die Benachrichtigung mit der hier angegebenen Häufigkeit wiederholt.
Until condition clears	Die Benachrichtigung wird wiederholt gesendet, bis der Zustand endet oder behoben wird.

Konfigurieren nach Ereignis. So definieren Sie Ereignisaktionen für ein einzelnes Ereignis:

1. Klicken Sie in der oberen Menüleiste auf die Registerkarte **Administration** anschließend auf **Notification** (Benachrichtigung), und klicken Sie dann im linken Navigationsmenü unter **Event Actions** (Ereignisaktionen) auf **by event** (Nach Ereignis).
2. Überprüfen Sie in der Ereignisliste die markierten Spalten, um festzustellen, ob die von Ihnen gewünschte Aktion bereits konfiguriert ist. (In der Grundeinstellung ist die Protokollierung für alle Ereignisse konfiguriert.)

3. Klicken Sie auf den Ereignisnamen, um sich die aktuelle Konfiguration anzusehen. Hierzu gehören beispielsweise die per E-Mail zu benachrichtigenden Empfänger oder die durch SNMP-Traps zu benachrichtigenden Netzwerkmanagementsysteme (NMS).

Wenn kein Syslog-Server konfiguriert ist, werden für die Syslog-Konfiguration relevante Elemente nicht angezeigt.

Auf der Anzeigeseite mit den Einzelheiten zu einer Ereigniskonfiguration können Sie die Konfiguration ändern, die Ereignisprotokollierung bzw. Syslog-Erfassung aktivieren oder deaktivieren und die Benachrichtigung bestimmter E-Mail-Empfänger oder Trap-Adressaten deaktivieren, jedoch keine Empfänger bzw. Adressaten hinzufügen oder löschen. Informationen zum Hinzufügen oder Entfernen von Empfängern bzw. Adressaten finden Sie in den folgenden Abschnitten:

- Identifizierung von Syslog-Servern
- E-Mail-Empfänger
- Trap-Empfänger

Konfigurieren nach Gruppe. So konfigurieren Sie mehrere Ereignisse gleichzeitig als Gruppe:

1. Klicken Sie in der oberen Menüleiste auf die Registerkarte **Administration** anschließend auf **Notification** (Benachrichtigung), und klicken Sie dann im linken Navigationsmenü unter **Event Actions** (Ereignisaktionen) auf **by group** (Nach Gruppe).

2. Wählen Sie eine Methode zum Gruppieren von Ereignissen für die Konfiguration:
   - Wählen Sie **Grouped by severity** (Nach Schweregrad gruppiert), und wählen Sie dann alle Ereignisse aus, die mindestens einem Schweregrad zugeordnet sind. Sie können den Schweregrad eines Ereignisses nicht ändern.
   - Wählen Sie **Grouped by category** (Nach Kategorie gruppiert), und wählen Sie dann alle Ereignisse aus, die mindestens einer vordefinierten Kategorie zugeordnet sind.
3. Klicken Sie auf **Next>>** (Weiter), um zur jeweils nächsten Seite zu gelangen und folgende Einstellungen vorzunehmen:

   a. Auswählen von Ereignisaktionen für die Ereignisgruppe.
   - Damit Sie weitere Vorgänge neben **Protokollierung** (die Voreinstellung) auswählen können, müssen Sie zuerst mindestens einen relevanten Empfänger bzw. Adressaten konfigurieren.
   - Wenn Sie die Option **Logging** (Protokollierung) wählen und einen Syslog-Server konfiguriert haben, wählen Sie auf der nächsten Seite **Event Log** (Ereignisprotokoll) oder **Syslog**(Systemprotokoll), oder wählen Sie beides.

   b. Geben Sie an, ob die neue konfigurierte Ereignisaktion für diese Ereignisgruppe aktiviert bleiben sollen, oder ob die Aktion deaktiviert werden soll.

Aktive, automatische, direkte Benachrichtigung

E-Mail-Benachrichtigung

Das Einrichtungsverfahren im Überblick. Über das Simple Mail Transfer Protocol (SMTP) können Sie beim Eintreten eines Ereignisses eine E-Mail an bis zu vier Empfänger senden.

Damit Sie die E-Mail-Funktion nutzen können, müssen Sie die folgenden Einstellungen festlegen:

- Die IP-Adressen des primären und gegebenenfalls vorhandenen sekundären DNS-Servers.

  Siehe DNS.

- Die IP-Adresse oder den DNS-Namen des **SMTP-Servers** sowie der **Absenderadresse**

  Siehe SMTP.

- Die E-Mail-Adressen von bis zu vier Empfängern.

  Weitere Informationen hierzu finden Sie unter E-Mail-Empfänger.

  Über die Einstellung **To Address** (Empfängeradresse) der Option **recipients** (Empfänger) können Sie den E-Mail-Versand an einen textfähigen Pager konfigurieren.

SMTP.

Befehlsfolge: Administration > Notification > E-mail > server

Einstellung	Beschreibung
Lokaler SMTP-Server	Die IPv4-/IPv6-Adresse oder der DNS-Name des lokalen SMTP-Servers. **HINWEIS:** Diese Definition ist nur erforderlich, wenn die Option **SMTP Server** auf **Local** eingestellt ist. Siehe E-Mail-Empfänger.
From Address	Der Inhalt des Felds **From** (Von) in E-Mail-Nachrichten, die von der Rack PDU gesendet werden: • Im Format *benutzer*@ [*IP-Adresse*] (falls eine IP-Adresse als **Lokaler SMTP-Server** angegeben wurde). • Im Format *benutzer@domaene* in den E-Mail-Nachrichten (falls DNS konfiguriert ist und der DNS-Name als **Lokaler SMTP-Server** angegeben wurde). **HINWEIS:** Damit diese Einstellung verwendet werden kann, verlangt der lokale SMTP-Server unter Umständen die Angabe eines gültigen, auf dem Server angelegten Benutzerkontos. Einzelheiten hierzu finden Sie in der Dokumentation zum Server.

E-Mail-Empfänger.

Befehlsfolge: Administration > Notification > E-mail > recipients

Hiermit geben Sie bis zu vier E-Mail-Empfänger an.

Einstellung	Beschreibung
To Address	Der Benutzer- und Domänenname des Empfängers. Zum Senden von E-Mails an einen Pager verwenden Sie die E-Mail-Adresse, die dem Pager-Gateway-Konto des Empfängers zugewiesen ist (z. B. **`myacct100@skytel.com`**). Das Pager-Gateway erstellt dann die Seite. Wenn Sie den DNS-Lookup nach der IP-Adresse des Mail-Servers umgehen möchten, geben Sie statt des E-Mail-Domänennamens die IP-Adresse in eckigen Klammern ein, z. B. jmeier@[xxx.xxx.x.xxx] statt jmeier@firma.com. Dies ist hilfreich, wenn die DNS-Lookups aus irgendeinem Grund nicht richtig funktionieren sollten. **HINWEIS:** Der Pager des Empfängers muss Textnachrichten verarbeiten können.
E-mail Generation	Hiermit aktivieren (Voreinstellung) oder deaktivieren Sie den E-Mail-Versand an den Empfänger.

Einstellung	Beschreibung

SMTP Server	Wählen Sie eine der folgenden Routing-Methoden für E-Mails aus:
	• **Lokal**: Über den SMTP-Server der Rack PDU. Dies ist die empfohlene Einstellung. Sie stellt sicher, dass die E-Mail vor Ablauf des 20-Sekunden-Timeouts der Rack PDU gesendet und der Sendevorgang mehrmals wiederholt wird, falls erforderlich. Nehmen Sie darüber hinaus auch eine der folgenden Einstellungen vor:
	  • Aktivieren Sie die Weiterleitung auf dem SMTP-Server der Rack PDU, damit diese E-Mails an externe SMTP-Server weiterleiten kann. SMTP-Server sind normalerweise nicht zum Weiterleiten von E-Mail konfiguriert. Halten Sie mit dem Administrator des SMTP-Servers Rücksprache, bevor Sie Weiterleitungen durch entsprechende Änderung der Konfiguration erlauben.
	  • Richten Sie ein spezielles E-Mail-Konto für die Rack PDU -ein, um E-Mails an externe E-Mail-Konten weiterleiten zu können.
	• **Empfänger**: Direkt an den SMTP-Server des Empfängers. Bei dieser Einstellung versucht die Rack PDU, die E-Mail nur ein einziges Mal zu senden. Bei einem sehr beschäftigten externen SMTP-Server kann der Timeout dazu führen, dass manche E-Mails nicht gesendet werden.
	Wenn der Empfänger den SMTP-Server der Rack PDU verwendet, bleibt diese Einstellung ohne Auswirkungen.

Format	Das lange Format enthält den Namen, den Standort, einen Ansprechpartner, die IP-Adresse, die Seriennummer des Geräts, Datum und Uhrzeit, den Ereigniscode und eine Beschreibung des Ereignisses. Das kurze Format enthält lediglich die Beschreibung des Ereignisses.
User Name Password Confirm Password	Geben Sie hier Ihren Benutzernamen und Ihr Passwort ein, wenn der Mail-Server eine Authentifizierung verlangt. Damit wird eine einfache Authentifizierung durchgeführt, kein SSI.

E-Mail-Test.

Befehlsfolge: Administration > Notification > E-mail > test

Hiermit senden Sie eine Test-Nachricht an einen konfigurierten Empfänger.

SNMP-Traps

Trap-Empfänger.

Befehlsfolge: Administration > Notification > SNMP Traps > trap receivers

Sie können sich Trap-Empfänger nach der IP-Adresse bzw. nach dem Host-Namen des NMS anzeigen lassen. Sie können bis zu sechs Trap-Empfänger konfigurieren.

- Zum Konfigurieren eines neuen Trap-Empfängers klicken Sie auf **Add Trap Receiver** (Trap-Empfänger hinzufügen).
- Zum Ändern oder Löschen eines Trap-Empfängers klicken Sie zuerst auf dessen IP-Adresse oder Hostnamen, um die dazugehörigen Einstellungen zu öffnen. (Wenn Sie einen Trap-Empfänger löschen, werden alle für diesen unter „Ereignisaktionen“ konfigurierten Benachrichtigungseinstellungen auf die Standardwerte zurückgesetzt.)
- Zum Festlegen des Trap-Typs für einen Trap-Empfänger klicken Sie auf das Optionsfeld „SNMPv1“ oder „SNMPv3“. Damit ein NMS beide Trap-Typen empfangen kann, müssen Sie für das betreffende NMS zwei Trap-Empfänger konfigurieren, einen für jeden Trap-Typ.

Element	Beschreibung
Trap Generation	Aktivieren (die Voreinstellung) oder deaktivieren Sie die Trap-Generierung für diesen Trap-Empfänger.
NMS IP/Host Name	Die IPv4-/IPv6-Adresse oder der Hostname dieses Trap-Empfängers. Mit der Voreinstellung 0.0.0.0 bleibt der Trap-Empfänger undefiniert.

SNMPv1-Option.

Element	Beschreibung
Community Name	Der Name (Voreinstellung: **`public`**) der als Kennung gesendet wird, wenn SNMPv1-Traps an diesen Trap-Empfänger gesendet werden.
Authenticate Traps	Wenn diese Option aktiviert ist (die Voreinstellung), empfängt das durch die Einstellung „NMS-IP/Host Name“ identifizierte NMS Authentifizierungs-Traps (Traps, die durch ungültige Anmeldeversuche auf diesem Gerät erzeugt werden). Zum Deaktivieren dieser Option löschen Sie das Häkchen aus dem Kontrollkästchen.

SNMPv3-Option. Hiermit wählen Sie die Kennung für das Benutzerprofil dieses Trap-Empfängers aus. (Zum Anzeigen der Einstellungen der Benutzerprofile, die durch die hier auswählbaren Benutzernamen identifiziert werden, wählen Sie in der oberen Menüleiste **Network** und im linken Navigationsmenü unter **SNMPv3** die Option **user profiles** (Benutzerprofile).)

Weitere Informationen zum Erstellen von Benutzerprofilen und zum Auswählen von Authentifizierungs- und Verschlüsselungsmethoden finden Sie unter SNMPv3.

SNMP-Trap-Test

Befehlsfolge: Administration > Notification > SNMP Traps > test

Letztes Testergebnis. Das Ergebnis des letzten SNMP-Trap-Tests. Durch einen erfolgreich verlaufenen SNMP-Trap-Test kann nur verifiziert werden, dass ein Trap gesendet wurde, nicht jedoch, dass der Trap beim ausgewählten Trap-Empfänger eingetroffen ist. Ein Trap-Test ist erfolgreich verlaufen, wenn alle nachfolgenden Bedingungen erfüllt sind:

- Die für den ausgewählten Trap-Empfänger konfigurierte SNMP-Version (SNMPv1 oder SNMPv3) ist auf diesem Gerät aktiviert.
- Der Trap-Empfänger ist aktiviert.
- Wenn ein Hostname als **Empfängeradresse** ausgewählt ist, kann dieser Hostname einer gültigen IP-Adresse zugeordnet werden.

An. Wählen Sie die IP-Adresse oder den Hostnamen aus, an den der SNMP-Trap gesendet werden soll. Wenn kein Trap-Empfänger konfiguriert ist, wird ein Link zur Konfigurationsseite **Trap-Empfänger** angezeigt.

Syslog

Befehlsfolge: Logs > Syslog > *Optionen*

Die Rack PDU kann beim Eintreten eines Ereignisses entsprechende Nachrichten an bis zu vier Syslog-Server senden. Auf den Syslog-Servern werden auf Netzwerkeinheiten eingetretene Ereignisse in einem zentralen Protokoll erfasst.

Dieses Benutzerhandbuch enthält keine eingehende Beschreibung zu Syslog und den dazugehörigen Konfigurationswerten. Weitere Informationen zu Syslog finden Sie in **RFC3164**.

Identifizierung von Syslog-Servern.

Befehlsfolge: Logs > Syslog > servers

Einstellung	Beschreibung
Syslog Server	Diese Einstellung verwendet IPv4-/IPv6-Adressen oder Hostnamen, um maximal vier Server zu identifizieren, die Syslog-Nachrichten der Rack PDU empfangen sollen.
Port	Der UDP-Port (User Datagram Protocol), der von der Rack PDU zum Übermitteln von Syslog-Meldungen verwendet wird. Die Voreinstellung lautet **514**; dies ist der normalerweise für Syslog reservierte UDP-Port.
Protokoll	Wählen Sie die Sprache für etwaige Syslog-Nachrichten aus.

Syslog-Einstellungen.

Befehlsfolge: Logs > Syslog > settings

Einstellung	Beschreibung
Message Generation	Hiermit aktivieren (Voreinstellung) oder deaktivieren Sie die Syslog-Funktion.
Facility Code	Hiermit wird der Anlagencode festgelegt, der den Syslog-Meldungen der Rack PDU zugeordnet werden (der Standardwert lautet **User**). **HINWEIS:** Der Einrichtungscode **User** definiert die von der Rack PDU gesendeten Syslog-Nachrichten am besten. Ändern Sie diese Einstellung **nicht**, es sei denn, Sie werden vom Syslog-Netzwerk oder vom Systemadministrator dazu aufgefordert.
Severity Mapping	Hiermit ordnen Sie die verschiedenen Schweregrade von Rack PDU- oder Umgebungsereignissen den verfügbaren Syslog-Prioritäten zu. Diese Zuordnungen müssen normalerweise nicht geändert werden. Die folgenden Definitionen stammen aus RFC3164: • **Emergency**: Das System kann nicht mehr verwendet werden. • **Alert**: Es muss umgehend eine entsprechende Maßnahme erfolgen. • **Critical**: Kritische Zustände. • **Error**: Fehlerzustände. • **Warning**: Warnzustände. • **Notice**: Normale aber wichtige Zustände. • **Informational**: Meldungen für Informationszwecke. • **Debug**: Meldungen auf Debug-Ebene. Die Standardeinstellungen für die Priorität **Local Priority** lauten wie folgt: • **Severe** ist **Critical** zugeordnet. • **Warning** ist **Warning** zugeordnet. • **Informational** ist **Info** zugeordnet. **HINWEIS:** Eine Anleitung zum Deaktivieren der Syslog-Nachrichten finden Sie unter Konfigurieren von Ereignisaktionen.

Beispiel für einen Syslog-Test und das Syslog-Format.

Befehlsfolge: Protokolle > Syslog > Test

Senden Sie eine Testnachricht an die Syslog-Server, die über die Option **Server** konfiguriert wurden.

1. Wählen Sie den Schweregrad aus, der dieser Testnachricht zugewiesen werden soll.
2. Definieren Sie die Testnachricht gemäß den Pflichtfeldern für die Nachricht.

– Die Priorität (PRI): Die dem Nachrichtenereignis zugeordnete Syslog-Priorität und der Einrichtungscode der von der Rack PDU gesendeten Nachrichten.

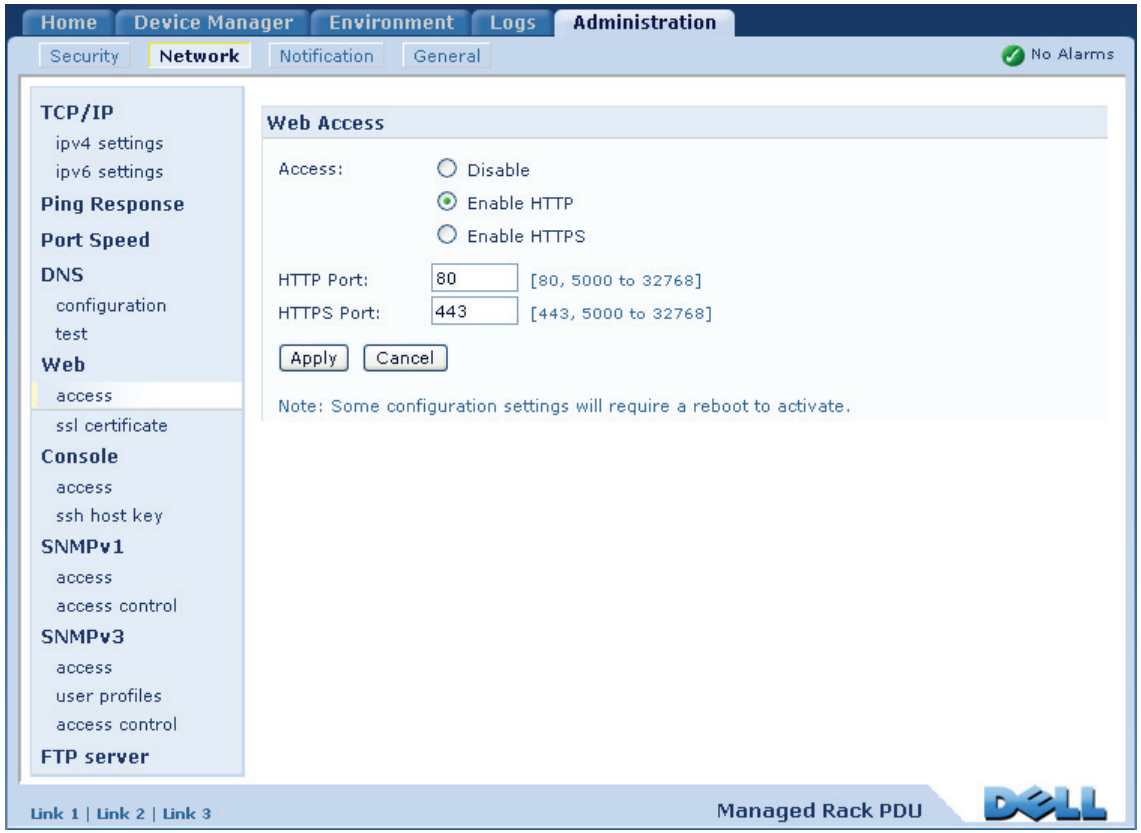
– Der Header: ein Zeiteintrag und die IP-Adresse der Rack PDU.

– Der Nachrichtenteil (MSG):

- Das Feld TAG, gefolgt von einem Doppelpunkt und einem Leerzeichen, identifiziert den Ereignistyp.
- Das Feld CONTENT enthält den Ereignistext, eventuell gefolgt von einem Leerzeichen und dem Ereigniscode.

  Beispiel: **`Dell: Test Syslog`** ist eine gültige Nachricht.

Verwaltung: Netzwerkfunktionen



TCP/IP und Kommunikationseinstellungen

TCP/IP-Einstellungen

Befehlsfolge: Administration > Network > TCP/IP

Die Option TCP/IP im linken Navigationsmenü wird standardmäßig aktiviert, wenn Sie in der oberen Menüleiste die Option **Network** (Netzwerk) wählen. Auf dieser Seite werden die aktuelle IPv4-Adresse, die Teilnetzmaske, das Standardgateway, die MAC-Adresse und der Boot-Modus der Rack PDU angezeigt.

Informationen zu DHCP und DHCP-Optionen finden Sie in **RFC2131** und **RFC2132**.

Einstellung	Beschreibung
Aktivieren	Über dieses Kontrollkästchen aktivieren oder deaktivieren Sie IPv4.
Manual	Hiermit konfigurieren Sie IPv4 manuell, indem Sie die IP-Adresse, die Teilnetzmaske und das Standardgateway eingeben.
1. Die auf der Konfigurationsseite angezeigten Standardwerte für diese drei Einstellungen müssen normalerweise nicht geändert werden: •**Vendor Class**: DELL •**Client ID**: Die MAC-Adresse der Rack PDU, die diese im lokalen Netzwerk (LAN) eindeutig identifiziert. •**User Class**: Der Name des Moduls der Anwendungs-Firmware	

Einstellung	Beschreibung
BOOTP	Die TCP/IP-Einstellungen werden von einem BOOTP-Server bezogen. Die Rack PDU fordert in Intervallen von 32 Sekunden von einem vorhandenen BOOTP-Server eine Netzwerkzuweisung an: • Wenn die Rack PDU eine gültige Antwort erhält, startet sie die Netzwerkdienste. • Wenn die Rack PDU einen BOOTP-Server findet, eine entsprechende Anfrage jedoch fehlschlägt oder zu lange unbeantwortet bleibt, unterlässt die Rack PDU die Anforderung von Netzwerkeinstellungen, bis sie neu gestartet wird. • Wenn bereits konfigurierte Netzwerkeinstellungen existieren und die Rack PDU auf fünf Anfragen (die erste Anfrage und vier Neuversuche) keine gültige Antwort erhält, verwendet sie standardmäßig die bereits konfigurierten Einstellungen, um erreichbar zu bleiben. Klicken Sie auf **Next>>** (Weiter), um die Konfigurationsseite für BOOTP zu öffnen und die Anzahl der Neuversuche oder den Vorgang zu ändern, der bei einem Fehlschlagen aller Anfragen durchgeführt werden soll[1]: • **Maximale Anzahl an Versuchen**: Geben Sie die Anzahl der Neuversuche ein, die unternommen werden sollen, wenn keine gültige Antwort empfangen wird. Wenn Sie den Wert Null (0) eingeben, wird die Anfrage unbegrenzt wiederholt. • **Wenn Versuche fehlschlagen**: Wählen Sie **Use prior settings** (die Voreinstellung) oder **Stop BOOTP request**.

1. Die auf der Konfigurationsseite angezeigten Standardwerte für diese drei Einstellungen müssen normalerweise nicht geändert werden:
   •**Vendor Class**: DELL
   •**Client ID**: Die MAC-Adresse der Rack PDU, die diese im lokalen Netzwerk (LAN) eindeutig identifiziert.
   •**User Class**: Der Name des Moduls der Anwendungs-Firmware

Einstellung	Beschreibung
DHCP	Die Standardeinstellung. Die Rack PDU fordert in Intervallen von 32 Sekunden von einem vorhandenen DHCP-Server eine Netzwerkzuweisung an: • Wenn die Rack PDU eine gültige Antwort erhält, fordert sie vom DHCP-Server das Hersteller-Cookie nicht an, um die Adressreservierung zu bestätigen, sondern startet die Netzwerkdienste sofort. • Wenn die Rack PDU einen DHCP-Server findet, eine entsprechende Anfrage jedoch fehlschlägt oder zu lange unbeantwortet bleibt, unterlässt die Rack PDU die Anforderung von Netzwerkeinstellungen, bis sie neu gestartet wird.[1] • **Herstellerspezifisches Cookie muss DHCP-Adresse akzeptieren** Durch Aktivieren dieses Kontrollkästchens kann der DHCP-Server angewiesen werden, ein Cookie bereitzustellen, das der Rack PDU Daten liefert.

1. Die auf der Konfigurationsseite angezeigten Standardwerte für diese drei Einstellungen müssen normalerweise nicht geändert werden:
   •**Vendor Class**: DELL
   •**Client ID**: Die MAC-Adresse der Rack PDU, die diese im lokalen Netzwerk (LAN) eindeutig identifiziert.
   •**User Class**: Der Name des Moduls der Anwendungs-Firmware

Optionen in DHCP-Antworten

Jede gültige DHCP-Antwort enthält Optionen, mit denen an die Rack PDU TCP/IP-Einstellungen übergeben werden, die diese zum Funktionieren in einem Netzwerk benötigt, sowie weitere Informationen, die sich auf das Verhalten der Rack PDU auswirken.

Herstellerspezifische Informationen (Option 43). Die Rack PDU verwendet diese Option in einer DHCP-Antwort, um festzustellen, ob die DHCP-Antwort gültig ist. Diese Option enthält bis zu zwei spezifische Optionen, die im Format TAG/LÄNGE/DATEN vorliegen: Diese Option ist in der Grundeinstellung deaktiviert.

- **Hersteller-Cookie. Tag 1, Len 4, Data “1APC”**
  Mit Option 43 wird dem Rack PDU mitgeteilt, dass ein DHCP-Server zum Bedienen der Dell Rack PDU konfiguriert wurde.
  Im Folgenden ist ein Beispiel für die Option „Herstellerspezifische Informationen“ im hexadezimalen Format dargestellt, die ein Hersteller-Cookie enthält:

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

TCP/IP-Einstellungen. Die Rack PDU verwendet die folgenden Optionen in einer gültigen DHCP-Antwort, um die TCP/IP-Einstellungen festzulegen: Alle diese Optionen mit Ausnahme der ersten sind in **RFC2132** beschrieben.

- **IP-Adresse** (aus dem Feld **yiaddr** der DHCP-Antwort, beschrieben in **RFC2131)**: Die IP-Adresse, die der DHCP-Server der Rack PDU in der Lease zuteilt.
- **Teilnetzmaske** (Option 1): Die Teilnetzmaske, die von der Rack PDU benötigt wird, um im Netzwerk zu funktionieren.
- **Router,** d. h. der Standard-Gateway (Option 3): Die Adresse des Standard-Gateways, die von der Rack PDU benötigt wird, um im Netzwerk zu funktionieren.
- **Zuteilungsdauer der IP-Adresse** (Option 51): Die Dauer der Zuteilung der IP-Adresse an die Rack PDU.
- **Erneuerungsdauer, T1** (Option 58): Wie lange die Rack PDU nach Zuteilung einer IP-Adresse warten muss, bevor sie eine Erneuerung dieser Zuteilung anfordern kann.

- **Neuanbindungsdauer, T2** (Option 59): Wie lange die Rack PDU nach Zuteilung einer IP-Adresse warten muss, bevor sie eine Neuanbindung dieser Zuteilung anfordern kann.

Weitere Optionen. Darüber hinaus verwendet die Rack PDU auch die nachstehend aufgeführten Optionen innerhalb einer gültigen DHCP-Antwort. Alle diese Optionen mit Ausnahme der letzten sind in **RFC2132** beschrieben.

- **Network Time Protocol-Server** (Option 42): Bis zu zwei NTP-Server (primär und sekundär), die von der Rack PDU verwendet werden können.
- **Zeitunterschied** (Option 2): Der Zeitunterschied des Teilnetzes der Rack PDU in Sekunden zur koordinierten Weltzeit „Coordinated Universal Time“ (UTC).
- **DNS-Server** (Option 6): Bis zu zwei Domain Name System-Server (DNS-Server) (primär und sekundär), die von der Rack PDU verwendet werden können.
- **Host Name** (Option 12): Der von der Rack PDU verwendete Host-Name (Höchstlänge 32 Zeichen).
- **Domänenname** (Option 15): Der von der Rack PDU verwendete Domänenname (Höchstlänge 64 Zeichen).
- **Boot-Dateiname** (aus dem Feld **file** der DHCP-Antwort, beschrieben in **RFC2131**): Der vollständige Pfad zu einer herunterzuladenden Benutzerkonfigurationsdatei (INI-Datei). Das Feld **siaddr** in der DHCP-Antwort enthält die IP-Adresse des Servers, von dem die Rack PDU die INI-Datei herunterladen wird. Nach dem Herunterladen der INI-Datei verwendet die Rack PDU diese als Boot-Datei zum Neukonfigurieren ihrer Einstellungen.

Befehlsfolge: Verwaltung > Netzwerk > TCP/IP > ipv6-Einstellungen

Einstellung	Beschreibung
Aktivieren	Über dieses Kontrollkästchen aktivieren oder deaktivieren Sie IPv6.
Manuell	Hiermit konfigurieren Sie IPv6 manuell, indem Sie die IP-Adresse und das Standardgateway eingeben.
Auto Configuration	Wenn das Kontrollkästchen „Auto Configuration“ markiert ist, bezieht das System die Adressierungspräfixe vom Router (falls verfügbar). Diese Präfixe werden verwendet, um die IPv6-Adressen automatisch zu konfigurieren.

Einstellung	Beschreibung
DHCPv6 Mode	**Router Controlled**: Wenn diese Option aktiviert ist, wird DHCPv6 über die in IPv6 Router Advertisements empfangenen Flags „Managed“ (= Verwaltet, „M“) und „Other“ (= Anderweitig, „O“) gesteuert. Wenn ein Router Advertisement empfangen wird, prüft die NMC, ob das Flag „M“ oder das Flag „O“ gesetzt ist. Bei der Interpretation des Zustands der Flags „M“ (Flag für verwaltete Adresskonfiguration) und „O“ (Flag für anderweitige Stateful-Konfiguration) unterscheidet die NMC folgende Möglichkeiten: • *Keines der beiden Flags ist gesetzt*: Dies bedeutet, dass dem lokalen Netzwerk die DHCPv6-Infrastruktur fehlt. Die NMC verwendet Router Advertisements und manuell konfigurierte Einstellungen, um Adressen zu beziehen, die nicht „link-local“ sind, sowie weitere Einstellungen. • *„M“ oder „M“ und „O“ sind gesetzt*: In dieser Situation kommt es zu einer vollständigen DHCPv6-Adresskonfiguration. DHCPv6 wird verwendet, um Adressen UND weitere Konfigurationseinstellungen zu beziehen. Dieser Zustand wird als „DHCPv6 Stateful“ bezeichnet. Nachdem das Flag „M“ empfangen wurde, bleibt die DHCPv6-Adresskonfiguration wirksam, bis die betreffende Schnittstelle geschlossen wird. Dies gilt auch dann, wenn nachfolgende Router Advertisement-Pakete empfangen werden, in denen das Flag „M“ nicht gesetzt ist. Wenn zuerst das Flag „O“ und anschließend das Flag „M“ empfangen wird, führt die NMC bei Erhalt des Flags „M“ die vollständige Adresskonfiguration durch. • *Nur Flag „O“ ist gesetzt:* In dieser Situation sendet die NMC ein DHCPv6 Info-Request-Paket. DHCPv6 wird zur Konfiguration der „anderweitigen“ Einstellungen (z. B. der Standorte von DNS-Servern) verwendet, NICHT jedoch zur Bereitstellung von Adressen. Dieser Zustand wird als „DHCPv6 Stateless“ bezeichnet. **Address and Other Information:** Wenn dieses Optionsfeld ausgewählt ist, werden sowohl Adressen als auch die anderweitigen Konfigurationseinstellungen über DHCPv6 bezogen. Dieser Zustand wird als „DHCPv6 Stateful“ bezeichnet. **Non-Address Information Only:** Wenn dieses Optionsfeld ausgewählt ist, wird DHCPv6 zur Konfiguration der „anderweitigen“ Einstellungen (z. B. der Standorte von DNS-Servern) verwendet, NICHT jedoch zur Bereitstellung von Adressen. Dieser Zustand wird als „DHCPv6 Stateless“ bezeichnet. **Never:** Mit dieser Option wird DHCPv6 deaktiviert.

Ping-Antwort

Befehlsfolge: Verwaltung > Netzwerk > Ping-Antwort

Markieren Sie das Kontrollkästchen „Enable“ (Aktivieren) für **IPv4 Ping Response** (IPv4 Ping-Antwort), um es der Netzwerkmanagement-Karte zu erlauben, auf Ping-Anfragen aus dem Netzwerk zu antworten. Entfernen Sie das Häkchen aus dem Kontrollkästchen, um Antworten der NMC zu unterbinden. Dies gilt nicht für IPv6.

Port Speed

Befehlsfolge: Administration > Network > Port Speed

Mit der Einstellung **Port Speed** legen Sie die Datenübertragungsgeschwindigkeit des TCP/IP-Ports fest.

- Bei Verwendung der Option **Auto-negotiation** („Automatische Aushandlung“, die Voreinstellung) handeln Ethernet-Geräte eine möglichst hohe Übertragungsgeschwindigkeit aus; wenn jedoch die beiden am Datenaustausch beteiligten Geräte unterschiedliche Geschwindigkeiten unterstützen, wird die niedrigere Geschwindigkeit verwendet.
- Statt dessen können Sie auch 10 MBit/s oder 100 MBit/s als Übertragungsgeschwindigkeit wählen, jeweils mit der Option „Halb-Duplex“ (Kommunikation immer nur in eine Richtung gleichzeitig) oder „Voll-Duplex“ (Kommunikation in beide Richtungen gleichzeitig auf demselben Kanal).

DNS

Befehlsfolge: Administration > Network > DNS > *Optionen*

Verwenden Sie die Optionen unter **DNS**, um das Domain Name System (DNS) zu konfigurieren und zu testen:

- Wählen Sie **Primary DNS Server** (Primärer DNS-Server) oder **Secondary DNS Server** (Sekundärer DNS-Server), um die IPv4- oder IPv6-Adresse des primären und eines optionalen sekundären DNS-Servers festzulegen. Damit die Rack PDU E-Mails senden kann, müssen Sie mindestens die IP-Adresse des primären DNS Servers angeben.
  - Die Rack PDU wartet bis zu 15 Sekunden auf eine Antwort vom primären oder sekundären DNS-Server (sofern bereits ein sekundärer DNS-Server definiert wurde). Wenn die Rack PDU innerhalb dieser Wartezeit keine Antwort erhält, kann keine E-Mail gesendet werden. Daher sollten DNS-Server auf dem gleichen Segment wie die Rack PDU oder auf einem nahe gelegenen Segment laufen (nicht jedoch in einem Weitverkehrsnetz (WAN)).
  - Nachdem Sie die IP-Adressen der DNS-Server angegeben haben, überzeugen Sie sich davon, dass das DNS einwandfrei funktioniert. Geben Sie dazu den DNS-Namen eines Computers in Ihrem Netzwerk ein, um nach der IP-Adresse für diesen Computer zu suchen.
- **Host Name**: Nachdem Sie hier einen Hostnamen und im Feld **Domain Name** einen Domänennamen konfiguriert haben, können Benutzer in alle Felder der Rack PDU, die Domänennamen verarbeiten können, einen Hostnamen eingeben (außer E-Mail-Adressen).

- **Domänenname (IPv4)**: Hier müssen Sie nur den Domänennamen konfigurieren. In allen anderen Feldern der Rack PDU (mit Ausnahme von Feldern für E-Mail-Adressen), die Domänennamen verarbeiten können, fügt die Rack PDU diesen Domänennamen automatisch ein, wenn nur ein Host-Name eingegeben wurde.
  - Wenn Sie die Ergänzung des eingegebenen Hostnamens durch Hinzufügen des Domänennamens überall aufheben möchten, setzen Sie das für den Domänennamen vorgesehene Feld auf seinen Standardwert, also auf `irgendeinedomaene.com` oder auf `0.0.0.0`.
  - Wenn Sie die Ergänzung eines bestimmten Host-Namens durch Hinzufügen des Domänennamens (z. B. beim Definieren eines Trap-Empfängers) aufheben möchten, geben Sie dazu einen nachgestellten Punkt ein. Die Rack PDU interpretiert einen Host-Namen mit nachgestelltem Punkt (z. B. *`mySnmpServer.`*) als vollständigen Domänennamen und hängt dann keinen Domänennamen mehr an.
- **Domänenname (IPv6)**: Geben Sie hier den IPv6-Domänennamen an.
- Wählen Sie **Test**, um eine DNS-Anfrage zum Testen der Konfiguration Ihrer DNS-Server zu senden:
  - Wählen Sie als **Query Type** (Abfragentyp) die für DNS-Abfragen zu verwendende Methode aus:
    - **nach Host**: der URL-Name des Servers
    - **nach FQDN**: nach vollständigem Domänennamen
    - **nach IP**: nach der IP-Adresse des Servers
    - **nach MX**: nach der vom Server verwendeten Mail Exchange

– Geben Sie als **Frage der Abfrage** den für den gewählten Abfragentyp zu verwendenden Wert ein:

Gewählter Abfragentyp	Frage der Abfrage
nach Host	Die URL
nach FQDN	Der vollständige Domänenname, *mein_server.meine_domaene*.
nach IP	Die IP-Adresse
nach MX	Die Mail Exchange-Adresse

– Im Feld **Letzte Abfrageantwort** können Sie sich das Ergebnis der letzten DNS-Testabfrage ansehen.

Web

Befehlsfolge: Administration > Network > Web > *Optionen*

Option	Beschreibung

Zugriff	Um Änderungen an einer dieser Auswahlmöglichkeiten aktivieren zu können, müssen Sie sich von der Rack PDU abmelden:
	• **Deaktivieren**: Hiermit deaktivieren Sie den Zugriff auf die Web-Oberfläche. (Zum erneuten Aktivieren des Zugriffs melden Sie sich über die Befehlszeile an und geben Sie dann den Befehl **`http -S enable`** ein. Für HTTPS-Zugriff geben Sie **`https -S enable`** ein.)
	• **Enable HTTP** (die Voreinstellung): Hiermit aktivieren Sie das Hypertext Transfer Protocol (HTTP), das den Web-Zugriff per Benutzername und Passwort ermöglicht, die Benutzernamen, Passwörter und Daten jedoch unverschlüsselt überträgt.
	• **Enable HTTPS**: Hiermit aktivieren Sie HTTPS (Hypertext Transfer Protocol over Secure Sockets Layer (SSL)). SSL verschlüsselt Benutzernamen, Passwörter und Daten während der Übertragung und authentifiziert die Rack PDU über ein digitales Zertifikat. Wenn HTTPS aktiviert ist, wird im Browser ein kleines Schloss-Symbol angezeigt.
	
	Entscheidungshilfen zur Auswahl einer Methode für die Verwendung digitaler Zertifikate finden Sie unter „Erstellen und Installieren von digitalen Zertifikaten“ in Anhang B: Sicherheitshandbuch.
	
	HTTP Port: Der TCP/IP-Port, über den der HTTP-Datenaustausch mit der Rack PDU erfolgen soll (Voreinstellung: 80).
	
	HTTPS Port: Der TCP/IP-Port, über den der HTTPS-Datenaustausch mit der Rack PDU erfolgen soll (Voreinstellung: 443).
	
	Für beide Protokolle (HTTP und HTTPS) haben Sie die Möglichkeit, die Port-Einstellung auf einen beliebigen freien Port zwischen 5000 und 32768 zu ändern, um die Sicherheit zu erhöhen. Der Benutzer muss dann einen Doppelpunkt und dahinter die Port-Nummer in das Adressfeld des Browsers eingeben. Für die IP-Adresse 152.214.12.114 und die Port-Nummer 5000 lautet die Eingabe beispielsweise wie folgt:
	`http://152.214.12.114:5000`
	`https://152.214.12.114:5000`

Option	Beschreibung
SSL-Zertifikat	Hiermit können Sie ein Sicherheitszertifikat hinzufügen, ersetzen oder entfernen. **Status**: • **Not installed**: Es ist kein Zertifikat installiert oder wurde über FTP oder SCP an einem falschen Speicherort installiert. Mit der Option **Add or Replace Certificate File** (Zertifikatdatei hinzufügen oder ersetzen) wird das Zertifikat am richtigen Speicherort auf der Rack PDU installiert, d. h. unter **/ssl**. • **Generating**: Die Rack PDU erzeugt ein Zertifikat, weil kein gültiges Zertifikat gefunden wurde. • **Loading**: Ein Zertifikat wird auf der Rack PDU aktiviert. • **Valid certificate**: Es wurde ein gültiges Zertifikat installiert oder von der Rack PDU erzeugt. Klicken Sie auf diesen Link, um sich den Inhalt des Zertifikats anzusehen. **Wenn Sie ein ungültiges Zertifikat installieren, oder falls bei der Aktivierung von SSL kein Zertifikat geladen wurde, erzeugt die** Rack PDU **ein Standard-Zertifikat; dadurch kann der Zugriff auf die Schnittstelle bis zu einer Minute lang blockiert werden.** Sie können das Standard-Zertifikat für einen einfachen, verschlüsselten Sicherheitsstandard verwenden; allerdings wird jedes Mal, wenn Sie sich anmelden, eine Sicherheitswarnung angezeigt. **Add or Replace Certificate File**: Geben Sie Name und Pfad der mit dem Security Wizard (Sicherheitsassistenten) erzeugten Zertifikatdatei ein, oder navigieren Sie im Dateisystem zu dieser. Entscheidungshilfen zur Auswahl einer Methode für die Verwendung der vom Sicherheitsassistenten oder von der Rack PDU erstellten digitalen Zertifikate finden Sie unter „Erstellen und Installieren von digitalen Zertifikaten“ in Anhang B: Sicherheitshandbuch. **Remove**: Hiermit löschen Sie das aktuelle Zertifikat.

Console

Befehlsfolge: Administration > Network > Console > *Optionen*

Option	Beschreibung

Zugriff	Wählen Sie eine der folgenden Optionen für den Zugriff über Telnet oder Secure SHell (SSH):
	• **Disable**: Hiermit deaktivieren Sie den Zugriff auf die Befehlszeile komplett.
	• **Telnet aktivieren** (die Voreinstellung): Telnet überträgt Benutzernamen, Passwörter und Daten ohne Verschlüsselung.
	• **Enable SSH**: SSH überträgt Benutzernamen, Passwörter und Daten in verschlüsselter Form und bietet somit Schutz gegen ein Mithören, Fälschen oder Verändern der Daten während der Übertragung.
	
	Konfigurieren Sie die Ports, die von diesen Protokollen verwendet werden sollen:
	• **Telnet Port**: Hiermit legen Sie den Telnet-Port fest, über den der Datenaustausch mit der Rack PDU erfolgen soll (Voreinstellung: 23) Sie haben die Möglichkeit, die Port-Einstellung auf einen beliebigen freien Port zwischen 5000 und 32768 zu ändern, um die Sicherheit zu erhöhen. Der Benutzer muss dann einen Doppelpunkt oder ein Leerzeichen (abhängig vom Telnet-Client) eingeben, um den nicht standardmäßigen Port anzugeben. Wenn beispielsweise der Port 5000 und die IP-Adresse 152.214.12.114 verwendet werden sollen, benötigt der Telnet-Client einen der folgenden Befehle:
	`telnet 152.214.12.114:5000`
	`telnet 152.214.12.114 5000`
	• **SSH Port**: Hiermit legen Sie den SSH-Port fest, über den der Datenaustausch mit der Rack PDU erfolgen soll (Voreinstellung: 22) Sie haben die Möglichkeit, die Port-Einstellung auf einen beliebigen freien Port zwischen 5000 und 32768 zu ändern, um die Sicherheit zu erhöhen. Die zum Festlegen eines nicht standardmäßigen Ports benötigte Befehlssyntax können Sie der Dokumentation zu Ihrem SSH-Client entnehmen.

Option	Beschreibung

ssh host key	**Status** zeigt den Status des Host-Schlüssels (privater Schlüssel) an:
	• **SSH Disabled: Es ist kein Host-Schlüssel in Verwendung:** Wenn diese Option deaktiviert ist, kann SSH keinen Host-Schlüssel verwenden.
	• **Generating**: Die Rack PDU erzeugt einen Host-Schlüssel, weil kein gültiger Host-Schlüssel gefunden wurde.
	• **Loading**: Ein Host-Schlüssel wird auf der Rack PDU aktiviert.
	• **Valid**: Einer der folgenden gültigen Host-Schlüssel befindet sich im Ordner **/ssh** (d. h. im erforderlichen Standardordner auf der Rack PDU):
	  • Ein vom Sicherheitsassistenten erstellter Host-Schlüssel mit einer Verschlüsselungsstärke von 1024 oder 2048 Bit
	  • Ein von der Rack PDU erstellter RSA-Host-Schlüssel mit einer Verschlüsselungsstärke von 2048 Bit
	
	Hinzufügen oder ersetzen: Hiermit navigieren Sie zu einer vom APC Sicherheitsassistenten erstellten Host-Schlüssel-Datei und übertragen diese an die Rack PDU.
	
	Informationen zur Verwendung des Sicherheitsassistenten finden Sie in Anhang B: Sicherheitshandbuch.
	
	HINWEIS: Sie können die zum Aktivieren von SSH benötigte Zeit verkürzen, indem Sie vorab einen Host-Schlüssel erstellen und an die Rack PDU übertragen. **Wenn Sie SSH aktivieren, ohne dass zuvor ein Host-Schlüssel geladen wurde**, benötigt die Rack PDU **bis zu einer Minute, um den Host-Schlüssel zu erstellen, und der SSH-Server bleibt während dieser Zeit unerreichbar.**
	
	Remove: Hiermit entfernen Sie den aktuellen Host-Schlüssel.

Damit Sie SSH verwenden können, muss ein SSH-Client installiert sein. Im Gegensatz zu Microsoft Windows-Betriebssystemen, beinhalten die meisten Linux-Distributionen und sonstigen UNIX-Plattformen einen SSH-Client. Clients können von verschiedenen Anbietern bezogen werden.

SNMP

Alle anderen Benutzernamen, Passwörter und Community-Namen für SNMP werden im Klartext über das Netzwerk übertragen. Sollte Ihr Netzwerk den durch Verschlüsselung gewährleisteten, hohen Sicherheitsstandard benötigen, sollten Sie den SNMP-Zugriff deaktivieren oder für alle Communitys das Zugriffsrecht „Nur Lesen“ einstellen. (Eine Community mit Nur-Lese-Zugriff kann Statusinformationen empfangen und SNMP-Traps verwenden.)

Ausführliche Informationen zur Erhöhung der Systemsicherheit finden Sie in Anhang B: Sicherheitshandbuch.

SNMPv1

Befehlsfolge: Administration > Network > SNMPv1 > *Optionen*

Option	Beschreibung
Zugriff	**Enable SNMPv1 Access:** Hiermit aktivieren Sie SNMP Version 1 als Methode für den Datenaustausch mit diesem Gerät.
access control	Sie können bis zu vier Einträge für die Zugriffssteuerung konfigurieren, um festzulegen, welche Netzwerkmanagementsysteme (NMS) auf dieses Gerät zugreifen dürfen. Auf der Startseite für die Zugriffssteuerung ist jeder der vier verfügbaren SNMPv1 Communitys als Voreinstellung genau ein Eintrag zugewiesen. Sie können diese Einstellungen jedoch dahin gehend ändern, dass einer bestimmten Community mehrere Einträge gleichzeitig zugewiesen werden, um den Zugriff durch mehrere spezifische IPv4- und IPv6-Adressen, Hostnamen oder IP-Adressmasken zu erlauben. Wenn Sie die Einstellungen für die Zugriffssteuerung für eine Community ändern möchten, klicken Sie auf den Community-Namen. • Wenn Sie den vorgegebenen Eintrag für die Zugriffssteuerung für eine Community unverändert lassen, kann diese Community von beliebigen Standorten im Netzwerk aus auf dieses Gerät zugreifen. • Wenn Sie zu einem Community-Namen mehrere Einträge für die Zugriffssteuerung gleichzeitig konfigurieren, führt die Beschränkung auf maximal vier Einträge dazu, dass mindestens eine der anderen Communitys keinen Eintrag für die Zugriffssteuerung erhält. Wenn zu einer bestimmten Community kein Eintrag für die Zugriffssteuerung aufgeführt ist, hat die betreffende Community keinen Zugriff auf dieses Gerät. **Community Name:** Der Name, den ein NMS verwenden muss, um auf die Community zugreifen zu können. Die maximale Länge beträgt 15 ASCII-Zeichen und die vorgegebenen Namen für die vier Communitys lauten **`public`**, **`private`**, **`public2`** und **`private2`**. **NMS-IP/Host Name:** Die IPv4- oder IPv6-Adresse, die IP-Adressmaske oder der Hostname, der den Zugriff durch NMS kontrolliert. Ein Host-Name oder eine bestimmte IP-Adresse (z. B. 149.225.12.1) ermöglicht dem NMS den Zugriff nur am betreffenden Standort. Bei IP-Adressen, die „255“ enthalten, ist der Zugriff wie folgt eingeschränkt: • 149.225.12.**255**: Zugriff ausschließlich durch ein NMS im Segment 149.225.12. • 149.225.**255.255**: Zugriff ausschließlich durch ein NMS im Segment 149.225. • 149.**255.255.255**: Zugriff ausschließlich durch ein NMS im Segment 149. • 0.0.0.0 (die Standardeinstellung), gleichbedeutend mit 255.255.255.255: Zugriff durch beliebige NMS in beliebigen Segmenten. **Access Type**: Die Vorgänge, die einem NMS über die Community erlaubt sind. • **Read**: Nur GETs, dies zu jeder Zeit • **Write**: GETs zu jeder Zeit und SETs, wenn kein Benutzer über die Web-Oberfläche oder die Befehlszeile angemeldet ist. • **Write+**: GETs und SETs zu jeder Zeit. • **Disable**: Keine GETs und keine SETs, zu keiner Zeit.

SNMPv3

Befehlsfolge: Administration > Network > SNMPv3 > *Optionen*

Für die SNMP-Befehle GET und SET sowie für die Trap-Empfänger verwendet SNMPv3 ein System mit Benutzerprofilen zur Identifikation der Benutzer. Einem SNMPv3-Benutzer muss in der MIB-Software ein Benutzerprofil zugewiesen werden, damit er die SNMP-Befehle GET und SET ausführen, die MIB durchsuchen und Traps empfangen kann.

Zur Verwendung von SNMPv3 müssen Sie ein MIB-Programm einsetzen, das SNMPv3 unterstützt.

Die Rack PDU unterstützt SHA- oder MD5-Authentifizierung sowie AES- oder DES-Verschlüsselung.

Option	Beschreibung
access	**SNMPv3-Zugang:** Hiermit aktivieren Sie SNMPv3 als Methode für den Datenaustausch mit diesem Gerät.

Option	Beschreibung
Benutzer-profile	In der Grundeinstellung werden hier die Einstellungen für vier Benutzerprofile angezeigt, konfiguriert mit den Benutzernamen **dell snmp profile1** bis **dell snmp profile4**, ohne Authentifizierung und ohne Datenschutz (keine Verschlüsselung). Wenn Sie die folgenden Einstellungen für ein Benutzerprofil ändern möchten, klicken Sie in der Liste auf einen Benutzernamen. **User Name:** Die Kennung des Benutzerprofils. SNMP Version 3 ordnet GETs, SETs und Traps einem Benutzerprofil zu, indem es den Benutzernamen im Profil mit dem Benutzernamen in dem zu übertragenden Datenpaket abgleicht. Ein Benutzername kann aus bis zu 32 ASCII-Zeichen bestehen. **Authentication Passphrase:** Eine aus 15 bis 32 ASCII-Zeichen bestehende Passphrase (Voreinstellung: **`dell auth passphrase`**), mit der verifiziert wird, dass das mit diesem Gerät über SNMPv3 kommunizierende NMS wirklich das NMS ist, das es zu sein vorgibt, dass die Nachricht während der Übertragung nicht geändert wurde, und dass die Nachricht im normalen Zeitrahmen übermittelt und somit nicht aufgehalten wurde, z. B. durch Kopieren und zeitversetztes Neuversenden. **Privacy Passphrase:** Eine aus 15 bis 32 ASCII-Zeichen bestehende Passphrase (Voreinstellung: **`dell crypt passphrase`**), mit der mittels Verschlüsselung die Geheimhaltung der zwischen diesem Gerät und einem NMS über SNMPv3 ausgetauschten Daten sichergestellt werden kann. **Authentication Protocol:** Die Dell-Implementierung von SNMPv3 unterstützt SHA- und MD5-Authentifizierung. Die Authentifizierung wird nur durchgeführt, wenn ein entsprechendes Authentifizierungsprotokoll ausgewählt wurde. **Privacy Protocol:** Die Dell-Implementierung von SNMPv3 unterstützt AES und DES als Protokolle zur Ver- und Entschlüsselung von Daten. Für die Geheimhaltung der übertragenen Daten muss ein Datenschutzprotokoll ausgewählt und eine Datenschutz-Passphrase in der Anfrage des NMS enthalten sein. Wenn ein Datenschutzprotokoll aktiviert ist, das NMS jedoch keine Datenschutz-Passphrase bereitstellt, wird die SNMP-Anfrage nicht verschlüsselt. **Hinweis:** Sie können das Datenschutzprotokoll nicht auswählen, solange kein Authentifizierungsprotokoll ausgewählt wurde.

Option	Beschreibung
Zugriffs-steuerung	Sie können bis zu vier Einträge für die Zugriffssteuerung konfigurieren, um festzulegen, welche NMS auf dieses Gerät zugreifen dürfen. Auf der Startseite für die Zugriffssteuerung ist jedem der vier Benutzerprofile als Voreinstellung genau ein Eintrag zugewiesen. Sie können diese Einstellungen jedoch dahin gehend ändern, dass einem bestimmten Benutzerprofil mehrere Einträge gleichzeitig zugewiesen werden, um den Zugriff durch mehrere spezifische IP-Adressen, Host-Namen oder IP-Adressmasken zu erlauben. • Wenn Sie den vorgegebenen Eintrag für die Zugriffssteuerung für ein Benutzerprofil unverändert lassen, können alle NMS, die dieses Profil verwenden, auf dieses Gerät zugreifen. • Wenn Sie zu einem Benutzerprofil mehrere Einträge für die Zugriffssteuerung gleichzeitig konfigurieren, führt die Beschränkung auf maximal vier Einträge dazu, dass mindestens eines der anderen Benutzerprofile keinen Eintrag für die Zugriffssteuerung erhält. Wenn zu einem bestimmten Benutzerprofil kein Eintrag für die Zugriffssteuerung aufgeführt ist, haben NMS, die dieses Profil verwenden, keinen Zugriff auf dieses Gerät. Wenn Sie die Einstellungen für die Zugriffssteuerung für ein Benutzerprofil ändern möchten, klicken Sie auf den Benutzernamen. **Access:** Markieren Sie das Kontrollkästchen **Enable** (Aktivieren), um die von den Parametern dieses Eintrags festgelegte Zugriffssteuerung zu aktivieren. **User Name:** Wählen Sie aus diesem Dropdown-Listenfeld das Benutzerprofil aus, für das dieser Eintrag für die Zugriffssteuerung gelten soll. Zur Auswahl stehen die vier Benutzernamen, die Sie über die Option **user profiles** (Benutzerprofile) im linken Navigationsmenü konfiguriert haben. **NMS-IP/Host Name:** Die IP-Adresse, die IP-Adressmaske oder der Host-Name, der den Zugriff durch das NMS kontrolliert. Ein Host-Name oder eine bestimmte IP-Adresse (z. B. 149.225.12.1) ermöglicht dem NMS den Zugriff nur am betreffenden Standort. Bei IP-Adressmasken, die „255“ enthalten, ist der Zugriff wie folgt eingeschränkt: • 149.225.12.**255**: Zugriff ausschließlich durch ein NMS im Segment 149.225.12. • 149.225.**255.255**: Zugriff ausschließlich durch ein NMS im Segment 149.225. • 149.**255.255.255**: Zugriff ausschließlich durch ein NMS im Segment 149. • 0.0.0.0 (die Standardeinstellung), gleichbedeutend mit 255.255.255.255: Zugriff durch beliebige NMS in beliebigen Segmenten.

FTP Server

Befehlsfolge: Administration > Network > FTP Server

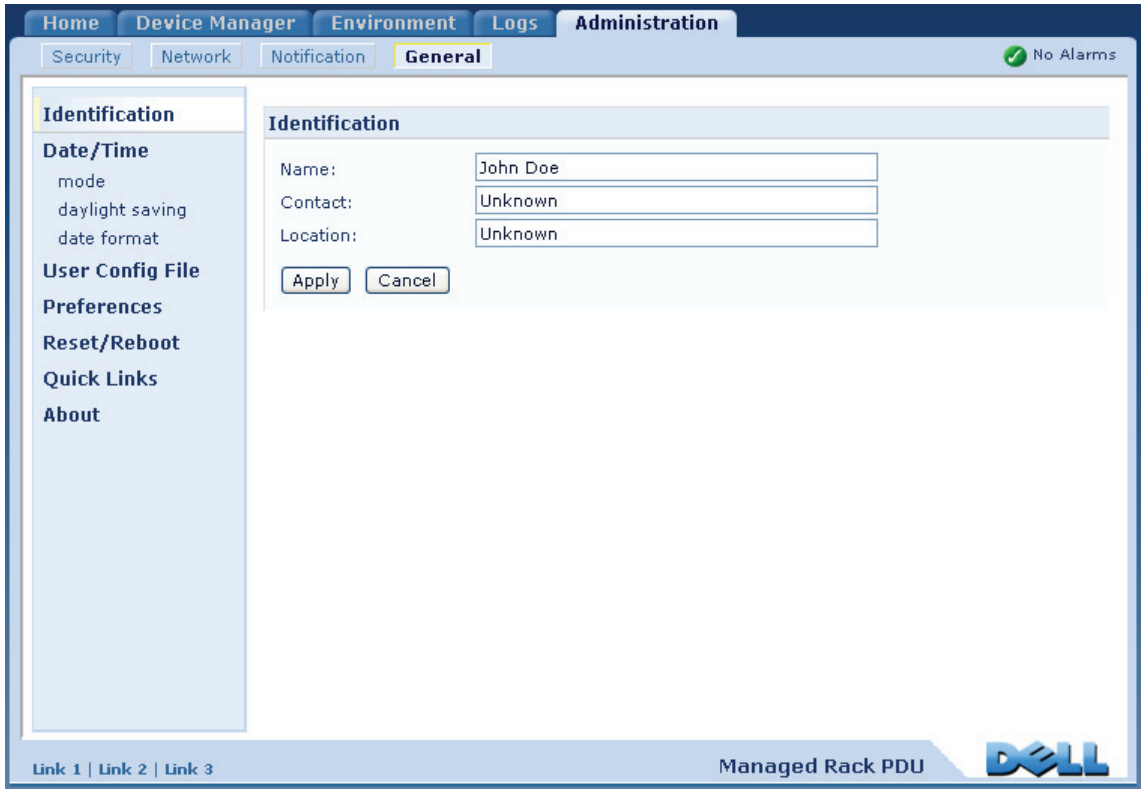
Anhand der Einstellungen unter **FTP Server** wird der Zugriff auf den FTP-Server aktiviert (dies ist die Voreinstellung) oder aktiviert und der TCP/IP-Port (Voreinstellung: 21) festgelegt, den der FTP-Server für den Datenaustausch mit der Rack PDU verwendet. Der FTP-Server verwendet stets den eingestellten Port und den unmittelbar darunter befindlichen Port.

Sie haben die Möglichkeit, die **Port**-Einstellung auf einen beliebigen freien Port zwischen 5001 und 32768 zu ändern, um die Sicherheit zu erhöhen. Der Benutzer muss dann einen Doppelpunkt und dahinter die Port-Nummer des nicht standardmäßigen Ports in das Adressfeld des Browsers eingeben. Für den Port 5001 und die IP-Adresse 152.214.12.114 lautet der Befehl beispielsweise **`ftp 152.214.12.114:5001`**.

FTP überträgt Dateien unverschlüsselt. Zur Erhöhung der Sicherheit können Sie den FTP-Server deaktivieren und die Dateien über SCP übertragen. Durch das Auswählen und Konfigurieren von Secure SHell (SSH) wird SCP automatisch aktiviert.

Ausführliche Informationen zur Erhöhung der Systemsicherheit finden Sie in Anhang B: Sicherheitshandbuch.

Verwaltung: Allgemeine Optionen



Identifizierung

Befehlsfolge: Administration > General > Identification

Geben Sie mit **Name** den Gerätenamen, mit **Location** den physikalischen Standort und mit **Contact** den verantwortlichen Ansprechpartner für das Gerät zur Verwendung durch den SNMP-Agent der Rack PDU an. Diese Einstellungen sind die Werte, die von den MIB-II Objektkennungen (OID) **sysName**, **sysContact** und **sysLocation** verwendet werden.

Weitere Informationen zu MIB-II OIDs finden Sie in der Dell Management Information Base (MIB).

Einstellen von Datum und Uhrzeit

Methode

Befehlsfolge: Administration > General > Date & Time > mode

Hiermit stellen Sie Datum und Uhrzeit der Rack PDU ein. Sie können die aktuellen Einstellungen manuell oder über einen NTP-Server ändern:

- **Manual Mode**: Führen Sie einen der folgenden Schritte durch:
  - Geben Sie Datum und Uhrzeit für die Rack PDU ein.
  - Markieren Sie das Kontrollkästchen **Apply Local Computer Time** um Datum und Uhrzeit des verwendeten Computers für die Rack PDU zu übernehmen.
- **Synchronize with NTP Server**: Hiermit können Sie einen NTP-Server angeben, von dem die Rack PDU das Datum und die Uhrzeit beziehen soll.

Einstellung	Beschreibung
Primary NTP Server	Geben Sie die IP-Adresse oder den Domänennamen des primären NTP-Servers ein.
Secondary NTP Server	Geben Sie die IP-Adresse oder den Domänennamen des sekundären NTP-Servers ein, falls dieser zur Verfügung steht.
Time Zone	Wählen Sie eine Zeitzone aus. Die den Zeitzonen in der Liste jeweils vorangestellte Stundenzahl ist der Zeitunterschied zur koordinierten Weltzeit „Coordinated Universal Time“ (UTC), früher als „Greenwich Mean Time“ bezeichnet.
Update Interval	Hiermit legen Sie fest, in welchen Abständen (in Stunden) die Rack PDU zur Aktualisierung auf den NTP-Server zugreift. *Mindestwert*: 1; *Maximalwert*: 8760 (1 Jahr).
Update Using NTP Now	Hiermit starten Sie eine sofortige Aktualisierung von Datum und Uhrzeit über den NTP-Server.

Sommerzeit

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

Aktivieren Sie die US-amerikanische Sommerzeit (DST) oder aktivieren und konfigurieren Sie eine benutzerdefinierte Sommerzeit, die den Gegebenheiten in Ihrer Region entspricht. Sommerzeit ist in der Grundeinstellung deaktiviert.

Beachten Sie beim Anpassen der Sommerzeit Folgendes:

- Wenn die lokale Sommerzeit z. B. immer am vierten Sonntag in einem bestimmten Monat beginnt oder endet, wählen Sie **Fourth/Last** (Vierter/Letzter). Wenn es in dem betreffenden Monat in einem Folgejahr einen fünften Sonntag gibt, erfolgt die Umstellung auf Sommerzeit trotzdem am vierten Sonntag.
- Wenn die lokale Sommerzeit z. B. immer am letzten Sonntag in einem bestimmten Monat beginnt oder endet, unabhängig davon, ob es sich dabei um den vierten oder fünften Sonntag handelt, wählen Sie **Fifth/Last** (Fünfter/Letzter).

Format

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

Wählen Sie das Zahlenformat, in dem alle Datumsangaben über diese Benutzerschnittstelle angezeigt werden sollen. Jeder der Buchstaben m (für Monat), d (für Tag) und y (für Jahr) steht in diesen Auswahlmöglichkeiten für eine Ziffer. Tage und Monate, die einer einzigen Ziffer entsprechen, werden mit vorangestellter Null angezeigt.

Verwendung einer INI-Datei

Befehlsfolge: Administration > General > User Config File

Sie können die Einstellungen einer Rack PDU verwenden, um damit eine andere Rack PDU zu konfigurieren. Rufen Sie die Datei config.ini aus der konfigurierten Rack PDU ab, passen Sie diese Datei entsprechend an (z. B. durch Ändern der IP-Adresse) und übertragen Sie die angepasste Datei an die neue Rack PDU. Der Dateiname darf bis zu 64 Zeichen enthalten und muss mit der Dateinamenserweiterung .ini versehen sein.

Status	Meldet den Fortgang der Übertragung. Die Übertragung wird auch dann zu Ende geführt, wenn die Datei Fehler enthält; diese Fehler werden jedoch als Systemereignis im Ereignisprotokoll erfasst.
Upload	Hiermit navigieren Sie zu der angepassten Datei und übertragen sie an die Rack PDU damit diese anhand der INI-Datei ihre eigene Konfiguration einstellen kann.

Eine Anleitung zum Abrufen und Anpassen der INI-Datei einer konfigurierten Rack PDU finden Sie unter Exportieren von Konfigurationseinstellungen.

Anstatt die Datei an eine einzige Rack PDU zu übertragen, können Sie die Datei auch mithilfe eines FTP- oder SCP-Skripts an mehrere Rack PDUs gleichzeitig übertragen.

Ereignisprotokoll und Temperatureinheiten

Befehlsfolge: Administration > General > Preferences

Farbkodierung im Ereignisprotokolltext

Diese Option ist in der Grundeinstellung deaktiviert. Markieren Sie das Kontrollkästchen **Ereignisprotokoll-Farbkodierung**, um die farbliche Kodierung der im Ereignisprotokoll erfassten Alarmtexte zu aktivieren. Einträge zu Systemereignissen und Konfigurationsänderungen behalten immer dieselbe Farbe.

Textfarbe	Schweregrad des Alarms
Rot	**Kritisch**: Es liegt ein kritischer Alarm vor, der ein sofortiges Eingreifen erfordert.
Orange	**Warnung**: Es liegt ein Alarm vor, dem genauer nachgegangen werden muss, und der zu einer Gefahr für Daten oder Hardware werden könnte, wenn seine Ursache nicht behoben wird.
Grün	**Alarm gelöscht**: Der Zustand, der zur Auslösung des Alarms geführt hat, besteht nicht mehr.
Schwarz	**Normal**: Keine Alarme vorhanden. Die Rack PDU und alle angeschlossenen Geräte funktionieren normal.

Ändern der voreingestellten Temperaturskala

Wählen Sie die Temperaturskala (Fahrenheit oder Celsius), in der alle Temperaturwerte auf dieser Benutzeroberfläche angezeigt werden sollen.

Zurücksetzen der Rack PDU

Befehlsfolge: Administration > General > Reset/Reboot

Vorgang	Beschreibung
Reboot Management Interface	Hiermit starten Sie die Verwaltungsschnittstelle der Rack PDU neu.
Reset All[1]	Entfernen Sie das Häkchen aus dem Kontrollkästchen **Exclude TCP/IP** (TCP/IP ausschließen), wenn Sie alle konfigurierten Werte zurücksetzen möchten; markieren Sie das Kontrollkästchen **Exclude TCP/IP** (TCP/IP ausschließen), wenn Sie alle Werte mit Ausnahme von TCP/IP zurücksetzen möchten.
Reset Only[1]	**TCP/IP-Einstellungen**: Wenn Sie die Option „TCP/IPC Configuration“ **DHCP & BOOTP** einstellen (die Standardeinstellung), muss die Rack PDU ihre TCP/IP-Einstellungen von einem DHCP- oder BOOTP-Server beziehen. Siehe TCP/IP und Kommunikationseinstellungen.
	Event configuration: Hiermit setzen Sie sämtliche nach Ereignis und nach Gruppe an der Ereigniskonfiguration vorgenommenen Änderungen auf die entsprechenden Standardwerte zurück.
	RPDU to Defaults: Hiermit setzen Sie nur Rack PDU-Einstellungen, nicht jedoch Netzwerkeinstellungen auf ihre jeweiligen Standardwerte zurück.
1. Das Zurücksetzen der Rack PDU kann bis zu einer Minute dauern.	

Konfigurieren der Links

Befehlsfolge: Administration > General > Quick Links

Klicken Sie in der oberen Menüleiste auf **Administration** und anschließend auf **General** (Allgemein), und wählen Sie dann im linken Navigationsmenü die Option **Quick Links**, um sich die URL-Verknüpfungen der links unten auf jeder Konfigurationsseite angezeigten Links anzusehen oder diese zu ändern.

In der Grundeinstellung führen diese Links auf die folgenden Webseiten:

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

Wenn Sie eines der folgenden Elemente neu konfigurieren möchten, klicken Sie in der Spalte **Display** (Anzeige) auf den Namen des Links:

- **Display**: Der Kurzname des auf jeder Konfigurationsseite angezeigten Links
- **Name**: Ein Name, der das Ziel oder den Zweck des Links vollständig identifiziert
- **Address**: Eine beliebige URL, z. B. die URL zu einem anderen Gerät oder Server

Informationen zur Rack PDU

Befehlsfolge: Administration > General > About

Die Informationen zur Hardware sind für die Fehlersuche bei Problemen mit der Rack PDU hilfreich. Die Seriennummer und die MAC-Adresse sind auch auf der Rack PDU selbst aufgedruckt.

Die Informationen zur Firmware für das Anwendungsmodul, Dell OS (AOS) und den APC-Boot-Monitor beinhalten die Namen und Versionsnummern der Firmware-Moduls sowie Datum und Uhrzeit der Erstellung der einzelnen Firmware-Module. Diese Informationen sind bei der Problembehandlung ebenfalls hilfreich.

Die **Verfügbare Verwaltungszeit** ist die bisherige ununterbrochene Laufzeit der Schnittstelle.

Exportieren von Konfigurationseinstellungen

Abrufen und Exportieren der INI-Datei

Das Verfahren im Überblick

Rack PDUEin Administrator kann die INI-Dateien einer Rack PDU abrufen und an beliebig viele andere Rack PDUs exportieren.

1. Konfigurieren Sie eine Rack PDU mit den Einstellungen, die Sie exportieren möchten.
2. Rufen Sie die INI-Dateien aus dieser Rack PDU ab.
3. Passen Sie die Datei an, indem Sie mindestens die TCP/IP-Einstellungen ändern.
4. Verwenden Sie ein von der Rack PDU unterstütztes Dateiübertragungsprotokoll, um die Datei an beliebig viele Rack PDUs zu übertragen. Für Übertragungen an mehrere Rack PDUs gleichzeitig können Sie ein FTP- oder SCP-Skript verwenden.

Wenn eine Rack PDU die INI-Datei empfängt, konfiguriert sie ihre eigenen Einstellungen neu und löscht anschließend die INI-Datei.

Inhalt der INI-Datei

Die aus einer Rack PDU abrufbare Datei config.ini enthält folgende Daten:

- *Abschnittsüberschriften* und *Schlüsselwörter* (nur diejenigen, die von dem Gerät unterstützt werden, von dem Sie die Datei abrufen)*:* Bei den Abschnittsüberschriften handelt es sich um in [eckige Klammern] eingeschlossene Kategoriebezeichnungen. Bei den unter den einzelnen Abschnittsüberschriften aufgeführten Schlüsselwörtern handelt es sich um Bezeichnungen für bestimmte Einstellungen der Rack PDU. Auf jedes Schlüsselwort folgt ein Gleichheitszeichen und ein Wert (entweder der Standardwert oder ein konfigurierter Wert).
- Das Schlüsselwort **`Override`**: Wenn für dieses Schlüsselwort der Standardwert eingestellt ist, verhindert es den Export eines oder mehrerer Schlüsselwörter und ihrer dazugehörigen, gerätespezifischen Werte. So blockiert beispielsweise im Abschnitt **`[NetworkTCP/IP]`** der Standardwert des Schlüsselworts **`Override`** (die MAC-Adresse der Rack PDU) den Export der Werte für **`SystemIP`**, **`SubnetMask`**, **`DefaultGateway`** und **`BootMode`**.

Ausführliche Verfahrensbeschreibungen

Abrufen. So rufen Sie eine INI-Datei ab und passen diese für den Export an:

1. Verwenden Sie nach Möglichkeit die Schnittstelle einer Rack PDU, um auf dieser die Einstellungen zu konfigurieren, die exportiert werden sollen. Eine direkte Bearbeitung der INI-Datei birgt immer ein gewisses Fehlerrisiko.
2. So rufen Sie die Datei config.ini per FTP von der konfigurierten Rack PDU ab:
   a. Öffnen Sie eine Verbindung zur Rack PDU, indem Sie deren IP-Adresse eingeben:

      `ftp> open` ***`ip-adresse`***

   b. Melden Sie sich mit einem entsprechenden Benutzernamen und Passwort als Administrator an.
   c. Rufen Sie die Datei config.ini mit den Einstellungen der Rack PDU ab:

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

      Die Datei wird in dem Ordner gespeichert, von dem aus Sie die FTP-Verbindung gestartet haben.

Anpassen. Sie müssen die Datei anpassen, bevor Sie sie exportieren.

1. Verwenden Sie einen Texteditor, um die Datei anzupassen.
   - Bei Abschnittsüberschriften, Schlüsselwörtern und vordefinierten Werten muss nicht auf die Groß-/Kleinschreibung geachtet werden, bei den dazugehörigen Werten hingegen schon.
   - Geben Sie nacheinander zwei hochgestellte Anführungszeichen ein, um anzugeben, dass kein Wert zugeordnet werden soll. Der Eintrag **`LinkURL1=""`** bedeutet beispielsweise, dass die URL absichtlich nicht angegeben wurde.
   - Schließen Sie alle Werte in Anführungszeichen ein, die vorangestellte oder nachgestellte Leerzeichen enthalten, oder die bereits in Anführungszeichen gesetzt sind.
   - Zum Exportieren geplanter Ereignisse konfigurieren Sie die entsprechenden Werte direkt in der INI-Datei.
   - Zum Exportieren einer möglichst exakten Systemzeit an Rack PDUs, die auf einen NTP-Server zugreifen können, geben Sie hinter **`NTPEnable`** den Wert **`enabled`** ein:

     `NTPEnable=enabled`

     Sie haben auch die Möglichkeit, die Übertragungsdauer zu reduzieren, indem Sie den Abschnitt **`[SystemDate/Time]`** als separate INI-Datei exportieren.
   - Kommentarzeilen müssen durch einen Strichpunkt (`;`) eingeleitet werden.
2. Kopieren Sie die angepasste Datei unter einem anderen Dateinamen in denselben Ordner:
   - Der Dateiname darf bis zu 64 Zeichen enthalten und muss mit der Dateinamenserweiterung .ini versehen sein.
   - Bewahren Sie die angepasste Originaldatei zur späteren Verwendung auf. **Dies ist die einzige Datei, in der auch Ihre Kommentare hinterlegt sind.**

Übertragen der Datei an eine einzelne Rack PDU. Führen Sie einen der folgenden Schritte durch, um die INI-Datei an eine andere Rack PDU zu übertragen:

- Wählen Sie auf der Web-Oberfläche der empfangenden Rack PDU die Registerkarte **Administration** und auf dieser in der oberen Menüleiste die Option **General** (Allgemein). Klicken Sie dann im linken Navigationsmenü auf **User Config File** (Benutzerkonfigurationsdatei). Geben Sie den vollständigen Pfad zu der Datei ein oder verwenden Sie die Schaltfläche **Browse**.
- Verwenden Sie ein beliebiges, von Rack PDUs unterstütztes Dateiübertragungsprotokoll, z. B. FTP, FTP Client, SCP oder TFTP. Im folgenden Beispiel wird FTP verwendet:
  a. Wechseln Sie in den Ordner, der die Kopie der angepassten INI-Datei enthält und melden Sie sich von dort aus mit dem folgenden Befehl über FTP bei der Rack PDU an, an die Sie die INI-Datei exportieren möchten:

     ```
     ftp> open ip-adresse
     ```

  b. Exportieren Sie die Kopie der angepassten INI-Datei in das Stammverzeichnis der empfangenen Rack PDU:

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

Exportieren der Datei an mehrere Rack PDUs. Zum Exportieren der INI-Datei an mehrere Rack PDUs gleichzeitig verwenden Sie FTP oder SCP, erstellen Sie jedoch ein Skript, das die zum Exportieren der Datei an eine einzelne Rack PDU erforderlichen Schritte mehrmals beinhaltet.

Ereignis- und Fehlermeldungen zur Dateiübertragung

Das Ereignis und die dazugehörigen Fehlermeldungen

Der folgende Ereignistext wird angezeigt, wenn die empfangende Rack PDU die Aktualisierung ihrer Einstellungen anhand der INI-Datei abgeschlossen hat.

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

(Hochladen der Konfigurationsdatei mit n gültigen Werten abgeschlossen.) Wenn ein Schlüsselwort, ein Abschnittsname oder ein Wert ungültig ist, wird die Übertragung an die empfangende Rack PDU zu Ende geführt und der Fehler durch einen zusätzlichen Ereignistext mitgeteilt.

Ereignistext	Beschreibung
Configuration file warning: Invalid keyword on line *number*. Configuration file warning: Invalid value on line *number*.	Zeilen mit einem ungültigen Schlüsselwort oder Wert werden ignoriert.
Configuration file warning: Invalid section on line *number.*	Wenn ein Abschnittsname ungültig ist, werden alle in diesem Abschnitt befindlichen Schlüsselwörter und Werte ignoriert.
Configuration file warning: Keyword found outside of a section on line *number*.	Ein ganz oben in der Datei (d. h. vor der ersten Abschnittsüberschrift) eingetragenes Schlüsselwort wird ignoriert.
Configuration file warning: Configuration file exceeds maximum size.	Wenn die Datei zu groß ist, kommt es zu einer unvollständigen Übertragung. Reduzieren Sie die Dateigröße oder teilen Sie die Datei in zwei kleinere Dateien auf und wiederholen Sie die Übertragung.

Meldungen in der Datei config.ini

Eine Rack PDU, aus der Sie die Datei config.ini heruntergeladen haben, muss vom System entdeckt werden, damit ihre Konfiguration einbezogen werden kann. Wenn die Rack PDU nicht vorhanden ist oder nicht entdeckt wurde, enthält die Datei config.ini unter dem betreffenden Abschnittsnamen statt Schlüsselwörtern und Werten eine Meldung. Beispiel:

```
Rack PDU not discovered
```

(Keine Rack PDU gefunden.) Wenn Sie nicht vorhaben, die Konfiguration der Rack PDU für einen späteren Import der INI-Datei zu exportieren, können Sie diese Meldungen ignorieren.

Durch außer Kraft gesetzte Werte erzeugte Fehlermeldungen

Durch das Schlüsselwort **`Override`** und den ihm zugewiesenen Wert werden im Ereignisprotokoll Fehlermeldungen erstellt, wenn die betreffende Einstellung das Exportieren von Werten blockiert.

Informationen zu außer Kraft gesetzten Werten finden Sie unter Inhalt der INI-Datei.

Da die außer Kraft gesetzten Werte gerätespezifisch und für den Export an andere Rack PDUs nicht relevant sind, können Sie diese Fehlermeldungen ignorieren. Sie können solche Fehlermeldungen verhindern, indem Sie die Zeilen löschen, die das Schlüsselwort **`Override`** und die außer Kraft zu setzenden Werte enthalten. Die Zeile mit der Abschnittsüberschrift darf jedoch keinesfalls gelöscht oder verändert werden.

Dateiübertragungen

Aktualisieren der Firmware

Vorteile der Firmware-Aktualisierung

Wenn Sie die Firmware auf der Rack PDU aktualisieren:

- erhalten Sie immer die neuesten Bugfixes und sonstige Verbesserungen
- können Sie neue Funktionen sofort verwenden.

Durch einheitliche Firmware-Versionen im gesamten Netzwerk ist sichergestellt, dass alle Rack PDU die gleichen Funktionen in einheitlicher Weise unterstützen.

Firmware-Dateien

Eine Firmware-Version besteht aus drei Modulen: Einem Betriebssystem-Modul (AOS), einem Anwendungsmodul und einem Boot-Monitor-Modul (bootmon). Jedes Modul beinhaltet mindestens eine zyklische Redundanzprüfung (Cyclical Redundancy Check, CRC), die zum Schutz der Daten während der Übertragung dient.

Die von der Rack PDU verwendeten Dateien zum Betriebssystem-Modul (AOS), Anwendungsmodul und Boot-Monitor-Modul haben ein gemeinsames Dateinamensformat:

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

- **`dell`**: Bedeutet, dass es sich um eine Dell-Datei handelt.
- ***`hardware-version`***: **`hw0`***`x`* identifiziert die Hardwareversion, auf der diese Binärdatei verwendet werden kann.
- ***`typ`***: Gibt an, ob es sich bei der Datei um das Betriebssystem-Modul (AOS), um das Anwendungsmodul oder um das Boot-Monitor-Modul der Rack PDU handelt.
- ***`version`***: Die Versionsnummer der Datei.
- **`bin`**: Bedeutet, dass dies eine Binärdatei ist.

Eine Anleitung zum Prüfen der Versionsnummern der einzelnen Firmware-Module einer Rack PDU finden Sie unter Informationen zur Rack PDU.

Übertragungsverfahren für Firmware-Dateien

Zur Aktualisierung der Firmware einer Rack PDU können Sie eine der folgenden Methoden verwenden:

- Auf einem Netzwerk-Computer, der unter einem beliebigen unterstützten Betriebssystem läuft, übertragen Sie das AOS-Modul und das Anwendungsmodul der Firmware per FTP oder SCP einzeln.
- Bei einer nicht in Ihrem Netzwerk befindlichen Rack PDU können Sie die einzelnen Firmware-Module per XMODEM über eine serielle Verbindung von Ihrem Computer an die Rack PDU übertragen.

Wenn Sie einzelne Firmware-Module übertragen, **müssen Sie** das Betriebssystem-Modul (AOS) an die Rack PDU übertragen, bevor Sie das Anwendungsmodul übertragen.

Aktualisieren einer einzelnen Rack PDU per FTP oder SCP

FTP. So aktualisieren Sie eine einzelne Rack PDU im Netzwerk per FTP:

- Die Rack PDU muss mit dem Netzwerk verbunden sein, und ihre System-IP, ihre Teilnetzmaske und ihr Standard-Gateway müssen konfiguriert sein.
- Der FTP-Server muss auf der Rack PDU aktiviert sein.
- Die Firmware-Dateien müssen von Dell.com heruntergeladen worden sein.

So übertragen Sie die Dateien:

1. Öffnen Sie auf einem im Netzwerk befindlichen Computer eine Befehlszeile. Wechseln Sie in das Verzeichnis, das die aktualisierten Dateien für die Firmware enthält, und zeigen Sie den Verzeichnisinhalt an:

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

   Der Wert *xxx* steht für die Firmware-Versionsnummer der aufgeführten Dateien:

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

2. Öffnen Sie eine FTP-Client-Sitzung:
   `C:\dell>ftp`
3. Geben Sie **`open`** und die IP-Adresse der Rack PDU ein und drücken Sie die EINGABETASTE. Falls sich die **Port**-Einstellung des FTP-Servers geändert hat und nicht mehr der Standardeinstellung **21** entspricht, müssen Sie im FTP-Befehl den von der Standardeinstellung abweichenden Wert verwenden.
   - Bei Windows FTP-Clients wird die nicht standardmäßige Port-Nummer mit einem Leerzeichen von der IP-Adresse getrennt. Beispiel:
     `ftp> open 150.250.6.10 21000`
   - Bei bestimmten FTP-Clients muss hingegen vor der Port-Nummer ein Doppelpunkt eingegeben werden.
4. Melden Sie sich als Administrator an; Benutzername und Passwort lauten in der Grundeinstellung **admin**.
5. Aktualisieren Sie das AOS. (Im nachstehenden Beispiel steht *xxx* für die Firmware-Versionsnummer):
   `ftp> bin`
   `ftp> put dell_hw05_aos_xxx.bin`
6. Geben Sie zum Beenden der Sitzung **quit** ein, wenn FTP die Übertragung bestätigt.
7. Wiederholen Sie nach 20 Sekunden Schritt 2 bis 5. Verwenden Sie in Schritt 5 den Dateinamen des Anwendungsmoduls.

SCP. So verwenden Sie Secure CoPy (SCP) zum Aktualisieren der Firmware der Rack PDU:

1. Identifizieren und lokalisieren Sie die in der vorstehenden Anleitung für FTP beschriebenen Firmware-Module.
2. Übertragen Sie das AOS-Firmware-Modul über eine SCP-Befehlszeile an die Rack PDU. Im folgenden Beispiel steht *xxx* für die Versionsnummer des AOS-Moduls:
   `scp dell_hw05_aos_xxx.bin`
   `dell@158.205.6.185:dell_hw05_aos_xxx.bin`
3. Verwenden Sie die gleiche SCP-Befehlszeile, diesmal jedoch unter Angabe des Anwendungsmodulnamens, um die Firmware für das Anwendungsmodul an die Rack PDU zu übertragen.

So aktualisieren Sie mehrere Rack PDUs gleichzeitig

Verwenden Sie FTP oder SCP zum Aktualisieren mehrerer Rack PDUs gleichzeitig. Zum Aktualisieren mehrerer Rack PDUs über einen FTP-Client oder über SCP schreiben Sie ein Skript, das den Vorgang automatisch durchführt.

Verwendung von XMODEM zum Aktualisieren einer Rack PDU

Zum Aktualisieren einer nicht im Netzwerk befindlichen Rack PDU über das Protokoll XMODEM müssen Sie zuerst die Firmware-Dateien von Dell.com herunterladen.

So übertragen Sie die Dateien:

1. Wählen Sie eine serielle Schnittstelle auf dem lokalen Computer aus, und deaktivieren Sie sämtliche Dienste, die diese Schnittstelle verwenden.
2. Verbinden Sie das mitgelieferte serielle Kabel mit dem betreffenden Anschluss am Computer und mit dem seriellen Anschluss der Rack PDU.
3. Führen Sie ein Terminalprogramm (z. B.HyperTerminal) aus und konfigurieren Sie den ausgewählten Anschluss mit 57600 bps, 8 Datenbits, ohne Paritätsbit, 1 Stoppbit und ohne Datenflusskontrolle.
4. Drücken Sie die RESET-Taste am Rack PDU und drücken Sie dann sofort mindestens zweimal die EINGABETASTE (bis die Boot-Monitor-Eingabeaufforderung angezeigt wird): **`BM>`**
5. Geben Sie **`XMODEM`** ein und drücken Sie die EINGABETASTE.
6. Wählen Sie im Menü des Terminal-Programms die Option XMODEM, und wählen Sie dann die binäre AOS-Firmware-Datei aus, um sie per XMODEM zu übertragen. Nach Abschluss der XMODEM-Übertragung wird die Boot-Monitor-Eingabeaufforderung erneut angezeigt.
7. Zum Installieren des Anwendungsmoduls wiederholen Sie Schritt 5 und Schritt 6. Verwenden Sie jedoch in Schritt 6 den Dateinamen des Anwendungsmoduls.
8. Geben Sie **`reset`** ein oder drücken Sie die Reset-Taste, um die Rack PDU neu zu starten.

Informationen zum Format der Firmware-Module finden Sie unter Firmware-Dateien.

Überprüfen von Upgrades und Aktualisierungen

Überprüfung des Ergebnisses der Übertragung

Wenn Sie überprüfen möchten, ob ein Firmware-Upgrade erfolgreich verlaufen ist, geben Sie den Befehl **`xferStatus`** in die Befehlszeile ein, um sich das letzte Übertragungsergebnis anzusehen. Eine andere Möglichkeit besteht darin, über den Befehl SNMP GET die OID **mfiletransferStatusLastTransferResult** anzuzeigen.

Ergebniscodes für die letzte Übertragung

Code	Beschreibung
Successful	Die Datei wurde erfolgreich übertragen.
Result not available	Es wurde keine Dateiübertragungen aufgezeichnet.
Failure unknown	Die letzte Dateiübertragung ist aus unbekannten Gründen fehlgeschlagen.
Server inaccessible	Der TFTP- oder FTP-Server konnte im Netzwerk nicht gefunden werden.
Server access denied	Der TFTP- oder FTP-Server hat den Zugriff verweigert.
File not found	Der TFTP- oder FTP-Server konnte die angeforderte Datei nicht finden.
File type unknown	Die Datei wurde heruntergeladen, der Inhalt wurde jedoch nicht erkannt.
File corrupt	Die Datei wurde heruntergeladen, mindestens eine zyklische Redundanzprüfung (Cyclical Redundancy Check, CRC) hat jedoch Fehler ergeben.

Überprüfen der Versionsnummern der installierten Firmware

Über die Web-Oberfläche können Sie die Versionen der aktualisierten Firmware-Module überprüfen. Klicken Sie dazu auf die Registerkarte **Administration**, wählen Sie in der oberen Menüleiste die Option **General** (Allgemein) und klicken Sie dann im linken Navigationsmenü auf **Info**, oder verwenden Sie den Befehl SNMP GET, um die MIB II OID **sysDescr** zu öffnen. In der Befehlszeile steht hierfür der Befehl **`about`** zur Verfügung.

Problembehandlung

Rack PDU Probleme beim Zugriff

Problem	Lösung
Die Rack PDU reagiert nicht auf den Ping-Befehl	Wenn die Status-LED der Rack PDU grün leuchtet, senden Sie den Ping-Befehl versuchsweise an eine andere Station im selben Netzwerksegment wie die Rack PDU. Wenn auch dann eine Antwort ausbleibt, hat das Problem nichts mit der Rack PDU zu tun. Wenn die Status-LED nicht grün leuchtet, oder wenn der Ping-Test erfolgreich verläuft, führen Sie die folgenden Überprüfungen durch: • Überprüfen Sie sämtliche Netzwerkverbindungen. • Überprüfen Sie die IP-Adressen der Rack PDU und des NMS. • Wenn sich das NMS in einem anderen physischen Netzwerk (oder Teilnetz) als die Rack PDU befindet, überprüfen Sie die IP-Adresse des Standard-Gateways (oder Routers). • Überprüfen Sie die Anzahl der Teilnetz-Bits in der Teilnetzmaske der Rack PDU.
Keine Zuweisung der Datenschnittstelle durch ein Terminalprogramm möglich	Damit Sie die Rack PDU über ein Terminalprogramm konfigurieren können, müssen Sie zuerst alle Anwendungen, Dienste oder Programme schließen, die momentan die Datenschnittstelle verwenden.
Kein Zugriff auf die Befehlszeile über eine serielle Datenverbindung möglich	Überzeugen Sie sich davon, dass Sie die Baud-Rate nicht geändert haben. Versuchen Sie es mit 2400, 9600, 19200 oder 38400.

Problem	Lösung
Kein Fernzugriff auf die Befehlszeile möglich	• Stellen Sie sicher, dass Sie die korrekte Zugriffsmethode verwenden, d. h. Telnet oder Secure SHell (SSH). Diese Zugriffsmethoden können von einem Administrator aktiviert werden. Standardmäßig ist Telnet aktiviert. Wenn SSH aktiviert wird, wird Telnet automatisch deaktiviert. • Bei einem Zugriff über SSH erstellt die Rack PDU möglicherweise gerade einen Host-Schlüssel. Es kann bis zu einer Minute dauern, bis die Rack PDU den Host-Schlüssel erstellt hat; während dieser Zeit kann auf SSH nicht zugegriffen werden.
Kein Zugriff auf die Web-Oberfläche möglich	• Überzeugen Sie sich davon, dass der HTTP- oder HTTPS-Zugriff aktiviert ist. • Achten Sie darauf, dass Sie eine korrekte URL eingeben - diese muss zu dem von der Rack PDU verwendeten Sicherheitssystem passen. Für SSL muss die URL mit **https** eingeleitet werden, nicht mit **http**. • Überprüfen Sie, ob die Rack PDU auf den Ping-Befehl reagiert. • Überzeugen Sie sich davon, dass Sie einen von der Rack PDU unterstützten Web-Browser verwenden. Siehe Unterstützte Web-Browser. • Falls die Rack PDU neu gestartet wurde und die Einrichtung der SSL-Sicherheit noch im Gange ist, erzeugt die Rack PDU möglicherweise gerade ein Server-Zertifikat. Es kann bis zu einer Minute dauern, bis die Rack PDU dieses Zertifikat erstellt hat; während dieser Zeit ist der SSL-Server nicht verfügbar.

Anhang A: Liste der unterstützten Befehle

Beschreibung der Befehle der Netzwerkmanagement-Karte

```
?
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 <primärer DNS-Server>]
    [-s <sekundärer DNS-Server>]
    [-d <Domänenname>]
    [-n <Domänenname (IPv6)>]
    [-h <Host-Name>]
eventlog
exit
format
```

```
ftp
    [-p <Port-Nummer>]
    [-S <enable | disable>]
help
netstat
ntp
    [-OM <enable | disable>]
    [-p <primärer NTP-Server>]
    [-s <sekundärer NTP-Server>]
ping
    [<IP-Adresse oder DNS-Name>]
portspeed
    [-s [auto | 10H | 10F | 100H | 100F]]
prompt
    [-s [long | short]]
quit
radius
    [-a <access> [local | radiusLocal | radius]]
    [-p# <Server-IP-Adresse>]
    [-s# <Geheimer Server-Schlüssel>]
    [-t# <Server-Timeout>]
reboot
resetToDef
    [-p <all | keepip>]
snmp, snmpv3
    [-S <enable | disable>]
system
    [-n <Systemname>]
    [-c <System-Ansprechpartner>]
    [-l <Systemstandort>]
tcpip
    [-i <IP-Adresse>]
    [-s <Teilnetzmaske>]
    [-g <Gateway>]
    [-d <Domänenname>]
    [-h <Host-Name>]
tcpip6
    [-S <enable | disable>]
    [-man <enable | disable>]
    [-auto <enable | disable>]
    [-i <IPv6-Adresse>]
    [-g <IPv6-Gateway>]
    [-d6 <router | stateful | stateless | never>]
```

user
[-an <Name des Administrators>]
[-dn <Name des Benutzers „Gerät“>]
[-rn <Name des Benutzers „schreibgeschützt“>]
[-ap <Administrator-Passwort>]
[-dp <Passwort des Benutzers „Gerät“>]
[-rp <Passwort des Benutzers „schreibgeschützt“>]
[-t <Timeout-Frist in Minuten bei Inaktivität>]
web
[-S <disable | http | https>]
[-ph <HTTP-Port-Nr.>]
[-ps <HTTPS-Port-Nr.>]
xferINI
xferStatus

Beschreibung der Gerätebefehle

devLowLoad
[<Leistung>]
devNearOver
[<Leistung>]
devOverLoad
[<Leistung>]
devReading
[<„power“ | „energy“>]
devStartDly
humLow
[<Feuchtigkeit>]
humMin
[<Feuchtigkeit>]
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 Nr.> <Stromstärke>]
phNearOver
[<„all“ | Phase Nr.> <Stromstärke>]
phOverLoad
[<„all“ | Phase Nr.> <Stromstärke>]
phReading
[<„all“ | Phase Nr.> <„current“ | „voltage“ | „power“>]
phRestrictn
[<“all” | phase#> <none | near | over>]
prodInfo
tempHigh
[<„F“ | „C“> <Temperatur>]
tempMax
[<„F“ | „C“> <Temperatur>]
tempReading
[<„F“ | „C“>]

userAdd
[<new user>]
userDelete
[<user>]
userList
userPasswd
[<user> <new password> <new password>]
whoami

Anhang B: Sicherheitshandbuch

Zweck und Inhalt dieses Anhangs

In diesem Anhang sind Sicherheitsfunktionen der Firmwareversion 5.*x*.*x* für Dell® Rack PDUs dokumentiert, die es ermöglichen, die Rack PDU über das Netzwerk per Fernzugriff zu steuern.

Dieser Anhang enthält Informationen zu den folgenden Protokollen und Funktionen sowie Angaben dazu, welche von ihnen für bestimmte Situationen geeignet sind und wie sie im Rahmen der Systemsicherheit eingerichtet und verwendet werden können:

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

Darüber hinaus ist in diesem Anhang beschrieben, wie Sie mithilfe des Sicherheitsassistenten der Rack PDU (Security Wizard) die Komponenten erstellen können, die für das von SSL und SSH gebotene, hohe Sicherheitsniveau benötigt werden.

Sicherheitsfunktionen

Schutz von Passwörtern und Passphrasen

Auf der Rack PDU werden Passwörter oder Passphrasen niemals als Klartext gespeichert.

- Passwörter werden mit einem One-Way-Hash-Algorithmus verschlüsselt.
- Die zur Authentifizierung und Verschlüsselung verwendeten Passphrasen werden verschlüsselt, bevor sie auf der Rack PDU gespeichert werden.

Übersicht über die Zugriffsmethoden

Serieller Zugriff auf die Befehlszeile.

Zugriffssicherheit	Beschreibung
Zugriff über Benutzernamen und Passwort.	Immer aktiviert.

Fernzugriff auf die Befehlszeile.

Zugriffssicherheit	Beschreibung
Verfügbare Methoden: • Benutzername und Passwort • Wählbarer Server-Port • Zugangsprotokolle, die aktiviert oder deaktiviert werden können • Secure Shell (SSH)	Für Zugriff auf hoher Sicherheitsstufe SSH verwenden. • Bei Telnet werden der Benutzername und das Passwort als Klartext übertragen. • Durch die Aktivierung von SSH wird Telnet deaktiviert und ein verschlüsselter Zugriff auf die Befehlszeile ermöglicht, der zusätzlichen Schutz gegen ein Mithören, Fälschen oder Verändern der Daten während der Übertragung bietet.

SNMPv1 und SNMPv3.

Zugriffssicherheit	Beschreibung
Verfügbare Methoden (SNMPv1): • Community-Name • Host-Name • NMS IP-Filter • Agenten, die aktiviert oder deaktiviert werden können • Vier Zugriffs-Communities mit Lese-/Schreib-/Deaktivierungsberechtigung	Sowohl bei SNMPv1 als auch bei SNMPv3 schränkt der Host-Name den Zugriff auf das Netzwerkmanagement-System (NMS) auf den betreffenden Standort ein, und die NMS IP-Filter ermöglichen Zugriffe ausschließlich auf die NMS, die durch eines der IP-Adressformate in den folgenden Beispielen angegeben werden: • 159.215.12.1: Nur das NMS an der IP-Adresse 159.215.12.1. • 159.215.12.255: Ein beliebiges NMS im Segment 159.215.12. • 159.215.255.255: Ein beliebiges NMS im Segment 159.215. • 159.255.255.255: Ein beliebiges NMS im Segment 159. • 0.0.0.0 oder 255.255.255.255: Ein beliebiges NMS. SNMPv3 verfügt über die folgenden, zusätzlichen Sicherheitsfunktionen: • Eine Authentifizierungs-Passphrase, mit der sichergestellt wird, dass das auf die Rack PDU zugreifende NMS wirklich das NMS ist, das es zu sein vorgibt. • Datenverschlüsselung während der Übertragung unter Verwendung einer Datenschutz-Passphrase, die zur Verschlüsselung und Entschlüsselung benötigt wird.
Verfügbare Methoden (SNMPv3): • Vier Benutzerprofile • Authentifizierung anhand einer Authentifizierungs-Passphrase • Verschlüsselung anhand einer Datenschutz-Passphrase • SHA- oder MD5-Authentifizierung • AES- oder DES-Verschlüsselungs-algorithmus • NMS IP-Filter	

Dateiübertragungsprotokolle.

Zugriffssicherheit	Beschreibung
Verfügbare Methoden: • Benutzername und Passwort • Wählbarer Server-Port • FTP-Server und Zugangsprotokolle, die aktiviert oder deaktiviert werden können • Secure CoPy (SCP)	Bei FTP werden Benutzernamen und Passwort als Klartext gesendet und Dateien ohne Verschlüsselung übertragen. Verwenden Sie SCP zur Verschlüsselung des Benutzernamens, des Passworts und der zu übertragenden Dateien, z. B. Firmware-Updates, Konfigurationsdateien, Protokolldateien, SSL-Zertifikate und SSH-Host-Schlüssel. Wenn Sie sich für SCP als Dateiübertragungsprotokoll entscheiden, müssen Sie SSH aktivieren und FTP deaktivieren.

Web-Server.

Zugriffssicherheit	Beschreibung
Verfügbare Methoden: • Benutzername und Passwort • Wählbarer Server-Port • Zugang über die Web-Oberfläche, der aktiviert oder deaktiviert werden kann • Secure Sockets Layer (SSL)	Im einfachen HTTP-Authentifizierungsmodus werden Benutzername und Passwort bei der Übertragung mit Base-64 kodiert (unverschlüsselt). SSL steht in den von der Rack PDU oder der sonstigen Netzwerkeinheit unterstützten Web-Browsern und auf den meisten Web-Servern zur Verfügung. Das Web-Protokoll „HyperText Transfer Protocol over Secure Sockets Layer“ (HTTPS) verschlüsselt und entschlüsselt an den Web-Server gerichtete Seitenaufrufe und die vom Web-Server an den Benutzer zurück gegebenen Seiten.

RADIUS.

Zugriffssicherheit	Beschreibung
Verfügbare Methoden: • Zentralisierte Authentifizierung der Zugriffsrechte • Der vom RADIUS-Server und der Rack PDU verwendete geheime Schlüssel	RADIUS (Remote Authentication Dial-In User Service) ist ein Authentifizierungs-, Autorisierungs- und Kontoverwaltungsdienst zur zentralen Administration des Remote-Zugriffs für jedes Rack PDU. (Die Rack PDU unterstützt die entsprechenden Authentifizierungs- und Autorisierungsfunktionen.)

Zugriffsprioritäten

Die Zugriffspriorität lautet wie folgt (in absteigender Folge):

- Lokaler Zugriff auf die Befehlszeile über einen Computer mit direkter serieller Verbindung zur Rack PDU
- Telnet- oder SSH-Zugriff auf die Befehlszeile über einen Remote-Computer
- Web-Zugriff

Standardmäßige Benutzernamen und Passwörter sofort ändern

Nach der Installation und Erstkonfiguration der Rack PDU sollten Sie die standardmäßig vorgegebenen Benutzernamen und Passwörter in eindeutige Benutzernamen und Passwörter umändern, um grundlegenden Schutz zu erreichen.

Zuweisen von Ports

Wenn Telnet, der FTP-Server, SSH/SCP oder der Web-Server einen Nicht-Standard-Port verwenden, muss der Benutzer den Port in der Befehlszeile oder Web-Adresse angeben, mit der auf die Rack PDU zugegriffen wird. Nicht-Standard-Ports bieten zusätzliche Sicherheit. In der Grundeinstellung sind die „gängigen“, von den Protokollen üblicherweise verwendeten Ports hinterlegt. Stellen Sie die Ports zur Erhöhung der Sicherheit auf freie Port-Nummern zwischen 5001 und 32768 (für den FTP-Server) bzw. zwischen 5000 und 32768 (für die anderen Protokolle und Server) um. (Der FTP-Server verwendet stets den eingestellten Port und den unmittelbar darunter befindlichen Port.)

Benutzernamen, Passwörter und Community-Namen bei SNMPv1

Sämtliche Benutzernamen, Passwörter und Community-Namen für SNMPv1 werden als Klartext über das Netzwerk übertragen. Ein Benutzer, der den Netzwerkverkehr überwachen kann, kann die Benutzernamen und Passwörter ermitteln und sich an den Konten für die Befehlszeile oder die Web-Oberfläche der Rack PDU anmelden. Wenn Sie für Ihr Netzwerk das höhere Sicherheitsniveau benötigen, wie es die verschlüsselungsfähigen Optionen für die Befehlszeile und die Web-Oberfläche bieten, deaktivieren Sie den Zugriff über SNMPv1 oder stellen Sie diesen auf **Read** (Nur-Lese-Zugriff) ein. (Bei einem **Nur-Lese-Zugriff** können Sie Statusinformationen empfangen und SNMP-Traps verwenden.)

Zum Deaktivieren des Zugriffs über SNMPv1 wählen Sie auf der Registerkarte **Administration** die Option **Network** in der oberen Menüleiste und klicken Sie auf **access** (Zugriff) unter der Überschrift **SNMPv1** im linken Navigationsmenü. Deaktivieren Sie das Kontrollkästchen **Enable SNMPv1 access** (SNMPv1-Zugriff aktivieren) und klicken Sie auf **Apply** (Übernehmen).

Zum Aktivieren der Option **Read** (Nur-Lese-Zugriff) für SNMPv1 wählen Sie auf der Registerkarte **Administration** die Option **Network** in der oberen Menüleiste und klicken Sie auf **access control** (Zugriffssteuerung) unter der Überschrift **SNMPv1** im linken Navigationsmenü. Klicken Sie dann für jedes konfigurierte Netzwerkmanagement-System (NMS) auf die dazugehörigen Community-Namen und stellen Sie über die Option **Read** den Nur-Lese-Zugriff ein.

Authentifizierung

Sie können zur Steuerung des Zugriffs auf die Rack PDU Sicherheitsfunktionen wählen, die den Zugriff durch einfache Authentifizierung über Benutzernamen, Passwörter und IP-Adressen (unverschlüsselt) kontrollieren. Diese grundlegenden Sicherheitsfunktionen reichen in den meisten Umgebungen aus, in denen keine vertraulichen Daten übermittelt werden.

SNMP GETS, SETS und Traps

Für eine erweiterte Authentifizierung bei Verwendung von SNMP zur Überwachung oder Konfiguration der Rack PDU wählen Sie SNMPv3. Die bei SNMPv3-Benutzerprofilen verwendete Authentifizierungs-Passphrase stellt sicher, dass das mit der Rack PDU kommunizierende Netzwerkmanagement-System (NMS) wirklich das NMS ist, das es zu sein vorgibt, dass die Nachricht während der Übertragung nicht geändert wurde, und dass die Nachricht im normalen Zeitrahmen übermittelt und somit nicht aufgehalten wurde, z. B. durch Kopieren und zeitversetztes Neuversenden. SNMPv3 ist in der Grundeinstellung deaktiviert.

Die Dell-Implementierung von SNMPv3 ermöglicht die Verwendung des Protokolls SHA-1 oder MD5 zur Authentifizierung.

Web-Oberfläche und Befehlszeile

Damit die Daten und die Kommunikation zwischen der Rack PDU und den Client-Schnittstellen (Befehlszeile und Web-Oberfläche) nicht abgefangen werden können, können Sie das Sicherheitsniveau durch Aktivieren einer der folgenden, verschlüsselungsfähigen Methoden erhöhen:

- Verwenden Sie für die Web-Oberfläche das Protokoll „Secure Sockets Layer“ (SSL).
- Zur Verschlüsselung von Benutzernamen und Passwörtern für den Zugriff über die Befehlszeile verwenden Sie das Protokoll „Secure Shell“ (SSH).
- Zur Verschlüsselung von Benutzernamen, Passwörtern und Daten für die sichere Übertragung von Dateien verwenden Sie das Protokoll „Secure CoPy“ (SCP).

Weitere Informationen zu verschlüsselungsfähigen Sicherheitsmethoden finden Sie unter Encryption.

Encryption

SNMP GETS, SETS und Traps

Für eine verschlüsselte Kommunikation bei Verwendung von SNMP zur Überwachung oder Konfiguration der Rack PDU wählen Sie SNMPv3. Die von den SNMPv3-Benutzerprofilen verwendete Datenschutz-Passphrase stellt durch Verschlüsselung mit dem Verschlüsselungsalgorithmus AES oder DES die Geheimhaltung der Daten sicher, die zwischen einem NMS und der Rack PDU ausgetauscht werden.

Secure Shell (SSH) und Secure CoPy (SCP) für die Befehlszeile

Das Protokoll Secure Shell. SSH bietet einen sicheren Mechanismus für den Fernzugriff auf Computer-Konsolen (auch als „Befehlszeilen“ oder *Shells* bezeichnet). Das Protokoll authentifiziert den Server (in diesem Fall die Rack PDU) und verschlüsselt alle Übertragungen zwischen dem SSH-Client und dem Server.

- SSH ist eine besonders sichere Alternative zu Telnet. Telnet bietet keine Verschlüsselung.
- SSH schützt die zur Authentifizierung verwendeten Eingaben (Benutzername und Passwort) vor einer unbefugten Nutzung durch Dritte, die den Netzverkehr womöglich abfangen.
- Für die Authentifizierung des SSH-Servers (der Rack PDU) gegenüber dem SSH-Client verwendet SSH einen Host-Schlüssel, der den SSH-Server eindeutig identifiziert. Das Host-Schlüssel ist ein fälschungssicheres Identifikationsmerkmal und verhindert, dass sich unbefugte Server im Netzwerk als gültige Server präsentieren können, um auf diesem Wege einen Benutzernamen und ein Passwort zu erlangen.

  Informationen zu unterstützten SSH-Client-Anwendungen finden Sie unter Telnet und Secure Shell (SSH). Das Erstellen eines Host-Schlüssels ist unter Erstellen eines SSH-Host-Schlüssels beschrieben.

- Die Rack PDU unterstützt SSH in der Version 2; diese bietet Schutz vor dem Versuch, Daten während der Übertragung abzufangen, zu verfälschen oder zu ändern.
- Wenn Sie SSH aktivieren, wird Telnet automatisch deaktiviert.
- Die Schnittstelle, die Benutzerkonten und die Benutzerrechte sind gleich, unabhängig davon, ob Sie über SSH oder Telnet auf die Befehlszeile zugreifen.

Secure CoPy. SCP ist eine sichere Datenübertragungsanwendung , die Sie anstelle von FTP verwenden können. SCP liegt das Transport-Protokoll SSH zugrunde, das die Verschlüsselung von Benutzernamen, Passwörtern und Dateien ermöglicht.

- Wenn Sie SSH aktivieren und konfigurieren, wird damit automatisch auch SCP aktiviert und konfiguriert. Es ist keine weitere SCP-Konfiguration erforderlich.
- Sie müssen FTP explizit deaktivieren. Dieses wird nicht automatisch durch die Aktivierung von SSH deaktiviert. Zum Deaktivieren von FTP wählen Sie auf der Registerkarte **Administration** die Option **Network** in der oberen Menüleiste und klicken Sie im linken Navigationsmenü auf **FTP Server**. Deaktivieren Sie das Kontrollkästchen **Enable** (Aktivieren) und klicken Sie auf **Apply** (Übernehmen).

Secure Sockets Layer (SSL) für die Web-Oberfläche

Aktivieren Sie für sichere Web-Kommunikation das Protokoll „Secure Sockets Layer“ (SSL). Wählen Sie dazu HTTPS als Protokollmodus für den Zugriff auf die Web-Oberfläche der Rack PDU. Das Web-Protokoll „HyperText Transfer Protocol over Secure Sockets Layer“ (HTTPS) verschlüsselt und entschlüsselt vom Benutzer an den Web-Server gerichtete Seitenaufrufe und die vom Web-Server an den Benutzer zurück gegebenen Seiten.

Die Rack PDU unterstützt SSL Version 3.0 und das dazugehörige Protokoll „Transport Layer Security“ (TLS) Version 1.0. Die meisten Browser bieten eine Auswahlmöglichkeit für die zu aktivierende SSL-Version.

Wenn SSL aktiviert ist, wird im Browser ein kleines Schloss-Symbol angezeigt.

SSL verwendet ein digitales Zertifikat, das dem Browser die Authentifizierung gegenüber dem Server (in diesem Fall die Rack PDU) ermöglicht. Der Browser verifiziert Folgendes:

- Das Format des Server-Zertifikats ist korrekt.
- Das Server-Zertifikat ist noch nicht abgelaufen.
- Die vom Benutzer bei der Anmeldung angegebenen Zugangsdaten (DNS-Name oder IP-Adresse) müssen dem gemeinsam verwendeten Namen im Server-Zertifikat entsprechen.
- Das Server-Zertifikat trägt die Signatur einer vertrauenswürdigen Zertifizierungsstelle.

Alle größeren Browser-Hersteller verteilen CA-Stammzertifikate der gewerblichen Zertifizierungsstellen (Certificate Authorities), die im Zertifikatspeicher (Cache) des Browsers gespeichert werden. Auf diese Weise kann der Browser die Signatur des Server-Zertifikats mit der Signatur eines CA-Stammzertifikats vergleichen.

Sie können mithilfe des Sicherheitsassistenten der Rack PDU eine Anforderung zur Zertifikatsignierung (Certificate Signing Request, CSR) an eine externe Zertifizierungsstelle richten. Wenn Sie keine der bestehenden Zertifizierungsstellen verwenden möchten, können Sie auch ein Dell-Stammzertifikat erstellen und dieses in den Zertifikatspeicher (Cache) des Browsers laden. Sie haben auch die Möglichkeit, mithilfe des Sicherheitsassistenten ein Server-Zertifikat zu erstellen und an die Rack PDU zu übertragen.

Eine Übersicht über die Verwendung dieser Zertifikate finden Sie unter Erstellen und Installieren von digitalen Zertifikaten.
Informationen zum Erstellen von Zertifikaten und Zertifikatanfragen finden Sie unter Erstellen eines Stammzertifikats und der Server-Zertifikate und Erstellen eines Server-Zertifikats und eines Signing Request.

SSL verwendet auch verschiedene Algorithmen und Verschlüsselungscodes zur Authentifizierung des Servers und der Verschlüsselungsdaten sowie zur Sicherstellung der Integrität der Daten, um auszuschließen, dass diese von einem anderen Server abgefangen und neu gesendet worden sein könnten.

Webseiten, die Sie vor kurzem aufgerufen haben, werden im Cache Ihres Web-Browsers gespeichert, damit Sie ohne erneute Eingabe Ihres Benutzernamens und Passworts wieder auf die betreffenden Seiten zurückkehren können. Schließen Sie noch geöffnete Browser-Sitzungen immer, bevor Sie ihren Computer unbeaufsichtigt lassen.

Erstellen und Installieren von digitalen Zertifikaten

Zweck

Für Netzwerk-Kommunikation, die ein höheres Maß an Sicherheit erfordert, als es die Passwortverschlüsselung bietet, unterstützt die Web-Oberfläche der Rack PDU die Verwendung von digitalen Zertifikaten mit dem Protokoll „Secure Sockets Layer“ (SSL). Digitale Zertifikate können die Rack PDU (den Server) gegenüber dem Web-Browser (dem SSL-Client) authentifizieren.

Sie können einen 1024-Bit-Schlüssel oder einen 2048--Bit-Schlüssel erzeugen. Letzterer bietet eine besonders komplexe Verschlüsselung und ein höheres Sicherheitsniveau.

In den folgenden Abschnitten werden die drei Methoden zur Erstellung, Implementierung und Verwendung digitaler Zertifikate umrissen, damit Sie die für Ihr System am besten geeignete Methode bestimmen können.

- Methode 1: Verwendung des von der Rack PDU automatisch erzeugten Standard-Zertifikats.
- Methode 2: Verwendung des Sicherheitsassistenten der Rack PDU zum Erstellen eines CA-Zertifikats und eines Server-Zertifikats.
- Methode 3: Verwendung des Sicherheitsassistenten der Rack PDU zum Erstellen einer Anforderung zur Signierung des Stammzertifikats durch eine externe Zertifizierungsstelle und Erstellung eines Server-Zertifikats.

Sie können auch Methode 3 verwenden, wenn Ihr Unternehmen oder Ihre Behörde eine eigene Zertifizierungsstelle betreibt. In diesem Fall verwenden Sie den Sicherheitsassistenten der Rack PDU in der gleichen Weise, geben jedoch anstelle einer gewerblichen Zertifizierungsstelle Ihre eigene an.

Wahl einer Methode für Ihr System

Bei Verwendung des Protokolls „Secure Sockets Layer“ (SSL) können Sie aus einer der folgenden Methoden für die Verwendung digitaler Zertifikate wählen.

Methode 1: Verwendung des von der Rack PDU automatisch erzeugten Standard-Zertifikats. Nachdem Sie SSL aktiviert haben, müssen Sie die Rack PDU neu starten. Wenn bei diesem Neustart noch kein Server-Zertifikat existiert, erzeugt die Rack PDU ein selbstsigniertes Standard-Server-Zertifikat, das nicht konfiguriert werden kann.

Methode 1 bietet die folgenden Vor- und Nachteile:

- **Vorteile:**
  - Benutzername und Passwort sowie alle anderen mit dem Rack PDUausgetauschten Daten werden vor der Übertragung verschlüsselt.
  - Sie können dieses Standard-Server-Zertifikat verwenden, um während der Einrichtung einer der beiden anderen Optionen für digitale Zertifikate ein verschlüsselungsbasierendes Sicherheitsniveau zu schaffen, oder Sie können es weiterverwenden, um die von SSL gebotenen Vorteile der Verschlüsselung zu nutzen.
- **Nachteile:**
  - Es kann bis zu einer Minute dauern, bis die Rack PDU das Zertifikat erstellt hat; während dieser Zeit ist die Web-Oberfläche nicht verfügbar. (Diese Verzögerung tritt bei der ersten Anmeldung nach Aktivierung von SSL ein.)
  - Diese Methode beinhaltet nicht die Authentifizierung, die von einem CA-Zertifikat (d. h. einem von einer Zertifizierungsstelle signierten Zertifikat) geboten wird, wie es bei Methode 2 und 3 vorgesehen ist. Im Browser-Cache wird kein CA-Zertifikat vorgehalten. Wenn Sie sich beim Rack PDU anmelden, gibt der Browser daher eine Sicherheitswarnung aus und teilt mit, dass kein von einer vertrauenswürdigen Zertifizierungsstelle signiertes Zertifikat verfügbar ist. Sie können dann entscheiden, ob der Vorgang fortgesetzt werden soll oder nicht. Um diese Meldung zu verhindern, müssen Sie das Standard-Server-Zertifikat bei jedem Benutzer, der

Zugriff auf die Rack PDU benötigt, im Zertifikatspeicher (Cache) des Browsers installieren, und jeder Benutzer muss bei der Anmeldung an der Rack PDU stets den vollständigen Domänennamen eingeben.

– Beim Standard-Server-Zertifikat findet sich statt eines gültigen *gemeinsamen Namens* (der DNS-Name oder die IP-Adresse der Rack PDU) die Seriennummer der Rack PDU. Daher kann zwar die Rack PDU den Zugriff auf ihre Web-Oberfläche mittels Benutzername, Passwort und Kontotyp (also **Administrator**, **Benutzer „Gerät“** oder **Benutzer „schreibgeschützt“**) kontrollieren, der Browser kann jedoch nicht authentifizieren, welche Rack PDU Daten sendet oder empfängt.

– Der *öffentliche Schlüssel* (RSA-Schlüssel), der beim Einrichten einer SSL-Sitzung zur Verschlüsselung verwendet wird, hat standardmäßig eine Länge von 2048 Bit.

Methode 2: Verwendung des Sicherheitsassistenten der Rack PDU zum Erstellen eines CA-Zertifikats und eines Server-Zertifikats. Erstellen Sie mithilfe des Sicherheitsassistenten der Rack PDU zwei digitale Zertifikate:

- Ein *CA-Stammzertifikat* (Zertifikat einer Zertifizierungsstelle), das der Sicherheitsassistent der Rack PDU zum Signieren aller Server-Zertifikate verwendet und von Ihnen dann für alle Benutzer, die auf die Rack PDU zugreifen müssen, in den Zertifikatspeicher (Cache) des Browsers geladen wird.
- Ein *Server-Zertifikat*, das Sie an die Rack PDU übertragen. Wenn der Sicherheitsassistent der Rack PDU ein Server-Zertifikat erstellt, verwendet er das CA-Stammzertifikat zur Signierung des Server-Zertifikats.

Der Web-Browser authentifiziert die Rack PDU, die Daten sendet oder anfordert:

- Zur Identifizierung der Rack PDU verwendet der Browser den *gemeinsamen Namen* (IP-Adresse oder DNS-Name der Rack PDU), der im Server-Zertifikat bei dessen Erstellung als *Distinguished Name* festgelegt wurde.
- Zur Bestätigung, dass das Server-Zertifikat von einer vertrauenswürdigen Signierstelle signiert wurde, vergleicht der Browser die Signatur des Server-Zertifikats mit der Signatur des im Browser-Cache befindlichen Stammzertifikats. Anhand eines Ablaufdatums wird festgestellt, ob das Server-Zertifikat noch gültig ist.

Methode 2 bietet die folgenden Vor- und Nachteile:

- **Vorteile:**
  - Benutzername und Passwort sowie alle anderen mit der Rack PDU ausgetauschten Daten werden vor der Übertragung verschlüsselt.
  - Sie können die Länge des *öffentlichen Schlüssels* (RSA-Schlüssels) ändern, der beim Einrichten einer SSL-Sitzung zur Verschlüsselung verwendet wird. (Sie können die Standardlänge von 1024 Bit oder eine Länge von 2048 Bit verwenden; letztere bietet eine besonders komplexe Verschlüsselung und ein höheres Sicherheitsniveau.)
  - Anhand des von Ihnen an die Rack PDU übertragenen Server-Zertifikats kann SSL den Datenaustausch mit der korrekten Rack PDU authentifizieren. Dadurch ist ein höheres Sicherheitsniveau gewährleistet, das über die Verschlüsselung des Benutzernamens und Passworts sowie der übertragenen Daten hinaus geht.
  - Das von Ihnen im Browser installierte Stammzertifikat befähigt den Browser, das Server-Zertifikat der Rack PDU zu authentifizieren, und bietet dadurch zusätzlichen Schutz vor unbefugten Zugriffen.
- **Nachteil:**
  Da die Zertifikate nicht die digitale Signatur einer gewerblichen Zertifizierungsstelle tragen, müssen Sie das Stammzertifikat einzelnen in den Zertifikatspeicher (Cache) der Browser der einzelnen Benutzer laden. (Viele Browser-Hersteller hinterlegen bereits im Zertifikatspeicher ihrer Browser Stammzertifikate für gewerbliche Zertifizierungsstellen, wie unter Methode 3 beschrieben.)

Methode 3: Verwendung des Sicherheitsassistenten der Rack PDU zum Erstellen einer Anforderung zur Signierung des Stammzertifikats durch eine externe Zertifizierungsstelle und Erstellung eines Server-Zertifikats. Mithilfe des Sicherheitsassistenten der Rack PDU eine Anforderung (in Form einer **.csr**-Datei) erstellen und an eine Zertifizierungsstelle senden. Die Zertifizierungsstelle sendet auf der Basis der in der Anforderung enthaltenen Daten ein signiertes Zertifikat (eine **.crt**-Datei) zurück. Anschließend erstellen Sie mithilfe des Sicherheitsassistenten der Rack PDU ein Server-Zertifikat (eine **.p15**-Datei) die die von der Zertifizierungsstelle zurück gesandte Signatur aus dem Stammzertifikat enthält. Das Server-Zertifikat übertragen Sie an die Rack PDU.

Sie können auch Methode 3 verwenden, wenn Ihr Unternehmen oder Ihre Behörde eine eigene Zertifizierungsstelle betreibt. In diesem Fall verwenden Sie den Sicherheitsassistenten der Rack PDU in der gleichen Weise, geben jedoch anstelle einer gewerblichen Zertifizierungsstelle Ihre eigene an.

Methode 3 bietet die folgenden Vor- und Nachteile:

- **Vorteile:**
  - Benutzername und Passwort sowie alle anderen mit der Rack PDU ausgetauschten Daten werden vor der Übertragung verschlüsselt.
  - Sie haben den Vorteil einer Authentifizierung durch eine Zertifizierungsstelle, die bereits über ein signiertes Stammzertifikat im Zertifikatspeicher des Browsers verfügt. (Die CA-Zertifikate gewerblicher Zertifizierungsstellen werden als Teil der Browser-Software vertrieben, und eine Zertifizierungsstelle Ihrer eigenen Firma oder Behörde hat wahrscheinlich bereits ihr eigenes CA-Zertifikat in den Browser-Cache der einzelnen Benutzer geladen.) Daher müssen Sie kein Stammzertifikat in die Browser der einzelnen Benutzer übertragen, die Zugriff auf die Rack PDU benötigen.
  - Sie können die Länge des *öffentlichen Schlüssels* (RSA-Schlüssels) ändern, der beim Einrichten einer SSL-Sitzung verwendet wird. (Sie können die Standardlänge von 1024 Bit oder eine Länge von 2048 Bit verwenden; letztere bietet eine besonders komplexe Verschlüsselung und ein höheres Sicherheitsniveau.)

  - Anhand des von Ihnen an die Rack PDU übertragenen Server-Zertifikats kann SSL den Datenaustausch mit der korrekten Rack PDU authentifizieren. Dadurch ist ein höheres Sicherheitsniveau gewährleistet, das über die Verschlüsselung des Benutzernamens und Passworts sowie der übertragenen Daten hinaus geht.
  - Der Browser gleicht die digitale Signatur des von Ihnen an die Rack PDU übertragenen Server-Zertifikats mit der Signatur des bereits im Browser-Cache befindlichen CA-Stammzertifikats ab, um zusätzlichen Schutz vor unbefugtem Zugriff zu erreichen.
- **Nachteile:**
  - Bei der Einrichtung muss als zusätzlicher Schritt ein signiertes Stammzertifikat von einer Zertifizierungsstelle angefordert werden.
  - Eine externe Zertifizierungsstelle erhebt unter Umständen Gebühren für die Bereitstellung signierter Zertifikate.

Firewalls

Auch wenn einige Authentifizierungsmethoden ein höheres Sicherheitsniveau als andere gewährleisten, kann ein vollständiger Schutz vor Sicherheitsverletzungen praktisch nicht erreicht werden. Eine gut konfigurierte Firewall ist daher ein wesentlicher Bestandteil eines umfassenden Sicherheitskonzepts.

Verwendung des Sicherheitsassistenten (Security Wizard) der Rack PDU

Der Sicherheitsassistent der Rack PDU erstellt für eine im Netzwerk befindliche Rack PDU Hochsicherheitskomponenten, die bei Verwendung von Secure Sockets Layer (SSL) und ähnlichen Protokollen sowie von Verschlüsselungsroutinen benötigt werden.

Authentifizierung durch Zertifikate und Host-Schlüssel

Durch die *Authentifizierung* wird die Identität eines Benutzers oder einer Netzwerkeinheit (etwa einer Rack PDU) verifiziert. Passwörter dienen in der Regel zur Identifizierung von Computerbenutzern. Für Transaktionen oder Datenübertragungen, die strengere Sicherheitsmethoden im Internet erfordern, unterstützt die Rack PDU jedoch sicherere Authentifizierungsmethoden.

- Das für sicheren Web-Zugriff verwendete Protokoll „Secure Sockets Layer“ (SSL) verwendet digitale Zertifikate zur Authentifizierung. Ein digitales *CA-Stammzertifikat* wird von einer Zertifizierungsstelle (Certificate Authority, CA) als Teil einer mit öffentlichen Schlüsseln agierenden Infrastruktur ausgestellt, und die digitale Signatur eines solchen Zertifikats muss der digitalen Signatur eines Server-Zertifikats auf der Rack PDU entsprechen.
- Secure Shell (SSH), das zum Zugriff auf die Befehlszeile der Rack PDU über ein Remote-Terminal dient, verwendet zur Authentifizierung einen öffentlichen *Host-Schlüssel*.

Wie Zertifikate verwendet werden. Die meisten Web-Browser, auch alle von der Rack PDU unterstützten Browser, enthalten mehrere CA-Stammzertifikate aller gewerblichen Zertifizierungsstellen.

Die Authentifizierung des Servers (in diesem Fall der Rack PDU) erfolgt bei jedem Verbindungsaufbau zwischen Browser und Server. Der Browser überzeugt sich davon, dass das Zertifikat des Servers von einer dem Browser bekannten Zertifizierungsstelle signiert ist.

Für die Authentifizierung müssen folgende Bedingungen erfüllt sein:

- Jeder Server (jede Rack PDU) mit aktiviertem SSL muss über ein auf dem Server selbst befindliches Server-Zertifikat verfügen.
- Jeder Browser, der zum Zugriff auf die Web-Oberfläche der Rack PDU verwendet wird, muss das zur Signierung des Server-Zertifikats verwendete CA-Stammzertifikat enthalten.

Wenn die Authentifizierung fehlschlägt, fragt der Browser nach, ob Sie fortfahren möchten, obwohl er den Server nicht authentifizieren kann.

Wenn Ihr Netzwerk die von digitalen Zertifikaten bereitgestellte Authentifizierung nicht benötigt, können Sie das von der Rack PDU automatisch erzeugte Standard-Zertifikat verwenden. Zwar wird die digitale Signatur des Standard-Zertifikats von Browsern nicht erkannt, doch können Sie mithilfe eines Standard-Zertifikats SSL zur Verschlüsselung der übertragenen Benutzernamen, Passwörter und Daten verwenden. (Wenn Sie das Standard-Zertifikat verwenden, fordert Sie der Browser auf, den Zugriff ohne Authentifizierung zu bestätigen, und meldet Sie erst danach bei der Web-Oberfläche der Rack PDU an.)

Wie SSH-Host-Schlüssel verwendet werden. Ein SSH-*Host-Schlüssel* authentifiziert die Identität des Servers (also der Rack PDU) jedesmal, wenn ein SSH-Client den betreffenden Server kontaktiert. Jeder Server mit aktiviertem SSH muss über einen auf dem Server selbst befindlichen SSH-Host-Schlüssel verfügen.

Von Ihnen für SSL- und SSH-Sicherheit erstellte Dateien

Mithilfe des Sicherheitsassistenten der Rack PDU können Sie die folgenden Komponenten eines SSL- und SSH-Sicherheitssystems erstellen:

- Das Server-Zertifikat der Rack PDU, wenn Sie die Vorteile der von einem solchen Zertifikat gebotenen Authentifizierung nutzen möchten. Sie können einen der folgenden Typen von Server-Zertifikaten erstellen:
  - Ein Server-Zertifikat, das die Signatur eines speziellen, ebenfalls vom Sicherheitsassistenten der Rack PDU erstellten CA-Stammzertifikats trägt. Verwenden Sie diese Methode, wenn Ihre Firma oder Behörde keine eigene Zertifizierungsstelle hat und Sie keine externe Zertifizierungsstelle zur Signierung des Server-Zertifikats verwenden möchten.
  - Ein von einer externen Zertifizierungsstelle signiertes Server-Zertifikat. Diese Zertifizierungsstelle kann von Ihrer eigenen Firma oder Behörde verwaltet werden, oder es kann sich dabei um eine der gewerblichen Zertifizierungsstellen handeln, deren CA-Stammzertifikate als Teil der Browser-Software vertrieben werden.
- Eine Anforderung zur Zertifikatsignierung (Certificate Signing Request, CSR), die alle für ein Server-Zertifikat benötigten Informationen enthält, mit Ausnahme der digitalen Signatur. Diese Anforderung benötigen Sie, wenn Sie eine externe Zertifizierungsstelle verwenden möchten.
- Ein CA-Stammzertifikat.
- Ein SSH-Host-Schlüssel, den das SSH-Client-Programm zur Authentifizierung der Rack PDU verwendet, wenn Sie sich bei der Befehlszeile anmelden.

Sie legen fest, ob es sich bei den vom Sicherheitsassistenten der Rack PDU erstellten öffentlichen Schlüsseln für SSL-Zertifikate und bei den Host-Schlüsseln für SSH um RSA-Schlüssel von 1024 Bit (die Grundeinstellung) oder 2048 Bit Länge handeln soll; letztere bieten eine besonders komplexe Verschlüsselung und ein höheres Sicherheitsniveau.

Wenn Sie keine SSL-Server-Zertifikate und SSH-Host-Schlüssel mit dem Sicherheitsassistenten der Rack PDU erstellen und verwenden, erzeugt die Rack PDU 2048-Bit-RSA-Schlüssel.

Nur Dell Rack PDU-Produkte können vom Sicherheitsassistenten der Rack PDU erstellte Server-Zertifikate, Host-Schlüssel und CA-Stammzertifikate verwenden. Dieses Dateien funktionieren nicht mit Produkten wie OpenSSL® oder Microsoft® Internet Information Services (IIS).

Erstellen eines Stammzertifikats und der Server-Zertifikate

Überblick

Verwenden Sie dieses Verfahren, wenn Ihre Firma oder Behörde keine eigene Zertifizierungsstelle hat und Sie keine gewerbliche Zertifizierungsstelle zur Signierung des Server-Zertifikats verwenden möchten.

Legen Sie die Größe des öffentlichen RSA-Schlüssels fest, der als Teil des vom Sicherheitsassistenten der Rack PDU erzeugten Zertifikats erstellt werden soll. Sie können einen 1024-Bit-Schlüssel oder einen 2048-Bit-Schlüssel erstellen; letzterer bietet eine besonders komplexe Verschlüsselung und ein höheres Sicherheitsniveau. (Bei Nichtverwendung des Sicherheitsassistenten erzeugt die Rack PDU standardmäßig einen 2048-Bit-Schlüssel.)

- Erstellen Sie ein CA-Stammzertifikat zur Signierung aller Server-Zertifikate, die in Verbindung mit der Rack PDU verwendet werden sollen. Hierbei werden zwei Dateien erstellt:
  - Die Datei mit der Erweiterung **.p15** ist verschlüsselt und enthält den privaten Schlüssel sowie das öffentliche Stammzertifikat der Zertifizierungsstelle. Diese Datei signiert Server-Zertifikate.
  - Die Datei mit der Erweiterung **.crt** enthält nur das öffentliche Stammzertifikat der Zertifizierungsstelle. Laden Sie diese Datei in jeden Web-Browser, der auf die Rack PDU zugreifen soll, damit der Browser das Server-Zertifikat der betreffenden Rack PDU validieren kann.
- Erstellen Sie ein Server-Zertifikat; diese wird in einer Datei mit der Erweiterung **.p15** gespeichert. Während dieses Vorgangs müssen Sie das zur Signierung des Server-Zertifikats benötigte CA-Stammzertifikat angeben.
- Laden Sie das Server-Zertifikat auf die Rack PDU.
- Wiederholen Sie die Schritte zum Erstellen und Laden des Server-Zertifikats für jede Rack PDU, die ein Server-Zertifikat benötigt.

Vorgehen

Erstellen Sie das CA-Stammzertifikat.

1. Falls der Sicherheitsassistent der Rack PDU noch nicht auf Ihrem Computer installiert ist, beschaffen Sie sich das Installationsprogramm (**Rack PDU Security Wizard.exe)** und führen Sie es aus.
2. Klicken Sie im Windows **Start**-Menü auf **Programme** und anschließend auf **Rack PDU Security Wizard**.
3. Wählen Sie in der Anzeige **Step 1** (Schritt 1) die Option **CA Root Certificate** (CA-Stammzertifikat) als zu erstellenden Dateityp aus und geben Sie dann die Länge des zu erzeugenden Schlüssels an (übernehmen Sie die Standardeinstellung 1024 Bit oder wählen Sie 2048 Bit, um eine besonders komplexe Verschlüsselung auf sehr hohem Sicherheitsniveau zu erreichen).
4. Geben Sie einen Namen für die Datei ein; diese enthält später das öffentliche Stammzertifikat und den privaten Schlüssel der Zertifizierungsstelle. Der Dateiname muss auf **.p15** enden, und die Datei wird normalerweise im Installationsordner **C:\Program Files\Dell\Rack PDU Security Wizard** erstellt.
5. Geben Sie in der Anzeige **Step 2** (Schritt 2) die Informationen ein, die zum Konfigurieren des CA-Stammzertifikats benötigt werden. Die einzigen Pflichtfelder sind **Country** (Land) und **Common Name** (Gemeinsamer Name). Geben Sie in das Feld **Common Name** (Gemeinsamer Name) einen Namen zur Identifizierung Ihrer Firma oder Behörde ein. Verwenden Sie nur alphanumerische Zeichen (keine Leerzeichen).

Ein CA-Stammzertifikat ist standardmäßig 10 Jahre ab dem Erstellungszeitpunkt gültig. Sie können diese Zeitspanne jedoch in den Feldern **Validity Period Start** (Beginn der Gültigkeitsdauer) und **Validity Period End** (Ende der Gültigkeitsdauer) ändern.

6. Überprüfen Sie in der nächsten Anzeige die Zusammenfassung der Zertifikatsdaten. Verschieben Sie die Anzeige nach unten, um sich die eindeutige Seriennummer und die Fingerprints des Zertifikats anzusehen. Klicken Sie auf **Back** (Zurück), falls Sie irgendwelche Änderungen an den von Ihnen eingegebenen Informationen vornehmen möchten. Sehen Sie sich die Informationen nochmals an.

   Die Informationen zum Eigentümer („Subject“) und Aussteller („Issuer“) des Zertifikats müssen identisch sein.

7. In der letzten Anzeige wird bestätigt, dass das Zertifikat erstellt wurde. Diese Anzeige enthält auch Informationen, die Sie für die nächsten Schritte benötigen:
   - Speicherort und Name der **.p15**-Datei, die zur Signierung der Server-Zertifikate benötigt wird.
   - Speicherort und Name der **.crt**-Datei, d. h. des CA-Stammzertifikats, das in die Browser der einzelnen Benutzer geladen wird, die auf die Rack PDU müssen.

Laden Sie das CA-Stammzertifikat in Ihren Browser. Laden Sie die **.crt**-Datei in die Browser aller Benutzer, die auf die Rack PDU zugreifen müssen.

Eine Anleitung zum Laden der **.crt**-Datei in den Zertifikatspeicher (Cache) eines Browsers finden Sie im Hilfesystem des betreffenden Browsers. Die nachstehende Verfahrensbeschreibung bezieht sich auf den Microsoft Internet Explorer.

1. Wählen Sie in der Menüleiste **Extras** und anschließend **Internetoptionen**.
2. Klicken Sie im Dialogfeld auf das Register **Inhalte**, wählen Sie die Schaltfläche **Zertifikate** und anschließend **Importieren...**.
3. Der Zertifikatimport-Assistent leitet Sie durch die restlichen Verfahrensschritte. Wählen Sie als Dateityp „X.509“. Bei dem öffentlichen CA-Stammzertifikat handelt es sich um die **.crt**-Datei, die im Verfahrensschritt Erstellen eines Stammzertifikats und der Server-Zertifikate erstellt wurde.

Erstellen Sie ein SSL-Serverbenutzer-Zertifikat.

1. Klicken Sie im Windows **Start**-Menü auf **Programme** und anschließend auf **Rack PDU Security Wizard**.
2. Wählen Sie in der Anzeige **Step 1** (Schritt 1) die Option **SSL Server Certificate** (SSL-Server-Zertifikat) als zu erstellenden Dateityp aus und geben Sie dann die Länge des zu erzeugenden Schlüssels an (übernehmen Sie die Standardeinstellung 1024 Bit oder wählen Sie 2048 Bit, um eine besonders komplexe Verschlüsselung auf sehr hohem Sicherheitsniveau zu erreichen).
3. Geben Sie einen Namen für die Datei ein; diese enthält später das Server-Zertifikat und den privaten Schlüssel. Der Dateiname muss auf **.p15** enden, und die Datei wird normalerweise im Installationsordner **C:\Program Files\Dell\Rack PDU Security Wizard** erstellt.
4. Klicken Sie auf **Browse** (Durchsuchen) und wählen Sie das im Verfahrensschritt Erstellen eines Stammzertifikats und der Server-Zertifikate erstellte CA-Stammzertifikat aus. Das CA-Stammzertifikat wird zur Signierung des erzeugten Serverbenutzer-Zertifikats verwendet.
5. Geben Sie in der Anzeige **Step 2** (Schritt 2) die Informationen ein, die zum Konfigurieren des Server-Zertifikats benötigt werden. Die einzigen Pflichtfelder sind **Country** (Land) und **Common Name** (Gemeinsamer Name). Geben Sie in das Feld **Common Name** (Gemeinsamer Name) die IP-Adresse oder den DNS-Namen des Servers (d. h. der Rack PDU) ein. Ein Server-Zertifikat ist standardmäßig 10 Jahre gültig. Sie können diese Zeitspanne jedoch in den Feldern **Validity Period Start** (Beginn der Gültigkeitsdauer) und **Validity Period End** (Ende der Gültigkeitsdauer) ändern.

   Da die Konfigurationsdaten Teil der Signatur sind, müssen diese Daten bei allen Zertifikaten eindeutig sein. Die Konfiguration eines Server-Zertifikats darf nicht mit der Konfiguration des CA-Stammzertifikats identisch sein. (Das Ablaufdatum ist nicht Bestandteil der eindeutigen Konfiguration. Es müssen sich noch weitere Konfigurationsdaten voneinander unterscheiden.)

6. Überprüfen Sie in der nächsten Anzeige die Zusammenfassung der Zertifikatsdaten. Verschieben Sie die Anzeige nach unten, um sich die eindeutige Seriennummer und die Fingerprints des Zertifikats anzusehen. Klicken Sie auf **Back** (Zurück), falls Sie irgendwelche Änderungen an den von Ihnen eingegebenen Informationen vornehmen möchten. Sehen Sie sich die Informationen nochmals an.
7. In der letzten Anzeige wird verifiziert, dass das Zertifikat erstellt wurde, und der Benutzer aufgefordert, das Server-Zertifikat in die Rack PDU zu laden. Speicherort und Name des Server-Zertifikats werden angezeigt. Die betreffende Datei hat die Erweiterung **.p15** und enthält den privaten Schlüssel und das öffentliche Stammzertifikat der Rack PDU.

Laden Sie das Server-Zertifikat auf die Rack PDU.

1. Wählen Sie auf der Registerkarte **Administration** in der oberen Menüleiste die Option **Network** und wählen Sie dann die Option **ssl certificate** unter der Überschrift **Web** im linken Navigationsmenü.
2. Wählen Sie **Add or Replace Certificate File** (Zertifikatdatei hinzufügen oder ersetzen) und navigieren Sie zu dem Server-Zertifikat, d. h. zu der **.p15**-Datei, die Sie im Verfahrensschritt Erstellen eines Stammzertifikats und der Server-Zertifikate erstellt haben. (Der Speicherort ist standardmäßig **C:\Program Files\Dell\Rack PDU Security Wizard**.)

Zum Übertragen des Server-Zertifikats können Sie auch FTP oder Secure CoPy (SCP) verwenden. Für SCP lautet der Befehl zum Übertragen eines Zertifikats mit dem Namen **cert.p15** an eine Rack PDU mit der IP-Adresse 156.205.6.185 wie folgt:

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

Erstellen eines Server-Zertifikats und eines Signing Request

Überblick

Verwenden Sie dieses Verfahren, wenn Ihre Firma oder Behörde über eine eigene Zertifizierungsstelle verfügt, oder wenn Sie eine gewerbliche Zertifizierungsstelle zur Signierung des Server-Zertifikats verwenden möchten.

- Erstellen Sie eine Certificate Signing Request (CSR). Die CSR (Anforderung zur Zertifikatsignierung) enthält alle für ein Server-Zertifikat benötigten Informationen, mit Ausnahme der digitalen Signatur. Bei diesem Vorgang entstehen zwei Ausgabedateien:
  - Die Datei mit der Erweiterung **.p15** enthält den privaten Schlüssel der Rack PDU.
  - Die Datei mit der Erweiterung **.csr** enthält die Certificate Signing Request, die Sie an eine externe Zertifizierungsstelle senden.
- Nach Rücksendung des von der Zertifizierungsstelle signierten Zertifikats importieren Sie dieses Zertifikat. Durch den Import des Zertifikats wird die **.p15**-Datei, die den privaten Schlüssel enthält, mit der Datei kombiniert, die das signierte Zertifikat der externen Zertifizierungsstelle enthält. Dabei entsteht eine verschlüsselte Server-Zertifikat-Datei mit der Erweiterung **.p15**.
- Laden Sie das Server-Zertifikat auf die Rack PDU.
- Wiederholen Sie die Schritte zum Erstellen und Laden des Server-Zertifikats für jede Rack PDU, die ein Server-Zertifikat benötigt.

Vorgehen

Erstellen Sie die Certificate Signing Request (CSR).

1. Falls der Sicherheitsassistent der Rack PDU noch nicht auf Ihrem Computer installiert ist, beschaffen Sie sich das Installationsprogramm (**Rack PDU Security Wizard.exe)** und führen Sie es aus.

2. Klicken Sie im Windows **Start**-Menü auf **Programme** und anschließend auf **Rack PDU Security Wizard**.
3. Wählen Sie in der Anzeige **Step 1** (Schritt 1) die Option **Certificate Request** (Zertifikatanforderung) als zu erstellenden Dateityp aus und geben Sie dann die Länge des zu erzeugenden Schlüssels an (übernehmen Sie die Standardeinstellung 1024 Bit oder wählen Sie 2048 Bit, um eine besonders komplexe Verschlüsselung auf sehr hohem Sicherheitsniveau zu erreichen).
4. Geben Sie einen Namen für die Datei ein; diese enthält später den privaten Schlüssel der Rack PDU. Der Dateiname muss auf **.p15** enden, und die Datei wird normalerweise im Installationsordner **C:\Program Files\Dell\Rack PDU Security Wizard** erstellt.
5. Geben Sie in der Anzeige **Step 2** (Schritt 2) die zum Konfigurieren der Anforderung zur Zertifikatsignierung (Certificate Signing Request, CSR) benötigten Informationen ein, d. h. die Daten, die im signierten Server-Zertifikat enthalten sein sollen. Die Felder **Country** (Land) und **Common Name** (Gemeinsamer Name) sind Pflichtfelder. Die anderen Felder sind wahlfrei. Geben Sie in das Feld **Common Name** (Gemeinsamer Name) die IP-Adresse oder den DNS-Namen der Rack PDU ein.

Ein Server-Zertifikat ist standardmäßig 10 Jahre ab dem Erstellungszeitpunkt gültig. Sie können diese Zeitspanne jedoch in den Feldern **Validity Period Start** (Beginn der Gültigkeitsdauer) und **Validity Period End** (Ende der Gültigkeitsdauer) ändern.

6. Überprüfen Sie in der nächsten Anzeige die Zusammenfassung der Zertifikatsdaten. Verschieben Sie die Anzeige nach unten, um sich die eindeutige Seriennummer und die Fingerprints des Zertifikats anzusehen. Klicken Sie auf **Back** (Zurück), falls Sie irgendwelche Änderungen an den von Ihnen eingegebenen Informationen vornehmen möchten. Sehen Sie sich die Informationen nochmals an.

   Die Informationen zum Eigentümer („Subject“) und Aussteller („Issuer“) des Zertifikats müssen identisch sein.

7. In der letzten Anzeige wird das Erstellen der Certificate Signing Request verifiziert und der Speicherort sowie der Name der Datei (mit der Erweiterung **.csr**) angezeigt.
8. Senden Sie die Certificate Signing Request an eine externe Zertifizierungsstelle, also entweder an eine gewerbliche Zertifizierungsstelle oder an eine gegebenenfalls von Ihrer Firma oder Behörde verwaltete Zertifizierungsstelle.

   Eine Anleitung zum Signieren und Ausstellen von Server-Zertifikaten erhalten Sie von der Zertifizierungsstelle.

Importieren Sie das signierte Zertifikat. Importieren Sie das von der externen Zertifizierungsstelle zurücksendete, signierte Zertifikat. Hierbei werden das signierte Zertifikat und der private Schlüssel zu einem SSL-Server-Zertifikat kombiniert, das Sie anschließend an die Rack PDU übertragen.

1. Klicken Sie im Windows **Start**-Menü auf **Programme** und anschließend auf **Rack PDU Security Wizard**.
2. Wählen Sie in der Anzeige **Step 1** (Schritt 1) die Option **Import Signed Certificate** (Signierte Zertifikate importieren).
3. Navigieren Sie zu dem signierten Server-Zertifikat, das Sie von der externen Zertifizierungsstelle erhalten haben. Die Datei hat die Erweiterung **.cer** oder **.crt**.
4. Navigieren Sie zu der Datei, die Sie in Schritt 4 des Verfahrens Erstellen Sie die Certificate Signing Request (CSR) erstellt haben, und wählen Sie sie aus. Diese Datei hat die Erweiterung **.p15** und enthält den privaten Schlüssel der Rack PDU. Standardmäßig befindet sie sich im Installationsordner **C:\Program Files\Dell\Rack PDU Security Wizard**.
5. Geben Sie einen Namen für die resultierende Datei an, die das signierte Server-Zertifikat enthalten wird und anschließend an die Rack PDU übertragen werden soll. Die Datei muss die **.p15** besitzen.
6. Klicken Sie auf **Next** (Weiter), um das Server-Zertifikat zu erzeugen. Unter **Issuer Information** (Ausstellerdaten) wird in der Übersichtsanzeige bestätigt, dass die externe Zertifizierungsstelle das Zertifikat signiert hat.
7. In der letzten Anzeige wird verifiziert, dass das Zertifikat erstellt wurde, und der Benutzer aufgefordert, das Server-Zertifikat in die Rack PDU zu laden. Hier werden Speicherort und Name des Server-Zertifikats (mit der Erweiterung **.p15**) angezeigt, das den privaten Schlüssel der Rack PDU und den aus der **.cer**- oder **.crt**-Datei bezogenen öffentlichen Schlüssel enthält.

Laden Sie das Server-Zertifikat auf die Rack PDU.

1. Wählen Sie auf der Registerkarte **Administration** in der oberen Menüleiste die Option **Network** und wählen Sie dann die Option **ssl certificate** unter der Überschrift **Web** im linken Navigationsmenü.
2. Wählen Sie **Add or Replace Certificate File** (Zertifikatdatei hinzufügen oder ersetzen) und navigieren Sie zu dem Server-Zertifikat, d. h. zu der **.p15**-Datei, die Sie im Verfahrensschritt Erstellen eines Stammzertifikats und der Server-Zertifikate erstellt haben. (Der Speicherort ist standardmäßig **C:\Program Files\Dell\Rack PDU Security Wizard**.)

Zum Übertragen des Server-Zertifikats an die Rack PDU können Sie auch FTP oder Secure CoPy (SCP) verwenden. Für SCP lautet der Befehl zum Übertragen eines Zertifikats mit dem Namen **cert.p15** an ein Rack PDU mit der IP-Adresse 156.205.6.185 wie folgt:

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

Erstellen eines SSH-Host-Schlüssels

Überblick

Dieses Verfahren ist wahlfrei. Wenn Sie sich für SSH-Verschlüsselung entschieden haben, jedoch keinen Host-Schlüssel erstellen, erzeugt die Rack PDU beim Neustart einen 2048-Bit-RSA-Schlüssel. Dabei geben Sie an, ob die vom Sicherheitsassistenten der Rack PDU erstellten SSH-Host-Schlüssel als 1024-Bit- oder 2048-Bit-RSA-Schlüssel angelegt werden sollen.

Sie können einen 1024-Bit-Schlüssel oder einen 2048-Bit-Schlüssel erzeugen. Letzterer bietet eine besonders komplexe Verschlüsselung und ein höheres Sicherheitsniveau.

- Erstellen Sie mithilfe des Sicherheitsassistenten der Rack PDU einen Host-Schlüssel. Dieser wird verschlüsselt und in einer Datei mit der Erweiterung **.p15** gespeichert.
- Übertragen Sie den Host-Schlüssel an die Rack PDU.

Vorgehen

Erstellen Sie den Host-Schlüssel.

1. Falls der Sicherheitsassistent der Rack PDU noch nicht auf Ihrem Computer installiert ist, beschaffen Sie sich das Installationsprogramm (**Rack PDU Security Wizard.exe)** und führen Sie es aus.
2. Klicken Sie im Windows **Start**-Menü auf **Programme** und anschließend auf **Rack PDU Security Wizard**.
3. Wählen Sie in der Anzeige **Step 1** (Schritt 1) die Option **SSH Server Host Key** (SSH-Server-Host-Schlüssel) als zu erstellenden Dateityp aus und geben Sie dann die Länge des zu erzeugenden Schlüssels an (übernehmen Sie die Standardeinstellung 1024 Bit oder wählen Sie 2048 Bit, um eine besonders komplexe Verschlüsselung auf sehr hohem Sicherheitsniveau zu erreichen).
4. Geben Sie einen Namen für die Datei ein; diese enthält später den Host-Schlüssel. Die Datei muss die **.p15** besitzen. Die Datei wird normalerweise im Installationsordner **C:\Program Files\Dell\Rack PDU Security Wizard** erstellt.
5. Klicken Sie auf **Next** (Weiter), um den Host-Schlüssel zu erzeugen.
6. In der Übersichtsanzeige werden die Fingerprints der SSH-Version 2 angezeigt; diese identifizieren jeden Host-Schlüssel eindeutig. Nachdem Sie den Host-Schlüssel an die Rack PDU übertragen haben, können Sie sich davon überzeugen, dass auch wirklich der korrekte Host-Schlüssel übertragen wurde, indem Sie die hier angezeigten Fingerprints mit den SSH-Fingerprints auf der Rack PDU vergleichen, wie vom SSH-Client-Programm angezeigt. Beide Fingerprints müssen identisch sein.
7. In der letzten Anzeige wird das Erstellen des Host-Schlüssels verifiziert und der Benutzer aufgefordert, den Host-Schlüssel an die Rack PDU zu übertragen. Zudem werden Speicherort und Name des Host-Schlüssels (mit der Dateinamenserweiterung **.p15**) angezeigt.

Übertragen Sie den Host-Schlüssel an die Rack PDU.

1. Wählen Sie auf der Registerkarte **Administration** in der oberen Menüleiste die Option **Network** und wählen Sie dann die Option **ssh host key** unter der Überschrift **Console** im linken Navigationsmenü.
2. Wählen Sie **Add or Replace Host Key** (Host-Schlüssel hinzufügen oder ersetzen) und navigieren Sie zu dem Host-Schlüssel, d. h. zu der **.p15**-Datei, die Sie im Verfahrensschritt Erstellen Sie den Host-Schlüssel erstellt haben. (Der Speicherort ist standardmäßig **C:\Program Files\Dell\Rack PDU Security Wizard**.)
3. Beachten Sie den im unteren Bereich der Seite **User Host Key** (Benutzer-Host-Schlüssel) angezeigten SSH-Fingerprint. Melden Sie sich über das SSH-Client-Programm bei der Rack PDU an und überzeugen Sie sich davon, dass auch wirklich der korrekte Host-Schlüssel übertragen wurde, indem Sie die hier angezeigten Fingerprints mit denen vergleichen, die im SSH-Client-Programm angezeigt werden. Beide Fingerprints müssen identisch sein.

Zum Übertragen der Host-Schlüssel-Datei an die Rack PDU können Sie auch FTP oder Secure CoPy (SCP) verwenden. Für SCP lautet der Befehl zum Übertragen eines Host-Schlüssels mit dem Namen **hostkey.p15** an eine Rack PDU mit der IP-Adresse 156.205.6.185 wie folgt:

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

Zugriff über die Befehlszeile und Sicherheitsaspekte

Administratoren und Benutzer mit dem Kontotyp „Gerät“ können über Telnet oder Secure SHell (SSH)auf die Befehlszeile zugreifen, je nachdem, was aktiviert ist. (Als Administrator öffnen Sie zum Aktivieren oder Deaktivieren dieser Zugriffsmethoden in der oberen Menüleiste der Registerkarte **Administration** das Menü **Network** und wählen dann die Option **access** (Zugriff) unter der Überschrift **Console**.) Standardmäßig ist Telnet aktiviert. Wenn SSH aktiviert wird, wird Telnet automatisch deaktiviert.

Telnet für einfachen Zugriff. Telnet bietet als einfachen Sicherheitsmechanismus eine Authentifizierung mit Anmeldename und Passwort. Es bietet jedoch nicht die Sicherheit einer verschlüsselten Anmeldung.

SSH für den Zugriff auf hoher Sicherheitsstufe. Wenn Sie für die Weboberfläche den hohen Sicherheitsstandard von SSL nutzen, verwenden Sie Secure SHell (SSH) für den Zugriff auf die Befehlszeilenoberfläche. SSH verschlüsselt Benutzernamen, Passwörter und übertragene Daten.

Die Schnittstelle, die Benutzerkonten und die Zugriffsrechte des Benutzers sind immer gleich, unabhängig davon, ob der Zugriff auf die Befehlszeile über SSH oder Telnet erfolgt. Um SSH verwenden zu können, müssen Sie SSH jedoch zuerst konfigurieren und einen SSH-Client auf dem Computer installieren.

Telnet und Secure Shell (SSH)

Solange SSH aktiviert ist, können Sie nicht über Telnet auf die Befehlszeile zugreifen. Wenn SSH aktiviert wird, wird SCP automatisch deaktiviert.

Wenn SSH aktiviert und der dazugehörige Port konfiguriert ist, ist keine weitere Konfiguration erforderlich, um Secure CoPy (SCP) verwenden zu können. SCP verwendet dieselbe Konfiguration wie SSH.

Damit Sie SSH verwenden können, muss ein SSH-Client installiert sein. Im Gegensatz zu Microsoft Windows-Betriebssystemen, beinhalten die meisten Linux-Distributionen und sonstigen UNIX®-Plattformen einen SSH-Client. SSH-Clients können von verschiedenen Anbietern bezogen werden.

Do konfigurieren Sie die Port-Einstellungen für Telnet und SSH.

1. Wählen Sie auf der Web-Oberfläche auf der Registerkarte **Administration** die Option **Network** in der oberen Menüleiste und klicken Sie auf **access** (Zugriff) unter der Überschrift **Console** im linken Navigationsmenü.
2. Konfigurieren Sie die Port-Einstellungen für Telnet und SSH.

   Informationen zur Erhöhung des Sicherheitsniveaus durch Auswahl eines Nicht-Standard-Ports finden Sie unter Zuweisen von Ports.

3. Wählen Sie unter **Console** im linken Navigationsmenü die Option **ssh host key** (SSH-Host-Schlüssel), wählen Sie eine zuvor mit dem Sicherheitsassistenten der Rack PDU erstellte Host-Schlüssel-Datei aus und übertragen Sie diese an die Rack PDU.

   Wenn Sie hier keine Host-Schlüssel-Datei auswählen, einen ungültigen Host-Schlüssel installieren oder SSH ohne installierten Host-Schlüssel aktivieren, erzeugt die Rack PDU eine RSA-Host-Schlüssel mit einer Länge von 2048 Bit. Damit die Rack PDU einen Host-Schlüssel erstellen kann, muss sie neu gestartet werden. **Es kann bis zu einer Minute dauern, bis die Rack PDU diesen Host-Schlüssel erstellt hat; während dieser Zeit ist SSH nicht verfügbar.**

   Sie haben auch die Möglichkeit, die Host-Schlüssel-Datei z. B. über die Befehlszeile eines Windows-Betriebssystems per FTP oder Secure CoPy (SCP) zu übertragen.

4. Lassen Sie sich den *Fingerprint* des SSH-Host-Schlüssels für SSH Version 2 anzeigen. Bei den meisten SSH-Clients wird der Fingerprint zu Beginn der Sitzung angezeigt. Vergleichen Sie den vom Client angezeigten Fingerprint mit demjenigen, der zuvor auf der Web-Oberfläche oder in der Befehlszeile der Rack PDU angezeigt worden war.

Zugriff über die Befehlszeile und Sicherheitsaspekte: HTTP und HTTPS (mit SSL)

Das Hypertext Transfer Protocol (HTTP) ermöglicht den Web-Zugriff per Benutzername und Passwort, überträgt die Benutzernamen, Passwörter und Daten jedoch unverschlüsselt. Das HyperText Transfer Protocol over Secure Sockets Layer (HTTPS) verschlüsselt Benutzernamen, Passwörter und Daten während der Übertragung und ermöglicht eine Authentifizierung der Rack PDU mittels digitaler Zertifikate.

Entscheidungshilfen zur Auswahl einer Methode für die Verwendung digitaler Zertifikate finden Sie unter Erstellen und Installieren von digitalen Zertifikaten.

So konfigurieren Sie HTTP und HTTPS:

1. Wählen Sie auf der Registerkarte **Administration** in der oberen Menüleiste die Option **Network** und wählen Sie dann die Option **access** (Zugriff) unter der Überschrift **Web** im linken Navigationsmenü.
2. Aktivieren Sie HTTP oder HTTPS und konfigurieren Sie die Ports, die von den Protokollen jeweils verwendet werden. Die Änderungen werden bei der nächsten Anmeldung wirksam. Wenn SSL aktiviert ist, wird im Browser ein kleines Schloss-Symbol angezeigt.

Informationen zur Erhöhung des Sicherheitsniveaus durch Auswahl eines Nicht-Standard-Ports finden Sie unter Zuweisen von Ports.

3. Wählen Sie die Option **ssl certificate** unter **Web** im linken Navigationsmenü, um festzustellen, ob ein Server-Zertifikat auf der Rack PDU installiert ist. Falls mit dem Sicherheitsassistenten der Rack PDU ein Zertifikat erstellt, dieses jedoch nicht installiert wurde:
   - Navigieren Sie auf der Web-Oberfläche zu der Zertifikatdatei und übertragen Sie diese an die Rack PDU.
   - Zum Übertragen der Zertifikatdatei an die Rack PDU können Sie auch das Protokoll Secure CoPy (SCP) oder FTP verwenden.

Durch das vorherige Erstellen und Übertragen eines Server-Zertifikats wird weniger Zeit zum Aktivieren von HTTPS benötigt. Wenn Sie HTTPS ohne installiertes Server-Zertifikat aktivieren, erstellt die Rack PDU das fehlende Zertifikat beim nächsten Neustart. **Es kann bis zu einer Minute dauern, bis die Rack PDU das Zertifikat erstellt hat; während dieser Zeit ist der SSL-Server nicht verfügbar.**

Bei einem von der Rack PDU erzeugten Zertifikat sind bestimmte Einschränkungen zu beachten. Siehe Methode 1: Verwendung des von der Rack PDU automatisch erzeugten Standard-Zertifikats.

4. Wenn ein gültiges digitales Server-Zertifikat geladen wurde, enthält der Feld **Status** den dazugehörigen Link. **Valid Certificate** (Gültiges Zertifikat). Klicken Sie auf diesen Link, um sich die Parameter des Zertifikats anzusehen.

Parameter	Beschreibung
Issued To:	**Common Name (CN)** (Gemeinsamer Name): Die IP-Adresse oder der DNS-Name der Rack PDU. Dieses Feld bestimmt, wie Sie sich bei der Web-Oberfläche anmelden müssen. • Wenn beim Erstellen des Zertifikats eine IP-Adresse für dieses Feld angegeben wurde, melden Sie sich mit der IP-Adresse an. • Wenn beim Erstellen des Zertifikats der DNS-Name für dieses Feld angegeben wurde, melden Sie sich mit dem DNS-Namen an. Wenn Sie bei der Anmeldung weder die für das Zertifikat festgelegte IP-Adresse noch den DNS-Namen verwenden, kann die Authentifizierung nicht durchgeführt werden, und Sie werden in einer entsprechenden Meldung gefragt, ob Sie fortfahren möchten. Bei einem von der Rack PDU standardmäßig erzeugten Server-Zertifikat enthält dieses Feld statt dessen die Seriennummer der Rack PDU. **Organization (O)**, **Organizational Unit (OU**)und **Locality, Country:** Name, Organisationeinheit und Standort der Organisation, die das Server-Zertifikat verwendet. Bei einem von der Rack PDU standardmäßig erzeugten Server-Zertifikat enthält das Feld **Organizational Unit (OU)** den Eintrag „Internally Generated Certificate“ (Intern erzeugtes Zertifikat). **Serial Number**: Die Seriennummer des Server-Zertifikats.
Issued By:	**Common Name (CN)**: Der im CA-Stammzertifikat angegebene gemeinsame Name. Bei einem von der Rack PDU standardmäßig erzeugten Server-Zertifikat enthält dieses Feld statt dessen die Seriennummer der Rack PDU. **Organization (O)** und **Organizational Unit (OU**): Name und Organisationeinheit der Organisation, die das Server-Zertifikat ausgestellt hat. Bei einem von der Rack PDU oder einem Gerät standardmäßig erzeugten Server-Zertifikat enthält dieses Feld den Eintrag „Internally Generated Certificate“ (Intern erzeugtes Zertifikat).
Validity:	**Issued on**: Datum und Uhrzeit der Ausstellung des Zertifikats. **Expires on**: Datum und Uhrzeit des Ablaufs des Zertifikats.

Parameter	Beschreibung
Fingerprints	Bei den beiden Fingerprints handelt es sich jeweils um eine lange, durch Doppelpunkte getrennte alphanumerische Zeichenfolge. Ein Fingerprint ist eine eindeutige Kennung zur erweiterten Authentifizierung des Servers. Erfassen Sie die Fingerprints, um sie mit den im Zertifikat enthaltenen und im Browser angezeigten Fingerprints zu vergleichen. **SHA1 Fingerprint**: Ein Fingerprint, der mit einem Secure Hash-Algorithmus (SHA-1) erstellt wurde. **MD5 Fingerprint**: Ein Fingerprint, der mit einem Message Digest 5-Algorithmus (MD5) erstellt wurde.

Unterstützte RADIUS-Funktionen und -Server

Unterstützte Funktionen

Unterstützte Authentifizierungs- und Autorisierungsfunktionen: Remote Authentication Dial-In User Service (RADIUS). Mit RADIUS können Sie Fernzugriffe für jede Rack PDU zentral verwalten. Wenn ein Benutzer auf die Rack PDU zugreift, wird eine Authentifizierungsanfrage an den RADIUS-Server gesendet, um die Zugriffsebene des Benutzers festzustellen.

Weitere Informationen zu Zugriffsebenen finden Sie unter Benutzerkontotypen.

Unterstützte RADIUS-Server

Unterstützte RADIUS-Server: FreeRADIUS und Microsoft IAS 2003. Andere gängige RADIUS-Anwendungen funktionieren möglicherweise auch, wurden jedoch nicht eingehend getestet.

Konfigurieren der Rack PDU

Authentifizierung

Für die Rack PDU verwendete RADIUS-Benutzernamen dürfen maximal 32 Zeichen enthalten.

Wählen Sie auf der Registerkarte **Administration** in der oberen Menüleiste die Option **Security**. Wählen Sie dann unter **Remote Users** im linken Navigationsmenü die Option **authentication**, um eine Authentifizierungsmethode festzulegen:

- **Local Authentication Only**: RADIUS ist deaktiviert. Lokale Authentifizierung ist aktiviert.
- **RADIUS, then Local Authentication** (RADIUS, dann lokale Authentifizierung): RADIUS-Authentifizierung und lokale Authentifizierung sind aktiviert. Zuerst wird die Authentifizierung vom RADIUS-Server angefordert; nur wenn der RADIUS-Server nicht reagiert, wird die lokale Authentifizierung verwendet.
- **RADIUS Only**: RADIUS ist aktiviert. Lokale Authentifizierung ist deaktiviert.

Wenn **RADIUS Only** (Nur RADIUS) ausgewählt ist und wenn der RADIUS-Server nicht verfügbar ist, nicht richtig identifiziert wurde oder falsch konfiguriert ist, steht der Fernzugriff nicht zur Verfügung, unabhängig vom Benutzerkontotyp. In diesem Fall müssen Sie über die serielle Schnittstelle eine Befehlszeile öffnen und die Zugriffseinstellung für RADIUS in `local` oder `radiusLocal` umändern, um wieder Zugriff zu erhalten. Mit dem folgenden Befehl können Sie die Zugriffseinstellung beispielsweise in `local` umändern:

```
radius -a local
```

RADIUS

Zum Konfigurieren von RADIUS wählen Sie auf der Registerkarte **Administration** in der oberen Menüleiste die Option **Security**. Wählen Sie dann unter **Remote Users** im linken Navigationsmenü die Option **RADIUS**.

Einstellung	Beschreibung
RADIUS Server	Der Servername oder die IP-Adresse des RADIUS-Servers. **HINWEIS:** RADIUS-Server verwenden normalerweise Port 1812, um Benutzer zu authentifizieren. Wenn Sie einen anderen Port verwenden möchten, hängen Sie an den Namen des RADIUS-Servers oder an dessen IP-Adresse einen Doppelpunkt an, gefolgt von der neuen Port-Nummer.
Secret	Der vom RADIUS-Server und von der Rack PDU verwendete geheime Schlüssel.
Reply Timeout	Die Zeit in Sekunden, die die Rack PDU auf eine Antwort vom RADIUS-Server wartet.
Test Settings	Geben Sie den Benutzernamen und das Passwort des Administrators sein, um den Pfad zu dem von Ihnen konfigurierten RADIUS-Server zu testen.
Skip Test and Apply	Hiermit wird der Test des Pfads zum RADIUS-Server unterlassen.

Hiermit legen Sie fest, welcher RADIUS-Server Benutzer authentifizieren soll, wenn zwei konfigurierte Server vorhanden sind, und wenn als Authentifizierungsmethode **RADIUS, then Local Authentication** (RADIUS, danach lokale Authentifizierung) oder **RADIUS Only** (Nur RADIUS) aktiviert ist. Klicken Sie dazu auf die Schaltfläche **Switch Server Priority** (Server-Priorität ändern).

Konfigurieren des RADIUS-Servers

Sie müssen den RADIUS-Server konfigurieren, um mit der Rack PDU arbeiten zu können. Die Beispiele in diesem Abschnitt unterscheiden sich möglicherweise etwas, von den Inhalten oder Formaten, die der von Ihnen verwendete RADIUS-Server benötigt. Wenn in diesen Beispielen von Ausgangsanschlüssen („Outlets“) die Rede ist, bezieht sich dies nur auf Rack PDUs, die den Benutzer „Ausgangsanschluss“ unterstützen.

1. Tragen Sie die IP-Adresse der Rack PDU in die Datei mit der Client-Liste des RADIUS-Servers ein.
2. Zu jedem Benutzer muss ein Diensttyp-Attribut konfiguriert werden, sofern statt dessen keine Vendor Specific Attributes (VSA) definiert sind. Wenn kein Diensttyp-Attribut konfiguriert ist, hat der Benutzer schreibgeschützten Zugriff (nur über die Web-Oberfläche). Als Diensttyp sind nur zwei Werte zulässig: „Administrative-User“ (6, erteilt dem Benutzer Administratorrechte) und „Login-User“ (1, erteilt dem Benutzer Geräterechte).

Informationen zur Radius-Benutzerdatei finden Sie in der Dokumentation zum RADIUS-Server.

Beispiel für die Verwendung von Diensttyp-Attributen

Im nachstehenden Beispiel für eine RADIUS-Benutzerdatei gilt Folgendes:

- **`RPDUAdmin`** entspricht **`Service-Type: Administrative-User, (6)`**
- **`RPDUDevice`** entspricht **`Service-Type: Login-User, (1)`**
- **`RPDUReadOnly`** entspricht **`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"
```

Beispiele für Vendor Specific Attributes

Vendor Specific Attributes („herstellerspezifische Attribute“, VSA) können statt der vom RADIUS-Server bereitgestellten Diensttyp-Attribute verwendet werden. Für diese Methode wird ein Wörterbucheintrag und eine RADIUS-Benutzerdatei benötigt. In der Wörterbuchdatei können Sie die Bezeichnungen für die Schlüsselwörter ATTRIBUTE und VALUE definieren, nicht jedoch für die numerischen Werte. Wenn Sie die numerischen Werte ändern, kann keine zuverlässige RADIUS-Authentifizierung und -Autorisierung durchgeführt werden. VSA haben Vorrang vor den standardmäßigen RADIUS-Attributen.

Wörterbuchdatei. Hier ein Beispiel für eine RADIUS-Wörterbuchdatei (dictionary.dell):

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

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

RADIUS-Benutzerdatei mit VSA. Nachfolgend ein Beispiel für eine RADIUS-Benutzerdatei mit 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

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

Beachten Sie auch die folgenden verwandten Themen:

- Informationen zu den drei grundlegenden Zugriffsebenen (für Administratoren sowie für die Benutzer „Gerät“ und „Schreibgeschützt“) finden Sie unter Benutzerkontotypen.
- Informationen zu von uns getesteten und unterstützten RADIUS-Servern finden Sie unter Unterstützte RADIUS-Server.

Beispiel mit UNIX-Shadow-Passwörtern. Wenn UNIX-Shadow-Passwortdateien (**/etc/passwd**) in Verbindung mit RADIUS-Wörterbuchdateien verwendet werden, können Benutzer mit den beiden folgenden Methoden authentifiziert werden:

- Wenn alle UNIX-Benutzer über Administratorrechte verfügen, tragen Sie die nachstehenden Zeilen in die RADIUS-Benutzerdatei „user“ ein. Wenn die Berechtigung nur für den Benutzer „Gerät“ gelten soll, ändern Sie den DELL-Diensttyp („DELL-Service-Type“) in **`Device`** um.

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

- Fügen Sie Benutzernamen und Attribute in die RADIUS-Benutzerdatei „user“ ein und gleichen Sie das Passwort mit **/etc/passwd** ab. Das folgende Beispiel gilt für die Benutzer **`bconners`** und **`thawk`**:

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

Index

Zahlen

10/100 Base-T-Anschluss, Frontblende 12
10/100-LED, Frontblende 12, 15

A

Abschnittsüberschriften, Benutzerkonfigurationsdatei 194
Absenderadresse (SMTP-Einstellung) 154
Aktivieren
  E-Mail an Empfänger 155
  E-Mail-Weiterleitung an externe SMTP-Server 156
  SSH-Versionen 177
  Telnet 177
  Umgekehrte Suche 132
Aktualisieren der Firmware 199
Aktualisierungsintervall, Einstellen von Datum und Uhrzeit 187
Alarmzustand, Eingangskontakte 127
Alle zurücksetzen 191
Anmeldedatum und -uhrzeit
  Steuerkonsole 20
Anmelden
  Web-Oberfläche 87
  Zugriffsprioritäten 2
Anmeldung
  lokal (über eine serielle Schnittstelle) an der Steuerkonsole 18
Anschlussgeschwindigkeit, Konfigurieren für Ethernet 171
Anzeigen des Protokolls in einem neuen Fenster, JavaScript als Voraussetzung 130
Ausgangsanschlüsse
  globale 100
Ausgangsanschlussereignisse
  Beschreibung 113, 118
Ausgangsanschlussgruppen
  aktivieren 104
  auslösende 100
  Bearbeiten 107
  Erstellen lokaler Gruppen 106
  globale 100
  lokale 100
  Löschen 107
  mitlaufende 101
  Regeln für Konfiguration 103
  Systemanforderungen 102
  typische Konfigurationen 109
  Zweck und Vorteile 101
Auslösende Ausgangsanschlussgruppen 100
Authentifizierung
  gegenüber der Web-Oberfläche und Befehlszeile 220
  mit RADIUS 256
  mit SNMPv3 219
  mit SSL 223
Authentifizierung von Benutzern über RADIUS 142
Authentifizierungs-Traps, Einstellung 158
Automatische Abmeldung bei Inaktivität 147

B

Befehlszeile 16
  Anmeldung 16
  Befehlsrückgabe-Codes 24
  Befehlssyntax 23

Beschreibung der Befehle 25
? 25
about 25
alarmcount 26
boot 27
cd 28
console 29
date 30, 36
delete 31
devLowLoad 48
devNearOver 48
devOverLoad 49
devReading 50
devStartDly 51
dir 31
dns 32
eventlog 33
exit 33
format 34
FTP 34
help 35
humLow 52
humMin 53
humReading 53
inNormal 54
inReading 54
netstat 35
olAssignUsr 55
olCancelCmd 56
olDlyOff 57
olDlyOn 58
olDlyReboot 59
olGroups 60
olLowLoad 61
olName 62
olNearOver 63
olOff 64
olOffDelay 65
olOn 66
olOnDelay 67
olOverLoad 68
olRboot 71
olRbootTime 69
olReading 70
olStatus 72
olUnasgnUsr 73
phLowLoad 74
phNearOver 75
phOverLoad 76
phReading 77
phRestrictn 78
ping 37
portSpeed 37
prodInfo 79
prompt 38
quit 38
radius 39
reboot 40
resetToDef 41
sensorName 80
system 42
tcpip 43, 44
tempHigh 81
tempMax 82
tempReading 83
user 45
userAdd 83
userDelete 83
userList 84
userPasswd 85
web 46
whoami 85
xferINI 47
xferStatus 47
Fernzugriff 16
Hauptmaske 19
Konfigurieren der TCP/IP-Einstellungen 8
Konfigurieren des Zugriffs 177
Benachrichtigung, Verzögerung oder Wiederholung 150
Benutzerkonfigurationsdateien
Abrufen und Exportieren 193
Anpassen 195
Ereignis- und Fehlermeldungen zur Dateiübertragung 197
gerätespezifische Werte außer Kraft setzen 194
Inhalt 194

Meldungen zu nicht entdeckten Geräten 198
separates Exportieren der Systemzeit 195
Verwendung der Datei als Boot-Datei bei DHCP 168
Verwendung von Dateiübertragungsprotokollen zur Übertragung 196
Benutzername
Vorgabe nach Kontotyp 87
Benutzername, sofort ändern aus Sicherheitsgründen 217
Benutzernamen
Festlegen für die einzelnen Kontotypen 141
maximale Zeichenanzahl für RADIUS 142
Betriebszeit
auf der Web-Oberfläche 192
Hauptmaske der Steuerkonsole 20
BOOTP
Kommunikation zwischen Rack PDU und BOOTP-Server 6
Status-LED zum Hinweis auf BOOTP-Anfragen 14
Browser
CA-Zertifikate im Browser-Speicher (Cache) 223
Fehlermeldungen 89
Gefahr bei Nichtbeenden des Browsers 224
Schloss-Symbol bei installiertem SSL 222
unterstützte Typen und Versionen 86

C

Cipher Suites
Zweck der Algorithmen und Codes 224
Coldstart Delay (Kaltstartverzögerung) 99
Community-Name
für Trap-Empfänger 158

D

Date & Time, Einstellungen für 187
Datenprotokoll
Abrufen per FTP oder SCP 136
Importieren in Tabellenkalkulation 136
Protokollintervall (Einstellung) 134
Rotation (Archivierung) 135
Datumsformat, konfigurieren 188
Deaktivieren
E-Mail an Empfänger 155
Telnet 177
Umgekehrte Suche 132
Verwendung eines Proxyservers 87
Device Manager (Geräte-Manager), Registerkarte 97
DHCP
Hersteller-Cookie 167
Kommunikation zwischen Rack PDU und DHCP-Server 7
DNS
Abfragetypen 173
Festlegen von DNS-Servern mittels IP-Adresse 172

E

Einheiten, einstellen 190
Einstellungen für Ausgangsanschlüsse
konfigurieren 115
Kontrollieren der Ausgangsanschlüsse 112
E-Mail
für Paging verwenden 155
Konfigurieren von Benachrichtigungsparametern 153
Konfigurieren von Empfängern 155
Testnachricht 156
Empfängeradresse, E-Mail-Empfänger 155
Environment (Umgebung), Registerkarte 125

Ereignisaktionen 149
Konfigurieren nach Ereignis 150
Konfigurieren nach Gruppe 151
Ereignisprotokoll
Abrufen per FTP oder SCP 136
anzeigen und verwenden 129
Fehlermeldungen durch außer Kraft gesetzte Werte in INI-Dateien 198
Ergebniscodes für die letzte Übertragung 204
Ethernet-Anschlussgeschwindigkeit 171
event.txt (Datei)
Importieren in Tabellenkalkulation 136
Inhalt 136

F

Facility Code (Einrichtungscode), Syslog-Einstellung 161
Fehlermeldungen
Browser 89
durch außer Kraft gesetzte Werte in INI-Dateien 198
Feuchtigkeitssensor
Konfigurieren von Grenzwerten 125
Fingerprints, Anzeigen und Vergleichen 250
Firmware
Aktualisieren mehrerer Rack PDUs gleichzeitig 203
Dateiübertragungsverfahren
FTP oder SCP 201
XMODEM 203
Vorteile der Aktualisierung 199
FTP
Deaktivieren von FTP bei Verwendung von SSH und SCP 222
Server-Einstellungen 184
Übertragen von Firmware-Dateien 201
Verwendung eines Nicht-Standard-Ports für zusätzliche Sicherheit 218
zum Abrufen eines Ereignis- oder Datenprotokolls 136
zum Übertragen von Host-Schlüsseln 250
zum Übertragen von Server-Zertifikaten 239, 252
Funktionstaste 12

G

Globale Ausgangsanschlüsse 100
Globale Ausgangsanschlussgruppen 100
Erstellen 107
Überprüfen von Einrichtung und Konfiguration 111

H

Hauptmaske
Anmeldedatum und -uhrzeit 20
Anzeige der Firmwareversion 20
Benutzerzugriff anzeigen 20
Betriebszeit 20
Identifizierung anzeigen 20
Status 21
Home (Registerkarte) 93
Hostname für Trap-Empfänger 157
Host-Schlüssel
Erstellen mit dem Sicherheitsassistenten 245
Hinzufügen oder ersetzen 178
Status 178
Übertragen an die Rack PDU 250
Hysterese 126

I

Identifikationsfelder in der Hauptmaske 20
Identifizierung (Name, Standort und Ansprechpartner)
  auf der Web-Oberfläche 186
Identifizierung eines Ansprechpartners (zur Kontaktaufnahme) 186
In der Hauptmaske angezeigte Firmwareversionen 20
Info-Optionen
  für Informationen zur Rack PDU 192
INI-Dateien, *Siehe* Benutzerkonfigurationsdateien

J

JavaScript, Voraussetzung zum Anzeigen des Protokolls in einem neuen Fenster 130

K

Konfigurieren
  RADIUS-Authentifizierung 143
  SSH 249
  SSL 251

L

Lastgrenzen 98
Laststatus 97
LED-Anzeige, Frontblende 12
Letzte Ereignisse
  Geräteereignisse auf Startseite 94
Link (als Einstellung für Ausgangsanschlüsse) 115
Links, Konfiguration 192
Lokale Ausgangsanschlussgruppen 100
  Erstellen 106
Lokale Benutzer, Einrichten von Zugriffsrechten 140
Lokaler SMTP-Server
  Definieren mittels IP-Adresse oder DNS-Name 154
  empfohlene Option für E-Mail-Routing 156

M

Menüs
  Benachrichtigung 149
  Logs (Protokolle) 128
  Netzwerk 163
  Sicherheit 139
Message Generation (Nachrichtengenerierung), Syslog-Einstellung 161
Mit NTP-Server synchronisieren (Datum und Uhrzeit) 187
Mitlaufende Ausgangsanschlussgruppen 101

N

Network (Netzwerk), Menü 163
Network Time Protocol (NTP) 187
Netzwerk-Status-LED, Frontblende 12, 14
Neustart
  Ausgangsanschlüsse 113, 118
NMS-IP/Hostname für Trap-Empfänger 157
Notification (Benachrichtigung), Menü 149
Nur zurücksetzen 191

O

Override (Schlüsselwort), Benutzerkonfigurationsdatei 194

P

Paging
per E-Mail 155
Passwörter
Datenprotokollarchiv 135
Festlegen für die einzelnen Kontotypen 141
sofort ändern aus Sicherheitsgründen 217
Verwendung von Nicht-Standard-Ports für zusätzliche Sicherheit 218
Vorgabe für alle Kontotypen 87
Wiederherstellung 9
Phasen-LEDs, Frontblende 11
Ping-Befehl bei der Problembehandlung 206
Ports
FTP-Server 34, 184
HTTP und HTTPS 175
RADIUS-Server 40, 143
Telnet und SSH 177
Ports, zuweisen 218
Potentialfreie Kontakte
Eingänge an der Frontblende 11
konfigurieren 127
Power Off Delay (Abschaltverzögerung) 115
Power On Delay (Einschaltverzögerung) 115
Primärer NTP-Server 187
Problembehandlung
Checkliste 206
Einstellung „RADIUS Only“ bei nicht verfügbarem RADIUS-Server 143
Probleme beim Zugriff auf die Rack PDU 206
Proxyserver
Umgehung für PDU konfigurieren 87
Verwendung deaktivieren 87

Q

Quick Links 92
Quick Links, Konfiguration 192

R

Rack PDU
erste Schritte 4
Frontblende 11
Funktionen des Produkts 1
Konfigurieren von Name und Standort 99
Zugriffsprobleme beheben 206
RADIUS
Konfiguration 143
Server-Konfiguration 145
unterstützte RADIUS-Server 146
RADIUS-Server-Einstellung 257
Reboot Duration (Neustartdauer) 115
Remote-Benutzer
Authentifizierung 142
Einrichten von Zugriffsrechten 142

S

Schlüsselwörter in Benutzerkonfigurationsdatei 194
SCP
aktiviert und konfiguriert bei SSH 222, 249
für Dateiübertragungen auf hoher Sicherheitsstufe 184
für verschlüsselte Dateiübertragung 221
Übertragen von Firmware-Dateien 201
Verwendung eines Nicht-Standard-Ports 218
zum Abrufen eines Ereignis- oder Datenprotokolls 136
zum Übertragen von Host-Schlüsseln 247
zum Übertragen von Server-Zertifikaten 239, 244
Secure CoPy. *Siehe* SCP.
Secure SHell. *Siehe* SSH.
Secure Sockets Layer. *Siehe* SSL

Security (Sicherheit), Menü
RADIUS-Einstellungen 257
Remote-Benutzer, Authentifizierung 256
Security Wizard (Sicherheitsassistent)
Erstellen von Signing Requests 240
Erstellen von SSH-Host-Schlüsseln 245
Erstellen von Zertifikaten
Zertifizierungsstelle 240
Sekundärer NTP-Server 187
serieller RJ-45-Anschluss, Frontblende 13
Server-Zertifikate
Erstellen für eine Zertifizierungsstelle 240
Erstellen ohne Zertifizierungsstelle 235
Severity Mapping (Schweregradzuordnung), Syslog-Einstellung 161
Sicherheit
Authentifizierung
mit SSH und SCP 220
über digitale Zertifikate mit SSL 223
über RADIUS 256
Certificate Signing Requests 223
Deaktivieren weniger sicherer Schnittstellen 220, 222
SCP als Alternative zu FTP 222
sofortiges Ändern von Benutzername und Passwort 217
SSL
Algorithmen und Codes in Cipher Suites 224
Wahl einer Methode zur Verwendung von Zertifikaten 225
Übersicht über die Zugriffsmethoden 214
unterstützte SSH-Clients 249
Verschlüsselung mit SSH und SCP 220
Verwendung von Nicht-Standard-Ports für zusätzliche Sicherheit 218
wie SSH-Host-Schlüssel verwendet werden 232
wie Zertifikate verwendet werden 232
Sicherheitsassistent (Security Wizard)
Erstellen von Zertifikaten
ohne Zertifizierungsstelle 235
Signing Requests, erstellen 240
SMTP-Server
Auswählen für E-Mail-Empfänger 156
Einstellungen 154
SMTP-Server des Empfängers 156
SNMP
Authentifizierungs-Traps 158
Deaktivieren von SNMPv1 für Systeme mit hohem Sicherheitsbedarf 179
v1
deaktivieren 218
READ-Zugriff 218
v3
Authentifizierung 219
Verschlüsselung 220
Zugriff und Zugriffssteuerung
SNMPv1 180
SNMPv3 181
Sommerzeit 188
Spitzenlast 97
Zurücksetzen, kWh
zurücksetzen 100
SSH 17
aktivieren 249
Beschaffung eines SSH-Clients 249
Fingerprints, Anzeigen und Vergleichen 250
Host-Schlüssel 178
als fälschungssichere Kennung 220
Erstellen mit dem Sicherheitsassistenten 245
Übertragen an die Rack PDU 250
konfigurieren 249
Verschlüsselung 220
SSL
Authentifizierung über digitale Zertifikate 223
Certificate Signing Requests 223
Erstellen, Anzeigen und Entfernen von Zertifikaten 176
Stammzertifikate, Erstellen 235
Standort (Systemwert) 186

Status
in der Hauptmaske der Steuerkonsole 21
Syslog
Identifizierung von Syslog-Server und -Port 160
Zuordnung von Ereignis-Schweregraden an Syslog-Prioritäten 161
Systemanforderungen, Ausgangsanschlussgruppen 102
Systemname 186

T

TCP/IP-Konfiguration 5, 8
Telnet 17
Temperatur-/Feuchtigkeitssensor, Anschluss an Frontblende 12
Temperatureinheiten (Fahrenheit oder Celsius) 190
Temperatursensor
Konfigurieren von Grenzwerten 125
Test
DNS-Abfrage 173
Einstellungen für E-Mail-Empfänger 156
Trap-Empfänger 159
Testen
Pfad zum RADIUS-Server 144
Timeout bei Inaktivität 147
Timeout-Einstellung für RADIUS 144, 257
Trap-Generierung, für Trap-Empfänger 157
Traps
Trap-Empfänger 157

U

Übertragungsereignis 197
Uhrzeit des lokalen Computers übernehmen 187
Umgekehrte Suche 132
Update Using NTP Now (Jetzt mit NTP aktualisieren, Datum und Uhrzeit), Einstellung 187
URL-Adressformate 88

V

Verschlüsselung
mit SNMPv3 220
mit SSH und SCP für die Befehlszeile 220
mit SSL für die Web-Oberfläche 251
Verwaltung
Network (Netzwerk), Menü 163
Notification (Benachrichtigung), Menü 148
Security (Sicherheit), Menü 139
Verwaltungsschnittstelle neu starten 191

W

Web-Oberfläche 90
Anmeldung 87
Konfigurieren des Zugriffs 175
URL-Adressformate 88
Zugriffsprobleme beheben 207

X

XMODEM zur Übertragung von Firmware-Dateien 203

Z

Zeiteinstellung 187
Zeitzone, zur Synchronisierung mit NTP-Server 187
Zertifikate
Erstellen und Installieren für SSL 225

Methoden
Sicherheitsassistent der Rack PDU erstellt alle Zertifikate 227
Standard-Zertifikat verwenden 226
Zertifizierungsstelle (Certificate Authority, CA) verwenden 229
Wahl einer Methode 225
Zertifikate, Erstellen, Anzeigen und Entfernen 176
Zugriff
Aktivieren oder Deaktivieren von Zugriffsmethoden
auf die Befehlszeile 177
auf die Web-Oberfläche 175
auf die Befehlszeile
Fernzugriff 16
Prioritäten 2
Problembehandlung 207
Zugriffsrechte der Benutzer
Identifizierung über die Anzeige der Steuerkonsole 20
Zugriffsrechte der Benutzer, Kontotypen 3

BENUTZERHANDBUCH

Metered Rack PDU (Überwachte Verteilerleiste)

11/2010 Teilenummer 990-3926-005

www.dell.com | support.dell.com