NetShelter™ Advanced 11000 Series Rack Power Distribution Units

Benutzerhandbuch

DE TME47353B
Freigabedatum: 01/2025

www.se.com

Rechtliche Informationen

Die in diesem Dokument enthaltenen Informationen umfassen allgemeine Beschreibungen, technische Merkmale und Kenndaten und/oder Empfehlungen in Bezug auf Produkte/Lösungen.

Dieses Dokument dient nicht als Ersatz für eine detaillierte Studie oder betriebliche und standortspezifische Entwicklung oder schematische Planung. Sie dürfen nicht zur Bestimmung der Eignung oder Zuverlässigkeit der Produkte/Lösungen für bestimmte Benutzeranwendungen verwendet werden. Es ist die Pflicht eines solchen Benutzers, die angemessene und umfassende Risikoanalyse, Bewertung und Prüfung der Produkte/Lösungen in Bezug auf die jeweilige spezifische Anwendung oder Verwendung durchzuführen oder von einem professionellen Experten seiner Wahl (Integrator, Spezifizierer oder dergleichen) davon durchführen zu lassen.

Die Marke Schneider Electric sowie alle anderen in diesem Dokument enthaltenen Markenzeichen von Schneider Electric SE und seinen Tochtergesellschaften sind das Eigentum von Schneider Electric SE oder seine Tochtergesellschaften. Alle anderen Marken können Markenzeichen ihrer jeweiligen Eigentümer sein.

Schneider Electric gewährt keine Rechte oder Lizenzen für die kommerzielle Nutzung des Dokuments oder seines Inhalts, mit Ausnahme einer nicht ausschließlichen und persönlichen Lizenz, es „wie besehen“ zu konsultieren.

Schneider Electric behält sich das Recht vor, jederzeit ohne entsprechende schriftliche Vorankündigung Änderungen oder Aktualisierungen mit Bezug auf den Inhalt bzw. am Inhalt dieses Dokuments oder dessen Format vorzunehmen.

Soweit gesetzlich zulässig, übernehmen Schneider Electric und seine Tochtergesellschaften keine Verantwortung oder Haftung für Fehler oder Auslassungen im Informationsinhalt dieses Dokuments sowie für die nicht beabsichtigte Verwendung oder den Missbrauch des Inhalts.

Inhaltsverzeichnis

Einführung

Produkteigenschaften

Die NetShelter APDU11000 schaltbare Rack Power Distribution Unit (PDU) von APC by Schneider Electric kann als eigenständiges, netzwerkbasiertes Stromverteilungsgerät verwendet werden, oder es können bis zu 32 Geräte über eine Netzwerkverbindung miteinander verbunden werden. Die Rack PDU ermöglicht eine Echtzeit-Fernüberwachung der angeschlossenen Lasten. Benutzerdefinierte Alarme warnen vor potenziellen Überlastungen der Schaltkreise. Die Rack PDU gibt Ihnen über entfernte Befehle und Einstellmöglichkeiten der Benutzeroberfläche die uneingeschränkte Kontrolle über die Ausgangsanschlüsse.

Sie können eine NetShelter APDU11000 Switched Rack PDU über die Web User Interface (UI), die Command Line Interface (CLI), StruxureWare Data Center Expert oder Simple Network Management Protocol (SNMP) verwalten. (Informationen zur Verwendung der PowerNet-MIB mit einem SNMP-Browser finden Sie im PowerNet SNMP Management Information Base (MIB)-Referenzhandbuch unter **www.se.com**).

NetShelter APDU11000 Series Switched Rack PDU haben Sie diese zusätzlichen Funktionen:

- Überwachung von Geräteleistung, Spitzenleistung, Scheinleistung, Leistungsfaktor und Energie.
- Überwachung von Phasenspannung, Strom, Spitzenstrom, Leistung, Scheinleistung und Leistungsfaktor.
- Bankstrom und Spitzenstrom (für Modelle, die Leistungsschalterbänke unterstützen).
- Konfigurierbare Alarmschwellen, die Netzwerkalarme und visuelle Alarme bei Schaltkreisüberlastung bereitstellen.
- Verschiedene Zugriffsebenen: Super-Benutzer, Administrator, Gerätebenutzer, Nur-Lese-Benutzer, Ausgangsbenutzer und Nur-Netzwerk-Benutzer (Diese Benutzer sind durch Benutzername und Passwort geschützt).
- Mehrbenutzer-Login-Funktion, bei der bis zu vier Benutzer gleichzeitig angemeldet sein können.
- Ferngesteuerte individuelle Ausgangskontrolle.
- Konfigurierbare Ein- oder Ausschaltverzögerungen.
- Ereignis- und Datenprotokollierung. Auf das Ereignisprotokoll kann über Telnet, Secure Copy Protocol (SCP), File Transfer Protocol (FTP), Serial connection oder einen Webbrowser (über HTTPS-Zugriff mit SSL/TLS oder HTTP-Zugriff) zugegriffen werden. Auf das Datenprotokoll kann über einen Web-Browser, SCP oder FTP zugegriffen werden.
- Unterstützung für Modbus TCP. Sie können diese Funktion verwenden, um die Rack PDU über ein Gebäudemanagementsystem zu überwachen.

  Die Registerzuordnungsdatei kann heruntergeladen werden unter https://www.apc.com/us/en/download/document/TME45037/
- E-Mail-Benachrichtigungen zu Systemereignissen der Rack PDU Network Management Card (NMC).
- SNMP traps, Syslog-Meldungen und E-Mail-Benachrichtigungen basierend auf dem Schweregrad oder der Kategorie der Rack PDU- und NMC-Systemereignisses.
- Sicherheitsprotokolle für Authentifizierung und Verschlüsselung.
- Network Port Sharing (NPS). Bis zu 32 APDU11000 Series Rack PDUs können über die In/Out Ports miteinander verbunden werden, sodass nur eine einzige Netzwerkverbindung erforderlich ist.
- Über die Funktion für automatische Firmware-Updates auf Gastsystemen kann NPS an die angeschlossenen Gastsysteme automatisch ein Firmware-Update übergeben.
- Protokolldateien können heruntergeladen werden, indem ein USB-Stick in den USB-Port an der Anzeigeschnittstelle der Rack PDU eingesteckt wird.

HINWEIS: Die Rack PDU bietet keinen Überspannungsschutz. Um sicherzustellen, dass das Gerät vor Stromausfall oder Spannungsspitzen geschützt ist, schließen Sie die Rack PDU an eine unterbrechungsfreie Stromversorgung (UPS) von APC by Schneider Electric an.

Informationen zu Netzwerkmanagement-Karten

Die Schneider Electric Network Management Card (NMC) ermöglicht die grundlegende und sichere Fernüberwachung und -verwaltung Ihrer Rack PDU.

Um sicherzustellen, dass Ihre Netzwerkmanagement-Karte über die neueste Firmware verfügt, die unabhängig voneinander gemäß IEC 62443-4-2 zertifiziert ist, enthält die NMC ein 1-Jahres-Abonnement für Secure NMC System (SNS).

Weitere Informationen, einschließlich der neuesten Dokumentation, finden Sie unter www.apc.com/secure-nmc. Wählen Sie die Software- und Firmware-Registerkarte aus, um das NMC-Systemupdate-Tool für Ihr Gerät herunterzuladen. Wählen Sie die Dokumente-Registerkarte aus, um das Secure NMC System (SNS)-Tool User Guide herunterzuladen.

HINWEIS: SNS-Abonnements sind derzeit in China oder Japan nicht verfügbar. Das SNS-Tool unterstützt derzeit nur Windows-Benutzer.

Arten von Benutzerkonten

Die Rack PDU verfügt über verschiedene Zugriffsebenen (Super-Benutzer, Administrator, Gerätebenutzer, Nur-Lese-Benutzer und Nur-Netzwerk-Benutzer), die durch Benutzername und Passwort geschützt sind. Es können sich bis zu vier Benutzer gleichzeitig an derselben Rack PDU anmelden.

- Ein Administrator oder Super-Benutzer kann alle Menüs der Web-UI und alle Befehle der CLI verwenden. Benutzer vom Typ Administrator können gelöscht werden, nicht jedoch der Super-Benutzer. Standard-Benutzername und -Kennwort für den Super-Benutzer sind beide **apc**. Der Super-Benutzer oder Administrator kann eines anderen Administratorkontos verwalten (aktivieren, deaktivieren, Kennwort ändern, usw.)
- Ein Gerätebenutzer hat Lese- und Schreibzugriff auf die für ein Gerät relevanten Bildschirmanzeigen. Administrative Funktionen wie die Sitzungsverwaltung im Sicherheit-Menü und Firewall unter Protokolle sind für diese Benutzerebene nicht verfügbar.
- Ein Nur-Lese-Benutzer hat Zugriff auf dieselben Menüs wie ein Gerätebenutzer, aber ohne die Möglichkeit, Konfigurationen zu ändern, Geräte zu steuern, Daten zu löschen, oder Dateiübertragungsoptionen verwenden. Die Links zu den Konfigurationsoptionen werden zwar angezeigt, sind jedoch deaktiviert. In den Ereignis- und Datenprotokollen wird keine Schaltfläche zum Löschen des Protokolls angezeigt.
- Ein Ausgangsbenutzer hat Zugriff über die Web-UI und die CLI. Der Ausgangsbenutzer hat Zugriff auf dieselben Menüs wie ein Gerätebenutzer, aber mit eingeschränkter Fähigkeit, Konfigurationen zu ändern, Geräte zu steuern, Daten zu löschen oder Dateiübertragungsoptionen zu verwenden. Links zu Konfigurationsoptionen sind sichtbar, aber deaktiviert. Der Ausgangsbenutzer hat Zugriff auf die Menüoption Ausgangsteuerung, mit der der Benutzer nur die vom Administrator zugewiesenen Ausgänge steuern kann. Ausgangsbenutzer können die Ereignis- oder Datenprotokolle nicht löschen. Benutzername und Passwort werden vom Administrator während des Hinzufügens eines neuen Ausgangsbenutzers festgelegt.
- Ein Nur-Netzwerk-Benutzer (Remotebenutzer) kann sich nur über die Web-UI und die CLI (Telnet oder SSH) anmelden. Ein Nur-Netzwerk-Benutzer hat nur Lese-/Schreibzugriff auf die netzwerkbezogenen Menüs.

Watchdog-Funktionen

Überblick

Zur Erkennung interner Probleme und zur Wiederherstellung nach unerwarteten Eingängen verwendet die Rack PDU interne, systemweite Watchdog-Mechanismen. Bei einem Neustart nach einem internen Problem wird ein Network Interface Restarted Ereignis im Ereignisprotokoll aufgezeichnet.

Mechanismus der Network Interface Watchdog

Die Rack PDU implementiert interne Watchdog-Mechanismen, um zu verhindern, dass sie über das Netzwerk nicht mehr zugänglich ist. Wenn die Rack PDU beispielsweise 9,5 minutes lang keinen direkten oder indirekten Netzverkehr (z.B. SNMP-Daten oder Daten für Broadcast-Nachrichten wie Adressauflösungsprotokoll [ARP] empfängt, geht sie davon aus, dass ein Problem mit ihrer Netzwerkschnittstelle vorliegt, und startet anschließend neu. Der Watchdog-Mechanismus für die Netzwerkschnittstelle ist nur auf einer PDU aktiviert, die beim Start eine aktive Netzwerkschnittstellenverbindung erkennt. Dadurch können Gast-PDUs in einer Network Port Sharing-Kette normal funktionieren, ohne dass alle 9,5 Minuten ein Neustart durchgeführt werden muss.

Zurücksetzen des Netzwerk-Timers

Stellen Sie sicher, dass die Rack PDU nicht neu gestartet wird, wenn 9,5 Minuten lang keine Daten über das Netzwerk übertragen wurden. Die Rack PDU versucht alle 4,5 Minuten, das Standardgateway zu erreichen. Wenn das Gateway vorhanden ist, antwortet es der Rack PDU und die Antwort startet den 9,5-minute timer neu. Wenn Ihre Applikation kein Gateway benötigt oder über ein solches verfügt, geben Sie die IP-Adresse eines Computers an, der im Netzwerk ausgeführt wird und sich im gleichen Subnetz befindet. Der Netzwerkverkehr dieses Computers führt zum Neustart des 9,5-minute timer, der den Neustart der Rack PDU verhindert.

Network Port Sharing (NPS)

Informationen zur Network Port Sharing-Funktion

Sie können die Funktion Network Port Sharing verwenden, um den Status von bis zu 32 Rack PDUs über nur eine Netzwerkverbindung anzuzeigen, zu konfigurieren und zu verwalten. Ermöglicht wird dies durch den Anschluss der Rack PDUs über die A- und B-Ports an der Frontplatte der Rack PDU.

> **HINWEIS:** Alle Rack PDUs in der Gruppe müssen aus der APDU11000-Serie stammen und dieselbe Firmware-Version der Rack PDU verwenden. Daten von Gastgeräten werden dem Benutzer erst angezeigt, wenn die Gast-PDUs auf die Firmware-Version der Host-PDU aktualisiert wurden. Der APDU11000 Series Rack PDU NPS Host vergleicht seine eigene Firmware-Version mit den Versionen, die auf jedem Gast gefunden werden. Im Falle eines Versionsunterschieds kopiert der Host seine Firmware über die NPS-Kette auf die nicht konformen Gäste.

Display ID

Die Display-ID ist eine Zahl von 1 bis 32, die verwendet wird, um die Rack PDUs in einer Gruppe eindeutig zu identifizieren. Nachdem zwei oder mehr Rack PDUs in einer NPS-Gruppe miteinander verbunden wurden, können sie über diese „Display-ID“ an den verschiedenen Schnittstellen identifiziert werden. Sie können diese Display-ID in der oberen linken Ecke des LCD-Displays anzeigen. Alternativ kann eine größere Display-ID „Schatten“ auf der LCD-Anzeige aktiviert werden, indem Sie die Option **Display Settings > Display ID > Show** auf dem LCD-Tastenfeld auswählen.

Installationsanweisungen

Schließen Sie bis zu 32 Rack PDUs über die Link A- und B-Ports an der Frontseite jedes Geräts an.

> **HINWEIS:** Um mögliche Kommunikationsprobleme zu verhindern, sollte die Gesamtlänge der Kabelverbindungen (Cat5e+) zwischen den Rack PDUs in einer Gruppe 10 Meter nicht überschreiten.

Verbinden Sie eine der zur Gruppe gehörenden Rack PDUs über den Anschluss "Network" mit einem Hub oder Switch im Netzwerk. Diese Einheit dient als Host für die Rack PDU-Gruppe. Die Daten der Gast-PDU können auf der Host-PDU angezeigt werden. Richten Sie die Netzwerkfunktionalität für diese Host-PDU ein, wie im Abschnitt „Netzwerkeinstellungen einrichten“ angegeben. Die Host-PDU erkennt automatisch alle über die A- und B-Ports verbundenen Gast-PDUs. Die Rack PDU-Gruppe ist jetzt über die IP-Adresse der Host PDU verfügbar.

HINWEIS: Es darf immer nur eine Rack PDU in einer NPS-Gruppe Host sein. Wenn zwei Host-Einheiten miteinander verbunden sind, wird automatisch eine als einzelner Host für die NPS-Gruppe ausgewählt. Sie haben auch die Möglichkeit, einen bestimmten Gast als Host auszuwählen, solange dieser Gast über eine aktive Netzwerkverbindung verfügt.

Die Host Rack PDU unterstützt viele Funktionen, die vom NPS-Gäste nicht unterstützt werden. Hierzu gehören unter anderem:

- SNMP rPDU2 Gruppen-OIDs
- Initiieren von AOS/APP-Firmware-Updates für Gast Rack PDUs
- Zeitsynchronisation für Gast Rack PDUs
- Datenprotokollierung für die Gast Rack PDUs

Spezifisch Zuweisung von Display-IDs

Die Display-ID kann über die Web-Benutzeroberfläche im Feld "Configuration > RPDU > Device > Display ID" konfiguriert werden. Die Display-ID kann auch über die CLI-Schnittstelle über den Befehl `dispID` oder von SNMP über OID rPDU2DeviceConfigModule konfiguriert werden.

Sie können bestimmte Display-IDs zuweisen, indem Sie die Geräte zum ersten Mal manuell in der gewünschten Reihenfolge (1 bis 32) einschalten.

Um die Display-ID-Reihenfolge direkt von den Rack PDUs aus zu konfigurieren, befolgen Sie die nachstehenden Anweisungen, bevor Sie eine der Rack PDUs in der Gruppe einschalten.

1. Bestimmen Sie vor dem Einschalten von Rack PDUs, die in einer Gruppe angeschlossen sind, die gewünschte Reihenfolge der Display-IDs.
2. Schalten Sie zuerst das Gerät ein, dessen Display-ID 1 angezeigt werden soll.
3. Nachdem das Gerät initialisiert wurde und das LCD mit der Anzeige seiner Bildschirme begonnen hat, schalten Sie das Gerät ein, dessen Display-ID 2 angezeigt werden soll.
4. Fahren Sie auf die gleiche Weise für die restlichen Einheiten fort, wie es für Ihre Einrichtung zutrifft.

Firmware-Aktualisierung mit NPS

Beim Start und routinemäßig während des Betriebs vergleicht der NPS-Host seine eigene Firmware Version mit der Versionen gefunden an jeder Gast. Im Falle eines Versionsunterschieds kopiert der Host seine Firmware über die NPS-Kette auf die nicht konformen Gäste.

HINWEIS: Geräte, die nicht dieselbe Firmwareversion unterstützen, können keine NPS-Gruppen bilden.

Erste Schritte

So starten Sie die Rack PDU:

1. Installieren Sie die Rack PDU gemäß den Installationsanweisungen für die Rack Power Distribution Unit, die mit Ihrer Rack PDU geliefert wurden.
2. Schalten Sie die Stromversorgung ein und verbinden Sie sich mit Ihrem Netzwerk. Befolgen Sie die Anweisungen in den Installationsanweisungen für die Rack Power Distribution Unit.
3. Netzwerkeinstellungen einrichten.
4. Beginnen Sie mit der Verwendung der Rack PDU anhand eines der folgenden Abschnitte in diesem Handbuch:
   - Web User Interface
   - Command Line Interface
   - Displaykonsole der Rack PDU

Netzwerkeinstellungen einrichten

IPv4-Ersteinrichtung

Sie müssen drei TCP/IP-Einstellungen für die Rack PDU definieren, bevor sie im Netzwerk betrieben werden kann.

- Die IP-Adresse der Rack PDU
- Die Subnetzmaske der Rack PDU
- Die IP-Adresse des Standard-Gateways (wird nur benötigt, wenn Sie das Segment verlassen)

  HINWEIS: Wenn ein Standardgateway nicht verfügbar ist, verwenden Sie die IP-Adresse eines Computers der sich im selben Subnetz wie die Rack PDU befindet und normalerweise ausgeführt wird. Die Rack PDU verwendet das Standard-Gateway, um das Netzwerk zu testen, wenn der Datenverkehr sehr gering ist.

  HINWEIS: Verwenden Sie nicht dieselbe Loopback-Adresse (121.0.0.1) wie die Standardad-Gateway. Dadurch wird die Karte deaktiviert. Zur erneuten Aktivierung müssen Sie sich über eine serielle Verbindung anmelden und die TCP/IP-Einstellungen auf ihre Standardwerte zurücksetzen.

Ausführliche Informationen zur Verwendung eines DHCP-Servers zum Konfigurieren der TCP/IP-Einstellungen an einer Rack PDU finden Sie unter **DHCP Response Options** in diesem Handbuch.

IPv6-Ersteinrichtung

Die IPv6-Netzwerkkonfiguration bietet Flexibilität, um Ihren Anforderungen gerecht zu werden. IPv6 kann überall dort verwendet werden, wo eine IP-Adresse auf dieser Schnittstelle eingegeben wird. Sie können die Konfiguration manuell, automatisch oder über DHCP vornehmen.

TCP/IP-Konfigurationsmethoden

Verwenden Sie eine der folgenden Methoden, um die von der Rack PDU benötigten TCP/IP-Einstellungen zu definieren (siehe in diesem Handbuch).

- Geräte-IP-Konfigurations-Assistent
- DHCP- und BOOTP-Konfiguration
- Command Line Interface

Dienstprogramm für .ini file

Sie können das Dienstprogramm zum Exportieren von .ini file verwenden, um .ini file-Einstellungen von konfigurierten Rack PDUs auf eine oder mehrere nicht konfigurierte Rack PDUs zu exportieren. Für mehr Informationen, siehe **Erstellen und Importieren von Einstellungen mit der config File (Creating and Importing Settings with the config File)** in diesem Handbuch.

DHCP- und BOOTP-Konfiguration

Bei der standardmäßigen TCP/IP-Konfigurationseinstellung DHCP wird davon ausgegangen, dass ein ordnungsgemäß konfigurierter DHCP-Server verfügbar ist, um TCP/IP-Einstellungen für die Rack PDU bereitzustellen. Sie können die Einstellung auch für BOOTP konfigurieren.

Sie können eine benutzerdefinierte Initialisierungsdatei (.ini) zum Anmelden des Geräts an einem BOOTP- oder DHCP-Server verwenden. Weitere Informationen finden Sie unter „Erstellen und Importieren von Einstellungen mit der config file (Creating and importing settings with the config file)“ in diesem Handbuch.

Wenn keiner dieser Server verfügbar ist, lesen Sie den Abschnitt „Assistent zur Geräte-IP-Konfiguration (Device IP Configuration Wizard)“ in diesem Handbuch.

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

Geben Sie in der BOOTPTAB-Datei des BOOTP-Servers die Rack PDU’s MAC address, IP address, subnet mask, and default gateway sowie optional einen Bootdateinamen ein. Die MAC-Adresse finden Sie auf der Unterseite der Rack-RDU oder auf dem in der Verpackung enthaltenen Qualitätskontrollabschnitt.

Wenn die Rack PDU neu gestartet wird, stellt der BOOTP-Server ihr die TCP/IP-Einstellungen zur Verfügung.

- Wenn Sie einen BOOTP-Dateinamen angegeben haben, versucht die Rack PDU, diese Datei mit TFTP oder FTP vom BOOTP-Server zu übertragen. Die Rack PDU übernimmt alle Einstellungen aus der BOOTP-Datei.
- Wenn Sie keinen BOOTP-Dateinamen angegeben haben, können Sie die anderen Einstellungen der Rack PDU remote über die Web User Interface oder die Command Line Interface konfigurieren, die in diesem Handbuch beschrieben werden.
- Der Benutzername und das Passwort lauten in der Standardeinstellung **apc**. Informationen zum Erstellen einer Bootup-Datei finden Sie in der Dokumentation Ihres BOOTP-Servers.

DHCP: Sie können einen RFC2131/RFC2132-kompatiblen DHCP-Server verwenden, um die TCP/IP-Einstellungen für die Rack PDU zu konfigurieren.

In diesem Abschnitt wird die Kommunikation der Rack PDU mit einem DHCP-Server zusammengefasst. Ausführlichere Informationen darüber, wie ein DHCP-Server die Netzwerkeinstellungen für eine PDU konfigurieren kann, finden Sie in diesem Handbuch unter „DHCP-Antwortoptionen (DHCP response options)“.

1. Die Rack PDU sendet eine DHCP-Anforderung aus, die Folgendes verwendet, um sich selbst zu identifizieren:
   - Ein Herstellerklassenbezeichner (Standardwert: APC)
   - Eine Client-Kennung (standardmäßig die MAC-Adresse der Rack PDU)
   - Ein Benutzerklassenbezeichner (standardmäßig die Identifizierung der Applikationsfirmware Installiert an der Rack- PDU). Dies ist bekannt als DHCP-Option 12.
2. Ein ordnungsgemäß konfigurierter DHCP-Server antwortet mit einem DHCP-Vorschlag, der alle Einstellungen enthält, die die Rack PDU für die Netzwerkkommunikation benötigt. Das DHCP-Angebot enthält auch die Option Herstellerspezifische Informationen (DHCP-Option 43). Die Rack PDU kann so konfiguriert werden, dass sie DHCP-Vorschläge ignoriert, die in DHCP-Option 43 keinen APC-Cookie im nachfolgend aufgeführten Hexadezimalformat enthalten. Die Rack-PDU erfordert dieses Cookie standardmäßig nicht.
   ```
   Option 43 = 01 04 31 41 50 43
   ```

Wobei:

- Das erste Byte (01) ist der Code.
- Das zweite Byte (04) ist die Länge.
- Die restlichen Bytes (31 41 50 43) sind das APC-Cookie.

Informationen zum Hinzufügen von Code zur Herstellerspezifische Informationen-Option finden Sie in der Dokumentation Ihres DHCP-Servers.
HINWEIS: Durch Aktivieren des Kontrollkästchens Herstellerspezifisches Cookie erforderlich zum Akzeptieren der DHCP-Adresse in der Web-UI können Sie vom DHCP-Server verlangen, dass er ein APC-Cookie bereitstellt, das Informationen an die Rack PDU liefert.

Netzwerkmanagement mit sonstigen Applikationen

Diese Applikationen und Dienstprogramme arbeiten mit einer Rack PDU, die mit dem Netzwerk verbunden ist.

- PowerNet® Management Information Base (MIB) mit einem Standard-MIB-Browser: Führen Sie SNMP SETs und GETs aus und verwenden Sie SNMP-Traps.
- StruxureWare Data Center Expert: Energiemanagement auf Unternehmensebene und Management von Agenten, Rack PDUs, und Umwelt-Monitors.
- Assistent für die Konfiguration von Geräte-IP-Adressen: Konfigurieren Sie die Grundeinstellungen einer oder mehrerer Rack PDUs über das Netzwerk. Siehe „Assistent für die Konfiguration von (Device IP Configuration Utility)“ in diesem Handbuch.
- Sicherheitsassistent: Erstellen Sie Komponenten, die für die Sicherheit der Rack PDUs erforderlich sind, wenn Sie Secure Sockets Layer (SSL) oder Transport Layer Security (TLS) und zugehörige Protokolle und Verschlüsselungsroutinen verwenden.

Command Line Interface (CLI)

HINWEIS: Diese Aufgabe wird ausgeführt, wenn keine anderen Benutzer an einer Schnittstelle der PDU angemeldet sind.

1. Melden Sie sich bei der CLI an.
2. Wenden Sie sich an Ihren Netzwerkadministrator, um die IP-Adresse, die Subnetzmaske und das Standardgateway für die Rack PDU zu erhalten.
3. Verwenden Sie zur Konfigurierung der Netzwerkeinstellungen die drei Befehle. (Kursiver Text kennzeichnet eine Variable.)
   ```
   tcpip -i yourIPaddress
   tcpip -s yoursubnetmask
   tcpip -g yourDefaultGateway
   ```
   Geben Sie für jede Variable einen numerischen Wert im Format `xxx.xxx.xxx.xxx` ein. Um beispielsweise eine System-IP-Adresse von 156.205.14.141 festzulegen, geben Sie den folgenden Befehl ein und drücken Sie die EINGABE taste:
   ```
   tcpip -i 156.205.14.141
   ```
4. Geben Sie `exit` ein. Die Rack PDU wird daraufhin neu gestartet, um die Änderungen zu übernehmen.

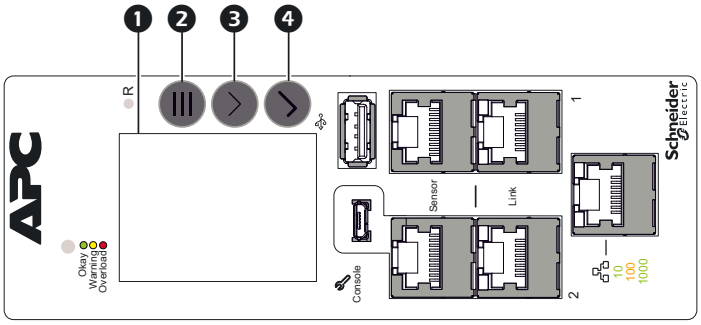
Zugriff nach Verlust des Passworts

HINWEIS: Durch Zurücksetzen der Rack PDU wird das Gerät auf seine Standardkonfiguration zurückgesetzt. Sie sollten die .ini file nach der Konfiguration Ihrer Rack PDU und bewahren Sie sie an einem sicheren Ort auf. Wenn Sie diese Datei gespeichert haben, können Sie Ihre Konfiguration nach einem verlorenen Kennwortereignis abrufen.

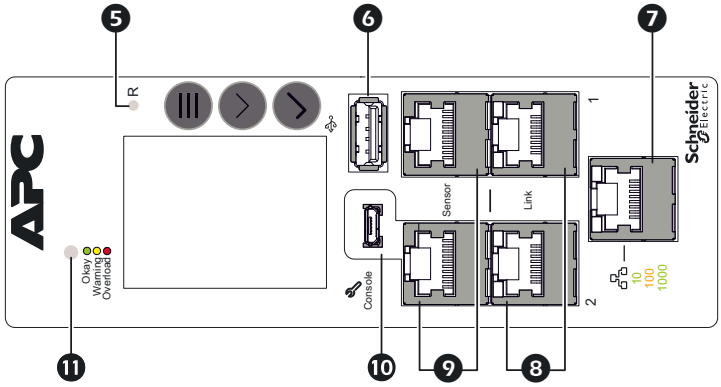
Sie können jede sichere Schnittstelle verwenden, um den Wiederherstellungsprozess abzuschließen. Dies umfasst die lokale CLI über eine serielle Verbindung, die entfernte CLI über SSH oder das Internet über HTTPS. Alle diese Punkte werden in diesem Handbuch behandelt.

1. Halten Sie die **Reset**-Taste 30 seconds lang gedrückt, um sicherzustellen, dass die Status-LED während dieser Zeit grün pulsiert. Wenn die Status-LED zu orange wechselt, lassen Sie **Reset**-Taste los, damit die Rack-PDU ihren Neustart abschließen kann.
2. Greifen Sie über eine der sicheren Schnittstellen auf das Gerät zu, um Ihr benutzerdefiniertes Kennwort festzulegen und das Gerät zu konfigurieren. Nach dem Zurücksetzen des Geräts auf die Standardeinstellungen kann die erste Anmeldung mit dem Standardbenutzernamen **apc** und dem Standardkennwort **apc** abgeschlossen werden.

Aufbau der Frontkonsole



Element	Beschreibung	Funktion
❶	Anzeigefeld	Zeigt Informationen über den Rack PDU. Im Ruhezustand werden die angezeigten Informationen alle fünf seconds aktualisiert. Der Bildschirm wird nach drei minutes Inaktivität automatisch ausgeschaltet. Diese Timeout-Dauer kann angepasst werden. Um den Text umzukehren, wählen Sie Display settings, scrollen Sie zur LCD Orientation und drücken Sie Select.
❷	Main Menu-Taste	Drücken Sie, um zur Seite mit der load status summary zurückzukehren.
❸	Taste Scroll	Drücken Sie diese Taste einmal, um das Menü anzuzeigen. Drücken Sie weitere Male, um den Markierungsbalken in der Menüliste nach unten zu bewegen, bis das gewünschte Element erreicht ist.
❹	Select taste	Wenn ein Menüpunkt hervorgehoben ist, drücken Sie die Select taste, um die entsprechende Statusseite zu öffnen.



Element	Beschreibung	Funktion
❺	Reset-Taste	Setzt die Netzwerkmanagement-Schnittstelle ohne Auswirkungen auf die Ausgänge der Rack PDU zurück. Um die Netzwerkmanagement-Schnittstelle zurückzusetzen, ohne die Konfiguration oder den Status der Ausgänge zu ändern, drücken Sie die Taste und lassen Sie sie wieder los. Um alle Konfigurationen zu löschen und die werkseitigen Standardeinstellungen wiederherzustellen, halten Sie die Taste 30 seconds lang gedrückt oder bis die Netzwerkstatus-LED orange blinkt.
❻	USB port 5V @ 500 mA	Zur Verwendung mit einem Flash-Laufwerk zum Herunterladen von Protokolldateien oder zur Versorgung von Hardware-Zubehör mit bis zu 100 mA bei 5V.
❼	10/100/1000 Base-T Connector (Network port)	Verbindet den Rack PDU über ein Cat5e+-Netzwerkkabel mit dem Netzwerk.
❽	Link 1- and Link 2-Ports	Zur Verwendung mit der Network Port Sharing (NPS)-Funktion zum Verbinden mehrerer Rack PDUs zu einer NPS-Gruppe. Dies ermöglicht den dezentralen Zugriff auf alle Geräte in der Gruppe, sofern mindestens eine PDU mit dem Netzwerk verbunden ist.
❾	Sensor- ports	Anschluss für optionales Zubehör zur Umgebungsüberwachung: AP9335T, AP9335TH, NBES0301, NBES0302, NBES0303, NBES0304, NBES0305 oder NBES0308. Weitere Informationen zu diesem Zubehör finden Sie unter **www.se.com**.
❿	Console port	Verbindet die Rack PDU über ein Micro-USB-Kabel (APC-Teilenummer 960-0603) mit einem lokalen Computer, um anfängliche Netzwerkeinstellungen zu konfigurieren oder auf die Befehlszeilenschnittstelle (CLI) zuzugreifen.
⓫	Lastanzeige-LED	Zeigen den Status der Rack PDU-Last und die Alarmpegel an.

Netzwerkstatus-LED

Zustand	Beschreibung
Aus	Eine von der nachfolgenden Situationen existiert: • Die Rack PDU empfängt keine Eingangsspannung • Die Rack PDU funktioniert nicht ordnungsgemäß. Sie muss möglicherweise repariert oder ersetzt werden. Wenden Sie sich an den Kundendienst.
Dauerhaft grün	Die Rack PDU verfügt über gültige TCP/IP-Einstellungen.
Dauerhaft orange	In der Rack PDU wurde ein Hardwareproblem festgestellt. Wenden Sie sich an den Kundendienst.
Blinkend grün	Die Rack PDU hat keine gültigen TCP/IP-Einstellungen.
Blinkend orange	Die Rack PDU sendet BOOTP-Anforderungen.
Abwechselnd grün und orange blinkend	Wenn die LED langsam blinkt, sendet die Rack PDU DHCP[2]-Anforderungen[1]. Wenn die LED schnell blinkt, wird die Rack PDU gerade gestartet.

1. Wenn Sie keinen BOOTP- oder DHCP-Server verwenden, lesen Sie **„Netzwerkeinstellungen festlegen (Establish Network Settings)“** in diesem Handbuch, um die TCP/IP-Einstellungen der Rack PDU zu konfigurieren.
2. Informationen zur Verwendung eines DHCP-Servers finden Sie unter **„TCP/IP- und Kommunikationseinstellungen (TCP/IP and Communication Settings)“** in diesem Handbuch.

10/100/1000 LED

Zustand	Beschreibung
Aus	Eine oder mehrere der folgenden Situationen sind eingetreten: • Die Rack PDU erhält keine Eingangsspannung. • Das Kabel, das die Rack PDU mit dem Netzwerk verbindet, ist getrennt oder nicht funktionsfähig. • Das Gerät, das die Rack PDU mit dem Netzwerk verbindet, ist ausgeschaltet. • Die Rack PDU selbst funktioniert nicht ordnungsgemäß. Sie muss möglicherweise repariert oder ersetzt werden. Wenden Sie sich an den Kundendienst.
Dauerhaft gelb	Die Rack PDU ist mit einem Netzwerk verbunden, das mit 10-100 Megabits pro second (Mbps) arbeitet.
Dauerhaft grün	Die Rack PDU ist mit einem Netzwerk verbunden, das mit einer Geschwindigkeit von 1000 Mbps arbeitet.
Blinkend gelb	Die Rack PDU empfängt oder sendet Datenpakete mit einer Geschwindigkeit von 10-100 Mbps.
Blinkend grün	Die Rack PDU empfängt oder sendet Datenpakete mit einer Geschwindigkeit von 1000 Mbps.

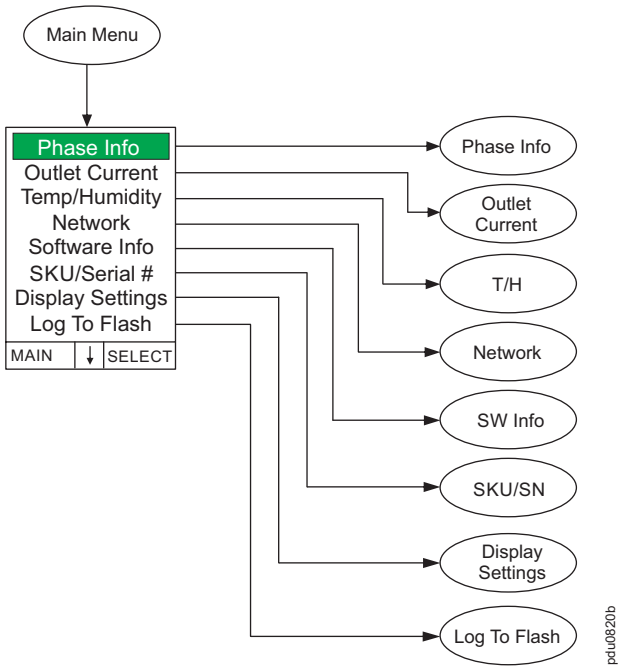
Lastanzeige-LED

Die Lastanzeige-LED identifiziert Überlast- und Warnbedingungen für die Rack PDU.

Zustand	Beschreibung
Dauerhaft grün	OK. Es liegen keine Überlast-(kritisch) oder nahe Überlast-(Warnung) Alarme vor.
Dauerhaft gelb	Warnung. Es liegt mindestens ein nahe Überlast-(Warnung) Alarm vor, es liegen jedoch keine Überlast-(kritischen) Alarme vor.
Blinkend rot	Überlast. Mindestens ein Überlast-(kritischer) Alarm liegt vor.

Beispiel 1

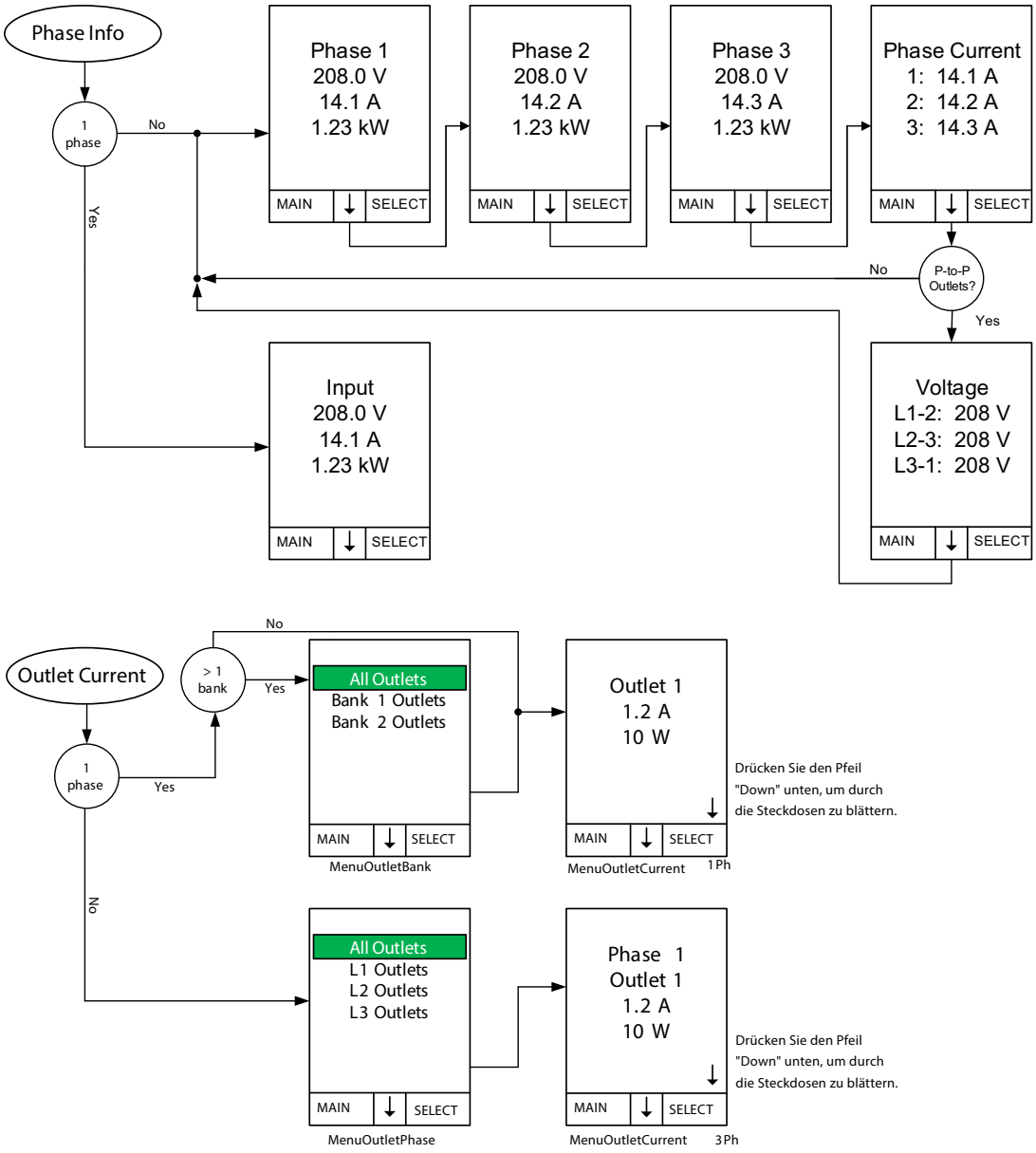
Anzeige-Baum — Hauptmenü



HINWEIS: Der MenuHomeScreen ist auf sechs Zeilen pro Menüseite beschränkt. Wenn mehr als sechs Auswahlen verfügbar sind, werden sie auf mehreren Seiten angezeigt. "Outlet Current" wird nur bei Metered-by-Outlet (MBO)-Geräten angezeigt. "Temp/Humidity" wird nur angezeigt, wenn ein AP9335T- oder AP9335TH-Sensor angeschlossen ist.

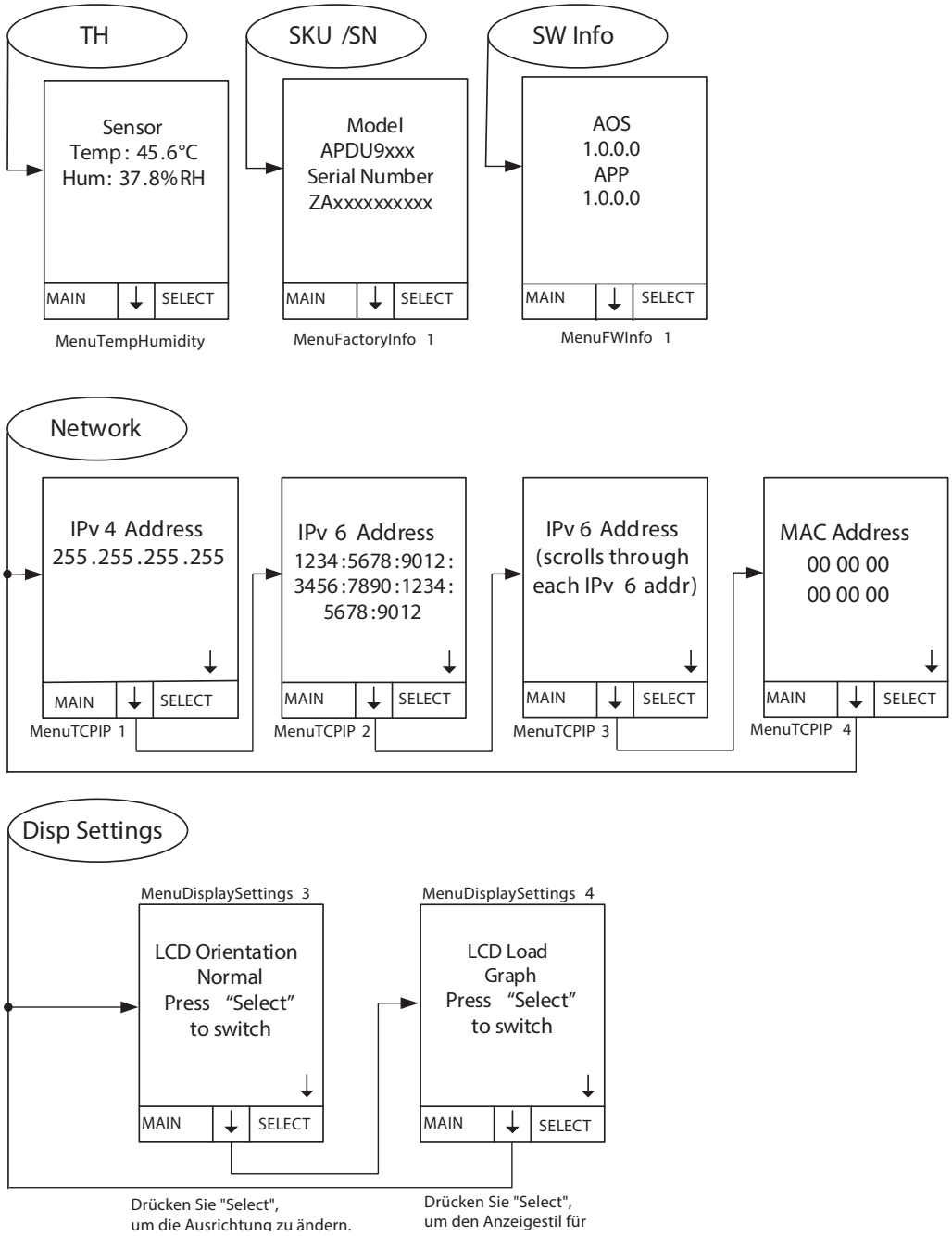
Beispiel 2

Anzeige-Baum — Untermenü 1



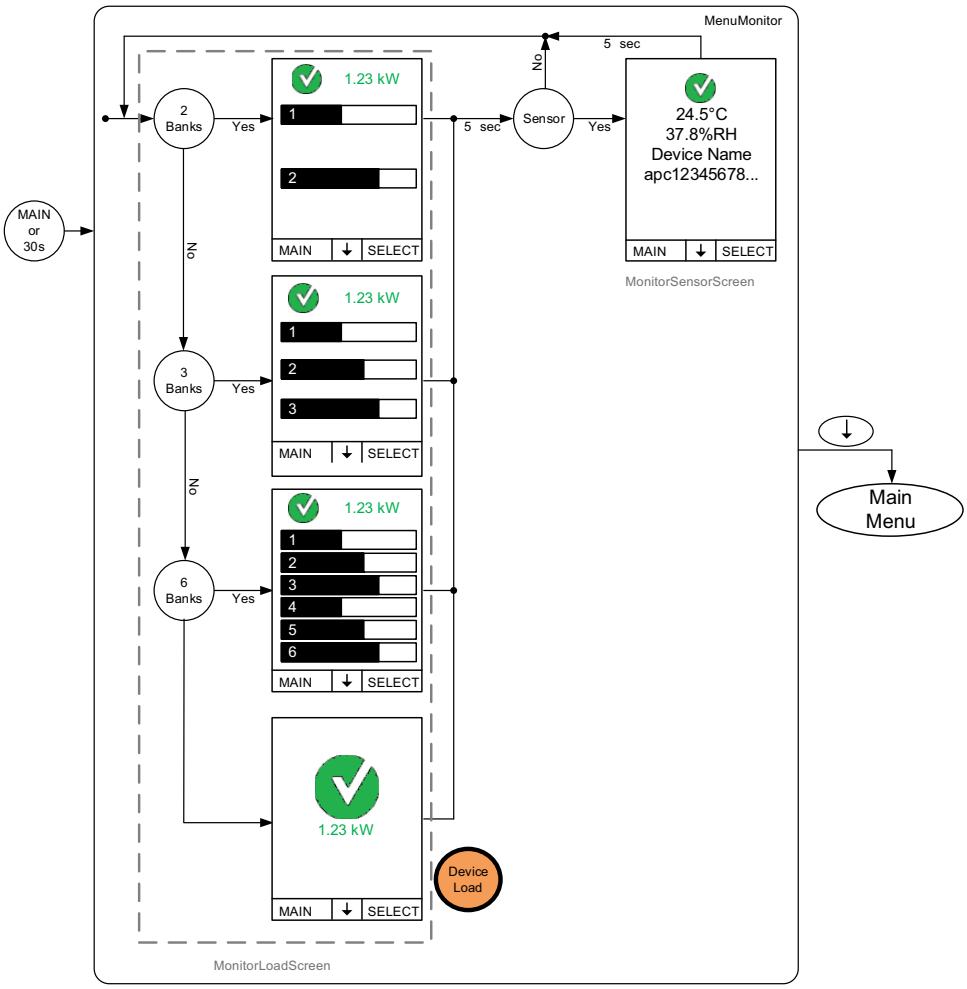
Beispiel 3

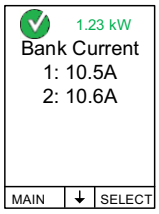
Anzeige-Baum — Untermenü 2



Beispiel 4

Anzeige-Baum — Monitor



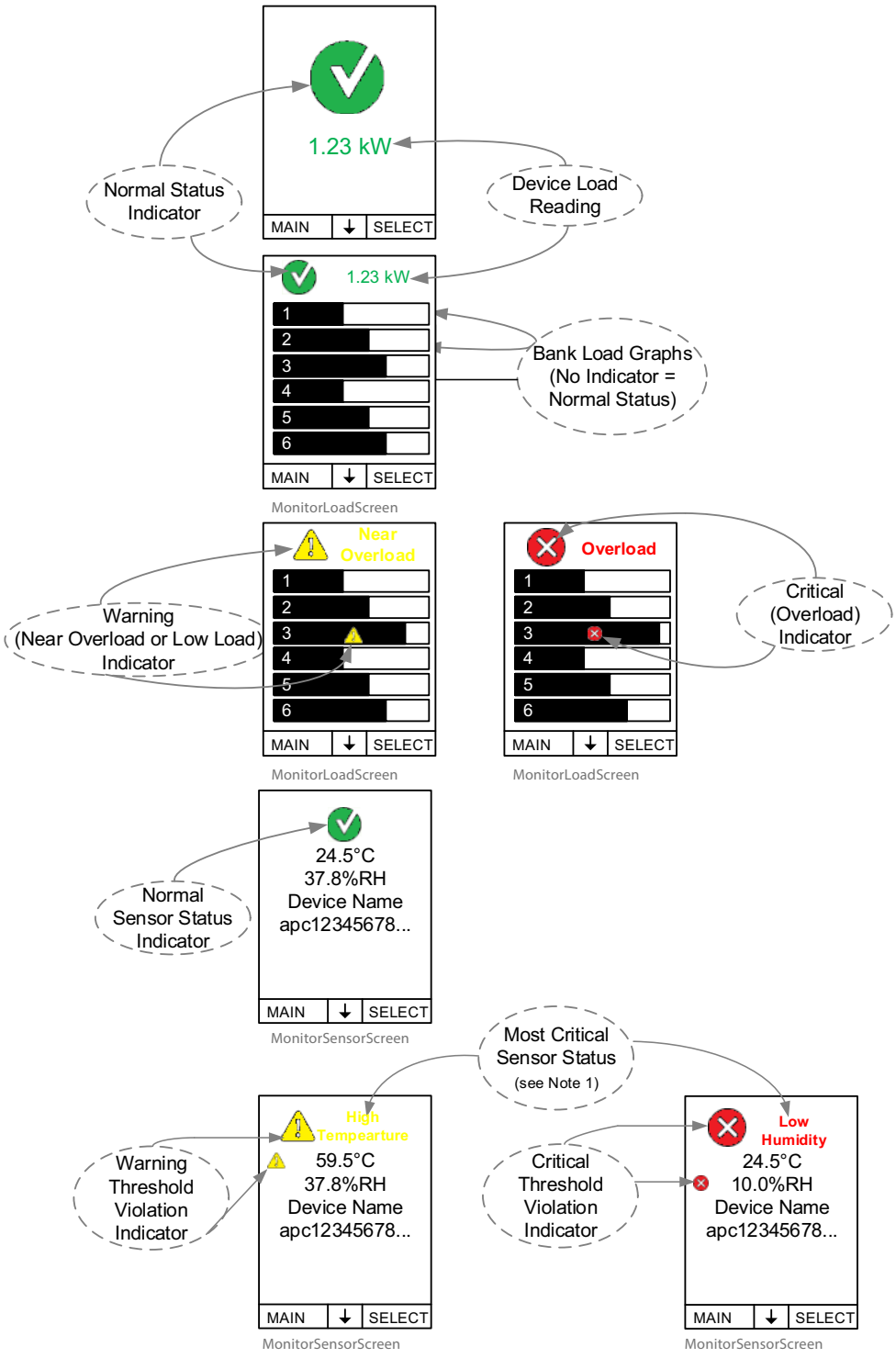


HINWEIS: Numeric- und graph-Anzeige unterscheiden sich nicht, wenn keine bank vorhanden ist. Bei Verwendung der numeric load display wird ein Gesamtleistungsbildschirm des Geräts hinzugefügt, wenn banken vorhanden sind.

Example of Numeric Load Display (Beispiel der numerischen Lastanzeige)

Beispiel 5

Anzeige-Baum — Monitorstatusanzeige

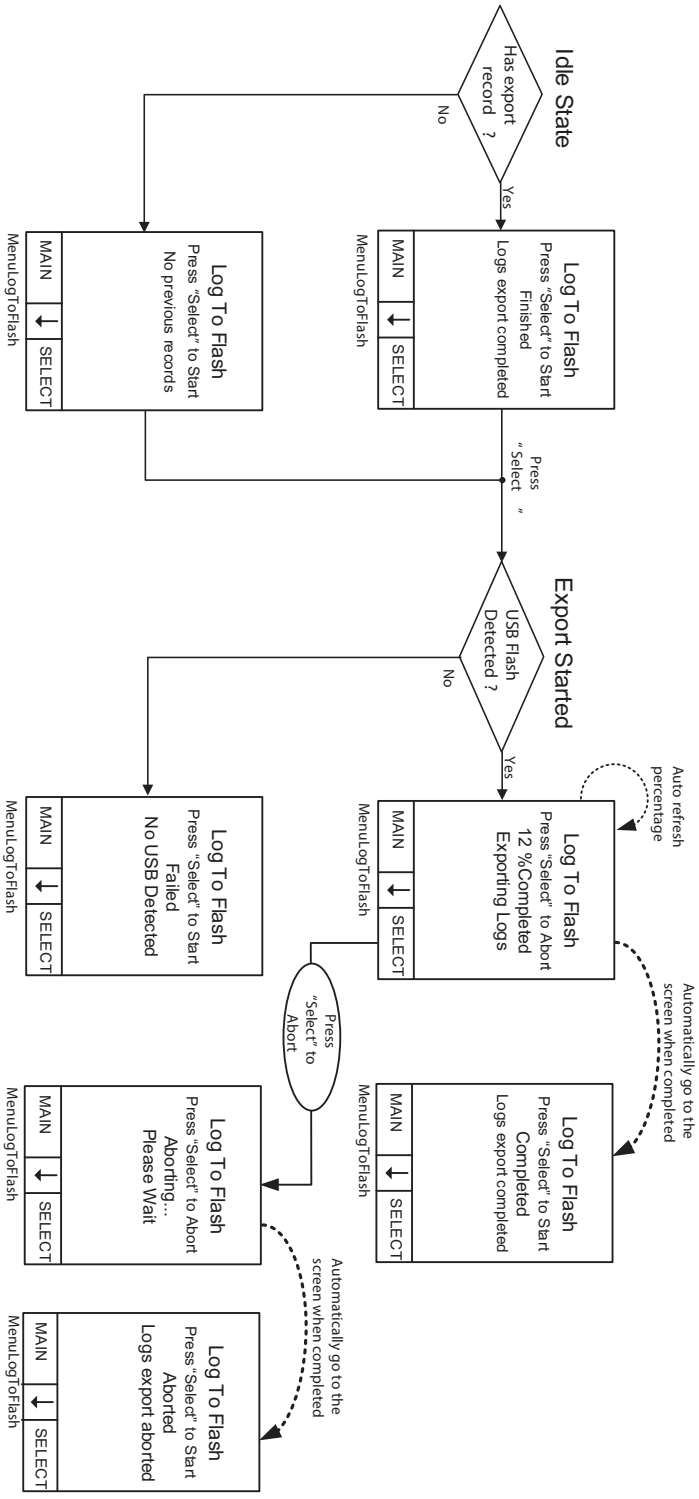


HINWEIS: 1 — Die vereinfachten LCD-Bildschirme zeigen Gerätelastungsalarme nur an, wenn keine Bänke vorhanden sind, **OR** nur Banklastalarme, wenn Bänke vorhanden sind. Phasen- und Ausgangsalarme und -warnungen werden **NOT** angezeigt.

HINWEIS: 2 — Der Einfachheit halber werden sowohl Warnungen als auch kritische Temperaturschwellenverletzungen als Hochtemperatur angezeigt. Ebenso werden sowohl Verstöße gegen die Warnschwelle als auch gegen die kritische Feuchtigkeitsschwelle als Low Humidity angezeigt.

Beispiel 6

Anzeige-Baum — Protokoll zum Flash-Laufwerk



Command Line Interface

Die Befehlszeile Command Line Interface (CLI)

Sie können die Befehlszeilenschnittstelle verwenden, um den Status der Rack PDU (und aller angeschlossenen Rack PDUs, wenn Sie die Funktion zur gemeinsamen Nutzung von Netzwerkports verwenden) anzuzeigen und sie zu konfigurieren und zu verwalten. Darüber hinaus können Sie über die Befehlszeilenschnittstelle Skripte für den automatisierten Betrieb erstellen. Sie können alle Parameter der Rack PDU konfigurieren (einschließlich derer, für die es keine spezifischen CLI-Befehle gibt), indem Sie über die CLI eine INI-Datei an die Rack PDU übertragen. Die CLI verwendet XMODEM, um die Übertragung durchzuführen, allerdings ist die aktuelle INI-Datei nicht über XMODEM lesbar.

Melden Sie sich an der CLI an

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

Lokaler Zugriff auf die Command Line Interface

Verwenden Sie für den lokalen Zugriff einen Computer, der über den Konsolenport mit der Rack PDU verbunden ist, um auf die Befehlszeilenschnittstelle zuzugreifen:

1. Wählen Sie einen seriellen Port an Ihrem Computer aus und deaktivieren Sie alle Dienste, die diesen Anschluss verwenden.
2. Schließen Sie ein Micro-USB-Kabel vom ausgewählten seriellen Port des Computers an den Konsolenanschluss der Rack PDU an.
3. Starten Sie ein Terminalprogramm (z.B. Tera Term oder HyperTerminal) und konfigurieren Sie den ausgewählten Port wie folgt: 9600 bps, 8 data bits, keine Parität, 1 stop bit, keine Datenflusskontrolle.

Fernzugriff auf die Command Line Interface

Sie können wählen, ob Sie über Telnet und/oder SSH auf die Befehlszeilenschnittstelle zugreifen möchten. SSH ist standardmäßig aktiviert. Sie müssen auch nicht aktivieren.

Sie können den `console`-befehl verwenden, um entweder Telnet oder SSH zu aktivieren oder zu deaktivieren.

Bei Bedarf können Sie auch die Web-UI verwenden, um entweder Telnet oder SSH zu aktivieren oder zu deaktivieren. Wählen Sie auf der **Configuration**-Registerkarte die Option **Network** aus dem Menü, um die **Console Access**-Seite zu öffnen. Klicken Sie, um das gewünschte **Enable** zu aktivieren. Klicken Sie auf **Apply**, um Ihre Änderungen zu speichern, oder **Cancel**, um die Seite zu verlassen.

Telnet für den Basiszugriff: Telnet bietet die grundlegende Sicherheit der Authentifizierung durch Benutzername und Kennwort, jedoch nicht die Hochsicherheitsvorteile der Verschlüsselung. Telnet ist standardmäßig deaktiviert.

1. Geben Sie auf einem Computer, der Zugriff auf das Netzwerk hat, in dem die Rack PDU installiert ist, an einer Eingabeaufforderung `telnet` und die IP-Adresse für die Rack PDU ein (z.B. `telnet 139.225.6.133`, wenn die Rack PDU den standardmäßigen Telnet-Port 23) verwendet, und drücken Sie die `ENTER`.
   Wenn die Rack PDU eine nicht standardmäßige Portnummer (von 5000 bis 32768) verwendet, müssen Sie je nach Telnet-Client einen Doppelpunkt oder ein Leerzeichen zwischen der IP-Adresse (oder dem DNS-Namen) und der Portnummer einfügen. (Dies sind Befehle für die allgemeine Verwendung: Einige Clients erlauben es Ihnen nicht, den Port als Argument anzugeben, und einige Linux-Typen benötigen möglicherweise zusätzliche Befehle).

2. Geben Sie den Benutzernamen und das Passwort ein (Der Standardbenutzername und das Standardkennwort für den **Super-Benutzer (Super user)** sind beide **apc**). Wenn Sie sich nicht an Ihren Benutzernamen oder Ihr Passwort erinnern können, lesen Sie Zugriff nach Verlust des Passworts in diesem Handbuch.

SSH für Hochsicherheitszugriff: Wenn Sie die hohe Sicherheit von SSL/TLS für die Web-UI verwenden, verwenden Sie SSH für den Zugriff auf die Befehlszeilenschnittstelle. SSH verschlüsselt Benutzernamen, Passwörter und übertragene Daten. Die Oberfläche, Benutzerkonten und Benutzerzugriffsrechte sind dieselben, unabhängig davon, ob Sie über SSH oder Telnet auf die Befehlszeilenschnittstelle zugreifen. Um SSH jedoch verwenden zu können, müssen Sie zuerst SSH konfigurieren und ein SSH-Clientprogramm auf Ihrem Computer installiert haben. SSH ist standardmäßig aktiviert.

About the Main Screen

Das Folgende ist ein Beispiel für den Hauptbildschirm, der angezeigt wird, wenn Sie sich an der Command Line Interface einer Rack PDU anmelden.

```
Schneider Electric                          Network Management Card AOS     v1.3.0.6
(c) Copyright 2019 All Rights Reserved      RPDU 2g APP                    v1.0.0.22
-------------------------------------------------------------------------------
Name        : Test Lab                                Date      :  02/20/2020
Contact     : Don Adams                               Time      :  5:58:30
Location    : Building 3                              User      : Administrator
Up Time     : 0 Days 21 Hours 21 Minutes              Stat      : P+ N4+ N6+ A+
-------------------------------------------------------------------------------
IPv4                : Enabled              IPv6                 : Enabled
Ping response       : Enabled
-------------------------------------------------------------------------------
HTTP                : Enabled              HTTPS                : Enabled
FTP                 : Enabled              Telne                : Disabled
SSH/SCP             : Enabled              SNMPv                : Read/Write
SNMPv3              : Enabled
-------------------------------------------------------------------------------
Super User          : Enabled              RADIUS               : Disabled
Administrator       : Disabled             Device User          : Disabled
Read-only User      : Disabled             Network-Only User    : Disabled

Type ? For command listing
Use tcpip for IP address (-i), subnet (-s), and gateway (-g)

apc>
```

- Der Firmwarename identifiziert den Gerätetyp, der eine Verbindung zum Netzwerk herstellt.
- Drei Felder identifizieren den Systemnamen, die Kontaktperson und den Standort der Rack PDU.
  ```
  Name      : Test Lab
  Contact : Don Adams
  Location : Building 3
  ```
- Das **Up Time** gibt an, wie lange die Rack PDU-Verwaltungsschnittstelle seit dem letzten Einschalten oder Zurücksetzen ausgeführt wurde.
- Zwei Felder identifizieren, wann Sie sich angemeldet haben, nach Datum und Uhrzeit.
  ```
  Date: 02/20/2020
  Time: 5:58:30
  ```
- Das **Benutzer (User)** gibt an, ob Sie sich über das Super-Benutzer, Administrator- oder Device-Manager-Konto angemeldet haben.
  ```
  User : Administrator
  ```

- Das **Stat** Feld meldet den Rack PDU-Status.
  `Stat: P+ N4+ N6+ A+`

`P+`	Das APC-Betriebssystem (AOS) funktioniert ordnungsgemäß

Nur IPv4	Nur IPv6	IPv4 und IPv6 *	Beschreibung
`N+`	`N+`	`N4+ N6+`	Die Netzwerk funkzioniert richtig.
`N?`	`N6?`	`N4? N6?`	Es wird ein BOOTP-Anfrage-Zyklus ausgeführt
`N-`	`N6-`	`N4- N6-`	Die Rack PDU hat keine Verbindung zum Netzwerk hergestellt
`N!`	`N6!`	`N4! N6!`	Ein anderes Gerät verwendet die IP-Adresse der Rack PDU
* Die Werte für N4 und N6 können sich voneinander unterscheiden: Sie können beispielsweise N4– N6+ haben.			

`A+`	Die Applikation funkzioniert richtig
`A-`	Die Applikation hat eine ungültige Prüfsumme
`A?`	Die Applikation wird initialisiert
`A!`	Die Anpplikation ist nicht mit dem AOS kompatibel

HINWEIS: Wenn P+ nicht angezeigt wird, wenden Sie sich an das Kundendienstzentrum von APC by Schneider Electric.

- Die restlichen Felder zeigen, welche Protokolle und Benutzerkonten aktiviert sind.

Verwendung der CLI

Über die Befehlszeilenschnittstelle können Sie Befehle zum Konfigurieren der Rack PDU verwenden. Um einen Befehl zu verwenden, geben Sie den Befehl ein und drücken Sie die ENTER taste. Befehle und Argumente sind in Klein-, Groß- oder Mischbuchstaben gültig. Bei den Optionen wird zwischen Groß- und Kleinschreibung unterschieden.

Während Sie die Befehlszeilenschnittstelle verwenden, können Sie auch Folgendes tun:

- Geben Sie ? ein und drücken die ENTER taste, um eine Liste der verfügbaren Befehle basierend auf Ihrem Kontotyp anzuzeigen.
- Um Informationen über den Zweck und die Syntax eines angegebenen Befehls zu erhalten, geben Sie den Befehl, ein Leerzeichen und ? oder das Wort `help`. Geben Sie beispielsweise Folgendes ein, um die Konfigurationsoptionen für RADIUS anzuzeigen: `radius ?` oder `radius help`
- Drücken Sie die UP pfeiltaste, um den Befehl anzuzeigen, der zuletzt in der Sitzung eingegeben wurde. Verwenden Sie die UP- und DOWN pfeiltasten, um durch eine Liste von bis zu zehn vorherigen Befehlen zu blättern.
- Geben Sie mindestens einen Buchstaben eines Befehls ein und drücken Sie die TAB-Taste, um durch eine Liste gültiger Befehle zu blättern, die mit dem Text übereinstimmen, den Sie in die Befehlszeile eingegeben haben.
- Geben Sie `exit` oder `quit` ein, um die Verbindung zur Befehlszeilenschnittstelle zu schließen.

Command Syntax

Element	Beschreibung
—	Optionen wird ein Bindestrich vorangestellt
< >	Beschreibungen von Benutzereingabeargumenten sind in spitze Klammern eingeschlossen. Zum Beispiel: `-dp <device password>`
[ ]	Wenn ein Befehl Optionen akzeptiert, können die Werte in Klammern eingeschlossen werden.
|	Eine vertikale Linie zwischen Elementen, die in Klammern oder spitzen Klammern eingeschlossen sind, zeigt an, dass sich die Elemente gegenseitig ausschließen. Sie müssen eines der Elemente verwenden.

Beispiel für einen Befehl, der mehrere Optionen unterstützt:

```
ftp [-p <port number>] [-S <enable | disable>]
```

In diesem Beispiel akzeptiert der `ftp`-Befehl die Option `-p`, die die Portnummer definiert, und die Option `-S`, die FTP-Funktion aktiviert oder deaktiviert.

So ändern Sie die FTP-Portnummer in 5010 und aktivieren FTP:

- Geben Sie den FTP-Befehl, die Portoption und das Argument `5010` ein:
  `ftp -p 5010`
- Nachdem der erste Befehl erfolgreich ausgeführt wurde, geben Sie den FTP-Befehl, die Option Aktivieren/Deaktivieren und `enable` ein:
  `ftp -S enable`

Beispiel für einen Befehl, der sich gegenseitig ausschließende Argumente für eine Option akzeptiert:

```
alarmcount [-p <all | warning | critical | informational>]
```

In diesem Beispiel akzeptiert die Option -p nur vier Argumente: all, warning oder critical. Zum Beispiel, geben Sie Folgendes ein, um die Anzahl der aktiven kritischen Alarme anzuzeigen:

```
alarmcount -p critical
```

Der Befehl wird nicht ausgeführt, wenn Sie ein Argument eingeben, das nicht angegeben ist.

Befehls-Antwortcodes

Die Befehls-Antwortcodes ermöglichen skriptgesteuerte Operationen, um Fehlerzustände zuverlässig zu erkennen, ohne den Text der Fehlermeldung abgleichen zu müssen:

Die CLI meldet alle Befehlsvorgänge im folgenden Format:

```
E [0-9] [0-9] [0-9]: Error message
```

Code	Meldung	Code	Meldung
E000	Erfolgreich	E200	Eingabefehler
E001	Erfolgreich ausgestellt	E201	Kein Antwort
E002	Neustart erforderlich, damit Änderungen wirksam werden	E202	Benutzer existiert bereits
E100	Befehl felgeschlagen	E203	Benutzer existiert nicht
E101	Befehl nicht gefunden	E204	Benutzer hat keinen Zugriff
E102	Parameterfehler	E205	Überschreitet die maximale Benutzeranzahl
E103	Befehlszeilenfehler	E206	Ungültiger Wert
E104	Verweigerung auf Benutzerebene	E207	Ausgangsbefehlfehler Gerät nicht initialisiert
E105	Befehlsvorfüllung	E208	Ausgangsbefehlfehler: Vorheriger Befehl steht aus
E106	Daten nicht verfügbar	E209	Ausgangsbefehlfehler: Datenbank abgelehnte Anfrage
E107	Die serielle Kommunikation mit der Rack PDU ist unterbrochen.	E210	Ausgangsbefehlsfehler: Ausgang beschränkt
E108	EAPoL deaktiviert aufgrund eines ungültigen/verschlüsselten Zertifikats.	E211	Befehl fehlgeschlagen
		E212	Speicher konnte nicht zugewiesen werden

Befehlsbeschreibungen der Network Management Card

?

Zugriff: Super-Benutzer (Super User), Administrator (Administrator), Gerätebenutzer (Device User), Nur-Netzwerk-Benutzer

Beschreibung: Eine Liste aller CLI-Befehle, die für Ihren Kontotyp verfügbar sind, anzeigen. Um den Hilfetext für einen bestimmten Befehl anzuzeigen, geben Sie den Befehl ein, gefolgt von einem Fragezeichen.

Argument	Beschreibung
`<command>`	`Hilfetext für einen bestimmten Befehl anzeigen.`

Beispiel 1: Um eine Liste aller verfügbaren Befehle anzuzeigen, geben Sie Folgendes ein

```
apc>? or apc>help
```

```
System Commands
------------------------------------------------------------------------------
For command help: command ?
?               about           alarmcount      boot            bye             cd
clrrst          console         date            delete          dir             dns
eapol           email           eventlog        exit            firewall        format
ftp             help            lang            lastrst         ldap            ledblink
logzip          netstat         ntp             ping            portspeed       prompt
pwd             quit            radius          reboot          resetToDef      session
smtp            snmp            snmptrap        snmpv3          ssh             ssl
system          tacacs+         tcpip           tcpip6          user            userauth
userdflt        web             whoami          wifi            xferINI         xferStatus


Device Commands
------------------------------------------------------------------------------
alarmList       bkLowLoad       bkNearOver      bkOverLoad      bkReading       bkPeakCurr
bkRestrictn     devLowLoad      devNearOver     devOverLoad     devReading      devPeakLoad
devStartDly     dispID          envSens         humSens         lcd             lcdBlink
logToFlash      modbus          nps             olAssignUsr     olCancelCmd     olDlyOff
olDlyOn         olDlyReboot     olGroups        olLowLoad       olName          olNearOver
olOff           olOffDelay      olOn            olOnDelay       olOverLoad      olRbootTime
olReading       olPeakLoad      olReboot        olStatus        olType          olUnasgnUsr
phBalAlGen      phBal           phLowLoad       phNearOver      phOverLoad      phReading
phPeakCurr      phRestrictn     prodInfo        stateSens       tempSens        userAdd
userDelete      userList        userPasswd      voltSens
```

Beispiel 2: Um eine Liste der Optionen anzuzeigen, die vom `alarmcount`-Befehl akzeptiert werden, geben Sie

```
apc> alarmcount ?
```

```
Usage: alarmcount -- Display Alarms
       alarmcount [-p <all | warning | critical | informational>]
```

Fehlermeldung: `E000, E102`

about

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer, Nur-Lese-Benutzer, Nur-Netzwerk-Benutzer

Beschreibung: Hardware- und Firmware-Informationen anzeigen. Diese Informationen sind bei der Fehlerbehebung hilfreich und ermöglichen es Ihnen festzustellen, ob aktualisierte Firmware auf der Website verfügbar ist.

Parameter: Keine

Fehlermeldung: `E000`

alarmcount

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer, Nur-Lese-Benutzer, Nur-Netzwerk-Benutzer

Beschreibung: Zeigt im System vorhandene Alarme an.

Parameter:

Option	Argument	Beschreibung
`-p`	`all`	Die Anzahl der aktiven Alarme an, die von der Rack PDU gemeldet wurden, anzeigen. Informationen zu den Alarmen finden Sie im Ereignisprotokoll.
	`warning`	Die Anzahl der aktiven Warnmeldungen anzeigen.
	`critical`	Die Anzahl der aktiven kritischen Alarme anzeigen.
	`informational`	Die Anzahl der aktiven Informationsalarme anzeigen.

Beispiel: Um alle aktiven Warnmeldungen anzuzeigen, geben Sie Folgendes ein

```
apc> alarmcount -p warning
E000: Success
WarningAlarmCount: 0
```

Fehlermeldung: `E000, E102`

boot

Zugriff: Super-Benutzer, Administrator, Nur-Netzwerk-Benutzer

Beschreibung: Definieren Sie, wie die Rack PDU ihre Netzwerkeinstellungen erhält, einschließlich IP-Adresse, Subnetzmaske und Standard-Gateway. Konfigurieren Sie dann die BOOTP- oder DHCP-Servereinstellungen.

Parameter:

Option	Argument	Beschreibung
`-b <boot mode>`	`dhcp | bootp | manual`	Definieren Sie, wie die TCP/IP-Einstellungen konfiguriert werden, wenn die Rack PDU eingeschaltet, zurückgesetzt oder neu gestartet wird.
`-c`	`[<enable | disable>] (Require DHCP Cookie)`	`dhcp` and `dhcpBootp` boot modes only. Hiermit aktivieren oder deaktivieren Sie die Anforderung, dass der DHCP-Server das APC-Cookie bereitstellt.
Die Standardwerte für diese drei Einstellungen müssen im Allgemeinen nicht geändert werden.		
`-v`	`[<vendor class>]`	APC.
`-i`	`[<client id>]`	Die MAC-Adresse der Rack PDU, die sie im Netzwerk eindeutig identifiziert.
`-u`	`[<user class>]`	Der Name des Applikationsfirmwaremoduls.

Beispiel: So verwenden Sie einen DHCP-Server zum Abrufen von Netzwerkeinstellungen

1. Geben Sie `boot -b dhcp`
2. Aktivieren Sie die Anforderung, dass der DHCP-Server das APC-Cookie bereitstellt
   ```
   apc> boot -c enable
   E000: Success
   ```
3. **Fehlermeldung:** `E000, E102`

bye

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer, Nur-Lese-Benutzer, Nur-Netzwerk-Benutzer

Beschreibung: Beenden Sie die CLI-Sitzung. Dies funktioniert genauso wie `exit`- oder `quit`-Befehle.

Parameter: Keine.

Beispiel:

```
apc> bye
Connection Closed - Bye
```

Fehlermeldung: Keine.

cd

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer, Nur-Lese-Benutzer

Beschreibung: Navigieren Sie zu einem Ordner in der Verzeichnisstruktur der Rack PDU. Das Arbeitsverzeichnis wird auf das Stammverzeichnis „/“ zurückgesetzt, wenn Sie sich von der CLI abmelden.

Parameter: `<directory name>`

Beispiel 1: So wechseln Sie in den ssh-Ordner und bestätigen, dass ein SSH-Sicherheitszertifikat auf die Rack PDU hochgeladen wurde,

1. Geben Sie `cd ssh` ein und drücken die ENTER taste.
2. Geben Sie `dir` ein und drücken Sie die ENTER taste, um die im SSH-Ordner gespeicherten Dateien aufzulisten.

Beispiel 2: Geben Sie `cd ..` ein, um zum vorherigen Verzeichnisordner zurückzukehren.

Fehlermeldung: `E000, E102`

clrrst

Zugriff: Super-Benutzer, Administrator

Beschreibung: Löschen Sie den Grund für das Zurücksetzen der Netzwerkschnittstelle. Siehe lastrst, Seite 44 für weitere Informationen zum Grund für das Zurücksetzen.

Beispiel: Keine

Fehlermeldung: Keine

console

Zugriff: Super-Benutzer, Administrator

Beschreibung: Legen Sie fest, ob Benutzer über Telnet, das standardmäßig deaktiviert ist, oder Secure SHell (SSH), das standardmäßig aktiviert ist und Schutz durch verschlüsselte Übertragung von Benutzernamen, Kennwörtern und Daten bietet, auf die Befehlszeilenschnittstelle zugreifen können. Sie können die Einstellung des Telnet- oder SSH-Ports ändern, um die Sicherheit zu erhöhen. Sie können auch den Netzwerkzugriff auf die Befehlszeile deaktivieren.

Parameter:

Option	Argument	Beschreibung
`-S`	`<enable | disable>`	Den SSH-Zugriff auf das Gerät aktivieren oder deaktivieren. Durch Aktivieren von SSH wird SCP aktiviert.
`-t`	`<enable | disable>`	Den Telnet-Zugriff auf das Gerät aktivieren oder deaktivieren.
`-pt`	`<telnet port n>`	Definieren Sie den Telnet-Port, der für die Kommunikation mit der Rack PDU verwendet wird (standardmäßig 23).
`-ps`	`<SSH port n>`	Definieren Sie den SSH-Port, der für die Kommunikation mit der Rack PDU verwendet wird (standardmäßig 22).
`-b`	`2400 | 9600 | 19200 | 38400`	Konfigurieren Sie die Geschwindigkeit der Konsolenportverbindung (standardmäßig 9600 bps).

Beispiel 1: Um den SSH-Zugriff auf die Befehlszeilenschnittstelle zu aktivieren, geben Sie Folgendes ein

```
console -S enable
```

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

```
console -pt 5000
```

Fehlermeldung: `E000, E102`

date

Zugriff: Super-Benutzer, Administrator

Definition: Konfigurieren Sie das Datum und die Uhrzeit, die von der Rack PDU verwendet werden.

> **HINWEIS:** Informationen zum Konfigurieren eines NTP-Servers zum Definieren von Datum und Uhrzeit für die Rack PDU finden Sie unter ntp, Seite 46.

Parameter:

Option	Argument	Beschreibung
`-d`	`<"datestring">`	Stellen Sie das aktuelle Datum ein. Das Format muss mit der aktuellen `-f-` Einstellung übereinstimmen.
`-t`	`<00:00:00>`	Konfigurieren Sie die aktuelle Uhrzeit in Stunden, Minuten und Sekunden. Verwenden Sie das 24-hour-Format.
`-f`	`mm/dd/yy | dd.mm.yyyy | mmm-dd-yy | dd-mmm-yy | yyyy-mm-dd`	Wählen Sie das numerische Format aus, in dem alle Datumsangaben in dieser Benutzeroberfläche angezeigt werden sollen. Jeder Buchstabe m (für Monat), d (für Tag) und y (für Jahr) steht für eine Ziffer. Einstellige Tage und Monate werden mit einer führenden Null angezeigt.
`-z`	`<time zone offset>`	Stellen Sie die Differenz mit GMT ein, um Ihre Zeitzone anzugeben. Auf diese Weise können Sie mit anderen Personen in verschiedenen Zeitzonen synchronisieren.

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

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

Beispiel 2: Geben Sie Folgendes ein, um das Datum als 30.Oktober 2009 unter Verwendung des im vorherigen Beispiel konfigurierten Formats zu definieren

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

Beispiel 3: Um die Uhrzeit als 5:21:03 Uhr zu definieren, geben Sie Folgendes ein

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

Fehlermeldung: `E000, E100, E102`

delete

Zugriff: Super-Benutzer, Administrator

Beschreibung: Löschen Sie eine Datei im Dateisystem. (Informationen zum Löschen des Ereignisprotokolls finden Sie unter eventlog, Seite 40)

Parameter:

Argument	Beschreibung
`<file name>`	Geben Sie den Namen der zu löschenden Datei ein.

Beispiel: Um eine Datei zu löschen,

1. Navigieren Sie zu dem Ordner, der die Datei enthält. Geben Sie beispielsweise Folgendes ein, um zum Ordner logs zu navigieren
   `cd logs`
2. Geben Sie Folgendes ein, um die Dateien im Ordner logs anzuzeigen
   `dir`
3. Um eine Datei zu löschen, geben Sie Folgendes ein
   `delete <file name>`

Fehlermeldungen: `E000, E102`

dir

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer, Nur-Lese-Benutzer, Nur-Netzwerk-Benutzer

Beschreibung: Die auf der Rack PDU gespeicherten Dateien und Ordner anzeigen.

Parameter: Keine

Beispiel:

```
apc> dir E000: Success
1024 Jan 2 4:34 apc_hw21_aos_2.5.0.8.bin
6249332 Jan 2 4:34 apc_hw21_rpdu2g_1.1.0.15.bin
45000 Sep 30 1996 config.ini
          0    Apr    23   18:53      db/
          0    Apr    23   18:53      ssl/
          0    Apr    23   18:53      ssh/
          0    Apr    23   18:53      logs/
          0    Apr    23   18:53      sec/
          0    Apr    23   18:53      fwl/
          0    Apr    23   18:53      email/
          0    Apr    23   18:53      eapol/
          0    Apr    23   18:53      tmp/
          0    Apr    23   18:53      upsfw/
```

Fehlermeldungen: `E000`

dns

Zugriff: Super-Benutzer, Administrator

Definition: Die manuellen Domänennamensystem (DNS)-Einstellungen konfigurieren.

Parameter:

Option	Argument	Beschreibung
`-OM`	`enable | disable`	Das manuelle DNS überschreiben. Wenn diese Einstellung aktiviert ist, haben Konfigurationsdaten aus anderen Quellen (normalerweise DHCP) Vorrang vor der hier festgelegten manuellen Konfiguration.
`-y`	`<enable | disable>`	System-hostname sync
`-p`	`<primary DNS Server>`	Den primären DNS-Server einstellen.
`-s`	`<secondary DNS Server>`	Den sekundären DNS-Server einstellen.
`-d`	`<domain name>`	Den Domänennamen einstellen.
`-n`	`<domain name IPv6>`	Den Domännennamen IPv6 einstellen.
`-h`	`<host name>`	Den Hostnamen einstellen.

Beispiel:

```
apc > dns -OM
E000: Success
Override Manual DNS Settings: enabled
```

Fehlermeldung: `E000, E102`

eapol

Zugriff: Super-Benutzer, Administrator

Beschreibung: Die EAPoL (802.1X-Sicherheit) Einstellungen konfigurieren.

Parameter:

Option	Argument	Beschreibung
`-S`	`enable | disable`	EAPoL aktivieren oder deaktivieren.
`-n`	`<supplicant name>`	Den Namen des Bittstellers einstellen.
`-p`	`<private key passphrase>`	Die Schlüssel-Phrase einstellen.

Beispiel 1: So zeigen Sie das Ergebnis eines `eapol`-Befehls an:

```
apc>eapol
E000: Success

Active EAPoL
Settings
----------------
-----

     Status:           enabled

     Supplicant        NMC-Supplicant
     Name:

     Passphrase:       <hidden>

     CA file           Valid Certificate

     Status
     Private Key       Valid Certificate

     Status
     Public Key        Valid Certificate

     Status
```

Beispiel 2: Um EAPoL zu aktivieren:

```
apc>eapol -S enable
E000: Success
Reboot required for change to take effect.
```

email

Zugriff: Super-Benutzer, Administrator

Beschreibung: Konfiguration von Parametern für die E-Mail, die Rack PDU zum Senden von Ereignisbenachrichtigungen verwendet.

Parameter:

Option	Argument	Beschreibung
`-g[n]`	`<enable | disable>`	Aktiviert (Standard) oder deaktiviert das Senden von E-Mails an den Empfänger.
`-t[n]`	`<To Address>`	Der Benutzer- und Domänenname des Empfängers. Um E-Mail für das Paging zu verwenden, verwenden Sie die E-Mail-Adresse für das Pager-Gateway-Konto des Empfängers (z.B., myacct100@skytel.com). Das Pager-Gateway generiert die Seite.
`-o[n]`	`<long | short> (Format)`	Das Langformat enthält Name, Standort, Kontakt, IP-Adresse, Seriennummer des Geräts, Datum und Uhrzeit, Ereigniscode und Ereignisbeschreibung. Das kurze Format enthält nur die Ereignisbeschreibung.
`-l[n]`	`<Language Code>`	Die Sprache, in der die E-Mail-Benachrichtigung gesendet wird. Nur English ist zu diesem Zeitpunkt verfügbar.
`-r [n]`	`<Local | recipient | custom> (Route)`	Stellen Sie die SMTP-Server-Optionen ein: `Local` (empfohlen): Wählen Sie diese Option, wenn sich Ihr SMTP-Server in Ihrem internen Netzwerk befindet oder für Ihre E-Mail-Domäne eingerichtet ist. Wählen Sie diese Einstellung, um Verzögerungen und Netzwerkausfälle zu begrenzen. Wenn Sie diese Einstellung wählen, müssen Sie auch die Weiterleitung am SMTP-Server des Geräts aktivieren und ein spezielles externes E-Mail-Konto einrichten, um die weitergeleitete E-Mail zu empfangen. **HINWEIS:** Erkundigen Sie sich bei Ihrem SMTP-Serveradministrator, bevor Sie diese Änderungen vornehmen. `Recipient`: Diese Einstellung sendet E-Mails direkt an den SMTP-Server des Empfängers, der durch eine MX-Record-Suche der Domäne der An-Adresse bestimmt wird. Das Gerät versucht nur einmal, die E-Mail zu senden. Ein Netzwerkausfall oder ein ausgelasteter Remote-SMTP-Server kann zu einer Zeitüberschreitung führen und dazu führen, dass die E-Mail verloren geht. Diese Einstellung erfordert keine zusätzlichen Verwaltungsaufgaben auf dem SMTP-Server. **HINWEIS:** Bei Verwendung dieser Einstellung stimmt die „Von-Adresse“ mit der „An-Adresse“ überein, werden Authentifizierung und Verschlüsselung (TLS) deaktiviert, und wird Port 25 verwendet. `Custom`: Mit dieser Einstellung kann jeder E-Mail-Empfänger seine eigenen Servereinstellungen haben. Diese Einstellungen sind unabhängig von den Einstellungen des `smtp`-Befehls.
`Custom Route Option`		
`-f[n]`	`<From Address>`	Der Inhalt des Von-Felds in E-Mail-Nachrichten, die von der Rack PDU gesendet werden, im Format *user@ [IP_address]* (wenn eine IP-Adresse als lokaler SMTP-Server angegeben ist) oder im Format *user@domain*, wenn DNS konfiguriert ist und der DNS-Name in den E-Mail-Nachrichten als lokaler SMTP-Server angegeben ist. Der lokale SMTP-Server erfordert möglicherweise, dass Sie für diese Einstellung ein gültiges Benutzerkonto auf dem Server verwenden. Siehe die Serverdokumentation.
`-s{n}`	`<SMTP Server>`	Die IPv4/IPv6-Adresse oder der DNS-Name des lokalen SMTP-Servers. Diese Definition ist nur erforderlich, wenn `-r-`Option auf `Local` gesetzt ist.
`-p[n]`	`<Port>`	Die SMTP-Portnummer, Standardwert ist 25. Gemeinsame Ports sind 25 für unverschlüsselte E-Mails und 465 und 587 für SSL/TLS-verschlüsselte E-Mails. Sie können die Port-Einstellung auf einen beliebigen Port zwischen 1 und 65535 ändern.
`-a[n]`	`<enable | disable> (Authentication)`	Aktivieren Sie diese Option, wenn der SMTP-Server eine Authentifizierung erfordert.
`-u[n]`	`<Username>`	Wenn der SMTP-Server eine Authentifizierung erfordert, geben Sie hier den Benutzernamen und das Kennwort ein. Dies führt eine einfache Authentifizierung durch, nicht SSL/TLS.
`-w[n]`	`<Password>`	
`-e[n]`	`<none | ifsupported | always | implicit>`	Geben Sie an, wann die Verschlüsselung verwendet wird. `none`: Der SMTP-Server erfordert oder unterstützt keine Verschlüsselung. `ifsupported`: Der SMTP-Server kündigt Unterstützung für STARTTLS an, erfordert jedoch keine Verschlüsselung der Verbindung. Der Befehl STARTTLS wird gesendet, nachdem die Ankündigung gegeben wurde. Dies wird normalerweise mit Port 25 verwendet. `always`: Der SMTP-Server erfordert, dass der Befehl STARTTLS bei der Verbindung zum Server gesendet wird. Dies wird normalerweise mit Port 587 verwendet. `implicit`: Der SMTP-Server akzeptiert nur Verbindungen, die verschlüsselt beginnen. Es wird keine STARTTLS-Nachricht an den Server gesendet. Dies wird normalerweise mit Port 465 verwendet.
`-c[n]`	`<enable | disable >`	CA-Stammzertifikat erforderlich: Dies sollte aktiviert werden, wenn die Sicherheitsrichtlinie Ihrer Organisation keine implizite Vertrauenswürdigkeit von SSL/TLS-Verbindungen zulässt. Wenn dies aktiviert ist, muss ein gültiges CA-Zertifikat für den SMTP-Server mithilfe des Zertifikatsladers im Zertifikatspeicher der Rack PDU installiert werden, damit eine TLS-Verbindung mit dem SMTP-Server erfolgreich hergestellt werden kann.

Option	Argument	Beschreibung
`-i[n]`	`<Certificate File Name>`	Dieses Feld hängt von den auf der Rack PDU installierten CA-Stammzertifikaten ab und davon, ob ein CA-Stammzertifikat erforderlich ist oder nicht.
`n =` E-Mail-Empfängernummer (Email Recipient Number) (1,2,3 oder 4)		

Beispiel: So aktivieren Sie das Senden von E-Mails an E-Mail-Empfänger 1 mit E-Mail-Adresse recipient1@apc.com, über den lokalen SMTP-Servers:

```
apc> email -g1 enable -r1 local -t1 recipient1@apc.com
E000: Success
```

Fehlermeldung: `E000, E102`

eventlog

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer, Nur-Lese-Benutzer

Beschreibung: Die Datum und Uhrzeit des Abrufs des Ereignisprotokolls, den Status der Rack PDU und den Status der an die Rack PDU angeschlossenen Sensoren anzeigen. Die letzten Geräteereignisse sowie Datum und Uhrzeit ihres Auftretens anzeigen. Verwenden Sie die folgenden Tasten, um im Ereignisprotokoll zu navigieren:

Parameter:

Taste	Beschreibung
ESC	Das Ereignisprotokoll schließen und zur Befehlszeilenschnittstelle zurückkehren.
ENTER	Die Protokollanzeige aktualisieren. Verwenden Sie diesen Befehl, um Ereignisse anzuzeigen, die aufgezeichnet wurden, nachdem Sie das Protokoll zuletzt abgerufen und angezeigt haben.
SPACEBAR	Die nächste Seite des Ereignisprotokolls anzeigen.
B	Die vorherige Seite des Ereignisprotokolls anzeigen. Dieser Befehl ist auf der Hauptseite des Ereignisprotokolls nicht verfügbar.
D	Das Ereignisprotokoll löschen. Befolgen Sie die Anweisungen, um den Löschvorgang zu bestätigen oder abzulehnen. Gelöschte Ereignisse können nicht abgerufen werden.

Beispiel:

```
apc> eventlog
-----Event Log -------------------------------------
   Date: 2/9/2024 Time: 13:22:26
   ---------------------------------------
   Metered Rack PDU: Communication Established
    Date        Time        User     Event
    ------------------------------------------------------
    2/9/2024    13:17:22    System   Set Time.
    2/9/2024    13:16:57    System   Configuration change.
                                     Date format preference.
    2/9/2024    13:16:49    System   Set Date.
    2/9/2024    13:16:35    System   Configuration change.
                                     Date format preference.
    2/9/2024    13:16:08    System   Set Date.
    2/9/2024    13:15:30    System   Set Time.
    2/9/2024    13:15:00    System   Set Time.
    2/9/2024    13:13:58    System   Set Date.
    2/9/2024    13:12:22    System   Set Date.
    2/9/2024    13:12:08    System   Set Date.
    2/9/2024    13:11:41    System   Set Date.
<ESC>- Exit, <ENTER>- Refresh, <SPACE>- Next, <D>- Delete
```

Fehlermeldung: E000, E100

exit

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer, Nur-Lese-Benutzer, Nur-Netzwerk-Benutzer

Beschreibung: Die CLI -Sitzung beenden. Dies funktioniert genauso wie die `bye`- oder `quit`-Befehle.

Parameter: Keine.

Beispiel:

```
apc> exit
Bye
```

Fehlermeldung: Keine.

firewall

Zugriff: Super-Benutzer, Administrator

Beschreibung: Die interne Rack PDU-Firewall-Funktion aktivieren, deaktivieren oder konfigurieren.

Parameter:

Parameter	Argument	Beschreibung
`-S`	`<enable | disable>`	Die Firewall aktivieren oder deaktivieren.
`-f`	`<file name to activate>`	Name der zu aktivierenden Firewall.
`-t`	`<file name to test> <duration time in minutes>`	Name der zu testenden Firewall und Dauer in Minuten.
`-fe`		Zeigt aktive Dateifehler an.
`-te`		Zeigt Testdateifehler an.
`-c`		Einen Firewall-Test abbrechen.
`-r`		Zeigt aktive Firewall-Regeln an.
`-l`		Zeigt das Firewall-Aktivitätsprotokoll an.
`-Y`		Firewall-Testaufforderung überspringen.

Beispiel: Um die Firewall-Richtliniendatei *example.fwl* zu aktivieren, geben Sie Folgendes ein

```
apc> firewall -f example.fwl
E000: Success
```

Fehlermeldung: `E000, E102`

format

Zugriff: Super-Benutzer, Administrator

Beschreibung: Formatieren Sie das Dateisystem der Rack PDU neu und löschen Sie alle Sicherheitszertifikate, Verschlüsselungscodes, Konfigurationseinstellungen sowie Ereignis- und Datenprotokolle. Seien Sie vorsichtig mit diesem Befehl.

HINWEIS: Sie müssen bestätigen, indem Sie „YES“ eingeben, wenn Sie dazu aufgefordert werden.

HINWEIS: Verwenden Sie stattdessen den `resetToDef`-Befehl, um die Rack PDU auf ihre Standardkonfiguration zurückzusetzen.

Parameter:

Option	Definition
`-f`	Dadurch werden alle Konfigurationsdaten, Ereignis- und Datenprotokolle, Zertifikate und Schlüssel gelöscht. Die Netzwerkeinstellungen werden NICHT beibehalten.
`-p`	Dadurch werden alle Konfigurationsdaten, Ereignis- und Datenprotokolle, Zertifikate und Schlüssel gelöscht. Die Netzwerkeinstellungen WERDEN beibehalten.

Beispiel:

```
apc> format -p

Format FLASH file system

Warning: This will delete all configuration data,
         event and data logs, certs and keys.

All network configuration settings WILL be preserved.

Enter 'YES' to continue or <ENTER> to cancel: YES
```

Fehlermeldung: Keine

ftp

Zugriff: Super-Benutzer, Administrator

Beschreibung: Den Zugriff auf den FTP-Server aktivieren oder deaktivieren. Ändern Sie optional die Porteinstellung auf die Nummer eines nicht verwendeten Ports von 5001 bis 32768, um die Sicherheit zu erhöhen.

HINWEIS: Das System wird neu gestartet, wenn eine Konfiguration geändert wird.

HINWEIS: FTP ist standardmäßig deaktiviert und das Secure Copy-Protokoll (SCP) wird automatisch aktiviert, wenn das Super-Benutzer-Kennwort über SSH festgelegt wird.

Parameter:

Option	Argument	Definition
`-p`	`<port number>` (valid ranges are: 21 and 5000–32768)	Definieren Sie den TCP/IP-Port, den der FTP-Server für die Kommunikation mit der Rack PDU verwendet (standardmäßig 21). Der FTP-Server verwendet sowohl den angegebenen Port als auch den Port, der eine Nummer niedriger als der angegebene Port ist.
`-s`	`<enable | disable>`	Konfigurieren Sie den Zugriff auf den FTP-Server.

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

```
apc> ftp -p 5001
E000: Success
```

Fehlermeldung: `E000, E102`

help

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer, Nur-Lese-Benutzer, Nur-Netzwerk-Benutzer

Beschreibung: Zeigen Sie eine Liste aller CLI-Befehle an, die für Ihren Kontotyp verfügbar sind. Um Hilfetext für einen bestimmten Befehl anzuzeigen, geben Sie den Befehl gefolgt von `help` ein.

Parameter: `[<command>]`

Beispiel 1: Um eine Liste der Befehle, die für jemanden verfügbar sind, der als Gerätebenutzer angemeldet ist, anzuzeigen, melden Sie sich als Gerätebenutzer an der CLI an, und geben Sie dann Folgendes ein

```
help
```

Beispiel 2: Geben Sie Folgendes ein, um eine Liste der Optionen anzuzeigen, die vom `alarmcount`-Befehl akzeptiert werden

```
apc> alarmcount help
Usage: alarmcount -- Display Alarms
         alarmcount [-p <all | warning | critical|
         informational>]
```

lang

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer

Beschreibung: Zeigt die verwendete Sprache an.

Parameter: Keine

Beispiel:

```
apc>lang
E000: Success

Languages
enUs - English
```

Fehlermeldung: Keine

lastrst

Zugriff: Super-Benutzer, Administrator

Beschreibung: Den Grund für das Zurücksetzen der letzten Netzwerkschnittstelle anzeigen. Verwenden Sie die Ausgabe dieses Befehls, um Probleme mit der Netzwerkschnittstelle unter Anleitung des technischen Supports zu beheben.

Option	Beschreibung
`02 NMI Reset`	Die Netzwerkschnittstelle wurde über die Reset-Taste auf dem Frontdisplay der Rack PDU zurückgesetzt.
`09 Coldstart Reset`	Die Netzwerkschnittstelle wurde zurückgesetzt, indem die Hardware von der Stromversorgung getrennt wurde.
`12 WDT Reset`	Die Netzwerkschnittstelle wurde über einen Firmware-Befehl zurückgesetzt.

Parameter: Keine

Beispiel:

```
apc> lastrst
09 Coldstart Reset
E000: Success
```

Fehlermeldung: `E000, E102`

ledblink

Zugriff: Super-Benutzer, Administrator

Beschreibung: Setzt die Status-LED so, dass sie für die angegebene Zeit blinkt. Verwenden Sie diesen Befehl, um die Rack PDU visuell zu lokalisieren.

Parameter:

Argument	Definition
`<time>`	Anzahl der Minuten zum Blinken der LED.

Beispiel:

```
apc> ledbllink 1
E000: Success
```

Fehlermeldung: `E000, E102`

logzip

Zugriff: Super-Benutzer, Administrator

Beschreibung: Erstellt ein einzelnes, komprimiertes Archiv der Protokolldateien, die von der NMC und der Rack PDU verfügbar sind. Diese Dateien können vom technischen Support zur Fehlerbehebung verwendet werden.

Parameter:

Option	Argument	Definition
`-m`	`<email recipient> (1-4)`	Die Identifikationsnummer (1-4) des E-Mail-Empfängers, an den die ZIP-Datei gesendet wird. Geben Sie die Nummer eines der vier konfigurierten möglichen E-Mail-Empfänger ein.

Beispiel:

```
apc> logzip -m 1
Generating files
/dbg/debug_ZA1023006009.tar
Emailing log files to email recipient - 1
E000: Success
```

Fehlermeldung: `E000, E102`

netstat

Zugriff: Super-Benutzer, Administrator

Beschreibung: Den Status des Netzwerks und aller aktiven IPv4- und IPv6-Adressen anzeigen.

Parameter: Keine

Beispiel:

```
apc> netstat

Current IP Information:

Family      mHome      Type       IPAddress                 Status
IPv6        4          auto       FE80::2CO:B7FF:FE51:      configured
                                  F304/64
IPv6        0          manual     ::1/128                   configured
IPv4        0          manual     127.0.0.1/32              configured
```

Fehlermeldung: `E000, E10`

ntp

Zugriff: Super-Benutzer, Administrator

Beschreibung: Anzeigen und Konfigurieren der Netzwerkzeitprotokollparameter.

Parameter:

Option	Argument	Definition
`-OM`	`enable | disable`	Die manuelle Einstellungen außer Kraft setzen.
`-p`	`<primary NTP Server>`	Geben Sie den primären Server an.
`-s`	`<secondary NTP Server>`	Geben Sie den sekundären Server an.
`-e`	`enable | disable`	Die Verwendung von NTP aktivieren oder deaktivieren.
`-u`	`<update now>`	Sofort die Rack PDU-Zeit vom NTP-Server aktualisieren.

Beispiel 1: Um die Überschreibung der manuellen Einstellung zu aktivieren, geben Sie Folgendes ein

```
ntp -OM enable
```

Beispiel 2: Um den primären NTP-Server anzugeben, geben Sie Folgendes ein

```
ntp -p 150.250.6.10
```

Fehlermeldung: `E000, E102`

ping

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer, Nur-Netzwerk-Benutzer

Beschreibung: Stellen Sie fest, ob das Gerät mit der von Ihnen angegebenen IP-Adresse oder dem DNS-Namen mit dem Netzwerk verbunden ist. Vier Anfragen werden an die Adresse gesendet.

Parameter:

Option	Argument	Beschreibung
n/a	`<IP address or DNS name>`	Geben Sie eine IP-Adresse im Format *xxx.xxx.xxx.xxx* oder den vom DNS-Server konfigurierten DNS-Namen ein.
-t		Anpingen bis gestoppt.

Beispiel: Um festzustellen, ob ein Gerät mit der IP-Adresse 192.168.1.50 mit dem Netzwerk verbunden ist, geben Sie Folgendes ein

```
apc> ping 192.168.1.50
E000: Success
Reply from 192.168.1.50: time(ms)= <10
Reply from 192.168.1.50: time(ms)= <10
Reply from 192.168.1.50: time(ms)= <10
Reply from 192.168.1.50: time(ms)= <10
```

Fehlermeldung: `E000, E100, E102`

portSpeed

Zugriff: Super-Benutzer, Administrator, Nur-Netzwerk-Benutzer

Beschreibung: Die Kommunikationsgeschwindigkeit des Ethernet-Ports definieren.

> **HINWEIS:** Die Einstellung der Portgeschwindigkeit kann auf 1000 Mbps Die Einstellung der Portgeschwindigkeit geändert werden. Allerdings kann diese Änderung nur über die Web-UI vorgenommen werden.

Parameter:

Option	Argumente	Beschreibung
`-s`	`auto | 10H | 10F | 100H | 100F`	`auto` aktiviert die Ethernet-Geräte zu verhandeln, um mit der höchstmöglichen Geschwindigkeit zu übertragen. `H =` Halbduplex (Kommunikation jeweils nur in eine Richtung) `F =` Vollduplex (Kommunikation in beide Richtungen gleichzeitig) `10` = 10 Megabits `100` = 100 Megabits

Beispiel: Geben Sie Folgendes ein, um den TCP/IP-Port für die Kommunikation mit 100 Mbps mit Halbduplex-Kommunikation zu konfigurieren

```
apc> portspeed -s 100H
E000: Success
Reboot required for change to take effect.
```

Fehlermeldung: `E000, E102`

prompt

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer, Nur-Netzwerk-Benutzer

Beschreibung: Die Eingabeaufforderung der Befehlszeilenschnittstelle konfigurieren, um den Kontotyp des aktuell angemeldeten Benutzers einzuschließen oder auszuschließen. Jeder Benutzer kann diese Einstellung ändern; alle Benutzerkonten werden aktualisiert, um die neue Einstellung zu verwenden.

Parameter:

Option	Argument	Beschreibung
`-s`	`long`	Die Eingabeaufforderung enthält den Kontotyp des aktuell angemeldeten Benutzers.
	`short`	Die Standardeinstellung. Die Eingabeaufforderung ist vier Zeichen lang: `apc>`

Beispiel:

```
apc> prompt -s long
E000: Success

Administrator@apc>prompt -s short
E000: Success
```

Fehlermeldung: `E000, E102`

pwd

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer, Nur-Lese-Benutzer, Nur-Netzwerk-Benutzer

Beschreibung: Den Pfad des aktuellen Arbeitsverzeichnisses ausgeben.

Parameter: Keine

Beispiel:

```
apc> pwd
/

apc> cd logs
E000: Success

apc> pwd
/logs
```

Fehlermeldung: `E000, E102`

quit

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer, Nur-Lese-Benutzer, Nur-Netzwerk-Benutzer

Beschreibung: Die CLI-Sitzung beenden. Dies funktioniert genauso wie die `exit-` oder `bye-`Befehle.

Parameter: Keine.

Beispiel:

```
apc> quit
Bye
```

Fehlermeldung: Keine.

radius

Zugriff: Super-Benutzer, Administratorr, Nur-NetzwerkBenutzer

Beschreibung: Die vorhandenen RADIUS-Einstellungen anzeigen und grundlegende Authentifizierungsparameter für bis zu zwei RADIUS-Server konfigurieren. In der Web-UI sind zusätzliche Authentifizierungsparameter verfügbar.

Ausführliche Informationen zur Konfiguration Ihres RADIUS-Servers finden Sie im Network Management Card 3 Security Handbook.

Parameter:

Option	Argument	Beschreibung
-a	<local | radiusLocal | radius>	Konfigurieren Sie die RADIUS-Authentifizierung: local = RADIUS ist deaktiviert. Lokale Authentifizierung ist aktiviert. radiusLocal = RADIUS, dann lokale Authentifizierung. RADIUS und lokale Authentifizierung sind aktiviert. Die Authentifizierung wird zuerst vom RADIUS-Server angefordert. Wenn der RADIUS-Server nicht antwortet, wird die lokale Authentifizierung verwendet. radius = RADIUS ist aktiviert. Lokale Authentifizierung ist deaktiviert.
-p1 -p2	<server IP>	Der Servername oder die IP-Adresse des primären oder sekundären RADIUS-Servers.
-o1 -o2	<port>	Die Portnummer des primären oder sekundären RADIUS-Servers. **HINWEIS:** RADIUS-Server verwenden standardmäßig Port 1812 zur Benutzerauthentifizierung. Die Rack PDU unterstützt die Ports 1 bis 65535.
-s1 -s2	<server secret>	Das gemeinsam genutzte Geheimnis zwischen dem primären oder sekundären RADIUS-Server und der Rack PDU.
-t1 -t2	<server timeout>	Die Zeit in Sekunden (seconds), die die Rack PDU auf eine Antwort vom primären oder sekundären RADIUS-Server wartet.

Beispiel 1: Um die vorhandenen RADIUS-Einstellungen für die Rack PDU anzuzeigen, geben Sie `radius` ein und drücken Sie die ENTER taste.

Beispiel 2: Geben Sie Folgendes ein, um ein Zeitlimit von 10 Sekunden für einen sekundären RADIUS-Server zu konfigurieren

```
apc> radius -t2 10
E000: Success
```

Fehlermeldung: `E000, E102`

reboot

Zugriff: Super-Benutzer, Administrator, Nur-Netzwerk-Benutzer

Beschreibung: Starten Sie nur die Netzwerkverwaltungsschnittstelle der Rack PDU neu. Dies hat keinen Einfluss auf die Ausgangsleistung der Rack PDU.

Option	Beschreibung
`-Y`	Bestätigungsaufforderung überspringen (nur Großbuchstaben Y)

Beispiel 1:

```
apc> reboot
E000: Success
Reboot Management Interface
Enter 'YES' to continue or <ENTER> to cancel:YES
Rebooting...
```

Beispiel 2:

```
apc> reboot -Y
E000: Success
Reboot Management Interface
Rebooting...
```

Fehlermeldung: `E000, E100`

resetToDef

Zugriff: Super-Benutzer, Administrator

Beschreibung: Alle konfigurierbaren Parameter auf ihre Standardwerte zurücksetzen. Löschen Sie alle Konten und löschen Sie Ereignis- und Datenprotokolle.

> **HINWEIS:** Bestimmte nicht konfigurierbare Parameter werden nicht mit `resetToDef` zurückgesetzt, und können nur von der Rack PDU gelöscht werden, indem das Dateisystem mit dem Befehl `format` formatiert wird.

Parameter:

Option	Argumente	Beschreibung
`-p`	`all | keepip`	Achtung: Dadurch werden alle konfigurierbaren Parameter auf ihre Standardwerte zurückgesetzt. `all =` Alle Konfigurationsänderungen, einschließlich Ereignisaktionen, Geräteeinstellungen und TCP/IP-Einstellungen zurücksetzen. `keepip =` Alle Konfigurationsänderungen zurücksetzen,mit *Ausnahme* der TCP/IP Einstellungen.

Beispiel: Um alle Konfigurationsänderungen mit Ausnahme der TCP/IP-Einstellungen zurückzusetzen, geben Sie Folgendes ein

```
apc> resettodef -p keepip
Reset to Defaults Except TCP/IP
Enter 'YES' to continue or <ENTER> to cancel: YES
```

Fehlermeldung: `E000, E100`

session

Zugriff: Super-Benutzer, Administrator

Beschreibung: Zeichnet auf, wer angemeldet ist (Benutzer), die Schnittstelle, die Adresse, die Uhrzeit und die ID.

Parameter:

Option	Argumente	Beschreibung
-d	[-d <session nID>] (Delete)	Sitzung für den aktuellen Benutzer mit der angegebenen Sitzungs-ID löschen.
-m	<enable | disable> (MultiUser Enable)	Aktivieren Sie diese Option, um zwei oder mehr Benutzern die gleichzeitige Anmeldung zu ermöglichen. Deaktivieren Sie diese Option, um jeweils nur einem Benutzer die Anmeldung zu gestatten.
-a	<enable | disable> (Remote Authentication Override)	Die Rack PDU unterstützt die RADIUS-Speicherung von Passwörtern auf einem Server. Aktivieren Sie die Überschreibung der Remoteauthentifizierung, damit sich ein lokaler Benutzer mit einem Benutzernamen und einem Kennwort für die Rack PDU anmelden kann, die lokal auf der Rack PDU gespeichert sind.

Beispiel:

```
apc> session
User    Interface    Address            Logged In Time   ID

-------------------------------------------------

apc     Telnet       10.169.118.1-00    00:00:03         19


E000: Success
```

Fehlermeldung: E000, E102

smtp

Zugriff: Super-Benutzer, Administrator, Nur-NetzwerkBenutzer

Beschreibung: Die Einstellungen für den lokalen E-Mail-Server konfigurieren.

Parameter:

Option	Argumente	Beschreibung
-f	<From Address>	Die Adresse, von der die E-Mail von der Rack PDU gesendet wird.
-s	<SMTP Server>	Die IPv4/IPv6-Adresse oder der DNS-Name des lokalen SMTP-Servers.
-p	<Port>	Die SMTP-Portnummer, standardmäßig 25. Gemeinsame Ports sind 25 für unverschlüsselte E-Mails und 465 und 587 für SSL/TLS-verschlüsselte E-Mails. Sie können die Porteinstellung auf einen beliebigen Port von 1 bis 65535 ändern.
-a	<enable | disable>	Aktivieren Sie diese Option, wenn Ihr SMTP-Server eine Authentifizierung erfordert.
-u	<Username>	Wenn der SMTP-Server eine Authentifizierung erfordert, geben Sie hier den Benutzernamen und das Kennwort ein.
-w	<Password>	
-e	<none | ifavail | always | implicit>	Verschlüsselungsoptionen: none: Der SMTP-Server benötigt/unterstützt keine Verschlüsselung. ifavail: Der SMTP-Server kündigt Unterstützung für STARTTLS an, erfordert jedoch keine Verschlüsselung der Verbindung. Der Befehl STARTTLS wird gesendet, nachdem die Ankündigung gegeben wurde. Dies wird normalerweise mit Port 25 verwendet. always: Der SMTP-Server erfordert, dass der Befehl STARTTLS bei der Verbindung zum Server gesendet wird. Dies wird normalerweise mit Port 587 verwendet. implicit: Der SMTP-Server akzeptiert nur Verbindungen, die verschlüsselt beginnen. Es wird keine STARTTLS-Nachricht an den Server gesendet. Dies wird normalerweise mit Port 465 verwendet.
-c	<enable | disable>	CA-Stammzertifikat anfordern. Dies sollte aktiviert werden, wenn die Sicherheitsrichtlinie Ihrer Organisation keine implizite Vertrauenswürdigkeit von SSL/TLS-Verbindungen zulässt. Wenn dies aktiviert ist, muss ein gültiges CA-Zertifikat für den SMTP-Server mithilfe des Zertifikatsladers im Zertifikatspeicher der Rack PDU installiert werden, damit eine TLS-Verbindung mit dem SMTP-Server erfolgreich hergestellt werden kann.
-i	<certificate file name>	Der Dateiname des Zertifikats.

Beispiel:

```
apc> smtp
E000: Success


 From:              address@example.com
 Server:            mail.example.com
 Port:              25
 Auth:              disabled
 User:              User
 Password:          <not set>
 Encryption:        none
 Req. Cert:         disabled
 Cert File:         <n/a>
```

Fehlermeldung: E000, E102

snmp

Zugriff: Super-Benutzer, Administrator, Nur-Netzwerk-Benutzer

Beschreibung: SNMPv1 aktivieren oder deaktivieren und konfigurieren.

HINWEIS: SNMPv1 ist standardmäßig deaktiviert. Der Community-Name `(-c[n])` muss festgelegt werden, bevor die SNMPv1-Kommunikation hergestellt werden kann.

Parameter:

Option	Argumente	Beschreibung
`-S`	`<enable | disable>`	SNMPv1 aktivieren oder deaktivieren
`-c [n]`	`<Community>`	Geben Sie einen Community-Namen oder eine Zeichenfolge an.
`-a [n]`	`<read | write | writeplus | disable>`	Geben Sie die Nutzungsrechte an.
`-n [n]`	`<IP or Domain Name>`	Geben Sie die IPv4/IPv6-Adresse oder den Domänennamen der Netzwerkverwaltungsstation an.
`[n]` = die Zugangskontrollnummer (the access control number): 1,2,3 oder 4.		

Beispiel: Um SNMP Version 1 zu aktivieren, geben Sie Folgendes ein

```
apc> snmp -S enable
E000: Success
Reboot required for change to take effect.
```

Fehlermeldung: `E000, E102`

snmpv3

Zugriff: Super-Benutzer, Administrator

Beschreibung: SNMPv3 aktivieren oder deaktivieren und konfigurieren.

HINWEIS: SNMPv3 ist standardmäßig deaktiviert. Ein gültiges Benutzerprofil muss mit festgelegten Passphrasen `(-a[n], -c[n])` aktiviert werden, bevor die SNMPv3 Kommunikation hergestellt werden kann.

Parameter:

Option	Argumente	Beschreibung
`-S`	`<enable | disable`	SNMPv3 aktivieren oder deaktivieren
`-u[n]`	`<Username>`	Geben Sie einen Benutzernamen, einen Authentifizierungsausdruck und einen Verschlüsselungsausdruck an.
`-a[n]`	`<Auth phrase>`	
`-c[n]`	`<Crypt phrase>`	
`-ap[n]`	`<sha | md5 | none>`	Geben Sie den Typ des Authentifizierungsprotokolls an.
`-pp[n]`	`<aes | des | none>`	Geben Sie das Datenschutzprotokoll (Verschlüsselungsprotokoll) an.
`-ac[n]`	`<enable | disable`	Zugriff aktivieren oder deaktivieren
`-au[n]`	`<User profile name>`	Gewähren Sie Zugriff auf ein bestimmtes Benutzerprofil.
`-n[n]`	`<IP or Domain Name>`	Geben Sie die IPv4/IPv6-Adresse oder den Hostnamen für die Netzwerkverwaltungsstation an.
`[n]` = Zugriffskontrolle # (Access Control #) = 1, 2, 3 bis 8		

Beispiel: Um dem Benutzer "JMurphy" Zugriffsebene 2 zu erteilen, geben Sie Folgendes ein

```
apc> snmpv3 -au2 "JMurphy"
E000: Success

*Reboot required for change to take effect
```

Fehlermeldung: `E000, E102`

snmptrap

Zugriff: Super-Benutzer, Administrator, Nur-Netzwerk-Benutzer

Beschreibung: SNMP-Trap-Generierung aktivieren oder deaktivieren

Parameter:

Option	Argumente	Beschreibung
-c[n]	<Community>	Geben Sie einen Community-Namen oder eine Zeichenfolge an.
-r[n]	<Receiver NMS IP>	Die IPv4/IPv6-Adresse oder der Hostname des Trap-Empfängers.
-l[n]	<Language code>	Geben Sie eine Sprache an. Englisch (enUS) ist derzeit die einzige verfügbare Option.
-t[n]	[snmpV1 | snmpV3]	Geben Sie den Trap-Typ an: SNMPv1 oder SNMPv3
-p[n]	<Port>	Geben Sie die SNMP-Trap-Portnummer für diesen Trap-Empfänger an (standardmäßig 162). Der Bereich reicht von 1 bis 65535.
-g[n]	[enable | disable]	Die Trap-Generierung für diesen Trap-Empfänger aktivieren oder deaktivieren. Standardmäßig aktiviert.
-a[n]	[enable | disable]	Die Authentifizierung von Traps für diesen Trap-Empfänger aktivieren oder deaktivieren, nur SNMPv1.
-u[n]	<profile1 | profile2 | profile3 | profile4>	Wählen Sie die Kennung des Benutzerprofils für diesen Trap-Empfänger aus, nur SNMPv3.
n = Trap-Empfänger # (Trap receiver #) = 1, 2, 3, 4, 5, oder 6		

Beispiel: Geben Sie Folgendes ein, um einen SNMPv1-Trap für Empfänger 1 mit dem Community-Namen public und der IP-Adresse von Empfänger 1, 10.169.118.100, in der englischen Standardsprache zu aktivieren und zu konfigurieren

```
apc> snmptrap -c1 public -r1 10.169.118.100 -l1 enUS -t1
snmpV1 -g1 enable
E000: Success
```

Fehlermeldung: E000, E102

ssh

Zugriff: Super-Benutzer, Administrator, Nur-Netzwerk-Benutzer

Beschreibung: Anzeigen, Löschen und Generieren von SSH-Serverschlüsseln.

HINWEIS: Sie müssen den `ssh key` befehl verwenden, um die folgenden Optionen zu verwenden.

Parameter:

Option	Argument	Beschreibung
`-s`		Anzeige des aktuell verwendeten SSH-Serverschlüssels.
`-f`		Anzeige des Fingerabdrucks des aktuellen SSH-Serverschlüssels.
`-d`		Löschen des aktuell verwendeten SSH-Serverschlüssels.
`-i`	`<filename>.p15`	Import des SSH-Serverschlüssels aus einer PKCS #15-Datei.
`-ecdsa`	`<256>` (bit size)	Generierung eines ECDSA-SSH Serverschlüssels (Elliptic Curve Digital Signature Algorithm) mit der angegebenen Größe in Bits.
`-rsa`	`<1024 | 2048 | 4096>`(bit size)	Generierung eines Rivest-Shamir-Adleman (RSA) SSH-Serverschlüssels mit der angegebenen Größe in Bits.

Beispiel 1: Um den SSH-Serverschlüssel zu löschen, geben Sie Folgendes ein

```
apc> ssh key -d
E000: Success
```

Beispiel 2: Um den SSH-Serverschlüssel von einer .p15-Datei, die vom CLI-Dienstprogramm NMC Security Wizard generiert wurde, zu importieren, geben Sie Folgendes ein

```
apc> ssh key -i nmc.p15
E000: Success
```

Fehlermeldungen: `E000, E102`

ssl

Zugriff: Super-Benutzer, Administrator, Nur-Netzwerk-Benutzer

Beschreibung: Konfiguration und Verwaltung des öffentlichen Schlüssels und des Web-UI-Zertifikats der Rack PDU sowie Erstellung einer Zertifikatsignierungsanforderung (CSR).

HINWEIS: Es gibt drei Sätze von Optionen für diesen Befehl, die unten angegeben sind (`key`, `csr`, und `cert`).

Konfiguration des öffentlichen Schlüssels (key):

Option	Argument	Beschreibung
`-s`		Zeigen Sie den aktuell verwendeten öffentlichen Schlüssel an.
`-d`		Löschen Sie den aktuell verwendeten öffentlichen Schlüssel.
`-i`	`<filename>.p15`	Importieren Sie den öffentlichen Schlüssel aus einer PKCS #15-Datei.
`-ecdsa`	`< 256 | 384 | 521>`	Generieren Sie eine digitale Signatur mit elliptischer Kurver Algorithmus (ECDSA) öffentlicher Schlüssel mit der angegebenen Größe in Bits.
`-rsa`	`< 1024 | 2048 | 4096>`	Generieren Sie einen öffentlichen Rivest–Shamir Adleman(RSA)-Schlüssel mit der angegebenen Größe in Bits.

*Sie können eine PCKS#15-Datei mit dem Netzwerkmanagement-Sicherheitsassistenten (verfügbar auf www.se.com) generieren.

Beispiel 1: Um einen neuen öffentlichen ECDSA-521-Schlüssel zu generieren, geben Sie Folgendes ein

```
apc> ssl key —ecdsa 521
E000: Success
```

Beispiel 2: Um den öffentlichen Schlüssel von einer .p15-Datei zu importieren, die vom CLI-Dienstprogramm NMC Security Wizard generiert wurde, geben Sie Folgendes ein

```
apc> ssl key -i nmc.p15
E000: Success
```

Zertifikatsignierungsanforderung (csr) konfigurieren:

Option	Argument	Beschreibung
`-s`	`<File Name>`	Zeigen Sie den aktuellen CSR an. Wenn kein Dateipfad angegeben ist, überprüft der Befehl den Standardspeicherort: ssl/nmc.csr.
`-q`	`<File Name>`	Erstellen Sie eine CSR aus einer aktiven Konfiguration. Wenn kein Dateipfad angegeben ist, wird die CSR am Standardspeicherort gespeichert: ssl/nmc.csr
`-CN`	`<Common Name>`	Erstellen Sie eine benutzerdefinierte CSR. Der Common-Name ist der vollqualifizierte Domänenname (FQDN) der Rack PDU. Zum Beispiel, ihre IP-Adresse oder *.nmc.local.
Benutzerdefinierte Optionen für Zertifikatsignierungsanforderungen (CSR). **HINWEIS:** Die folgenden Optionen sind nur für `-CN` verfügbar		
`-O`	`<organisation>`	Der Name Ihrer Organisation.
`-OU`	`<organization unit>`	Die Abteilung Ihrer Organisation, die das Zertifikat verwaltet.
`-C`	`<country>`	Der zweibuchstabige Ländercode, in dem sich Ihre Organisation befindet.
`-san`	`<Common Name | IP Address>`	Der Common-Name oder die IP-Adresse der Rack PDU.

HINWEIS: Erstellte Zertifikatsignierungsanforderungen werden im ssl-Verzeichnis der Rack PDU gespeichert. Siehe dir, Seite 35.

Beispiel 3: Geben Sie Folgendes ein, um eine schnelle CSR aus der aktuellen Konfiguration zu erstellen

```
apc> ssl csr -q
E000: Success
```

Beispiel 4: Geben Sie Folgendes ein, um eine minimale CSR zu erstellen

```
apc> ssl csr -CN 192.168.1.100 -C US
E000: Success
```

Beispiel 5: Geben Sie zum Erstellen einer benutzerdefinierten Zertifikatsignieranforderung (CSR) Folgendes ein

```
apc> ssl csr -CN apcXXXXXX.nmc.local -C US -san *.nmc.local
-san 190.0.2.0
E000: Success
```

Konfigurieren Sie das Zertifikat der Web-UI (cert):

Option	Argument	Beschreibung
-s	<File Name>	Zeigen Sie das angegebene Zertifikat an. **HINWEIS:** Wenn Sie diese Option ohne Argument ausführen, wird das aktuell verwendete Zertifikat angezeigt.
-f	<File Name>	Zeigen Sie den Fingerabdruck des angegebenen Zertifikats an. **HINWEIS:** Wenn Sie diese Option ohne Argument ausführen, wird der Fingerabdruck des aktuellen Zertifikats angezeigt.
-i	<File Name>	Importieren Sie ein Zertifikat.
HINWEIS: Das Argument ist für alle drei Optionen optional. Wenn kein Dateipfad angegeben ist, überprüft der Befehl den Standardspeicherort: ssl/nmc.crt.		

Beispiel 6: Um das aktive Zertifikat anzuzeigen, geben Sie Folgendes ein

```
apc> ssl cert -s
E000: Success
Certificate

  Serial Number: XXXXxXXXXXXxXXXXx

  Issuer: CN=., C=US

  Validity:
      Not Before: Mon Oct 11 16:46:44 2021 UTC
      Not Before: Sat Dec 15 23:59:59 2035 UTC


  Subject: CN=., C=US

  Subject Public Key Info:


      Public Key Algorithm: ECDSA (256 bit)
      X:
         xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:
         xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx
      Y:
         xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:
         xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx
      Curve: P-256

  Thumbprint: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

  Fingerprint:

  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

Beispiel 7: Geben Sie Folgendes ein, um nmc.crt im SSL-Verzeichnis anzuzeigen

```
ssl cert -s ssl/nmc.crt
```

Beispiel 8: Um ein anderes Zertifikat (*other.crt*) zu importieren, geben Sie Folgendes ein

```
apc> ssl cert -i other.crt
```

Fehlermeldungen: E000, E102

system

Zugriff: Super-Benutzer, Administrator

Beschreibung: Zeigen Sie den Systemnamen, den Kontakt und den Standort an und stellen sie ein. Konfigurieren Sie Systemmeldungen, zeigen Sie die Betriebszeit sowie Datum und Uhrzeit, den angemeldeten Benutzer und den übergeordneten Systemstatus P, N, A an. (Weitere Informationen zum Systemstatus finden Sie unter About the Main Screen, Seite 26).

Parameter:

Option	Argument	Beschreibung
-n	<system name>	Definieren Sie den Gerätenamen, den Namen der für das Gerät verantwortlichen Person und den physischen Standort des Geräts. **HINWEIS:** Wenn Sie einen Wert mit mehr als einem Wort definieren, müssen Sie den Wert in Anführungszeichen einschließen. Diese Werte werden auch von StruxureWare Data Center Expert oder EcoStruxure IT Expert und dem SNMP-Agenten der Rack PDU verwendet.
-c	<system contact>	
-l	<system location>	
-m	<system message>	Eine konfigurierbare benutzerdefinierte Nachricht oder ein Banner auf der Anmeldeseite der Web-UI, CLI (Seriell, Telnet, SSH), FTP oder SCP anzeigen.
-s	<enable | disable>	Erlauben, dass der Hostname mit dem Systemnamen synchronisiert wird, damit beide Felder automatisch den gleichen Wert enthalten. Dies ist dasselbe wie bei der Verwendung von „dns -y“. **HINWEIS:** Wenn Sie diese Funktion aktivieren, darf die Systemnamenkennung kein Leerzeichen mehr enthalten (da sie mit dem Feld Hostname synchronisiert wird).

Beispiel 1: Geben Sie Folgendes ein, um den Gerätestandort als Test Lab festzulegen

```
apc> system -l "Test Lab"
E000: Success
```

Beispiel 2: Um den Systemnamen als Don Adams festzulegen, geben Sie Folgendes ein

```
apc> system -n "Don Adams"
E000: Success
```

Fehlermeldung: E000, E102

tcpip

Zugriff: Super-Benutzer, Administrator

Beschreibung: Die IPV4-TCP/IP-Einstellungen für die Rack PDU anzeigen und manuell konfigurieren.

Parameter:

Option	Argument	Beschreibung
`-S`	`enable | disable`	TCP/IP v4 aktivieren oder deaktivieren.
`-l`	`<IPv4 address>`	Geben Sie die IP-Adresse der Rack PDU im Format *xxx.xxx.xxx.xxx* ein
`-s`	`<subnet mask>`	Geben Sie die Subnetzmaske 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`	`<domain name>`	Geben Sie den vom DNS-Server konfigurierten DNS-Namen ein.
`-h`	`<host name>`	Geben Sie den Hostnamen ein, den die Rack PDU verwenden soll.

Beispiel 1: Um die Netzwerkeinstellungen für die Rack PDU anzuzeigen, geben Sie ein

```
apc> tcpip
E000: Success
IP Address:     192.168.1.50
MAC Address:    XX XX XX XX XX XX
Subnet Mask:    255.255.255.0
Gateway:        192.168.1.1
Domain Name:    example.com
Host Name:      HostName
```

Beispiel 2: Um eine IP-Adresse von `192.168.1.49` manuell zu konfigurieren, geben Sie Folgendes ein

```
apc> tcpip -i 192.168.1.49
E000: Success
Reboot required for change to take effect
```

Fehlermeldung: `E000, E102`

tcpip6

Zugriff: Super-Benutzer, Administrator

Beschreibung: IPv6 aktivieren. Anzeigen und manuelles Konfigurieren dieser Netzwerkeinstellungen für die Rack PDU:

Parameter:

Option	Argument	Beschreibung
`-S`	`enable | disable`	IPv6 aktivieren oder deaktivieren.
`-man`	`enable | disable`	Aktivieren Sie die manuelle Adressierung für die IPv6-Adresse der Rack PDU.
`-auto`	`enable | disable`	Aktivieren Sie die Rack PDU, um die IPv6-Adresse automatisch zu konfigurieren
`-i`	`<IPv6 address>`	Stellen Sie die IPv6-Adresse der Rack PDU ein
`-g`	`<IPv6 gateway>`	Hiermit stellen Sie die IPv6-Adresse des Standard-Gateways ein
`-d6`	`router | stateful | stateless | never`	Stellen Sie den DHCPv6-Modus mit Parametern `router` controlled, `stateful` (für Adressen und andere Informationen behalten sie ihren Status bei), `stateless` (für andere Informationen als Adressen wird der Status nicht beibehalten) oder `never` ein.

Beispiel 1: Um die Netzwerkeinstellungen der Rack PDU anzuzeigen, geben Sie `tcpip6` ein und drücken Sie die ENTER taste.

```
apc> tcpip6
E000: Success
IPv6:                    enabled
Manual Settings:         disabled
IPv6 Address:            ::/64
MAC Address:             XX XX XX XX XX XX
Gateway:                 ::
IPv6 Manual Address:     disabled
IPv6 Autoconfiguration: enabled
DHCPv6 Mode:             router controlled
```

Beispiel 2: So konfigurieren Sie manuell eine IPv6-Adresse von 2001:0:0:0:0:FFD3:0:57ab, geben Sie ein

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

Fehlermeldung: `E000, E102`

user

Zugriff: Super-Benutzer, Administrator

Beschreibung: Den Benutzernamen, das Kennwort und das Inaktivitäts-Timeout für jeden Kontotyp konfigurieren.

HINWEIS: Sie können einen Benutzernamen nicht bearbeiten. Sie müssen ihn löschen und dann einen neuen Benutzer erstellen.

HINWEIS: Um die Einstellungen des Super-Benutzer-Kontos remote zu ändern, müssen Sie das aktuelle Kennwort (`-cp`) eingeben.

Parameter:

Option	Argument	Beschreibung
-n	<user>	Geben den Benutzer ein.
-cp	<current password>	Für einen Super-Benutzer müssen Sie das aktuelle Passwort angeben. **HINWEIS:** Die Option `-cp` wird nur benötigt, wenn die Einstellungen des Super-Benutzers remote geändert werden.
-pw	<user password>	Geben Sie diese Optionen für einen Benutzer an. **HINWEIS:** Die Beschreibung muss in Anführungszeichen gesetzt werden.
-pe	<user permission>	
-d	<user description>	
-e	enable | disable	Aktivieren oder deaktivieren Sie den Zugriff für das jeweilige Benutzerkonto.
-te	enable | disable	Den Touchscreen-Zugriff aktivieren oder deaktivieren.
-tp	<touch screen access pin>	Diese Option ist nur auf bestimmten Geräten verfügbar.
-tr	enable | disable	Die Touchscreen-Fernautorisierungsüberschreibung aktivieren. Diese Option ist nur auf bestimmten Geräten verfügbar. Wenn Sie diese Überschreibung aktivieren, ermöglicht die Rack PDU einem lokalen Benutzer die Anmeldung mit dem Kennwort für die Rack PDU, das lokal auf der Rack PDU gespeichert ist.
-st	<session timeout>	Geben Sie an, wie lange eine Sitzung dauert, wenn die Tastatur inaktiv ist, bevor der Benutzer automatisch abgemeldet wird.
-sr	enable | disable	Umgehen des RADIUS mithilfe der seriellen Konsolenverbindung (CLI), auch bekannt als Überschreibung der seriellen Remoteauthentifizierung
-el	enable | disable	Geben Sie die Farbcodierung des Ereignisprotokolls an.
-lf	tab | csv	Geben Sie das Format für den Export einer Protokolldatei an.
-ts	us | metric	Geben Sie die Temperaturskala Fahrenheit oder Celsius an.
-df	<mm/dd/yyyy | dd.mm.yyyy | mmm-dd-yy | dd-mmm-yy | yyyy-mm-dd>	Geben Sie ein Datumsformat an.
-lg	<language code (e.g. enUs)>	Geben Sie eine Benutzersprache an. Englisch ist derzeit die einzige verfügbare Sprache.
-del	<username>	Ein Benutzer löschen.
-l		Zeigen Sie die aktuelle Benutzerliste an.

Beispiel 1: Um die Abmeldezeit für den Benutzer "JMurphy" auf 10 minutes zu ändern, geben Sie Folgendes ein

```
user -n "JMurphy" -st 10
```

Beispiel 2: Um die Abmeldezeit für den Super-Benutzer "apc" auf 10 minutes zu ändern, geben Sie Folgendes ein:

```
user -n "apc" –cp <password> –st 10
```

Fehlermeldung: `E000, E102`

userdflt

Zugriff: Super-Benutzer, Administrator

Beschreibung: Ergänzende Funktion zu „user“, die Standardbenutzereinstellungen festlegt. Es gibt zwei Hauptfunktionen für die Standard-Benutzereinstellungen:

Legen Sie die Standardwerte fest, die in die einzelnen Felder eingefügt werden sollen, wenn das Konto auf Super-Benutzer- oder Administratorebene einen neuen Benutzer erstellt. Diese Werte können geändert werden, bevor die Einstellungen auf das System angewendet werden.

Für Remotebenutzer (nicht im System gespeicherte Benutzerkonten, die remote authentifiziert werden, z.B. RADIUS) sind dies die Werte, die für diejenigen verwendet werden, die nicht vom Authentifizierungsserver bereitgestellt werden. Wenn ein RADIUS-Server dem Benutzer beispielsweise keine Temperaturpräferenz bereitstellt, wird der in diesem Abschnitt definierte Wert verwendet.

Parameter:

Optionen	Argument	Beschreibung
-e	<enable | disable>	Standardmäßig wird der Benutzer bei der Erstellung aktiviert oder deaktiviert.
-pe	<Administrator | Device | Read-Only | Network-Only>	Berechtigungsstufe und Kontotyps des Benutzers angeben.
-d	<user description>	Benutzerbeschreibung angeben. Die Beschreibung muss in Anführungszeichen gesetzt werden.
-st	<session timeout> minute(s)	Standard-Timeout für die Sitzung angeben.
-bl	<bad login attempts>	Anzahl der fehlerhaften Anmeldeversuche eines Benutzers, bevor das System sein Konto deaktiviert. Bei Erreichen dieses Limits wird eine Meldung angezeigt, die den Benutzer darüber informiert, dass das Konto gesperrt wurde. Der Super-Benutzer oder ein Konto auf Administratorebene wird benötigt, um das Konto wieder zu aktivieren, damit sich der Benutzer erneut anmelden kann. **HINWEIS:** Ein Super-Benutzer-Konto kann nicht gesperrt, aber bei Bedarf manuell deaktiviert werden.
-el	<enable | disable> (Ereignisprotokoll-Farbcodierung)	Aktivieren oder Deaktivieren der Farbcodierung des Ereignisprotokolls.
-lf	<tab | csv> (Protokollformat exportieren)	Geben Sie das Format für den Protokollexport, Tab oder CSV an.
-ts	<us | metrics> (Temperaturskala)	Geben Sie dieTemperaturskala des Benutzers an. Diese Einstellung wird auch vom System verwendet, wenn eine Benutzereinstellung nicht verfügbar ist (z.B. E-Mail-Benachrichtigungen).
-df	<mm/dd/yyyy | dd.mm.yyyy | mmm-dd-yy | dd-mmm-yy | yyyy-mm-dd> (Datumsformat)	Geben das bevorzugten Datumsformat des Benutzers an.
-lg	<language code (enUs, etc)>	Benutzersprache. Derzeit wird nur enUs unterstützt.
-sp	<enable | disable>	Anforderungen an ein sicheres Passwort. Wann aktiviert: Das Passwort muss 8-64 Zeichen lang sein. Das Passwort muss mindestens einen Kleinbuchstaben, einen Großbuchstaben, eine Ziffer und ein Symbol (! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~) enthalten.
-pp	<interval in days>	Erforderliches Passwort-Änderungsintervall.

Beispiel: Geben Sie Folgendes ein, um das Sitzungszeitlimit des Standardbenutzers auf 60 minutes festzulegen

```
apc> userdflt -st 60
E000: Success
```

Fehlermeldung: E000, E102

web

Zugriff: Super-Benutzer, Administrator

Beschreibung: Aktivieren Sie den Zugriff auf die Web-UI über HTTP oder HTTPS.

Für zusätzliche Sicherheit können Sie die Porteinstellung für HTTP und HTTPS auf einen beliebigen nicht verwendeten Port von 5000 bis 32768 ändern. Benutzer müssen dann einen Doppelpunkt (:) im Adressfeld des Browsers verwenden, um die Portnummer anzugeben. 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`

Parameter:

Option	Argument	Definition
`-h`	`enable | disable`	Hiermit aktivieren oder deaktivieren Sie den Zugriff auf die Benutzeroberfläche für HTTPS. Standardmäßig ist HTTP deaktiviert.
`-s`	`enable | disable`	Hiermit aktivieren oder deaktivieren Sie den Zugriff auf die Benutzeroberfläche für HTTPS. Standardmäßig ist HTTPS aktiviert. Wenn HTTPS aktiviert ist, werden Daten während der Übertragung verschlüsselt und durch ein digitales Zertifikat authentifiziert.
`-mp`	`<minimum protocol>`	Geben Sie das Mindestprotokoll an, das von der Webschnittstelle verwendet wird: SSL v3.0, TLS v1.1 oder TLS v1.2.
`-ph`	`<http port #>`	Geben Sie den TCP/IP-Port an, der von HTTP für die Kommunikation mit der Rack PDU verwendet wird (standardmäßig 80). Der andere verfügbare Bereich ist 5000– 32768.
`-ps`	`<https port #>`	Geben Sie den TCP/IP-Port an, der von HTTPS für die Kommunikation mit der Rack PDU verwendet wird (standardmäßig 443). Der andere verfügbare Bereich ist 5000–32768.
`-lsp`	`enable | disable`	Den Zugriff auf die Eingeschränkte Statusseite in der Web-UI aktivieren oder deaktivieren.
`-lsd`	`enable | disable`	Aktivieren oder deaktivieren Sie die eingeschränkte Statusseite, die als Standardseite beim Zugriff auf die IP-Adresse oder den Hostnamen des Geräts in einem Webbrowser verwendet wird.
`-cs`	`<0 | 1 | 2 | 3 | 4>`	Wählen Sie die Sicherheitsstufe von TLS v1.2-Verschlüsselungssammlungen zwischen 0 und 4 aus, wobei 4 die höchste Sicherheitsstufe und 0 die niedrigste Sicherheitsstufe ist. Der Standardwert ist 4. **HINWEIS:** Die Option -cs wird nur angewendet, wenn -mp auf TLS v1.2 gesetzt ist. Wenn ein Wert zwischen 0 und 4 eingegeben wird, antwortet die CLI mit einer Liste der derzeit zulässigen SSL-Verschlüsselungssammlungen.
`-hs`	`enable | disable`	Aktivieren/deaktivieren Sie den HTTP Strict Transport Security Header (HSTS)-Antwortheader.

Beispiel 1: Geben Sie Folgendes ein, um jeglichen Zugriff auf die Web-UI zu verhindern

```
apc> web -h disable -s disable
```

Beispiel 2: Geben Sie Folgendes ein, um den von HTTP verwendeten TCP/IP-Port zu ändern

```
apc> web -ph 80
E000: Success
```

Fehlermeldung: `E000, E102`

whoami

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer, Nur-Lese-Benutzer, Nur-Netzwerk-Benutzer

Beschreibung: Stellt Anmeldeinformationen für den aktuellen Benutzer bereit.

Parameter: Keine

Beispiel:

```
apc> whoami
E000: Success
admin
```

Fehlermeldung: `E000, E102`

wifi

Reserviert für zukünftige Verwendung.

xferINI

Zugriff: Super-Benutzer, Administrator

Beschreibung: Verwenden Sie XMODEM, um eine INI-Datei hochzuladen, während Sie über eine serielle Verbindung auf die Befehlszeilenschnittstelle zugreifen. Nachdem der Upload abgeschlossen ist:

- Bei System- oder Netzwerkänderungen wird die Befehlszeilenschnittstelle neu gestartet und Sie müssen sich erneut anmelden.
- \Wenn Sie eine Baudrate für die Dateiübertragung ausgewählt haben, die nicht mit der Standardbaudrate für die NMC-Karte übereinstimmt, müssen Sie die Baudrate auf die Standardwerte zurücksetzen, um die Kommunikation mit der NMC-Karte wiederherzustellen.

Parameter: Keine

Beispiel:

```
apc> xferINI
Enter 'YES' or 'Y' to continue or <ENTER> to cancel: <user enters
'YES' or 'Y'>
---- File Transfer Baud Rate -------------------------------
      1- 2400
      2- 9600
      3- 19200
      4- 38400
> <user enters baudrate selection>
Transferring at current baud rate (9600), press <ENTER>...
<user presses <ENTER>>
Start XMODEM-CRC Transfer Now!
CC
<user starts sending INI>
150 bytes have successfully been transmitted.

apc>
```

Fehlermeldung: Keine

xferStatus

Zugriff: Super-Benutzer, Administrator

Beschreibung: Das Ergebnis der letzten Dateiübertragung anzeigen.

Parameter: Keine

Beispiel:

```
apc> xferStatus
E000: Success

Result of last file transfer: Successful
```

Beschreibungen der Übertragungsergebniscodes finden Sie unter Ergebniscodes der letzten Übertragung, Seite 163.

Fehlermeldung: `E000`

Gerätebefehlsbeschreibungen

Network Port Sharing-Befehle

Die CLI ermöglicht das Senden von Befehlen an die Gast-Rack PDUs. Der Benutzer kann die Display-ID der zu befehlenden Rack PDU angeben, gefolgt von einem Doppelpunkt vor dem ersten Argument (oder als erstes Argument, wenn der Befehl normalerweise keine Argumente enthält). Wenn eine Display-ID optional ist, wird durch Weglassen der ID lediglich die lokale Rack PDU angesteuert.

Zum Beispiel: `<command> [<id#>:]<arg1> <arg2>`

Dadurch wird `<command> <arg1> <arg2>` mit der durch `[<id#>:]` angegebenen Display-ID an die Rack PDU gesendet. Auf die Display-ID folgt ein Doppelpunkt (:), gefolgt von `arg1` ohne Leerzeichen. Leerzeichen werden verwendet, um Argumente abzugrenzen.

alarmList

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer

Beschreibung: Zeigt Alarme an, die auf dem Gerät (oder einem anderen Gerät in der Gruppe, wenn NPS verwendet wird) vorhanden sind. Die id# kann je nach Gruppengröße zwischen 1 und 32 liegen.
Parameter: Keine.

Beispiel: Um alle aktiven Warnmeldungen anzuzeigen, geben Sie Folgendes ein:

```
apc> alarmList [<id#>:]
-----Device Alarm Status------------------
      1 Critical Alarm Present.
-----------------------------------------
[Critical] rack PDU 1: Internal power supply #2 fault, under
voltage.
   <ESC>- Exit, <ENTER>- Refresh
```

Fehlermeldung: `E102`

bkLowLoad

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer

Beschreibung: Stellen Sie den Niedriglastschwellenstrom der Bank in Ampere ein oder zeigen Sie ihn an. Sie können alle Bänke, eine einzelne Bank, einen Bereich oder eine durch Kommas getrennte Liste einzelner Bänke und/oder Bereiche angeben. Die id# kann je nach Gruppengröße zwischen 1 und 32 liegen.

Parameters: `[<id#>:] <all | bank#> [<current>]`

`bank#` = Eine einzelne Zahl oder ein Zahlenbereich, getrennt durch einen Bindestrich oder ein Komma; getrennte Liste einzelner Banknummern und/oder Nummernbereiche.
`current` = Die neue Bankschwelle (Ampere)

Beispiel 1: Um den Niedriglastschwellenwert für alle Banken auf 1A festzulegen, geben Sie Folgendes ein:

```
apc> bkLowLoad all 1
E000: Success
```

Beispiel 2: Geben Sie Folgendes ein, um die Einstellung für den Niedriglastschwellenwert für die Banken 1 bis 3 anzuzeigen:

```
apc> bkLowLoad 1-3
E000: Success
1: 1 A
2: 1 A
3: 1 A
```

Fehlermeldung: `E000, E102`

bkNearOver

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer

Beschreibung: Den Schwellenstrom für die Bank nahe der Überlast in Ampere einstellen oder anzeigen. Sie können alle Banken, eine einzelne Bank, einen Bereich oder eine kommagetrennte Liste einzelner Banken und/oder Bereiche angeben. Die id# kann je nach Gruppengröße zwischen 1 und 32 liegen.

Parameters: `[<id#>:] <all | bank#> [<current>]`

Beispiel 1: Geben Sie Folgendes ein, um den Überlastungsgrenzwert für alle Banken auf 10A festzulegen:

```
apc> bkNearOver all 10
E000: Success
```

Beispiel 2: Geben Sie Folgendes ein, um die Einstellung für den Schwellenwert für nahezu Überlastung für die Banken 1 bis 3 anzuzeigen:

```
apc> bkNearOver 1-3
E000: Success
1: 10 A
2: 10 A
3: 10 A
```

Beispiel 3: Geben Sie Folgendes ein, um die Einstellung für den Schwellenwert für nahezu Überlast für die Banken 1 und 2 auf der Gast-Rack PDU 3 anzuzeigen:

```
apc> bkNearOver 3:1-2
E000: Success
1: 16 A
2: 16 A
```

Fehlermeldung: `E000, E102`

bkOverLoad

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer

Beschreibung: Den Banküberlastschwellenstrom in Ampere einstellen oder anzeigen. Sie können alle Banken, eine einzelne Bank, einen Bereich oder eine kommagetrennte Liste einzelner Banken und/oder Bereiche angeben. Die id# kann je nach Gruppengröße zwischen 1 und 32 liegen.

Parameters: `[<id#>:] <all | bank#> [<current>]`

Beispiel 1: Geben Sie Folgendes ein, um den Schwellenwert für die Banküberlastung für alle Banken auf 13A festzulegen:

```
apc> bkOverLoad all 13
E000: Success
```

Beispiel 2: Geben Sie Folgendes ein, um die Einstellung des Banküberlastungsschwellenwerts für die Banken 1 bis 3 anzuzeigen:

```
apc> bkOverLoad 1-3
E000: Success
1: 13 A
2: 13 A
3: 13 A
```

Fehlermeldung: `E000, E102`

bkPeakCurr

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer

Beschreibung: Anzeige der Spitzenstrommessung von einer Bank oder Banken. Die id# kann je nach Gruppengröße zwischen 1 und 32 liegen.

Parameters: `[<id#>:] <"all" | bank#>`

Beispiel:

```
apc> bkPeakCurr 2
E000: Success
2: 0.0 A
```

```
apc> bkPeakCurr all
E000: Success
1: 0.0 A
2: 0.0 A
```

Fehlermeldung: `E000, E102`

bkReading

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer, Nur-Lese-Benutzer

Beschreibung: Den aktuellen Messwert einer Bank in Ampere anzeigen. Sie können alle Banken, eine einzelne Bank, einen Bereich oder eine kommagetrennte Liste einzelner Banken und/oder Bereiche angeben. Die id# kann je nach Gruppengröße zwischen 1 und 32 liegen.

Parameters: `[<id#>:] [<all | bank#>]`

Beispiel 1: Um den aktuellen Messwert für Bank 3 anzuzeigen, geben Sie Folgendes ein:

```
apc> bkReading 3
E000: Success
3: 4.2 A
```

Beispiel 2: Um den aktuellen Messwert für alle Banken anzuzeigen, geben Sie Folgendes ein:

```
apc> bkReading all
E000: Success
1: 6.3 A
2: 5.1 A
3: 4.2 A
```

Fehlermeldung: `E000, E102`

bkRestrictin

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer

Beschreibung: Einstellen oder Lesen der Überlastungsbeschränkungsfunktion, um zu verhindern, dass Benutzer Ausgänge mit Strom versorgen, wenn eine Überlastungsschwelle verletzt wird. Die id# kann je nach Gruppengröße zwischen 1 und 32 liegen.

Parameter: `[<id#>:] < all | phase#> [< none | near | over >]`

Akzeptable Argumente sind `none`, `near`, und `over`.

Wählen Sie zum Angeben von Phasen eine der folgenden Optionen aus.

Geben Sie an: `all`, eine einzelne Phase, ein Bereich oder eine durch Kommas getrennte Liste von Phasen.
`phase# =` Eine einzelne Zahl oder ein Zahlenbereich, der durch einen Bindestrich getrennt ist, oder eine durch Kommas getrennte Liste von einphasigen Nummern und / oder Nummernbereichen.

Beispiel 1: Geben Sie Folgendes ein, um die Überlastungsbeschränkung für Phase drei auf keine festzulegen:

```
apc> bkRestrictn 3 none
E000: Success
```

Beispiel 2: Um die Überlastbeschränkungen für alle Phasen anzuzeigen, geben Sie Folgendes ein:

```
apc> bkRestrictn all
E000: Success
1: over
2: near
3: none
```

Beispiel 3: Geben Sie Folgendes ein, um die Überlastungsbeschränkungen für alle Phasen auf der Gast-Rack PDU 2 anzuzeigen:

```
apc> bkRestrictn 2:all
E000: Success
1: None
2: None
```

Fehlermeldung: `E000, E102`

devLowLoad

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer

Beschreibung: Einstellen oder Anzeigen der Warnschwelle für niedrige Last des Geräts in Kilowatt. Die id# kann je nach Gruppengröße zwischen 1 und 32 liegen.

Parameters: `[<id#>:] [<threshold>]` = Neue Leistungsschwelle (Kilowatts).

Beispiel 1: Geben Sie Folgendes ein, um den Schwellenwert für niedrige Last anzuzeigen:

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

Beispiel 2: Um die Niedriglastschwelle auf 1 kW einzustellen, geben Sie Folgendes ein:

```
apc> devLowLoad 1.0
E000: Success
```

Fehlermeldung: `E000, E102`

devNearOver

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer

Beschreibung: Einstellen oder Anzeigen des Schwellenwerts für die Beinahe-Überlastung in Kilowatt für das Gerät. Die id# kann je nach Gruppengröße zwischen 1 und 32 liegen.

Parameters: `[<id#>:] [<threshold>]` = Neue Ausgangsschwelle (Kilowatts).

Beispiel 1: Geben Sie Folgendes ein, um den Schwellenwert für die Beinahe-Überlastung anzuzeigen:

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

Beispiel 2: Um den Schwellenwert für die Beinahe-Überlastung auf 21.3 kW einzustellen, geben Sie Folgendes ein:

```
apc> devNearOver 21.3
E000: Success
```

Fehlermeldung: `E000, E102`

devOverLoad

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer

Beschreibung: Einstellen oder Anzeigen der Überlastschwelle in Kilowatt für das Gerät. Die id# kann je nach Gruppengröße zwischen 1 und 32 liegen.

Parameters: `[<id#>:] [<threshold>]` = Neue Ausgangsschwelle (Kilowatts).

Beispiel 1: Um den Überlastungsschwellenwert anzuzeigen, geben Sie Folgendes ein:

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

Beispiel 2: Um den Überlastungsschwellenwert auf 25.5 kW einzustellen, geben Sie Folgendes ein:

```
apc> devOverLoad 25.5
E000: Success
```

Beispiel 3: Geben Sie Folgendes ein, um den Überlastungsschwellenwert für die Gast-Rack PDU 3 anzuzeigen:

```
apc> devOverLoad 3:
E000: Success
5.0 kW
```

Fehlermeldung: `E000, E102`

devPeakLoad

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer

Beschreibung: Anzeige der Spitzenleistungsmessung vom Gerät. Die id# kann je nach Gruppengröße zwischen 1 und 32 liegen.

Parameter: `[<id#>:]`

Beispiel:

```
apc> devPeakLoad
E000: Success
0.0 kW
```

Fehlermeldung: `E000, E102`

devReading

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer, Nur-Lese-Benutzer

Beschreibung: Die Gesamtleistung in Kilowatt oder die Gesamtenergie in kilowatt-hours für das Gerät anzeigen.

Parameters: `[<id#>:] <power | energy | appower | pf>`

Argument	Definition
`<power>`	Anzeige der Gesamtleistung in Kilowatt
`<energy>`	Anzeige der Gesamtenergie in kilowatt-hours
`<appower>`	Anzeige der gesamten Scheinleistung in kVA
`<pf>`	Anzeigen des Leistungsfaktors

Beispiel 1: Um die Gesamtleistung anzuzeigen, geben Sie Folgendes ein:

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

Beispiel 2: Um die Gesamtenergie anzuzeigen, geben Sie Folgendes ein:

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

Fehlermeldung: `E000, E102`

devStartDly

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer

Beschreibung: Einstellen oder Anzeigen der Zeit in Sekunden, die zu der Einschaltverzögerung jedes Ausgangs addiert wird, bevor sich der Ausgang einschaltet, nachdem die PDU mit Strom versorgt wurde (Kaltstartverzögerung). Zulässige Werte liegen im Bereich von 1 bis 300 seconds oder nie (nie einschalten). Die id# kann je nach Gruppengröße zwischen 1 und 32 liegen.

Parameters: `[<id#>:] [<time | never>]`

Argument	Definition
`[time | "never"]`	time = Kaltstartverzögerungszeit in ganzen Sekunden oder „never“; Groß- und Kleinschreibung wird nicht beachtet

Beispiel 1: Um die Kaltstartverzögerung anzuzeigen, geben Sie Folgendes ein:

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

Beispiel 2: Um die Kaltstartverzögerung auf sechs seconds einzustellen, geben Sie Folgendes ein:

```
apc> devStartDly 6
E000: Success
```

Beispiel 3: Geben Sie Folgendes ein, um die Kaltstartverzögerung auf der Gast-Rack PDU 2 auf sechs seconds einzustellen:

```
apc> devStartDly 2:6
E000: Success
```

Beispiel 4: Geben Sie Folgendes ein, um die Kaltstartverzögerung auf der Gast-Rack PDU 2 anzuzeigen:

```
apc> devStartDly 2:
E000: Success
6 sec
```

Fehlermeldung: `E000, E102`

dispID

Zugriff: Super-Benutzer, Administrator

Beschreibung: Einstellen oder Lesen der Display-ID des Geräts. Die id# kann je nach Gruppengröße zwischen 1 und 32 liegen.

Parameters: `[<id#>:] [<new_id#>]` = Einstellen der Anzeige-ID.

Beispiel:

```
apc> dispID
E000: Success
RPDU ID: 1*
apc> dispID 2
E000: Success
RPDU ID: 2*
apc> dispID 3: 2
E000: Success
```

Fehlermeldung: `E000, E102`

envSens

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer

Beschreibung: Lesen oder Schreiben von Werten, die sich auf die allgemeinen Eigenschaften des angeschlossenen Sensorzubehörs beziehen. Die id# sollte die Display-ID des Zielgeräts sein.

Parameter: `[<id#>:][-<opt>[ <sens_id_num>[ <cfg_input>]]]`

Beispiel 1: Geben Sie Folgendes ein, um alle allgemeinen Informationen zu lesen, die auf dem Sitzungshost verfügbar sind:

```
apc>envsens

     Sens. Type 1        : Temperature Sensor
     Sens. Status 1      : OK
     Sens. Name 1        : SensorName

     Sens. Type 2        : Temperature and Humidity Sensor
     Sens. Status 2      : OK
     Sens. Name 2        : SensorName

 E000: Success
```

Beispiel 2: Geben Sie Folgendes ein, um den Namen der beiden verbundenen Sensoren des Sitzungshosts zu lesen:

```
apc>envsens -n
     Sens. Name 1 : SensorName
     Sens. Name 2 : SensorName
E000: Success
```

Beispiel 3: Geben Sie Folgendes ein, um den Sensornamen von Port 2 des Sitzungshosts zu lesen:

```
apc>envsens -n 2
    SensorName
E000: Success
```

Beispiel 4: Geben Sie Folgendes ein, um den Sensornamen von Port 2 des Sitzungshosts zu ändern

```
apc>envsens -n 2 "Sensor 2"
     Old Sens. Name 2 : SensorName
     New Sens. Name 2 : Sensor 2
E000: Success
```

Beispiel 5: So wenden Sie den Befehl "`envSens`" auf Gastgerät 3 statt auf den Sitzungshost, geben Sie Folgendes ein:

```
apc>envsens 3:

     Sens. Type 1        : Temperature and Humidity Sensor
     Sens. Status 1      : OK
     Sens. Name 1        : SensorName

     Sens. Type 2        : Temperature and Humidity Sensor
     Sens. Status 2      : OK
     Sens. Name 2        : SensorName

E000: Success
```

Fehlermeldung: `E000, E100, E102, E106`

Temperatur-/Feuchtigkeitssensoren

HINWEIS: Sie müssen einen optionalen Temperature/Humidity Sensors von APC by Schneider Electric (AP9335TH) an Ihrer Rack PDU installiert haben, um die feuchtigkeitsbezogenen Befehle verwenden zu können.

humAlGen

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer

Beschreibung: Einstellen und Ablesen, ob Feuchtigkeitsalarme aktiviert oder deaktiviert sind. Die id# kann je nach Gruppengröße zwischen 1 und 32 liegen.

Parameter: `[<id#>:][<enable> | disable>]`

`enable` = Die Luftfeuchtigkeitsalarme aktivieren.
`disable` = Die Luftfeuchtigkeitsalarme deaktivieren.

Beispiel:

```
apc> humAlGen enable
E000: Success

apc> humAlGen disable
E000: Success
```

Fehlermeldung: `E000, E102`

humHyst

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer

Beschreibung: Einstellen und Ablesen des Hysteresewertes für die Feuchtigkeitsschwelle. Die id# kann je nach Gruppengröße zwischen 1 und 32 liegen.

Parameters: `[<id#>:] [<value>]` = neuer Hystereseschwellenwert (% RH)

Beispiel:

```
apc> humHyst
E000: Success
6 %RH

apc> humHyst 5
E000: Success
```

Fehlermeldung: `E000, E102`

humLow

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer

Beschreibung: Einstellen oder Anzeigen der Schwelle für niedrige Luftfeuchtigkeit in Prozent der relativen Luftfeuchtigkeit. Die id# kann je nach Gruppengröße zwischen 1 und 32 liegen.

Parameters: `[<id#>:] [<humidity>]` = neue niedrige Feuchtigkeitsschwelle

Beispiel 1: Um den Schwellenwert für niedrige Luftfeuchtigkeit anzuzeigen, geben Sie Folgendes ein:

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

Beispiel 2: Um den Schwellenwert für niedrige Luftfeuchtigkeit festzulegen, geben Sie Folgendes ein:

```
apc> humLow 12
E000: Success
```

Beispiel 3: Um den Schwellenwert für niedrige Luftfeuchtigkeit auf der Gast-Rack PDU 3 anzuzeigen, geben Sie Folgendes ein:

```
apc> humLow 3:
E000: Success
10 %RH
```

Fehlermeldung: `E000, E102`

humMin

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer

Beschreibung: Einstellen oder Anzeigen der Mindestfeuchtigkeitsschwelle in Prozent der relativen Luftfeuchtigkeit. Die id# kann je nach Gruppengröße zwischen 1 und 32 liegen.

Parameters: `[<id#>:] [<humidity>]` = neue Mindestfeuchtigkeitsschwelle

Beispiel 1: Um den Mindestfeuchtigkeitsschwellenwert anzuzeigen, geben Sie Folgendes ein:

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

Beispiel 2: Um den Mindestfeuchtigkeitsschwellenwert festzulegen, geben Sie Folgendes ein:

```
apc> humMin 8
E000: Success
```

Beispiel 3: Geben Sie Folgendes ein, um den Mindestfeuchtigkeitsschwellenwert für die Gast-Rack PDU 3 auf 18% RH festzulegen:

```
apc> humMin 3:18
E000: Success
```

Fehlermeldung: `E000, E102`

humReading

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer, Ausgangsbenutzer, Nur-Lese-Benutzer

Beschreibung: Den Feuchtigkeitswert vom Sensor anzeigen. Die id# kann je nach Gruppengröße zwischen 1 und 32 liegen.

Parameter: `[<id#>:]`

Beispiel 1: Um den Feuchtigkeitswert anzuzeigen, geben Sie Folgendes ein:

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

Beispiel 2: Um den Feuchtigkeitswert auf der Gast-Rack PDU 2 anzuzeigen, geben Sie Folgendes ein:

```
apc> humReading 2:
E000: Success
48 %RH
```

Fehlermeldung: `E000, E102, E201`

humSens

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer

Beschreibung: Lesen oder Schreiben der Werte in Bezug auf das angeschlossene Feuchtigkeitsmesssensor-Zubehör. Die id# sollte die Display-ID des Zielgeräts sein.

Parameter: `[<id#>:][-<opt>[ <sens_id_num>[ <cfg_input>]]]`

Beispiel 1: Geben Sie Folgendes ein, um alle auf dem Sitzungshost verfügbaren feuchtigkeitsbezogenen Informationen zu lesen:

```
apc>humsens

            Humidity 2  : 22 %RH
              H. Low 2  : 15 %RH
          H. Minimum 2  : 10 %RH
       H. Hysteresis 2  : 2 %RH
            H. Alarms 2  : Enabled
             H. State 2  : Normal

E000: Success
```

Beispiel 2: Um die gemessene Luftfeuchtigkeit des einen angeschlossenen Sensors des Sitzungshosts zu lesen, geben Sie Folgendes ein:

```
apc>humsens -h
     Humidity 2 : 22 %RH
E000: Success
```

Beispiel 3: Geben Sie Folgendes ein, um die Feuchtigkeit des Sensors von Port 2 des Sitzungshosts zu lesen:

```
apc>humsens -h 2
     22 %RH
E000: Success
```

Beispiel 4: Geben Sie Folgendes ein, um die Erzeugung von Luftfeuchtigkeitsalarmen für Port 2 des Sitzungshosts zu deaktivieren:

```
apc>humsens -g 2 Disabled
     Old H. Alarms 2 : Enabled
     New H. Alarms 2 : Disabled
E000: Success
```

Beispiel 5: So wenden Sie den Befehl "`humsens -g 1 Disabled`" auf Gastgerät 3 statt auf den Sitzungshost, geben Sie Folgendes ein:

```
apc>humsens 3:-g 1 Disabled
     Old H. Alarms 1 : Enabled
     New H. Alarms 1 : Disabled
E000: Success
```

Fehlermeldung: `E000, E100, E102, E106`

humStatus

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer, Nur-Lese-Benutzer

Beschreibung: Zeigt den Status des Sensors an. Die id# kann je nach Gruppengröße zwischen 1 und 32 liegen. Antworten: Not Connected (Nicht angeschlossen), Min. Schwellenwert unterschritten (Min Threshold Violation), Niedriger Schwellenwert unterschritten (Low Threshold Violation), Normal.

Parameter: `[<id#>:]`

Beispiel: Um den Status des Feuchtigkeitssensors anzuzeigen, geben Sie Folgendes ein:

```
apc> humStatus
Not Connected
```

Fehlermeldung: Keine

lcd

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer

Beschreibung: Einstellen oder Lesen des LCD (Ein/Aus). Die id# kann je nach Gruppengröße zwischen 1 und 32 liegen.

Parameter: `[<id#>:] [<on|off>]`

Beispiel:

```
apc> lcd off
E000: Success
apc> lcd 1: on
E000: Success
```

Fehlermeldung: `E000, E100, E102`

lcdBlink

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer

Beschreibung: Blinken des LCD-Displays für den angegebenen Zeitraum. Die id# kann je nach Gruppengröße zwischen 1 und 32 liegen. Gültiger Timeout-Bereich: 1 bis 10 minutes.

Parameter: `[<id#>:] <timeout>` = ist die Anzahl der Minuten, die das Display blinken soll.

Beispiel:

```
apc> lcdBlink
E000: Success
```

Fehlermeldung: `E000, E102`

logToFlash

Zugriff: Super-Benutzer, Administrator

Beschreibung: Export der Logdateien auf den USB-Stick. Die Datei wird eine komprimierte Datei sein. Sie wird event.txt, config.ini. debug.txt, data.txt enthalten. Wenn eine Ausnahme auftritt, enthält sie auch dump.txt.

Parameter: `[<filename>]` = ist der Anhang zum .tar-Namen der Debug-Datei. Wenn kein Name eingegeben wird, wird die Seriennummer des Geräts als Name für die Datei verwendet.

Beispiel 1:

```
apc>logToFlash 01292018
Creating report file: /debug_01292018.tar Press <ESC> to abort
0% completed...
Exporting logs... please do not remove USB flash
12% completed...Exporting logs... please do not remove USB flash...
Exporting logs... please do not remove USB
flash 60% completed...
Logs export completed. You may remove USB flash now
```

Beispiel 2:

```
apc>logToFlash
Creating report file:
/debug_ZA1234567890.tar Press <ESC> to abort
0% completed...Exporting logs... please do not remove USB flash
12% completed...Exporting logs... please do not remove USB flash...
Exporting logs... please do not remove USB flash
60% completed...Logs export completed. You may remove USB flash now
```

Fehlermeldungen: `E000, E102`

modbus

Zugriff: Super-Benutzer, Administrator

Beschreibung: Hiermit öffnen und konfigurieren Sie die Optionen für Modbus TCP. Modbus TCP ermöglicht einem Gebäudemanagementsystem (Building Management System, BMS) die Rack PDU.

Parameter:

Option	Argument	Definition
`-te`	`<enable | disable>`	Aktiviert oder deaktiviert Modbus TCP.
`-tp`		Zeigt die Modbus TCP-Portnummer an. (Sie können die Modbus TCP-Portnummer in der Web-UI einstellen.)
`-tTo`	`<minimum protocol>`	Gibt das Modbus TCP-Kommunikations-Timeout in Sekunden an, wobei 0 bedeutet, dass für die Verbindung niemals ein Timeout auftritt.
`-ka`	`<enable | disable>`	Modbus TCP Keep-Alive. • Wenn keine Kommunikation erkannt wird, sendet die PDU alle 2 hours und 75 seconds ein Datenpaket an den Server. • Verhindert einen Kommunikations-Timeout, wenn der **Kommunikations-Timeout (Communication Timeout)** auf 7.275 seconds oder mehr eingestellt ist.
`-rDef`		Setzt die Modbus-Konfiguration auf die Standardwerte zurück.

Beispiel 1: Geben Sie Folgendes ein, um die Modbus-Einstellungen anzuzeigen

```
apc> modbus
E002: Success
TCP Status = DISABLED
TCP Port Number = 502
TCP Communication Timeout = 5 secs
Keep-alive = ENABLED
```

Beispiel 2: Geben Sie Folgendes ein, um Modbus TCP zu aktivieren

```
apc> modbus -tE enable E002: Success
Reboot required for change to take effect.
```

Fehlermeldung: `E000, E002, E101, E102`

nps

Zugriff: Super-Benutzer, Administrator

Beschreibung: Lesen oder Schreiben von Werten, die sich auf die network port sharing (NPS) Gruppe. beziehen. Die id# sollte die Display-ID des Zielgeräts sein.

Parameter: `[<id#>:][-<opt>[ <opt_index>[ <cfg_input>]]]`

Beispiel 1: Geben Sie Folgendes ein, um alle auf dem Sitzungshost verfügbaren gruppenbezogenen Informationen zu lesen:

```
apc>nps

        Type  : Host
   PwrShr En  : Enabled

 PwrShr St 1  : Active

 PwrShr St 2  : Active

 E000: Success
```

Beispiel 2: Geben Sie Folgendes ein, um die Konfiguration zur Aktivierung der NPS-Stromfreigabe des Sitzungshosts zu lesen:

```
apc>nps -pe
     Enabled
E000: Success
```

Beispiel 3: Geben Sie Folgendes ein, um die Konfiguration zur Aktivierung der NPS-Stromfreigabe für den Sitzungshost zu deaktivieren:

```
apc>nps -pe Disabled
     Old PwrShr En : Enabled
     New PwrShr En : Disabled
E000: Success
```

Beispiel 4: Geben Sie Folgendes ein, um zu versuchen, den Stromverteilungsfehler an Port 2 des Gastgeräts 4 zu beheben:

```
apc>nps 4:-ps 2 Active
     Old PwrShr St 2 : Fault
     New PwrShr St 2 : Inactive
E000: Success
```

Beispiel 5: Geben Sie Folgendes ein, um Gastgerät 1 zum NPS-Gruppenhost zu machen:

```
apc>nps 1:-t Host
     Old Type : Guest
     New Type : Host
E000: Success
```

Fehlermeldung: `E000, E100, E102, E106`

olAssignUsr

Zugriff: Super-Benutzer, Administrator

Beschreibung: Zuweisen der Steuerung von Ausgänge zu einem Ausgangsbenutzer, der in der lokalen Datenbank vorhanden ist. Die id# kann je nach Gruppengröße zwischen 1 und 32 liegen.

Parameter: `[<id#>:] <all | "outlet name" | outlet#> <user>`

Argument	Definition
`all`	Alle Geräteausgänge
`<outlet name>`	Der für einen bestimmten Ausgang konfigurierte Name. Der Ausgangsname muss als "outlet name" (in Anführungszeichen) angegeben werden, wenn der Ausgangsname ein Leerzeichen enthält.
`<outlet#>`	Eine einzelne Nummer oder ein durch einen Bindestrich getrennter Nummernbereich oder eine durch Kommas getrennte Liste einzelner Ausgangsnummern und Nummernbereiche.
`<user>`	Ein Benutzer, der in der lokalen Datenbank vorhanden ist.

Beispiel 1: Um einen Benutzer namens Bobby den Ausgängen 3, 5 bis 7 und 10 zuzuweisen, geben Sie Folgendes ein:

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

Beispiel 2: Um allen Ausgängen einen Benutzer namens Billy zuzuweisen, geben Sie Folgendes ein:

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

Beispiel 3: Geben Sie Folgendes ein, um allen Ausgängen auf der Gast-Rack PDU 3 einen Benutzer namens Billy zuzuweisen:

```
apc> olAssignUsr 3:all billy
E000: Success
```

Fehlermeldung: `E000, E102`

olCancelCmd

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer, und Ausgangsbenutzer, aber nur für die Ausgänge, denen der Benutzer zugeordnet ist.

Beschreibung: Bricht alle ausstehenden Befehle für einen Ausgang oder eine Gruppe von Ausgänge ab. Die id# kann je nach Gruppengröße zwischen 1 und 32 liegen.

Parameters: `[<id#>:] <all | "outlet name" | outlet#>`

Argument	Definition
`all`	Alle Geräteausgänge.
`<outlet name>`	Der für einen bestimmten Ausgang konfigurierte Name.
`<outlet#>`	Eine einzelne Nummer oder ein durch einen Bindestrich getrennter Nummernbereich oder eine durch Kommas getrennte Liste einzelner Ausgangsnummern und Nummernbereiche.

Beispiel 1: Um alle Befehle für Ausgang 3 abzubrechen, geben Sie Folgendes ein:

```
apc> olCancelCmd 3
E000: Success
```

Beispiel 2: Um alle Befehle für Ausgang 3 auf der Gast-Rack PDU 3 abzubrechen, geben Sie Folgendes ein:

```
apc> olCancelCmd 3:all
E000: Success
```

Fehlermeldung: `E000, E102 E104`

olDlyOff

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer und Ausgangsbenutzer, aber nur für Ausgänge, denen der Benutzer zugewiesen ist.

Beschreibung: Schaltet einen Ausgang oder eine Gruppe von Ausgängen nach der Ausschaltverzögerung aus. Die id# kann je nach Gruppengröße zwischen 1 und 32 liegen.

Parameter: `[<id#>:] <all | "outlet name" | outlet#>`

Argument	Definition
`all`	Alle Geräteausgänge.
`<outlet name>`	Der für einen bestimmten Ausgang konfigurierte Name.
`<outlet#>`	Eine einzelne Nummer oder ein durch einen Bindestrich getrennter Nummernbereich oder eine durch Kommas getrennte Liste einzelner Ausgangsnummern und Nummernbereiche.

Beispiel 1: Um die Ausgänge 3, 5 bis 7 und 10 auszuschalten, geben Sie Folgendes ein:

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

Beispiel 2: Um alle Ausgänge auszuschalten, geben Sie Folgendes ein:

```
apc> olDlyOff all
E000: Success
```

Beispiel 3: Um alle Ausgänge an der Gast-Rack PDU 2 auszuschalten, geben Sie Folgendes ein:

```
apc> olDlyOff 2:all
E000: Success
```

Fehlermeldung: `E000, E102, E104`

olDlyOn

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer und Ausgangsbenutzer, aber nur für Ausgänge, denen der Benutzer zugewiesen ist.

Beschreibung: Schaltet einen Ausgang oder eine Gruppe von Ausgängen nach der Einschaltverzögerung ein. Die id# kann je nach Gruppengröße zwischen 1 und 32 liegen.

Parameter: `[<id#>:] <all | "outlet name" | outlet#>`

Argument	Definition
`all`	Alle Geräteausgänge.
`<outlet name>`	Der für einen bestimmten Ausgang konfigurierte Name.
`<outlet#>`	Eine einzelne Nummer oder ein durch einen Bindestrich getrennter Nummernbereich oder eine durch Kommas getrennte Liste einzelner Ausgangsnummern und Nummernbereiche.

Beispiel 1: Um die Ausgänge 3, 5 bis 7 und 10 einzuschalten, geben Sie Folgendes ein:

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

Beispiel 2: Um einen Ausgang mit dem konfigurierten Namen Outlet1 einzuschalten, geben Sie Folgendes ein:

```
apc> olDlyOn outlet1
E000: Success
```

Fehlermeldung: `E000, E102 E104`

olDlyReboot

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer und Ausgangsbenutzer, aber nur für Ausgänge, denen der Benutzer zugewiesen ist.

Beschreibung: Verzögert die Stromzufuhr zu einem Ausgang oder einer Gruppe von Ausgängen. Die angegebenen Ausgänge werden entsprechend der konfigurierten Abschaltverzögerung ausgeschaltet. Nach der längsten Neustartdauer des ausgewählten Ausgangs beginnen sich die Ausgänge dann basierend auf den konfigurierten Einschaltverzögerungen einzuschalten, die für die angegebenen Ausgänge eingestellt sind. Die id # kann je nach Gruppengröße zwischen 1 und 32 liegen.

Parameter: `[<id#>:] <all | "outlet name" | outlet#>`

Beispiel 1: Um die Ausgänge 3, 5 bis 7 und 10 mit Strom zu versorgen, geben Sie Folgendes ein:

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

Beispiel 2: Um einen Ausgang mit dem konfigurierten Namen Outlet1 mit Strom zu versorgen, geben Sie Folgendes ein:

```
apc> olDlyReboot outlet1
E000: Success
```

Beispiel 3: Um alle Ausgänge auf der Gast-Rack PDU 2 mit Strom zu versorgen, geben Sie Folgendes ein:

```
apc> olDlyReboot 2:all
E000: Success
```

Fehlermeldung: `E000, E102, E104`

olGroups

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer und Ausgangsbenutzer.

Beschreibung: Die CLI lässt die Zuweisung oder Verwaltung von Ausgangssynchronisierungsgruppen nicht zu, außer über eine INI-Datei put/get. Mit diesem Befehl können jedoch Gruppeninformationen abgerufen werden. Ausgangssynchronisierungsgruppen können auch über die Web-Oberfläche zugewiesen und verwaltet werden. Ein Ausgangsbenutzer kann Steuerbefehle an allen Ausgängen ausführen, die in einer Ausgang-Synchronisationsgruppe definiert sind, solange ihm einer der Ausgänge zugewiesen wurde. Die Ausgangssynchronisierung kann je nach Konfiguration lokal auf einer Rack PDU oder über das Netzwerk mit mehreren Rack PDUs erfolgen. Wenn ein Ausgang Teil einer Synchronisierungsgruppe ist, wird sie immer mit den anderen Mitgliedern der Gruppe synchronisiert. Die id # kann je nach Gruppengröße zwischen 1 und 32 liegen.

Listet die Ausgangssynchronisierungsgruppen auf, die auf der schaltbaren Rack PDU definiert sind. Wenn die Synchronisierung von Ausgängen zwischen Geräten aktiviert ist, werden auch die Informationen dieser Geräte aufgelistet.

Parameter: `[<id#>:]`

Beispiel 1: Geben Sie Folgendes ein, um Ausgangssynchronisierungsgruppen auf der Host-Rack PDU aufzulisten:

```
apc> olGroups
Outlet Group Method: Enabled via Network
Outlet Group A:
159.215.6.141 Outlets: 2,4-7,9
159.215.6.143 Outlets: 2,7,8
Outlet Group B:
159.215.6.141 Outlets: 1
159.215.6.166 Outlets: 1
E000: Success
```

Beispiel 2: Geben Sie Folgendes ein, um Ausgangssynchronisierungsgruppen auf der Gast-Rack PDU 2 aufzulisten:

```
apc> olGroups 2:
Outlet Group Method: Local Only
Outlet Grp A:
RPDU Outlets: 3, 10-12, 16
Outlet Grp B:
RPDU Outlets: 13, 14 Outlet Grp C:
RPDU Outlets: 6, 7
Outlet Grp E:
RPDU Outlets: 23, 24

E000: Success
```

Beispiel 3: Geben Sie Folgendes ein, um Ausgangssynchronisierungsgruppen auf der Gast-Rack PDU 3 aufzulisten:

```
apc> olGroups 3:
Outlet Group Method: Enabled via In/Out Ports Outlet Grp A:
RPDU1 Outlets: 3,9,24
RPDU2 Outlets: 3,10,11,16
RPDU4 Outlets: 3,8
Outlet Grp B:
RPDU1 Outlets: 5,8,13
RPDU4 Outlets: 5,6
Outlet Grp C:
RPDU1 Outlets: 10,11,19
E000: Success
```

Fehlermeldung: `E000, E102, E104`

olName

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer, Nur-Lese-Benutzer und Ausgangsbenutzer, aber nur für Ausgänge, denen der Benutzer zugewiesen ist.

Beschreibung: Einstellen oder Anzeigen des einem Ausgang zugewiesenen Namens. Die id # kann je nach Gruppengröße zwischen 1 und 32 liegen.

Parameters: `[<id#>:] <all | outlet#> [<newname>]`

Argument	Definition
`all`	Alle Geräteausgänge
`<outlet#>`	Eine einzelne Nummer oder ein durch einen Bindestrich getrennter Nummernbereich oder eine durch Kommas getrennte Liste einzelner Ausgangsnummern und Nummernbereiche.
`<newname>`	Der Name für einen bestimmten Ausgang. Verwenden Sie nur Buchstaben und Zahlen.

Beispiel 1: Geben Sie Folgendes ein, um den Namen für Ausgang 3 für BobbysServer zu konfigurieren:

```
apc> olName 3 BobbysServer
E000: Success
```

Beispiel 2: Geben Sie Folgendes ein, um die Namen der Ausgänge 3 bis 5 auf der Gast-Rack PDU 2 anzuzeigen:

```
apc> olName 2:3-5
E000: Success
3: BobbysServer
4: Outlet 4
5: Outlet 5
```

Fehlermeldung: `E000, E102, E104`

olOff

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer und Ausgangsbenutzer, aber nur für Ausgänge, denen der Benutzer zugewiesen ist.

Beschreibung: Ausschalten eines Ausgangs oder einer Gruppe von Ausgängen ohne Verzögerung. Die id # kann je nach Gruppengröße zwischen 1 und 32 liegen.

Parameter: `[<id#>:] <all | "outlet name" | outlet#>`

Beispiel 1: Um die Ausgänge 3 und 5 bis 7 auszuschalten, geben Sie Folgendes ein:

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

Beispiel 2: Um die Ausgänge 1 bis 3 an der Gast-Rack PDU 2 auszuschalten, geben Sie Folgendes ein:

```
apc> olOff 2:1-3
E000: Success
```

Fehlermeldung: `E000, E102, E104`

olOffDelay

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer und Ausgangsbenutzer, aber nur für Ausgänge, denen der Benutzer zugewiesen ist.

Beschreibung: Einstellen oder Anzeigen der Zeitverzögerung für den Off Delayed-Befehl und für einen Reboot Delayed-Befehl. Die id # kann je nach Gruppengröße zwischen 1 und 32 liegen.

Parameter: `[<id#>:] <all | "outlet name" | outlet#> [<time>]`

Argument	Definition
`all`	Alle Geräteausgänge
`<outlet name>`	Der für einen bestimmten Ausgang konfigurierte Name.
`<outlet#>`	Eine einzelne Nummer oder ein durch einen Bindestrich getrennter Nummernbereich oder eine durch Kommas getrennte Liste einzelner Ausgangsnummern und Nummernbereiche.
`<time>`	Eine Zeit für die Verzögerung im Bereich von 1 bis 7200 seconds (2 hours).

Beispiel 1: Um eine Verzögerung von 9 Sekunden für das Ausschalten der Ausgänge 3 und 5 bis 7 einzustellen, geben Sie Folgendes ein:

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

Beispiel 2: Geben Sie Folgendes ein, um die Verzögerung für den Off Delayed-Befehl für die Ausgänge 3 und 5 bis 7 anzuzeigen:

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

Beispiel 3: Um eine Verzögerung von 15 Sekunden für das Ausschalten der Ausgänge 2-4 auf der Gast-Rack PDU 2 einzustellen, geben Sie Folgendes ein:

```
apc> olOffDelay 2:2-4 15
E000: Success
```

Fehlermeldung: `E000, E102, E104`

olOn

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer und Ausgangsbenutzer, aber nur für Ausgänge, denen der Benutzer zugewiesen ist.

Beschreibung: Einschalten eines Ausgangs oder einer Gruppe von Ausgängen ohne Verzögerung. Die id # kann je nach Gruppengröße zwischen 1 und 32 liegen.

Parameter: `[<id#>:] <all | "outlet name" | outlet#>`

Argument	Definition
`all`	Alle Geräteausgänge
`<outlet name>`	Der für einen bestimmten Ausgang konfigurierte Name.
`<outlet#>`	Eine einzelne Nummer oder ein durch einen Bindestrich getrennter Nummernbereich oder eine durch Kommas getrennte Liste einzelner Ausgangsnummern und Nummernbereiche.

Beispiel 1: Um die Ausgänge 3 und 5 bis 7 einzuschalten, geben Sie Folgendes ein:

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

Beispiel 2: Um die Ausgänge 3 und 5 bis 7 an der Gast-Rack PDU 3 einzuschalten, geben Sie Folgendes ein:

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

Fehlermeldung: `E000, E102, E104`

olOnDelay

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer und Ausgangsbenutzer, aber nur für Ausgänge, denen der Benutzer zugewiesen ist.

Beschreibung: Einstellen oder Anzeigen der Zeitverzögerung für den On Delayed-Befehl und für einen Reboot Delayed-Befehl. Die id # kann je nach Gruppengröße zwischen 1 und 32 liegen.

Parameter: `[<id#>:] <all | "outlet name" | outlet#> [<time>]`

Argument	Definition
`all`	Alle Geräteausgänge
`<outlet name>`	Der für einen bestimmten Ausgang konfigurierte Name.
`<outlet#>`	Eine einzelne Nummer oder ein Nummernbereich, der durch einen Bindestrich getrennt ist, oder eine durch Kommas getrennte Liste einzelner Ausgangsnummern und Nummernbereiche.
`<time>`	Eine Zeit für die Verzögerung im Bereich von 1 bis 7200 seconds (2 hours).

Beispiel 1: Um eine Verzögerung von 6 Sekunden für das Einschalten der Ausgänge 3 und 5 bis 7 einzustellen, geben Sie Folgendes ein:

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

Beispiel 2: Geben Sie Folgendes ein, um die Verzögerung für den On Delayed-Befehl für die Ausgänge 3 und 5 bis 7 anzuzeigen:

```
apc> olOnDelay 3,5-7
E000: Success
3: BobbyServer: 6 sec
5: BillyServer: 6 sec
6: JoesServer:  6 sec
7: JacksServer: 6 sec
```

Fehlermeldung: `E000, E102, E104`

olRbootTime

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer und Ausgangsbenutzer, aber nur für Ausgänge, denen der Benutzer zugewiesen ist.

Beschreibung: Einstellen oder Anzeigen der Zeitspanne, in der ein Ausgang für einen Befehl mit verzögerter Neustartverzögerung ausgeschaltet bleibt. Die id # kann je nach Gruppengröße zwischen 1 und 32 liegen.

Parameter: `[<id#:>] <all | "outlet name" | outlet#> [<time>]`

Argument	Definition
`all`	Alle Geräteausgänge
`<outlet name>`	Der für einen bestimmten Ausgang konfigurierte Name.
`<outlet#>`	Eine einzelne Nummer oder ein Nummernbereich, der durch einen Bindestrich getrennt ist, oder eine durch Kommas getrennte Liste einzelner Ausgangsnummern und Nummernbereiche.
`<time>`	Eine Zeit für die Verzögerung im Bereich von 1 bis 7200 seconds (2 hours).

Beispiel 1: Geben Sie Folgendes ein, um die für die Ausgänge 3 und 5 bis 7 eingestellte Zeit anzuzeigen:

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

Beispiel 2: Geben Sie Folgendes ein, um die Zeit einzustellen, zu der die Ausgänge 3 und 5 bis 7 während eines Neustarts ausgeschaltet bleiben sollen:

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

Fehlermeldung: `E000, E102, E104`

olStatus

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer, und Nur-Lese-Benutzer Die Ausgangsbenutzer haben ebenfalls Zugriff, aber nur für Ausgänge, denen der Benutzer zugewiesen ist.

Beschreibung: Anzeigen des Status der angegebenen Ausgänge. Die id # kann je nach Größe der Gruppe zwischen 1 und 32 liegen.

Parameter: `[<id#>:] <all | "outlet name" | outlet#>`

Argument	Definition
`all`	Alle Geräteausgänge
`<outlet name>`	Der für einen bestimmten Ausgang konfigurierte Name.
`<outlet#>`	Eine einzelne Nummer oder ein durch einen Bindestrich getrennter Nummernbereich oder eine durch Kommas getrennte Liste einzelner Ausgangsnummern und Nummernbereiche.

Beispiel 1: Geben Sie Folgendes ein, um den Status für die Ausgänge 3 und 5 bis 7 anzuzeigen:

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

Beispiel 2: Geben Sie Folgendes ein, um den Status für die Ausgänge 5 bis 7 auf der Gast-Rack PDU 2 anzuzeigen:

```
apc> olStatus 2:5-7
E000: Success
5: Outlet 5: On
6: Outlet 6: On*
7: Outlet 7: On*
```

HINWEIS: Ein nachgestelltes * bedeutet, dass eine Steuerungsaktion aussteht.

Fehlermeldung: `E000, E102, E104`

olUnsignUsr

Zugriff: Super-Benutzer, Administrator

Beschreibung: Aufheben der Zuweisung von Ausgängen zu einem Benutzer, der in der lokalen Datenbank vorhanden ist. Ausgang-Berechtigungen für RADIUS-definierte Benutzer können nur am RADIUS-Server festgelegt werden. Dieser Befehl steht nur dem Administrator zur Verfügung. Wenn ein Ausgang angegeben ist, die keinem Benutzer zugewiesen ist, wird kein Fehler generiert. Die id # kann je nach Gruppengröße zwischen 1 und 32 liegen.

Parameter: `[<id#>:] <all | "outlet name" | outlet#> <user>`

Argument	Definition
`all`	Alle Geräteausgänge
`<outlet name>`	Der für einen bestimmten Ausgang konfigurierte Name.
`<outlet#>`	Eine einzelne Nummer oder ein durch einen Bindestrich getrennter Nummernbereich oder eine durch Kommas getrennte Liste einzelner Ausgangsnummern und Nummernbereiche.
`<user>`	Ein Benutzer, der in der lokalen Datenbank vorhanden ist.

Beispiel 1: Geben Sie Folgendes ein, um einen Benutzer namens Bobby aus der Steuerung der Ausgänge 3, 5 bis 7 und 10 zu entfernen:

```
apc> olUnasgnUsr 3,5-7,10 Bobby
E000: Success
```

Beispiel 2: Geben Sie Folgendes ein, um einen Benutzer namens Billy aus der Kontrolle über alle Outlets zu entfernen:

```
apc> olUnasgnUsr all Billy
E000: Success
```

Fehlermeldung: `E000, E102`

phBal

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer, Ausgangsbenutzer, und Nur Lese-Benutzer

Beschreibung: Dient zum Einstellen oder Lesen des Schwellenwerts für den Phasenlastausgleich. Gilt nur für Modelle mit zwei oder mehr gemessenen Phasen. Die ID # kann je nach Gruppengröße zwischen 1 und 32 liegen.

Parameter: `[<id#>:] [<current>]` = The new phase threshold (Amps).

Beispiel:

```
apc> phBal 13
E000: Success

apc> phBal
E000: Success
13A
```

Fehlermeldung: `E000, E102`

phBalAlGen

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer, Ausgangsbenutzer, und Nur Lese-Benutzer

Beschreibung: Einstellen oder Lesen, ob Phasenlastausgleichsalarme aktiviert oder deaktiviert sind. Gilt nur für Modelle mit zwei oder mehr gemessenen Phasen. Die id # kann je nach Gruppengröße zwischen 1 und 32 liegen.

Parameter: `[<id#>:] [<enable | disable>]`
`enable` = Phasenlastausgleich-Alarme aktivieren
`disable` = Phasenlastausgleich-Alarme deaktivieren

Beispiel:

```
apc> phBalAlGen enable E000: Success
apc> phBalAlGen disable E000: Success
```

Fehlermeldung: `E000, E102`

phLowLoad

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer

Beschreibung: Hiermit können Sie den Schwellenwert für niedrige Phasenlast in Ampere einstellenoder anzeigen. Um Phrasen anzugeben, wählen Sie aus den folgenden Optionen. Geben Sie an: `all`, eine einzelne Phase, ein Bereich oder eine kommagetrennte Liste von Phasen. Die id # kann je nach Gruppengröße zwischen 1 und 32 liegen.

Parameters: `[<id#>:] <all | phase#> [<current>]`
`phase#` **=** Eine einzelne Zahl oder ein Zahlenbereich, der durch einen Bindestrich oder eine kommagetrennte Liste einzelner Banknummern und/oder Nummernbereiche getrennt ist.
`current` **=** Der neue Phasenschwellwert (Ampere).

Beispiel 1: Um die Niedriglastschwelle für alle Phasen auf 1 A einzustellen, geben Sie Folgendes ein:

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

Beispiel 2: Um die Niedriglastschwelle für die Phasen 1 bis 3 anzuzeigen, geben Sie Folgendes ein:

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

Fehlermeldung: `E000, E102`

phNearOver

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer

Beschreibung: Einstellen oder Anzeigen der Phasennahüberlastungsschwelle in Ampere. Die id # kann je nach Gruppengröße zwischen 1 und 32 liegen.

Parameters: `[<id#>:] <all | phase#> [<current>`
`phase# =` Eine einzelne Zahl oder ein Zahlenbereich, der durch einen Bindestrich oder eine kommagetrennte Liste einzelner Banknummern und/oder Nummernbereiche getrennt ist.
`current` = Der neue Phasenschwellwert (Ampere).

Beispiel 1: Um die überlastnahe Schwelle für alle Phasen auf 10 A einzustellen, geben Sie Folgendes ein:

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

Beispiel 2: Geben Sie Folgendes ein, um den Schwellenwert für die Beinahe-Überlastung für die Phasen 1 bis 3 anzuzeigen:

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

Fehlermeldung: `E000, E102`

phOverLoad

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer

Beschreibung: Einstellen oder Anzeigen der Phasenüberlastungsschwelle. Die ID # kann je nach Gruppengröße zwischen 1 und 32 liegen.

Parameters: `[<id#>:] <all | phase#> [<current>]`
`phase#` = Eine einzelne Zahl oder ein Zahlenbereich, der durch einen Bindestrich oder eine kommagetrennte Liste einzelner Banknummern und/oder Nummernbereiche getrennt ist.
`current` = Der neue Phasenschwellwert (Ampere).

Beispiel 1: Um die Überlastschwelle für alle Phasen auf 13 A einzustellen, geben Sie ein:

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

Beispiel 2: Um die Überlastschwelle für die Phasen 1 bis 3 anzuzeigen, geben Sie ein:

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

Fehlermeldung: `E000, E102`

phPeakCurr

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer

Beschreibung: Anzeige der Spitzenstrommessung von einer Phase oder Phasen. Die id # kann je nach Gruppengröße zwischen 1 und 32 liegen.

Parameter: `[<id#>:] <all | phase#>`
`phase# =` Eine einzelne Zahl oder ein Zahlenbereich, der durch einen Bindestrich oder eine kommagetrennte Liste einzelner Banknummern und/oder Nummernbereiche getrennt ist.

Beispiel:

```
apc> phPeakCurr 2
E000: Success
2: 0.0 A

apc> phPeakCurr all
E000: Success
1: 0.0 A
2: 0.0 A
3: 0.0 A
```

Fehlermeldung: `E000, E102`

phReading

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer, Nur-Lese-Benutzer

Beschreibung: Den Strom, die Spannung oder die Leistung einer Phase anzeigen. Den Grenzwert für beinahe Überlast der Phase in Kilowatt einstellen oder angezeigen. Sie können alle Phasen, eine einzelne Phase, einen Bereich oder eine durch Kommas getrennte Liste von Phasen angeben. Die id # kann je nach Gruppengröße zwischen 1 und 32 liegen.

Parameters: `[<id#>:] < all | phase# > < current | voltage | power | appower | pf >`

Beispiel 1: Um die Messung für Strom für Phase 3 anzuzeigen, geben Sie Folgendes ein:

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

Beispiel 2: Um die Spannung für jede Phase anzuzeigen, geben Sie Folgendes ein:

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

Beispiel 3: Geben Sie Folgendes ein, um die Stromversorgung für Phase 2 auf der Gast-Rack PDU 3 anzuzeigen:

```
apc> phReading 3:2 power
E000: Success
2: 40 W
```

Fehlermeldung: `E000, E102`

phRestrictn

Zugriff: Super-Benutzer, Administrator

Beschreibung: Hiermit stellen Sie die Funktion zur Überlastbeschränkung ein bzw. zeigen sie an, um zu verhindern, dass sich Ausgänge einschalten, wenn der Überlastalarm Ansprechwert überschritten wird. Zulässige Argumente sind none, near und over. Zur Angabe von Phasen stehen Ihnen folgende Optionen zur Auswahl: Geben Sie an: `all`, eine einzelne Phase, ein Bereich oder eine kommagetrennte Liste von Phasen. Die id # kann je nach Gruppengröße zwischen 1 und 32 liegen.

Parameters: `[<id#>:] < all | phase#> [<none | near | over>]`
`phase#` = Eine einzelne Zahl oder ein Zahlenbereich, der durch einen Bindestrich oder eine kommagetrennte Liste einzelner Banknummern und/oder Nummernbereiche getrennt ist.

Beispiel 1: Geben Sie Folgendes ein, um die Überlastungsbeschränkung für Phase drei auf none einzustellen:

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

Beispiel 2: Um die Überlastbeschränkungen für alle Phasen anzuzeigen, geben Sie Folgendes ein:

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

Fehlermeldung: `E000, E102`

phTophVolts

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer, Ausgangsbenutzer, und Nur-Lese-Benutzer

Beschreibung: Ablesen der Phase-zu-Phase-Spannung an mehrphasigen Geräten. Die ID # kann je nach Gruppengröße zwischen 1 und 32 liegen.

Parameter: `[<id#>:]`
`id#` = Die Anzeigekennung der Rack Power Distribution Unit (RPDU) – normalerweise 1. In einer NPS-Umgebung ist der Wert jedoch 1 bis Anzahl der NPS-Fernbedienungen.

Beispiel:

```
apc> phTophVolts 1
E000: Success
1: L1-2 208 V
2: L2-3 208 V
3: L3-1 208 V
```

Fehlermeldung: `E000, E102`

prodInfo

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer, Ausgangsbenutzer, und Nur-Lese-Benutzer

Beschreibung: Anzeigen von Informationen über die Rack PDU. Die id # kann je nach Gruppengröße zwischen 1 und 32 liegen.

Parameter: `[<id#: | all>]`

Beispiel: Um die Produktinformationen für diese Rack PDU anzuzeigen, geben Sie Folgendes ein:

```
apc> prodInfo
E000: Success
RPDU ID:              1
AOS X.X.X
Switched Rack PDU     XXXXXX
Model:                XXXXXX
Name:                 room555Main
Location:             Room 555
Contact:              (xxx) 555-1234
Present Outlets:      XX
Switched Outlets:     XX
Metered Outlets:      XX
Max Current:          XX
Phases:               XX
Banks:                X
Uptime:               0 Days 0 Hours 0 Minutes
NPS Type:             Host
NPS Status:           Active
Network Link:         Link Active
```

Fehlermeldung: `E000`

sensorName

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer

Beschreibung: Einstellen oder Anzeigen des Namens, der dem Rack PDU-Temperatur-/Feuchtigkeits-Port zugewiesen ist.

Parameter: `[<id#>:][<newname>]`

Beispiel 1: Um den Namen für den Port auf "Sensor1" einzustellen, geben Sie Folgendes ein:

```
apc> sensorName Sensor1
E000: Success
```

Beispiel 2: Um dann den Namen für den Sensoranschluss anzuzeigen, geben Sie Folgendes ein:

```
apc> sensorName
E000: Success
Sensor1
```

Beispiel 3: Geben Sie Folgendes ein, um den Namen für den Sensoranschluss an der Gast-Rack PDU 2 auf "Sensor1" einzustellen:

```
apc> sensorName 2:Sensor1
E000: Success
```

Fehlermeldung: `E000, E102`

stateSens

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer

Beschreibung: Lesen oder Schreiben von Werten in Bezug auf das angeschlossene Sensorzubehör zur Statusverfolgung. Die ID# sollte die Display-ID des Zielgeräts sein.

Parameter: `[<id#>:][-<opt>[ <sens_id_num>[ <cfg_input>]]`

Beispiel 1: Geben Sie Folgendes ein, um alle auf dem Sitzungshost verfügbaren zustandsbezogenen Informationen zu lesen:

```
apc>statesens

             D. Normal 2  : Closed
       D. State (desc.) 2  : Door Closed
     D. State (n./abn.) 2  : Normal
           D. Abn. Sev. 2  : Warn
              D. Alarms 2  : Enabled

 E000: Success
```

Beispiel 2: Geben Sie Folgendes ein, um den diskreten abnormalen Schweregrad des einen angeschlossenen Sensors des Sitzungshosts zu lesen:

```
apc>statesens -sv
     D. Abn. Sev. 2 : Warn
E000: Success
```

Beispiel 3: Geben Sie Folgendes ein, um den diskreten abnormalen Schweregrad des Sensors von Port 2 des Sitzungshosts zu lesen:

```
apc>statesens -sv 2
     Warn
E000: Success
```

Beispiel 4: Geben Sie Folgendes ein, um den diskreten abnormalen Schweregrad des Sensors von Port 2 des Sitzungshosts zu ändern:

```
apc>statesens -sv 2 Crit
     Old D. Abn. Sev. 2 : Warn
     New D. Abn. Sev. 2 : Crit
 E000: Success
```

Beispiel 5: So wenden Sie den Befehl "`stateSens`" auf Gastgerät 5 statt auf den Sitzungshost, geben Sie Folgendes ein:

```
apc>statesens 5:

            D. Normal 1  : Open
      D. State (desc.) 1  : Open
   D. State (n./abn.) 1  : Normal
         D. Abn. Sev. 1  : Crit
            D. Alarms 1  : Enabled

            D. Normal 2  : Closed
      D. State (desc.) 2  : Spot Dry
   D. State (n./abn.) 2  : Abnormal
         D. Abn. Sev. 2  : Crit
            D. Alarms 2  : Enabled

E000: Success
```

Fehlermeldung: `E000, E100, E102, E106`

Temperatursensor Hinweis:

Sie müssen einen optionalen Temperatursensor von APC by Schneider (AP9335T) an Ihrer Rack PDU installiert haben, um die temperaturbezogenen Befehle verwenden zu können.

tempAlGen

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer

Beschreibung: Einstellen oder Ablesen, ob Temperaturalarme aktiviert oder deaktiviert sind. Die id # kann je nach Gruppengröße zwischen 1 und 32 liegen.

Parameter: `[<id#>:][<enable> | disable>]`
`enable` = Temperaturalarme aktivieren.
`disable` = Temperaturalarmedeaktivieren.

Beispiel:

```
apc> tempAlGen enable
E000: Success

apc> tempAlGen disable
E000: Success
```

Fehlermeldung: `E000, E102`

tempHigh

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer

Beschreibung: Einstellen oder Anzeigen der Hochtemperaturschwelle in Fahrenheit oder Celsius. Die id # kann je nach Gruppengröße zwischen 1 und 32 liegen.

Parameter: `[<id#>:] < F | C > [<temperature>]` = Neue Hochtemperaturschwelle

Beispiel 1: Um den Hochtemperaturschwellenwert auf 70º Fahrenheit einzustellen, geben Sie Folgendes ein:

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

Beispiel 2: Geben Sie Folgendes ein, um den Hochtemperaturschwellenwert in Celsius anzuzeigen:

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

Beispiel 3: Geben Sie Folgendes ein, um den Hochtemperaturschwellenwert der Gast Rack PDU 2 in Fahrenheit anzuzeigen:

```
apc> tempHigh 2:F
E000: Success
70 F
```

Fehlermeldung: `E000, E102`

tempHyst

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer

Beschreibung: Einstellen und Anzeigen der Temperaturschwellenhysterese. Die id # kann je nach Gruppengröße zwischen 1 und 32 liegen.

Parameter: `[<id#>:] < F | C > [<temperature>]`= neuer Temperaturhysteresewert.

Beispiel:

```
apc> tempHyst F 6
E000: Success

apc> tempHyst C
E000: Success
3 C
```

Fehlermeldung: `E000, E102`

tempMax

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer

Beschreibung: Einstellen oder Anzeigen der maximalen Temperaturschwelle in Fahrenheit oder Celsius. Die id # kann je nach Gruppengröße zwischen 1 und 32 liegen.

Parameter: `[<id#>:] < F | C > [<temperature>]` = neue maximale Temperaturschwelle.

Beispiel 1: Um die maximale Temperaturschwelle auf 80º Fahrenheit einzustellen, geben Sie Folgendes ein:

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

Beispiel 2: Um den Schwellenwert für die maximale Temperatur in Celsius anzuzeigen, geben Sie Folgendes ein:

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

Beispiel 3: Um den Schwellenwert für die maximale Temperatur der Gast-Rack PDU 3 in Fahrenheit anzuzeigen, geben Sie Folgendes ein:

```
apc> tempMax 3:F
E000: Success
95 F
```

Fehlermeldung: `E000, E102`

tempReading

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer, Ausgangsbenutzer, und Nur-Lese-Benutzer

Beschreibung: Anzeigen des Temperaturwerts in Fahrenheit oder Celsius vom Sensor. Die id # kann je nach Gruppengröße zwischen 1 und 32 liegen.

Parameter: `[<id#>:] < F | C >` = Temperatur

Beispiel 1: Um den Temperaturwert in Fahrenheit anzuzeigen, geben Sie Folgendes ein:

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

Beispiel 2: Um den Temperaturwert der Gast-Rack PDU 3 in Celsius anzuzeigen, geben Sie Folgendes ein:

```
apc> tempReading 3:C
E000: Success
23.5 C
```

Fehlermeldung: `E000, E102, E201`

tempSens

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer

Beschreibung: Ablesen oder Schreiben von Werten in Bezug auf das angeschlossene Zubehör für Temperaturmesssensoren. Die ID# sollte die Display-ID des Zielgeräts sein.

Parameter: `[<id#>:][-<opt>[ <sens_id_num>[ <cfg_input>]]]`

Beispiel 1: Geben Sie Folgendes ein, um alle auf dem Sitzungshost verfügbaren temperaturbezogenen Informationen zu lesen:

```
apc>tempsens

      Temperature 1  : 35.0 C
       T. Maximum 1  : 60 C
          T. High 1  : 59 C
    T. Hysteresis 1  : 1 C
     T. Peak Temp 1  : 35.5 C
    T. Peak Since 1  : 07/16/2024 15:25:21
     T. Peak Time 1  : 07/22/2024 11:50:32
        T. Alarms 1  : Enabled
         T. State 1  : Normal
      Temperature 2  : 33.4 C
       T. Maximum 2  : 60 C
          T. High 2  : 55 C
```

```
      T. Hysteresis 2  : 1 C
       T. Peak Temp 2  : 34.2 C
      T. Peak Since 2  : 07/16/2024 15:25:16
       T. Peak Time 2  : 07/22/2024 11:40:36
          T. Alarms 2  : Enabled
           T. State 2  : Normal

E000: Success
```

Beispiel 2: Geben Sie Folgendes ein, um den oberen Temperaturschwellenwert der beiden angeschlossenen Sensoren des Sitzungshosts zu lesen:

```
apc>tempsens -h

          T. High 1  : 59 C
          T. High 2  : 55 C

E000: Success
```

Beispiel 3: Geben Sie Folgendes ein, um den oberen Temperaturschwellenwert des Sensors von Port 1 des Sitzungshosts zu lesen:

```
apc>tempsens -h 1
     59 C
E000: Success
```

Beispiel 4: Geben Sie Folgendes ein, um den Schwellenwert für hohe Temperatur des Sensors an Port 1 des Sitzungshosts zu ändern:

```
apc>tempsens -h 1 33
     Old T. High 1 : 59 C
     New T. High 1 : 33 C
E000: Success
```

Beispiel 5: So wenden Sie den Befehl "`tempsens -h`" auf Gastgerät 3 statt auf den Sitzungshost, geben Sie Folgendes ein:

```
apc>tempsens 3:-h
     T. High 1 : 59 C
     T. High 2 : 59 C
E000: Success
```

Fehlermeldung: `E000, E100, E102, E106`

tempStatus

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer, Nur-Lese-Benutzer

Beschreibung: Anzeige des Status des Sensors. Die id # kann je nach Gruppengröße zwischen 1 und 32 liegen.

Parameter: `[<id#>:]`

Beispiel: Um den Status des Temperatursensors anzuzeigen, geben Sie Folgendes ein:

```
apc> tempStatus
Normal
```

Fehlermeldung: Keine

userAdd

Zugriff: Super-Benutzer, Administrator

Beschreibung: Hinzufügen eines Ausgangsbenutzers zur lokalen Benutzerdatenbank.

Das Passwort für den neuen Benutzer entspricht dem Benutzernamen. Verwenden Sie den `userPasswd`-Befehl, um das Kennwort des Benutzers zu ändern.

Parameter: `<user>`
`user =` Ein Benutzer, der in der lokalen Datenbank NICHT vorhanden ist.

Beispiel: Um einen Benutzer namens Bobby hinzuzufügen, geben Sie Folgendes ein:

```
apc> userAdd Bobby
E000: Success
```

Fehlermeldung: `E000, E102, E202`

userDelete

Zugriff: Super-Benutzer, Administrator

Beschreibung: Entfernen eines Ausgangsbenutzers aus der lokalen Benutzerdatenbank.

Parameter: `<user>`
`user =` Ein Benutzer, der in der lokalen Datenbank vorhanden ist.

Beispiel: Um einen Benutzer namens Bobby zu entfernen, geben Sie Folgendes ein:

```
apc> userDelete Bobby
E000: Success
```

Fehlermeldung: `E000, E102, E203`

userList

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer, Nur-Lese-Benutzer und Ausgangsbenutzer, aber nur für Ausgänge, denen der Benutzer zugewiesen ist.

Beschreibung: Auflistung der Benutzer und der ihnen zugewiesenen Ausgängen.

Bei Verwendung durch den Administrator werden die Benutzer in der lokalen Datenbank und die ihnen zugewiesenen Ausgangsnummern aufgelistet. Bei Verwendung durch einen Ausgangsbenutzer werden nur dieser Benutzer und seine Ausgänge aufgelistet. Wenn der aktive Benutzer über RADIUS authentifiziert wurde, werden die Benutzer- und Ausgang Berechtigungen basierend auf dem angemeldeten Benutzertyp angezeigt.

Wenn mehrere Rack PDUs über die Ein-/Ausgänge angeschlossen sind, werden die Ausgänge wie folgt aufgelistet:

```
<id> [<outlet list>];<id>[<outlet list>];<id>[<outlet list>];
<id>[<outlet list>]
```

`<id>` ist die Display-ID der Rack PDU, und die Liste der eigenen Ausgänge ist in den folgenden eckigen Klammern enthalten. Ein Semikolon wird verwendet, um ein Rack PDU Gerät vom nächsten zu trennen.

Parameter: Keine

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

```
apc> userList
E000: Success

Name            User Type           Status       Outlets
----            ---------           ------       -------

apc             Super               ******       1-24

device          Device              Enabled      1-24

network         NetworkOnly         Enabled      1-24

dobby           Outlet              Enabled      1-24
```

Beispiel 2: Wenn Ausgangsbenutzer 'dobby' angemeldet ist:

```
apc> userList
E000: Success

Name            User Type              Status        Outlets
----            ---------              ------        -------

dobby           Outlet                 Enabled       1-12
```

Beispiel 3: Wenn ein Radius-Ausgang-Benutzer 'RadOutlet' angemeldet ist:

```
apc> userList
E000: Success

Name            User Type              Status        Outlets
----            ---------              ------        -------

RadOutlet       Outlet (Radius)        ******        1[1,3,5]
```

Beispiel 4: Wenn ein Radius-Gerätebenutzer 'RadDevice' angemeldet ist:

```
apc> userList
E000: Success

Name            User Type              Status        Outlets
----            ---------              ------        -------

raddev          Device (Radius)        ******        1-24

readonly        ReadOnly               Enabled       1-24

network         NetworkOnly            Enabled       1-24

dobby           Outlet                 Enabled       1-12
```

Beispiel 5: Wenn ein Administrator angemeldet ist und mehrere Rack PDUs an den Ein-/Ausgängen vorhanden sind:

```
apc> userList

E000: Success

Name            User Type              Status        Outlets
----            ---------              ------        -------

apc             Super                  ******        1[1-24];
                                                     2[1-24];
                                                     3[1-24];
                                                     4[1-24]

administrator   Admin                  Enabled       1[1-24];
                                                     2[1-24];
                                                     3[1-24];
                                                     4[1-24]

device          Device                 Enabled       1[1-24];
                                                     2[1-24];
                                                     3[1-24];
                                                     4[1-24]

readonly        ReadOnly               Enabled       1[1-24];
                                                     2[1-24];
                                                     3[1-24];
                                                     4[1-24]

network         NetworkOnly            Enabled       1[1-24];
                                                     2[1-24];
                                                     3[1-24];
                                                     4[1-24]

dobby           Outlet                 Enabled       1[1];
                                                     3[3];
                                                     4[4]
```

Fehlermeldung: E000

userPassword

Zugriff: Super-Benutzer, Administrator.

Beschreibung: Stellen Sie ein Ausgangsbenutzerkennwort ein. Der Administrator Benutzer kann Kennwörter für alle Benutzer ändern.

Parameter: `<user> <password1> <password2>` = Benutzername, dessen Passwort geändert wird. Passwort 2 ist eine Bestätigung und muss mit Passwort 1 identisch sein.

Beispiel: Geben Sie Folgendes ein, um das Passwort für dobby auf "riddle" einzustellen:

```
apc> userPasswd dobby riddle riddle
E000: Success
```

Fehlermeldungen: `E000, E102, E104`

voltSens

Zugriff: Super-Benutzer, Administrator, Gerätebenutzer

Beschreibung: Ablesen oder Schreiben von Werten in Bezug auf das angeschlossene Zubehör für Spannungsmesssensoren. Die ID# sollte die Display-ID des Zielgeräts sein.

Parameter: `[<id#>:][-<opt>[ <sens_id_num>[ <cfg_input>]]`

Beispiel 1: Geben Sie Folgendes ein, um alle auf dem Sitzungshost verfügbaren spannungsbezogenen Informationen zu lesen:

```
apc>voltsens

          Voltage 2  : 0.00 V
    V. Max Thresh 2  : 4.50 V
    V. Min Thresh 2  : 0.50 V
    V. Hysteresis 2  : 0.50 V
        V. Alarms 2  : Enabled
         V. State 2  : Below Min

 E000: Success
```

Beispiel 2: Geben Sie Folgendes ein, um die Spannungshysterese des an den Session Host angeschlossenen Sensors abzulesen:

```
apc>voltsens -hy
     V. Hysteresis 2 : 0.50 V
E000: Success
```

Beispiel 3: Geben Sie Folgendes ein, um die Spannungshysterese des Sensors von Port 2 des Sitzungshosts abzulesen:

```
apc>voltsens -hy 2
     0.50 V
E000: Success
```

Beispiel 4: Geben Sie Folgendes ein, um den Wert der Spannungshysterese des Sensors von Port 2 des Sitzungshosts zu ändern:

```
apc>voltsens -hy 2 0.81
     Old V. Hysteresis 2 : 0.50 V
     New V. Hysteresis 2 : 0.81 V
E000: Success
```

Beispiel 5: So wenden Sie den Befehl "`Volt -v 1`" auf Gastgerät 2 statt auf den Sitzungshost, geben Sie Folgendes ein:

```
apc>voltsens 2:-v 1
     1.38 V
E000: Success
```

Fehlermeldung: `E000, E100, E102, E106`

Web User Interface

Unterstützte Webbrowser

Sie können die neueste Version von Microsoft Edge®, Google Chrome®, Apple Safari® oder Mozilla Firefox® verwenden, um über die Web-Benutzeroberfläche auf die Rack PDU zuzugreifen. Andere allgemein verfügbare Browser und Versionen funktionieren möglicherweise, wurden jedoch nicht vollständig getestet.

Die Rack-PDU kann nicht mit einem Proxy-Server verwendet werden. Bevor Sie mit einem Webbrowser auf die Web-Benutzeroberfläche der Rack PDU zugreifen können, müssen Sie einen der folgenden Schritte ausführen:

- Konfigurieren Sie den Webbrowser, um die Verwendung eines Proxyservers für die Rack PDU zu deaktivieren.
- Konfigurieren Sie den Proxyserver so, dass er die spezifische IP-Adresse der Rack PDU nicht weiterleitet.

In der Web User Interface anmelden

Überblick

Sie können den DNS-Namen oder die System-IP-Adresse der Rack PDU für die URL Adresse der Web-Benutzeroberfläche verwenden. Melden Sie sich mit Ihrem Benutzernamen und Kennwort unter Beachtung der Groß-/Kleinschreibung an.

Standardmäßig lauten sowohl der Benutzername als auch das Passwort für den **Super Benutzer (Super User) apc**. Für alle anderen Benutzertypen gibt es keinen Standardbenutzernamen oder kein Standardkennwort. Der **Super-Benutzer (Super User)** oder ein vom **Super-Benutzer** erstellter **Administrator** muss den Benutzernamen und das Passwort sowie andere Kontomerkmale für diese Benutzer definieren.

> **HINWEIS:** Wenn Sie HTTPS (SSL/TLS) als Zugriffsprotokoll verwenden, werden Ihre Anmeldeinformationen mit Informationen in einem Serverzertifikat abgeglichen. Wenn das Zertifikat mit dem Sicherheitsassistenten erstellt wurde und eine IP-Adresse als allgemeiner Name im Zertifikat angegeben wurde, müssen Sie eine IP-Adresse verwenden, um sich an der Rack PDU anzumelden. Wenn ein DNS-Name als allgemeiner Name auf dem Zertifikat angegeben wurde, müssen Sie einen DNS-Namen für die Anmeldung verwenden.

Möglicherweise erhalten Sie eine Meldung, dass die Webseite nicht sicher ist. Dies ist normal; Sie können trotzdem fortfahren und die Web-Oberfläche öffnen. Die „Zertifikatsfehlermeldung (Certificate Error Message)“-Meldung wird generiert, da Ihr Webbrowser das Standardzertifikat für die Verschlüsselung über HTTPS nicht erkennt. Die über HTTPS übertragenen Daten werden dennoch verschlüsselt. Über HTTPS übertragene Informationen sind jedoch weiterhin verschlüsselt. Weitere Informationen zu HTTPS und Anweisungen zur Behebung der „Zertifikatsfehlermeldung (Certificate Error Message)“ finden Sie im *Security Handbook (Sicherheitshandbuch)* auf www.se.com.

URL-Adressformate

Geben Sie den DNS-Namen oder die IP-Adresse der Rack PDU in das URL-Adressfeld des Webbrowsers ein und drücken Sie die ENTER TASTE. Bis HTTP aktiviert ist, müssen Sie https:// in die URL aufnehmen. Wenn Sie in Internet Explorer einen nicht standardmäßigen Webserverport angeben, müssen Sie http:// oder https:// in die URL aufnehmen.

Häufige Browser-Fehlermeldungen bei der Anmeldung:

Fehlermeldung	Browser	Fehlerursache
„Diese Seite kann nicht angezeigt werden.“ (“This page cannot be displayed.”)	Internet Explorer	Der Webzugriff ist deaktiviert oder die URL war nicht korrekt.
„Verbindung nicht möglich.“ (“Unable to connect.”)	Firefox	

Beispiele für URL-Formate:

HINWEIS: HTTP ist standardmäßig deaktiviert und HTTPS ist standardmäßig aktiviert.

- Für einen DNS-Namen von Web1:
  `http://Web1` wenn HTTP Ihr Zugriffsmodus ist
  `https://Web1` wenn HTTPS (HTTP mit SSL/TLS) Ihr Zugriffsmodus ist
- Für eine System-IP-Adresse von 139.225.6.133 und den Standard-Webserver-Port (80): `http://139.225.6.133` wenn HTTP Ihr Zugriffsmodus ist
  `https://139.225.6.133:5000` wenn HTTPS (HTTP mit SSL/TLS) Ihr Zugriffsmodus ist
- Für die System-IPv6-Adresse 2001:db8:1::2c0:b7ff:fe00:1100 und ein Nicht-Standard Port für Webserver
  `http://[2001:db8:1::2c0:b7ff:fe00:1100]:5000` wenn HTTP Ihr Zugriffsmodus ist

Erste Anmeldung

Wenn Sie sich zum ersten Mal bei der Netzwerkmanagement-Karte anmelden, werden Sie aufgefordert, das Standardkennwort für das Super-Benutzer-Konto (**apc**) zu ändern. Nachdem Sie sich angemeldet haben, werden Sie zum Bildschirm mit der **Konfigurationszusammenfassung (Configuration Summary)** weitergeleitet. Dieser Bildschirm ist eine Übersicht über alle Systemprotokolle und ihre aktuellen Werte (z.B. aktiviert/deaktiviert).
Sie können diesen Bildschirm später jederzeit aufrufen, indem Sie dem Pfad folgen: **Configuration > Network > Summary.**

Eingeschränkter Statuszugriff

Die Seite Eingeschränkter RPDU-Status **(Configuration > Network >Summary)** enthält eingeschränkte Informationen, ohne dass Sie sich anmelden müssen. Greifen Sie mit einem Webbrowser auf die IP-Adresse der RPDU zu, um die Anmeldeseite anzuzeigen. Wenn diese Option aktiviert ist, wird in der unteren rechten Ecke des Rahmens ein Hyperlink „Eingeschränkter Status“ ("Limited Status") angezeigt. Wenn Sie auf „Eingeschränkter Status“ ("Limited Status") klicken, wird anstelle der regulären Felder für Benutzername/Passwort eine begrenzte Zusammenfassung der Geräte- und Systeminformationen zur Anzeige bereitgestellt. Ein „Anmelden“ ("Log On") Hyperlink, wie er unmittelbar oben zu sehen ist, ermöglicht den einfachen Zugriff auf die Standard Anmeldeseite.

Funktionen der Web-Benutzeroberfläche

Lesen Sie die folgenden Informationen, um sich mit den grundlegenden Web-UI-Funktionen für Ihre Rack PDU vertraut zu machen.

Registerkarten

Die folgende Registerkarten sind verfügbar:

- **Home:** Erscheint, wenn Sie sich anmelden. (Dies ist die Standardregisterkarte, wenn Sie sich anmelden. Um die Anmeldeseite in eine andere Seite zu ändern, klicken Sie auf den grünen Pin  oben rechts im Browserfenster, während Sie sich auf der gewünschten Seite befinden.)
- **Status:** Gibt dem Benutzer den Status der Rack PDU und des **Network** an.Die RPDU Diese Registerkarte enthält Informationen zum Status von Alarmen, Gruppen, Geräten, Phasen, Banken und Umgebung. **Network**-Registerkarte deckt nur das Netzwerk ab.
- **Control:** Die Control-Registerkarte umfasst drei Themen: **RPDU**, **Security** und **Network**. Weitere Informationen finden Sie unter den einzelnen Registerkarten. Eine Beschreibung finden Sie im **Control**-Registerkartenabschnitt.
- **Configuration:** Die **Configuration**-Registerkarte umfasst **RPDU**, **Security**, **Network**, **Notification** und **General Configuration**.
- **Tests:** Die **Tests**-Registerkarte umfasst **RPDU** und **Network**. Die **RPDU**-Registerkarte enthaltet das LCD-Blinken und die **Network**-Registerkarte das LED-Blinken. Beide werden später im **Tests** -Abschnitt des Dokuments.
- **Logs:** Der **Logs**-Abschnitt behandelt: **Event**, **Data** und **Firewall**. Die Registerkarten **Event** und **Data** enthalten weitere Informationen, die später im **Logs**-Abschnitt des Dokuments näher erläutert werden.
- **About:** Der **About**-Abschnitt behandelt **RPDU**, **Network** und **Support**, auf die später im **About**-Abschnitt des Dokuments näher eingegangen wird.

Gerätestatussymbole

Ein oder mehrere Symbole und begleitender Text zeigen den aktuellen Betriebsstatus der Rack PDU an:

Symbol	Beschreibung
	**Kritisch:** 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 Alarme vor, und die Rack PDU und die Netzwerkmanagement-Karte funktionieren normal.

In der oberen rechten Ecke jeder Seite zeigt die Web-Benutzeroberfläche dieselben Symbole an, die derzeit auf der **Home** angezeigt werden, um den Rack PDU-Status zu melden:

- Das **No Alarms**-Symbol, wenn keine Alarme vorhanden sind.
- Eines oder beide der anderen Symbole **(Kritisch** und **Warnung (Critical** und **Warning))** falls Alarme vorhanden sind, und nach jedem Symbol die Anzahl der aktiven Alarme dieses Schweregrads.

Schnellverknüpfungen

Unten links auf jeder Seite der Benutzeroberfläche befinden sich drei konfigurierbare Links. Standardmäßig greifen die Links auf die URLs dieser Webseiten zu:

- **Link 1:** Die Homepage der Website von APC by Schneider Electric
- **Link 2:** Demonstrationen von webfähigen Produkten von APC by Schneider Electric
- **Link 3:** Informationen zu EcoStruxure IT

Befindet sich in der oberen rechten Ecke jeder Seite:

- Username (klicken, um Benutzereinstellungen zu ändern)
- Language (falls verfügbar, klicken Sie hier, um die Spracheinstellung zu ändern)
- Log Off (Klicken Sie, um den aktuellen Benutzer von der Weboberfläche abzumelden)
- Help (klicken, um Hilfeinhalte anzuzeigen)
- Klicken Sie auf das pushpin-Symbol, um die aktuelle Webseite als Anmeldehomepage festzulegen.

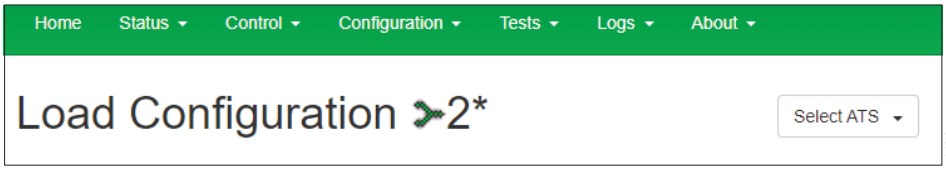
  Beispiel:

  Log In Home: Um einen beliebigen Bildschirm zum „Heim“ zu machen (d.h. der Bildschirm, der bei der Anmeldung zuerst angezeigt wird), gehen Sie zu diesem Bildschirm und klicken Sie auf das Pin-symbol in der oberen rechten Ecke. Klicken Sie auf dieses Symbol, um bei der Anmeldung zur Anzeige des Startbildschirms zurückzukehren.

Network Port Sharing (NPS) auf der Web-UI

Die Web-Benutzeroberfläche des Rack-ATS verfügt über zusätzliche Funktionen, wenn der Rack-ATS Teil einer NPS-Gruppe ist. Dazu gehören eine NPS-Gruppenstatusseite (**Status > ATS > Group Status**) und eine NPS-Gruppenkonfigurationsseite **Configuration > ATS > Group**. Bei Webseiten, die NPS-Funktionen unterstützen, können Sie außerdem einen anderen Rack-ATS in der Gruppe anzeigen, indem Sie die Display-ID der betreffenden Einheit auswählen.

Jeder Rack-ATS in der NPS-Gruppe wird mit einem Rack-ITS-Symbol gefolgt von seiner Display-ID (1 bis 32) gekennzeichnet. Der Rack-ATS, bei dem Sie angemeldet sind, wird mit einem zusätzlichen Sternchen (*) nach der Display-ID angezeigt.



Gruppensteuerung über Network Port Sharing

Die Web-Benutzeroberfläche der Rack PDU verfügt über zusätzliche Funktionen, wenn die Rack PDU Teil einer NPS-Gruppe ist. Dazu gehören eine NPS-Gruppenstatus-Webseite und eine NPS-Gruppenkonfigurationsseite. Darüber hinaus kann der Benutzer für Webseiten, die NPS-Rack PDUs unterstützen, eine andere Rack PDU in der anzuzeigenden Gruppe auswählen, indem er das Display-ID der Rack PDU der Einheit auswählt, die er anzeigen möchte.

Jede Rack PDU in der NPS-Gruppe ist mit einem Rack PDU-Symbol gefolgt von ihrer Display-ID (1 bis 32) gekennzeichnet. Die Rack PDU, bei der der Benutzer angemeldet ist, wird mit einem zusätzlichen Sternchen (*) nach der Display-ID angezeigt.

HINWEIS: Die Webseite zum **Reset/Reboot** enthält viele zusätzliche Optionen zum Zurücksetzen/Neustart für Rack PDU-Gruppen. Dazu gehören das Zurücksetzen einzelner Rack PDUs auf die Standardwerte, das Neustarten einzelner Rack PDUs und das Löschen von Alarmen bei Kommunikationsausfall der Gast-PDUs durch Entfernen der Gäste aus der Gruppe.

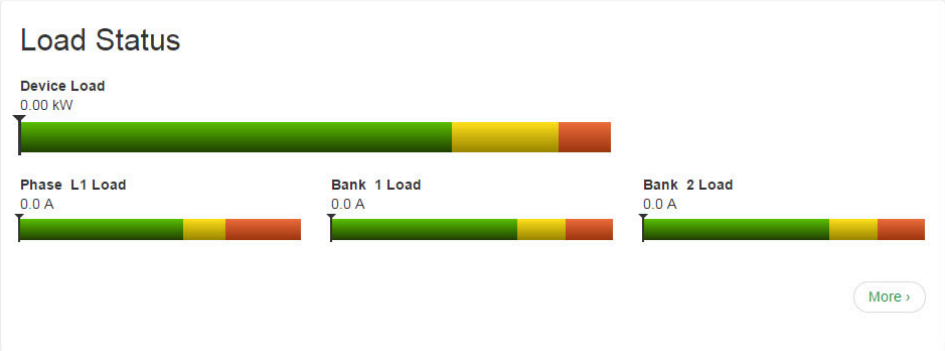
Home

Die **Home** enthält die folgenden Informationen: Aktive Alarme, Laststatus und letzte Geräteereignisse. Aktive Alarme werden angezeigt, wenn Alarme vorliegen. Wenn keine Alarme vorhanden sind, wird ein grünes Häkchen mit den Wörtern **No Alarms Present** angezeigt. Der Laststatus zeigt einen farbigen Balken, der die Höhe der Bank-, Phasen und Gerätelasten anzeigt. Um den Gerätestatus anzuzeigen, wählen Sie den **More**-Link am Ende der Liste. Das Letzte Geräteereignisse-Feld listet die fünf letzten Geräteereignisse des Geräts nach Datum, Uhrzeit und Ereignis auf.

Überblick

Im Bereich **Load Status** können Sie die Last für das Gerät in kW und gegebenenfalls für die Phasen und Bänke in Ampere anzeigen. Das grüne, gelbe und rote Messgerät zeigt den aktuellen Laststatus an: normal, nahe Überlast oder Überlast.

HINWEIS: Wenn eine niedrige Lastschwelle konfiguriert wurde, enthält das Messgerät auch ein blaues Segment links neben dem grünen.



Im **Rack PDU Parameters** findet der Leser den Namen, den Standort, den Kontakt, die Modellnummer, die Bewertung, den Benutzer (Typ des Benutzerkontos, das auf die Rack PDU zugreift) und die Betriebszeit (die Zeit, die Rack PDU seit dem letzten Neustart nach einem Aus- oder Neustart der Verwaltungsschnittstelle in Betrieb war).

Im **Recent Device Events** finden Sie die Ereignisse, die zuletzt aufgetreten sind, sowie die Daten und Zeiten, zu denen sie aufgetreten sind. Es werden maximal fünf Ereignisse gleichzeitig angezeigt. Klicken Sie auf **More Events**, um zur **Logs**-Registerkarte zu gelangen und das gesamte Ereignisprotokoll anzuzeigen.

Status Tab

Über die Status Tab

Verwenden Sie die **Status**-Registerkarte, um:

- den Status des Rack PDU-Geräts oder des Netzwerks anzuzeigen
- Auf der RPDU-Registerkarte können Benutzer auf Folgendes zugreifen: Alarme, Gerät, Phase, Bank, Ausgänge und Umgebung
- Ausgänge verwalten
- Wählen Sie Network, um die aktuellen IPv4- und IPv6-Einstellungen anzuzeigen.

Anzeige des Laststatus und der Spitzenlast

Path: Status > RPDU

Alarms: Listet den Alarmstatus des Geräts auf.

Group: NPS-Status. Listet die Eigenschaften, Mess- und Firmware-Versionsinformationen auf. **Change Host RPDU** kann über den Link unten auf der Seite zugegriffen werden.

Device: Zeigt den Status des Geräts an. Listet Status-, Eigenschaften- und Konfigurationsinformationen auf.

Phase: Zeigt den Phasenstatus an. Delta-Werte für den Phasenlastausgleich werden für Modelle mit zwei oder mehr gemessenen Phasen angezeigt. Die Phaseneinstellungen können auch über den **Configure Phase Settings** unten auf der Seite konfiguriert werden. Die Konfiguration kann ebenfalls geändert werden.

Bank: Zeigt den Bankstatus an (nur bei Geräten mit dieser Funktion). Listet die aktuelle Größe auf und demonstriert die Reichweite auf einer farbigen roten, grünen und gelben Schieberegler. Die Bankeinstellungen können über den **Configure Bank Status** unten auf der Seite geändert werden.

Outlet: Zeigt: Ausgangsname, Phase, Status und Ausgangslast.

Switched Outlet: Wählen Sie aus den folgenden Optionen:

- **Scheduling:** Zeigt geplante Ausgang-Aktionen an. Auf dieser Seite können Sie auch Ausgang-Aktionen planen.
- **Outlet Alarm Actions:** Zeigt Alarmaktionen für Ausgänge an. Auf dieser Seite können Sie auch Alarmaktionen konfigurieren.
- **Outlet Groups:** Zeigt Ausgänge entweder als aktiviert oder deaktiviert an. Auf dieser Seite können Sie auch Gruppen konfigurieren.

Environment: Zeigt Alarmstatus, Temperatur, und Luftfeuchtigkeit an und kann die Temperatur- und Luftfeuchtigkeitskonfiguration einstellen, nachdem Sie auf den Konfigurieren-Link geklickt haben.

Anzeigen des Network status

Path: Status > Network

Der **Network** zeigt Informationen zu Ihrem Netzwerk an.

Aktuelle IPv4-Einstellungen

System IP: Die IP-Adresse des Geräts.

Subnet Mask: Die IP-Adresse des Subnetzwerks.

Default Gateway: Die IP-Adresse des Routers, der für die Verbindung mit dem Netzwerk verwendet wird.

MAC Address: Die MAC-Adresse des Geräts.

Mode: Zuweisung der IPv4-Einstellungen: **Manual**, **DHCP** oder **BOOTP**.

DHCP Server: Die IP-Adresse des DHCP-Servers. Dies wird nur angezeigt, wenn **Mode** **DHCP** ist.

Lease Acquired: Datum/Uhrzeit, zu der die IP-Adresse vom DHCP-Server angenommen wurde.

Lease Expires: Datum und Uhrzeit, zu der die vom DHCP-Server akzeptierte IP-Adresse abläuft und erneuert werden muss.

Aktuelle IPv6-Einstellungen

Type: Zuweisung der IPv6-Einstellungen.

IP Address: Die IP-Adresse des Geräts.

Prefix Length: Der Adressbereich für das Subnetz.

Systemstatus des Domänennamens

Active Primary DNS Server: Die IP-Adresse des primären DNS-Servers.

Active Secondary DNS Server: Die IP-Adresse des sekundären DNS-Servers.

Active Host Name: Der Hostname des aktiven DNS-Servers.

Active Domain Name (IPv4/IPv6): Der IPv4/IPv6-Domänenname, der derzeit verwendet wird.

Active Domain Name (IPv6): Der IPv6-Domänenname, der derzeit verwendet wird.

Geschwindigkeit des Ethernet-Ports

Current Speed: Die dem Ethernet-Port zugewiesene aktuelle Geschwindigkeit.

Control

Die **Control**-Menüoptionen ermöglichen es Ihnen, sofortige Maßnahmen zu ergreifen, die die aktive Benutzerverwaltung und die Sicherheit Ihres Netzwerks beeinflussen.

Steuerung der Geräteausgänge

Path: Control > RPDU > Outlet

Zeigt die Ausgangssteuerung, die Steuerungsaktion und die ausgewählten Ausgänge an. Im Select Outlet-Dialogfeld wird der Name des Ausgangs, ihr Status und ihre Phase angezeigt.

HINWEIS: Wenn Sie einen Ausgängesteueraktion auf Ausgänge oder Ausgängegruppen anwenden, werden für die Aktion die folgenden Verzögerungen verwendet:

- Für einen einzelnen Ausgang (nicht zu einer Ausgängegruppe) verwendet der Vorgang die für diesen Ausgang konfigurierten Verzögerungszeiten und die Dauer für den Neustart.
- Bei einer globalen Ausgängegruppe verwendet der Vorgang die für den globalen Ausgang konfigurierten Verzögerungszeiten und die Dauer für den Neustart.
- Bei einer lokalen Ausgängegruppe verwendet der Vorgang die Verzögerungszeiten, die für den Ausgang mit der niedrigsten Nummer in der Gruppe konfiguriert sind.

Steuerung der Ausgänge an der Rack PDU

Markieren Sie die Kontrollkästchen für jeden einzelnen Ausgang oder Ausgängegruppe, die Sie steuern möchten, oder wählen Sie die **All Outlets** ein.

Wählen Sie eine **Control Action** aus der Liste, und klicken Sie auf **Next >>**. Wählen Sie auf der Bestätigungsseite, auf der die Aktion erläutert wird, die Option Übernehmen oder Abbrechen aus.

Steueraktionen, die Sie auswählen können

Option	Kopfzeile
No Action	Nichts tun
On Immediate	Die Stromversorgung zu den ausgewählten Ausgängen einschalten
On Delayed	Die Stromversorgung für jeden ausgewählten Ausgang entsprechend ihrem Wert einschalten **Power On Delay**†
Off Immediate	Die ausgewählten Ausgänge von der Stromversorgung ausschalten
Off Delayed	Die Stromversorgung von jedem ausgewählten Ausgang entsprechend ihrem Wert für die **Power Off Delay**†
Reboot Immediate	Die Stromversorgung von jedem ausgewählten Ausgang ausschalten Dann die Stromversorgung zu jeden diesen Ausgänge entsprechend seinem Wert für die **Reboot Duration**†
Reboot Delayed	Die Stromversorgung von jedem ausgewählten Ausgängen entsprechend ihrem Wert für die **Power Off Delay**. Warten Sie, bis alle Ausgänge ausgeschaltet sind (der höchste Wert für die **Reboot Duration**), und schalten Sie dann jeden Ausgang entsprechend ihrem Wert für die **Power On Delay**† ein.
Cancel Pending Commands	Ale Befehle abbrechen, die für die ausgewählten Ausgänge ausstehen, und behalten sie im aktuellen Zustand beibehalten. **HINWEIS:** Bei globalen Ausgängegruppen können Sie einen Befehl nur über die Schnittstelle der Ausgängegruppe des Initiators abbrechen. Die Aktion bricht den Befehl für die Ausgängegruppe des Initiators und alle Folgeausgängegruppen ab.
† Wenn eine lokale Ausgängegruppe ausgewählt ist, werden nur die konfigurierten Verzögerungen und die Neustartdauer des Ausgängegruppen-Moduls mit der niedrigsten Nummer verwendet. Wenn eine globale Ausgängegruppe ausgewählt ist, werden nur die konfigurierten Verzögerungen und die Neustartdauer des globalen Ausgangs verwendet.	

Verwalten von Benutzersitzungen

Path: Control > Security > Session Management

Das **Session Management** zeigt alle aktiven Benutzer an, die derzeit mit der RPDU verbunden sind. Um Informationen über einen bestimmten Benutzer anzuzeigen, klicken Sie auf dessen Benutzernamen. Der **Session Details** zeigt grundlegende Informationen über den Benutzer an, einschließlich der Schnittstelle, an der er angemeldet ist, seiner IP Adresse und der Benutzerauthentifizierung. Es gibt auch eine Option, **Terminate Session** zu beenden.

Zurücksetzen der Netzwerkschnittstelle

Path: Control > Network > Reset/Reboot

In diesem Menü haben Sie die Möglichkeit, verschiedene Komponenten der Netzwerkschnittstelle zurückzusetzen und neu zu starten.

Benutzer haben die folgende Möglichkeiten:

- **Reboot Management Interface** — Startet die Netzwerkverwaltungsschnittstelle der Rack PDU neu. Er hat keinen Einfluss auf den EIN/AUS-Status des Ausgangs.
- **Reset all** — Deaktivieren Sie das **Exclude TCP/IP**, um alle Konfigurationswerte zurückzusetzen; markieren Sie das **Exclude TCP/IP**, um alle Werte außer TCP/IP und EAPoL zurückzusetzen.

  HINWEIS: Wenn Sie **Reset all** auswählen, werden alle Netzwerkschnittstellen auf ihre Standardeinstellungen zurückgesetzt. Nachdem Sie sich mit dem Standard-Login und -Passwort (**apc)** angemeldet haben, müssen Sie Ihr Login und Passwort ändern.
- **Reset Only** — (Das Zurücksetzen kann bis zu einer Minute dauern) Optionen umfassen:

  TCP/IP settings: Setzen Sie die TCP/IP-Konfiguration auf **DHCP & BOOTP**, die Standardeinstellung. Diese Anforderung erfordert, dass die Rack PDU ihre TCP/IP Einstellungen von einem DHCP- oder BOOTP-Server empfängt. Siehe „Ergebnis des DNS-Tests im Feld für die letzte Abfrageantwort anzeigen“ auf der Webseite. EAPoL wird auf deaktiviert zurückgesetzt.

  Event configuration: Alle Änderungen an der Ereigniskonfiguration nach Ereignis und Gruppe auf ihre Standardeinstellungen zurücksetzen.

  Host Display ID and remove all guest PDUs: Ermöglicht der RPDU die erneute Erkennung der vorhandenen Gruppe, löscht alle Alarme, die durch die nicht mehr reagierenden Geräte ausgelöst wurden, und setzt die Display-ID der RPDU zurück.

  RPDU to Defaults: Zurücksetzen der RPDU-Einstellungen auf ihre Standardkonfiguration für die ausgewählte RPDU. Alle RPDU-spezifischen Konfigurationen werden auf ihre Standardeinstellungen zurückgesetzt.

Configuration

Über die Configuration-Registerkarte

Unter der Configuration-Registerkarte stehen mehrere Menüoptionen zur Verfügung, um Änderungen an den Rack PDUs vorzunehmen:

- Den Ladezustand für die Rack PDU anzeigen.
- Ausgänge verwalten und steuern
- Einen Namen und einen Speicherort für die Rack PDU konfigurieren
- Die Spitzenlastmessung anzeigen und verwalten
- Klicken auf vom Benutzer konfigurierbare Links, um Webseiten für bestimmte an die Rack PDU angeschlossene Geräte zu öffnen

Konfigurieren von Lastschwellenwerten

Path: Configuration > RPDU

Zeigt die Last für das Gerät, die Phasen, Bänke und Steckdosen an. Die Anzeige im grünen, gelben und roten Messgerät zeigt den aktuellen Laststatus an: normal, nahe Überlast oder Überlast. Wenn ein niedriger Lastschwellenwert konfiguriert wurde, zeigt das Messgerät ein blaues Segment links neben dem grünen an. Bei der Anzeige der **Device Load** das Dreieck über dem Messgerät die Spitzenlast an.

HINWEIS: Die Rack PDU erzeugt einen Alarm, wenn eine Bank ihren Nennwert überschreitet. Wenn jedoch ein Leistungsschalter auslöst, gibt es keinen endgültigen Hinweis darauf, dass der Leistungsschalter geöffnet ist, außer dass der Strom für diese Bank abfällt.
Setzen Sie die Warnung bei geringer Last aus folgenden Gründen auf 1 amp:

- Die Standardeinstellung für die Low Load Warning ist 0 amps. Dadurch wird die Warnung deaktiviert. Bei einer Einstellung von 0 amps für die Low Load Warning zeigt die Web-Benutzeroberfläche nicht an, dass möglicherweise ein Leistungsschalter ausgelöst hat.
- Eine Erkennungsschwelle von 1 Ampere für die Low Load Warning für das Bank Load Management zeigt an, dass möglicherweise ein Leistungsschalter ausgelöst hat.

So konfigurieren Sie Lastschwellenwerte

1. Um Lastschwellenwerte für das Gerät, die Phasen oder die Bänke zu konfigurieren, treffen Sie eine Auswahl aus dem Dropdown-Menü **Configuration > RPDU > Device** und **Phase** und **Bank**. Um die Lastschwellenwerte für Ausgänge zu konfigurieren, klicken Sie auf **Configuration** und klicken Sie dann auf einen Ausgang.
2. Stellen Sie den Überlastalarm, die nahe Überlastwarnung und die Warnschwellen für die Niedriglastwarnung ein.
3. Klicken Sie auf **Apply**, um Ihre Einstellungen zu speichern.

Konfigurieren des Namens und des Standorts der Rack PDU

Path: Configuration > RPDU > Device

Der Name und der Ort, den Sie eingeben, werden auf der **Home**-Registerkarte angezeigt.

1. Geben Sie einen Namen, einen Standort und einen Kontakt ein.
2. Klicken Sie zum Speichern auf **Apply**.

Einstellen der Kaltstartverzögerung für die Rack PDU

Path: Configuration > RPDU > Device

Die Kaltstartverzögerung ist die Anzahl der seconds, die der Einschaltverzögerung jedes Ausgangs hinzugefügt wird, bevor sich ein Ausgang einschaltet, nachdem die Rack PDU mit Strom versorgt wurde. Zulässige Werte sind 1 bis 300 seconds, **Sofort** oder **nie** (nie einschalten).

1. Wählen Sie **Coldstart Delay**.
2. Klicken Sie **Apply**.

Spitzenlast und kWh zurücksetzen

Path: Configuration > RPDU > Device

1. Klicken Sie auf die **Configuration**-Registerkarte, dann auf **RPDU** und dann auf **Device**.
2. Klicken Sie wie gewünscht auf die **Peak Load** und **Kilowatt-Hours**.
3. Klicken Sie **Apply**.

Überlastauslassbeschränkungen einstellen

Parameter

Path: Configuration > RPDU > Phase and **Bank**

Verhindern Sie, dass Benutzer während einer Überlastung Ausgänge mit Strom versorgen. Sie können die folgenden Einschränkungen für jede Phase und Bank einstellen:

- **None**: Benutzer können Ausgänge unabhängig von einem Überlastalarm oder einer nahe Überlastwarnung mit Strom versorgen.
- **On Warning:** Benutzer können einen Ausgang der ausgewählten Phase oder Bank nicht mit Strom versorgen, wenn der Strom für diese Phase oder Bank die Warnschwelle für nahe Überlastungwarnung überschritten hat.
- **On Overload:** Benutzer können einen Ausgang der ausgewählten Phase oder Bank nicht mit Strom versorgen, wenn der Strom für diese Phase oder Bank die Überlastalarmschwelle überschritten hat.

So stellen Sie Überlastungsbeschränkungen für Ausgänge ein

1. Klicken Sie auf die **Configuration**-Registerkarte, dann auf **RPDU** und dann im Menü auf **Phase** oder **Bank**.
2. Wählen Sie **Overload Outlet Restriction**.
3. Klicken Sie **Apply**.

Konfigurieren des Phasenlastausgleichs

Path: Configuration > RPDU > Phase

Der Phasenlastausgleichsalarm ist nur für Geräte mit zwei oder mehr gemessenen Phasen verfügbar.

Geben Sie einen Warnschwellenwert (in Ampere) zwischen 0 und dem maximalen Phasenstrom an und wählen Sie dann **Enable** unter **Alarm Generation**. Sobald diese Funktion aktiviert ist, generiert die RPDU einen Warnalarm, wenn die Phasen um mehr als die angegebene Anzahl von Ampere abweichen.

Konfigurieren und Steuern von Ausgängegruppen

Ausgängegruppe - Terminologie

Eine *Ausgängegruppe* besteht aus Ausgängen, die logisch auf derselben Rack PDU miteinander verbunden sind. Ausgänge in einer Ausgängegruppe werden synchronisiert ein- und ausgeschaltet und neu gestartet:

- Eine *lokale Ausgängegruppe* besteht aus zwei oder mehr Ausgängen auf einer Rack PDU. Nur die Ausgänge in dieser Gruppe sind synchronisiert.
- Eine *globale Ausgängegruppe* besteht aus einer oder mehreren Ausgängen auf einer Rack PDU. Ein Ausgang ist als globaler Ausgang konfiguriert, der die Ausgängegruppe logisch mit Ausgängegruppen auf bis zu drei anderen Rack PDUs verknüpft. Alle Ausgänge in den verknüpften globalen Ausgängegruppen werden synchronisiert.
  - Bei globalen Ausgängegruppen ist die Ausgängegruppe des Initiators die Gruppe, die die Aktion ausgegeben hat.
  - Bei globalen Ausgängegruppen ist eine Follower-Gruppe jede andere Ausgängegruppe, die mit Ausgängegruppe des Initiators synchronisiert ist.

Wenn Sie eine Ausgang-Steuerungsaktion auf Ausgänge anwenden, die Mitglieder einer Ausgängegruppe sind, werden die Ausgänge wie folgt synchronisiert:

- Verwenden Sie für eine globale Ausgängegruppe die Verzögerungszeiträume und die Neustartdauer, die für den globalen Ausgang der Ausgängegruppe des Initiators konfiguriert sind.
- Bei einer lokalen Ausgängegruppe verwenden die Ausgänge die Verzögerungszeiten und die Neustartdauer des Ausgangs mit der niedrigsten Nummer in der Gruppe.

Zweck und Vorteile von Ausgängegruppen

Durch die Verwendung von Gruppen synchronisierter Ausgänge auf Rack PDUs können Sie sicherstellen, dass Ausgänge synchron ein-, ausgeschaltet und neu gestartet werden. Das Synchronisieren von Kontrollgruppenaktionen über Ausgängegruppen bietet die folgenden Vorteile:

- Synchronisiertes Herunterfahren und Hochfahren der Stromversorgungen von Dual-Corded-Servern verhindert fehlerhafte Meldungen von Stromversorgungsausfällen während eines geplanten Herunterfahrens oder Neustarts des Systems.
- Die Synchronisierung von Ausgängen mithilfe von Ausgängegruppen bietet präzisere Abschalt- und Neustartzeiten als die Verwendung der Verzögerungszeiten einzelner Ausgänge.
- Ein globaler Ausgang ist für die Benutzeroberfläche jeder Rack PDU sichtbar, mit der er verbunden ist.

Systemanforderungen für Ausgängegruppen

Einstellen und Verwenden synchronisierter Ausgängesteuerungsgruppen:

- Sie benötigen einen Computer, der synchronisierte Steuerungsvorgänge über die Web-Benutzeroberfläche oder CLI der Rack PDUs oder über SNMP initiieren kann.
- Alle Rack PDUs müssen Firmware verwenden, die sowohl für das APC Operating System (AOS)-Modul von APC by Schneider Electric als auch für das Applikationsmodul dieselbe Versionsnummer aufweist.
- Alle Rack PDUs müssen mit demselben „Mitgliedsname“ ("Member Name") konfiguriert sein.
- Wenn Sie den Netzwerkmodus verwenden, benötigen Sie außerdem die folgenden Elemente. Diese sind nicht erforderlich, wenn Sie den NPD-Modus über die Ein-/Ausgänge verwenden.
  - Sie benötigen ein 10/100/1000 Base-T TCP/IP-Netzwerk mit einem Ethernet-Hub oder -Switch, dessen Stromquelle nicht von den Computern oder anderen zu synchronisierenden Geräten gemeinsam genutzt wird.
  - Alle Rack PDUs müssen sich im selben Subnetz befinden.
  - Ausgängegruppen, die Sie synchronisieren, müssen dieselbe Multicast-IP-Adresse, denselben Ausgängegruppenport, dieselbe Authentifizierungsphrase und dieselbe Verschlüsselungsphrase aufweisen. Stellen Sie sicher, dass jeder Ethernet-Switch, der die Rack-PDUs verbindet, Multicast-Netzwerkverkehr für diese Multicast-IP-Adresse zulässt.

Regeln für die Konfiguration von Ausgängegruppen

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

- Eine Rack PDU kann mehr als eine Ausgängegruppe haben, aber ein Ausgang kann nur zu einer Ausgängegruppe gehören.
- Eine lokale Ausgängegruppe, die keine globale Ausgänge hat, muss aus zwei oder mehr Verkaufsstellen bestehen.
- Sie können eine globale Ausgängegruppe auf einer Rack PDU mit einer globalen Ausgängegruppe auf jedem der drei anderen Rack PDUs synchronisieren.
  - In einer globalen Ausgängegruppe können Sie festlegen, dass nur ein Ausgang den globale Ausgang ist, die zum Zweck der Synchronisierung mit Ausgängegruppen an anderen Rack PDUs verbunden wird. Dieser globale Ausgang kann der einzige Ausgang in ihrer Gruppe sein oder die Gruppe kann aus mehreren Ausgängen bestehen.
  - Ein globaler Ausgang einer Ausgängegruppe muss dieselbe physische Ausgangsnummer haben wie der globale Ausgang einer anderen Ausgängegruppe, mit der er verknüpft ist.
- Um Ausgängegruppen zu erstellen und zu konfigurieren, müssen Sie die Web Benutzeroberfläche verwenden oder Einstellungen aus der Konfigurationsdatei (.ini-Datei) einer konfigurierten Rack PDU exportieren. Mit der Befehlszeilenschnittstelle können Sie anzeigen, ob ein Ausgang Mitglied einer Ausgängegruppe ist, und Steuerungsaktionen auf eine Ausgängegruppe anwenden, aber mit der Befehlszeilenschnittstelle können Sie keine Ausgängegruppe einrichten oder konfigurieren.

Ausgängegruppen aktivieren

Path: Configuration > RPDU > Switched Outlet > Outlet Groups

Konfigurieren Sie die folgenden Parameter und klicken Sie auf **Apply**.

Erstellung von Ausgängegruppen aktivieren:

Parameter	Beschreibung
Device Level Outlet Group	Um eine Ausgängegruppe zu erstellen, müssen Sie die gewünschte Gruppenmethode aktivieren. Folgende Optionen stehen zur Auswahl: Disabled, Local Only, Enabled über Netzwerk und Aktiviert über Ein-/Ausgänge (Netzwerk-Portfreigabe (Network Port Sharing)).

Aktivieren Sie die Unterstützung für globale Ausgängegruppen (verknüpfte Gruppen):

Parameter	Beschreibung
Member Name	Um Ausgängegruppen an mehreren Switched Rack PDUs miteinander zu verbinden, müssen Sie auf jeder Rack PDUs denselben Mitgliednamen definieren. **HINWEIS:** Es können maximal vier Geräte mit demselben Elementnamen konfiguriert werden.

Einstellen von Parametern für Ausgängegruppen im Netzwerkmodus:

Parameter	Beschreibung
Multicast IP	Um Ausgängegruppen an mehreren Switched Rack PDUs zu verbinden, müssen Sie dieselbe Multicast-IP-Adresse an jeder der Rack PDUs definieren.
Authentication Phrase	Ein aus 15 bis 32 ASCII-Zeichen bestehender Kennwortsatz, der verifiziert, dass das Gerät mit anderen Geräten kommuniziert, dass die Nachricht während der Übertragung nicht geändert wurde und dass die Nachricht rechtzeitig kommuniziert wurde. Die Authentifizierungsphrase zeigt an, dass sie nicht verzögert wurde und dass sie nicht kopiert und später zu einem unangemessenen Zeitpunkt erneut gesendet wurde.
Encryption Phrase	Eine Phrase von 15 bis 32 ASCII-Zeichen, der die Vertraulichkeit der Daten gewährleistet (durch Verschlüsselung).
Outlet Group Port	Die Portnummer, über die das Gerät mit anderen Geräten kommuniziert. Dies muss bei allen Rack PDUs in einer Gruppe gleich sein.

HINWEIS: Geräte, die versuchen, sich im Netzwerkmodus mit Ausgängegruppen auf anderen Geräten zu synchronisieren, müssen alle dieselbe Authentifizierungs- und Verschlüsselungsphrase haben. Die Werte werden für den Benutzer ausgeblendet.

Eine lokale Ausgängegruppe erstellen

Path: Configuration > RPDU > Switched Outlet > Outlet Groups

1. Stellen Sie sicher, dass Ausgängegruppen aktiviert sind.
2. Klicken Sie **Create Local Outlet Group**.
3. Aktivieren Sie die Kontrollkästchen der Ausgänge, die in der Gruppe enthalten sein sollen, und weisen Sie der Gruppe im Feld **Outlet Group Name** einen Namen zu. Sie müssen mindestens zwei Ausgänge auswählen.

Eine globale Ausgängegruppe erstellen

Path: Configuration > RPDU > Switched Outlet > Outlet Groups

So richten Sie mehrere globale Ausgängegruppen ein, die mit Ausgängegruppen auf anderen NMC verknüpft sind:

1. Stellen Sie sicher, dass Ausgängegruppen aktiviert sind.
2. Klicken Sie **Create Global Outlet Groups**.
3. Aktivieren Sie die Kontrollkästchen der Ausgänge, die in der Gruppe enthalten sein sollen, und klicken Sie dann auf **“Apply and Select Global Outlets”**, um die globale Ausgänge für die Gruppe auszuwählen. Wenn es nur ein Ausgang in der Gruppe gibt, wird dieser automatisch als globaler Ausang zugewiesen.
4. Informationen zum Hinzufügen von Ausgänge zu einer der von Ihnen erstellten globalen Ausgängegruppen finden Sie unter “Edit or delete an outlet group”.

Bearbeiten oder Löschen einer Ausgängegruppe

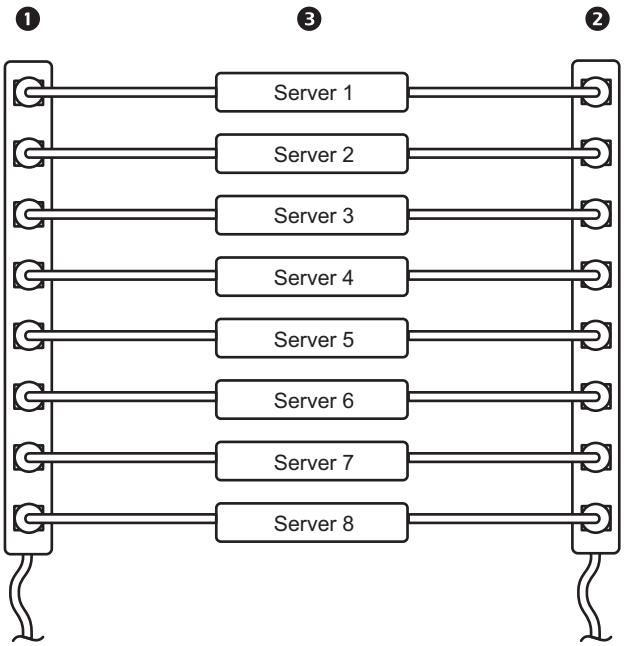
Path: Configuration > RPDU > Switched Outlet > Outlet Groups

1. Klicken Sie in der Tabelle **Configure Group** auf die Nummer oder den Namen der Ausgängegruppe, die Sie bearbeiten oder löschen möchten.
2. Beim Bearbeiten einer Ausgängegruppe können Sie eine der folgenden Aktionen ausführen:
   - Die Ausgängegruppe umbenennen.
   - Fügen Sie Ausgänge hinzu oder entfernen Sie sie, indem Sie auf die Kontrollkästchen klicken, um sie zu markieren oder zu entfernen.

     HINWEIS: Sie können einen Ausgang nicht aus einer Ausgängegruppe entfernen, die nur zwei Ausgänge enthält, es sei denn, der verbleibende Ausgang ist ein globaler Ausgang.
3. Um die Ausgängegruppe zu löschen, klicken Sie auf **Delete Outlet Group**.

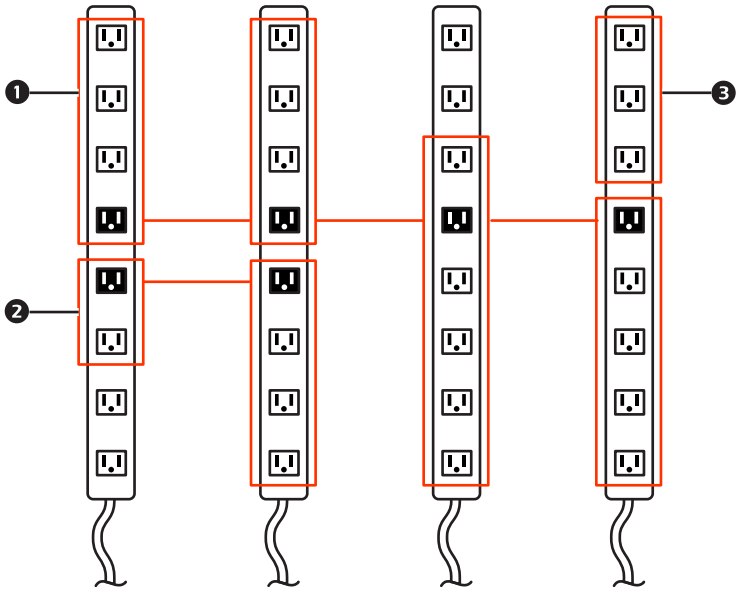
TypischeKonfigurationen von Ausgängegruppen

Die folgende Konfiguration zeigt zwei Rack PDUs mit jeweils acht Ausgängegruppen. Jede Ausgängegruppe besteht aus einem einzigen globalen Ausgang. Jede Ausgängegruppe 1 auf der ersten Rack PDU ist mit der Ausgängegruppe 2 an derselben Stelle auf der zweiten Rack PDU verbunden. Ein Netzkabel eines Servers mit zwei Kabeln 3 ist mit jedem Ausgang an der ersten Rack PDU verbunden, und sein anderes Kabel ist mit dem entsprechenden Ausgang an der zweiten Rack PDU verbunden, wodurch sichergestellt wird, dass die Ausgangsleistung von beiden Stromquellen an den Server als Reaktion auf eine Ausgangssteuerungsaktion synchron ein- oder ausgeschaltet wird.



Die folgende Konfiguration zeigt drei Sätze synchronisierter Ausgänge. Globale Ausgänge werden schwarz angezeigt. Ausgängegruppen werden in rote Rechtecke eingeschlossen.

1	Diese vier globalen Ausgängegruppen synchronisieren insgesamt 19 Ausgänge.
2	Diese beiden globalen Ausgängegruppen synchronisieren 6 Ausgänge, 2 in einer Gruppe und 4 in der anderen.
3	Diese lokale Ausgängegruppe synchronisiert 3 Ausgänge an derselben Rack PDU.



Überprüfen Sie Ihre Einrichtung und Konfiguration für globale Ausgängegruppen

Path: Configuration > RPDU > Switched Outlet > Outlet Groups

Zeigen Sie die Gruppen und ihre Verbindungen an, um sicherzustellen, dass Ihre Einrichtung alle Systemanforderungen für Ausgängegruppen erfüllt und dass Sie die Ausgängegruppen korrekt konfiguriert haben:

- Die **Configure Group**-Tabelle zeigt Folgendes an:
  - Alle konfigurierten Ausgängegruppen auf der aktuellen Rack PDU.
  - Die Ausgänge in jeder Gruppe nach Ausgangsnummer.
  - Alle Ausgängegruppen auf anderen Rack PDUs, mit denen ein globaler Ausgang synchronisiert ist. Jede Rack-PDU wird durch ihre IP-Adresse identifiziert, wenn sie den Netzwerkmodus verwendet, oder durch die Display-ID, wenn sie die Netzwerk-Port-Freigabe über Ein-/Ausgänge verwendet. Jeder globale Ausgang wird in Fettschrift dargestellt.
- Der **Global Outlet Overview**-Übersicht zeigt Folgendes an:
  - Die IP-Adresse oder Display-ID der aktuellen Rack PDU.
  - Die IP-Adresse oder Display-ID aller Rack PDUs, die globale Ausgänge enthalten, die für die Synchronisierung mit Ausgängegruppen auf anderen Rack PDUs verfügbar sind.
  - Alle globalen Ausgänge, die auf den Rack PDUs konfiguriert sind, unabhängig davon, ob sie mit Ausgängegruppen auf der aktuellen Rack PDU synchronisiert sind.

Ausgangseinstellungen

Wählen Sie aus den Optionen aus, um die Ausgänge an Ihrer Rack PDU zu steuern.

Path: Configuration > RPDU > Switched Outlet (or Outlet Groups)

Konfigurieren der Ausgangseinstellungen und des Ausgangnamens

Die nachfolgende Einstellungen sind verfügbar:

Einstellung	Beschreibung
Name	Stellen Sie den Namen für einen oder mehrere Ausgänge ein. Der Name wird in den Statusanzeigen neben der Ausgangsnummer angezeigt.
External Link	Hiermit stellen Sie einen HTTP- oder HTTPS-Link zu einer Website oder IP Adresse ein. Der Weblink des externen Geräts kann auf die IP-Adresse des externen Geräts eingestellt werden, das an den Ausgang angeschlossen ist (falls zutreffend). Alternativ kann es auf die Herstellerwebseite des Geräts eingestellt werden, um die Benutzerhandbücher usw. leichter anzeigen zu können. Durch Klicken auf den Link auf der Seite Ausgangsverbindungen wird ein neues Browserfenster für den Link geöffnet.
Power On Delay	Stellen Sie die Anzahl der Sekunden ein, die die Rack-PDU nach der Ausgabe eines Befehls wartet, bevor sie einen Ausgang mit Strom versorgt. **HINWEIS:** Um einen Ausgang so zu konfigurieren, dass sie jederzeit ausgeschaltet bleibt, wählen Sie die **Never**-Option neben Einschaltverzögerung.
Power Off Delay	Stellen Sie die Anzahl der Sekunden ein, die die Rack-PDU nach Ausgabe eines Befehls wartet, bevor Sie einen Ausgang mit Strom versorgt. **HINWEIS:** Um einen Ausgang so zu konfigurieren, dass sie jederzeit eingeschaltet bleibt, wählen Sie die **Never**-Option neben Ausschaltverzögerung.
Reboot Duration	Stellen Sie die Anzahl der Sekunden ein, für die ein Ausgang ausgeschaltet bleibt, bevor sie neu gestartet wird.

Path: Configuration > RPDU > Switched Outlet > Configuration

Klicken Sie im **Configure Multiple Outlets** auf die Mehrere **Outlet Configuration** Schaltfläche oder klicken Sie auf den Namen des Ausgangs.

- Konfigurieren von Ausgangseinstellungen für mehrere Ausgänge:
  - Aktivieren Sie die Kontrollkästchen neben den Nummern der Ausgänge, die Sie ändern möchten, oder aktivieren Sie das Kontrollkästchen **All Outlets**.
  - Geben Sie Werte für **Name** und **Link** ein und klicken Sie auf die **Apply** Schaltfläche direkt unter der Liste.
  - Geben Sie Werte für die **Einschaltverzögerung (Power On Delay), Ausschaltverzögerung (Power Off Delay)** oder **Neustartdauer (Reboot Duration)** ein und klicken Sie auf die **Apply**-Schaltfläche direkt unter der Liste.
- Konfigurieren der Ausgangseinstellungen für einen einzelnen Ausgang:
  - Geben Sie Werte für **Name** und **Link** ein und klicken Sie auf die **Apply**-Schaltfläche direkt unter der Liste.
  - Geben Sie Werte für die **Einschaltverzögerung (Power On Delay), Ausschaltverzögerung (Power Off Delay)** oder **Neustartdauer (Reboot Duration)** ein und klicken Sie auf die **Apply**-Schaltfläche direkt unter der Liste.

Ausgangsaktionen planen

Aktionen, die Sie planen können

So konfigurieren Sie Werte für die **Einschaltverzögerung (Power On Delay), Ausschaltverzögerung (Power Off Delay)** oder **Neustartdauer (Reboot Duration)** für jeden Ausgang. Obwohl Sie die Webbenutzeroberfläche zum Planen von Ausgangsaktionen verwenden müssen, können Sie diese Werte entweder in der Web- oder Befehlszeilenschnittstelle festlegen. Für alle von Ihnen ausgewählten Ausgänge können Sie eine der in der folgenden Tabelle aufgeführten Aktionen so planen, dass sie täglich, in Abständen von einer, zwei, vier oder acht Wochen oder nur einmal ausgeführt werden.

Option	Beschreibung
No Action	Nichts tun
On Immediate	Ausgewählte Ausgänge mit Strom versorgen
On Delayed	Schalten Sie die Stromversorgung für jeden ausgewählten Ausgang entsprechend dem Wert für **Power On Delay** ein.†
Off Immediate	Die ausgewählten Ausgänge ausschalten.
Off Delayed	Die Stromversorgung von jedem ausgewählten Ausgängen entsprechend ihrem Wert für die **Power Off Delay** ausschalten.†
Reboot Immediate	Die Stromversorgung von jedem ausgewählten Ausgang ausschalten. Schalten Sie dann jeden dieser Ausgänge entsprechend seinem Wert für die **Reboot Duration** mit Strom.†
Reboot Delayed	Die Stromversorgung von jedem ausgewählten Ausgängen entsprechend ihrem Wert für die **Power Off Delay**. Warten Sie, bis alle Ausgänge ausgeschaltet sind (der höchste Wert für die **Reboot Duration**), und schalten Sie dann jeden Ausgang entsprechend seinem Wert für die **Power On Delay**†
†Bei Auswahl einer lokalen Steckdosengruppe werden nur die konfigurierten Verzögerungen und die Neustartdauer des Ausgängegruppe-Moduls mit der niedrigsten Nummer verwendet. Wenn eine globale Ausgängegruppe ausgewählt ist, werden nur die konfigurierten Verzögerungen und die Neustartdauer des globalen Aisgangs verwendet.	

Planen eines Ausgangsereignis

Path: Configuration > RPDU > Switched Outlet > Scheduling

1. Wählen Sie auf der **Outlet Scheduling** aus, wie oft das Ereignis stattfinden soll (**One-Time**, **Daily** oder **Weekly**), und klicken Sie auf die **Next**-Schaltfläche.

   HINWEIS: Wenn Sie **Weekly** auswählen, können Sie festlegen, dass das Ereignis einmal pro Woche oder einmal alle zwei, vier oder acht Wochen stattfindet.
2. Ersetzen Sie auf der Seite **Schedule a Daily Action** im **Name of event**-Textfeld den Standardnamen, `Outlet Event`, durch einen Namen, der Ihr neues Ereignis identifiziert.
3. Verwenden Sie die Dropdown-Listen, um den Ereignistyp und den Zeitpunkt des Ereignisses auszuwählen. Das Datumsformat für einmalige Ereignisse ist *mm/dd* und das Zeitformat für alle Ereignisse ist *hh/mm*, wobei die zweistellige Stunde in der 24-hour-Zeit angegeben ist.
   - — Ein Ereignis, das täglich oder in einem der in der **Weekly** Auswahl verfügbaren Intervalle geplant ist, tritt weiterhin im geplanten Intervall auf, bis das Ereignis gelöscht oder deaktiviert wird.
   - — Sie können ein einmaliges Ereignis so planen, dass es nur an einem Datum innerhalb von 12 Monaten nach dem Datum auftritt, an dem Sie die Planung durchführen. Beispielsweise können Sie am 26.März 2020 ein einmaliges Ereignis an einem beliebigen Datum vom aktuellen Datum bis zum 26.März 2021 planen.
4. Verwenden Sie die Kontrollkästchen, um auszuwählen, welche Ausgänge von der Aktion betroffen sind. Sie können einen oder mehrere einzelne Ausgänge auswählen oder **All Outlets**.
5. Klicken Sie auf **Apply**, um die Planung des Ereignisses zu bestätigen, oder auf **Cancel**, um es zu löschen.

Wenn Sie das Ereignis bestätigen, wird die Zusammenfassungsseite erneut angezeigt, wobei das neue Ereignis in der Liste der geplanten Ereignisse angezeigt wird.

Bearbeiten, deaktivieren, Aktivieren oder Löschen eines geplanten Ausgangsereignisses

Path: Configuration > RPDU > Switched Outlet > Scheduling

1. Klicken Sie in der Ereignisliste im **Scheduled Outlet Action** der **Scheduling** auf den Namen des Ereignisses.
2. Auf der **Daily/Weekly scheduled action detail** können Sie eine der folgenden Aktionen ausführen:
   - Ändern Sie Details des Ereignisses, z.B. den Namen des Ereignisses, wann es stattfinden soll und welche Ausgänge betroffen sind.
   - Unter **Status of event** oben auf der Seite können Sie die folgenden Aufgaben ausführen:
     * Deaktivieren Sie das Ereignis und lassen Sie alle Details konfiguriert, damit es später wieder aktiviert werden kann. Ein deaktiviertes Ereignis tritt nicht auf. Ein Ereignis ist standardmäßig aktiviert, wenn Sie es erstellen.
     * Aktivieren Sie das Ereignis, wenn es zuvor auf **Disable** eingestellt war.
     * Löschen Sie das Ereignis und entfernen Sie es vollständig aus dem System. Ein gelöschtes Ereignis kann nicht abgerufen werden.

Wenn Sie die Änderungen auf dieser Seite abgeschlossen haben, klicken Sie auf **Apply**, um die Änderungen zu bestätigen oder **Cancel**.

Ausgangsbenutzer-Manager

Die Webseite Ausgangsbenutzer-Manager ermöglicht es einem Benutzer mit Administratorrechten, vorhandene Ausgangsbenutzerinformationen anzuzeigen und neue Benutzer hinzuzufügen. Jedem Ausgangsbenutzer können individuelle Ausgänge zugewiesen werden. Wenn sich ein Ausgangsbenutzer bei der Rack PDU anmeldet, kann er nur Ausgänge anzeigen oder steuern, die dem Ausgangsbenutzer zugewiesen wurden.

Um die einem vorhandenen Ausgangsbenutzer zugewiesenen Ausgänge zu ändern, klicken Sie auf die Ausgangsliste unter dem gewünschten RPDU-Symbol. Um die Eigenschaften eines vorhandenen Ausgangsbenutzers zu ändern, klicken Sie auf den gewünschten Benutzernamen.

Um ein neues Ausgangsbenutzerkonto zu erstellen, klicken Sie auf der Webseite auf die **Add User** Schaltfläche. Dadurch gelangen Sie zur Webseite für die neue Benutzerkonfiguration. Stellen Sie sicher, dass Sie **Outlet** im Feld **User Type**. Nachdem Sie alle Felder ausgefüllt haben, klicken Sie auf **Next >>**, um zur nächsten Seite zu gelangen, auf der Sie die gewünschten Ausgänge für den Ausgangsbenutzer auswählen können.

Konfigurieren eines Ausgangsbenutzer

Path: Configuration > RPDU > Outlet User

1. Klicken Sie auf die Schaltfläche **Add New User**.
2. Geben Sie die Informationen für die folgenden Optionen ein und klicken Sie auf **Apply**, um die Änderungen zu bestätigen.

Option	Beschreibung
Username	Einstellen des Ausgangsbenuternamens. „Neuer Benutzer“ ist reserviert und nicht erlaubt. **HINWEIS:** Ein orangefarbener Benutzername zeigt an, dass das Benutzerkonto deaktiviert wurde.
Password	Einstellen des Ausgangsbenutzerkennworts.
User Description	Identifikation/Beschreibung des Ausgangsbenutzers einstellen.
Account Status	Das Konto des Ausgangsbenutzers aktivieren, deaktivieren oder löschen.
Device outlet access	Wählen Sie die Ausgänge aus, auf die der Benutzer zugreifen kann.

Ausgang-Manager und gemeinsame Nutzung von Netzwerkports

Augangsbenutzern können Ausgänge an jeder Rack PDU in einer Gruppe mit geschalteten Ausgängen zugewiesen werden. Die Ausgangsbenutzer werden auf der Host-PDU gespeichert. In der Web-UI können Sie Ausgänge anzeigen, die einer bestimmten PDU zugewiesen sind, indem Sie im Fenster auf ihre Display-ID klicken.

Temperatur- und Feuchtigkeitssensoren konfigurieren

Path: Configuration > RPDU > Environment

HINWEIS: Um diese Funktion nutzen zu können, müssen Sie einen optionalen Temperatursensor von APC by Schneider Electric (AP9335T) oder einen Temperatur-/Feuchtigkeitssensor von APC by Schneider Electric (AP9335TH) an Ihrer Rack PDU installiert haben.

Für Temperatur:

- Wenn die hohe Temperaturschwelle erreicht ist, erzeugt das System einen Warnalarm.
- Wenn die maximale Temperaturschwelle erreicht ist, erzeugt das System einen kritischen Alarm.

Ebenso, für Feuchtigkeit:

- Wenn die niedrige Feuchtigkeitsschwelle erreicht ist, erzeugt das System einen Warnalarm.
- Wenn die Mindestfeuchtigkeitsschwelle erreicht ist, erzeugt das System einen kritischen Alarm.

HINWEIS: Klicken Sie auf das Thermometersymbol in der oberen rechten Ecke, um zwischen Fahrenheit und Celsius umzuschalten.

So konfigurieren Sie Temperatur- und Feuchtigkeitssensoren:

1. Geben Sie Werte für minimale, maximale, hohe und niedrige Schwellenwerte ein.
2. Genen Sie **Hysteresis**-Werte ein.
3. Aktivieren Sie die Alarmgenerierung wie gewünscht.
4. Klicken Sie **Apply**.

Hysteresis: Dieser Wert gibt an, wie weit nach einem Schwellenwert die Temperatur oder Luftfeuchtigkeit zurückkehren muss, um eine Schwellenwertverletzung zu beheben.

- Für maximale und hohe Temperaturschwellenverletzungen ist der Klärpunkt der Schwellenwert minus der Hysterese.
- Für Schwellenwertverletzungen bei minimaler und niedriger Luftfeuchtigkeit ist der Klärpunkt der Schwellenwert plus die Hysterese.

Erhöhen Sie den Wert für Temperaturhysterese oder Feuchtigkeitshysterese, um Mehrfachalarme zu vermeiden, wenn Temperatur oder Feuchtigkeit, die eine Verletzung verursacht haben, dann leicht auf und ab schwanken. Wenn der Hysteresewert zu niedrig ist, kann ein solches Schwanken wiederholt eine Schwellwertverletzung verursachen und beseitigen.

Beispiel für eine steigende, aber schwankende Temperatur: Der maximale Temperaturgrenzwert beträgt 85 °F und die Temperaturhysterese beträgt 3 °F. Die Temperatur steigt auf über 85 °F an und verletzt damit den Schwellenwert. Es schwankt dann wiederholt auf 84° F und dann auf 86° F, aber es tritt kein Löschen-Ereignis und keine neue Verletzung auf. Damit die bestehende Abweichung beseitigt wird, müsste die Temperatur auf 82 ° F (3° F unter dem Schwellenwert) fallen.

Beispiel für fallende, aber schwankende Luftfeuchtigkeit: Die minimale Feuchtigkeitsschwelle beträgt 18% und die Feuchtigkeitshysterese beträgt 8%. Die Luftfeuchtigkeit fällt unter 18% und verletzt die Schwelle. Es schwankt dann wiederholt bis zu 24% und bis zu 13%, aber es tritt kein Löschen-Ereignis und keine neue Verletzung auf. Damit sich die bestehende Abweichung klärt, müsste die Luftfeuchtigkeit auf über 26% steigen (8% über den Schwellenwert).

Sicherheit

Sitzungsverwaltung-Bildschirm

Path: Configuration > Security > Session Management

Die Aktivierung von **Allow Concurrent Logins** bedeutet, dass sich zwei oder mehr Benutzer gleichzeitig anmelden können. Jeder Benutzer hat den gleichen Zugriff und jede Schnittstelle (HTTP, FTP, Telnet-Konsole, serial console (CLI) usw.) zählt als angemeldeter Benutzer.

Remote Authentication Override: Die Rack PDU unterstützt die Radius-Speicherung von Passwörtern auf einem Server. Wenn Sie diese Überschreibung jedoch aktivieren, ermöglicht die Rack PDU einem lokalen Benutzer die Anmeldung mit dem Kennwort für die Rack PDU, das lokal auf der Rack PDU gespeichert ist. Siehe auch „Lokale Benutzer“ ("Local Users") und „Authentifizierung von Remote-Benutzern“.

Ping-Antwort

Path: Configuration > Security > Ping Response

Aktivieren Sie das Aktivieren-Kontrollkästchen für **IPv4 Ping Response**, damit die Rack PDU auf Netzwerk-Pings reagieren kann. Deaktivieren Sie das Kontrollkästchen, um eine Rack PDU-Antwort zu deaktivieren. Dies gilt nicht für IPv6.

Lokale Benutzer

Verwenden Sie diese Menüoptionen, um den Zugriff und individuelle Einstellungen (wie das angezeigte Datumsformat) auf die Rack PDU-Benutzeroberflächen anzuzeigen und einzurichten. Dies gilt für Benutzer, die über ihren Anmeldenamen definiert sind.

Path: Configuration > Security > Local Users > Management

Setting user access: Mit dieser Option kann ein Administrator oder Super-Benutzer die Benutzer auflisten und konfigurieren, die Zugriff auf die Web-UI haben. Der Super-Benutzer hat immer Zugriff auf die Rack-PDUs.

Klicken Sie auf **Add User**, um einen Benutzer hinzuzufügen. Auf dem daraufhin angezeigten Bildschirm **User Configuration** können Sie einen Benutzer hinzufügen und den **Access** verweigern, indem Sie das Zugriff-Kontrollkästchen deaktivieren. Bei Benutzernamen und Passwörtern wird zwischen Groß- und Kleinschreibung unterschieden. Die maximale Länge für den Namen und das Kennwort beträgt 64 Byte, bei Mehrbytezeichen weniger. Sie müssen ein Passwort eingeben. Leere Passwörter (Passwörter ohne Zeichen) sind nicht zulässig.

> **HINWEIS:** Werte über 64 Byte in Name und Passwort werden möglicherweise abgeschnitten. Um eine Administrator-/Super-Benutzer-Einstellung zu ändern, müssen Sie alle drei Kennwortfelder eingeben.

Verwenden Sie das **Session Timeout**, um die Zeit (standardmäßig 3 minutes) zu konfigurieren, die die Webbenutzeroberfläche wartet, bevor ein inaktiver Benutzer abgemeldet wird. Wenn Sie diesen Wert ändern, müssen Sie sich abmelden, damit die Änderung wirksam wird.

> **HINWEIS:** Dieser Timer läuft weiter, wenn ein Benutzer das Browserfenster schließt, ohne sich vorher abzumelden, indem er oben rechts auf **Log Off** klickt. Da dieser Benutzer weiterhin als angemeldet gilt, kann sich kein Benutzer anmelden, bis die als **Minutes of Inactivity** angegebene Zeit abgelaufen ist. Wenn beispielsweise mit dem Standardwert für **Minutes of Inactivity** ein Benutzer das Browserfenster schließt, ohne sich abzumelden, kann sich 3 minutes lang kein Benutzer anmelden.

Serial Remote Authentication Override: Wenn Sie diese Option auswählen, können Sie RADIUS mithilfe der seriellen Konsolenverbindung (CLI) umgehen. Dieser Bildschirm aktiviert es für den ausgewählten Benutzer, muss aber auch global aktiviert werden, um zu funktionieren (über den Bildschirm “Session Management”).

Default settings: Stellen Sie die Standardwerte ein, die in die einzelnen Felder eingefügt werden sollen, wenn das Konto auf Super-Benutzer- oder Administratorebene einen neuen Benutzer erstellt. Diese Werte können geändert werden, bevor die Einstellungen auf das System angewendet werden.

- Access: Aktivieren Sie das **Enable**-Kontrollkästchen, um den Zugriff zu ermöglichen.
- User Type: Wählen Sie den Benutzertyp aus dem Dropdown-Menü aus.
- User Description: Geben Sie die Benutzerbeschreibung in das Feld ein.
- Session Timeout: Wählen Sie zwischen 1 und 60 minutes.
- Bad Login Attempts: Stellen Sie die Anzahl der erfolglosen Anmeldeversuche ein, die der Benutzer haben kann. Wählen Sie zwischen 0 und 99 Versuche. 0 = unbegrenzt

User Preferences: Standardmäßig ist diese Option aktiviert.

- **Event Log Color Coding:** Aktivieren Sie das Kontrollkästchen, um die Farbcodierung des im Ereignisprotokoll aufgezeichneten Alarmtextes zu aktivieren. Systemereigniseinträge und Konfigurationsänderungseinträge ändern ihre Farbe nicht.

Textfarbe	Alarmstufe
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:** Die Bedingungen, die den Alarm verursacht haben, haben sich verbessert.
Schwarz	**Normal:** Es liegen keine Alarme vor. Die Rack PDU und alle angeschlossenen Geräte arbeiten normal.

- **Change the default temperature scale:** Wählen Sie die in den **US Customary** (Fahrenheit) oder **Metric** (Celsius) Temperaturskala aus, in der alle Temperaturmessungen in dieser Benutzeroberfläche angezeigt werden sollen.
- **Export Log Format:** Konfigurieren Sie, in welchem Format das Ereignisprotokoll beim Exportieren (Herunterladen) angezeigt werden soll. Die Registerkarte (Standard) ermöglicht das Trennen von Feldern durch Registerkarten, während CSV durch Kommas getrennt ist.
- **Date Format:** Wählen Sie das Zahlenformat, in dem alle Daten in dieser Benutzeroberfläche angezeigt werden sollen. In den Auswahlen steht jeder Buchstabe m (für Monat), d (für Tag) und y (für Jahr) für eine Ziffer. Einstellige Tage und Monate werden mit einer vorangestellten Null angezeigt.
- **Language:** Wählen Sie die Anzeigesprachen der Benutzeroberfläche aus dem Dropdown-Feld aus.

Passwortanforderungen:

- **Starke Passwörter:** Konfigurieren Sie, ob für neue Kennwörter, die für Benutzerkonten erstellt wurden, zusätzliche Regeln erforderlich sind, z.B. mindestens ein Kleinbuchstabe, ein Großbuchstabe, eine Zahl und ein Symbol.
- **Passwortrichtlinie:** Wählen Sie die Dauer (in Tagen) aus, bis zu der der Benutzer sein Passwort ändern muss. Ein Wert von 0 Tagen deaktiviert diese Funktion (standardmäßig).

Fernbenutzer

Authentication: Geben Sie an, wie Benutzer bei der Anmeldung authentifiziert werden sollen.

Path: Configuration > Security > Remote Users > Authentication

Informationen zur lokalen Authentifizierung (nicht zur zentralen Authentifizierung eines RADIUS-Servers) finden Sie im Sicherheitshandbuch, das unter verfügbar ist **www.se.com**.

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

- Wenn ein Benutzer auf die Network Management Card oder ein anderes netzwerkfähiges Gerät zugreift, für das RADIUS aktiviert ist, wird eine Authentifizierungsanforderung an den RADIUS-Server gesendet, um die Benutzerberechtigungsstufe zu bestimmen.
- RADIUS-Benutzernamen, die mit der Rack PDU verwendet werden, sind auf 32 Zeichen begrenzt.

Wählen Sie eine der folgenden Optionen aus:

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

  HINWEIS: Wenn **RADIUS Only** ausgewählt ist und der RADIUS-Server nicht verfügbar oder nicht ordnungsgemäß konfiguriert ist, ist der Remotezugriff für alle Benutzer nicht verfügbar. Sie müssen eine serielle Verbindung zur Befehlszeilenschnittstelle verwenden und die Zugriffseinstellung in **local** oder **radiusLocal** ändern, um den Zugriff wiederherzustellen.

  Der Befehl zum Ändern der Zugriffseinstellung in **local** wäre beispielsweise: **radius -a local**

RADIUS:

Path: Configuration > Security > Remote Users > RADIUS

Verwenden Sie diese Option, um Folgendes zu tun:

- Listen Sie die RADIUS-Server (maximal zwei) auf, die für die Rack PDU verfügbar sind, und den Timeout-Zeitraum für jeden.
- Klicken Sie auf einen Link und konfigurieren Sie die Parameter für die Authentifizierung durch einen neuen RADIUS-Server.
- Klicken Sie auf einen aufgelisteten RADIUS-Server, um seine Parameter anzuzeigen und zu ändern.

RADIUS-Einstellung	Definition
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 standardmäßig Port 1812, um Benutzer zu authentifizieren. Die Rack PDU unterstützt die Ports 1812, 5000 bis 32768.
Secret	Das gemeinsames Geheimnis zwischen dem RADIUS-Server und der NMC der Rack PDU.
Reply Timeout	Die Zeit in Sekunden, die die Rack PDU auf eine Antwort vom RADIUS-Server wartet.
Test Settings	Geben Sie den Administratorbenutzernamen und das Administratorkennwort ein, um den von Ihnen konfigurierten RADIUS-Serverpfad zu testen.
Skip Test and Apply	Testen Sie den RADIUS-Serverpfad nicht. (Nicht empfohlen)

Konfigurieren des RADIUS Servers

Zusammenfassung des Konfigurationsverfahrens:

Sie müssen Ihren RADIUS-Server so konfigurieren, dass er mit der Rack PDU funktioniert.

Beispiele für die RADIUS-Benutzerdatei mit herstellerspezifischen Attributen (VSAs) und ein Beispiel für einen Eintrag in der Wörterbuchdatei auf dem RADIUS-Server finden Sie im *Security Handbook (Sicherheitshandbuch)*.

1. Fügen Sie der RADIUS-Server-Client-Liste (Datei) die IP-Adresse der Rack PDU hinzu.
2. Benutzer müssen mit Diensttypattributen konfiguriert werden, sofern nicht herstellerspezifische Attribute (VSAs) definiert sind. Wenn keine Service-Type-Attribute konfiguriert sind, haben Benutzer schreibgeschützten Zugriff (nur auf der Web-UI). Informationen zur RADIUS-Benutzerdatei finden Sie in der Dokumentation Ihres RADIUS-Servers, und ein Beispiel finden Sie im Sicherheitshandbuch.
3. VSAs können anstelle der vom RADIUS-Server bereitgestellten Diensttypattribute verwendet werden. VSAs benötigen einen Wörterbucheintrag und eine RADIUS Benutzerdatei. Definieren Sie in der Wörterbuchdatei die Namen für die Schlüsselwörter ATTRIBUTE und VALUE, jedoch nicht für die numerischen Werte. Wenn Sie numerische Werte ändern, ist die RADIUS-Authentifizierung und Autorisierung nicht erfolgreich. VSAs haben Vorrang vor standardmäßigen RADIUS Attributen.

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

Wenn UNIX Shadow-Passwortdateien (/etc/passwd) mit den RADIUS-Wörterbuchdateien verwendet werden, können die folgenden zwei Methoden zur Authentifizierung von Benutzern verwendet werden:

- Wenn alle UNIX-Benutzer über Administratorrechte verfügen, fügen Sie der RADIUS Server Datei "user" Folgendes hinzu. Um nur Gerätebenutzer zuzulassen, ändern Sie den APC-Service-Type in `Device`.

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

- Fügen Sie der RADIUS-Datei "user" Benutzernamen und Attribute hinzu und überprüfen Sie das Passwort anhand von /etc/passwd. Das folgende Beispiel ist für Benutzer `bconners` und `thawk`:

```
bconners        Auth-Type = System
                APC-Service-Type = Admin

thawk           Auth-Type = System
                APC-Service-Type = Device
```

Unterstützte RADIUS-Server

FreeRADIUS v 1.x und v 2.x, Microsoft Server 2008 und 2012
Network Policy Server (NPS) sind unterstützt. Andere allgemein verfügbare RADIUS-Anwendungen funktionieren möglicherweise, wurden jedoch nicht vollständig getestet.

RADIUS und Netzwerk-Portfreigabe

HINWEIS: Weitere Informationen zur Verwendung von RADIUS finden Sie im Sicherheitshandbuch.

Für RADIUS-Benutzerdateien mit VSAs können Ausgänge auf Gast-Rack PDUs RADIUS Benutzern mithilfe der Methode im folgenden Beispiel zugeordnet werden:

```
# give user access to outlets 1, 2, and 3 on unit 1,
# outlet 7 on 2, outlets 1 through 6
# on unit 3, and outlets 1,2,4 through 6,7 through 10,
# and 20 on unit 4
newOutletUser Auth-Type = Local, User-Password =
“newoutlets”
     APC-Service-Type = Outlet,
     APC-Outlets = “1[1,2,3];2[7];3[1-6];4[1,2,4-6,7-
10,20];”
```

Firewall-Menüs

Path: Configuration > Security > Firewall

Configuration: Aktivieren oder deaktivieren Sie die Firewall-Funktionalität. Die konfigurierte Richtlinie wird standardmäßig aufgelistet. Aktivieren Sie das **Enable**-Kontrollkästchen, um die Firewall zu aktivieren. Das Kontrollkästchen ist standardmäßig deaktiviert.

- Klicken Sie auf **Apply**, um eine Firewall-Richtlinie zu bestätigen, die Sie zum Aktivieren ausgewählt haben. Die **Firewall Confirmation** wird geöffnet.
  - Die Bestätigungsseite enthält eine Empfehlung, die Firewall vor der Aktivierung zu testen. Es ist nicht obligatorisch.
  - Der erste Hyperlink führt zur Seite Firewall-Richtlinie.
  - Der zweite Hyperlink führt zur Firewall-Testseite.
  - Klicken Sie auf **Apply**, um die Firewall zu aktivieren und zur Konfigurationsseite zurückzukehren.
  - Klicken Sie auf **Cancel**, um zur Konfigurationsseite zurückzukehren, ohne die Firewall zu aktivieren.
- Klicken Sie auf **Cancel:** Es wird keine neue Auswahl aktiviert. Sie bleiben auf der Konfigurationsseite.

Active Policy: Wählen Sie eine aktive Richtlinie aus der Dropdown-Liste Verfügbare Richtlinien aus, und zeigen Sie die Gültigkeit dieser Richtlinie an.
Die aktuelle aktive Richtlinie wird standardmäßig angezeigt; Sie können einen anderen in der Liste auswählen.

- Klicken Sie auf **Apply**, um Ihre Änderungen zu speichern. Wenn eine andere Firewall ausgewählt und aktiviert wurde, wird die Änderung sofort wirksam. Wenn eine neu konfigurierte Firewall-Richtlinie ausgewählt wurde, wird empfohlen, die neue Firewall zu testen, bevor Sie sie aktivieren.

Klicken Sie auf **Cancel**, um die ursprüngliche aktive Richtlinie wiederherzustellen und auf der Aktive Richtlinie-Seite zu bleiben.

Active Rules: Wenn eine Firewall aktiviert ist, listet diese schreibgeschützte Seite die einzelnen Regeln auf, die von einer aktuell aktiven Richtlinie erzwungen werden. Beschreibungen der Felder (Priorität, Ziel, Quelle, Protokoll, Aktion und Protokoll) finden Sie im Abschnitt **Create/Edit Policy**.

Create/Edit Policy: Erstellen einer neuen Richtlinie; Löschen oder Bearbeiten einer vorhandenen Richtlinie:

> **HINWEIS:** Während das Löschen einer aktiven aktivierten Firewall-Richtlinie nicht möglich ist, kann eine laufende Richtlinie bearbeitet werden, wird jedoch nicht empfohlen, da Änderungen sofort angewendet werden. Deaktivieren Sie stattdessen die Firewall, bearbeiten Sie die Richtlinie, testen Sie sie, und aktivieren Sie die Richtlinie dann erneut.

Create a new policy: Klicken Sie auf **Add Policy** und geben Sie den Dateinamen für die neue Firewall-Datei ein. Der Dateiname sollte eine .fwl-Dateierweiterung haben. Wenn ohne Dateierweiterung gelassen, wird .fwl automatisch an den Namen angehängt.

- Klicken Sie auf **Apply**: Wenn der Dateiname zulässig ist, wird die leere Firewall-Richtliniendatei erstellt. Sie befindet sich im Ordner /fwl mit den anderen Richtlinien im System.
- Klicken Sie auf **Cancel**, um zur vorherigen Seite zurückzukehren, ohne eine neue Firewall-Datei zu erstellen.

Edit an existing policy: Wählen Sie **Edit Policy**, um zur Bearbeitungsseite zu gelangen. Sie können eine Firewall-Richtlinie bearbeiten, die nicht aktiv ist.

Warnseite: Wenn Sie versuchen, die aktivierte Richtlinie zu bearbeiten, wird eine Warnseite geöffnet:

„Wenn Sie die aktive Firewall-Richtlinie bearbeiten, werden alle Änderungen sofort übernommen. Es wird empfohlen, die Firewall zu deaktivieren und die Richtlinie zu testen, bevor Sie sie aktivieren.“ ("Editing the active firewall policy will cause all changes made to be applied immediately. It is recommended to disable the firewall and test the policy before enabling it.")

- Klicken Sie auf **Apply**, um die Warnseite zu verlassen und zur Seite Richtlinie bearbeiten zurückzukehren.
- Klicken Sie auf **Cancel**, um die Warnseite zu verlassen und zur Seite Richtlinie erstellen/bearbeiten zurückzukehren

So bearbeiten Sie eine vorhandene Richtlinie:

1. Wählen Sie die Richtlinie, die Sie bearbeiten möchten, aus der **Policy Name**-Dropdown-Liste aus und klicken Sie auf **Edit Policy**.
2. Klicken Sie auf **Add Rule** oder wählen Sie die **Priority** einer vorhandenen Regel aus, um zur **Edit Rule** bearbeiten zu gelangen. Auf dieser Seite können Sie die Regeleinstellungen ändern oder die ausgewählte Regel löschen.

Einstellung	Beschreibung
Priority	Wenn 2 Regeln in Konflikt geraten, bestimmt die Regel mit der höheren Priorität, was passiert. Die höchste Priorität ist 1, die niedrigste 250.
Type	**host:** Im IP-/beliebige Feld geben Sie eine einzelne IP-Adresse ein **subnet:** Im IP-/beliebige Feld geben Sie eine Subnetzadresse ein. **range:** Im IP-/beliebige Feld geben Sie einen Bereich von IP-Adressen ein
IP/any	Geben Sie die IP-Adresse oder den Adressbereich an, für den diese Regel gilt, oder wählen Sie eine der folgenden Optionen aus: • **any:** Die Regel gilt unabhängig von der IP-Adresse • **anyipv4:** Die Regel gilt für jede IPv4-Adresse. • **anyipv6:** Die Regel gilt für jede IPv6-Adresse.
Port	Geben Sie einen Port an, auf den die Regel angewendet wird. • **None:** Die Regel gilt für jeden Port • **Common Configured ports:** Wählen Sie einen Standardport aus • **Other:** Geben Sie eine nicht standardmäßige Portnummer an
Protocol	Geben Sie das Protokoll an, für das die Regel gilt • **any:** beliebiges Protokoll • **tcp:** wird für den zuverlässigen Informationstransfer zwischen Anwendungen verwendet • **udp:** alternative zu TCP für schnellere Informationsübertragung mit geringerer Bandbreite. Obwohl es weniger Verzögerungen hat, ist UDP weniger zuverlässig als TCP. • **icmp:** wird verwendet, um Fehler zur Fehlerbehebung zu melden • **icmpv6:** wird verwendet, um Fehler zur Fehlerbehebung bei Anwendungen zu melden, die IPv6 verwenden
Action	**allow:** Zulassen des Pakets, das dieser Regel entspricht **discard**: Verwerfen des Pakets, das dieser Regel entspricht
Log	Wenn diese Regel auf ein Paket angewendet wird, unabhängig davon, ob das Paket blockiert oder zugelassen ist, wird dem Firewall-Protokoll ein Eintrag hinzugefügt.

Es wird empfohlen, dass Sie eine der folgenden Regeln als Regel mit der niedrigsten Priorität in Ihre Firewall-Richtlinie aufnehmen:

- Um die Firewall als Whitelist zu verwenden, fügen Sie Folgendes hinzu
  `250 Dest any / Source any / protocol any / discard`
- Um die Firewall als Blacklist zu verwenden, fügen Sie hinzu
  `250 Dest any / Source any / protocol any / allow`

Delete a policy: Wählen Sie **Delete Policy** aus, um die Löschen bestätigen-Seite zu öffnen. Klicken Sie zur Bestätigung auf **Apply**, und die ausgewählte Firewall-Datei wird aus dem Dateisystem entfernt.

Load Policy: Eine Richtlinie (mit dem .fwl-Suffix) von einer Quelle außerhalb dieses Geräts hochladen.

Test: Vorübergehend die Regeln einer ausgewählten Richtlinie für einen von Ihnen angegebenen Zeitraum erzwingen.

802.1 X Security Configuration

Path: Configuration > Security > 802.1X Security

Die Netzwerkmanagement-Karte übernimmt die Rolle eines Bittstellers in einer EAPoL-Architektur (Erweiterbares Authentifizierungsprotokoll über LAN), die in der IEEE 802.1X-portbasierten Netzwerkzugriffskontrolle verwendet wird.
Die Netzwerkmanagement-Karte unterstützt EAP-TLS als Authentifizierungsmethode, bei der der Benutzer 3 clientseitige Zertifikate hochladen muss. Der private Schlüssel wird in einem verschlüsselten Format gespeichert. Der Benutzer muss eine gültige Passphrase angeben, um den 802.1X-Sicherheitszugriff aktivieren zu können.

HINWEIS: Die Netzwerkmanagement-Karte unterstützt nur die EAP-TLS-Authentifizierungsmethode.

Die Web-UI bietet die folgenden Optionen für die EAPoL-Konfiguration:

Einstellung	Beschreibung
EAPoL Access	Verwendet, um den 802.1X-Sicherheitszugriff zu aktivieren oder zu deaktivieren. **HINWEIS:** Der 802.1X-Sicherheitszugriff ist standardmäßig deaktiviert. Der Benutzer kann nur aktivieren, wenn der Benutzer gültige Zertifikate und eine gültige Passphrase für den privaten Schlüssel zur Verfügung stellt.
Supplicant Identifier	Ermöglicht den Benutzern, ihre eigene Bittsteller-ID festzulegen (bis zu 32 Zeichen einschließlich Leerzeichen). **HINWEIS:** Standardmäßig ist die Supplicant-ID auf "NMC- Supplicant-xx:xx:xx:xx:xx" festgelegt, wobei sechs Oktette von "xx" die MAC-ID der Netzwerkmanagement-Karte sind.
CA Certificate	Ein CA-Stammzertifikat laden/ersetzen oder entfernen. Die unterstützte Dateiformate sind PEM (Privacy Enhanced Mail) oder DER (Distinguished Encoding Rules) mit den zulässigen Dateierweiterungen .pem, .PEM, .der oder .DER.
Private Key Certificate	Einen verschlüsselten privaten Schlüssel laden/ersetzen oder entfernen. Die unterstützte Dateiformate sind PEM (Privacy Enhanced Mail) oder DER (Distinguished Encoding Rules) mit den zulässigen Dateierweiterungen .key oder .KEY. **HINWEIS:** Unverschlüsselter privater Schlüssel wird nicht akzeptiert.
Private Key Passphrase	Geben Sie die Passphrase zum Entschlüsseln des verschlüsselten privaten Schlüssels an. Ermöglicht bis zu 64 Zeichen, einschließlich Leerzeichen.
User/Public Certificate	Hochladen/ersetzen oder Entfernen eines Benutzer- /öffentlichen Zertifikats. Die unterstützte Dateiformate sind PEM (Privacy Enhanced Mail) oder DER (Distinguished Encoding Rules) mit den zulässigen Dateierweiterungen .pem, .PEM, .der oder .DER.

Netzwerk-Funktionen

Zusammenfassung der Protokollkonfiguration

Path: Configuration > Network > TCP/IP

Auf dieser Seite können Sie alle Protokolle anzeigen, die auf Ihrer Rack PDU aktiviert oder deaktiviert sind. Wählen Sie einen Link für ein beliebiges Protokoll aus, um zur entsprechenden Konfigurationsseite zu gelangen.

TCP/IP- und Kommunikation-Einstellungen

TCP/IP:

Path: Configuration > Network > TCP/IP

Die TCP/IP-Option im linken Navigationsmenü, die standardmäßig ausgewählt ist, wenn Sie Netzwerk in der oberen Menüleiste auswählen, zeigt die aktuelle IPv4-Adresse, die Subnetzmaske, das Standard-Gateway, die MAC-Adresse und den Startmodus der Rack PDU an. Informationen zu den DHCP-Optionen finden Sie online unter **RFC2131** und **RFC2132**

Einstellung	Beschreibung
Enable	Aktivieren oder deaktivieren Sie IPv4 mit diesem Kontrollkästchen.
Manual	Konfigurieren Sie IPv4 manuell, indem Sie die IP-Adresse, die Subnetzmaske und das Standard-Gateway eingeben.
BOOTP	Ein BOOTP-Server stellt die TCP/IP-Einstellungen bereit. In Intervallen von 32 Sekunden fordert die Rack PDU die Netzwerkzuweisung von einem beliebigen BOOTP-Server an: • Wenn die Rack PDU eine gültige Antwort erhält, startet sie die Netzwerkdienste. • Wenn die Rack PDU einen BOOTP-Server findet, eine Anforderung an diesen Server jedoch nicht erfolgreich ist oder eine Zeitüberschreitung auftritt, beendet die Rack PDU die Anforderung von Netzwerkeinstellungen, bis sie neu gestartet wird. • Wenn zuvor konfigurierte Netzwerkeinstellungen vorhanden sind und die Rack PDU auf fünf Anforderungen (die ursprüngliche und vier Wiederholungen) keine gültige Antwort erhält, verwendet sie standardmäßig die zuvor konfigurierten Einstellungen, damit weiterhin darauf zugegriffen werden kann. Klicken Sie auf **Next >>**, um auf die BOOTP-Konfigurationsseite zuzugreifen und die Anzahl der Wiederholungen oder die auszuführende Aktion zu ändern, wenn alle Wiederholungen nicht erfolgreich sind:[1] • **Maximum retries:** Geben Sie die Anzahl der Wiederholungen ein, die auftreten, wenn keine gültige Antwort empfangen wird, oder Null (0) für eine unbegrenzte Anzahl von Wiederholungen. • **If retries do not succeed:** Wählen Sie **Use prior settings** (Standardeinstellung) oder **Stop BOOTP request**.
DHCP	Die Standardeinstellung. In Intervallen von 32 Sekunden fordert die Rack PDU die Netzwerkzuweisung von einem beliebigen DHCP-Server an. • Wenn die Rack PDU eine gültige Antwort erhält, benötigt sie (wie bisher) nicht das APC-Cookie vom DHCP-Server, um die Lease zu akzeptieren und die Netzwerkdienste zu starten. • Wenn die Rack PDU einen DHCP-Server findet, die Anforderung an diesen Server jedoch nicht erfolgreich ist oder eine Zeitüberschreitung auftritt, werden die Netzwerkeinstellungen erst nach einem Neustart angefordert.[1] • **Require vendor specific cookie to accept DHCP Address:** Durch Aktivieren dieses Kontrollkästchens können Sie den DHCP-Server auffordern, ein Cookie bereitzustellen, das Informationen an die Rack PDU liefert.

[1]Die Standardwerte für diese drei Einstellungen auf den Konfigurationsseiten müssen im Allgemeinen nicht geändert werden:

- **Vendor Class:** APC
- **Client ID:** Die MAC-Adresse der Netzwerkmanagement-Karte der Rack PDU, die sie im lokalen Netzwerk (LAN) eindeutig identifiziert
- **User Class:** Der Name des Anwendungs-Firmware-Moduls

DHCP-Antwortoptionen:

Jede gültige DHCP-Antwort enthält Optionen, die die TCP/IP-Einstellungen bereitstellen, die die Rack PDU für den Betrieb in einem Netzwerk benötigt, sowie andere Informationen, die sich auf den Betrieb der Rack PDU auswirken.

Vendor Specific Information (option 43): Die Rack-PDU verwendet diese Option in einer DHCP-Antwort, um festzustellen, ob die DHCP-Antwort gültig ist. Diese Option enthält eine APC-spezifische Option im Format TAG/LEN/ DATA, das so genannte APC-Cookie. Dies ist standardmäßig deaktiviert.

- **APC Cookie. Tag 1, Len 4, Data “1APC”**

Option 43 teilt der Rack-PDU mit, dass ein DHCP-Server für die Bedienung von Geräten konfiguriert ist.

Im Folgenden sehen Sie ein Beispiel für die Option "Herstellerspezifische Informationen" im hexadezimalen Format, die das APC-Cookie enthält:

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

TCP/IP-Optionen:

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

- **IP Address** (von der **yiaddr** Feld der DHCP-Antwort, beschrieben in RFC2131): Die IP-Adresse, die der DHCP-Server der Rack-PDU zur Verfügung stellt.
- **Subnet Mask (option 1):** Der Subnetzmaskenwert, den die Rack PDU für den Betrieb im Netzwerk benötigt.
- **Router, i.e., Default Gateway (option 3):** Die Standard-Gateway-Adresse, die die Rack-PDU für den Betrieb des Netzwerks benötigt.
- **IP Address Lease Time (option 51):** Die Dauer der Zuteilung der IP-Adresse an die Rack-PDU.
- **Renewal Time, T1 (option 58):** Die Zeit, die die Rack-PDU nach Zuteilung einer IP-Adresse warten muss, bevor sie eine Erneuerung dieser Zuteilung anfordern kann.
- **Rebinding Time, T2 (option 59):** Die Zeit, die die Rack-PDU nach Zuteilung einer IP-Adresse warten muss, bevor sie eine Neuanbindung dieser Zuteilung anfordern kann.

Weitere Optionen:

Die Rack PDU verwendet diese Optionen auch innerhalb einer gültigen DHCP-Antwort. Alle diese Optionen mit Ausnahme der letzten sind in beschrieben. **RFC2132.**

- **Network Time Protocol Servers (option 42):** Bis zu zwei NTP-Server (primär und sekundär), die die Rack-PDU verwenden kann.
- **Time Offset (option 2):** Der Zeitunterschied des Subnetzes der Rack-PDU (in Sekunden) von der koordinierten Weltzeit (UTC).
- **Domain Name Server (option 6):** Bis zu zwei Domänennamenserver (DNS-Server) (primär und sekundär), die die Rack-PDU verwenden kann.
- **Host Name (option 12):** Der von der Rack-PDU verwendete Hostname (Höchstlänge 32 Zeichen).
- **Domain Name (option 15):** Der von der Rack-PDU verwendete Domänenname (Höchstlänge 64 Zeichen).
- **Boot File Name** (von der **file** Feld der DHCP-Antwort, beschrieben in **RFC2131**): Der vollständige Pfad zu einer herunterzuladenden Benutzerkonfigurationsdatei (.ini-Datei). Das **siaddr**-Feld der DHCP-Antwort gibt die IP-Adresse des Servers an, von dem das Gerät die .ini-Datei herunterlädt. Nach dem Download, wird die .ini-Datei als Boot-Datei verwendet, um die Einstellungen neu zu konfigurieren.

Path: Configuration > Network > TCP/IP > IPv6 settings

Einstellung	Beschreibung
Enable	Aktivieren oder deaktivieren Sie IPv6 mit diesem Kontrollkästchen.
Manual	Konfigurieren Sie IPv6 manuell, indem Sie die IP-Adresse und das Standard Gateway eingeben.
Auto Configuration	Wenn das Autokonfiguration-Kontrollkästchen aktiviert ist, bezieht das System Adressierungspräfixe vom Router (falls verfügbar). Es verwendet diese Präfixe, um IPv6-Adressen automatisch zu konfigurieren.
DHCPv6 Mode	**Router Controlled (Routergesteuert):** Die Auswahl dieser Option bedeutet, dass DHCPv6 von den verwalteten (M) und anderen (O) Flags gesteuert wird, die in IPv6-Routerankündigungen empfangen werden. Wenn eine Router Ankündigung empfangen wird, prüft die Rack PDU, ob diese oder das O-Flag gesetzt ist. Die Rack PDU interpretiert den Status von M (Managed Address Configuration Flag) und O (Other Stateful Configuration Flag) für die folgenden Fälle: • *Neither is set:* Dies bedeutet, dass dem lokalen Netzwerk die DHCPv6 Infrastruktur fehlt. Die Rack PDU verwendet Router-Ankündigungen und manuelle Konfiguration, um Adressen zu erhalten, die nicht linklokal sind, und andere Einstellungen. • *M, or M and O are set:* In dieser Situation kommt es zu einer vollständigen DHCPv6-Adresskonfiguration. DHCPv6 wird verwendet, um Adressen UND andere Konfigurationseinstellungen abzurufen. Dieser Zustand wird als `DHCPv6 Stateful` bezeichnet. Sobald das M-Flag empfangen wurde, bleibt die DHCPv6-Adresskonfiguration in Kraft, bis die betreffende Schnittstelle geschlossen wurde. Dies gilt auch dann, wenn nachfolgende Router-Ankündigungspakete empfangen werden, in denen das M-Flag nicht eingestellt ist. Wenn zuerst ein O-Flag empfangen wird und anschließend ein M-Flag empfangen wird, führt die Rack PDU nach Empfang des M-Flags eine vollständige Adresskonfiguration durch. • *Only O is set:* In dieser Situation sendet die Rack-PDU eine DHCPv6 Info-Anfrage-Paket. DHCPv6 wird zur Konfiguration der "others" Einstellungen (z.B. der Standorte von DNS-Servern) verwendet, aber NICHT zur Bereitstellung von Adressen. Dies wird als `DHCPv6 stateless` bezeichnet. **Address and Other Information (Adresse und weitere Informationen):** Wenn dieses Optionsfeld ausgewählt ist, wird DHCPv6 verwendet, um Adressen UND andere Konfigurationseinstellungen zu erhalten. Dieser Zustand wird als `DHCPv6 Stateful` bezeichnet. **Non-Address Information Only (Nur Nicht-Adressinformationen):** Wenn dieses Optionsfeld ausgewählt ist, wird DHCPv6 verwendet, um "others" Einstellungen (z.B. Standort von DNS-Servern) zu konfigurieren, aber KEINE Adressen bereitzustellen. Dieser Zustand wird als `DHCPv6 Stateless` bezeichnet. **Never (Niemals):** Wählen Sie diese Option, um DHCPv6 zu deaktivieren.

Portgeschwindigkeit

Path: Configuration > Network > Port Speed

Die Einstellung **Port Speed** definiert die Kommunikationsgeschwindigkeit des TCP/IP-Ports.

- Bei der **Auto-negotiation** (Standardeinstellung) verhandeln Ethernet-Geräte, um mit der höchstmöglichen Geschwindigkeit zu übertragen. Wenn jedoch die unterstützten Geschwindigkeiten von zwei Geräten nicht übereinstimmen, wird die langsamere Geschwindigkeit verwendet.
- Alternativ können Sie zwischen 10 Mbps oder 100 Mbps wählen, jeweils mit der Option Halbduplex (Kommunikation jeweils nur in eine Richtung) oder Vollduplex (full-duplex) (Kommunikation in beide Richtungen auf demselben Kanal gleichzeitig).

DNS

Konfiguration:

Path: Configuration > Network > DNS > Configuration

Verwenden Sie die Optionen unter **Configuration**, um das Domänennamensystem (DNS) zu konfigurieren und zu testen:

- **Override Manual DNS Settings:** Die Auswahl von Manuellen DNS-Einstellungen überschreiben führt dazu, dass Konfigurationsdaten aus anderen Quellen (normalerweise DHCP) Vorrang vor den hier festgelegten manuellen Konfigurationen haben.
- Wählen Sie **Primary DNS Server** oder **Secondary DNS Server** aus, um die IPv4- oder IPv6-Adressen des primären und optionalen sekundären DNS-Servers anzugeben. Damit die Rack PDU E-Mails senden kann, müssen Sie mindestens die IP-Adresse des primären DNS-Servers definieren.

  — Die Rack PDU wartet bis zu 15 seconds auf eine Antwort vom primären DNS-Server oder sekundären DNS-Server (falls angegeben). Wenn die Rack PDU innerhalb dieser Zeit keine Antwort erhält, kann keine E-Mail gesendet werden. Verwenden Sie DNS-Server auf demselben Segment wie die Rack-PDU oder auf einem nahe gelegenen Segment (jedoch nicht in einem Weitverkehrsnetz [WAN]).

  — Definieren Sie die IP-Adressen der DNS-Server und geben Sie dann den DNS-Namen eines Computers in Ihrem Netzwerk ein, um die IP-Adresse für diesen Computer nachzuschlagen und den korrekten Betrieb zu überprüfen.
- **System Name Synchronization:** Erlauben Sie, dass der Hostname mit dem Systemnamen synchronisiert wird, damit beide Felder automatisch denselben Wert enthalten.

  HINWEIS: Wenn Sie diese Funktion aktivieren, kann der Systemnamensbezeichner kein Leerzeichen mehr enthalten (da er mit dem Hostnamenfeld synchronisiert wird).
- **Host Name:** Konfigurieren Sie hier einen Hostnamen und einen **Domain Name** im Feld Domänenname, dann können Benutzer einen Hostnamen in jedes Feld der Rack PDU-Schnittstelle (außer E-Mail-Adressen) eingeben, das einen Domänennamen akzeptiert.
- **Domain Name (IPv4/IPv6)**: Konfigurieren Sie den Domänennamen nur hier. In allen anderen Feldern der Rack PDU-Schnittstelle (außer E-Mail-Adressen), die Domänennamen akzeptieren, fügt die Rack PDU diesen Domänennamen hinzu, wenn nur ein Hostname eingegeben wird.

  — Um alle Instanzen der Erweiterung eines angegebenen Hostnamens durch Hinzufügen des Domänennamens zu überschreiben, setzen Sie das Feld Domänenname auf den Standardwert, `somedomain.com` oder auf `0.0.0.0`.

  — Fügen Sie einen abschließenden Punkt ein, um die Erweiterung eines bestimmten Hostnamenseintrags zu überschreiben. Die Rack PDU erkennt einen Hostnamen mit einem abschließenden Punkt (z.B. *`mySnmpServer`*.) als wäre es ein vollqualifizierter Domänenname und hängt den Domänennamen nicht an.
- **Domain Name (IPv6):** Geben Sie hier den IPv6-Domänennamen an.

Test:

Path: Configuration > Network > DNS > Test

Verwenden Sie diese Option, um eine DNS-Abfrage zu senden, die die Einrichtung Ihrer DNS-Server durch Nachschlagen der IP-Adresse testet. Zeigen Sie das Ergebnis eines Tests im Feld **Last Query Response** an.

- Wählen Sie **test** aus, um eine DNS-Abfrage zu senden, die die Einrichtung Ihrer DNS Server testet:

  — Identifizieren Sie als **Query Question** den Wert, der für den ausgewählten Abfragetyp verwendet werden soll:

Ausgewählter Abfragetyp	Die Abfrage
by Host	Die URL
by FQDN	Der vollqualifizierte Domainname, *my_server.my_domain*
by IP	Die IP Adresse
by MX	Die E-Mail-Austauschadresse

Web

Path: Configuration > Network > Web

Option	Beschreibung

access	Um Änderungen an einer dieser Auswahlen zu aktivieren, melden Sie sich von der Rack PDU ab:
	• **Disable:** Deaktiviert den Zugriff auf die Web-Oberfläche. (Um den Zugriff wieder zu aktivieren, melden Sie sich bei der Befehlszeilenschnittstelle an und geben Sie den Befehl `http -S enable` ein. Geben Sie für den HTTPS-Zugriff `https -S enable` ein.)
	• **Enable HTTP:** Aktiviert das Hypertext Transfer Protocol (HTTP), das den Webzugriff über Benutzername und Passwort ermöglicht, Benutzernamen, Passwörter und Daten während der Übertragung jedoch nicht verschlüsselt. Standardmäßig ist HTTP deaktiviert.
	• **Enable HTTPS:** Aktiviert Hypertext Transfer Protocol (HTTPS) über Secure Sockets Layer/Transport Layer Security (SSL/TLS). SSL/TLS verschlüsselt Benutzernamen, Passwörter und Daten während der Übertragung und authentifiziert die Rack PDU per digitalem Zertifikat. Wenn HTTPS aktiviert ist, zeigt Ihr Browser ein kleines Schlosssymbol an. Standardmäßig ist HTTPS aktiviert.
	Siehe „Erstellen und Installieren digitaler Zertifikate“ im *Security Handbook (Sicherheitshandbuch)*, verfügbar unter **www.se.com**.
	
	HTTP Port: Der TCP/IP-Port (standardmäßig 80), der für die Kommunikation per HTTP mit der Rack PDU verwendet wird.
	
	HTTPS Port: Der TCP/IP-Port (standardmäßig 443), der für die Kommunikation über HTTPS mit der Rack PDU verwendet wird.
	
	Für jeden dieser Ports können Sie die Porteinstellung für zusätzliche Sicherheit in einen beliebigen nicht verwendeten Port von 5000 bis 32768 ändern. Benutzer müssen dann einen Doppelpunkt (:) im Adressfeld des Browsers verwenden, um die Portnummer anzugeben. Zum Beispiel für eine Portnummer von 5000 und eine IP-Adresse von 152.214.12.114:
	`http://152.214.12.114:5000`
	`https://152.214.12.114:5000`
	
	Minimum Protocol: Wählen Sie aus dem Dropdown-Menü SSL 3.0, TLS 1.0, TLS 1.1 oder TLS 1.2 aus
	
	Require Authentication Cookie: Klicken Sie, um das **Enable box** zu aktivieren.
	
	Limited Status Access: Klicken Sie, um ein Häkchen in das Kästchen zu setzen, bevor Sie es **Enable** oder **Use as a default page**.

ssl Zertifikat	Hinzufügen, Ersetzen oder Entfernen eines Sicherheitszertifikats. **Status**: • **Not installed:** Ein Zertifikat ist nicht installiert oder wurde per FTP oder SCP an einem falschen Speicherort installiert. Mit **Add or Replace Certificate File** wird das Zertifikat am richtigen Speicherort /**ssl** auf der Rack PDU installiert. • **Generating:** Die Rack PDU generiert ein Zertifikat, da kein gültiges Zertifikat gefunden wurde. • **Loading:** Auf der Rack PDU wird ein Zertifikat aktiviert. • **Valid certificate:** Es wurde ein gültiges Zertifikat installiert oder von der Rack PDU generiert. Klicken Sie auf diesen Link, um den Inhalt des Zertifikats anzuzeigen. Wenn Sie ein ungültiges Zertifikat installieren oder wenn beim Aktivieren von SSL/ TLS kein Zertifikat geladen wird, generiert die Rack PDU ein Standardzertifikat, das den Zugriff auf die Schnittstelle um bis zu eine minute verzögert. Sie können das Standardzertifikat für grundlegende verschlüsselungsbasierte Sicherheit verwenden, aber bei jeder Anmeldung wird eine Sicherheitswarnung angezeigt. **Add or Replace Certificate File:** Geben Sie die mit dem *Security Handbook (Sicherheitshandbuch)* erstellte Zertifikatsdatei ein oder navigieren Sie zu ihr. Siehe „Erstellen und Installieren digitaler Zertifikate“ im *Sicherheitshandbuch*, verfügbar unter **www.se.com**, um eine Methode für die Verwendung digitaler Zertifikate auszuwählen, die vom Sicherheitsassistenten erstellt oder von der Rack PDU generiert wurden. **Remove:** Löschen des aktuellen Zertifikat.

Console

Path: Configuration > Network > Console > *options*

Option	Beschreibung

access	• **Telnet Enable/Disable:** Ermöglicht die Aktivierung bzw. Deaktivierung des dezentralen CLI-Zugriffs über Telnet. Telnet ist standardmäßig deaktiviert.
	• **SSH Enable/Disable:** Ermöglicht die Aktivierung bzw. Deaktivierung des dezentralen CLI-Zugriffs über SSH. SSH ist standardmäßig aktiviert. SSH überträgt Benutzernamen, Passwörter und Daten in verschlüsselter Form und bietet so Schutz vor dem Abfangen, Fälschen oder Verändern von Daten während der Übertragung.
	Konfigurieren Sie die Ports, die von diesen Protokollen verwendet werden sollen:
	• **Telnet Port:** Der Telnet-Port für die Kommunikation mit der Rack-PDU (standardmäßig 23). Sie können die Porteinstellung für zusätzliche Sicherheit in einen beliebigen nicht verwendeten Port von 5000 bis 32768 ändern. Benutzer müssen dann einen Doppelpunkt (:) oder ein Leerzeichen verwenden, wie von Ihrem Telnet-Clientprogramm gefordert, um den nicht standardmäßigen Port anzugeben. Beispiel: Für Port 5000 und die IP-Adresse 152.214.12.114 benötigt der Telnet-Client einen der folgenden Befehle:
	`telnet 152.214.12.114:5000`
	`telnet 152.214.12.114 5000`
	• **SSH Port:** Der SSH-Port für die Kommunikation mit der Rack-PDU (Standardwert: 22). Sie können die Port-Einstellung auf einen beliebigen freien Port zwischen 5000 und 32768 ändern, um die Sicherheit zu erhöhen. Informationen zum Befehlszeilenformat, das zum Angeben eines nicht standardmäßigen Ports erforderlich ist, finden Sie in der Dokumentation Ihres SSH-Clients.

ssh host key	**Status** zeigt den Status des Hostschlüssels (privates Schlüssels) an: • **SSH Disabled, No host key in use:** Wenn deaktiviert, kann SSH keinen Hostschlüssel verwenden. • **Generating:** Die Rack PDU erstellt einen Hostschlüssel, da kein gültiger Hostschlüssel gefunden wurde. • **Loading:** Ein Hostschlüssel wird auf der Rack PDU aktiviert. • **Valid:** Einer der folgenden gültigen Hostschlüssel befindet sich im Verzeichnis /ssh (der erforderliche Speicherort auf der Rack PDU): — Ein 1024–Bit- oder 2048-Bit-Hostschlüssel, der vom Sicherheitsassistenten erstellt wurde — Ein von der Rack PDU generierter 2048-Bit-RSA-Hostschlüssel **Add or Replace:** Navigieren Sie zu einer Hostschlüsseldatei, die vom Sicherheitsassistenten erstellt wurde, und laden Sie sie hoch. Informationen zur Verwendung des Sicherheitsassistenten finden Sie im Sicherheitshandbuch, das unter verfügbar ist **www.se.com** **HINWEIS:** Um die für die Aktivierung von SSH erforderliche Zeit zu verkürzen, erstellen und laden Sie im Voraus einen Hostschlüssel hoch. Wenn Sie SSH ohne geladenen Hostschlüssel aktivieren, benötigt die Rack PDU bis zu einer minute, um einen Hostschlüssel zu erstellen, und der SSH-Server ist während dieser Zeit nicht zugänglich. **Remove:** Entfernen Sie den aktuellen Hostschlüssel.

HINWEIS: Um SSH verwenden zu können, muss ein SSH-Client installiert sein. Die meisten Linux- und anderen UNIX-Plattformen enthalten einen SSH-Client, Microsoft Windows-Betriebssysteme jedoch nicht. Clients sind von verschiedenen Anbietern erhältlich.

SNMP

Alle Benutzernamen, Passwörter und Community-Namen für SNMP werden als Klartext über das Netzwerk übertragen. Wenn Ihr Netzwerk die hohe Sicherheit der Verschlüsselung erfordert, deaktivieren Sie den SNMP-Zugriff oder legen Sie den Zugriff für jede Community auf Lesen fest. (Eine Community mit Lesezugriff kann Statusinformationen empfangen und SNMP-Traps verwenden).

Wenn Sie StruxureWare Data Center Expert zum Verwalten einer Rack PDU im öffentlichen Netzwerk verwenden, muss SNMP in der Rack PDU-Schnittstelle aktiviert sein. Lesezugriff ermöglicht es dem StruxureWare Data Center Expert, Traps von der Rack PDU zu empfangen, aber Schreibzugriff ist erforderlich, während Sie die Schnittstelle der Rack PDU verwenden, um den StruxureWare Data Center Expert als Trap-Empfänger einzustellen.

Ausführliche Informationen zur Verbesserung und Verwaltung der Sicherheit Ihres Systems finden Sie im *Security Handbook (Sicherheitshandbuch)*, das unter **www.se.com** verfügbar ist.

Gemeinsame Nutzung von Netzwerkports (NPS)

Auf alle Rack PDUs in einer Gruppe kann über die Host-Rack PDU über SNMP "rPDU2" OIDs zugegriffen werden, die in unserer PowerNet-MIB verfügbar sind.

Der vollständige Pfad zu diesen OIDs lautet:
iso(1).org(3).dod(6).internet(1).private(4).companies(1).apc(318).products(1).
hardware(1).rPDU2(26)

Einzelne Rack PDUs können in den SNMP-MIB-Tabellen identifiziert werden, indem die entsprechenden „Modul“-OIDs in jeder Tabelle angezeigt werden. Diese Modul-OIDs geben die Display-ID der Rack PDU zurück.

Beispielmodul-OIDs: rPDU2IdentModule, rPDU2DeviceConfigModule, rPDU2SensorTempHumidityConfigModule

Um abwärtskompatibel zu früheren Versionen zu sein, ist die Host-Rack PDU immer der erste Index in jeder Tabelle, die mehrere Rack PDUs unterstützt. Darüber hinaus sollte sich nach dem Einrichten der Rack PDU-Gruppe die Indexreihenfolge der Gast-Rack PDUs auch dann nicht ändern, wenn die Display-ID geändert wird oder eine PDU vorübergehend die Kommunikation verliert. Die Indexreihenfolge sollte sich nur ändern, wenn Sie eine Rack PDU manuell aus der Gruppe entfernen.

Bei einer Überprüfung der MIB-Tabelle sollten die Indizes übersprungen werden, die einer Rack PDU zugeordnet sind, bei der die Kommunikation vorübergehend unterbrochen wurde.

SNMPv1

Path: Configuration > Network > SNMPv1 > *options*

HINWEIS: SNMPv1 ist standardmäßig deaktiviert. SNMPv2c wird in dieser Konfiguration unter SNMPv1 unterstützt.

Option	Beschreibung
access	**Enable SNMPv1 Access:** Aktiviert SNMP Version 1 als Kommunikationsmethode mit diesem Gerät. **HINWEIS:** Diese Konfiguration unterstützt auch SNMPv2c.
access control	Sie können bis zu vier Zugriffssteuerungseinträge konfigurieren, um anzugeben, welche Netzwerkverwaltungssysteme (NMS) Zugriff auf dieses Gerät haben. Auf der Startseite für die Zugriffssteuerung wird standardmäßig jeder der vier verfügbaren SNMPv1-Communities ein Eintrag zugewiesen. Sie können diese Einstellungen jedoch bearbeiten, um mehr als einen Eintrag auf eine Community anzuwenden und den Zugriff über mehrere spezifische IPv4- und IPv6-Adressen, Hostnamen oder IP-Adressmasken zu gewähren. Um die Zugriffssteuerungseinstellungen für eine Community zu bearbeiten, klicken Sie auf den Community-Namen. • Wenn Sie den Standardzugriffssteuerungseintrag für eine Community unverändert lassen, hat diese Community von jedem Standort im Netzwerk aus Zugriff auf dieses Gerät. • Wenn Sie mehrere Zugriffssteuerungseinträge für einen Communitynamen konfigurieren, erfordert das Limit von vier Einträgen, dass eine oder mehrere der anderen Communitys keinen Zugriffssteuerungseintrag haben dürfen. Wenn kein Eintrag für die Zugriffssteuerung für eine Community aufgelistet ist, hat diese Community keinen Zugriff auf dieses Gerät. **Community Name:** Der Name, den ein NMS verwenden muss, um auf die Community zuzugreifen. Die maximale Länge beträgt 15 ASCII-Zeichen. **NMS IP/Host Name:** Die IPv4- oder-IPv6-Adresse, die IP-Adressmaske oder der Hostname, die bzw. der den Zugriff durch Netzwerkmanagementstationen steuert. Ein Hostname oder eine bestimmte IP-Adresse (z.B. 149.225.12.1) ermöglicht nur dem NMS an diesem Standort den Zugriff. Durch IP-Adressen, die 255 enthalten, wird der Zugriff folgendermaßen beschränkt: • 149.225.12.**255:** Zugriff nur über ein NMS auf das 149.225.12-Segment. • 149.225.**255.255:** Zugriff nur über ein NMS auf das 149.225-Segment. • 149.**255.255.255:** Zugriff nur über ein NMS auf das 149-Segment. • 0.0.0.0 (die Standardeinstellung), die auch als 255.255.255.255 ausgedrückt werden kann:Zugriff durch ein beliebiges NMS in jedem Segment. **Access Type:** Die Aktionen, die ein NMS über die Community ausführen kann. • **Read:** Nur GETs, jederzeit ab. • **Write:** GETs jederzeit ab und SETs, wenn kein Benutzer an der Web Benutzeroberfläche oder CLI angemeldet ist. • **Write+:** GETs und SETs jederzeit ab. • **Disable:** Zu keiner Zeit GETs oder SETs.

SNMPv3

Path: Configuration > Network > SNMPv3 > *options*

Für die SNMP-Befehle GETs und SETs sowie für die Trap-Empfänger verwendet SNMPv3 ein System mit Benutzerprofilen zur Identifikation der Benutzer. Einem SNMPv3-Benutzer muss im MIB-Softwareprogramm ein Benutzerprofil zugewiesen sein, um GETs und SETs auszuführen, die MIB zu durchsuchen und Traps zu empfangen.

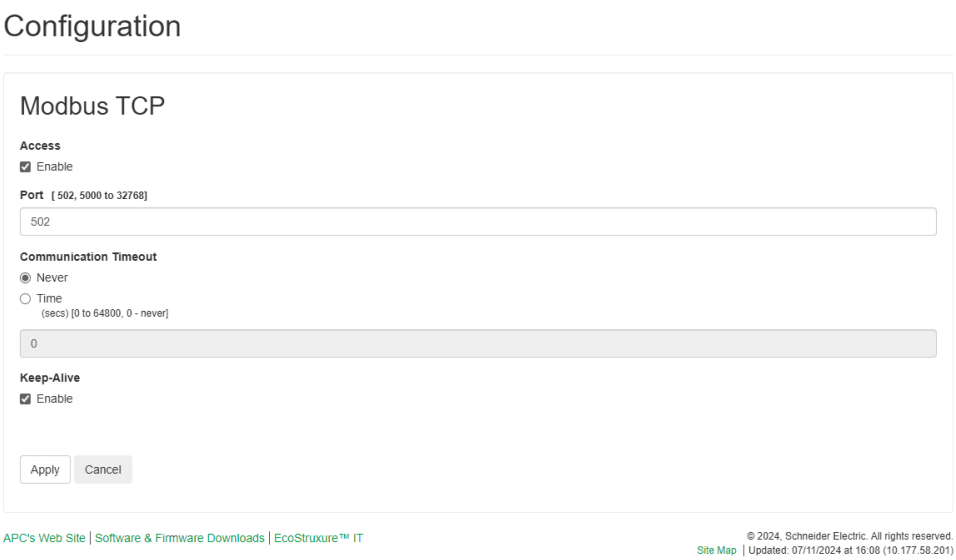
HINWEIS: SNMPv3 ist standardmäßig deaktiviert. Zur Verwendung von SNMPv3 müssen Sie ein MIB-Programm einsetzen, das SNMPv3 unterstützt. Die Rack-PDU unterstützt SHA- oder MD5-Authentifizierung und AES- oder DES-Verschlüsselung.

Option	Beschreibung
access	**SNMPv3 Access:** Aktiviert SNMPv3 als Kommunikationsmethode mit diesem Gerät.
user profiles	Standardmäßig werden die Einstellungen von vier Benutzerprofilen aufgelistet, die mit den Benutzernamen **apc snmp profile1** bis **apc snmp profile4** und ohne Authentifizierung und ohne Datenschutz (keine Verschlüsselung) konfiguriert sind. Um die folgenden Einstellungen für ein Benutzerprofil zu bearbeiten, klicken Sie auf einen Benutzernamen in der Liste. **Username:** Die Kennung des Benutzerprofils. SNMP Version 3 ordnet GETs, SETs und Traps einem Benutzerprofil zu, indem der Benutzername des Profils mit dem Benutzernamen im übertragenen Datenpaket abgeglichen wird. Ein Benutzername kann bis zu 32 ASCII-Zeichen enthalten. **Authentication Passphrase:** Ein Satz von 15 bis 32 ASCII-Zeichen, der überprüft, ob das NMS, das über SNMPv3 mit diesem Gerät kommuniziert, das NMS ist, für das es sich ausgibt, dass die Nachricht während der Übertragung nicht geändert wurde und dass die Nachricht rechtzeitig übermittelt wurde, was darauf hinweist, dass sie nicht verzögert wurde und dass sie nicht kopiert und später zu einem unangemessenen Zeitpunkt erneut gesendet wurde. **Privacy Passphrase:** Eine Phrase mit 15 bis 32 ASCII-Zeichen (standardmäßig `apc crypt passphrase`), die den Datenschutz der Daten (durch Verschlüsselung) gewährleistet, die ein NMS an dieses Gerät sendet oder von diesem Gerät über SNMPv3 empfängt. **Authentication Protocol:** Die APC by Schneider Electric-Implementierung von SNMPv3 unterstützt die SHA- und MD5-Authentifizierung. Die Authentifizierung erfolgt nur, wenn ein Authentifizierungsprotokoll ausgewählt ist. **Privacy Protocol:** Die Implementierung von SNMPv3 unterstützt AES und DES als Protokolle zum Verschlüsseln und Entschlüsseln von Daten. Der Schutz der übertragenen Daten erfordert, dass ein Datenschutzprotokoll ausgewählt wird und dass in der Anfrage vom NMS eine Datenschutzpassphrase angegeben wird. Wenn ein Datenschutzprotokoll aktiviert ist, das NMS jedoch keine Datenschutzpassphrase bereitstellt, wird die SNMP-Anforderung nicht verschlüsselt. **HINWEIS:** Sie können das Datenschutzprotokoll nicht auswählen, wenn kein Authentifizierungsprotokoll ausgewählt ist.
access control	Sie können bis zu vier Zugriffssteuerungseinträge konfigurieren, um anzugeben, welche NMS Zugriff auf dieses Gerät haben. Die Startseite für die Zugriffssteuerung weist standardmäßig jedem der vier Benutzerprofile einen Eintrag zu, aber Sie können diese Einstellungen bearbeiten, um mehr als einen Eintrag auf jedes Benutzerprofil anzuwenden, um den Zugriff über mehrere bestimmte IP-Adressen, Hostnamen oder IP-Adressmasken zu gewähren. • Wenn Sie den Standardzugriffssteuerungseintrag für ein Benutzerprofil unverändert lassen, haben alle NMS, die dieses Profil verwenden, Zugriff auf dieses Gerät. • Wenn Sie mehrere Zugriffseinträge für ein Benutzerprofil konfigurieren, erfordert das Limit von vier Einträgen, dass eines oder mehrere der anderen Benutzerprofile keinen Zugriffssteuerungseintrag haben dürfen. Wenn für ein Benutzerprofil kein Zugriffssteuerungseintrag aufgeführt ist, hat kein NMS, der dieses Profil verwendet, Zugriff auf dieses Gerät. Um die Zugriffssteuerungseinstellungen für ein Benutzerprofil zu bearbeiten, klicken Sie auf seinen Benutzernamen. **Access:** Aktivieren Sie das **Enable**, um die durch die Parameter in diesem Zugriffssteuerungseintrag festgelegte Zugriffskontrolle zu aktivieren. **Username:** Wählen Sie aus der Dropdown-Liste das Benutzerprofil aus, für das dieser Zugriffssteuerungseintrag gelten soll. Die verfügbaren Optionen sind die vier **user profile**, die Sie über die Option user profile im linken Navigationsmenü konfigurieren. **NMS IP/Host Name:** Die IP-Adresse, die IP-Adressmaske oder der Hostname, die den Zugriff durch das NMS steuern. Ein Hostname oder eine bestimmte IP-Adresse (z.B. 149.225.12.1) ermöglicht nur dem NMS an diesem Standort den Zugriff. Eine IP-Adressmaske, die 255 enthält, schränkt den Zugriff wie folgt ein: • 149.225.12.**255:** Zugriff nur über ein NMS auf das 149.225.12-Segment. • 149.225.**255.255:** Zugriff nur über ein NMS auf das 149.225-Segment. • 149.**255.255.255**: Zugriff nur über ein NMS auf das 149-Segment. • 0.0.0.0 (die Standardeinstellung), die auch als 255.255.255.255 ausgedrückt werden kann: Zugriff durch ein beliebiges NMS in jedem Segment.

Modbus TCP

Sie müssen Modbus aktivieren, damit das Gebäudemanagementsystem die Rack-PDU über Modbus TCP überwachen kann.

Path: Configuration > Network > Modbus > TCP



Access: Wählen Sie **Enable** aus, um Modbus TCP zu aktivieren.

Port: Geben Sie den Port für die TCP-Verbindung an (standardmäßig 502 oder 5000 bis 32768).

Communication Timeout: Geben Sie die Anzahl der Sekunden ein, die die Rack-PDU wartet, bevor sie die Verbindung zur Modbus Poll-Software trennt.

Keep-Alive: Wenn Sie **Enable** auswählen, sendet die Rack-PDU alle 2 hours und 75 seconds ein Paket an den Server, wenn keine andere Kommunikation erkannt wird. Dadurch wird ein Kommunikations-Timeout verhindert, wenn **Communication Timeout** auf 7.275 seconds oder mehr eingestellt ist.

Sie müssen sich abmelden, damit die Änderungen wirksam werden.

FTP-Server

Path: Configuration > Network > FTP Server

Die **FTP Server** aktivieren oder deaktivieren den Zugriff auf den FTP-Server. FTP ist standardmäßig deaktiviert.

Standardmäßig kommuniziert der FTP-Server mit der Rack PDU über TCP/IP-Port 21. Der FTP-Server verwendet sowohl den angegebenen Port als auch den Port, der eine Nummer niedriger als der angegebene Port ist.

Sie können die **Port** für zusätzliche Sicherheit auf die Nummer eines nicht verwendeten Ports von 5001 bis 32768 ändern. Benutzer müssen dann einen Doppelpunkt (:) verwenden, um die nicht standardmäßige Portnummer anzugeben. Zum Beispiel für Port 5001 und IP-Adresse 152.214.12.114, wäre der Befehl `ftp 152.214.12.114:5001`.

> **HINWEIS:** FTP überträgt Dateien unverschlüsselt. Übertragen Sie Dateien für eine höhere Sicherheit mit dem Secure Copy Protocol (SCP). Secure SHell (*SSH*) ist standardmäßig aktiviert und aktiviert SCP automatisch. SCP lässt jedoch keine Dateiübertragung zu, bis das Super-Benutzer-Standardpasswort (**apc**) geändert wurde. Wenn Sie möchten, dass eine Rack-PDU für die Verwaltung durch StruxureWare Data Center Expert zugänglich ist, muss der FTP-Serverzugriff in der Schnittstelle der PDU aktiviert sein.

Ausführliche Informationen zur Verbesserung und Verwaltung der Sicherheit Ihres Systems finden Sie im *Sicherheitshandbuch (Security Handbook)*, das unter **www.se.com** verfügbar ist.

Notification

Event Actions

Path: Configuration > Notification

Typen von Benachrichtigung:

Sie können Ereignisaktionen so konfigurieren, dass sie als Reaktion auf ein Ereignis oder eine Gruppe
von Ereignissen auftreten. Mit diesen Aktionen können Benutzer auf verschiedene Weise über das Ereignis informiert werden:

- Active, automatic notification. Die angegebenen Benutzer oder Überwachungsgeräte werden direkt angeschlossen.
  — e-mail-Benachrichtigung
  — SNMP-Traps
  — Syslog-Benachrichtigung
- Indirect notification
  — Event log. Wenn keine direkte Benachrichtigung konfiguriert ist, müssen Benutzer das Protokoll überprüfen, um festzustellen, welche Ereignisse aufgetreten sind.
  Sie können auch Systemleistungsdaten protokollieren, um sie für die Geräteüberwachung zu verwenden. Informationen zur Konfiguration und Verwendung dieser Datenprotokollierungsoption finden Sie unter
  "Logs in the Configuration Menu" in diesem Handbuch.
  — Queries (SNMP GETs)
  SNMP ermöglicht es einem NMS, Informationsabfragen durchzuführen. Für SNMPv1, bei dem Daten vor der Übertragung nicht verschlüsselt werden, ermöglicht die Konfiguration des restriktivsten SNMP-Zugriffstyps (READ) Informationsabfragen ohne das Risiko, Remote-Konfigurationsänderungen zuzulassen.

Event Actions konfigurieren

Path: Configuration > Notification > Event Actions > By Event

Standardmäßig ist die Protokollierung eines Ereignisses für alle Ereignisse ausgewählt. So definieren Sie Ereignisaktionen für
ein einzelnes Ereignis:

1. Um ein Ereignis zu finden, klicken Sie auf eine Spaltenüberschrift, um die Listen unter den **Device Events** oder **System Events** anzuzeigen.
   Oder Sie können auf eine Unterkategorie unter diesen Überschriften klicken, z.B. **Security** oder **Temperature**.
2. Klicken Sie auf den Ereignisnamen, um die aktuelle Konfiguration anzuzeigen oder zu ändern, z.B. Empfänger, die per E-Mail benachrichtigt werden sollen, oder Netzwerkverwaltungssysteme (NMS), die von SNMP-Traps benachrichtigt werden sollen. Wenn kein Syslog-Server konfiguriert ist, werden Elemente, die sich auf die Syslog-Konfiguration beziehen, nicht angezeigt.

   HINWEIS: Wenn Sie Details zu einer Ereigniskonfiguration anzeigen, können Sie die Ereignisprotokollierung oder Syslog aktivieren oder deaktivieren oder die Benachrichtigung bestimmter E-Mail-Empfänger oder Trap-Empfänger deaktivieren. Sie können jedoch keine Empfänger oder Empfänger hinzufügen oder entfernen. Informationen zum Hinzufügen oder Entfernen von Empfängern finden Sie in den folgenden Themen in diesem Handbuch:

   - Identifizieren von Syslog-Servern
   - Konfiguration > Benachrichtigung > email > Empfänger (Configuration > Notification > email >Recipients)
   - SNMP-Trap-Empfänger-Bildschirm

Path: Configuration > Notification > Event Actions > By Group

So konfigurieren Sie eine Gruppe von Ereignissen gleichzeitig:

1. Auswählen Sie, wie Ereignisse für die Konfiguration gruppiert werden sollen:

   — Wählen Sie **Events by Severity** aus, und wählen Sie dann einen oder mehrere Schweregrade aus.
   Der Schweregrad eines Ereignisses kann nicht geändert werden.

2. Klicken Sie auf **Next**, um zum nächsten Bildschirm zu gelangen, und führen Sie die folgenden Schritte aus:

   — Wählen Sie Ereignisaktionen für die Ereignisgruppe aus.
   a. Um eine Aktion außer der **Logging** (Standardeinstellung) auszuwählen, müssen Sie zuerst mindestens einen relevanten Empfänger konfiguriert haben.
   b. Wenn Sie **Logging** ausgewählt und einen Syslog-Server konfiguriert haben, wählen Sie **Event Log** oder **Syslog** auf dem nächsten Bildschirm.

3. Klicken Sie auf **Next**, um zum nächsten Bildschirm zu gelangen und Folgendes zu tun:

   — Wenn Sie im vorherigen Bildschirm **Logging** ausgewählt haben, wählen Sie **Enable Notifications** oder **Disable Notification**.
   — Wenn Sie im vorherigen Bildschirm **Email Recipients** ausgewählt haben, wählen Sie die zu konfigurierenden E-Mail-Empfänger aus.
   — Wenn Sie im vorherigen Bildschirm **Trap Receivers** ausgewählt haben, wählen Sie den zu konfigurierenden Trap-Empfänger aus.

4. Klicken Sie auf **Next**, um zum nächsten Bildschirm zu gelangen und Folgendes zu tun:

   — Wenn Sie **Logging** seinstellungen konfigurieren, zeigen Sie die ausstehenden Aktionen an und klicken Sie auf **Apply**, um die Änderungen zu akzeptieren, oder **Cancel**, um zu den vorherigen Einstellungen zurückzukehren.
   — Wenn Sie **Email Recipients** oder **Trap Receivers** konfigurieren, wählen Sie **Enable Notifications** oder **Disable Notification** und legen Sie die Benachrichtigungszeiteinstellungen fest.

5. Klicken Sie auf **Next**, um zum nächsten Bildschirm zu gelangen und Folgendes zu tun:

   — Zeigen Sie die ausstehenden Aktionen an und klicken Sie auf **Apply**, um die Änderungen zu akzeptieren, oder **Cancel**, um zu den vorherigen Einstellungen zurückzukehren.

Notification parameters: Diese Konfigurationsfelder definieren E-Mail-Parameter zum Senden von Benachrichtigungen über Ereignisse.

Sie werden normalerweise durch Klicken auf den Empfängernamen aufgerufen.

Feld	Beschreibung
Delay n time before sending	Wenn das Ereignis für die angegebene Zeit andauert, wird die Benachrichtigung gesendet. Wenn der Zustand vor Ablauf der Zeit endet, wird keine Benachrichtigung gesendet.
Repeat at an interval of *n*	Die Benachrichtigung wird wiederholt im angegebenen Intervall gesendet (standardmäßig alle 2 minutes, bis die Bedingung behoben ist).
Up to *n* times	Während eines aktiven Ereignisses wird die Benachrichtigung so oft wiederholt.
oder	
Until condition clears	Die Benachrichtigung wird wiederholt gesendet, bis die Bedingung beendet oder gelöst ist.

HINWEIS: Für Ereignisse, denen ein Löschereignis zugeordnet ist, können Sie diese Parameter auch einstellen.

E-Mail-Benachrichtigungsbildschirme

Verwenden Sie Simple Mail Transfer Protocol (SMTP), um E-Mails bei Eintritt eines Ereignisses an bis zu vier Empfänger zu senden. Um die E-Mail-Funktion verwenden zu können, müssen Sie die folgenden Einstelungen definieren:

- Die IP-Adressen der primären und optional der sekundären Domänennamensystem (DNS)-Server.
- Die IP-Adresse oder der DNS-Name für den SMTP-Server und die Absender Adresse.
- Die E-Mail-Adressen für maximal vier Empfänger.
- Sie können die Einstellung **To Address** der Option des Empfängers verwenden, um E-Mails an einen textbasierten Bildschirm zu senden.

Path: Configuration > Notification > email > Server

Dieser Bildschirm listet Ihre primären und sekundären DNS-Server auf und zeigt die folgenden Felder an:
From Address: Der Inhalt des Felds **From** in E-Mail-Nachrichten, die von der Rack PDU gesendet werden:

- Im Format **user@ [IP_address]** (wenn eine IP-Adresse als lokaler SMTP-Server angegeben ist)
- Im Format **user@domain** (wenn DNS konfiguriert ist und der DNS-Name als lokaler SMTP-Server angegeben ist) in den E-Mail-Nachrichten.

  HINWEIS: Der lokale SMTP-Server erfordert möglicherweise, dass Sie für diese Einstellung ein gültiges Benutzerkonto auf dem Server verwenden. Siehe die Serverdokumentation.

SMTP Server: Die IPv4/IPv6-Adresse oder der DNS-Name des lokalen SMTP-Servers.

HINWEIS: Diese Definition ist nur erforderlich, wenn der SMTP-Server auf **Local** eingestellt ist.

Authentication: Aktivieren Sie diese Option, wenn der SMTP-Server eine Authentifizierung erfordert.

Port: Die SMTP-Portnummer mit einem Standardwert von 25. Der Bereich reicht von 25, 465, 587, 2525, 5000 bis 32768.

Username, Password und Confirm Password: Wenn Ihr Mailserver eine Authentifizierung erfordert, geben Sie hier Ihren Benutzernamen und Ihr Passwort ein. Dies führt eine einfache Authentifizierung durch, nicht SSL/TLS.

Use SSL/TLS: Wählen Sie aus, wann Verschlüsselung verwendet wird.

- **Never:** Der SMTP-Server benötigt und unterstützt keine Verschlüsselung.
- **If Supported:** Der SMTP-Server kündigt Unterstützung für STARTTLS an, erfordert jedoch keine Verschlüsselung der Verbindung. Der STARTTLS-Befehl wird gesendet, nachdem die Ankündigung gegeben wurde.
- **Always:** Der SMTP-Server erfordert, dass der STARTTLS-Befehl bei der Verbindung zu ihm gesendet wird.
- **Implicitly:** Der SMTP-Server akzeptiert nur Verbindungen, die verschlüsselt beginnen. Es wird keine STARTTLS-Nachricht an den Server gesendet.

Require CA Root Certificate: Dies sollte nur aktiviert werden, wenn die Sicherheitsrichtlinie Ihrer Organisation keine implizite Vertrauenswürdigkeit von SSL/TLS-Verbindungen zulässt. Wenn dies aktiviert ist, muss ein gültiges CA-Stammzertifikat auf die RPDU geladen werden, damit verschlüsselte E-Mails gesendet werden können.

File Name: Dieses Feld hängt von den auf der Rack PDU installierten CA Stammzertifikaten ab und davon, ob ein CA-Stammzertifikat erforderlich ist oder nicht.

Path: Configuration > Notification > email > Recipients

Geben Sie bis zu vier E-Mail-Empfänger an. Klicken Sie auf einen Namen, um die Einstellungen zu konfigurieren.

Generation: Aktiviert (Standard) oder deaktiviert das Senden von E-Mails an den Empfänger.

To Address: Die Benutzer- und Domänennamen des Empfängers. Wenn Sie E-Mail für das Paging verwenden möchten, geben Sie die E-Mail-Adresse für das Pager-Gateway-Konto des Empfängers ein (z.B. myacct100@skytel.com).
Das Pager-Gateway generiert die Seite. Um die DNS-Suche der IP-Adresse des Mailservers zu umgehen, verwenden Sie die IP-Adresse in Klammern anstelle des E-Mail-Domänennamens, z.B. verwenden Sie jsmith@[xxx.xxx.x.xxx] anstelle von jsmith@company.com. Dies ist nützlich, wenn DNS-Lookups nicht ordnungsgemäß funktionieren.

Language: Die Sprache, in der die E-Mail-Benachrichtigung gesendet wird. Dies ist abhängig vom installierten Sprachpaket (falls zutreffend).

Port: Die SMTP-Portnummer mit einem Standardwert von 25. Der Bereich reicht von 25, 465, 587, 2525, 5000 bis 32768.

Format: Das Langformat enthält Name, Standort, Kontakt, IP-Adresse, Seriennummer des Geräts, Datum und Uhrzeit, Ereigniscode und Ereignisbeschreibung. Das kurze Format enthält nur die Ereignisbeschreibung.

Server: Wählen Sie eine der folgenden Methoden zum Weiterleiten von E-Mails aus:

- **Local:** Dies geschieht über den standortlokalen SMTP-Server. Diese empfohlene Einstellung stellt sicher, dass die E-Mail über den standortlokalen SMTP-Server gesendet wird. Die Auswahl dieser Einstellung begrenzt Verzögerungen und Netzwerkausfälle und wiederholt das Senden von E-Mails für viele Stunden. Wenn Sie die Einstellung Lokal wählen, müssen Sie auch die Weiterleitung auf dem SMTP-Server Ihres Geräts aktivieren und ein spezielles externes E-Mail-Konto einrichten, um die weitergeleitete E-Mail zu empfangen. Wenden Sie sich an Ihren SMTP-Serveradministrator, bevor Sie diese Änderungen vornehmen.
- **Recipient:** Dies ist der SMTP-Server des Empfängers. Die Rack PDU führt eine Suche nach MX-Datensätzen an der E-Mail-Adresse des Empfängers durch und verwendet diese als SMTP-Server. Die E-Mail wird nur einmal gesendet, sodass sie leicht verloren gehen kann.
- **Custom:** Diese Einstellung ermöglicht es jedem E-Mail-Empfänger, seine eigenen Servereinstellungen zu verwenden. Diese Einstellungen sind unabhängig von den oben unter "SMTP-Server" angegebenen Einstellungen.

Path: Configuration > Notification > email > SSL Certificates

Laden Sie ein E-Mail-SSL/TLS-Zertifikat auf die Rack PDU, um die Sicherheit zu erhöhen. Die Datei muss eine Erweiterung von `.crt` oder `.cer` haben. Es können bis zu fünf Dateien gleichzeitig geladen werden.

Nach der Installation werden hier auch die Zertifikatsdetails angezeigt. Ein ungültiges Zertifikat zeigt für alle Felder außer **File Name** "n/a" an.

Zertifikate können über diesen Bildschirm gelöscht werden. Alle E-Mail-Empfänger, die das Zertifikat verwenden, sollten manuell geändert werden, um den Verweis auf dieses Zertifikat zu entfernen.

Path: Configuration > Notification > email > Test

Senden Sie eine Testnachricht an einen konfigurierten Empfänger.

SNMP-Trap-Receiver Screen

Path: Configuration > Notification > SNMP Traps > Trap Receivers

Mit Einfaches Netzwerkverwaltungsprotokoll (SNMP) Traps können Sie automatisch Benachrichtigungen für wichtige Geräteereignisse erhalten. Sie sind ein nützliches Werkzeug zur Überwachung von Geräten in Ihrem Netzwerk.

Die Trap-Empfänger werden nach **NMS IP/Host Name** angezeigt, wobei NMS für Network Management System steht. Sie können bis zu sechs Trap-Empfänger konfigurieren.

Um einen neuen Trap-Empfänger zu konfigurieren, klicken Sie auf **Add Trap Receiver**. Um einen zu bearbeiten (oder zu löschen), klicken Sie auf ihre IP-Adresse/ihren Hostnamen.

Trap Generation: Aktivieren (Standardeinstellung) oder Deaktivieren der Trap-Generierung für diesen Trap-Empfänger.

NMS IP/Host Name: Die IPv4/ IPv6-Adresse oder der Hostname dieses Trap-Empfängers. Bei der Standardeinstellung 0.0.0.0 bleibt der Trap-Empfänger undefiniert.

Language: Wählen Sie eine Sprache aus der Dropdown-Liste aus. Dies kann sich von der Web-Benutzeroberfläche und von anderen Trap-Empfängern unterscheiden.

Wählen Sie entweder das Optionsfeld **SNMPv1** oder **SNMPv3**, um den Trap-Typ anzugeben. Wenn ein NMS beide Trap-Typen empfangen soll, müssen Sie für dieses NMS zwei Trap-Empfänger konfigurieren, einen für jeden Trap-Typ.

SNMPv1: Einstellungen für SNMPv1

- **Community Name:** Der Name, der als Kennung verwendet wird, wenn SNMPv1 Traps an diesen Trap-Empfänger gesendet werden.
- **Authenticate Traps:** Wenn diese Option aktiviert ist (Standardeinstellung), erhält der NMS, der durch die Einstellung NMS IP/Hostname identifiziert wird, Authentifizierungsfallen (Fallen, die durch ungültige Anmeldeversuche an diesem Gerät generiert werden).

SNMPv3: Einstellungen für SNMPv3

- **Username:** Wählen Sie die Kennung des Benutzerprofils für diesen Trap-Empfänger aus.

Wenn Sie einen Trap-Empfänger löschen, werden alle Benachrichtigungseinstellungen, die unter „Ereignisaktionen konfigurieren“ für den gelöschten Trap-Empfänger konfiguriert wurden, auf ihre Standardwerte gesetzt.

SNMP-Traps-Test-Screen

Path: Configuration > Notification > SNMP Traps > Test

Last Test Result: Das Ergebnis des letzten SNMP-Trap-Tests. Ein erfolgreicher SNMP Trap-Test überprüft nur, ob ein Trap gesendet wurde; er überprüft nicht, ob der Trap vom ausgewählten Trap-Empfänger empfangen wurde. Ein Trap-Test ist erfolgreich, wenn alle folgende Punkte wahr sind:

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

To: Wählen Sie die IP-Adresse oder den Hostnamen aus, an die ein Test-SNMP-Trap gesendet werden soll. Wenn kein **Trap Receiver** konfiguriert ist, wird ein Link zum Konfigurationsbildschirm des Trap-Empfängers angezeigt.

Allgemein-Menü

Dieses Menü enthält verschiedene Konfigurationselemente, einschließlich Geräteidentifikation, Datum und Uhrzeit, Export und Import der Konfigurationsoptionen der RPDU, die drei Links unten links auf dem Bildschirm und die Konsolidierung von Daten zur Fehlerbehebung.

Identification Screen

Path: Configuration > General > Identification

Definieren Sie den **Name**, den **Location** (den physischen location) und den **Contact** (die für das Gerät verantwortliche Person), die von:

- SNMP-Agentder Rack PDU und
- StruxureWare Data Center Expert verwendet werden.

Insbesondere wird das Feld name von den OIDs **sysName**, **sysContact** und **sysLocation** Object Identifiers (OIDs) im SNMP-Agenten der Rack PDU verwendet. Weitere Informationen zu MIB-II-OIDs finden Sie im PowerNet® *SNMP Management Information Base (MIB)-Referenzhandbuch*, verfügbar unter **www.se.com**.

Host Name Synchronization ermöglicht die Synchronisierung des Hostnamens mit dem Systemnamen, sodass beide Felder automatisch denselben Wert enthalten.

> **HINWEIS:** Wenn Sie diese Funktion aktivieren, kann der Systemnamensbezeichner kein Leerzeichen mehr enthalten (da er mit dem Hostnamenfeld synchronisiert wird).

Systemmeldung: Wenn definiert, wird eine benutzerdefinierte Meldung auf dem Anmeldebildschirm für alle Benutzer angezeigt.

Date/Time Screen

Path: Configuration > General > Date/Time > Mode

Stellen Sie die vom Gerät verwendete Uhrzeit und das Datum ein. (Beachten Sie, dass das verwendete Zeitformat nur 24 Stunden beträgt.) Sie können die aktuellen Einstellungen manuell oder über einen Netzwerkzeitprotokoll (Network Time Protocol) (NTP)-Server ändern.

Mit beiden wählen Sie die **Time Zone**. Dies ist Ihre Ortszeitdifferenz zur koordinierten Weltzeit (Coordinated Universal Time) (UTC), auch bekannt als Greenwich Mean Time (GMT).

Manual Modus

Sie haben dann folgende Möglichkeiten:

- Geben Sie Datum und Uhrzeit für das Gerät ein
- Aktivieren Sie das Kontrollkästchen **Apply Local Computer Time**, um die Datums und Uhrzeiteinstellungen des von Ihnen verwendeten Computers zu übernehmen

Mit NTP-Server synchronisieren

Einen NTP-Server (Netzwerkzeitprotokoll) bereitstellen, um Datum und Uhrzeit für die Rack PDU einzustellen. Standardmäßig erhält jede Rack PDU auf der privaten Seite eines StruxureWare Data Center Expert ihre Zeiteinstellungen, indem StruxureWare Data Center Expert als NTP-Server verwendet wird.

- **Override Manual NTP Settings:** Wenn Sie diese Option auswählen, haben Daten aus anderen Quellen (normalerweise DHCP) Vorrang vor den hier festgelegten NTP-Konfigurationen.
- **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, wenn ein sekundärer Server verfügbar ist.
- **Update Interval:** Definieren Sie in Stunden, wie oft die Rack PDU für ein Update auf den NTP-Server zugreift. Minimum: 1; Maximum: 8760 (1 Jahr).
- **Update Using NTP Now:** Initiieren Sie eine sofortige Aktualisierung von Datum und Uhrzeit durch den NTP-Server.

Daylight Saving

Path: Configuration > General > Date /Time > Daylight Saving

Die Sommerzeit (Daylight Saving Time) (DST) ist standardmäßig deaktiviert. Sie können die traditionelle Sommerzeit in den USA DST oder eine benutzerdefinierte Sommerzeit aktivieren und konfigurieren, die der Implementierung der Sommerzeit in Ihrer Region entspricht.

Beim Anpassen der Sommerzeit stellt das System die Uhr um eine Stunde vor, wenn die Uhrzeit und das Datum, die Sie unter **Start** angeben, erreicht sind, und stellt die Uhr um eine Stunde zurück, wenn die Uhrzeit und das Datum, die Sie unter **End** angeben, erreicht sind.

- Wenn Ihre lokale DST immer am vierten Vorkommen eines bestimmten Wochentags eines Monats beginnt oder endet (z.B. am vierten Sonntag), wählen Sie Vierter/Letzter. Wenn in diesem Monat ein fünfter Sonntag stattfindet, sollten Sie trotzdem Vierter/Letzter wählen.
- Wenn Ihre lokale DST immer am letzten Vorkommen eines bestimmten Wochentags eines Monats beginnt oder endet, unabhängig davon, ob es sich um das vierte oder fünfte Vorkommen handelt, wählen Sie Fünftes/Letztes.

Einstellungen mit der Konfigurationsdatei erstellen und importieren

Path: Configuration > General > User Config File

Verwenden Sie die Einstellungen von einer Rack PDU, um eine andere zu konfigurieren. Rufen Sie die config.ini-Datei aus der konfigurierten Rack-PDU ab, passen Sie diese Datei an (z.B. Ändern der IP-Adresse) und laden Sie die angepasste Datei in die neue Rack PDU hoch.
Der Dateiname kann bis zu 64 Zeichen lang sein und muss die .ini-Endung haben.

Status	Meldet den Fortschritt des Uploads. Der Upload gelingt auch dann, wenn die Datei Fehler enthält, aber ein Systemereignis meldet die Fehler im Ereignisprotokoll.
Upload	Navigieren Sie zu der angepassten Datei und laden Sie sie hoch, damit die aktuelle Rack PDU damit ihre eigene Konfiguration festlegen kann.
Download	Ermöglicht das Herunterladen der Konfigurationsdatei (config.ini) direkt über den Webbrowser auf den Computer des Benutzers übertragen.

Informationen zum Abrufen und Anpassen der Datei einer konfigurierten Rack PDU finden Sie unter So exportieren Sie Konfigurationseinstellungen in diesem Handbuch.
Anstatt die Datei auf eine Rack PDU hochzuladen, können Sie die Datei mithilfe eines FTP- oder SCP-Skripts auf mehrere Rack PDUs exportieren.

Konfigurieren von Verknüpfungen

Path: Configuration > General > Quick Links

Wählen Sie **Configuration > General > Quick Links**, um die URL-Links anzuzeigen und zu ändern, die unten links auf jeder Seite der Benutzeroberfläche angezeigt werden.

Standardmäßig greifen diese Links auf die folgenden Webseiten zu:

- **Link 1**: Die Homepage der Website von APC by Schneider Electric
- **Link 2:** Demonstrationen von webfähigen Produkten von APC by Schneider Electric
- **Link 3:** Informationen zu EcoStruxure IT

Protokolle im Konfigurationsmenü

Identifizieren vo Syslog-Servern

Path: Configuration > Logs > Syslog > Servers

Klicken Sie auf **Add Server**, um einen neuen Syslog-Server zu konfigurieren.

Syslog Server: Verwendet IPv4/ IPv6-Adressen oder Hostnamen, um einen bis vier Server für den Empfang von Syslog-Nachrichten zu identifizieren, die von der Rack PDU gesendet werden.

Port: Der Port, den die Rack PDU zum Senden von Syslog-Nachrichten verwendet. Der Syslog zugewiesene Standard-UDP-Port ist 514.

Language: Wählen Sie die Sprache für alle Syslog-Nachrichten aus.

Protocol: Wählen Sie entweder UDP oder TCP aus.

Syslog-Einstellungen

Path: Configuration > Logs > Syslog > Settings

Message Generation: Aktivieren Sie die Generierung und Protokollierung von Syslog Nachrichten für Ereignisse, für die Syslog als Benachrichtigungsmethode konfiguriert ist.

Facility Code: Wählt den Einrichtungscode aus, der den Syslog-Meldungen der Rack PDU zugewiesen ist (standardmäßig Benutzer).

> **HINWEIS:** Der **User** definiert am besten die Syslog-Nachrichten, die von der Rack PDU gesendet werden. Ändern Sie diese Auswahl nur, wenn Sie vom Syslog-Netzwerk oder Systemadministrator dazu aufgefordert werden.

Severity Mapping: In diesem Abschnitt wird jeder Schweregrad der Rack PDU oder Umgebungsereignisse den verfügbaren Syslog-Prioritäten zugeordnet. Die lokalen Optionen sind **Critical**, **Warning** und **Informational**. Sie sollten die Zuordnungen nicht ändern müssen.

- **Emergency:** Das System ist unbrauchbar
- **Alert:** Maßnahmen müssen sofort ergriffen werden
- **Critical:** Kritische Bedingungen
- **Error:** Fehlerbedingungen
- **Warning:** Warnungbedingungen
- **Notice:** Normal aber bedeutende Bedingungen
- **Informational:** Informative Nachrichten
- **Debug:** Debug-Ebene-Nachrichten

Im Folgenden sind die Standardeinstellungen für die **Local Priority** stellungen aufgeführt:

- **Critical** ist bis **Critical**
- **Warning** ist bis **Warning**
- **Informational** ist bis **Info** zugeordnet

Syslog-Test und Formatbeispiel

Path: Configuration > Logs > Syslog > Test

Senden Sie eine Testnachricht an die Syslog-Server (konfiguriert über die Option „Syslog Server identifizieren“ oben). Das Ergebnis wird an alle konfigurierten Syslog-Servern gesendet.

Wählen Sie einen Schweregrad aus, der der Testnachricht zugewiesen werden soll, und definieren Sie dann die Testnachricht. Formatieren Sie die Nachricht so, dass sie aus dem Ereignistyp (z.B. APC, System oder Gerät) gefolgt von einem Doppelpunkt, einem Leerzeichen und dem Ereignistext besteht. Die Nachricht kann maximal 50 Zeichen lang sein.

- Die Priorität (PRI): Die dem Nachrichtenereignis zugewiesene Syslog-Priorität und der Einrichtungscode der von der Rack PDU gesendeten Nachrichten.
- Der Header: ein Zeitstempel und die IP-Adresse der Rack PDU.
- Die Nachrichtteil (MSG):

  — Das **TAG-**Feld, gefolgt von einem Doppelpunkt und einem Leerzeichen, identifiziert den Ereignistyp.
  — Das CONTENT ist der Ereignistext, gefolgt (optional) von einem Leerzeichen und dem Ereigniscode.

  Beispiel:

```
APC: Test Syslog is valid.
```

Tests Tab

Einstellen des Blinkens der Networkstatus-LED oder des Geräte-LCD

Path: Tests > Network > LED Blink

Wenn Sie Probleme haben, Ihr Gerät zu finden, geben Sie eine Anzahl von Minuten in das Feld **LED Blink Duration** ein, klicken Sie auf **Apply**, und die Status-LED auf dem Display blinkt.

Path: Tests > RPDU > LCD Blink

In diesem Menü können Sie eine Anzahl von Minuten in das Feld **LCD Blink Duration** eingeben und auf **Apply** klicken, und die LCD-Hintergrundbeleuchtung beginnt zu blinken.

Logs Tab

Event-, Data- und Firewall Logs

Event Log

Path: Logs > Events

Standardmäßig zeigt das Protokoll alle Ereignisse an, die in den letzten zwei Tagen aufgezeichnet wurden, beginnend mit den neuesten Ereignissen.

Darüber hinaus zeichnet das Protokoll alle Ereignisse auf, die einen SNMP-Trap senden, mit Ausnahme von SNMP-Authentifizierungsfehlern und abnormalen internen Systemereignissen.

Sie können die Farbcodierung für Ereignisse auf dem Bildschirm **Configuration > Security > Local Users Management** lokaler Benutzer aktivieren.

Path: Logs > Events > Log

Standardmäßig zeigt das Ereignisprotokoll die neuesten Ereignisse zuerst an. Um die Ereignisse zusammen auf einer Webseite aufgelistet anzuzeigen, klicken Sie auf Launch Log in New Window.

Um das Protokoll in einer Textdatei zu öffnen oder auf der Festplatte zu speichern, klicken Sie auf das Diskettensymbol

 in derselben Zeile wie die Überschrift des **Event Log**.

Sie können auch FTP oder Secure Copy Protocol (SCP) verwenden, um das Ereignisprotokoll anzuzeigen. Siehe **FTP oder SCP zum Abrufen von Protokolldateien** in diesem Handbuch.

Event Logs filtern

Verwenden Sie die Filterung, um Informationen auszulassen, die Sie nicht anzeigen möchten.

- Filtern des Protokolls nach Datum oder Uhrzeit: Verwenden Sie die Optionsfelder **Last** oder **From**. (Die Filterkonfiguration bleibt gespeichert, bis die Rack-PDU neu gestartet wird.)
- Filtern des Protokolls nach Ereignisschweregrad oder Kategorie:
  — Klicken Sie **Filter Log**.
  — Deaktivieren Sie ein Kontrollkästchen, um es aus der Ansicht zu entfernen.
  — Nachdem Sie auf **Apply** geklickt haben, zeigt Text in der oberen rechten Ecke der **Event Log** an, dass ein Filter aktiv ist. Der Filter ist aktiv, bis Sie ihn löschen oder bis die Rack PDU neu gestartet wird.
- Entfernen eines aktives Filter:
  — Klicken Sie **Filter Log**.
  — Klicken Sie **Clear Filter (Show All)**.
  — Klicken Sie als Administrator auf **Save As Default**, um diesen Filter als neue Standardprotokollansicht für alle Benutzer zu speichern.

Wichtige Punkte zum Filtern:

- Ereignisse werden mithilfe der ODER-Logik durch den Filter verarbeitet. Wenn Sie einen Filter anwenden, funktioniert er unabhängig von den anderen Filtern.
- Ereignisse, die Sie in der Liste **Filter By Severity** gelöscht haben, werden im gefilterten **Event Log** nie angezeigt, auch wenn sie in der Liste **Filter by Category** ausgewählt sind.
- Ebenso werden Ereignisse, die Sie in der Liste Nach Kategorien filtern löschen, nie im gefilterten **Event Log** angezeigt.

Löschen Event logs

Um alle Ereignisse zu löschen, klicken Sie auf **Clear Log**. Gelöschte Ereignisse können nicht abgerufen werden.

Informationen zum Deaktivieren der Protokollierung von Ereignissen basierend auf dem zugewiesenen Schweregrad oder der Ereigniskategorie finden Sie unter **Konfigurieren von Ereignisaktionen (Configure Event Actions)** in diesem Handbuch.

Path: Logs > Events > Reverse Lookup

Wenn Reverse-Lookup aktiviert ist, werden beim Auftreten eines netzwerkbezogenen Ereignisses sowohl die IP-Adresse als auch der Domänenname für das Netzwerkgerät mit dem Ereignis im Ereignisprotokoll protokolliert. Wenn für das Gerät kein Domänennameneintrag vorhanden ist, wird nur seine IP-Adresse mit dem Ereignis protokolliert.

Da sich Domänennamen im Allgemeinen seltener ändern als IP-Adressen, kann die Reverse-Lookup-Aktivierung die Fähigkeit verbessern, Adressen von Netzwerkgeräten zu identifizieren, die Ereignisse verursachen.

Reverse-Lookup ist standardmäßig deaktiviert. Sie sollten es nicht aktivieren müssen, wenn Sie keinen DNS-Server konfiguriert haben oder eine schlechte Netzwerkleistung aufgrund von starkem Netzwerkverkehr aufweisen.

Path: Logs > Events > Size

Verwenden Sie **Event Log Size**, um die maximale Anzahl von Protokolleinträgen anzugeben.

> **HINWEIS:** Wenn Sie die Ereignisprotokollgröße ändern, um eine maximale Größe anzugeben, werden alle vorhandenen Protokolleinträge gelöscht. Wenn das Protokoll anschließend die maximale Größe erreicht, werden die älteren Einträge gelöscht.

Network Port Sharing Event Logs und Traps

Rack PDU-Ereignisse von Gast-Rack PDUs werden zur Aufnahme in das Protokoll an die Host-Rack PDU gesendet. Der Protokolleintrag enthält die Display-ID der Einheit, die das Ereignis eingetreten an. Diese Ereignisse werden dann genauso behandelt wie lokale Ereignisse von der Host-PDU. Aus diesem Grund unterstützen Alarme, SNMP-Traps, E-Mails, Syslog usw. Ereignisse der Rack-PDU und Alarme von allen Rack-PDU einer Gruppe.
Ereignisprotokoll Beispiel: `Rack PDU 4: Device low load.`

> **HINWEIS:** Systemereignisse werden nur für die Host-Rack PDU protokolliert. Systemereignisse von Gast-Rack PDUs werden nicht auf der Host-PDU protokolliert.

Data Log

Verwenden Sie das Datenprotokoll, um Messungen über die Rack PDU, die Stromzufuhr zur Rack PDU und die Umgebungstemperatur der Rack PDU anzuzeigen.

Die Schritte zum Anzeigen und Ändern der Größe des Datenprotokolls sind die gleichen wie für das Ereignisprotokoll, außer dass Sie mich verwenden, außer dass Sie Menüoptionen unter **Data** anstelle von **Events** verwenden.

Path: Logs > Data > Log

Data Logs filtern

Verwenden Sie die Filterung, um Informationen auszulassen, die Sie nicht anzeigen möchten. Mithilfe des **Network Port Sharing Data Log** ruft die Host-Rack PDU Daten von der Gast-Rack PDU ab, sodass Daten von allen Rack PDUs in einer Gruppe verfügbar sind. Um Daten von einer anderen Rack PDU in einer Gruppe anzuzeigen, wählen Sie die gewünschte Rack PDU aus der Pulldown-Liste “Filter Log” aus.

Ähnlich können Sie für die Datenprotokollgrafik eine andere Rack PDU auswählen, indem Sie auf die Schaltfläche **Change Data Filter** klicken.

- Filtern des Protokolls nach Datum oder Uhrzeit: Verwenden Sie die Optionsfelder **Last** oder **From**. (Die Filterkonfiguration bleibt gespeichert, bis die Rack-PDU neu gestartet wird.)
- Filtern des Protokolls nach Ereignisschweregrad oder Kategorie:

  — Klicken Sie **Filter Log**.

  — Deaktivieren Sie ein Kontrollkästchen, um es aus der Ansicht zu entfernen.

  — Nachdem Sie auf **Apply** geklickt haben, zeigt Text in der oberen rechten Ecke der **Data Log** an, dass ein Filter aktiv ist. Der Filter ist aktiv, bis Sie ihn löschen oder bis die Rack PDU neu gestartet wird.

- Entfernen eines aktives Filter:
  — Klicken Sie **Filter Log**.
  — Klicken Sie **Clear Filter (Show All)**.
  — Klicken Sie als Administrator auf **Save As Default**, um diesen Filter als neue Standardprotokollansicht für alle Benutzer zu speichern.

Data logs löschen

Klicken Sie auf **Clear Data Log**, um alle Datenprotokolldatensätze zu löschen. Gelöschte Datenprotokollsätze können nicht abgerufen werden.

Path: Logs > Data > Interval

Stellen Sie in der Einstellung **Log Interval** ein, wie häufig Daten gesucht und im Datenprotokoll gespeichert werden. Wenn Sie auf **Apply** klicken, wird die Anzahl der möglichen Lagertage neu berechnet und oben auf dem Bildschirm angezeigt. Wenn das Protokoll voll ist, werden die ältesten Einträge gelöscht.

> **HINWEIS:** Da das Intervall angibt, wie oft die Daten aufgezeichnet werden, gilt: je kleiner das Intervall, desto öfter werden die Daten aufgezeichnet und desto größer ist die Protokolldatei.

Data Log Graphing

Path: Logs > Data > Graphing

Die Datenprotokollgrafik bietet eine grafische Anzeige der protokollierten Daten und ist eine Erweiterung der vorhandenen Datenprotokollfunktion. Wie die Grafikverbesserung Daten anzeigt und wie effizient sie funktioniert, hängt von Ihrer Computerhardware, Ihrem Computerbetriebssystem und dem Webbrowser ab, den Sie für den Zugriff auf die Benutzeroberfläche des Geräts verwenden.

> **HINWEIS:** JavaScript® muss in Ihrem Browser aktiviert sein, um die Grafikfunktion nutzen zu können. Alternativ können Sie FTP oder SCP verwenden, um das Datenprotokoll in eine Tabellenkalkulationsanwendung zu importieren und Daten in der Tabelle grafisch darzustellen.

Graph Data: Wählen Sie die Datenelemente aus, die den abgekürzten Spaltenüberschriften im Datenprotokoll entsprechen, um mehrere Datenelemente grafisch darzustellen. Halten Sie die CTRL-Taste gedrückt, um mehrere Elemente auszuwählen.

Graph Time: Wählen Sie **Last** aus, um alle Datensätze grafisch darzustellen oder die Anzahl der Stunden, Tage oder Wochen zu ändern, für die Datenprotokollinformationen grafisch dargestellt werden. Wählen Sie eine Zeitoption aus dem Dropdown-Menü aus. Auswählen **From** zur Darstellung von Daten, die während eines bestimmten Zeitraums aufgezeichnet wurden.

> **HINWEIS**: Geben Sie die Uhrzeit im 24-hour-Format ein.

Apply: Klicken Sie auf **Apply**, um die Daten grafisch darzustellen.

Launch Graph in New Window: Klicken Sie auf **Launch Graph in New Window**, um das Datenprotokolldiagramm in einem neuen Browserfenster zu starten, das eine größere Ansicht des Diagramms bietet.

Data Log-Rotation

Path: Logs > Data > Rotation

Durch die Rotation wird der Inhalt des Datenprotokolls an die Datei angehängt, die Sie nach Name und Speicherort angeben. Verwenden Sie diese Option, um den Passwortschutz und andere Parameter einzustellen.

- **FTP Server:** Die IP-Adresse oder der Hostname des Servers, auf dem sich die Datei befindet.
- **Username/Password:** Der Benutzername mit Passwort, der zum Senden von Daten an die Repository-Datei erforderlich ist. Dieser Benutzer muss auch so konfiguriert sein, dass er Lese- und Schreibzugriff auf die Daten-Repository-Datei und das Verzeichnis (Ordner) hat, in dem sie gespeichert ist.
- **File Path:** Der Pfad zur Repository-Datei.

- **Filename:** Der Name der Repository-Datei (eine ASCII-Textdatei), z.B. datalog.txt. Neue Daten werden an diese Datei angehängt, sie werden jedoch nicht überschrieben.
- **Unique Filename:** Aktivieren Sie dieses Kontrollkästchen, um das Protokoll als *mmddyyyy_* zu speichern *<filename>.txt*, wobei Dateiname das ist, was Sie oben im Feld **Filename** angegeben haben. Alle neuen Daten werden an die Datei angehängt, aber jeder Tag hat seine eigene Datei.
- **Delay n hours between uploads:** Die Anzahl der Stunden zwischen den Uploads von Daten in die Datei (max. 24 hours).
- **Upon unsuccessful attemp, try uploading every n minutes:** Die Anzahl der Minuten zwischen den Versuchen, Daten nach einem erfolglosen Upload in die Datei hochzuladen.

  — **Up to n times:** Die maximale Häufigkeit, mit der der Upload versucht wird, nachdem er anfänglich nicht erfolgreich war.

  — Until upload succeeds: Versuchen Sie, die Datei hochzuladen, bis die Übertragung abgeschlossen ist.

Data Log Size

Path: Logs > Data > Size

Verwenden Sie **Data Log Size**, um die maximale Anzahl von Protokolleinträgen anzugeben.

HINWEIS: Wenn Sie die Größe des Datenprotokolls ändern, um eine maximale Größe anzugeben, werden alle vorhandenen Protokolleinträge gelöscht. Wenn das Protokoll anschließend die maximale Größe erreicht, werden die älteren Einträge gelöscht.

Firewall-Logs

Path: Logs > Firewall

Wenn Sie eine Firewall-Richtlinie erstellen, werden Firewall-Ereignisse hier protokolliert.

Die Informationen im Protokoll können hilfreich sein, um dem technischen Supportteam bei der Lösung von Problemen zu helfen. Protokolleinträge enthalten Informationen über den Datenverkehr und die Regelaktion (erlaubt, verworfen). Wenn diese Ereignisse hier protokolliert werden, werden sie nicht im Hauptereignisprotokoll protokolliert.

Ein Firewall-Protokoll enthält bis zu 50 der letzten Ereignisse. Das Firewall-Protokoll wird gelöscht, wenn die Verwaltungsschnittstelle neu gestartet wird.

Verwenden Sie FTP oder SCP, um Protokolldateien abzurufen

Ein Administrator oder Gerätebenutzer kann FTP oder SCP verwenden, um eine tabulatorgetrennte Ereignisprotokolldatei (`event.txt`) oder Datenprotokolldatei (`data.txt`) abzurufen und in eine Tabelle importieren.

- Die Datei meldet alle Ereignisse oder Daten, die aufgezeichnet wurden, seit das Protokoll zuletzt gelöscht oder (für das Datenprotokoll) abgeschnitten wurde, weil es die maximale Größe erreicht hat.
- Die Datei enthält Informationen, die im Ereignis- oder Datenprotokoll nicht angezeigt werden.

  — Die Version des Dateiformats (erstes Feld)

  — Datum und Uhrzeit des Abrufs der Datei

  — Die Werte für **Name**, **Contact** und **Location** sowie die IP-Adresse der Rack PDU.

  — Der eindeutige **Event Code** für jedes aufgezeichnete Ereignis (nur event.txt-Datei)

  HINWEIS: Die Rack PDU verwendet ein vierstelliges Jahr für Protokolleinträge. Möglicherweise müssen Sie in Ihrer Tabellenkalkulationsanwendung ein vierstelliges Datumsformat auswählen, um alle vier Ziffern anzuzeigen.

Wenn Sie die verschlüsselungsbasierten Sicherheitsprotokolle für Ihr System verwenden, verwenden Sie SCP, um die Protokolldatei abzurufen. Wenn Sie zur Sicherheit Ihres Systems unverschlüsselte Authentifizierungsmethoden verwenden, verwenden Sie FTP, um die Protokolldatei abzurufen.

HINWEIS: Standardmäßig ist FTP deaktiviert und SCP (über SSH) aktiviert.

Informationen zu verfügbaren Protokollen und Methoden zum Einrichten der von Ihnen benötigten Sicherheitsart finden Sie im *Sicherheitshandbuch (Security Handbook)* unter **www.se.com**.

So verwenden Sie SCP zum Abrufen der Dateien

Um die `event.txt`-Datei abzurufen, verwenden Sie den folgenden Befehl:
`scp -c` *<cipher> username@hostname_or_ip_address:*`event.txt ./event.txt`

Um die `data.txt`-Datei abzurufen, verwenden Sie den folgenden Befehl:

`scp -c` *<cipher> username@hostname_or_ip_address:*`data.txt ./data.txt`

HINWEIS:

- Dieser SCP-Befehl ist für OpenSSH. Der Befehl kann je nach verwendetem SSH-Tool unterschiedlich sein.
- Bei Verwendung von OpenSSH kann <cipher> entweder aes256-cbc oder 3des-cbc sein.

Um FTP zum Abrufen der `event.txt`- oder `data.txt`-Dateien zu verwenden

1. Geben Sie an einer Eingabeaufforderung ftp und die IP-Adresse der Rack PDU ein und drücken Sie die ENTER TASTE.
   Wenn die **Portinstellung** für die Option **FTP Server** (über das Menü **Network** auf der **Administration** festgelegt) von der Standardeinstellung (**21**) geändert wurde, müssen Sie den nicht standardmäßigen Wert im Befehl FTP verwenden. Für Windows FTP-Clients, verwenden Sie den folgenden Befehl, einschließlich Leerzeichen. (Bei einigen FTP-Clients müssen Sie einen Doppelpunkt anstelle eines Leerzeichens zwischen der IP-Adresse und dem Portnummer verwenden.)
   `ftp>open ip_address port_number`
   Um einen nicht standardmäßigen Portwert einzustellen, um die Sicherheit für den FTP-Server zu erhöhen, können Sie einen beliebigen Port zwischen 5001 und 32768 angeben.
2. Verwenden Sie den **Username** und das **Password** für Administrator- oder Gerätebenutzer, bei denen zwischen Groß- und Kleinschreibung unterschieden wird, um sich anzumelden. Für Administratoren ist **apc** die Standardeinstellung für **Username** und **Password**. Für den Gerätebenutzer sind die Standardwerte device für **Username** und **apc** für **Password**.
3. Verwenden Sie den **get**, um den Text eines Protokolls auf Ihr lokales Laufwerk zu übertragen.
   `ftp>get event.txt`

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

About Tab

About zur Rack PDU

Path: About > RPDU/Network

Die Hardwareinformationen sind für den Kundensupport von APC by Schneider Electric bei der Fehlerbehebung bei der Rack PDU hilfreich. Die Seriennummer und die MAC-Adresse sind auch auf der Rack PDU selbst verfügbar.

Firmware-Informationen für das Anwendungsmodul, APC OS (AOS) und APC Boot Monitor geben den Namen, die Firmware-Version sowie Datum und Uhrzeit der Erstellung jedes Firmware-Moduls an. Diese Informationen sind auch bei der Fehlerbehebung hilfreich und ermöglichen es Ihnen festzustellen, ob aktualisierte Firmware auf der Website www.se.com verfügbar ist.

Management Uptime ist die Zeitspanne, in der die Netzwerkverwaltungsschnittstelle kontinuierlich ausgeführt wurde.

Support Screen

Path: About > Support

Mit dieser Option können Sie verschiedene Daten in dieser Schnittstelle zu Fehlerbehebungszwecken und zur Kundenbetreuung in einer einzigen komprimierten Datei zusammenfassen. Die Daten umfassen die Ereignis- und Datenprotokolle, die Konfigurationsdatei und komplexe Debugging-Informationen.

Klicken Sie auf **Generate Logs**, um die Datei zu erstellen, und dann **Download**. Sie werden gefragt, ob Sie die komprimierte Datei anzeigen oder speichern möchten.

Device IP Configuration Wizard

Funktionen, Anforderungen und Installation

Verwendung des Assistenten zum Konfigurieren von TCP/IP-Einstellungen

Der Assistent für die Device IP Configuration Wizard kann Rack PDUs erkennen, denen keine IP-Adresse zugewiesen ist. Einmal erkannt, können Sie die IP-Adresseinstellungen für die Karten konfigurieren.

Sie können auch nach Geräten suchen, die sich bereits im Netzwerk befinden, indem Sie einen IP-Bereich eingeben, um die Suche zu definieren. Das Dienstprogramm fragt die IP Adressen im definierten Bereich ab und erkennt Rack PDUs, die bereits über eine über DHCP zugewiesene IP-Adresse verfügen.

HINWEIS: Detaillierte Informationen zum Dienstprogramm finden Sie auf der Website von APC by Schneider Electric im Abschnitt Häufig gestellte Fragen (FAQs). Gehen Sie zu **https://www.se.com/ww/en/faqs/FA156064/** um die FAQ-Seite für FA156064 aufzurufen. Sie können diese URL nach Bedarf anpassen, um auf andere FAQs zuzugreifen.

HINWEIS: Informationen zur Verwendung der DHCP-Option 12 finden Sie unter FAQ FA156110.

Systemanforderungen

Der Assistent für die Device IP Configuration Wizard ist eine Windows-Applikation, die speziell für die Fernkonfiguration der grundlegenden TCP/IP-Einstellungen von NMC entwickelt wurde. Der Assistent läuft unter Microsoft® Windows® 2000, Windows Server 2003, Windows Vista, Windows XP, Windows 7, Windows Server® 2008, Windows 8 und Windows 10 sowie Windows 2012. Dieses Dienstprogramm unterstützt Karten mit Firmware-Version 3.x.x oder höher und ist nur für IPv4.

Installation

So installieren Sie den Assistent für die Konfiguration von Geräte-IP-Adressen aus einer heruntergeladenen ausführbaren Datei:

1. Gehen Sie zu **www.se.com**.
2. Laden Sie den Assistent für die Device IP Configuration Wizard herunter.
3. Führen Sie die heruntergeladene ausführbare Datei aus.

Nach der Installation ist der Assistent für die Device IP Configuration Wizard über die Windows-Startmenüoptionen verfügbar.

So exportieren Sie Konfigurationseinstellungen

Abrufen und Exportieren der .ini-Datei

Zusammenfassung des Verfahrens

Ein Super-Benutzer/Administrator kann die .ini-Datei eines Geräts abrufen und sie auf ein anderes Gerät oder auf mehrere Geräte exportieren. Die Schritte werden unten beschrieben; Siehe Details in den folgenden Abschnitten.

1. Konfigurieren Sie ein Gerät mit den gewünschten Einstellungen und exportieren Sie diese.
2. Rufen Sie die .ini-Datei von diesem Gerät ab.
3. Passen Sie die Datei an, um zumindest die TCP / IP-Einstellungen zu ändern.
4. Verwenden Sie ein vom Gerät unterstütztes Dateiübertragungsprotokoll, um eine Kopie auf ein oder mehrere andere Geräte zu übertragen. Für eine Übertragung auf mehrere Geräte, verwenden Sie FTP oder SCP-Skript oder das Dienstprogramm für .ini-Dateien.

   HINWEIS: FTP ist standardmäßig deaktiviert.

Jedes empfangende Gerät verwendet die Datei, um seine eigenen Einstellungen neu zu konfigurieren, und löscht sie dann.

HINWEIS: Verwalten von Benutzern über config.ini - Benutzer werden nicht mehr über die config.ini in irgendeiner Form. Benutzer werden jetzt über eine separate Datei mit dem .csf-Erweiterung verwaltet. **www.se.com**.

Inhalt der .ini-Datei

Die config.ini–Datei, die Sie von einem Gerät abrufen, enthält Folgendes:

- Abschnittsüberschriften und Schlüsselwörter (nur diejenigen, die für das jeweilige Gerät unterstützt werden, von dem Sie die Datei abrufen): **Abschnittsüberschriften (Section headings)** sind Kategorienamen, die in Klammern ([ ]) eingeschlossen sind. **Schlüsselwörter (Keywords)** unter jeder Abschnittsüberschrift sind Beschriftungen, die bestimmte Geräteeinstellungen beschreiben. Jedem Schlüsselwort folgen ein Gleichheitszeichen und ein Wert (entweder der Standardwert oder ein konfigurierter Wert).
- Das `Override`-Schlüsselwort: Mit seinem Standardwert verhindert dieses Schlüsselwort den Export eines oder mehrerer Schlüsselwörter und ihrer gerätespezifischen Werte. Beispielsweise blockiert der Standardwert für `Override` (die MAC-Adresse des Geräts) im Abschnitt [`NetworkTCP/IP`] den Export von Werten für System-IP, `SubnetMask`, `DefaultGateway` und `BootMode`.

.ini und Network Port Sharing

Der .ini-Konfigurationsdienstprogramm kann Werte für alle Geräte in einer Gruppe abrufen und einstellen.
Um abwärtskompatibel zu sein, wird die Host-Rack PDU immer als die erste, "PDU_A", bezeichnet. Alle Gast-Rack PDUs werden dann basierend auf ihrer Display-ID in aufsteigender Reihenfolge bis zu PDU_Z als "PDU_B", "PDU_C" und "PDU_D" bezeichnet. Danach werden weitere PDUs als PDU_AA bezeichnet, bis PDU_FF. Daher korreliert "PDU_A" nicht unbedingt mit Anzeige-ID 1, usw.

HINWEIS: Aufgrund der großen Anzahl von Konfigurationswerten, die in einer Rack PDU-Gruppe möglich sind, kann die Verarbeitung eines .ini-Dateisatzes sehr lange dauern. Beispielsweise kann es bei einer Rack PDU-Gruppe mit 4 Einheiten, bei der sich alle Werte ändern, 30 minutes dauern, bis die Verarbeitung abgeschlossen ist.

Detaillierte Verfahren

Abrufen: Zum Einrichten und Abrufen einer zu exportierende ini-Datei:

1. Verwenden Sie nach Möglichkeit die Schnittstelle einer Rack PDU, um sie mit den zu exportierenden Einstellungen zu konfigurieren. (Bei der direkten Bearbeitung der .ini-Datei besteht die Gefahr, dass Fehler auftreten.)
2. Verwenden Sie FTP oder SCP, um die *config.ini* von der konfigurierten Rack PDU abzurufen:

   — Um FTP zu verwenden:

   a. Öffnen Sie eine Verbindung zur Rack PDU unter Verwendung ihrer IP-Adresse:
   `ftp> open ip_address`

   b. Melden Sie sich mit dem Benutzernamen und dem Passwort des Super-Benutzers/ Administrators an.

   c. Rufen Sie die *config.ini*-Datei mit den Einstellungen der Rack PDU ab:
   `ftp > get config.ini`
   Die Datei wird in den Ordner geschrieben, von dem aus Sie den FTP gestartet haben.
   Informationen zum Abrufen von Konfigurationseinstellungen von mehreren Rack PDUs und zum Exportieren in die anderen Rack PDUs finden Sie in "Versionshinweisen: .ini-Datei-Dienstprogramm, Version 2.0", verfügbar unter **www.se.com**.

— Geben Sie den folgenden Befehl ein, um SCP zu verwenden:

```
scp -c <cipher> username@hostname_or_ip_address:config.ini
./config.ini
```

Geben Sie dann das richtige Passwort ein.

HINWEIS: Dieser SCP-Befehl ist für OpenSSH. Der Befehl kann je nach verwendetem SSH-Tool unterschiedlich sein.

HINWEIS: Bei Verwendung von OpenSSH kann <*cipher*> entweder aes 256-cbc oder 3des-cbc sein

Individuelle Anpassung: Sie müssen die Datei anpassen, bevor Sie sie exportieren.

1. Verwenden Sie einen Texteditor, um die Datei anzupassen.
   - Bei Abschnittsüberschriften, Schlüsselwörtern und vordefinierten Werten wird die Groß-/Kleinschreibung nicht beachtet, bei den von Ihnen definierten Zeichenfolgenwerten wird zwischen Groß- und Kleinschreibung unterschieden.
   - Verwenden Sie benachbarte Anführungszeichen, um keinen Wert anzugeben. Zum Beispiel LinkURL1="" gibt an, dass die URL absichtlich undefiniert ist.
   - Um geplante Ereignisse zu exportieren, konfigurieren Sie die Werte direkt in der .ini-Datei.
   - Um eine Systemzeit mit der größten Genauigkeit zu exportieren, wenn die empfangende NMC 2s auf einen Netzwerkzeitprotokoll (Network Time Protocol) Server zugreifen kann, konfigurieren Sie `enabled` für `NTPEnable: NTPEnable=enabled`
   - Alternativ können Sie die Übertragungszeit reduzieren, indem Sie den Abschnitt [Systemdatum/Uhrzeit] als separaten Abschnitt exportieren .ini-Datei.
   - Um Kommentare hinzuzufügen, beginnen Sie jede Kommentarzeile mit einem Semikolon (;).
2. Kopieren Sie die angepasste Datei in einen anderen Dateinamen im selben Ordner:
   - Der Dateiname kann bis zu 64 Zeichen lang sein und muss die .ini-Endung haben.
   - Bewahren Sie die ursprüngliche angepasste Datei für die zukünftige Verwendung auf. **Die Datei, die Sie aufbewahren, ist die einzige Aufzeichnung Ihrer Kommentare.**

Übertragen der Datei auf eine einzelne Rack PDU: Um die .ini-Datei zu einer anderen Rack PDU zu übertragen, führen Sie einen der folgenden Schritte aus:

- Wählen Sie auf der Web-Benutzeroberfläche der empfangenden Rack PDU **Configuration > General > User Config File** aus. Geben Sie den vollständigen Pfad der Datei ein oder verwenden Sie Durchsuchen auf Ihrem lokalen PC.
- Verwenden Sie ein beliebiges Dateiübertragungsprotokoll, das von Rack PDUs unterstützt wird, z.B. FTP, FTP-Client, SCP oder TFTP. Im folgenden Beispiel wird FTP verwendet:

- Aus dem Ordner, der die Kopie der benutzerdefinierten .ini-Datei enthält, verwenden Sie FTP, um sich bei der Rack PDU anzumelden, in die Sie die .ini-Datei exportieren:
  `ftp> open ip_address`
- Exportieren Sie die Kopie der benutzerdefinierten .ini-Datei in das Stammverzeichnis der empfangenden Rack PDU:
  `ftp> put filename.ini`

Exportieren der Datei in mehrere Rack PDUs: Um die .ini-Datei in mehreren Rack PDUs zu exportieren:

- Verwenden Sie FTP oder SCP, schreiben Sie jedoch ein Skript, das die Schritte zum Exportieren der Datei in eine einzelne Rack PDU enthält und wiederholt.
- Verwenden Sie eine Batchdatei und das Dienstprogramm für .ini-Dateien.
- Informationen zum Erstellen der Batchdatei und zum Verwenden des Dienstprogramms finden Sie in den *Versionshinweisen: Dienstprogramm für .ini-Dateien, Version 2.0*, verfügbar unter **www.se.com**.

Das Upload-Ereignis und Fehlermeldungen

Das Ereignis und seine Fehlermeldungen

Das folgende Ereignis tritt auf, wenn die empfangende Rack PDU die .ini-Datei zum Aktualisieren ihrer Einstellungen verwendet.
`Configuration file upload complete, with number valid values`
Wenn ein Schlüsselwort, ein Abschnittsname oder ein Wert ungültig ist, ist der Upload durch die empfangende Rack PDU erfolgreich, und ein zusätzlicher Ereignistext gibt den Fehler an.

Ereignistext	Beschreibung
Configuration file warning: Invalid keyword on line *number.* Configuration file warning: Invalid value on line *number.*	Eine Zeile mit einem ungültigen Schlüsselwort oder Wert wird ignoriert.
Configuration file warning: Invalid section on line *number.*	Wenn ein Abschnittsname ungültig ist, werden alle Schlüsselwort/Wert-Paare in diesem Abschnitt ignoriert.
Configuration file warning: Keyword found outside of a section on line *number.*	Ein Schlüsselwort, das am Anfang der Datei eingegeben wird (d.h. vor Abschnittsüberschriften), wird ignoriert.
Configuration file warning: Configuration file exceeds maximum size.	Wenn die Datei zu groß ist, wird ein unvollständiger Upload durchgeführt. Verkleinern Sie die Datei oder teilen Sie sie in zwei Dateien auf und versuchen Sie erneut, sie hochzuladen.

Meldungen in config.ini

Eine Rack PDU, von der Sie die .ini-Datei herunterladen, muss erfolgreich erkannt werden, damit ihre Konfiguration einbezogen werden kann. Wenn die Rack PDU nicht vorhanden ist oder nicht erkannt wurde, enthält die config.ini-Datei unter dem entsprechenden Abschnittsnamen statt Schlüsselwörtern und Werten eine Meldung.
Zum Beispiel: `Rack PDU not discovered`
Wenn Sie nicht beabsichtigten, die Rack PDU-Konfiguration als Teil des zu exportieren .ini-Datei importieren, ignorieren Sie diese Meldungen.

Fehler, die durch überschriebene Werte generiert werden

Das `Override`-Schlüsselwort und sein Wert erzeugen Fehlermeldungen im Ereignisprotokoll, wenn es den Export von Werten blockiert. Informationen zu den außer Kraft gesetzten Werten finden Sie unter „Inhalt der .ini-Datei“ in diesem Handbuch.

Da die überschriebenen Werte gerätespezifisch sind und nicht für den Export in die anderen Rack PDUs geeignet sind, ignorieren Sie diese Fehlermeldungen. Um diese Fehlermeldungen zu vermeiden, löschen Sie die Zeilen, die `Override` enthalten, und die Zeilen, die Werte enthalten, die sie überschreiben. Die Zeile mit der Abschnittsüberschrift darf weder gelöscht noch geändert werden.

Verwandte Themen

Unter Windows-Betriebssystemen können Sie anstelle der Übertragung von .ini-Dateien den Assistent für die Konfiguration von Geräte-IP-Adressen verwenden, um die grundlegenden TCP/IP-Einstellungen der Rack PDU zu aktualisieren und andere Einstellungen über die Benutzeroberfläche zu konfigurieren.

Aktualisieren der Firmware

Wenn Sie die Firmware auf der Rack PDU aktualisieren:

- Sie erhalten die neuesten Fehlerbehebungen und Leistungsverbesserungen.
- Neue Funktionen stehen zur sofortigen Verwendung zur Verfügung.

Wenn Sie die Firmware-Versionen in Ihrem Netzwerk konsistent halten, können Sie sicherstellen, dass alle Rack PDUs dieselben Funktionen auf dieselbe Weise unterstützen.

Verwenden Sie das Firmware-Aktualisierungsprogramm

Das Sicheres NMC-System (SNS)-Tool bietet neue Firmware-Versionen, die sicherstellen, dass Ihre vernetzten Geräte vor unbekannten Bedrohungen geschützt sind (IEC 62443-4-2), mit sich entwickelnden Vorschriften konform sind und über die gesamte Lebensdauer Ihrer Hardware hinweg stabil bleiben. Weitere Informationen finden Sie unter www.apc.com/secure-nmc.

HINWEIS: Für ein Upgrade auf die Firmware-Version 3.x.x.x oder höher mit dem SNS-Tool ist ein gültiges SNS-Abonnement erforderlich. Ihr Kauf umfasst ein 1-Jahres-SNS-Abonnement, das Sie mit dem Secure NMC System-Tool aktivieren können. Sie können das SNS-Tool von www.apc.com/secure-nmc herunterladen. Weitere Informationen finden Sie im SNS-Tool - Benutzerhandbuch.

Überprüfen von Upgrades und Updates

Überprüfen Sie den Erfolg oder Misserfolg der Übertragung

Um zu überprüfen, ob ein Firmware-Update erfolgreich war, verwenden Sie den Befehl `xferStatus` in der CLI, um das letzte Übertragungsergebnis anzuzeigen, oder verwenden Sie ein SNMP GET zu **mfiletransferStatusLastTransferResult** OID.

Ergebniscodes der letzten Übertragung

Mögliche Übertragungsfehler sind, dass der TFTP- oder FTP-Server nicht gefunden wird oder der Server den Zugriff verweigert, der Server die Übertragungsdatei nicht findet oder nicht erkennt oder eine beschädigte Übertragungsdatei vorliegt.

SNMP Rückgabewert	Code	Beschreibung
1	`Successful`	Die Dateiübertragung war erfolgreich.
2	`Result not available`	Es gibt keine aufgezeichneten Dateiübertragungen.
3	`Failure unknown`	Die letzte Dateiübertragung ist aus einem unbekannten Grund nicht erfolgreich.
4	`Server inaccessible`	Der TFTP- oder FTP-Server wurde im Netzwerk nicht gefunden.
5	`Server access denied`	Der TFTP- oder FTP-Server hat den Zugriff verweigert.
6	`File not found`	Der TFTP- oder FTP-Server konnte die angeforderte Datei nicht finden.
7	`File type unknown`	Die Datei wurde heruntergeladen, aber der Inhalt wurde nicht erkannt.
8	`File corrupt`	Die Datei wurde heruntergeladen, aber mit mindestens einer falschen zyklischen Redundanzprüfung (CRC).

Versionsnummern der installierten Firmware überprüfen

Path: About > Network

Verwenden Sie die Web-Oberfläche, um die Versionen der aktualisierten Firmware-Module zu überprüfen. Sie können auch einen SNMP-GET auf die MIB II sysDescr OID verwenden. In der Befehlszeilenschnittstelle, verwenden Sie den **About**-Befehl.

Fehlerbehebung

Rack PDU-Zugriff

Bei Problemen, die weiterhin bestehen oder hier nicht beschrieben sind, wenden Sie sich an den Kundendienst von APC by Schneider Electric unter **www.se.com**.

Problem	Lösung
Nachdem ein NPS-Host auf eine neue Firmware aktualisiert wurde, zeigen die Gäste-Rack PDUs den Alarm “firmware version does not match” an.	Dies wird von der Host-PDU zu gegebener Zeit automatisch behoben. Die Ereignisse werden in der folgenden Reihenfolge protokolliert: “Remote RPDU 2 (SN: xxxxxxxxxxx) firmware version does not match.” > “Guest RPDU firmware download started.” > Guest RPDU firmware download completed.” > “Remote RPDU 2 (SN: xxxxxxxxxxx) firmware version alarm has been cleared.” > “Remote RPDU 2 (SN: xxxxxxxxxxx) communication established.”
Die Rack PDU kann nicht gepingt werden	Wenn die Status-LED der Rack PDU grün leuchtet, versuchen Sie, einen anderen Knoten im selben Netzwerksegment wie die Rack PDU anzupingen. Wenn es nicht funktioniert, ist die Rack-PDU in Ordnung. Wenn die Status-LED nicht grün leuchtet oder der Ping-Test erfolgreich verläuft, führen Sie folgende Prüfungen aus: • Überprüfen Sie alle Netzwerkverbindungen. • Überprüfen Sie die IP-Adressen der Rack PDU und des NMS. • Wenn sich das NMS in einem anderen physischen Netzwerk (oder Subnetzwerk) als die Rack PDU befindet, überprüfen Sie die IP-Adresse des Standard-Gateways (oder Routers). • Überprüfen Sie die Anzahl der Subnetzbits für die Subnetzmaske der Rack PDU.
Die Kommunikationsschnittstelle kann nicht über ein Terminalprogramm zugeteilt werden	Bevor Sie ein Terminalprogramm verwenden können, um die Rack PDU zu konfigurieren, müssen Sie jede Applikation, jeden Dienst und jedes Programm abschalten, die den Kommunikationsanschluss verwendet.
Die Befehlszeilenschnittstelle kann nicht über eine serielle Verbindung aufgerufen werden	Vergewissern Sie sich, dass Sie die Baudrate nicht geändert haben. 2400, 9600, 19200, oder 38400. Die Baudrate kann von der Netzwerkmanagement-Karte mit dem CLI-Befehl konfiguriert werden: `console –b <baud rate>` Die Standard-Baudrate ist 9600.
Remote-Zugriff auf die Befehlszeile ist nicht möglich	Vergewissern Sie sich, dass Sie die korrekte Zugriffsmethode, Telnet oder Secure SHell (SSH), verwenden. Diese Zugriffsmethoden können von einem Super-Benutzer oder Administrator aktiviert werden. Standardmäßig ist SSH aktiviert und Telnet deaktiviert. SSH und Telnet können unabhängig voneinander aktiviert/deaktiviert werden. • Bei SSH erstellt die Rack PDU möglicherweise einen Hostschlüssel. Die Erstellung des Hostschlüssels durch die Rack PDU kann bis zu einer minute dauern, und SSH ist für diese Zeit nicht zugänglich.
Kein Zugriff auf die Web Benutzeroberfläche	• Stellen Sie sicher, dass der HTTP- oder HTTPS-Zugriff aktiviert ist. • Stellen Sie sicher, dass Sie die richtige URL angeben — eine, die mit dem von der Rack PDU verwendeten Sicherheitssystem übereinstimmt. SSL/TLS erfordert **https**, nicht **http**, am Anfang der URL. • Stellen Sie sicher, dass Sie die Rack PDU anpingen können. • Überprüfen Sie, dass Sie einen Webbrowser verwenden, der vom Rack PDU unterstützt wird. • Wenn die Rack PDU gerade neu gestartet wurde und die SSL/TLS-Sicherheit eingerichtet wird, generiert die Rack PDU möglicherweise ein Serverzertifikat. Die Erstellung dieses Zertifikats durch die Rack-PDU kann bis zu einer minute dauern. Während dieser Zeit ist der SSL/TLS-Server nicht verfügbar. • Überprüfen Sie, ob die auf der Rack PDU konfigurierte Mindestprotokolleinstellung für SSL/TLS mit der in Ihrem Webbrowser aktivierten oder konfigurierten übereinstimmt. **HINWEIS:** Prüfen Sie die spezifische Fehlermeldung, die vom Browser gemeldet wird. Dies beschreibt unter Umständen das genaue Problem.

Problem	Lösung
Kommunikation über Netzwerk Portfreigabe (NPS) nicht möglich	• Wenn die Kommunikation mit Netzwerk-Portfreigabe (Network Port Sharing) nicht funktioniert, stellen Sie sicher, dass die Gesamtlänge des Netzwerkkabels zwischen bis zu 32 units nicht mehr als 10 Meter beträgt. • Wenn Sie NPS verwenden und eines oder mehrere Geräte in der Gruppe nicht sehen, überprüfen Sie, ob alle Geräte in der Gruppe dieselbe Firmware-Version verwenden. Gast-PDUs sollten Firmware-Updates von ihren Hosts erhalten, aber eine manuelle Aktualisierung von Einheiten, die auf die Firmware Revision des Hosts nicht zu reagieren scheinen, kann das Problem beheben. Sie können die entsprechenden Firmware Versionen von der APC by Schneider Electric-Website herunterladen. **www.se.com**.
Die Rack PDU meldet Alarme “Component communications lost with Phase Meter” und/oder “Communication lost”	Siehe FAQ FA168022 unter **www.se.com**.
Die Rack PDU meldet den Alarm “CAN bus off”	Siehe FAQ FA173637 unter **www.se.com**.

SNMP

Problem	Lösung
Es kann kein GET-Befehl ausgeführt werden	• Überprüfen Sie den (GET) Community-Namen für Lesezugriff (SNMPv1) oder die Benutzerprofilkonfiguration (SNMPv3). • Verwenden Sie die CLI oder die Web-Benutzeroberfläche, um sicherzustellen, dass das NMS Zugriff hat.
Es kann kein SET-Befehl ausgeführt werden	• Vergewissern Sie sich, dass SNMP aktiviert ist. SNMPv1 und SNMPv3 sind standardmäßig deaktiviert. • Überprüfen Sie den Community-Namen für Lese-/Schreibzugriff (SNMPv1) oder die Benutzerprofilkonfiguration (SNMPv3). • Verwenden Sie die CLI oder die Web-Benutzeroberfläche, um sicherzustellen, dass das NMW-Schreibzugriff (SET-Zugriff) (SNMPv1) hat oder über die Zugriffssteuerungsliste (SNMPv3) Zugriff auf die Ziel-IP-Adresse gewährt wird.
Es können am NMS keine Traps empfangen werden	• Vergewissern Sie sich, dass der Trap-Typ (SNMPv3 oder SNMPv1) ordnungsgemäß als Trap-Empfänger für das NMS konfiguriert ist. • Fragen Sie für SNMPv1 **mconfigTrapReceiverTable** MIB OID ab, um zu überprüfen, ob die NMS-IP-Adresse korrekt aufgeführt ist und ob der für den NMS definierte Community-Name mit dem Community-Namen in der Tabelle übereinstimmt. Wenn beides nicht korrekt ist, verwenden Sie SETs für **mconfigTrapReceiverTable** OIDS oder korrigieren Sie die Trap Empfängerdefinition über die Befehlszeilenschnittstelle oder die Webbenutzeroberfläche. • Überprüfen Sie für SNMPv3 die Benutzerprofil-Konfiguration für das NMS und führen Sie einen Trap-Test aus.
Am NMS empfangene Traps werden nicht identifiziert	Überprüfen Sie in Ihrer NMS-Dokumentation, ob die Traps ordnungsgemäß in die Alarm-/Trapsdatenbank integriert sind.

Protokolldateien auf ein USB-Stick herunterladen

1. Stecken Sie ein USB-Stick in den USB-Anschluss der Displayschnittstelle der Rack-PDU ein. Stellen Sie vor Beginn der Übertragung sicher, dass das USB-Laufwerk in FAT32 formatiert ist.
2. Scrollen Sie auf dem Bildschirm zu **Log to Flash** und drücken Sie die **Select**.
3. Drücken Sie die **Select** erneut, um die Protokolldateien auf Ihr USB-Stick zu exportieren.
4. Sie können den Donwload jederzeit während des Downloadvorgangs durch Drücken der **Select** abbrechen.

   HINWEIS: Wenn die Datei debug.txt oder dump.txt auf der Rack-PDU nicht vorhanden ist, kann sie nicht auf das USB-Flash-Laufwerk heruntergeladen werden. Diese Dateien werden nur nach einem unerwarteten Systemabsturz oder einem Zurücksetzen der Netzwerkmanagementkarte (NMC) erstellt. Die Dateien debug.txt und dump.txt werden nur für den technischen Support verwendet.

Copyright-Hinweis zum Quellcode

cryptlib copyright Digital Data Security New Zealand Ltd 1998.

Copyright© 1990, 1993, 1994 The Regents of the University of California. Alle Rechte vorbehalten.
Dieser Code stammt von Software, die Berkeley by Mike Olson.

Die Weitergabe und Verwendung in Quell- und Binärform mit oder ohne Änderung ist zulässig, sofern die folgenden Bedingungen erfüllt sind:

1. Weiterverbreitungen des Quellcodes müssen den obigen Urheberrechtshinweis, diese Liste der Bedingungen und den folgenden Haftungsausschluss enthalten.
2. Weiterverbreitungen in binärer Form müssen den obigen Urheberrechtshinweis, diese Liste der Bedingungen und den folgenden Haftungsausschluss in der Dokumentation und/oder anderen mit der Verteilung bereitgestellten Materialien wiedergeben.
3. Alle Werbematerialien, in denen Funktionen oder die Verwendung dieser Software erwähnt werden, müssen den folgenden Hinweis enthalten: Dieses Produkt enthält Software, die von der University of California, Berkeley und ihren Mitwirkeden entwickelt wurde.
4. Weder der Name der Universität noch die Namen ihrer Mitwirkenden dürfen ohne ausdrückliche vorherige schriftliche Genehmigung verwendet werden, um von dieser Software abgeleitete Produkte zu unterstützen oder zu bewerben.

DIESE SOFTWARE WIRD VON DEN REGENTEN UND MITWIRKENDEN „WIE BESEHEN“ ZUR VERFÜGUNG GESTELLT, UND JEGLICHE AUSDRÜCKLICHEN ODER STILLSCHWEIGENDEN GARANTIEN, EINSCHLIEßLICH, ABER NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDEN GARANTIEN DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, WERDEN ABGELEHNT. IN KEINEM FALL HAFTEN DIE REGENTEN ODER MITWIRKENDEN FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, EXEMPLARISCHE ODER FOLGESCHÄDEN (EINSCHLIEßLICH, ABER NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZGÜTERN ODER -DIENSTLEISTUNGEN; NUTZUNGS-, DATEN- ODER GEWINNVERLUST; ODER BETRIEBSUNTERBRECHUNG), UNABHÄNGIG VON DER URSACHE UND DER HAFTUNGSTHEORIE, SEI ES AUS VERTRAG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER UNERLAUBTER HANDLUNG (EINSCHLIEßLICH FAHRLÄSSIGKEIT ODER ANDERWEITIG), DIE IN IRGENDEINER WEISE AUS DER VERWENDUNG DIESER SOFTWARE ENTSTEHEN, SELBST WENN AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WURDE.

Hochfrequenzstörungen

USA—FCC

Dieses Gerät wurde getestet und entspricht den Grenzwerten für digitale Geräte der Klasse A gemäß Abschnitt 15 der FCC-Vorschriften. Diese Grenzwerte bieten hinreichenden Schutz gegen schädliche Störungen, wenn das Gerät in einer kommerziellen Umgebung betrieben wird. Dieses Gerät erzeugt, verwendet und kann Hochfrequenzenergie abstrahlen und kann, wenn es nicht in Übereinstimmung mit dieser Bedienungsanleitung installiert und verwendet wird, schädliche Störungen der Funkkommunikation verursachen. Der Betrieb dieses Geräts in einem Wohngebiet kann schädliche Störungen verursachen. Der Benutzer trägt die alleinige Verantwortung für die Behebung solcher Störungen.

Kanada—ICES

Dieses digitale Gerät der Klasse A erfüllt die Anforderungen der kanadischen Norm ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada

APC
70 Mechanic Street
02035 Foxboro, MA
USA

www.se.com

Da sich Normen, Spezifikationen und Design von Zeit zu Zeit ändern,
fragen Sie bitte nach einer Bestätigung der in dieser Publikation gemachten Angaben.

DE TME47353B