

Befehlszeilenhandbuch

UPS Network Management Card 2

AP9630, AP9631, AP9635

**990-4879K-005
05/2022**

Rechtlicher Hinweis von Schneider Electric

Schneider Electric garantiert nicht für die Verbindlichkeit, Richtigkeit oder Vollständigkeit der Informationen in diesem Handbuch. Diese Veröffentlichung stellt keinen Ersatz für einen ausführlichen betrieblichen und standortspezifischen Entwicklungsplan dar. Daher übernimmt Schneider Electric keinerlei Haftung für Schäden, Gesetzesübertretungen, unsachgemäße Installationen, Systemausfälle oder sonstige Probleme, die aus der Verwendung dieser Publikation resultieren können.

Die in dieser Veröffentlichung enthaltenen Informationen werden ohne Gewähr bereitgestellt und wurden ausschließlich zu dem Zweck zusammengestellt, den Entwurf und Bau von Datenzentren zu bewerten. Diese Publikation wurde in gutem Glauben durch Schneider Electric zusammengestellt. Wir übernehmen jedoch keine Haftung oder Gewährleistung – weder ausdrücklich noch stillschweigend – für die Vollständigkeit oder Richtigkeit der Informationen in dieser Veröffentlichung.

KEINESFALLS HAFTEN SCHNEIDER ELECTRIC, MUTTER-, SCHWESTER- ODER TOCHTERGESELLSCHAFTEN VON SCHNEIDER ELECTRIC ODER DEREN JEWELIGE VERANTWORTLICHE, DIREKTOREN ODER MITARBEITER FÜR DIREKTE, INDIREKTE, IN DER FOLGE ENTSTANDENE, SCHADENERSATZFORDERUNGEN BEGRÜNDENDE, SPEZIELLE ODER BEILÄUFIG ENTSTANDENE SCHÄDEN (AUCH NICHT FÜR ENTGANGENE GESCHÄFTE, VERTRÄGE, EINKÜNFTE ODER VERLORENE DATEN BZW. INFORMATIONEN SOWIE UNTERBRECHUNGEN VON BETRIEBSABLÄUFEN, UM NUR EINIGE ZU NENNEN), DIE AUS ODER IN VERBINDUNG MIT DER VERWENDUNG ODER UNMÖGLICHKEIT DER VERWENDUNG DIESER PUBLIKATION ODER IHRER INHALTE RESULTIEREN ODER ENTSTEHEN KÖNNEN, UND ZWAR AUCH DANN NICHT, WENN SCHNEIDER ELECTRIC VON DER MÖGLICHKEIT SOLCHER SCHÄDEN AUSDRÜCKLICH UNTERRICHTET WURDE. SCHNEIDER ELECTRIC BEHÄLT SICH DAS RECHT VOR, HINSICHTLICH DER PUBLIKATION, IHRES INHALTS ODER FORMATS JEDERZEIT UNANGEKÜNDIGT ÄNDERUNGEN ODER AKTUALISIERUNGEN VORZUNEHMEN.

Das Urheberrecht, das Recht am geistigen Eigentum und alle anderen Eigentumsrechte an den vorliegenden Inhalten (auch in Form von Software, Ton- und Videoaufzeichnungen, Text und Fotografien, um nur einige zu nennen) verbleibt bei Schneider Electric oder seinen Lizenzgebern. Alle Rechte am Inhalt, die hierin nicht ausdrücklich eingeräumt werden, bleiben vorbehalten. Es werden keine Rechte jeglicher Art an Personen lizenziert, zugewiesen oder anderweitig übertragen, die Zugang zu diesen Informationen haben.

Diese Veröffentlichung darf nicht – weder vollständig noch teilweise – weiterverkauft werden.

Command Line Interface (CLI)

Vorgehensweise zur Anmeldung

Übersicht

Für den Zugriff auf die Befehlszeile können Sie entweder eine lokale, serielle Verbindung oder eine Remote-Verbindung (über Telnet oder SSH) über einen im selben Netzwerk wie die Netzwerkmanagement-Karte (Network Management Card – NMC) befindlichen Computer verwenden.



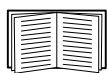
Für den Zugriff auf die im vorliegenden Benutzerhandbuch beschriebene Befehlszeilenoberfläche muss auf der Netzwerkmanagement-Karte die Smart-UPS- oder Single Phase Symmetra-Firmware installiert sein und die Netzwerkmanagement-Karte muss in einem USV-Modell der Reihe Smart-UPS oder Single Phase Symmetra eingebaut sein. Weitere Informationen zu USV-Modellen, die mit Ihrer Netzwerkmanagement-Karte 2 kompatibel sind, finden Sie im Knowledge Base-Artikel [FA237786](#) unter www.apc.com/support.

Geben Sie zur Anmeldung den Benutzernamen und das Kennwort unter Beachtung der Groß-/Kleinschreibung ein (Standardwerte: **apc** und **apc** für einen Superuser oder Administrator). Der Standardbenutzername für einen Gerätebenutzer ist **device**. Benutzer „schreibgeschützt“ kann nicht auf die Befehlszeile zugreifen.

HINWEIS: Ab Version v6.8.0 werden Sie aufgefordert, ein neues Passwort zu erstellen, wenn Sie sich erstmalig über das Superuser-Konto auf der Netzwerkmanagement-Karte einloggen.

Sicherheitssperre. Wenn ein Benutzername aufeinander folgend für die in der Web-Oberfläche der Netzwerkmanagement-Karte unter **Configuration** (Konfiguration) > **Security** (Sicherheit) > **Local Users** (Lokale Benutzer) > **Default Settings** (Standardeinstellungen) festgelegte Anzahl mit einem ungültigen Passwort verwendet wird, wird das Konto Benutzer „Gerät“ gesperrt, bis ein Superuser oder Administrator das Konto erneut aktiviert.

Weitere Informationen zu diesen Optionen finden Sie im *Benutzerhandbuch* für die USV-Netzwerkmanagement-Karte 2 (für AP9630, AP9631, AP9635) auf der [APC-Website](#).



Sollten Sie Ihren Benutzernamen oder Ihr Kennwort vergessen lesen Sie bitte die Anleitung unter „Wiederherstellen des Zugriffs bei vergessenem Kennwort“ im *Benutzerhandbuch* auf der [APC-Website](#).

Remote-Zugriff auf die Befehlszeilenoberfläche

Sie können über Telnet oder SSH auf die Befehlszeile zugreifen. In Version v6.8.0 und neuer ist nur SSH standardmäßig deaktiviert.

Zum Aktivieren oder Deaktivieren dieser Zugriffsmethoden verwenden Sie die Weboberfläche. Wählen Sie im Menü **Konfiguration** die Option **Network** (Netzwerk) > **Console** (Konsole) > **Access** (Zugriff) aus.



Sie können den Zugriff auf die Befehlszeile über Telnet oder SSH ebenfalls aktivieren bzw. deaktivieren. Siehe „console“ auf Seite 15.

SSH für den Zugriff auf hoher Sicherheitsstufe. Wenn Sie für die Weboberfläche den hohen Sicherheitsstandard von SSL/TLS nutzen möchten, verwenden Sie SSH für den Zugriff auf die Befehlszeile. SSH verschlüsselt Benutzernamen, Kennwörter und die übertragenen Daten. Die Schnittstelle, die Benutzerkonten und die Zugriffsrechte des Benutzers sind immer gleich, unabhängig davon, ob der Zugriff auf die Befehlszeile über SSH oder Telnet erfolgt. Um SSH verwenden zu können, müssen Sie SSH jedoch zuerst konfigurieren und einen SSH-Client auf dem Computer installieren. Durch die Aktivierung von SSH wird auch SCP (Secure Copy) für die sichere Dateiübertragung aktiviert. Verwenden Sie den folgenden Beispielbefehl, um per SSH auf die Netzwerkmanagement-Karte zuzugreifen:

```
ssh -c 3des-cbc apc@156.205.14.141
```

HINWEIS: Dieser SSH-Befehl gilt für OpenSSH. Der Befehl kann je nach verwendetem SSH-Tool abweichen.

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

So greifen Sie über Telnet auf die Befehlszeile zu:

1. Öffnen Sie eine Befehlszeile auf einem Computer mit Zugriff auf das Netzwerk, in dem die NMC installiert ist, und geben Sie `telnet` und die IP-Adresse der NMC ein (z. B. `telnet 139.225.6.133`, wenn die NMC den standardmäßigen Telnet-Port 23 verwendet) und betätigen Sie die EINGABETASTE.

HINWEIS: Dieses Beispiel gilt für befehlszeilenbasierte Telnet-Clients. Dieser Befehl kann sich bei anderen Telnet-Clients unterscheiden.

Wenn die NMC einen Nicht-Standard-Port (zwischen 5000 und 32768) verwendet, müssen Sie je nach Telnet-Client einen Doppelpunkt oder ein Leerzeichen zwischen der IP-Adresse (oder dem DNS-Namen) und der Port-Nummer einfügen. (Diese Befehle funktionieren in den meisten Fällen; bestimmte Clients erlauben jedoch keine Port-Eingabe als Argument und einige Linux-Varianten benötigen eventuell zusätzliche Befehle).

2. Geben Sie Benutzernamen und Kennwort ein.

Zugriff auf die Befehlszeilenoberfläche über eine Einwählverbindung (nur AP9635). Gehen Sie zum Einwählen in die Befehlszeilenoberfläche der Netzwerkmanagement-Karte AP9635 über ein Modem wie folgt vor:

1. Schließen Sie ein aktives Telefonkabel (RJ-11) an die Modem-Schnittstelle an der Frontplatte der AP9635 an.
2. Um die Telefonnummer, die dem mit der AP9635-Karte verbundenen Kabel zugewiesen ist, zu wählen, verwenden Sie auf dem mit einem Modem verbundenen Computer eine Modem-Terminalsoftware (z. B. Terminal-Emulatorprogramme Dritter wie HyperTerminal oder Tera Term).
3. Sobald die Verbindung hergestellt ist, öffnet die Modem-Terminalsoftware ein Befehlszeilenterminal. Geben Sie bei entsprechender Aufforderung Benutzernamen und Kennwort ein.

Konfiguration der Modemeinstellungen der Netzwerkmanagement-Karte AP9635.

Die Konfiguration des AP9635-Modems ist ausschließlich in der INI-Konfigurationsdatei enthalten.



Weitere Informationen zur direkten Bearbeitung der INI-Konfigurationsdatei finden Sie unter „Abrufen und Exportieren der INI-Datei – Anpassen“ im Benutzerhandbuch der Netzwerkmanagement-Karte auf der [APC-Website](#).

Die Modemeinstellungen werden folgendermaßen in der INI-Konfigurationsdatei vorgenommen:

1. Öffnen Sie die INI-Konfigurationsdatei in einem Texteditor
2. Gehen Sie zur Abschnittsüberschrift `[SystemModem]` und aktualisieren Sie folgende Einstellungen:

Option	Argument	Beschreibung
ConsoleDialIn	enabled disabled	Aktivieren Sie diese Option, um die Remote-Einwählverbindung über Modem mit der Befehlszeilenoberfläche zu erlauben. Standardmäßig aktiviert.
InitString	[AT command] [& Command] [MNP Command]	Die InitString-Option akzeptiert die Optionen des Hayes-Standardprotokolls. Der InitString muss nicht bearbeitet werden. Die Standardeinstellung ist [AT&F0E0].
Country	Text-Zeichenkette	Dient zur Kennzeichnung des Lands der Einwählnummer des an die Netzwerkmanagement-Karte angeschlossenen aktiven Telefonkabels.
DialBack	enabled disabled	Aktivieren Sie diese Option, wenn das NMC-Modem beim Empfang einer Einwählaufforderung auflegen und die entsprechende Nummer zurückrufen soll. DialBack ist standardmäßig deaktiviert.
DialBackString	Telefonnummer	Wenn DialBack aktiviert ist, handelt es sich hierbei um die Telefonnummer, die zurückgerufen wird, wenn die NMC eine Einwählaufforderung empfängt.

Lokaler Zugriff auf die Befehlszeile

Sie können über einen lokalen Computer, der über die serielle Konsolenschnittstelle der Netzwerkmanagement-Karte mit dieser verbunden ist, auf die Befehlszeile zugreifen:

1. Wählen Sie eine serielle Schnittstelle auf dem Computer aus und deaktivieren Sie sämtliche Dienste, die diese Schnittstelle verwenden.
2. Verbinden Sie das mitgelieferte serielle Kabel (Teilenummer 940-0299) mit dem am Computer ausgewählten Anschluss und dem Konfigurationsanschluss der NMC.
3. Führen Sie ein Terminalprogramm (z. B. Terminal-Emulatorprogramme Dritter wie HyperTerminal, PuTTY oder Tera Term) aus und konfigurieren Sie die ausgewählte Schnittstelle mit 9600 Bit/s, 8 Datenbits, keinem Paritätsbit, 1 Stoppbit und ohne Datenflusskontrolle.
4. Betätigen Sie die EINGABETASTE. Geben Sie hinter den entsprechenden Eingabeaufforderungen Ihren Benutzernamen und Ihr Kennwort ein.

Hauptbildschirm

Beispiel für die Hauptmaske

Die nachfolgende Abbildung zeigt ein Beispiel für die Anzeige, die erscheint, wenn Sie sich über die Befehlszeile bei der Netzwerkmanagement-Karte (NMC) anmelden.

```
Schneider Electric                      Network Management Card AOS  vx.x.x
(c)Copyright 2019 All Rights Reserved Symmetra APP                      vx.x.x
-----
Name      : Test Lab                      Date : 10/30/2018
Contact   : Don Adams                    Time : 5:58:30
Location  : Building 3                   User  : Super User
Up Time   : 0 Days, 21 Hours, 21 Minutes Stat : P+ N4+ N6+ A+
-----

                        Network Protocols Configuration Summary
-----
Protocol   | Status   | Protocol   | Status   | Protocol   | Status
-----
HTTP       | disabled | HTTPS      | enabled  | FTP        | enabled
Telnet     | disabled | SSH/SFTP   | enabled  | SNMPv1     | enabled
SNMPv3     | disabled | Modbus TCP | enabled  |            |
IPv6       | disabled | IPV4       | enabled  | Ping       | enabled
-----

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

apc>
```

Informations- und Statusfelder

Informationsfelder in der Hauptanzeige.

- Zwei Felder enthalten Angaben zu den Firmware-Versionen des American Power Conversion-Betriebssystems (AOS) und der Anwendung (APP). Der Name der Anwendungs-Firmware identifiziert das Gerät, das über diese Netzwerkmanagement-Karte mit dem Netzwerk verbunden ist. Im vorstehenden Beispiel verwendet die Netzwerkmanagement-Karte die Anwendungs-Firmware für eine Symmetra USV.

Network Management Card AOS vx.x.x
Symmetra APP vx.x.x

- Drei Felder identifizieren den Systemnamen, eine Kontaktperson und den Standort der Netzwerkmanagement-Karte.

Name : Test Lab
Contact : Don Adams
Location : Building 3

- Im Feld „Up Time“ können Sie die Betriebszeit der Management-Oberfläche der Netzwerkmanagement-Karte seit dem letzten Einschalten oder Zurücksetzen ablesen.

Up Time : 0 Days 21 Hours 21 Minutes

- Zwei Felder geben Datum und Uhrzeit Ihrer aktuellen Anmeldung an.

Date : 10/30/2018
Time : 5:58:30

- Das Feld „User“ zeigt an, ob Sie sich als **Super User**, **Administrator**, **Gerätemanager**, **Nur-Netzwerk-Benutzer**, oder **Benutzer „schreibgeschützt“** angemeldet haben.

(Der **Benutzer „schreibgeschützt“** kann auf die Befehlszeile nicht zugreifen.)

Wenn Sie sich als Gerätebenutzer (auf der Benutzeroberfläche als „Benutzer 'device“ bezeichnet) angemeldet haben, können Sie auf das Ereignisprotokoll zugreifen, bestimmte USV-Einstellungen konfigurieren und sich die Zahl der aktiven Alarmer ansehen.

User : Super User

Statusfelder in der Hauptmaske.

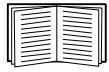
- Das Feld **Stat** zeigt den Status der Netzwerkmanagement-Karte an. Der mittlere Status variiert in Abhängigkeit davon, ob IPv4, IPv6 oder beides aktiv ist, wie in der zweiten Tabelle unten angegeben.

Stat : P+ N+ A+

P+	Das Betriebssystem (AOS) funktioniert einwandfrei.
----	--

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

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



Sollte der Wert P+ nicht angezeigt werden, wenden Sie sich bitte an den Kundendienst unter <http://www.apc.com/site/support/>.

Arbeiten mit der Befehlszeile

Übersicht

Die Befehlszeile bietet Optionen zum Konfigurieren der Netzwerkeinstellungen und zum Verwalten der USV und ihrer Netzwerkmanagement-Karte (NMC).

Eingabe von Befehlen

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

Beim Arbeiten mit der Befehlszeile haben Sie auch folgende Möglichkeiten:

- Geben Sie `?` ein und betätigen Sie die EINGABETASTE, um eine Liste der für Ihren Kontotyp verfügbaren Befehle angezeigt zu bekommen.

Informationen zur Funktion und Syntax eines bestimmten Befehls erhalten Sie, wenn Sie den Befehl, dahinter ein Leerzeichen und `?` bzw. das Wort `help` eingeben. Wenn Sie sich beispielsweise die Konfigurationsoptionen für `RADIUS` ansehen möchten, geben Sie Folgendes ein:

```
radius ?  
oder  
radius help
```

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

Befehlssyntax

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

Syntaxbeispiele

Ein Befehl, der mehrere Optionen haben kann:

```
user -n <Benutzername> -pw <Benutzerpasswort>
```

Hier wird im Befehl des Benutzers sowohl die Option `-n`, wodurch der Benutzername festgelegt wird, als auch die Option `-pw`, wodurch das Passwort geändert wird, akzeptiert.

Wenn Sie beispielsweise das Passwort in XYZ ändern möchten, geben Sie Folgendes ein:

```
user -n apc -pw XYZ
```

HINWEIS: Für Super User ist bei einer Remote-Passwortänderung zudem das aktuelle Passwort erforderlich. Siehe Abschnitt „user“.

Ein Befehl, der zu einer Option mehrere sich gegenseitig ausschließende Argumente akzeptiert:

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

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

```
alarmcount -p critical
```

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

Befehlsrückgabe-Codes

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

Die Befehlszeile meldet die Verarbeitung aller Befehle im folgenden Format:

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

Code	Fehlermeldung
E000	Erfolg
E001	Erfolgreich ausgeführt
E002	Befehl wird erst nach Neustart wirksam
E100	Befehl fehlgeschlagen
E101	Befehl nicht gefunden
E102	Parameterfehler
E103	Befehlszeilenfehler
E104	Wegen fehlender Benutzerrechte zurückgewiesen
E105	Befehl vorbelegt
E106	Daten nicht verfügbar
E107	Serielle Kommunikation mit der USV unterbrochen
E108	EAPoL durch ungültiges/verschlüsseltes Zertifikat deaktiviert

Beschreibung der Befehle



Die Verfügbarkeit der unten stehenden Befehle und Optionen kann für verschiedene USV-Geräte unterschiedlich sein.

?

Zugriff: Superuser, Administrator, Gerätebenutzer

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

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

`alarmcount ?`

info

Zugriff: Super User, Administrator, Gerätebenutzer, Nur-Netzwerk-Benutzer, Benutzer „schreibgeschützt“

Beschreibung: Zum Anzeigen von Hardware- und Firmware-Informationen. Diese Informationen sind bei der Fehlersuche nützlich und können verwendet werden, um auf der Website nach etwaigen Firmware-Updates zu suchen.

alarmcount

Zugriff: Superuser, Administrator, Gerätebenutzer, Schreibgeschützt

Beschreibung:

Option	Argumente	Beschreibung
-p	all	Zeigt die Anzahl der von der Netzwerkmanagement-Karte gemeldeten aktiven Alarmer an. Nähere Informationen zu den einzelnen Alarmen finden sich im Ereignisprotokoll.
	warning	Zeigt die Anzahl der aktiven Warnungen an.
	kritisch	Zeigt die Anzahl der aktiven kritischen Alarmer an.

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

`alarmcount -p warning`

bacnet

Zugriff: Superuser, Administrator, Gerätebenutzer

Beschreibung: Anzeigen und definieren der BACnet-Einstellungen.



Weitere Informationen zu den USV-Datenpunkten, die über BACnet bereitgestellt werden, finden Sie in den BACnet-Anwendungstabellen auf der [APC-Website](#).

Option	Argumente	Beschreibung
-S	enable disable	Wählen Sie diese Option aus, um BACnet zu aktivieren oder zu deaktivieren. Wenn BACnet deaktiviert ist, kann über BACnet nicht auf die Netzwerkmanagement-Karte zugegriffen werden. BACnet ist standardmäßig deaktiviert. HINWEIS: In Version v6.8.0 und neuer kann BACnet erst aktiviert werden, nachdem das Passwort für die Gerätekommunikationskontrolle („- pw“) eingerichtet wurde.
-d	0-4194303	Eine eindeutige Bezeichnung für diese BACnet-Gerät, welche zur Adressierung des Geräts verwendet wird.
-n	<Gerätename>	Ein Name für dieses BACnet-Gerät, der im BACnet-Netzwerk eindeutig sein muss. Der standardmäßige Gerätename ist „BACn“ und die letzten acht Ziffern der MAC-Adresse der Netzwerkmanagement-Karte. Die Länge muss zwischen 1 und 150 Zeichen betragen. Sonderzeichen sind erlaubt.
-t	1000 - 30000	Legt das APDU-Timeout fest. Das ist die Länge der Zeit in Millisekunden, während der die Netzwerkmanagement-Karte auf die Antwort einer BACnet-Anfrage wartet. Der Standardwert ist 6000.
-r	0 - 10	Legt die APDU-Wiederholungen fest. Das ist die Anzahl der BACnet-Wiederholungsversuche, welche die Netzwerkmanagement-Karte durchführt, bevor die Anfrage abgebrochen wird. Der Standardwert ist 3.
-pw	<Passwort>	Der Device-Communication-Control-Dienst wird von einem BACnet-Client verwendet, um ein Remotegerät (z. B. eine BACnet-fähige Netzwerkmanagement-Karte) anzuweisen, für einen festgelegten Zeitraum die Initiierung oder Beantwortung aller APDUs (außer des Device-Communication-Control-Dienstes) anzuhalten. Dieser Dienst kann zur Diagnose eingesetzt werden. Legen Sie das Device-Communication-Control-Passwort fest und stellen Sie damit sicher, dass ein BACnet-Client nur dann die BACnet-Kommunikation einer Netzwerkmanagement-Karte steuern kann, wenn das hier festgelegte Passwort angegeben wird. Das Passwort muss zwischen 8 und 20 Zeichen lang sein und Folgendes enthalten: <ul style="list-style-type: none"> • Eine Zahl • Einen Großbuchstaben • Einen Kleinbuchstaben • Ein Sonderzeichen Es wird empfohlen, das Passwort bei der Erstaktivierung von BACnet zu aktualisieren. Sie können das Passwort aktualisieren, ohne das aktuelle Passwort zu kennen.
BACnet-IP-Einstellungen:		
-o	47808, 5000-65535	Legt den UDP-/IP-Port fest, den die Netzwerkmanagement-Karte zum Senden und Empfangen von BACnet-/IP-Nachrichten verwendet. HINWEIS: Die Adresse einer BACnet-/IP-fähigen Netzwerkmanagement-Karte besteht aus der IP-Adresse der Netzwerkmanagement-Karte und dem lokalen Port.

Option	Argumente	Beschreibung
-fdre	enable disable	Wenn Sie dies aktivieren, können Sie die Netzwerkmanagement-Karte bei einem BBMD (BACnet Broadcast Management Device) registrieren. HINWEIS: Sie müssen Ihre Netzwerkmanagement-Karte als fremdes Gerät bei einem BBMD registrieren, wenn sich gerade kein BBMD auf dem Subnetz der Netzwerkmanagement-Karte befindet oder wenn die Netzwerkmanagement-Karte einen anderen lokalen Port zum BBMD verwendet. Weitere Informationen zur Registrierung fremder Geräte erhalten Sie im Benutzerhandbuch für die Netzwerkmanagement-Karte auf der APC-website .
-rip	IP-Adresse	Die IP-Adresse oder der FQDN (Fully Qualified Domain Name) des BBMD, mit der/dem diese Netzwerkmanagement-Karte registriert wird.
-rpo	5000 - 65535	Der Port des BBMD, mit dem diese Netzwerkmanagement-Karte registriert wird.
-fdrttl	1-65535	Die Dauer in Sekunden (Time To Live), für die das BBMD die Netzwerkmanagement-Karte als registriertes Gerät beibehält. Wenn die Netzwerkmanagement-Karte nicht vor Ablauf dieser Zeit erneut registriert wird, löscht das BBMD sie aus der eigenen Tabelle mit den fremden Geräten. Die Karte kann dann keine Broadcastmeldungen mehr über das BBMD senden oder empfangen.

Beispiel:

```

bacnet
E000: Success
Enabled: yes
Device ID: 1013
Device name: BACnB7D7E5F2
Network Protocol: BACnet/IP
APDU timeout (ms): 6000
APDU retries: 3
IP Port: 47808 (0xBAC0)
Registration Enabled: no
Registration Status: Foreign device registration inactive
Registration BBMD: 0.0.0.0
Registration BBMD port: 47808 (0xBAC0)
Registration TTL: 7200

```

boot

Zugriff: Super User, Administrator, Nur Netzwerk

Beschreibung: Hiermit legen Sie fest, wie die Netzwerkmanagement-Karte ihre Netzwerkeinstellungen (IP-Adresse, Subnetzmaske, Standardgateway) beziehen soll. Konfigurieren Sie anschließend die Einstellungen für den BOOTP- oder DHCP-Server.

Option	Argument	Beschreibung
-b <boot mode>	dhcp bootp manual	Hiermit legen Sie fest, wie die TCP/IP-Einstellungen beim Einschalten, beim Zurücksetzen oder bei einem Neustart der Netzwerkmanagement-Karte konfiguriert werden sollen.

Option	Argument	Beschreibung
-c	enable disable	Nur für die Startmethode <code>dhcp</code> . Hiermit aktivieren oder deaktivieren Sie die Vorschrift, dass der DHCP-Server das APC-Cookie bereitstellen muss.
-r	1-99	Hiermit geben Sie an, in welchen Abständen (in Stunden) die Netzwerkmanagement-Karte ihre Netzwerkeinstellungen abrufen soll. Verwenden Sie 0, um diese Option zu deaktivieren.
-f	always once	Hiermit definieren Sie, wie oft die Netzwerkmanagement-Karte die DHCP-Boot-Datei abrufen soll.
Die Standardwerte für diese drei Einstellungen müssen normalerweise nicht geändert werden:		
-v	<vendor class>	APC.
-i	<client id>	Die MAC-Adresse der Netzwerkmanagement-Karte, die diese im Netzwerk eindeutig identifiziert.
-u	<user class>	Der Name des Moduls der Anwendungs-Firmware.

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

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

bye

Zugriff: Super User, Administrator, Gerätebenutzer, Nur-Netzwerk-Benutzer, Benutzer „schreibgeschützt“

Beschreibung: Hiermit schließen Sie die Befehlszeile. Dies hat dieselbe Wirkung wie die Befehle „exit“ oder „quit“.

Beispiel:

`bye`

Connection Closed - Bye

cd

Zugriff: Super User, Administrator, Gerätebenutzer, Nur-Netzwerk-Benutzer, Benutzer „schreibgeschützt“

Beschreibung: Mit diesem Befehl navigieren Sie zu einem Ordner in der Ordnerstruktur der Netzwerkmanagement-Karte.

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

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

Beispiel 2: Geben Sie Folgendes ein, um zum vorherigen Ordner zurückzukehren:

`cd.`

cipher

Zugriff: Super User, Administrator

Beschreibung: Aktivieren oder Deaktivieren von kryptografischen Algorithmen für Web UI-Sitzungen. Diese Algorithmen lassen sich nicht direkt über die Weboberfläche aktivieren/deaktivieren. Sie müssen Ihre Netzwerkmanagement-Karte nach dem Aktivieren oder Deaktivieren von Algorithmen neu starten, damit Änderungen wirksam werden.

Algorithmen sind in drei Kategorien eingeteilt: Authentifizierungs-Algorithmen, Block-Cipher-Algorithmen und MAC-Algorithmen. Verfügbare und blockierte Cipher-Suites werden auch aufgelistet.



Durch Deaktivieren des einzigen Algorithmus einer Kategorie werden alle SSL/TLS-Sitzungen geblockt und abhängig von Ihrem Browser und dessen Konfiguration kann der HTTPS-Zugriff nicht funktionieren.

HINWEIS: Ab Version v6.7.2 müssen Sie einen Algorithmus explizit aktivieren oder deaktivieren.

Option	Argument	Beschreibung
-3des	enable disable	Triple DES aktivieren oder deaktivieren.
-aes	enable disable	Advanced Encryption Standard (AES) aktivieren oder deaktivieren.
-dh	enable disable	Diffie-Hellman (DH) aktivieren oder deaktivieren.
-rsake	enable disable	RSA-Key-Exchange aktivieren oder deaktivieren.
-rsaau	enable disable	RSA-Authentifizierung aktivieren oder deaktivieren.
-sha1	enable disable	Secure Hash Algorithm 1 (SHA-1) aktivieren oder deaktivieren.
-sha2	enable disable	Secure Hash Algorithm 2 (SHA-2) aktivieren oder deaktivieren.
-ecdhe	enable disable	Elliptic Curve Diffie-Hellman Exchange (ECDHE) aktivieren oder deaktivieren.

Beispiel: Triple DES deaktivieren.

```
cipher -3des disable
```

```
E000: Success
```

```
Reboot required for change to take effect.
```

cfgshutdn

Zugriff: Superuser, Administrator, Gerätebenutzer

Beschreibung: Konfigurieren der Shutdown-Parameter: Hiermit können Sie die USV-Shutdown-Verzögerung, die USV-Einschaltverzögerung, die USV-Restlaufzeit, die USV-Ruhezustand-Zeit, die minimale USV-Batteriekapazität und die minimale Laufzeit für USV-Neustart anzeigen und konfigurieren.



Diese Optionen sind nicht bei allen USV-Geräten verfügbar.

Option	Argument	Beschreibung
-all		Hiermit lassen Sie sich alle verfügbaren Shutdown-Parameter für diese USV anzeigen.
-sd	000 090 180 270 360 450 540 630	Hiermit legen Sie die Shutdown-Verzögerung in Sekunden fest.
-lo	02 05 08 11 14 17 20 23	Hiermit legen Sie die Restlaufzeit in Minuten fest.
-rd	000 060 120 180 240 300 360 420	Hiermit legen Sie die USV-Einschaltverzögerung, also die Zeit bevor sich die USV wieder einschaltet, in Sekunden fest.
-rrt	0–3600	Hiermit legen Sie die minimale Laufzeit für den Neustart fest. Das bedeutet, dass die Laufzeit der Batterie zur Unterstützung der Last diesen Wert erreichen muss, bevor die USV sich wieder einschaltet.
-sl	0,0–359,9	Hiermit legen Sie die Ruhezeit in Stunden fest. Das Argument kann eine Zahl zwischen 0,0 und 359,9 sein.
-rsc	00 15 30 45 60 75 90	Hiermit legen Sie die minimale Batteriekapazität als prozentualen Anteil der Gesamtkapazität fest.

Beispiel:

```
cfgshutdn -all
E000: Success
Low Battery Duration: 4 min
Sleep Time: 0.0 hr
```

cfgpower

Zugriff: Superuser, Administrator, Gerätebenutzer

Beschreibung: Konfigurieren der Leistungsparameter: Hiermit können Sie Spannungstransferpunkte, Sensitivität und Ausgangsspannung anzeigen und konfigurieren.



Diese Optionen sind nicht bei allen USV-Geräten verfügbar.

Option	Argument Diese Werte können für verschiedene Geräte unterschiedlich sein.	Beschreibung
-all		Hiermit lassen Sie sich alle verfügbaren Leistungsparameter für diese USV anzeigen.

Option	Argument Diese Werte können für verschiedene Geräte unterschiedlich sein.	Beschreibung
-l	97-106	Hiermit legen Sie den unteren Spannungstransferpunkt in VAC fest.
-h	127-136	Hiermit legen Sie den oberen Spannungstransferpunkt in VAC fest.
-ov	100 120 110	Hiermit legen Sie die Ausgangsspannung in VAC fest.
-s	Normal Reduced Low	Hier legen Sie mithilfe von einem der drei Argumente die Sensitivität fest.
-bu	127 130 133 136 139 142 145 148	Hiermit legen Sie die obere Bypass-Spannung in VAC fest. Wenn die Spannung über diesen Wert ansteigt, schaltet sich das Gerät in den Bypass.
-bl	086 088 090 092 094 096 098 100	Hiermit legen Sie die untere Bypass-Spannung in VAC fest. Wenn die Spannung unter diesen Wert sinkt, schaltet sich das Gerät in den Bypass.
-rda	Never n+1 n+2	Hiermit stellen Sie einen Alarm ein, wenn die verfügbare redundante Stromversorgung unter n+1 oder n+2 fällt. Geben Sie „Never“ ein, wenn Sie keinen Alarm bezüglich eines Redundanzverlustes einstellen möchten. Diese Option ist nur beim Modell Symmetra-USV verfügbar.
-lda	Never 01,0 02,0 03,0 04,0 05,0 06,0 07,0 08,0 09,0 10,0 12,0 14,0 16,0	Hiermit stellen Sie einen Alarm ein, wenn die Last die festgelegte kVA-Belastungshöhe übersteigt. Geben Sie „Never“ ein, wenn Sie keinen Alarm bezüglich Änderungen der Belastungshöhe einstellen möchten. Diese Option ist nur beim Modell Symmetra-USV verfügbar.
-rta	Never 005 010 015 030 045 060 120 180 240 300 360 420 480	Hiermit stellen Sie einen Alarm ein, wenn die verfügbare Batterielaufzeit unter die festgelegte Minutenanzahl fällt. Die verfügbare Batterielaufzeit ist die Anzahl der Minuten, welche die USV die Stromlast im Batteriebetrieb unterstützen kann. Geben Sie „Niemals“ ein, wenn Sie keinen Alarm bezüglich eines Abfalls der verfügbaren Batterielaufzeit einstellen möchten. Diese Option ist nur beim Modell Symmetra-USV verfügbar.

Beispiel:

```

cfgpower -all
E000: Success
Low Transfer Voltage: 106 VAC
High Transfer Voltage: 127 VAC
Sensitivity: Normal

```

clrrst

Zugriff: Superuser, Administrator

Definition: Den Netzwerkschnittstellen-Resetgrund löschen. Siehe „lastrst“ auf Seite 23.

console

Zugriff: Superuser, Administrator, Nur Netzwerk

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

HINWEIS: In Version v6.8.0 und neuer ist Telnet deaktiviert und SSH standardmäßig aktiviert.

Option	Argument	Beschreibung
-s	enable disable	Hiermit aktivieren oder deaktivieren Sie SSH. Wenn SSH aktiviert wird, wird SCP aktiviert.
-t	enable disable	Hiermit aktivieren oder deaktivieren Sie Telnet.
-pt	<Telnet-Port-Nummer>	Hiermit legen Sie die Telnet-Port-Nummer fest, über die der Datenaustausch mit der Netzwerkmanagement-Karte erfolgen soll (Voreinstellung: 23). Der übrige zulässige Bereich ist 5000-32768.
-ps	<SSH-Port-Nummer>	Hiermit legen Sie die SSH-Port-Nummer fest, über die der Datenaustausch mit der Netzwerkmanagement-Karte erfolgen soll (Voreinstellung: 22). Der übrige zulässige Bereich ist 5000-32768.
-b	2400 9600 19200 38400	Hiermit konfigurieren Sie die Baud-Rate für den seriellen Anschluss (Voreinstellung: 9600).

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

```
console -t
```

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

```
console -ps 5000
```

date

Zugriff: Superuser, Administrator

Definition: Hiermit konfigurieren Sie das von der Netzwerkmanagement-Karte verwendete Datum.



Wenn Sie einen NTP-Server konfigurieren möchten, von dem die Netzwerkmanagement-Karte das Datum und die Uhrzeit beziehen soll, schlagen Sie bitte im *Benutzerhandbuch* nach.

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

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

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

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

```
date -d "30.10.2009"
```

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

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

delete

Zugriff: Superuser, Administrator

Beschreibung: Hiermit löschen Sie eine Datei im Dateisystem. (Zum Löschen des Ereignisprotokolls siehe das *Benutzerhandbuch*).

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

Beispiel: So löschen Sie eine Datei:

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 im Ordner `logs` enthaltenen Dateien anzuzeigen:
`dir`
3. Typ
`delete <Dateiname>`

detbat



Dieser Befehl ist nicht auf allen USV-Geräten verfügbar.

Für einige USV-Geräte mit dem SRT-Präfix stehen andere Einstellungen zur Verfügung.

Zugriff: Superuser, Administrator, Gerätebenutzer

Beschreibung: Anzeige detaillierter USV-Batterieinformationen.

Option	Argumente	Beschreibung
-all	<#>	Anzeige aller Batterieinformationen.
-f	<#>	Firmware-Versionen der Module.
-t	<#>	Temperaturen der Module.
-pe	<#>	Batterie-Modul-Status.
-s	<#> <#>	Zustand von Modul/Kassette.
-ph	<#>	Modulzustand. HINWEIS: Diese Option ist nur bei einigen USV-Geräten mit dem SRT-Präfix verfügbar.
-rd	<#> <#>	Datum zum empfohlenen Austausch der Batterie von Modul/Kassette.
-pr	<#>	Datum zum empfohlenen Austausch des Moduls. HINWEIS: Diese Option ist nur bei einigen USV-Geräten mit dem SRT-Präfix verfügbar.

Option	Argumente	Beschreibung
-id	<#> <#> <„Datumszeichenfolge“>	Einbaudatum der Batterie von Modul/Kassette im aktuellen Datumsformat.
-pi	<#> <"datestring">	Einbaudatum des Batterie-Moduls im aktuellen Datumsformat. HINWEIS: Diese Option ist nur bei einigen USV-Geräten mit dem SRT-Präfix verfügbar.
-ce	<#> <#>	Batteriestatus von Modul/Kassette.

Beispiel: detbat -all

E000: Success

Firmware Revision (IP): BMC 12.5

Temperature (IP): 26.00C

Pack Status (IP): No Errors

Health (IP, C1): Battery Life OK

Predicted Replacement Date (IP, C1): 02.07.2019

Installation Date (IP, C1): 12.02.2015

Status (IP, C1): OK

detstatus

Zugriff: Superuser, Administrator, Gerätebenutzer

Beschreibung: Hiermit zeigen Sie den detaillierten Status der USV an. Siehe auch die -st-Option unter „ups“ auf Seite 34.

Option	Beschreibung
-all	Hiermit lassen Sie sich alle verfügbaren Statusinformationen für diese USV anzeigen.
-rt	Verbleibende Laufzeit in Stunden und Minuten.
-ss	USV-Statuszusammenfassung: online, Batteriebetrieb etc.
-soc	USV-Batteriekapazität als prozentualen Anteil der Gesamtkapazität.
-om	Ausgangswerte: Spannung, Frequenz, Watt in %, VA in %, Strom.
-im	Eingangswerte: Spannung und Frequenz.
-bat	Batteriespannung.
-tmp	Interne Temperatur der USV.
-dg	Diagnosetestergebnisse: Ergebnis des Selbsttests und Datum, Kalibrierungsergebnis und Datum.

Beispiel:

detstatus -rt

E000: Success

Runtime Remaining: 9 hr 22 min 30 sec

dir

Zugriff: Super User, Administrator, Gerätebenutzer, Nur-Netzwerk-Benutzer, Benutzer „schreibgeschützt“

Beschreibung: Hiermit zeigen Sie eine Liste der auf der Netzwerkmanagement-Karte gespeicherten Dateien und Ordner an.

Beispiel:

```
dir
```

```
E000: Success
```

```
3069184 Jun 28 18:07 apc_hw05_aos_664.bin
3031604 Jul 30 19:05 apc_hw05_sumx_664.bin
45000 Aug 17 10:54 config.ini
    0 May 14 2018 db/
    0 May 14 2018 ssl/
    0 May 14 2018 ssh/
    0 May 14 2018 logs/
    0 May 14 2018 sec/
    0 May 14 2018 dbg/
    0 May 14 2018 fwl/
    0 May 14 2018 email/
    0 May 14 2018 lang/
    0 May 14 2018 tmp/
    0 May 14 2018 upsfw/
    0 May 14 2018 rms/
    0 May 14 2018 scg/
```

dns

Zugriff: Superuser, Administrator

Beschreibung: Hiermit konfigurieren Sie die DNS-Einstellungen manuell bzw. zeigen sie an.

Option	Argument	Beschreibung
-OM	enable disable	Hiermit überschreiben Sie die manuell konfigurierten DNS-Einstellungen.
-y	enable disable	Hiermit synchronisieren Sie das System und den Hostnamen. Das hat dieselbe Wirkung wie „system -s“.
-p	<primärer DNS-Server>	Hiermit legen Sie den primären DNS-Server fest.
-s	<sekundärer DNS-Server>	Hiermit legen Sie den sekundären DNS-Server fest.
-d	<Domänenname>	Hiermit legen Sie den Domänennamen fest.

Option	Argument	Beschreibung
-n	<Domänenname IPv6>	Hiermit legen Sie den Domännennamen für IPv6 fest.
-h	<Host-Name>	Hiermit legen Sie den Hostnamen fest.

Beispiel:

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

eapol

Zugriff: Superuser, Administrator

Beschreibung: Die Einstellungen für EAPoL (802.1X Security) konfigurieren.

Option	Argument	Description
-S	enable disable	EAPoL aktivieren oder deaktivieren.
-n	<supplicant-name>	Supplicant-Name festlegen.
-p	<private-key-passphrase>	Private-Key-Passphrase festlegen.

Beispiel 1: Um das Ergebnis eines EAPoL-Befehls anzuzeigen:

```
apc>eapol
E000: Success
Active EAPoL Settings
-----
Status:enabled
Supplicant Name:NMC-Supplicant Passphrase:<hidden>
CA file Status:Valid Certificate
Private Key Status:Valid Certificate
Public Key Status:Valid Certificate
Result:Success
```

Beispiel 2: Um EAPoL zu aktivieren:

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

email

Zugriff: Superuser, Administrator, Nur Netzwerk-Benutzer

Beschreibung: Verwenden Sie die folgenden Befehle, um die von der Netzwerkmanagement-Karte verwendeten E-Mail-Parameter zum Versenden von Ereignisbenachrichtigungen zu konfigurieren.

Option	Argument	Beschreibung
-g[n]	<enable disable>	Hiermit aktivieren (Standardeinstellung) oder deaktivieren Sie den E-Mail-Versand an den Empfänger.
-t[n]	<Empfängeradresse>	Die E-Mail-Adresse des Empfängers.
-o[n]	<long short> (Format)	Das lange Format enthält den Namen, den Standort, einen Ansprechpartner, die IP-Adresse, die Seriennummer des Geräts, Datum und Uhrzeit, den Ereigniscode und eine Beschreibung des Ereignisses. Das kurze Format enthält lediglich die Beschreibung des Ereignisses.
-l[n]	<Sprachcode>	Die Sprache, in der die E-Mails versendet werden. Dies hängt vom installierten Sprachpaket ab.
-r [n]	<Local recipient custom> (Route)	<p>Hiermit legen Sie die SMTP-Serveroptionen fest:</p> <ul style="list-style-type: none"> • Local (lokal) (empfohlen): Wählen Sie diese Option aus, wenn sich Ihr SMTP-Server in Ihrem internen Netzwerk befindet oder für Ihre E-Mail-Domäne eingerichtet wurde. Wählen Sie diese Einstellung, um Verzögerungen und Netzwerkausfälle zu minimieren. Wenn Sie diese Einstellung wählen, müssen Sie am SMTP-Server des Geräts auch die Weiterleitung aktivieren und ein spezielles externes E-Mail-Konto einrichten, an das die weitergeleitete E-Mail gesendet werden soll. HINWEIS: Sprechen Sie mit dem Administrator Ihres SMTP-Servers, bevor Sie diese Änderungen vornehmen. • Recipient (Empfänger): Bei dieser Einstellung wird die E-Mail direkt an den SMTP-Server des Empfängers gesendet, der über eine MX-Eintragssuche der Domain der Empfängeradresse ermittelt wird. Das Gerät unternimmt nur einen Versuch, die E-Mail zu senden. Ein Netzwerkausfall oder ein ausgelasteter Remote-SMTP-Server kann ein Time-out auslösen und dazu führen, dass die E-Mail verloren geht. Diese Einstellung erfordert keine zusätzlichen administrativen Aufgaben am SMTP-Server. • Custom (benutzerdefiniert): Diese Einstellung ermöglicht für jeden E-Mail-Empfänger eigene Servereinstellungen. Diese Einstellungen sind von den Einstellungen der Option -s[n] unabhängig.
-f[n]	<Absenderadresse>	Die von der Netzwerkmanagement-Karte im Feld Von: der gesendeten E-Mail verwendete Absenderadresse.
-s[n]	<SMTP-Server>	Die IPv4-/IPv6-Adresse oder der DNS-Name des lokalen SMTP-Servers. Verwenden Sie diese Option, wenn die Option -r[n] auf Local (lokal) gesetzt ist.
-p[n]	<Port>	Die SMTP-Port-Nummer mit einem Standardwert von 25. Alternative Ports: 465, 587, 2525, 5000 bis 32768.
-a[n]	<enable disable> (Authentifizierung)	Aktivieren Sie diese Option, wenn der SMTP-Server eine Authentifizierung verlangt.
-u[n]	<Benutzername>	Geben Sie hier Ihren Benutzernamen und Ihr Kennwort ein, wenn der Mail-Server eine Authentifizierung verlangt.
-w[n]	<Kennwort>	
-e[n]	<none ifsupported always implicit> (Verschlüsselung)	<ul style="list-style-type: none"> • None (Keine): Der SMTP-Server erfordert und unterstützt auch keine Verschlüsselung. • If Supported (Wenn unterstützt): Der SMTP-Server zeigt an, dass STARTTLS unterstützt wird, erfordert jedoch keine verschlüsselte Verbindung. Der STARTTLS-Befehl wird nach dem Advertisement gesendet. • Always (Immer): Der SMTP-Server erfordert das Senden des STARTTLS-Befehls, sobald eine Verbindung zum Server hergestellt wird. • Implicit (Implizit): Der SMTP-Server akzeptiert nur Verbindungen, die von vornherein verschlüsselt sind. Es wird keine STARTTLS-Nachricht an den Server gesendet.

Option	Argument	Beschreibung
-c[n]	<enable disable > (erforderliches Zertifikat)	Diese Option sollte nur dann aktiviert werden, wenn die Sicherheitsrichtlinie Ihres Unternehmens das implizite Vertrauen von SSL-Verbindungen nicht unterstützt. Wenn sie aktiviert ist, muss ein gültiges Root-Zertifikat der Zertifizierungsstelle auf die Netzwerkmanagement-Karte geladen werden, um verschlüsselte E-Mails senden zu können.
-i[n]	<Zertifikatsdateiname>	Dieses Feld ist von den auf der Netzwerkmanagement-Karte installierten Root-Zertifikaten der Zertifizierungsstelle abhängig sowie davon, ob ein Root-Zertifikat der Zertifizierungsstelle erforderlich ist oder nicht. Die Datei muss die Erweiterung. crt oder. cer haben.
n=	E-Mail-Empfängernummer (1, 2, 3 oder 4)	Kennzeichnet den Empfänger der E-Mail durch die Empfängernummer.

Beispiel: Um das Senden von E-Mails an den E-Mail-Empfänger 1 mit der E-Mail-Adresse recipient1@apc.com über den lokalen SMTP-Server zu aktivieren:

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

eventlog

Zugriff: Super User, Administrator, Gerätebenutzer, Nur-Netzwerk-Benutzer, Benutzer „schreibgeschützt“

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

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

exit

Zugriff: Super User, Administrator, Gerätebenutzer, Nur-Netzwerk-Benutzer, Benutzer „schreibgeschützt“

Beschreibung: Hiermit schließen Sie die Befehlszeile.

firewall

Zugriff: Super User, Administrator, Nur Netzwerk

Beschreibung: Interne NMC-Firewall

aktivieren, deaktivieren oder konfigurieren.

Option	Argument	Beschreibung
-S	<enable disable>	Hiermit aktivieren oder deaktivieren Sie die Firewall.
-f	<Zu aktivierender Dateiname>	Name der zu aktivierenden Firewall-Richtliniendatei.
-t	<Zu testender Dateiname>	Name der zu testenden Firewall sowie Dauer in Minuten.
-fe		Hiermit zeigen Sie eine Liste aktiver Dateifehler an.
-te		Hiermit zeigen Sie eine Liste von Testdateifehlern an.
-c		Hiermit brechen Sie einen Firewall-Test ab.
-r		Hiermit zeigen Sie eine Liste aktiver Firewall-Regeln an.
-l		Hiermit zeigen Sie ein Firewall-Aktivitätsprotokoll an.

Beispiel: Geben Sie Folgendes ein, um die Firewall-Richtliniendatei `example.fwl` zu aktivieren:

```
firewall -f example.fwl
```

```
E000: Success
```

format

Zugriff: Superuser, Administrator

Beschreibung: Hiermit formatieren Sie das Dateisystem der Netzwerkmanagement-Karte neu und löschen sämtliche Sicherheitszertifikate, Verschlüsselungsschlüssel, Konfigurationseinstellungen sowie die Ereignis- und Datenprotokolle. Seien Sie mit diesem Befehl vorsichtig.



Zum Zurücksetzen der Netzwerkmanagement-Karte auf ihre Standardkonfiguration verwenden Sie den Befehl `resetToDef`.

ftp

Zugriff: Super User, Administrator, Nur Netzwerk

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

HINWEIS: In Version v6.8.0 und neuer ist FTP standardmäßig deaktiviert.

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

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

```
ftp -p 5001
```


help

Zugriff: Superuser, Administrator, Gerätebenutzer, Schreibgeschützt

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

Beispiel 1: Geben Sie Folgendes ein, um sämtliche Befehle angezeigt zu bekommen, die einer als Benutzer „device“ angemeldeten Person zur Verfügung stehen:

```
help
```

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

```
alarmcount help
```

lang

Zugriff: Superuser, Administrator, Gerätebenutzer, Benutzer „schreibgeschützt“, Nur Netzwerk-Benutzer

Beschreibung: Verwendete Sprache

Beispiel:

```
lang
```

```
Languages
```

```
enUS - English
```

lastrst

Zugriff: Superuser, Administrator

Beschreibung: Letzter Netzwerkschnittstellen-Resetgrund. Verwenden Sie diesen Befehl, um Probleme der Netzwerkschnittstelle mit Hilfe des technischen Supports zu beheben.

Beispiel:

```
lastrst
```

```
09 Coldstart Reset
```

```
E000: Success
```

ledblink

Zugriff: Superuser, Administrator

Beschreibung: Setzt die Status-LED der Netzwerkmanagement-Karte für die festgelegte Dauer auf Blinken. Verwenden Sie diesen Befehl, um das optische Auffinden der Netzwerkmanagement-Karte zu erleichtern.

Parameter: Zeit in Minuten

Beispiel:

```
ledblink 2
```

```
E000: Success
```

logzip

Zugriff: Superuser, Administrator

Beschreibung: Erstellt ein einzelnes, komprimiertes Archiv der Protokolldateien aus der NMC oder USV. Diese Dateien können vom technischen Support zur Problembehandlung verwendet werden.

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

Beispiel:

```
logzip -m 1
Generating files
Compressing files into /dbg/debug_ZA1752123456.tar
Emailing log files to email recipient - 1
E000: Success
```

modbus

Zugriff: Superuser, Administrator, Gerätebenutzer

Beschreibung: Hiermit können Sie die Modbus-Parameter anzeigen und konfigurieren.

Option	Argument	Beschreibung
-a	<enable disable> (Modbus-Status)	Hiermit aktivieren oder deaktivieren Sie Modbus Seriell. ¹
-br	<9600 19200> (Baudrate)	Hiermit legen Sie die Baudrate in Bits pro Sekunde fest. ¹
-pr	event odd none	Hiermit stellen Sie das Paritätsbit ein. ¹
-s	<1-F7> (hexadezimale Slave-Adresse)	Hiermit stellen Sie die hexadezimale Modbus-Slave-Adresse ein. ¹
-rDef		Hiermit setzen Sie die Modbus-Konfiguration auf die Standardwerte zurück.
-tE	<enable disable> (Modbus-TCP-Status)	Hiermit aktivieren oder deaktivieren Sie Modbus TCP. ²
-tP		Hiermit legen Sie die Modbus-TCP-Portnummer fest. Die standardmäßige Portnummer ist 502 und kann auf einen Wert zwischen 5000 und 32768 ² gesetzt werden.
¹ Modbus Seriell wird nur auf der AP9635-Karte unterstützt. ² Modbus TCP wird auf den Karten AP9630, AP9631 und AP9635 unterstützt.		

Beispiel:

```
modbus
E000: Success
Slave Address = 0x1
Status = ENABLED
Baud Rate = 9600
Parity = none
TCP Status = ENABLED
TCP Port Number = 502
```

netstat

Zugriff: Super User, Administrator, Nur Netzwerk

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

Beispiel:

```
netstat
Current IP information
```

Family	mHome	Type	IP Address	Status
IPv6	4	auto	FE80::2C0:B7FF:FEEA:D325/64	configured
IPv4	0	manual	10.125.43.115/22	configured
IPv6	0	manual	::1/128	configured
IPv4	0	manual	127.0.0.1/32	configured

ntp

Zugriff: Super User, Administrator, Nur Netzwerk

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

Option	Argument	Beschreibung
-OM	enable disable	Hiermit überschreiben Sie die manuell konfigurierten Einstellungen.
-p	<Primärer NTP-Server>	Hiermit legen Sie den primären Server fest.
-s	<Sekundärer NTP-Server>	Hiermit legen Sie den sekundären Server fest.
-e	enable disable	Hiermit aktivieren oder deaktivieren Sie NTP.
-u	<update now>	Hiermit starten Sie eine sofortige Aktualisierung der NMC-Zeit über den NTP-Server.

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

```
ntp -OM enable
```

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

```
ntp -p 150.250.6.10
```

ping

Zugriff: Super User, Administrator, Gerätebenutzer, Nur Netzwerk

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

Argument	Beschreibung
<IP-Adresse oder DNS-Name>	Geben Sie eine IP-Adresse im Format <i>xxx.xxx.xxx.xxx</i> oder einen DNS-Namen ein.

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

```
ping 150.250.6.10
```

portspeed

Zugriff: Super User, Administrator, Nur Netzwerk

Beschreibung:

Option	Argumente	Beschreibung
-s	auto 10H 10F 100H 100F	Hiermit konfigurieren Sie die Übertragungsgeschwindigkeit des Ethernet-Anschlusses. Mit dem Befehl <code>auto</code> wird es den Ethernet-Geräten ermöglicht, die höchstmögliche Geschwindigkeit für die Datenübertragung auszuhandeln.

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

```
portspeed -s 100H
```

prompt

Zugriff: Super User, Administrator, Gerätebenutzer, Nur Netzwerk

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

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

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

```
prompt -s long
```

pwd

Zugriff: Superuser, Administrator, Gerätebenutzer, Benutzer „schreibgeschützt“, Nur Netzwerk-Benutzer

Beschreibung: Wird zur Ausgabe des Pfads des momentanen Arbeitsverzeichnisses verwendet.

quit

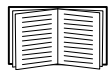
Zugriff: Super User, Administrator, Gerätebenutzer, Nur-Netzwerk-Benutzer, Benutzer „schreibgeschützt“

Beschreibung: Hiermit schließen Sie die Befehlszeile (funktionsgleich mit den Befehlen „exit“ und „bye“).

radius

Zugriff: Super User, Administrator, Nur Netzwerk

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



Eine Übersicht über die RADIUS-Server-Konfiguration sowie eine Liste der unterstützten RADIUS-Server finden Sie im *Benutzerhandbuch* auf der [APC-Website](#).

Auf der Benutzeroberfläche der Netzwerkmanagement-Karte stehen zusätzliche Authentifizierungsparameter für RADIUS-Server zur Verfügung.

Ausführliche Informationen zum Konfigurieren des von Ihnen verwendeten RADIUS-Servers finden Sie im *Sicherheitshandbuch* auf der [APC-Website](#).

Option	Argument	Beschreibung
-a	local radiusLocal radius	Konfigurieren der RADIUS-Authentifizierung: local – RADIUS ist deaktiviert. Lokale Authentifizierung ist aktiviert. radiusLocal – Zuerst RADIUS-Authentifizierung, dann lokale Authentifizierung. RADIUS-Authentifizierung und lokale Authentifizierung sind aktiviert. Die Authentifizierung wird zuerst beim RADIUS-Server angefordert. Wenn der RADIUS-Server nicht reagiert oder über das Netzwerk nicht erreicht werden kann, wird die lokale Authentifizierung verwendet. radius – RADIUS ist aktiviert. Lokale Authentifizierung ist deaktiviert.
-p1 -p2 -o1 -o2	<Server-IP>	Der Servername oder die IP-Adresse des primären oder sekundären RADIUS-Servers. HINWEIS: RADIUS-Server verwenden normalerweise Port 1812, um Benutzer zu authentifizieren. Wenn Sie einen anderen Port verwenden möchten, hängen Sie an den Namen des RADIUS-Servers oder an dessen IP-Adresse einen Doppelpunkt an, gefolgt von der neuen Port-Nummer. Die Netzwerkmanagement-Karte unterstützt die Ports 1812, 5000 bis 32768.
-s1 -s2	<Server-Schlüssel>	Der vom primären oder sekundären RADIUS-Server und der Netzwerkmanagement-Karte verwendete geheime Schlüssel.
-t1 -t2	<Server-Timeout>	Die Zeit in Sekunden, die die Netzwerkmanagement-Karte auf eine Antwort vom primären oder sekundären RADIUS-Server wartet.

Beispiel 1: Geben Sie `radius` ein und betätigen Sie die EINGABETASTE, um sich die aktuellen RADIUS-Einstellungen für die Netzwerkmanagement-Karte anzeigen zu lassen.

Beispiel 2: Sie aktivieren die RADIUS-Authentifizierung und die lokale Authentifizierung, indem Sie Folgendes eingeben:

```
radius -a radiusLocal
```

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

```
radius -t2 10
```

reboot

Zugriff: Super User, Administrator, Nur Netzwerk

Beschreibung: Neustart der Netzwerk-Management-Oberfläche der Netzwerkmanagement-Karte.



Die Ausgangsleistung des Geräts, in dem die Netzwerkmanagement-Karte installiert ist, wird dadurch nicht beeinträchtigt.

resetToDef

Zugriff: Superuser, Administrator

Beschreibung: Hiermit setzen Sie alle Parameter auf ihre Standardeinstellungen zurück.

Option	Argumente	Beschreibung
-p	all keepip	Vorsicht: Hiermit setzen Sie alle Parameter auf ihre Standardeinstellungen zurück. Hiermit setzen Sie alle Konfigurationsänderungen zurück, auch Ereignisvorgänge, Geräteeinstellungen und gegebenenfalls TCP/IP-Konfigurationseinstellungen. Wählen Sie „keepip“, um die Einstellungen zu erhalten, die festlegen, wie die Netzwerkmanagement-Karte ihre TCP/IP-Konfigurationswerte (standardmäßig DHCP) erhält.



Bestimmte nicht konfigurierbare Parameter werden durch den Befehl `resetToDef` nicht zurückgesetzt und können nur durch die Formatierung des Dateisystems mit dem Befehl **format** von der Netzwerkmanagement-Karte gelöscht werden.

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

```
resetToDef -p keepip
```

session

Zugriff: Superuser, Administrator

Beschreibung: Zeichnet die angemeldete Person (Benutzer), die Schnittstelle, die Adresse, die Uhrzeit und die ID auf.

Option	Argumente	Beschreibung
-d	<session ID> (Löschen)	Hiermit löschen Sie die Sitzung des aktuellen Benutzers mit der angegebenen Sitzungs-ID.
-m	<enable disable> (Mehrfachbenutzung aktivieren)	Durch die Aktivierung ermöglichen Sie zwei oder mehr Benutzern, sich gleichzeitig anzumelden. Durch die Deaktivierung ermöglichen Sie nur jeweils einem Benutzer, sich anzumelden.
-a	<enable disable> (Remote-Authentifizierungsüberschreibung)	Die Netzwerkmanagement-Karte unterstützt die RADIUS-Speicherung von Kennwörtern auf einem Server. Aktivieren Sie die Remote-Authentifizierungsüberschreibung, um einem lokalen Benutzer zu erlauben, sich mit einem Benutzernamen und einem Kennwort für die Netzwerkmanagement-Karte anzumelden, die lokal auf der Netzwerkmanagement-Karte gespeichert ist.

Beispiel:

session

User	Interface	Address	Logged In Time	ID
apc	Telnet	10.169.118.100	00:00:03	19

smtp

Zugriff: Super User, Administrator, Nur Netzwerk

Beschreibung: Konfigurieren der Einstellungen des lokalen E-Mail-Servers.

Option	Argumente	Beschreibung
-f	<Absenderadresse>	Die Adresse, von der E-Mails von der Netzwerkmanagement-Karte gesendet werden.
-s	<SMTP-Server>	Die IPv4-/IPv6-Adresse oder der DNS-Name des lokalen SMTP-Servers.
-p	<Port>	Die SMTP-Port-Nummer mit einem Standardwert von 25. Die möglichen Port-Nummern sind 25, 465, 587, 2525, 5000 bis 32768.
-a	<enable disable>	Aktivieren Sie diese Option, falls Ihr SMTP-Server eine Authentifizierung verlangt.
-u	<Benutzername>	Geben Sie hier den Benutzernamen und das Kennwort ein, wenn der SMTP-Server eine Authentifizierung verlangt.
-w	<Kennwort>	
-e	<none ifavail always implicit>	Verschlüsselungsoptionen: <ul style="list-style-type: none">• none (keine): Der SMTP-Server erfordert/unterstützt keine Verschlüsselung.• ifavail: Der SMTP-Server zeigt an, dass STARTTLS unterstützt wird, erfordert jedoch keine verschlüsselte Verbindung.• always (immer): Der SMTP-Server erfordert das Senden des STARTTLS-Befehls, sobald eine Verbindung zum Server hergestellt wird.• implicit (implizit): Der SMTP-Server akzeptiert nur Verbindungen, die von vornherein verschlüsselt sind. Es wird keine STARTTLS-Nachricht an den Server gesendet.
-c	<enable disable>	Root-Zertifikat der Zertifizierungsstelle erforderlich: Diese Option sollte nur dann aktiviert werden, wenn die Sicherheitsrichtlinie Ihres Unternehmens das implizite Vertrauen von SSL-/TLS-Verbindungen nicht unterstützt. Wenn sie aktiviert ist, muss ein gültiges Root-Zertifikat der Zertifizierungsstelle auf die Netzwerkmanagement-Karte geladen werden, um verschlüsselte E-Mails senden zu können.
-i	<Zertifikatsdateiname>	Dieses Feld ist von den auf der Netzwerkmanagement-Karte installierten Root-Zertifikaten der Zertifizierungsstelle abhängig sowie davon, ob ein Root-Zertifikat der Zertifizierungsstelle erforderlich ist oder nicht.

Beispiel:

```
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>

snmp

Zugriff: Super User, Administrator, Nur Netzwerk

Beschreibung: Hiermit aktivieren oder deaktivieren und konfigurieren Sie SNMPv1.

In der nachstehenden Tabelle entspricht n der Zugriffssteuerungsnummer: 1, 2, 3 oder 4.

HINWEIS: In Version v6.8.0 und neuer ist SNMPv1 standardmäßig deaktiviert. Der Community-Name (-c [n]) muss festgelegt werden, bevor SNMPv1-Kommunikation hergestellt werden kann.

Option	Argumente	Beschreibung
-S	enable disable	Hiermit aktivieren oder deaktivieren Sie SNMP 1.
-c[n]	Community	Hiermit geben Sie eine Community an.
-a[n]	read write writeplus disable	Hiermit legen Sie die Nutzungsrechte fest.
-n[n]	IP-Adresse oder Domänenname	Hiermit geben Sie die IPv4/IPv6 -Adresse oder den Domännennamen der Netzwerk-Managementstation an.

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

```
snmp -S enable
```

snmpv3

Zugriff: Super User, Administrator, Nur Netzwerk

Beschreibung: Hiermit aktivieren oder deaktivieren und konfigurieren Sie SNMPv3.

In der nachstehenden Tabelle entspricht n der Zugriffssteuerungsnummer: 1, 2, 3 oder 4.

HINWEIS: In Version v6.8.0 und neuer ist SNMPv3 standardmäßig deaktiviert. Ein gültiges Benutzerprofil muss mit Kennwortsätzen (-a[n], -c[n]) aktiviert werden, bevor SNMPv3-Kommunikation hergestellt werden kann.

Option	Argumente	Beschreibung
-S	enable disable	Hiermit aktivieren oder deaktivieren Sie SNMPv3.
-u[n]	<Benutzername>	Hiermit geben Sie einen Benutzernamen, einen Authentifizierungskennwortsatz und einen Verschlüsselungskennwortsatz an.
-a[n]	<Authentifizierungskennwortsatz>	
-c[n]	<Verschlüsselungskennwortsatz>	
-ap[n]	sha md5 none	Hiermit geben Sie den Typ des Authentifizierungsprotokolls an.
-pp[n]	aes des none	Hiermit geben Sie das Datenschutzprotokoll (Verschlüsselung) an.
-ac[n]	enable disable	Hiermit aktivieren oder deaktivieren Sie den Zugriff.
-au[n]	<Benutzerprofilname>	Hiermit gestatten Sie einen angegebenen Benutzerprofil den Zugriff.

Option	Argumente	Beschreibung
-n[n]	<IP-Adresse oder Hostname für NMS>	Hiermit geben Sie die IPv4/IPv6 -Adresse oder den Hostnamen der Netzwerk-Managementstation an.

Beispiel: Geben Sie Folgendes ein, um dem Benutzer JMurphy die Zugriffsebene 2 zuzuweisen:

```
snmpv3 -au2 "JMurphy"
```

snmptrap

Zugriff: Superuser, Administrator, Nur Netzwerk-Benutzer

Beschreibung: Hiermit aktivieren oder deaktivieren Sie die SNMP-Trap-Generierung.

Option	Argumente	Beschreibung
-c[n]	<Community>	Hiermit geben Sie eine Community an.
-r[n]	<Empfänger-NMS-IP>	Die IPv4-/IPv6-Adresse oder der Hostname des Trap-Empfängers.
-l[n]	<Sprache> [Sprachcode]	Legen Sie eine Sprache fest. Dazu muss ein Sprachpaket mit der gewünschten Sprache installiert sein, wobei folgende Sprachcodes zur Verfügung stehen: <ul style="list-style-type: none"> • enUS - Englisch • deDe - Deutsch • ruRu - Russisch • zhCn - Chinesisch • jaJa - Japanisch • koKo - Koreanisch • itIt - Italienisch • ptBr - Portugiesisch • frFr - Französisch • esEs – Spanisch
-t[n]	<Trap-Typ> [snmpV1 snmpV3]	Hiermit legen Sie SNMPv1 oder SNMPv3 fest.
-g[n]	<Generierung> [enable disable]	Hiermit aktivieren oder deaktivieren Sie die Trap-Generierung für diesen Trap-Empfänger. Standardmäßig aktiviert.
-a[n]	<Auth Traps> [enable disable]	Hiermit aktivieren oder deaktivieren Sie die Trap-Authentifizierung für diesen Trap-Empfänger (nur SNMPv1).
-u[n]	<profile1 profile2 profile3 profile4> (Benutzername)	Hiermit wählen Sie die Kennung für das Benutzerprofil dieses Trap-Empfängers aus (nur SNMPv3).
n= Trap-Empfängernummer = 1, 2, 3, 4, 5 oder 6		

Beispiel: Geben Sie folgenden Befehl ein, wenn Sie einen SNMPv1-Trap für Empfänger 1 mit Community-Namen „public“, IP-Adresse 10.169.118.100 für Empfänger 1 und Verwendung der Standardsprache Englisch aktivieren und konfigurieren möchten:

```
snmptrap -c1 public -r1 10.169.118.100 -l1 enUS -t1 snmpV1 -g1 enable
```

```
E000: Success
```

system

Zugriff: Superuser, Administrator

Beschreibung: Hiermit können Sie den Systemnamen, den Ansprechpartner und den Standort anzeigen und einstellen sowie das Datum und die Uhrzeit, den angemeldeten Benutzer und den höchstrangigen Systemstatus (P, N oder A) anzeigen – weitere Informationen finden Sie unter „Statusfelder in der Hauptmaske“.

Option	Argument	Beschreibung
-n	<Systemname>	Hiermit legen Sie den Gerätenamen, den Namen der für das Gerät verantwortlichen Person und den physischen Standort des Geräts fest. Hinweis: Wenn Sie einen aus mehreren Wörtern bestehenden Wert eingeben, müssen Sie Ihre Eingabe in doppelte Anführungszeichen setzen. Diese Werte werden auch von StruxureWare Data Center Expert oder EcoStruxure IT Expert und vom SNMP-Agenten der Netzwerkmanagement-Karte verwendet.
-c	<Systemkontakt>	
-l	<Systemposition>	
-m	<Systemmeldung>	Hiermit zeigen Sie eine benutzerdefinierte Meldung oder ein Banner auf der Anmeldeseite der Web- oder Benutzeroberfläche an.
-s	enable disable	Hiermit synchronisieren Sie das System und den Hostnamen. Das hat dieselbe Wirkung wie „dns -y“.

Beispiel 1: Geben Sie Folgendes ein, um den Gerätestandort Labor für Prüfzwecke festzulegen:
system -l "Labor für Prüfzwecke"

Beispiel 2: Geben Sie Folgendes ein, um den Systemnamen Frank Weber festzulegen:
system -n "Frank Weber"

tcpip

Zugriff: Super User, Administrator, Nur Netzwerk

Beschreibung: Hiermit konfigurieren Sie folgende IPv4-TCP/IP-Einstellungen für die Netzwerkmanagement-Karte und zeigen diese an:

Option	Argument	Beschreibung
-S	enable disable	Hiermit aktivieren oder deaktivieren Sie TCP/IP v4.
-i	<IP-Adresse>	Geben Sie die IP-Adresse der Netzwerkmanagement-Karte im Format xxx.xxx.xxx.xxx ein.
-s	<Subnetzmaske>	Geben Sie die Subnetzmaske für die Netzwerkmanagement-Karte ein.
-g	<Gateway>	Geben Sie die IP-Adresse des Standardgateways ein. <i>Verwenden Sie nicht</i> die Loopback-Adresse (127.0.0.1) als Standardgateway.
-d	<Domänenname>	Geben Sie den vom DNS-Server konfigurierten DNS-Namen ein.
-h	<Host-Name>	Geben Sie den Host-Namen ein, den die Netzwerkmanagement-Karte verwenden soll.

Beispiel 1: Geben Sie tcpip ein und betätigen Sie die EINGABETASTE, um sich die aktuellen Netzwerk-Einstellungen für die Netzwerkmanagement-Karte anzeigen zu lassen.

Beispiel 2: Geben Sie Folgendes ein, um die IP-Adresse 150.250.6.10 für die Netzwerkmanagement-Karte manuell zu konfigurieren:
tcpip -i 150.250.6.10

tcpip6

Zugriff: Super User, Administrator, Nur Netzwerk

Beschreibung: Hiermit aktivieren Sie IPv6, konfigurieren manuell die folgenden IPv6-TCP/IP-Einstellungen für die Netzwerkmanagement-Karte und zeigen diese an:

Option	Argument	Beschreibung
-S	enable disable	Hiermit aktivieren oder deaktivieren Sie TCP/IP v6.
-man	enable disable	Hiermit aktivieren Sie die manuelle Adressierung für die IPv6-Adresse der Netzwerkmanagement-Karte.
-auto	enable disable	Hiermit aktivieren Sie die automatische Konfiguration der IPv6-Adresse durch die Netzwerkmanagement-Karte.
-i	<IPv6-Adresse>	Hiermit stellen Sie die IPv6-Adresse der Netzwerkmanagement-Karte ein.
-g	<IPv6-Gateway>	Hiermit stellen Sie die IPv6-Adresse des Standardgateways ein.
-d6	router statefull stateless never	Hiermit stellen Sie die DHCPv6-Betriebsart über die Parameter „router“, „statefull“ (der Status der Adresse und anderer Daten wird jeweils beibehalten), „stateless“ (mit Ausnahme der Adresse wird der Status nicht beibehalten) und „never“ (nie) ein.

Beispiel 1: Geben Sie `tcpip6` ein und betätigen Sie die EINGABETASTE, um sich die aktuellen Netzwerkeinstellungen für die Netzwerkmanagement-Karte anzeigen zu lassen.

Beispiel 2: Geben Sie Folgendes ein, um die IPv6-Adresse 2001:0:0:0:FFD3:0:57ab für die Netzwerkmanagement-Karte manuell zu konfigurieren:

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

uio

Zugriff: Superuser, Administrator, Gerätebenutzer

Beschreibung: Dieser Befehl ist für die Netzwerkmanagement-Karte 2 AP9631 oder AP9635 mit angeschlossenem E/A-Zusatzmodul für potenzialfreie Kontakte (AP9810) verfügbar.

Option	Argument	Beschreibung
-rc <UIO-Port-Nr.>	open close	Hiermit ändern Sie den Status einer angeschlossenen Datenausgabe und legen den verwendeten UIO-Port fest.
-st	<UIO-Port-Nr.> <UIO-Port-Nr.>, <UIO-Port-Nr.> <UIO-Port-Nr.>– <UIO-Port-Nr.>	Hiermit können Sie sich den Status der am E/A-Zusatzmodul für potenzialfreie Kontakte angeschlossenen Sensoren anzeigen lassen. Wenn Sie sich den Status eines bestimmten Sensors oder mehrerer Sensoren ansehen möchten, geben Sie deren UIO-Port-Nummern ein.
-disc	<UIO-Port-Nr.> <UIO-Port-Nr.>, <UIO-Port-Nr.> <UIO-Port-Nr.>– <UIO-Port-Nr.>	Hiermit identifizieren Sie neue Anschlüsse für Eingangskontakte oder Ausgangsrelais.

Beispiel 1: Geben Sie Folgendes ein, um den Ausgang zu öffnen:

```
uio -rc 2 open
```

Beispiel 2: Geben Sie Folgendes ein, um sich den Status der Geräte anzusehen, die an einem auf dem UIO-Port 2 installierten E/A-Zusatzmodul für potenzialfreie Kontakte angeschlossen sind:

```
uio -st 2
```

ups



Einige **ups**-Optionen sind vom USV-Modell abhängig. Möglicherweise unterstützen nicht alle Konfigurationen die Optionen des **ups**-Befehls.

Zugriff: Superuser, Administrator, Gerätebenutzer

Beschreibung: Hiermit steuern Sie die USV und zeigen entsprechende Statusinformationen an. Weitere Informationen zur Bedeutung dieser Optionen für diesen Bildschirm finden Sie im *Benutzerhandbuch* auf der [APC-Website](#).

Option	Argumente	Beschreibung
-c	reboot	Hiermit starten Sie die angeschlossenen Geräte wie folgt: <ul style="list-style-type: none"> • Schaltet die Stromversorgung der USV aus. • Schaltet die Stromversorgung an der USV nach Erreichen des konfigurierten Prozentsatzes des Werts Minimale Batteriekapazität ein. Siehe „cfgshutdn“.
	on	Hiermit schalten Sie die Stromversorgung der USV ein.
	off	Schaltet die Ausgangsversorgung der USV ohne Abschaltverzögerung umgehend ab. Die USV bleibt abgeschaltet, bis Sie sie wieder einschalten.
	graceoff	Schaltet die Ausgangsversorgung der USV nach Ablauf der als Maximal erforderliche Verzögerung eingestellten Wartezeit aus.
	gracereboot	Diese Aktion ist ähnlich der vorher beschriebenen Aktion „reboot“, aber mit einer zusätzlichen Verzögerung vor der Abschaltung. Die verbundenen Geräte werden erst nach Ablauf der in der USV als Maximal erforderliche Verzögerung eingestellten Wartezeit abgeschaltet, deren Berechnung im Benutzerhandbuch unter „Abschaltverzögerungen und PowerChute Network Shutdown“ beschrieben wird.
-c	sleep	Hiermit versetzen Sie die USV in den Ruhezustand, indem Sie ihre Ausgangsversorgung für eine bestimmte Zeit abschalten. Die USV schaltet die Ausgangsversorgung nach Ablauf der als Abschaltverzögerung konfigurierten Wartezeit ab. Wenn die Eingangsversorgung wieder vorliegt, schaltet die USV die Ausgangsversorgung nach Ablauf der als Ruhezustand konfigurierten Wartezeit wieder ein. Siehe „cfgshutdn“.
-c	gracesleep	Hiermit versetzen Sie die USV in den Ruhezustand, indem Sie die Stromversorgung für eine bestimmte Zeit abschalten: <ul style="list-style-type: none"> • Die USV schaltet die Ausgangsversorgung nach Ablauf der als Maximal erforderliche Verzögerung konfigurierten Wartezeit aus, damit PowerChute Network Shutdown seinen Server regulär mit seiner Abschaltverzögerung herunterfahren kann. • Wenn die Eingangsversorgung wieder vorliegt, schaltet die USV die Ausgangsversorgung nach Ablauf der als Ruhezustand konfigurierten Wartezeit wieder ein. Siehe „cfgshutdn“.
-r	start stop	Hiermit starten oder beenden Sie eine Laufzeitkalibrierung. Bei einer Kalibrierung wird die verbleibende Laufzeit neu berechnet. Dazu müssen folgende Voraussetzungen erfüllt sein: <ul style="list-style-type: none"> • Da die USV-Batterien bei einer Kalibrierung vorübergehend entleert werden, können Sie eine Kalibrierung nur bei einer Batteriekapazität von 100 % durchführen. • Damit eine Kalibrierung akzeptiert werden kann, muss die Last mindestens 15 % betragen.
-s	start	Hiermit starten Sie einen USV-Selbsttest.

Option	Argumente	Beschreibung
-b	enter exit	Hiermit steuern Sie den Bypass-Betrieb. Dieser Befehl ist modellspezifisch und für Ihre USV eventuell nicht relevant.
-o#	Off DelayOff On DelayOn Reboot DelayReboot Shutdown DelayShutdown Cancel	<p>Steuern Sie die USV-Steckdosengruppen. Ersetzen Sie # durch die Nummer der Steckdosengruppe.</p> <p>Wenn die Steckdosengruppe den Status „Ein“, hat, akzeptiert die Option die folgenden drei Argumente:</p> <ul style="list-style-type: none"> • Off – Hiermit wird die Steckdosengruppe sofort ausgeschaltet. • DelayOff – Hiermit wird die Steckdosengruppe nach der als Abschaltverzögerung definierten Wartezeit in Sekunden ausgeschaltet. • Reboot – Hiermit wird die Steckdosengruppe sofort ausgeschaltet und anschließend nach der als Neustartdauer und Einschaltverzögerung definierten Wartezeit in Sekunden wieder eingeschaltet. • DelayReboot – Hiermit wird die Steckdosengruppe nach der als Abschaltverzögerung konfigurierten Wartezeit in Sekunden ausgeschaltet und anschließend nach der als Neustartdauer und Einschaltverzögerung konfigurierten Wartezeit in Sekunden wieder eingeschaltet. • Shutdown – Hierdurch wird die Steckdosengruppe neu gestartet, wenn die USV eingeschaltet ist. Wenn sich die USV im Batteriebetrieb befindet, fährt sie die Steckdosengruppe herunter und schaltet sie erst wieder ein, wenn die Netzstromversorgung hergestellt wurde. • DelayShutdown – Hiermit wird die Steckdosengruppe nach der als Abschaltverzögerung definierten Wartezeit in Sekunden ausgeschaltet. • Cancel – Hiermit brechen Sie vorherige Befehle ab, z. B. Abschalten. <p>Wenn die Steckdosengruppe den Status off hat, akzeptiert die Option zwei Argumente:</p> <ul style="list-style-type: none"> • On – Hiermit wird die Steckdosengruppe sofort eingeschaltet. • DelayOn – Hiermit wird die Steckdosengruppe nach der als Einschaltverzögerung definierten Wartezeit in Sekunden eingeschaltet. <p>Die Einschaltverzögerung, die Abschaltverzögerung und die Neustartdauer müssen über die Benutzeroberfläche konfiguriert werden.</p>
-os#		<p>Hiermit zeigen Sie den Status („on“, „off“ oder „rebooting“) aller Steckdosengruppen an.</p> <p>Geben Sie die Nummer der Steckdosengruppe an, deren Status Sie sich ansehen möchten. Geben Sie beispielsweise <code>ups -os1</code> ein, um den Status der Steckdosengruppe 1 angezeigt zu bekommen.</p> <p>Aber:</p> <p>a) Wenn Sie diese Option für eine USV mit einer Hauptsteckdosengruppe verwenden: 1 – identifiziert die Hauptsteckdosengruppe, 2 – identifiziert die geschaltete Steckdosengruppe 1, 3 – identifiziert die geschaltete Steckdosengruppe 2 usw.</p> <p>b) Bei einer USV OHNE Hauptsteckdosengruppe: 1 – identifiziert die geschaltete Steckdosengruppe 1 usw.</p>
-st		Hiermit zeigen Sie den Status der USV an.
-a	start	Hiermit testen Sie den akustischen USV-Alarm.

USV-Befehlsoptionen für MGE Galaxy-spezifische USV-Geräte:



Diese Befehle stehen nur für die USV-Geräte MGE Galaxy 300 und MGE Galaxy 7000 zur Verfügung. Manche Optionen stehen möglicherweise nur für bestimmte USV-Modelle zur Verfügung.

Option	Argument	Beschreibung
-input	<phase#> all	Hiermit zeigen Sie die Eingangswerte für die ausgewählte Phase der USV an. Geben Sie „all“ ein, um die Information für alle Phasen der USV anzugeben.
	voltage current frequency all	Geben Sie den Eingangswert für den ups-Befehl ein. Beispiel: ups -input 2 frequency Hiermit wird die Frequenz für Phase 2 der USV angezeigt.
-bypass	<phase#> all	Hiermit zeigen Sie die Eingangswerte für die ausgewählte Phase der Bypass-Leitung an. Geben Sie „all“ ein, um alle Phasen der Bypass-Leitung anzuzeigen.
	voltage current frequency all	Geben Sie den Eingangswert für den ups-Befehl ein. Beispiel: ups -bypass 2 current Hiermit wird der Strom für Phase 2 der Bypass-Leitung angezeigt.
-output	<phase#> all	Hiermit zeigen Sie die Ausgangswerte für die ausgewählte Phase der USV an. Geben Sie „all“ ein, um die Information für alle Phasen der USV anzugeben.
	voltage current load power perclload pf frequency all	Geben Sie den Ausgangswert für den ups-Befehl ein. Beispiel: ups -output 2 perclload Hiermit wird die Last in Prozent für Phase 2 der USV angezeigt.
-batt		Hiermit zeigen Sie den Batteriestatus der USV an.
-about		Hiermit zeigen Sie Informationen zur USV an.
-al	c w	Hiermit zeigen Sie alle vorhandenen Alarmer an. Geben Sie „c“ oder „w“ an, damit das Display entweder nur kritische (c) oder nur warnende (w) Alarmer anzeigt.

Beispiel 1: Geben Sie Folgendes ein, um eine Laufzeitkalibrierung zu starten:

```
ups -r start
```

Beispiel 2: Geben Sie Folgendes ein, um die Steckdosengruppe 2 an einer Smart-UPS XLM sofort auszuschalten:

```
ups -o2 off
```

upsabout



Alle über den Befehl **upsabout** angeführten USV-Informationen sind möglicherweise nicht bei allen USV-Geräten verfügbar.

Zugriff. Superuser, Administrator, Gerätebenutzer

Beschreibung: Zeigt Informationen zur USV an, einschließlich:

Modell, Artikelnummer, Seriennummer, USV-Firmwareversion, Herstellungsdatum, Nennscheinleistung, Nennwirkleistung, Artikelnummer interne Batterie sowie Artikelnummer externe Batterie.

upswupdate



Dieser Befehl ist möglicherweise nicht bei allen USV-Geräten verfügbar.

Zugriff Superuser, Administrator, Gerätebenutzer

Beschreibung: Hiermit starten Sie die Aktualisierung der USV-Firmware:



Folgen Sie den Anweisungen in der Befehlszeile, um festzulegen, ob die Ausgangsversorgung der USV vor einer Firmware-Aktualisierung ausgeschaltet werden soll.

- Die Knowledge-Base-Artikel [FA164737](#) und [FA170679](#) auf der [APC-Website](#) enthalten Informationen zum Aufrufen einer Firmware-Aktualisierungsdatei sowie weitere Anweisungen.
- Aktualisierung mit einem USB-Speichermedium (nur AP9631 und AP9635):
 - Das USB-Speichermedium muss die USB-Version v1.1 unterstützen und in FAT, FAT16 oder FAT32 formatiert ist.
 - Die Firmware-Aktualisierungsdatei kann in das Root-Verzeichnis des USB-Speichermediums oder in ein Verzeichnis „/upsw/“ auf dem USB-Speichermedium gespeichert werden.
 - Stecken Sie das USB-Speichermedium in den USB-Anschluss der Netzwerkmanagement-Karte.



Hinweis: Die Aktualisierung der Firmware kann einige Minuten dauern. Entfernen Sie das USB-Speichermedium nicht von der Netzwerkmanagement-Karte, bevor die Aktualisierung der USV-Firmware abgeschlossen ist. Wenn Sie das USB-Speichermedium vor Beendigung entfernen, kann die Firmware-Aktualisierung nicht erfolgreich abgeschlossen werden.

Option	Argument	Beschreibung
-install	-file <Dateipfad> -ver <Firmware-Version>	<p>Hinweis: Diese Option ist nicht bei allen USV-Geräten verfügbar.</p> <p>Hiermit installieren Sie eine USV-Firmware-Aktualisierung von einem USB-Speichermedium, das sich im USB-Anschluss der Netzwerkmanagement-Karte befindet. Fügen Sie den Dateipfad zur Firmware-Aktualisierungsdatei auf dem USB-Speichermedium hinzu. Der USB-Anschluss ist auf der Netzwerkmanagement-Karte mit dem Laufwerksbuchstaben „C:“ installiert.</p> <p>Wenn sich mehrere Firmware-Aktualisierungen auf dem USB-Speichermedium befinden, stellen Sie die Firmware-Version in folgendem Format bereit: [USV-ID-Nummer] [USV-Firmware-Version]</p> <p>Hinweis: Die USB-ID-Nummer finden Sie mithilfe des nachfolgend beschriebenen Befehls „-info“.</p>
-info	-file <Dateipfad> -ver <Firmware-Version>	<p>Hiermit erhalten Sie Informationen über die auf dem USB-Speichermedium im USB-Anschluss Ihrer Netzwerkmanagement-Karte verfügbare Firmware.</p> <p>Fügen Sie den Dateipfad zur Firmware-Aktualisierungsdatei auf dem USB-Speichermedium hinzu. Wenn sich mehrere Firmware-Aktualisierungen auf dem USB-Speichermedium befinden, stellen Sie die Firmware-Version in folgendem Format bereit: [USV-ID-Nummer] [USV-Firmware-Version]</p>
-list		Hiermit zeigen Sie eine Liste der verfügbaren Firmware-Versionen auf dem USB-Speichermedium im USB-Anschluss der Netzwerkmanagement-Karte an.
-status		Hiermit prüfen Sie den Status einer bereits gestarteten Firmware-Aktualisierung.
-lastresult		Hiermit zeigen Sie das Ergebnis der letzten versuchten Firmware-Aktualisierung an.

Beispiel 1:

```
upsfwupdate -info -ver "ID11 UPS 03.8"
Searching for version 'UPS 03.8'... found.
Version 'UPS 03.8' at C:\SMX11UPS_03-8.enc
E000: Success
Update File: C:\SMX11UPS_03-8.enc
Compatible with UPS: Yes
Update Version: UPS 03.8
```

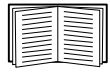
Beispiel 2:

```
upsfwupdate -status
E000: Success
Status: 3k/257k (1%)
```


user

Zugriff: Superuser, Administrator

Beschreibung: Hiermit konfigurieren Sie den Benutzernamen und das Kennwort für die einzelnen Kontotypen und konfigurieren die Wartezeit bis zur automatischen Abmeldung bei Inaktivität. (Sie können einen Benutzernamen nicht editieren, sondern müssen ihn löschen und dann einen neuen Benutzer anlegen.)



Informationen zu den Berechtigungen, die Sie den einzelnen Kontotypen (Superuser, Administrator, Gerätebenutzer, Benutzer „schreibgeschützt“, Nur Netzwerk-Benutzer) erteilen können, finden Sie im *Benutzerhandbuch* auf der [APC-Website](#).

Option	Argument	Beschreibung
-n	<Benutzer>	Hier wird der Benutzer angezeigt.
-cp	<Aktuelles Passwort>	Für einen Super User müssen Sie das aktuelle Passwort festlegen. HINWEIS: Die Einstellung -cp ist nur bei einer Remote-Änderung des Passworts des Super Users erforderlich.
-pw	<Kennwort des Benutzers>	Hiermit legen Sie die entsprechenden Optionen für einen Benutzer fest. HINWEIS: Die Beschreibung muss in Anführungszeichen stehen.
-pe	<Benutzerberechtigung>	
-d	<Benutzerbeschreibung>	
-e	enable disable	Hiermit aktivieren oder deaktivieren Sie den Zugriff eines bestimmten Benutzerkontos.
-te	enable disable	Hiermit aktivieren oder deaktivieren Sie Touchscreen-Zugriff.
-tp	<Touchscreen-PIN-Nummer>	Noch nicht verfügbar.
-tr	enable disable	Hiermit aktivieren oder deaktivieren Sie den Override der Touchscreen-Remote-Autorisierung. Diese Option steht nur bei bestimmten Geräten zur Verfügung. Wenn Sie diese Override-Funktion aktivieren, erlaubt die Netzwerkmanagement-Karte, dass sich ein lokaler Benutzer mit dem Kennwort für die Netzwerkmanagement-Karte anmeldet, das lokal auf der Netzwerkmanagement-Karte gespeichert ist.
-st	<Sitzungs-Timeout>	Hiermit geben Sie an, wie lange eine Sitzung dauert bzw. bis zum Abmelden eines Benutzers wartet, wenn keine Tasteneingaben erfolgen.
-sr	enable disable	Hiermit umgehen Sie RADIUS durch Verwenden der seriellen Konsolen-(Befehlszeilen-) Verbindung, auch Override der seriellen Remote-Authentifizierung genannt.
-el	enable disable	Hiermit geben Sie die Farbcodierung des Ereignisprotokolls an.
-lf	tab csv	Hiermit legen Sie das Format für den Export einer Protokolldatei fest.
-ts	us metric	Hiermit legen Sie die Temperatureinheit (Fahrenheit oder Celsius) fest.
-df	<mm/dd/yyyy dd.mm.yyyy mmm-dd-yy dd-mmm-yy yyyy-mm-dd>	Hiermit legen Sie ein Datumsformat fest.
-lg	<Sprachcode (z. B. enUs)>	Hiermit legen Sie eine Benutzersprache fest. Geben Sie „lang“ ein, um alle verfügbaren Sprachen anzuzeigen.
-del	<Benutzername>	Hiermit löschen Sie einen Benutzer.
-l		Hiermit zeigen Sie die Liste der aktuellen Benutzer an.

Beispiel: Geben Sie Folgendes ein, um die Wartezeit bis zur automatischen Abmeldung für Benutzer JMurphy zu 10 Minuten zu ändern:

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

userdfit

Zugriff: Superuser, Administrator

Beschreibung: Zusatzfunktion zum Befehl „user“ zur Festlegung von Standard-Benutzerpräferenzen. Es gibt zwei Hauptfunktionen für die Standard-Benutzereinstellungen:

- Bestimmen Sie die Standardwerte, mit denen die einzelnen Felder befüllt werden, wenn über das Superuser- oder Administrator-Konto ein neuer Benutzer angelegt wird. Diese Werte können geändert werden, bevor die Einstellungen im System übernommen werden.
- Bei Remote-Usern (nicht im System gespeicherte Benutzerkonten mit Remote-Authentifizierung wie etwa RADIUS) handelt es sich um jene Werte, die für die nicht vom Authentifizierungsserver bereitgestellten Werte verwendet werden.

Wenn beispielsweise ein RADIUS-Server keine Temperaturpräferenz für den Benutzer bereitstellt, wird der in diesem Abschnitt festgelegte Wert verwendet.

Option	Argument	Beschreibung
-e	<enable disable> (Enable)	Der Benutzer wird bei der Erstellung standardmäßig aktiviert oder deaktiviert. Entfernen Sie (Enable) am Ende.
-pe	<Administrator Device Read-Only Network-Only> (Benutzerberechtigung)	Hiermit legen Sie die Berechtigungsstufe und den Kontotyp des Benutzers fest.
-d	<Benutzerbeschreibung>	Hiermit geben Sie eine Benutzerbeschreibung an. Die Beschreibung muss in Anführungszeichen stehen.
-st	<Sitzungs-Timeout> Minute(n)	Hiermit legen Sie ein standardmäßiges Sitzungs-Timeout fest.
-bl	<Fehlgeschlagene Anmeldeversuche>	Anzahl fehlgeschlagener Anmeldeversuche, die einem Benutzer zur Verfügung stehen, bevor das System das Konto deaktiviert. Bei Erreichen der maximalen Anzahl wird eine Meldung angezeigt, die den Benutzer über die Sperre seines Kontos informiert. Zur erneuten Aktivierung des Kontos und Freischaltung der Benutzeranmeldung ist das Superuser- oder ein Administrator-Konto erforderlich. HINWEIS: Ein Superuser-Konto kann nicht gesperrt, aber ggf. manuell deaktiviert werden.
-el	<enable disable> (Ereignisprotokoll-Farbcodierung)	Hiermit aktivieren oder deaktivieren Sie die Farbcodierung des Ereignisprotokolls.
-lf	<tab csv> (Protokoll-Exportformat)	Hiermit legen Sie das Protokoll-Exportformat fest: tab oder CSV.
-ts	<us metric> (Temperaturskala)	Hiermit geben Sie die Temperaturskala des Benutzers an. Diese Einstellung wird auch dann vom System verwendet, wenn keine Benutzerpräferenz verfügbar ist (z. B. E-Mail-Benachrichtigungen).
-df	<mm/dd/yyyy dd.mm.yyyy mmm-dd-yy dd-mmm-yy yyyy-mm-dd> (Datumsformat)	Hiermit legen Sie das bevorzugte Datumsformat des Benutzers fest.
-lg	<Sprachcode (enUs, etc.)>	Hiermit legen Sie die bevorzugte Sprache des Benutzers fest. Geben Sie „lang“ ein, um alle verfügbaren Sprachen anzuzeigen.

Option	Argument	Beschreibung
-sp	<enable disable>	Hiermit aktivieren oder deaktivieren Sie das sichere Kennwort.
-pp	<Intervall in Tagen>	Intervall, in dem das Kennwort gewechselt werden muss.

Beispiel. Geben Sie Folgendes ein, um das standardmäßige Sitzungs-Timeout des Benutzers auf 60 Minuten einzustellen:

```
userdfilt -st 60
E000: Success
```

web

Zugriff: Super User, Administrator, Nur Netzwerk

Beschreibung: Hiermit aktivieren Sie den Zugriff auf die Benutzeroberfläche über HTTP oder HTTPS.

HINWEIS: In Version v6.8.0 und neuer ist HTTP deaktiviert und HTTPS standardmäßig aktiviert.

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

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

Option	Argument	Beschreibung
-h	enable disable	Hiermit aktivieren oder deaktivieren Sie den Zugriff auf die Benutzeroberfläche für HTTP.
-hs	enable disable	<p>HSTS (HTTP Strict Transport Security) ist ein HTTP-Header, der verwendet wird, um unsichere HTTP-Anforderungen an eine HTTPS-Version der Seite umzuleiten. Dies ist sicherer als die einfache Verwendung einer Umleitung, da dies nicht anfällig für Man-in-the-Middle-Angriffe ist, weil hierbei kein unsicherer HTTP-Kanal verwendet wird.</p> <p>Diese Funktion legt den Strict-Transport-Security-Header im Browser fest, wenn ein Benutzer zum ersten Mal eine HTTPS-Seite auf der Netzwerkmanagement-Karte besucht, und ist nur verfügbar, wenn sowohl HTTP als auch HTTPS aktiviert sind. Sie weist den Browser an, niemals eine unsichere Version der Seite zu besuchen, wenn der Header gültig ist.</p> <p>HSTS funktioniert nur, wenn ein nicht selbstsigniertes Zertifikat auf der Netzwerkmanagement-Karte geladen ist. Daher ist es notwendig, ein Zertifikat auf die Netzwerkmanagement-Karte zu laden, das vom Browser als vertrauenswürdig eingestuft wird.</p>
-s	enable disable	<p>Hiermit aktivieren oder deaktivieren Sie den Zugriff auf die Benutzeroberfläche für HTTPS.</p> <p>Wenn HTTPS aktiviert ist, werden die Daten während der Übertragung verschlüsselt und über ein digitales Zertifikat mittels SSL/TLS authentifiziert.</p>
-mp	<minimum protocol>	Geben Sie das Mindestprotokoll an, das die Weboberfläche verwenden soll: SSL v3.0, TLS v1, TLS v1.1 oder TLS v1.2.
-ph	<HTTP-Port-Nr.>	Hiermit legen Sie den TCP/IP-Port fest, über den der HTTP-Datenaustausch mit der Netzwerkmanagement-Karte erfolgen soll (Voreinstellung: 80). Der übrige zulässige Bereich ist 5000-32768.

Option	Argument	Beschreibung
-ps	<HTTPS-Port-Nr.>	Hiermit legen Sie den TCP/IP-Port fest, über den der HTTPS-Datenaustausch mit der Netzwerkmanagement-Karte erfolgen soll (Voreinstellung: 443). Der übrige zulässige Bereich ist 5000-32768.
-lsp	enable disable	Zugriff auf die Seite „Begrenzter Status“ im Web-UI aktivieren oder deaktivieren.
-lsd	enable disable	Aktivieren oder deaktivieren Sie die Seite „Begrenzter Status“, die als Standardseite verwendet wird, wenn Sie auf die IP oder den Hostnamen des Geräts in einem Webbrowser zugreifen.

Beispiel: Geben Sie Folgendes ein, um jeglichen Zugriff auf die Benutzeroberfläche für HTTPS zu verhindern:
`web -s disable`

whoami

Zugriff: Superuser, Administrator, Gerätebenutzer, Benutzer „schreibgeschützt“, Nur Netzwerk-Benutzer

Beschreibung: Zeigt Anmeldeinformationen des aktuellen Benutzers an.

Beispiel:

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

xferINI

Zugriff: Superuser, Administrator. Dieser Befehl funktioniert nur über die serielle/lokale Konsolen-Befehlszeile.

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

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

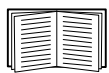
xferStatus

Zugriff: Superuser, Administrator

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

Beispiel:

```
xferStatus
E000: Success
Result of last file transfer: OK
```



Eine Beschreibung der Codes für die Übertragungsergebnisse finden Sie im *Benutzerhandbuch* auf der [APC-Website](#).

Copyright-Hinweise

Kryptographische Bibliothek cryptlib

cryptlib Copyright © Digital Data Security New Zealand Ltd 1998.

Berkeley Database

Copyright © 1991, 1993 Verwaltungsrat der Universität Kalifornien. Alle Rechte vorbehalten.

Weiterverbreitung und Verwendung in nicht kompilierter oder kompilierter Form, mit oder ohne Veränderung, sind unter den folgenden Bedingungen zulässig:

1. Weiterverbreitete nicht kompilierte Exemplare müssen das obige Copyright, diese Liste der Bedingungen und den folgenden Haftungsausschluss im Quelltext enthalten.
2. Weiterverbreitete kompilierte Exemplare müssen das obige Copyright, diese Liste der Bedingungen und den folgenden Haftungsausschluss in der Dokumentation und/oder anderen Materialien, die mit dem Exemplar verbreitet werden, enthalten.
3. Sämtliche Werbematerialien, in denen Funktionen oder die Nutzung dieser Software erwähnt werden, müssen folgenden Vermerk enthalten: Dieses Produkt enthält Software, die von der Universität Kalifornien, Berkeley und den Beitragsleistenden entwickelt wurde.
4. Weder der Name der Universität noch die Namen der Beitragsleistenden dürfen zum Kennzeichnen oder Bewerben von Produkten, die von dieser Software abgeleitet wurden, ohne spezielle vorherige schriftliche Genehmigung verwendet werden.

DIESE SOFTWARE WIRD VON DEN VERWALTUNGSRÄTEN UND BEITRAGSLEISTENDEN „WIE BESEHEN“ ZUR VERFÜGUNG GESTELLT UND ALLE AUSDRÜCKLICHEN ODER STILLSCHWEIGENDEN GEWÄHRLEISTUNGEN, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDEN GEWÄHRLEISTUNGEN DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, WERDEN ABGELEHNT. AUF KEINEN FALL SIND DIE VERWALTUNGSRÄTE ODER DIE BEITRAGSLEISTENDEN FÜR IRGENDWELCHE DIREKTEN, INDIREKTEN, ZUFÄLLIGEN, SPEZIELLEN, BEISPIELHAFTEN ODER FOLGENDEN SCHÄDEN (UNTER ANDEREM VERSCHAFFEN VON ERSATZGÜTERN ODER -DIENSTLEISTUNGEN; EINSCHRÄNKUNG DER NUTZUNGSFÄHIGKEIT; VERLUST VON NUTZUNGSFÄHIGKEIT; DATEN; PROFIT ODER GESCHÄFTSUNTERBRECHUNG), WIE AUCH IMMER VERURSACHT UND UNTER WELCHER VERPFLICHTUNG AUCH IMMER, OB IN VERTRAG, STRIKTER VERPFLICHTUNG ODER UNERLAUBTE HANDLUNG (INKLUSIVE FAHRLÄSSIGKEIT) VERANTWORTLICH, AUS WELCHEM WEG SIE AUCH IMMER DURCH DIE BENUTZUNG DIESER SOFTWARE ENTSTANDEN SIND, SOGAR, WENN SIE AUF DIE MÖGLICHKEIT EINES SOLCHEN SCHADENS HINGEWIESEN WORDEN SIND.

Weltweiter Kundendienst von APC by Schneider Electric

Der Kundendienst für dieses oder jedes andere Produkt steht Ihnen kostenfrei wie folgt zur Verfügung:

- Besuchen Sie die Schneider Electric-Webseite. Dort können Sie auf die Dokumente der Schneider Electric Knowledge Base zugreifen und Anfragen an den Kundendienst senden.
 - www.apc.com (Firmensitz)
Auf der lokalisierten Schneider Electric-Website des gewünschten Landes können Sie die Informationen des Kundendienstes in der entsprechenden Sprache abrufen.
 - www.apc.com/support/
Weltweiter Kundendienst über Abfragen der Schneider Electric Knowledge Base sowie mittels e-Support.
- Wenden Sie sich per Telefon oder E-Mail an den Schneider Electric-Kundendienst.
 - Lokale, länderspezifische Zentren: Kontaktinformationen finden Sie unter www.apc.com/support/contact.

Wenden Sie sich an die Vertretung oder einen anderen Händler, bei dem Sie Ihr Produkt erworben haben, um zu erfahren, wo Sie Kundendienstunterstützung erhalten können.