Befehlszeilenhandbuch

Netzwerkmanagement-Karte 3, Firmwareversion 3.1.x

AP9640, AP9641, AP9643

USV-Geräte mit einer eingebetteten Netzwerkmanagement-Karte 3, wie Smart-USV-Geräte mit dem Präfix SRT, Smart-USV Ultra-Geräte mit dem Präfix SRTL oder Smart-USV Modular Ultra-Geräte mit dem Präfix SRYLF.

990-91149H-005
6/2024

Schneider Electric

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 JEWEILIGE 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.

Befehlszeilenoberfläche

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.

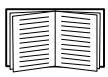
Um auf die in diesem CLI-Handbuch beschriebene Befehlszeilenschnittstelle zugreifen zu können, muss auf der Netzwerkmanagement-Karte die Smart-UPS-, Single Phase Symmetra- oder Smart-UPS Ultra 5-20 kVA-Firmware installiert sein und die Netzwerkmanagement-Karte muss in einem USV-Modell der Reihe Smart-UPS oder Single Phase Symmetra eingebaut sein. Weitere Informationen zu USV-Modellen, die mit Ihrer Netzwerkmanagement-Karte kompatibel sind, finden Sie im Knowledge Base-Artikel **FA237786**.

Geben Sie zur Anmeldung den Benutzernamen und das Kennwort unter Beachtung der Groß-/Kleinschreibung ein (standardmäßig „**apc**“ und „**apc**“ für einen Superuser). Der Standardbenutzername für einen Gerätebenutzer ist „**device**“. Ein Nur-Lesen-Benutzer hat eingeschränkten Zugriff auf die Befehlszeilenschnittstelle.

HINWEIS: Sie werden 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 Benutzerkonto eine Stunde lang gesperrt bzw. bis ein Superuser oder Administrator das Konto entsperrt.

Weitere Informationen finden Sie im **Benutzerhandbuch** für die Netzwerkmanagement-Karte 3 (für AP9640, AP9641, AP9643 und SRTL/SRYLF-Geräte).

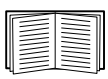


Sollten Sie Ihren Benutzernamen oder Ihr Kennwort vergessen haben, lesen Sie bitte die Anleitung unter **Wiederherstellen des Zugriffs bei vergessenem Kennwort** im ***Benutzerhandbuch***.

Remote-Zugriff auf die Befehlszeilenoberfläche

Sie können über Telnet oder SSH auf die Befehlszeile zugreifen. Nur SSH ist standardmäßig aktiviert.

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. Weitere Informationen finden Sie unter **console**.

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.

1. Verwenden Sie den folgenden Beispielbefehl, um per SSH auf die Netzwerkmanagement-Karte zuzugreifen:

   ```
   ssh -c aes256-ctr apc@156.205.14.141
   ```

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

2. Geben Sie den Benutzernamen und das Kennwort ein.

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

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.

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

Lokaler Zugriff auf die Befehlszeilenschnittstelle

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

1. Verbinden Sie das mitgelieferte Micro-USB-Kabel (Teilenummer 960-0603) mit einem USB-Anschluss des Computers und dem Konsolenport der Netzwerkmanagement-Karte.
2. Geben Sie in der Windows-Suche „Gerätemanager“ ein oder öffnen Sie diesen über die Systemsteuerung. Wählen Sie „Ports“ und notieren Sie sich die COM-Portnummer, die der NMC zugewiesen wurde.
3. Führen Sie ein Terminalprogramm (z. B. Terminal-Emulatorprogramme Drittanbieter wie HyperTerminal, PuTTy oder Tera Term) aus und konfigurieren Sie die (in Schritt 2 notierte) COM-Schnittstelle mit 9600 Bit/s, 8 Datenbits, keinem Paritätsbit, 1 Stoppbit und ohne Datenflusskontrolle. Speichern Sie die Änderungen.
4. Drücken Sie die EINGABETASTE ggf. mehrmals, um die Eingabeaufforderung **User Name (Benutzername)** aufzurufen.
5. Geben Sie den Benutzernamen und das Kennwort ein.

   HINWEIS: Der Benutzername lautet beim ersten Einloggen über das Superuser-Konto „apc“. Nach dem Einloggen werden Sie aufgefordert, ein neues Kennwort zu erstellen.

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.x
(c)Copyright 2022 All Rights Reserved Smart-UPS APP               vx.x.x.x
-------------------------------------------------------------------------------
Name     : Test Lab                                    Date : 01/15/2022
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+
-------------------------------------------------------------------------------
IPv4                 : Enabled          IPv6               : Enabled
Ping Response        : Enabled
-------------------------------------------------------------------------------
HTTP                 : Disabled         HTTPS              : Enabled
FTP                  : Disabled         Telnet             : Disabled
SSH/SCP              : Enabled          SNMPv1             : Disabled
SNMPv3               : Disabled         Modbus TCP         : Disabled
BACnet/IP            : Disabled
-------------------------------------------------------------------------------
Super User           : Enabled         User authentication: Local
Administrator        : Disabled        Device User        : Disabled
Read-Only User       : Disabled        Network-Only User  : Disabled

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 Smart-UPS USV.

  ```
  Network Management Card AOS    vx.x.x.x
  Smart-UPS- und Matrix-UPS-APP  vx.x.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 : 01/15/2022
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 Alarme ansehen.

```
User : Super User
```

Statusfelder in der Hauptmaske.

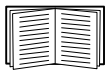
- Das Feld **Stat** zeigt den Status der Netzwerkmanagement-Karte an. Der mittlere Status variiert in Abhängigkeit davon, ob IPv4, IPv6 oder beides aktiv ist, wie in der zweiten Tabelle unten angegeben.

```
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 DHCP- oder 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 TABULATORTASTE, 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: `-pw <Benutzerpasswort>`
[ ]	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 Alarme anzusehen:

```
alarmcount -p critical
```

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

Befehlsrückgabe-Codes

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

Die Befehlszeile meldet die Verarbeitung aller Befehle im folgenden Format:

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

Code	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, Nur-Lesen-Benutzer, Nur-Netzwerk-Benutzer

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: Anzeigen der Alarm-Informationen.

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

Beispiel: Geben Sie Folgendes ein, um die Anzahl der aktiven Warnungen angezeigt zu bekommen:

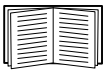
```
alarmcount -p warning
```

bacnet

Zugriff: Superuser, Administrator

Beschreibung: Anzeigen und definieren der BACnet-Einstellungen.

Dieser Befehl ist nicht bei allen USV-Geräten verfügbar.



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:** BACnet kann erst aktiviert werden, nachdem das Passwort für die Gerätekommunikationskontrolle (-pw) eingerichtet wurde.
-d	0-4194303	Eine eindeutige Bezeichnung für dieses 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 der Zeitraum in Millisekunden, während dessen 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: • 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.

Option	Argumente	Beschreibung
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.
-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	<IPv4 address or DNS host>	Die IP-Adresse oder der FQDN (Fully Qualified Domain Name) des BBMD, mit der/dem diese Netzwerkmanagement-Karte registriert wird.
-rpo	0 - 65535	Der Port des BBMD, mit dem diese Netzwerkmanagement-Karte registriert wird.
-fttl	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.
-fst		Der Registrierungsstatus fremder Geräte.

Beispiel 1: Um die aktuellen BACnet-Einstellungen zu sehen, geben Sie Folgendes ein:

```
bacnet
```

Beispiel 2: Um BACnet zu aktivieren, geben Sie Folgendes ein:

```
bacnet -S enable
```

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	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.
-c	enable | disable	Nur für die Startmethode `dhcp`. Hiermit aktivieren oder deaktivieren Sie die Vorschrift, dass der DHCP-Server das APC-Cookie bereitstellen muss.

Option	Argument	Beschreibung
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 1: Um einen DHCP-Server zu verwenden, um die Netzwerkeinstellungen zu beziehen, geben Sie Folgendes ein:

```
boot -b dhcp
```

Beispiel 2: Um die Vorschrift zu aktivieren, dass der DHCP-Server das APC-Cookie bereitstellen muss, geben Sie Folgendes ein:

```
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
```

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 einen USV-Neustart 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 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	0–30	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	0.0–336.0	Hiermit legen Sie die Ruhezeit in Stunden fest. Das Argument kann eine Zahl zwischen 0,0 und 336,0 sein.
-rsc	00 | 15 | 30 | 45 | 60 | 75 | 90	Hiermit legen Sie die minimale Batteriekapazität als prozentualen Anteil der Gesamtkapazität fest.

Beispiel 1: Um alle von diesem USV-Gerät unterstützten Shutdown-Parameter anzuzeigen, geben Sie Folgendes ein:

```
cfgshutdn -all
```

Beispiel 2: Um die Dauer einer schwachen Batterie auf 5 Minuten zu setzen, geben Sie Folgendes ein:

```
cfgshutdn -lo 5
```

Die Optionen des Befehls cfgshutdn für USV-Geräte, auf denen die Anwendung Smart-USV Ultra 5-20 kW läuft:

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.
-lo	0–30	Hiermit legen Sie die NMC-Restlaufzeit in Minuten fest.
-pod	0–600	Hiermit legen Sie die Einschaltverzögerung in Sekunden fest.
-pfd	0–32767	Hiermit legen Sie die Ausschaltverzögerung in Sekunden fest.
-rbd	4–300	Hiermit legen Sie die Neustartdauer in Sekunden fest.

Option	Argument	Beschreibung
`-mrr`	`0-32767`	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.
`-lsb`	`disabled, 5-32767`	Hiermit deaktivieren Sie den Lastabwurf oder aktivieren ihn und legen (in Sekunden) fest, wie lange die USV im Akkubetrieb eingeschaltet bleibt, bevor sie ausgeschaltet wird.
`-lsr`	`disabled, 0-3600`	Hiermit deaktivieren Sie den Lastabwurf oder aktivieren ihn und legen solange die Batterie noch funktioniert, die verbleibende Laufzeit (in Sekunden) fest, bevor die USV ausgeschaltet wird.
`-lss`	`enable | disable`	Hiermit aktivieren oder deaktivieren Sie das Überspringen der Verzögerung beim Ausschalten der USV.
`-lsp`	`enable | disable`	Hiermit geben Sie an, ob die USV ausgeschaltet bleibt, wenn die Stromversorgung wiederhergestellt wurde.
`-sl`	`0.0-336.0`	Hiermit legen Sie die Ruhezeit in Stunden fest. Das Argument kann eine Zahl zwischen 0,0 und 336,0 sein.

Beispiel 3: Um die Ausschaltverzögerung auf 120 Sekunden (2 Minuten) einzustellen, geben Sie Folgendes ein:
`cfgshutdn -pfd 120`

cfgoutlet

Dieser Befehl ist nicht bei allen USV-Geräten verfügbar.

Zugriff: Superuser, Administrator, Gerätebenutzer

Beschreibung: Konfigurieren Sie die Parameter der Stromanschlussgruppe: Hier können Sie die Ein- und Ausschaltverzögerungen und den Lastabwurf der Stromanschlussgruppen anzeigen und konfigurieren.

Bei der Einstellung der Parameter ist die Stromanschlussgruppe 1 die ungeschaltete Stromanschlussgruppe und 2 die geschaltete Stromanschlussgruppe 1 usw., es sei denn, das USV-Gerät verfügt nicht über eine ungeschaltete Stromanschlussgruppe; in diesem Fall ist die Stromanschlussgruppe 1 die geschaltete Stromanschlussgruppe 1 usw. Durch Eingabe von `cfgoutlet ?` werden das angeschlossene USV-Gerät und die zugehörigen Stromanschlussgruppennummern beschrieben.

Option	Argument	Beschreibung
`-all`		Hiermit lassen Sie sich alle verfügbaren Shutdown-Parameter für Stromanschlussgruppen für diese USV anzeigen.
`-pod`	`[Stromanschlussgruppe Nr.] 0-600`	Hiermit legen Sie die Einschaltverzögerung in Sekunden fest.
`-pfd`	`[Stromanschlussgruppe Nr.] 0-32767`	Hiermit legen Sie die Ausschaltverzögerung in Sekunden fest.
`-rbd`	`[Stromanschlussgruppe Nr.] 4-300`	Hiermit legen Sie die Neustartdauer in Sekunden fest.

Option	Argument	Beschreibung
-mrr	[Stroman-schlussgruppe Nr.] 0-32767	Legen Sie die Mindestlaufzeit für den Neustart in Sekunden fest.
-lsb	[Stroman-schlussgruppe Nr.] deaktiviert, 5-32767	Hiermit deaktivieren Sie den Lastabwurf oder aktivieren ihn und legen (in Sekunden) fest, wie lange die USV im Akkubetrieb eingeschaltet bleibt, bevor sie ausgeschaltet wird.
-lsr	[Stroman-schlussgruppe Nr.] deaktiviert, 0-3600	Hiermit deaktivieren Sie den Lastabwurf oder aktivieren ihn und legen (in Sekunden) die verbleibende Laufzeit fest, bevor die USV ausgeschaltet wird.
-lss	[Stroman-schlussgruppe Nr.] aktivieren | deaktivieren	Hiermit aktivieren oder deaktivieren Sie das Überspringen der Verzögerung beim Ausschalten der USV.
-lsp	[Stroman-schlussgruppe Nr.] aktivieren | deaktivieren	Hiermit geben Sie an, ob die USV ausgeschaltet bleibt, wenn die Stromversorgung wiederhergestellt wurde.

Beispiel 1: Um alle Einstellungen der Ausgangskonfiguration für dieses USV-Gerät anzuzeigen, geben Sie Folgendes ein:

```
cfgoutlet -all
```

Beispiel 2: So stellen Sie die Ausschaltverzögerung der Stromanschlussgruppe 1 auf 120 Sekunden in einem USV-Gerät mit einer ungeschalteten Stromanschlussgruppe, Typ:

```
cfgoutlet -pfd 2 120
```

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.
-l	97-106	Hiermit legen Sie den unteren Spannungstransferpunkt in VAC fest.

Option	Argument Diese Werte können für verschiedene Geräte unterschiedlich sein.	Beschreibung
`-h`	`127-136`	Hiermit legen Sie den oberen Spannungstransferpunkt in VAC fest.
`-ov`	`100 | 120 | 110 |`	Dient zum Einstellen der Ausgangsspannung, in VAC.
`-s`	`Normal | Reduced | Low`	Hier legen Sie mithilfe von einem der drei Argumente die Sensitivität fest.
`-bu`	`127-148`	Dient zum Einstellen der oberen Bypass-Spannung, in VAC.
`-bl`	`86-100`	Dient zum Einstellen der unteren Bypass-Spannung, in VAC.

Beispiel 1: Um alle Energieeinstellungen für dieses USV-Gerät anzuzeigen, geben Sie Folgendes ein:

```
cfgpower -all
```

Beispiel 2: Um den unteren Übertragungspunkt auf 100 VAC einzustellen, geben Sie Folgendes ein:

```
cfgpower -l 100
```

Um alle Energieeinstellungen für dieses USV-Gerät zu sehen, geben Sie Folgendes ein:

Diese Optionen sind nicht bei allen USV-Geräten verfügbar.

Option	Argument	Beschreibung
`-all`		Hiermit lassen Sie sich alle verfügbaren Leistungsparameter für diese USV anzeigen.
`-rda`	`Nie | 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.
`-lda`	`Nie | 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.
`-rta`	`Nie | 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 „Never“ ein, wenn Sie keinen Alarm bezüglich eines Abfalls der verfügbaren Batterielaufzeit einstellen möchten.

Die Optionen des Befehls cfgpower für USV-Geräte, auf denen die Anwendung Smart-USV Ultra 5-20 kW läuft:

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.
`-l`	`187-192`	Hiermit legen Sie den unteren Spannungstransferpunkt in VAC fest.
`-h`	`218-230`	Hiermit legen Sie den oberen Spannungstransferpunkt in VAC fest.
`-bl`	`160-184`	Dient zum Einstellen der unteren Bypass-Spannung, in VAC.
`-bu`	`220-270`	Dient zum Einstellen der oberen Bypass-Spannung, in VAC.
`-ov`	`120/208 | 120/240 | 100/200`	Dient zum Einstellen der Ausgangsspannung, in VAC.
`-of`	`Auto_50/60 | 50+/-0,1 | 50+/-3,0 | 60+/-0,1 | 60+/-3,0`	Dient zum Einstellen der Ausgangsfrequenz, in Hz.
`-ofsr`	`0,50 | 1,00 | 2,00 | 4,00`	Legen Sie die Anstiegsrate der Ausgangsfrequenz in Hz/Sekunde fest.
`-red`	`Nie | N+1 | N+2`	Stellen Sie die Einstellung für den Redundanzalarm ein.

Beispiel 3: Um die Ausgangsfrequenz auf 60 +/- 3 Hz einzustellen, geben Sie Folgendes ein:

```
cfgpower -of 60+/-3.0
```

cfguio

Dieser Befehl ist nur auf den Karten AP9641 oder AP9643 oder einem eingebetteten NMC3 mit einem universellen Eingabe-/Ausgabe-Anschluss (UIO) verfügbar.

Zugriff: Superuser, Administrator, Gerätebenutzer
Definition: Zeigt oder konfiguriert die von einer angeschlossenen UIO-Sonde verwendeten Parameter.

HINWEIS: Die Temperatureinstellungen werden in Grad Celsius oder Grad Fahrenheit angezeigt, je nachdem, was der angemeldete Benutzer eingestellt hat. Die Temperatureinstellungen werden immer in Grad Celsius gespeichert, so dass nicht alle Werte in Grad Fahrenheit eingestellt werden können.

Option	Argument	Beschreibung
<none>		Zeigt alle angeschlossenen UIO-Sonden und die mit diesen Sonden verbundenen Parameter an.
-thname	[UIO-Anschluss-Nr.] <Name>	Name der Temperatur- oder Temperatur/Feuchtesonde.
-thloc	[UIO-Anschluss-Nr.] <Position>	Position der Temperatur- oder Temperatur/Feuchtesonde.
-tenable	[UIO-Anschluss-Nr.] [min | low | high | max] <aktivieren | deaktivieren>	Aktivieren oder deaktivieren Sie die Erzeugung von Temperaturalarmen für die verschiedenen Temperatureinstellungen.
-tmin	[UIO-Anschluss-Nr.] <0-60 Grad C>	Minimaler Temperaturschwellenwert, ein kritischer Alarm.
-tlow	[UIO-Anschluss-Nr.] <0-60 Grad C>	Niedrige Temperaturschwelle, ein Warnalarm.
-thigh	[UIO-Anschluss-Nr.] <0-60 Grad C>	Hohe Temperaturschwelle, ein Warnalarm.
-tmax	[UIO-Anschluss-Nr.] <0-60 Grad C>	Maximaler Temperaturschwellenwert, ein kritischer Alarm.
-thyst	[UIO-Anschluss-Nr.] <0-10 Grad C>	Temperatur-Hysterese.
-henable	[UIO-Anschluss-Nr.] [min | low | high | max] <aktivieren | deaktivieren>	Aktivieren oder deaktivieren Sie die Erzeugung von Luftfeuchtigkeitsalarmen für die verschiedenen Feuchtigkeitseinstellungen.
-hmin	[UIO-Anschluss-Nr.] <0-60%>	Minimaler Luftfeuchtigkeits-Schwellenwert, ein kritischer Alarm.
-hlow	[UIO-Anschluss-Nr.] <0-60%>	Niedriger Luftfeuchtigkeits-Schwellenwert, ein Warnalarm.
-hhigh	[UIO-Anschluss-Nr.] <0-60%>	Hoher Luftfeuchtigkeits-Schwellenwert, ein Warnalarm.
-hmax	[UIO-Anschluss-Nr.] <0-60%>	Maximaler Luftfeuchtigkeits-Schwellenwert, ein kritischer Alarm.
-hhyst	[UIO-Anschluss-Nr.] <0-20%>	Luftfeuchtigkeits-Hysterese.
-cname	[UIO-Anschluss-Nr.] [Kontakt-Nr.] <Name>	Eingangskontakt-Name.
-cloc	[UIO-Anschluss-Nr.] [Kontakt-Nr.] <Position>	Eingangskontakt-Position.
-cnormst	[UIO-Anschluss-Nr.] [Kontakt-Nr.] <offen | geschlossen>	Eingangskontakt Normalstatus.
-csever	[UIO-Anschluss-Nr.] [Kontakt-Nr.] <Warnung | kritisch>	Eingangskontakt Alarmschwere.

Option	Argument	Beschreibung
-cenable	[UIO-Anschluss-Nr.] [Kontakt-Nr.] <aktivieren | deaktivieren>	Aktivieren oder deaktivieren Sie die Erzeugung von Eingangskontaktalarmen.
-orname	[UIO-Anschluss-Nr.] <Name>	Ausgangsrelais-Name.
-orloc	[UIO-Anschluss-Nr.] <Position>	Ausgangsrelais-Position:
-ornormst	[UIO-Anschluss-Nr.] <offen | geschlossen>	Ausgangsrelais-Normalstatus.
-ordelay	[UIO-Anschluss-Nr.] <0-65535 sekunden>	Aktivierungsverzögerung Ausgangsrelais. Wie lange ein Alarmzustand vorliegen muss (Zeit in Sekunden), bevor das Ausgangsrelais aktiviert wird.
-orhold	[UIO-Anschluss-Nr.] <0-65535 sekunden>	Ausgangsrelais-Haltezeit. Die Zeit in Sekunden, während der das Ausgangsrelais nach Eintreten des Alarms mindestens aktiviert bleibt.
-fname	[UIO-Anschluss-Nr.] <Name>	Name des Flüssigkeitssensors.
-floc	[UIO-Anschluss-Nr.] <Position>	Position des Flüssigkeitssensors.
-fenable	[UIO-Anschluss-Nr.] <aktivieren | deaktivieren>	Aktivieren oder deaktivieren Sie die Erzeugung von Flüssigkeitssensor-Alarmen.

Beispiel 1: Um alle angeschlossenen UIO-Sonden und ihre zugehörigen Parameter anzuzeigen, geben Sie Folgendes ein:
`cfguio`

Beispiel 2: Geben Sie den Namen der Temperatursonde ein, die an den UIO-Anschluss 1 angeschlossen ist:
`cfguio -thname 1` „neuer Sondenname“

clrrst

Zugriff: Superuser, Administrator

Definition: Den Netzwerkschnittstellen-Resetgrund löschen. Siehe **lastrst** `auf Seite 26`.

console

Zugriff: Superuser, Administrator, Nur Netzwerk

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

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.

Option	Argument	Beschreibung
-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 | 57600 | 115200	Hiermit konfigurieren Sie die Baud-Rate für den seriellen Anschluss (Voreinstellung: 9600).

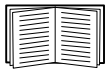
Beispiel 1: Geben Sie Folgendes ein, um den Zugriff auf die Befehlszeile über SSH zu aktivieren:
```
console -s enable
```

Beispiel 2: Geben Sie Folgendes ein, um den Telnet-Port auf 5000 zu ändern:
```
console -pt 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 `date -f` vorgegebene Datumsformat.
-t	<00:00:00>	Hiermit konfigurieren Sie die aktuelle Uhrzeit in Stunden, Minuten und Sekunden. Verwenden Sie dabei das 24-Stunden-Zeitformat.
-f	mm/dd/yy | dd.mm.yyyy | mmm-dd-yy | dd-mmm-yy | yyyy-mm-dd	Wählen Sie das Zahlenformat, in dem alle Datumsangaben über diese Benutzerschnittstelle angezeigt werden sollen. Jeder der Buchstaben m (für Monat), d (für Tag) und y (für Jahr) steht für eine Ziffer. Tage und Monate, die einer einzigen Ziffer entsprechen, werden mit vorangestellter Null angezeigt. **HINWEIS:** Diese Einstellung wird beim nächsten Einloggen mit dem in den Benutzereinstellungen in der NMC-Benutzeroberfläche konfigurierten Datumsformat überschrieben.
-z	<Zeitzonen-Differenz>	Hiermit geben Sie die Differenz zwischen Ihrer Zeitzone und der Normalzeit GMT ein. Dadurch können Sie eine Synchronisierung mit Personen in anderen Zeitzonen durchführen.

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

Beispiel 2: Geben Sie Folgendes ein, um das Datum „30. Oktober 2009“ in dem Format einzustellen, das im vorhergehenden Beispiel konfiguriert wurde:
```
date -d "30.10.2009"
```

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

Diese Optionen sind nicht bei allen USV-Geräten verfügbar.

Zugriff: Superuser, Administrator, Gerätebenutzer

Beschreibung: Anzeigen von detaillierten Informationen zur USV-Batterie über die im USV-Gerät installierten Batteriepakete und Batteriekassetten (falls zutreffend). Bei einigen USV-Geräten stellen Sie das Datum für die Installation des Batteriepacks oder der Kassette ein.

Diese Optionen sind nicht bei allen USV-Geräten verfügbar.

Option	Argument Dies ist optional, außer bei der Ausführung einer Set-Funktion mit -id oder -pi.	Beschreibung
`-all`	`<pack_#>`	Anzeige aller Batterieinformationen.
`-f`	`<pack_#>`	Firmware-Version(en) der Module.
`-t`	`<pack_#>`	Temperaturen der Module.
`-pe`	`<pack_#>`	Batterie-Modul-Status (Fehlerbedingungen).
`-s`	`<pack_#>` `<cartridge_#>`	Kassettenzustand.
`-ph`	`<pack_#>`	Modulzustand.
`-rd`	`<pack_#>` `<cartridge_#>`	Datum zum empfohlenen Austausch der Batterie der Kassette.

Option	Argument Dies ist optional, außer bei der Ausführung einer Set-Funktion mit -id oder -pi.	Beschreibung
-pr	<pack_#>	Datum zum empfohlenen Austausch der Batterie des Moduls.
-id	<pack_#> <cartridge_#> <"datestring">	Einbaudatum von Kassette im aktuellen Datumsformat.
-pi	<pack_#> <"datestring">	Einbaudatum des Batterie-Moduls im aktuellen Datumsformat.
-ce	<pack_#> <cartridge#>	Batteriestatus von Kassette.
-pm	<pack_#>	Herstellungsdatum des Moduls.
-ps	<pack_#>	Seriennummer des Moduls.
-pk	<pack_#>	SKU-Nummer des Moduls.

Beispiel 1: Um alle batteriebezogenen Informationen für das USV-Gerät anzuzeigen, geben Sie Folgendes ein:
```
detbat -all
```

Beispiel 2: Um die Modultemperatur(en) für alle Batterieeinheiten anzuzeigen, geben Sie Folgendes ein:
```
detbat -t
```

Beispiel 3: Um die Modultemperatur(en) nur für die erste (normalerweise interne) Batterie anzuzeigen, geben Sie Folgendes ein:
```
detbat -t 1
```

detstatus

Zugriff: Superuser, Administrator, Gerätebenutzer

Beschreibung: Hiermit zeigen Sie den detaillierten Status der USV an. Siehe auch die -st-Option unter **ups** auf Seite 35.

Option	Beschreibung
-all	Hiermit lassen Sie sich alle verfügbaren Statusinformationen für diese USV anzeigen.
-rt	Verbleibende Laufzeit in Stunden, Minuten und Sekunden.
-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	Temperaturmessungen.
-dg	Diagnosetestergebnisse: Ergebnis des Selbsttests und Datum, Kalibrierungsergebnis und Datum.

Beispiel 1: Um alle detaillierten Statusinformationen der USV anzuzeigen, geben Sie Folgendes ein:

```
detstatus -all
```

Beispiel 2: Um nur die Restlaufzeit anzuzeigen, geben Sie Folgendes ein:

```
detstatus -rt
```

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
1024 Jan 2 4:34 apc_hw21_aos_1.1.0.15.bin
     6249332 Jan 2 4:34 apc_hw21_su_1.1.0.15.bin
       45000 Sep 30 1996 config.ini
           0 Apr 23 18:53 db/
           0 Apr 23 18:53 ssl/
           0 Apr 23 18:53 ssh/
           0 Apr 23 18:53 logs/
           0 Apr 23 18:53 sec/
           0 Apr 23 18:53 fwl/
           0 Apr 23 18:53 email/
           0 Apr 23 18:53 eapol/
           0 Apr 23 18:53 tmp/
           0 Apr 23 18:53 upsfw/
```

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.
-n	<Domänenname IPv6>	Hiermit legen Sie den Domänennamen 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	Beschreibung
`-S`	`enable | disable`	EAPoL aktivieren oder deaktivieren.
`-n`	`<supplicant-name>`	Supplicant-Name festlegen.
`-c`	`<certificate filename>`	Der Name der Datei, die das Gerätezertifikat einer End-Entität enthält, das für die EAPoL-Authentifizierung verwendet werden soll.
`-r`		Starten Sie die Authentifizierung mit den aktuellen Einstellungen neu.

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

```
apc>eapol
E000: Success
Active EAPoL Settings
---------------------
EAPoL: enabled
Supplicant Name: NMC-Supplicant
Certificate: nmc.pem
Certificate status: loaded
Status: Authenticated
```

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)	Hiermit legen Sie die SMTP-Serveroptionen fest: • **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. **Hinweis:** Wenn Sie diese Einstellung verwenden, stimmt die Absenderadresse mit der Empfängeradresse überein, Authentifizierung und Verschlüsselung (TLS) werden deaktiviert und Port 25 wird verwendet. • **Custom** (benutzerdefiniert): Diese Einstellung ermöglicht für jeden E-Mail-Empfänger eigene Servereinstellungen. Diese Einstellungen sind unabhängig von den Einstellungen, die durch den Befehl „`smtp`“ vorgegeben werden.
-f[n]	<Absenderadresse>	Die Adresse, von der E-Mails von der NMC gesendet werden.
-s[n]	<SMTP-Server>	Die IPv4-/IPv6-Adresse oder der DNS-Name des lokalen SMTP-Servers.
-p[n]	<Port>	Die SMTP-Portnummer, der Standardwert ist 25. Übliche Ports sind 25 für unverschlüsselte E-Mails bzw. 465 und 587 für SSL/TLS-verschlüsselte E-Mails. Sie haben die Möglichkeit, die Port-Einstellung auf einen beliebigen freien Port zwischen 1 und 65535 zu ändern.
-a[n]	<enable | disable>	Aktivieren Sie diese Option, falls Ihr SMTP-Server eine Authentifizierung verlangt.
-u[n]	<Benutzername>	Geben Sie hier den Benutzernamen und das Kennwort ein, wenn der SMTP-Server eine Authentifizierung verlangt.
-w[n]	<Kennwort>	

Option	Argument	Beschreibung
-e[n]	<none | ifsupported | always | implicit>	• **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. Dies wird in der Regel mit Port 25 verwendet. • **Always** (Immer): Der SMTP-Server erfordert das Senden des STARTTLS-Befehls, sobald eine Verbindung zum Server hergestellt wird. Dies wird in der Regel mit Port 587 verwendet. • **Implicit** (Implizit): Der SMTP-Server akzeptiert nur Verbindungen, die von vornherein verschlüsselt sind. Es wird keine STARTTLS-Nachricht an den Server gesendet. Dies wird in der Regel mit Port 465 verwendet.
-c[n]	<enable | disable >	Stammzertifikat der Zertifizierungsstelle erforderlich machen: Diese Option sollte dann aktiviert werden, wenn die Sicherheitsrichtlinie Ihres Unternehmens das implizite Vertrauen von SSL-/TLS-Verbindungen nicht unterstützt. Wenn diese Option aktiviert ist, muss ein gültiges Zertifikat einer Zertifizierungsstelle für den SMTP-Server mithilfe des Zertifikatladers im Zertifikatspeicher der NMC installiert werden, um eine TLS-Verbindung mit dem SMTP-Server erfolgreich herzustellen. Weitere Informationen zum Laden von TLS-Zertifikaten finden Sie im **Benutzerhandbuch**.
n=	E-Mail-Empfängernummer (1, 2, 3 oder 4)	Kennzeichnet den Empfänger der E-Mail durch die Empfängernummer.

Beispiel: Wenn Sie über den lokalen SMTP-Server E-Mails an den E-Mail-Empfänger 1 mit der E-Mail-Adresse empfänger1@apc.com senden möchten, geben Sie Folgendes ein:

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

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.
-Y		Überspringen Sie die Firewall-Testaufforderung.

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

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

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`.

Option	Argument	Definition
`-f`		Löschen und Formatieren des Low-Level-Flashs durchführen.
`-p`		Behalten Sie die Netzwerkeinstellungen bei, während Sie die Formatierungsfunktionen ausführen.

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: FTP ist standardmäßig deaktiviert und Secure CoPy (SCP) wird automatisch aktiviert, wenn das Superuser-Passwort über SSH eingestellt wird.

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: Auflistung der verfügbaren Sprachen für Benutzer auf der Web-Benutzeroberfläche.

Beispiel: Um die Liste der verfügbaren Sprachen anzuzeigen, geben Sie Folgendes ein:

```
lang
```

lastrst

Zugriff: Superuser, Administrator

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

Option	Beschreibung
`02 NMI Reset`	Die Netzwerkschnittstelle wurde über die Reset-Taste auf der Blende der Netzwerkmanagement-Karte zurückgesetzt.
`09 Coldstart Reset`	Die Netzwerkschnittstelle wurde zurückgesetzt, indem die Stromzufuhr der Hardware unterbrochen wurde.
`12 WDT Reset`	Die Netzwerkschnittstelle wurde über einen Firmware-Befehl zurückgesetzt.

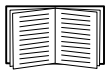
Beispiel:

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

ldap

Zugriff: Superuser, Administrator, Nur-Netzwerk-Benutzer

Beschreibung: Hiermit können Sie die LDAP-Einstellungen anzeigen und konfigurieren. Sie können das Gerät so einrichten, dass es einen LDAP-Server zur Authentifizierung von Remote-Benutzern verwendet. Zwei gängige Beispiele hierfür sind Microsoft Active Directory und OpenLDAP. Die Authentifizierung erfolgt immer mit einer einfachen Bindungsanfrage über eine TLS-Verbindung. Stellen Sie sicher, dass das CA-Zertifikat des LDAP-Servers installiert ist, damit die TLS-Verbindung zum LDAP-Server hergestellt werden kann.



Weitere Informationen zur Verwendung von LDAP finden Sie im Benutzerhandbuch.

Option	Argument	Beschreibung
`-s`	`<Benutzer-URI suchen>`	Ein LDAP-URI, der den Speicherort eines Benutzerobjekts angibt, an das Sie sich zunächst binden müssen. Dieses Benutzerobjekt muss die Berechtigung haben, in der LDAP-Datenbank nach Benutzern zu suchen. Bei einem Anmeldeversuch eines Benutzers wird eine Verbindung mit dem LDAP-Server in diesem URI hergestellt und eine Bindung an den DN mit dem in -p (Benutzerpasswort suchen) angegebenen Kennwort durchgeführt. Wenn diese Bindung erfolgreich ist, wird nach dem Benutzer gesucht, der versucht, sich anzumelden. Dieser LDAP-URI muss entweder das Schema „ldap“ oder „ldaps“ enthalten. Wenn „ldaps“ verwendet wird, ist die TLS-Verbindung implizit und die TCP-Verbindung wird standardmäßig über Port 636 hergestellt. Wenn „ldap“ verwendet wird, wird die TLS-Verbindung durch Senden einer StartTLS-Anforderung initiiert und die TCP-Verbindung verwendet standardmäßig Port 389. Die Verwendung von „ldaps“ ist nicht standardisiert und wird nicht empfohlen. Dieser LDAP-URI kann die Adresse des LDAP-Servers und optional die Portnummer enthalten. Es folgt der DN des gesuchten Benutzerobjekts. Wenn der DN des Suchbenutzers mit DC-Komponenten endet, wird ein DNS-Lookup des SRV-Eintrags für den LDAP-Dienst in dieser Domäne durchgeführt. Wird der SRV-Eintrag gefunden, so wird er anstelle des im URI angegebenen Hosts verwendet. Wird der SRV-Eintrag nicht gefunden, so wird der im URI angegebene Host verwendet. Die Host-Komponente des URI kann weggelassen werden, wenn der SRV-Eintrag für LDAP bekannt ist. Wenn der DN weggelassen wird, muss die Host-Komponente vorhanden sein, und es wird eine anonyme Bindung durchgeführt.

Option	Argument	Beschreibung
		Beschreibung: • **ldap://ldap.domain.com/ CN=searchuser,OU=users,DC=domain,DC=com** Wenn DNS verfügbar ist, wird eine DNS-Abfrage des SRV-Eintrags für den LDAP-Dienst unter domain.com durchgeführt. Wenn er gefunden wird, wird er mit ihm verbunden. Wenn er nicht gefunden wird, wird eine Verbindung zu „ldap.domain.com“ an Port 389 hergestellt. Nach dem Senden einer StartTLS-Anforderung wird TLS eingerichtet und eine Bindung an das Objekt „CN=searchuser,OU=users,DC=domain,DC=com“ mit dem in –p (Benutzerpasswort suchen) angegebenen Passwort durchgeführt. Von hier aus wird eine Suche nach dem sich anmeldenden Benutzer durchgeführt. • **ldap:///CN=searchuser,OU=users,DC=domain,DC=com** Wenn DNS verfügbar ist, wird eine DNS-Abfrage des SRV-Eintrags für den LDAP-Dienst unter domain.com durchgeführt. Wenn er gefunden wird, wird er mit ihm verbunden. Wenn er nicht gefunden wird, wird keine Verbindung hergestellt, da die Host-Komponente des URI weggelassen wird und die LDAP-Authentifizierung nicht fortgesetzt werden kann. Wenn die Verbindung erfolgreich ist, werden StartTLS, Bindung und Suche wie oben beschrieben durchgeführt. • **ldaps://ldap.domain.com** „ldap.domain.com“ an Port 636 verbunden und es wird sofort ein TLS-Handshake durchgeführt, ohne eine StartTLS-Anfrage zu senden. Wenn dies gelingt, wird eine anonyme Bindung durchgeführt. Von hier aus wird eine Suche nach dem sich anmeldenden Benutzer durchgeführt. • **ldap://ldap.domain.com:42/ CN=searchuser,OU=users,DC=domain,DC=com** Dies ist dasselbe wie das erste Beispiel, außer dass eine Verbindung zu „ldap.domain.com“ an Port 42 hergestellt wird, wenn der SRV-Eintrag nicht gefunden wird.
-p	<Benutzerpasswort suchen>	Das Passwort, das in der ersten Bindungsanfrage an den Suchbenutzer zu verwenden ist, wie oben beschrieben. Bleibt diese Option leer, wird entweder eine anonyme oder eine unauthentifizierte Verbindung hergestellt, je nachdem, ob ein Suchbenutzer-DN angegeben wird oder nicht.
-t	<2-60>	Die Zeitüberschreitung in Sekunden, die für die Verbindung zum und die Kommunikation mit dem LDAP-Server verwendet wird. Die erste TCP-Verbindung muss innerhalb dieser Zeitspanne abgeschlossen werden. Wenn dies der Fall ist, muss jede LDAP-Antwort vom Server innerhalb dieser Zeitspanne nach jeder LDAP-Anfrage empfangen werden. Da eine einzelne LDAP-Authentifizierung aus mehreren Anfragen bestehen kann (und sogar an mehrere Server, wenn Verweise verfolgt werden), kann die Gesamtauthentifizierungszeit am Ende viel länger sein als der hier angegebene Timeout-Wert.

Option	Argument	Beschreibung
-u	<Benutzer-Basis-DN>	Dies ist der DN des Basisobjekteintrags, unter dem alle Benutzer, die sich anmelden, existieren müssen.
-g	<Gruppen-Basis-DN>	Dies ist der DN des Basisobjekteintrags, unter dem die in den folgenden Einstellungen angegebenen Benutzergruppen existieren müssen.
-ag	<Admin-Gruppenname>	Dies ist der Common Name (CN) der LDAP-Gruppe, in der die NMC-Administratoren Mitglied sind. Wenn der sich anmeldende Benutzer Mitglied dieser Gruppe ist, erhält der Benutzer Administrator-Zugriff.
-dg	<Gerätebenutzer Gruppenname>	Dies ist der Common Name (CN) der LDAP-Gruppe, in der die NMC-Gerätebenutzer Mitglied sind. Wenn der sich anmeldende Benutzer Mitglied dieser Gruppe ist, erhält der Benutzer Gerätebenutzer-Zugriff.
-ng	<Netzwerkbenutzer Gruppenname>	Dies ist der Common Name (CN) der LDAP-Gruppe, in der die NMC-Netzwerkbenutzer Mitglied sind. Wenn der sich anmeldende Benutzer Mitglied dieser Gruppe ist, erhält der Benutzer Netzwerkbenutzer-Zugriff.
-rg	<Schreibschutz Benutzer Gruppenname>	Dies ist der Common Name (CN) der LDAP-Gruppe, in der die NMC-Schreibschutz-Benutzer Mitglied sind. Wenn der sich anmeldende Benutzer Mitglied dieser Gruppe ist, erhält der Benutzer Schreibschutz-Benutzer-Zugriff.
-ad	<aktivieren | deaktivieren>	Wenn diese Option aktiviert ist, werden LDAP-Verzeichnisse mit Benutzern der Klasse „Benutzer“ und Gruppen der Klasse „Gruppe“ nach dem Standardschema von Active Directory unterstützt.
-posix	<aktivieren | deaktivieren>	Wenn dies aktiviert ist, werden LDAP-Verzeichnisse mit Benutzern der Klasse „posixAccount“ und Gruppen der Klasse „posixGroup“ nach dem in RFC 2307 definierten Schema unterstützt.
-4519	<aktivieren | deaktivieren>	Wenn dies aktiviert ist, werden LDAP-Verzeichnisse unterstützt, die Benutzer der Klasse „uidObject“ und Gruppen entweder der Klasse „groupOfNames“ oder der Klasse „groupOfUniqueNames“ gemäß dem in RFC 4519 definierten Schema enthalten.
-2798	<aktivieren | deaktivieren>	Wenn dies aktiviert ist, werden LDAP-Verzeichnisse mit Benutzern der Klasse „inetOrgPerson“ gemäß RFC 2798 unterstützt.
-cuser	<aktivieren | deaktivieren>	Wenn diese Option aktiviert ist, können LDAP-Verzeichnisse unterstützt werden, die Benutzer mit Klassen enthalten, die keiner der oben genannten unterstützten Klassen entsprechen. Wenn dies aktiviert ist, müssen die Einstellungen –ucn (Benutzerdefinierter Benutzerklassenname) und –ucua (Attribut des benutzerdefinierten Benutzerklassennamens) angegeben werden, und – ucga (Attribut der benutzerdefinierten Benutzergruppennummer) kann optional angegeben werden.
-cgroup	<aktivieren | deaktivieren>	Wenn diese Option aktiviert ist, können LDAP-Verzeichnisse unterstützt werden, die Gruppen mit Klassen enthalten, die keiner der oben genannten unterstützten Klassen entsprechen. Wenn dies aktiviert ist, müssen die Einstellungen –gcn (Benutzerdefinierter Gruppenklassenname) und – gcma (Attribut des benutzerdefinierten Gruppenklassennamens) angegeben werden, und – gcga (Attribut der benutzerdefinierten Gruppengruppennummer) kann optional angegeben werden. – gcmt (Typ des benutzerdefinierten Gruppenmitglieds) muss ebenfalls korrekt eingestellt sein.

Option	Argument	Beschreibung
-ucn	<Benutzerdefinierter Benutzerklassenname>	Dies ist der Name der Objektklasse, zu der die Benutzereinträge gehören. Sie wird nur verwendet, wenn –cuser (Benutzerdefinierte Benutzerklasse) aktiviert ist.
-ucua	<Attribut des benutzerdefinierten Benutzerklassennamens>	Dies ist der Name des Attributs, das den Benutzernamen eines Benutzers für die durch –ucn (Benutzerdefinierter Benutzerklassenname) angegebene Objektklasse enthält. Es wird nur verwendet, wenn –cuser (Benutzerdefinierte Benutzerklasse) aktiviert ist.
-ucga	<Attribut der benutzerdefinierten Benutzergruppennummer>	Dies ist der Name des Attributs, das die Gruppennummer für die primäre Gruppe eines Benutzers für die durch –ucn (Benutzerdefinierter Benutzerklassenname) angegebene Objektklasse enthält. Dies ist optional und wird nur verwendet, wenn –cuser (Benutzerdefinierte Benutzerklasse) aktiviert ist. Es wird auf die gleiche Weise verwendet wie das Attribut „gidNumber“ in der Klasse „posixAccount“.
-gcn	<Benutzerdefinierter Gruppenklassenname>	Dies ist der Name der Objektklasse, zu der die Gruppeneinträge gehören. Es wird nur verwendet, wenn –cgroup (Benutzerdefinierte Gruppenklasse) aktiviert ist.
-gcma	<Attribut des benutzerdefinierten Gruppenmitglieds>	Dies ist der Name des Attributs, das die Mitglieder der Gruppe für die durch -gcn (Benutzerdefinierter Gruppenklassenname) angegebene Objektklasse enthält. Es wird nur verwendet, wenn -cgroup (Benutzerdefinierte Gruppenklasse) aktiviert ist. Wenn -gcmt (Typ des benutzerdefinierten Gruppenmitglieds) auf DN gesetzt ist, dann sind die Werte in diesem Attribut DNs. Wenn es auf „username“ gesetzt ist, sind die Werte in diesem Attribut Benutzernamen.
-gcga	<Attribut der benutzerdefinierten Gruppe Gruppennummer>	Dies ist der Name des Attributs, das die Gruppennummer der Gruppe für die durch –-gcn (Benutzerdefinierter Gruppenklassenname) angegebene Objektklasse enthält. Dies ist optional und wird nur verwendet, wenn –-cgroup (Benutzerdefinierte Gruppenklasse) aktiviert ist. Es wird auf die gleiche Weise verwendet wie das Attribut „gidNumber“ in der Klasse „posixGroup“.
-gcmt	<DN | Benutzername>	Dies legt fest, wie die Mitglieder der Gruppe für die durch –gcn (Benutzerdefinierter Gruppenklassenname) angegebene Objektklasse angegeben werden. Er kann entweder auf DN oder Benutzername gesetzt werden.

Beispiel 1: Um die vorhandenen LDAP-Einstellungen für den NMC anzuzeigen, geben Sie Folgendes ein:

```
ldap
```

Beispiel 2: Um LDAP so zu konfigurieren, dass es eine Verbindung zu einem LDAP-Server herstellt, der nur ein Active Directory-Schema unter ldap.company.com verwendet (oder den ldap-SRV-Eintrag unter company.com verwendet, falls verfügbar), mit einem Timeout von fünf Sekunden, und sich mit einem anfänglichen Benutzer mit Suchprivilegien unter DN cn=admin, dc=company, dc=com mit dem Kennwort „password“ verbindet, mit NMC-Administratoren in der Gruppe nmc-admins, NMC-Nur-Lese-Benutzern in der Gruppe nmc-ro-users und deaktivierten Nur-Netzwerk- und Nur-Geräte-Benutzern, geben Sie ein:

```
ldap -s ldap://ldap.company.com/cn=admin,dc=company,dc=com -p password -t 5 -u
ou=users,dc=company,dc=com -g ou=groups,dc=company,dc=com -ag nmc-admins -rg nmc-
ro-users -dg "" -ng "" -ad enable -posix disable -4519 disable -2798 disable -
cuser disable -cgroup disable
```

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`

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
```

modbus

Dieser Befehl ist nicht auf allen USV-Geräten verfügbar.

Zugriff: Superuser, Administrator

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

Diese Optionen sind nicht bei allen USV-Geräten verfügbar.

Option	Argument	Beschreibung
-a	<enable | disable>	Hiermit aktivieren oder deaktivieren Sie Modbus Seriell.[1]
-br	<2400 | 9600 | 19200 | 38400>	Hiermit legen Sie die Baudrate in Bits pro Sekunde fest.[1]
-pr	<even | odd | none>	Diese Option ist nur noch für Legacy-Zwecke vorgesehen, verwenden Sie stattdessen -m.[1]
-s	<1-F7>	Hiermit wird die hexadezimale Modbus-Slave-Adresse eingestellt.[1]

Option	Argument	Beschreibung
-rDef		Hiermit setzen Sie die Modbus-Konfiguration auf die Standardwerte zurück.
-tE	<enable | disable>	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.
-tTo	<0-64800>	Geben Sie den Modbus TCP-Kommunikationstimeout in Sekunden an, wobei 0 bedeutet, dass die Verbindung nie unterbrochen wird.[2]
-ka	<enable | disable>	Modbus-TCP Keep Alive.
[1]Modbus Seriell wird nur auf den AP9641- und AP9643-Karten unterstützt. [2]Modbus TCP wird auf den AP9640-, AP9641-,und AP9643-Karten unterstützt.		

Beispiel 1: Um die Modbus-Parameter anzuzeigen, geben Sie Folgendes ein:

```
modbus
```

Beispiel 2: Um den seriellen Modbus-Modus auf 8-N-2 (8 Bits, keine Parität, 2 Stoppbits) einzustellen, geben Sie Folgendes ein:

```
modbus -m 8n2
```

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.

Option	Argument	Beschreibung
-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 xxx.xxx.xxx.xxx 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: Hiermit konfigurieren Sie die Übertragungsgeschwindigkeit des Anschlusses.

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

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`

HINWEIS: Die Port-Geschwindigkeit kann auf 1000 Mbit/s geändert werden. Diese Änderung kann jedoch nur über die Web-Benutzeroberfläche vorgenommen werden. Weitere Informationen finden Sie im Benutzerhandbuch unter **Bildschirm für Port-Geschwindigkeit.**

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: `apc>`

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

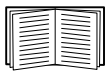
Zugriff: Super User, Administrator, Gerätebenutzer, Nur-Netzwerk-Benutzer, Benutzer „schreibgeschützt“

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 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 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**.

Option	Argument	Beschreibung
`-p1` `-p2`	`<server IP>`	Der Servername oder die IP-Adresse des primären oder sekundären RADIUS-Servers.
`-o1` `-o2`	`<port>`	Die Portnummer des primären oder sekundären RADIUS-Servers. **HINWEIS:** RADIUS-Server verwenden normalerweise Port 1812, um Benutzer zu authentifizieren. Die NMC unterstützt die Ports 1 bis 65535.
`-s1` `-s2`	`<Server-Schlüssel>`	Der vom primären oder sekundären RADIUS-Server und der Netzwerk-Management-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 Folgendes ein, um sich die aktuellen RADIUS-Einstellungen für die Netzwerkmanagement-Karte anzeigen zu lassen.

```
radius
```

Beispiel 2: 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.

Option	Argumente	Beschreibung
-a	<enable | disable> (Remote-Authentifizierungsüber-schreibung)	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-Portnummer, der Standardwert ist 25. Übliche Ports sind 25 für unverschlüsselte E-Mails bzw. 465 und 587 für SSL/TLS-verschlüsselte E-Mails. Sie haben die Möglichkeit, die Port-Einstellung auf einen beliebigen freien Port zwischen 1 und 65535 zu ändern.
-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: • **keine:** Der SMTP-Server benötigt bzw. unterstützt keine Verschlüsselung. • **falls unterstützt:** Der SMTP-Server zeigt an, dass STARTTLS unterstützt wird, erfordert jedoch keine verschlüsselte Verbindung. Der STARTTLS-Befehl wird nach dem Advertisement gesendet. Dies wird in der Regel mit Port 25 verwendet. • **immer:** Der SMTP-Server erfordert das Senden des STARTTLS-Befehls, sobald eine Verbindung zum Server hergestellt wird. Dies wird in der Regel mit Port 587 verwendet. • **implizit:** Der SMTP-Server akzeptiert nur Verbindungen, die von vornherein verschlüsselt sind. Es wird keine STARTTLS-Nachricht an den Server gesendet. Dies wird in der Regel mit Port 465 verwendet.
-c	<enable | disable>	Stammzertifikat der Zertifizierungsstelle erforderlich machen: Diese Option sollte dann aktiviert werden, wenn die Sicherheitsrichtlinie Ihres Unternehmens das implizite Vertrauen von SSL-/TLS-Verbindungen nicht unterstützt. Wenn diese Option aktiviert ist, muss ein gültiges Zertifikat einer Zertifizierungsstelle für den SMTP-Server mithilfe des Zertifikatladers im Zertifikatspeicher der NMC installiert werden, damit eine TLS-Verbindung mit dem SMTP-Server erfolgreich hergestellt werden kann. Weitere Informationen zum Laden von TLS-Zertifikaten finden Sie im **Benutzerhandbuch**.

Beispiel:

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

snmp

Zugriff: Super User, Administrator, Nur Netzwerk

Beschreibung: Hiermit aktivieren oder deaktivieren und konfigurieren Sie SNMPv1. SNMPv1 ist standardmäßig deaktiviert. Der Community-Name (-c [n]) muss festgelegt werden, bevor SNMPv1-Kommunikation hergestellt werden kann.

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

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 Domänennamen 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.SNMPv3 ist standardmäßig deaktiviert. Ein gültiges Benutzerprofil muss mit Kennwortsätzen (-a [n],-c [n]) aktiviert werden, bevor SNMPv3-Kommunikation hergestellt werden kann.

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

Option	Argumente	Beschreibung
-S	enable | disable	Hiermit aktivieren oder deaktivieren Sie SNMPv3.
-u[n]	<Benutzername>	Hiermit geben Sie einen Benutzernamen, einen Authentifizierungs-Kennwortsatz und einen Verschlüsselungs-Kennwortsatz an.
-a[n]	<Authentifizierungs-Kennwortsatz>	
-c[n]	<Verschlüsselungs-Kennwortsatz>	
-ap[n]	sha-256 | sha | md5 | none	Hiermit geben Sie den Typ des Authentifizierungsprotokolls an.
-pp[n]	aes-256 | aes| des | none	Hiermit geben Sie das Datenschutzprotokoll (Verschlüsselung) an.
-ac[n]	enable | disable	Hiermit aktivieren oder deaktivieren Sie den Zugriff.

Option	Argumente	Beschreibung
-au[n]	<Benutzerprofilname>	Hiermit gestatten Sie einen angegebenen Benutzerprofil den Zugriff.
-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: S

uperuser, 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: • 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.
-p[n]	<Port>	Hiermit legen Sie die SNMP-Trap-Portnummer für diesen Trap-Empfänger fest (Standardwert: 162). Der Bereich liegt zwischen 1 und 65535.
-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 dem Community-Namen „public“, der IP-Adresse `10.169.118.100` des Empfängers 1 und unter Verwendung der Standardsprache Englisch aktivieren und konfigurieren möchten:

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

ssh

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

Beschreibung: Anzeigen, Löschen und Generieren von SSH-Serverschlüsseln. **HINWEIS:** Die Optionen in der folgenden Tabelle sind mit dem Befehl „`ssh key`“ verfügbar.

Option	Argumente	Beschreibung
`-s`		Zeigt den aktuellen SSH-Serverschlüssel an, der verwendet wird.
`-f`		Zeigen Sie den aktuellen Fingerabdruck des SSH-Serverschlüssels an.
`-d`		Löschen Sie den aktuellen SSH-Serverschlüssel, der verwendet wird.
`-i`	`<File Name>.pk15`	Importieren Sie den SSH-Serverschlüssel aus einer PKCS-#15-Datei.
`-ecdsa`	`256`	Generieren Sie einen SSH-Serverschlüssel der Art „Elliptic Curve Digital Signature Algorithm“ (ECDSA) mit der angegebenen Bit-Größe.
`-rsa`	`1024 | 2048 | 4096`	Generieren Sie einen SSH-Serverschlüssel der Art „Rivest-Shamir-Adleman (RSA)“ mit der angegebenen Bit-Größe.

Beispiel 1: Um den aktuellen SSH-Serverschlüssel anzuzeigen, geben Sie Folgendes ein:

```
ssh key -s
```

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

```
ssh key -i nmc.p15
```

ssl

Zugriff: Superuser, Administrator, nur Netzwerkbenutzer

Beschreibung: Konfigurieren und verwalten Sie den öffentlichen Schlüssel und das Zertifikat der Web-Benutzeroberfläche der Netzwerkmanagement-Karte und erstellen Sie eine Zertifikatsignieranforderung (Certificate Signing Request, CSR).

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

Konfigurieren der öffentlichen Schlüssel (`key`):

Option	Argumente	Beschreibung
`-s`		Zeigen Sie den aktuell verwendeten öffentlichen Schlüssel an.
`-d`		Löschen Sie den aktuell verwendeten öffentlichen Schlüssel.
`-i`	`<Dateiname>.pl5`	Importieren Sie den öffentlichen Schlüssel aus einer PKCS-#15-Datei.
`-ecdsa`	`256 | 384 | 521`	Generieren Sie einen öffentlichen Schlüssel der Art „Elliptic Curve Digital Signature Algorithm“ (ECDSA) mit der angegebenen Bit-Größe.
`-rsa`	`1024 | 2048 | 4096`	Generieren Sie einen öffentlichen Schlüssel der Art „Rivest–Shamir–Adleman“ (RSA) mit der angegebenen Bit-Größe.

Beispiel 1: Über die folgende Eingabe generieren Sie einen neuen öffentlichen ECDSA-521-Schlüssel:

```
ssl key -ecdsa 521
```

Beispiel 2: Über die folgende Eingabe importieren Sie den öffentlichen Schlüssel aus einer. p15-Datei, die vom Befehlszeilenschnittstellen-Dienstprogramm „NMC Security Wizard“ generiert wurde:

```
ssl key -i nmc.p15
```

Konfigurieren der Zertifikatsignieranforderung (`csr`):

Option	Argumente	Beschreibung
`-s`	`<Dateiname>`	Zeigen Sie die aktuelle Zertifikatsignieranforderung (CSR) an.
`-q`	`<Dateiname>`	Erstellen Sie eine Zertifikatsignieranforderung (CSR) über die aktive Konfiguration.
`-CN`	`<Allgemeiner Name>`	Erstellen Sie eine benutzerdefinierte Zertifikatsignierungsanforderung (CSR). Der allgemeine Name ist der vollständig qualifizierte Domänennamen (Fully-Qualified Domain Name, FQDN) der Netzwerkmanagement-Karte. Beispielsweise dessen IP-Adresse oder *.nmc.local.
Optionen für Zertifikatsignieranforderungen (CSR). **HINWEIS:** Die folgenden Optionen sind nur für `-CN` verfügbar.		
`-O`	`<Organisation>`	Der Name Ihrer Organisation.
`-OU`	`<Organisationseinheit>`	Die Abteilung Ihrer Organisation, die das Zertifikat abwickelt.
`-C`	`<Land>`	Der aus zwei Buchstaben bestehende Ländercode des Landes, in dem sich Ihre Organisation befindet.
`-san`	`<Allgemeiner Name | IP-Adresse>`	Der allgemeine Name oder die IP-Adresse der Netzwerkmanagement-Karte.

HINWEIS: Erstellte Zertifikatsignieranforderungen werden im SSL-Verzeichnis der Netzwerkmanagement-Karte gespeichert. Siehe **dir**.

Beispiel 3: Mithilfe der folgenden Eingabe generieren Sie rasch eine Zertifikatsignieranforderung (CSR) über die aktive Konfiguration:

```
ssl csr -q
```

Beispiel 4: Über die folgende Eingabe generieren Sie eine minimale Zertifikatsignieranforderung (CSR):

```
ssl csr -CN 190.0.2.0 -C US
```

Beispiel 5: Über die folgende Eingabe generieren Sie eine benutzerdefinierte Zertifikatsignieranforderung (CSR):

```
ssl csr -CN apcXXXXXX.nmc.local -C US -san *.nmc.local -san 190.0.2.0
```

Konfigurieren des Zertifikats der Web-Benutzeroberfläche (`cert`):

Option	Argumente	Beschreibung
`-s`	`<Dateiname>`	Zeigen Sie das angegebene Zertifikat an. **HINWEIS:** Wenn Sie diese Option ohne Argument ausführen, wird das aktuell verwendete Zertifikat angezeigt.
`-f`	`<Dateiname>`	Zeigen Sie den Fingerabdruck des angegebenen Zertifikats an. **HINWEIS:** Wenn Sie diese Option ohne Argument ausführen, wird der Fingerabdruck des aktuellen Zertifikats angezeigt.
`-i`	`<Dateiname>`	Importieren Sie ein Zertifikat.

Beispiel 6: Über die folgende Eingabe zeigen Sie das aktive Zertifikat an:

```
ssl cert -s
```

Beispiel 7: Über die folgende Eingabe zeigen Sie das im SSL-Verzeichnis befindliche nmc.crt an:

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

Beispiel 8: Über die folgende Eingabe importieren Sie weitere .crt:

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

system

Zugriff: Superuser, Administrator

Beschreibung: Hiermit zeigen Sie den Systemnamen, den Kontakt und den Standort an und legen diese Werte fest. Hiermit konfigurieren Sie Systemmeldungen, zeigen die Verfügbarkeit sowie das Datum und die Uhrzeit, den angemeldeten Benutzer und den höchstrangigen Systemstatus (P, N oder A) an (siehe **Statusfelder des Hauptbildschirms**).

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 EcoStruxure™ IT Expert oder Data Center Expert und vom SNMP-Agenten der Netzwerkmanagement-Karte verwendet.
-c	<Systemkontakt>	
-l	<Systemposition>	
-m	<Systemmeldung>	Hiermit zeigen Sie eine konfigurierbare, benutzerdefinierte Meldung oder ein Banner auf der Anmeldeseite von Web-Benutzeroberfläche, Befehlszeilenschnittstelle (Serial, Telnet, SSH), FTP oder FCP 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"`

tacacs+

Zugriff: Superuser, Administrator, Nur-Netzwerk-Benutzer

Beschreibung: Hiermit können Sie sich die aktuellen TACACS+-Einstellungen anzeigen lassen und grundlegende Authentifizierungsparameter für bis zu zwei TACACS+-Server konfigurieren.

Eine Übersicht über die TACACS+-Server-Konfiguration sowie eine Liste der unterstützten TACACS+-Server finden Sie im **Benutzerhandbuch**.

Ausführliche Informationen zur Konfiguration Ihres TACACS+-Servers finden Sie im **Sicherheitshandbuch**

Option	Argument	Beschreibung
`-p1` `-p2`	`<server IP>`	Der Servername oder die IP-Adresse des primären oder sekundären TACACS+-Servers.

`-o1`
 	
`-o2`
	`<port>`	Die Portnummer des primären oder sekundären TACACS+-Servers.
		HINWEIS: TACACS+-Server verwenden standardmäßig Port 49, um Benutzer zu authentifizieren. Die NMC unterstützt die Ports 1 bis 65535.

`-s1` `-s2`	`<server-Schlüssel>`	Der vom primären oder sekundären TACACS+-Server und der NMC verwendete geheime Schlüssel.
`-t1` `-t2`	`<server timeout>`	Die Zeit in Sekunden, die eine NMC auf eine Antwort vom primären oder sekundären TACACS+-Server wartet.

Option	Argument	Beschreibung

`-d1`
 	
`-d2`
		Hiermit löschen Sie die Konfiguration des primären oder sekundären TACACS+-Servers.

`-r`	`<0-15>`	Berechtigungsstufe: Nur-Lesen-Benutzer.
`-a`	`<0-15>`	Berechtigungsstufe : Administrator.

Beispiel 1: Geben Sie Folgendes ein, um die aktuellen TACACS+-Einstellungen für die NMC anzuzeigen.

```
tacacs+
```

Beispiel 2: Geben Sie Folgendes ein, um einen Timeout von 10 Sekunden für einen sekundären TACACS+-Server zu konfigurieren: `tacacs+ -t2 10`

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	<IPv4-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. *Verwenden Sie nicht* 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 Folgendes ein, um sich die aktuellen Netzwerk-Einstellungen für die Netzwerkmanagement-Karte anzeigen zu lassen.

```
tcpip
```

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

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.

Option	Argument	Beschreibung
-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 Folgendes ein, um sich die aktuellen Netzwerkeinstellungen für die Netzwerkmanagement-Karte anzeigen zu lassen.

```
tcpip6
```

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

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

uio

Dieser Befehl ist nur auf den Karten AP9641 oder AP9643 oder einem eingebetteten NMC3 mit einem universellen Eingabe-/Ausgabe-Anschluss (UIO) verfügbar.

Zugriff: Superuser, Administrator, Gerätebenutzer

Beschreibung: Hiermit zeigen Sie den Status aller angeschlossenen UIO-Sonden an.

HINWEIS: Die Temperatureinstellungen werden in Grad Celsius oder Grad Fahrenheit angezeigt, je nachdem, was vom angemeldeten Benutzer eingestellt wurde.

Option	Argument	Beschreibung
-rc	<UIO-Port-Nr> <open | close >	Ändern Sie den Zustand eines angeschlossenen Ausgangs an der angegebenen UIO-Anschlussnummer, wenn an diesem UIO-Anschluss ein Trockenkontakt-E/A-Zusatzgerät (AP9810) angeschlossen ist.
-st	<UIO-Port-Nr.> | <UIO-Port-Nr.>, <UIO-Port-Nr.> | <UIO-Port-Nr.>– <UIO-Port-Nr.>	Hiermit zeigen Sie den Status der verbundenen Sensoren an. 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.>	Identifizieren Sie die an den UIO-Anschluss/die UIO-Anschlüsse angeschlossenen Sonde(n), falls vorhanden. t = Temperaturfühler, th = Temperatur-/Feuchtigkeitsfühler, 9810 = Trockenkontakt-E/A-Zusatzgerät (AP9810), spotFluid= Punktflüssigkeitssensor, falls unterstützt (NBES0301).

Beispiel 1: Um das Ausgangsrelais am zweiten UIO-Port zu öffnen, geben Sie Folgendes ein:
`uio -rc 2 open`

Beispiel 2: Um den Status des an den UIO-Port 2 angeschlossenen Geräts anzuzeigen, geben Sie Folgendes ein:
`uio -st 2`

ups

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***.

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

Option	Argumente	Beschreibung
-c	reboot	Hiermit starten Sie die angeschlossenen Geräte wie folgt: • 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.
	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: • 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**.

Option	Argumente	Beschreibung
-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: • 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.
-b	enter | exit	Hiermit steuern Sie den Bypass-Betrieb. Dieser Befehl ist modellspezifisch und für- Ihre USV eventuell nicht relevant.
-o	<outlet #> <Off | DelayOff | On | DelayOn | Reboot | DelayReboot | Shutdown | DelayShutdown | Cancel>	Steuern Sie die USV-Steckdosengruppen. Ersetzen Sie <outlet#> durch die Nummer der Steckdosengruppe. Wenn die Steckdosengruppe den Status **„Ein“**, hat, akzeptiert die Option die folgenden drei Argumente: • `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. Wenn die Steckdosengruppe den Status **off** hat, akzeptiert die Option zwei Argumente: • `On` – Hiermit wird die Steckdosengruppe sofort eingeschaltet. • `DelayOn` – Hiermit wird die Steckdosengruppe nach der als **Einschaltverzögerung** definierten Wartezeit in Sekunden eingeschaltet. Die **Einschaltverzögerung**, die **Abschaltverzögerung** und die **Neustartdauer** müssen über die Benutzeroberfläche konfiguriert werden.

Option	Argumente	Beschreibung
-os	<outlet #>	Hiermit zeigen Sie den Status („on“, „off“ oder „rebooting“) aller Steckdosengruppen an. Geben Sie die Nummer der Steckdosengruppe an, deren Status Sie sich ansehen möchten. Geben Sie beispielsweise `ups -os 1` ein, um den Status der Steckdosengruppe 1 angezeigt zu bekommen. Aber: 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. b) Bei einer USV OHNE Hauptsteckdosengruppe: 1 – identifiziert die geschaltete Steckdosengruppe 1 usw.
-st		Hiermit zeigen Sie den Status der USV an.
-a	start	Hiermit testen Sie den akustischen USV-Alarm.

Beispiel 1: Geben Sie Folgendes ein, um eine Laufzeitkalibrierung zu starten:
`ups -r start`

Beispiel 2: Um die Ausgangsgruppe 2 bei einem Smart-UPS XLM sofort auszuschalten, geben Sie Folgendes ein:
`ups -o 2 off`

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 | percload | pf | frequency | all	Geben Sie den Ausgangswert für den ups-Befehl ein. **Beispiel:** `ups -output 2 percload` Hiermit wird die Last in Prozent für Phase 2 der USV angezeigt.

Option	Argument	Beschreibung
-batt		Hiermit zeigen Sie den Batteriestatus der USV an.
-about		Hiermit zeigen Sie Informationen zur USV an.
-al	c | w | i	Die Angabe von „c“, „w“ oder „i“ beschränkt die Anzeige auf die Alarme Critical (c), Warning (w) oder Informational (i).

Beispiel 3: Um den Batteriestatus des MGE Galaxy-Geräts anzuzeigen, geben Sie Folgendes ein:

```
ups -batt
```

upsabout

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.

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

upslog

Dieser Befehl ist nicht bei allen USV-Geräten verfügbar.

Zugriff: Superuser, Administrator, Gerätebenutzer

Beschreibung: Zeigt das USV-Ereignisprotokoll an.

Beispiel:

```
upslog
-- Event Log -----------------------------------------------------------------
   Date: 01/13/2022               Time: 11:02:07
   ---------------------------------------------
   Date       Time     User   Event
   ------------------------------------------------------------------------
   01/09/2022 20:34:52 Device UPS: Battery module detected in location 0.
   01/09/2022 20:34:51 Device UPS: The number of unknown batteries decreased.

<ESC>- Exit, <ENTER>- Refresh, <SPACE>- Next
```

upsfwupdate

Dieser Befehl ist 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** enthalten Informationen zum Aufrufen einer Firmware-Aktualisierungsdatei sowie weitere Anweisungen.
- Aktualisierung mit einem USB-Speichermedium (nur AP9641 und AP9643):
  - 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 „/upsfw/“ 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>	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 Laufwerkbuchstaben „`D:\“ installiert`. 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]` **HINWEIS:** Die USB-ID-Nummer finden Sie mithilfe des nachfolgend beschriebenen Befehls „`-info`“.
-info	-file <Dateipfad>| -ver <Firmware-Version>	Hiermit erhalten Sie Informationen über die auf dem USB-Speichermedium im USB-Anschluss Ihrer Netzwerkmanagement-Karte verfügbare Firmware. 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]`
-instpend		Installieren Sie ein anstehendes USV-Firmware-Update.
-instabort		Abbruch einer laufenden oder anstehenden USV-Firmware-Aktualisierung.
-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
```

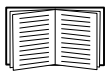
Beispiel 2:

```
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***.

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.

Option	Argument	Beschreibung
-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. Für eine Liste der verfügbaren Sprachen und der entsprechenden Sprachcodes geben Sie Folgendes ein lang. Um eine Liste der Optionen anzuzeigen, die vom Befehl „alarmcount“ akzeptiert werden, geben Sie in der Eingabeaufforderung Folgendes ein: alarmcount help.
-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
```

userauth

Zugriff: Superuser, Administrator, Nur-Netzwerk-Benutzer

Beschreibung: Hiermit zeigen Sie die Benutzerauthentifizierungsmethode an oder konfigurieren sie. Lokale Authentifizierung sowie LDAP, RADIUS- und TACACS+-Protokolle werden unterstützt.

Option	Argument	Beschreibung
-l	erste | letzte | Aus	Geben Sie an, ob und wann die lokale Benutzerdatenbank überprüft wird: erste: Die lokale Benutzerdatenbank wird immer zuerst überprüft. Wenn der Benutzername gefunden wird, wird das Passwort überprüft und die Anmeldung ist entweder erfolgreich oder nicht erfolgreich. Wenn der Benutzername nicht gefunden wird, wird die Remote-Authentifizierung verwendet, sofern sie aktiviert ist. **letzte**: Die lokale Benutzerdatenbank wird nach dem Versuch der Remote-Authentifizierung überprüft, wenn ein Fehler bei der Kontaktaufnahme mit dem Remote-Authentifizierungsserver auftritt. Wenn die Remote-Authentifizierung deaktiviert ist, verhält sie sich genauso wie **erste**. **off (aus)**: Die lokale Benutzerdatenbank wird niemals überprüft. **Hinweis**: Die Einstellung `off (aus)` wird nicht empfohlen, da dies dazu führen kann, dass Sie dauerhaft vom NMC ausgesperrt werden, wenn der Remote-Authentifizierungsserver ausfällt oder auf dem NMC falsch konfiguriert ist. Wenn off (aus) verwendet wird, wird dringend empfohlen, die Einstellung Remote Authentication Override (Remote-Authentifizierung überschreiben) `(Sitzung -a)` zu aktivieren und die Option Serial Remote Authentication Override (Serielle Remote-Authentifizierung überschreiben) `(Benutzer -sr)` für den Superuser oder einen Administrator zu setzen. **Hinweis**: Wenn sowohl die Einstellungen für die lokale als auch die entfernte Benutzerauthentifizierung auf **off (aus)** eingestellt sind, wird die Local User Authentication (lokale Benutzerauthentifizierung) automatisch auf **erste**.

Option	Argument	Beschreibung
-r	aus | Radius | tacacs+ | ldap	Geben Sie an, ob und welches Remote-Authentifizierungsprotokoll verwendet wird: **off (aus)**: Verwenden Sie keine Remote-Benutzerauthentifizierung und führen Sie immer eine lokale Benutzerauthentifizierung durch. **Radius**: Authentifizierung von Remote-Benutzern wird RADIUS verwenden. **tacacs+**: Authentifizierung von Remote-Benutzern wird TACACS+ verwenden. **ldap**: Authentifizierung von Remote-Benutzern wird LDAP verwenden.

Beispiel: Um zuerst die lokale Authentifizierung und dann die TACACS+-Authentifizierung zu konfigurieren, geben Sie Folgendes ein:

```
userauth -l first -r tacacs+
```

userdflt

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>	Der Benutzer wird bei der Erstellung standardmäßig aktiviert oder deaktiviert. Entfernen Sie (Enable) am Ende.
-pe	<Administrator | Device | Read-Only | Network-Only>	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>	Hiermit legen Sie ein standardmäßiges Sitzungs-Timeout in Minuten 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.

Option	Argument	Beschreibung
-el	<enable | disable>	Hiermit aktivieren oder deaktivieren Sie die Farbcodierung des Ereignisprotokolls.
-lf	<tab | csv>	Hiermit legen Sie das Protokoll-Exportformat fest: tab oder Comma Separated Values (CSV).
-ts	<us | metric>	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-ddyy | dd-mmm-yy | yyyymm-dd>	Hiermit legen Sie das bevorzugte Datumsformat des Benutzers fest.
-lg	<language code (e.g. enUS)>	Hiermit legen Sie eine Benutzersprache fest. Für eine Liste der verfügbaren Sprachen und der entsprechenden Sprachcodes geben Sie Folgendes ein lang. Um eine Liste der Optionen anzuzeigen, die vom Befehl „alarmcount“ akzeptiert werden, geben Sie in der Eingabeaufforderung Folgendes ein: alarmcount help.
-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:

```
userdflt -st 60
```

web

Zugriff: Super User, Administrator, Nur Netzwerk

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

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. HTTP ist standardmäßig deaktiviert.
-s	<enable | disable>	Hiermit aktivieren oder deaktivieren Sie den Zugriff auf die Benutzeroberfläche für HTTPS. HTTPS ist standardmäßig deaktiviert. Wenn HTTPS aktiviert ist, werden die Daten während der Übertragung verschlüsselt und über ein digitales Zertifikat mittels SSL/TLS authentifiziert.
-mp	<minimum protocol>	Geben Sie das Mindestprotokoll an, das die Weboberfläche verwenden soll: TLS v1.1, TLS v1.2 oder TLS v1.3.
-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.
-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.

Option	Argument	Beschreibung
-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.
`-cs`	<0 | 1 | 2 | 3 | 4>	Wählen Sie das Sicherheitsniveau der TLS v1.2-Cipher-Suites. Die Optionen sind 0 bis 4, wobei 4 die höchste und 0 die niedrigste Sicherheitsstufe bedeutet. Der Standardwert ist 4. **HINWEIS:** Die Option „`-cs`“ wird nur dann angewendet, wenn „`-mp`“ auf „TLS v1.2“ gesetzt ist. Wenn ein Wert zwischen 0 und 4 eingegeben wird, antwortet die Befehlszeilenoberfläche mit einer Liste der derzeit erlaubten SSL-Cipher-Suites.
`-hs`	`<enable | disable>`	Hiermit aktivieren/deaktivieren Sie den HTTP Strict Transport Security (HSTS)-Antwortheader.

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
```

wifi

Zugriff: Superuser, Administrator

Beschreibung: Aktivieren oder deaktivieren Sie WiFi und konfigurieren Sie die Einstellungen des WiFi-Netzwerks. **HINWEIS:** Für diesen Befehl muss das optionale APC-USB-WiFi-Gerät (AP9834) in einen USB-Anschluss einer AP9641/AP9643-Karte eingesetzt sein.

Wichtig: Es wird empfohlen, nicht die config.ini Datei von einem kabelgebundenen Gerät herunterzuladen und auf ein Gerät mit Wi-Fi Funktion hochzuladen. Es wird ebenso nicht empfohlen, die config.ini Datei eines Gerätes mit Wi-Fi Funktion herunterzuladen und die komplette Datei auf ein kabelgebundenes Gerät aufzuspielen, außer wenn die gesamte `[NetworkWiFi]` Sektion entfernt oder mit Semikolons auskommentiert wurde (zum Beispiel `;WiFi=enabled`).

Die `[NetworkWiFi]` Sektion enthält Wi-Fi spezifische Geräteeinstellungen. Diese Einstellungen sollten nicht auf ein kabelgebundenes Gerät geladen warden.

Option	Argument	Definition
`-S`	`enable | disable`	Aktivieren oder deaktivieren Sie WiFi. Standardmäßig deaktiviert. **HINWEIS:** Durch Aktivieren/Deaktivieren von WiFi wird die kabelgebundene LAN-Verbindung deaktiviert/aktiviert.

Option	Argument	Definition
-n	<Netzwerkname (SSID)>	Geben Sie den Netzwerknamen (SSID) des WiFi-Netzwerks an. Die Höchstlänge beträgt 32 Zeichen.
-t	WPA | WPA2-AES | WPA2-Gemischt | WPA2-TKIP | WPA2-Enterprise	Geben Sie den Sicherheitstyp (Authentifizierung und Verschlüsselung) des WiFi-Netzwerks an.
-p	<WiFi-Passwort>	Geben Sie ein Passwort für das WiFi-Netzwerk an. Die Höchstlänge beträgt 64 Zeichen. **HINWEIS:** Dies ist für die Sicherheitstypen WPA, WPA2-AES und WPA2-Gemischt erforderlich.
-eu	<WPA2-Enterprise-Benutzernamen>	Der Benutzername für die WPA2-Enterprise-Authentifizierung. Die Höchstlänge beträgt 32 Zeichen.
-ep	<WPA2-Enterprise-Passwort>	Das Passwort für die WPA2-Enterprise-Authentifizierung. Die Höchstlänge beträgt 32 Zeichen.
-eo	<Äußere Identität von WPA2-Enterprise>	Geben Sie die äußere Identität von WPA-2-Enterprise an. Dies ist eine optionale, unverschlüsselte Identifikation, die vom WPA-2-Enterprise-Server verwendet wird. Zum Beispiel: Benutzer@Beispiel.com oder anonym. Die Höchstlänge beträgt 32 Zeichen.
-fw	<Pfad/Dateiname>	Geben Sie die Firmwaredatei an, um die Firmware des APC-USB-WiFi-Geräts zu aktualisieren. Dabei muss es sich um eine .ism-Datei auf einem USB-Laufwerk handeln, das im USB-Anschluss der Netzwerkmanagement-Karte eingesetzt ist. **HINWEIS:** Das WiFi-Netzwerk ist während des Firmware-Upgrades nicht verfügbar.

Beispiel 1: Über die folgende Eingabe aktivieren Sie das WiFi und konfigurieren die Einstellungen des WiFi-Netzwerks:

```
wifi -S enable -n NETGEAR06 -t WPA2-AES -p apc123
```

Beispiel 2: Über die folgende Eingabe aktualisieren Sie die Firmware des APC-USB-WiFi-Geräts:

```
wifi -fw apc_uw01_wni_1-26-7.ism
```

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

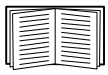
Zugriff: Superuser, Administrator

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***.

Copyright-Hinweise

Copyright-Hinweise finden Sie **hier**.

APC von Schneider Electric, weltweiter Kundendienst

Die Bedingungen für den Zugang zum Kundensupport können je nach Produkt variieren. Unser Kundendienst ist auf folgende Arten verfügbar:

- Besuchen Sie die Schneider Electric-Webseite. Dort können Sie auf die Dokumente der APC 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 Kundendiensts 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.