Befehlszeilenhandbuch

Netzwerkmanagement-Karte für Einphasen- und Dreiphasen-Easy-UPS-Geräte

AP9544, AP9547

990-91547B–005
01/2023

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.

Für den Zugriff auf die im vorliegenden Benutzerhandbuch beschriebene Befehlszeilenoberfläche muss auf der Netzwerkmanagement-Karte die Firmware für Einphasen- und Dreiphasen-Easy-UPS-Geräte installiert sein und die Netzwerkmanagement-Karte muss in einem unterstützten Easy-UPS-Gerät installiert sein. Weitere Informationen zu USV-Modellen, die mit Ihrer Netzwerkmanagement-Karte kompatibel sind, finden Sie im Knowledge Base-Artikel **FA237786** auf der APC-Support-Website, **www.apc.com/support**

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 schreibgeschützter Benutzer kann nicht auf die Befehlszeile zugreifen.

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 Konto des Benutzers „device“ gesperrt, bis ein Superuser oder Administrator das Konto erneut aktiviert.

Weitere Informationen zu diesen Optionen finden Sie im **Benutzerhandbuch** für die USV-Netzwerkmanagement-Karte 3.

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. Siehe „console“ auf Seite 11.

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
(c)Copyright 2022 All Rights Reserved Easy UPS 3-Phase APP         vx.x.x
-------------------------------------------------------------------------
Name     : Test Lab                                  Date : 02/30/2022
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             : Read/Write
SNMPv3               : Disabled         Modbus TCP         : Disabled

-------------------------------------------------------------------------
Super User           : Enabled          RADIUS             : Disabled
Administrator        : Disabled         Device User        : Disabled
Read-Only User       : Disabled         Network-Only User  : Read/Write
-------------------------------------------------------------------------
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 ein Dreiphasen-Easy-UPS-Gerät.

  ```
  Network Management Card AOS    vx.x.x
  Easy UPS 3-Phase APP           vx.x.x
  ```

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

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

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

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

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

```
Date : 02/30/2022
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

Code	Fehlermeldung
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.

Für einige der nachstehenden Befehle müssen Sie eine Lizenz erwerben.

Weitere Informationen finden Sie im **Funktionsübersichts**- und **Lizenz-FAQ**-Dokument zu Netzwerkmanagement-Karten für Easy-UPS-Geräte auf der APC-Website.

?

Zugriff: Superuser, Administrator, Gerätebenutzer

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

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

```
alarmcount ?
```

about

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

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

alarmcount

Zugriff: Superuser, Administrator, Gerätebenutzer, Schreibgeschützt

Beschreibung:

Option	Argumente	Beschreibung
`-p`	`all`	Zeigt die Anzahl der von der Netzwerkmanagement-Karte gemeldeten aktiven 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 alle aktiven Alarme angezeigt zu bekommen:

```
alarmcount -p warning
```

bacnet

Zugriff: Superuser, Administrator, Gerätebenutzer

Beschreibung: Anzeigen und definieren der BACnet-Einstellungen.

BACnet wird auf der AP9544-Karte nicht unterstützt.

Für den Zugriff auf diesen Befehl auf der AP9547-Karte ist eine Lizenz erforderlich. Siehe „license“.

Weitere Informationen zu den USV-Datenpunkten, die über BACnet bereitgestellt werden, finden Sie in den BACnet-Anwendungstabellen auf der APC-Website www.apc.com.

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 diese BACnet-Gerät, welche zur Adressierung des Geräts verwendet wird.
`-n`	`<Gerätename>`	Ein Name für dieses BACnet-Gerät, der im BACnet-Netzwerk eindeutig sein muss. Der standardmäßige Gerätename ist „BACn” und die letzten acht Ziffern der MAC-Adresse der Netzwerkmanagement-Karte. Die Länge muss zwischen 1 und 150 Zeichen betragen. Sonderzeichen sind erlaubt.
`-t`	`1000 - 30000`	Legt das APDU-Timeout fest. Das ist 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.
BACnet-IP-Einstellungen:		

Option	Argumente	Beschreibung
`-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`	`IP-Adresse`	Die IP-Adresse oder der FQDN (Fully Qualified Domain Name) des BBMD, mit der/dem diese Netzwerkmanagement-Karte registriert wird.
`-rpo`	`5000 - 65535`	Der Port des BBMD, mit dem diese Netzwerkmanagement-Karte registriert wird.
`-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.
`-fsl`		Der Registrierungsstatus fremder Geräte.

Beispiel:

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

boot

Zugriff: Super User, Administrator, Nur Netzwerk

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

Option	Argument	Beschreibung
`-b <boot mode>`	`dhcp | bootp | manual`	Hiermit legen Sie fest, wie die TCP/IP-Einstellungen beim Einschalten, beim Zurücksetzen oder bei einem Neustart der Netzwerkmanagement-Karte konfiguriert werden sollen.
`-c`	`enable | disable`	Nur für die Startmethode `dhcp`. Hiermit aktivieren oder deaktivieren Sie die Vorschrift, dass der DHCP-Server das APC-Cookie bereitstellen muss.
Die Standardwerte für diese drei Einstellungen müssen normalerweise nicht geändert werden:		
`-v`	`<vendor class>`	APC.
`-i`	`<client id>`	Die MAC-Adresse der Netzwerkmanagement-Karte, die diese im Netzwerk eindeutig identifiziert.
`-u`	`<user class>`	Der Name des Moduls der Anwendungs-Firmware.

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

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

bye

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

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

Beispiel:

```
bye
Connection Closed - Bye
```

cd

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

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

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

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

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

clrrst

Zugriff: Superuser, Administrator

Definition: Den Netzwerkschnittstellen-Resetgrund löschen. Siehe „lastrst“ auf Seite 18.

console

Zugriff: Superuser, Administrator, Nur Netzwerk

Beschreibung: 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.
`-pt`	`<Telnet-Port-Nummer>`	Hiermit legen Sie die Telnet-Port-Nummer fest, über die der Datenaustausch mit der Netzwerkmanagement-Karte erfolgen soll (Voreinstellung: 23). Der übrige zulässige Bereich ist 5000-32768.
`-ps`	`<SSH-Port-Nummer>`	Hiermit legen Sie die SSH-Port-Nummer fest, über die der Datenaustausch mit der Netzwerkmanagement-Karte erfolgen soll (Voreinstellung: 22). Der übrige zulässige Bereich ist 5000-32768.
`-b`	`2400 | 9600 | 19200 | 38400`	Hiermit konfigurieren Sie die Baud-Rate für den seriellen Anschluss (Voreinstellung: 9600).

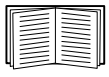
Beispiel 1: Geben Sie Folgendes ein, um den Zugriff auf die Befehlszeile über SSH zu aktivieren:
```
console -s
```

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.

Option	Argument	Beschreibung
`-z`	`<Zeitzonen-Differenz>`	Hiermit geben Sie die Differenz zwischen Ihrer Zeitzone und der Normalzeit GMT ein. Dadurch können Sie eine Synchronisierung mit Personen in anderen Zeitzonen durchführen.

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

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

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

delete

Zugriff: Superuser, Administrator

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

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

Beispiel: So löschen Sie eine Datei:

1. Navigieren Sie zu dem Ordner, der die Datei enthält. Geben Sie beispielsweise Folgendes ein, um zum Ordner `logs` zu navigieren:
   ```
   cd logs
   ```
2. Geben Sie Folgendes ein, um die im Ordner `logs` enthaltenen Dateien anzuzeigen:
   ```
   dir
   ```
3. Typ
   ```
   delete <Dateiname>
   ```

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
5165388 Dec 17  2021  apc_hw21_aos_2.1.0.6.bin
     5166412 Jan 17  2021  apc_hw21_eu3p_1.1.0.40.bin
       45000 Dec 17  5:14  config.ini
           0 Feb 23  4:31  db/
           0 Feb 23  4:31  ssl/
           0 Feb 23  4:31  ssh/
           0 Feb 23  4:31  logs/
           0 Feb 23  4:31  sec/
           0 Feb 23  4:31  fwl/
           0 Feb 23  4:31  email/
           0 Feb 23  4:31  eapol/
           0 Feb 23  4:32  license/
           0 Feb 23  4:34  fne/
```

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

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

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

Beispiel 2: Um EAPoL zu aktivieren:

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

email

Zugriff: Superuser, Administrator, Nur Netzwerk-Benutzer

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

Für den Zugriff auf diesen Befehl ist eine Lizenz erforderlich.
Siehe „license“.

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.

Option	Argument	Beschreibung
-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. • **Custom** (benutzerdefiniert): Diese Einstellung ermöglicht für jeden E-Mail-Empfänger eigene Servereinstellungen. Diese Einstellungen sind von den Einstellungen der Option -s[n] unabhängig.
-f[n]	<Absenderadresse>	Die von der Netzwerkmanagement-Karte im Feld **Von:** der gesendeten E-Mail verwendete Absenderadresse.
-s[n]	<SMTP-Server>	Die IPv4-/IPv6-Adresse oder der DNS-Name des lokalen SMTP-Servers. Verwenden Sie diese Option, wenn die Option -r[n] auf Local (lokal) gesetzt ist.
-p[n]	<Port>	Die SMTP-Port-Nummer mit einem Standardwert von 25. Alternative Ports: 465, 587, 2525, 5000 bis 32768.
-a[n]	<enable | disable> (Authentifizierung)	Aktivieren Sie diese Option, wenn der SMTP-Server eine Authentifizierung verlangt.
-u[n]	<Benutzername>	Geben Sie hier Ihren Benutzernamen und Ihr Kennwort ein, wenn der Mail-Server eine Authentifizierung verlangt.
-w[n]	<Kennwort>	
-e[n]	<none | ifsupported | always | implicit> (Verschlüsselung)	• **None** (Keine): Der SMTP-Server erfordert und unterstützt auch keine Verschlüsselung. • **If Supported** (Wenn unterstützt): Der SMTP-Server zeigt an, dass STARTTLS unterstützt wird, erfordert jedoch keine verschlüsselte Verbindung. Der STARTTLS-Befehl wird nach dem Advertisement gesendet. • **Always** (Immer): Der SMTP-Server erfordert das Senden des STARTTLS-Befehls, sobald eine Verbindung zum Server hergestellt wird. • **Implicit** (Implizit): Der SMTP-Server akzeptiert nur Verbindungen, die von vornherein verschlüsselt sind. Es wird keine STARTTLS-Nachricht an den Server gesendet.

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

Beispiel: 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
E000: Success
```

eventlog

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

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

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

exit

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

Beschreibung: Hiermit schließen Sie die Befehlszeile.

firewall

Zugriff: Super User, Administrator, Nur Netzwerk

Beschreibung: Interne NMC-Firewall aktivieren, deaktivieren oder konfigurieren.

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

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

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

format

Zugriff: Superuser, Administrator

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

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

ftp

Zugriff: Super User, Administrator, Nur Netzwerk

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

Beispiel:

```
lang
Languages
enUS - English
```

lastrst

Zugriff: Superuser, Administrator

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

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
```

ledblink

Zugriff: Superuser, Administrator

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

Parameter: Zeit in Minuten

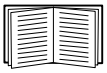
Beispiel: `ledblink 2`

```
E000: Success
```

license

Zugriff: Superuser, Administrator, Nur-Netzwerk-Benutzer

Beschreibung: Anzeige der Details der aktuellen Lizenz für Ihre Netzwerkmanagement-Karte und Online- oder Offline-Aktivierung einer Lizenz.



Weitere Informationen zu Lizenzen finden Sie im **Benutzerhandbuch** für die Netzwerkmanagement-Karte für Easy-UPS-Geräte und im **Lizenz-FAQ-Dokument**, das auf der APC-Website verfügbar ist.

Die Premium-Lizenz für AP9547 (Network Management Card for Easy UPS, 3-Phase) ist im ersten Jahr enthalten. Um die lizenzierten Funktionen nach Ablauf dieses Zeitraums weiter nutzen zu können, ist der Kauf einer Standard- oder Premium-Lizenz erforderlich.

Option	Argument	Definition
`-a`	`<Aktivierungs-ID>`	Die Aktivierungs-ID der Lizenz. Diese erhalten Sie per E-Mail, wenn Sie eine Lizenz erwerben oder verlängern. Sie hat das Format ACT-XXXX-XXXX-XXXX-XXXX.
`-u`	`<Server-URL>`	Diese URL dient zum Kontakt mit dem Lizenzserver. Sie muss auf den Standardwert eingestellt sein, um Ihre Lizenz online über den Cloud-Licensing-Server zu aktivieren.
`-r`		Anfordern der Lizenzdatei vom Cloud-Licensing-Server.
`-d`		Deaktivieren der aktuellen Lizenz.
`-g`		Erzeugen der `capabilityRequest.bin`-Datei.
`-p`		Verarbeiten der `capabilityResponse.bin`-Datei.
`-m`	`enable | disable`	Aktivieren oder deaktivieren Sie lizenzbezogene Benachrichtigungen in der Kommandozeilenoberfläche und der Web-Benutzeroberfläche. HINWEIS: Lizenzbezogene Ereignisse werden weiterhin im Ereignisprotokoll protokolliert.

Beispiel 1: Um die aktuellen Lizenzdetails anzeigen zu lassen, geben Sie `license` ein:

```
E000: Success

License Information

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

License Type:           Standard

Activation Date:        02/14/2022
```

```
Expiration Date:        02/13/2023
Activation ID:          ACT-1234-ABCD-5678-EFGH
License Server URL:     https://schneider-
electric.compliance.flexnetoperations.com/deviceservices
```

Beispiel 2: Um Ihre Lizenz online zu aktivieren, geben Sie ein:

```
license -a ACT-1234-ABCD-5678-EFGH -r
```

Beispiel 3: So aktivieren Sie Ihre Lizenz offline:

1. Geben Sie folgenden Befehl ein: `license -a ACT-1234-ABCD-5678-EFGH -g`
2. Laden Sie die `capabilityRequest.bin`-Datei mittels SCP oder FTP von der Netzwerkmanagement-Karte herunter, z. B.:
   `scp<NMC_Benutzername>@<NMC_IP_Adresse>:license/capabilityRequest.bin capabilityRequest.bin`
3. Melden Sie sich im **Lizenzportal** mit Ihrer **Aktivierungs-ID** an und gehen Sie zu **Devices > Offline Device Management** (Geräte > Offline-Geräteverwaltung). Laden Sie die `capabilityRequest.bin`-Datei hoch und die Datei `capabilityResponse.bin` herunter.
4. Laden Sie die `capabilityResponse.bin`-Datei mittels SCP oder FTP auf die Netzwerkmanagement-Karte hoch, z. B.: `scp capabilityResponse.bin <NMC_Benutzername>@<NMC_IP_Adresse>:license/capabilityResponse.bin`
5. Geben Sie folgenden Befehl ein: `license -p`

logzip

Zugriff: Superuser, Administrator

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

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

Beispiel: `logzip -m 1`

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

modbus

Zugriff: Superuser, Administrator, Gerätebenutzer

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

Modbus wird auf der AP9544-Karte nicht unterstützt.

Für den Zugriff auf diesen Befehl ist eine Lizenz erforderlich. Siehe „license“.

Option	Argument	Beschreibung
-tE	<enable | disable> (Modbus-TCP-Status)	Hiermit aktivieren oder deaktivieren Sie Modbus TCP.[2]
-tP		Hiermit legen Sie die Modbus-TCP-Portnummer fest. Die standardmäßige Portnummer ist 502 und kann auf einen Wert zwischen 5000 und 32768[2] gesetzt werden.
-tTo		Geben Sie den Modbus TCP-Kommunikationstimeout in Sekunden an, wobei 0 bedeuted, dass die Verbindung nie unterbrochen wird.[2]

Beispiel: `modbus`

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

netstat

Zugriff: Super User, Administrator, Nur Netzwerk

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

Beispiel:

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

ntp

Zugriff: Super User, Administrator, Nur Netzwerk

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

Option	Argument	Beschreibung
-OM	enable | disable	Hiermit überschreiben Sie die manuell konfigurierten Einstellungen.

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

Beispiel 1: Geben Sie Folgendes ein, um die manuell konfigurierte Einstellung überschreiben zu können:
`ntp -OM enable`

Beispiel 2: Geben Sie Folgendes ein, um den primären NTP-Server festzulegen:
`ntp -p 150.250.6.10`

ping

Zugriff: Super User, Administrator, Gerätebenutzer, Nur Netzwerk

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

Argument	Beschreibung
<IP-Adresse oder DNS-Name>	Geben Sie eine IP-Adresse im Format 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:

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“

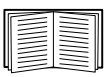
Beschreibung: Hiermit schließen Sie die Befehlszeile (funktionsgleich mit den Befehlen „exit“ und „bye“).

radius

Zugriff: Super User, Administrator, Nur Netzwerk

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

Für den Zugriff auf diesen Befehl ist eine Lizenz erforderlich. Siehe „license“.



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

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

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

```
radius -a radiusLocal
```

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

```
radius -t2 10
```

reboot

Zugriff: Super User, Administrator, Nur Netzwerk

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

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

resetToDef

Zugriff: Superuser, Administrator

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

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

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

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

```
resetToDef -p keepip
```

session

Zugriff: Superuser, Administrator

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

Option	Argumente	Beschreibung
-d	<session ID> (Löschen)	Hiermit löschen Sie die Sitzung des aktuellen Benutzers mit der angegebenen Sitzungs-ID.
-m	<enable | disable> (Mehrfachbenutzung aktivieren)	Durch die Aktivierung ermöglichen Sie zwei oder mehr Benutzern, sich gleichzeitig anzumelden. Durch die Deaktivierung ermöglichen Sie nur jeweils einem Benutzer, sich anzumelden.
-a	<enable | disable> (Remote-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.

Für den Zugriff auf diesen Befehl ist eine Lizenz erforderlich. Siehe „license“.

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

Beispiel:

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

```
Cert File: <n/a>
```

snmp

Zugriff: Super User, Administrator, Nur Netzwerk

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

SNMPv1-Unterstützung gehört nicht zum Basic-Funktionsumfang. Ohne eine Lizenz erkennen EcoStruxure-Dienste nur Ihr Gerät. Sie können keine volle Unterstützung bieten. Für eine vollständige EcoStruxure-Integration müssen Sie eine Standard- oder Premium-Lizenz inklusive SNMP-Unterstützung erwerben. Weitere Informationen finden Sie im **Funktionsübersichts**- und **Lizenz-FAQ**-Dokument zu Netzwerkmanagement-Karten für Easy-UPS-Geräte auf der APC-Website.

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.

SNMPv3-Unterstützung gehört nicht zum Basic-Funktionsumfang. Ohne eine Lizenz erkennen EcoStruxure-Dienste nur Ihr Gerät. Sie können keine volle Unterstützung bieten. Für eine vollständige EcoStruxure-Integration müssen Sie eine Standard- oder Premium-Lizenz inklusive SNMP-Unterstützung erwerben. Weitere Informationen finden Sie im **Funktionsübersichts**- und **Lizenz-FAQ**-Dokument zu Netzwerkmanagement-Karten für Easy-UPS-Geräte auf der APC-Website.

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.

Option	Argumente	Beschreibung
-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 | md5 | none	Hiermit geben Sie den Typ des Authentifizierungsprotokolls an.
-pp[n]	aes | des | none	Hiermit geben Sie das Datenschutzprotokoll (Verschlüsselung) an.
-ac[n]	enable | disable	Hiermit aktivieren oder deaktivieren Sie den Zugriff.
-au[n]	<Benutzerprofilname>	Hiermit gestatten Sie einen angegebenen Benutzerprofil den Zugriff.
-n[n]	<IP-Adresse oder Hostname für NMS>	Hiermit geben Sie die IPv4/IPv6 -Adresse oder den Hostnamen der Netzwerk-Managementstation an.

Beispiel: Geben Sie Folgendes ein, um dem Benutzer JMurphy die Zugriffsebene 2 zuzuweisen:
`snmpv3 -au2 "JMurphy"`

snmptrap

Zugriff: Superuser, Administrator, Nur Netzwerk-Benutzer

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

Für den Zugriff auf diesen Befehl ist eine Lizenz erforderlich. Siehe „license“.

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.

Option	Argumente	Beschreibung
-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
E000: Success
```

ssh

Zugriff: Super User, Administrator

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
E000: Success.
```

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
E000: Success.
```

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
E000: Success
```

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
E000: Success
```

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
E000: Success
```

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

```
ssl csr -CN 190.0.2.0 -C US
E000: Success
```

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

E000: Success
```

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

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

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

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

tcpip

Zugriff: Super User, Administrator, Nur Netzwerk

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

Option	Argument	Beschreibung
-S	enable | disable	Hiermit aktivieren oder deaktivieren Sie TCP/IP v4.
-i	<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 `tcpip` ein und betätigen Sie die EINGABETASTE, um sich die aktuellen Netzwerk-Einstellungen für die Netzwerkmanagement-Karte anzeigen zu lassen.

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

tcpip6

Die ups-Befehlsoptionen für Easy UPS-spezifische USV-Geräte:

Diese Befehle sind nur auf unterstützten Dreiphasen-Easy-UPS-Geräten verfügbar. Manche Optionen stehen möglicherweise nur für bestimmte USV-Modelle zur Verfügung. Eine Liste der USV-Geräte, mit denen die Netzwerkmanagement-Karten kompatibel sind, finden Sie im Knowledge-Base-Artikel **FA237786** auf der **APC-Website**.

Option	Argument	Beschreibung
-im	<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.
-bym	<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.
-om	<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.
-bat		Hiermit zeigen Sie den Batteriestatus der USV an.
-abt		Hiermit zeigen Sie Informationen zur USV an.
-al	c | w | i	Hiermit zeigen Sie alle vorhandenen Alarme an. Die Angabe von „c“, „w“ oder „i“ beschränkt die Anzeige auf die Alarme Critical (c), Warning (w) oder Informational (i).
-amb		Hiermit zeigen Sie die Umgebungstemperatur der USV an.
-maint		Hiermit zeigen Sie die Wartungsparameter der USV an.

Beispiel 1: Um Wartungsparameter anzuzeigen, geben Sie Folgendes ein:

```
ups -main
```

Diese Befehle sind nur auf unterstützten Einphasen-Easy-UPS-Geräten verfügbar. Manche Optionen stehen möglicherweise nur für bestimmte USV-Modelle zur Verfügung. Eine Liste der USV-Geräte, mit denen die Netzwerkmanagement-Karten kompatibel sind, finden Sie im Knowledge-Base-Artikel **FA237786** auf der **APC-Website**.

Option	Beschreibung
-im	Hiermit zeigen Sie die folgenden Eingangswerte der USV an: Eingangsspannung, Eingangsfehlerspannung und Frequenz.
-om	Hiermit zeigen Sie die folgenden Ausgangswerte der USV an: Ausgangsspannung, Ausgangsstrom, Wirkleistung und Scheinleistung.
-bat	Hiermit zeigen Sie die folgenden Batteriewerte der USV an: Batteriespannung und Batterietemperatur.
-al	Hiermit zeigen Sie alle vorhandenen kritischen, Warn- und Informationsalarme an.
-abt	Hiermit zeigen Sie Informationen zur USV an.

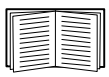
Beispiel 2: Um die Eingangswerte anzuzeigen, geben Sie Folgendes ein:

```
ups -im

E000: Success

UPS Input Measurement(s)

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

Voltage:       245.7 VAC

Frequency:     59.99 Hz

Fault Voltage: 200.0 VAC
```

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.
-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. Wenn Sie eine Liste der verfügbaren Sprachen und der entsprechenden Sprachcodes anzeigen möchten, geben Sie in der Befehlszeile „lang“ ein.
-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
```

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

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

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

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

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: SSL v3.0, TLS v1.1 oder TLS v1.2.
-ph	<HTTP-Port-Nr.>	Hiermit legen Sie den TCP/IP-Port fest, über den der HTTP-Datenaustausch mit der Netzwerkmanagement-Karte erfolgen soll (Voreinstellung: 80). Der übrige zulässige Bereich ist 5000-32768.
-ps	<HTTPS-Port-Nr.>	Hiermit legen Sie den TCP/IP-Port fest, über den der HTTPS-Datenaustausch mit der Netzwerkmanagement-Karte erfolgen soll (Voreinstellung: 443). Der übrige zulässige Bereich ist 5000-32768.
-lsp	enable | disable	Zugriff auf die Seite „Begrenzter Status“ im Web-UI aktivieren oder deaktivieren.
-lsd	enable | disable	Aktivieren oder deaktivieren Sie die Seite „Begrenzter Status“, die als Standardseite verwendet wird, wenn Sie auf die IP oder den Hostnamen des Geräts in einem Webbrowser zugreifen.

Option	Argument	Beschreibung
`-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.

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 AP9544/AP9547-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.
`-n`	`<Netzwerkname (SSID)>`	Geben Sie den Netzwerknamen (SSID) des WiFi-Netzwerks an. Die Höchstlänge beträgt 32 Zeichen.

Option	Argument	Definition
-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.

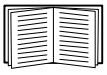
xferStatus

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

Kryptographische Bibliothek cryptlib

Berkeley Database

Lua

APC von Schneider Electric, weltweiter Kundendienst

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

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

990-91547B-005 **01/2023**