Benutzerhandbuch

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

AP9544, AP9547

990-91545B-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.

Inhalt

Einführung

Produktbeschreibung

Funktionen

Bei den nachfolgend beschriebenen Netzwerkmanagement-Karten für Einphasen- und Dreiphasen-Easy-UPS-Geräte von Schneider Electric (AP9544 und AP9547) handelt es sich um webbasierte, IPv6-fähige Produkte. Geräte mit installierter Netzwerkmanagement-Karte können mithilfe verschiedener offener Standards verwaltet werden:

Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS)	Secure SHell (SSH)
Secure Copy (SCP)	Secure Boot with Root of Trust for enhanced security
RADIUS	Extensible Authentication Protocol (EAP) over LAN (EAPoL)
Building Automation and Control Networks Protocol (BACnet) - Nur AP9547	Simple Network Management Protocol versions 1, 2c and 3
Syslog	Telnet
Modbus - Nur AP9547	Hypertext Transfer Protocol (HTTP)
File Transfer Protocol (FTP)	

Die **AP9544-** und **AP9547**-Netzwerkmanagement-Karten bieten:

- Einen USB-A-Anschluss.
- Daten- und Ereignisprotokolle.
- Möglichkeit zur Einrichtung von Benachrichtigungen mithilfe von Ereignisprotokollierung, E-Mail, Syslog und SNMP-Traps.
- Unterstützung für PowerChute® Network Shutdown. **HINWEIS:** Die AP9547-Karte in Dreiphasen-Easy-UPS-Geräten unterstützt nur das Herunterfahren vernetzter Server und Anwendungen auf diesen Servern. Das Herunterfahren der USV selbst wird nicht unterstützt.
- Unterstützt die Verwendung eines DHCP-Servers (Dynamic Host Configuration Protocol) oder eines BOOTP-Servers (BOOTstrap Protocol) zur Bereitstellung der TCP-/IP-Netzwerkparameter der NMC.
- Ermöglicht das Exportieren einer benutzerdefinierten Konfigurationsdatei (INI-Datei) von einer konfigurierten Karte an mindestens eine unkonfigurierte Karte, ohne dass die Datei dazu in eine Binärdatei konvertiert werden muss.
- Bietet mehrere Sicherheitsprotokolle für Authentifizierung und Verschlüsselung.
- Kommuniziert mit Data Center Expert, Operation oder EcoStruxure™ IT.
- Unterstützt Modbus TCP/IP (Nur AP9547).

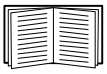
HINWEIS: Für einige dieser Protokolle und Funktionen müssen Sie eine Lizenz erwerben.

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

Unterstützte Geräte

Die Netzwerkmanagement-Karte für Easy-UPS-Geräte ist kompatibel mit:

- Einphasen-Easy-UPS-Geräten (nur AP9544).
- Dreiphasen-Easy-UPS-Geräten (nur AP9547)



Eine Liste der USV-Geräte, mit denen die Netzwerkmanagement-Karten kompatibel sind, finden Sie im Knowledge-Base-Artikel **FA237786** auf der **APC-Website**.

IPv4-Erstkonfiguration

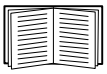
Sie müssen die folgenden TCP-/IP-Einstellungen für die Netzwerkmanagement-Karte festlegen, bevor sie im Netzwerk verwendet werden kann:

- IP-Adresse der Netzwerkmanagement-Karte
- Subnetzmaske der Netzwerkmanagement-Karte
- IP-Adresse des Standardgateways (nur erforderlich, wenn die Karte außerhalb des bestehenden Netzwerksegments betrieben werden soll)

HINWEIS: Wenn kein Standardgateway zur Verfügung steht, geben Sie die IP-Adresse eines Computers an, der sich in demselben Subnetz wie die Netzwerkmanagement-Karte befindet und normalerweise in Betrieb ist. Bei geringem Netzwerkverkehr verwendet die Netzwerkmanagement-Karte das Standardgateway, um das Netzwerk zu testen.

HINWEIS: Das Präfix der MAC-Adresse von der Netzwerkmanagement-Karte lautet 00:C0:B7 oder 28:29:86. Die MAC-Adresse Ihrer Netzwerkmanagement-Karte erfahren Sie unter **Protokolle > Firewall**. Sie können dieses MAC-Adressen-Präfix für die Konfiguration Ihres DHCP-Dienstes verwenden.

HINWEIS: Verwenden Sie nicht die Loopback-Adresse (127.0.0.1) als Standardgateway. Dadurch wird die Karte deaktiviert. Sie müssen sich dann über eine serielle Datenverbindung bei der Netzwerkmanagement-Karte anmelden und die TCP/IP-Einstellungen auf ihre Standardwerte zurücksetzen.



Informationen zum Konfigurieren der TCP/IP-Einstellungen finden Sie in der **Installationsanleitung zur Netzwerkmanagement-Karte für Easy-UPS-Geräte** (auf der **APC-Website** und als gedrucktes Dokument mitgeliefert).

Eine ausführliche Anleitung zur Verwendung eines DHCP-Servers zum Konfigurieren der TCP/IP-Einstellungen einer Netzwerkmanagement-Karte finden Sie unter „Optionen in DHCP-Antworten“.

IPv6-Erstkonfiguration

Die IPv6-Netzwerkkonfiguration bietet die nötige Flexibilität, um Ihre besonderen Anforderungen umsetzen zu können. IPv6 kann überall eingesetzt werden, wo eine IP-Adresse an dieser Schnittstelle eingegeben wird. Sie können die Konfiguration manuell, automatisch oder per DHCP (siehe Bildschirm „TCP/IP-Einstellungen für IPv6“) vornehmen.

Netzwerkmanagement mit anderen Anwendungen

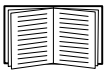
Die nachfolgend aufgeführten Anwendungen und Dienstprogramme können mit einer USV verwendet werden, die über eine Netzwerkmanagement-Karte in das Netzwerk eingebunden ist.

- PowerChute Network Shutdown – Ermöglicht ein unbeaufsichtigtes, reguläres Herunterfahren von Computern, die an USV-Geräten angeschlossen sind.
- APC PowerNet® MIB – Ermöglicht den Zugriff auf USV-Geräte über SNMP.
- Data Center Expert – Ermöglicht Power-Management und die Verwaltung von SNMPAgenten wie Netzwerk-USVs und Umgebungssensoren auf Unternehmensebene.
- EcoStruxure IT — Mit dieser cloudbasierten Überwachungssoftware können Sie Ihre USV-Geräte über SNMP und Modbus überwachen (Nur AP9547).
- Konfigurationsdienstprogramm für IP-Adressen – Dient zum Konfigurieren der Standardeinstellungen beliebig vieler Netzwerkmanagement-Karten über das Netzwerk (siehe „Assistent für die Konfiguration von Geräte-IP-Adressen“).
- Sicherheitsassistent – Dient zur Erstellung oder zum Import von TLS-Serverzertifikaten (Transport Layer Security) und SSH-Hostschlüsseln (Secure SHell), die zum Schutz der Integrität und Vertrauenswürdigkeit der Kommunikation mit der Netzwerkmanagement-Karte beitragen.

Interne Verwaltungsfunktionen

Übersicht

Verwenden Sie die Web-Benutzeroberfläche oder die Befehlszeile (Command Line Interface, CLI), um sich den Status der USV anzeigen zu lassen und die USV sowie die Netzwerkmanagement-Karte zu verwalten. Sie können auch SNMP verwenden, um den Status der USV zu überwachen.



Weitere Informationen zu den Benutzeroberflächen finden Sie unter „Web-Benutzeroberfläche“ und im **Befehlszeilenhandbuch für die Netzwerkmanagement-Karte für Easy-UPS-Geräte** auf der **APC-Website**. Informationen dazu, wie der SNMP-Zugriff auf die Netzwerkmanagement-Karte kontrolliert wird, finden Sie unter „Bildschirme für SNMP“.

Zugriffspriorität für Anmeldung

Sie können einstellen, dass sich gleichzeitig mehrere Benutzer mit gleichen Zugriffsrechten anmelden können. Siehe Bildschirm „Sitzungsverwaltung“.

Arten von Benutzerkonten

Die Netzwerkmanagement-Karte kennt verschiedene Zugriffsebenen - Superuser, Administrator, Benutzer „Gerät“, Benutzer „schreibgeschützt“ und Benutzer „nur Netzwerk“:

- Der **Superuser** darf alle Menüs der Benutzeroberfläche und alle Befehle der Befehlszeile verwenden. Der Superuser darf außerdem zusätzliche Benutzerkonten erstellen und Variablen für diese zusätzlichen Benutzer einstellen. Der voreingestellte Benutzername und das voreingestellte Passwort lauten beide beim ersten Einloggen „apc“. Nach dem Einloggen werden Sie aufgefordert, ein neues Passwort einzugeben.
  Hinweis: Der Superuser kann nicht umbenannt oder gelöscht werden, kann aber deaktiviert werden. Wir empfehlen das Konto des Superusers zu deaktivieren, nachdem weitere Administrator-Konten erstellt wurden. Stellen Sie sicher, dass mindestens ein Administrator-Konto aktiv ist, bevor Sie das Konto des Superusers deaktivieren.
- Ein **Administrator** darf alle Menüs der Benutzeroberfläche und alle Befehle der Befehlszeile verwenden. Der Standardbenutzername ist „apc“ und es muss ein Kennwort festgelegt werden, bevor das Benutzerkonto aktiviert werden kann.
- Der **Benutzer „Gerät“** besitzt Lese- und Schreibzugriff auf Gerätebildschirme. Administrative Funktionen wie die Sitzungsverwaltung im Sicherheitsmenü und die Firewall in den Protokollen sind ausgegraut.

  Der Standardbenutzername ist „device“ und es muss ein Kennwort festgelegt werden, bevor das Benutzerkonto aktiviert werden kann.
- Der **Benutzer „schreibgeschützt“** verfügt lediglich über die folgenden, eingeschränkten Zugriffsmöglichkeiten:
  - Zugriff ausschließlich über die Benutzeroberfläche.
  - Zugriff auf dieselben Menüs wie der Benutzer „Gerät“, jedoch ohne die Möglichkeit, Konfigurationen zu ändern, Geräte zu steuern, Daten zu löschen oder Optionen für Dateiübertragungen zu verwenden. Links auf die Konfigurationsoptionen sind sichtbar, aber deaktiviert. (Zu den Ereignis- und Datenprotokollen wird keine Schaltfläche zum Löschen der Protokolldaten angezeigt.)

  Der Standardbenutzername ist „readonly“ und es muss ein Kennwort festgelegt werden, bevor das Benutzerkonto aktiviert werden kann.
- Der **Benutzer „nur Netzwerk“** kann sich lediglich über die Web-Benutzeroberfläche oder die Befehlszeile (Telnet/SSH nicht seriell) anmelden. Es gibt keinen Standard-Benutzernamen und kein Standard-Kennwort.

Die Konten der Administratoren, der Gerätebenutzer, der Nur-Lesezugriff-Benutzer und der Nur-Netzwerk-Benutzer sind standardmäßig deaktiviert und können erst aktiviert werden, nachdem das standardmäßige Superuser-Passwort („apc“) geändert wurde.

Informationen zum Ändern des **Benutzernamens** und des **Passworts** für die Kontoarten Administrator, Benutzer „Gerät“ und Benutzer „schreibgeschützt“ finden Sie unter „Lokale Benutzer“.

Zurücksetzen bei vergessenem Passwort

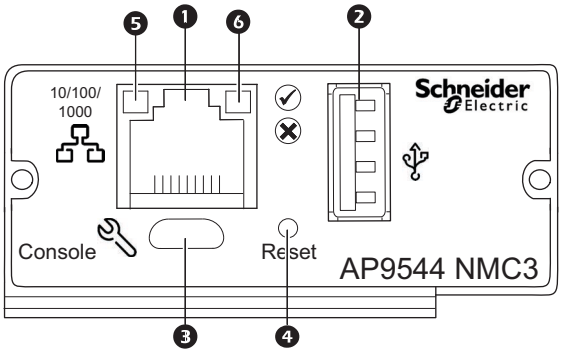
HINWEIS: Das Zurücksetzen Ihrer Netzwerkmanagement-Karte (NMC) setzt die Karte auf die Standardkonfiguration zurück.

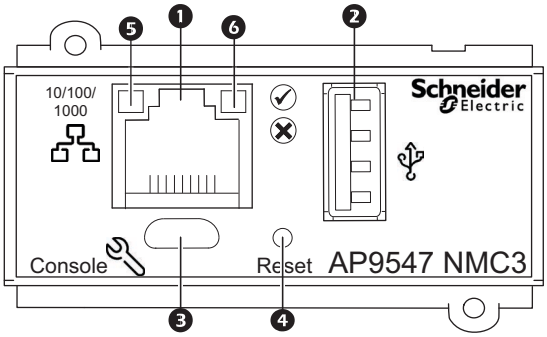
Wenn Sie Ihr Passwort vergessen haben, müssen Sie die **Reset**-Taste auf der NMC verwenden, um die gesamte Konfiguration, einschließlich des Passworts, zu löschen. Halten Sie die **Reset**-Taste 20–25 Sekunden lang gedrückt und prüfen Sie, ob die Status-LED während dieser Zeit grün pulsiert. Wenn die Status-LED zu Gelb oder Orange wechselt, geben Sie die **Reset**-Taste frei, damit der Neustart der NMC abgeschlossen werden kann.

Nach dem Neustart der NMC müssen Sie die NMC neu konfigurieren. Weitere Informationen finden Sie in der **Installationsanleitung zur Netzwerkmanagement-Karte für Easy-UPS-Geräte** oder im Knowledge Base-Artikel **FA156064** auf der APC-Website.

Es wird empfohlen, die .ini-Datei nach der Konfiguration Ihrer NMC zu exportieren, um Datenverluste im Falle eines vergessenen Passworts zu vermeiden. Siehe „Abrufen und Exportieren der .ini-Datei“.

Frontblende (AP9544/AP9547)





	Element	Beschreibung
1	10/100/1000 Base-T-Anschluss	Anschluss der Netzwerkmanagement-Karte an das Ethernet-Netzwerk.
2	USB-Anschluss	Unterstützung für das optionale APC-USB-WiFi-Gerät (AP9834). Siehe „WiFi-Bildschirm“.
3	Port für USB-Konsole	Zum Anschluss der Netzwerkmanagement-Karte über ein Micro-USB-Kabel (APC-Teilenummer 960-0603) an einen lokalen Computer, zur erstmaligen Konfiguration der Netzwerkeinstellungen und für den Zugriff auf die Befehlszeilenoberfläche.
4	Taste „Reset“	Ermöglicht das Zurücksetzen der Netzwerkmanagement-Schnittstelle. **HINWEIS:** Die Ausgangsleistung des Geräts, in dem die Netzwerkmanagement-Karte installiert ist, wird dadurch nicht beeinträchtigt.
5	Link-RX/TX-LED (10/100/1000)	Siehe „Link-RX/TX-LED (10/100/1000)“
6	Status-LED	Eine LED (Leuchtdiode) ist eine Lichtquelle. Siehe „Status-LED“.

Beschreibung der LEDs

Status-LED

Diese LED (Leuchtdiode) gibt den Status der Netzwerkmanagement-Karte an.

Zustand	Beschreibung
Aus	Eine der folgenden Situationen liegt vor: • Die Netzwerkmanagement-Karte wird nicht mit Strom versorgt. • Die Netzwerkmanagement-Karte funktioniert nicht richtig. und muss möglicherweise repariert oder ersetzt werden. Wenden Sie sich an den Kundendienst. Siehe „Weltweiter APC-Kundendienst“.
Grünes Dauerleuchten	Die Netzwerkmanagement-Karte besitzt gültige TCP/IP-Einstellungen.
Orangefarbenes Dauerleuchten	Eine der folgenden Situationen liegt vor: • In der Netzwerkmanagement-Karte wurde ein Hardwarefehler erkannt. Wenden Sie sich an den Kundendienst. Siehe „Weltweiter Kundendienst von APC by Schneider Electric“. • Die Netzwerkmanagement-Karte befindet sich im Bootmonitor-Modus. Weitere Informationen finden Sie unter „Firmware-Moduldateien (Netzwerkmanagement-Karte)“.
Grünes Blinken	Die Netzwerkmanagement-Karte verfügt nicht über gültige TCP/IP-Einstellungen.[1]
Orangefarbenes Blinken	Die Netzwerkmanagement-Karte sendet BOOTP-Anfragen.[1]
Abwechselnd grünes und orangefarbenes Blinken	Wenn die LED langsam blinkt, sendet die Netzwerkmanagement-Karte DHCP[2]-Anfragen.[1] Wenn die LED schnell blinkt, wird die Netzwerkmanagement-Karte gerade gestartet.

1. Die Konfiguration der TCP/IP-Einstellungen der Netzwerkmanagement-Karte bei Nichtverwendung eines BOOTP- oder DHCP-Servers ist in der **Installationsanleitung für Netzwerkmanagement-Karten für Easy-UPS-Geräte** Informationen beschrieben. Diese wird in gedruckter Form und auf der **APC-Website** zur Verfügung gestellt.
2. Bei Verwendung eines DHCP-Servers finden Sie entsprechende Informationen unter „Optionen in DHCP-Antworten“.

HINWEIS: Wenn das Micro-USB-Kabel während des Hochfahrens der NMC angeschlossen ist, wartet die NMC 90 Sekunden, damit Zeit für den Zugriff auf den Boot-Monitor bleibt. Siehe „Verwenden von XMODEM zum Aktualisieren einer Netzwerkmanagement-Karte“. Während dieser Verzögerungszeit sind keine LEDs aktiv. Es wird empfohlen, das Micro-USB-Kabel zu trennen, wenn kein lokaler Zugriff auf die CLI erforderlich ist.

Link-RX/TX-LED (10/100/1000)

Diese LED lässt den Netzwerkstatus der Netzwerkmanagement-Karte erkennen.

Zustand	Beschreibung
Off (Aus)	Mindestens eine der folgenden Situationen liegt vor: • Die Netzwerkmanagement-Karte wird nicht mit Strom versorgt. • Das zum Anschluss der Netzwerkmanagement-Karte an das Netzwerk verwendete Kabel wurde abgezogen oder funktioniert nicht richtig. • Das zum Anschluss der Netzwerkmanagement-Karte an das Netzwerk verwendete Gerät wurde abgeschaltet oder funktioniert nicht richtig. • Die Netzwerkmanagement-Karte funktioniert nicht richtig und muss möglicherweise repariert oder ersetzt werden. Wenden Sie sich an den Kundendienst. Siehe „Weltweiter APC-Kundendienst“.
Stetig gelb	Die Netzwerkmanagement-Karte ist mit einem Netzwerk verbunden, das mit einer Geschwindigkeit von 10–100 Megabit pro Sekunde (MBit/s) betrieben wird.

Zustand	Beschreibung
Grünes Dauerleuchten	Die Netzwerkmanagement-Karte ist mit einem Netzwerk verbunden, das mit einer Geschwindigkeit von 1000 MBit/s arbeitet.
Blinkt gelb	Die Netzwerkmanagement-Karte empfängt oder sendet Datenpakete mit einer Geschwindigkeit von 10–100 MBit/s.
Grünes Blinken	Die Netzwerkmanagement-Karte empfängt oder sendet Datenpakete mit einer Geschwindigkeit von 1000 MBit/s.

Selbstüberwachungsfunktionen

Übersicht

Um interne Probleme erkennen und nach unerwarteten Dateneingaben normal weiterarbeiten zu können, verwendet die Netzwerkmanagement-Karte interne, systemweit funktionierende Selbstüberwachungsmechanismen. Wenn die Netzwerkmanagement-Karte nach einem internen Problem neu gestartet wird, wird das Ereignis **System: Netzwerkschnittstelle neu gestartet** im Ereignisprotokoll erfasst.

Selbstüberwachungsmechanismus der Netzwerkschnittstelle

Die Netzwerkmanagement-Karte besitzt interne Selbstüberwachungsmechanismen, mit denen der Zugriff über das Netzwerk gewährleistet wird. Wenn die Netzwerkmanagement-Karte beispielsweise 9,5 Minuten lang keinen direkten oder indirekten Netzverkehr (z. B. SNMP-Daten oder Daten eines Broadcast-Protokoll) empfängt, interpretiert sie dies als Problem mit der eigenen Netzwerkschnittstelle und startet sich automatisch neu.

Zurücksetzen des Netzwerk-Timers

Um zu verhindern, dass die Netzwerkmanagement-Karte immer dann neu gestartet wird, wenn 9,5 Minuten lang keine Daten über das Netzwerk übertragen wurden, versucht die Netzwerkmanagement-Karte alle 4,5 Minuten, das Standardgateway zu erreichen. Wenn das Gateway vorhanden ist, antwortet es der Netzwerkmanagement-Karte, wodurch der Netzwerk-Timer zurückgesetzt wird und die 9,5 Minuten erneut heruntergezählt werden. Wenn in Ihrem konkreten Fall kein Gateway benötigt wird oder keines vorhanden ist, geben Sie die IP-Adresse eines im selben Subnetz des Netzwerks laufenden Computers an. Durch den von diesem Computer ausgehenden Netzverkehr wird der 9,5-Minuten-Timer häufig genug zurückgesetzt, um einen Neustart der Netzwerkmanagement-Karte zu verhindern.

Automatische Abmeldung

Die Benutzer werden standardmäßig nach einer Inaktivität von 3 Minuten von der Web- und Befehlszeilenoberfläche der Netzwerkmanagement-Karte abgemeldet. Die Standard-Abmeldezeit jedes Benutzers kann über die Weboberfläche eingestellt werden:

Konfiguration > Sicherheit > Lokale Benutzer > Verwaltung

- Klicken Sie auf den Hyperlink des jeweiligen Benutzernamens, um Änderungen an dem gewünschten Konto durchzuführen.
- Ändern Sie unter „Sitzungs-Timeout“ die Anzahl der Minuten.

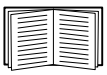
Automatische Abmeldung	Dauer (min)
Standard	3
Min.	1
Max.	60 (1 h)

Web-Benutzeroberfläche

Einführung

Übersicht

Die Web-Benutzeroberfläche enthält Optionen zur Verwaltung der USV und der Netzwerkmanagement-Karte 3 (NMC 3) in der USV sowie zum Anzeigen des USV-Status.



Informationen dazu, wie Sie die für den Zugriff auf die Benutzeroberfläche relevanten Protokolle auswählen, aktivieren und deaktivieren und die für diese Protokolle maßgeblichen Ports auf dem Web-Server einstellen, finden Sie unter Bildschirm „Web-Zugriff“.

Unterstützte Web-Browser

Die Web-Benutzeroberfläche der Netzwerkmanagement-Karte 3 ist kompatibel mit:

- Windows® Betriebssystemen:
  - Aktuelle Version von Microsoft® Edge®

Hinweis: Der Bildschirm „Firmware-Aktualisierung“ der USV ist nicht mit dem Edge®-Browser kompatibel. Siehe PowerChute Network Shutdown-Clients auf Seite 26.

- Allen Betriebssystemen:
  - Aktuelle Version von Mozilla® Firefox® oder Google® Chrome®

Eventuell funktionieren auch andere Browser, diese wurden jedoch nicht umfassend getestet.

Die Netzwerkmanagement-Karte funktioniert nicht in Verbindung mit einem Proxy-Server. Bevor Sie einen Browser zum Zugriff auf die Benutzeroberfläche der Netzwerkmanagement-Karte verwenden können, müssen Sie eine der folgenden Aktionen durchführen:

- Konfigurieren Sie den Browser so, dass kein Proxy-Server für die Netzwerkmanagement-Karte verwendet wird.
- Konfigurieren Sie den Proxy-Server so, dass er nicht als Proxy für die IP-Adresse der Netzwerkmanagement-Karte dient.

Vorgehensweise zur Anmeldung

Übersicht

Sie können den DNS-Namen oder die IP-Adresse der Netzwerkmanagement-Karte als URL-Adresse der Benutzeroberfläche verwenden. Melden Sie sich mit Ihrem Benutzernamen und Kennwort unter Beachtung der Groß-/Kleinschreibung an. Der Standard-Benutzername ist je nach Kontotyp verschieden:

- Verwenden Sie „`apc`“ als Standardwerte für Benutzername und Passwort, um sich als Administrator oder Superuser anzumelden.
- `device` für einen Benutzer „Gerät“
- `readonly` für einen Benutzer „schreibgeschützt“

Siehe auch „Arten von Benutzerkonten“.

Sie können die gewünschte Sprache der Benutzeroberfläche bei der Anmeldung aus dem Dropdown-Listenfeld **Sprache** auswählen. Siehe „Ändern der Sprache der Benutzeroberfläche“.

Wenn HTTPS aktiviert ist, erstellt die Netzwerkmanagement-Karte ihr eigenes Zertifikat. Dieses Zertifikat handelt Verschlüsselungsmethoden mit Ihrem Browser aus. Weitere Informationen finden Sie im ***Sicherheitsleitfaden*** auf der **APC-Website**.

URL-Adressformate

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

HINWEIS: HTTP ist standardmäßig deaktiviert und HTTPS ist standardmäßig aktiviert.

Typische Fehlermeldungen verschiedener Browser bei der Anmeldung.

Fehlermeldung	Browser	Fehlerursache
„Diese Seite kann nicht angezeigt werden.“	Internet Explorer	Der Webzugriff ist deaktiviert oder die URL wurde nicht richtig eingegeben.
„Verbindungsaufbau nicht möglich.“	Firefox, Chrome	

Beispiele für das URL-Format. Siehe auch Bildschirm „TCP/IP-Einstellungen für IPv6“.

Beispiel und Zugriffsmethode	URL-Format
DNS-Name von `Web1`	
HTTP	`http://Web1`
HTTPS	`https://Web1`
IP-Systemadresse `139.225.6.133` und ein standardmäßiger Web-Server-Port (80)	
HTTP	`http://139.225.6.133`
HTTPS	`https://139.225.6.133`
IP-Systemadresse `139.225.6.133` und ein nicht standardmäßiger Web-Server-Port (5000)	
HTTP	`http://139.225.6.133:5000`
HTTPS	`http://139.225.6.133:5000`
IPv6-Systemadresse `2001:db8:1:2c0:b7ff:fe00:1100` und ein nicht standardmäßiger Web-Server-Port (5000)	
HTTP	`http://[2001:db8:1:2c0:b7ff:fe00:1100]:5000`

Erstmaliges Einloggen

Wenn Sie sich zum ersten Mal auf der Netzwerkmanagement-Karte einloggen, werden Sie aufgefordert, das Standardpasswort des Superuser-Kontos („apc“) zu ändern. Nachdem Sie sich eingeloggt haben, werden Sie zum Bildschirm für die zusammenfassende Konfigurationsübersicht weitergeleitet. Dieser Bildschirm bietet eine Übersicht aller Systemprotokolle und deren aktueller Werte (z. B. aktiviert/deaktiviert). Sie können diesen Bildschirm jederzeit nachträglich über den folgenden Pfad aufrufen: **Konfiguration > Netzwerk > Zusammenfassung**.

Startbildschirm

Übersicht

Befehlsfolge: Start

Auf dem **Startbildschirm** der Benutzeroberfläche können Sie sich aktive Alarmzustände und die zuletzt im Ereignisprotokoll erfassten Ereignisse ansehen.

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

Symbol	Beschreibung
	**Keine Alarme**: Es liegen keine Alarme vor und die USV sowie die Netzwerkmanagement-Karte funktionieren normal.
	**Warnung**: Es liegt ein Alarm vor, dem genauer nachgegangen werden muss und der zu einer Gefahr für Daten oder Hardware werden könnte, wenn seine Ursache nicht behoben wird.
	**Kritisch**: Es liegt ein kritischer Alarm vor, der ein sofortiges Eingreifen erfordert.

In der oberen rechten Ecke jedes Bildschirms wird der USV-Status mithilfe der stets identischen Symbole angegeben. Bei dem Alarmzustand **Kritisch** oder **Warnung** wird zudem die Anzahl der aktiven Alarmzustände angezeigt.

Klicken Sie auf **Mehr Ereignisse**, um das gesamte Ereignisprotokoll anzuzeigen.

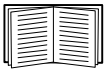
Symbole und Links

Um einen beliebigen Bildschirm zum Startbildschirm zu machen (d. h. dieser Bildschirm wird als Erstes nach Ihrer Anmeldung angezeigt), wechseln Sie zu diesem Bildschirm und klicken auf das  Symbol oben rechts.

Klicken Sie auf  , wenn Sie wieder den standardmäßigen Startbildschirm nach Ihrer Anmeldung anzeigen möchten.

Links unten auf jedem Bildschirm befinden sich drei konfigurierbare Links zu nützlichen Websites. In der Grundeinstellung führen diese Links auf die folgenden Webseiten:

- Link 1: die Seite **Knowledge Base** von www.apc.com mit nützlichen Informationen zur Fehlersuche
- Link 2: die Seite **Product Information** von www.apc.com mit Hintergrundinformationen zu Ihrer Hardware
- Link 3: die Seite **Downloads** von www.apc.com mit verfügbarer Firmware und Software



Das Umkonfigurieren dieser Links ist unter Bildschirm „Schnellverknüpfungen“ beschrieben.

Überwachung der USV: Menü „Status“

Die Optionen im Menü „Status“ melden den aktuellen Status Ihrer USV und Ihres Netzwerks.

Sie können Ihre USV und Ihr Netzwerk mithilfe der Optionen im Menü „Konfiguration“ konfigurieren (siehe „Konfiguration Ihrer Einstellungen: 1“ und „Konfiguration Ihrer Einstellungen: 2“).

Siehe dazu die folgenden Abschnitte:

- USV im Menü „Status“
- Übersicht im Menü „Status“
- Messungen im Menü „Status“
- Netzwerk im Menü „Status“
- Wartung im Menü „Status“

USV im Menü „Status“

Befehlsfolge: Status > USV

Die folgenden Optionen sind nur für unterstützte Einphasen-Easy-UPS-Geräte mit installierter AP9544-Karte relevant.

Hier sehen Sie USV-Last, Batterieladung, Spannung und andere nützliche Informationen.

Feld	Beschreibung
USV-Eingangsmesswerte	
Spannung	Die von der USV empfangene Wechselspannung.
Frequenz	Die Frequenz der Eingangsspannung in Hertz.
Maximalspannung	Die höchste Eingangsspannung an der USV in der letzten Betriebsminute.
Minimalspannung	Die niedrigste Eingangsspannung an der USV in der letzten Betriebsminute.
USV-Ausgangsmesswerte	
Spannung	Die Wechselspannung, die die USV an die angeschlossene Last liefert.
Strom	Der an die Last gespeiste Strom in Ampere.
Prozentuale Wirkleistung	Die Wirkleistung in Prozent.
Frequenz	Der Ist-Wert der Frequenz der Ausgangsspannung in Hertz.
Prozentuale Scheinleistung	Die Scheinleistung in Prozent.
USV-Batterieangaben	
Batteriespannung	Die Gleichstromspannung der Batterien.
Verbleibende Batteriekapazität	Die Batteriekapazität der USV in Prozent, die verfügbar ist, um die angeschlossene Last mit Strom zu versorgen.
Letzter Batterieaustausch	Das Datum, an dem zuletzt eine Batterie ausgetauscht wurde, im Format MM/TT/JJ.

Feld	Beschreibung
Batteriespannungsnennwert	Die Nennspannungskapazität der USV-Batterien; die Gleichstromnennspannung, die die Batterien liefern können, wenn die USV ihre Batterie als Ausgangsversorgung verwendet.
Innentemperatur	Umgebungstemperatur der USV.
Verbleibende Laufzeit	Die Dauer in Stunden und Minuten, wie lange die USV die Stromlast im Batteriebetrieb unterstützen kann.
Batteriestrom	Der Ausgangsstrom der Batterie.
Batteriekapazität	Die Batteriekapazität der USV in Prozent, die verfügbar ist, um die angeschlossenen Geräte mit Strom zu versorgen.
Bypass-Frequenzbereich	
Untergrenze	Die Untergrenze des Bypass-Frequenzbereichs in Hertz (Hz).
Obergrenze	Die Obergrenze des Bypass-Frequenzbereichs in Hertz (Hz).
Eco-Spannungsbereich	
Untergrenze	Die Untergrenze des Spannungsbereichs im Eco-Modus.
Obergrenze	Die Obergrenze des Spannungsbereichs im Eco-Modus.
USV-Batteriemodul-Status	
Batteriemodul N	Der Status des Batteriemoduls des USV-Geräts. Zum Beispiel: Installiert, Nicht installiert.
Batterie-ID	Die ID des Batteriemoduls.

Übersicht im Menü „Status“

Befehlsfolge: Status > Übersicht

Die folgenden Optionen sind nur für unterstützte Dreiphasen-Easy-UPS-Geräte mit installierter AP9547-Karte relevant.

Sie bieten eine Übersicht des USV-Geräts, einschließlich aktiver Alarme, Batteriekapazität und anderer nützlicher Informationen.

Feld	Beschreibung
Schnellstatus	
Last	Eine Grafik der Last der von der USV versorgten angeschlossenen Geräte als Prozentsatz der Nennleistung.
Batteriekapazität	Eine Grafik, die den für angeschlossene Geräte verfügbaren Prozentsatz der Gesamtkapazität der USV-Batterie zeigt.
Eingangsspannung	Die von Phase zu Phase der USV empfangene Wechselspannung.
Ausgangsspannung	Die der Last von der USV bereitgestellte Wechselspannung.
Verbleibende Laufzeit	Die Dauer in Stunden und Minuten, wie lange die USV die Stromlast im Batteriebetrieb unterstützen kann.

Feld	Beschreibung
Letztes Umschalten auf Batterieversorgung	Der Grund für die letzte Umschaltung auf Batteriestrom in der USV.
Umgebungstemperatur	Umgebungstemperatur der USV.
Letzte Geräteereignisse	
Eine Liste der zuletzt aufgetretenen USV-Ereignisse in umgekehrter chronologischer Reihenfolge. Um das gesamte Ereignisprotokoll anzuzeigen, klicken Sie auf **Mehr Ereignisse**.	

Messungen im Menü „Status“

Die folgenden Optionen sind nur für unterstützte Dreiphasen-Easy-UPS-Geräte mit installierter AP9547-Karte relevant.

Befehlsfolge: Status > Messungen > Eingang

Feld	Beschreibung
Frequenz	Die Frequenz der Eingangsspannung in Hertz.
Spannung	Die von jeder Phase der USV empfangene Wechselspannung in Volt.
Strom	Der Strom in Ampere, der für jede Phase durch die Eingangsspannung bereitgestellt wird.

Befehlsfolge: Status > Messungen > Bypass

Feld	Beschreibung
Frequenz	Die Frequenz der Bypass-Eingangsspannung in Hertz.
Spannung	Die zwischen den Phasen gemessene Wechselspannung des Bypass-Eingangs in Volt. Die Spannung zwischen Phase und Nullleiter wird nicht gemessen.

Befehlsfolge: Status > Messungen > Ausgang

Feld	Beschreibung
Gesamtwirkleistung	Die durch die angeschlossenen Geräte erzeugte Last am Ausgang der USV in kW.
Gesamtscheinleistung	Die durch die angeschlossenen Geräte erzeugte Last am Ausgang der USV in kVA.
Prozentuale Gesamtausgangslast	Die Leistung (Last) der von der USV versorgten angeschlossenen Geräte als Prozentsatz der Nennleistung.
Frequenz	Der Ist-Wert der Frequenz der Ausgangsspannung in Hertz.
Ausgangs-Nennscheinleistung	Dies ist die maximale Leistung (in kVA), die der USV zur Verfügung steht. Wenn die Last über diesem Wert liegt, wird ein Überlast-Alarm ausgelöst.
Spannung	Die von jeder Phase der USV an die angeschlossene Last gelieferte Wechselspannung in Volt.
Strom	Der von jeder Phase an die Last gespeiste Strom in Ampere.
Wirkleistung	Die durch die angeschlossenen Geräte erzeugte Last auf jeder Phase der USV in kW.
Scheinleistung	Die durch die angeschlossenen Geräte erzeugte Last auf jeder Phase der USV in kVA.

Befehlsfolge: Status > Messungen > Batterie

Feld	Beschreibung
Verbleibende Laufzeit	Die Dauer in Stunden und Minuten, wie lange die USV die Stromlast im Batteriebetrieb unterstützen kann.
Verbleibende Batteriekapazität	Die derzeitige Batteriekapazität als Prozentsatz der vollen Batteriekapazität.
Batteriebetriebszeit	Die Dauer, wie lange die USV von der Batterie anstelle der Netzstromversorgung betrieben wurde.
Batteriespannung (+/-)	Der Ist-Wert der gemessenen Gleichstromspannung der Batterie.
Batteriestrom (+/-)	Der Ist-Wert des gemessenen Batteriestroms.
Batterietemperatur	Der Ist-Wert der Batterietemperatur.
Ergebnis des letzten Batterietests	Das Ergebnis des automatischen Batterietests.
Letztes Umschalten auf Batterieversorgung	Der Grund für die letzte Umschaltung auf Batteriestrom in der USV.

Befehlsfolge: Status > Messungen > Andere Parameter

Feld	Beschreibung
ECO-Modus	Gibt an, ob der ECO-Modus aktiviert oder deaktiviert ist. Wenn die USV auf den Energiesparmodus eingestellt ist und die Netzstromversorgung im Toleranzbereich liegt, arbeitet die USV „offline“, direkt am Netz (am Bypass), und geht wieder „online“ (am Umrichter), wenn die Stromversorgung nicht mehr im Toleranzbereich liegt.
USV-Typ	Gibt an, wie die USV konfiguriert ist: Einfach, 1+1 redundant, parallel oder 3:3 parallel.
Netzstromversorgung	Gibt an, ob die Netzstromversorgung als Quelle für den Leistungswandler verwendet wird.
Status des statischen USV-Bypass-Schalters	Dieser Schalter befindet sich im Inneren der USV und ermöglicht dem Schaltgerät, die USV in den Bypass-Modus umzuschalten. Wenn der statische Bypass-Schalter geschlossen ist, versorgt die Quelle die Last mit Strom und das Schaltgerät kann die USV in den Bypass-Modus versetzen. Wenn der statische Bypass-Schalter geöffnet ist, versorgt die USV die Last mit Strom.

Netzwerk im Menü „Status“

Befehlsfolge: Status > Netzwerk

Auf dem Netzwerkbildschirm finden Sie Ihre IP-Adresse, den Domänennamen und die Einstellungen des Ethernet-Anschlusses. Siehe „Netzwerk im Menü „Konfiguration““ für Hintergrunddetails zu den Feldern.

Wartung im Menü „Status“

Befehlsfolge: Status > Wartung

Die folgenden Optionen sind nur für unterstützte Dreiphasen-Easy-UPS-Geräte mit installierter AP9547-Karte relevant.

Sie bieten eine Übersicht des USV-Geräts, einschließlich aktiver Alarme, Batteriekapazität und anderer nützlicher Informationen.

Feld	Beschreibung
Wartungszyklus	
DC-Kondensator	Der Wartungszyklus des DC-Kondensators.
AC-Kondensator	Der Wartungszyklus des AC-Kondensators.
Hilfsstromversorgung	Der Wartungszyklus der Hilfsstromversorgung.
Luftfilter	Der Wartungszyklus des Luftfilters.
Batterie	Der Wartungszyklus der Batterie.
Garantiezyklus	
Garantie	Der USV-Garantiezyklus.
Laufzeit	
AC-Kondensator	Die Laufzeit des AC-Kondensators seit der letzten Änderung.
DC-Kondensator	Die Laufzeit des DC-Kondensators seit der letzten Änderung.

USV-Steuerung

Über die Optionen im Menü „Steuerung“ können Sie sofortige Aktionen für Ihre USV durchführen und zudem auf bestimmte Sicherheits- und Netzwerkfunktionen zugreifen.

Siehe dazu die folgenden Abschnitte:

- USV im Menü „Steuerung“
- „Sicherheit“ im Menü „Steuerung“
- „Netzwerk“ im Menü „Steuerung“

USV im Menü „Steuerung“

Befehlsfolge: Steuerung > USV

Die folgenden Optionen sind nur für unterstützte Einphasen-Easy-UPS-Geräte mit installierter AP9544-Karte relevant.

Wenn Sie die Option einer Optionsschaltfläche auswählen und auf „Weiter“ klicken, wird die durchzuführende Aktion in einem anderen Bildschirm zusammengefasst. Klicken Sie auf „Übernehmen“, um mit der Aktion fortzufahren.

Vorgang	Beschreibung
USV neu starten	Startet die angeschlossenen Geräte neu, indem die USV aus- und wieder eingeschaltet wird. Folgende Parameter steuern den Neustart: • Shutdown-Verzögerung • Minimale Batteriekapazität • Einschaltverzögerung
USV abschalten	Schaltet die Ausgangsversorgung der USV ohne Abschaltverzögerung umgehend ab. Die USV bleibt abgeschaltet, bis Sie sie wieder einschalten.
USV in Ruhezustand versetzen	Hiermit versetzen Sie die USV in den Ruhezustand, indem Sie ihre Ausgangsversorgung für eine bestimmte Zeit abschalten. Klicken Sie auf „Weiter“, um bestimmte Informationen zu Zeit und Verzögerungen anzuzeigen. • 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 zweier konfigurierter Wartezeiten wieder ein: „Ruhezustand-Zeit“ und „Anschaltverzögerung“.
USV in Bypass-Modus versetzen/USV aus Bypass-Modus schalten	Mit diesen Optionen steuern Sie die Verwendung des Bypass-Modus, in welchem Sie Wartungsarbeiten an der USV ausführen können, ohne die Stromversorgung der USV ausschalten zu müssen.

Vorgang	Beschreibung
PowerChute®-Server-Shutdown signalisieren	Wählen Sie diese Option aus, um allen als „PowerChute Network Shutdown-Clients“ konfigurierten Servern, die mit dieser USV kommunizieren, ein Signal zu geben, gemäß den für „PowerChute-Shutdown-Parameter“ konfigurierten Werten herunterzufahren. Mit dieser Option werden keine Server benachrichtigt, wenn Bypass-Steuerungsaktionen durchgeführt werden.

„Sicherheit“ im Menü „Steuerung“

Befehlsfolge: Steuerung > Sicherheit > Sitzungsverwaltung

Der Bildschirm enthält Details zu angemeldeten Benutzern, der verwendeten Oberfläche (z. B. die Web-Benutzeroberfläche, die Befehlszeile), ihrer IP-Adresse und wie lange sie schon angemeldet sind.

Wenn Sie über ausreichende Rechte verfügen, klicken Sie auf den Namen, um anzuzeigen, welche Authentifizierungsmethoden zur Überprüfung des Benutzers verwendet wurden. Sie können dann außerdem die Schaltfläche **Sitzung beenden** verwenden, um einen Benutzer abzumelden.

„Netzwerk“ im Menü „Steuerung“

Befehlsfolge: Steuerung > Netzwerk > Zurücksetzen/neu starten

Verwenden Sie diese Optionen, um verschiedene Optionen der Netzwerkmanagement-Karte und die Benutzeroberfläche zurückzusetzen.

Vorgang	Beschreibung
Management-Schnittstelle neu starten	Startet die Management-Schnittstelle (d. h. die Web-Benutzeroberfläche oder die Befehlszeile) neu, indem Sie abgemeldet werden. Die USV-Geräte und die Netzwerkmanagement-Karte werden nicht neu gestartet.
Alle zurücksetzen[1]	Vorsicht: Hiermit setzen Sie alle Konfigurationswerte auf ihre Standardeinstellungen zurück. • Wenn Sie nicht **TCP/IP ausschließen** wählen, werden alle konfigurierten Werte und Einstellungen auf ihre Standardwerte zurückgesetzt, einschließlich der Einstellung, die festlegt, wie dieses Gerät seine TCP/IP-Konfigurationswerte und die EAPoL-Konfiguration abrufen muss.Die Voreinstellung für die TCP/IP-Konfigurationseinstellungen ist DHCP und die Voreinstellung für EAPoL-Zugriff ist deaktiviert. • Wenn Sie **TCP/IP ausschließen** wählen, werden alle konfigurierten Werte und Einstellungen mit Ausnahme der Einstellung, die bestimmt, wie dieses Gerät seine TCP/IP abrufen muss, und die EAPoL-Konfigurationswerte auf ihre Standardwerte zurückgesetzt.
Nur zurücksetzen[1]	**TCP/IP**: Setzt nur die Einstellung zurück, die festlegt, wie dieses Gerät seine TCP/IP-Konfigurationswerte einschließlich der EAPoL-Konfiguration abrufen muss, die auf deaktiviert zurückgesetzt wird.Die Voreinstellung für die TCP/IP-Konfiguration ist DHCP und die Voreinstellung für EAPoL-Zugriff ist deaktiviert.
	Ereigniskonfiguration: Setzt die Ereignisse auf die Standardkonfiguration zurück.Jedes speziell konfigurierte Ereignis oder jede Gruppe wird auch auf den Standardwert zurückgesetzt.Siehe „Benachrichtigungsmenü“
[1]Das Zurücksetzen der Netzwerkmanagement-Karte kann bis zu einer Minute dauern. Der von Ihnen konfigurierte USV-Name wird nicht zurückgesetzt (siehe Planung für das Herunterfahren).	

Konfiguration Ihrer Einstellungen: 1

Mithilfe der Optionen im Menü „Konfiguration“ können Sie die grundlegenden Werte für den Betrieb Ihrer USV und der Netzwerkmanagement-Karte festlegen.

Siehe dazu die folgenden Abschnitte sowie „Konfiguration Ihrer Einstellungen: 2“.

- „Stromversorgungseinstellungen“ im Menü „Konfiguration“
- Bildschirme „USV Allgemein“
- Bildschirm „Selbsttest-Planung“
- „Herunterfahren“ im Menü „Konfiguration“
- „Planung für das Herunterfahren“
- „PowerChute Network Shutdown-Clients“
- Menü „Sicherheit“

HINWEIS: Sie können einige der Konfigurationseinstellungen über den Bildschirm für die Konfigurationsübersicht (Konfiguration > Netzwerk > Zusammenfassung) einsehen.

„Stromversorgungseinstellungen“ im Menü „Konfiguration“

Pfad: Konfiguration > Stromversorgungseinstellungen

Die folgenden Optionen sind nur für unterstützte Einphasen-Easy-UPS-Geräte mit installierter AP9544-Karte relevant.

Die **Nennausgangsspannung** ist die Wechselspannung, die die USV an die angeschlossene Last liefert. Sie können die folgenden Komponenten gerätespezifisch konfigurieren:

- **Hohe** und **niedrige Übergangsspannung**: Hohe und niedrige Übergangsspannung in VAC
- **Ausgangsfrequenz**: Die Ausgangsfrequenz in Hertz (Hz).

Bildschirme „USV Allgemein“

Pfad: Konfiguration > USV

Die folgenden Optionen sind nur für unterstützte Einphasen-Easy-UPS-Geräte mit installierter AP9544-Karte relevant.

Feld	Beschreibung
USV-Name	Ein Name zur Identifizierung der USV.
Last Battery Replacement (Einstellung)	Geben Sie Monat und Jahr des letzten USV-Batteriewechsels ein.
Anzahl der externen Batterien	Die Anzahl der Batterien, über die die USV verfügt, jedoch ohne eingebaute Batterien. Bei einigen Geräten mit mehr als 16 Batterien muss die Anzahl der hinzugefügten Batterien ein Vielfaches von 16 betragen (also 16, 32, 48 usw.); diese Zahl kann jedoch dann an den richtigen Wert angeglichen werden.

Befehlsfolge: Konfiguration > USV > Stromversorgung

Die folgenden Optionen sind nur für unterstützte Dreiphasen-Easy-UPS-Geräte mit installierter AP9547-Karte relevant.

Alarmgrenzwerte beruhen auf der verfügbaren Laufzeit und redundanten Leistung sowie der USV-Last. Sie können den Schwellenwert für „**Alarm bei Last über**“ konfigurieren, der einen Alarm auslöst, wenn die Last den konfigurierten Wert in kVA überschreitet.

Bildschirm „Selbsttest-Planung“

Pfad: USV > Konfiguration > Selbsttest-Planung

Die folgenden Optionen sind nur für unterstützte Einphasen-Easy-UPS-Geräte mit installierter AP9544-Karte relevant.

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

Verwenden Sie diese Option, um festzulegen, wann Ihre USV einen Selbsttest startet.

„Herunterfahren“ im Menü „Konfiguration“

Pfad: Konfiguration > Herunterfahren

Verwenden Sie diese Option, um die Parameter für das Herunterfahren der USV zu konfigurieren. Weitere Informationen finden Sie in der folgenden Tabelle sowie unter „Gesteuertes vorzeitiges Herunterfahren und Ende des Herunterfahrens“.

Herunterfahren starten

Definieren Sie die Verzögerungen und Zeitspannen, die in Betracht gezogen werden, wenn die USV heruntergefahren werden muss.

Feld	Beschreibung
Betriebsdauer bei schwacher Batterie	Legt bei einer USV, die mit Batteriestrom läuft, fest, bei welcher verbleibenden Batterielaufzeit die USV einen niedrigen Batteriestand signalisiert. Wenn beispielsweise die Option „Betriebsdauer bei schwacher Batterie“ auf zehn Minuten eingestellt ist und die voraussichtlich verbleibende Laufzeit der USV zehn Minuten oder weniger beträgt, wird ein niedriger Batteriestand signalisiert. Wird die Stromversorgung der USV nicht wiederhergestellt, schaltet sich diese bei aufgebrauchter Batterie aus. Ein niedriger Batteriestand führt dazu, dass alle mit der Netzwerkmanagement-Karte verbundenen PowerChute Network Shutdown-Clients heruntergefahren werden.
Maximal erforderliche Verzögerung	Berechnet die Verzögerung, die erforderlich ist, damit jeder PowerChute-Client genügend Zeit hat, um ohne Datenverluste herunterzufahren, wenn die USV oder der PowerChute-Client ein reguläres Herunterfahren initiiert. • Es ist die längste Abschaltverzögerung, die von einem unter den PowerChute Network Shutdown-Clients aufgeführten Servern benötigt wird. • Sie wird immer dann berechnet, wenn die Management-Schnittstelle der USV eingeschaltet oder zurückgesetzt wird oder wenn die Option *Aushandlung erzwingen* ausgewählt und auf „Übernehmen“ geklickt wird. Siehe „Verzögertes Abschalten und PowerChute Network Shutdown“.

Dauer des Herunterfahrens

Legen Sie fest, wie lange die USV ausgeschaltet bleibt.

Feld	Beschreibung
Ruhezustand-Zeit	Legt fest, wie lange die USV die Ausgangsversorgung ausgeschaltet lässt, wenn Sie die USV in den Ruhezustand versetzen. Wenn die USV ausgeschaltet wird, schaltet sie sich nach Verstreichen der hier festgelegten Ruhezustand-Zeit und der Neustartzeit wieder ein. Wurde die Netzstromversorgung noch nicht wiederhergestellt, wartet die USV mit dem Einschalten bis zu deren Wiederherstellung. Der Ruhezustand-Befehl kann über USV im Menü „Steuerung“ auf dem USV-Display per SNMP-Befehl oder PowerChute Business Edition ausgegeben werden.

PowerChute-Shutdown-Parameter

Befehlsfolge: Konfiguration > PowerChute > PowerChute®-Konfiguration

Dies ist die Befehlsfolge für Dreiphasen-Easy-UPS-Geräte.

Diese Optionen sind nicht bei allen USV-Geräten verfügbar.

Legen Sie die von PowerChute Network Shutdown verwendeten Shutdown-Parameter fest.

Feld	Beschreibung
Maximal erforderliche Verzögerung – Aushandlung erzwingen	Durch Aktivieren von *Aushandlung erzwingen* wird die „Maximal erforderliche Verzögerung“ zurückgesetzt und an die „Betriebsdauer bei schwacher Batterie“ angepasst. Die Netzwerkmanagement-Karte sendet ein aktualisiertes Statuspaket an alle registrierten PowerChute-Agenten. PowerChute vergleicht anschließend den im Paket enthaltenen Wert „Betriebsdauer bei schwacher Batterie“ mit der erforderlichen Gesamtabschaltzeit und erhöht den Wert „Maximal erforderliche Verzögerung“ entsprechend oder die registrierte Abschaltverzögerung für die Steckdosengruppe. PowerChute führt alle 30 Sekunden eine Überprüfung der verbleibenden Laufzeit durch, wobei die erforderliche PowerChute-Gesamtabschaltdauer mit dem Wert „Betriebsdauer bei schwacher Batterie“ der Netzwerkmanagement-Karte verglichen wird. Durch Auswahl von „Aushandlung erzwingen“ wird die Abschaltverzögerung aller Steckdosengruppen auf den Wert des Felds „Betriebsdauer bei schwacher Batterie“ zurückgesetzt. Die Ausführung von „Aushandlung erzwingen“ kann bis zu zehn Minuten in Anspruch nehmen, um den erforderlichen Wert aller auf der Netzwerkmanagement-Karte registrierten PowerChute-Clients zu berechnen. Weitere Informationen finden Sie unter „Verzögertes Abschalten und PowerChute Network Shutdown“ auf Seite 24.
Maximale ausgehandelte Verzögerung	Die maximale ausgehandelte Verzögerung ist die längste Abschaltverzögerung, die von einem unter den PowerChute Network Shutdown-Clients aufgeführten Servern zum sicheren Herunterfahren benötigt wird, wenn die USV einen regulären Shutdown initiiert. Diese Verzögerung wird jedes Mal berechnet, wenn die Verwaltungsschnittstelle der USV eingeschaltet oder zurückgesetzt wird.
Shutdown-Einstellungen bei Batteriebetrieb	Legt das Verhalten der USV nach einem Shutdown fest: • Neu starten, wenn Stromversorgung wiederhergestellt ist – Bei wiederhergestellter Netzstromversorgung wird die USV neu gestartet. • Abschalten und abgeschaltet bleiben – Die USV bleibt selbst nach Wiederherstellung der Netzstromversorgung abgeschaltet.
Benutzername	Geben Sie den Benutzernamen für PowerChute Ein.
Authentication Phrase	Dieser Kennwortsatz dient zur Authentifizierung zwischen PowerChute und der Netzwerkmanagement-Karte. Der Kennwortsatz ist standardmäßig leer und muss eingerichtet werden, bevor Sie PowerChute aktivieren können.
PCNS Kommunikationsprotokolle	Wählen Sie das Kommunikationsprotokoll aus, um mit PowerChute zu kommunizieren: HTTPS oder HTTP.

Gesteuertes vorzeitiges Herunterfahren und Ende des Herunterfahrens.

Diese Optionen sind nicht bei allen USV-Geräten verfügbar.

Mit den Optionen unter „Gesteuertes vorzeitiges Herunterfahren“ können Sie im Batteriebetrieb laufende USV-Geräte herunterfahren, wenn EINE der folgenden von Ihnen festgelegte Bedingungen erfüllt ist:

- Wenn die Batteriebetriebsdauer eine bestimmte Minutenzahl überschreitet
- Wenn die verbleibende Laufzeit der USV weniger als eine bestimmte Minutenzahl beträgt (die Laufzeit beschreibt, wie lange die USV die angeschlossene Last mit Batteriestrom versorgen kann).
- Wenn die Batterieladung unter einem festgelegten Prozentsatz der Gesamtkapazität liegt.
- Wenn die Last am USV-Ausgang einen bestimmten Prozentsatz unterschreitet.

Mit **Nach Wiederherstellen der Stromversorgung ausgeschaltet bleiben** können Sie auch festlegen, ob die USV nach Wiederherstellung der Netzstromversorgung erneut eingeschaltet werden soll.

Mit den Optionen **Ende des Herunterfahrens** können Sie eine Bedingung und eine Verzögerungszeit einstellen, nach der sich eine USV nach Wiederherstellung der Netzstromversorgung wieder einschaltet. In Abhängigkeit des USV-Modells können Sie eine **Minimale Batteriekapazität** oder **Minimale Laufzeit für Neustart** einstellen, bevor sich die USV wieder einschaltet.

Verzögertes Abschalten und PowerChute Network Shutdown.

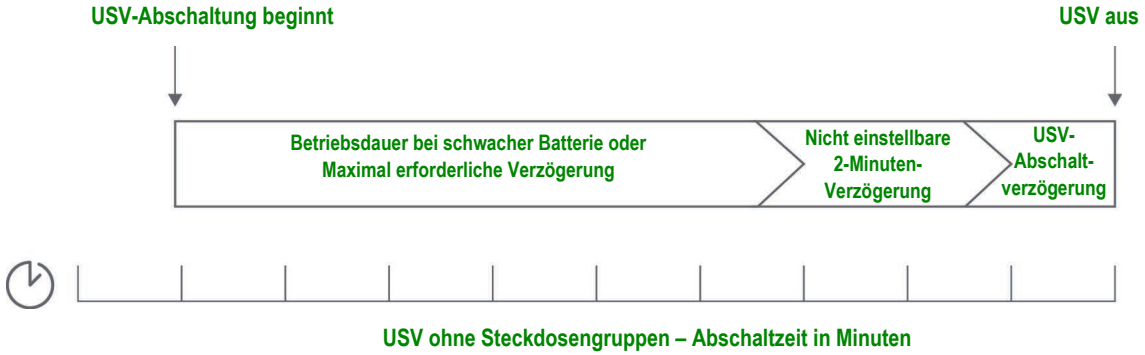
Im nachfolgenden Abschnitt wird erläutert, wie sich die Werte „Betriebsdauer bei schwacher Batterie“, „Maximal erforderliche Verzögerung“ und „Steckdosengruppen-Abschaltverzögerungen“ auf die PowerChute-Abschaltsequenz auswirken.

Weitere Informationen zu den PowerChute-Abschaltsequenzen finden Sie im *PowerChute Network Shutdown-Benutzerhandbuch*.

Bei beiden USV-Typen (mit und ohne Steckdosengruppen) handelt die Netzwerkmanagement-Karte die Abschaltzeit mit PowerChute Network Shutdown wie folgt aus:

USV ohne Steckdosengruppen

Bei einer USV OHNE Steckdosengruppen entspricht die USV-Abschaltzeit dem größeren der beiden Werte **Maximal erforderliche Verzögerung** und **Betriebsdauer bei schwacher Batterie** am Bildschirm **Abschaltung** der Netzwerkmanagement-Karte, zuzüglich einer nicht einstellbaren Verzögerung von 2 Minuten zuzüglich der Abschaltverzögerung für die USV.



Hinweise:

•Wird die Abschaltung durch einen niedrigen Batteriestand ausgelöst, hat der Wert „Betriebsdauer bei schwacher Batterie“ gegenüber dem Wert „Maximal erforderliche Verzögerung“ Vorrang.

Hinweise:

Weitere Informationen zu den PowerChute-Abschaltsequenzen finden Sie unter „*Beispielhafte Abschaltszenarien*“ im **PowerChute Network Shutdown-Benutzerhandbuch auf der APC-Website**.

Beim Vergleich der erforderlichen PowerChute-Abschaltzeit und der maximal erforderlichen Verzögerung/Steckdosengruppen-Abschaltverzögerung der Netzwerkmanagement-Karte wird der größere Wert herangezogen. Wenn beispielsweise die Befehlszeilenabschaltzeit des PowerChute-Clients auf 8 Minuten eingestellt ist, der Wert „Betriebsdauer bei schwacher Batterie“ der USV jedoch 10 Minuten beträgt, zieht die Netzwerkmanagement-Karte den größeren Wert von 10 Minuten für die „Maximal erforderliche Verzögerung“ heran.

Bei der erzwungenen Aushandlung führt die Netzwerkmanagement-Karte eine Abfrage der PowerChute-Clients durch, um die erforderliche Abschaltzeit zu erlangen. Demzufolge kann die Aktualisierung der Werte „Maximal erforderliche Verzögerung/Steckdosengruppen-Abschaltverzögerung“ bis zu zehn Minuten in Anspruch nehmen.

PowerChute ändert niemals den NMC-Wert im Feld **Betriebsdauer bei schwacher Batterie**.

Bei PowerChute Network Shutdown v3.x oder höher verwendet die Netzwerkmanagement-Karte niemals den Wert **Maximal erforderliche Verzögerung** für USVs mit Steckdosengruppen.

Planung für das Herunterfahren

Pfad: Konfiguration > Planung

Die folgenden Optionen sind nur für unterstützte Einphasen-Easy-UPS-Geräte mit installierter AP9544-Karte relevant.

FFür den Zugriff auf diesen Bildschirm ist eine Lizenz erforderlich. Siehe „Lizenz“.

Hinweis: Erstellen Sie keine sich überschneidenden Abschaltzeitpläne. Ein Beispiel für einen sich überschneidenden Abschaltzeitplan ist eine wöchentliche Abschaltung, eingestellt auf 20:00 - 21:00 Uhr und eine einmalige Abschaltung, eingestellt auf 20:10 - 20:30 Uhr. Sich überschneidende Abschaltzeitpläne führen zu unbekanntem und ungetestetem Verhalten.

Für die USV

Sie können das Herunterfahren eines USV-Geräts unter **USV** planen.

Alle konfigurierten Abschaltpläne werden oben auf dem Bildschirm angezeigt, wenn Sie die **USV** auswählen, und geben unter anderem an, ob diese aktuell aktiviert oder deaktiviert sind.

Bearbeiten, Aktivieren, Deaktivieren oder Löschen eines geplanten Herunterfahrens. Klicken Sie auf den Planungsnamen in der Liste der Planungen im oberen Bereich des Bildschirms **USV**. Dadurch werden die vollständigen Details angezeigt, wo Sie die Parameter bearbeiten können. Hierzu gehört auch die zeitweilige Deaktivierung, indem Sie das Kontrollkästchen **Aktivieren** deaktivieren, oder die dauerhafte Löschung.

Erstellen eines Plans zum Herunterfahren für eine USV.

1. Wählen Sie unter **Planung** die Option **UPS** aus.
2. Wählen Sie über die Optionsschaltflächen die Art des Herunterfahrens, die Sie planen möchten, also **Einmal herunterfahren**, **Täglich herunterfahren** oder **Wöchentlich herunterfahren**, und klicken Sie auf die Schaltfläche **Weiter**.
3. Um einen Zeitplan vorübergehend zu deaktivieren, entfernen Sie das Häkchen aus dem Kontrollkästchen **Aktivieren**.
4. Geben Sie einen Namen sowie Planungsdatum und -zeit an.
   Geben Sie das Intervall für das wöchentliche Herunterfahren mithilfe der Dropdown-Liste an.
5. Geben Sie an, ob das Gerät nach dem Herunterfahren wieder eingeschaltet werden soll:

Wieder einschalten: Legen Sie fest, ob sich die USV an einem bestimmten Tag zu einer bestimmten Uhrzeit einschalten soll, oder wählen Sie **Nie** (die USV muss dann manuell eingeschaltet werden) bzw. **Sofort** (Die USV schaltet sich nach einer Wartezeit von 6 Minuten ein).

Signal an PowerChute Network Shutdown Clients: Geben Sie an, ob PowerChute-Clients eine Meldung erhalten sollen (siehe „PowerChute Network Shutdown-Clients“).

Diese Option ermöglicht die Verwendung des Dienstprogramms PowerChute Network Shutdown, mit dem Sie bis zu 50 im Netzwerk befindliche Server herunterfahren können, auf denen die Client-Version des Dienstprogramms läuft.

PowerChute Network Shutdown-Clients

Pfad: USV > Konfiguration > PowerChute

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

Die Befehlsfolge für Dreiphasen-Easy-UPS-Geräte ist **Konfiguration > PowerChute > PowerChute®**

PowerChute Network Shutdown ermöglicht das Herunterfahren Ihrer UPS-Geräte per Fernzugriff.

Sie können einen PowerChute Network Shutdown-Client in Ihrem Netzwerk installieren; er wird dann automatisch dieser Liste hinzugefügt. Wenn Sie einen PowerChute Network Shutdown-Client deinstallieren, wird er automatisch entfernt.

Klicken Sie auf **Client hinzufügen**, um die IP-Adresse eines neuen PowerChute Network Shutdown-Clients einzugeben. Zum Löschen eines Clients klicken Sie auf die IP-Adresse des Clients in der Liste und dann auf **Client löschen**. Sie können die IP-Adressen von bis zu 50 Clients in die Liste aufnehmen.

Bei Steckdosengruppen müssen Sie außerdem festlegen, welche Steckdosengruppe den PowerChute-Client mit Strom versorgt.

HINWEIS: PowerChute kann sich nicht mit der Netzwerkmanagement-Karte verbinden, wenn HTTP auf der Netzwerkmanagement-Karte deaktiviert ist. Beziehen Sie sich auf „Bildschirm für Webzugriff“, um HTTP oder HTTPS zu aktivieren.

Menü „Sicherheit“

Bildschirm „Sitzungsverwaltung“

Pfad: Konfiguration > Sicherheit > Sitzungsverwaltung

Ist die Option **Gleichzeitige Anmeldung zulassen** aktiviert, können sich zwei oder mehr Benutzer gleichzeitig anmelden. Jeder Benutzer besitzt gleiche Zugriffsrechte und jede Schnittstelle (HTTP, FTP, Telnet-Konsole, serielle Konsole (CLI) etc.) zählt als angemeldeter Benutzer. Die Option **Gleichzeitige Anmeldung zulassen** erlaubt die gleichzeitige Anmeldung von maximal acht Benutzern über die Weboberfläche, fünf Benutzern über die Befehlszeile und einem Benutzer über die serielle Konsole.

Remote-Authentifizierungsüberschreibung: Die Netzwerkmanagement-Karte unterstützt die Radius-Speicherung von Kennwörtern auf einem Server. Wenn Sie jedoch 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. Siehe auch „Lokale Benutzer“ und „Authentifizierung von Remote-Benutzern“.

Ping-Antwort

Pfad: Konfiguration > Sicherheit > Ping-Antwort

Markieren Sie das Kontrollkästchen **IPv4 Ping-Antwort**, um zuzulassen, dass die Netzwerkmanagement-Karte 3 auf Ping-Anfragen aus dem Netzwerk antwortet. Dies gilt nicht für IPv6.

Lokale Benutzer

Verwenden Sie diese Menüoptionen, um den Zugriff und individuelle Einstellungen (wie das angezeigte Datumsformat) für die Benutzerschnittstellen anzuzeigen bzw. einzurichten. Dies gilt für Benutzer, die durch ihren Anmeldenamen definiert werden. Dies gilt nicht für IPv6.

Pfad: Konfiguration > Sicherheit > Lokale Benutzer > Verwaltung

Einrichten von Zugriffsrechten. Mit dieser Option kann ein Administrator oder Superuser den für Benutzer zulässigen Zugriff auf die Benutzeroberfläche auflisten und konfigurieren. Klicken Sie auf den Namens-Link, um Details anzuzeigen und einen Benutzer zu bearbeiten oder zu löschen.

Klicken Sie auf **Benutzer hinzufügen**, um einen Benutzer hinzuzufügen. Auf dem anschließend angezeigten Bildschirm **Benutzerkonfiguration** können Sie einen Benutzer hinzufügen und den Zugriff durch Abwählen des Kontrollkästchens **Zugriff** verweigern. Die maximale Länge für Name und Kennwort beträgt 64 Byte (bei Multibyte-Zeichen entsprechend weniger). Sie müssen ein Kennwort eingeben.

Werte über 64 Byte bei Name und Kennwort werden unter Umständen abgeschnitten!
Erstellen Sie ein Passwort bestehend aus Groß- und Kleinschreibung sowie Zahlen und Sonderzeichen.
Passwörter können nicht länger als 64 ASCII-Zeichen sein.

Verwenden Sie **Zeitüberschreitung bei Sitzung**, um die Zeit zu konfigurieren, die diese Benutzeroberfläche wartet, bis der Benutzer abgemeldet wird (standardmäßig drei Minuten). Wenn Sie diesen Wert ändern, müssen Sie sich abmelden, damit die Änderung wirksam wird.

Serielle Remote-Authentifizierungsüberschreibung: Durch Auswahl dieser Option können Sie RADIUS mithilfe der seriellen Konsolenverbindung (CLI) umgehen. Dieser Bildschirm aktiviert die Option für den ausgewählten Benutzer, doch sie muss auch global über den Bildschirm „Sitzungsverwaltung“ aktiviert werden, um zu funktionieren.

Siehe auch „Konfiguration > Sicherheit > Lokale Benutzer > Standardeinstellungen“ weiter unten.
Hintergrundinformationen zu Konten finden Sie unter „Arten von Benutzerkonten“.

BenutzervoreinstellungenAktivieren Sie das Kontrollkästchen **Ereignisprotokoll-Farbcodierung**, um die farbliche Kodierung der im Ereignisprotokoll erfassten Alarmtexte zu aktivieren. (Einträge zu Systemereignissen und Konfigurationsänderungen behalten immer dieselbe Farbe.)

Textfarbe	Schweregrad des Alarms
Rot	**Kritisch**: Es liegt ein kritischer Alarm vor, der ein sofortiges Eingreifen erfordert.
Orange	**Warnung**: Es liegt ein Alarm vor, dem genauer nachgegangen werden muss und der zu einer Gefahr für Daten oder Hardware werden könnte, wenn seine Ursache nicht behoben wird.

Textfarbe	Schweregrad des Alarms
Grün	**Alarm gelöscht**: Der Zustand, der zur Auslösung des Alarms geführt hat, besteht nicht mehr.
Schwarz	**Normal**: Keine Alarme vorhanden. Die Netzwerkmanagement-Karte und alle angeschlossenen Geräte funktionieren normal.
Blau	**Zur Information**: Ein informativer Alarm. Die Netzwerkmanagement-Karte und alle angeschlossenen Geräte funktionieren normal.

Protokollformat exportieren: Exportierte Protokolldateien können im CSV-Format (kommagetrennte Werte) oder als Registerkarten exportiert werden. Siehe „Anzeigen des Ereignisprotokolls“.

Wählen Sie die Temperaturskala für Messungen in dieser Benutzeroberfläche aus. **USA-spezifisch** entspricht Fahrenheit und **Metrisch** entspricht Celsius.

Sie können die Standardsprache für die Benutzeroberfläche über das Feld **Sprache** ändern. Diese Einstellung kann auch bei der Anmeldung vorgenommen werden.

Sie haben auch die Möglichkeit, für E-Mail-Empfänger und SNMP-Trap-Adressaten unterschiedliche Sprachen einzustellen. Siehe „E-Mail-Empfänger“ und „Trap-Empfänger“.

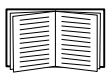
Pfad: Konfiguration > Sicherheit > Lokale Benutzer > Standardeinstellungen

Durch das Einrichten von Standardeinstellungen können Benutzer schneller hinzugefügt werden. Verwenden Sie diese Option, um Standardeinstellungen für die zahlreichen Optionen im Bildschirm „Verwaltung“ einzurichten (siehe „Konfiguration > Sicherheit > Lokale Benutzer > Verwaltung“ weiter oben).

Authentifizierung von Remote-Benutzern

Pfad: Konfiguration > Sicherheit > Remote-Benutzer > Authentifizierung

Authentifizierung. Legen Sie fest, wie Benutzer bei der Anmeldung authentifiziert werden sollen.



Informationen zur lokalen Authentifizierung (nicht mithilfe der zentralisierten Authentifizierung eines RADIUS-Servers) finden Sie im *Sicherheitshandbuch* auf der APC-Website.

Die folgenden Authentifizierungs- und Autorisierungsfunktionen von RADIUS (Remote Authentication Dial-In User Service) werden unterstützt:

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

Wählen Sie eine der folgenden Möglichkeiten:

- **Nur lokale Authentifizierung**: RADIUS ist deaktiviert. Siehe „Lokale Benutzer“.
- **RADIUS, dann lokale Authentifizierung**: Beides ist aktiviert. Die Authentifizierung wird zuerst beim RADIUS-Server angefordert. Wenn der RADIUS-Server nicht reagiert, wird die lokale Authentifizierung verwendet.
- **Nur RADIUS**: Keine lokale Authentifizierung.

Wenn **Nur RADIUS** ausgewählt ist und wenn der RADIUS-Server nicht verfügbar ist, nicht richtig identifiziert wurde oder falsch konfiguriert ist, steht der Fernzugriff nicht zur Verfügung, unabhängig vom Benutzerkontotyp. Um wieder Zugriff zu erhalten, müssen Sie über die serielle Schnittstelle eine Befehlszeile öffnen und die **Zugriffseinstellung** zu **local** oder **radiusLocal** ändern.

Mit dem folgenden Befehl können Sie die Zugriffseinstellung beispielsweise zu **local** ändern:

```
radius -a local
```

Siehe auch „RADIUS-Bildschirm“ weiter unten sowie „Konfigurieren des RADIUS-Servers“.

RADIUS-Bildschirm

Pfad: Konfiguration > Sicherheit > Remote-Benutzer > RADIUS

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

Sie können einen RADIUS-Server zur Authentifizierung von Remote-Benutzern verwenden. Verwenden Sie diese Option für Folgendes:

- Die für die Netzwerkmanagement-Karte verfügbaren RADIUS-Server (maximal zwei) und ihre jeweiligen Timeout-Werte anzeigen.
- Die Authentifizierungswerte für einen neuen oder bestehenden RADIUS-Server durch Klicken auf einen **RADIUS-Server**-Link konfigurieren.

RADIUS-Einstellung	Beschreibung
RADIUS-Server	Der Name oder die IP-Adresse des Servers (IPv4 oder IPv6). **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.
Geheimnis	Der vom RADIUS-Server und der Netzwerkmanagement-Karte verwendete geheime Schlüssel.
Zeitlimit bis zur Antwort	Die Zeit in Sekunden, die die Netzwerkmanagement-Karte auf eine Antwort vom RADIUS-Server wartet.
Testeinstellungen	Geben Sie den Benutzernamen und das Kennwort des Administrators ein, um den Pfad zu dem von Ihnen konfigurierten RADIUS-Server zu testen.
Test überspringen und übernehmen	Hiermit wird der Test des Pfads zum RADIUS-Server unterlassen.

Siehe auch „Authentifizierung von Remote-Benutzern“ weiter oben sowie „Konfigurieren des RADIUS-Servers“ weiter unten.

Konfigurieren des RADIUS-Servers

Das Konfigurationsverfahren im Überblick.

Sie müssen Ihren RADIUS-Server konfigurieren, um mit der Netzwerkmanagement-Karte zusammenarbeiten zu können (siehe dazu die nachfolgenden Schritte).

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

1. Fügen Sie die IP-Adresse der Netzwerkmanagement-Karte der Client-Liste des RADIUS-Servers (Datei) hinzu.
2. Zu jedem Benutzer muss ein Diensttyp-Attribut konfiguriert werden, sofern keine Vendor Specific Attributes (VSAs) definiert sind. Wenn keine Diensttyp-Attribute konfiguriert sind, haben die Benutzer schreibgeschützten Zugriff (nur über die Benutzeroberfläche).

Informationen zur Radius-Benutzerdatei finden Sie in der Dokumentation zum RADIUS-Server. Ein Beispiel für eine Radius-Benutzerdatei finden Sie im ***Sicherheitshandbuch***.

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

Konfigurieren eines RADIUS-Servers unter UNIX® mit Shadow-Kennwörtern.

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

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

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

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

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

Unterstützte RADIUS-Server.

FreeRADIUS v1.x und v2.x sowie Microsoft Server 2008 und 2012 Netzwerkrichtlinienserver (NPS) werden unterstützt. Andere allgemein verfügbare RADIUS-Anwendungen könnten funktionieren, wurden aber nicht vollständig getestet.

Firewall-Bildschirm

Pfad: Konfiguration > Sicherheit > Firewall > Konfiguration

Aktivieren oder deaktivieren der Firewall-Funktion. Die konfigurierte Richtlinie wird standardmäßig aufgelistet. Aktivieren Sie das Kontrollkästchen **Aktivieren**, um die Firewall zu aktivieren. Das Kontrollkästchen ist standardmäßig deaktiviert.

- Klicken Sie auf **Übernehmen**, um die Aktivierung der ausgewählten Firewall-Richtlinie zu bestätigen. Die Seite **Firewall-Bestätigung** wird geöffnet.
  - Die Bestätigungsseite empfiehlt, die Firewall vor der Aktivierung zu testen. Dies ist nicht zwingend erforderlich.
  - Der erste Hyperlink verweist auf die Seite „Firewall-Richtlinie“.
  - Der zweite Hyperlink verweist auf die Seite „Firewall-Test“.

  - Klicken Sie auf **Übernehmen**, um die Firewall zu aktivieren und zur Seite „Konfiguration“ zurückzukehren.
  - Klicken Sie auf **Abbrechen**, um zur Seite „Konfiguration“ zurückzukehren, ohne die Firewall zu aktivieren.
- Klicken Sie auf **Abbrechen**: Keine neue Auswahl wird aktiviert. Sie bleiben auf der Konfigurationsseite.

Pfad: Konfiguration > Sicherheit > Firewall > Aktive Richtlinie

Wählen Sie eine aktive Richtlinie von der Dropdown-Liste „Aktive Richtlinien“ aus und überprüfen Sie die Validität dieser Richtlinie. Standardmäßig wird die momentan aktive Richtlinie angezeigt. Sie können eine andere aus der Liste auswählen.

- Klicken Sie auf **Übernehmen**, um Ihre Änderungen anzuwenden. Wenn eine andere Firewall ausgewählt und aktiviert wurde, ist die Änderung umgehend wirksam. Wenn eine neu konfigurierte Firewall-Richtlinie ausgewählt wurde, wird empfohlen, die neue Firewall vor der Aktivierung zu testen. (Siehe Konfiguration oben.)
- Klicken Sie auf **Abbrechen**, um die ursprünglich aktive Richtlinie wiederherzustellen und auf der Seite „Aktive Richtlinien“ zu bleiben.

Pfad: Konfiguration > Sicherheit > Firewall > Aktive Regeln

Wenn eine Firewall aktiviert ist, werden auf dieser schreibgeschützten Seite die einzelnen Regeln aufgelistet, die von einer aktuellen aktiven Richtlinie umgesetzt werden. Beschreibungen der Felder (Priorität, Ziel, Quelle, Protokoll, Aktion und Anmeldung) finden Sie im Abschnitt **Richtlinien erstellen/bearbeiten**.

Pfad: Konfiguration > Sicherheit > Firewall > Richtlinien erstellen/bearbeiten

Erstellen Sie eine neue Richtlinie oder löschen bzw. bearbeiten Sie eine bestehende Richtlinie:

Hinweis: Eine aktive aktivierte Firewall-Richtlinie kann zwar nicht gelöscht werden, aber bearbeitet werden. Dies wird jedoch nicht empfohlen, da Änderungen unmittelbar wirksam werden. Stattdessen sollten Sie die Firewall deaktivieren, die Richtlinie bearbeiten, testen und danach wieder aktivieren.

Erstellen einer neuen Richtlinie: Klicken Sie auf **Richtlinie hinzufügen** und geben Sie den Dateinamen für die neue Firewall-Datei ein. Der Dateiname sollte die Dateierweiterung „.fwl“ haben. Wenn keine Dateierweiterung eingegeben wird, wird „.fwl“ automatisch an den Namen angehängt.

- Klicken Sie auf **Übernehmen**: Wenn der Dateiname zulässig ist, wird die leere Firewall-Richtlinien-Datei erstellt. Die Datei befindet sich dann im Ordner „/fwl“ mit den anderen Richtlinien auf dem System.
- Klicken Sie auf **Abbrechen**, um keine neue Firewall-Datei zu erstellen und zur vorherigen Seite zurückzukehren.

Bearbeiten einer bestehenden Richtlinie:

Wählen Sie **Richtlinie bearbeiten** aus, um zur Bearbeitungsseite zu gelangen. Sie können eine inaktive Firewall-Richtlinie bearbeiten.

Warnung: Wenn Sie versuchen, die aktive aktivierte Richtlinie zu bearbeiten, wird eine Warnung angezeigt: **„Wenn Sie die aktive Firewall-Richtlinie bearbeiten, werden alle vorgenommenen Änderungen unmittelbar übernommen. Es wird empfohlen, die Firewall zu deaktivieren und die Richtlinie vor der Aktivierung zu testen.“**

  - Klicken Sie auf **Übernehmen**, um die Warnung zu schließen und zur Seite „Richtlinie bearbeiten“ zurückzukehren.
  - Klicken Sie auf **Abbrechen**, um die Warnung zu schließen und zur Seite „Richtlinie erstellen/bearbeiten“ zurückzukehren.

1. Wählen Sie aus der Dropdown-Liste **Richtlinienname** die zu bearbeitende Richtlinie aus und klicken Sie auf **Richtlinie bearbeiten**.
2. Klicken Sie auf **Regel hinzufügen** oder wählen Sie die **Priorität** einer bestehenden Regel aus, um zur Seite **Regel bearbeiten** zu wechseln. Auf dieser Seite können Sie die Regeleinstellungen ändern oder die ausgewählte Regel löschen.

Einstellung	Beschreibung
Priorität	Wenn es einen Konflikt zwischen zwei Regeln gibt, wird die Regel mit der höheren Priorität angewendet. Die Priorität muss zwischen 1 und 250 liegen.
Typ	**host**: In das Feld „IP/any“ geben Sie eine einzelne IP-Adresse ein. **subnet**: In das Feld „IP/any“ geben Sie eine einzelne Subnetz-Adresse ein. **range**: In das Feld „IP/any“ geben Sie eine Reihe von IP-Adressen ein.
IP/any	Legen Sie die IP-Adresse oder die Reihe von IP-Adressen fest, für die diese Regel angewendet wird, oder wählen Sie eine der folgenden Optionen aus: • **any**: Die Regel wird unabhängig von der IP-Adresse angewendet. • **anyipv4**: Die Regel wird auf alle IPv4-Adressen angewendet. • **anyipv6**: Die Regel wird auf alle IPv6-Adressen angewendet.
Port	Geben Sie einen Port an, für den die Regel angewendet werden soll. • **None**: Die Regel wird für alle Ports angewendet. • **Common Configured ports**: Wählen Sie einen Standardport aus. • **Other**: Legen Sie eine nicht standardmäßige Portnummer fest.
Protokoll	Legen Sie fest, auf welches Protokoll die Regel angewendet werden soll. • **any**: Alle Protokolle. • **tcp**: Wird verwendet für zuverlässige Datenübertragung zwischen Anwendungen. • **udp**: Alternative zu TCP für schnellere Datenübertragung bei niedrigerer Bandbreite. UDP hat weniger Verzögerungen, doch TCP ist zuverlässiger. • **icmp**: Wird verwendet, um Fehler zur Fehlerbehebung zu melden. • **icmpv6**: Wird verwendet, um Fehler zur Fehlerbehebung auf Anwendungen mit IPv6 zu melden.
Vorgang	**allow**: Erlaubt Pakete, die diese Regel erfüllen. **discard**: Lehnt Pakete ab, die diese Regel erfüllen.
Protokoll	Wenn diese Regel auf ein Paket angewendet wird, wird unabhängig davon, ob das Paket abgelehnt oder erlaubt wird, ein Eintrag zum Firewall-Protokoll hinzugefügt. Siehe „Firewall-Protokoll“ auf Seite 75.

Es wird empfohlen, dass Sie eine der folgenden Regeln als Regel mit der geringsten Priorität zu Ihrer Firewall-Richtlinie hinzufügen:

- Fügen Sie folgendes hinzu, wenn Sie die Firewall als Whitelist verwenden möchten:
  `250 Dest any / Source any / protocol any / discard`
- Fügen Sie folgendes hinzu, wenn Sie die Firewall als Blacklist verwenden möchten:
  `250 Dest any / Source any / protocol any / allow`

Löschen einer Richtlinie:

Wählen Sie **Richtlinie löschen** aus, um die Seite „Löschung bestätigen“ zu öffnen.

Klicken Sie zum Bestätigen auf **Übernehmen** und die ausgewählte Firewall-Datei wird aus dem Dateisystem entfernt.

Pfad: Konfiguration > Sicherheit > Firewall > Richtlinie laden

Laden Sie eine Richtlinie (mit dem Suffix „.fwl“) von einer externen Quelle auf dieses Gerät hoch.

Pfad: Konfiguration > Sicherheit > Firewall > Test

Erzwingen Sie vorübergehend die Regeln einer ausgewählten Richtlinie für einen von Ihnen festgelegten Zeitraum.

802.1X Sicherheitskonfiguration

Pfad: Konfiguration > Sicherheit > 802.1X Security

Die NMC übernimmt die Rolle eines Supplicants in einer EAPoL-Architektur (Extensible Authentication Protocol over LAN), die in der IEEE 802.1X-Port-basierten Netzwerk-Zugangskontrolle verwendet wird.Die NMC unterstützt EAP-TLS als Authentifizierungsmethode, die erfordert, dass Sie 3 kundenseitige Zertifikate hochladen.Der Private Key wird verschlüsselt gespeichert.Sie müssen eine gültige Passphrase zur Verfügung stellen, um den 802.1X-Sicherheitszugriff aktivieren zu können.

HINWEIS: Die NMC unterstützt nur die EAP-TLS-Authentifizierungsmethode.

Das Web-UI bietet folgende Optionen für die EAPoL-Konfiguration:

Einstellung	Beschreibung
EAPoL-Zugang	Wird verwendet, um 802.1X Sicherheitszugriff zu aktivieren oder zu deaktivieren. **HINWEIS:** Der Sicherheitszugriff von 802.1X ist standardmäßig deaktiviert.Sie können den Zugriff nur dann aktivieren, wenn gültige Zertifikate und eine gültige Passphrase für den Private Key zur Verfügung gestellt werden.
Supplicant-Kennung	Ermöglicht es Ihnen, Ihre eigene Supplicant-Kennung (bis zu 32 Zeichen inklusive Leerzeichen) festzulegen. **HINWEIS:** Standardmäßig wird die Supplicant-Kennung auf „NMC-Supplicantxx:xx:xx:xx:xx“ gesetzt, wobei sechs Oktette von „xx“ die MAC-ID der NMC sind.
CA-Zertifikat	Ein CA-Root-Zertifikat hochladen/ersetzen oder entfernen.Die unterstützten Dateiformate sind PEM (Privacy Enhanced Mail) oder das DER (Distinguished Encoding Rules)-Format mit erlaubter Dateierweiterung .pem,. PEM, .der oder .DER.
Private-Key-Zertifikat	Einen verschlüsselten Private Key hochladen/ersetzen oder entfernen.Die unterstützten Dateiformate sind PEM (Privacy Enhanced Mail) oder das DER (Distinguished Encoding Rules)-Format mit erlaubten Dateierweiterungen .key oder .KEY. **HINWEIS:** Unverschlüsselte Private Keys werden nicht akzeptiert.
Private-Key-Passphrase	Geben Sie die Passphrase zur Entschlüsselung des verschlüsselten Private Key an.Bis zu 64 Zeichen inklusive Leerzeichen zulässig.
Benutzer-/öffentliches Zertifikat	Ein Benutzer-/öffentliches Zertifikat hochladen/ersetzen oder entfernen.Die unterstützten Dateiformate sind PEM (Privacy Enhanced Mail) oder das DER (Distinguished Encoding Rules)-Format mit erlaubten Dateierweiterungen .pem,. PEM, .der oder .DER.

Konfiguration Ihrer Einstellungen: 2

Mithilfe der Optionen im Menü „Konfiguration“ können Sie die grundlegenden Werte für den Betrieb Ihrer USV und der Netzwerkmanagement-Karte festlegen.

Siehe dazu die folgenden Abschnitte sowie „Konfiguration Ihrer Einstellungen: 1“.

- Netzwerk im Menü „Konfiguration“
- Menü „Notification“
- Menü „Allgemein“
- Menü „Konfigurationsprotokolle“

HINWEIS: Sie können einige der Konfigurationseinstellungen über den Bildschirm für die Konfigurationsübersicht (**Konfiguration > Netzwerk > Zusammenfassung**) einsehen.

Netzwerk im Menü „Konfiguration“

Bildschirm „TCP/IP-Einstellungen für IPv4“

Befehlsfolge: Konfiguration > Netzwerk > TCP/IP > IPv4-Einstellungen

Diese Option zeigt die aktuelle IPv4-Adresse, die Subnetzmaske, das Standardgateway, die MAC-Adresse und den Boot-Modus der Netzwerkmanagement-Karte an. Im unteren Bereich des Bildschirms können Sie alle diese Einstellungen konfigurieren. Sie können dort auch IPv4 abschalten.

Weitere Einzelheiten über DHCP und die DHCP-Optionen finden Sie in RFC2131 und RFC2132.

Option	Beschreibung
Manuell	Geben Sie hier Ihre IPv4-Adresse, die Subnetzmaske und das Standardgateway an.
BOOTP*	Das Gerät fordert in Intervallen von 32 Sekunden von einem vorhandenen BOOTP-Server eine Netzwerkzuweisung an: • Wenn es eine gültige Antwort erhält, startet es die Netzwerkdienste. • Wenn bereits konfigurierte Netzwerkeinstellungen existieren und das Gerät auf fünf Anfragen (die erste Anfrage und vier Neuversuche) keine gültige Antwort erhält, verwendet es standardmäßig diese bereits konfigurierten Einstellungen. Auf diese Weise bleibt es auch dann weiterhin erreichbar, wenn kein BOOTP-Server mehr erreichbar ist. • Wenn das Gerät einen BOOTP-Server findet, eine entsprechende Anfrage jedoch fehlschlägt oder zu lange unbeantwortet bleibt, unterlässt es eine erneute Anforderung von Netzwerkeinstellungen, bis es neu gestartet wird.
DHCP*	Das Gerät fordert in Intervallen von 32 Sekunden von einem vorhandenen DHCP-Server eine Netzwerkzuweisung an: • Wenn das Gerät einen DHCP-Server findet, eine entsprechende Anfrage jedoch fehlschlägt oder zu lange unbeantwortet bleibt, unterlässt es eine erneute Anforderung von Netzwerkeinstellungen, bis es neu gestartet wird. • Optional können Sie für das Gerät **Require vendor specific cookie to accept DHCP Address** einstellen, um die Zuteilung zu akzeptieren und die Netzwerkdienste zu starten. Siehe „Optionen in DHCP-Antworten“.

*** Vendor Class: APC**
Client-ID: Die MAC-Adresse des Geräts. Wenn Sie diesen Wert ändern, muss der neue Wert für das LAN eindeutig sein.
User Class: Der Name des Moduls der Anwendungs-Firmware (siehe „Dateiübertragungen“).

Bildschirm „TCP/IP-Einstellungen für IPv6“

Befehlsfolge: Konfiguration > Netzwerk > TCP/IP > IPv6-Einstellungen

Diese Option zeigt die aktuellen IPv6-Einstellungen der Netzwerkmanagement-Karte an. Im unteren Bereich des Bildschirms können Sie alle diese Einstellungen konfigurieren. Sie können dort auch IPv6 deaktivieren.

Sie können zwischen manueller und automatischer IP-Adressierung wählen. Beide Optionen können auch gleichzeitig verwendet werden. Aktivieren Sie das Kontrollkästchen für **Manuell** und geben Sie dann die **System-IPv6-Adresse** und das **Standardgateway** ein.

Aktivieren Sie das Kontrollkästchen **Automatische Konfiguration**, damit das System die Adressierungspräfixe vom Router (falls verfügbar) abrufen kann. Diese Präfixe werden verwendet, um die IPv6-Adressen automatisch zu konfigurieren.

Mögliche IPv6-Formate	Beschreibung
fe80:0000:0000:0000:0204:61ff:fe9d:f156	vollständige Form von IPv6
fe80:0:0:0:204:61ff:fe9d:f156	voranstehende Nullen entfallen
fe80:204:61ff:fe9d:f156	Zusammenfassung mehrerer Nullen zu: in der IPv6-Adresse
fe80:0000:0000:0000:0204:61ff:254.157.241.86	IPv4 in Dotted Quad-Notation am Ende
fe80:0:0:0:0204:61ff:254.157.241.86	führende Nullen entfallen, IPv4 in Dotted Quad-Notation am Ende
fe80:204:61ff:254.157.241.86	Dotted Quad-Notation am Ende, mehrere Nullen zusammengefasst
:1	localhost
fe80:	link-local-Präfix
2001:	globales Unicast-Präfix

Die Angaben für den **DHCPv6-Modus** finden Sie in der folgenden Tabelle.

DHCPv6-Modus für die IPv6-Konfiguration	
Option	**Beschreibung**
Router-gesteuert	Wenn dieses Kontrollkästchen aktiviert ist, wird DHCPv6 über das Flag **M** (Managed Address Configuration Flag) und das Flag **O** (Other Stateful Configuration Flag) gesteuert, die über IPv6 Router Advertisements empfangen werden. Wenn ein Router Advertisement empfangen wird, prüft die Netzwerkmanagement-Karte, ob das Flag „M“ oder das Flag „O“ gesetzt ist. Die Netzwerkmanagement-Karte interpretiert diese Flags wie folgt: • **Keines der beiden Flags ist gesetzt**: Dies bedeutet, dass dem lokalen Netzwerk die DHCPv6-Infrastruktur fehlt. Die Netzwerkmanagement-Karte verwendet Router Advertisements und manuell konfigurierte Einstellungen, um Adressen, die nicht „link-local“ sind, sowie weitere Einstellungen zu beziehen. • **„M“ oder „M“ und „O“ sind gesetzt**: In dieser Situation kommt es zu einer vollständigen DHCPv6-Adresskonfiguration. DHCPv6 wird verwendet, um Adressen UND weitere Konfigurationseinstellungen zu beziehen. Dieser Zustand wird als „DHCPv6 Stateful“ bezeichnet. Nachdem das Flag „M“ empfangen wurde, bleibt die DHCPv6-Adresskonfiguration wirksam bis die betreffende Schnittstelle geschlossen wird. Das gilt auch für den Fall, dass Router Advertisement-Pakete empfangen werden, in denen das Flag „M“ nicht gesetzt ist. Wenn zuerst das Flag „O“ und anschließend das Flag „M“ empfangen wird, führt die Netzwerkmanagement-Karte bei Erhalt des Flags „M“ die vollständige Adresskonfiguration durch. • **Nur das Flag „O“ ist gesetzt**: In dieser Situation sendet die Netzwerkmanagement-Karte ein DHCPv6 Info-Request-Paket. DHCPv6 wird zur Konfiguration der „anderweitigen“ Einstellungen (z. B. der Standorte von DNS-Servern) verwendet, NICHT jedoch zur Bereitstellung von Adressen. Dieser Zustand wird als „DHCPv6 Stateless“ bezeichnet.
Adresse und sonstige Informationen:	DHCPv6 wird verwendet, um Adressen UND weitere Konfigurationseinstellungen zu beziehen. Dieser Zustand wird als „DHCPv6 Stateful“ bezeichnet.
Nur Nicht-Adres-sinformationen:	DHCPv6 wird zur Konfiguration der „anderweitigen“ Einstellungen (z. B. der Standorte von DNS-Servern) verwendet, NICHT jedoch zur Bereitstellung von Adressen. Dieser Zustand wird als „DHCPv6 Stateless“ bezeichnet.
Never (Nie)	DHCPv6 wird NIEMALS für Konfigurationseinstellungen verwendet.

Optionen in DHCP-Antworten

Jede gültige DHCP-Antwort enthält Optionen, mit denen TCP/IP-Einstellungen an die Netzwerkmanagement-Karte übergeben werden, die diese zum Funktionieren in einem Netzwerk benötigt. Außerdem enthält jede Antwort weitere Informationen, die sich auf das Verhalten der Netzwerkmanagement-Karte auswirken. Siehe auch Knowledge Base-Artikel **FA156110**.

Herstellerspezifische Informationen (Option 43). Die Netzwerkmanagement-Karte verwendet diese Option in einer DHCP-Antwort, um festzustellen, ob die DHCP-Antwort gültig ist. Diese Option enthält das sogenannte APC-Cookie im Format TAG/LEN/DATA. Diese Option ist in der Grundeinstellung deaktiviert.

- **APC-Cookie. Tag 1, Len 4, Data „1APC“**

  Mit Option 43 wird der Netzwerkmanagement-Karte mitgeteilt, dass ein DHCP-Server zum Bedienen von Geräten konfiguriert wurde.

  Im Folgenden ist ein Beispiel für die Option „Herstellerspezifische Informationen“ im hexadezimalen Format dargestellt, die das APC-Cookie enthält:

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

TCP/IP-Einstellungen. Innerhalb einer gültigen DHCP-Antwort verwendet die Netzwerkmanagement-Karte die nachstehenden Optionen, um ihre TCP/IP-Einstellungen zu definieren. Alle diese Optionen mit Ausnahme der ersten sind in RFC2132 beschrieben.

- **IP-Adresse** (aus dem Feld **yiaddr** der DHCP-Antwort, beschrieben in RFC2131): Die IP-Adresse, die der DHCP-Server der Netzwerkmanagement-Karte zur Verfügung stellt.
- **Subnetzmaske** (Option 1): Der Wert der Subnetzmaske, der von der Netzwerkmanagement-Karte benötigt wird, um im Netzwerk zu funktionieren.
- **Router,** d. h. der Standardgateway (Option 3): Die Adresse des Standardgateways, die von der Netzwerkmanagement-Karte benötigt wird, um im Netzwerk zu funktionieren.
- **Zuteilungsdauer der IP-Adresse** (Option 51): Die Dauer der Zuteilung der IP-Adresse an die Netzwerkmanagement-Karte.
- **Erneuerungsdauer, T1** (Option 58): Wie lange die Netzwerkmanagement-Karte nach Zuteilung einer IP-Adresse warten muss, bevor sie eine Erneuerung dieser Zuteilung anfordern kann.
- **Neuanbindungsdauer, T2** (Option 59): Wie lange die Netzwerkmanagement-Karte nach Zuteilung einer IP-Adresse warten muss, bevor sie eine Neuanbindung dieser Zuteilung anfordern kann.

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

- **Network Time Protocol-Server** (Option 42): Bis zu zwei NTP-Server (primär und sekundär), die von der Netzwerkmanagement-Karte verwendet werden können.
- **Zeitunterschied** (Option 2): Der Zeitunterschied des Subnetzes der Netzwerkmanagement-Karte in Sekunden zur koordinierten Weltzeit „Coordinated Universal Time“ (UTC).
- **DNS-Server** (Option 6): Bis zu zwei Domain Name System-Server (DNS-Server) (primär und sekundär), die von der Netzwerkmanagement-Karte verwendet werden können.
- **Hostname** (Option 12): Der von der Netzwerkmanagement-Karte verwendete Hostname (Höchstlänge 32 Zeichen).
- **Domänenname** (Option 15): Der von der Netzwerkmanagement-Karte verwendete Domänenname (Höchstlänge 64 Zeichen).
- **Boot-Dateiname** (aus dem Feld **file** der DHCP-Antwort, beschrieben in RFC2131): Der vollständige Pfad zu einer herunterzuladenden Benutzerkonfigurationsdatei (INI-Datei). Das Feld **siaddr** in der DHCP-Antwort enthält die IP-Adresse des Servers, von dem die Netzwerkmanagement-Karte die INI-Datei herunterladen wird. Nach dem Herunterladen der INI-Datei verwendet die Netzwerkmanagement-Karte diese als Boot-Datei zum Neukonfigurieren ihrer Einstellungen.
- **Vollständig qualifizierter Domänenname** (FQDN, Option 81): Der vollständig qualifizierte Domänenname der Netzwerkmanagement-Karte.

Bildschirm „Anschlussgeschwindigkeit“

Befehlsfolge: Konfiguration > Netzwerk > Anschlussgeschwindigkeit

Mit der Einstellung „Anschlussgeschwindigkeit“ legen Sie die Datenübertragungsgeschwindigkeit des Ethernet-Netzwerk-Ports fest. Die aktuelle Einstellung wird unter **Current Speed** angezeigt.

Sie können die Einstellung ändern, indem Sie unter **Anschlussgeschwindigkeit** eine Optionsschaltfläche verwenden:

- Bei Verwendung der Option **Automatische Aushandlung** (die Voreinstellung) handeln Netzwerkgeräte eine möglichst hohe Übertragungsgeschwindigkeit aus; wenn jedoch die beiden am Datenaustausch beteiligten Geräte unterschiedliche Geschwindigkeiten unterstützen, wird die niedrigere Geschwindigkeit verwendet.
- Alternativ können Sie **10** MBit/s oder **100** MBit/s verwenden. Für beide gibt es folgende Optionen:
  - **halb-duplex** (Kommunikation nur in jeweils eine Richtung) oder
  - **voll-duplex** (gleichzeitige Kommunikation in beide Richtungen über denselben Kanal).

HINWEIS: Sie können die Port-Geschwindigkeit nur auf 1000 Mbit/s ändern, indem Sie die **Auto-Negotiation**-Taste wählen.

Bildschirm „DNS“

Befehlsfolge: Konfiguration > Netzwerk > DNS > Konfiguration

Die Werte unter **Domain Name System Status** geben den aktuellen Status und die aktuelle Konfiguration an.

Verwenden Sie die Optionen unter **Manuelle Domain Name System-Einstellungen**, um das Domain Name System (DNS) zu konfigurieren:

- Wenn Sie **Manuelle DNS-Einstellungen überschreiben** aktivieren, haben Konfigurationsdaten aus anderen Quellen wie DHCP Vorrang vor der manuellen Konfiguration.
- Geben Sie den **primären DNS-Server** und optional den **sekundären DNS-Server** mit den IPv4- oder IPv6-Adressen an. Damit die Netzwerkmanagement-Karte E-Mails senden kann, müssen Sie mindestens die IP-Adresse des primären DNS-Servers angeben.
  - Die Netzwerkmanagement-Karte wartet bis zu 15 Sekunden auf eine Antwort vom primären oder sekundären DNS-Server. Wenn die Netzwerkmanagement-Karte innerhalb dieser Wartezeit keine Antwort erhält, kann keine E-Mail gesendet werden. Daher sollten DNS-Server auf dem gleichen Segment wie die Netzwerkmanagement-Karte oder auf einem nahe gelegenen Segment laufen (nicht jedoch in einem Weitverkehrsnetz (WAN)).
  - Testen Sie die IP-Adressen der DNS-Server, nachdem Sie sie definiert haben (siehe Bildschirm „DNS testen“).
- **System Name Synchronization**: Wenn Sie diese Option aktivieren, wird der DNS-Hostname mit dem Systemnamen der Netzwerkmanagement-Karte synchronisiert. Klicken Sie auf den Link „Systemname“, um den Namen zu definieren.

  Wenn der DNS-Hostname mit dem Systemnamen der Netzwerkmanagement-Karte synchronisiert ist, ist der Systemname auf eine bestimmte Anzahl von Zeichen, basierend auf DNS RFC, beschränkt. Ist keine Synchronisierung erfolgt, ist der Systemname auf 255 Zeichen beschränkt.
- **Hostname**: Nachdem Sie hier einen Hostnamen und im Feld **Domain Name** einen Domänennamen konfiguriert haben, können Benutzer in alle Felder der Netzwerkmanagement-Karte, die Domänennamen verarbeiten können, einen Hostnamen eingeben (außer E-Mail-Adressen).
- **Domänenname (IPv4/IPv6)**: Für die Schnittstelle der Netzwerkmanagement-Karte müssen Sie hier lediglich den Domänennamen konfigurieren. In allen anderen Feldern dieser Benutzeroberfläche (mit Ausnahme von Feldern für E-Mail-Adressen), die Domänennamen verarbeiten können, fügt die Netzwerkmanagement-Karte diesen Domänennamen standardmäßig ein, wenn nur ein Hostname eingegeben wurde.
  - Wenn Sie die Ergänzung des eingegebenen Hostnamens durch Hinzufügen des Domänennamens aufheben möchten, setzen Sie das für den Domänennamen vorgesehene Feld auf seinen Standardwert, also auf `irgendeinedomaene.com` oder auf `0.0.0.0`.
  - Wenn Sie die Ergänzung eines *bestimmten* Hostnamens durch Hinzufügen des Domänennamens (z. B. beim Definieren eines Trap-Empfängers) aufheben möchten, geben Sie dazu einen nachgestellten Punkt ein. Die Netzwerkmanagement-Karte interpretiert einen Hostnamen mit nachgestelltem Punkt (z. B. `meinSnmpServer.`) als vollständigen Domänennamen und hängt dann keinen Domänennamen mehr an.
- **Domänenname (IPv6)**: Geben Sie hier den IPv6-Domänennamen an.

Bildschirm „DNS testen“

Befehlsfolge: Konfiguration > Netzwerk > DNS > Test

Verwenden Sie diese Option, um eine DNS-Abfrage zum Testen der Konfiguration Ihrer DNS-Server zu senden, indem Sie die IP-Adresse nachschlagen. Siehe Bildschirm „DNS“ zur Einrichtung Ihrer Server.

Im Feld **Letzte Abfrageantwort** können Sie sich das Ergebnis der Testabfrage ansehen.

- Wählen Sie als **Abfragetyp** die für DNS-Abfragen zu verwendende Methode aus (siehe Tabelle unten).
- Geben Sie als **Frage der Abfrage** entsprechend der Erklärung in der Tabelle den für den gewählten Abfragetyp zu verwendenden Wert ein.

Gewählter Abfragetyp	Frage der Abfrage
nach Host	Der Hostname, die URL
nach FQDN	Der vollständige Domänenname `my_server.my_domain.com`
nach IP	Die IP-Adresse des Servers
nach MX	Die Mail Exchange-Adresse

Bildschirm „Web-Zugriff“

Befehlsfolge: Konfiguration > Netzwerk > Web > Zugriff

Verwenden Sie diese Option zur Konfiguration der Zugriffsmethode für die Web-Oberfläche. (Um hier Änderungen vornehmen zu können, müssen Sie die Netzwerkmanagement-Karte neu starten.) Siehe „Netzwerk“ im Menü „Steuerung“.)

Über die Kontrollkästchen „Aktivieren“ können Sie den Zugriff auf diese Benutzeroberfläche entweder über **HTTP** oder **HTTPS** oder über beide Möglichkeiten aktivieren. HTTP ist standardmäßig deaktiviert und HTTPS ist standardmäßig aktiviert. Bei HTTPS werden Benutzernamen, Kennwörter und Daten für die Übertragung verschlüsselt, bei HTTP nicht.

Außerdem authentifiziert HTTPS die Netzwerkmanagement-Karte durch ein digitales Zertifikat. Alles Wissenswerte zur Verwendung digitaler Zertifikate finden Sie unter „Erstellen und Installieren von digitalen Zertifikaten“ im ***Sicherheitshandbuch*** auf der **APC-Website**.

Für die **Ports** können Sie die Einstellung auf einen beliebigen freien Port zwischen 5000 und 32768 ändern, um die Sicherheit zu erhöhen. Sie müssen 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(s)://152.214.12.114:5000
```

Bildschirm „SSL-Zertifikat“

Befehlsfolge: Konfiguration > Netzwerk > Web > SSL-Zertifikat

Hiermit können Sie ein Sicherheitszertifikat hinzufügen, ersetzen oder entfernen. SSL (Secure Socket Layer) ist ein Protokoll, das zur Verschlüsselung von Daten bei der Übertragung zwischen Ihrem Browser und dem Web-Server verwendet wird.

Folgende **Status** sind möglich:

- **Gültiges Zertifikat**: Es wurde ein gültiges Zertifikat installiert oder von der Netzwerkmanagement-Karte erzeugt. Klicken Sie auf diesen Link, um sich den Inhalt des Zertifikats anzusehen.
- **Zertifikat nicht installiert**: Es ist kein Zertifikat installiert oder wurde über FTP oder SCP an einem falschen Speicherort installiert. Mit der Option **Hinzufügen oder ersetzen einer Zertifikatdatei** wird das Zertifikat am richtigen Speicherort installiert, d. h. unter **/ssl** auf der Netzwerkmanagement-Karte.
- **Wird generiert**: Die Netzwerkmanagement-Karte erzeugt ein Zertifikat, weil kein gültiges Zertifikat gefunden wurde.
- **Wird geladen**: Ein Zertifikat wird auf der Netzwerkmanagement-Karte aktiviert.

Wenn Sie ein ungültiges Zertifikat installieren oder falls bei der Aktivierung von SSL kein Zertifikat geladen wurde, erzeugt die Netzwerkmanagement-Karte ein Standard-Zertifikat; dadurch kann der Zugriff auf die Schnittstelle bis zu einer Minute lang blockiert werden. Sie können das Standard-Zertifikat für einen einfachen, verschlüsselten Sicherheitsstandard verwenden; allerdings wird jedes Mal, wenn Sie sich anmelden, eine Sicherheitswarnung angezeigt.

Hinzufügen oder ersetzen einer Zertifikatdatei: Navigieren Sie im Dateisystem zu der mit dem *Sicherheitsassistenten* erzeugten Zertifikatdatei. Alles Wissenswerte zur Verwendung digitaler Zertifikate, die vom Sicherheitsassistenten oder von der Netzwerkmanagement-Karte erstellt wurden, finden Sie unter „Erstellen und Installieren von digitalen Zertifikaten“ im ***Sicherheitshandbuch*** auf der **APC-Website**.

Entfernen: Hiermit löschen Sie das Zertifikat. Siehe hierzu auch den Text auf dem Bildschirm.

Bildschirm „Konsole“

Befehlsfolge: Konfiguration > Netzwerk > Konsole > Zugriff

Befehlsfolge: Konfiguration > Netzwerk > Konsole > SSH-Host-Schlüssel

Konsolenzugriff. Sie müssen den Konsolenzugriff aktivieren, um Ihre USV-Firmware zu aktualisieren (siehe „Bildschirm Firmware-Aktualisierung“). Der Konsolenzugriff ermöglicht die Verwendung der Befehlszeile.

Über die Kontrollkästchen „Aktivieren“ können Sie den Zugriff auf die Befehlszeile entweder über **Telnet** oder **SSH** oder über beide Möglichkeiten aktivieren. Telnet ist standardmäßig deaktiviert und SSH ist standardmäßig aktiviert. Bei Telnet werden Benutzernamen, Kennwörter und Daten für die Übertragung nicht verschlüsselt, bei SSH schon.

Hinweis: Durch die Aktivierung von SSH wird auch SCP (SeCure CoPy) für die sichere Dateiübertragung aktiviert. Weitere Informationen zur Verwendung von SCP finden Sie unter „Dateiübertragungen“.

Für die **Ports**, die zur Kommunikation mit der Netzwerkmanagement-Karte verwendet werden sollen, können Sie die Einstellung auf einen beliebigen freien Port zwischen 5000 und 32768 ändern, um die Sicherheit zu erhöhen.

- **Telnet-Anschluss**: Die Standardeinstellung ist „23“. Sie müssen dann einen Doppelpunkt (:) oder ein Leerzeichen (abhängig vom Telnet-Client) eingeben, um den nicht standardmäßigen Port anzugeben.

  Wenn beispielsweise der Port 5000 und die IP-Adresse 152.214.12.114 verwendet werden sollen, benötigt der Telnet-Client einen der folgenden Befehle:

  `telnet 152.214.12.114:5000` *oder* `telnet 152.214.12.114 5000`

- **SSH-Anschluss**: Die Standardeinstellung ist „22“. Die zum Festlegen eines nicht standardmäßigen Ports benötigte Befehlssyntax können Sie der Dokumentation zu Ihrem SSH-Client entnehmen. Siehe auch „SSH-Host-Schlüssel“ weiter unten.

SSH-Host-Schlüssel. Wenn Sie SSH (Secure Shell Protocol) für den Konsolenzugriff verwenden, können Sie den Host-Schlüssel über den Bildschirm „SSL-Host-Schlüssel“ hinzufügen, ersetzen oder löschen.

Status zeigt an, ob der Host-Schlüssel (privater Schlüssel) gültig ist. Folgende Status sind möglich:

- **SSH deaktiviert**: Es ist kein Host-Schlüssel in Verwendung.
- **Wird generiert**: Die Netzwerkmanagement-Karte erzeugt einen Host-Schlüssel, weil kein gültiger Host-Schlüssel gefunden wurde.

- **Wird geladen**: Ein Host-Schlüssel wird auf der Netzwerkmanagement-Karte aktiviert.
- **Gültig**: Einer der folgenden gültigen Host-Schlüssel befindet sich im Ordner **/ssh** (d. h. im erforderlichen Standardordner auf der Netzwerkmanagement-Karte):
  - Ein vom Sicherheitsassistenten erstellter Host-Schlüssel mit einer Verschlüsselungsstärke von 1024 oder 2048 Bit
  - Ein von der Netzwerkmanagement-Karte erstellter RSA-Host-Schlüssel mit einer Verschlüsselungsstärke von 2048 Bit

Hinzufügen oder ersetzen eines Host-Schlüssels: Übertragen Sie eine vom Sicherheitsassistenten erstellte Host-Schlüssel-Datei an die Netzwerkmanagement-Karte. Eine Anleitung zur Verwendung des Sicherheitsassistenten finden Sie im Sicherheitshandbuch auf der **APC-Website**. Um einen extern erstellten Host-Schlüssel zu verwenden, übertragen Sie den Host-Schlüssel vor der Aktivierung von SSH (mit „Konsolenzugriff“).

Hinweis: Sie können die zum Aktivieren von SSH benötigte Zeit verkürzen, indem Sie vorab einen Host-Schlüssel erstellen und an die Netzwerkmanagement-Karte übertragen. *Wenn Sie SSH aktivieren, ohne dass zuvor ein Host-Schlüssel geladen wurde, benötigt die Netzwerkmanagement-Karte bis zu einer Minute, um den Host-Schlüssel zu erstellen, und der SSH-Server bleibt während dieser Zeit unerreichbar.*

Entfernen: Löschen Sie den Host-Schlüssel. Siehe hierzu auch den Text auf dem Bildschirm.

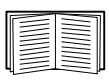
Damit Sie SSH verwenden können, muss ein SSH-Client installiert sein. Die meisten Linux-Distributionen und sonstigen UNIX-Plattformen beinhalten einen SSH-Client. Bei Microsoft Windows-Betriebssystemen (außer Windows 10) ist dies nicht der Fall. Clients für Windows sind bei verschiedenen Anbietern erhältlich, wie etwa PuTTY unter www.putty.org.

Bildschirme „SNMP“

SNMPv1- und SNMPv3-Unterstützung gehören 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. Siehe „Lizenz“.

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

Damit Sie **Data Center Expert** zur Verwaltung einer USV im öffentlichen Netzwerk eines Systems verwenden können, *muss* SNMPv1 oder SNMPv3 über die Schnittstelle der Netzwerkmanagement-Karte aktiviert werden (SNMPv1 ist standardmäßig aktiviert). Mit Lesezugriff kann das Gerät Traps von der Netzwerkmanagement-Karte empfangen; während der Verwendung der Schnittstelle zur Netzwerkmanagement-Karte wird jedoch Schreibzugriff benötigt, um das Gerät als Trap-Empfänger einzurichten.



Ausführliche Informationen zur Erhöhung und Verwaltung der Systemsicherheit finden Sie im *Sicherheitshandbuch* auf der **APC-Website**.

SNMPv1.

Befehlsfolge: Konfiguration > Netzwerk > SNMPv1 > Zugriff und Zugriffssteuerung

Verwenden Sie **Zugriff**, um SNMP Version 1 als Kommunikationsmethode mit der Netzwerkmanagement-Karte zu aktivieren bzw. zu deaktivieren.

SNMPv1 ist standardmäßig deaktiviert. Der **Community-Name** muss festgelegt werden, bevor SNMPv1-Kommunikation hergestellt werden kann.

Die Verwendung von SNMPv2c wird durch die Optionen von SNMPv1 unterstützt.

Zugriffssteuerung. Sie können bis zu vier Einträge für die Zugriffssteuerung konfigurieren, um festzulegen, welche Netzwerkmanagementsysteme auf diese Netzwerkmanagement-Karte zugreifen dürfen. Zum Bearbeiten klicken Sie auf einen Community-Namen.

Standardmäßig ist jeder der vier verfügbaren SNMPv1-Communitys ein Eintrag zugewiesen. Sie können diese Einstellungen dahingehend bearbeiten, dass *jeder Community mehrere Einträge* zugewiesen sind, damit mehrere spezielle IPv4- und IPv6-Adressen, Hostnamen oder IP-Adressmasken darauf zugreifen können.

- Standardmäßig hat eine Community von jedem Standort im Netzwerk aus Zugriff auf die Netzwerkmanagement-Karte.
- Wenn Sie für einen Community-Namen mehrere Einträge für die Zugriffssteuerung konfigurieren, bedeutet das, dass eine oder mehrere der anderen Communitys nicht auf das Gerät zugreifen können.

Community-Name: Der Name, den ein Netzwerkmanagementsystem (NMS) verwenden muss, um auf die Community zugreifen zu können. Die Höchstlänge beträgt 16 ASCII-Zeichen.

NMS-IP/Hostname: Die IPv4- oder IPv6-Adresse, die IP-Adressmaske oder der Hostname, der den Zugriff durch NMS kontrolliert. Ein Hostname oder eine bestimmte IP-Adresse (z. B. 149.225.12.1) ermöglicht dem NMS den Zugriff nur am betreffenden Standort. Bei IP-Adressen, die „255“ enthalten, ist der Zugriff wie folgt eingeschränkt:

- 149.225.12.**255**: Zugriff ausschließlich durch ein NMS im Segment 149.225.12.
- 149.225.**255.255**: Zugriff ausschließlich durch ein NMS im Segment 149.225.
- 149.**255255255**: Zugriff ausschließlich durch ein NMS im Segment 149.
- 0.0.0.0 (die Standardeinstellung), gleichbedeutend mit 255.255.255.255: Zugriff durch beliebige NMS in beliebigen Segmenten.

Zugriffstyp: Die Vorgänge, die bei einem NMS über die Community erlaubt sind.

- **Read**: Nur GETs, dies zu jeder Zeit
- **Write**: GETs zu jeder Zeit und SETs, wenn kein Benutzer über die Benutzeroberfläche oder die Befehlszeile angemeldet ist.
- **Write+**: GETs und SETs zu jeder Zeit.
- **Deaktivieren**: Keine GETs und keine SETs, zu keiner Zeit.

SNMPv3.

> **Befehlsfolge: Konfiguration > Netzwerk > SNMPv3 > Zugriff**, **Benutzerprofile** und **Zugriffssteuerung**

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

SNMPv3 ist standardmäßig deaktiviert. Ein gültiges Benutzerprofil muss mit Kennwortsätzen (**Kennwortsatz für Authentifizierung, Kennwortsatz für Datenschutz**) aktiviert werden, bevor SNMPv3-Kommunikation hergestellt werden kann.

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

Die Netzwerkmanagement-Karte unterstützt SHA- oder MD5-Authentifizierung und AES- oder DES-Verschlüsselung.

SNMPv3-Zugriff aktivieren in den Zugriffseinstellungen ermöglicht diese Methode der Kommunikation mit diesem Gerät.

Benutzerprofile. In der Grundeinstellung werden hier die Einstellungen für vier Benutzerprofile angezeigt, konfiguriert mit den Benutzernamen **apc snmp profile1** bis **apc snmp profile4**, ohne Authentifizierung und ohne Datenschutz (keine Verschlüsselung). Wenn Sie die folgenden Einstellungen für ein Benutzerprofil ändern möchten, klicken Sie in der Liste auf einen Benutzernamen.

- **User Name (Benutzername)**: Die Kennung des Benutzerprofils. SNMP Version 3 ordnet GETs, SETs und Traps einem Benutzerprofil zu, indem es den Benutzernamen im Profil mit dem Benutzernamen in dem zu übertragenden Datenpaket abgleicht. Ein Benutzername kann aus bis zu 32 ASCII-Zeichen bestehen.
- **Authentication Phrase**: Ein aus 15 bis 32 ASCII-Zeichen bestehender Kennwortsatz, der verifiziert, dass es sich bei dem mit diesem Gerät über SNMPv3 kommunizierenden NMS tatsächlich um dieses NMS handelt. Des Weiteren wird verifiziert, dass die Nachricht während der Übertragung nicht verändert und die Nachricht zeitnah übertragen wurde. Dadurch ist ersichtlich, dass sich die Nachricht nicht verzögert hat und sie nicht kopiert und später erneut gesendet wurde.
- **Datenschutz-Kennwortsatz**: Ein aus 15 bis 32 ASCII-Zeichen bestehender Kennwortsatz, mit dem mittels Verschlüsselung die Geheimhaltung der zwischen diesem Gerät und einem NMS über SNMPv3 ausgetauschten Daten sichergestellt werden kann.
- **Authentifizierungsprotokoll**: Die Implementierung von SNMPv3 unterstützt SHA- und MD5-Authentifizierung. Eine dieser Optionen muss ausgewählt werden.
- **Datenschutzprotokoll**: Die Implementierung von SNMPv3 unterstützt AES und DES als Protokolle zur Ver- und Entschlüsselung von Daten. Sie müssen sowohl ein Datenschutzprotokoll als auch ein Datenschutzkennwort verwenden, da die SNMP-Anfrage sonst nicht verschlüsselt wird.

  Das Datenschutzprotokoll wiederum kann nicht ausgewählt werden, solange kein Authentifizierungsprotokoll ausgewählt wurde.

Zugriffssteuerung. Sie können bis zu vier Einträge für die Zugriffssteuerung konfigurieren, um festzulegen, welche Netzwerkmanagementsysteme auf diese Netzwerkmanagement-Karte zugreifen dürfen. Zum Bearbeiten klicken Sie auf einen Benutzernamen.

Standardmäßig ist jedem der vier Benutzerprofile ein Eintrag zugewiesen. Sie können diese Einstellungen dahingehend bearbeiten, dass *jedem Benutzernamen mehrere Einträge* zugewiesen sind, damit mehrere spezielle IP-Adressen, Hostnamen oder IP-Adressmasken darauf zugreifen können.

- Standardmäßig haben alle NMS, die dieses Profil verwenden, Zugriff auf dieses Gerät.
- Wenn Sie für einen Benutzernamen mehrere Einträge für die Zugriffssteuerung konfigurieren, bedeutet das, dass einer oder mehrere der anderen Benutzernamen nicht auf dieses Gerät zugreifen können.

User Name (Benutzername): Wählen Sie aus diesem Dropdown-Listenfeld das Benutzerprofil aus, für das dieser Eintrag für die Zugriffssteuerung gelten soll. Verfügbar sind diejenigen vier Benutzernamen, die Sie über die Option „Benutzerprofile“ konfigurieren.

NMS-IP/Hostname: Die IP-Adresse, die IP-Adressmaske oder der Hostname, der den Zugriff durch das NMS kontrolliert. Ein Hostname oder eine bestimmte IP-Adresse (z. B. 149.225.12.1) ermöglicht dem NMS den Zugriff nur am betreffenden Standort. Bei IP-Adressmasken, die „255“ enthalten, ist der Zugriff wie folgt eingeschränkt:

- 149.225.12.**255**: Zugriff ausschließlich durch ein NMS im Segment 149.225.12.
- 149.225.**255.255**: Zugriff ausschließlich durch ein NMS im Segment 149.225.
- 149.**255255255**: Zugriff ausschließlich durch ein NMS im Segment 149.
- 0.0.0.0 (die Standardeinstellung), gleichbedeutend mit 255.255.255.255: Zugriff durch beliebige NMS in beliebigen Segmenten.

Bildschirme „Modbus“

Modbus wird auf der AP9544-Karte nicht unterstützt.

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

Nutzen Sie die Modbus-Optionen, um Ihre Netzwerkmanagement-Karte für die Verwendung des Modbus-Protokolls zu konfigurieren, das den Anschluss eines Gebäudemanagementsystems (BMS) ermöglicht. Die AP9547-Karte unterstützt Modbus TCP.

Weitere Informationen über die Modbus-Implementierung auf Ihrem USV finden Sie im Modbus-Dokumentationsanhang und auf den *Modbus-Registerkarten* auf der **APC-Website**.

HINWEIS: Die Netzwerkmanagement-Karte unterstützt 5 gleichzeitige Modbus-TCP-Verbindungen.

Modbus TCP.

Befehlsfolge: Konfiguration > Netzwerk > Modbus > TCP

1. Verwenden Sie **Zugriff**, um Modbus TCP als Kommunikationsmethode mit der Netzwerkmanagement-Karte zu aktivieren bzw. zu deaktivieren.
2. Legen Sie die **Portnummer** der TCP-Verbindung fest. Sie kann auf 502 (Standard) oder einen Wert zwischen 5000 und 32768 eingestellt werden.
3. Klicken Sie auf „Apply“ (Übernehmen), um Ihre Änderungen zu speichern.

BACnet-Bildschirm

BACnet wird auf der AP9544-Karte nicht unterstützt.

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

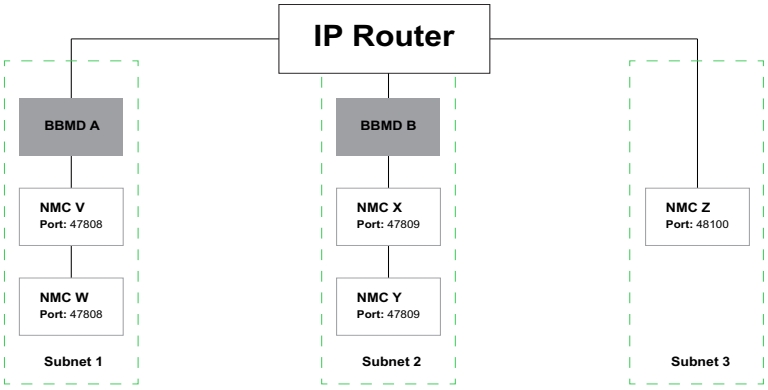
Verwenden Sie die BACnet-Optionen, um Ihre Netzwerkmanagement-Karte zur Verwendung des BACnet-Protokolls zu konfigurieren und um USV-Daten für BACnet bereitzustellen.

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

BACnet-Konfiguration

Option	Beschreibung
Zugriff	Aktivieren Sie das Kontrollkästchen, um BACnet zu aktivieren. Wenn es nicht aktiviert ist, kann auf die Netzwerkmanagement-Karte nicht über BACnet zugegriffen werden. BACnet ist standardmäßig deaktiviert. **HINWEIS:** BACnet kann erst aktiviert werden, nachdem das **Passwort für die Gerätekommunikationskontrolle** eingerichtet wurde.
Geräte-ID	Eine eindeutige Bezeichnung des BACnet Geräts, welches zur Adressierung des Geräts verwendet wird. Zulässiger Bereich: 0–4194303.
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.
Netzwerkprotokoll	Wählen Sie das Protokoll, das verwendet werden soll: • BACnet/IP
APDU-Timeout	Die Zeitspanne in Millisekunden, in der die Netzwerkmanagement-Karte auf die Antwort einer BACnet-Anfrage wartet. Zulässiger Bereich: 1000-30000. Der Standardwert ist 6000.
APDU-Wiederholungen	Die Anzahl der BACnet-Wiederholungsversuche, welche die Netzwerkmanagement-Karte durchführt, bevor die Anfrage abgebrochen wird. Zulässiger Bereich: 1–10. Der Standardwert ist 3.
Device-Communication-Control-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

Option	Beschreibung
Lokaler Port	Der UDP-/IP-Port, den die Netzwerkmanagement-Karte zum senden und empfangen von BACnet-/IP-Nachrichten verwendet. Zulässiger Bereich: 5000–65535. Standard: 47808. **Hinweis**: Die Adresse einer BACnet-/IP-fähigen Netzwerkmanagement-Karte besteht aus der IP-Adresse der Netzwerkmanagement-Karte und dem lokalen Port.
Registrierung fremder Geräte zulassen	Wenn Sie das Kontrollkästchen aktivieren, wird die Netzwerkmanagement-Karte bei einem BBMD (BACnet Broadcast Management Device) registriert. **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. Im obigen Beispiel: • BBMD A managed die Broadcastmeldung der NMCs V und W. • BBMD B managed die Broadcastmeldung der NMCs X und Y. • Nur NMC Z muss als Fremdgerät bei BBMD A oder BBMD B registriert werden, da kein BBMD im Subnetz verfügbar ist. • Sobald NMC Z registriert ist, kann diese die Broadcast Meldungen der BBMD, an welcher Sie registriert ist empfangen und selber Meldungen senden. Dieses BBMD überträgt diese dann an alle Geräte des eigenen Subnetzes und an die anderen BBMDs im Netzwerk über den IP-Router.

Option	Beschreibung
Status	Der Status der Registrierung fremder Geräte (FDR): • **Registrierung fremder Geräte inaktiv** FDR ist inaktiv wenn: – FDR aktiviert und BACnet deaktiviert ist – FDR deaktiviert und BACnet aktiviert ist – FDR deaktiviert und BACnet deaktiviert ist • **Registrierung erfolgreich** FDR wurde erfolgreich abgeschlossen. • **Registrierung abgelehnt** FDR wurde nicht erfolgreich abgeschlossen. Die Netzwerkmanagement-Karte versucht die Registrierung automatisch erneut, aber Sie können auch das Kontrollkästchen **Registrierung fremder Geräte aktivieren** aktivieren, um die Netzwerkmanagement-Karte zu einem erneuten Registrierungsversuch aufzufordern. • **Registrierung abgesendet** Die FDR-Anfrage wurde abgesendet, aber noch nicht abgeschlossen.
BACnet/IP-Broadcast-Management-Gerät	Die IP-Adresse oder der FQDN (Fully Qualified Domain Name) des BBMD, mit der/dem diese Netzwerkmanagement-Karte registriert wird.
Port	Der Port des BBMD, mit dem diese Netzwerkmanagement-Karte registriert wird.
TTL	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. TTL steuert, wie häufig sich die Netzwerkmanagement-Karte beim BBMD registriert, da die Netzwerkmanagement-Karte versuchen wird, sich erneut zu registrieren, bevor diese Zeit abläuft.

WiFi-Bildschirm

Pfad: Konfiguration > Netzwerk > WiFi

Hinweis: Dieser Bildschirm ist relevant, wenn das optionale APC-USB-WiFi-Gerät (AP9834) im USB-Anschluss einer AP9544/AP9547-Karte eingesetzt ist.

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.

Verwenden Sie diesen Bildschirm, um den aktuellen Status des WiFi-Netzwerks anzuzeigen, WiFi zu aktivieren/deaktivieren und die Einstellungen des WiFi-Netzwerks zu konfigurieren.

Hinweis: Durch Aktivieren/Deaktivieren von WiFi wird die kabelgebundene LAN-Verbindung deaktiviert/aktiviert. Die Netzwerkmanagement-Karte wird neu gestartet, wenn die WiFi-Einstellungen konfiguriert wurden. Nach dem Neustart wird das kabelgebundene Netzwerk deaktiviert und die Netzwerkmanagement-Karte versucht, eine Verbindung zum angegebenen **Netzwerknamen (SSID)** herzustellen.

Netzwerkname (SSID): Geben Sie den Netzwerknamen (SSID) des WiFi-Netzwerks an. Die Höchstlänge beträgt 32 Zeichen.

Sicherheitstyp: Geben Sie den Sicherheitstyp des WiFi-Netzwerks und die Authentifizierungsdetails an:

Option	Beschreibung
WPA	**WiFi-Passwort:** Geben Sie ein Passwort für das WiFi-Netzwerk an. Die Höchstlänge beträgt 64 Zeichen.
WPA2-AES	
WPA2-Gemischt	
WPA2-TKIP	
WPA2-Enterprise	• **Benutzername:** Der Benutzername für die WPA2-Enterprise-Authentifizierung. Die Höchstlänge beträgt 32 Zeichen. • **Passwort:** Das Passwort für die WPA2-Enterprise-Authentifizierung. Die Höchstlänge beträgt 32 Zeichen. • **Äußere Identität:** 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.

Informationen zum Aktualisieren der Firmware des APC-USB-WiFi-Geräts (AP9834) erhalten Sie über den `wifi`-Befehl im **Befehlszeilenhandbuch für die Netzwerkmanagement-Karte für Easy-UPS-Geräte**.

Informationen zur Fehlerbehebung bei der Verbindung mit dem APC-USB-WiFi-Gerät (AP9834) und die LED-Beschreibungen des Geräts finden Sie unter „Probleme mit dem APC-USB-WiFi-Dongle (AP9834)“.

Menü „Notification“

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

Siehe die folgenden Abschnitte:

- „Benachrichtigungsarten“
- „Konfigurieren von Ereignisaktionen“
- „Bildschirme für die E-Mail-Benachrichtigung“
- Bildschirm „SNMP-Trap-Test“
- Bildschirm „SNMP-Trap-Empfänger“

Benachrichtigungsarten

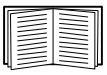
Sie können Benachrichtigungsaktionen konfigurieren, die als Reaktion auf ein Ereignis durchgeführt werden. Dadurch können Sie Benutzer auf unterschiedliche Art und Weise über ein Ereignis in Kenntnis setzen:

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

    Zur Überwachung bestimmter Geräte können Sie auch Daten zum Systemverhalten protokollieren. Informationen zur Konfiguration und Verwendung dieser Datenerfassungsoption finden Sie unter „Datenprotokoll“.

  - Abfragen (SNMP GETs)

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

Die NMC unterstützt die Verwendung der **RFC1628 MIB** (Management Information Base). Eine Anleitung zum Einrichten eines Trap-Empfängers finden Sie unter Bildschirm „SNMP-Trap-Empfänger“. Die aus drei Ereignissen zusammengesetzte Gruppe **1628 MIB** funktioniert nur mit dieser MIB, nicht jedoch mit der alternativen Powernet MIB. Die Ereignisse können wie jedes andere Ereignis konfiguriert werden (siehe „Konfigurieren von Ereignisaktionen“ weiter unten).

Konfigurieren von Ereignisaktionen

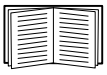
Konfigurieren nach Ereignis.

Befehlsfolge: Konfiguration > Benachrichtigung > Ereignisaktionen > Nach Ereignis

In der Grundeinstellung ist die Protokollierung für alle Ereignisse konfiguriert. So definieren Sie Ereignisaktionen für ein einzelnes Ereignis:

1. Wählen Sie das Menü **Konfiguration** und dann **Benachrichtigung**, **Ereignisaktionen** und **Nach Ereignis**.
2. Um Ereignisse zu finden, klicken Sie auf eine Spaltenüberschrift, um die Listen in den Kategorien **Stromereignisse**, **Umgebungsereignisse** oder **Systemereignisse** anzuzeigen.
   Oder klicken Sie auf eine Unterkategorie unter diesen Überschriften wie **Eingangsstatus** oder **Temperatur**.
3. Klicken Sie auf den Ereignisnamen, um die aktuelle Konfiguration anzuzeigen oder zu bearbeiten. Hierzu gehören beispielsweise die per E-Mail zu benachrichtigenden Empfänger oder die durch SNMP-Traps zu benachrichtigenden Netzwerkmanagement-Systeme (NMS). Siehe „Benachrichtigungsparameter“. Klicken Sie auf das Kontrollkästchen **Ereignisprotokoll**, um einen Ereignisprotokolleintrag für dieses Ereignis zu aktivieren oder zu deaktivieren.

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



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

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

Konfiguration nach Ereignisgruppen.

Befehlsfolge: Konfiguration > Benachrichtigung > Ereignisaktionen > Nach Gruppe

So konfigurieren Sie mehrere Ereignisse gleichzeitig als Gruppe:

1. Wählen Sie das Menü **Konfiguration** und dann **Benachrichtigung**, **Ereignisaktionen** und **Nach Gruppe**.
2. Wählen Sie eine Methode zum Gruppieren von Ereignissen für die Konfiguration:
   – Wählen Sie **Ereignisse nach Schweregrad** und wählen Sie dann mindestens einen Schweregrad aus. Sie können den Schweregrad eines Ereignisses nicht ändern.
   – Wählen Sie **Ereignisse nach Kategorie** und wählen Sie dann alle Ereignisse aus, die mindestens einer vordefinierten Kategorie zugeordnet sind.
3. Klicken Sie auf „Weiter“, um zum jeweils nächsten Bildschirm zu gelangen und folgende Einstellungen vorzunehmen:
   a. Auswählen von Ereignisaktionen für die Ereignisgruppe.
      - Damit Sie weitere Vorgänge außer der Option für die **Protokollierung** (die Voreinstellung) auswählen können, müssen Sie zuerst mindestens einen relevanten Empfänger bzw. Adressaten konfigurieren.
      - Wenn Sie die Option **Protokollierung** wählen und einen Syslog-Server konfiguriert haben, wählen Sie auf dem nächsten Bildschirm **Ereignisprotokoll** oder `Syslog` (oder beides). (Weitere Informationen hierzu finden Sie auf Menü „Konfigurationsprotokolle“.)
   b. Geben Sie an, ob die neue konfigurierte Ereignisaktion für diese Ereignisgruppe aktiviert bleiben sollen, oder ob die Aktion deaktiviert werden soll.

   Siehe „Benachrichtigungsparameter“ direkt im Anschluss.

Benachrichtigungsparameter. Über diese Konfigurationsfelder können Sie die Parameter für die Benachrichtigungen zu Ereignissen festlegen. Siehe „Konfigurieren nach Ereignis“ und „Konfiguration nach Ereignisgruppen“.

Zum Öffnen dieser Parameter klicken Sie auf den Namen des Adressaten bzw. Empfängers.

Feld	Beschreibung
Benachrichtigungsverzögerung	Wenn das Ereignis über die angegebene Zeit hinaus andauert, wird eine Benachrichtigung gesendet. Wenn dieser Zustand vor Ablauf der angegebenen Zeit endet, wird keine Benachrichtigung gesendet.
Wiederholintervall	Die Benachrichtigung wird im angegebenen Intervall wiederholt gesendet (die Standardeinstellung beträgt 2 Minuten, bis der Zustand endet).
Benachrichtigungsanzahl insgesamt	Während eines aktiven Ereignisses wird die Benachrichtigung mit der hier angegebenen Häufigkeit wiederholt.
oder	
Benachrichtigung bis Zustandsbehebung	Die Benachrichtigung wird wiederholt gesendet, bis der Zustand endet oder behoben wird.

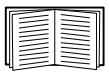
Für Ereignisse mit einem Löschereignis können Sie diese Parameter ebenfalls festlegen. (Ein Beispiel für ein Ereignis mit einem Löschereignis ist `USV: Kommunikation mit Batterie-Modulen unterbrochen` und `USV: Kommunikation mit Batterie-Modulen wiederhergestellt`.)

Bildschirme für die E-Mail-Benachrichtigung

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

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

- Die IP-Adressen des primären und gegebenenfalls vorhandenen sekundären DNS-Servers. (Siehe Bildschirm „DNS“)
- Die IP-Adresse oder den DNS-Namen des **SMTP-Servers** sowie der **Absenderadresse**. (Siehe „SMTP-Server“ weiter unten.)
- Die E-Mail-Adressen von bis zu vier Empfängern. (Siehe „E-Mail-Empfänger“)



Über die Einstellung **Empfängeradresse** der Option **Empfänger** können Sie den E-Mail-Versand an einen textbasierten Bildschirm konfigurieren.

SMTP-Server.

Befehlsfolge: Konfiguration > Benachrichtigung > E-Mail > Server

Auf diesem Bildschirm sind der primäre und der sekundäre DNS-Server (siehe Bildschirm „DNS“) sowie diese Felder angegeben:

Feld	Beschreibung
E-Mail-Konfiguration für ausgehende Nachrichten	
Absenderadresse	Der Inhalt des Felds **Von** in E-Mail-Nachrichten, die von der Netzwerkmanagement-Karte gesendet werden: • Im Format *benutzer@* [*IP-Adresse*] (falls eine IP-Adresse als **Lokaler SMTP-Server** angegeben wurde). • Im Format *benutzer@domaene* in den E-Mail-Nachrichten (falls DNS konfiguriert ist und der DNS-Name als **Lokaler SMTP-Server** angegeben wurde). Hinweis: Damit diese Einstellung verwendet werden kann, verlangt der lokale SMTP-Server unter Umständen die Angabe eines gültigen, auf dem Server angelegten Benutzerkontos. Einzelheiten hierzu finden Sie in der Dokumentation zum Server.
SMTP-Server	Die IPv4-/IPv6-Adresse oder der DNS-Name des lokalen SMTP-Servers. Hinweis: Diese Definition ist nur erforderlich, wenn die Option **SMTP-Server** auf **Lokal** eingestellt ist. Siehe „E-Mail-Empfänger“
Authentifizierung	Aktivieren Sie diese Option, falls der SMTP-Server eine Authentifizierung verlangt.
Port	Der SMTP-Standardport ist 25. Alternative Ports: 465, 587, 2525, 5000 bis 32768.
Benutzername/ Kennwort/ Kennwort bestätigen	Geben Sie hier Ihren Benutzernamen und Ihr Kennwort ein, wenn der Mail-Server eine Authentifizierung verlangt. Damit wird eine einfache Authentifizierung durchgeführt, kein SSI.
Fortgeschr.	
SSL/TLS verwenden	• **Nie**: Der SMTP-Server erfordert und unterstützt auch keine Verschlüsselung. • **Wenn unterstützt**: Der SMTP-Server zeigt an, dass STARTTLS unterstützt wird, erfordert jedoch *keine* verschlüsselte Verbindung. Der STARTTLS-Befehl wird nach dem Advertisement gesendet. • **Immer**: Der SMTP-Server erfordert das Senden des STARTTLS-Befehls, sobald eine Verbindung zum Server hergestellt wird. • **Implizit**: Der SMTP-Server akzeptiert nur Verbindungen, die von vornherein verschlüsselt sind. Es wird keine STARTTLS-Nachricht an den Server gesendet.

Feld	Beschreibung
Root-Zertifikat der Zertifizierungsstelle erforderlich machen	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.
Dateiname	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.

E-Mail-Empfänger.

Befehlsfolge: Konfiguration > Benachrichtigung > E-Mail > Empfänger

Hiermit geben Sie bis zu vier E-Mail-Empfänger an. Klicken Sie auf einen Namen, um die Einstellungen zu konfigurieren. Siehe auch „SMTP-Server“ weiter oben.

Feld	Beschreibung
E-Mail-Generierung	Hiermit aktivieren (Standardeinstellung) oder deaktivieren Sie den E-Mail-Versand an den Empfänger.
Empfängeradresse	Der Benutzer- und Domänenname des Empfängers. Zum Senden von E-Mails an einen Pager verwenden Sie die E-Mail-Adresse, die dem Pager-Gateway-Konto des Empfängers zugewiesen ist (z. B. `myacct100@skytel.com`). Das Pager-Gateway erstellt dann die Seite. Wenn Sie die DNS-Suche nach der IP-Adresse des Mail-Servers umgehen möchten, geben Sie statt des E-Mail-Domänennamens die IP-Adresse in eckigen Klammern ein, z. B. jmeier@[xxx.xxx.x.xxx] statt jmeier@firma.com. Dies ist hilfreich, wenn die DNS-Suche aus irgendeinem Grund nicht richtig funktionieren sollte. Hinweis: Der Pager des Empfängers muss Textnachrichten verarbeiten können.
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.
Sprache	Wählen Sie aus dem Dropdown-Listenfeld die Sprache aus, in der die E-Mails gesendet werden sollen. Sie können verschiedene Sprachen für verschiedene Benutzer verwenden. Siehe „Ändern der Sprache der Benutzeroberfläche“.
Server	Wählen Sie eine der folgenden Routing-Methoden für E-Mails aus: • **Lokal**: Über den site-local SMTP-Server. Diese empfohlene Einstellung sorgt dafür, dass die E-Mail über den site-local SMTP-Server gesendet wird. Mit dieser Einstellung werden Verzögerungen, Netzwerkausfälle und stundenlange erneute Sendeversuche beschränkt. Wenn Sie die Einstellung „Lokal“ wählen, müssen Sie am SMTP-Server Ihres Geräts auch die Weiterleitung aktivieren und ein spezielles externes E-Mail-Konto einrichten, an das die weitergeleitete E-Mail gesendet werden soll. Sprechen Sie mit dem Administrator Ihres SMTP-Servers, bevor Sie diese Änderungen vornehmen. • **Empfänger**: Über den SMTP-Server des Empfängers. Die Netzwerkmanagement-Karte führt einen MX-Datensatz-Lookup für die E-Mail-Adresse des Empfängers durch und verwendet ihn als seinen SMTP-Server. Die E-Mail wird nur einmal gesendet und könnte daher leicht verloren gehen. • **Benutzerdefiniert**: Diese Einstellung ermöglicht für jeden E-Mail-Empfänger eigene Servereinstellungen. Diese Einstellungen sind von den unter „SMTP-Server“ oben angegebenen Einstellungen unabhängig.

E-Mail SSL-Zertifikate.

Befehlsfolge: Konfiguration > Benachrichtigung > E-Mail > SSL-Zertifikate

Laden Sie für mehr Sicherheit ein SSL-Zertifikat für E-Mails auf die Netzwerkmanagement-Karte. Die Datei muss die Erweiterung `.crt` oder `.cer` haben. Es können zu jeder Zeit bis zu fünf Dateien geladen sein.

Nach der Installation werden hier auch die Zertifikatdetails angezeigt. Bei einem ungültigen Zertifikat wird für alle Felder außer „Dateiname“ „n/a“ angezeigt.

Zertifikate können über diesen Bildschirm gelöscht werden. Alle E-Mail-Empfänger, die das Zertifikat verwenden, sollten per Hand geändert werden, um Verweise auf dieses Zertifikat zu löschen.

E-Mail-Test.

Befehlsfolge: Konfiguration > Benachrichtigung > E-Mail > Test

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

Bildschirm „SNMP-Trap-Empfänger“

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

Trap-Empfänger.

Befehlsfolge: Konfiguration > Benachrichtigung > SNMP-Traps > Trap-Empfänger

Mit SNMP-Traps (Simple Network Management Protocol) können Sie sich bei wichtigen USV-Ereignissen automatisch benachrichtigen lassen. Sie sind ein hilfreiches Tool zur Überwachung von mit Ihrem Netzwerk verbundenen Geräten.

Die Trap-Empfänger werden nach **NMS-IP/Hostname** angezeigt, wobei die Abkürzung NMS für Netzwerkmanagementsystem steht. Sie können bis zu sechs Trap-Empfänger konfigurieren.

Zum Konfigurieren eines neuen Trap-Empfängers klicken Sie auf **Trap-Empfänger hinzufügen**. Um einen Trap-Empfänger zu bearbeiten (oder zu löschen), klicken Sie auf seine IP-Adresse oder seinen Hostnamen.

(Wenn Sie einen Trap-Empfänger löschen, werden alle für ihn unter „Konfigurieren von Ereignisaktionen“ konfigurierten Benachrichtigungseinstellungen auf die Standardwerte zurückgesetzt.

Aktivieren Sie die Optionsschaltflächen **SNMPv1** oder **SNMPv3**, um den Trap-Typ anzugeben. Damit ein NMS *beide* Trap-Typen empfangen kann, müssen Sie für das betreffende NMS zwei Trap-Empfänger konfigurieren, einen für jeden Trap-Typ.

Feld	Beschreibung
Trap-Generierung	Aktivieren (die Voreinstellung) oder deaktivieren Sie die Trap-Generierung für diesen Trap-Empfänger.
Powernet MIB Trap-Generierung/ RFC1628	Wählen Sie für jeden generierten Trap zwischen diesen beiden Arten der MIB Trap-Generierung. Die Option „Powernet“ ist eine Spezialversion für Schneider Electric, die viele zusätzliche, für die Produkte dieses Unternehmens relevante Variablen enthält. RFC1628 ist die normale, nicht produktspezifische Management Information Base (MIB) für USV-Geräte. Wenn Sie die RFC1628 MIB verwenden, können Sie auch Benachrichtigungen für die drei RFC1628-Ereignisse verwenden (siehe „Konfigurieren von Ereignisaktionen“). Diese können verwendet werden, um keine Benachrichtigungsereignisse außerhalb der NMC-Umgebung konfigurieren zu müssen, siehe RFC1628 MIB.
NMS-IP/Hostname	Die IPv4-/IPv6-Adresse oder der Hostname dieses Trap-Empfängers. Mit der Voreinstellung 0.0.0.0 bleibt der Trap-Empfänger undefiniert.

Feld	Beschreibung
Sprache	Wählen Sie eine Sprache aus dem Dropdown-Listenfeld aus. Diese Sprache kann sich von der Sprache der Benutzeroberfläche und von der anderer Trap-Empfänger unterscheiden.
SNMPv1	Community-Name: Der Name, der als Kennung gesendet wird, wenn SNMPv1-Traps an diesen Trap-Empfänger gesendet werden. Traps authentifizieren: Wenn diese Option aktiviert ist (die Voreinstellung), empfängt das durch die Einstellung „NMS-IP/Hostname“ identifizierte NMS Authentifizierungs-Traps (Traps, die durch ungültige Anmeldeversuche auf diesem Gerät erzeugt werden).
SNMPv3	User Name (Benutzername): Hiermit wählen Sie die Kennung für das Benutzerprofil dieses Trap-Empfängers aus. Siehe auch „Benutzerprofile“ unter Bildschirme „SNMP“.

Bildschirm „SNMP-Trap-Test“

Befehlsfolge: Konfiguration > Benachrichtigung > SNMP-Traps > Test

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

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

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

An: Wählen Sie die IP-Adresse oder den Hostnamen aus, an den der SNMP-Trap gesendet werden soll. Wenn kein **Trap-Empfänger** konfiguriert ist, wird ein Link zum Konfigurationsbildschirm Trap-Empfänger angezeigt. Siehe Bildschirm „SNMP-Trap-Empfänger“ oben.

Menü „Allgemein“

In diesem Menü finden Sie verschiedene Konfigurationsfunktionen, unter anderem für die Geräteidentifizierung, Datum und Uhrzeit, Export und Import der Konfigurationsoptionen Ihrer Netzwerkmanagement-Karte, für die drei Links unten links auf dem Bildschirm und für die Konsolidierung von Daten für die Fehlerbehebung.

Bildschirm „Identifizierung“

Befehlsfolge: Konfiguration > Allgemein > Identifizierung

Definieren Sie den **Namen** (der NMC-Systemname; siehe hierzu Bildschirm „DNS“), den **Standort** (den physischen Einbauort) und den **Ansprechpartner** (die für das Gerät zuständige Person) zur Verwendung:

- durch den SNMP-Agenten der Netzwerkmanagement-Karte
- Data Center Expert

Insbesondere das Namensfeld wird von den Object Identifiers (OIDs) **sysName**, **sysContact** und **sysLocation** im SNMP-Agenten der Netzwerkmanagement-Karte verwendet. Weitere Informationen zu MIB-II OIDs finden Sie im *Referenzhandbuch für die PowerNet® SNMP Management Information Base (MIB)* auf der. **APC-Website**.

Bildschirm „Datum und Uhrzeit“

Modus.

Befehlsfolge: Konfiguration > Allgemein > Datum und Uhrzeit > Modus

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

Mit beiden wählen Sie die **Zeitzone** aus. Hierbei handelt es sich um Ihren lokalen Zeitunterschied zur koordinierten Weltzeit „Coordinated Universal Time“ (UTC), auch bekannt als „Greenwich Mean Time“ (GMT).

- **Manueller Modus**: Führen Sie einen der folgenden Schritte durch:
  - Geben Sie Datum und Uhrzeit der Netzwerkmanagement-Karte ein oder
  - Aktivieren Sie das Kontrollkästchen **Uhrzeit des lokalen Computers übernehmen**, um Datum und Uhrzeit des verwendeten Computers für die Netzwerkmanagement-Karte zu übernehmen.
- **Mit NTP-Server synchronisieren**: Hiermit können Sie einen NTP-Server angeben, von dem die Netzwerkmanagement-Karte das Datum und die Uhrzeit beziehen soll.

In der Voreinstellung bezieht jede auf der privaten Seite eines Data Center Expert befindliche Netzwerkmanagement-Karte ihre Zeiteinstellungen über Data Center Expert, das der Netzwerkmanagement-Karte als NTP-Server dient.

Feld	Beschreibung
Manuelle NTP-Einstellungen überschreiben	Wenn Sie diese Option auswählen, haben Daten aus anderen Quellen (üblicherweise DHCP) Vorrang vor der hier eingestellten NTP-Konfiguration.
Primärer NTP-Server	Geben Sie die IP-Adresse oder den Domänennamen des primären NTP-Servers ein.
Sekundärer NTP-Server	Geben Sie die IP-Adresse oder den Domänennamen des sekundären NTP-Servers ein, falls dieser zur Verfügung steht.

Feld	Beschreibung
Aktualisierungsintervall	Hiermit legen Sie fest, in welchen Abständen (in Stunden) die Netzwerkmanagement-Karte zur Aktualisierung auf den NTP-Server zugreift. *Mindestwert*: 1; *Maximalwert*: 8760 (1 Jahr).
Jetzt mit NTP aktualisieren	Hiermit starten Sie eine sofortige Aktualisierung von Datum und Uhrzeit über den NTP-Server.

Sommerzeit.

Befehlsfolge: Konfiguration > Allgemein > Datum und Uhrzeit > Sommerzeit

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

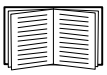
Beim Einstellen der Sommerzeit stellt das System die Uhr um eine Stunde vor, wenn die von Ihnen unter **Start** eingegebenen Einstellungen für Uhrzeit und Datum erreicht werden. Wenn die unter **Ende** eingegebenen Einstellungen erreicht werden, wird die Uhr um eine Stunde zurückgestellt.

- Wenn die lokale Sommerzeit beispielsweise immer am *vierten* Sonntag in einem bestimmten Monat beginnt oder endet, wählen Sie **Vierter/Letzter**. Wenn in diesen Monat ein fünfter Sonntag fällt, sollten Sie trotzdem **Vierter/Letzter** wählen.
- Wenn die lokale Sommerzeit immer am *letzten* Sonntag in einem bestimmten Monat beginnt oder endet, unabhängig davon, ob es sich dabei um den vierten oder fünften Sonntag handelt, wählen Sie **Fünfter/Letzter**.

Erstellen und Importieren von Einstellungen mit der Konfigurationsdatei

Befehlsfolge: Konfiguration > Allgemein > Benutzerkonfigurationsdatei

Sie können die Konfiguration neuer Geräte beschleunigen und vereinfachen, indem Sie die bestehenden Konfigurationseinstellungen mithilfe dieser Option wiederverwenden. Verwenden Sie **Hochladen**, um die Konfigurationsdaten an diese Schnittstelle zu übertragen, und **Herunterladen**, um sie von dieser Schnittstelle zu übertragen (und dann zur Konfiguration einer anderen Schnittstelle zu verwenden). Der Standardname der Datei lautet **config.ini**.



Eine Anleitung zum Abrufen und Anpassen der INI-Datei einer konfigurierten Netzwerkmanagement-Karte finden Sie unter „Export von Konfigurationseinstellungen“.

Bildschirm „Schnellverknüpfungen“

Befehlsfolge: Konfiguration > Allgemein > Schnellverknüpfungen

Verwenden Sie diese Option, um die URLs unten links auf jedem Bildschirm der Schnittstelle anzuzeigen und zu bearbeiten.

Um einen Link erneut zu konfigurieren, klicken Sie auf den Namen des Links in der Spalte **Name**. Sie können die Links auf die Standardeinstellungen zurücksetzen, indem Sie auf **Auf Standardwerte zurücksetzen** klicken.

Menü „Konfigurationsprotokolle“

Befehlsfolge: Konfiguration > Protokolle > Syslog > *Optionen*

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

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

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

Identifizierung von Syslog-Servern

Befehlsfolge: Konfiguration > Protokolle > Syslog > Server

Feld	Beschreibung
Syslog-Server	Diese Einstellung verwendet IPv4-/IPv6-Adressen oder Hostnamen, um maximal vier Server zu identifizieren, die Syslog-Nachrichten der Netzwerkmanagement-Karte empfangen sollen.
Port	Der UDP-Port, den die Netzwerkmanagement-Karte zum Senden von Syslog-Nachrichten verwendet. Die Voreinstellung lautet 514, was dem für Syslog reservierten UDP-Port entspricht.
Sprache	Wählen Sie die Sprache für etwaige Syslog-Nachrichten aus.
Protokoll	Wählen Sie zwischen UDP und TCP.

Syslog-Einstellungen

Befehlsfolge: Konfiguration > Protokolle > Syslog > Einstellungen

Feld	Beschreibung
Nachrichtengenerierung	Aktivieren Sie die Erstellung und damit die Protokollierung von Syslog-Mitteilungen für Ereignisse, in denen Syslog als Benachrichtigungsmethode konfiguriert ist. Siehe „Konfigurieren von Ereignisaktionen“.
Einrichtungscode	Hiermit wird der Anlagencode festgelegt, der den Syslog-Meldungen der Netzwerkmanagement-Karte zugeordnet wird (der Standardwert lautet **User**). Hinweis: Der Einrichtungscode **User** definiert die von der Netzwerkmanagement-Karte gesendeten Syslog-Nachrichten am besten. Ändern Sie diese Einstellung *nicht*, es sei denn, Sie werden vom Syslog-Netzwerk oder vom Systemadministrator dazu aufgefordert.

Feld	Beschreibung
Schweregradzuordnung	Hiermit ordnen Sie die verschiedenen Schweregrade von Netzwerkmanagement-Karten- oder Umgebungsereignissen den verfügbaren Syslog-Prioritäten zu. Die lokalen Optionen sind „Kritisch“, „Warnung“ und „Zur Information“. Diese Zuordnungen müssen normalerweise nicht geändert werden. Die folgenden Definitionen stammen aus RFC3164: • **Notfall**: Das System kann nicht mehr verwendet werden. • **Alarm**: Es muss umgehend eine entsprechende Maßnahme erfolgen. • **Kritisch**: Kritische Zustände. • **Fehler**: Fehlerzustände. • **Warnung**: Warnzustände. • **Hinweis**: Normale aber wichtige Zustände. • **Zur Information**: Meldungen für Informationszwecke. • **Debug**: Meldungen auf Debug-Ebene. Die Standardeinstellungen für die Priorität **Local Priority** lauten wie folgt: • **Schwerwiegend** ist **Kritische** zugeordnet. • **Warnung** ist **Warnung** zugeordnet. • **Zur Information** ist **Info** zugeordnet. Hinweis**:** Eine Anleitung zum Deaktivieren der Syslog-Nachrichten finden Sie unter „Konfigurieren von Ereignisaktionen“.

Beispiel für einen Syslog-Test und das Syslog-Format

Befehlsfolge: Protokolle > Syslog > Test

Senden Sie eine Testnachricht an die Syslog-Server (konfiguriert über die Option „Identifizierung von Syslog-Servern“ oben). Das Ergebnis wird an alle konfigurierten Syslog-Server versandt.

Wählen Sie den Schweregrad aus, der dieser Testnachricht zugewiesen werden soll, und definieren Sie anschließend die Testnachricht. Formatieren Sie die Meldung so, dass sie den Ereignistyp (z. B. APC, System oder Gerät) mit anschließendem Doppelpunkt, Leerzeichen und den Ereignistext umfasst. Die Meldung kann bis zu 50 Zeichen lang sein.

- Die Priorität (PRI): Die dem Nachrichtenereignis zugeordnete Syslog-Priorität und der Einrichtungscode der von der Netzwerkmanagement-Karte gesendeten Nachrichten.
- Der Header: Ein Zeiteintrag und die IP-Adresse der Netzwerkmanagement-Karte.
- Der Nachrichtenteil (MSG):
  - Das Feld TAG, gefolgt von einem Doppelpunkt und einem Leerzeichen, identifiziert den Ereignistyp.
  - Das Feld CONTENT enthält den Ereignistext, eventuell gefolgt von einem Leerzeichen und dem Ereigniscode.

  Beispiel: `APC: Test Syslog ist eine gültige Nachricht.`

Testmenü

Prüfung und Kalibrierung

Befehlsfolge: Tests > USV

Die folgenden Optionen sind nur für unterstützte Einphasen-Easy-UPS-Geräte mit installierter AP9544-Karte relevant.
Für den Zugriff auf diesen Bildschirm ist eine Lizenz erforderlich. Siehe „Lizenz“.

Bei einigen USV-Geräten können Sie einen Selbsttest, einen Alarmtontest oder eine Kalibrierung der Laufzeit Ihrer USV durchführen. In den Feldern **Selbsttest** und **Kalibrierung** werden die Ergebnisse der letzten Prüfung und Kalibrierung angezeigt.

Eine Kalibrierung der Laufzeit veranlasst die USV zu einer Neuberechnung der verfügbaren Laufzeit-Kapazität basierend auf ihrer aktuellen Last. Auf diese Weise wird die Präzision der gemeldeten Laufzeit gewährleistet. 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 USV-Last ohne Schwankungen mindestens 15 % betragen.

Vorsicht – Kalibrierungen der Laufzeit verursachen Tiefenentladungen der USV-Batterien. Infolgedessen besteht die Möglichkeit, dass eine USV im Falle eines Stromausfalls ihre angeschlossene Last vorübergehend nicht unterstützt.

Häufige Kalibrierungen reduzieren die Lebensdauer der Batterien.

Kalibrierungen können dann durchgeführt werden, wenn die von der USV unterstützte Last erheblich zunimmt.

Der Alarmtontest für eine USV ist gerätespezifisch und daher für Ihre USV möglicherweise nicht verfügbar. Informationen zum Aktivieren des Alarmtons finden Sie hier: Planung für das Herunterfahren.

- Wenn Sie **USV-Alarmtest** wählen, gibt die USV vier Sekunden lang einen Piepton aus und die LEDs leuchten auf.
- Wenn Sie **USV-Alarmtest - Daueralarm** wählen, gibt die USV einen Piepton aus und die LEDs leuchten so lange auf, bis Sie die Prüfung abbrechen. Auf dem Bildschirm wird eine separate Option namens **Daueralarmtest abbrechen** angezeigt. Wählen Sie diese Option, um den Test abzubrechen, und klicken Sie auf „Übernehmen“. Alternativ können Sie eine beliebige Taste auf der LED-Anzeige der USV drücken. Dieser Test eignet sich zur Ortung einer USV.

Einstellung der LEDs der Netzwerkmanagement-Karte auf Blinkbetrieb

Befehlsfolge: Tests > Netzwerk > Blinken der LED

Wenn Sie Probleme beim Auffinden Ihres USV-Geräts haben, geben Sie eine bestimmte Minutenzahl in das Feld **Blinken der LED, Dauer** ein, klicken Sie auf „Übernehmen“ und die LEDs Ihrer Netzwerkmanagement-Karte beginnen zu blinken. So können Sie das physische Gerät leichter finden.

„Protokolle“ Menü

Arbeiten mit Ereignis- und Datenprotokollen

Das Ereignisprotokoll erfasst individuelle Ereignisse. Das Datenprotokoll bietet Ihnen dagegen einen Snapshot Ihres Systems, indem regelmäßig Werte erfasst werden.

Ereignisprotokoll

Befehlsfolge: Protokolle > Ereignisse > *verfügbare Optionen*

Beim Basic-Funktionsumfang werden nur die letzten 25 Ereignisse im Ereignisprotokoll gespeichert. Um mehr Ereignisse zu speichern, ist eine Standard- oder Premium-Lizenz erforderlich. Siehe „Lizenz“.

Standardmäßig enthält das Protokoll alle Ereignisse, die während der letzten zwei Tage erfasst wurden, beginnend mit den aktuellsten Ereignissen. Siehe „Konfigurieren nach Ereignis“.

Zusätzlich, die Protokollsätze: i) Jedes Ereignis, das eine SNMP-Trap aussendet, außer fehlgeschlagene SNMP-Authentifizierungsversuche. ii) Abnormale interne Systemereignisse.

Sie können die Ereignis-Farbcodierung über „Lokale Benutzer“ im Menü „Konfiguration“ aktivieren.

Anzeigen des Ereignisprotokolls.

Befehlsfolge: Protokolle > Ereignisse > Protokoll

Standardmäßig werden im Ereignisprotokoll die aktuellsten Ereignisse zuerst angezeigt. Um die Ereignisse auf einer Webseite zusammengefasst anzuzeigen, klicken Sie auf die Schaltfläche **Protokoll in neuem Fenster** öffnen. Dazu muss JavaScript in Ihrem Browser aktiviert sein.

Um das Protokoll in einer Textdatei zu öffnen oder auf einem Datenträger zu speichern, klicken Sie auf das Datenträgersymbol in der gleichen Zeile wie die Überschrift **Ereignisprotokoll**.

Sie können das Ereignisprotokoll auch über Secure CoPy (SCP) oder FTP abrufen. Siehe „Abrufen von Protokolldateien über SCP oder FTP“.

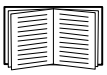
Filtern des Ereignisprotokolls. Verwenden Sie die Filterfunktion, um Informationen, die Sie nicht anzeigen möchten, auszublenden.

Filtern des Ereignisprotokolls nach Datum oder Uhrzeit	Verwenden Sie die Optionsschaltflächen **Letzte** oder **Von**. (Die Filterkonfiguration bleibt gespeichert, bis die Netzwerkmanagement-Karte neu gestartet wird.)
Filtern des Protokolls nach Schweregrad oder Kategorie des Ereignisses	Klicken Sie auf **Protokoll filtern**. Deaktivieren Sie ein Kontrollkästchen, um es aus der Ansicht zu entfernen. Nachdem Sie auf **Übernehmen** geklickt haben, gibt Text in der rechten oberen Ecke des Ereignisprotokolls an, dass ein Filter aktiv ist. Der Filter ist aktiv, bis Sie ihn löschen oder die Netzwerkmanagement-Karte neu gestartet wird. Wenn Sie einen aktiven Filter entfernen möchten, klicken Sie auf **Protokoll filtern** und anschließend auf **Filter löschen (Alle zeigen)**. Wenn Sie als Administrator angemeldet sind, klicken Sie auf **Als Standard speichern**, um diesen Filter als Protokoll-Standardansicht für alle Benutzer zu speichern.

Wichtige Hinweise zur Filterfunktion:

- Zum Filtern von Ereignissen wird eine ODER-Logik angewandt. Wenn Sie einen Filter anwenden, funktioniert er unabhängig von den anderen Filtern.
- Ereignisse, die Sie nicht in der Liste **Nach Schweregrad filtern** ausgewählt haben, werden niemals im gefilterten Ereignisprotokoll angezeigt, selbst wenn diese in der Liste **Nach Kategorie filtern** ausgewählt wurden.
- Dementsprechend werden auch Ereignisse, die Sie nicht in der Liste **Nach Kategorie filtern** ausgewählt haben, niemals im gefilterten Ereignisprotokoll angezeigt.

Löschen des Ereignisprotokolls. Um alle Ereignisse zu löschen, klicken Sie auf **Protokoll löschen**. Gelöschte Ereignisse können nicht abgerufen werden.



Eine Anleitung zum Deaktivieren der Protokollierung von Ereignissen auf der Basis ihres Schweregrads oder ihrer Ereigniskategorie finden Sie unter „Konfiguration nach Ereignisgruppen“.

Konfigurieren der umgekehrten Suche:

Befehlsfolge: Protokolle > Ereignisse > Reverse Lookup

Wenn die Option „Reverse Lookup“ aktiviert ist, werden beim Eintreten eines Netzwerk-Ereignisses die IP-Adresse *und* der Domänenname der für das Ereignis relevanten Netzwerkeinheit im Ereignisprotokoll erfasst. Wenn kein Domänenname für die Einheit vorhanden ist, wird nur ihre IP-Adresse zusammen mit dem Ereignis protokolliert.

Da sich Domänennamen im Allgemeinen weniger oft ändern als IP-Adressen, lassen sich die Adressen von Netzwerkeinheiten, die entsprechende Ereignisse auslösen, bei aktivierter umgekehrter Suche häufig leichter identifizieren.

Umgekehrte Suchen sind in der Grundeinstellung deaktiviert. Sie müssen diese Funktion normalerweise nicht aktivieren, wenn Sie keinen DNS-Server konfiguriert haben oder wenn das Netzwerk aufgrund zu starken Datenverkehrs eine schlechte Leistung aufweist.

Ändern der Größe des Ereignisprotokolls.

Befehlsfolge: Protokolle > Ereignisse > Größe

Verwenden Sie die Option „Ereignisprotokollgröße“, um die maximale Anzahl von Protokolleinträgen festzulegen.

Vorsicht: Wenn Sie die Größe des Ereignisprotokolls ändern, um eine Maximalgröße anzugeben, *werden alle bestehenden Protokolleinträge gelöscht*. Um den Verlust von Protokolldaten zu vermeiden, verwenden Sie SCP oder FTP, um zuerst das Protokoll abzurufen. Siehe „Abrufen von Protokolldateien über SCP oder FTP“. Wenn das Protokoll anschließend die Maximalgröße erreicht, werden die älteren Einträge gelöscht.

Datenprotokoll

Befehlsfolge: Protokolle > Daten > *Optionen*

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

Verwenden Sie das Datenprotokoll, um Messwerte zur USV, zur Leistungsaufnahme der USV sowie zu deren Umgebungstemperatur und Batterien anzuzeigen.

Die Schritte zum Anzeigen und Ändern der Größe des Datenprotokolls sind dieselben wie beim Ereignisprotokoll, allerdings müssen Sie die Menüoptionen unter **Daten** anstelle von **Ereignisse** verwenden. Siehe „Anzeigen des Ereignisprotokolls“ und „Ändern der Größe des Ereignisprotokolls“.

Zum Filtern des Datenprotokolls nach Datum oder Uhrzeit verwenden Sie die Optionsschaltflächen **Letzte** oder **Von**. (Die Filterkonfiguration bleibt gespeichert, bis die Netzwerkmanagement-Karte neu gestartet wird.) Um alle im Datenprotokoll aufgezeichneten Daten zu löschen, klicken Sie auf **Datenprotokoll löschen**. Gelöschte Daten können nicht abgerufen werden.

Festlegen des Intervalls für die Erfassung der Daten (Protokolle > Daten > Intervall): Legen Sie über die Einstellung **Protokollintervall** fest, in welchem Abstand nach Daten gesucht wird und diese im Datenprotokoll gespeichert werden. Wenn Sie auf „Übernehmen“ klicken, wird die Anzahl der möglichen Speichertage berechnet und im oberen Bildschirmbereich angezeigt.

Wenn das Protokoll voll ist, werden die ältesten Einträge gelöscht. Um zu vermeiden, dass ältere Daten automatisch gelöscht werden, lesen Sie „Konfigurieren der Datenprotokollrotation (Protokolle > Daten > Rotation):“ direkt im Anschluss.

Hinweis: Da durch das Intervall festgelegt wird, wie oft die Daten erfasst werden, gilt: *Je kürzer das Intervall*, desto öfter werden Daten erfasst und desto größer wird die Protokolldatei.

Konfigurieren der Datenprotokollrotation (Protokolle > Daten > Rotation): Bei der Rotation wird der Inhalt des Datenprotokolls an eine Datei angehängt, deren Name und Speicherort von Ihnen festgelegt wird. Das heißt, Sie können die Daten speichern, bevor sie gelöscht werden (siehe „Festlegen des Intervalls für die Erfassung der Daten (Protokolle > Daten > Intervall):“ weiter oben).

Verwenden Sie diese Option, um den Kennwortschutz und andere Parameter einzurichten.

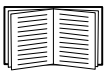
Feld	Beschreibung
FTP-Server	Die IP-Adresse oder der Hostname des Servers, auf dem sich die Datei befindet.
Benutzername **Kennwort**	Der Benutzername und das Kennwort, das zum Senden von Daten an die Archivdatei benötigt wird. Dieser Benutzer muss außerdem Lese- und Schreibzugriff auf die Archivdatei und den Ordner haben, in dem diese gespeichert werden soll.
Dateipfad	Der Pfad zur Archivdatei.
Dateiname	Der Name der Archivdatei (eine ASCII-Textdatei), zum Beispiel `datenprotokoll.txt`. Alle neuen Daten werden in diese Datei übernommen. Es werden keine Daten überschrieben.
Eindeutiger Dateiname	Aktivieren Sie dieses Kontrollkästchen, um das Protokoll als `mmttjjjj_<Dateiname>.txt` zu speichern, wobei „Dateiname“ für den Eintrag im obigen Feld **Dateiname** steht. Neue Daten werden in der Datei angefügt, doch es wird für jeden Tag eine eigene Datei erstellt.
Verzögerung *n* Stunden zwischen Hochladevorgängen.	Der Abstand in Stunden, in dem Daten in die Datei übertragen werden (max. 24 Stunden).
Wiederholung bei Fehler alle *n* Minuten	Die Zeit in Minuten, die nach einer fehlgeschlagenen Datenübertragung abgewartet wird, bevor erneut versucht wird, die Daten in die Datei zu schreiben.
Bis zu *n*-mal	Wie oft die Übertragung wiederholt wird, nachdem ein Übertragungsfehler erstmals eingetreten ist.
bis Hochladevorgang erfolgreich ist	Mit dieser Option wird versucht, die Daten immer wieder hochzuladen, bis die Übertragung erfolgreich verläuft.

Abrufen von Protokolldateien über SCP oder FTP

Administratoren und Gerätebenutzer können eine Ereignisprotokolldatei (*event.txt*) bzw. Datenprotokolldatei (*data.txt*) mit Tabulatortrennung per SCP oder FTP abrufen und in eine Tabelle importieren. Beide befinden sich auf der Netzwerkmanagement-Karte.

- Diese Datei enthält alle Ereignisse oder Datenelemente, die seit dem letzten Löschen oder Abkürzen der Datei bei Überschreitung ihrer Maximalgröße erfasst wurden.
- Diese Datei enthält Informationen, die im Ereignisprotokoll oder im Datenprotokoll nicht angezeigt werden.
  - Die AOS- und Anwendungsversion der Netzwerkmanagement-Karte
  - Datum und Uhrzeit des erstmaligen Abrufs der Datei
  - Den **Namen**, den **Ansprechpartner** und den **Standort** sowie die IP-Adresse der Netzwerkmanagement-Karte
  - Die Modellbezeichnung der USV (nur in der Datei *data.txt*)
  - Den eindeutigen **Ereigniscode** zu jedem erfassten Ereignis (nur in der Datei *event.txt*)
  - Die Netzwerkmanagement-Karte verwendet vierstellige Jahresangaben für Protokolleinträge. Unter Umständen müssen Sie in Ihrem Tabellenkalkulationsprogramm das Datumsformat auf vier Ziffern einstellen, damit das Datum vollständig angezeigt wird.

Wenn Sie die verschlüsselten Sicherheitsprotokolle verwenden, beachten Sie die Informationen unter „So rufen Sie Dateien mit SCP ab.“. Wenn Sie unverschlüsselte Authentifizierungsmethoden verwenden, beachten Sie die Informationen unter „Abrufen der Dateien mithilfe von FTP“.



Informationen zu den verfügbaren Protokollen und Methoden zur Einrichtung des benötigten Sicherheitstyps finden Sie im ***Sicherheitshandbuch*** auf der **APC-Website**.

So rufen Sie Dateien mit SCP ab. Aktivieren Sie SSH auf der Netzwerkmanagement-Karte, siehe „Konsolenzugriff“. **Hinweis:** Die nachstehenden Befehle sind lediglich Beispiele.

Zum Abrufen der Datei *„event.txt“* verwenden Sie den folgenden Befehl:

```
scp <benutzername@hostname> oder <ip-adresse>:event.txt ./event.txt
```

Zum Abrufen der Datei *„data.txt“* verwenden Sie den folgenden Befehl:

```
scp <benutzername@hostname> oder <ip-adresse>:data.txt ./data.txt
```

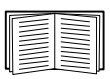
Abrufen der Dateien mithilfe von FTP. So rufen Sie die Datei *event.txt* oder *data.txt* per FTP ab:

1. Geben Sie in einer Befehlszeile `ftp` und die IP-Adresse der Netzwerkmanagement-Karte ein und drücken Sie die EINGABETASTE.

   Falls sich die **Port**-Einstellung des **FTP-Servers** geändert hat (siehe „FTP-Server“) und nicht mehr der Standardeinstellung `21` entspricht, müssen Sie im FTP-Befehl den von der Standardeinstellung abweichenden Wert verwenden.

   Verwenden Sie bei Windows FTP-Clients den nachfolgenden Befehl einschließlich der Leerzeichen. (Bei einigen FTP-Clients müssen Sie zwischen der IP-Adresse und der Port-Nummer einen Doppelpunkt statt eines Leerzeichens setzen.)

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

   Für Informationen zur Festlegung eines nicht standardmäßigen Werts zur Optimierung der Sicherheit für den FTP-Server siehe „FTP-Server“. Sie können einen beliebigen Port

zwischen 5001 und 32768 angeben.

2. Als Administrator oder Benutzer „Gerät“ müssen Sie sich unter Beachtung der Groß- und Kleinschreibung mit Ihrem **Benutzernamen** und Ihrem **Kennwort** anmelden. Für Administratoren ist standardmäßig „apc“ als Benutzername vorgegeben. Für den Gerätebenutzer lautet der Standardbenutzername „device“.
3. Geben Sie Folgendes ein, um den Dateiübertragungsmodus auf binär zu setzen:

   ```
   ftp>bin
   ```

   Geben Sie Folgendes ein, um einen Fortschrittsbalken während der Dateiübertragung anzuzeigen:

   ```
   ftp>hash
   ```
4. Verwenden Sie den Befehl `get`, um den Text aus einem Protokoll auf die lokale Festplatte zu übertragen.

   ```
   ftp>get event.txt
   ```

   oder

   ```
   ftp>get data.txt
   ```
5. Mit dem Befehl `del` können Sie beide Protokolle löschen.

   ```
   ftp>del event.txt
   ```

   oder

   ```
   ftp>del data.txt
   ```

   Der Löschvorgang erfolgt ohne Rückfrage und Bestätigung.

   – Wenn Sie das Datenprotokoll löschen, wird dieses Ereignis im Ereignisprotokoll erfasst.
   – Wenn Sie das Ereignisprotokoll löschen, wird dieses Ereignis in der neu angelegten Datei *event.txt* erfasst.
6. Geben Sie den Befehl `quit` hinter der Eingabeaufforderung `ftp>` ein, um FTP zu verlassen.

USV-Protokolle

Befehlsfolge: Protokolle > USV

Diese Menüoption ist nicht bei allen USV-Geräten verfügbar.

Diese Informationen werden Ihrem USV-Gerät entnommen und sind getrennt von den Protokollen Ihrer Netztwerkmanagement-Karte zu betrachten. (Sie stehen nicht in direktem Zusammenhang mit der Netzwerkmanagement-Karte oder einem Teil der Netzwerkmanagement-Karte „Ereignisprotokoll“.)

Die Informationen können dem technischen Supportteam bei der Lösung von Problemen helfen.

USV-Übertragungsprotokolle Zeigt eine Tabelle mit den von der USV gespeicherten Übertragungsereignissen an, einschließlich Übertragungen zur Batterie und Übertragungen zum Bypass-Betrieb.

USV-Fehlerprotokolle Zeigt eine Tabelle mit den von der USV gespeicherten Fehlern an.

Firewall-Protokoll

Befehlsfolge: Protokolle > Firewall

Wenn Sie eine Firewall-Richtlinie erstellen, werden Firewall-Ereignisse hier erfasst. Weitere Informationen zum Umsetzen einer Richtlinie finden Sie unter „Firewall-Bildschirm“.

Die Informationen können dem technischen Support-Team bei der Lösung von Problemen helfen.

Protokolleinträge können Informationen über den Datenverkehr und die laut Regel definierte Aktion (erlaubt, verworfen) enthalten. Wenn diese Ereignisse hier erfasst werden, werden sie nicht im Haupt-Ereignisprotokoll erfasst. Siehe „Ereignisprotokoll“.

Ein Firewall-Protokoll enthält bis zu 50 der aktuellsten Ereignisse. Das Firewall-Protokoll wird beim Neustart der Netzwerkmanagement-Karte gelöscht.

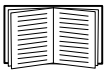
Lizenz

Einführung

Übersicht

Die AP9544- und AP9547-Netzwerkmanagement-Karten sind lizenzierte Produkte. Es stehen drei Lizenzstufen zur Wahl:

- **„Basic“** ist kostenlos und bietet begrenzte Funktionen.
- **Standard** bietet alle Funktionen mit Ausnahme der unternehmensweiten Integration.
- **Premium** bietet den vollen Funktionsumfang.



Weitere Informationen zu den Funktionen, die in den einzelnen Lizenzstufen enthalten sind, finden Sie im **Funktionsübersichtsdokument** zu Netzwerkmanagement-Karten für Easy-UPS-Geräte, das auf der APC-Website verfügbar ist.

Häufig gestellte Fragen zu Lizenzen finden Sie im **Lizenz-FAQ-Dokument** zu Netzwerkmanagement-Karten für Easy-UPS-Geräte auf der APC-Website.

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.

Erwerben einer Lizenz

Eine NMC-Lizenz kann über Schneider Electric Exchange oder über Ihren Schneider Electric IT-Partner erworben werden. Ausführliche Informationen zum Kauf einer Lizenz über Schneider Electric Exchange finden Sie im Network Management Card für Easy UPS Lizenz FAQ-Dokument auf der APC-Website.

Menü „Lizenz“

Befehlsfolge: Lizenz

Lizenzinformationen

Feld	Beschreibung
Lizenztyp	Der aktivierte Lizenztyp: **Basic**, **Standard** oder **Premium**.
Ablaufdatum der Lizenz	Das Datum, an dem Ihre aktuelle Lizenz abläuft. HINWEIS: Die Basic-Lizenz läuft nicht ab.
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. Eine Aktivierungs-ID kann für mehrere Netzwerkmanagement-Karten erworben werden. Sie können sich im **Lizenzportal** anmelden, um zu sehen, wie viele Lizenzen aktiviert wurden: 1. Melden Sie sich mit Ihrer **Aktivierungs-ID** an. 2. Gehen Sie zu **Activation & Entitlements > List Entitlements** (Aktivierung und Berechtigungen > Liste der Berechtigungen). 3. Hier finden Sie die Gesamtanzahl, die verfügbare Anzahl und das Ablaufdatum der mit Ihrer Aktivierungs-ID verknüpften Lizenzen.
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.
Erinnerung an den Ablauf der Lizenz	Aktivieren Sie dieses Kontrollkästchen, um lizenzbezogene Benachrichtigungen in der Web-Benutzeroberfläche zu deaktivieren. HIM**HINWEIS:** Lizenzbezogene Ereignisse werden weiterhin im Ereignisprotokoll protokolliert.

Lizenzaktivierung/-deaktivierung

Aktivierung

Vergewissern Sie sich, dass eine Aktivierungs-ID bereitgestellt wurde, bevor Sie versuchen, Ihre Lizenz zu aktivieren.

Sie können Ihre Netzwerkmanagement-Kartenlizenz **online** aktivieren, wenn die Karte direkten Internetzugang hat, oder **offline**, wenn sie keinen Internetzugang hat. Bei Aktivierung der Lizenz wird ein Ereignis im Ereignisprotokoll erfasst.

Online-Aktivierung

Klicken Sie auf **Activate** (Aktivieren), um zum Bildschirm Confirm License Activation (Lizenzaktivierung bestätigen) zu gelangen. Überprüfen Sie, ob Datum und Uhrzeit des Systems korrekt sind, und klicken Sie auf **Apply** (Anwenden). Das Datum und die Uhrzeit müssen korrekt sein, damit die Lizenz korrekt funktioniert. Sind das angezeigte Datum und die Uhrzeit nicht korrekt, klicken Sie auf **Update** (Aktualisieren), um die Einstellungen zu aktualisieren, bevor Sie fortfahren.

Wenn unter **Configuration > Network > DNS > Configuration** (Konfiguration > Netzwerk > DNS > Konfiguration) kein gültiger DNS-Eintrag für die Netzwerkmanagement-Karte vorhanden ist, kann die Aktivierung nicht durchgeführt werden. Siehe Bildschirm „DNS“.

Um die Lizenzänderungen zu übernehmen, müssen Sie die Netzwerkmanagement-Karte neu starten. Der Neustart erfolgt automatisch, wenn Sie sich von der Benutzeroberfläche abmelden. Alternativ kann er über **Control > Network > Reset/Reboot > Reboot Management Interface** (Steuerung > Netzwerk > Zurücksetzen/Neustart > Verwaltungsschnittstelle neu starten) ausgelöst werden. Weitere Informationen finden Sie unter „Netzwerk“ im Menü „Steuerung“.

Offline-Aktivierung

1. Klicken Sie auf **Obtain License Request File** (Lizenzanforderungsdatei abrufen), um eine `capabilityRequest.bin`-Datei zu erzeugen. Die erzeugte Datei finden Sie in Ihrem Downloads-Ordner.
2. So rufen Sie die Datei `capabilityResponse.bin` ab:
   a. **Option A:** Wenn Ihr Browser über einen direkten Internetzugang verfügt, klicken Sie auf den Link, um das **Lizenzportal** zu öffnen. Melden Sie sich mit Ihrer **Aktivierungs-ID** an und gehen Sie zu **Devices > Offline Device Management** (Geräte > Offline-Geräteverwaltung). Laden Sie die im ersten Schritt erzeugte `capabilityRequest.bin`-Datei aus dem Downloads-Ordner hoch und die Datei `capabilityResponse.bin` herunter.
   b. **Option B:** Wenn Ihr Browser keinen direkten Internetzugang hat, übertragen Sie die Datei `capabilityRequest.bin` aus Ihrem Downloads-Ordner auf einen anderen Computer, der direkten Internetzugang hat, z. B. mithilfe eines USB-Sticks. Rufen Sie am Computer mit Internetzugang das **Lizenzportal** auf. Melden Sie sich mit Ihrer **Aktivierungs-ID** an und gehen Sie zu **Devices > Offline Device Management** (Geräte > Offline-Geräteverwaltung). Laden Sie die `capabilityRequest.bin`-Datei hoch (z. B. vom USB-Stick) und die Datei `capabilityResponse.bin` herunter. Verschieben Sie diese `capabilityResponse.bin`-Datei zurück in den Browser, der mit der Netzwerkmanagement-Karte verbunden ist, (z. B. vom USB-Stick) und speichern Sie sie im Downloads-Ordner.
3. Klicken Sie auf **Choose File** (Datei auswählen) und wählen Sie die im zweiten Schritt abgerufene `capabilityResponse.bin`-Datei aus. Klicken Sie anschließend auf **Upload License File** (Lizenzdatei hochladen). Dadurch wird die `capabilityResponse.bin`-Datei an die Netzwerkmanagement-Karte gesendet und die Lizenz aktiviert.

Wenn die Datei `capabilityResponse.bin` geändert oder beim Herunterladen beschädigt wird, ist sie ungültig und die Lizenz kann nicht aktiviert werden. Erscheint in der Web-Benutzeroberfläche eine Fehlermeldung mit Verweis auf die „Capability Response“, wiederholen Sie die vorgenannten Schritte, um eine neue `capabilityResponse.bin`-Datei zu erzeugen und herunterzuladen.

Die Dateien `capabilityRequest.bin` und `capabilityResponse.bin` enthalten Ihre Lizenzinformationen. Wir empfehlen, diese Dateien an einem sicheren Ort zu speichern und sie zu löschen, wenn sie im Lizenzaktivierungsprozess nicht mehr benötigt werden.

Um die Lizenzänderungen zu übernehmen, müssen Sie die Netzwerkmanagement-Karte neu starten. Der Neustart erfolgt automatisch, wenn Sie sich von der Benutzeroberfläche abmelden. Alternativ kann er über **Control > Network > Reset/Reboot > Reboot Management Interface** (Steuerung > Netzwerk > Zurücksetzen/Neustart > Verwaltungsschnittstelle neu starten) ausgelöst werden. Weitere Informationen finden Sie unter „Netzwerk“ im Menü „Steuerung“.

Online-Deaktivierung

Klicken Sie auf **Deactivate** (Deaktivieren), um die verwendete Netzwerkmanagement-Kartenlizenz an den Lizenzserver zurückzugeben. So können Sie diese Lizenz für eine ähnliche Karte wiederverwenden. Klicken Sie auf **Apply** (Anwenden), um zum Bildschirm **Remove License Confirmation** (Lizenzbestätigung entfernen) zu gelangen, und klicken Sie zur Bestätigung auf **Apply**. Bei Deaktivierung der Lizenz wird ein Ereignis im Ereignisprotokoll erfasst.

Um die Lizenzänderungen zu übernehmen, müssen Sie die Netzwerkmanagement-Karte neu starten. Der Neustart erfolgt automatisch, wenn Sie sich von der Benutzeroberfläche abmelden. Alternativ kann er über **Control > Network > Reset/Reboot > Reboot Management Interface** (Steuerung > Netzwerk > Zurücksetzen/Neustart > Verwaltungsschnittstelle neu starten) ausgelöst werden. Weitere Informationen finden Sie unter „Netzwerk“ im Menü „Steuerung“.

Die Lizenzrückgabe wird nicht unterstützt, wenn Sie Ihre Lizenz **offline** aktiviert haben. Wenn Sie Lizenzen für Netzwerkmanagement-Karten ohne direkten Internetzugang wiederverwenden möchten, wenden Sie sich an den **technischen Support**.

Lizenz verlängern

Ihre Netzwerkmanagement-Kartenlizenz läuft an dem angezeigten **Lizenzablaufdatum** ab. Sie können Ihre Lizenz über Schneider Electric Exchange *bis zu* diesem **Ablaufdatum** verlängern. Ausführliche Informationen zur Verlängerung Ihrer Lizenz in Schneider Electric Exchange finden Sie im Network Management Card für Easy UPS License FAQ-Dokument auf der APC-Website.

Sie können nach Ablauf Ihrer Lizenz noch 30 Tage lang auf die in Ihrer Lizenz enthaltenen Funktionen der Netzwerkmanagement-Karte zugreifen. Dazu gehören etwa SNMP. **HINWEIS:** Sie können Ihre Lizenz *nicht* mehr verlängern, wenn sie abgelaufen ist. Siehe „Abgelaufene Lizenz“.

Die Netzwerkmanagement-Karte benachrichtigt Sie 60 Tage im Voraus, ehe Ihre Lizenz abläuft. Ein Ereignis wird im Ereignisprotokoll erfasst und alle E-Mail-Empfänger, die unter **Konfiguration > Benachrichtigung > E-Mail-Empfänger** eingetragen sind, erhalten eine E-Mail. Siehe „E-Mail-Empfänger“. Zudem werden 30 Tage vor Lizenzablauf, am Ablaufdatum und zum Ende der 30-tägigen Nachfrist E-Mails versendet und Ereignisse protokolliert.

Abgelaufene Lizenz

Sie können nach Ablauf Ihrer Lizenz noch 30 Tage lang auf die Funktionen der Netzwerkmanagement-Karte zugreifen und eine neue Lizenz erwerben. Wenn Sie während dieser Nachfrist keine Lizenz erwerben, werden Sie standardmäßig auf eine Basislizenz zurückgestuft. Siehe „Erwerben einer Lizenz“.

HINWEIS: Vorgenommene Einstellungen für lizenzierte Funktionen, wie SNMP, bleiben erhalten, bis eine neue Lizenz erworben und aktiviert wird.

Menü „Info“

Info zur Netzwerkmanagement-Karte

Wissenswertes zum USV-Gerät

Befehlsfolge: Info > USV

Die unter der USV angezeigten Informationen variieren je nach verwendetem Gerät.

Feld	Beschreibung
Produktname	Der Name der USV-Produktreihe.
Modell	Ihr USV-Gerät wird über diese Felder identifiziert.
Seriennummer	Die eindeutige Seriennummer der USV. Diese steht auch auf der Außenseite der USV.
Herstellungsdatum	Das Datum, an dem Ihre USV hergestellt wurde.
Firmwareversion	Die Versionsnummern der zurzeit in der USV installierten Firmware-Module.
Name des Herstellers	Der Hersteller der USV.
Nennscheinleistung	Die Nennscheinleistung der USV in VA.
Nenneingangsspannung	Die Nenneingangsspannung der USV in VAC.
Nennausgangsspannung	Die Nennausgangsspannung der USV in VAC.
Nennausgangsfrequenz	Die Nennfrequenz der Ausgangsspannung der USV in Hz.
Nennausgangsstrom	Der Nennausgangsstrom der USV in A.
Batterie-Nennspannung	Die Nennspannung der USV-Batterie in VDC.
Eingangsphasen	Die Anzahl der Eingangsphasen der USV.
Ausgangsphasen	Die Anzahl der Ausgangsphasen der USV.

In der Tabelle **Infos zu USV-Batteriemodulen** sind die Firmware-Version, das Modell, die Seriennummer und das Herstellungsdatum der USV-Batteriemodule aufgeführt.

Info zur Netzwerkmanagement-Karte und den Firmware-Modulen

Befehlsfolge: Info > Netzwerk

Hardware-Hersteller: Diese Hardware-Informationen sind bei der Behebung von Fehlern mit Ihrer Netzwerkmanagement-Karte nützlich.

Verfügbare Verwaltungszeit gibt an, wie lange diese Management-Schnittstelle ohne Unterbrechung lief, d. h. die Zeit seit dem letzten Warm- oder Kaltstart der Netzwerkmanagement-Karte.

Anwendungsmodul, **APC OS (AOS)** und **Boot-Monitor**: Diese Informationen sind nützlich, um Fehler zu beheben und herauszufinden, ob eine Firmware-Aktualisierung verfügbar ist (www.apc.com/shop/us/en/tools/software-firmware).

Feldbeschriftung	Beschreibung
Name	Der Name des Firmware-Moduls Der Name des **Anwendungsmoduls** variiert je nach USV-Gerätetyps„**su**“ gilt z. B. für Smart-UPS-Geräte, „**sy**“ für Symmetra-Geräte. Das **APC AOS-Modul** heißt stets **aos** und das **Boot-Monitor-Modul** heißt stets boot.
Version	Die Versionsnummer des Firmware-Moduls. Die Versionsnummern der Module können variieren, doch kompatible Module werden zusammen veröffentlicht. Siehe “Aktualisierung der Firmware”.
Datum / Zeit	Herstellungsdatum und -zeit des Firmware-Moduls.

Siehe auch “Überprüfen der Versionsnummern der installierten Firmware”.

Support-Bildschirm

Befehlsfolge: Info > Support

Mit dieser Option können Sie verschiedene Daten in dieser Schnittstelle in einer einzelnen ZIP-Datei zur Fehlerbehebung und für den Kundendienst zusammenfassen. Die Daten beinhalten die Ereignis- und Datenprotokolle, die Konfigurationsdatei (siehe “Erstellen und Importieren von Einstellungen mit der Konfigurationsdatei”) und komplexe Debugging-Informationen.

Klicken Sie auf **Protokolle erstellen**, um die Datei zu erstellen, und klicken Sie dann auf **Herunterladen**. Sie werden gefragt, ob Sie die ZIP-Datei öffnen oder speichern möchten.

Assistent für die Konfiguration von Geräte-IP-Adressen

Möglichkeiten, Anforderungen und Installation

Der Assistent für die Konfiguration von Geräte-IP-Adressen kann Netzwerkkarten ohne zugewiesene IP-Adresse erkennen. Sobald diese erkannt wurden, können Sie die IP-Adresseneinstellungen für die Karten konfigurieren.

Sie können außerdem nach bereits im Netzwerk vorhandenen Geräten suchen, indem Sie einen IP-Bereich für Ihre Suche eingeben. Der Assistent durchsucht die IP-Adressen in dem definierten Bereich und zeigt Netzwerkkarten an, die bereits über eine von DHCP zugewiesene IP-Adresse verfügen.

HINWEISE:

• Sie können nicht nach zugewiesenen Geräten suchen, die sich bereits im Netzwerk befinden, indem Sie einen IP-Bereich verwenden, es sei denn, Sie aktivieren auf der NMC SNMPv1 und legen den Community-Name auf „öffentlich“ fest. Weitere Informationen finden Sie unter „SNMP-Bildschirme“.

• Wenn die NMC-IP-Adresse konfiguriert ist, müssen Sie die URL von http auf https aktualisieren, um auf die NMC-Webbenutzeroberfläche in einem Browser zuzugreifen.

Detaillierte Informationen über der Assistent finden Sie in der Knowledge Base auf der Support-Seite der Website www.apc.com. Suchen Sie dort nach FA156064 (ID des entsprechenden Artikels).

Knowledge Base-Artikel **FA156064** enthält auch Informationen über die Verwendung der DHCP-Option 12 (AOS 5.1.5 und höher).

Systemanforderungen

Der Assistent kann auf den Betriebssystemen Windows Server® 2012, Windows Server 2016, Windows Server 2019 und auf der 32-Bit- und 64-Bit-Version von Windows 8.1 und Windows 10 ausgeführt werden.

Der Assistent unterstützt Karten mit der Firmwareversion 3.0.x oder höher und wurde nur für IPv4 konzipiert.

Installation

So installieren Sie den Assistenten von einer heruntergeladenen EXE-Datei:

1. Gehen Sie zu **www.apc.com/shop/tools/software-firmware**.
2. Filtern Sie nach Software/Firmware> Wizards and Configurators.
3. Laden Sie den Assistent für die Konfiguration von Geräte-IP-Adressen herunter.
4. Doppelklicken Sie im Zielordner des Downloads auf die ausführbare Datei.

Nach der Installation ist der Assistent über die Menüoptionen von Windows verfügbar.

Export von Konfigurationseinstellungen

Abrufen und Exportieren der INI-Datei

Das Verfahren im Überblick

Ein Administrator kann die INI-Dateien einer Netzwerkmanagement-Karte abrufen und an beliebig viele andere Netzwerkmanagement-Karten exportieren.

1. Konfigurieren Sie eine Netzwerkmanagement-Karte mit den gewünschten Einstellungen und exportieren Sie diese (siehe „Erstellen und Importieren von Einstellungen mit der Konfigurationsdatei“).
2. Rufen Sie die INI-Dateien aus dieser Netzwerkmanagement-Karte ab.
3. Passen Sie die Datei an, indem Sie mindestens die TCP/IP-Einstellungen ändern.
4. Verwenden Sie ein von der Netzwerkmanagement-Karte unterstütztes Dateiübertragungsprotokoll, um eine Kopie auf eine oder mehrere Netzwerkmanagement-Karten zu übertragen. Verwenden Sie für eine Übertragung auf mehrere Netzwerkmanagement-Karten ein FTP- oder SCP-Skript oder das Dienstprogramm für INI-Dateien.

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

Inhalt der INI-Datei

Die von einer Netzwerkmanagement-Karte abrufbare Datei config.ini enthält folgende Daten:

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

Ausführliche Verfahrensbeschreibungen

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

1. Verwenden Sie nach Möglichkeit die Schnittstelle einer Netzwerkmanagement-Karte, um auf dieser die Einstellungen zu konfigurieren, die exportiert werden sollen. (Eine direkte Bearbeitung der INI-Datei birgt immer ein gewisses Fehlerrisiko.)
2. Das nachfolgende Beispiel zeigt, wie die Datei „config.ini“ per FTP von der konfigurierten Netzwerkmanagement-Karte mit der Eingabeaufforderung eines Clients abgerufen wird:
   a. Öffnen Sie eine Verbindung zur Netzwerkmanagement-Karte, indem Sie deren IP-Adresse eingeben:

      ```
      ftp> ip_address
      ```

   b. Melden Sie sich mit einem entsprechenden Benutzernamen und Kennwort als Administrator an.
   c. Geben Sie Folgendes ein, um den Dateiübertragungsmodus auf binär zu setzen:

      ```
      ftp> bin
      ```

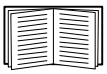
      Geben Sie Folgendes ein, um einen Fortschrittsbalken während der Dateiübertragung anzuzeigen:

```
ftp> hash
```

d. Rufen Sie die Datei „config.ini“ mit den Einstellungen der Netzwerkmanagement-Karte ab:

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

Die Datei wird in dem Ordner gespeichert, von dem Sie den FTP-Client gestartet haben.



Wenn Sie Konfigurationseinstellungen von mehreren Netzwerkmanagement-Karten abrufen und an andere Netzwerkmanagement-Karten exportieren möchten, lesen sie die *Versionshinweise: Dienstprogramm für .ini-Dateien* auf der **APC website** oder beziehen Sie sich auf den Knowledge Base-Artikel **FA156117** auf **http://www.apc.com/support**.

Anpassen. Sie müssen die Datei anpassen, bevor Sie sie auf eine andere Netzwerkmanagement-Karte übertragen können.

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

   ```
   NTPEnable=enabled
   ```

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

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

- Wählen Sie über die Benutzeroberfläche der empfangenden Netzwerkmanagement-Karte die Option **Konfiguration** - **Allgemein** - **Benutzerkonfigurationsdatei** aus. Geben Sie den vollständigen Pfad zu der Datei ein oder verwenden Sie die Schaltfläche **Durchsuchen** auf Ihrem lokalen PC.
- Verwenden Sie ein beliebiges, von Netzwerkmanagement-Karten unterstütztes Dateiübertragungsprotokoll, z. B. FTP, FTP Client, SCP oder TFTP. Im folgenden Beispiel wird FTP verwendet:
  a. Wechseln Sie in den Ordner, der die Kopie der angepassten INI-Datei enthält, und melden Sie sich von dort aus mit dem folgenden Befehl über FTP bei der Netzwerkmanagement-Karte an, an die Sie die INI-Datei exportieren möchten:

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

  b. Geben Sie Folgendes ein, um den Dateiübertragungsmodus auf binär zu setzen:

  ```
  ftp> bin
  ```

  Geben Sie Folgendes ein, um einen Fortschrittsbalken während der Dateiübertragung anzuzeigen:

  ```
  ftp> hash
  ```

c. Exportieren Sie die Kopie der angepassten INI-Datei in das Stammverzeichnis der empfangenen Netzwerkmanagement-Karte:

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

Übertragen der Datei auf mehrere Netzwerkmanagement-Karten. Befolgen Sie diese Schritte:

- Verwenden Sie FTP oder SCP, erstellen Sie jedoch ein Skript, das die zum Exportieren der Datei an eine einzelne Netzwerkmanagement-Karte erforderlichen Schritte mehrmals beinhaltet.
- Verwenden Sie eine Stapelverarbeitungsdatei und das Dienstprogramm für INI-Dateien.

Wenn Sie die Stapeldatei erstellen und das Dienstprogramm verwenden möchten, lesen Sie die *Versionshinweise: Dienstprogramm für .ini-Dateien* auf der **APC-Website** oder beziehen Sie sich auf den Knowledge Base-Artikel **FA156117** auf **http://www.apc.com/support**.

Ereignis- und Fehlermeldungen zur Dateiübertragung

Das Ereignis und die dazugehörigen Fehlermeldungen

Das folgende Ereignis tritt ein, wenn die empfangende Netzwerkmanagement-Karte die Aktualisierung ihrer Einstellungen anhand der INI-Datei abgeschlossen hat:

```
Hochladen der Konfigurationsdatei mit n gültigen Werten abgeschlossen.
```

Wenn ein Schlagwort, ein Abschnittsname oder ein Wert ungültig ist, wird die Übertragung an die empfangende Netzwerkmanagement-Karte zu Ende geführt und der Fehler durch einen zusätzlichen Ereignistext mitgeteilt.

Ereignistext	Beschreibung
Konfigurationsdateiwarnung: Ungültiges Schlüsselwort in Zeile *x*. Konfigurationsdateiwarnung: Ungültiger Wert in Zeile *x*.	Zeilen mit einem ungültigen Schlüsselwort oder Wert werden ignoriert.
Konfigurationsdateiwarnung: Ungültiger Abschnitt in Zeile *x*.	Wenn ein Abschnittsname ungültig ist, werden alle in diesem Abschnitt befindlichen Schlüsselwörter und Werte ignoriert.
Konfigurationsdateiwarnung: Schlüsselwort außerhalb eines Abschnitts in Zeile *x* gefunden.	Ein ganz oben in der Datei (d. h. vor der ersten Abschnittsüberschrift) eingetragenes Schlüsselwort wird ignoriert.
Konfigurationsdateiwarnung: Konfigurationsdatei überschreitet Maximalgröße.	Wenn die Datei zu groß ist, kommt es zu einer unvollständigen Übertragung. Reduzieren Sie die Dateigröße oder teilen Sie die Datei in zwei kleinere Dateien auf und wiederholen Sie die Übertragung.

Meldungen in der Datei config.ini

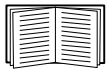
Ein Gerät in Verbindung mit der Netzwerkmanagement-Karte, aus der Sie die Datei config.ini heruntergeladen haben, muss vom System entdeckt werden, damit seine Konfiguration einbezogen werden kann. Wenn das Gerät (z. B. eine USV) nicht vorhanden ist oder nicht entdeckt wurde, enthält die Datei config.ini unter dem betreffenden Abschnittsnamen statt Schlüsselwörtern und Werten eine Meldung. Zum Beispiel:

```
UPS not discovered
```

Wenn Sie nicht vorhaben, die Konfiguration des betreffenden Geräts für einen späteren Import der INI-Datei zu exportieren, können Sie diese Meldungen ignorieren.

Durch außer Kraft gesetzte Werte erzeugte Fehlermeldungen

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

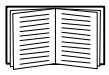


Informationen zu außer Kraft gesetzten Werten finden Sie unter „Inhalt der INI-Datei“.

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

Verwandte Themen

Anstatt INI-Dateien zu übertragen, können Sie unter Windows-Betriebssystemen das Konfigurationsdienstprogramm für IP-Adressen verwenden, um die grundlegenden TCP/IP-Einstellungen der Netzwerkmanagement-Karte zu aktualisieren und andere Einstellungen über die Benutzeroberfläche des Assistenten vorzunehmen.



Siehe „Assistent für die Konfiguration von Geräte-IP-Adressen“.

Dateiübertragungen

Aktualisierung der Firmware

Wenn Sie die Firmware auf der Netzwerkmanagement-Karte aktualisieren, erhalten Sie die neuesten Funktionen, Sicherheits- und Leistungsoptimierungen sowie Fehlerbehebungen.

Zur Aktualisierung muss die .nmc3-Datei lediglich auf die Netzwerkmanagement-Karte übertragen werden. Eine eigentliche Installation ist nicht erforderlich. Unter **www.apc.com/shop/tools/software-firmware** erhalten Sie ständig die neuesten Aktualisierungen.

Der Name der `.nmc3`-Datei hat folgendes Format:

```
apc-hardwareversion_typ_firmware-version.nmc3
```

- `apc`: Gibt den Kontext an.
- `hardware-version: Bei hw0n` steht n für die Hardwareversion, auf der Sie diese Datei verwenden können.
- `type`: Identifiziert das Modul.
- `version`: Die Versionsnummer der Datei.

Übertragungsverfahren für Firmware-Dateien

Die neueste Firmware-Version erhalten Sie kostenlos unter **www.apc.com/shop/tools/software-firmware**. Verwenden Sie zur Aktualisierung von Netzwerkmanagement-Karten eine der folgenden Methoden:

- Für Windows-Systeme verwenden Sie das von der **APC-Website** heruntergeladene **Firmware Upgrade Utility**. Siehe „Verwenden des NMC Firmware Upgrade Utility“.
- Verwenden Sie **FTP oder SCP** auf einem beliebigen unterstützten Betriebssystem, um die `.nmc3`-Datei zu übertragen. Siehe „Aktualisieren einer einzelnen Netzwerkmanagement-Karte per FTP oder SCP“.
- Verwenden Sie für eine Netzwerkmanagement-Karte, die sich NICHT in Ihrem Netzwerk befindet, **XMODEM** über einen virtuellen USB-Kommunikationsport unter Verwendung des Bootloaders, um die `.nmc3`-Datei von Ihrem Computer auf die Netzwerkmanagement-Karte zu übertragen. Siehe „Verwenden von XMODEM zum Aktualisieren einer Netzwerkmanagement-Karte“.
- Verwenden Sie ein **USB-Speichermedium**, um die Firmware-Datei von Ihrem Computer zu übertragen (nur AP9641, AP9643). Siehe „Verwenden Sie ein USB-Speichermedium zum Übertragen und Aktualisieren der Dateien“.
- Informationen zum **Aktualisieren mehrerer Netzwerkmanagement-Karten** finden Sie unter „Aktualisieren der Firmware auf mehreren Netzwerkmanagement-Karten“ und „Einsatz des NMC Firmware Upgrade Utility für mehrere Upgrades unter Windows“.

Verwenden des NMC Firmware Upgrade Utility

Dieses Firmware-Upgrade-Dienstprogramm ist Teil des Firmware-Upgrade-Pakets, das auf der **APC-Website** verfügbar ist. (Verwenden Sie *niemals* ein für ein bestimmtes Produkt vorgesehenes Utility, um damit die Firmware eines anderen Produkts zu aktualisieren.)

Aktualisierungen auf Windows-Systemen mit dem Utility. Das Dienstprogramm für die NMC-Firmware-Aktualisierung sorgt auf allen unterstützten Windows-Systemen für eine automatische Übertragung der `.nmc3`-Datei.

Dekomprimieren Sie die heruntergeladene Aktualisierungsdatei und doppelklicken Sie auf die EXE-Datei. Geben Sie die Host-IP-Adresse, den Benutzernamen und das Kennwort in die Dialogfelder ein. Sie müssen auch entweder „FTP“ oder „SCP“ und den zugehörigen Port auswählen.

HINWEIS: Das ausgewählte Protokoll muss auf dem NMC-Gerät aktiviert sein, damit das Firmware-Upgrade abgeschlossen werden kann. Siehe auch „Einsatz des NMC Firmware Upgrade Utility für mehrere Upgrades unter Windows“.

Aktualisieren einer einzelnen Netzwerkmanagement-Karte per FTP oder SCP

FTP. So aktualisieren Sie eine Netzwerkmanagement-Karte per FTP über das Netzwerk:

- Die Netzwerkmanagement-Karte muss mit dem Netzwerk verbunden sein und ihre System-IP, ihre Subnetzmaske und ihr Standardgateway müssen konfiguriert sein.
- Der FTP-Server muss auf der Netzwerkmanagement-Karte aktiviert sein (siehe „FTP-Server“).

Führen Sie die folgenden Schritte aus, um die Datei zu extrahieren:

1. Öffnen Sie auf einem im Netzwerk befindlichen Computer eine Befehlszeile. Wechseln Sie in das Verzeichnis, das die aktualisierte Datei für die Firmware enthält, und zeigen Sie den Verzeichnisinhalt an:

   ```
   C:\>cd apc
   C:\apc>dir
   ```

   Weitere Informationen hierzu finden Sie unter „Firmware-Moduldateien (Netzwerkmanagement-Karte 3)“.

2. So öffnen Sie eine FTP-Client-Sitzung:

   ```
   C:\apc>ftp
   ```

3. Geben Sie `open` und die IP-Adresse der Netzwerkmanagement-Karte ein und betätigen Sie die EINGABETASTE. Falls sich die Port-Einstellung des FTP-Servers geändert hat und nicht mehr der Standardeinstellung 21 entspricht, müssen Sie im FTP-Befehl den von der Standardeinstellung abweichenden Wert verwenden.
   - Bei Windows FTP-Clients wird die nicht standardmäßige Port-Nummer mit einem Leerzeichen von der IP-Adresse getrennt. Zum Beispiel (Leerzeichen vor 21000): `ftp> open 150.250.6.10 21000`
   - Bei bestimmten FTP-Clients muss hingegen vor der Port-Nummer ein Doppelpunkt eingegeben werden.
4. Melden Sie sich als Administrator an.
5. Aktualisieren Sie die Firmware.

   `ftp> bin`
   `ftp> put apc_hw21_AA_v-v-v-v.nmc3` (wobei `AA` für die Anwendung steht, z. B. eu3p, und `v-v-v-v` steht für die Nummer der Firmware-Version)
6. Nachdem FTP die Übertragung bestätigt hat, geben Sie `quit` ein, um die Sitzung zu schließen.

SCP. Gehen Sie wie folgt vor, wenn Sie Secure Copy (SCP) zur Aktualisierung von Firmware für die Netzwerkmanagement-Karte verwenden möchten

1. Übertragen Sie die `.nmc3`-Datei über eine SCP-Befehlszeile an die Netzwerkmanagement-Karte. Im folgenden Beispiel steht `v-v-v-v` für die Versionsnummer des Anwendungsmoduls:

   ```
   scp apc_hw21_eu3p_v-v-v-v.nmc3 apc@158.205.6.185:apc_hw21_eu3p_v-v-v-v.nmc3
   ```

Hinweis: Zur Verwendung von SCP muss SSH aktiviert werden. Zur Aktivierung von SSH siehe Bildschirm „Konsole“.

Verwendung von XMODEM zum Aktualisieren einer Netzwerkmanagement-Karte

Wenn Sie eine einzelne, noch nicht in das Netzwerk eingebundene Netzwerkmanagement-Karte über XMODEM aktualisieren möchten:

1. Verbinden Sie das mitgelieferte Micro-USB-Kabel (Teilenummer 960-0603) mit der Netzwerkmanagement-Karte und dem USB-Port eines lokalen Computers.
2. Drücken Sie die Taste „**Reset**“ auf der NMC.
3. Wenn die NMC beim Hochfahren eine USB-Verbindung erkennt, wartet sie 90 Sekunden, damit das Betriebssystem genügend Zeit zum Erkennen und Konfigurieren eines virtuellen Kommunikationsports hat. Wenn der virtuelle Kommunikationsport bereit ist, führen Sie ein Terminalprogramm wie HyperTerminal oder Tera Term aus, um den virtuellen Kommunikationsport auszuwählen.
4. Drücken Sie zweimal die **Eingabetaste**, oder bis die Boot-Monitor-Eingabeaufforderung angezeigt wird: BM>HINWEIS: Wenn innerhalb von 90 Sekunden nach dem Neustart der NMC keine Verbindung zum Boot-Monitor hergestellt wird, wird der normale Startvorgang der NMC fortgesetzt.
5. Geben Sie „XMODEM“ ein und betätigen Sie die **Eingabetaste**.
6. Wählen Sie im Menü des Terminal-Programms die Option XMODEM aus und wählen Sie dann die `.nmc3`-Datei aus, um sie per XMODEM zu übertragen. Nach Abschluss der XMODEM-Übertragung wird die Boot-Monitor-Eingabeaufforderung erneut angezeigt.

   Geben Sie „reset“ ein oder drücken Sie die Taste „**Reset**“, um die Netzwerkmanagement-Karte neu zu starten.

HINWEIS: Ein Treiber ist erforderlich, um über Windows 7 eine Verbindung mit der NMC-Konsole herzustellen. Der Treiber kann auf der APC-Website von der AP9544/AP9547-Produktseite im Abschnitt **„Software/Firmware“** heruntergeladen werden. Für Windows 10 ist kein Treiber erforderlich.

1. Wenn Sie die NMC über das Micro-USB-Kabel anschließen, wird unter „Andere Geräte“ ein Gerät namens „NMC3-CDC“ erkannt.

2. Klicken Sie mit der rechten Maustaste auf dieses Gerät und wählen Sie „Treiber-Software aktualisieren...“

3. Wählen Sie die Option „Auf dem Computer nach Treibersoftware suchen“ und navigieren Sie zum Download-Speicherort des Treibers (usb_cdc_ser.inf).

4. Akzeptieren Sie die Sicherheitsmeldung zur fehlenden Signatur des Treibers.

Windows erkennt nun die NMC und weist dem Gerät einen COM-Port zu.

Verwenden Sie ein USB-Speichermedium zum Übertragen und Aktualisieren der Dateien

Diese Funktion ist in der Bootloader-Version 1.3.3.1 und höher verfügbar. Bevor mit der Übertragung begonnen wird, sollten Sie sicherstellen, dass das USB-Speichermedium als FAT, FAT16 oder FAT32 formatiert ist.

1. Laden Sie die Firmware-Aktualisierungsdatei herunter.
2. Erstellen Sie auf dem USB-Speichermedium einen Ordner mit dem Namen **apcfirm**.
3. Legen Sie die `.nmc3`-Datei im Verzeichnis **apcfirm** ab.
4. Erstellen Sie mit dem Text-Editor eine Datei mit dem Namen nmc3.rcf. (Die Dateierweiterung muss .rcf lauten und nicht .txt beispielsweise.)
5. In **nmc3.rcf**, fügen Sie eine Zeile für das zu aktualisierende Firmware-Paket hinzu. Geben Sie z. B. für ein Upgrade der Dreiphasen-Easy-UPS-**Anwendung** Version v1.5.0.6 Folgendes ein:

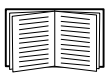
NMC3=apc_hw21_eu3p_1-5-0-6.nmc3

6. Fügen Sie „nmc3.rcf“ in den Ordner **apcfirm** auf dem Flash-Laufwerk ein.
7. Verbinden Sie das Flash-Laufwerk mit dem USB-Anschluss Ihrer Netzwerkmanagement-Karte; siehe dazu „Frontblende (AP9544/AP9547)“.
8. Starten Sie die Netzwerkmanagement-Karte neu und warten Sie bis die Karte vollständig neu gestartet wurde.
9. Prüfen Sie, ob die Aktualisierung erfolgreich durchgeführt wurde, indem Sie die Verfahren unter „Prüfen der Aktualisierungen“ verwenden.

Aktualisieren der Firmware auf mehreren Netzwerkmanagement-Karten

Verwenden Sie eine der folgenden beiden Methoden:

- **NMC Firmware Upgrade Utility für Windows**. Siehe „Einsatz des NMC Firmware Upgrade Utility für mehrere Upgrades unter Windows“.
- **Verwenden von FTP oder SCP**. Zum Aktualisieren mehrerer Netzwerkmanagement-Karten über einen FTP-Client oder über SCP schreiben Sie ein Skript, das den Vorgang automatisch durchführt.
- **Exportieren von Konfigurationseinstellungen**. Sie können Stapelverarbeitungsdateien erstellen und mithilfe eines Dienstprogramms Konfigurationseinstellungen aus mehreren Netzwerkmanagement-Karten gleichzeitig abrufen, um diese an andere Netzwerkmanagement-Karten zu exportieren.



Siehe Versionshinweise: Dienstprogramm für .ini-Dateien in der Knowledge Base, **http://www.apc.com/site/support/**.

Einsatz des NMC Firmware Upgrade Utility für mehrere Upgrades unter Windows.

Nachdem Sie das Upgrade-Dienstprogramm von der NMC-Downloadseite auf der **APC-Website** heruntergeladen haben, machen Sie einen Doppelklick auf die EXE-Datei und entpacken Sie den Inhalt.

1. Suchen Sie im Verzeichnis mit dem Dienstprogramm nach der Datei „devices.txt“. Öffnen und bearbeiten Sie diese Datei mit einem Texteditor, um die für alle zu aktualisierenden NMC-Geräte erforderlichen Informationen einzugeben:
   - [Device]: Dieser Abschnittsheader muss für jede NMC, für die ein Upgrade durchgeführt werden soll, enthalten sein.
   - Host: Die IPv4-Adresse des Geräts.
   - Protocol: SCP oder FTP.
   - Port: Der zugehörige SCP- oder FTP-Port.
   - Username: Der auf der Netzwerkmanagement-Karte aktivierte Benutzername eines Administrators.
   - Password: Das Kennwort eines Administrators, auf der NMC aktiviert

   Entfernen Sie alle Kommentare und Strichpunkte aus „devices.txt“, und speichern Sie Ihre Änderungen.

   Zum Beispiel:

```
[Device]
Host=192.168.0.1
Protocol=SCP
Port=22
Username=apc
Password=apc
```

```
[Device]
Host=192.168.0.2
Protocol=SCP
Port=22
Username=apc
Password=apc
```

Sie können eine vorhandene Datei „devices.txt“ verwenden, wenn bereits eine existiert.

2. Öffnen des Firmware Upgrade Utility Wenn die richtigen Angaben in der Datei „devices.txt“ gemacht wurden, wird die folgende Meldung im Dienstprogramm angezeigt:

   ```
   Eine Geräteliste wurde erkannt und importiert, daher werden die im
   unteren Ereignisfenster aufgeführten Hosts als aktiv verwendet.
   ```

3. Klicken Sie im Dienstprogramm auf „Update starten“, um die Upgrade(s) der Firmware-Versionen zu starten.

Prüfen der Aktualisierungen

Ergebniscodes für die letzte Übertragung

Zu den möglichen Übertragungsfehlern zählen ein nicht gefundener TFTP- oder FTP-Server, Zugriffsverweigerung durch den Server, die fehlende Erkennung der Übertragungsdatei durch den Server oder eine beschädigte Übertragungsdatei.

Überprüfen der Versionsnummern der installierten Firmware

Path: Info – Netzwerk

Verwenden Sie die Web-Oberfläche, um die Versionen der aktualisierten Firmware-Module zu überprüfen. Sie können auch den Befehl SNMP GET an die MIB-II OID **sysDescr** verwenden. In der Befehlszeile steht hierfür der Befehl about zur Verfügung.

Ändern der Sprache der Benutzeroberfläche

Sie können die Benutzeroberfläche der Netzwerkmanagement-Karte in verschiedenen Sprachen anzeigen. Die Sprache kann über das Aufklappmenü für die Sprache auf dem Bildschirm für das Einloggen geändert werden.

Für die Benutzeroberfläche stehen neun Sprachen zur Verfügung: Französisch, Italienisch, Deutsch, Spanisch, Portugiesisch (Brasilien), Russisch, Koreanisch, Japanisch und vereinfachtes Chinesisch.

Fehlerbehebung

Probleme beim Zugriff auf die Netzwerkmanagement-Karte

Für eine Schritt-für-Schritt-Anleitung zur Problembehebung und hilfreiche Lösungen für gängige Probleme besuchen Sie die Knowledge Base unter www.apc.com/support. Die Kontaktdaten unseres Kundendienstes finden Sie unter „Weltweiter Kundendienst von APC by Schneider Electric“.

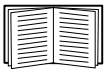
Problem	Lösung
Die Netzwerkmanagement-Karte reagiert nicht auf den Ping-Befehl	Wenn die Status-LED der Netzwerkmanagement-Karte grün leuchtet, senden Sie den Ping-Befehl versuchsweise an eine andere Station in dem Netzwerksegment, in dem sich die Netzwerkmanagement-Karte befindet. Wenn auch dann eine Antwort ausbleibt, hängt das Problem nicht mit der Netzwerkmanagement-Karte zusammen. Wenn die Status-LED nicht grün leuchtet oder wenn der Ping-Test erfolgreich verläuft, führen Sie die folgenden Prüfungen durch: • Stellen Sie sicher, dass die Netzwerkmanagement-Karte richtig in der USV sitzt. • Überprüfen Sie sämtliche Netzwerkverbindungen. • Überprüfen Sie die IP-Adressen der Netzwerkmanagement-Karte und des NMS. • Wenn sich das NMS in einem anderen physischen Netzwerk (oder Subnetz) als die Netzwerkmanagement-Karte befindet, überprüfen Sie die IP-Adresse des Standardgateways (oder Routers). • Überprüfen Sie die Anzahl der Subnetzbits in der Subnetzmaske der Netzwerkmanagement-Karte.
Keine Zuweisung der Datenschnittstelle durch ein Terminalprogramm möglich	Damit Sie die Netzwerkmanagement-Karte über ein Terminalprogramm konfigurieren können, müssen Sie zuerst alle Anwendungen, Dienste oder Programme schließen, die momentan die Datenschnittstelle verwenden.
Kein Zugriff auf die Befehlszeile über eine serielle Datenverbindung möglich	Überzeugen Sie sich davon, dass Sie die Baudrate nicht geändert haben. Versuchen Sie es mit 2400, 9600, 19200 oder 38400.
Kein Fernzugriff auf die Befehlszeile möglich	• Stellen Sie sicher, dass Sie die korrekte Zugriffsmethode verwenden, d. h. Telnet oder Secure SHell (SSH). Diese Zugriffsmethoden können von einem Administrator aktiviert werden. Standardmäßig ist Telnet deaktiviert und SSH ist aktiviert. SSH und Telnet können unabhängig voneinander aktiviert/deaktiviert werden. • Bei einem Zugriff über SSH erstellt die Netzwerkmanagement-Karte möglicherweise gerade einen Host-Schlüssel. Es kann bis zu einer Minute dauern, bis die Netzwerkmanagement-Karte den Host-Schlüssel erstellt hat; während dieser Zeit kann auf SSH nicht zugegriffen werden.

Problem	Lösung
Kein Zugriff auf die Benutzeroberfläche möglich	• Überzeugen Sie sich davon, dass der HTTP- oder HTTPS-Zugriff aktiviert ist. • Achten Sie darauf, dass Sie eine korrekte URL eingeben – diese muss zu dem von der Netzwerkmanagement-Karte verwendeten Sicherheitssystem passen. Für SSL muss die URL mit **https** eingeleitet werden, nicht mit **http**. • Überprüfen Sie, ob die Netzwerkmanagement-Karte auf den Ping-Befehl reagiert. • Überzeugen Sie sich davon, dass Sie einen von der Netzwerkmanagement-Karte unterstützten Webbrowser verwenden. Siehe „Weltweiter Kundendienst von APC by Schneider Electric“. • Falls die Netzwerkmanagement-Karte neu gestartet wurde und die Einrichtung der SSL-Sicherheit noch nicht abgeschlossen ist, erzeugt die Netzwerkmanagement-Karte möglicherweise gerade ein Serverzertifikat. Es kann bis zu einer Minute dauern, bis die Netzwerkmanagement-Karte dieses Zertifikat erstellt hat; während dieser Zeit ist der SSL-Server nicht verfügbar.

SNMP-Probleme

Problem	Lösung
GET-Anweisung kann nicht durchgeführt werden	• Überprüfen Sie die Leserechte (GET), den Community-Namen (SNMPv1) oder die Konfiguration des Benutzerprofils (SNMPv3). • Stellen Sie über die Befehlszeile oder die Web-Oberfläche sicher, dass das NMS Zugriff hat. Siehe Bildschirme „SNMP“.
SET-Anweisung kann nicht durchgeführt werden	• Überprüfen Sie, ob SNMP aktiviert ist. SNMPv1 und SNMPv3 sind standardmäßig deaktiviert. • Überprüfen Sie die Lese-/Schreibrechte (SET), den Community-Namen (SNMPv1) oder die Konfiguration des Benutzerprofils (SNMPv3). • Stellen Sie über die Befehlszeile oder die Web-Oberfläche sicher, dass das NMS Schreibzugriff (SET), generellen Zugriff (SNMPv1) bzw. Zugriff auf die betreffende IP-Zieladresse über die Zugriffssteuerungsliste (SNMPv3) hat. Siehe Bildschirme „SNMP“.
Vom NMS können keine Traps empfangen werden	• Stellen Sie sicher, dass der Trap-Typ (SNMPv1 oder SNMPv3) für das NMS als Trap-Empfänger richtig konfiguriert ist. • Fragen Sie bei SNMPv1 die MIB OID **mconfigTrapReceiverTable** ab, um sich davon zu überzeugen, dass die IP-Adresse des NMS darin richtig aufgeführt ist und dass der für das NMS definierte Community-Name dem Community-Namen in der Tabelle entspricht. Sollte einer dieser Einträge nicht stimmen, richten Sie entsprechende SET-Anweisungen an die OIDs **mconfigTrapReceiverTable** oder korrigieren Sie über die Befehlszeile oder die Web-Oberfläche die Definition des Trap-Empfängers. • Überprüfen Sie bei SNMPv3 die Benutzerprofil-Konfiguration für das NMS und führen Sie einen Trap-Test durch. Siehe Bildschirme „SNMP“, „Trap-Empfänger“ und Bildschirm „SNMP-Trap-Test“.
Von einem NMS empfangene Traps werden nicht erkannt	Lesen Sie in der Dokumentation zum NMS nach, um zu überprüfen, ob die Traps vorschriftsmäßig in die Alarm-/Trap-Datenbank aufgenommen wurden.

Modbus-Probleme



Ausführliche Informationen zu den Modbus-Registern und Bit-Beschreibungen finden Sie auf den *Modbus-Registerkarten* auf der **APC-Website**.

Probleme mit dem APC-USB-WiFi-Device (AP9834)

Problem	Lösung
Verbindung mit dem WiFi-Netzwerk kann nicht hergestellt werden	• Stellen Sie sicher, dass das APC-USB-WiFi-Gerät korrekt im USB-Anschluss einer AP9544/AP9547-Karte eingesetzt ist. • Stellen Sie sicher, dass die richtigen WiFi-Einstellungen in der Web-Benutzeroberfläche oder Befehlszeilenschnittstelle der Netzwerkmanagement-Karte bereitgestellt werden. • Stellen Sie sicher, dass im Ereignisprotokoll der Netzwerkmanagement-Karte keine WiFi-bezogenen Ereignisse vorhanden sind. Wenn die WiFi-Einstellungen falsch eingegeben oder leer gelassen wurden, protokolliert die Netzwerkmanagement-Karte einen Fehler im Ereignisprotokoll. Zum Beispiel: „USB-WiFi-Gerätefehler. WiFi-Einstellungen“. Wenn das Problem weiterhin besteht, wenden Sie sich an einen Netzwerkadministrator, um Verbindungsprobleme zu diagnostizieren.
Der LED-Zustand (rotes Dauerleuchten) des Geräts kann nicht behoben werden.	• Stellen Sie sicher, dass die richtigen WiFi-Einstellungen in der Web-Benutzeroberfläche oder Befehlszeilenschnittstelle der Netzwerkmanagement-Karte bereitgestellt werden. • Beheben Sie alle WiFi-bezogenen Ereignisse im Ereignisprotokoll der Netzwerkmanagement-Karte. Zum Beispiel: „USB-WiFi-Gerätefehler. WiFi-Einstellungen“. • Aktivieren Sie die kabelgebundene Verbindung erneut und konfigurieren Sie die WiFi-Einstellungen über eine alternative Methode: – Web-Benutzeroberfläche (**Konfiguration > Netzwerk > WiFi**) – Befehlszeilenschnittstelle (`wifi` -Befehl) – config.ini-Datei (`Netzwerk-WiFi` -Abschnitt) Wenn die kabelgebundene Verbindung nicht mehr verfügbar ist, schließen Sie das Micro-USB-Kabel (960-0603) an den Konsolenanschluss der Netzwerkmanagement-Karte an, um auf die Befehlszeilenschnittstelle zuzugreifen, und übertragen Sie die config.ini-Datei mit dem xferINI-Befehl. Weitere Informationen finden Sie im **Befehlszeilenhandbuch für die Netzwerkmanagement-Karte für Easy-UPS-Geräte**. Wenn das Problem weiterhin besteht, wenden Sie sich an den Kundendienst. Siehe „Weltweiter APC-Kundendienst“.

Beschreibung der LEDs

Zustand	Beschreibung
Aus	Eine der folgenden Situationen ist eingetreten: • Das Gerät ist nicht im USB-Anschluss einer AP9544/AP9547-Netzwerkmanagement-Karte eingesteckt. • Die Firmware der Netzwerkmanagement-Karte unterstützt kein WiFi. WiFi-Unterstützung ist ab Firmwareversion 1.4 verfügbar. Siehe „Dateiübertragungen“. • Das Gerät funktioniert nicht ordnungsgemäß. Möglicherweise muss es repariert oder ersetzt werden. Wenden Sie sich an den Kundendienst. Siehe „Weltweiter APC-Kundendienst“.
Grünes Dauerleuchten	Das Gerät ist mit einem Zugriffspunkt verbunden, es liegt jedoch keine Netzwerkaktivität vor.
Grünes Blinken	Das Gerät ist mit einem Zugriffspunkt verbunden und das WiFi-Netzwerk ist aktiv.
Rotes Dauerleuchten	Eine der folgenden Situationen ist eingetreten: • Es liegt ein permanenter Gerätefehler vor. • Es liegt ein permanenter Fehler bei den WiFi-Einstellungen der Netzwerkmanagement-Karte vor. • Es gibt unlösbare Probleme beim Herstellen einer Verbindung zu einem Zugriffspunkt.
Rotes Blinken	Das Gerät stellt eine WiFi-Verbindung zu einem Zugriffspunkt her.

2 Jahre Werksgarantie

Diese Garantie gilt nur für jene Produkte, die Sie zu Ihrer Verwendung kaufen und die in diesem Handbuch angeführt sind.

Garantiebedingungen

APC garantiert, dass seine Produkte für eine Zeitdauer von zwei Jahren ab dem Kaufdatum frei von Material- und Arbeitsmängeln sind. APC wird alle mangelhaften Produkte, die unter diese Garantie fallen, reparieren oder ersetzen. Diese Garantie gilt nicht für Ausrüstungen, die durch einen Unfall, Fahrlässigkeit oder falsche Verwendung beschädigt oder auf irgendeine Art und Weise geändert oder modifiziert wurden. Die Reparatur oder der Austausch eines fehlerhaften Produkts oder Teils verlängert nicht den ursprünglichen Garantiezeitraum. Alle Teile, die im Rahmen dieser Garantie ausgeliefert werden, sind neu oder wurden werksmäßig-wiederaufbereitet.

Nicht übertragbare Garantie

Diese Garantie gilt nur für den Original-Käufer, der das Produkt ordnungsgemäß registriert haben muss. Der Käufer kann das Produkt auf der Website von APC unter www.apc.com registrieren.

Ausnahmen

APC entsteht durch diese Garantie keine Verpflichtung, wenn seine eigenen Tests und Prüfungen ergeben, dass der angebliche Defekt des Produkts infolge von Missbrauch, Unachtsamkeit, falscher Installation oder Prüfung durch den Endverbraucher entstanden ist. Ferner übernimmt APC im Rahmen dieser Garantie keine Haftung für nicht autorisierte Reparatur- oder Änderungsversuche an falscher oder inadäquater elektrischer Spannung oder Verbindungen bei nicht vorschriftsmäßigen Betriebsbedingungen vor Ort, korrosiver Atmosphäre, unsachgemäßer Reparatur oder Installation, höherer Gewalt, Feuer, Diebstahl, beim Missachten der Empfehlungen oder Spezifikationen von APC beim Einbau oder wenn die Seriennummer von APC verändert, unkenntlich gemacht oder entfernt wurde sowie wenn eine andere Ursache außerhalb des vorgesehenen Verwendungszwecks vorliegt.

FÜR PRODUKTE, DIE IM RAHMEN DIESER VEREINBARUNG ODER IM ZUSAMMENHANG DAMIT VERKAUFT, GEWARTET ODER BEREITGESTELLT WERDEN, GIBT ES KEINE GESETZLICHEN ODER SONSTIGEN GARANTIEN, WEDER AUSDRÜCKLICH NOCH STILLSCHWEIGEND. APC SCHLIESST ALLE STILLSCHWEIGENDEN GARANTIEN IN BEZUG AUF MARKTGÄNGIGKEIT, ZUFRIEDENHEIT ODER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK AUS. DIE AUSDRÜCKLICHEN GARANTIEN VON APC WERDEN VON APC NICHT ERWEITERT, GESCHMÄLERT ODER BEEINTRÄCHTIGT UND KEINE VERPFLICHTUNG ODER HAFTUNG ENTSTEHT DADURCH, DASS APC IM ZUSAMMENHANG MIT DEN PRODUKTEN TECHNISCHE ODER ANDERE SERVICES ERBRINGT ODER RATSCHLÄGE ERTEILT. DIE OBEN BESCHRIEBENEN GARANTIEN UND GEWÄHRLEISTUNGSANSPRÜCHE SIND EXKLUSIV UND GELTEN ANSTELLE ALLER ANDEREN GARANTIEN UND GEWÄHRLEISTUNGSANSPRÜCHE. DIE OBEN GENANNTEN GARANTIEN BEGRÜNDE N DIE EINZIGE LEISTUNGSVERPFLICHTUNG VON APC UND STELLEN IHRE EINZIGEN RECHTSMITTEL IM FALLE VON GARANTIEVERLETZUNGEN DAR. DIE GARANTIEN VON APC GELTEN NUR FÜR DEN KÄUFER UND KÖNNEN NICHT AUF DRITTE ÜBERTRAGEN WERDEN.

AUF KEINEN FALL HAFTEN APC, SEINE LEITENDEN ANGESTELLTEN, DIREKTOREN, ANGESCHLOSSENEN UNTERNEHMEN ODER MITARBEITER FÜR IRGENDWELCHE INDIREKTEN, SPEZIELLEN, FINANZIELLEN ODER FOLGESCHÄDEN, DIE AUF DIE NUTZUNG, DIE WARTUNG ODER DIE INSTALLATION DER PRODUKTE ZURÜCKZUFÜHREN SIND, EGAL OB SOLCHE SCHÄDEN AUFGRUND EINER VERTRAGSVERLETZUNG ODER UNERLAUBTEN HANDLUNG ENTSTEHEN, UNABHÄNGIG VON DER SCHULD, VON FAHRLÄSSIGKEIT ODER KAUSALHAFTUNG UND UNABHÄNGIG DAVON, OB APC IM VORAUS VON DER MÖGLICHKEIT SOLCHER SCHÄDEN INFORMIERT WURDE ODER NICHT. INSBESONDERE HAFTET APC NICHT FÜR IRGENDWELCHE KOSTEN WIE ENTGANGENE GEWINNE ODER EINKOMMEN, VERLORENE AUSRÜSTUNGEN, NUTZUNGSAUSFALL DER AUSRÜSTUNG, SOFTWARE- UND DATENVERLUST, KOSTEN FÜR ERSATZAUSRÜSTUNGEN, FORDERUNGEN VON DRITTEN ODER SONSTIGES.

KEIN VERKÄUFER, MITARBEITER ODER VERTRETER VON APC IST BEFUGT, DIESE GARANTIEBEDINGUNGEN ZU ÄNDERN ODER BEDINGUNGEN HINZUZUFÜGEN. WENN ÜBERHAUPT, DÜRFEN DIE GARANTIEBESTIMMUNGEN AUSSCHLIESSLICH SCHRIFTLICH GEÄNDERT WERDEN UND MÜSSEN VON EINEM HANDLUNGSBEVOLLMÄCHTIGTEN UND DER RECHTSABTEILUNG VON APC UNTERSCHRIEBEN WERDEN.

Garantieansprüche

Garantieansprüche können im APC-Kundendienst-Netzwerk über die Support-Seiten auf der Website von APC unter www.apc.com/support geltend gemacht werden. Wählen Sie auf dieser Webseite ganz oben im Pulldown-Menü Ihr Land aus. Klicken Sie dann auf die Registerkarte „Support“, um die Kontaktinformationen Ihres lokalen Kundendienstes zu erhalten.

Copyright-Hinweise

Kryptographische Bibliothek cryptlib

Berkeley Database

Lua

DIE SOFTWARE WIRD „WIE BESEHEN“ OHNE JEGLICHE AUSDRÜCKLICHE ODER STILLSCHWEIGENDE GEWÄHRLEISTUNG, EINSCHLIEßLICH, ABER NICHT BESCHRÄNKT AUF DIE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND DER NICHTVERLETZUNG VON RECHTEN DRITTER, ZUR VERFÜGUNG GESTELLT IN KEINEM FALL SIND DIE AUTOREN ODER URHEBERRECHTSINHABER HAFTBAR FÜR ANSPRÜCHE, SCHÄDEN ODER ANDERE VERPFLICHTUNGEN, OB IN EINER VERTRAGS- ODER HAFTUNGSKLAGE, EINER UNERLAUBTEN HANDLUNG ODER ANDERWEITIG, DIE SICH AUS, AUS ODER IN VERBINDUNG MIT DER SOFTWARE ODER DER NUTZUNG ODER ANDEREN GESCHÄFTEN MIT DER SOFTWARE ERGEBEN.

Hochfrequenzstörungen

Änderungen oder Modifikationen dieses Geräts, die von der für Übereinstimmung verantwortlichen Partei nicht ausdrücklich genehmigt wurden, können dazu führen, dass die Nutzungsberechtigung für dieses Gerät erlischt.

USA: FCC

Dieses Gerät wurde getestet und entspricht den Grenzwerten für digitale Geräte der Klasse A, gemäß Abschnitt 15 der FCC-Vorschriften. Diese Grenzwerte bieten hinreichenden Schutz gegen schädliche Störungen, wenn das Gerät in einer kommerziellen Umgebung betrieben wird. Dieses Gerät erzeugt und verwendet Hochfrequenzenergie, kann diese ausstrahlen und verursacht, wenn es nicht gemäß der Bedienungsanleitung installiert und benutzt wird, schädliche Störungen des Funkverkehrs. Der Betrieb dieses Geräts in Wohngebieten verursacht wahrscheinlich schädliche Störungen. Der Benutzer trägt die alleinige Verantwortung für die Beseitigung solcher Interferenzen.

Kanada: ICES

Dieses Digitalgerät der Klasse A entspricht den kanadischen ICES-003-Vorschriften.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Japan: VCCI

Dies ist ein Produkt der Klasse A entsprechend dem VCCI-Standard (Voluntary Control Council for Interference by Information Technology Equipment). Wenn dieses Produkt in häuslicher Umgebung eingesetzt wird, kann es zu Funkstörungen kommen, für deren Beseitigung der Endbenutzer entsprechende Maßnahmen zu treffen hat.

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラス A 情報技術装置です。この装置を家庭環境で使用すると、電波

妨害を引き起こすことがあります。この場合には、使用者が適切な対策を講ずるように要求されることがあります

Taiwan: BSMI

警告使用者：
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

Australien und Neuseeland

Achtung: Dies ist ein Produkt der Klasse A. In einem Wohnumfeld kann dieses Produkt Funkstörungen erzeugen. In diesem Fall müssen ggf. geeignete Gegenmaßnahmen getroffen werden.

Europäische Union

Dieses Produkt entspricht den Schutzanforderungen der Richtlinie 2004/108/EC des Europäischen Rats zur Angleichung der Rechtsvorschriften der Mitgliedstaaten über die elektromagnetische Verträglichkeit. APC kann keine Verantwortung für eine etwaige Nichteinhaltung der Schutzvorschriften übernehmen, die aus einer nicht empfohlenen Abwandlung des Produkts resultieren kann.

Dieses Gerät wurde getestet und liegt innerhalb der Grenzwerte für IT-Ausrüstung der Klasse A entsprechend der europäischen Norm CISPR 22, EN 55022. Die Grenzwerte für die Klasse A wurden aus dem kommerziellen und industriellen Umfeld abgeleitet, um einen angemessenen Schutz gegen Störungen von zugelassenen Kommunikationsgeräten zu erreichen.

Achtung: Dies ist ein Produkt der Klasse A. In einem Wohnumfeld kann dieses Produkt Funkstörungen erzeugen. In diesem Fall müssen ggf. geeignete Gegenmaßnahmen getroffen werden.

Koreanisch 한국

A 급 기기 (업무용 방송통신기기)

이 기기는 업무용 (A 급) 으로 전자파적합등록을 한 기기이오니판매자 또는 사용자는 이 점을 주의하시기 바라며 , 가정외의지역에서 사용하는 것을 목적으로 합니다 .

Weltweiter Kundendienst von APC by Schneider Electric

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

- Besuchen Sie die Website von Schneider Electric. Dort können Sie auf die Dokumente der Schneider Electric Knowledge Base zugreifen und Anfragen an den Kundendienst senden.
  - www.apc.com (Firmensitz)
    Auf der lokalisierten Schneider Electric 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 Kundendienst von Schneider Electric.
  - 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.

990-91545B–005 **01/2023**