Benutzerhandbuch

Netzwerkmanagement-Karte 3

AP9640, AP9641, AP9643

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

990-91148N-005
5/2025

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

Die Netzwerkmanagement-Karten von Schneider Electric (AP9640, AP9641 und AP9643) und USV-Geräte mit integrierter Netzwerkmanagementkarte 3 sind webbasierte, IPv6-fähige Produkte.

Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS)	Secure SHell (SSH)
Secure Copy (SCP)	Lightweight Directory Access Protocol (LDAP) – v3.1.x und höher
Terminal Access Controller Access-Control System Plus (TACACS+) – v3.0.x und höher	Extensible Authentication Protocol (EAP) over LAN (EAPoL)
Building Automation and Control Networks Protocol (BACnet)	Syslog
Simple Network Management Protocol versions 1, 2c and 3	Telnet
RADIUS	Hypertext Transfer Protocol (HTTP)
Modbus	File Transfer Protocol (FTP)

Die **AP9640**-Netzwerkmanagement-Karte:

- Bietet Funktionen zur Steuerung der USV und zur planmäßigen Durchführung von Selbsttests an der USV.
- Liefert Daten- und Ereignisprotokolle.
- Bietet die Möglichkeit, Benachrichtigungen mithilfe von Ereignisprotokollierung, E-Mail, Syslog und SNMP-Traps einzurichten.
- Bietet Unterstützung für PowerChute® Network Shutdown.
- Unterstützt die Verwendung eines DHCP-Servers (Dynamic Host Configuration Protocol) oder eines BOOTP-Servers (BOOTstrap Protocol) zur Bereitstellung der TCP-/IP-Netzwerkparameter der Netzwerkmanagement-Karte.
- 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 EcoStruxure™ IT oder Data Center Expert.
- Unterstützt Modbus TCP/IP.
- Unterstützt BACnet/IP

Die **AP9641**-Netzwerkmanagement-Karte verfügt über sämtliche Funktionen der AP9640-Netzwerkmanagement-Karte und bietet darüber hinaus folgende Funktionen:

- Zwei USB-Anschlüsse, die Firmware-Aktualisierungen der Netzwerkmanagement-Karte und der USV-Firmware über einen USB-Stick unterstützen.
- Unterstützung für zwei universelle Eingabe-/Ausgabe-Anschlüsse, die mit folgenden Geräten verbunden werden können:
  - Temperatur- (AP9335T) oder Temperatur-/Feuchtigkeitssensoren (AP9335TH)
  - Eingabe-/Ausgabe-Relaisstecker mit Unterstützung für zwei Eingangskontakte und ein Ausgangsrelais (mithilfe des optionalen E/A-Zusatzmoduls AP9810 für potenzialfreie Kontakte)
  - Flüssigkeits-Sensor (Spot Fluid Sensor) (NBES0301, ein optionales Zusatzmodul) – v3.1.x und höher

- Unterstützung von Modbus RTU über den universellen E/A-Port 2 zusätzlich zu Modbus TCP/IP. Informationen zur Konfiguration von Modbus RTU finden Sie im Modbus-Dokumentationsanhang.

Die **AP9643**-Netzwerkmanagement-Karte verfügt über sämtliche Funktionen der AP9640-Netzwerkmanagement-Karte und bietet darüber hinaus folgende Funktionen:

- Zwei USB-Anschlüsse, die Firmware-Aktualisierungen der Netzwerkmanagement-Karte und der USV-Firmware über einen USB-Stick unterstützen.
- Unterstützung für einen universellen Eingabe-/Ausgabe-Anschluss, der mit folgenden Geräten verbunden werden kann:
  - Temperatursensor (AP9335T) oder Temperatur-/Feuchtigkeitssensor (AP9335TH)
  - Relais-Eingangs-/Ausgangsanschluss, die zwei Eingangskontakte und ein Ausgangsrelais unterstützen (mit dem AP9810 E/A-Zusatzmodul für potenzialfreie Kontakte als optionales Add-On)
  - Flüssigkeitssensor (Spot Fluid Sensor) (NBES0301, ein optionales Zusatzmodul) – v3.1.x und höher
- Unterstützt Modbus RTU über den seriellen RS485-Anschluss, zusätzlich zu Modbus TCP/IP. Informationen zur Konfiguration von Modbus RTU finden Sie im Modbus-Dokumentationsanhang.

USV-Geräte mit dem SRTL/SRYLF-Präfix und einer integrierten Netzwerkmanagement-Karte verfügen über sämtliche Funktionen der AP9640-Netzwerkmanagement-Karte (außer Modbus- und BACnet-Unterstützung) und bieten darüber hinaus folgende Funktion:

- Ein oder zwei USB-Anschlüsse, die Firmware-Aktualisierungen der Netzwerkmanagement-Karte und der USV-Firmware über einen USB-Stick unterstützen.
- Unterstützung für einen universellen Eingabe-/Ausgabe-Anschluss, der mit folgenden Geräten verbunden werden kann:
  - Temperatur- bzw. Temperatur-/Luftfeuchtigkeitssensor (AP9335T bzw. AP9335TH).
  - Eingabe-/Ausgabe-Relaisstecker mit Unterstützung für zwei Eingangskontakte und ein Ausgangsrelais (mithilfe des optionalen E/A-Zusatzmoduls AP9810 für potenzialfreie Kontakte).
  - Flüssigkeitssensor (Spot Fluid Sensor) (NBES0301, ein optionales Zusatzmodul) – v3.1.x und höher

Unterstützte Geräte

Die Netzwerkmanagement-Karte 3 ist kompatibel mit:

- Smart-UPS® Geräten mit einem SmartSlot mit den Präfixen SMT, SMX, SRT, SURTD sowie SUA-Geräten, die nach 2008* hergestellt wurden.
- Einphasigen Symmetra® UPS-Geräten.

*Eine vollständige Auflistung kompatibler USVs, in denen eine Netzwerkmanagement-Karte 3 installiert werden kann, siehe Knowledge-Base-Artikel **FA237786**.

IPv4-Erstkonfiguration

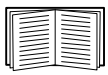
Sie müssen die folgenden TCP-/IP-Einstellungen für die Netzwerkmanagement-Karte festlegen, bevor sie im Netzwerk verwendet werden kann:

- 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 **Support-Bildschirm**. 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 (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.
- EcoStruxure IT — Mit dieser Cloud-basierten Überwachungssoftware können Sie Ihre USV-Geräte über SNMP und Modbus TCP überwachen.
- EcoStruxure™ IT Data Center Expert – Ermöglicht Power-Management und die Verwaltung von SNMP Agenten wie Netzwerk-USVs und Umgebungssensoren auf Unternehmensebene.
- Befehlszeilenschnittstelle (CLI) des Sicherheitsassistenten für die Netzwerkmanagement-Karte (NMC) – 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 **Handbuch zur Befehlszeilenoberfläche**. 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. Weitere Informationen finden Sie unter Bildschirm „Sitzungsverwaltung“.

Arten von Benutzerkonten

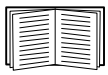
Die Netzwerkmanagement-Karte kennt verschiedene Zugriffsebenen - Superuser, Administrator, Benutzer „Gerät“, Benutzer „schreibgeschützt“ und Benutzer „nur Netzwerk“:

- 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. In v3.0.x und höher gibt es keinen Standard-Benutzernamen und kein Standard-Kennwort.
- Ein Gerätebenutzer besitzt Lese- und Schreibzugriff auf das Gerät betreffende Bildschirme und Befehle in der Web-Benutzeroberfläche. Administrative Funktionen wie die Sitzungsverwaltung im Sicherheitsmenü sowie Menüs und Befehle im Abschnitt „Netzwerk“ 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.

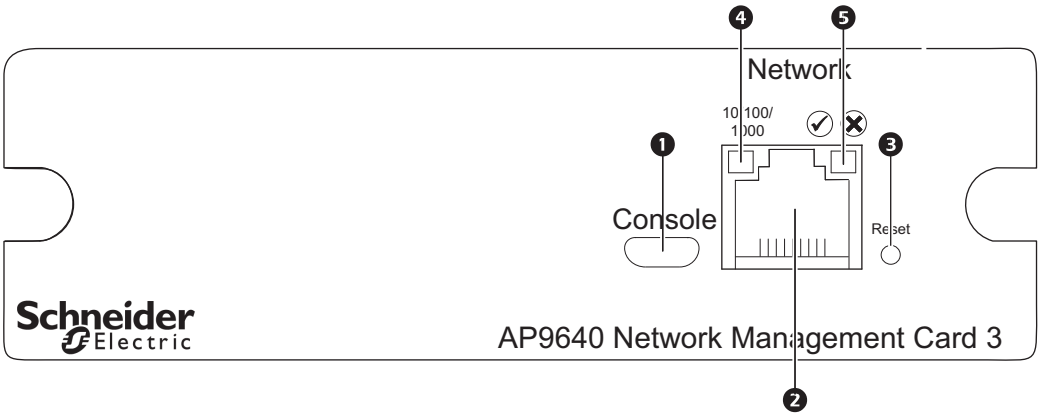
HINWEIS: Es wird dringend empfohlen, aktive Benutzersitzungen nach einer Kennwortänderung zu beenden.

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 im **Installationshandbuch** oder im Knowledge Base-Artikel **FA156064**.

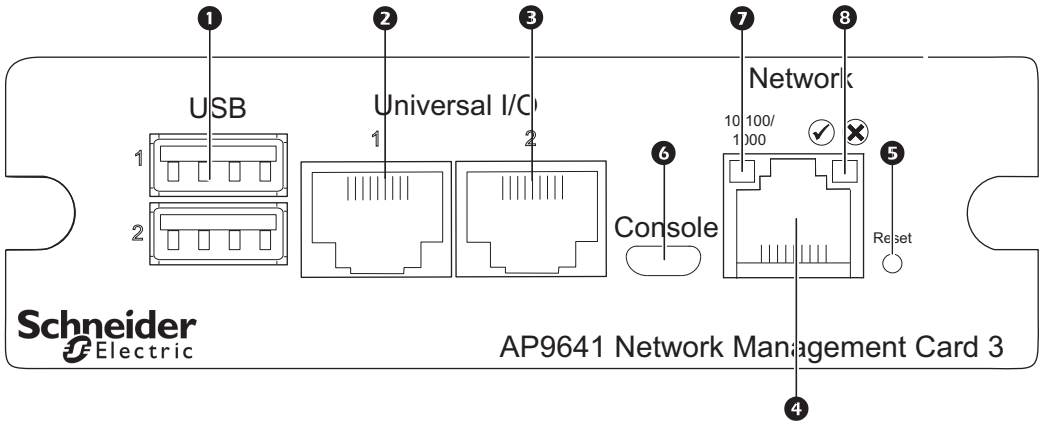
Es wird empfohlen, die .ini-Datei nach der Konfiguration Ihrer NMC zu exportieren, um Datenverluste im Falle eines vergessenen Passworts zu vermeiden. Weitere Informationen finden Sie unter „Abrufen und Exportieren der .ini-Datei“.

Frontblende (AP9640)



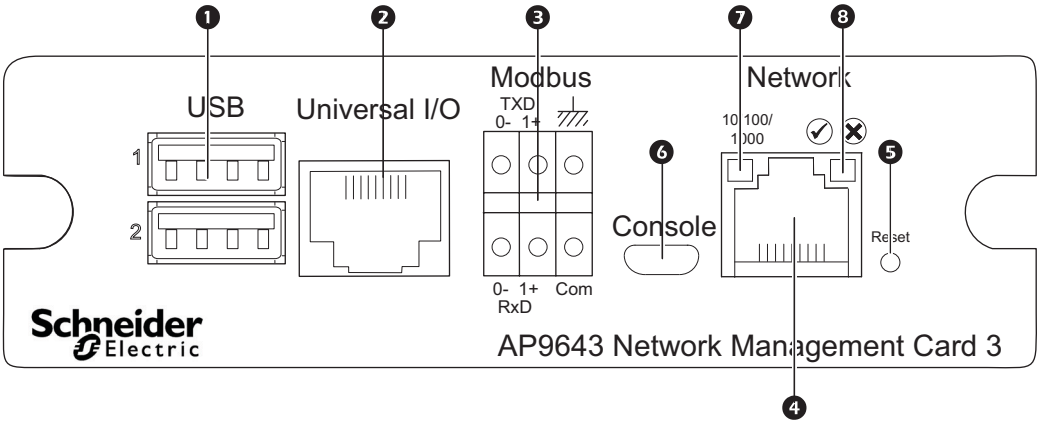
	Element	Beschreibung
1	Port für USB-Konsole	Zum Anschluss der Netzwerkmanagement-Karte über ein Micro-USB-Kabel (APC-Teilenummer 960-0603) an einen lokalen Computer, zur erstmaligen Konfiguration der Netzwerkeinstellungen und für den Zugriff auf die Befehlszeilenoberfläche.
2	10/100/1000 Base-T-Anschluss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

Frontblende (AP9641)



	Element	Beschreibung
1	USB-Anschlüsse	Unterstützung für NMC- und USV-Firmware-Updates. Siehe „**NMC Firmware-Upgrades**“, „**Aktualisierung der USV-Firmware mit einem USB-Speichermedium (nur AP9641, AP9643 und eingebettete NMC-Geräte)**“.
2 **3**	Universelle E/A-Anschlüsse (UIO-Ports)	Anschluss von Temperatursensoren, kombinierten Temperatur-/Feuchtigkeitssensoren, Eingabe/Ausgabe-Relaiszusatzsteckern und Flüssigkeitssensor (Spot Fluid Sensor) an den UIO-Port (v3.1.x und höher). Der Eingabe/Ausgabe-Relaiszusatzstecker verfügt über zwei Eingangskontakte und ein Ausgangsrelais.
4	10/100/1000 Base-T-Anschluss	Anschluss der Netzwerkmanagement-Karte an das Ethernet-Netzwerk.
5	Taste „Reset“	Ermöglicht das Zurücksetzen der Netzwerkmanagement-Schnittstelle. **Hinweis:** Die Ausgangsleistung des Geräts, in dem die Netzwerkmanagement-Karte installiert ist, wird dadurch nicht beeinträchtigt.
6	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.
7	Link-RX/TX-LED (10/100/1000)	Siehe „Link-RX/TX-LED (10/100/1000)“.
8	Status-LED	Eine LED (Leuchtdiode) ist eine Lichtquelle. Siehe „Status-LED“.

Frontblende (AP9643)



	Element	Beschreibung
1	USB-Anschlüsse	Unterstützung für NMC- und USV-Firmware-Updates. Siehe „**NMC Firmware-Upgrades**“, „**Aktualisierung der USV-Firmware mit einem USB-Speichermedium (nur AP9641, AP9643 und eingebettete NMC-Geräte)**“.
2	Universeller E/A-Anschluss (UIO-Port)	Anschluss von Temperatursensoren, kombinierten Temperatur-/Feuchtigkeitssensoren, Eingabe/Ausgabe-Relaiszusatzsteckern und Flüssigkeitssensor (Spot Fluid Sensor) an den UIO-Port (v3.1.x und höher). Der Eingabe/Ausgabe-Relaiszusatzstecker verfügt über zwei Eingangskontakte und ein Ausgangsrelais.
3	Modbus-Stecker	Zum Verbinden der Netzwerkmanagement-Karte mit einem Building Management System (BMS). Zwei Klemmleisten-Steckverbinder sind im Lieferumfang enthalten (Teilenummer 730-0532). Lesen Sie in den Anleitungen Ihrer USV nach, ob Modbus von Ihrer USV unterstützt wird.
4	10/100/1000 Base-T-Anschluss	Anschluss der Netzwerkmanagement-Karte an das Ethernet-Netzwerk.
5	Taste „Reset“	Ermöglicht das Zurücksetzen der Netzwerkmanagement-Schnittstelle. **HINWEIS:** Die Ausgangsleistung des Geräts, in dem die Netzwerkmanagement-Karte installiert ist, wird dadurch nicht beeinträchtigt.
6	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.
7	Link-RX/TX-LED (10/100/1000)	Siehe „Link-RX/TX-LED (10/100/1000)“
8	Status-LED	Eine LED (Leuchtdiode) ist eine Lichtquelle. Siehe „Status-LED“.

Bei eingebetteten NMC3-Geräten innerhalb einer USV finden Sie die Platzierung der verschiedenen NMC-Anschlüsse im Benutzerhandbuch, das dem Gerät beiliegt.

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 „Info zur Netzwerkmanagement-Karte und den Firmware-Modulen“.
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** zur Netzwerkmanagement-Karte beschrieben.
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 15 Sekunden, damit Zeit für den Zugriff auf den Boot-Monitor bleibt. 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.
Grünes Dauerleuchten	Die Netzwerkmanagement-Karte ist mit einem Netzwerk verbunden, das mit einer Geschwindigkeit von 1000 MBit/s arbeitet.

Zustand	Beschreibung
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 3 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 3 besitzt interne Selbstüberwachungsmechanismen, mit denen der Zugriff über das Netzwerk gewährleistet wird. Wenn die Netzwerkmanagement-Karte 3 beispielsweise 9,5 Minuten lang keinen direkten oder indirekten Netzverkehr (z. B. SNMP-Daten oder Daten eines Broadcast-Protokolls wie ARP [Address Resolution Protocol]) 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 3 immer dann neu gestartet wird, wenn 9,5 Minuten lang keine Daten über das Netzwerk übertragen wurden, versucht die Netzwerkmanagement-Karte 3 alle 4,5 Minuten, das Standardgateway zu erreichen. Wenn das Gateway vorhanden ist, antwortet es der Netzwerkmanagement-Karte 3, 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 3 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.

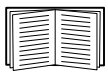
Automatische Abmeldung	Dauer (min)
Standard	3
Min.	1
Max.	60 (1 h)

Web-Benutzeroberfläche

Einführung

Übersicht

Die Web-Benutzeroberfläche enthält Optionen zur Verwaltung der USV und der Netzwerkmanagement-Karte 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 NMC ist kompatibel mit den neuesten Versionen von:

- Microsoft Edge
- Firefox
- 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. In v3.0.x und höher wird das Kennwort bei der Eingabe nicht angezeigt. Wenn die Anmeldung nicht erfolgreich ist, wird eine entsprechende Meldung angezeigt. 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. Weitere Informationen finden Sie unter „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*.

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	Der Webzugriff ist deaktiviert oder die URL wurde nicht richtig eingegeben.

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. Beim Einloggen in die Web-Benutzeroberfläche werden Sie gefragt, ob Sie am Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) für die Netzwerkmanagement-Karte teilnehmen möchten. Sie können nicht fortfahren, ohne Ihre Auswahl zu treffen. Sie können dem CEIP unter **Konfiguration > CEIP > Einstellungen** jederzeit beitreten oder austreten. Weitere Informationen finden Sie unter **CEIP im Menü „Konfiguration“**. Anschließend 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.

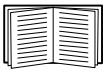
Symbole und Links

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** mit nützlichen Informationen zur Fehlersuche
- Link 2: die Seite **Product Information** mit Hintergrundinformationen zu Ihrer Hardware



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“
- Steckdosengruppen im Menü „Status“
- Batteriesystem im Menü „Status“
- Universeller E/A im Menü „Status“
- Netzwerk im Menü „Status“

USV im Menü „Status“

Befehlsfolge: Status > USV

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

Feld	Beschreibung
Letztes Umschalten auf Batterieversorgung	Die Ursache für die letzte Umschaltung auf Batterieversorgung. Kein Selbsttest.
Innentemperatur	Temperatur im Inneren der USV.
Verbleibende Laufzeit	Wie lange die USV die angeschlossene Last mit Batteriestrom versorgen kann.
USV-Eingang	
Input Voltage (Eingangsspannung)	Die von der USV empfangene Wechselspannung.
Bypass-Eingangsspannung	Die verwendete Wechselspannung, wenn sich die USV im Bypass-Betrieb befindet. Diese Option ist nicht bei allen USV-Geräten verfügbar.
USV-Ausgang	
Output Voltage (Ausgangsspannung)	Die Wechselspannung, die die USV an die angeschlossene Last liefert.
Laststrom	Der Strom in Ampere, der durch die Eingangsspannung bereitgestellt wird.
Ausgangslast	Die durch die angeschlossenen Geräte erzeugte Last auf jeder Phase in kVA.
Prozentuale Ausgangslast	Die durch die angeschlossenen Geräte erzeugte Last auf jeder Phase als Prozentsatz der verfügbaren Leistung in kVA ohne Redundanz.
Prozentuale Ausgangsleistung	Die durch die angeschlossenen Geräte erzeugte Last auf jeder Phase als Prozentsatz der verfügbaren Leistung in kVA.
Ausgangsleistung Watt	Die Last an der USV als Prozentsatz der verfügbaren Leistung in Watt.
Ausgangsleistung VA	Die Last an der USV als Prozentsatz der verfügbaren Leistung in VA.
Ausgangsleistung	Der Prozentsatz der direkt an die Last gespeisten Eingangsleistung. Die nicht an die Last gespeiste Eingangsleistung wird von der USV verbraucht.
Ausgangsenergieverbrauch	Die von der Last verwendete Energie, beginnend mit der letzten USV-Zurücksetzung auf die Standardwerte.

Feld	Beschreibung
Batteriestatus	
Batteriekapazität	Die Batteriekapazität der USV in Prozent, die verfügbar ist, um die angeschlossenen Geräte mit Strom zu versorgen.
Batteriespannung	Die Gleichstromspannung der Batterien.
Externe Batterien	Die Anzahl der an die USV angeschlossenen Batterien ohne interne Batterien.

Die folgenden Optionen stehen nicht für alle USV-Geräte zur Verfügung.

Feld	Beschreibung
Batteriespannungsnennwert	Die Nennspannungskapazität der USV-Batterien; die Gleichstromnennspannung, die die Batterien liefern können, wenn die USV ihre Batterie als Ausgangsversorgung verwendet.
Tatsächliche Batteriebusspannung	Die verfügbare Gleichstromspannung.
Nennwert des externen Batterieschranks	Die Anzahl der Amperestunden eines externen Batterieschranks.
Batterien	Die Gesamtanzahl der Batterien (intern und extern) der USV.
Fehlerhafte Batterien	Die Anzahl fehlerhafter Batterien (Batterien, die ausgetauscht werden müssen).
Batteriestrom	Der Ausgangsstrom der Batterie.
Datum des nächsten Batterieaustauschs	Das früheste empfohlene Datum für den Austausch Ihrer Batterien in den eingebauten USV-Batteriekassetten.
Intelligenzmodul	Informationen über das Intelligenzmodul. Sie werden unter Umständen um diese Informationen gebeten (Firmwareversion, Herstellungsdatum, Seriennummer und Hardwareversion), wenn Sie sich an den APC-Kundendienst wenden.
Input Voltage (Eingangsspannung)	Die von der USV empfangene Wechselspannung.
Bypass-Eingangsspannung	Die verwendete Wechselspannung, wenn sich die USV im Bypass-Betrieb befindet.
Eingangsfrequenz	Die Frequenz der von der USV empfangenen Spannung in Hertz (Hz).
Frequenz	Die von der Eingangs- und Ausgangsspannung gemeinsam genutzte Frequenz in Hertz (Hz).
Bypass-Frequenz	Die von der Spannung verwendete Frequenz in Hertz (Hz), wenn sich die USV im Bypass-Betrieb befindet.
Ausgangsstrom	Der an die Last gespeiste Strom in Ampere.
Output Frequency (Ausgangsfrequenz)	Die Frequenz der Ausgangsspannung in Hertz (Hz).
Lastleistung	Die Last an der USV als Prozentsatz der verfügbaren Leistung in Watt.
Scheinbare Lastleistung	Die Last an der USV als Prozentsatz der verfügbaren Leistung in VA.
Module	Informationen über die in der USV installierten Module. Sie werden unter Umständen um diese Informationen gebeten (Firmwareversion, Herstellungsdatum, Seriennummer und Hardwareversion), wenn Sie sich an den APC-Kundendienst wenden.

Feld	Beschreibung
Stromversorgungsmodul	Informationen über das in der USV installierte Stromversorgungsmodul. Sie werden unter Umständen um diese Informationen gebeten, wenn Sie sich an den APC-Kundendienst wenden.

Befehlsfolge: Status > USV > Messungen

Die folgenden Optionen gelten nur für USV-Geräte mit dem SRTL/SRYLF-Präfix mit integrierter Netzwerkmanagement-Karte.

Hier sehen Sie die verbleibende USV-Laufzeit, Batterieladung, Spannung und andere nützliche Informationen.

Feld	Beschreibung
Letztes Umschalten auf Batterieversorgung	Die Ursache für die letzte Umschaltung auf Batterieversorgung. Kein Selbsttest.
Verbleibende Laufzeit	Wie lange die USV die angeschlossene Last mit Batteriestrom versorgen kann.
USV-Eingang	
Eingangsspannung	Die von der USV empfangene Wechselspannung.
Frequenz	Die von der USV empfangene Frequenz in Hertz (Hz).
USV-Ausgang	
Ausgangsspannung	Die Wechselspannung, die die USV an die angeschlossene Last liefert.
Frequenz	Die von der USV gesendete Frequenz in Hertz (Hz).
Laststrom	Der Strom in Ampere, der durch die Eingangsspannung bereitgestellt wird.
Ausgangsleistung VA	Die Last an der USV als Prozentsatz der verfügbaren Leistung in VA.
Ausgangsleistung Watt	Die Last an der USV als Prozentsatz der verfügbaren Leistung in Watt.
Ausgangsenergieverbrauch	Die von der Last verwendete Energie, beginnend mit der letzten USV-Zurücksetzung auf die Standardwerte.
Leistungsfaktor	Dieser Wert gibt an, wie effektiv Sie Strom verbrauchen. Der ideale Wert ist 1; alles unter 1 zeigt an, dass es elektrische Verluste gibt.
Ausgangsleistung	Der Prozentsatz der direkt an die Last gespeisten Eingangsleistung. Die nicht an die Last gespeiste Eingangsleistung wird von der USV verbraucht.
Batteriestatus	
Ladezustand	Die Batteriekapazität der USV in Prozent, die verfügbar ist, um die angeschlossenen Geräte mit Strom zu versorgen.
Batteriespannung	Die Gleichstromspannung der Batterien.
Zustand	Dazu gehören alle Fehler des Batteriesystems einschließlich der einzelnen Rahmenfehler. Fehler werden als Ereignisse protokolliert.
Datum des nächsten Batterieaustauschs	Das früheste empfohlene Datum für den Austausch Ihrer Batterien in den eingebauten USV-Batterierahmen.

Befehlsfolge: Status > USV > Übersicht

Die folgenden Optionen gelten nur für USV-Geräte mit dem Präfix SRYLF und eingebetteter Netzwerkmanagement-Karte.

Diese Seite zeigt Ihnen, was in verschiedenen Positionen des USV-Hauptrahmens vorhanden ist. Zum Beispiel: Leistungsmodul, Batteriemodul, Intelligenzmodul, externer Batterierahmen.

Befehlsfolge: Status > USV > Stromversorgung

Die folgenden Optionen gelten nur für USV-Geräte mit dem Präfix SRYLF und eingebetteter Netzwerkmanagement-Karte.

Auf dieser Seite werden die vorhandenen Leistungsmodule, ihre Position und der Status der einzelnen Module angezeigt.

Befehlsfolge: Status > USV > Batterie

Die folgenden Optionen gelten nur für USV-Geräte mit dem SRTL/SRYLF-Präfix mit integrierter Netzwerkmanagement-Karte.

Hier erhalten Sie eine Übersicht über den Status des Batteriesystems und des Batterierahmens.

Feld	Beschreibung
Batteriesystemstatus	
Batteriekapazität	Die Batteriekapazität der USV in Prozent, die verfügbar ist, um die angeschlossenen Geräte mit Strom zu versorgen.
Verbleibende Laufzeit	Wie lange die USV die angeschlossene Last mit Batteriestrom versorgen kann.
Batteriespannungs-Nennwert	Die Nennspannungskapazität der USV-Batterien; die Gleichstromnennspannung, die die Batterien liefern können, wenn die USV ihre Batterie als Ausgangsversorgung verwendet.
Tatsächliche Batteriebusspannung	Die verfügbare Gleichstromspannung.
Maximale Batterietemperatur über alle Module hinweg	Die höchste Temperatur aller installierten Module.
Minimale Batterietemperatur über alle Module hinweg	Die niedrigste Temperatur aller installierten Module.
Maximale Zellspannung	Die höchste Spannung aller Zellen in allen installierten Modulen.

Feld	Beschreibung
Minimale Zellspannung	Die niedrigste Spannung aller Zellen in allen installierten Modulen.
Batterierahmenstatus	
Status	Der Status des Batterierahmens sowie der Status der einzelnen Batterierahmen. Neben „OK“ zeigt dieser Wert an, dass die Batterielebensdauer bald zur Neige geht oder für das Modul überschritten wurde. Fehler werden als Ereignisse protokolliert.
Kritisch	Wenn ein höherer Wert als 0 angezeigt wird, liegt ein Problem mit dem Batterierahmen vor, das sofort behoben werden sollte.
Warnung	Wenn ein höherer Wert als 0 angezeigt wird, liegt ein Problem mit dem Batterierahmen vor, das möglicherweise behoben werden muss.
Gut	Wenn ein höherer Wert als 0 angezeigt wird, funktioniert alles wie erwartet.
Frei	Wenn ein höherer Wert als 0 angezeigt wird, ist kein Batterie-Modul in einem Steckplatz installiert.

Klicken Sie auf das Hauptmenü oder XRn/Batterierahmen n, um zum Bildschirm Batteriestatus: Hauptrahmen / Batteriestatus: Batterierahmen n zu gelangen.

Feld	Beschreibung
Modul	Das Batterie-Modul und seine Position innerhalb des Rahmens.
Status	Der Status des Batterierahmens. Neben „OK“ zeigt dieser Wert an, dass die Batterielebensdauer bald zur Neige geht oder überschritten wurde. Fehler werden als Ereignisse protokolliert.
Zustand	Dazu zählen alle Fehler am Batteriesystem. Fehler werden als Ereignisse protokolliert.
Letzter Batterieaustausch	Das Datum, an dem die Batterie zuletzt ausgetauscht wurde.

Befehlsfolge: Status > USV > Intelligenzmodul

Die folgenden Optionen gelten nur für USV-Geräte mit dem Präfix SRYLF und eingebetteter Netzwerkmanagement-Karte.

Auf dieser Seite werden die vorhandenen Intelligenzmodule, ihre Position und der Status der einzelnen Module angezeigt.

Steckdosengruppen im Menü „Status“

Befehlsfolge: Status > Steckdosengruppen

Diese Option ist nicht bei allen USV-Geräten verfügbar. Sie zeigt die Statusdetails aller Steckdosengruppen auf der USV an. Weitere Informationen finden Sie unter Steckdosengruppen im Menü „Steuerung“ und Steckdosengruppen im Menü „Konfiguration“.

Batteriesystem im Menü „Status“

Befehlsfolge: Status > Batteriesystem

Diese Option ist nicht bei allen USV-Geräten verfügbar.

Feld	Beschreibung
Batteriesystemstatus	
Ladezustand	Die Batteriekapazität der USV in Prozent, die verfügbar ist, um die angeschlossenen Geräte mit Strom zu versorgen.
Verbleibende Laufzeit	Wie lange die USV die angeschlossene Last mit Batteriestrom versorgen kann.
Positive Busspannung	Das USV-Gerät unterstützt sowohl positive als auch negative Batteriespannungen.
Negative Busspannung:	
Artikelnummer der Austausch-Batteriekassette	Die Artikelnummer, die Sie angeben müssen, um eine Austausch-Batteriekassette zu erhalten.
Batterie-Modul-Status	
Batterie-Modul 1, 2...	Die Batterie-Modul-Nummer leitet sich von der internen Nummerierung ab.
Seriennummer	Die Seriennummer des Batterie-Moduls.
Zustand	Dazu zählen Systemfehler am Batterie-Modul sowie Fehler an den einzelnen Batteriekassetten. Fehler werden als Ereignisse protokolliert.
Status	Der Status des Batterie-Moduls sowie der Status der einzelnen Batteriekassetten. Neben „OK“ zeigt dieser Wert an, dass die Batterielebensdauer bald zur Neige geht oder für das Modul überschritten wurde. Fehler werden als Ereignisse protokolliert.

Klicken Sie auf „Batterie-Modul 1, 2...“, um die Bildschirmseite **Batterie-Modul n** aufzurufen.

Feld	Beschreibung
Batterie-Modul 1, 2... **oder** **Internes Modul**	
Seriennummer (sofern vorhanden)	Die Seriennummer des Batterie-Moduls.
Firmware-Version	Die Versionsnummer des Batterie-Moduls.
Temperatur	Die vom Sensor gemeldete Temperatur im Batteriefach.
Modulstatus	Nur Fehler am Batterie-Modul ohne Fehler an den einzelnen Batteriekassetten. Fehler werden als Ereignisse protokolliert und können wie folgt lauten: • Temperatur nicht im Bereich • allgemeine Fehler • Kommunikationsfehler • ein nicht angeschlossener Modulrahmen • nicht mit der Hardware kompatible Firmware

Feld	Beschreibung
Batteriekassette 1 und (sofern vorhanden) **Batteriekassette 2**	
Zustand	Dieser kann OK sein, die Batterielebensdauer geht bald zur Neige, die Batterielebensdauer wurde überschritten oder es wurde ermittelt, dass die Batterielebensdauer für die Kassette zur Neige geht. Fehler werden als Ereignisse protokolliert.
Installationsdatum	Das Datum, an dem die einzelnen Batteriekassetten eingebaut wurden. Sie können dieses Datum bearbeiten.
Vorhergesagtes Austauschdatum	Die USV berechnet, wann die Batterie ausgetauscht werden sollte. Das obige Feld **Zustand** leitet sich von diesem Datum ab.
Status	Dieser bezieht sich auf eine bestimmte Batteriekassette. Siehe „Modulstatus“ oben für allgemeine Modulfehler. Fehler werden als Ereignisse protokolliert und können wie folgt lauten: • nicht angeschlossene Batteriekassette • Batteriekassette muss ausgetauscht werden • Batteriekassettentemperatur ist zu hoch: kritisch • Batteriekassettentemperatur ist zu hoch: Warnung. Diese Meldung wird üblicherweise, aber nicht immer vor „kritisch“ angezeigt.

Universeller E/A im Menü „Status“

Befehlsfolge: Status > Universeller E/A

Diese Option ist nicht bei allen Geräten verfügbar.

Unter **Temperatur und Luftfeuchtigkeit** wird der Name, der Alarmzustand, die Temperatur und die Luftfeuchtigkeit (sofern unterstützt) für jeden Sensor angezeigt. Klicken Sie auf den Namen eines Sensors, um Name und Standort zu bearbeiten sowie um die Grenzwerte und die Hysterese zu konfigurieren. Weitere Informationen finden Sie unter Bildschirm „Temperatur und Luftfeuchtigkeit“.

Unter **Eingangskontakte** werden der Name, der Alarmzustand und der Status (offen oder geschlossen) jedes Kontakts angezeigt. Diese Informationen werden automatisch ermittelt und hier angezeigt, wenn Sie das Umgebungszubehör installieren. Klicken Sie auf den Namen eines Eingangskontakts, um ausführliche Angaben zu dessen Alarmzustand anzuzeigen oder um seine Werte zu konfigurieren. Wenn Kontakte konfiguriert und deaktiviert wurden, werden sie hier nicht angezeigt. Weitere Informationen finden Sie unter Bildschirm „Eingangskontakte“.

Unter **Ausgangsrelais** werden der Name und der Status (offen oder geschlossen) jedes Relais angezeigt. Diese Informationen werden automatisch ermittelt und hier angezeigt, wenn Sie das Umgebungszubehör installieren. Klicken Sie auf den Namen eines Ausgangsrelais, um den detaillierten Status anzuzeigen oder seine Werte zu konfigurieren. Weitere Informationen finden Sie unter Bildschirm „Ausgangsrelais“.

Unter **Flüssigkeitssensor** (v3.1.x und höher) werden der Name, der Alarmzustand und der Status (Flüssigkeit erkannt oder keine Flüssigkeit) jedes Flüssigkeitssensors angezeigt. Diese Informationen werden automatisch ermittelt und hier angezeigt, wenn Sie das Umgebungszubehör installieren. Klicken Sie auf den Namen des Flüssigkeitssensors, um einen detaillierten Status zu erhalten oder seine Werte zu konfigurieren. Weitere Informationen finden Sie im **Bildschirm „Flüssigkeitssensor“ (v3.1.x und höher)**.

Unter **Letzte Umgebungsereignisse** werden Ereignisse in Verbindung mit Ihrer Umgebungsüberwachung angezeigt, zum Beispiel ein über- oder unterschrittener Temperaturschwellenwert oder eine Warnung in Bezug auf einen Umgebungsüberwachungs-Eingangskontakt. Klicken Sie auf den Link „Mehr Ereignisse“, um eine vollständige Liste aller jüngsten Ereignisse anzuzeigen.

Netzwerk im Menü „Status“

Befehlsfolge: Status > Netzwerk

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

USV-Steuerung

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

Siehe dazu die folgenden Abschnitte:

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

USV im Menü „Steuerung“

Befehlsfolge: Steuerung > USV

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.

Die Aktionen variieren je nachdem, ob Sie ein USV-Gerät mit Steckdosengruppen verwenden oder nicht. Dies wird in den beiden nachfolgenden Tabellen separat behandelt.

- Aktionen im USV-Bildschirm für Geräte MIT Steckdosengruppen.
- Aktionen im USV-Bildschirm für Geräte **OHNE** Steckdosengruppen.

Die Kontrollkästchen des Bildschirms direkt im Anschluss gelten für beide Tabellen.

Kontrollkästchen	Beschreibung
Signal PowerChute Network Shutdown-Clients	Wenn kein PowerChute-Client vorhanden ist, ist die Option bei einer USV mit Steckdosengruppen ausgegraut (siehe PowerChute Network Shutdown-Clients). 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 Network Shutdown-Parameter** konfigurierten Werten herunterzufahren (siehe „Herunterfahren“ im Menü „Konfiguration“). Allerdings werden mit dieser Option keine Server benachrichtigt, wenn Bypass-Steuerungsaktionen durchgeführt werden.
Abschaltverzögerungen für Steckdosen überspringen	Diese Option ist nur für einer USV mit Steckdosengruppen verfügbar. Schaltet Steckdosen umgehend ab und überspringt die konfigurierten Verzögerungen für Steckdosengruppen. Sie sollten diese Option nur im Notfall aktivieren, oder um Laufzeit zu sparen. Es kann auch sein, dass die Lastgeräte bereits manuell abgeschaltet wurden.

Weitere Informationen über Verzögerungen und Einstellungen finden Sie unter „Herunterfahren“ im Menü „Konfiguration“, „Bildschirme „Universeller E/A““ und „Steckdosengruppen im Menü „Steuerung““.

Aktionen im USV-Bildschirm für Geräte MIT Steckdosengruppen

Vorgang	Beschreibung
USV-Steckdosengruppen neu starten	Führt den Befehl „Sofort herunterfahren, Neustart bei Netzstrom“ bei allen Steckdosengruppen aus (siehe „Steckdosengruppen im Menü „Steuerung““). Klicken Sie auf „Weiter“, um bestimmte Informationen zu Zeit und Verzögerungen anzuzeigen. Schaltet die Ausgangsversorgung der geschalteten Steckdosengruppen und dann (sofern vorhanden) die der Hauptsteckdosengruppe aus. Jede Steckdosengruppe, auf die die Aktion angewendet wird, wartet die unter Neustartdauer und Einschaltverzögerung konfigurierte Anzahl an Sekunden. (Anschließend schalten sich die Steckdosengruppen ein, wenn Wechselspannung zur Verfügung steht, oder warten mit dem Einschalten, bis Wechselspannung verfügbar ist. Siehe „Was sind Steckdosengruppen?“.) Die USV schaltet sich ein, wenn Wechselspannung zur Verfügung steht oder wartet mit dem Einschalten, bis Wechselspannung verfügbar ist.
USV-Steckdosengruppen einschalten	Schaltet die Hauptsteckdosengruppe (sofern vorhanden) und dann alle geschalteten Steckdosengruppen ein. Diese Option wird nur angezeigt, wenn die USV aktuell abgeschaltet ist. Klicken Sie auf „Weiter“, um bestimmte Informationen zu Zeit und Verzögerungen anzuzeigen. Dann schaltet sich die USV und die Steckdosengruppen ein.
USV-Steckdosengruppen abschalten	Schaltet die Ausgangsversorgung der geschalteten Steckdosengruppen und dann (sofern vorhanden) die der Hauptsteckdosengruppe aus. Jede Steckdosengruppe, auf die diese Aktion angewendet wird, bleibt ausgeschaltet, bis Sie die Stromversorgung wieder einschalten. Klicken Sie auf „Weiter“, um bestimmte Informationen zu Zeit und Verzögerungen anzuzeigen.
USV-Steckdosengruppen in Ruhezustand versetzen	Versetzt die USV-Steckdosengruppen in den Ruhezustand, indem die Ausgangsversorgung der USV über einen durch die folgenden Parameter definierten Zeitraum abgeschaltet wird. Klicken Sie auf „Weiter“, um bestimmte Informationen zu Zeit und Verzögerungen anzuzeigen. • Die Steckdosengruppen warten die als Abschaltverzögerung konfigurierte Zeit, bevor die Stromversorgung abgeschaltet wird. • Wenn die Eingangsversorgung wieder vorliegt, schaltet die USV die Ausgangsversorgung nach Ablauf zweier konfigurierter Wartezeiten wieder ein: Ruhezustand-Zeit und Einschaltverzögerung. Dann schaltet sich die USV aus. Nach der unter „Ruhezustand“ konfigurierten Zeit schaltet sich die USV ein, wenn Wechselspannung zur Verfügung steht oder wartet mit dem Einschalten, bis Wechselspannung verfügbar ist.
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. Diese Optionen sind nur für Symmetra UPS und einige Smart-UPS-Geräte verfügbar.

Weitere Informationen über Verzögerungen und Einstellungen finden Sie unter „Herunterfahren“ im Menü „Konfiguration“ und Steckdosengruppen im Menü „Steuerung“.

Aktionen im USV-Bildschirm für Geräte OHNE Steckdosengruppen

Vorgang	Beschreibung
USV neu starten	Hiermit starten Sie die angeschlossenen Geräte wie folgt. (Klicken Sie auf „Weiter“, um bestimmte Informationen zu Zeit und Verzögerungen anzuzeigen.) • Schaltet die Stromversorgung an der USV aus. • Schaltet die Stromversorgung der USV nach Erreichen des konfigurierten Prozentsatzes des Werts „Minimale Batteriekapazität“ (Konfiguration – Herunterfahren – Ende des Herunterfahrens, siehe „Konfigurieren der Reaktion eines Ausgangs auf Ereignisse“) ein.
USV einschalten	Hiermit schalten Sie die Stromversorgung der USV ein. Diese Option wird nur angezeigt, wenn die USV abgeschaltet ist. Klicken Sie auf „Weiter“, um bestimmte Informationen zu Zeit und Verzögerungen anzuzeigen.
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 „Verzögertes Abschalten und PowerChute Network Shutdown“ konfigurierten Wartezeit ab. • Wenn die Eingangsversorgung wieder vorliegt, schaltet die USV die Ausgangsversorgung nach Ablauf der als „Ruhezustand-Zeit“ konfigurierten Wartezeit wieder ein.
USV in Bypass-Modus versetzen und **USV aus Bypass-Modus schalten**	Diese Optionen steuern die Verwendung des Bypass-Betriebs, der es ermöglicht, Wartungsarbeiten an bestimmten Smart-UPS-Geräten durchzuführen, ohne die Stromversorgung der USV ausschalten zu müssen. Klicken Sie auf „Weiter“, um bestimmte Informationen zu Zeit und Verzögerungen anzuzeigen. Diese Optionen sind nur für Symmetra UPS und einige Smart-UPS-Geräte verfügbar.

Steckdosengruppen im Menü „Steuerung“

Befehlsfolge: Steuerung > Steckdosengruppen

Diese Option ist nicht bei allen USV-Geräten verfügbar.

Verwenden Sie diese Option, um einzelne Steckdosengruppen getrennt von dem USV-Gerät einzuschalten, abzuschalten oder neu zu starten. (Dieser Bildschirm führt den Namen und den Status jeder USV-Steckdosengruppe auf, die über die Option **Konfiguration - Steckdosengruppen** konfiguriert wurde. Siehe „Stromversorgungseinstellungen“ im Menü „Konfiguration“).

Sie können für jede Steckdosengruppe einen der folgenden Vorgänge (oder keinen Vorgang) auswählen. Es handelt sich um einmalige Aktionen.

- Wenn der Zustand der Steckdosengruppe **Aus** ist:
  - **Sofort ein**
  - **Einschalt mit Verzögerung**: Hiermit wird die Steckdosengruppe nach der als **Einschaltverzögerung** definierten Wartezeit in Sekunden eingeschaltet (Weitere Informationen finden Sie unter „Herunterfahren“ im Menü „Konfiguration“).
- Wenn der Zustand der Steckdosengruppe **Ein** ist:
  - **Sofort aus**
  - **Ausschalt mit Verzögerung:** Hiermit wird die Steckdosengruppe nach der als **Abschaltverzögerung** definierten Wartezeit in Sekunden ausgeschaltet (Weitere Informationen finden Sie unter „Herunterfahren“ im Menü „Konfiguration“).
  - **Sofort neu starten**: Hiermit wird die Steckdosengruppe sofort ausgeschaltet und anschließend nach der als **Neustartdauer** (siehe „Herunterfahren“ im Menü „Konfiguration“) und **Einschaltverzögerung** definierten Wartezeit in Sekunden wieder eingeschaltet.
  - **Neustart mit Verzögerung**: Hiermit wird die Steckdosengruppe nach der als **Abschaltverzögerung** konfigurierten Wartezeit in Sekunden ausgeschaltet und anschließend nach der als **Neustartdauer** und **Einschaltverzögerung** konfigurierten Wartezeit in Sekunden wieder eingeschaltet.
  - **Sofort herunterfahren, Neustart bei Netzstrom**: Hiermit wird die Steckdosengruppe sofort ausgeschaltet. Stellen Sie nach Ablauf der als **Neustartdauer** und **Einschaltverzögerung** konfigurierten Wartezeit in Sekunden sicher, dass wieder Netzspannung anliegt und die USV imstande ist, die Mindestlaufzeit nach einem Neustart zu überbrücken; schalten Sie dann die Gruppe ein.
  - **Verzögert herunterfahren, Netzspannung-Neustart**: Hiermit wird die Steckdosengruppe nach der als **Abschaltverzögerung** definierten Wartezeit in Sekunden ausgeschaltet. Stellen Sie nach Ablauf der als **Neustartdauer** und **Einschaltverzögerung** konfigurierten Wartezeit in Sekunden sicher, dass wieder Netzspannung anliegt und die USV imstande ist, die Mindestlaufzeit nach einem Neustart zu überbrücken; schalten Sie dann die Gruppe ein.

Nachdem Sie einen Vorgang ausgewählt haben, klicken Sie auf „Weiter“, um eine detaillierte Beschreibung des Vorgangs einschließlich der Dauer etwaiger Verzögerungen angezeigt zu bekommen. Klicken Sie auf „Übernehmen“, um den Vorgang zu starten.

„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“

Web-CLI

Pfad: Steuerung > Netzwerk- > Web-CLI

Stellt eine webbasierte Befehlszeilenschnittstelle (CLI) für den aktuell angemeldeten Benutzer bereit.

Zurücksetzen/neu starten

Pfad: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 Menü „Benachrichtigungen“
	Alarme bei unterbrochener Umgebungskommunikation: Hiermit setzen Sie den Alarm bei unterbrochener Umgebungskommunikation zurück, der ausgelöst wird, wenn das Gerät eines universellen E/A-Anschlusses ausgesteckt wird.
	Steuerungsrichtlinie: Hiermit setzen Sie die Einstellungen zurück, mit denen festgelegt wird, wie die Netzwerkmanagement-Karte auf Alarme reagieren soll, die am E/A-Zusatzmodul für potenzialfreie Kontakte vorgefunden wurden.

[1]Das Zurücksetzen der Netzwerkmanagement-Karte kann bis zu einer Minute dauern. Der von Ihnen konfigurierte USV-Name wird nicht zurückgesetzt (siehe Bildschirm „USV Allgemein“).

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“.

- Steckdosengruppen im Menü „Konfiguration“
- „Stromversorgungseinstellungen“ im Menü „Konfiguration“
- „Herunterfahren“ im Menü „Konfiguration“
- Bildschirm „USV Allgemein“
- Bildschirm „Selbsttest-Planung“
- „Planung für das Herunterfahren“
- „Bildschirm Firmware-Aktualisierung“
- „PowerChute Network Shutdown-Clients“
- Bildschirme „Universeller E/A“
- Menü „Sicherheit“

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

Steckdosengruppen im Menü „Konfiguration“

Pfad: Konfiguration > Steckdosengruppen

Diese Option ist nicht bei allen USV-Geräten verfügbar. Sie können damit Ihre Steckdose und Sequenzierungsverzögerungen anzeigen und konfigurieren.

Siehe auch Steckdosengruppen im Menü „Steuerung“ und „Herunterfahren“ im Menü „Konfiguration“.

Was sind Steckdosengruppen?

Steckdosengruppen sind nur bei bestimmten USV-Geräten verfügbar. Um festzustellen, ob Ihr USV-Gerät Steckdosengruppen unterstützt, sehen Sie bitte in der Dokumentation zur USV nach.

Die verfügbaren Einstellungen variieren je nach USV-Gerät.

Hauptsteckdosengruppen. Einige USV-Geräte stellen einer Hauptsteckdosengruppe Wechselspannung zur Verfügung. Die Hauptsteckdosengruppe steuert die Stromverteilung an alle geschalteten Steckdosengruppen (sofern vorhanden) für die USV.

- Wenn die Hauptsteckdosengruppe ausgeschaltet ist, können die geschalteten Steckdosengruppen nicht eingeschaltet werden.
- Wenn Sie die Hauptsteckdosengruppe ausschalten, schaltet die USV zuerst die geschalteten Steckdosengruppen aus und dann die Hauptsteckdosengruppe.
- Zum Einschalten einer geschalteten Steckdosengruppe muss die USV zuerst die Hauptsteckdosengruppe einschalten.

Geschaltete Steckdosengruppen.

- Jede geschaltete Steckdose kann unabhängige Aktionen durchführen. Sie können diese Steckdosen der Reihe nach starten oder stoppen und außerdem an diese Steckdosen angeschlossene Geräte neu starten.

Konfigurieren Ihrer Steckdosengruppen

Name und Typ der Steckdosengruppe. Zeigen Sie den Namen, den Typ und Verzögerungen Ihrer USV-Steckdosen auf dem Bildschirm **Konfiguration – Steckdosengruppen** an. Klicken Sie auf den Namen einer Steckdosengruppe unter **Gruppe**, um deren Einstellungen wie Sequenzierungsverzögerungen und Lastabschaltungsoptionen zu ändern.

Sequenzierungseinstellungen. Diese Einstellungen variieren je nach USV-Gerät. Über die Sequenzierungsoptionen definieren Sie, wie die USV auf Befehle von Benutzern reagieren soll.

Feld	Beschreibung
Abschaltverzögerung	Wenn diese Steckdosengruppe eingeschaltet ist, wartet sie die eingestellte Verzögerung in Sekunden, bevor sie sich abschaltet. Wenn Sie hier verschiedene Zeiten für Steckdosen einstellen, können Sie ihre Abschaltungen sequenzieren, d. h. Sie können festlegen, in welcher Reihenfolge sie sich abschalten.
Neustartdauer	Die Steckdose wartet die eingestellte Zeit, bevor sie neu startet.
Einschaltverzögerung	Wenn diese Steckdosengruppe ausgeschaltet ist und ein Signal zum Einschalten erhält, wartet sie die eingestellte Verzögerung in Sekunden, bevor sie sich einschaltet. Wenn Sie hier verschiedene Zeiten für Steckdosen einstellen, können Sie ihre Einschaltungen sequenzieren.
Minimale Laufzeit für Neustart	Die Mindestüberbrückungsdauer, die von der USV für die Last bereitgestellt werden muss, damit sie wieder eingeschaltet werden kann.

Lastabschaltungsoptionen. Mithilfe der Lastabschaltung können Sie Bedingungen festlegen, bei denen die Leistung einzelner geschalteter Steckdosengruppen herabgesetzt wird.

Hinweis: Wenn Sie zum Verwalten Ihrer USV PowerChute Network Shutdown verwenden, empfehlen wir, die Lastabwurfoptionen für die Netzwerkmanagement-Karte nicht zu verwenden, da sie mit den in PowerChute angegebenen Einstellungen für die Steckdosengruppe in Konflikt stehen können.

Ein Beispiel für den Einsatz der Lastabschaltung wäre das Abschalten nicht kritischer Lasten wie Monitore, wenn die USV im Batteriebetrieb läuft oder überlastet ist. Dadurch werden die Batterieladung und die Laufzeit für wichtige Lasten gespart. Ein weiteres Beispiel wäre das Deaktivieren eines automatischen Neustarts nach einer Überlastung, um die Ursache der Überlastung zu ermitteln, bevor die Steckdosengruppe wieder eingeschaltet wird.

Mit den Optionen können Sie eine Steckdosengruppe abschalten, wenn EINE der folgenden von Ihnen festgelegten 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).
- Die USV ist überlastet (der Strombedarf der an die USV angeschlossenen Geräte übersteigt die Möglichkeiten der USV).

Sie können außerdem die folgenden Aktionen aktivieren:

- **Die Abschaltverzögerung der Steckdosengruppe überspringen**. (Dabei schalten Sie die Steckdosengruppe sofort aus, ohne die als **Abschaltverzögerung** definierte Wartezeit in Sekunden abzuwarten. In der Grundeinstellung ist diese Option deaktiviert.)
- **Nach Wiederherstellen der Stromversorgung ausgeschaltet bleiben**. (Ausgeschaltet bleiben, wenn wieder Netzspannung anliegt. Diese Option ist in der Grundeinstellung deaktiviert, d. h. die USV wartet die als **Einschaltverzögerung** konfigurierte Sekundenzahl ab und schaltet erst dann die Steckdosengruppen ein.)

Steckdosengruppen-Ereignisse und -Traps. Eine Veränderung des Zustands einer Steckdosengruppe erzeugt das Ereignis **USV: Steckdosengruppe eingeschaltet** mit dem Schweregrad „Zur Information“ oder **USV: Steckdosengruppe ausgeschaltet** mit dem Schweregrad „Warnung“. Das Format der Ereignismeldungen lautet „USV: Steckdosengruppe *Gruppennummer*, *Gruppenname*, *Vorgang* aufgrund *Ursache*“. Zum Beispiel:

```
USV: Steckdosengruppe 1, Webserver, eingeschaltet.
```

```
USV: Steckdosengruppe 3, ausgeschaltet.
```

Das Ereignis erzeugt immer einen Eintrag im Ereignisprotokoll, eine E-Mail und eine Syslog-Meldung.

Wenn Sie Trap-Empfänger für das Ereignis konfigurieren, wird Trap 298 erzeugt, wenn sich eine Steckdosengruppe einschaltet, und Trap 299, wenn sich eine Steckdosengruppe ausschaltet. Die Ereignismeldung ist das Trap-Argument. Der standardmäßige Schweregrad ist derselbe wie für das Ereignis.

„Stromversorgungseinstellungen“ im Menü „Konfiguration“

Pfad: Konfiguration > Stromversorgungseinstellungen

Die Befehlsfolge für USV-Geräte mit dem SRTL/SRYLF-Präfix mit einer integrierten Netzwerkmanagement-Karte lautet **Konfiguration > USV > Stromversorgungseinstellungen**.

Die verfügbaren Einstellungen variieren je nach USV-Gerät.

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

- Die höchsten und niedrigsten Angaben unter **Spannung** bestimmen den Bereich, in dem die USV die Batterieausgangsleistung automatisch an die Last anpasst. Dadurch wird die Last geschützt.

  Wenn der obere Spannungsgrenzwert überschritten wird, verwendet die USV die Funktion „AVR Trim“. Wenn der untere Spannungsgrenzwert unterschritten wird, verwendet die USV die Funktion „AVR Boost“ (oder schaltet in den Batteriebetrieb, wenn die USV nicht über diese Funktion verfügt).
- Durch die Aktivierung des **Energiespar-Modus** wird die USV im Bypass-Betrieb ausgeführt, was zu einem effizienteren Energieverbrauch führt. Allerdings wird in diesem Modus der benötigte Batteriestrom langsamer an die USV übertragen. Wenn Sie in Ihrer Umgebung eine schnelle Umschaltzeit benötigen, können Sie den Energiespar-Modus deaktivieren.
- Bei Schwankungen in der Eingangsversorgungsleitung schaltet die USV auf die Versorgung mit Batteriestrom um. Über **Empfindlichkeit** können Sie die Zeitspanne einstellen, nach der die USV auf Schwankungen reagiert. Verwenden Sie die Optionen **Reduziert** und **Niedrig**, wenn die USV ein Schwanken der Eingangsleitung über einen längeren Zeitraum tolerieren soll, bevor auf Batteriestrom umgeschaltet wird. Verwenden Sie **Niedrig**, wenn bekannt ist, dass die jeweilige Eingangsversorgung ein starkes Schwanken mit sich bringt, wie beispielsweise bei der Stromversorgung durch einen Generator.
- **Ausgangsleistung Watt**: die maximale Nennleistung, die die Anforderungen Ihrer Lastgeräte erfüllt.
- **Bypass**-Einstellungen zum Definieren von Zuständen, in denen die USV auf Bypass-Betrieb umschalten kann.
- **Alarmgrenzwerte** auf der Basis der verfügbaren Laufzeit und der redundanten Leistung sowie der USV-Last.
- **Ausgangsfrequenzbereich:** Der Bereich, in dem die USV den Onlinebetrieb aufrecht erhält, ohne auf Batteriebetrieb umzuschalten.
- **Anstiegsgeschwindigkeit der Ausgangsfrequenz:** Der maximale Umfang, den sich die Ausgangsfrequenz über einen bestimmten Zeitraum ändern kann, wenn die USV eine Phasensperre an der Eingangsquelle erhält. Dieser Wert wird in Hz/s (Hertz/Sekunde) ausgedrückt.

„Herunterfahren“ im Menü „Konfiguration“

Pfad: Konfiguration > Herunterfahren

Die Befehlsfolge für USV-Geräte mit dem SRTL/SRYLF-Präfix mit einer integrierten Netzwerkmanagement-Karte lautet **Konfiguration > USV > 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“.

Basic Signaling-Shutdown.

Basic Signaling bzw. „Simple Signaling“ ist eine einfache Kommunikationsmethode zwischen einer USV und einem Server, einer Arbeitsstation oder einem Fremdanbietersystem. Der Interface Expander 2 (AP9624) ist ein SmartSlot-Zubehör, das Ihrer USV die Verwendung von Simple Signaling ermöglicht. Simple Signaling gewährleistet ein sicheres Herunterfahren der USV und entsprechende Benachrichtigungen, jedoch ohne die bei Advanced oder Smart Signaling verfügbaren Funktionen zur stetigen, erweiterten Überwachung.

Hinweis: Bei Verwendung von PowerChute Network Shutdown wird der Einsatz von Basic Signaling Shutdown nicht empfohlen. Bei bestimmten USV-Modellen können Optionen wie Basic Shutdown-Verzögerung das Herunterfahren der USV beeinflussen und die „Betriebsdauer bei schwacher Batterie“ aufheben, die von PowerChute zur Berechnung der erforderlichen Gesamtzeit für das Herunterfahren verwendet wird.

Feld	Beschreibung
Basic Signaling-Shutdown	Aktivieren Sie Basic Signaling-Shutdown, wenn ein Server, eine Arbeitsstation oder ein Fremdanbietersystem über ein Basic-Signaling-Kabel mit Ihrer USV verbunden ist. Aktivieren Sie diese Option, wenn Ihre USV kein Advanced Signaling unterstützt oder für die Basic-Signaling-Kommunikation konfiguriert wurde.
Basic Betriebsdauer bei schwacher Batterie	Legt bei einer USV, die mit Batteriestrom läuft, fest, bei welcher verbleibenden Batterielaufzeit die USV einen niedrigen Batteriestand signalisiert. Die USV wird in diesem Fall: • Den niedrigen Batteriestand am USV-Display anzeigen. • Die Benachrichtigung „niedriger Batteriestand“ von der USV über das Simple-Signaling-Kabel an die angeschlossenen Geräte senden. Wird die Stromversorgung der USV nicht wieder hergestellt, schaltet sich diese bei aufgebrauchter Batterie aus. Diese Option ist nur für die Smart-UPS-Modelle SMT, SMX, SRC, SURTD und SRT verfügbar.
Basic Shutdown-Verzögerung	Legt fest, wie lange die USV wartet, bevor sie als Reaktion auf eine Basic Shutdown-Benachrichtigung herunterfährt. Nach Verstreichen dieser Zeitspanne fährt die USV unabhängig von der verbleibenden Batterielaufzeit herunter. Diese Option ist nur für die Smart-UPS-Modelle SMT, SMX, SRC, SURTD und SRT verfügbar.

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/Steckdosengruppe in den Ruhezustand versetzen. Wenn die USV/Steckdosengruppe ausgeschaltet wird, schaltet sie sich nach Verstreichen der hier festgelegten Ruhezustand-Zeit und der Neustartzeit oder Einschaltverzögerung wieder ein. Wurde die Netzstromversorgung noch nicht wiederhergestellt, wartet die USV mit dem Einschalten bis zu deren Wiederherstellung. Siehe „Herunterfahren“ im Menü „Konfiguration“. 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

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“.
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. • Befehle zum PCNS-Herunterfahren ignorieren - Die UPS wird heruntergefahren und ignoriert alle konfigurierten PowerChute-Befehle zum Herunterfahren.
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 Kommunikation sprotokolle	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. Diese Optionen sind **nicht** für die Smart-UPS-Modelle SMT, SMX, SRC, SURTD und SRT verfügbar. Informationen zur Steuerung des vorzeitigen Herunterfahrens von Steckdosengruppen bei diesen Modellen finden Sie unter „Lastabschaltungsoptionen“.

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.

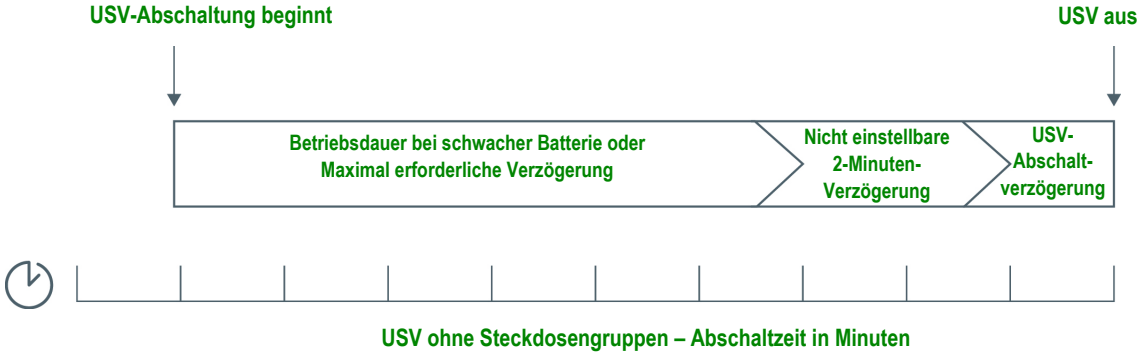
Im nachfolgenden Abschnitt wird erläutert, wie sich die Werte „Betriebsdauer bei schwacher Batterie“, „Maximal erforderliche Verzögerung“ und „Steckdosengruppen-Abschaltverzögerungen“ auf die PowerChute-Abschaltsequenz auswirken.

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.



USV ohne Steckdosengruppen – Abschaltzeit in Minuten

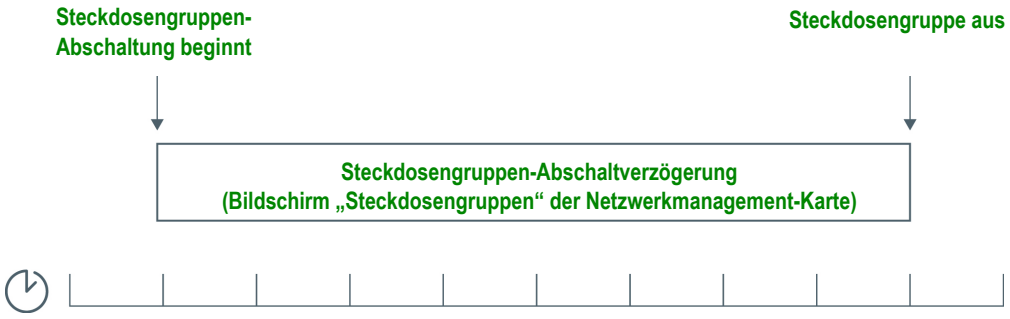
Hinweise:

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

•Als Ausnahme verwenden USV-Modelle mit Präfix SUM, die über Steckdosengruppen verfügen, die Methode der USV-Modelle ohne Steckdosengruppen, um die USV-Abschaltzeit zu berechnen.

USV mit Steckdosengruppen

Bei einer USV MIT Steckdosengruppen entspricht die Abschaltzeit dem Wert **Abschaltverzögerung** im Bildschirm **Steckdosengruppen** der Netzwerkmanagement-Karte (siehe Steckdosengruppen im Menü „Konfiguration“). (Nicht bei allen USV-Geräten verfügbar.)



USV mit Steckdosengruppen – Abschaltzeit in Minuten

Hinweise:

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

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.

Bildschirm „USV Allgemein“

Pfad: Konfiguration > USV

Die Befehlsfolge für USV-Geräte mit dem SRTL/SRYLF-Präfix mit einer integrierten Netzwerkmanagement-Karte lautet **Konfiguration > USV > Allgemein**.

Dieser Bildschirm ist nicht bei allen USV-Geräten verfügbar.

Einige der nachfolgend beschriebenen Optionen werden unter Umständen bei manchen USV-Geräten NICHT angezeigt.

Feld	Beschreibung
USV-Name	Ein Name zur Identifizierung der USV.
USV-Position	Die physische Ausrichtung der USV, Rack oder Tower.
Akustischer Alarm	Hiermit aktivieren oder deaktivieren Sie die Alarmtöne der USV und definieren bei bestimmten USV-Geräten den Zustand, der einen Alarmton auslöst.
LCD-Spracheinstellung	Geben Sie an, welche Sprache Sie für Ihre USV-Anzeige verwenden möchten.
LCD-Display	Schreibzugriff auf die USV-Anzeige deaktivieren oder aktivieren. Ist die Option deaktiviert, verfügt der Benutzer weiterhin über Lesezugriff auf die meisten Bildschirme, jedoch nicht auf Unterbildschirme der Menüs „Steuerung“ und „Konfiguration“.
Vorwarnzeit für Batteriezustandsalarm	Stellt die Anzahl der Tage ein, bevor der kritische Alarm für einen Batterieaustausch auf dem LCD-Display der USV angezeigt wird. Auf -1 eingestellt, wird keine Warnmeldung angezeigt.
Ruhezustand des Batteriezustandsalarms	Stellt die Anzahl der Tage ein, die der Batteriezustandsalarm im LCD-Display der USV nach der ersten Bestätigung im Ruhezustand verbringt, bevor er erneut angezeigt wird. Auf -1 eingestellt, wird nach Bestätigen der ersten Warnung keine weitere Warnung mehr angezeigt.
Last Battery Replacement (Einstellung)	Geben Sie Monat und Jahr des letzten USV-Batteriewechsels ein.

Feld	Beschreibung
Anzahl der Batterien oder **Externe 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.
Externer Batterieschrank	Die Anzahl der Amperestunden eines externen Batterieschranks.
Batterieladegerätfrequenz	Mit diesem Feld können Sie die Ladefrequenz der USV-Batterien prozentual ändern. Hier steht 100 % für die empfohlene Ladefrequenz des Herstellers. Um beispielsweise die Ladefrequenz zu verdoppeln, muss dieser Wert auf 200 % gesetzt werden. Wenn die Batterieladegerätfrequenz beispielsweise auf 100 % gesetzt ist: • Wenn die Gesamtbatteriekapazität erhöht wird, wird der vom USV-Batterieladegerät bereitgestellte Batterieladestrom automatisch erhöht, um die Ladegerätfrequenz von 100 % zu erreichen. Die Ladegerätfrequenz muss nicht geändert werden. • Wenn die Gesamtbatteriekapazität verringert wird, wird der vom USV-Batterieladegerät bereitgestellte Batterieladestrom automatisch verringert, um die Ladegerätfrequenz von 100 % zu erreichen. Die Ladegerätfrequenz muss nicht geändert werden. Nähere Informationen zur Batteriekapazität finden Sie im USV-Benutzerhandbuch. Vorsicht: Das Laden bei einer zu hohen Frequenz kann zum Kochen bzw. Entgasen der Elektrolyte bzw. zu einem hohen Gasdruck führen. Ändern Sie diese Einstellung nur, wenn Sie sich auf diesem Gebiet sehr gut auskennen.
Batterietyp	Gibt den Batterietyp an, wobei **VRLA** für eine ventilregulierte Blei-Säure-Batterie und **Belüftete Zelle** für eine (in Autos verwendete) Nassbatterie steht.
Gesamtbatteriekapazität	Verwenden Sie diese Einstellung, um die Gesamtkapazität Ihrer USV-Batterien zwischen 7 und 200 Amperestunden (Ah) anzugeben. Dieser Wert dient dazu, die Betriebszeit einzuschätzen und den erforderlichen Batterieladestrom zu bestimmen. Wenn Ihre USV über die Option „Gesamtbatteriekapazität“ verfügt, aktualisieren Sie den Wert „Gesamtbatteriekapazität“ beim Hinzufügen oder Entfernen von USV-Batterien. Nähere Informationen zur Batteriekapazität finden Sie im USV-Benutzerhandbuch.

Bildschirm „Selbsttest-Planung“

Pfad: USV > Konfiguration > Selbsttest-Planung

Die Befehlsfolge für USV-Geräte mit dem SRTL/SRYLF-Präfix mit einer integrierten Netzwerkmanagement-Karte lautet **Konfiguration > USV > Selbsttest-Planung**.

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

Planung für das Herunterfahren

Pfad: Konfiguration > Planung

Die Befehlsfolge für USV-Geräte mit dem SRTL/SRYLF-Präfix mit einer integrierten Netzwerkmanagement-Karte lautet **Konfiguration > USV > Planung**.

Diese Option ist nicht bei allen USV-Geräten verfügbar. Die Selbsttest-Planungsoptionen sind nicht bei allen USV-Geräten gleich ausgeführt.

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 USV- und Steckdosengruppenoptionen

Sie können das Herunterfahren eines USV-Geräts unter **USV** bzw. für eine einzelne geschaltete Steckdosengruppe (falls zutreffend) unter **Steckdosengruppen** planen.

Alle konfigurierten Abschaltpläne werden oben auf dem Bildschirm angezeigt, wenn Sie die **USV** oder die **Steckdosengruppen** 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** oder **Steckdosengruppen**. 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 oder eine geschaltete Steckdosengruppe.

1. Wählen Sie unter **Planung** entweder **USV** oder **Steckdosengruppe** 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 oder die Steckdosengruppe 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).

Geben Sie die Steckdosengruppe an, die heruntergefahren werden soll, indem Sie die entsprechende Schaltfläche auswählen.

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.

Bildschirme für Firmware-Aktualisierung

Pfad: Konfiguration > Firmware-Aktualisierung

Die Befehlsfolge für USV-Geräte mit dem SRTL/SRYLF-Präfix mit einer integrierten Netzwerkmanagement-Karte lautet **USV > Konfiguration > Firmware-Aktualisierung > Hochladen**.

Diese Option ist nicht bei allen USV-Geräten verfügbar.

Diese Aktualisierung gilt für *die Firmware der USV*. Verwechseln Sie diese nicht mit einer Firmware-Aktualisierung der Netzwerkmanagement-Karte (siehe „NMC Firmware-Upgrades“).

Folgen Sie den Anweisungen auf dem Bildschirm **Firmware-Aktualisierung**, um festzulegen, ob die Ausgangsversorgung der USV vor einer Firmware-Aktualisierung ausgeschaltet werden soll. Dies ist vom USV-Modell abhängig.

Hinweis: Um den Bildschirm **Firmware-Aktualisierung** mit dem Internet Explorer® anzuzeigen, verwenden Sie die Version 10 oder höher mit abgeschalteter Kompatibilitätsansicht. Der Bildschirm „Firmware-Aktualisierung“ ist nicht mit dem Edge®-Browser kompatibel.

Befolgen Sie diese Schritte, um die Firmware zu aktualisieren. (Siehe auch **„Aktualisierung der USV-Firmware mit einem USB-Speichermedium (nur AP9641, AP9643 und eingebettete NMC-Geräte)“** und alternativ **„Aktualisieren der USV-Firmware über FTP“**.)

1. Die Knowledge-Base-Artikel FA164737 und FA170679 enthalten Informationen zum Aufrufen einer Firmware-Aktualisierungsdatei sowie weitere Anweisungen.
2. Wählen Sie **Konfiguration** – **Firmware-Aktualisierung**.
3. Klicken Sie auf die Schaltfläche, um zu der heruntergeladenen Aktualisierungsdatei auf Ihrem Computer zu navigieren.
4. Klicken Sie auf die Schaltfläche **USV aktualisieren**, um die USV-Firmware zu aktualisieren.
5. Prüfen Sie nach Beendigung der Aktualisierung den Status unter **Letztes Aktualisierungsergebnis** und **Aktuelle Version** oder im Ereignisprotokoll.

Aktualisierung der USV-Firmware mit einem USB-Speichermedium (nur AP9641, AP9643 und eingebettete NMC-Geräte)

Stellen Sie vor der Aktualisierung der USV-Firmware sicher, dass das USB-Laufwerk USB v1.1 unterstützt und im FAT-, FAT16- oder FAT32-Format formatiert ist.

1. Stecken Sie das USB-Speichermedium in einen USB-Anschluss Ihres Computers.
2. Lesen Sie die Knowledge-Base-Artikel mit den IDs **FA164737** und **FA170679** zum Herunterladen der korrekten Firmware-Aktualisierungsdatei für Ihre USV und speichern Sie die Datei in das Root-Verzeichnis Ihres USB-Speichermediums oder in ein Verzeichnis „/upsfw/“ auf dem USB-Speichermedium.
3. Entfernen Sie das USB-Speichermedium mit der enthaltenen Firmware-Datei aus Ihrem Computer und stecken Sie es in den USB-Anschluss der Netzwerkmanagement-Karte.
4. Öffnen Sie die Web-Oberfläche der Netzwerkmanagement-Karte und gehen Sie zu **Konfiguration > Firmware-Aktualisierung**.
5. Wählen Sie die Firmware-Datei aus der Dropdown-Liste unter „Aktualisierung mit einem USB-Speichermedium“.
6. Klicken Sie auf die Schaltfläche **„USV aktualisieren“**, um die USV-Firmware zu aktualisieren.

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

7. Prüfen Sie nach Beendigung der Aktualisierung den Status unter **„Letztes Aktualisierungsergebnis“** oder im Ereignisprotokoll.

Aktualisierung der USV-Firmware mit der Netzwerkmanagement-Karte

Gehen Sie folgendermaßen vor, um die Firmware zu aktualisieren:

1. Die Knowledge-Base-Artikel FA164737 und FA170679 auf der APC-Website enthalten Informationen zum Aufrufen einer Firmware-Aktualisierungsdatei sowie weitere Anweisungen.
2. Greifen Sie per SCP oder FTP auf die Karte zu und legen Sie die Aktualisierungsdatei im Verzeichnis root ab. Zum Beispiel: `scp <Firmware-Datei>.enc <NMC-Benutzername>@<NMC-IP-Adresse>:<Firmware-Datei>.enc`
3. Öffnen Sie die Web-Oberfläche der Netzwerkmanagement-Karte und gehen Sie zu **Konfiguration > Firmware-Aktualisierung**.
4. Wählen Sie die Firmware-Datei aus der Dropdown-Liste unter dem Bereich für die **Aktualisierung mit einer Netzwerkmangement-Karte** aus.
5. Klicken Sie auf die Schaltfläche **USV aktualisieren**, um die USV-Firmware zu aktualisieren.
6. Überprüfen Sie nach Abschluss der Aktualisierung den Status unter **Letztes Aktualisierungsergebnis** oder im Ereignisprotokoll.

Aktualisieren der USV-Firmware über FTP

Mehrere USV-Geräte können per FTP schneller aktualisiert werden. Die nachfolgenden Schritte erläutern die Vorgehensweise anhand eines Beispiels. Hierbei handelt es sich um eine **Alternative** zur Aktualisierung über den „Bildschirme für Firmware-Aktualisierung“.

HINWEIS: FTP ist standardmäßig deaktiviert und muss aktiviert werden, bevor Sie fortfahren. Siehe „Bildschirm „FTP-Server““.

1. Die Knowledge-Base-Artikel FA164737 und FA170679 enthalten Informationen zum Aufrufen einer Firmware-Aktualisierungsdatei sowie weitere Anweisungen.
2. Greifen Sie per FTP auf die Karte zu und legen Sie die Datei in dem Verzeichnis **upsfw** ab, um die Firmware-Aktualisierung zu starten.

   Die Netzwerkmanagement-Karte bricht die FTP-Firmware-Übertragung unter Umständen ab, falls festgestellt wird, dass die Aktualisierungsdatei beschädigt oder nicht für die USV anwendbar ist.

   Beispiel für das Laden einer Aktualisierungsdatei mithilfe des DOS FTP-Befehls:

```
$ ftp <NMC-Netzwerkadresse>
Connected to <NMC-Netzwerkadresse>.
220 AP9641 Network Management Card AOS vX.Y.Z FTP server ready.
User (<NMC-Netzwerkadresse>:(none)): apc
331 User name okay, need password.
Password:
230 User logged in, proceed.
ftp> bin
200 TYPE Command okay.
ftp> hash
Hash mark printing On ftp:(2048 bytes/hash mark).
ftp> cd upsfw
```

```
250 CWD requested file action okay, completed.
ftp> put "<Pfad zu USV-Firmwaredatei>"
200 PORT Command okay.
150 File status okay; about to open data connection.
226 Closing data connection.
ftp: 121984 bytes sent in 1.39Seconds 87.70Kbytes/sec.
ftp> quit
221 Goodbye.
```

3. Überprüfen Sie nach Abschluss der Aktualisierung den Status unter **Letztes Aktualisierungsergebnis** auf der Firmware-Aktualisierungsseite der Web-Schnittstelle oder im Ereignisprotokoll.

Konfigurationsbildschirm der Einstellungen für die Firmware-Aktualisierung

Befehlsfolge: Konfiguration > USV > Firmware-Aktualisierung > Einstellungen

Die folgenden Optionen gelten nur für USV-Geräte mit dem SRTL/SRYLF-Präfix mit integrierter Netzwerkmanagement-Karte.

Legen Sie fest, wann auf die neue USV-Firmware umgeschaltet werden soll: nur im manuellen Bypass oder wenn die Ausgangsleistung nach dem Download ausgeschaltet ist (nicht bei allen USV-Geräten/USV-Firmwareversionen unterstützt), nur wenn **die Ausgangsleistung nach dem Download ausgeschaltet ist,** oder **manuell**.

PowerChute Network Shutdown-Clients

Pfad: USV > Konfiguration > 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 „Web-Zugriff““, um HTTP oder HTTPS zu aktivieren.

Bildschirme „Universeller E/A“

Das Menü **Universeller E/A** wird benötigt, wenn Sie die Temperatur- und Luftfeuchtigkeitssensoren (AP9335T/TH), das E/A-Zusatzmodul für potenzialfreie Kontakte (AP9810) oder den Flüssigkeitssensor (Spot Fluid Sensor) (NBES0301) – v3.1.x und höher installiert haben. Der Einsatz dieser Geräte wird oft als Umweltbeobachtung bezeichnet.

Bildschirm „Temperatur und Luftfeuchtigkeit“

Pfad: Universeller E/A > Temperatur und Luftfeuchtigkeit

Hier werden der Name, der Alarmzustand, die Temperatur und die Luftfeuchtigkeit (sofern unterstützt) für jeden Sensor angezeigt. Klicken Sie auf den Namen eines Sensors, um Name und Standort zu bearbeiten sowie um die Grenzwerte und die Hysterese zu konfigurieren.

Grenzwerte. Für jeden Sensor legen Sie die Grenzwerte für die am Sensor gemessene Temperatur und Luftfeuchtigkeit (sofern unterstützt) fest. Ein Alarm wird ausgegeben, sobald ein Grenzwert über- oder unterschritten wird.

Hoch und **Niedrig** sind Warnmeldungen. **Höchstwert** und **Mindestwert** sind kritische Meldungen, bei denen sofortige Maßnahmen ergriffen werden müssen.

Hysterese. Verwenden Sie den Hysterese-Wert, um zu vermeiden, dass wiederholt Alarme für denselben Verstoß gegen einen Temperatur- oder Luftfeuchtigkeitsgrenzwert ausgegeben werden.

Wenn die Temperatur oder Luftfeuchtigkeit, die einen Verstoß zur Folge hat, leicht nach oben oder unten schwankt, kann ein Alarm wiederholt ausgelöst werden. Ein höherer Hysteresewert kann dem vorbeugen.

Ist der Hysteresewert nicht hoch genug, kann die Schwankung zunächst einen Grenzwertverstoß auslösen und danach wieder löschen, wodurch der Alarm mehrmals ausgelöst werden kann. Sehen Sie sich die nachstehenden Beispiele an und beachten Sie dabei Folgendes:

- Bei Verletzungen des Grenzwerts „Höchstwert“ und „Hoch“ wird der Grenzwert *abzüglich* der Hysterese als Löschpunkt verwendet.
- Bei Verletzungen des Grenzwerts „Mindestwert“ und „Niedrig“ wird der Grenzwert *zuzüglich* der Hysterese als Löschpunkt verwendet.

Beispiel für eine steigende und zugleich schwankende Luftfeuchtigkeit: Angenommen, der Grenzwert für die *maximale* Luftfeuchtigkeit beträgt 65 % und die Luftfeuchtigkeits-Hysterese beträgt 10 %. Die Luftfeuchtigkeit steigt auf über 65 % an und löst damit einen Alarm aus. Sie schwankt anschließend wiederholt zwischen 60 % und 70 %, jedoch wird – aufgrund des Hysteresewerts von 10 % – der Alarm nicht gelöscht und dadurch auch kein neuer Alarm ausgelöst. Damit der vorhandene Alarm gelöscht wird, muss die Luftfeuchtigkeit unter 55 % sinken (also 65 % *abzüglich* 10 %).

Beispiel für eine abfallende und zugleich schwankende Temperatur: Angenommen, der Grenzwert für die *minimale* Temperatur beträgt 12 °C und die Temperatur-Hysterese beträgt 2 °C. Die Temperatur fällt unter 12 °C und löst damit einen Alarm aus. Sie schwankt anschließend wiederholt zwischen 13 °C und 11 °C, jedoch wird – aufgrund des Hysteresewerts von 2 °C – der Alarm nicht gelöscht und dadurch auch kein neuer Alarm ausgelöst. Damit der vorhandene Alarm gelöscht wird, muss die Temperatur auf über 14 °C steigen (also 12 °C *zuzüglich* 2 °C).

Bildschirm „Eingangskontakte“

Pfad: Universeller E/A > Eingangskontakte

Unter **Eingangskontakte** werden der Name, der Alarmzustand und der Status (offen oder geschlossen) jedes Kontakts angezeigt. Diese Informationen werden automatisch ermittelt und hier angezeigt, wenn Sie das Umgebungszubehör installieren.

Klicken Sie auf den Namen eines Eingangskontakts, um ausführliche Angaben zu dessen Alarmzustand anzuzeigen oder um seine Werte zu konfigurieren. Ein deaktivierter Kontakt erzeugt auch bei einem abnormen Schaltzustand niemals einen Alarm. Weitere Felder werden nachfolgend beschrieben:

Feld	Beschreibung
Alarmzustand	**Normal**, wenn dieser Eingangskontakt keinen Alarm meldet bzw. der Schweregrad des Alarms, wenn dieser Eingangskontakt einen Alarm meldet. Ist diese Option für einen Kontakt nicht aktiviert, wird **Deaktiviert** angezeigt.

Feld	Beschreibung
Zustand	Der aktuelle Schaltzustand dieses Eingangskontakts: **Geschlossen** oder **Offen**.
Normal State (Normalzustand)	Der Normalzustand dieses Eingangskontakts (bei Nichtvorliegen eines Alarms): **Geschlossen** oder **Offen**.
Schweregrad	Der Schweregrad des Alarms, der durch den abnormen Schaltzustand dieses Eingangskontakts erzeugt wird: **Warnung** oder **Kritisch**.

Bildschirm „Ausgangsrelais“

Pfad: Universeller E/A > Ausgangsrelais

Unter **Ausgangsrelais** werden der Name und der Status (offen oder geschlossen) jedes Relais angezeigt. Diese Informationen werden automatisch ermittelt und hier angezeigt, wenn Sie das Umgebungszubehör installieren.

Klicken Sie auf den Namen eines Eingangskontakts, um ausführliche Angaben zu dessen Alarmzustand anzuzeigen oder um seine Werte zu konfigurieren. Die Felder werden nachfolgend beschrieben:

Feld	Beschreibung
Zustand	Der aktuelle Schaltzustand dieses Ausgangsrelais: **Geschlossen** oder **Offen**.
Normal State (Normalzustand)	Der Normalzustand dieses Ausgangsrelais (bei Nichtvorliegen eines Alarms): **Geschlossen** oder **Offen**.
Steuerung	Um den aktuellen Schaltzustand dieses Ausgangsrelais zu ändern, markieren Sie dieses Kontrollkästchen und klicken Sie auf „Übernehmen“.
Verzögerung	Wie lange ein ausgewählter Alarmzustand vorliegen muss (Zeit in Sekunden), bevor das Ausgangsrelais aktiviert wird. Verwenden Sie diese Einstellung, um die Aktivierung von Alarm bei nur kurzzeitig anhaltenden Zuständen zu vermeiden. Wenn nach Beginn dieser Verzögerung weitere Alarme erfasst werden sollten, wird die Verzögerung nicht neu gestartet, sondern zählt weiter herunter, bis das Ausgangsrelais aktiviert wird.
Halten	Die Zeit in Sekunden, während der das Ausgangsrelais nach Eintreten des Alarms mindestens aktiviert bleibt. Selbst wenn der aktivierende Alarmzustand behoben werden sollte, bleibt das Ausgangsrelais bis zum Ablauf dieser Wartezeit aktiviert.

Bildschirm „Flüssigkeitssensor“ (v3.1.x und höher)

Pfad: Universeller E/A > Flüssigkeitssensor

Unter **Flüssigkeitssensor** werden der Name und der Status (Flüssigkeit erkannt oder keine Flüssigkeit) jedes Sensors angezeigt. Diese Informationen werden automatisch ermittelt und hier angezeigt, wenn Sie das Umgebungszubehör installieren.

Klicken Sie auf den Namen eines Flüssigkeitssensors, um einen detaillierten Status zu erhalten oder seine Werte zu konfigurieren. Die Felder werden nachfolgend beschrieben:

Feld	Beschreibung
Alarmzustand	**Normal**, wenn dieser Flüssigkeitssensor keinen Alarm meldet bzw. **Kritisch**, wenn dieser Flüssigkeitssensor einen Alarm meldet. Ist diese Option für einen Flüssigkeitssensor nicht aktiviert, wird **Deaktiviert** angezeigt.
State	Der Zustand dieses Sensors: **Flüssigkeit erkannt** oder **keine Flüssigkeit**.

Konfigurieren der Steuerungsrichtlinien

Pfad: Universeller E/A > Steuerungsrichtlinien

Bei einer Netzwerkmanagement-Karte AP9641 oder AP9643 mit verbundenen E/A-Zusatzmodulen für potenzialfreie Kontakte (AP9810) haben Sie folgende Möglichkeiten:

- Öffnen oder Schließen der Ausgangsrelais anhand der USV-Ereignisse und Eingangskontakte (siehe „Konfigurieren der Reaktion eines Ausgangs auf Ereignisse“)
- Konfiguration der USV, um Maßnahmen anhand der Eingangskontakte zu ergreifen (siehe „Konfigurieren der Reaktion der USV oder eines Ausgangs auf einen eingehenden Alarm“)

Nicht alle USV-Geräte können so konfiguriert werden, dass sie auf Eingangskontakte reagieren.

Konfigurieren der Reaktion eines Ausgangs auf Ereignisse.

1. Wählen Sie im Menü **Konfiguration** die Optionen **Universeller E/A** und **Steuerungsrichtlinien** aus.
2. Klicken Sie auf die Schaltfläche **Richtlinien hinzufügen**.
3. Klicken Sie auf den Namen einer Kategorie oder Unterkategorie, um entsprechende Ereignisse anzuzeigen.
4. Klicken Sie auf einen Ereignisnamen, um ihn zu konfigurieren, markieren Sie das Kontrollkästchen des Ausgangsrelais, das seinen Status beim Auftreten dieses Ereignisses ändert, und klicken Sie auf **Richtlinie speichern**.

Konfigurieren der Reaktion der USV oder eines Ausgangs auf einen eingehenden Alarm.

1. Wählen Sie im Menü **Konfiguration** die Optionen **Universeller E/A** und **Steuerungsrichtlinien** aus.
2. Klicken Sie auf die Schaltfläche **Richtlinien hinzufügen**.
3. Klicken Sie auf die Unterkategorie **E/A-Kontakt**.
4. Wählen Sie das Ereignis mit dem gleichen Schweregrad wie der Eingangskontakt. Wenn der Schweregrad des Eingangskontakts beispielsweise „kritisch“ ist, wählen Sie ein kritisches Ereignis.

   Die Netzwerkmanagement-Karte unterstützt bis zu vier Eingänge. Sie müssen das Eingangssignal angeben, das mit diesem Ereignis verknüpft werden soll.
5. Wählen Sie im Dropdown-Listenfeld **Anschluss** die **Nummer des universellen Sensoranschlusses** (1 oder 2), mit dem das E/A-Zusatzmodul für potenzialfreie Kontakte verbunden ist.
6. Wählen Sie im Dropdown-Listenfeld **Zone** den Buchstaben der Zone (A oder B) des Kontakts, mit dem der Eingang verbunden ist.
7. Definieren Sie die von der USV durchgeführte Aktion (falls zutreffend), wenn sich der Eingangsstatus ändert.
8. Wählen Sie den öffnenden oder schließenden Ausgang (sofern zutreffend).
9. Klicken Sie auf **Richtlinie speichern**.

Die von Ihnen konfigurierte Reaktion erfolgt nur einmal.

Wenn Sie den Ausgang auf seinen normalen Schaltzustand zurücksetzen, bevor der Alarmzustand gelöscht wird, wird sich der Ausgang erst wieder öffnen oder schließen, wenn der Alarmzustand gelöscht wird und dann erneut auftritt.

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: Das NMC unterstützt mehrere Remote-Authentifizierungsprotokolle. 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!
Zum Ändern einer Superuser-Einstellung müssen Sie das aktuelle Passwort eingeben.
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 Remote-Authentifizierungsprotokolle 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.

Weitere Informationen finden Sie unter „Konfiguration > Sicherheit > Lokale Benutzer > Standardeinstellungen“ unten. Hintergrundinformationen zu Konten finden Sie unter „Arten von Benutzerkonten“.

Benutzervoreinstellungen Aktivieren 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.
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“.

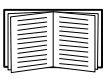
Pfad: Konfiguration > Sicherheit > Lokale Benutzer > Standardeinstellungen

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*.

Die folgenden Authentifizierungs- und Autorisierungsfunktionen von LDAP (Lightweight Directory Access Protocol – v3.1.x und höher), RADIUS (Remote Authentication Dial-In User Service) und TACACS+ (Terminal Access Controller Access Control System – v3.0.x und höher) werden unterstützt:

- Wenn ein Benutzer auf die NMC oder eine andere RADIUS- oder TACACS+-fähige Netzwerkeinheit zugreift, wird eine Authentifizierungsanfrage an den Server gesendet, um die Zugriffsebene des Benutzers festzustellen.
- Für die NMC verwendete LDAP-, RADIUS- und TACACS+-Benutzernamen dürfen maximal 64 Zeichen enthalten.

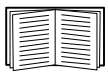
Siehe die nachstehenden Optionen für die Authentifizierungsmethode:

Einstellung	Beschreibung
Lokale Benutzer-Authentifizierung	Geben Sie an, ob und wann die lokale Benutzerdatenbank überprüft wird: **Erste**: Die lokale Benutzerdatenbank wird immer zuerst überprüft. Wenn der Benutzername gefunden wird, wird das Passwort überprüft und die Anmeldung ist entweder erfolgreich oder schlägt fehl. Wenn der Benutzername nicht gefunden wird, wird die Remote-Authentifizierung verwendet, falls sie aktiviert ist. **Letzte**: Die lokale Benutzerdatenbank wird nach dem Versuch der Remote-Authentifizierung überprüft, wenn ein Fehler bei der Kontaktaufnahme mit dem Remote-Authentifizierungsserver auftritt. Wenn die Remote-Authentifizierung deaktiviert ist, verhält sie sich genauso wie **Erste**. **Off (Aus)**: Die lokale Benutzerdatenbank wird niemals überprüft. **HINWEIS**: Die Einstellung **OFF (AUS)** wird nicht empfohlen, da dies dazu führen kann, dass Sie dauerhaft vom NMC ausgesperrt werden, wenn der Remote-Authentifizierungsserver ausfällt oder auf dem NMC falsch konfiguriert ist. Wenn **Off (Aus)** verwendet wird, wird dringend empfohlen, die Einstellung Remote Authentication Override (Remote-Authentifizierung überschreiben) (Sitzung a) zu aktivieren und die Option Serial Remote Authentication Override (Serielle Remote-Authentifizierung überschreiben) für den Superuser oder einen Administrator zu setzen. Hinweis: Wenn sowohl die Einstellungen für die lokale als auch die entfernte Benutzerauthentifizierung auf **Off (Aus)** eingestellt sind, wird die Local User Authentication (lokale Benutzerauthentifizierung) automatisch auf **Erste**.
Authentifizierung von Remote-Benutzern	Geben Sie an, ob und welches Remote-Authentifizierungsprotokoll verwendet wird: **Off (Aus)**: Verwenden Sie keine Remote-Benutzerauthentifizierung und führen Sie immer eine lokale Benutzerauthentifizierung durch. **RADIUS**: Authentifizierung von Remote-Benutzern wird RADIUS verwenden. Hinweis: Die Meldung „Es wurden keine konfigurierten RADIUS-Server hinzugefügt“ zeigt an, dass Sie einen ordnungsgemäß konfigurierten RADIUS-Server hinzufügen müssen, damit die RADIUS-Authentifizierung funktionieren kann. **TACACS+**: Authentifizierung von Remote-Benutzern wird TACACS+ verwenden. Hinweis: Die Meldung „Es wurden keine konfigurierten TACTACS+-Server hinzugefügt“ zeigt an, dass Sie einen ordnungsgemäß konfigurierten TACTACS+-Server hinzufügen müssen, damit die TACTACS+-Authentifizierung funktionieren kann. **LDAP**: Authentifizierung von Remote-Benutzern wird LDAP verwenden. **HINWEIS:** Die Meldung „Es wurden keine konfigurierten LDAP-Server hinzugefügt“ zeigt an, dass Sie LDAP ordnungsgemäß konfigurieren müssen, damit die LDAP-Authentifizierung funktionieren kann.

Wenn **Lokale Authentifizierung** auf **Off (Aus)** gesetzt ist und die Authentifizierungsserver nicht erreichbar, nicht richtig identifiziert oder nicht richtig konfiguriert sind, ist der Fernzugriff für alle Benutzer nicht verfügbar. Um wieder Zugriff zu erhalten, müssen Sie über die serielle Schnittstelle eine Befehlszeile öffnen und die **Zugriffseinstellung** zu **„local“**, **„radiusLocal“** oder **„tacacs+“** ändern.

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

```
userauth -a local
```



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

Siehe auch „TACACS+ -Bildschirm (v3.0.x und höher)“ weiter unten sowie „Konfigurieren des TACACS+-Servers“.

Siehe auch „LDAP-Bildschirm (v3.1.x und höher)“ weiter unten sowie „Konfigurieren des LDAP-Servers“.

LDAP-Bildschirm (v3.1.x und höher)

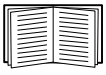
Pfad: Konfiguration > Sicherheit > Remote-Benutzer > LDAP

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

LDAP-Einstellung	Beschreibung
Benutzer-URI suchen	Ein LDAP-URI, der den Speicherort eines Benutzerobjekts angibt, an das Sie sich zunächst binden müssen. Dieses Benutzerobjekt muss die Berechtigung haben, in der LDAP-Datenbank nach Benutzern zu suchen. Bei einem Anmeldeversuch eines Benutzers wird eine Verbindung mit dem LDAP-Server in diesem URI hergestellt und eine Bindung an den DN mit dem in „Benutzerpasswort suchen“ angegebenen Kennwort durchgeführt. Wenn diese Bindung erfolgreich ist, wird nach dem Benutzer gesucht, der versucht, sich anzumelden. Dieser LDAP-URI muss entweder das Schema „ldap“ oder „ldaps“ enthalten. Wenn „ldaps“ verwendet wird, ist die TLS-Verbindung implizit und die TCP-Verbindung wird standardmäßig über Port 636 hergestellt. Wenn „ldap“ verwendet wird, wird die TLS-Verbindung durch Senden einer StartTLS-Anforderung initiiert und die TCP-Verbindung verwendet standardmäßig Port 389. Verwendung von „ldaps“ ist nicht standardisiert und wird nicht empfohlen. Dieser LDAP-URI kann die Adresse des LDAP-Servers und optional die Portnummer enthalten. Es folgt der DN des gesuchten Benutzerobjekts. Wenn der DN des Suchbenutzers mit DC-Komponenten endet, wird ein DNS-Lookup des SRV-Eintrags für den LDAP-Dienst in dieser Domäne durchgeführt. Wird der SRV-Eintrag gefunden, so wird er anstelle des im URI angegebenen Hosts verwendet. Wird der SRV-Eintrag nicht gefunden, so wird der im URI angegebene Host verwendet. Die Host-Komponente des URI kann weggelassen werden, wenn der SRV-Eintrag für LDAP bekannt ist. Wenn der DN weggelassen wird, muss die Host-Komponente vorhanden sein, und es wird eine anonyme Bindung durchgeführt. Beispiele: • **"ldap://ldap.domain.com/CN=searchuser,OU=users,DC=domain,DC=com** Wenn DNS verfügbar ist, wird eine DNS-Abfrage des SRV-Eintrags für den LDAP-Dienst unter domain.com durchgeführt. Wenn er gefunden wird, wird er mit ihm verbunden. Wenn er nicht gefunden wird, wird eine Verbindung zu „ldap.domain.com“ an Port 389 hergestellt. Nach dem Senden einer StartTLS-Anforderung wird TLS eingerichtet und eine Bindung an das Objekt „CN=searchuser,OU=users,DC=domain,DC=com“ mit dem in „Benutzerpasswort suchen“ angegebenen Passwort durchgeführt. Von hier aus wird eine Suche nach dem sich anmeldenden Benutzer durchgeführt. • **"ldap:///CN=searchuser,OU=users,DC=domain,DC=com** Wenn DNS verfügbar ist, wird eine DNS-Abfrage des SRV-Eintrags für den LDAP-Dienst unter domain.com durchgeführt. Wenn er gefunden wird, wird er mit ihm verbunden. Wenn er nicht gefunden wird, wird keine Verbindung hergestellt, da die Host-Komponente des URI weggelassen wird und die LDAP-Authentifizierung nicht fortgesetzt werden kann. Wenn die Verbindung erfolgreich ist, werden StartTLS, Bindung und Suche wie oben beschrieben durchgeführt. • **"ldaps://ldap.domain.com** „ldap.domain.com“ an Port 636 verbunden und es wird sofort ein TLS-Handshake durchgeführt, ohne eine StartTLS-Anfrage zu senden. Wenn dies gelingt, wird eine anonyme Bindung durchgeführt. Von hier aus wird eine Suche nach dem sich anmeldenden Benutzer durchgeführt. • **"ldap://ldap.domain.com:42/CN=searchuser,OU=users,DC=domain,DC=com** • Dies ist dasselbe wie das erste Beispiel, außer dass eine Verbindung zu „ldap.domain.com“ an Port 42 hergestellt wird, wenn der SRV-Eintrag nicht gefunden wird.

LDAP-Einstellung	Beschreibung
Benutzerpasswort suchen	Das Passwort, das in der ersten Bindungsanfrage an den Suchbenutzer zu verwenden ist, wie oben beschrieben. Bleibt diese Option leer, wird entweder eine anonyme oder eine unauthentifizierte Verbindung hergestellt, je nachdem, ob ein Suchbenutzer-DN angegeben wird oder nicht.
Zeitlimit bis zur Antwort	Die Zeitüberschreitung in Sekunden, die für die Verbindung zum und die Kommunikation mit dem LDAP-Server verwendet wird. Die erste TCP-Verbindung muss innerhalb dieser Zeitspanne abgeschlossen werden. Wenn dies der Fall ist, muss jede LDAP-Antwort vom Server innerhalb dieser Zeitspanne nach jeder LDAP-Anfrage empfangen werden. Da eine einzelne LDAP-Authentifizierung aus mehreren Anfragen bestehen kann (und sogar an mehrere Server, wenn Verweise verfolgt werden), kann die Gesamtauthentifizierungszeit am Ende viel länger sein als der hier angegebene Timeout-Wert.
Benutzer-Basis-DN	Dies ist der DN des Basisobjekteintrags, unter dem alle Benutzer, die sich anmelden, existieren müssen.
Gruppen-Basis-DN	Dies ist der DN des Basisobjekteintrags, unter dem die in den folgenden Einstellungen angegebenen Benutzergruppen existieren müssen.
Admin-Gruppenname	Dies ist der Common Name (CN) der LDAP-Gruppe, in der die NMC-Administratoren Mitglied sind. Wenn der sich anmeldende Benutzer Mitglied dieser Gruppe ist, erhält der Benutzer Administrator-Zugriff.
Gerätebenutzer Gruppenname	Dies ist der Common Name (CN) der LDAP-Gruppe, in der die NMC-Gerätebenutzer Mitglied sind. Wenn der sich anmeldende Benutzer Mitglied dieser Gruppe ist, erhält der Benutzer Gerätebenutzer-Zugriff.
Netzwerkbenutzer Gruppenname	Dies ist der Common Name (CN) der LDAP-Gruppe, in der die NMC-Netzwerkbenutzer Mitglied sind. Wenn der sich anmeldende Benutzer Mitglied dieser Gruppe ist, erhält der Benutzer Netzwerkbenutzer-Zugriff.
Schreibschutz Benutzer Gruppenname	Dies ist der Common Name (CN) der LDAP-Gruppe, in der die NMC-Schreibschutz-Benutzer Mitglied sind. Wenn der sich anmeldende Benutzer Mitglied dieser Gruppe ist, erhält der Benutzer Schreibschutz-Benutzer-Zugriff.
Active Directory-Schema	Wenn diese Option aktiviert ist, werden LDAP-Verzeichnisse mit Benutzern der Klasse „Benutzer“ und Gruppen der Klasse „Gruppe“ nach dem Standardschema von Active Directory unterstützt.
RFC2307 POSIX Schema	Wenn dies aktiviert ist, werden LDAP-Verzeichnisse mit Benutzern der Klasse „posixAccount“ und Gruppen der Klasse „posixGroup“ nach dem in RFC 2307 definierten Schema unterstützt.
RFC4519 Benutzer Schema	Wenn dies aktiviert ist, werden LDAP-Verzeichnisse unterstützt, die Benutzer der Klasse „uidObject“ und Gruppen entweder der Klasse „groupOfNames“ oder der Klasse „groupOfUniqueNames“ gemäß dem in RFC 4519 definierten Schema enthalten.
RFC2798 inetOrgPerson	Wenn dies aktiviert ist, werden LDAP-Verzeichnisse mit Benutzern der Klasse „inetOrgPerson“ gemäß RFC 2798 unterstützt.
Benutzerdefinierte Benutzerklasse	Wenn diese Option aktiviert ist, können LDAP-Verzeichnisse unterstützt werden, die Benutzer mit Klassen enthalten, die keiner der oben genannten unterstützten Klassen entsprechen. Wenn dies aktiviert ist, müssen die Einstellungen **Benutzerdefinierter Benutzerklassenname** und **Attribut des benutzerdefinierten Benutzerklassennamens** angegeben werden, und **Attribut der benutzerdefinierten Benutzergruppennummer** kann optional angegeben werden.

LDAP-Einstellung	Beschreibung
Benutzerdefinierte Gruppenklasse	Wenn diese Option aktiviert ist, können LDAP-Verzeichnisse unterstützt werden, die Gruppen mit Klassen enthalten, die keiner der oben genannten unterstützten Klassen entsprechen. Wenn dies aktiviert ist, müssen die Einstellungen **Benutzerdefinierter Gruppenklassenname** und **Attribut des benutzerdefinierten Gruppenklassennamens** angegeben werden, und **Attribut der benutzerdefinierten Gruppengruppennummer** kann optional angegeben werden. **Typ des benutzerdefinierten Gruppenmitglieds** muss ebenfalls korrekt eingestellt sein.
Benutzerdefinierter Benutzerklassenname	Dies ist der Name der Objektklasse, zu der die Benutzereinträge gehören. Es wird nur verwendet, wenn **Benutzerdefinierte Benutzerklasse** aktiviert ist.
Attribut des benutzerdefinierten Benutzerklassennamens	Dies ist der Name des Attributs, das den Benutzernamen eines Benutzers für die durch **Benutzerdefinierter Benutzerklassenname** angegebene Objektklasse enthält. Es wird nur verwendet, wenn **Benutzerdefinierte Benutzerklasse** aktiviert ist.
Attribut der benutzerdefinierten Benutzergruppennummer	Dies ist der Name des Attributs, das die Gruppennummer für die primäre Gruppe eines Benutzers für die durch **Benutzerdefinierter Benutzerklassenname** angegebene Objektklasse enthält. Dies ist optional und wird nur verwendet, wenn **Benutzerdefinierte Benutzerklasse** aktiviert ist. Es wird auf die gleiche Weise verwendet wie das Attribut „gidNumber“ in der Klasse „posixAccount“.
Benutzerdefinierter Gruppenklassenname	Dies ist der Name der Objektklasse, zu der die Gruppeneinträge gehören. Es wird nur verwendet, wenn **Benutzerdefinierte Gruppenklasse** aktiviert ist.
Attribut des benutzerdefinierten Gruppenmitglieds	Dies ist der Name des Attributs, das die Mitglieder der Gruppe für die durch **Benutzerdefinierter Gruppenklassenname** angegebene Objektklasse enthält. Es wird nur verwendet, wenn **Benutzerdefinierte Gruppenklasse** aktiviert ist. Wenn **Typ des benutzerdefinierten Gruppenmitglieds** auf „DN“ gesetzt ist, dann sind die Werte in diesem Attribut DNs. Wenn es auf „Benutzername“ gesetzt ist, sind die Werte in diesem Attribut Benutzernamen.
Attribut der benutzerdefinierten Gruppennummer	Dies ist der Name des Attributs, das die Gruppennummer der Gruppe für die durch **Benutzerdefinierter Gruppenklassenname** angegebene Objektklasse enthält. Dies ist optional und wird nur verwendet, wenn **Benutzerdefinierte Gruppenklasse** aktiviert ist. Es wird auf die gleiche Weise verwendet wie das Attribut „gidNumber“ in der Klasse „posixGroup“.
Typ des benutzerdefinierten Gruppenmitglieds	Dies legt fest, wie die Mitglieder der Gruppe für die durch **Benutzerdefinierter Gruppenklassenname** angegebene Objektklasse angegeben werden. Er kann entweder auf „DN“ oder „Benutzername“ gesetzt werden.
Testeinstellungen	Geben Sie den Benutzernamen und das Kennwort eines beliebigen Serverkontos ein, um die neu konfigurierten Einstellungen vor dem Anwenden zu testen. Wenn sich der Benutzer erfolgreich authentifiziert und Mitglied mindestens einer der angegebenen Gruppen ist, werden die Einstellungen übernommen. Andernfalls werden sie nicht angewendet.
Test überspringen und übernehmen	Wendet die Einstellungen an, ohne vorher eine Testauthentifizierung durchzuführen.



Siehe auch **Authentifizierung von Remote-Benutzern** oben.

Konfigurieren des LDAP-Servers

Die Konfiguration eines OpenLDAP-, Active Directory- oder anderen LDAP-Servers geht über den Rahmen dieses Dokuments hinaus. Wie in den obigen Beschreibungen der Einstellungen erwähnt, werden die gängigsten Schemata standardmäßig unterstützt, darunter Active Directory-Benutzer und -Gruppen, das in RFC2307 definierte POSIX-Schema, das in RFC4519 definierte Benutzerschema und die in RFC2798 definierte Benutzerklasse inetOrgPerson. Bei der Konfiguration eines neuen Servers empfiehlt es sich, eines dieser Schemata zu wählen. Stellen Sie sicher, dass für jeden NMC-Benutzertyp, den Sie unterstützen möchten, Gruppen erstellt werden und dass die Benutzer entsprechend hinzugefügt werden.

RADIUS-Bildschirm

Pfad: Konfiguration > Sicherheit > Remote-Benutzer > RADIUS

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 Servername oder die IP-Adresse des primären oder sekundären RADIUS-Servers.
Port	Die Portnummer des primären oder sekundären RADIUS-Servers. **HINWEIS:** RADIUS-Server verwenden standardmäßig Port 1812, um Benutzer zu authentifizieren. Die NMC unterstützt die Ports 1 bis 65535.
Geheimnis	Der vom RADIUS-Server und der Netzwerkmanagement-Karte verwendete geheime Schlüssel.
Message-Authenticator erforderlich	Beim Aktivieren dieser Einstellung (standardmäßig deaktiviert) muss die NMC in der Antwort vom RADIUS-Server ein gültiges Message-Authenticator-Attribut erhalten.
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.

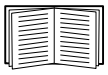
Konfigurieren des RADIUS-Servers

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*.

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 auf der Web-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.

TACACS+ -Bildschirm (v3.0.x und höher)

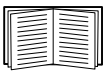
Pfad: Konfiguration > Sicherheit > Remote-Benutzer > TACACS+

Sie können einen TACACS+-Server verwenden, um Remote-Benutzer zu authentifizieren. Diese Option bietet folgende Möglichkeiten:

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

TACACS+-Einstellung	Beschreibung
TACACS+ Server	Der Servername oder die IP-Adresse des primären oder sekundären TACACS+-Servers.
Port	Die Portnummer des primären oder sekundären TACACS+-Servers. **HINWEIS:** TACACS+-Server verwenden standardmäßig Port 49, um Benutzer zu authentifizieren. Die NMC unterstützt die Ports 1 bis 65535.
Geheim	Der vom TACACS-+ Server und der NMC verwendete geheime Schlüssel.
Timeout Antwort	Die Zeit in Sekunden, die eine NMC auf eine Antwort vom TACACS+-Server wartet.
Einstellungen testen	Geben Sie den Benutzernamen und das Kennwort des Administrators ein, um den Pfad zu dem von Ihnen konfigurierten TACACS+-Server zu testen.

TACACS+-Einstellung	Beschreibung
Test überspringen und anwenden	Hiermit wird der Test des Pfades zum TACACS+-Server unterlassen.



Siehe auch „Authentifizierung von Remote-Benutzern“ weiter oben und „Konfigurieren des TACACS+-Servers“ weiter unten.

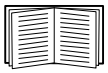
Es gibt zwei globale TACACS+-Optionen, die für alle Server gelten:

Berechtigungs-stufe: Nur-Lesen-Benutzer	Geben Sie einen Wert zwischen 0 und 15 ein. Wenn die Berechtigungsstufe eines autorisierten Benutzers (Autorisierungsargument „priv-lvl“) größer oder gleich dem angegebenen Wert und kleiner als die **Berechtigungsstufe des Administrators** ist, wird dem Benutzer schreibgeschützter Zugriff gewährt. Dieser Wert muss kleiner als die **Berechtigungsstufe des Administrators** sein.
Berechtigungs-stufe des Administrators	Geben Sie einen Wert zwischen 0 und 15 ein. Wenn die Berechtigungsstufe eines autorisierten Benutzers (Autorisierungsargument „priv-lvl“) größer oder gleich diesem Wert ist, wird dem Benutzer Administratorzugriff gewährt. Dieser Wert muss größer als die **Berechtigungsstufe** „**Nur-Lesen-Benutzer**“ sein.

Konfigurieren des TACACS+-Servers

Das Konfigurationsverfahren im Überblick.

Sie müssen Ihren TACACS+-Server so konfigurieren, dass er mit der NMC arbeiten kann.



Weitere Informationen zur Konfiguration des TACACS+-Servers finden Sie im **Sicherheitshandbuch**.

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 **Richtliniename** 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.

Einstellung	Beschreibung
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. Weitere Informationen finden Sie unter „Firewall-Protokoll“.

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:
  `priority 250, destination host any, source host any, protocol any, action discard`
- Fügen Sie Folgendes hinzu, wenn Sie die Firewall als Blacklist verwenden möchten:
  `priority 250, destination host any, source host any, protocol any, action 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 die EAP-TLS-Authentifizierungsmethode.

Bei der EAP-TLS-Methode wird eine gegenseitige Authentifizierung in einem TLS-Handshake durchgeführt, sodass das Netzwerk die NMC authentifizieren kann und die NMC das Netzwerk authentifizieren kann. Auf der NMC müssen ein Zertifikat einer End-Entität und der zugehörige private Schlüssel installiert sein. Dieses Zertifikat wird während des Handshakes an die Echtheitsbestätigung übergeben. Das Zertifikat der Echtheitsbestätigung wird während des Handshakes auch an die NMC übergeben. Damit die NMC dieses Zertifikat überprüfen kann, muss darauf auch das Zertifikat für die Zertifizierungsstelle installiert sein, die dieses Zertifikat signiert hat (oder die Stammzertifizierungsstelle, wenn eine Vertrauenskette verwendet wird). Diese Zertifikate müssen mithilfe des Zertifikatladers im Zertifikatspeicher der NMC installiert werden.
Siehe **„SSL-Zertifikate“**.

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

Die verfügbaren Optionen unterscheiden sich zwischen v2.5.x und v3.x.

Einstellung	Beschreibung
EAPoL-Zugang	Aktiviert die IEEE 802.1X-Authentifizierung (EAPoL) mit der EAP-TLS-Authentifizierungsmethode. **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, siehe **„SSL-Zertifikate“**.
Supplicant-Kennung	Die Identität des EAP-Supplicants, der an die Echtheitsbestätigung gesendet werden soll (bis zu 32 Zeichen einschließlich Leerzeichen). **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.
Client-Zertifikat	Das Client-Zertifikat der NMC, das im EAP-TLS-Handshake für die Authentifizierung verwendet werden soll. Es wird eine Liste der installierten Zertifikate von End-Entitäten bereitgestellt, von denen eines ausgewählt werden muss. Client-Zertifikate können auf der Seite **„SSL-Zertifikate“** installiert werden.

SSL-Zertifikate

Pfad: Konfiguration > Sicherheit > SSL-Zertifikate

Die Netzwerkmanagement-Karte unterstützt TLS (Transport Layer Security) und SSL (Secure Sockets Layer), wodurch eine weitere Sicherheitsstufe zusätzlich zu TCP geschaffen wird, indem Authentifizierung und Verschlüsselung zur Verbindung hinzugefügt werden. Zur Unterstützung von TLS/SSL-Verbindungen bietet die Netzwerkmanagement-Karte einen Zertifikatspeicher, in den sowohl X.509-Zertifikate als auch private Schlüssel hochgeladen werden können. Sowohl Zertifizierungsstellenzertifikate (CA, Certificate Authority) als auch Endeinheitzertifikate können hochgeladen werden.

Eine Liste aller installierten Zertifikate wird auf dieser Seite angezeigt. Durch Klicken auf den allgemeinen Namen eines Zertifikats werden Sie zur Seite mit den Zertifikatdetails weitergeleitet. Die Seite mit den Zertifikatdetails liefert zusätzliche Informationen zum Zertifikat und ermöglicht die Deinstallation der Datei, die das Zertifikat enthält.

Hochladen eines Zertifizierungsstellenzertifikats	
Einstellung	**Beschreibung**
Zertifikatdatei	Geben Sie das Zertifizierungsstellenzertifikat an. Die unterstützten Dateiformate sind das PEM- und DER-verschlüsselte X.509-Format. Die Dateierweiterung sollte .crt, .cer, .pem oder .der sein. PEM-Dateien können eine Liste mit einer beliebigen Anzahl an Zertifizierungsstellenzertifikaten enthalten.

Hochladen eines lokalen Gerätezertifikats	
Einstellung	**Beschreibung**
Zertifikatdatei	Geben Sie das Endeinheitzertifikat an. Die unterstützten Dateiformate sind das PEM- und DER-verschlüsselte X.509-Format. Die Dateierweiterung sollte .crt, .cer, .pem oder .der sein. PEM-Dateien können eine Zertifikatskette enthalten, wobei das erste Zertifikat das Endeinheitzertifikat ist. Die darauffolgenden Zertifikate müssen für Zwischenzertifizierungsstellen sein, wobei jedes Zertifikat das darauffolgende Zertifikat direkt zertifiziert.
Datei des privaten Schlüssels	Geben Sie den privaten Schlüssel für das Endeinheitzertifikat ein. Die Datei kann verschlüsselt oder unverschlüsselt sein und muss mit PEM- oder DER-Verschlüsselung im PKCS#8-Format vorliegen. Die Dateierweiterung sollte .p8, .key, .pem oder .der sein. **HINWEIS:** Alle privaten Schlüssel werden vor dem Speichern von der Netzwerkmanagement-Karte verschlüsselt.
Passphrase für den privaten Schlüssel	Geben Sie die Passphrase zur Entschlüsselung des verschlüsselten privaten Schlüssels an. Bis zu 64 Zeichen inklusive Leerzeichen sind zulässig. Wenn die Datei des privaten Schlüssels nicht verschlüsselt ist, muss dieses Feld leer bleiben.

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 „Benachrichtigungen“
- 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 3 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 „NMC Firmware-Upgrades“).

Bildschirm „TCP/IP-Einstellungen für IPv6“

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

Diese Option zeigt die aktuellen IPv6-Einstellungen der Netzwerkmanagement-Karte 3 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.

DHCPv6-Modus für die IPv6-Konfiguration	
Option	**Beschreibung**
Adresse und sonstige Informationen:	DHCPv6 wird verwendet, um Adressen UND weitere Konfigurationseinstellungen zu beziehen. Dieser Zustand wird als „DHCPv6 Stateful“ bezeichnet.
Nur Nicht-Adress-Informationen:	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.

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

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*.

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
```

Geben Sie das **minimale Protokoll** an, das zum Sichern der Kommunikation zwischen dem Browser und der Netzwerkmanagement-Karte verwendet wird: **TLS v1.1**, **TLS v1.2** oder **TLS v1.3** **(v3.1.x und höher)**.

Sie können die Verwendung eines Sitzungscookies für die Authentifizierungsverfolgung im Browser aktivieren, indem Sie die Option zum **Anfordern der Aktivierung des Authentifizierungscookies** verwenden. **ANMERKUNG:** Das Cookie wird entfernt, wenn die Sitzung endet.

Geben Sie mithilfe der Kontrollkästchen für den **eingeschränkten Statuszugriff** an, ob eine schreibgeschützte, öffentliche Webseite mit Basisgerätestatus angezeigt werden soll oder nicht. Diese Funktion ist standardmäßig deaktiviert und kann über die Option **Als Standardseite verwenden** so eingestellt werden, dass sie als Standardzielseite angezeigt wird, wenn ein Benutzer nur mit der IP/dem Hostnamen auf das Gerät zugreift.

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*.

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 „NMC Firmware-Upgrades“.

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. 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“

Alle Benutzernamen, Kennwörter und Community-Namen für SNMPv1 werden über das Netzwerk als Klartext übertragen. Sollte Ihr Netzwerk den durch Verschlüsselung gewährleisteten, hohen Sicherheitsstandard benötigen, sollten Sie den SNMPv1-Zugriff deaktivieren oder für alle Communitys das Zugriffsrecht „Nur Lesen“ einstellen. (Eine Community mit Nur-Lese-Zugriff kann Statusinformationen empfangen und SNMPv1-Traps verwenden.)

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

Ausführliche Informationen zur Erhöhung und Verwaltung der Systemsicherheit finden Sie im *Sicherheitshandbuch*.

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-256-, SHA- oder MD5-Authentifizierung und AES-256-, 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 8 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 8 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-256-, SHA- und MD5-Authentifizierung. Eine dieser Optionen muss ausgewählt werden.
- **Datenschutzprotokoll**: Die Implementierung von SNMPv3 unterstützt AES-256, 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.

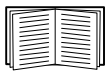
NMS-IP/Hostname: Die IP-Adresse, die IP-Adressmaske oder der Hostname, der den Zugriff durch das NMS kontrolliert. Ein Hostname oder eine bestimmte IP-Adresse (z. B. 149.225.12.1) ermöglicht dem NMS den Zugriff nur am betreffenden Standort. Bei IP-Adressmasken, die „255“ enthalten, ist der Zugriff wie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

USV-Geräte mit dem SRTL/SRYLF-Präfix mit integrierter Netzwerkmanagement-Karte unterstützen Modbus nicht.

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 NMC-Karte AP9640 unterstützen Modbus-TCP, die NMC-Karten AP9641 und AP9643 unterstützen serielle Modbus-Kommunikation sowie 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**.

Weitere Informationen zum Management geschalteter Steckdosengruppen über Modbus bei Smart-UPS-Modellen mit Präfix SMT, SMX, SURTD, SRC und SRT, siehe Anwendungshinweis Nr. 177.

HINWEIS: Temperatur- und Feuchtigkeitssensoren, die an die UIO-Ports der Netzwerkmanagement-Karten AP9641 und AP9643 angeschlossen sind, werden nicht über Modbus unterstützt.

Modbus seriell (nur AP9641 oder AP9643).

Befehlsfolge: Konfiguration > Netzwerk > Modbus > Seriell

1. Verwenden Sie **Zugriff**, um Modbus seriell als Kommunikationsmethode mit der Netzwerkmanagement-Karte zu aktivieren bzw. zu deaktivieren.
2. Legen Sie die Verbindungsparameter für die serielle Modbus-Verbindung fest:
   - Die **Baudrate** unterstützt 2400 (v3.0.x und höher), 9600 (Standard), 19200, 38400 (v3.0.x und höher), 57600 (v3.1.x und höher) oder 115200 (v3.1.x und höher).
   - **Paritätsbit** ist das Prüfbit und kann auf „Even“, „Odd“ oder „None“ eingestellt werden.
   - **Einzigartige Ziel-ID** ist die einzigartige ID des Zielgeräts. Sie kann auf einen Wert zwischen 1 und 247 eingestellt werden.
3. Klicken Sie auf „Apply“ (Übernehmen), um Ihre Änderungen zu speichern.

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

USV-Geräte mit dem SRTL/SRYLF-Präfix mit integrierter Netzwerkmanagement-Karte unterstützen BACnet nicht.

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

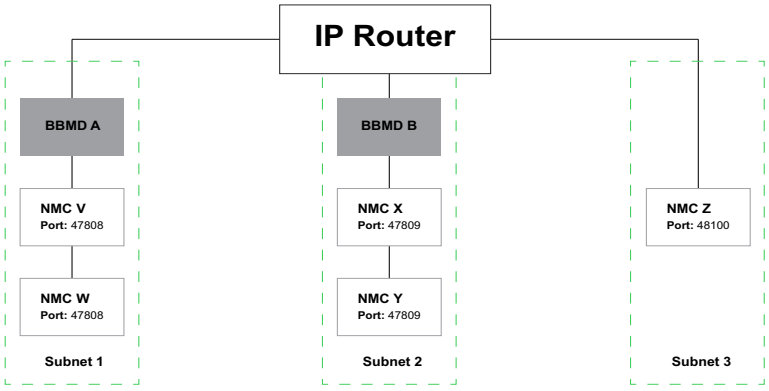
Weitere Informationen zu den USV-Datenpunkten, die über BACnet bereitgestellt werden, finden Sie in den BACnet-Anwendungstabellen auf der APC-Website www.apc.com.

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

Option	Beschreibung
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. 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.

Bildschirm „FTP-Server“

Befehlsfolge: Konfiguration > Netzwerk > FTP-Server

Verwenden Sie diesen Bildschirm, um den Zugriff auf einen FTP-Server zu aktivieren und einen Port festzulegen.

Option	Beschreibung
Zugriff	Per FTP werden Dateien unverschlüsselt übertragen. FTP ist standardmäßig deaktiviert. Verwenden Sie für eine verschlüsselte Dateiübertragung „Secure CoPy (SCP)“. SCP (über SSH) ist in der Voreinstellung aktiviert. Die Übertragung von Daten wird jedoch erst zugelassen, nachdem das standardmäßige Superuser-Passwort („apc“) geändert wurde. Ausführliche Informationen zur Erhöhung und Verwaltung der Systemsicherheit finden Sie im **Sicherheitshandbuch**.

Option	Beschreibung
Port	Der TCP/IP-Port des FTP-Servers (standardmäßig 21). Der FTP-Server verwendet stets den eingestellten Port und den unmittelbar darunter befindlichen Port. Die zulässigen, nicht standardmäßigen Portnummern sind auf dem Bildschirm angegeben: 21 und 5001–32768. **Hinweis**: Die Konfiguration des FTP-Servers zur Verwendung eines nicht standardmäßigen Ports verbessert die Sicherheit, da Benutzer dadurch den Portnamen in einer FTP-Befehlszeile an die IP-Adresse anhängen müssen. Vor dem angehängten Portnamen muss je nach verwendetem FTP-Client ein Leerzeichen oder ein Doppelpunkt stehen.

Menü „Benachrichtigungen“

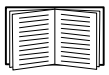
Siehe die folgenden Abschnitte:

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

Benachrichtigungsarten

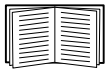
Sie können Benachrichtigungsaktionen konfigurieren, die als Reaktion auf ein Ereignis durchgeführt werden. Dadurch können Sie Benutzer auf unterschiedliche Art und Weise über ein Ereignis in Kenntnis setzen:

- 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

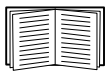
Konfigurieren nach Ereignis.

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 soll, 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 für die angegebene Zeit anhält (Standardwert ist 0), 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.

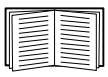
Für Ereignisse mit einem Löschereignis können Sie diese Parameter ebenfalls festlegen. (Ein Beispiel für ein Ereignis mit einem Löschereignis ist `USV: Kommunikation mit Batterie-Modulen unterbrochen` und `USV: Kommunikation mit Batterie-Modulen wiederhergestellt`.)

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 der DNS-Name für den SMTP-Server und die Absenderadresse, wenn „Server“ für mindestens einen E-Mail-Empfänger auf „Lokal“ festgelegt ist. Siehe **„SMTP-Server“** und **„E-Mail-Empfänger“** 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	Die Adresse, von der E-Mails von der Netzwerkmanagement-Karte gesendet werden.
SMTP-Server	Die IPv4-/IPv6-Adresse oder der DNS-Name des lokalen SMTP-Servers.
Authentifizierung	Aktivieren Sie diese Option, falls Ihr SMTP-Server eine Authentifizierung verlangt.
Port	Die SMTP-Portnummer, der Standardwert ist 25. Übliche Ports sind 25 für unverschlüsselte E-Mails bzw. 465 und 587 für SSL/TLS-verschlüsselte E-Mails. Sie haben die Möglichkeit, die Port-Einstellung auf einen beliebigen freien Port zwischen 1 und 65535 zu ändern.

Feld	Beschreibung
Benutzername/ Kennwort/ Kennwort bestätigen	Geben Sie hier Ihren Benutzernamen und Ihr Kennwort ein, wenn der SMTP-Server eine Authentifizierung verlangt.
Fortgeschr.	
SSL/TLS verwenden	• **Nie**: Der SMTP-Server benötigt/unterstützt keine Verschlüsselung • **Falls unterstützt**: Der SMTP-Server zeigt an, dass STARTTLS unterstützt wird, erfordert jedoch keine verschlüsselte Verbindung. Der STARTTLS-Befehl wird nach dem Advertisement gesendet. Dies wird in der Regel mit Port 25 verwendet. • **Immer**: Der SMTP-Server erfordert das Senden des STARTTLS-Befehls, sobald eine Verbindung zum Server hergestellt wird. Dies wird in der Regel mit Port 587 verwendet. • **Implizit**: Der SMTP-Server akzeptiert nur Verbindungen, die von vornherein verschlüsselt sind. Es wird keine STARTTLS-Nachricht an den Server gesendet. Dies wird in der Regel mit Port 465 verwendet.
Root-Zertifikat der Zertifizierungs-stelle erforderlich machen	Diese Option sollte dann aktiviert werden, wenn die Sicherheitsrichtlinie Ihres Unternehmens das implizite Vertrauen von SSL-/TLS-Verbindungen nicht unterstützt. Wenn diese Option aktiviert ist, muss ein gültiges Zertifikat einer Zertifizierungsstelle für den SMTP-Server mithilfe des Zertifikatladers im Zertifikatspeicher der NMC installiert werden, damit eine TLS-Verbindung mit dem SMTP-Server hergestellt werden kann. Weitere Informationen finden Sie auf der Seite **„SSL-Zertifikate“**.

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.
Empfänger-adresse	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“.

Feld	Beschreibung
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. **HINWEIS**: Wenn Sie diese Einstellung verwenden, stimmt die Absenderadresse mit der Empfängeradresse überein, Authentifizierung und Verschlüsselung (TLS) werden deaktiviert und Port 25 wird verwendet. • **Benutzerdefiniert**: Diese Einstellung ermöglicht für jeden E-Mail-Empfänger eigene Servereinstellungen. Wenn diese Option ausgewählt ist, werden die folgenden Servereinstellungen aktiviert. Diese Einstellungen sind die gleichen wie die oben unter **„SMTP-Server“** beschriebenen und sind unabhängig davon.

Bildschirm „SNMP-Trap-Empfänger“

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

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“

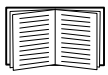
In diesem Menü finden Sie verschiedene Konfigurationsfunktionen, unter anderem für die Geräteidentifizierung, Datum und Uhrzeit, Export und Import der Konfigurationsoptionen Ihrer Netzwerkmanagement-Karte, für die drei Links unten links auf dem Bildschirm und für die Konsolidierung von Daten für die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

Bildschirm „Identifizierung“

Befehlsfolge: Konfiguration > Allgemein > Identifizierung

Definieren Sie den Namen (den NMC-Systemnamen, siehe „Bildschirm „DNS““), den Standort (den physischen Einbauort), die Systemnachricht (eine benutzerdefinierte Nachricht, die bei der Anmeldung angezeigt wird) und den Ansprechpartner (die für das Gerät verantwortliche Person), die verwendet werden von:

- durch den SNMP-Agenten der Netzwerkmanagement-Karte
- EcoStruxure™ IT oder 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 EcoStruxure™ IT oder Data Center Expert befindliche Netzwerkmanagement-Karte ihre Zeiteinstellungen über EcoStruxure™ IT oder 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.

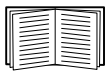
Beim Einstellen der Sommerzeit stellt das System die Uhr um eine Stunde vor, wenn die von Ihnen unter **Start** eingegebenen Einstellungen für Uhrzeit und Datum erreicht werden. Wenn die unter **Ende** eingegebenen Einstellungen erreicht werden, wird die Uhr um eine Stunde zurückgestellt.

- 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

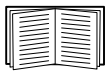
Verwenden Sie diese Option, um die URLs unten links auf jedem Bildschirm der Schnittstelle anzuzeigen und zu bearbeiten.

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*

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 RFC5424.

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 Port, den die Netzwerkmanagement-Karte verwendet, um Syslog-Nachrichten zu versenden. Der Standard-Port ist 6514. Dieser Port ist sicherem Syslog (TLS) zugewiesen.
Sprache	Wählen Sie die Sprache für etwaige Syslog-Nachrichten aus.
Protokoll	Wählen Sie zwischen UDP, TCP oder TLS.
TLS-Client-Zertifikat	Wenn TLS als Protokoll ausgewählt wurde, wählen Sie ein Client-Zertifikat, das zur gegenseitigen Authentifizierung mit dem Syslog-Server verwendet werden soll. Die standardmäßige Option „Keine“ deaktiviert die gegenseitige Authentifizierung. Client-Zertifikate können auf den **SSL-Zertifikate** installiert werden.

Syslog-Einstellungen

Befehlsfolge: Konfiguration > Protokolle > Syslog > Einstellungen

Feld	Beschreibung
Nachrichten-generierung	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
Schweregrad-zuordnung	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 RFC5424: • **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.`

CEIP im Menü „Konfiguration“

Pfad: Konfiguration > CEIP > Einstellungen

Das Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) der Netzwerkmanagement-Karte stellt uns Informationen zur Verfügung, die es uns ermöglichen, unsere Produkte und Dienstleistungen zu verbessern, und hilft uns, Sie zu beraten, wie Sie die Netzwerkmanagement-Karte am besten bereitstellen und konfigurieren können.

Im Rahmen des CEIP erfassen wir bestimmte Informationen darüber, wie Sie Ihre Netzwerkmanagement-Karte in Ihrer Umgebung konfigurieren und verwenden. Diese Informationen sind völlig anonym und können nicht verwendet werden, um eine Person zu identifizieren. Weitere Informationen finden Sie in den häufig gestellten Fragen zum Programm zur Verbesserung der **Benutzerfreundlichkeit (CEIP)**.

Testmenü

Prüfung und Kalibrierung

Befehlsfolge: Tests > USV

Diese Option ist nicht bei allen USV-Geräten verfügbar.

Es besteht keine Unterstützung für die Durchführung einer Kalibrierung von Lithium-Ionen-USV-Geräten, einschließlich USV-Geräten mit dem Präfix SRTL/SRYLF.

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: Bildschirm „USV Allgemein“.

- 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.

Die Menüs „Protokolle“ und „Info“

Arbeiten mit Ereignis- und Datenprotokollen

Das Ereignisprotokoll erfasst individuelle Ereignisse. Das Datenprotokoll bietet Ihnen dagegen einen Snapshot Ihres Systems, indem regelmäßig Werte erfasst werden.
In v3.0.x und höher enthält jedes Ereignis die folgenden Informationen:

Ereignis	Beschreibung
Datum	Das Datum, an dem das Ereignis eingetreten ist.
Zeit	Der Zeitpunkt, zu dem das Ereignis eingetreten ist.
Benutzer	Der Benutzer, der die Aktion initiiert hat. Dies kann sein: der Benutzername, „System“, wenn sie Teil eines internen Dienstes war, oder „Gerät“, wenn sie vom verbundenen Gerät initiiert wurde.
Ereignis	Der Informationstext, der das Ereignis beschreibt.
Code	Der Ereignisbezeichner. (Nicht in allen Benutzeroberflächen verfügbar.)

Ereignisprotokoll

In v3.0.x und höher werden standardmäßig alle Ereignisse im Protokoll angezeigt. Siehe „Konfigurieren nach Ereignis“.

Das Ereignisprotokoll zeichnet alle Ereignisse auf, z. B. Zugriffskontrolle, Anforderungsfehler, Systemereignisse, Konfigurationsänderungen (auch über die Datei „config.ini“) und Überwachungsereignisse. Es kann so konfiguriert werden, dass 25 bis 30.000 Ereignisse gespeichert werden. Der Standardwert ist 1500. Wenn das Ereignisprotokoll voll ist und ein neues Ereignis auftritt, wird das älteste Ereignis überschrieben. Wenn Sie Ihre Ereignisse beibehalten möchten, sollten Sie den Export von Ereignissen auf einen Syslog-Server konfigurieren.

Sie können die Farbcodierung für Ereignisse über „Lokale Benutzer“ im Menü „Konfiguration“ aktivieren.

HINWEIS: Ereignisprotokolle werden mit AES-256 ESSIV verschlüsselt und vor der Verwendung von der NMC kryptografisch mit HMAC-SHA256 authentifiziert.

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. Weitere Informationen finden Sie unter „Abrufen von Protokolldateien über SCP oder FTP“.

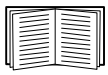
Filtern des Ereignisprotokolls. Verwenden Sie die Filterfunktion, um Informationen, die Sie nicht anzeigen möchten, auszublenden.

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*

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

Hinweis: Datenprotokolle werden mit AES-256 ESSIV verschlüsselt und vor der Verwendung von der NMC kryptografisch mit HMAC-SHA256 authentifiziert.

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***.

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
```

HINWEIS: Wenn der SCP-Befehl in OpenSSH Version 9.0 oder höher verwendet wird, wird SFTP standardmäßig für Dateiübertragungen verwendet. Dies führt zu einem Problem, da die NMC SFTP nicht unterstützt. Um SCP in der Version 9.0 oder höher zu verwenden, muss dem SCP-Befehl die Option „-O“ hinzugefügt werden, damit das SCP-Protokoll verwendet wird (scp -O <file> <user>@<remote>:<file>).

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.

Die Befehlsfolge für USV-Geräte mit dem SRTL/SRYLF-Präfix mit einer integrierten Netzwerkmanagement-Karte lautet Protokolle > Stromereignisse.

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.

Energieverbrauch

Befehlsfolge: Protokolle > Energieverbrauch

Diese Menüoption ist nicht bei allen USV-Geräten verfügbar.

Der kumulative Energieverbrauch für Ihr USV-Gerät wird zusammen mit einer wochenweisen Aufschlüsselung in der Tabelle im unteren Bildschirmbereich angezeigt.

Feld	Beschreibung
Energieverbrauch	Die bisher von Ihrer USV verbrauchte Energiemenge in Kilowattstunden. Zum Beispiel verbraucht eine USV, die eine 350-W-Glühlampe 1000 Stunden mit Strom versorgt, 350 kWh Energie.
Gesamtkosten	Die bisher anfallenden geschätzten Gesamtkosten an Energie. Für eine Glühlampe, die über 1000 Stunden 350 kWh Energie zu einem Preis von 0,10 US-Dollar pro kWh verbraucht, entstehen z. B. während dieses Zeitraums Kosten von 35 US-Dollar.
CO_2-Emissionen	Die geschätzte Menge an CO_2, die von dem Stromanbieter in die Umwelt freigesetzt wurde, um die bisher verbrauchte Energie bereitzustellen.

Die Kosten und CO_2-Emissionen können je nach Energiequelle und Verteilungsnetzwerk stark abweichen. Sie erhalten eine ungefähre Schätzung, indem Sie Ihr Land aus dem Dropdown-Listenfeld **Standort** auswählen oder den Link „**(bearbeiten)**“ verwenden, um Ihre eigenen Daten für Kosten und Emissionen einzugeben.

Durch das Bearbeiten eines Standorts wird ein benutzerdefinierter Standort erstellt. Die Standardzahlen für diesen Standort werden dadurch nicht geändert. Wenn Sie beispielsweise **IE-Irland** aus dem Dropdown-Listenfeld auswählen und demzufolge die Bearbeitungsfunktion zum Ändern der Daten verwenden, wird ein Eintrag namens **Benutzerdefiniert (IE-Irland)** oben in dem Dropdown-Listenfeld erstellt.

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.

Info zur Netzwerkmanagement-Karte 3

Wissenswertes zum USV-Gerät

Befehlsfolge: Info > USV

Die Befehlsfolge für USV-Geräte mit dem SRTL/SRYLF-Präfix mit einer integrierten Netzwerkmanagement-Karte lautet **Info > USV > Allgemein**.

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

Feld	Beschreibung
Modell/ Artikelnummer/ Seriennummer	Ihr USV-Gerät wird über diese Felder identifiziert.
Herstellungsdatum	Das Datum, an dem Ihre USV hergestellt wurde.
Firmware-Version	Die Versionsnummern der zurzeit in der USV installierten Firmware-Module.
Firmwareversion2	Die zweite Versionsnummer der derzeit in der USV installierten Firmware. Diese wird verwendet, wenn mehrere Prozessoren unterschiedliche Versionen benötigen.
Scheinbare Nennleistung	Die gesamte VA-Leistung der USV.
Tatsächliche Nennleistung	Das gesamte Belastungsvermögen (in Watt) der USV.
Scheinbare Nennleistung/Phase	Die VA-Leistung jeder USV-Phase. Technischer ausgedrückt beschreibt dies die aktuelle Scheinleistung für jede Phase in Voltampere (VA). Die Scheinleistung ist das Produkt aus den Effektivwerten von Spannung und Stromstärke.
Tatsächliche Leistung Nennleistung/Phase	Das gesamte Belastungsvermögen (in Watt) der USV. Die aktuelle Bypass-Wirkleistung je Phase in Watt (W). Die Wirkleistung ist das über die Zeit gemittelte Produkt aus Spannung und Stromstärke.
Artikelnummer der internen Batterie/ Artikelnummer der externen Batterie/	In diesen Feldern stehen die Teilenummern Ihrer Batterien. Diese können bei der Behebung von Fehlern oder bei der Bestellung von Ersatzteilen nützlich sein.

Befehlsfolge: Informationen > USV > Stromversorgung

Die folgenden Optionen gelten nur für USV-Geräte mit dem Präfix SRYLF und eingebetteter Netzwerkmanagement-Karte.

Feld	Beschreibung
Seriennummer	Die Seriennummer des Leistungsmoduls.
Artikelnummer	Die SKU des Leistungsmoduls.
Datum	Das Herstellungsdatum des Leistungsmoduls.
Version	Die Firmwareversion des Leistungsmoduls.

Befehlsfolge: Info > USV > Batterie

Die folgenden Optionen gelten nur für USV-Geräte mit dem SRTL/SRYLF-Präfix mit integrierter Netzwerkmanagement-Karte.

Feld	Beschreibung
Seriennummer	Die Seriennummer des Batterierahmens/-moduls.
Artikelnummer	Die Artikelnummer des Batterierahmens/-moduls.
Datum	Das Herstellungsdatum des Batterierahmens/-moduls.
Version	Die Firmwareversion des Batterierahmens/-moduls.

Klicken Sie auf das Hauptmenü oder XRn/Batterierahmen n, um zum Bildschirm **Hauptrahmen / Batterierahmen n** zu gelangen, der zusätzliche Informationen enthält.

Befehlsfolge: Informationen > USV > Intelligenzmodul

Die folgenden Optionen gelten nur für USV-Geräte mit dem Präfix SRYLF und eingebetteter Netzwerkmanagement-Karte.

Feld	Beschreibung
Seriennummer	Die Seriennummer des Intelligenzmoduls.
Artikelnummer	Die SKU des Intelligenzmoduls.
Datum	Das Herstellungsdatum des Intelligenzmoduls.
Version	Die Firmwareversion des Intelligenzmoduls.

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 und umfassen unter anderem Modell- und Seriennummer, Hardware-Revision, Herstellungsdatum, MAC-Adresse und Verwaltungsverfügbarkeit.

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. 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 „Aktualisieren 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.

Export von Konfigurationseinstellungen

Abrufen und Exportieren der INI-Datei

Das Verfahren im Überblick

Ein Administrator kann die .ini-Dateien einer Netzwerkmanagement-Karte 3 (NMC) 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**.

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.*
   - Ab Version 3.2.x kann der benutzerdefinierte Name der INI-Datei optional den CRC32 zur Integritätsprüfung der INI-Datei vor der Verarbeitung enthalten. Damit diese Prüfung aktiviert werden kann, muss das Namensformat der INI-Datei wie folgt lauten: <name>_CRC32-<8 hexidecimal CRC32>.ini.
     Wenn die INI-Datei beispielsweise den CRC32 von 47C6C10D berechnet hat, könnte der Name der benutzerdefinierten INI-Datei wie folgt lauten: config_CRC32-47C6C10D.ini. Wenn die NMC3 eine INI-Datei mit dieser Namenskonvention empfängt, berechnet sie den CRC32 der Datei und überprüft, ob dieser übereinstimmt, bevor der Inhalt verarbeitet wird.

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:

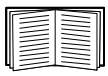
```
ftp> hash
```

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**.

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.
Konfigurationsdateiwarnung: Konfigurationsdatei kann nicht verarbeitet werden. Integritätsprüfung fehlgeschlagen: Der berechnete Wert war CRC32 (v3.2.x und höher).	Wenn die Datei so benannt ist, dass sie den CRC32 enthält, und der berechnete CRC32 nicht mit dem angegebenen CRC32 übereinstimmt, wird er nicht verarbeitet. Überprüfen Sie den Inhalt, und benennen Sie die Datei korrekt in „CRC32“ um.

Meldungen in der Datei config.ini

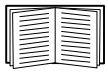
Ein Gerät in Verbindung mit der Netzwerkmanagement-Karte, aus der Sie die Datei config.ini heruntergeladen haben, muss vom System entdeckt werden, damit seine Konfiguration einbezogen werden kann. Wenn das Gerät (z. B. eine USV) nicht vorhanden ist oder nicht entdeckt wurde, enthält die Datei config.ini 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.

NMC Firmware-Upgrades

Aktualisieren der Firmware

Die Firmware-Version 2.5.x ist die letzte NMC3-Firmware, die ohne ein Secure NMC System-Abonnement verfügbar ist. Das Secure NMC System (SNS) schützt Ihr Unternehmen, indem es sicherstellt, dass Ihre angeschlossenen Geräte vor unbekannten Bedrohungen geschützt sind (IEC 62443-4-2), den sich ändernden Vorschriften entsprechen und über die gesamte Lebensdauer Ihrer Hardware stabil sind. Um mehr zu erfahren, besuchen Sie bitte **www.apc.com/secure-nmc**.

Methoden zur Übertragung von Firmware-Dateien

Um die Firmware eines oder mehrerer NMCs zu aktualisieren, laden Sie das Secure NMC System Tool für Ihre Anwendung von der APC Website herunter. Weitere Informationen zur Verwendung des Secure NMC System Tools finden Sie im **Benutzerhandbuch**.

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.

Sicherer Start mit Vertrauensanker

Der sichere Start mit Vertrauensanker bietet verbesserte Sicherheit auf NMC-Hardwareebene. Der Prozessor der NMC verwendet ECDSA, um die Signatur des Bootloaders mit einem bekannten öffentlichen Schlüssel zu überprüfen. Der Bootloader verwendet ECDSA auch, um Firmware-Signaturen mithilfe des im Bootloader gespeicherten öffentlichen Schlüssels der Zertifizierungsstelle für die Firmware-Signatur von Schneider Electric zu überprüfen.

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“.

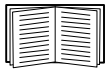
Problem	Lösung
Die Netzwerkmanagement-Karte reagiert nicht auf den Ping-Befehl	Wenn die Status-LED der Netzwerkmanagement-Karte grün leuchtet, senden Sie den Ping-Befehl versuchsweise an eine andere Station in dem Netzwerksegment, in dem sich die Netzwerkmanagement-Karte befindet. Wenn auch dann eine 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, 38400, 57600 oder 115200.
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



Weitere Informationen zur Modbus-Verbindung und seriellen Konfiguration für die Karten AP9641 und AP9643 finden Sie im Modbus-Dokumentationsanhang. Ausführliche Informationen zu den Modbus-Registern und Bit-Beschreibungen finden Sie auf den *Modbus-Registerkarten* auf der **APC-Website**.

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

Die Copyright-Hinweise für die Netzwerkmanagement-Karte 3 können Sie **hier** anzeigen.

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

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

- 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.

990-91148N–005 **5/2025**