

Installationshandbuch

USV-Netzwerkmanagement-Karte 4

AP9644

990-91053A-005

Veröffentlichungsdatum: October 2020



Rechtlicher Hinweis von Schneider Electric IT

Schneider Electric IT 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 IT 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 IT 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 IT, MUTTER-, SCHWESTER- ODER TOCHTERGESELLSCHAFTEN VON SCHNEIDER ELECTRIC IT 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 IT VON DER MÖGLICHKEIT SOLCHER SCHÄDEN AUSDRÜCKLICH UNTERRICHTET WURDE. SCHNEIDER ELECTRIC IT BEHÄLT SICH DAS RECHT VOR, HINSICHTLICH DER PUBLIKATION, IHRES INHALTS ODER FORMATS JEDERZEIT UNANGEKÜNDIGT ÄNDERUNGEN ODER AKTUALISIERUNGEN VORZUNEHMEN.

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

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

Inhalt

- Wichtige Sicherheitsinformationen 1**
 - Sicherheitsinformationen für die
Netzwerkmanagement-Karte 4 2
- Einleitende Informationen 3**
 - Funktionen 3
 - Unterstützte Geräte 3
 - Zugehörige Dokumente 4
 - Lieferumfang 4
 - Haftungsausschluss 4
 - Ändern der Sprache der Web-Benutzeroberfläche 4
- Einbau in eine USV. 5**
 - Einbau der Karte in unterschiedliche USV-Modelle 5
 - Schritt 1: Einbau der Network Management Card 5
 - Schritt 2: Konfigurieren der Network Management Card . . . 6
- Schnellkonfiguration 7**
 - Übersicht 7
 - Verfahren für die TCP/IP-Konfiguration 7
 - Konfiguration über BOOTP und DHCP 7
 - Lokaler Zugriff auf die Weboberfläche 9
 - Remotezugriff auf die Befehlszeilenschnittstelle 9
 - Lokaler Zugriff auf die Befehlszeilenschnittstelle 10
 - Befehlszeilenschnittstelle 10
 - USV-Benutzeroberfläche 11
- Zurücksetzen bei vergessenem Passwort. 12**
- Zugriff auf eine konfigurierte Netzwerkmanagement-Karte . . . 13**
 - Übersicht 13
 - Weboberfläche 13
 - Zugriff auf die Befehlszeilenschnittstelle 14
 - Simple Network Management Protocol (SNMP) 14
 - SFTP 15

Sicherheitsverwaltung des Systems 15

Technische Daten AP9644..... 16

Wichtige Sicherheitsinformationen

Lesen Sie die Anweisungen sorgfältig durch und machen Sie sich mit dem Gerät vertraut, bevor Sie versuchen, es zu installieren, zu bedienen, zu reparieren oder zu warten. In diesem Handbuch bzw. auf dem Gerät sind hin und wieder die folgenden speziellen Hinweise zu sehen, die Sie vor potenziellen Gefahren warnen oder Ihre Aufmerksamkeit auf Informationen richten sollen, die eine Vorgehensweise verdeutlichen oder vereinfachen.



Wenn zusätzlich zu einem Sicherheitskennzeichen mit einem Gefahren- oder Warnhinweis dieses Symbol zu sehen ist, wird auf eine elektrische Gefahr hingewiesen, die bei Nichtbeachtung der Anweisungen zu Verletzungen führen kann.



Dieses Symbol ist eine Sicherheitswarnung. Es weist auf mögliche Verletzungsgefahren hin. Beachten Sie alle Sicherheitshinweise, die auf dieses Symbol folgen, um mögliche schwere oder tödliche Verletzungen zu verhindern.

⚠ GEFAHR

GEFAHR weist auf eine gefährliche Situation hin, die bei Nichtverhinderung zum Tod oder zu schweren Verletzungen **führen wird**.

⚠ WARNUNG

WARNUNG zeigt eine potenziell gefährliche Situation an, die bei Nichtverhinderung zum Tod oder zu schweren Verletzung **führen kann**.

⚠ VORSICHT

VORSICHT zeigt eine potenziell gefährliche Situation an, die bei Nichtverhinderung zu einer kleineren oder mittelschweren Verletzung **führen kann**.

HINWEIS

HINWEIS verweist auf Vorgehensweisen, die nicht im Zusammenhang mit Verletzungen stehen, einschließlich bestimmter Umweltgefahren, möglicher Schäden oder Datenverluste.

Sicherheitsinformationen für die Netzwerkmanagement-Karte 4

Die Netzwerkmanagement-Karte (NMC) enthält eine herausnehmbare Batterie. Wenn diese Batterie verschluckt wird, müssen Sie sich umgehend in ärztliche Behandlung begeben.

⚠ WARNUNG
GEFAHR INNERER VERBRENNUNGEN
<ul style="list-style-type: none">• Die Batterie darf nicht verschluckt werden.• Die Batterien müssen von Kinder ferngehalten werden.
Die Nichtbeachtung dieser Vorschrift kann zu schweren Verletzungen oder zum Tode führen.

HINWEIS: Befestigen Sie die NMC mit Schrauben am SmartSlot des USV-Geräts, sodass sich die Batterie außer Reichweite befindet.

Einleitende Informationen

Funktionen

Die im vorliegenden Dokument beschriebene USV-Netzwerkmanagement-Karte (AP9644) von Schneider Electric ist ein webbasiertes Produkt. Geräte mit installierter Netzwerkmanagement-Karte (NMC) können mithilfe verschiedener offener Standards verwaltet werden:

Hypertext Transfer Protocol (HTTP)	Secure Shell (SSH)
Simple Network Management Protocol Version 1, 2c und 3	Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS)
File Transfer Protocol (FTP)	Secure File Transfer Protocol (SFTP)
Syslog	Modbus



HINWEIS: Nur HTTPS und SSH sind standardmäßig aktiviert.

Die **AP9644** Network Management Card:

- *Stellt Ereignisprotokolle bereit.*
- *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 NMC.*
- *Bietet mehrere Sicherheitsprotokolle für Authentifizierung und Verschlüsselung.*
- *Kommuniziert mit EcoStruxure IT und StruxureWare Data Center Expert.*
- *Unterstützt Modbus TCP/IP und Modbus RTU. Informationen zur Konfiguration von Modbus RTU finden Sie im Modbus-Dokumentationsanhang.*
- *Unterstützt einen universellen Eingabe-/Ausgabe-Anschluss, an den Sie einen Temperatursensor (AP9335T) oder Temperatur-/Feuchtigkeitssensor (AP9335TH) anschließen können.*

Unterstützte Geräte

Die Netzwerkmanagement-Karte 4 ist kompatibel mit 3-phasigen Galaxy VS-USV-Geräten.

Zugehörige Dokumente

Folgende Dokumentation ist auf der [Schneider Electric-Website](#) abrufbar:

- *Befehlszeilenhandbuch für die USV-Netzwerkmanagement-Karte 4*
- *Modbus-Dokumentationsanhang für die USV-Netzwerkmanagement-Karte 4*
- *Galaxy VS Modbus Register Map*
- *Sicherheitshandbuch*
- *PowerNet® Management Information Base (MIB) Referenzhandbuch*
- *Konformitätserklärung*

Lieferumfang

Die folgenden Elemente sind im Lieferumfang der Network Management Card enthalten:

- *Dieses Installationshandbuch*
- *USV-Netzwerkmanagement-Karte 4*
- *Micro-USB-Konfigurationskabel (Teilenummer 960-0603)*
- *Temperatursensor (AP9335T)*
- *Modbus-Dokumentationsanhang für die USV-Netzwerkmanagement-Karte 4*
- *Network Management Card Qualitätskontrollabschnitt*
- *Garantie-Registrierungskarte*

Haftungsausschluss

Schneider Electric haftet nicht für während der Rücksendung dieses Produkts aufgetretene Schäden.



Recycling

Die Network Management Card 4 reagiert empfindlich auf statische Elektrizität. Berühren Sie bei der Handhabung der Netzwerkmanagement-Karte nur die Endplatte und verwenden Sie eine oder mehrere dieser Elektrostatik-Schutzvorrichtungen (ESDs): Armbänder, Fersenbänder, Zehenschlaufen, leitfähige Schuhe.

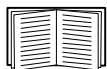


Die Verpackung besteht aus wiederverwertbarem Material. Bewahren Sie die Verpackung für die spätere Verwendung auf, oder entsorgen Sie sie ordnungsgemäß.



Management-Produkte enthalten auswechselbare Lithium-Knopfzellenbatterien – dies gilt auch für die Netzwerkmanagement-Karte. Halten Sie beim Entsorgen dieser Batterien die geltenden Vorschriften für das Recycling ein.

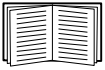
Ändern der Sprache der Web-Benutzeroberfläche



Sie können die Sprache, in der die Web-Benutzeroberfläche der Netzwerkmanagement-Karte angezeigt wird, über den Anmeldebildschirm für die Web-Benutzeroberfläche ändern.

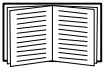
Einbau in eine USV

Einbau der Karte in unterschiedliche USV-Modelle



Eine vollständige Auflistung kompatibler USVs, in denen eine Netzwerkmanagement-Karte eingebaut werden kann, finden Sie im Knowledge Base-Artikel [FA237786](#) auf der [Schneider Electric-Website](#).

Schritt 1: Einbau der Network Management Card



Zum Einbau der NMC in einem unterstützten Galaxy-USV-Gerät müssen Sie das Gerät nicht ausschalten. Wenn Sie Ihre USV vor der Installation der Netzwerkmanagement-Karte ausschalten möchten, lesen Sie den Knowledge Base-Artikel [FA156132](#) auf der [Schneider Electric-Website](#).

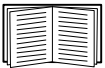


Die Netzwerkmanagement-Karte reagiert empfindlich auf statische Elektrizität. Berühren Sie bei der Handhabung der Netzwerkmanagement-Karte nur die Endplatte und verwenden Sie eine oder mehrere dieser Elektrostatik-Schutzvorrichtungen (ESDs): Armbänder, Fersenbänder, Zehenschlaufen, leitfähige Schuhe.

Die Netzwerkmanagement-Karte (NMC) enthält eine herausnehmbare Batterie. Wenn diese Batterie verschluckt wird, müssen Sie sich umgehend in ärztliche Behandlung begeben.

WARNUNG	
GEFAHR INNERER VERBRENNUNGEN	
<ul style="list-style-type: none">• Die Batterie darf nicht verschluckt werden.• Die Batterien müssen von Kinder ferngehalten werden.	
Die Nichtbeachtung dieser Vorschrift kann zu schweren Verletzungen oder zum Tode führen.	

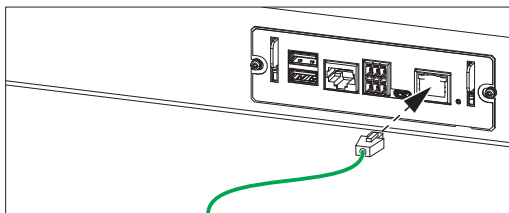
HINWEIS: Befestigen Sie die NMC mit Schrauben am SmartSlot des USV-Geräts, sodass sich die Batterie außer Reichweite befindet.



Weitere Informationen zur Position des USV-Kartensteckplatzes finden Sie in der Dokumentation zur USV.

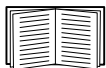
1. Lokalisieren Sie den USV-Kartensteckplatz.
2. Verwenden Sie die Schrauben, mit denen das Abdeckblech befestigt ist, um die Netzwerkmanagement-Karte im Kartensteckplatz der USV zu befestigen.

3. Schließen Sie ein Netzwerkkabel an den 10/100/1000Base-T-Netzwerkanschluss 1 der Netzwerkmanagement-Karte an.



Sobald das Netzwerkkabel angeschlossen ist, versucht die Netzwerkmanagement-Karte, über DHCP eine IP-Adresse zu erhalten. Siehe „Verfahren für die TCP/IP-Konfiguration“ auf Seite 7. **HINWEIS:** Die IP-Adresse der Karte wird auf dem Display der USV angezeigt.

Schritt 2: Konfigurieren der Network Management Card



Siehe „Schnellkonfiguration“ auf Seite 7.

Schnellkonfiguration

Übersicht

DHCP ist bei der Netzwerkmanagement-Karte (NMC) standardmäßig aktiviert. Bevor die USV-Netzwerkmanagement-Karte jedoch in einem Netzwerk betrieben werden kann, müssen Sie bei einer manuellen Konfiguration die folgenden Einstellungen für TCP/IP festlegen:

- IP-Adresse der Netzwerkmanagement-Karte
- Subnetzmaske
- Standardgateway



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.



Verwenden Sie nicht die Loopback-Adresse (127.0.0.1) als Standardgateway-Adresse der Netzwerkmanagement-Karte. Damit deaktivieren Sie die Karte und müssen die TCP/IP-Einstellungen über eine serielle lokale Anmeldung auf die Standardwerte zurücksetzen.

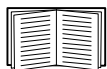
Verfahren für die TCP/IP-Konfiguration

Verwenden Sie eine der folgenden Methoden, um die von der benötigten TCP/IP -Einstellungen Netzwerkmanagement-Karte für IPv4 festzulegen:

- „Konfiguration über BOOTP und DHCP“ auf Seite 7
- „Zurücksetzen bei vergessenem Passwort“ auf Seite 12
- Ein mit dem Netzwerk verbundener Computer:
 - „Remotezugriff auf die Befehlszeilenschnittstelle“ auf Seite 9

Konfiguration über BOOTP und DHCP

Die Standardeinstellung für die TCP/IP-Konfiguration, **DHCP**, setzt voraus, dass ein ordnungsgemäß konfigurierter DHCP-Server verfügbar ist, von dem Netzwerkmanagement-Karte ihre TCP/IP-Einstellungen beziehen können. Sie können die Einstellung auch für BOOTP konfigurieren.

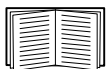


Falls kein solcher Server vorhanden ist, können Sie die erforderlichen TCP/IP-Einstellungen wie unter „Remotezugriff auf die Befehlszeilenschnittstelle“ auf Seite 9 oder „USV-Benutzeroberfläche“ auf Seite 11 beschrieben konfigurieren.

BOOTP. Damit die Network Management Card einen BOOTP-Server zum Konfigurieren ihrer TCP/IP-Einstellungen verwenden kann, muss sie einen ordnungsgemäß konfigurierten, RFC951-konformen BOOTP -Server vorfinden.

Geben Sie in der Datei BOOTPTAB des BOOTP -Servers die MAC-Adresse, die IP-Adresse, die Subnetzmaske und das Standardgateway der Netzwerkmanagement-Karte sowie gegebenenfalls den Namen einer verwendeten Bootdatei ein. Die MAC-Adresse befindet sich auf der Unterseite der Netzwerkmanagement-Karte oder auf dem Qualitätskontrollabschnitt im Karton.

DHCP. Sie können einen RFC2131/RFC2132-konformen DHCP -Server verwenden, um die TCP/IP -Einstellungen für die Netzwerkmanagement-Karte zu konfigurieren.



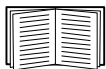
Dieser Abschnitt beschreibt die Kommunikation der Netzwerkmanagement-Karte mit einem DHCP -Server.

1. Die NMC sendet eine DHCP -Anfrage und identifiziert sich darin mit folgenden Angaben:
 - einem Vendor Class Identifier (Herstellerklassenkennung, Standardwert:APC)
 - einem Client Identifier (in der Grundeinstellung die MAC-Adresse der NMC)
 - einem User Class Identifier (in der Grundeinstellung die Kennung der auf der NMC installierten Anwendungsfirmware).
2. Ein ordnungsgemäß konfigurierter DHCP -Server antwortet mit einem DHCP -Angebot, das alle Einstellungen enthält, die von der NMC für die Kommunikation im Netzwerk benötigt werden. Das DHCP -Angebot enthält auch die Option „Herstellerspezifische Informationen“ (DHCP -Option 43). Die NMC kann so konfiguriert werden, dass sie DHCP -Angebote ignoriert, die in der DHCP-Option 43 nicht das entsprechende APC-Cookie im nachfolgend aufgeführten Hexadezimalformat enthalten. (Die Karte benötigt dieses Cookie in der Grundeinstellung nicht.)

Option 43 = 01 04 31 41 50 43

Hierbei ist

- das erste Byte (01) der Code
- das zweite Byte (04) die Länge und
- die übrigen Bytes (31 41 50 43) sind das APC -Cookie.



Die Dokumentation zum DHCP -Server enthält Informationen über das Hinzufügen von Code zur Option „Herstellerspezifische Informationen“.



Die Web-Benutzeroberfläche der NMC verfügt über Optionen zur Nutzung von anbieterspezifischen Daten, um Daten von einem DHCP-Server anzufordern und ein „APC“-Cookie anzulegen, über welches Informationen an die Karte übermittelt werden.

Lokaler Zugriff auf die Weboberfläche

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

1. Verbinden Sie das mitgelieferte Micro-USB-Kabel (Teilenummer 960-0603) mit dem USB-Anschluss des Computers und dem Konsolenport der Netzwerkmanagement-Karte.
2. Geben Sie <https://169.254.252.1> in die Adressleiste eines [unterstützten Browsers](#) und drücken Sie die **EINGABETASTE**. **Hinweis:** In der Firmware Version 6.3 und darunter wurde die IP Adresse "172.16.2.1" verwendet.
3. Verwenden Sie **apc** als **Benutzername** und **Passwort**.
HINWEIS: Beim ersten Anmelden beim Superuser-Konto ist das Passwort „apc“. Nach dem Einloggen werden Sie aufgefordert, ein neues Passwort zu erstellen.



Wenn das Micro-USB-Kabel während des Hochfahrens der NMC mit dem Computer verbunden ist, wird die NMC nicht erkannt. Zur Behebung des Problems trennen Sie das Micro-USB-Kabel und verbinden es wieder, wenn die NMC komplett hochgefahren ist.

HINWEIS: Die Status-LED der NMC leuchtet dauerhaft grün, wenn das Hochfahren abgeschlossen ist. Weitere Informationen zu den LEDs der NMC finden Sie im Knowledge Base-Artikel [FA265129](#).

Remotezugriff auf die Befehlszeilenschnittstelle

Auf einem Computer in demselben Netzwerk wie die Netzwerkmanagement-Karte können Sie die IP-Adresse über die USV-HMI erhalten. Danach können Sie über Secure Shell (SSH) auf die Befehlszeilenschnittstelle der NMC zugreifen und die anderen TCP/IP -Einstellungen konfigurieren.



Nachdem die Netzwerkmanagement-Karte IP-Adresse der konfiguriert wurde, können Sie mit SSH auf die Netzwerkmanagement-Karte zugreifen.

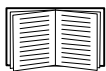
1. Verwenden Sie SSH, um unter der neu zugewiesenen IP-Adresse auf die Netzwerkmanagement-Karte zuzugreifen. Zum Beispiel:

```
ssh apc@156.205.14.141
```

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

2. Verwenden Sie **apc** als **Benutzername und Passwort**.

HINWEIS: Beim ersten Anmelden beim Superuser-Konto ist das Passwort „apc“. Nach dem Einloggen werden Sie aufgefordert, ein neues Passwort zu erstellen.



Informationen über das Abschließen der Konfiguration finden Sie unter „Befehlszeilenschnittstelle“ auf Seite 10.

Lokaler Zugriff auf die Befehlszeilenschnittstelle

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

1. Verbinden Sie das mitgelieferte Micro-USB-Kabel (Teilenummer 960-0603) mit dem USB-Anschluss des Computers und dem Konsolenport der Netzwerkmanagement-Karte.
2. Führen Sie ein Terminalprogramm (z. B. Terminal-Emulatorprogramme von Drittanbietern wie HyperTerminal, PuTTY oder Tera Term) aus und konfigurieren Sie Folgendes:
 - **IP address (IP-Adresse):** 169.254.252.1. **Hinweis:** In der Firmware Version 6.3 und darunter wurde die IP Adresse "172.16.2.1" verwendet.
 - **Port:** 22
 - **Connection type (Verbindungsart):** SSH/SFTP
3. Drücken Sie die `EINGABETASTE` ggf. mehrmals, um die Eingabeaufforderung **User Name** (Benutzername) aufzurufen.
4. Verwenden Sie **apc** als **Benutzername** und **Passwort**.
HINWEIS: Beim ersten Anmelden beim Superuser-Konto ist das Passwort „apc“. Nach dem Einloggen werden Sie aufgefordert, ein neues Passwort zu erstellen.



Wenn das Micro-USB-Kabel während des Hochfahrens der NMC mit dem Computer verbunden ist, wird die NMC nicht erkannt. Zur Behebung des Problems trennen Sie das Micro-USB-Kabel und verbinden es wieder, wenn die NMC komplett hochgefahren ist.

HINWEIS: Die Status-LED der NMC leuchtet dauerhaft grün, wenn das Hochfahren abgeschlossen ist. Weitere Informationen zu den LEDs der NMC finden Sie im Knowledge Base-Artikel [FA265129](#).

Befehlszeilenschnittstelle

Nachdem Sie sich wie in „Remotezugriff auf die Befehlszeilenschnittstelle“ auf Seite 9 beschrieben bei der Befehlszeilenschnittstelle angemeldet haben, können Sie manuell Netzwerkeinstellungen konfigurieren.

1. Wenden Sie sich an Ihren Netzwerkadministrator, um die IP-Adresse, die Subnetzmaske und das Standardgateway für die Netzwerkmanagement-Karte zu erhalten.
2. Verwenden Sie zur Konfiguration der Netzwerkeinstellungen diese drei Befehle. (Kursiver Text steht für eine Variable.)

```
tcpip
-i IhreIPAdresse
-s IhreSubnetzMaske
-g IhrStandardGateway
```

Geben Sie für jede Variable einen numerischen Wert im Format `xxx.xxx.xxx.xxx` ein.

Der Befehl kann in eine einzige Zeile eingegeben werden. Wenn Sie

beispielsweise die System-IP-Adresse 156.205.14.141, die Subnetzmaske 255.255.255.0 und das Standardgateway 156.205.14.1 einstellen möchten, geben Sie den folgenden Befehl ein und drücken Sie anschließend die EINGABETASTE:


```
tcpip -i 156.205.14.141 -s 255.255.255.0 -g 156.205.14.1
```

3. Verwenden Sie diesen Befehl, damit die NMC die in Schritt 1 erhaltene statische IP-Adresse verwendet, anstatt die IP-Adresse von DHCP abzurufen:

```
boot -b manual
```

USV-Benutzeroberfläche

Die IP-Adresse der NMC kann in der Benutzeroberfläche der USV konfiguriert werden:

1. Wenn Sie die Netzwerkeinstellungen manuell zuweisen möchten, wenden Sie sich an Ihren Systemadministrator, um eine gültige IP-Adresse, die Subnetzmaske und das Standardgateway für die Netzwerkmanagement-Karte zu erhalten.
2. Drücken Sie in der Benutzeroberfläche das Symbol  (Menü) und dann das Symbol für **Konfiguration** oder **Steuerung**, um sich bei der USV anzumelden.
3. Geben Sie bei der Aufforderung das **Benutzer** -Passwort für die USV ein (standardmäßig **admin/admin**).
4. Wählen Sie **Configuration > Network** (Konfiguration Netzwerk). Sie können IPv4- oder IPv6-Einstellungen für die NMC konfigurieren. Drücken Sie die Schaltfläche **Integrated NMC** (Integrierte NMC) unter dem benötigten IP-Format. **HINWEIS:** Wenn Sie eine weitere AP9644-Karte im SmartSlot der NMC eingesetzt haben, können Sie deren Netzwerkeinstellungen durch Auswahl von **Optional NMC** (Optionale NMC) konfigurieren.
5. Konfigurieren Sie die Netzwerkeinstellungen der Netzwerkmanagement-Karte:
 - a. **IPv4.** Wählen Sie die Netzwerkkonfigurationsoption für Ihr System aus: **Manual** (Manuell), **DHCP** oder **BOOTP**.
 - Wenn Sie **Manual** (Manuell) ausgewählt haben, geben Sie die IP-Adresse, die Subnetzmaske und das Standardgateway ein, die Sie in Schritt 1 erhalten haben.
 - Wenn Sie **DHCP** oder **BOOTP** auswählen, weist ein DHCP- oder BOOTP-Server automatisch IP-Adresse, Subnetzmaske und Standardgateway für die Netzwerkmanagement-Karte zu.
 - b. **IPv6.** Wählen Sie die Netzwerkkonfigurationsoption für Ihr System aus: **Auto configuration** (Auto-Konfiguration) oder **Manual** (Manuell).
 - Wenn Sie **Manual** (Manuell) auswählen, geben Sie die IP-Adresse und das Standardgateway ein, die Sie in Schritt 1 erhalten haben.
 - Wenn Sie **Auto configuration** (Auto-Konfiguration) auswählen, weist ein DHCPv6-Server automatisch die IP-Adresse und das Standardgateway für die Netzwerkmanagement-Karte zu. Sie können den DHCPv6-Modus auswählen: **Address and other information** (Adresse und sonstige Informationen), **non-address information only** (Nur Informationen außer Adresse) oder **IPv6 never** (IPv6 nie).
6. Wählen Sie **Ok**, um die Änderungen zu speichern.

Zurücksetzen bei vergessenem Passwort



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

Wenn Sie Ihr Passwort vergessen haben, müssen Sie die Taste **Reset** (Zurücksetzen) auf der NMC verwenden, um die gesamte Konfiguration, einschließlich des Passworts, zu löschen. Halten Sie die **Reset** -Taste 30 Sekunden lang gedrückt und prüfen Sie, ob die Status-LED während dieser Zeit grün blinkt. Wenn die Status-LED zu Gelb oder Orange wechselt, lassen Sie die **Reset** -Taste los, damit der Neustart der NMC abgeschlossen werden kann.

Nach dem Neustart der NMC müssen Sie die NMC neu konfigurieren. Siehe „Schnellkonfiguration“ auf Seite 7.

Zugriff auf eine konfigurierte Netzwerkmanagement-Karte

Übersicht

Sobald die USV-Netzwerkmanagement-Karte im Netzwerk ausgeführt wird, können Sie die nachstehend beschriebenen Schnittstellen zum Zugriff auf die Karte verwenden: Weboberfläche, SSH, SNMP, FTP und SFTP.



HINWEIS: Nur HTTPS und SSH sind standardmäßig aktiviert.

Weboberfläche

Die Weboberfläche der Netzwerkmanagement-Karte 4 ist kompatibel mit:

- Microsoft® Internet Explorer® (IE) 11 oder höher mit aktivierter Kompatibilitätsansicht
- Aktuelle Version von Mozilla® Firefox® oder Google® Chrome®

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

Sie können eines der folgenden Protokolle mit der Weboberfläche verwenden:

- Standardmäßig ist nur HTTPS aktiviert. Das HTTPS-Protokoll (standardmäßig aktiviert) bietet zusätzliche Sicherheit durch TLS (Transport Layer Security), verschlüsselt Benutzernamen und Passwörter sowie die übertragenen Daten und führt die Authentifizierung der Network Management Cardn über digitale Zertifikate durch.
- Das HTTP-Protokoll, bei dem die Authentifizierung über den Benutzernamen und das Passwort erfolgt, das aber keine Verschlüsselung bietet.

HINWEIS: HTTP ist standardmäßig deaktiviert. Beim ersten Einloggen in der Web-Benutzeroberfläche muss das HTTPS-Protokoll verwendet werden.

So greifen Sie auf die Weboberfläche zu und konfigurieren die Sicherheit des Geräts im Netzwerk:

1. Greifen Sie über die IP-Adresse (oder den DNS-Namen, sofern konfiguriert) auf die Network Management Card zu.
2. Geben Sie den Benutzernamen und das Passwort ein (Grundeinstellung für Superuser: **apc** und **apc**).
3. Verwenden Sie die Weboberfläche der NMC, um HTTPS zu aktivieren oder zu deaktivieren oder HTTP zu aktivieren.



Weitere Informationen zur Auswahl und Konfiguration der Netzwerksicherheit finden Sie im [Sicherheitshandbuch](#) zur *Netzwerkmanagement-Karte 4*, das auf der [Schneider Electric-Website](#) verfügbar ist.

Zugriff auf die Befehlszeilenschnittstelle

Der Zugriff auf die Befehlszeilenschnittstelle erfolgt über Secure Shell (SSH), das Benutzernamen, Passwörter und übertragene Daten verschlüsselt. SSH ist standardmäßig aktiviert.

Damit Sie SSH verwenden können, müssen Sie SSH zuerst konfigurieren und ein SSH-Client-Programm auf Ihrem Computer installiert haben.

Wenn Sie über SSH auf die Befehlszeilenschnittstelle zugreifen möchten, geben Sie in der Befehlszeile Folgendes ein:

```
ssh <Benutzername>@<IP-Adresse>
```

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

Simple Network Management Protocol (SNMP)



SNMPv1, SNMPv2c und SNMPv3 sind standardmäßig deaktiviert. Sie müssen Community-Namen in der Web-Benutzeroberfläche konfigurieren, bevor Sie eine beliebige Version von SNMP aktivieren können.

Der SNMP-Zugriff kann nur von einem Administrator aktiviert oder deaktiviert werden. Verwenden Sie zur Einrichtung die Weboberfläche oder die Befehlszeilenschnittstelle der Netzwerkmanagement-Karte.

Nur SNMPv1. Nachdem Sie einem SNMP MIB-Browser die PowerNet[®]-MIB hinzugefügt haben, können Sie diesen Browser für den Zugriff auf die Network Management Card verwenden.



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

Nur SNMPv3. Für den SNMP-Befehl GET sowie für 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.



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

Die Network Management Card unterstützt SHA- oder MD5-Authentifizierung und AES- oder DES-Verschlüsselung.

SNMPv1 und SNMPv3. Wenn Sie EcoStruxure IT oder StruxureWare Data Center Expert zum Verwalten der Network Management Card im öffentlichen Netzwerk eines StruxureWare-Systems verwenden, müssen Sie in der Benutzeroberfläche der Einheit SNMPv1 oder SNMPv3 aktiviert haben. Lesezugriff erlaubt es EcoStruxure IT und StruxureWare Data Center Expert, Alarme, Daten und Traps von der Network Management Card zu empfangen. Schreibzugriff ist erforderlich, wenn Sie EcoStruxure IT oder StruxureWare Data Center Expert als Alarm-, Daten- und Trap-Empfänger festlegen.



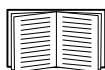
Sowohl SNMPv1 als auch SNMPv3 werden unterstützt; es empfiehlt sich jedoch, SNMPv3 zu verwenden, da diese Version sicherer ist und Verschlüsselung und Authentifizierung bietet.

SFTP

HINWEIS: Standardmäßig ist nur SFTP aktiviert. Sie können SFTP verwenden, sobald Sie über SSH oder HTTPS ein Benutzerpasswort erstellt haben.

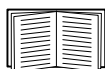
Um StruxureWare Data Center Expert zum Verwalten der UPS zu verwenden, müssen Sie in der Benutzeroberfläche der Network Management Card die Option **FTP-Server** aktiviert haben.

Der SFTP-Serverzugriff kann nur von einem Administrator aktiviert oder deaktiviert werden. Verwenden Sie zur Einrichtung die Weboberfläche oder die Befehlszeilenschnittstelle der Netzwerkmanagement-Karte.



Die SCP-Oberfläche ist aktiviert, wenn SSH aktiviert ist, da sie zur selben Protokollsuite gehören.

Sicherheitsverwaltung des Systems



Ausführliche Informationen zur Erhöhung der Systemsicherheit nach der Installation und Erstkonfiguration finden Sie im [Sicherheitshandbuch](#) zur *Netzwerkmanagement-Karte 4*, das auf der [Schneider Electric-Website](#) verfügbar ist.

Technische Daten AP9644

Maßangaben

Größe (H x B x T)	38,1 x 120,7 x 108,0 mm (1,50 x 4,75 x 4,25 in)
Gewicht	0,14 kg (0,30 lb)
Versandgewicht	0,91 kg (2,00 lb)

Umgebung

Höhe (über dem Meeresspiegel)	
Betrieb	0 bis 3.000m (0 bis 10.000 ft)
Lagerung	0 bis 15.000 m (0 bis 50.000 ft)
Temperatur	
Betrieb	0 bis 45°C (32 bis 113 °F)
Lagerung	-5 bis 45 °C (23 bis 113 °F)
Betriebsluftfeuchtigkeit	0 bis 95 %, nicht kondensierend

Einhaltung von gesetzlichen Vorschriften

Erfüllung der Normen zu Strahlungsemissionen	FCC Teil 15 Klasse A, VCCI Klasse A, ICES-003 Klasse A, EN 55032 Klasse A, AS/NZS CISPR 32, GOST-R 51318.22
Erfüllung der Normen zur Strahlungsimmunität	GOST-R 51318.24, EN 55024

Hochfrequenzstörungen



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

USA—FCC

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this user manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference. The user will bear sole responsibility for correcting such interference.

Canada—ICES

This Class A digital apparatus complies with Canadian ICES-003.

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

Japan—VCCI

この装置は、クラスA機器です。この装置を住宅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要求されることがあります。

VCCI-A

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。

Australia and New Zealand

Attention: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

European Union

This product is in conformity with the protection requirements of EU Council Directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility. Schneider Electric cannot accept responsibility for any failure to satisfy the protection requirements resulting from an unapproved modification of the product.

This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to CISPR 22/European Standard EN 55022. The limits for Class A equipment were derived for commercial and industrial environments to provide a reasonable protection against interference with licensed communication equipment.

Attention: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Weltweiter Kundendienst

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

- Besuchen Sie die Website von Schneider Electric, um auf Dokumente in der Schneider Electric Knowledge Base zuzugreifen und Anfragen an den Kundendienst zu senden.
 - **www.schneider-electric.com** (Unternehmenszentrale)
Auf den lokalisierten Websites von Schneider Electric für bestimmte Länder erhalten Sie Informationen zum Kundensupport.
 - **www.schneider-electric.com/support/**
Weltweite Unterstützung unserer Kunden mit der Schneider Electric Knowledgebase und dem elektronischen -Support.
- Sie sich per Telefon oder E-Mail an den Kundendienst von Schneider Electric wenden.
 - Lokale, länderspezifische Kundendienstzentren: Kontaktinformationen finden Sie unter **www.schneider-electric.com > Support > Unsere Niederlassungen finden.**

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