Installation Manual

Network Management Card for Easy UPS, 1-Phase & 3-Phase

AP9544, AP9547

990-6521E-001

Publication Date: May 2025

Schneider Electric

Schneider Electric IT Corporation Legal Disclaimer

The information presented in this manual is not warranted by the Schneider Electric IT Corporation to be authoritative, error free, or complete. This publication is not meant to be a substitute for a detailed operational and site specific development plan. Therefore, Schneider Electric IT Corporation assumes no liability for damages, violations of codes, improper installation, system failures, or any other problems that could arise based on the use of this Publication.

The information contained in this Publication is provided as is and has been prepared solely for the purpose of evaluating data center design and construction. This Publication has been compiled in good faith by Schneider Electric IT Corporation. However, no representation is made or warranty given, either express or implied, as to the completeness or accuracy of the information this Publication contains.

IN NO EVENT SHALL SCHNEIDER ELECTRIC IT CORPORATION, OR ANY PARENT, AFFILIATE OR SUBSIDIARY COMPANY OF SCHNEIDER ELECTRIC IT CORPORATION OR THEIR RESPECTIVE OFFICERS, DIRECTORS, OR EMPLOYEES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL, OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS, CONTRACT, REVENUE, DATA, INFORMATION, OR BUSINESS INTERRUPTION) RESULTING FROM, ARISING OUT, OR IN CONNECTION WITH THE USE OF, OR INABILITY TO USE THIS PUBLICATION OR THE CONTENT, EVEN IF SCHNEIDER ELECTRIC IT CORPORATION HAS BEEN EXPRESSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SCHNEIDER ELECTRIC IT CORPORATION RESERVES THE RIGHT TO MAKE CHANGES OR UPDATES WITH RESPECT TO OR IN THE CONTENT OF THE PUBLICATION OR THE FORMAT THEREOF AT ANY TIME WITHOUT NOTICE.

This manual is available in English on the APC website (www.apc.com).

Dieses Handbuch ist in Deutsch auf der APC webseite (www.apc.com) verfügbar.

Данное руководство на русском языке доступно на сайте APC (www.apc.com)

本マニュアルの日本語版は APC ウェブサイト (www.apc.com) からダウンロードできます。

在 APC 公司的网站上（www.apc.com）有本手册的中文版。

Contents

Important Safety Information

Read the instructions carefully to become familiar with the equipment before trying to install, operate, service, or maintain it. The following special messages may appear throughout this manual or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

The addition of this symbol to a Danger or Warning safety label indicates that an electrical hazard exists which will result in personal injury if the instructions are not followed.

This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

⚠ DANGER

DANGER indicates an imminently hazardous situation which, if not avoided, **will result in** death or serious injury.

⚠ WARNING

WARNING indicates a potentially hazardous situation which, if not avoided, **can result in** death or serious injury.

⚠ CAUTION

CAUTION indicates a potentially hazardous situation which, if not avoided, **can result in** minor or moderate injury.

NOTICE

NOTICE addresses practices not related to physical injury including certain environmental hazards, potential damage or loss of data.

Safety Information for the Network Management Card for Easy UPS

The Network Management Card (NMC) contains a removable battery. If this battery is ingested, seek immediate medical attention.

⚠WARNING

HAZARD OF INTERNAL BURNS

- Do not ingest the battery.
- Keep batteries out of reach of children.

Failure to follow these instructions can result in serious injury or death.

Note: Secure the NMC to the UPS device's SNMP Slot using screws to keep the battery out of reach.

Preliminary Information

Features

The Schneider Electric Network Management Cards for Easy UPS, 1-Phase & 3-Phase (AP9544, AP9547) discussed in this document are Web-based, IPv6 Ready products. Devices with the NMC installed can be managed using multiple open standards such as:

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

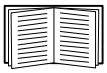
The **AP9544** and **AP9547** Network Management Cards:

- *Provide one USB-A host port.*
- *Provide data and event logs.*
- *Enable you to set up notifications through event logging, e-mail, Syslog and SNMP traps.*
- *Provide support for PowerChute® Network Shutdown.* ***NOTE:*** *The AP9547 card in 3-Phase Easy UPS devices only support the shut down of the connected servers and applications running on the servers. It is not supported to shut down the UPS device(s).*
- *Support using a Dynamic Host Configuration Protocol (DHCP) or BOOTstrap Protocol (BOOTP) server to provide the network (TCP/IP) values of the NMC.*
- *Provide the ability to export a user configuration (.ini) file from a configured card to one or more unconfigured cards without converting the file to a binary file.*
- *Provide a selection of security protocols for authentication and encryption.*
- *Communicate with Data Center Expert, Data Center Operation, or EcoStruxure™ IT.*
- *Support Modbus TCP/IP.*

Supported Devices

The Network Management Card for Easy UPS is compatible with:

- 1-Phase: Easy UPS On-line devices (AP9544 only).
- 3-Phase: Easy UPS 3S, 3S Pro, 3M, 3L, Galaxy 3L and Galaxy PW 2nd Gen.(AP9547 only).



Please refer to Knowledge Base article FA237786 for a list of UPS devices the Network Management Cards are compatible with.

Related documents

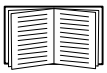
The following documentation is available on the APC website:

- *Network Management Card for Easy UPS, 1-Phase & 3-Phase User Guide*
- *Network Management Card for Easy UPS, 1-Phase & 3-Phase Command Line Interface (CLI) Guide*
- *Network Management Card for Easy UPS, 1-Phase & 3-Phase Modbus Register Maps*
- *Network Management Card for Easy UPS, 1-Phase & 3-Phase BACnet Application Maps*
- *Security Handbook*
- *PowerNet® Management Information Base (MIB) Reference Guide*
- *Declaration of Conformity*

Inventory

The Network Management Card package includes the following items:

- *This Installation Manual*
- *Network Management Card for Easy UPS*
- *Micro-USB configuration cable (part number 960-0603)*
- *Ferrite bead*
- *Alternate bracket (AP9544 only)*
- *Network Management Card quality assurance test slip*
- *Warranty registration form*



The quality assurance test slip contains the MAC address that you may need when performing the procedures in “UPS User Interface display”. You can also find the MAC address on the bottom of your NMC.

Disclaimer

Schneider Electric is not responsible for damage sustained during reshipment of this product.

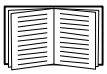
The Network Management Card (NMC) for Easy UPS is sensitive to static electricity. When handling the NMC, touch only the end plate while using one or more of these electrostatic-discharge devices (ESDs): wrist straps, heel straps, toe straps, or conductive shoes.

Please recycle

The shipping materials are recyclable. Save them for later use, or dispose of them appropriately.

Management products, including the NMC, contain removable, lithium coin-cell batteries. When discarding these batteries, you must follow local rules for recycling.

Changing Web UI Language



You can change the language the NMC Web interface is displayed in via the log in screen. See “Changing UI Language” in the User Guide for more information.

Installation in a UPS

How to install the card for different UPS models

To view the full list of compatible UPS in which an NMC can be installed, see Knowledge Base article FA237786.

Step 1: Install the Network Management Card

You do not need to turn off power to install the NMC in a supported Easy UPS. If you want to turn off your UPS before installing the Network Management Card, see the Knowledge Base article FA156132.

The NMC is sensitive to static electricity. When handling the NMC, touch only the end plate while using one or more of these electrostatic-discharge devices (ESDs): wrist straps, heel straps, toe straps, or conductive shoes.

The Network Management Card (NMC) contains a removable battery. If this battery is ingested, seek immediate medical attention.

⚠WARNING

HAZARD OF INTERNAL BURNS

- Do not ingest the battery.
- Keep batteries out of reach of children.

Failure to follow these instructions can result in serious injury or death.

Note: Secure the NMC to the UPS device's SNMP Slot using screws to keep the battery out of reach.

For the location of the UPS card slot, see the UPS documentation.

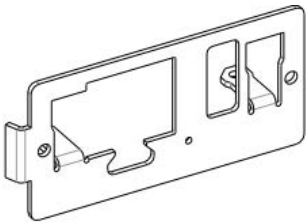
For some UPS devices with the SRV prefix, for example SRVPM10KRIL, you must screw an alternate bracket (pictured below) to the NMC before you insert the NMC into the Easy UPS. This is required because the original bracket does not fit these UPS devices.

Please refer to Knowledge Base article FA237786 for a list of UPS devices that require the alternate bracket.

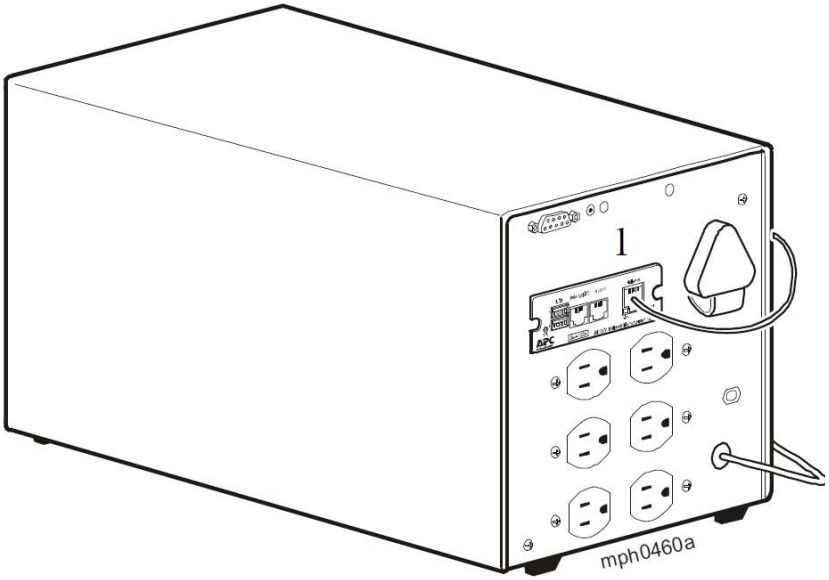
To install the alternate bracket:

1. Unscrew the original bracket attached to the NMC.
2. Screw the alternate bracket to the NMC.

A Torx T-8 screwdriver is required.



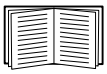
1. Locate the UPS card slot. Remove the slot cover or Network Management Card from the UPS card slot.
2. Use the same screws that hold the slot cover in place to secure the NMC in the UPS card slot.
3. Connect a network interface cable to the 10/100/1000Base-T network connector 1 on the NMC.
4. Open the provided ferrite bead and clip it around the network interface cable near the NMC's RJ45 connector.



NOTE: This image depicts a Smart-UPS and is used as an example only.

When the network interface cable is connected, the NMC will attempt to obtain an IP address via DHCP. See "TCP/IP Configuration Methods".

Step 2: Configure the Network Management Card



See "Quick Configuration".

Quick Configuration

Overview

Disregard the procedures described in this chapter if you have Data Center Expert as part of your system. See the documentation for your device for more information.

This chapter details how to configure the Network Management Card's (NMC) TCP/IP settings and configure its network protocols.

Configure TCP/IP Settings

You must configure the following TCP/IP settings before the NMC can operate on a network:

- IP address of the NMC
- Subnet mask
- Default gateway

If your network has a DHCP server, which most networks do, this is the easiest way to start configuring your NMC.Starting with DHCP has 2 advantages:

1. The user-friendly Web UI allows you to configure settings and enable protocols.
2. DHCP will correctly set the subnet mask and default gateway. Misconfiguration of these settings can be difficult to diagnose.

If a default gateway is unavailable, use the IP address of a computer that is located on the same subnet as the NMC and that is usually running. The NMC uses the default gateway to test the network when traffic is very light.

Do not use the loopback address (127.0.0.1) as the default gateway address for the NMC. It disables the card and requires you to reset TCP/IP settings to their defaults using a local serial login.

See "Watchdog Features" in the NMC User Guide for more information about the watchdog role of the default gateway.

TCP/IP Configuration Methods

When you first connect the Ethernet cable, the Link-RX/TX LED (

) will illuminate either green or yellow. Network activity will cause the LED to flicker.

The Status LED () will alternate between green and orange until the NMC has acquired an IP address via DHCP, and it will then stay solid green.

If the Status LED is solid green after 1-2 minutes, your network has a DHCP server, and the NMC has received an IP address from the DHCP server. You can retrieve the NMC's acquired IP address using the below methods:

- "Retrieve IP Address via Local Command Line Interface"
- "Device IP Configuration Wizard"

If the Status LED is still alternating between green and amber after ~3 minutes, your network does not have a DHCP server or the NMC was not able to contact the server. You can configure the TCP/IP network settings using the below method:

- "Configure IP Address via Local Command Line Interface"

When you know the NMC's IP address and have access to the NMC, you can re-configure the IP address using the below methods:

- "DHCP and BOOTP Configuration"
- ".INI File Utility"

Retrieve IP Address via Local Command Line Interface

Use a computer that connects to the Network Management Card through the USB virtual serial port too access the local command line interface. For a Mac device, use Terminal. For a Windows PC:

1. In Windows Search, type “Device Manager”, or open it from the Control Panel. Open “Ports (COM & LPT)”.
2. Connect the provided micro-USB cable (part number 960-0603) from the console port on the NMC to a USB port on the computer.
3. Note the COM port number that was added when you connected the micro-USB cable. For example, “USB Serial Device (COM7)”.

4. Run a terminal emulator program (e.g. HyperTerminal, PuTTy, or Tera Term) and connect to the COM port number noted in step 3. It is not necessary to configure the port.
5. Press ENTER, repeatedly if necessary, to display the **User Name** prompt.
6. Use **apc** for the **user name** and **password**.

   NOTE: The user name will be “apc” at first log for the Super User account. You will be prompted to enter a new password after you log in.

NOTE: A driver is required to connect to the NMC console via Windows 7. The driver can be downloaded from the NMC product pages on the APC website, located in the **Software / Firmware** section. No driver is required for Windows 10.

1.When you connect the NMC via the micro-USB cable, a device called “NMC3-CDC” is discovered in “Other Devices”.

2.Right-click on this device and select “Update Driver Software...”

3.Select the “Browse my computer for driver software” option and navigate to the download location of the driver (usb_cdc_ser.inf).

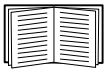
4.Accept the unsigned driver security message.

Windows will now recognize the NMC and assign a COM port to the device.

If the micro-USB cable is left connected to the NMC, the NMC will wait 15 seconds at each boot up to access the Boot Monitor. To avoid this 15 second boot delay, disconnect the micro-USB cable if local access to the CLI is not required.

After you log in to the CLI, you can retrieve the NMC's IP address or manually configure the NMC's network settings. To retrieve the DHCP assigned IP address:

1. Type `tcpip` and press ENTER.
2. The active IP address, subnet mask, and default gateway will be displayed.



See "How to Access a Configured Network Management Card" to finish the configuration.

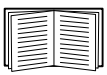
Device IP Configuration Wizard

The Device IP Configuration Wizard is useful in one of two situations:

1. **Unconfigured NMCs:** By default, an unconfigured NMC will send DHCP requests. The Device IP Configuration Wizard functions as a constrained DHCP server that only responds to APC/Schneider Electric MAC addresses and it can be used to assign an IP address, subnet mask, and gateway information to an unconfigured NMC.
2. **Configured NMCs with SNMPv1 enabled and configured with the Community Name set to "public":** By entering an IP range to define the search, the Wizard scans the IP addresses in the defined range and discovers and reports NMCs. The Wizard can then list the MAC address, IP address, device description, and firmware version of an NMC and allow the table to be printed.

   The NMC IP address will be displayed with an HTTP prefix. If the NMC is configured to use HTTPS, the prefix must be updated from `http` to `http`**`s`**. For more information on SNMPv1, see the User Guide.

NOTE: The Device IP Configuration Wizard is not useful for NMCs with an IP address that do not have SNMPv1 enabled and configured.



For detailed information on the Wizard, see Knowledge Base article FA156064 on the APC website.

To use the DHCP Option 12, see Knowledge Base article FA156110.

System requirements

The Wizard runs on Microsoft Server® 2012, Windows Server 2016, Windows Server 2019 and on both 32- and 64-bit versions of Windows 8.1 and Windows 10 operating systems.

This Wizard is for IPv4 only.

Installation

To install the Wizard from a downloaded executable file:

1. Go to www.apc.com/tools/download.
2. Under the **Software** tab, select **Tools and Resources** > **Software and Firmware downloads**.
3. Search the Network Management Device IP Configuration Wizard and download the file.
4. Open the folder where you downloaded the Wizard, and run the executable file.

When installed, the Wizard is available through the Windows “Start Menu” option.

See “How to Access a Configured Network Management Card” to finish the configuration.

Configure IP Address via Local Command Line Interface

Use a computer that connects to the Network Management Card through the USB virtual serial port too access the local command line interface:

1. In Windows Search, type “Device Manager”, or open it from the Control Panel. Open “Ports (COM & LPT)”.
2. Connect the provided micro-USB cable (part number 960-0603) from the console port on the NMC to a USB port on the computer.
3. Note the COM port number that was added when you connected the micro-USB cable. For example, “USB Serial Device (COM7)”.

4. Run a terminal emulator program (e.g. HyperTerminal, PuTTy, or Tera Term) and connect to the COM port number noted in step 3. It is not necessary to configure the port.
5. Press ENTER, repeatedly if necessary, to display the **User Name** prompt.
6. Use **apc** for the **user name** and **password**.

   NOTE: The user name will be “apc” at first log for the Super User account. You will be prompted to enter a new password after you log in.

NOTE: A driver is required to connect to the NMC console via Windows 7. The driver can be downloaded from the NMC product pages on the APC website, located in the **Software / Firmware** section. No driver is required for Windows 10.

1.When you connect the NMC via the micro-USB cable, a device called “NMC3-CDC” is discovered in “Other Devices”.

2.Right-click on this device and select “Update Driver Software...”

3.Select the “Browse my computer for driver software” option and navigate to the download location of the driver (usb_cdc_ser.inf).

4.Accept the unsigned driver security message.

Windows will now recognize the NMC and assign a COM port to the device.

If the micro-USB cable is left connected to the NMC, the NMC will wait 15 seconds at each boot up to access the Boot Monitor. To avoid this 15 second boot delay, disconnect the micro-USB cable if local access to the CLI is not required.

To set a static IP address:

1. Contact your network administrator to obtain the IP address, subnet mask, and default gateway for the Network Management Card.
2. Use this command to configure network settings. (Text in italics indicates a variable.)

   `tcpip`

   `-i` *yourIPaddress*

   `-s` *yourSubnetMask*

   `-g` *yourDefaultGateway*

   For each variable, type a numeric value that has the format *xxx.xxx.xxx.xxx*.

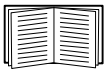
   The command can be entered on one line. For example, to set a system IP address of 156.205.14.141, a Subnet Mask of 255.255.255.0 and a default gateway of 156.205.14.1, type the following command and press ENTER:

   `tcpip -i 156.205.14.141 -s 255.255.255.0 -g 156.205.14.1`
3. Type `reboot`. The Network Management Card restarts to apply the changes.

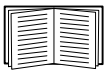
See “How to Access a Configured Network Management Card” to finish the configuration.

DHCP and BOOTP Configuration

The default TCP/IP configuration setting, **DHCP**, assumes that a properly configured DHCP server is available to provide TCP/IP settings to Network Management Cards. You can also configure the setting for BOOTP.



A user configuration (.ini) file can function as a BOOTP or DHCP boot file. For more information, see the TCP/IP configuration section of the Network Management Card User Guide.



If neither of these servers is available, see “TCP/IP Configuration Methods” to configure the needed TCP/IP settings.

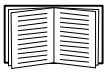
BOOTP

For the Network Management Card to use a BOOTP server to configure its TCP/IP settings, it must find a properly configured RFC951-compliant BOOTP server.

In the BOOTPTAB file of the BOOTP server, enter the Network Management Card’s MAC address, IP address, subnet mask, and default gateway, and, optionally, a bootup file name. Look for the MAC address on the bottom of the Network Management Card or on the Quality Assurance slip included in the package.

When the Network Management Card reboots, the BOOTP server provides it with the TCP/IP settings.

- If you specified a bootup file name, the Network Management Card attempts to transfer that file from the BOOTP server using TFTP or FTP. The Network Management Card assumes all settings specified in the bootup file.
- If you did not specify a bootup file name, you can configure the other settings of the Network Management Card remotely through its Web interface or command line interface; the **user name** and **password** are both **apc**, by default.



To create a bootup file, see your BOOTP server documentation.

DHCP

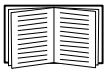
You can use an RFC2131/RFC2132-compliant DHCP server to configure the TCP/IP settings for the Network Management Card (NMC).

1. The NMC sends out a DHCP request that uses the following to identify itself:
   - A Vendor Class Identifier (APC by default)
   - A Client Identifier (by default, the MAC address of the NMC)
   - A User Class Identifier (by default, the identification of the application firmware installed on the NMC)
2. A properly configured DHCP server responds with a DHCP offer that includes all the settings that the NMC needs for network communication. The DHCP offer also includes the Vendor Specific Information option (DHCP option 43). The NMC can be configured to ignore DHCP offers that do not encapsulate the APC cookie in DHCP option 43 using the following hexadecimal format. (The card does not require this cookie by default).

```
Option 43 = 01 04 31 41 50 43
```

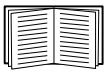
where

- the first byte (`01`) is the code
- the second byte (`04`) is the length
- the remaining bytes (`31 41 50 43`) are the APC cookie.



See your DHCP server documentation to add code to the Vendor Specific Information option.

The NMC Web interface has options to utilize vendor-specific data to require the DHCP server to provide an “APC” cookie which will supply information to the NMC. See the User Guide for information.



See “How to Access a Configured Network Management Card” to finish the configuration.

.INI File Utility

You can use the .INI file export utility to export .INI file settings from configured NMCs to one or more unconfigured NMCs. The utility and documentation are available on the APC website, and are also available in Knowledge Base article FA156117.

How to Access a Configured Network Management Card

Overview

After the UPS Network Management Card (NMC) is running on your network, you can use the interfaces summarized here: Web interface, Telnet, SSH, SNMP, FTP, and SCP. The Web interface is recommended for ease of configuration.

For more information about the interfaces, see the User Guide.

Web interface

The Network Management Card 3 Web interface is compatible with:

- Windows® operating systems:
  - The latest release of Microsoft® Edge®
- All operating systems:
  - The latest releases of Mozilla® Firefox® or Google® Chrome®

Other commonly available browsers may work but have not been fully tested by APC by Schneider Electric.

You can use either of the following protocols when you use the Web interface:

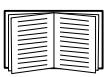
- By default, only HTTPS is enabled. The HTTPS protocol (enabled by default), which provides extra security through Secure Socket Layer (SSL); encrypts user names, passwords, and data being transmitted; and authenticates Network Management Cards by means of digital certificates.
- The HTTP protocol, which provides authentication by user name and password but no encryption.

  NOTE: HTTP is disabled by default. The first log in to the Web UI must be using the HTTPS protocol.

To access the Web interface and configure the security of your device on the network:

1. Address the Network Management Card by its IP address (or its DNS name, if a DNS name is configured). For example:

   `https://156.205.14.141`
2. Enter the user name and password (**apc**/**apc** by default).
3. If the NMC received an IP address via DHCP and you want to assign a static IP address to the NMC, navigate to **Configuration > Network > TCP/IP > IP v4 Settings**.
4. To enable or disable HTTPS, or enable HTTP, use the NMC Web interface.



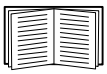
See the Security Handbook for more information on selecting and configuring network security.

Command Line Interface access - SSH and Telnet Access

You can access the command line interface through Secure SHell (SSH) or Telnet, depending on which is enabled. To enable these access methods, use the NMC Web interface. By default, only SSH is enabled.

SSH for high-security access. If you use the high security of SSL for the Web interface, use Secure SHell (SSH) for access to the command line interface. SSH encrypts user names, passwords, and transmitted data.

The interface, user accounts, and user access rights are the same whether you access the command line interface through SSH or Telnet, but to use SSH, you must first configure SSH and have an SSH client program installed on your computer.



See the User Guide for more information on configuring and using SSH.

To access the command line interface using SSH, at a command prompt enter:

```
ssh -c aes256-ctr <username>@<IP address>
```

NOTE: This SSH command is for OpenSSH. The command may differ depending on the SSH tool used.

Telnet for basic access. By default, Telnet is disabled. Telnet provides the basic security of authentication by user name and password, but not the high-security benefits of encryption. To use Telnet to access the command line interface of the Network Management Card from any computer on the same subnet:

1. At a command prompt, use the following command line, and press ENTER:

   `telnet` *address*

   As *address*, use the Network Management Card's IP address (or DNS name, if configured).

2. Enter the user name and password.

Simple Network Management Protocol (SNMP)

SNMPv1, SNMPv2c, and SNMPv3 are all disabled by default. You must configure community names in the Web UI before you can enable any version of SNMP.

To enable or disable SNMP access, you must be an Administrator. Use the NMC Web interface or Command Line interface to set it up.

SNMPv1 only. After you add the PowerNet® MIB to a standard SNMP MIB browser, you can use that browser to access the Network Management Card. All user names, passwords, and community names for SNMP are transferred over the network as plain text.

Use of SNMPv2c is supported by the SNMPv1 options.

SNMPv3 only. For SNMP GETs, SETs, and trap receivers, SNMPv3 uses a system of user profiles to identify users. An SNMPv3 user must have a user profile assigned in the MIB software program to perform GETs and SETs, browse the MIB, and receive traps.

To use SNMPv3, you must have a MIB program that supports SNMPv3.

The Network Management Card supports SHA or MD5 authentication and AES or DES encryption.

SNMPv1 and SNMPv3. To use Data Center Expert and EcoStruxure IT to manage the Network Management Card on the public network of an EcoStruxure IT system, you must have SNMPv1 enabled in the unit interface. Read access allows Data Center Expert and EcoStruxure IT to receive traps from the Network Management Card. Write access is required while you set Data Center Expert and EcoStruxure IT as a trap receiver.

SCP and FTP

You can use SCP or FTP to transfer downloaded firmware to the Network Management Card, or to access a copy of the Network Management Card's event or data logs.

NOTE: By default, only SCP is enabled. You can use SCP once you have used SSH or HTTPS to create a user password.

To use Data Center Expert to manage the UPS, you must have the **FTP Server** option enabled in the Network Management Card interface.

To enable or disable FTP server access, you must be an Administrator. Use the NMC Web interface or Command Line interface to set it up.

To transfer firmware, see the User Guide.

The SCP interface is enabled when SSH is enabled, as they are part of the same protocol suite. See the User Guide for more information on configuring and using SSH.

To retrieve a copy of the event or data log, see the User Guide.

Manage the security of your system

For detailed information on enhancing the security of your system after installation and initial configuration, see the Security Handbook.

How to Reset after a Lost Password

NOTE: Resetting your NMC will reset the card to its default configuration.

If you forget your password, you must use the **Reset** button on the NMC to wipe all configuration, including the password. Hold down the **Reset** button for 20-25 seconds, ensuring the Status LED is pulsing green during this time. When the Status LED changes to amber or orange, release the **Reset** button to allow the NMC to complete its reboot process.

After the NMC reboots, you must re-configure your NMC. See “Quick Configuration”.

It is recommended you export the .ini file after configuring your NMC to prevent loss of data in the event of a lost password. See “Retrieving and Exporting the .ini File” in the NMC User Guide for more information.

Specifications AP9544

Physical	
Size (H x W x D)	44 x 80 x 52 mm (1.7 x 3.1 x 2.1 in)
Weight	0.05 kg (0.10 lb)
Shipping weight	0.30 kg (0.66 lb)

Environmental	
Elevation (above MSL)	
Operating	0 to 3000 m (0 to 10,000 ft)
Storage	0 to 15 000 m (0 to 50,000 ft)
Temperature	
Operating	-5 to 45°C (32 to 113°F)
Storage	-15 to 65°C (5 to 149°F)
Operating humidity	0 to 95%, non-condensing

Regulatory compliance	
Emissions	FCC Class A, ICES-003, Issue 6, Class A, VCCI Class A, AS/NZS, CISPR 32 Class A
Immunity	EN 55024, BS EN 55024, EN 61000-4-2, BS EN 61000-4-2, EN 61000-4-3, BS EN 61000-4-3, EN 61000-4-4, BS EN 61000-4-4, EN 61000-4-5, BS EN 61000-4-5, EN 61000-4-6, BS EN 61000-4-6, EN 61000-4-8, BS EN 61000-4-8, EN 61000-6-2, BS EN 61000-6-2, EN 62040-2, BS EN 62040-2

Specifications AP9547

Physical	
Size (H x W x D)	44 x 80 x 66 mm (1.7 x 3.1 x 2.6 in)
Weight	0.05 kg (0.10 lb)
Shipping weight	0.30 kg (0.66 lb)

Environmental	
Elevation (above MSL)	
Operating	0 to 3000 m (0 to 10,000 ft)
Storage	0 to 15 000 m (0 to 50,000 ft)
Temperature	
Operating	-5 to 45°C (32 to 113°F)
Storage	-15 to 65°C (5 to 149°F)
Operating humidity	0 to 95%, non-condensing

Regulatory compliance	
Emissions	FCC Class A, ICES-003, Issue 6, Class A, VCCI Class A, AS/NZS, CISPR 32 Class A
Immunity	EN 55024, BS EN 55024, EN 61000-4-2, BS EN 61000-4-2, EN 61000-4-3, BS EN 61000-4-3, EN 61000-4-4, BS EN 61000-4-4, EN 61000-4-5, BS EN 61000-4-5, EN 61000-4-6, BS EN 61000-4-6, EN 61000-4-8, BS EN 61000-4-8, EN 61000-6-2, BS EN 61000-6-2, EN 62040-2, BS EN 62040-2

Copyright Notices

Cryptlib Cryptology Library

Cryptlib copyright © Digital Data Security New Zealand Ltd 1998.

Berkeley Database

Copyright © 1991, 1993 The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that thefollowing conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANYWAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Lua

Radio Frequency Interference

Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

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. APC 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.

Worldwide Customer Support

Access to customer support terms may vary by product. Customer support is available in the following ways:

- Visit the Schneider Electric Web site to access documents in the Schneider Electric Knowledge Base and to submit customer support requests.
  - **www.schneider-electric.com** (Corporate Headquarters)
    Connect to localized Schneider Electric Web sites for specific countries, each of which provides customer support information.
  - **www.schneider-electric.com/support/**
    Global support searching Schneider Electric Knowledge Base and using e-support.
- Contact the Schneider Electric Customer Support Center by telephone or mail.
  - Local, country-specific centers: go to **www.schneider-electric.com > Support > Operations** around the world for contact information.

For information on how to obtain local customer support, contact the representative or other distributors from whom you purchased your product.

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

Schneider Electric
Stafford Park 5
Telford
United Kingdom
TF3 3BL

990-6521E-001 **05/2025**